Study Guide

Application of the MITRE ATT&CK Framework

Created By: Pratyay Milind, Teaching Assistant

Module 1: Course Introduction

Lesson 1.1: Course Overview

Skills Learned From This Lesson: Objectives, Pre Requisites, Target Audience

- Course Objectives
    - What is the MITRE Attack Framework?
    - What is:
        - Initial Access
        - Execution
        - Persistence
        - Privilege Escalation
        - Defense Evasion
        - Credential Access
        - Discovery
        - Lateral Movement
        - Collection
        - Command and Control
        - Exfiltration
        - Impact

Lesson 1.2: What is the MITRE ATT&CK Framework?

Skills Learned From This Lesson: Definition, Framework, Enterprise

- What is the MITRE ATT&CK Framework?
    - What is
        - Per MITRE:
            - MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a

foundation for the development of specific threat models and methodologies in the private sector, in government, and the cybersecurity product and service community.

- With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

  - ATT&CK Matrix for Enterprise
    - https://attack.mitre.org/

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-Stage Channels
	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	Launchctl	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	Kerberoasting	Remote System Discovery	SSH Hijacking	Screen Capture		Multiband Communication
	Local Job Scheduling	Create Account	Image File Execution Options Injection	DLL Side-Loading	Keychain	Security Software Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	Disabling Security Tools	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
		External Remote		Exploitation for Defense		System Network				

Lesson 1.3: Where is the MITRE ATT&CK Framework Being Used?

Skills Learned From This Lesson: Red Teams, Blue Teams, Vendors

- Red Teams
  - Can use the Framework as a common ground for communication and research
  - Can use the Framework as a common ground for Training
  - Can use the Framework as a guide for systems testing
- Blue Teams

    - Can use the Framework to identify common attack vectors
    - Can use the Framework to potentially backtrack (find the point of entry)
    - Can use the Framework to assist in the implementation of compensating or mitigating controls
- Vendors
    - Allows vendors to clearly define where their solution provides prevention or detection measures
        - This allows consumers to know if a product is overlapping with another
        - This can be beneficial in eliminating the cost and improving control coverage throughout an environment
    - Red Teams can conduct proof of concept attacks against the solution knowing what it should defend against

Lesson 1.4: Navigation and Review
Skills Learned From This Lesson: Components, Navigation, Review

- Website » https://attack.mitre.org/

Module 2: Initial Access

Lesson 2.1: What is Initial Access?
Skills Learned From This Lesson: Definition, Techniques, Examples

- What is Initial Access?
    - Consists of techniques that an adversary would use to get into your network. This can be anything from Spear-phishing to the exploitation of public-facing web servers or services.
- Techniques as Defines by MITRE ATT&CK Framework
    - Drive-by Compromise
    - Exploit Public-Facing Application
    - External Remote Services
    - Hardware Additions
    - Replication Through Removable Media
    - Spear phishing Link
    - Spear phishing via Service
    - Supply Chain Compromise
    - Trusted Relationship

    - Valid Account
- Attack Example
    - Supply Chain Compromise
        - CCleaner compromised by hackers for over a month, the tool was impacted by malware that gave attackers a backdoor to the user's system (2.27 million downloads)
        - Mobile games such as Infestation and Point Blank were identified by Kaspersky and ESET as having backdoored version of the game being distributed.

Lesson 2.2: External Remote Services

Skills Learned From This Lesson: Definitions, Mitigation Techniques, Detection Techniques

- External Remote Services
    - External Remote Services are manners in which an organization can remotely manage or access otherwise protected systems.
    - This can include:
        - VPNs
        - Remote Desktop
        - SSH
        - Telnet
- Linux Rabbit and Rabbit
    - A malware made for install cryptocurrency miners that could not carry out attacks in restricted geolocations
    - The malware is broken into four main functions:
        - Establish Command and Controls server (Using TOR)
        - Setup Persistence
            - Using rc.local files and bashrc files
        - SSH brute force
        - Install the cryptocurrency miner
- OilRig
    - OilRig is an APT group that has been noted as having ties to Iran. Also known as APT34 and HelixKitten.
    - Targets governmental agencies and businesses in:

        - Financial
        - Energy
        - Chemical
        - Telecommunications
    - Primarily Known For:
        - DNS Tunneling and using tools such as Glimpse, PoisonFrog and Hypershell.
- Mitigation Techniques
    - Disable or Remove Features
    - Limit Access to resources over connections such as VPNs
    - Multi-Factor Authentication
    - Network Segmentation
- Detection Best Practices
    - Use some form of log collection
        - Authentication logs
    - Looks for unusual access attempts
        - Focus on Business Hours
        - Abnormal, none business-related, activities

Lesson 2.3: Spear phishing Link

Skills Learned From This Lesson: Definitions, Mitigation Techniques, Detection Techniques

- Spear phishing Link
    - An attempt by an attacker to have a victim use a link to download malware instead of using attachments or to send them to a malicious site to attempt to steal credentials / access.
    - The spear phishing technique uses similar social engineering methods that require the user interact with the content to execute the payload.
    - Example:
        - www.<yourbank>.com is actually (https://yourbank.com/account?redirectURL=https://evilsite.com/account)
- Turls (Waterbug) (https://attack.mitre.org/groups/G0010/)

    - A Russian based group that has impacted organizations in over 45 countries. Known for watering hole and Spear phishing campaigns.
    - Targets Include:
        - Government
        - Embassies
        - Military
        - Education
        - Research and Pharmaceutical
- Mitigation Techniques
    - Restrict the sites that user can visit to those necessary to conduct business operations
    - Implement end user awareness training
- Detection Techniques
    - Email URL Inspection
    - Block and alert on known malicious site access attempts (not helpful for new sites)
    - Have a system in place for users to report suspicious emails.

Lesson 2.4: Supply Chain Compromise Part 1
Skills Learned From This Lesson: Compromise, Examples, Mitigation, Detection

- Supply Chain Compromise
    - The manipulation of a product or products delivery mechanism prior to consumer receipt
    - Can include but is not limited to:
        - Hardware manipulation
        - Pre-installed malware (phones, cameras)
        - Signed malicious apps using the identity of the trusted company
- Examples:
    - Supply Chain Compromise
        - CCleaner compromised by hackers for over a month, the tool was impacted by malware that gave attackers a backdoor to the user's system (2.27 million downloads)

    - Mobile games such as Infestation and Point Blank were identified by Kaspersky and ESET as having backdoored version of the game being distributed.
- Article:
    - https://threatpost.com/avast-network-breached-as-hackers-target-ccleaner-again/149358/

Lesson 2.5: Supply Chain Compromise Part 2
Skills Learned From This Lesson: Compromise, Examples, Mitigation, Detection

- Mitigation
    - Look for unused dependencies
    - Look at previously vulnerable dependencies
    - Remove unnecessary components
    - Use manual or automatic code review
    - Check for anomalous network activity
- Detection Techniques
    - Use verification methods such as integrity or hash checking mechanisms
    - Run software prior to full installation and look for potentially malicious activity
    - Inspect hardware for potentially malicious components

Lesson 2.6: Trusted Relationship
Skills Learned From This Lesson: Trusted Relationships, Examples, Mitigation, Detection

- Trusted Relationship versus Supply Chain Compromise
    - A trusted relationship leverages the access a third party has to the potential victims' system where a Supply Chain Compromise involves the manipulation of trusted tools or code that is then delivered to the victims environment.
    - Trusted Relationship = Direct Access to Systems or Data
    - Supply Chain Compromise = Access after the victim install a malicious update or uses infected hardware
    - Look at previously vulnerable dependencies
- Managed Service Provider Example

    - Hackers working for China broke into networks of eight major MSPs and technology service providers, based on a Reuters report.
    - These attacks lead to damages in areas such as:
        - Banking
        - Telecommunications
        - Medical Equipment
        - Packaging
        - Manufacturing
        - Consulting
        - Healthcare
        - Biotechnology
        - Automotive
- Mitigation Techniques
    - Look to implement proper network segmentation
    - Keep the timeframe and permission sets that third parties use limited
- Detection Techniques
    - Monitor activity of designated third-party accounts (not using the third-party controls)
    - Implement Network and Endpoint Monitoring tools that can report on anomalous activity

Lesson 2.7: Valid Accounts Part 1
Skills Learned From This Lesson: Definition, Mitigation, Detection

- What is / are valid accounts
    - Valid accounts are accounts used by users or services in an organization. Threat actors steal account information in a variety of ways and then use those credentials to later gain initial access to an organization.
    - Accounts can fall into the given categories:
        - Default – Built into a system
        - Local – Single system accounts
        - Domain Accounts – Managed by a central server and provide access across systems connected to the domain

- Review of Statistics
    - Varonis 2018 – 65% of Companies have over 1,000 stale user accounts
    - Blackhat 2017 – 32% of black hat hackers admit privilege accounts are the numbers one way to gain access to critical data
    - 2019 Verizon DBR – 80% data breaches caused by compromised and weak credentials, 29% involve the use of stolen credentials

Lesson 2.8: Valid Accounts Part 2
Skills Learned From This Lesson: Definition, Mitigation, Detection

- Mitigation Activities
    - Enforce password policies that require complex and unique passwords across all systems
    - When possible implement multi-factor authentication, it has been found that this can greatly reduce the risk of account compromise
    - Ensure that defaults accounts are notes and changes on all network and end user systems
    - Properly review privileged and standard user accounts on a regular basis
- Detection Activities
    - Implement a system that can alert on suspicious account behavior across systems
        - Multiple logins at one time across several systems
    - Look for accounts that were recently enabled or changed from a disabled state
    - Look for login activity from users that is suspicious or not possible

Lesson 2.9: Initial Access Case Study
Skills Learned From This Lesson: Case Study, Initial Access, Mitigation

- HSBC Discloses a “Security Incident”
    - The Notification Letter
        - What Happened?
            - HSBC became aware of online accounts being accessed by unauthorized users between October 4, 2018 and October 14, 2018. When HSBC discovered your online account was impacted, we suspended online access to prevent further unauthorized entry of your account. You may have received a call or email from us so

we could help you change your online banking credentials and access your account. If you need help accessing your account, please call <>. We apologize for this inconvenience. HSBC takes this very seriously and the security of your information is very important to us.

- What Information Was Involved
  - The information that may have been accessed includes your full name, mailing address, phone number, email address, date of birth, account numbers, account types, account balances, transaction history, payee account information, and statement history where available.

- What Should've Been Done?
  - Sources indicated that credential stuffing was a likely reason that the accounts were compromised.
    - This is when an attack uses a combination of usernames and passwords, which may have been obtained from a previous breach.
  - In the MITRE Framework, which Initial Access vector most suites this scenario, and would the mitigating factors under that vector have prevented or reduced the risk of compromise?
  - While a sensitive question, do the users of the bank have any culpability if they reused credentials?

Lesson 2.10: Module 2 Summary

Skills Learned From This Lesson: Summary, Module, Initial Access

- What is Initial Access
  - Defined Initial Access
  - Defined some attack types and examples
- External Remote Services
  - Defined what External Remote Services are
  - Reviewed Linux Rabbit
  - Reviewed OilRig
  - Reviewed Mitigation techniques
  - Reviewed Detection best practices
- Spear Phishing Link

    - Defined what a Spear Phishing Link is
    - Looked at Turla (Waterbug)
    - Reviewed Mitigation Techniques
    - Reviewed Detection Techniques
- Supply Chain Compromise
    - Described a Supply Chain Compromise
    - Reviewed examples
    - Reviewed Mitigation Techniques
    - What are some Detection Techniques
- Trusted Relationship
    - Reviewed differences between Trusted Relationship versus Supply Chain Compromise
    - Reviewed example (Managed Service Providers)
    - Reviewed Mitigation Techniques
    - Reviewed Detection Techniques
- Valid Accounts
    - Reviewed is/are valid accounts
        - Types of Accounts
        - Reviewed of statistics associated with Valid Accounts
        - Reviewed Mitigation Activities
        - Reviewed Detection Activities
- Initial Access Case Study
    - Reviewed and should have been able to apply MITRE Attack Framework Controls to the Scenario

Module 3: Execution

Lesson 3.1: What is Execution?

Skills Learned From This Lesson: Definition, Execution, Examples

- What is Execution?
    - This is the phase after Initial Access where an adversary is trying to run malicious code. Attackers will use this phase to do things such as:
        - System discovery
        - Network discovery
        - Start the process of stealing data

Lesson 3.2: What is Execution?

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Command-Line Interface - (https://attack.mitre.org/techniques/T1059/)
    - A manner that provides a way to interact with a computer system. Some examples of command line interfaces include:
        - Windows (DOS)
        - OS X (Bash Shell)
        - Linux (Bash Shell)
- Goal
    - To Remotely control the target system
        - To Execute changes to the target system
        - To install other tools
- Mitigation Techniques
    - Restrict user accounts to not allow for elevated command prompts
    - Block non-essential or unnecessary command line interpreters
- Detection Techniques
    - Ensure that security solutions or activities are logging process execution with command-line arguments.

Lesson 3.3: Execution Through API

Skills Learned From This Lesson: Tools, Mitigation, Detection

- Execution Through API
    - These attacks involve the use of tools that may directly use the Windows application programming interface (API) to execute binaries.
    - Some examples of API calls that can be used to execute binaries include:
        - CreateProcessA() and CreateProcessW()
        - CreateProcessAsUserA() and CreateProcessAsUserW()
        - LoadLibraryExA() and LoadLibraryExW()
        - LoadModule()
- Tools Used
    - BOOSTWRITE Loader
        - A loader created to be launched via abuse of the DLL search order of applications. The Application loads several libraries and finally loads ‘Dwrite’. This causes the import of a malicious dll that is then used to load an instance of the CARBANAK backdoor.
    - RFSNIFFER Module

        - Loaded by BOOSTWRITE it will hook WIN32 API functions and can be used to hijack elements of NCR Aloha Command Center. There is also a backdoor component that enables it to inject commands into an active RDFClientSession.
- Mitigation Techniques
    - Identify and block malicious payloads or software through execution prevention methods.
- Detection Techniques
    - Utilize intrusion prevention and detection systems to correlate events surrounding potentially malicious behavior involving Windows API.

Lesson 3.4: Control Panel Items

Skills Learned From This Lesson: Definition, Methods, Mitigation, Detection

- Control Panel Items
    - The items used in Windows to allow users to view and adjust system settings. They are registered as executables (.exe) or Control Panel (.cpl) files.
    - These items can be executed from the command line, via an API, or through interaction with the file.
    - These file have been used as execution payloads to run arbitrary commands.
    - Common delivery method of malicious control panel items is done through Spearphishing attachments or through multi-stage malware.
- Method for Attacking
    - Could be popular when environments have defenses in place such as application whitelisting and process whitelisting.

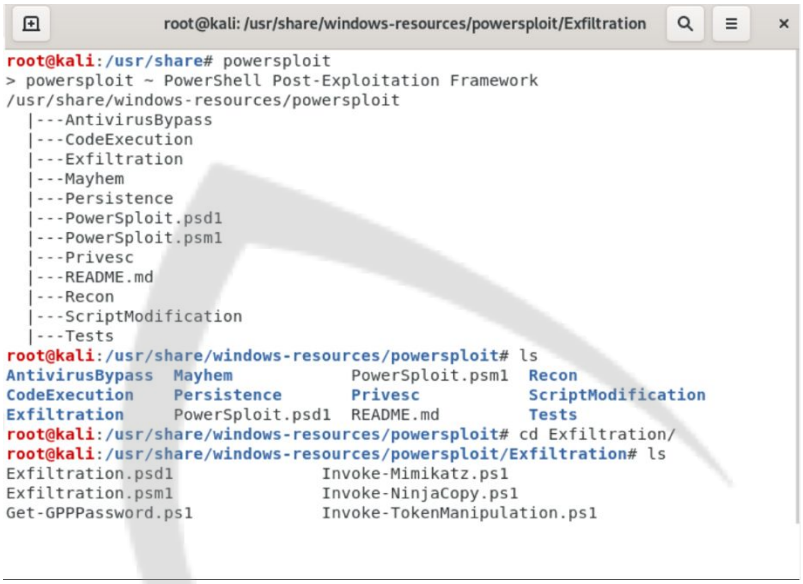
- Mitigation Techniques
    - Execution prevention can still be obtained through means such as antivirus.
        - If the payload calls out to a known malicious IP or System, then the connection can be blocked.
        - Control Panel Items can be protected and restricted.
- Detection Techniques

- Items related to or associated with CPL files can be monitored and analyzed with monitoring tools.
  - Control_RunDLL
  - ControlRunDLLAsUser
- An inventory of control panel items can be conducted to attempt to find unregistered or potentially malicious files.

Lesson 3.5: PowerShell

Skills Learned From This Lesson: Definition, Mitigation, Detection

- PowerShell
  - PowerShell is an interactive command-line and scripting environment included in the Windows Operating System.
  - PowerShell can be used to download and run executables, which can then be run on the disk or in memory.
  - Offensive Tools Include:
    - Empire
    - PowerSploit
    - PSAttack
- What can you do with it?
  - PowerShell Scripts Installed as Services
    - This allows the threat actor to work in a manner that could evade detection by posing as a legitimate part of the operating system
  - Using Malicious Macros to Launch run commands or scripts in the background
    - Typically starts with the user interacting with malicious email attachments
  - Injecting Malicious Code Into Memory
    - This Provides a means for threat actors to evade antivirus systems
  - PowerSploit
    - Can be found in the Kali Linux Distribution
      - Series of Microsoft PowerShell scripts that can be used in post-exploitation



- Mitigation
  - Use code signing to only allow PowerShell to execute signed scripts
  - Remove the PowerShell features from the system, only after confirm how this will impact administration and if there are any dependencies
  - Only allow PowerShell execution as an administrator
- Detection
  - Look for changes to execution policy, this is typically performed by threat actors looking to use PowerShell
  - If your environment does not use PowerShell then the use of the tool should be reviewed
  - Take advantage of the logging capabilities, this can assist security teams in gathering PowerShell execution details

Lesson 3.6: Scripting

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Scripting
  - Scripts are used to perform multiple actions in a quick and automated manner. This provides the following advantages:
    - Reduced time to gain access to resources

        - Can potentially bypass monitoring mechanisms
        - Can be ran without the end user's knowledge
    - Common languages in Windows include VBScript, PowerShell, and batch scripts.
- Uses for Scripting
    - Threat actors can embed scripts inside of Office documents using macros once the file is interacted with
    - Scripting can be used for information gathering prior to the threat actor using the system
    - Scripting can be used to silently install applications and then run commands from those applications
    - Metasploit
        - A Security tool that can also be used by threat actors, Metasploit can be installed on both Linux and, Mac OS X, and Windows based systems.
        - Provides capabilities to include:
            - Information Gathering Capabilities
            - Vulnerability Validation
            - Built in Exploits
            - Ability to add custom exploits
- Mitigation
    - Enable capabilities that allow for the sandboxing and blocking of macros
    - Disable, remove, or restrict access to scripting engines
- Detection
    - Log any attempts made by standard users to run scripts
    - Monitor command line arguments for script execution
    - Monitor/alert on scripts that spawn unusual processes:
        - Word Document that attempts to run powershell.exe

Lesson 3.7: User Execution

Skills Learned From This Lesson: Definition, Mitigation, Detection

- User Execution
    - The reliance on an end user to perform a specific action in order to gain execution. That can be things such as:
    - Direct code execution
        - Opening malicious executables
    - Code Execution through links
        - Browser or application exploits
- Common Methods

    - Drive-by Compromise
        - Threat actors gain access by having a user visit a website that has infected ads or other functions of the site.
    - Spearphishing Attachments
        - Uses malware that is attached to an email. Users must interact with the attachment to execute the payload.
    - Spear Phishing Links
        - Users must interact with a link sent via email that then downloads the malware.
- Common File Types
    - Word Processing Document (.doc)
    - Portable Document Format (.pdf)
    - Microsoft Excel (.xls)
    - Rich Text Format (.rtf)
    - Executable (.exe)
    - Control Panel (.cpl)
- Mitigation Techniques
    - Execution prevention of executables
    - Use of antivirus to stop known bad files from running
    - Network Intrusion Prevention to block known bad activity
    - Restrict web content and prevent users from visiting known bad sites
    - End User Awareness Training
- Detection Techniques
    - Monitor for the execution of command line arguments
    - Monitor hits on Antivirus and have a security team member review activity pre and post alert

Lesson 3.8: Execution Case Study

Skills Learned From This Lesson: Case Study, Example, Execution

- "Living Off The Land"
    - Symantec 2019 Internet Security Threat Report (pg.17)
        - At the time of this report PowerShell attacks had increased by 1000%, based on those that were blocked in 2018 on the endpoint.
        - At the time of this report Microsoft Office files accounted for almost half (48%) of all malicious email attachments, previously in 2017 this had only been 5%.

        - Groups such as Mealybug and Necurs were identified as preferring to use macros in Office files as their preferred method to propagate payloads.
        - It was noted that on average 115,000 malicious PowerShell scripts were blocked each month, only accounting for less than 1% of PowerShell use.
- Living Off The Land (LotL)
    - The Concept that an attacker uses pre-installed and trusted system tools to carry out their work.
        - There are many tools within Windows that can be used to carry out Cyber Attacks
        - Growth in Lot activity is in part from a reduction in the availability of zero-day vulnerabilities, plus it takes a lot of work to find them. (Silver Bullets)
    - Tools Include:
        - PowerShell Scripts
        - VB Scripts
        - WMI
        - PsExec
- How is This Being Addressed in Your Organization?
    - Consider your current controls, do you feel confident they could catch anomalous activity?
    - Aside from the tools mentioned, what other ways could you see an attacker LotL?

Lesson 3.9: Module 3 Summary
Skills Learned From This Lesson: Summary, Example, Execution

- Summary of what was covered in this module.

Module 4: Persistence

Lesson 4.1: What is Persistence?
Skills Learned From This Lesson: Definition, Persistence, Examples

- Persistence
    - When a threat actor attempts to maintain access to the environment, also known as a foothold.
    - Threat Actors commonly attempt to maintain access after:
        - Restarts
        - Changes to Credentials

        - Changes to the Network
    - This can include things like the replacement of legitimate code or adding items to the startup tasks.
- What Will We Be Looking At?
    - Accessibility Features
    - Bootkit
    - Browser Extension
    - Component Firmware
    - Create Account
    - Hooking
    - New Service

Lesson 4.2: Accessibility Features

Skills Learned From This Lesson: Definition, Methods, Examples, Mitigation, Detection

- Accessibility Features
    - Windows contains features that can be launched with key combinations before a user logs into a system. Threat Actors have the capability to modify the way these accessibility features launch to get a command prompt or backdoor without having to log into the system.
- Common Attack Methods
    - Threat actors have a number of ways they can manipulate the accessibility features. A few noted are:
        - Using sticky-keys to obtain unauthenticated, privileged console access
        - Threat actors have replaced binaries associated with the sethc.exe to establish persistence
        - Sticky Keys replacement within RDP sessions to obtain persistence
            - This can also be used to bypass the RDP login screen on remote systems
        - WMI debugging has been used to remotely replace binaries like sethc.exe, Utilman.exe, and Magnify.exe with cmd.exe
- Sticky Keys on RDP
    - In understanding these types of attacks it's beneficial to break down a simplified version of how the RDP exploit works.
        - Threat actor would have to replace the Sethc.exe (sticky Keys) to spawn cmd.exe

        - This means even if the account is removed the system still allows you to spawn the command prompt as SYSTEM
    - Threat actor opens an RDP session to the server and uses an invalid user to stay on the screen
    - The Threat actor then hits Shift x 5 and it would then spawn a system level command prompt
- Mitigation Techniques
    - Use some form of execution prevention like antivirus, whitelisting tools, etc.
    - Limit Access to resources over the network and if remote connections are allowed, access to the internal network should be even more limited
    - Utilize Network Level Authentication prior to giving a user the session to login to the network, this is especially important with RDP as the user must provide legitimate credentials prior to being given a session to log in to
- Detection Techniques
    - Any changes made to accessibility utility binaries should be reviewed
    - Changes to the paths of these utilities should be reviewed as well

Lesson 4.3: Bootkit

Skills Learned From This Lesson: Definition, Usage, Mitigation, Detection

- Bootkits
    - A bootkit is malware that modifies the boot sector of a hard drive impacting areas such as:
        - The Master Boot Record (MBR)
        - The Volume Boot Record (VBR)
    - This is a persistence mechanism that exists below the operating system and these types of tools are typically difficult to remediate.
    - Bootkits Include:
        - Rockboot
        - BootRash
- Use cases of Bootkits
    - Changes to the Master Boot Record
        - A threat actor can make changes to the MBR, which is the section of the disk that is first loaded after completion of hardware initiation by the BIOS. This can result in the actor diverting normal startup execution to malicious code.
    - Changes to the Volume Boot Record

        - The MBR passes control of boot processes to the VBR. Much like the changes made to the MBR, an adversary can divert execution during startup to malicious code.
- Mitigation Techniques
    - Utilize some form of boot integrity. Use the Trusted Platform Module technology and trusted boot processes.
    - Ensure that least privilege is properly implemented within the environment to make the job of installing a Bootkit harder for the threat actor.
- Detection Techniques
    - Perform checks on the MBR and VBR
        - Compare the checks to known good samples
        - Changes to either should be report and reviewed

Lesson 4.4: Browser Extension

Skills Learned From This Lesson: Definition, Usage, Mitigation, Detection

- Browser Extension
    - Browser Extensions, or plugins, are programs that can add function and customization to internet browsers.
    - Malicious extensions can be installed through malicious application downloads that seem legitimate, through social engineering, or through some phase of an already installed malicious payload.
    - Functions of Malicious Extensions Include:
        - Website browsing in the background
        - Stealing information a user inputs into the browser
        - Command and Control Purposes
        - For the installation of other tools such as RATs (Remote Access Tools)
- Kimsuky and Google Chrome
    - Information indicates that the group has been active since September 2013.
    - A report released December 5th 2018 indicated that the APT infected systems using a Google Chrome extension to infect systems, steal passwords, and cookie information from browsers.
    - Several phishing campaigns were conducted using the extension on the academic sector, with no information on the victims provided.
    - A part of the attack may have been motivated by the research the academics were doing in their given fields such as biomedical engineering.
- Mitigation Techniques
    - Set extension white or blacklists as appropriate for the business security policy

- Do not allow the installation of software by standard user accounts, practice least privilege
- Implement regular end user awareness training, covering such attack methods

- Detection Techniques
  - Audit web browser extensions to ensure that the ones installed are for business purposes and that they are not masquerading as legitimate ones
  - Network monitoring tools can be used to look for communication with a Command & Control server.
  - Monitor for new files written to the Registry or Portable Execution
  - files written to disk.

Lesson 4.5: Component Firmware

Skills Learned From This Lesson: Definition, Usage, Mitigation, Detection

- Component Firmware
  - Considered a sophisticated means to compromise a computer component, the technique is like System Firmware but takes advantage of system components that may not have the same capability. Malicious device firmware can provide a persistent level of access.
- Use cases of Component Firmware
  - There are several means when component firmware could be a likely avenue for attackers.
    - LoJaxand Hacking Team UEFI Rootkit
      - these are types of UEFI rootkits, and they are dangerous in that they have the capability to survive measures such as operating system reinstallation and a hard disk replacement.
    - Physical Tampering
      - With generic proof of concept backdoor firmware modules and the accessibility of tools has made it possible to install firmware rootkits in as little as 4 minutes of physical access.
    - Supply Chain Attacks
      - When a threat actor compromises hardware or firmware before it ever reaches the customer environment. This has been seen with everything from chip sets to pre-installed applications.
- Mitigation Techniques
  - Per MITRE
  - This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

- Detection Techniques
    - Forensic utilities may be capable of finding things such as:
        - Strings
        - Unexpected disk partition table entries
        - Blocks of unusual memory
    - A comparison of the component hashes to known good ones may provide some insight into potential system tampering

Lesson 4.6: Create Account

Skills Learned From This Lesson: Definition, Usage, Mitigation, Detection

- Create Account
    - The creation of a local system, domain, or cloud account is considered a form of persistence for the threat actor. Also, this allows the threat actor to avoid malicious software detection tools and other protectors because the account is considered “normal”.
    - Command line commands such as net user in Windows allows for the creation of accounts.
- ServHelper Malware
    - ServHelper is malware that has been classified as a backdoor. It has several functions that include the following:
        - Extracting and dropping an OpenSSH binary
        - Extracting, dropping and configuring the RDP Wrapper Library
        - Creating a new user “support account” with a password of “Ghar4f5”
        - Adding this user to the Remote Desktop and Administrators groups
- Mitigation Techniques
    - Use multi-factor authentication for user and privileged accounts
    - Utilize network segmentation to provide systems and users access to resources necessary to achieve their core functions.
    - Implement best practice security configuration for servers, such as domain controllers
    - Do not allow day to day operations with domain administrator accounts
- Detection Techniques
    - Utilize log collection tools to alert on account creation within the network
        - Event ID 4720, generated when a user account is created
        - The event should be validated as a legitimate action
    - Log collection from cloud administration accounts can be used to identify unusual activity

- Alert on members that are assigned to the administrator roles

Lesson 4.7: Hooking

Skills Learned From This Lesson: Definition, Usage, Mitigation, Detection

- Hooking
  - The act of leveraging application programming interface functions to perform tasks that require reusable system resources.
  - Hooking involves redirecting calls via:
    - Hooks Procedures
    - Import Address Table (IAT) Hooking
    - Inline Hooking
  - Like Process Injection threat actors can use hooking to load and execute malicious code as though it were another process.
- Use cases of Hooking
  - Classic DLL Injection via CreateRemoteThreat and LoadLibrary
    - Malware writes the path to its malicious DLL in the virtual address space of another process
  - Portable Executable Injection (PE Injection)
    - Doesn't pass the address of the LoadLibrary, it makes of copy of malicious code into an existing open process and causes it to execute
  - Thread Execution Hijacking
    - Like process hollowing, thread execution hijacking targets an existing thread of a process and avoid any noisy process or thread creation operations.
- Mitigation Techniques
  - Prevention techniques are difficult to achieve
  - Some methods may include the use of malicious patch detection
- Detection Techniques
  - Include monitors for calls to the SetWindowsHookExand SetWinEventHookFunctions
  - Implement software specific for rootkit detection, any alerts should be reviewed

Lesson 4.8: New Service

Skills Learned From This Lesson: Definition, Usage, Mitigation, Detection

- New Service

    - Threat Actors take advantage of systems by installing a new service that can be configured to execute at startup using utilities to interact with the service or by modifying the Registry.
    - Threat Actors will typically name services after legitimate software to attempt to circumvent controls or bypass detection methods.
    - Services are commonly used to perform privilege escalation to get an administrator account to SYSTEM level.
- Trojan Rikamanu
    - Rikamanu is a trojan that steals information from the compromised system.
    - Creates the following files:
        - %Windir%\Help\CNDY.DAT
        - %System%\drivers\Irmon.dll
    - Then creates a service as follows:
        - Display name: Irmon
        - Image path: %System%\svchost.exe -k netsvcs
        - Description: The infrared Port Monitor is present for all computers with infrared ports. It initiates file transfer between your computer and another device, like a PDA or mobile phone.
- Mitigation Techniques
    - Limit user account privileges to those necessary and do not allow accounts to have administrative access for daily tasks
    - Utilize malware detection and prevention tools to slow down or stop known variants
- Detection Techniques
    - Monitor service creation and changes in the Registry
    - Analysis should be done on multiple events to determine if a threat actor is potentially in the network
    - Look for changes in systems that do not correlate with patching and other system management practices

Lesson 4.9: Persistence Case Study

Skills Learned From This Lesson: Case Study, Persistence, Example

- Dwell Time and Threat Removal
    - Numbers to Consider
        - The average containment time in 2017 was five days
            - This containment time was applicable only after detection which on average was 66 days

        - Average Time it Takes for Hackers to Get In:
            - 4 hours and 37 minutes, depending on the nation state it could be much faster
        - A realistic, minimum goal is to stop breaches within 8 to 12 hours
            - Organizations such as CrowdStrike advocate a full investigation within 10 minutes and complete removal of the threat actor in 60 minutes
    - What Should We Start to Consider
        - What Capabilities would an organization need to implement to at least meet the minimum 8-12-hour cyber response plan time?
        - Once the plan is written for the minimum time, how does an organization then move, either in increments or all at once, to get to a 60-minute removal time?
        - Do either of these metrics have feasibility based on your organizations cost benefit analysis?
        - Imagine you are a threat actor looking to steal high value information from the organization you work for. What would you look to steal and based on the mechanisms discussed up to this point, are any of them feasible?

Lesson 4.10: Module 4 Summary

Skills Learned From This Lesson: Summary, Persistence, Module

- Summary of what was covered in this module.

Module 5: Privilege Escalation

Lesson 5.1: What is Privilege Escalation?

Skills Learned From This Lesson: Definition, Privilege Escalation, Introduction

- Privilege Escalation
    - Privilege escalation consists of methods in which a Threat Actor is able to gain a higher-level permission set on a system or network.
    - This allows attackers to do more than just explore the network and its endpoints.
    - They commonly use methods such as:
        - System Weaknesses
        - Misconfigurations
        - Vulnerabilities

- What Will We Be Reviewing
    - Access Token Manipulation
    - Elevated Execution With Prompt
    - Exploitation for Privilege Escalation
    - File System Permission Weakness
    - Scheduled Task
    - Sudo
    - Web Shell

Lesson 5.2: Access Token Manipulation

Skills Learned From This Lesson: Definition, Methods, Mitigation, Detection

- Access Token Manipulation
    - Windows uses tokens to determine ownership of a running process. These access tokens can be manipulated to appear as though it belongs to someone else.
    - There are three primary methods in which threat actors take advantage of this method:
        - Token Impersonation/Theft
        - Create Process with a Token
        - Make and Impersonate Token
- Access Token Manipulation Methods
    - Token Impersonation/Theft
        - A threat actor creates a new token that duplicates an existing token. Commands such as DuplicateToken, ImpersonateLoggedOnUser, and SetThreadToken.
    - Create Process with a Token
        - A threat actor creates a process with the token, impersonating the security context of the user.
    - Make and Impersonate Token
        - The threat actor uses the user's credentials to log in and create a token that they can then assign to a thread. The creation of Impersonation tokens does not require access to an administrator account.
- Mitigation Techniques
    - Limit users permission to no allow token creation. This can be done through a local system account only.
        - Using group policy you can limit the user's rights to create and replace tokens.

    - Limit user permissions to not allow for administrative account use in day to day tasks.
- Detection Techniques
    - Audit command line activity for token manipulation commands
        - Look for instances of runascommand
        - Enable any detailed logging functions

Lesson 5.3: Elevation Escalation with Prompt

Skills Learned From This Lesson: Elevation, Escalation, Examples

- Elevated Execution with Prompt
    - Threat actors use AuthorizationExecuteWithPrivileges API to escalate privileges by prompting the user for credentials.
    - The API has no validation to determine if the request has come from a reputable source.
    - This can be abused in that threat actors will install malicious software and other persistence mechanisms by taking advantage of this API.
- MacOS Malware Variant of Shlayer
    - The Malware attempts to get the user to install malicious updates, claiming to be for Flash Player.
    - The Malware does some of the following:
        - Collects system information such as MacOS version and IOPlatformUUID
        - Generates a Session GUID using the uuidgencommand
        - Creates a custom URL using the information from the previous steps to download an additional, second stage payload
        - Attempts to download a zip file payload using curl
        - Creates directories in /tmpto unzip payloads
        - Makes the binary
        - Executes the payload
        - Performs a Kill All
- Mitigation Techniques
    - In the case of MacOS prevent applications from running that haven't been downloaded through the Apple Store.
    - Do not allow unsigned applications to be run on the system.
- Detection Techniques
    - Consider monitoring for /usr/libexec/security_authtrampolineexecutions which could indicate that AuthorizeationExecuteWithPrivilegesis being executed.

Lesson 5.4: Exploitation for Privilege Escalation

Skills Learned From This Lesson: Privilege Escalation, Examples, Exploitation

- Exploitation for Privilege Escalation
    - When a threat actor takes advantage of a software vulnerability through things such as:
        - Programming Error
        - Service Error
        - Operating System Software Error
        - Kernel Error
    - The reason for these types of exploits is to allow the Threat Actor to conduct a technique known as privilege escalation, which can circumvent system/account restrictions.
    - In practice this is when a Threat Actor can take an unprivileged or user level account to SYSTEM or root permissions.
- CVE-2015-1701 -Microsoft Windows -Local Privilege Escalation (MS15-051)
    - CVE-2015-1701 is an elevation of privilege vulnerability that exists when the Win32k kernel-mode does not properly handle objects in memory.
    - CVE-2015-1701 is a local privilege escalation vulnerability so Threat Actors would need access to the system, prior to being able to exploit this vulnerability.
    - Systems Impacted
        - Windows Server 2003 SP2
        - Windows Server 2008 SP2
        - Windows Vista SP2
        - Windows 7 SP1
- Mitigation Techniques
    - Implement application isolation and sandboxing. Virtualization and application segmentation may further mitigate.
    - Update software and apply patches to systems regularly, especially those that are known to be vulnerable.
- Detection Techniques
    - Evaluate systems that are performing in a manner that indicates potential tampering with components such as:
        - Crashing Regularly
            - Other Types of Stability Issues
    - Implement monitor that looks for abnormal behavior or processes

Lesson 5.5: File System Permission Weakness

Skills Learned From This Lesson: Definition, Usage, Mitigation, Detection

- File System Permission Weakness
    - As a part of their process's binaries may automatically execute binaries as needed to perform their functions or other actions.
    - It is possible for these binaries to be targeted and the binary overwritten with another binary, as a standard user, and executed by the original process.
    - If the original process is running with a higher permission set then the replaced binary will execute under the higher permission set.
- Areas That Could Be Manipulated
    - Services
        - Windows service binary manipulation is one technique that can be used in this vector. In some cases threat actors can replace a legitimate service executable with their own and use it to gain persistence and/or privilege escalation on the account.
    - Executable Installers
        - This takes advantage of a weakness that is common in executable, self-extracting, installers. The unpacking of these files can result in the execution of untrusted code placed in subdirectories and files, which can overwrite binaries used in the installation process.
- Mitigation Techniques
    - Tools like PowerSploit can be used to audit systems identify potential permission weaknesses
    - Turn off UAC privilege escalation for standard users to automatically deny elevation requests.
    - Limit privilege of users to those that are necessary and restrict their ability to make service changes
- Detection Techniques
    - Review systems looking for changes to binaries and service executables
    - Do hashing of known good binaries and service executables, doing regular comparison against a known good database

Lesson 5.6: Scheduled Tasks

Skills Learned From This Lesson: Definition, Usage, Mitigation, Detection

- Scheduled Task
    - A threat actor can utilize utilities such as at.exe and schtasks, in addition to the Windows Task Scheduler, to schedule payloads, scripts, or programs to run at a certain date and time.

- How Has Scheduled Task Been Used
    - Zlob Variants use task scheduler, a trojan with the capability to take over a system.
    - Bamital, a click fraud trojan, that will attempt to escalate privilege using task scheduler
    - Overall, the method can be used to continuously re-infect a system
- Mitigation Techniques
    - Use Powersploitor other tools to find system permission weaknesses in scheduled tasks prior to them being taken advantage of
    - Force scheduled tasks to run under the authenticated account instead of system
    - Limit user privileges to those necessary to achieve their business functions
- Detection Techniques
    - Alert on scheduled tasks creation from command line
    - Monitor for process execution from task scheduler
    - Configure event logging for scheduled task creation and changes○Event ID 106, 140, 141, 4698, 4700 and 4701

Lesson 5.7: Sudo

Skills Learned From This Lesson: Definition, Usage, Mitigation, Detection

- Sudo
    - Sudo makes use of members of the sudoers file in /etc/sudoers. The command allows users to temporarily escalate their privileges when it is necessary for administrative purposes.
    - The file can be manipulated to not prompt users for a password by modifying the sudoers file in a manner such as:
        - User1 ALL=(ALL) NOPASSWD: ALL
    - However, this would be counter intuitive, as the function could potentially slow a threat actor down or alert the user of malicious activity.
- How can Sudo be used?
    - A threat actor can compromise a standard user who is a member of the sudoers group
        - In some cases there may not be a need to enter credentials and then the threat actor can operate with elevated privileges
    - CVE-2019-14287 (Sudo before 1.8.28)
        - The threat actor, or standard user, can craft a user ID that allows them to bypass of !root configuration.
- Mitigation Techniques

    - Do not allow sudo to be executed without providing a password
    - The Sudoers file should be controlled and users should not be allowed to spawn risky processes
- Detection Techniques
    - Linux provides an alert any time a user's actual ID and effective ID are different
    - Sudo incidents should be reviewed regularly to detect potentially manipulation or privilege escalation attempts

Lesson 5.8: Web Shell

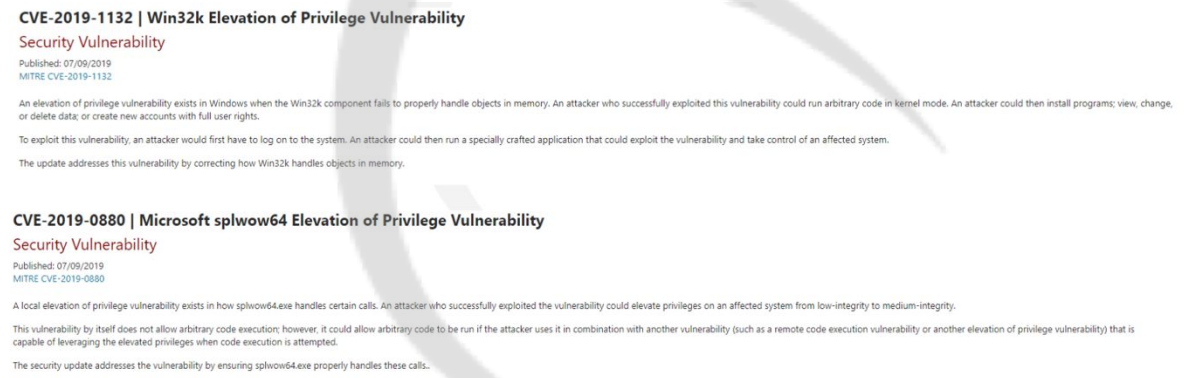
Skills Learned From This Lesson: Definition, Usage, Mitigation, Detection

- Web Shell
    - A Web Shell is a script that takes advantage of accessible Web Servers. This allows a threat actor to use the system in ways the administrator may not have intended to either attack end users and steal personal information or to further compromise the organizations systems.
- Types of Web Shell Tools
    - ASPXSpy
        - A Web Shell that takes advantage of .NET ASP.
    - ReGeorg
        - Uses Python 2.7, allows users to create a TCP circuit through valid HTTP requests
    - Antak
        - Web Shell written in ASP .Netwhich utilizes PowerShell
    - China Chopper
        - A simple backdoor that has two key components. A web shell that provides Command-and-Control functions and a text-based web shell payload.
- Mitigation Techniques
    - Ensure that least privilege is practiced on accounts
        - External server accounts should not match internal accounts in the event of compromise
    - Ensure that server software is up to date
- Detection Techniques
    - Process monitoring may be used to detect web servers that perform suspicious activities such as:
        - Running cmd○Access files that are not in web directories
    - Log authentication attempts and look for unusual patterns

Lesson 5.9: Privilege Escalation Case Study

Skills Learned From This Lesson: Case Study, Privilege Escalation, Examples

- Two For The Price of One!
    - July 10th, 2019 (Privilege Escalation Vulns 2019-0880 & 1132)
        - Patch Tuesday in the month of July brought great news! Two Zero-Days were fixed!



CVE-2019-1132 | Win32k Elevation of Privilege Vulnerability

Security Vulnerability

Published: 07/09/2019
MITRE CVE-2019-1132

An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.

The update addresses this vulnerability by correcting how Win32k handles objects in memory.

CVE-2019-0880 | Microsoft splwow64 Elevation of Privilege Vulnerability

Security Vulnerability

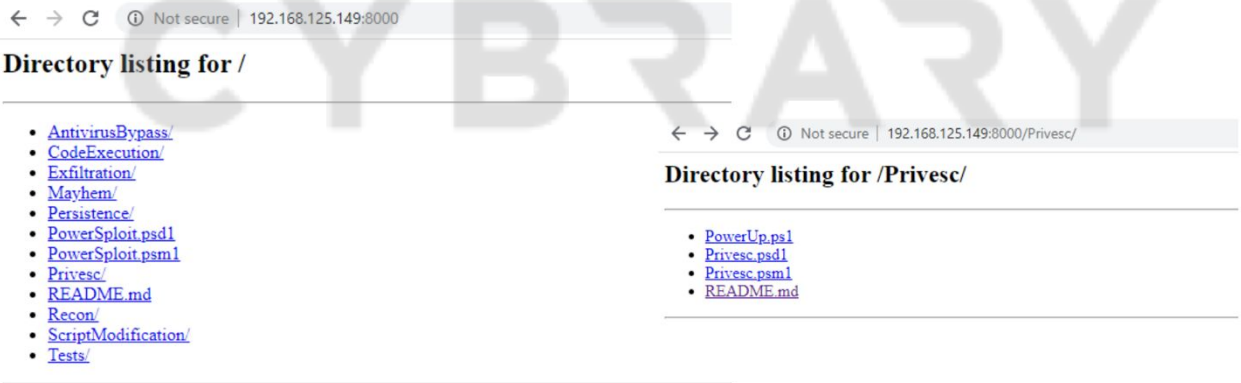
Published: 07/09/2019
MITRE CVE-2019-0880

A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls. An attacker who successfully exploited the vulnerability could elevate privileges on an affected system from low-integrity to medium-integrity.

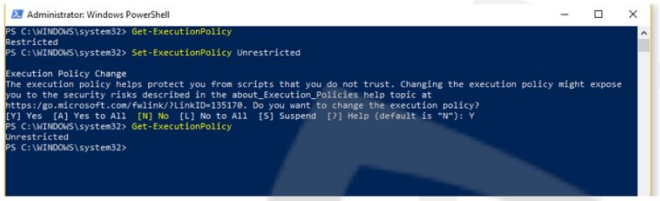
This vulnerability by itself does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability (such as a remote code execution vulnerability or another elevation of privilege vulnerability) that is capable of leveraging the elevated privileges when code execution is attempted.

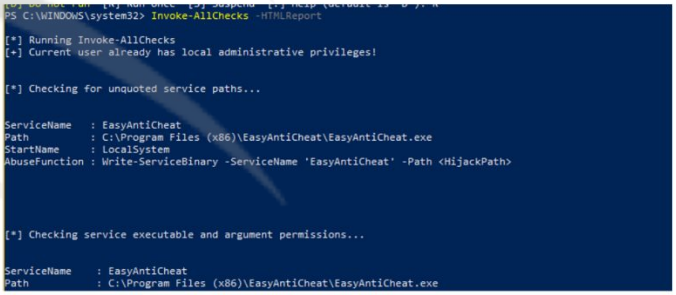
The security update addresses the vulnerability by ensuring splwow64.exe properly handles these calls..

- What can we do to look for potential privilege escalation?



- Potential Privilege Escalation





Lesson 5.10: Module 5 Summary

Skills Learned From This Lesson: Summary, Module, Privilege Escalation

- Summary of what was discussed in this module.

Module 6: Defense Evasion

Lesson 6.1: What is Defense Evasion?

Skills Learned From This Lesson: Definition, Defense Evasion, Introduction

- Defense Evasion
    - In this vector, the Threat Actor is attempting to avoid detection.
    - These techniques can include but are not limited to:
        - Uninstalling security components
        - Obfuscating information/data
            - This can include things like payloads or scripts
- What Will We Be Reviewing
    - Clear Command History
    - Compile After Delivery
    - Disabling Security Tools

- Hidden Files and Directories
- Hidden Users
- Hidden Window
- Process Hollowing
- Software Packing

Lesson 6.2: Clear Command History

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Clear Command History
  - In both macOS and Linux the commands a user enters in a terminal are kept track of.
  - The primary area this information is stored is:
    - ~/.bash_history
    - Anything passed through the command line is saved in this file, to include credentials. A threat actor will clear this information to ensure the job of tracking their actions is a little more difficult.
- It's Worth a Shot...
  - Most threat actors will likely put commands in their scripts to remove the command history.
  - Such commands can include things like:
    - Unset HISTFILE
    - Export HISTFILESIZE=0
    - History –c
    - Rm ~/.bash_history
  - However, this should not deter you from looking to see if there are indicators of compromise in the terminals history.
  - Windows command prompts typically lose their history as soon as the session ends.
- Mitigation Techniques
  - Make the history file read only so it cannot be manipulated
  - Ensure that the users permissions are limited
- Detection Techniques
  - Any alteration/clearing of the history file should be logged as suspicious and reviewed

Lesson 6.3: Compile After Delivery

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Compile After Delivery
  - Threat actors will deliver code to the victim system in an uncompiled manner.
  - Delivering the code in an uncompiled manner is done so in an attempt to subvert technical controls by compiling the payload before execution.
- Things to Look For
  - Payloads may be encrypted
  - Payloads may be encoded within other file
  - Delivery can be done via phishing attachments
  - Payloads could be in a format that is not native to the operating system in use
- Mitigation Techniques
  - End user awareness training
- Detection Techniques
  - Monitoring systems for abnormal activity such as
    - Command-line arguments for compilers like csc.exe and GCC
  - Look for non-native binary formats and cross-platform compilers

Lesson 6.4: Disabling Security Tools

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Disabling Security Tools
  - In short, Threat Actors disable security tools to avoid detection.
  - This can include:
    - Killing software services
    - Disabling logging processes
    - Removing Registry keys
- Backspace
  - A backdoor that targets windows operating systems.
  - Associated with APT30
  - Can download and execute various binaries on the impacted system
  - Known to check for host-based firewalls and will make them accept/allow connections out
- Mitigation Techniques
  - Ensure file, process, and registry permissions are in place to prevent threat actors from disabling services
  - Ensure that users are setup to use least privilege in the environment
- Detection Techniques

- Process and command line arguments should be monitored for suspicious activity
  - Service killed
  - Registry edits
- Removal of or gaps in log or event files

Lesson 6.5: Hidden Files and Directories

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Hidden Files and Directories
  - Files that are typically hidden from end users to prevent them from accidentally overwriting or changing critical system files.
  - Threat Actors can use this to hide files and folders on the system for persistence or evading purposes.
- How to do it
  - Windows Systems
    - Mark files as hidden by using the attrib.exe binary. Attrib+h <filename>
  - Linux/Mac
    - Put a "." at the beginning of the file or folder name. ".example.txt"
- Mitigation Techniques
  - End user training
  - Implementation of least privilege
- Detection Techniques
  - Look for commands that add the "." on the front of files and the use of attrib.exe in windows.

Lesson 6.6: Hidden Users

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Hidden Users
  - In MacOS, a userID is associated with every account. When a user is made, you can specify the userID for the account.
  - In a preferences directory there is a property value in com.apple.loginwindow called Hide500Users, and this keeps userIDs 500 and lower hidden.
  - You can create an account using this technique and put its value under 500 by enabling this property.
- Command Syntax

    - Sudo dscl . –create /Users/username UniqueID 301
- Mitigation Techniques
    - If domain joined, then use group policy to restrict the ability to create or hide users.
    - Prevent modification of the Hide500Users value
- Detection Techniques
    - Even though the user is hidden they still sign in and create a home directory and will appear in authentication logs

Lesson 6.7: Process Hollowing

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Process Hollowing
    - Happens when a process is created in a suspended state, then its memory is unmapped and replaced with malicious code.
    - Can be masked under legitimate processes and can evade defenses.
- ISM Injector
    - Described as a Trojan
    - Used to install other backdoors
    - Is associated with the OilRig Threat group
    - Obfuscated with SmartAssembly.NET obfuscator

```
if (!File.Exists(Class8.path_SrvHealth))
{
    Interaction.Shell("cmd.exe /c " + Class5.getTsk1Resource(), AppWinStyle.Hide, false, -1);
    Thread.Sleep(500);
    Interaction.Shell("cmd.exe /c " + Class5.getTsk2Resource(), AppWinStyle.Hide, false, -1);
}
```

Snip is from Palo Alto Networks | Unit 42

- Mitigation Techniques
    - Implement least privilege on user accounts
    - Implement awareness training
- Detection Techniques
    - Monitor API calls that un-map process memory and those that can modify memory within another process

Lesson 6.8: Software Packing

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Software Packing
    - When a threat actor compresses or encrypts an executable in an attempt to change the files signature to avoid detection.
    - Utilities used to perform such actions are called packers.
- Machete Cyber espionage tool set
    - Toolset developed by a Spanish speaking group.
    - Attacks focus primarily on Latin American countries, allowing them to collect intelligence.
    - Main backdoor is Python-based
    - Downloaders are UPX packed, (The Ultimate Packer for eXecutables, which is a free tool)
- Mitigation Techniques
    - Heuristic based malware detection, which focuses on both signatures and behaviors
- Detection Techniques
    - Use scanning to look for known software packers or artifacts

Lesson 6.9: Defense Evasion Case Study

Skills Learned From This Lesson: Case Study, Examples, Review

- What's Watching Your Back?
    - Dwell Time – Successful Defense Evasion?
        - A FireEye Analysis of global breach data from 2018 indicates that half of all organizations last year took 50 days or longer to detect an intrusion
            - Previously this number was 57 days in 2017
        - In some cases business were learning of attackers from other agencies up to six months after a breach
        - Cryptomining tools and ransomware were among those that were easier to spot
        - Typically organizations that were previously compromised were retargeted by attackers
- What Tools Are Out There?
    - Cryptcat
        - A simple Unix utility which reads and writes data across network connections, using TCP or UDP while encrypting the data.
    - Dns2tcp
        - Network tool designed to relay TCP connections through DNS traffic. Doesn't need to run with specific privileges.

- Shellter
  - Can be used in order to inject shellcode into native windows applications.

Lesson 6.10: Module 6 Summary
Skills Learned From This Lesson: Summary, Module, Defense Evasion

- Summary of what was covered in this module.

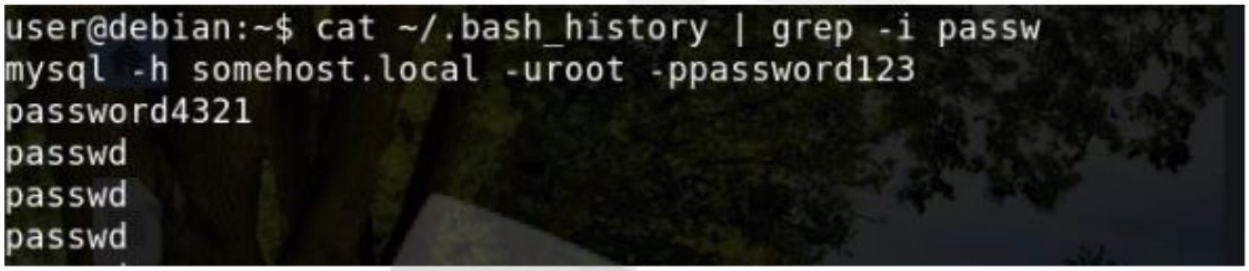
Module 7: Credential Access

Lesson 7.1: What is Credential Access?
Skills Learned From This Lesson: Definition, Credential Access, Introduction

- Credential Access
  - In this phase of the MITRE Attack Framework the threat actor is attempting to steal account names and passwords.
  - Techniques can Include:
    - Keylogging
    - Credential Dumping
    - Stealing from Web Browsers
- What Will We Be Reviewing
  - Bash History
  - Brute Force
  - Credential Dumping
  - Steal Web Session Cookie

Lesson 7.2: Bash History
Skills Learned From This Lesson: Definition, Mitigation, Detection

- Bash History
  - Simply put, bash keeps track of the commands users' types using the command line with the “history” utility.
  - Upon log out the history is flushed to the .bash_history file.
  - The files reside at the same location: ~/.bash_history
  - Typically limited to 500 commands.
- Presence of Credentials in Bash History



- Mitigation Techniques
  - The following can be used to prevent user's history from flushing to the .bash_history file
    - Set +o history
    - Unset HISTFILE (added to a users .bash_rc file)
- Detection Techniques
  - Monitor for when a user's history file is read, make sure the activity is alerted on

Lesson 7.3: Brute Forces

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Brute Force
  - When the threat actor cannot obtain credential hashes then the other option is brute forcing. This is when the attacker attempts to guess passwords.
  - This can be done against a possible list of passwords, either generated or pre-built. This would be considered a high risk for detection since it would create numerous failed login attempts.
- Commonly Brute Forced Ports
  - SSH (22/TCP)
  - Telnet (23/TCP)
  - FTP (21/TCP)
  - NetBIOS / SMB / Samba (139/TCP & 445/TCP)
  - LDAP (389/TCP)
  - Kerberos (88/TCP)
  - RDP / Terminal Services (3389/TCP)
  - HTTP/HTTP Management Services (80/TCP & 443/TCP)
  - MSSQL (1433/TCP)
  - Oracle (1521/TCP)
  - MySQL (3306/TCP)

    - VNC (5900/TCP)
- Mitigation Techniques
    - Set account lockouts to prevent password guessing
    - Enable multi-factor authentication, when able
    - Determine best password policies for the organization based on NIST or Compliance guidelines
- Detection Techniques
    - Look for high authentication failures on systems
        - Look for failed login attempts across various accounts
    - On the Domain controllers
        - DC: Audit Logon Success & Failure for Event ID 4625
        - DC: Audit Kerberos Authentication Service Success & Failure for event ID 4771
        - All systems: Audit Logon Success & Failure for Event ID 4648

Lesson 7.4: Credential Dumping

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Credential Dumping
    - When a threat actor obtains account login and password information, typically the form of a hash or clear text password.
- Common Tools
    - Pwdumpx.exe
        - Able to acquire password hash from remote hosts , can be used to log into systems with the hash.
    - Gsecdump
        - Extracts password hash from SAM/AD or logon sessions.
    - Mimikatz
        - Used to view and save authentication credentials like Kerberos tickets. (Among Other attack types)
    - Secretsdump.py
        - Dump hashes from the remote machine without executing any agent there.
- Mitigation Techniques
    - Disable or restrict NTLM
    - Ensure Local Administrator accounts have complex and unique passwords
    - Limit credential overlap across accounts (Limit the reuse of passwords)

- Detection Techniques
    - Windows
        - Monitor for processes interacting with lsass.exe
        - Monitor for network protocols and other replication requests from IPs not associated with known domain controllers
    - Linux
        - Use the AuditDmonitoring tool, which ships stock in many Linux distributions, can be used to watch for hostile processes opening this file in the proc file system, alerting on the pid, process name, and arguments of such programs.

Lesson 7.5: Steal Web Session Cookie

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Steal Web Session Cookie
    - A web application or service session cookie can be used by a threat actor to gain access to the application or Internet Service without needing to authenticate.
    - Other places cookies can be found are on the disk, in memory, and in network traffic.
    - Session cookies can be used to bypass some multi-factor authentication protocols.
- Open Source Frameworks
    - Evilginx 2
        - Standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies.
- Mitigation Techniques
    - A physical second factor key that uses the target login domain as part of the negotiation protocol will prevent session cookie theft through proxy methods
    - Force browsers to delete persistent cookies
    - End User training to look for phishing and other credential gathering techniques
- Detection Techniques
    - Look for repository access on local systems used to store browser session cookies
        - Chrome: "C:\Users\Your User Name\AppData\Local\Google\Chrome\User Data\Default.“
        - Mozilla: Cookies are all stored in thecookies.sqlitefile.
    - Monitor for attempts to inject into or dump browser process memory

Lesson 7.6: Credential Access Case Study

Skills Learned From This Lesson: Case Study, Credential Access, Example

- Old News, but a relevant discussion
    - Time to crack versus an attacker with a match
        - 5 Characters = .03 Seconds
        - 7 Characters = 9 minutes
        - 8 Characters = 2.6 days
        - 9 Characters = 9.1 Years
        - 12 Characters = 7.5 Million Years
        - Attacker who stole your password = 0.00 seconds
- So what's the point?
    - Do you change passwords often enough to subvert a threat actors attempts to log in with stolen credentials?
    - Do you have password monitoring measures in place to tell you when a user might be reusing their password?
    - Have you done a search recently for passwords across your file shares?

Lesson 7.7: Module 7 Summary

Skills Learned From This Lesson: Definition, Credential Access, Introduction

- Summary of what was covered in this module.

Module 8: Discovery

Lesson 8.1: What is Discovery?

Skills Learned From This Lesson: Definition, Discovery, Introduction

- Discovery
    - Discovery is essentially when the threat actor is working out what is in your environment.
    - Can include things like:
        - Operating Systems
        - Internal Network Information
- What Will We Be Reviewing
    - Account Discovery
    - Browser Bookmark Discovery
    - System Owner/User Discovery

Lesson 8.2: Account Discovery

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Account Discovery
  - Threat Actors will work to get a listing of local system or domain accounts
- Commands Used
  - Windows
    - Net user
    - Net group
    - Net localgroup
  - MAC
    - Groups
    - Id
    - Dscl . List /Groups
    - Dscacheutil–q group
  - Linux
    - /etc/passwd
    - Groups
    - Id
- Mitigation Techniques
  - Prevent administrator accounts from being enumerated when an application is elevating through UAC.
    - Use GPO: Computer Configuration > [Policies] > Administrative Templates > Windows Components > Credential User Interface: E numerate administrator accounts on elevation
- Detection Techniques
  - Look at patterns of behavior that could indicate a threat actor is attempting to discover information about your network
  - Monitor processes and command-line arguments for actions that could be used to gather system information

Lesson 8.3: Browser Bookmark Discovery

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Browser Bookmark Discovery
  - A Threat Actor can use bookmarks to reveal personal information about the target, in addition to possible internal details about the organization and its infrastructure.
- Mitigation Techniques

    - End User Awareness training
- Detection Techniques
    - Monitor for commands that provide arguments that could be used to gather browser bookmark information

Lesson 8.4: System Owner / User Discovery

Skills Learned From This Lesson: Definition, Mitigation, Detection

- System Owner/User Discovery
    - When a threat actor attempts to identify the primary user logged into a system. The threat actor may then use this information to determine next steps and how to use that individual account.
- User Lookup Commands
    - Windows
        - Whoami
    - Mac
        - Id –un
        - W
    - Linux
        - Whoami
        - W
- Mitigation Techniques
    - Prevent user command line use
- Detection Techniques
    - Gather various system events and determine if they amount to a malicious threat actor or normal business activity.

Lesson 8.5: Discovery Case Study

Skills Learned From This Lesson: Case Study, Discovery, Example

- A Tool of the trade
    - The Power of NMAP

File smb-enum-users

Script Output

```
Host script results:
|  smb-enum-users:
|_ |_ Domain: RON-WIN2K-TEST; Users: Administrator, Guest, IUSR_RON-WIN2K-TEST, IWAM_RON-WIN2K-TEST, test1234, TsInternetUser

Host script results:
|  smb-enum-users:
|  |  RON-WIN2K-TEST\Administrator (RID: 500)
|  |  |  Description: Built-in account for administering the computer/domain
|  |  |_ Flags:       Password does not expire, Normal user account
|  |  RON-WIN2K-TEST\Guest (RID: 501)
|  |  |  Description: Built-in account for guest access to the computer/domain
|  |  |_ Flags:       Password not required, Password does not expire, Normal user account
```

File smb-os-discovery

Script Output

```
Host script results:
| smb-os-discovery:
|   OS: Windows Server (R) 2008 Standard 6001 Service Pack 1 (Windows Server (R) 2008 Standard 6.0)
|   OS CPE: cpe:/o:microsoft:windows_2008::sp1
|   Computer name: Sql2008
|   NetBIOS computer name: SQL2008
|   Domain name: lab.test.local
|   Forest name: test.local
|   FQDN: Sql2008.lab.test.local
|   NetBIOS domain name: LAB
|_  System time: 2011-04-20T13:34:06-05:00
```

Lesson 8.6: Module 8 Summary

Skills Learned From This Lesson: Summary, Module, Discovery

- Summary of what was covered in this module.

Module 9: Lateral Movement

Lesson 9.1: What is Lateral Movement?

Skills Learned From This Lesson: Definition, Credential Access, Introduction

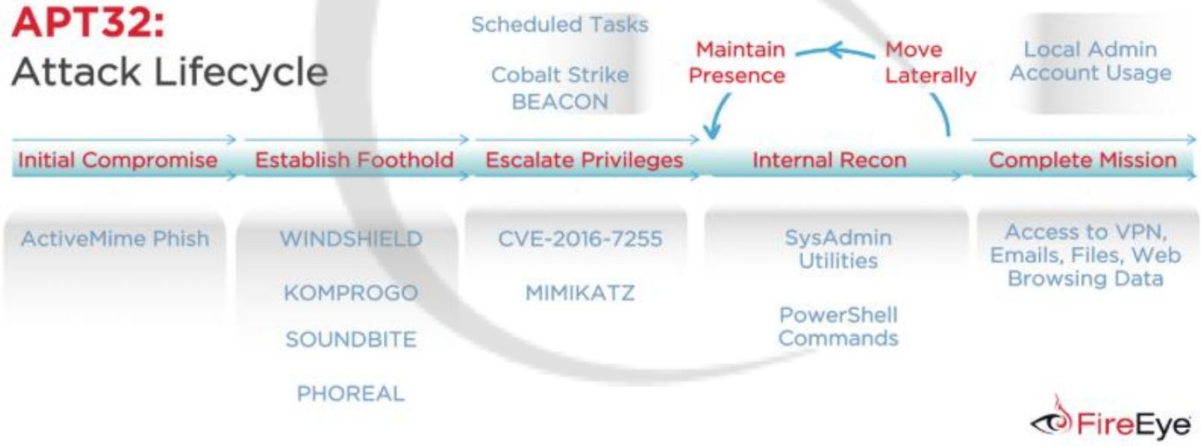
- Lateral Movement
  - The actions an adversary takes to move through your network/environment.
  - Getting to their primary objective often requires exploring the network to find targets
  - Pivoting through multiple systems
  - Might use custom tools to provide remote access
- What Will We Be Reviewing
  - Application Deployment Software
  - Exploitation of Remote Services

- SSH Hijacking

Lesson 9.2: Application Development Software

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Application Deployment Software
  - Threat actors deploy software to systems within the victim network using application deployment systems commonly used by system administrators.
  - Permissions may vary; results may vary
- APT 32



- Mitigation Techniques
  - Use of Multifactor Authentication for accounts associated with application deployment software
  - Regular updates to reduce the likelihood of exploitation of privilege escalation
  - Use proper network segmentation to isolate critical systems, using other forms of network protections to make the task of exploitation systems difficult
- Detection Techniques
  - Monitor applications deployments from a secondary system
    - Produce a standard schedule for application deployment; looking for abnormal activity

- Monitor login activity for deployment systems

Lesson 9.3: Exploitation of Remote Services
Skills Learned From This Lesson: Definition, Mitigation, Detection

- Exploitation of Remote Services
  - A threat actor takes advantage of a programming error in a program, service, or within the operating system software or kernel to execute adversary-controlled code.
  - Systems are identified using:
    - Network service scanning
    - Identifying commonly vulnerable software
    - Patching gaps that leave a system open to attack
- Windows SMB Server Remote Code Execution
  - Systems Impacted
    - Windows 7
    - Windows 8.1
    - Windows 10
    - Windows Server 2008
    - Windows Server 2012
    - Windows Server 2016
    - Core 2008
    - Core 2012
    - Windows XP
    - Windows Server 2003
  - CVEs are show to be associated with SMBv1 primarily.
  - An unauthenticated attacker could send a specially crafted packet to a targeted SMBv1 server. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged-on user.
- Mitigation Techniques
  - Disable or remove features that are not necessary
  - Keep Software up to date
  - Identify vulnerabilities with vulnerability scanning, remediate findings
  - Network Segmentation to reduce the ability for a threat actor to easily reach critical systems
- Detection Techniques
  - Monitor for behavior on endpoint systems that could be an indicator of compromise

- Suspicious files written to disk
- Process injection attempts or success

Lesson 9.4: SSH Hijacking

Skills Learned From This Lesson: Definition, Mitigation, Detection

- SSH Hijacking
  - A threat actor may use the trusted relationship between systems to established connections to other systems by taking advantage of public key authentication in active SSH sessions.
  - The threat actor will hijack the session, which becomes trivial, if the threat actor has root privilege.
  - SSH Hijacking differs from use of Remote Services because it injects into an existing SSH session rather than creating a new session using Valid Accounts.
- Ebury – SSH Rootkit
  - Ebury is an SSH rootkit/backdoor trojan for Linux style systems.
  - Typically it is installed by attackers with root level access to the system either through replacing SSH binaries or by making changes to an SSH library.
  - Some Antivirus products can detect Ebury, but there may be some limitations depending on the vendor and variant.
- Mitigation Techniques
  - If SSH is not needed, then remove the ability to use it on systems
  - Do not allow remote access via SSH as root or other elevated account types
  - Properly harden systems to prevent root privilege escalation
- Detection Techniques
  - Monitor the use of SSH activity and ensure that it is not being used in a manner that is contrary to the organizations policies

Lesson 9.5: Lateral Movement Case Study

Skills Learned From This Lesson: Case Study, Lateral Movement, Example

- Detecting Lateral Movement
  - Things that must be done
    - Don't get complacent from alert fatigue
    - Be aware of how your network is laid out and how it works
    - Have the ability to hunt for threats and proactively investigate activity
  - Points to Consider
    - When was the last time you had an event or incident?

- Do you utilize a third party to do threat hunting and alert you on events/incidents?
    - How often do you hear from them?
    - What things are they alerting you on?
- How would you know if a threat actor was moving through your network?

Lesson 9.6: Module 9 Summary
Skills Learned From This Lesson: Summary, Module, Lateral Movement

- Summary of what was covered in this module.

Module 10: Collection

Lesson 10.1: What is Collection?
Skills Learned From This Lesson: Definition, Collection, Introduction

- Collection
    - The threat actor is collecting data of interest or that meets their goal. Typically this leads to data exfiltration.
    - Common Information of Interest Includes:
        - Browser Data
        - Audio Data
        - Video Data
        - Email
- What Will We Be Reviewing
    - Audio Capture
    - Clipboard Data
    - Data from Local System

Lesson 10.2: Audio Capture
Skills Learned From This Lesson: Definition, Mitigation, Detection

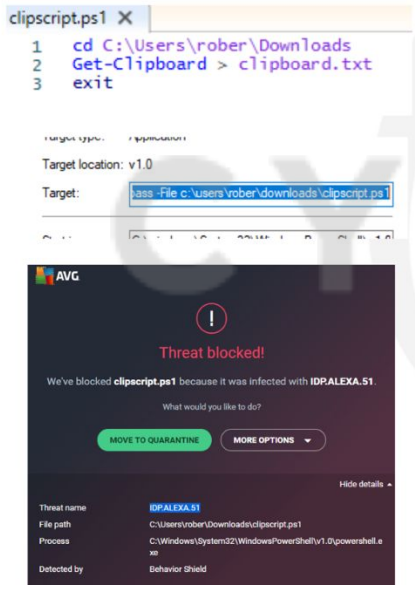
- Audio Capture
    - A threat actor uses computer devices such as microphones and webcams or applications such as voice or video calls to capture audio recordings, in the hopes that sensitive information can be collected.
- Bandook
    - A commercially available RAT, written in Delphi.
    - Capability:
        - Has ability to capture audio

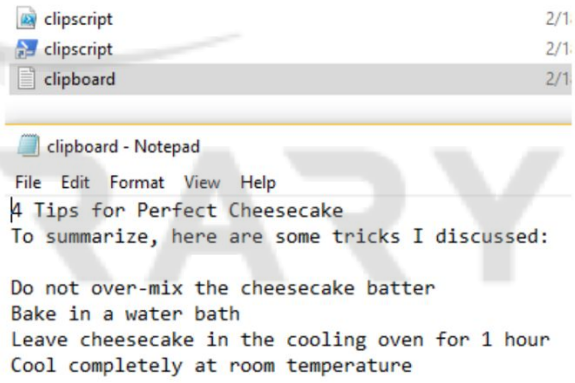
        - Can spawn windows command shell
        - Has the ability to conduct keylogging
        - Replaces iexplore.exe with a Bandook payload
        - Can capture information from the victim's webcam
- Mitigation Techniques
    - End user awareness training to reduce the risk of infection
- Detection Techniques
    - Look for unusual processes accessing APIs associated with devices or software that interacts with peripheral devices

Lesson 10.3: Clipboard Data

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Clipboard Data
    - Threat actors will attempt to collect data stored in Windows clipboard
    - Windows
        - Application can access clipboard data by using the windows API
    - Mac
        - OSX provides a native command, pbpaste, to grab clipboard content
- PowerShell Get-Clipboard





- Mitigation Techniques
    - End User awareness training to reduce the risk of a successful attack
- Detection Techniques
    - The organization will need to look for suspicious behavior patterns that indicate a threat actor may be on the network or system

Lesson 10.4: Data from Local System

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Data From Local System
    - A threat actor will attempt to collect data from the file system or database of information residing on systems prior to Exfiltration.
    - Threat actors will use the command-line interface to look for sensitive information.
- CosmicDuke(MiniDuke)
    - Malware used by APT 29 from 2010 to 2015
    - Capabilities
        - Persistence mechanisms include starting via windows task scheduler
        - Reconnaissance mechanisms includes looking for files with extensions like:
            - Mp3
            - Docx
            - Xlsx
        - Implements several network connectors to exfiltrate data like uploading via FTP and HTTP mechanisms
- Mitigation Techniques
    - End user awareness training to reduce the likelihood of end user infection
- Detection Techniques
    - Monitor for use of command-line arguments that could be actions that represent data collection activity

Lesson 10.5: Collection Case Study

Skills Learned From This Lesson: Case Study, Collection, Example

- What's the Pot of Gold?
    - Items of Interest
        - Targets to hold for ransom
        - Targets to sell access to

        - Your internal infrastructure
        - Your Office 365 Tenant
    - Data to sell
        - Credit Card Information
        - Medical Data
        - Personal Data
- Data Breaches 2019
    - Capital One –106 Million records
    - Evite – 100 Million records
    - Door Dash – 4.9 million potential records breached
    - Elasticsearch Server Breach – 108 million records
    - Third party Facebook app data – 540 million records
    - Items for sale on Dream Market – 620 million records across multiple companies

Lesson 10.6: Module 10 Summary
Skills Learned From This Lesson: Summary, Module, Collection
- Summary of what was covered in this module.

Module 11: Command and Control

Lesson 11.1: What is Command Control?
Skills Learned From This Lesson: Definition, Command and Control, Introduction
- Command and Control
    - The threat actor will attempt to communicate with compromised systems to control them. Commonly threat actors mimic normal behaviors to attempt to avoid detection. Methods used can include
    - Connection Proxies
    - Data Encoding
    - Data Obfuscation
- What Will We Be Reviewing
    - Commonly Used Ports
    - Custom Command and Control Protocol
    - Uncommonly Used Ports

Lesson 11.2: Commonly Used Ports
Skills Learned From This Lesson: Definition, Mitigation, Detection
- Commonly Used Port(s)

    - Threat actors may communicate over common ports to bypass the firewall, and to blend into normal activity.
    - Such Ports can include:
        - TCP:80 (HTTP)
        - TCP:443 (HTTPS)
        - TCP:25 (SMTP)
        - TCP/UDP:53 (DNS)
    - Common ports used internally include:
        - TCP/UDP:135 (RPC)
        - TCP/UDP:22 (SSH)
        - TCP/UDP:3389 (RDP)
- Mitigation Techniques
    - Network Intrusion Prevention to stop Command and Control (C2) activity
    - Network Segmentation to block traffic or protocols that do not need access to other systems
- Detection Techniques
    - Monitor network data communications to look for uncommon data flows

Lesson 11.3: Custom Command and Control Protocol

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Custom Command and Control Protocol
    - Threat actors may communicate using custom C2 protocols instead of using existing standard application layer protocol.
    - This can include using raw sockets on top of fundamental protocols provided by TCP/IP/another standard network stack.
- Naid
    - A trojan used by Elderwood to open a backdoor on compromised hosts.
    - Campaigns with Naid may trace to as early as 2010.
    - Naid drops files that makes registry changes allowing its different components to launch automatically.
    - Port 443 is used to create a backdoor where instructions can be issued to launch attacks and upload collected files.
- Mitigation Techniques
    - Filter network traffic to look for odd protocols
    - Use NIPs to stop common attacks
    - Use Network Segmentation to slow attackers down
- Detection Techniques

- Review ICMP messages and other protocols, looking for abnormal data sets

Lesson 11.4: Uncommonly Used Ports

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Uncommonly Used Ports
  - Threat actors conduct command and control attacks over non-standard ports to bypass proxies and firewalls that are not properly configured.
- Agent Tesla
  - A Spyware Trojan written in Visual basic.
  - Capabilities Include:
    - Account Discovery
    - Data encryption prior to sending
    - Input Capture
    - Remote File Copy
    - Video Capture
    - Has TCP port 587 enabled for C2 Communication
- Mitigation Techniques
  - Use NIPS to block common, known signatures
  - Use network segmentation to limit outgoing traffic
- Detection Techniques
  - Analyze network data flows to look for uncommon patterns (things like high data to and from a system)

Lesson 11.5: Command and Control Case Study

Skills Learned From This Lesson: Case Study, Command and Control, Example

- Zombies...but real
  - Zombie, AKA Botnet
    - A machine infected by a trojan and being controlled by a C2 Server
    - Use for things like
      - Sending Spam
      - Infecting other machines
      - Conducting DDoS attacks
    - Typically a private computer
    - Infection methods are usually delivered with email attachment or compromised software
  - Points to Consider
    - How would you know if your system is acting as a zombie?

- What methods do you currently use to detect anomalous activity?
- Have you had any IP addresses blacklisted recently?

Lesson 11.6: Module 11 Summary
Skills Learned From This Lesson: Summary, Module, Command and Control

- Summary of what was covered in this module.

Module 12: Exfiltration

Lesson 12.1: What is Exfiltration?
Skills Learned From This Lesson: Definition, Exfiltration, Introduction

- Exfiltration
  - The threat actor is trying to steal information or data.
  - Exfiltration can consist of techniques that include things such as compression and encryption to attempt to avoid protections.
- What Will We Be Reviewing
  - Automated Exfiltration
  - Data Compressed
  - Data Transfer Size Limits

Lesson 12.2: Automated Exfiltration
Skills Learned From This Lesson: Definition, Mitigation, Detection

- Automated Exfiltration
  - Threat actors attempt to take data through automated processing or scripting after everything is gathered during the collection phase.
  - This can be done through exfiltration over C2 and over alternative protocols.
- A few Tools
  - Rover
    - Automatically searches for files on local drives based on predefined list of files extensions and sends them to C2 server every 60 minutes.
  - TINYTYPHON
    - Searches for documents and when one is found with a matching extension it uploads it to the C2 Server.
  - USBStealer
    - Automatically exfiltrates collected files via removeable media when an infected device is connected to a second victim.
- Mitigation Techniques

    - End user awareness training to reduce the risk of compromise
- Detection Techniques
    - Monitor process file access patterns and network behavior

Lesson 12.3: Data Compromised
Skills Learned From This Lesson: Definition, Mitigation, Detection

- Data Compressed
    - A threat actor will compress data that is collected prior to exfiltration to minimize the amount of data sent over the network. Can be done with custom program or a common compression method such as 7zip, RAR, ZIP, or zlib.
- Mitigation Techniques
    - Use of Network Intrusion Prevention to block specific file types from leaving the network over unencrypted channels. Threat actor may then use other means to attempt to bypass protections.
- Detection Techniques
    - Monitor for command line arguments and other activities dealing with compression utilities.

Lesson 12.4: Data Transfer Size / Limits
Skills Learned From This Lesson: Definition, Mitigation, Detection

- Data Transfer Size Limits
    - A threat actor will exfiltrate data in fixed size chunks to limit packet sizes below a certain threshold.
    - This is done to avoid triggering alerts concerning data transfer thresholds.
- OopsIE
    - A Trojan used by OilRig (APT) to remotely execute commands.
    - Functions can include:
        - Data Encoding
        - Data Transfer Size Limitation
        - File Deletion
        - Obfuscation of Files or Information
- Mitigation Techniques
    - Network Intrusion Prevention to look for traffic to C2 systems and malware
- Detection Techniques
    - Monitor network traffic for consistent fixed sized data packets and other odd activities.

Lesson 12.5: Exfiltration Case Study
Skills Learned From This Lesson: Case Study, Exfiltration, Example

- Sneaky Bits of Data
    - Potential Exfiltration Methods
        - Encode data into something like Base64 prior to sending it out
        - An SSH tunnel
        - Uploading to a public HTTPS repo
            - Dropbox
            - OneDrive
- Points to Consider
    - What controls are you using today to help block unwanted data exfiltration?
    - Would you know if a threat actor or employee was removing data from your network?
    - What could you change today to help reduce the risk of exfiltration?

Lesson 12.6: Module 12 Summary
Skills Learned From This Lesson: Definition, Credential Access, Introduction

- Summary of what was covered in this module.

Module 13: Impact

Lesson 13.1: What is Impact?
Skills Learned From This Lesson: Definition, Impact, Introduction

- Impact
    - The Threat Actor is attempting to manipulate, interrupt, or destroy your systems and data.
    - Techniques can Include:
        - Disruption in Availability
            - Destroying Data
        - Compromising Integrity
            - Tampering with Data
- What Will We Be Reviewing
    - Account Access Removal
    - Defacement

Lesson 13.2: Account Access Removal

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Account Access Removal
    - When a threat actor interrupts availability of a system or network by inhibiting access to accounts utilized by legitimate users.
    - Accounts May Be
        - Deleted
        - Locked
        - Manipulated (changed credentials)
- LockerGoga
    - LockerGogais a ransomware that has been tied to various attacks on European companies.
    - Has the Ability To:
        - Change account passwords and Log off current users
        - Disable AV with task kill commands
        - Delete its original launcher after execution
        - Can shut down infected systems
- Mitigation Techniques
    - End user awareness training to reduce the potential for infection
- Detection Techniques
    - Look for the following event IDs:
        - Event ID 4723 - An attempt was made to change an account's password
        - Event ID 4724 - An attempt was made to reset an account's password
        - Event ID 4726 - A user account was deleted
        - Event ID 4740 - A user account was locked out

Lesson 13.3: Defacement

Skills Learned From This Lesson: Definition, Mitigation, Detection

- Defacement
    - A threat actor may modify visual content available internal or externally to an enterprise network.
    - Reasons can include delivering a message, or claiming credit for an intrusion.
    - Internal can include changing internal forms or posting disturbing content to internal sites to attempt to get the organization to comply with a request.
    - External can be defacement of a website or other externally facing resource.
- Mitigation Techniques
    - Conduct regular backups of critical systems
- Detection Techniques

- Monitor internal and external sites for unplanned changes

Lesson 13.4: Impact Case Study
Skills Learned From This Lesson: Case Study, Impact, Example

- Rather Be Safe Than Sorry
  - Top Disaster Recovery Failures
    - The Media is not working (device failure)
    - Human error
      - Improper backup scheduling
      - Improper storage
    - Software updates lead to failure
    - Threat Actors remove backups
    - Infrastructure Issues
- Points to Consider
  - How do you know if the plan will work?
  - Do you test backups ever?
  - Do you have the ability to recover in a timely manner?
  - Have you ever validated that your system administrators are backing up the right information?

Lesson 13.5: Module 13 Summary
Skills Learned From This Lesson: Summary, Impact, Module

- Summary of what was covered in this module

Module 14: Conclusion

Lesson 14.1: Course Summary
Skills Learned From This Lesson: Summary, Course, Outro

- What Should We Know?
  - What Phases Did We Cover
    - Initial Access
    - Execution
    - Persistence
    - Privilege Escalation
    - Defense Evasion
    - Credential Access

        - Discovery
        - Lateral Movement
        - Collection
        - Command and Control
        - Exfiltration
        - Impact
- The Key Points
    - Threat actors aren't always easy to spot
    - Threat actors are crafty in their ability to bypass controls
        - Threat Actors have ways to bypass automated controls
        - Human intervention and review is a must
    - End User Awareness Training and Dues Diligence can make a difference
        - Mapping Your efforts can aid in overall risk reduction and attack surface awareness