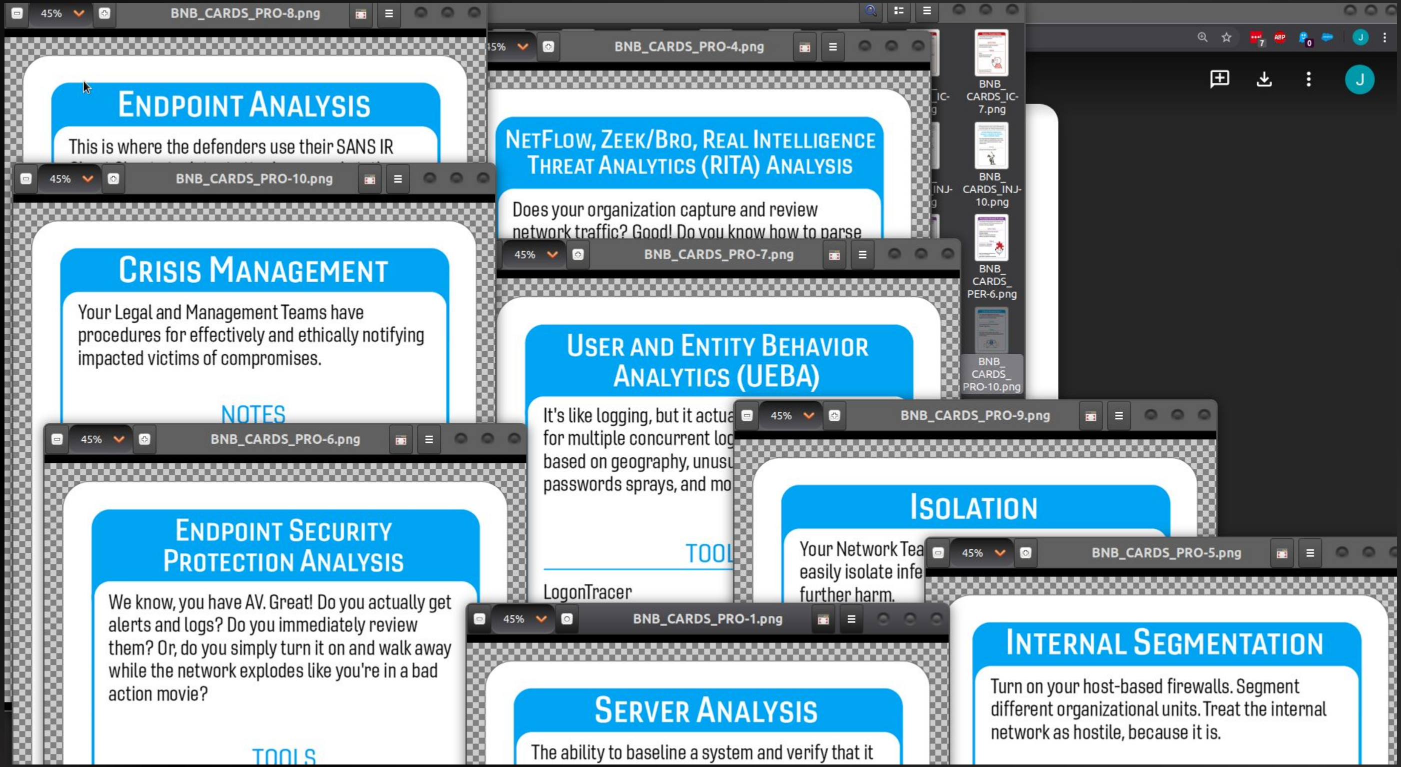
Getting Started With BHIS: SOC Analyst Key Skills

John Strand

The Right Way

SOC "Legos"



Endpoint Analysis

This is where the defenders use their SANS IR

NetFlow, Zeek/Bro, Real Intelligence Threat Analytics (RITA) Analysis

Does your organization capture and review network traffic? Good! Do you know how to parse

Crisis Management

Your Legal and Management Teams have procedures for effectively and ethically notifying impacted victims of compromises.

NOTES

User and Entity Behavior Analytics (UEBA)

It's like logging, but it actua
for multiple concurrent log
based on geography, unusu
passwords sprays, and mo

TOOL

LogonTracer

Endpoint Security Protection Analysis

We know, you have AV. Great! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes like you're in a bad action movie?

TOOLS

Isolation

Your Network Tea
easily isolate infe
further harm.

Internal Segmentation

Turn on your host-based firewalls. Segment different organizational units. Treat the internal network as hostile, because it is.

Server Analysis

The ability to baseline a system and verify that it

BLACK HILLS
Information Security
CELEBRATING 10 YEARS
• 2008-2018 •

Server Analysis

Key Server Points

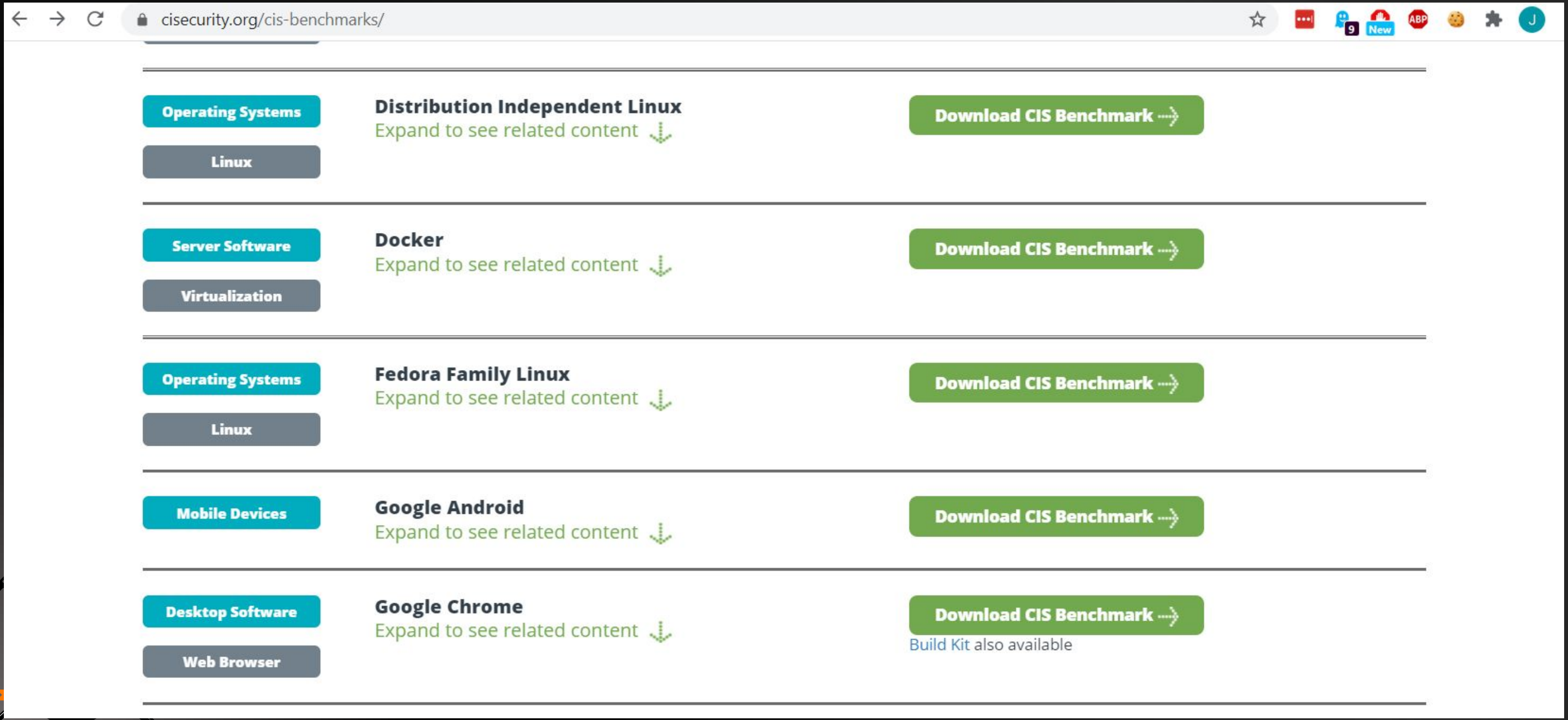
- Look at the following:
  - Processes
  - Users
  - Network Connections
  - Open Ports
  - Logs
- How is this different from looking at endpoints?
  - We are looking at all the above as it relates to the server processes!
  - This becomes even more important in the cloud

How To Learn This?

Hardening guides…. Yeah… That's it..

R T F M

CIS

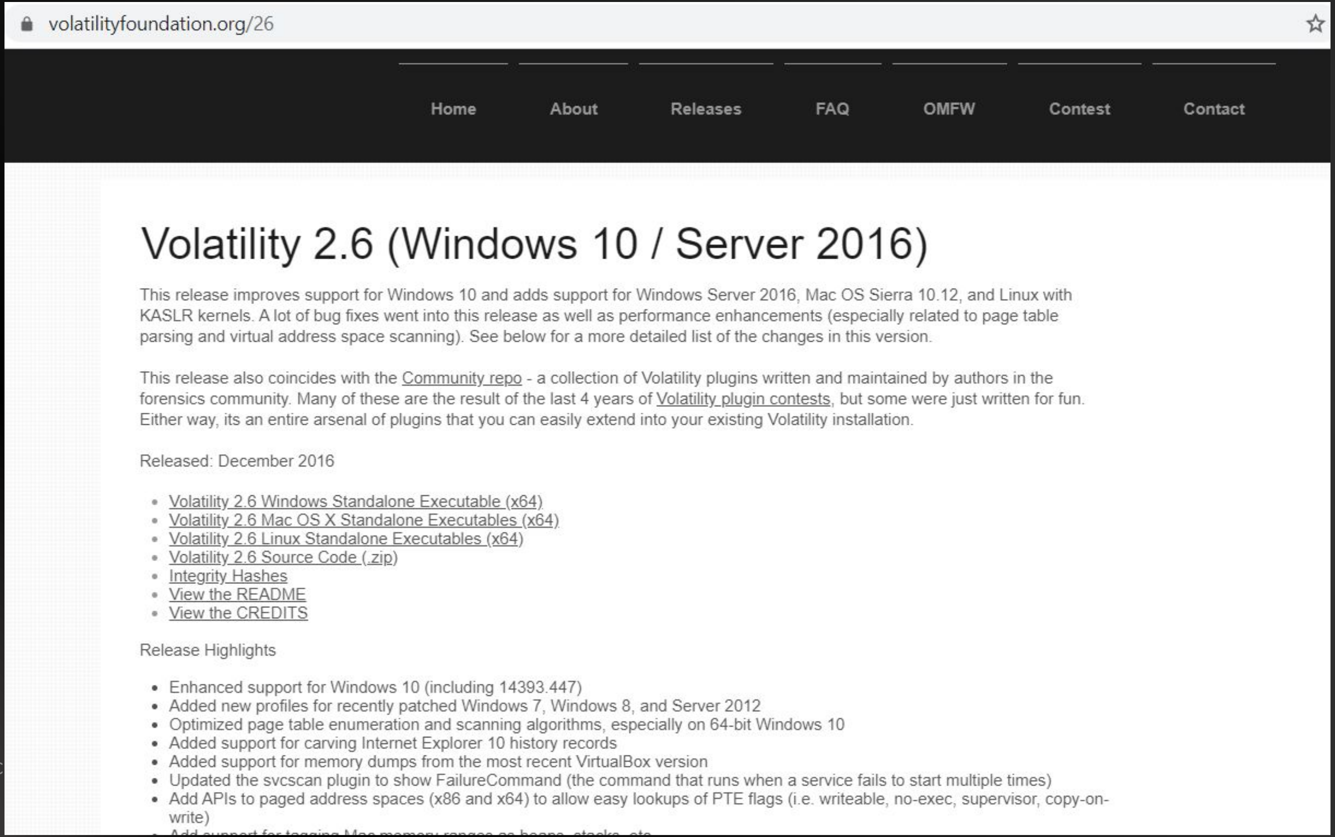


cisecurity.org/cis-benchmarks/

Operating Systems Linux	**Distribution Independent Linux** Expand to see related content	Download CIS Benchmark
Server Software Virtualization	**Docker** Expand to see related content	Download CIS Benchmark
Operating Systems Linux	**Fedora Family Linux** Expand to see related content	Download CIS Benchmark
Mobile Devices	**Google Android** Expand to see related content	Download CIS Benchmark
Desktop Software Web Browser	**Google Chrome** Expand to see related content	Download CIS Benchmark Build Kit also available

Memory Forensics

Volatility



Volatility 2.6 (Windows 10 / Server 2016)

This release improves support for Windows 10 and adds support for Windows Server 2016, Mac OS Sierra 10.12, and Linux with KASLR kernels. A lot of bug fixes went into this release as well as performance enhancements (especially related to page table parsing and virtual address space scanning). See below for a more detailed list of the changes in this version.

This release also coincides with the Community repo - a collection of Volatility plugins written and maintained by authors in the forensics community. Many of these are the result of the last 4 years of Volatility plugin contests, but some were just written for fun. Either way, its an entire arsenal of plugins that you can easily extend into your existing Volatility installation.

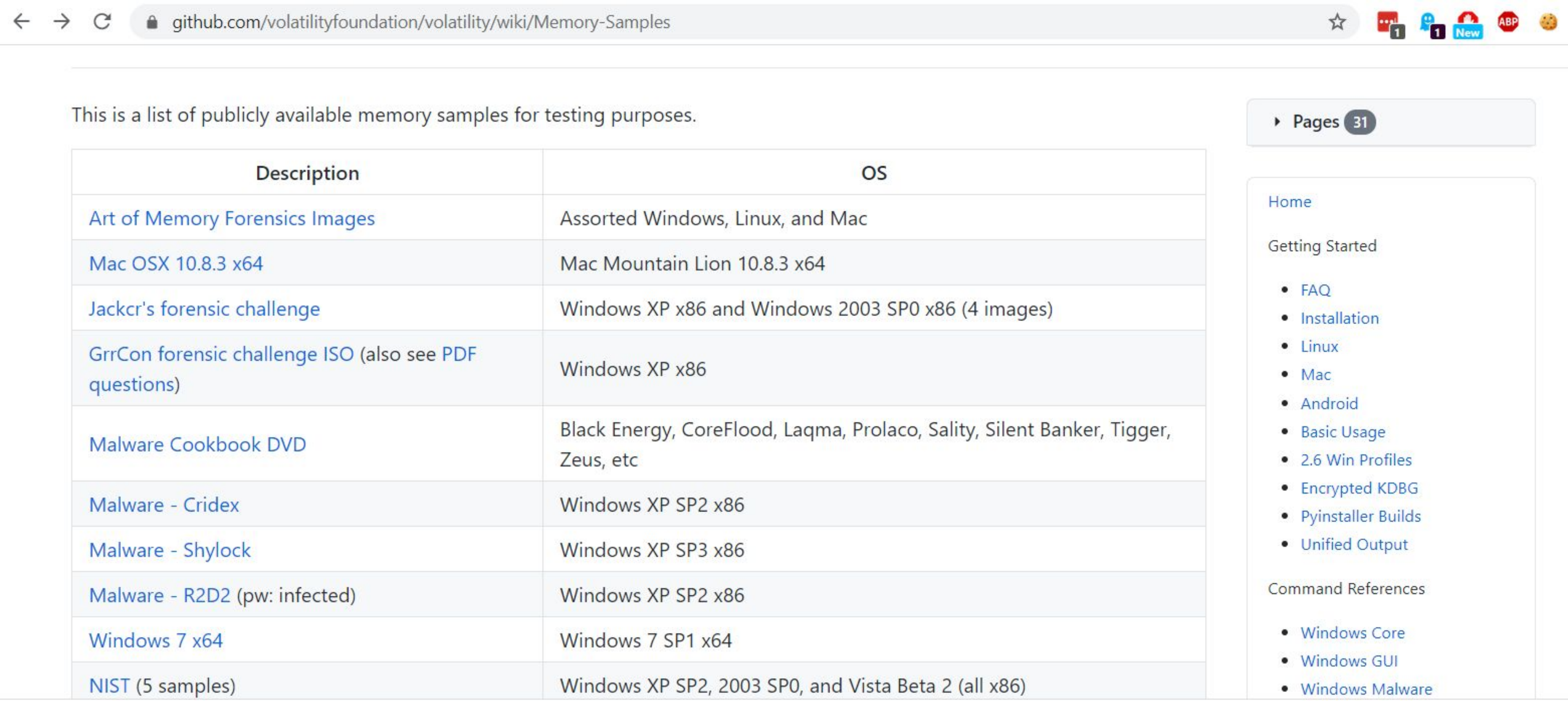
Released: December 2016

- Volatility 2.6 Windows Standalone Executable (x64)
- Volatility 2.6 Mac OS X Standalone Executables (x64)
- Volatility 2.6 Linux Standalone Executables (x64)
- Volatility 2.6 Source Code (.zip)
- Integrity Hashes
- View the README
- View the CREDITS

Release Highlights

- Enhanced support for Windows 10 (including 14393.447)
- Added new profiles for recently patched Windows 7, Windows 8, and Server 2012
- Optimized page table enumeration and scanning algorithms, especially on 64-bit Windows 10
- Added support for carving Internet Explorer 10 history records
- Added support for memory dumps from the most recent VirtualBox version
- Updated the svcscan plugin to show FailureCommand (the command that runs when a service fails to start multiple times)
- Add APIs to paged address spaces (x86 and x64) to allow easy lookups of PTE flags (i.e. writeable, no-exec, supervisor, copy-on-write)
- Add support for tagging Mac memory ranges as heaps, stacks, etc

Go Learn!



github.com/volatilityfoundation/volatility/wiki/Memory-Samples

This is a list of publicly available memory samples for testing purposes.

Description	OS
Art of Memory Forensics Images	Assorted Windows, Linux, and Mac
Mac OSX 10.8.3 x64	Mac Mountain Lion 10.8.3 x64
Jackcr's forensic challenge	Windows XP x86 and Windows 2003 SP0 x86 (4 images)
GrrCon forensic challenge ISO (also see PDF questions)	Windows XP x86
Malware Cookbook DVD	Black Energy, CoreFlood, Laqma, Prolaco, Sality, Silent Banker, Tigger, Zeus, etc
Malware - Cridex	Windows XP SP2 x86
Malware - Shylock	Windows XP SP3 x86
Malware - R2D2 (pw: infected)	Windows XP SP2 x86
Windows 7 x64	Windows 7 SP1 x64
NIST (5 samples)	Windows XP SP2, 2003 SP0, and Vista Beta 2 (all x86)

Links

https://www.youtube.com/watch?v=HcUMXxyYsnw&ab_channel=JohnStrand

https://www.youtube.com/watch?v=BMFCdAGxVN4&ab_channel=BlackHat

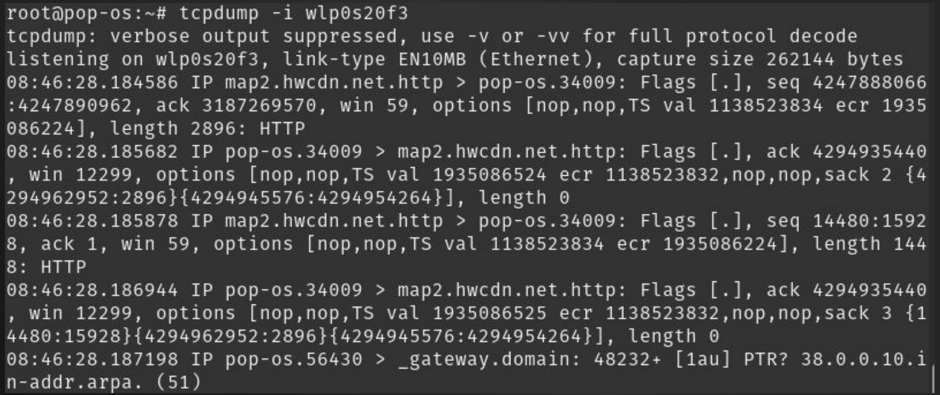
https://www.youtube.com/watch?v=R6ZvEIyS_O4&ab_channel=BlackPerl

Egress Traffic Analysis

Zeek

- Speed
- Large user base
- Lots of support
- Consistency
- Timestamps are key
- Many devices handle timestamps in different/odd ways
- Generates required log files
- We are moving away from signature-based detection
- Too many ways to obfuscate
- Encryption, Encoding, use of third-party services like Google DNS

Full pcap

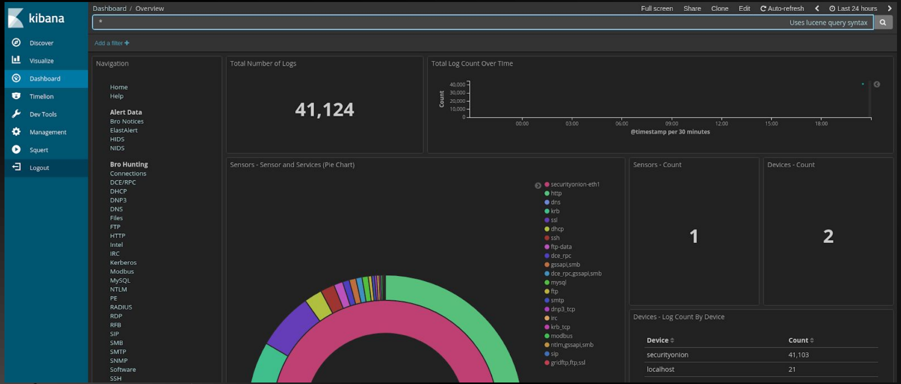


```
root@pop-os:~# tcpdump -i wlp0s20f3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp0s20f3, link-type EN10MB (Ethernet), capture size 262144 bytes
08:46:28.184586 IP map2.hwcdn.net.http > pop-os.34009: Flags [.], seq 4247888066
:4247890962, ack 3187269570, win 59, options [nop,nop,TS val 1138523834 ecr 1935
086224], length 2896: HTTP
08:46:28.185682 IP pop-os.34009 > map2.hwcdn.net.http: Flags [.], ack 4294935440
, win 12299, options [nop,nop,TS val 1935086524 ecr 1138523832,nop,nop,sack 2 {4
294962952:2896}{4294945576:4294954264}], length 0
08:46:28.185878 IP map2.hwcdn.net.http > pop-os.34009: Flags [.], seq 14480:1592
8, ack 1, win 59, options [nop,nop,TS val 1138523834 ecr 1935086224], length 144
8: HTTP
08:46:28.186944 IP pop-os.34009 > map2.hwcdn.net.http: Flags [.], ack 4294935440
, win 12299, options [nop,nop,TS val 1935086525 ecr 1138523832,nop,nop,sack 3 {1
4480:15928}{4294962952:2896}{4294945576:4294954264}], length 0
08:46:28.187198 IP pop-os.56430 > _gateway.domain: 48232+ [1au] PTR? 38.0.0.10.i
n-addr.arpa. (51)
```

- Very portable
- Everything supports it
- Issues of size
- Encryption can cause issues
- Learning curve
- Tcpdump and Wireshark are the key tools to learn
- Let’s play with it now

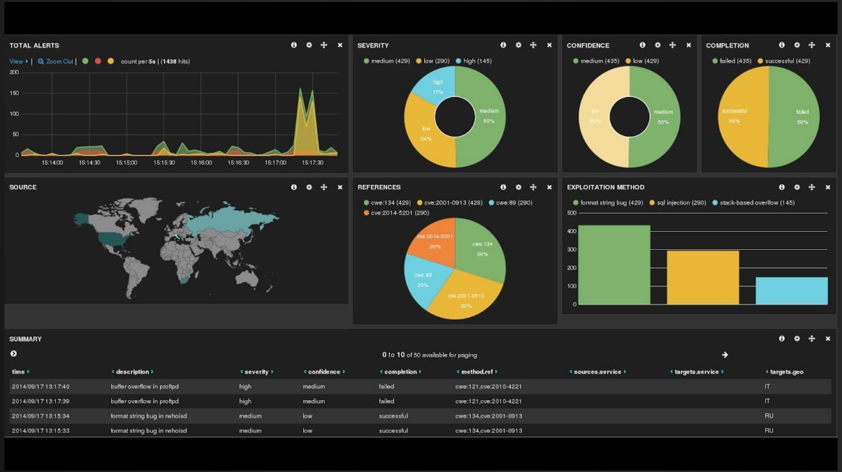
Security Onion

- Security Onion is free and kicks most commercial tools to the curb
- They offer training
- Zeek, Suricata and so much more are included
- Works with RITA!!!



Devices - Log Count By Device

Device	Count
securityonion	41,103
localhost	21



time	description	severity	confidence	completion	method.ref	sources.service	targets.service	targets.geo
2014/09/17 13:17:40	buffer overflow in proftpd	high	medium	failed	cwe:121,cve:2010-4221			IT
2014/09/17 13:17:39	buffer overflow in proftpd	high	medium	failed	cwe:121,cve:2010-4221			IT
2014/09/17 13:15:34	format string bug in rwhoisd	medium	low	successful	cwe:134,cve:2001-0913			RU
2014/09/17 13:15:33	format string bug in rwhoisd	medium	low	successful	cwe:134,cve:2001-0913			RU

Links

https://www.activecountermeasures.com/blog/

https://www.activecountermeasures.com/category/video-blog/

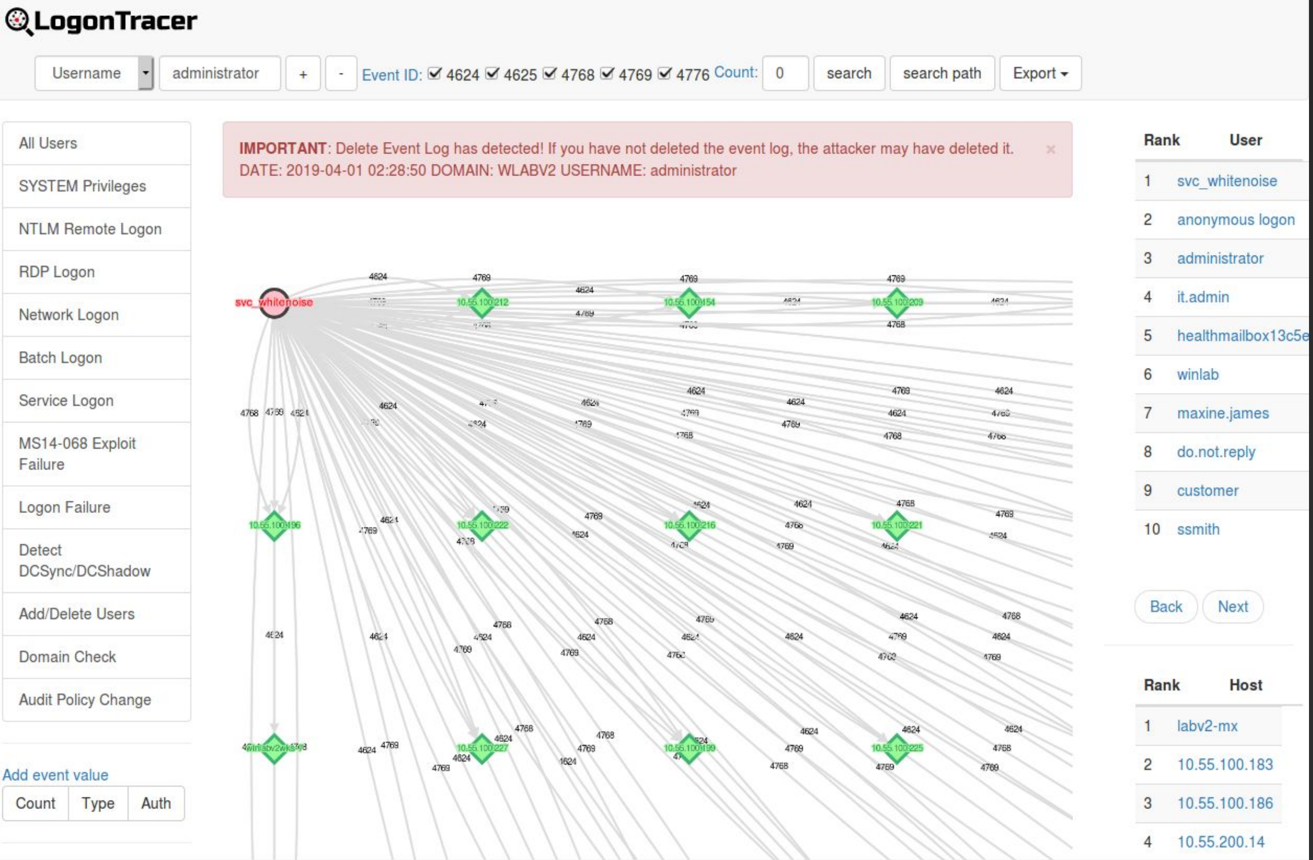
Logs Are A Trainwreck

- There is no “You have been Hacked!!!” Log
- Traditional Windows logs do not log useful data for security
- An example of changing the security policy
- Less than 5% detects are from logs
- Logs and percentages?
- Linux Logs are not much better
    - Note on Bash logging

Why UEBA?

- Let's look at behaviors of attacks
- Reflected in the logs
- Reflected across multiple logs!!!
- Can require AD, Exchange and OWA logs to tell a story
- Often requires log tuning
- For example: Internal Password Spray
    - One ID, accessing multiple systems

Lateral Movement



LogonTracer

Username ▾ | administrator | + | - | Event ID: ☑ 4624 ☑ 4625 ☑ 4768 ☑ 4769 ☑ 4776 Count: 0 | search | search path | Export ▾

- All Users
- SYSTEM Privileges
- NTLM Remote Logon
- RDP Logon
- Network Logon
- Batch Logon
- Service Logon
- MS14-068 Exploit Failure
- Logon Failure
- Detect DCSync/DCShadow
- Add/Delete Users
- Domain Check
- Audit Policy Change

Add event value

Count | Type | Auth

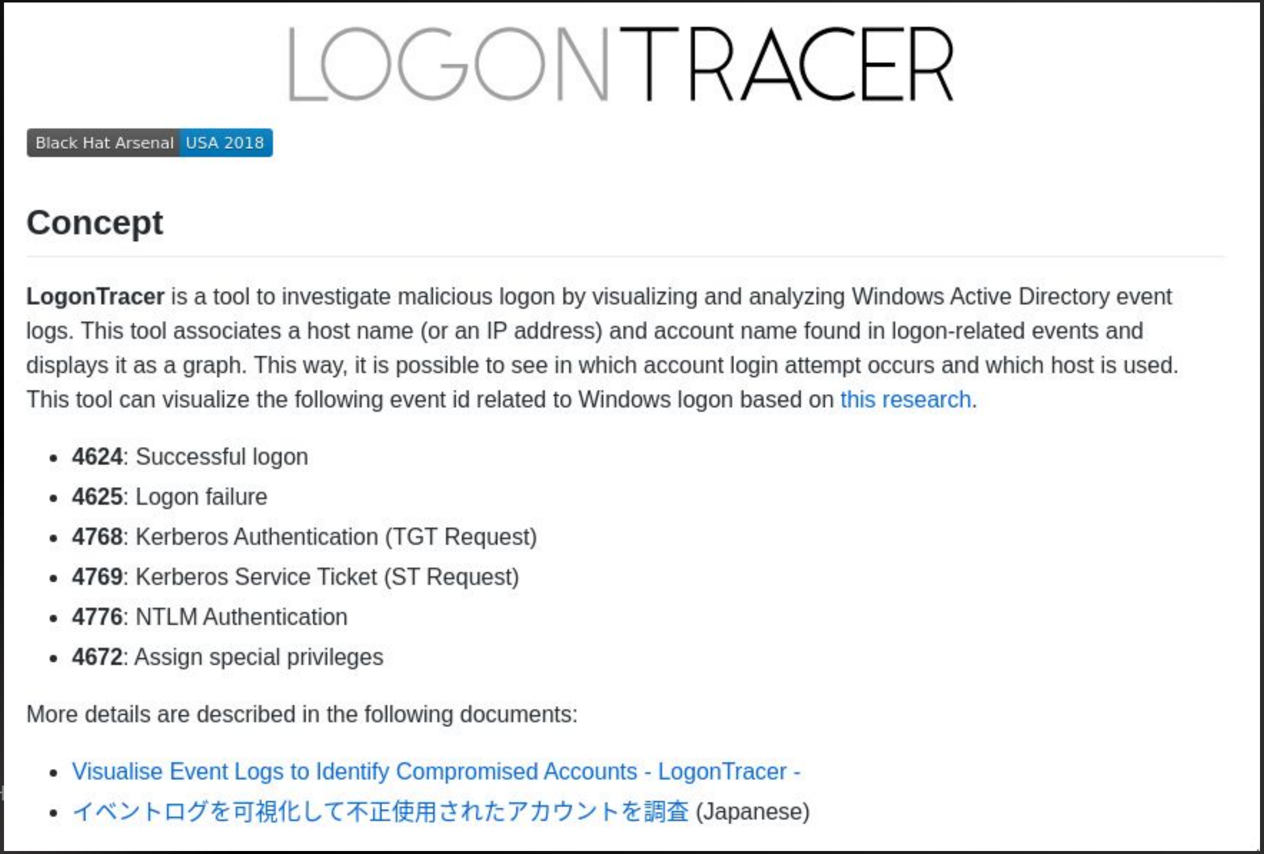
IMPORTANT: Delete Event Log has detected! If you have not deleted the event log, the attacker may have deleted it. ×
DATE: 2019-04-01 02:28:50 DOMAIN: WLABV2 USERNAME: administrator

Rank	User
1	svc_whitenoise
2	anonymous logon
3	administrator
4	it.admin
5	healthmailbox13c5e
6	winlab
7	maxine.james
8	do.not.reply
9	customer
10	ssmith

Back | Next

Rank	Host
1	labv2-mx
2	10.55.100.183
3	10.55.100.186
4	10.55.200.14

6 Event IDs



LOGONTRACER

Black Hat Arsenal USA 2018

Concept

LogonTracer is a tool to investigate malicious logon by visualizing and analyzing Windows Active Directory event logs. This tool associates a host name (or an IP address) and account name found in logon-related events and displays it as a graph. This way, it is possible to see in which account login attempt occurs and which host is used. This tool can visualize the following event id related to Windows logon based on this research.

- **4624**: Successful logon
- **4625**: Logon failure
- **4768**: Kerberos Authentication (TGT Request)
- **4769**: Kerberos Service Ticket (ST Request)
- **4776**: NTLM Authentication
- **4672**: Assign special privileges

More details are described in the following documents:

- Visualise Event Logs to Identify Compromised Accounts - LogonTracer -
- イベントログを可視化して不正使用されたアカウントを調査 (Japanese)

“False Positives”

- Not a thing (Watch people's heads explode)
- Usually a problem of tuning
- Service accounts
- Help Desk
- Systems administrators
- Scripts
- Backups
- TUNING TUNING TUNING <- This is our job!

Links

https://www.blackhillsinfosec.com/tag/elk/

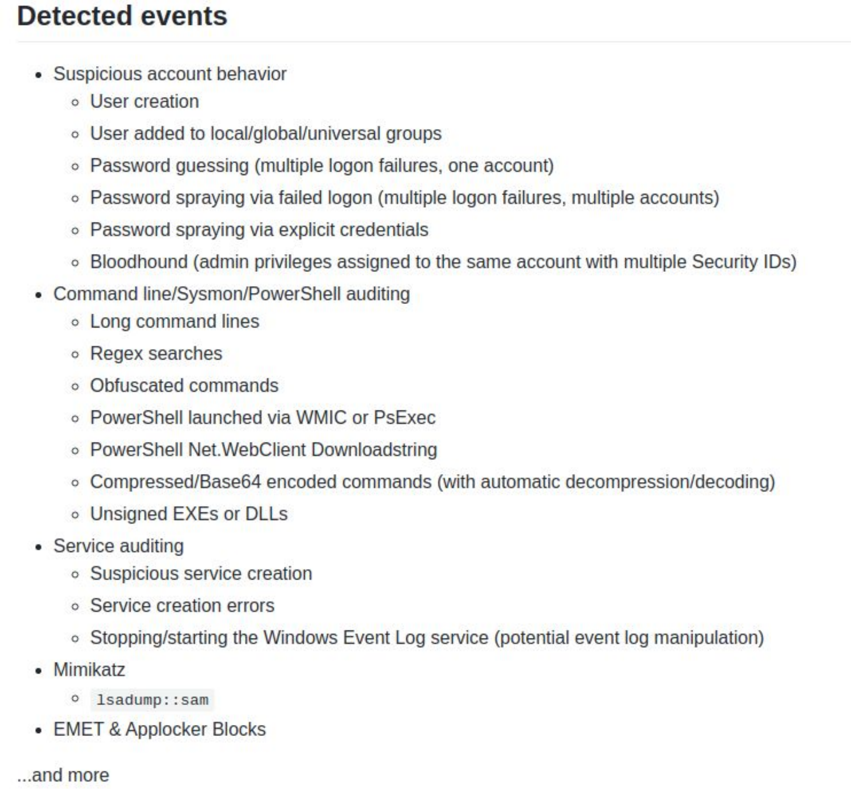
https://www.youtube.com/watch?v=c0qOmu3pChc&ab_channel=BlackHillsInformationSecurity

https://www.youtube.com/watch?v=jL6Somex_58&ab_channel=BlackHillsInformationSecurity

Endpoint Analysis

DeepBlueCLI

- https://github.com/sans-blue-team/DeepBlueCLI

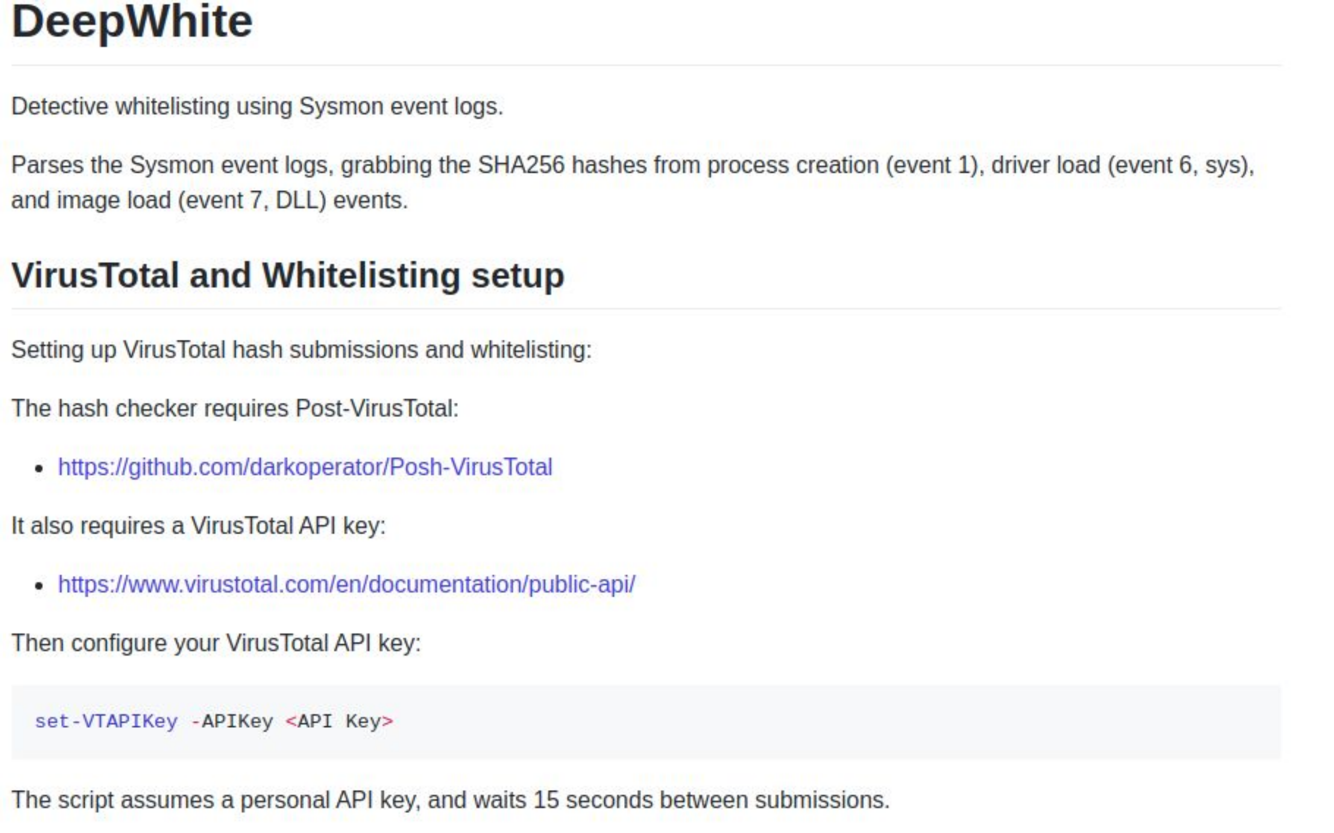


Detected events

- Suspicious account behavior
  - User creation
  - User added to local/global/universal groups
  - Password guessing (multiple logon failures, one account)
  - Password spraying via failed logon (multiple logon failures, multiple accounts)
  - Password spraying via explicit credentials
  - Bloodhound (admin privileges assigned to the same account with multiple Security IDs)
- Command line/Sysmon/PowerShell auditing
  - Long command lines
  - Regex searches
  - Obfuscated commands
  - PowerShell launched via WMIC or PsExec
  - PowerShell Net.WebClient Downloadstring
  - Compressed/Base64 encoded commands (with automatic decompression/decoding)
  - Unsigned EXEs or DLLs
- Service auditing
  - Suspicious service creation
  - Service creation errors
  - Stopping/starting the Windows Event Log service (potential event log manipulation)
- Mimikatz
  - `lsadump::sam`
- EMET & Applocker Blocks

...and more

DeepWhiteCLI



DeepWhite

Detective whitelisting using Sysmon event logs.

Parses the Sysmon event logs, grabbing the SHA256 hashes from process creation (event 1), driver load (event 6, sys), and image load (event 7, DLL) events.

VirusTotal and Whitelisting setup

Setting up VirusTotal hash submissions and whitelisting:

The hash checker requires Post-VirusTotal:

- https://github.com/darkoperator/Posh-VirusTotal

It also requires a VirusTotal API key:

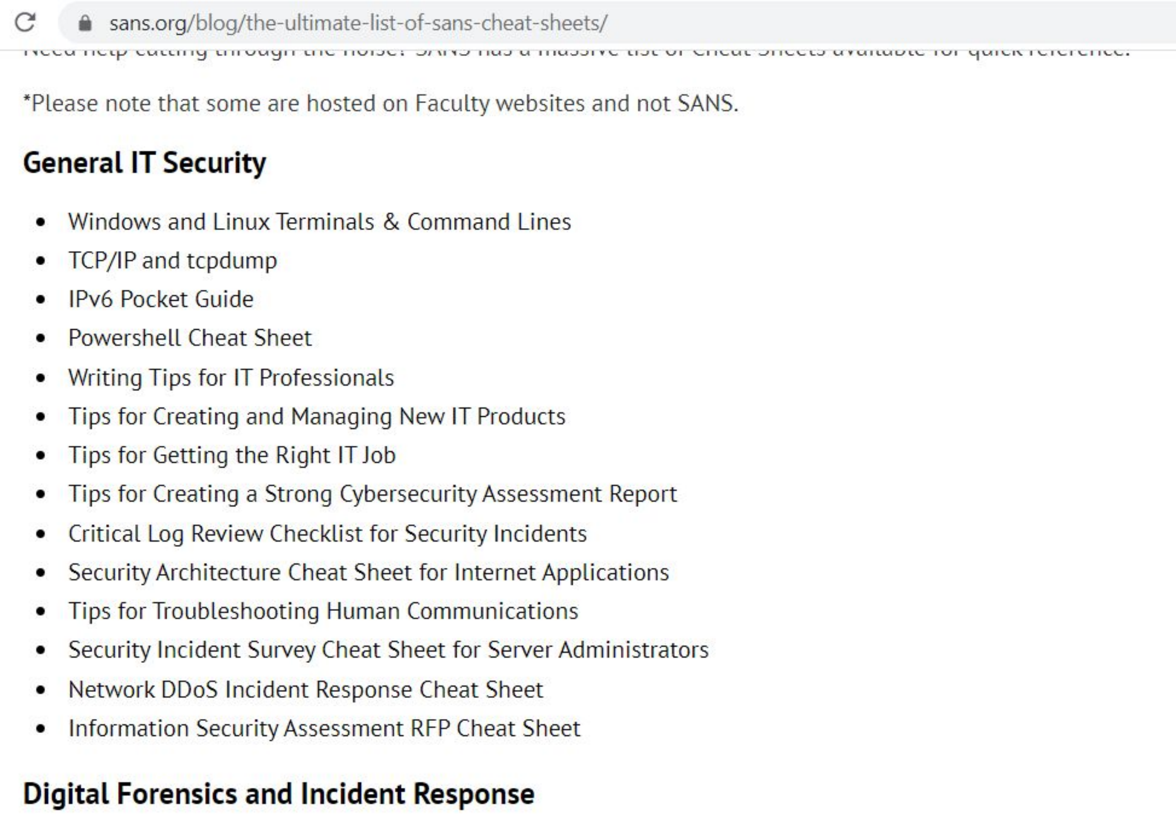
- https://www.virustotal.com/en/documentation/public-api/

Then configure your VirusTotal API key:

```
set-VTAPIKey -APIKey <API Key>
```

The script assumes a personal API key, and waits 15 seconds between submissions.

SANS Cheat Sheets



sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/

Need help cutting through the noise? SANS has a massive list of Cheat Sheets available for quick reference.

*Please note that some are hosted on Faculty websites and not SANS.

General IT Security

- Windows and Linux Terminals & Command Lines
- TCP/IP and tcpdump
- IPv6 Pocket Guide
- Powershell Cheat Sheet
- Writing Tips for IT Professionals
- Tips for Creating and Managing New IT Products
- Tips for Getting the Right IT Job
- Tips for Creating a Strong Cybersecurity Assessment Report
- Critical Log Review Checklist for Security Incidents
- Security Architecture Cheat Sheet for Internet Applications
- Tips for Troubleshooting Human Communications
- Security Incident Survey Cheat Sheet for Server Administrators
- Network DDoS Incident Response Cheat Sheet
- Information Security Assessment RFP Cheat Sheet

Digital Forensics and Incident Response

Links

https://www.blackhillsinfosec.com/rainy-day-windows-command-research-results/

https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/

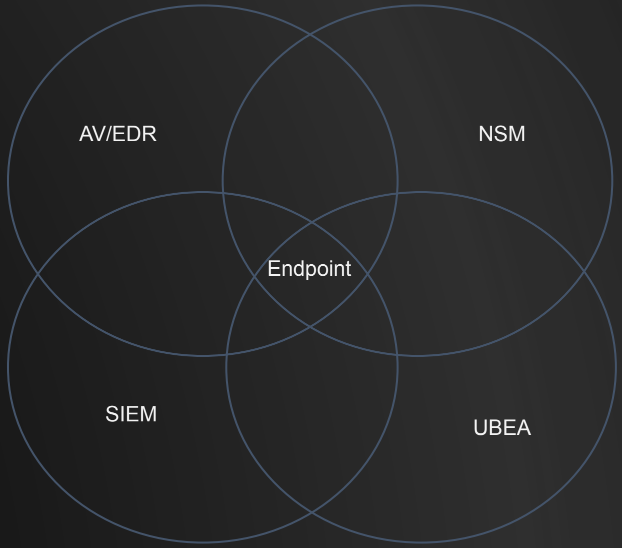
https://www.youtube.com/watch?v=fEip9gl2MTA&t=17s&ab_channel=BlackHillsInformationSecurity

https://www.youtube.com/watch?v=dtyX7XO-GSg&ab_channel=BlackHillsInformationSecurity

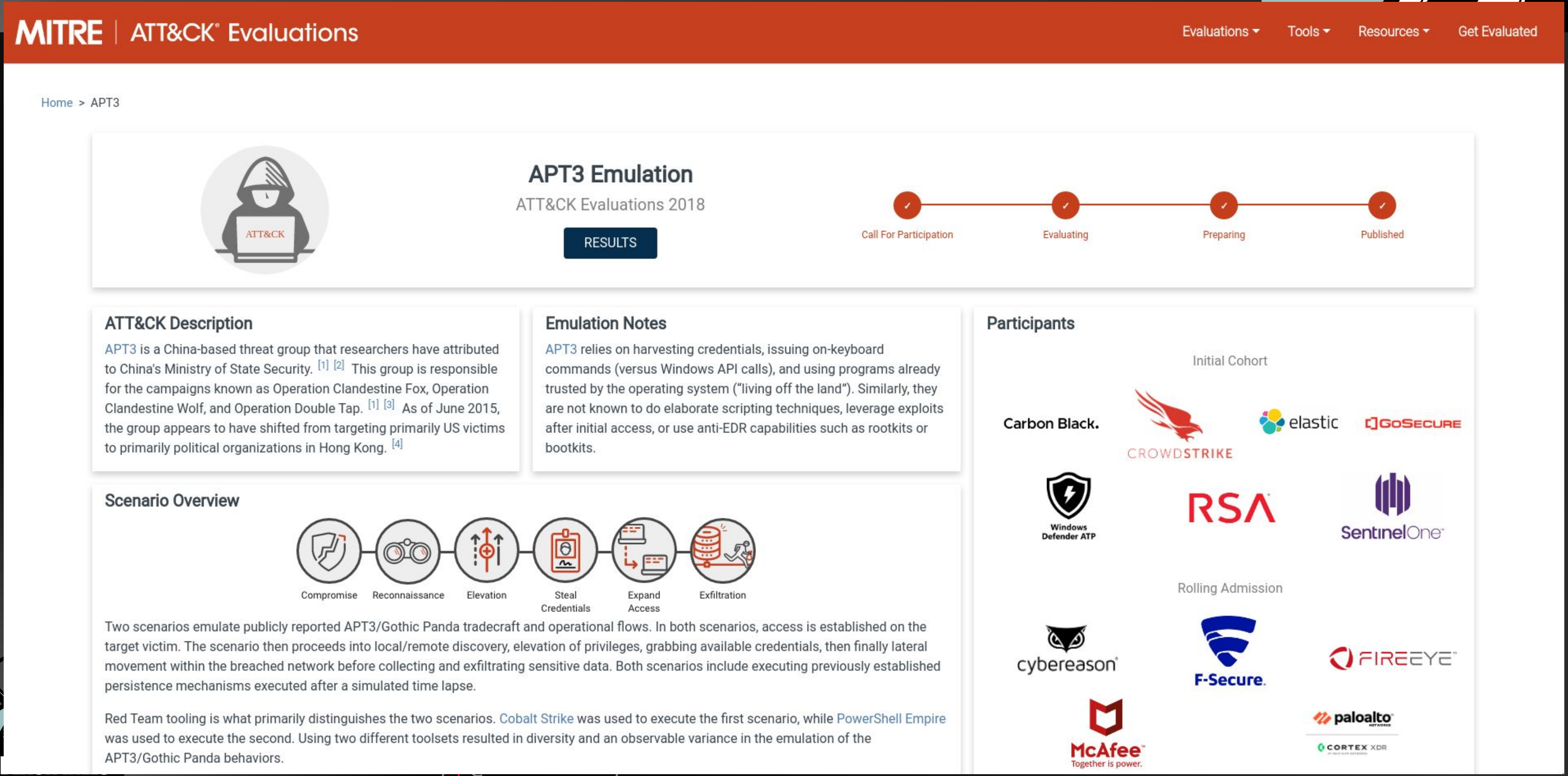
Endpoint Protection Analysis

Overlapping Fields of View

- The key is overlapping fields of visibility
- Endpoint
- SIEM/UBEA
- Network Monitoring
- Sandboxing
- Internal Segmentation



Everyone's a Winner!



Home > APT3

APT3 Emulation

ATT&CK Evaluations 2018

RESULTS

ATT&CK Description

APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security. [1] [2] This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap. [1] [3] As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong. [4]

Emulation Notes

APT3 relies on harvesting credentials, issuing on-keyboard commands (versus Windows API calls), and using programs already trusted by the operating system ("living off the land"). Similarly, they are not known to do elaborate scripting techniques, leverage exploits after initial access, or use anti-EDR capabilities such as rootkits or bootkits.

Scenario Overview

Two scenarios emulate publicly reported APT3/Gothic Panda tradecraft and operational flows. In both scenarios, access is established on the target victim. The scenario then proceeds into local/remote discovery, elevation of privileges, grabbing available credentials, then finally lateral movement within the breached network before collecting and exfiltrating sensitive data. Both scenarios include executing previously established persistence mechanisms executed after a simulated time lapse.

Red Team tooling is what primarily distinguishes the two scenarios. Cobalt Strike was used to execute the first scenario, while PowerShell Empire was used to execute the second. Using two different toolsets resulted in diversity and an observable variance in the emulation of the APT3/Gothic Panda behaviors.

Participants

Initial Cohort

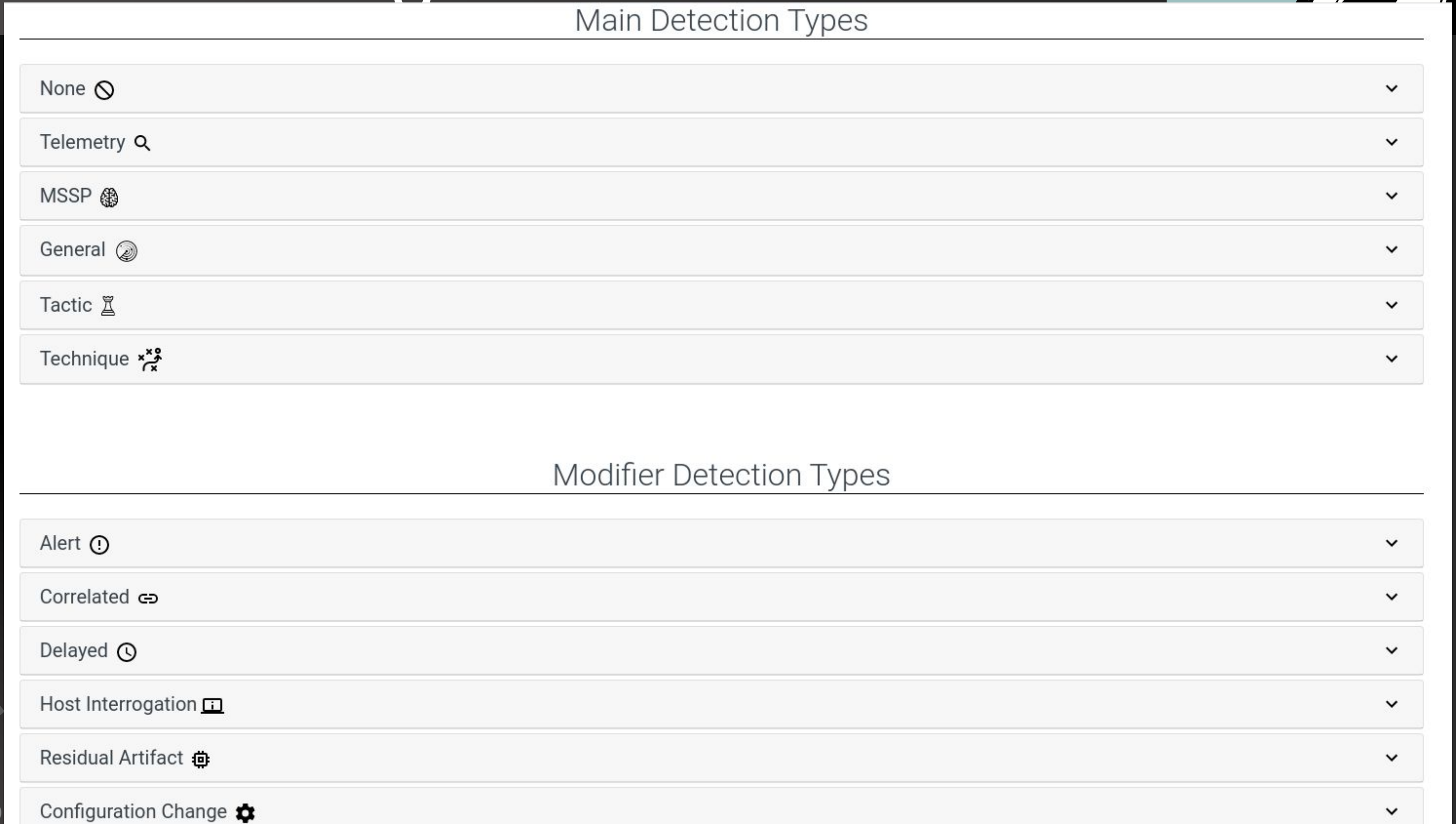
Carbon Black. CROWDSTRIKE elastic GoSecure Windows Defender ATP RSA SentinelOne

Rolling Admission

cybereason F-Secure FIREEYE McAfee Together is power. paloalto CORTEX XDR

Information Security
CELEBRATING 10 YEARS
• 2008-2018 •

Detection Categories



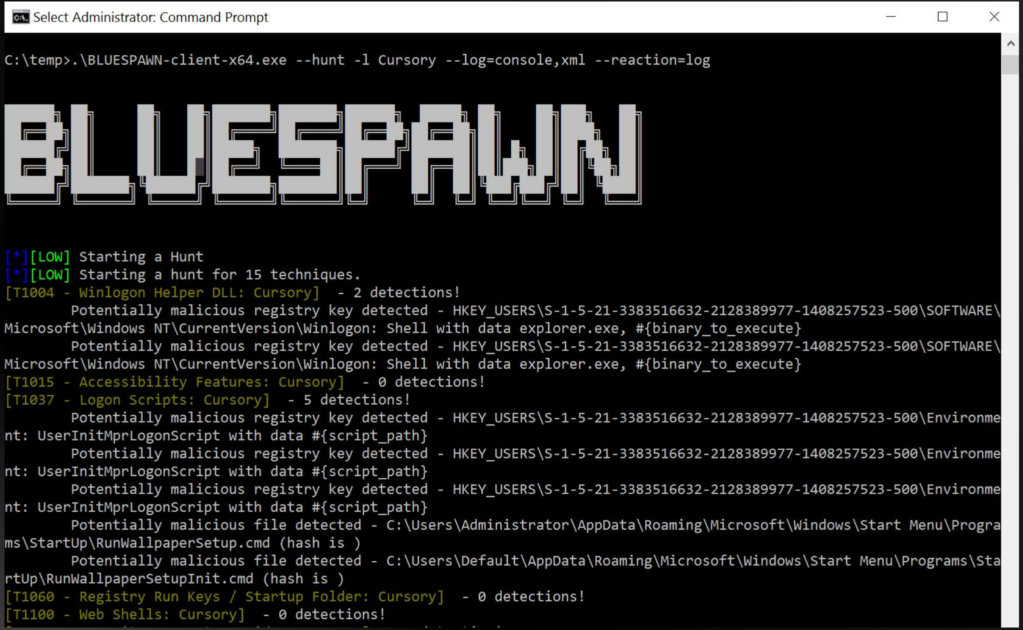
Main Detection Types

- None
- Telemetry
- MSSP
- General
- Tactic
- Technique

Modifier Detection Types

- Alert
- Correlated
- Delayed
- Host Interrogation
- Residual Artifact
- Configuration Change

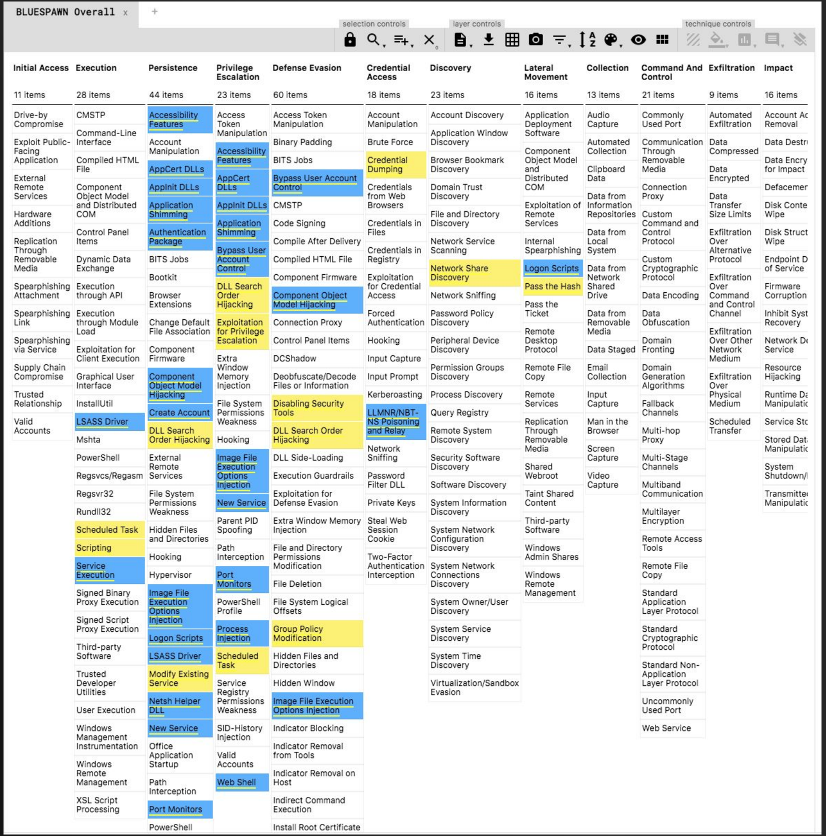
Play at Home!: EDR with Bluespawn



```
C:\temp>.\BLUESPAWN-client-x64.exe --hunt -l Cursory --log=console,xml --reaction=log

BLUESPAWN

[*][LOW] Starting a Hunt
[*][LOW] Starting a hunt for 15 techniques.
[T1004 - Winlogon Helper DLL: Cursory]  - 2 detections!
        Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\SOFTWARE\
Microsoft\Windows NT\CurrentVersion\Winlogon: Shell with data explorer.exe, #{binary_to_execute}
        Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\SOFTWARE\
Microsoft\Windows NT\CurrentVersion\Winlogon: Shell with data explorer.exe, #{binary_to_execute}
[T1015 - Accessibility Features: Cursory]  - 0 detections!
[T1037 - Logon Scripts: Cursory]  - 5 detections!
        Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\Environme
nt: UserInitMprLogonScript with data #{script_path}
        Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\Environme
nt: UserInitMprLogonScript with data #{script_path}
        Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\Environme
nt: UserInitMprLogonScript with data #{script_path}
        Potentially malicious file detected - C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Progra
ms\StartUp\RunWallpaperSetup.cmd (hash is )
        Potentially malicious file detected - C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Sta
rtUp\RunWallpaperSetupInit.cmd (hash is )
[T1060 - Registry Run Keys / Startup Folder: Cursory]  - 0 detections!
[T1100 - Web Shells: Cursory]  - 0 detections!
```



Initial Access
11 items
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts

Execution
28 items
CMSTP
Command-Line Interface
Compiled HTML File
Component Object Model and Distributed COM
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
LSASS Driver
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
Service Execution
Signed Binary Proxy Execution
Signed Script Proxy Execution
Third-party Software
Trusted Developer Utilities
User Execution
Windows Management Instrumentation
Windows Remote Management
XSL Script Processing

Persistence
44 items
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Hooking
Hypervisor
Image File Execution Options Injection
Logon Scripts
LSASS Driver
Modify Existing Service
Netsh Helper DLL
New Service
Office Application Startup
Path Interception
Port Monitors
PowerShell

Privilege Escalation
23 items
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bypass User Account Control
DLL Search Order Hijacking
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
New Service
Parent PID Spoofing
Path Interception
Port Monitors
PowerShell Profile
Process Injection
Scheduled Task
Service Registry Permissions Weakness
SID-History Injection
Valid Accounts
Web Shell

Defense Evasion
60 items
Access Token Manipulation
Binary Padding
BITS Jobs
Bypass User Account Control
CMSTP
Code Signing
Compile After Delivery
Compiled HTML File
Component Firmware
Component Object Model Hijacking
Connection Proxy
Control Panel Items
DCShadow
Deobfuscate/Decode Files or Information
Disabling Security Tools
DLL Search Order Hijacking
DLL Side-Loading
Execution Guardrails
Exploitation for Defense Evasion
Extra Window Memory Injection
File and Directory Permissions Modification
File Deletion
File System Logical Offsets
Group Policy Modification
Hidden Files and Directories
Hidden Window
Image File Execution Options Injection
Indicator Blocking
Indicator Removal from Tools
Indicator Removal on Host
Indirect Command Execution
Install Root Certificate

Credential Access
18 items
Account Manipulation
Brute Force
Credential Dumping
Credentials from Web Browsers
Credentials in Files
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Input Prompt
Kerberoasting
LLMNR/NBT-NS Poisoning and Relay
Network Sniffing
Password Filter DLL
Private Keys
Steal Web Session Cookie
Two-Factor Authentication Interception

Discovery
23 items
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion

Lateral Movement
16 items
Application Deployment Software
Component Object Model and Distributed COM
Exploitation of Remote Services
Internal Spearphishing
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management

Collection
13 items
Audio Capture
Automated Collection
Clipboard Data
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Man in the Browser
Screen Capture
Video Capture

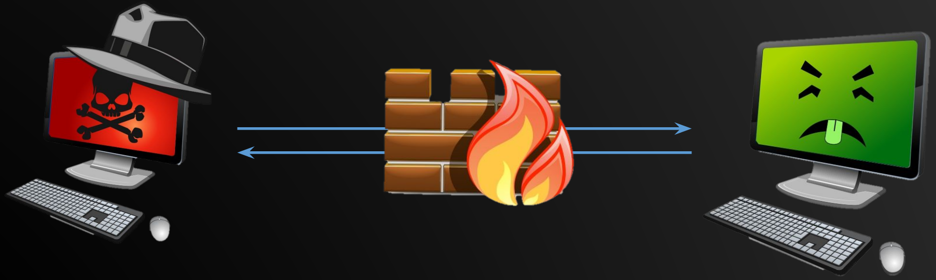
Command And Control
21 items
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Domain Generation Algorithms
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service

Exfiltration
9 items
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Scheduled Transfer

Impact
16 items
Account Ac Removal
Data Destr
Data Encry for Impact
Defacemer
Disk Conte Wipe
Disk Struct Wipe
Endpoint D of Service
Firmware Corruption
Inhibit Syst Recovery
Network De Service
Resource Hijacking
Runtime Da Manipulatio
Service Sto
Stored Dat Manipulatio
System Shutdown/
Transmitte Manipulatio

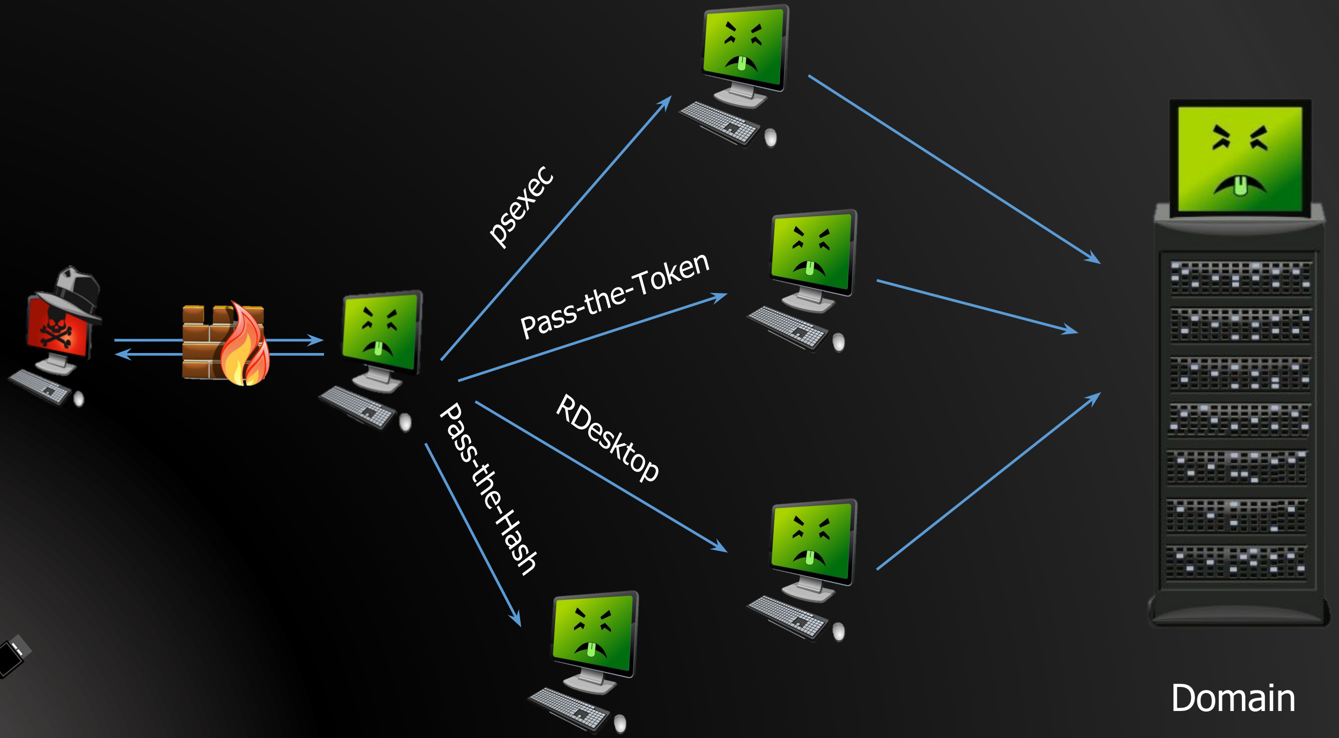
Lateral Movement

Just Your Standard Exploit



This is usually delivered as a client-side exploit or a drive-by download.

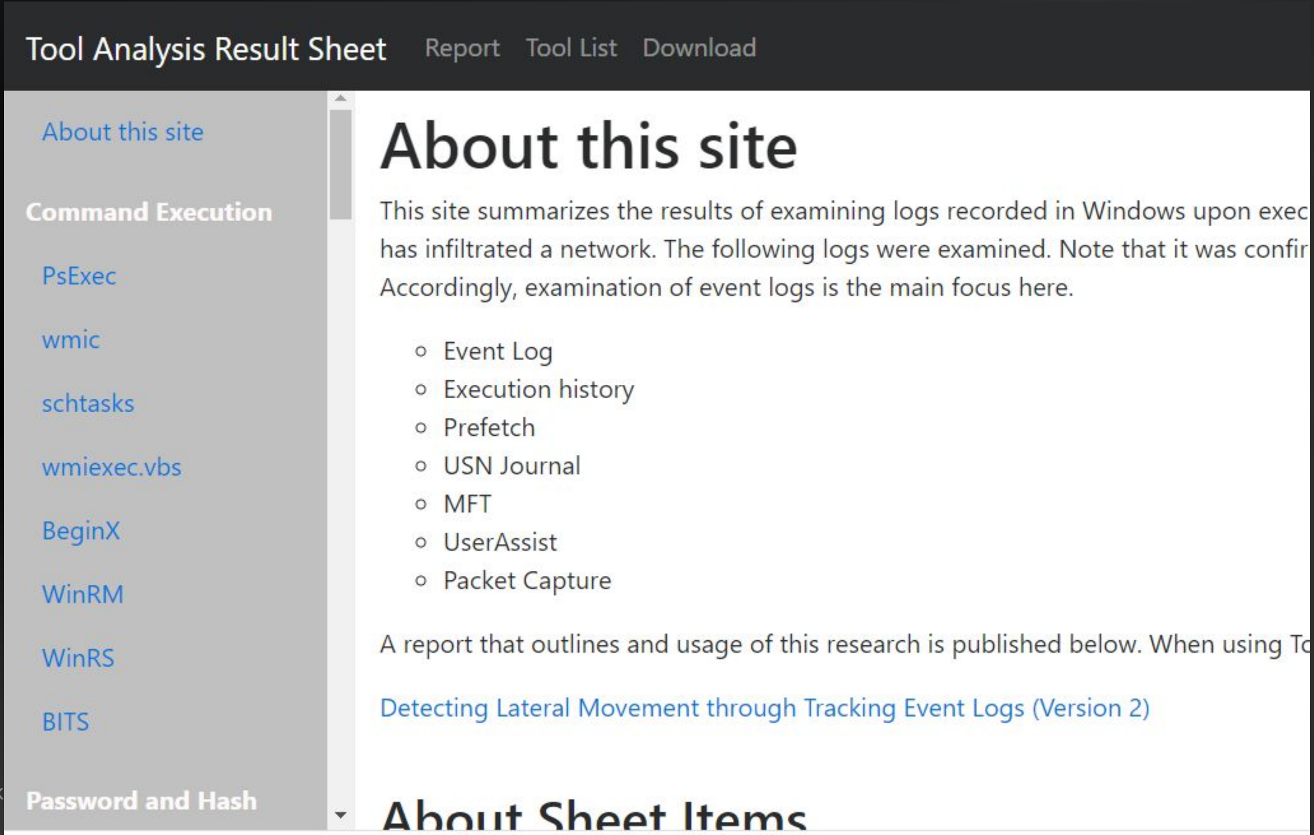
Most Likely They Will Not



Know These Protocols/Commands!

1. SMB
2. Psexec
3. WMI
4. RDP
5. WinRM
6. MS Kerberos
7. LANMAN/NTLM/NTLMv2

JPCert



Tool Analysis Result Sheet   Report   Tool List   Download

About this site

Command Execution

PsExec

wmic

schtasks

wmiexec.vbs

BeginX

WinRM

WinRS

BITS

Password and Hash

About this site

This site summarizes the results of examining logs recorded in Windows upon exec
has infiltrated a network. The following logs were examined. Note that it was confir
Accordingly, examination of event logs is the main focus here.

- Event Log
- Execution history
- Prefetch
- USN Journal
- MFT
- UserAssist
- Packet Capture

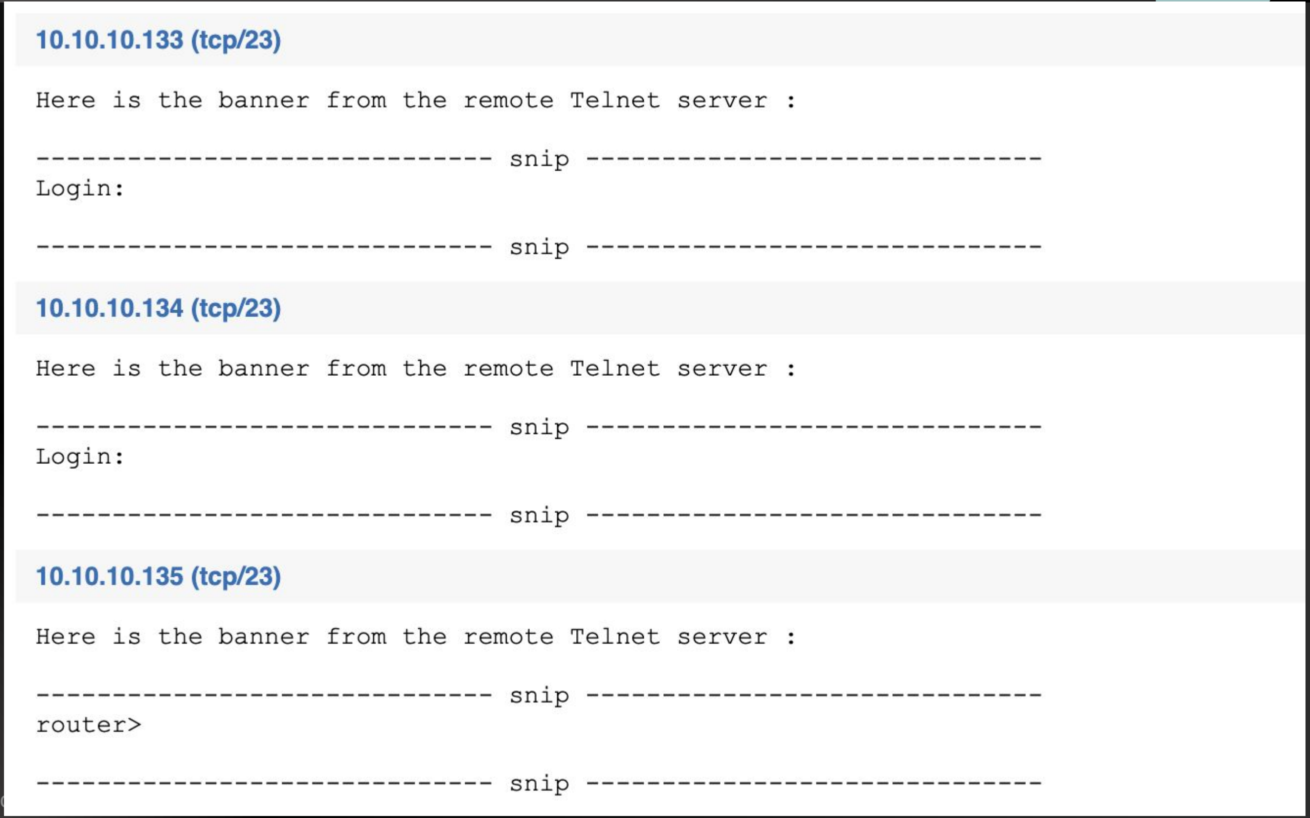
A report that outlines and usage of this research is published below. When using To

Detecting Lateral Movement through Tracking Event Logs (Version 2)

About Sheet Items

Vulnerability Management

Low and Informational Blind Spots: Example



10.10.10.133 (tcp/23)

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------
Login:

------------------------------ snip ------------------------------
```

10.10.10.134 (tcp/23)

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------
Login:

------------------------------ snip ------------------------------
```

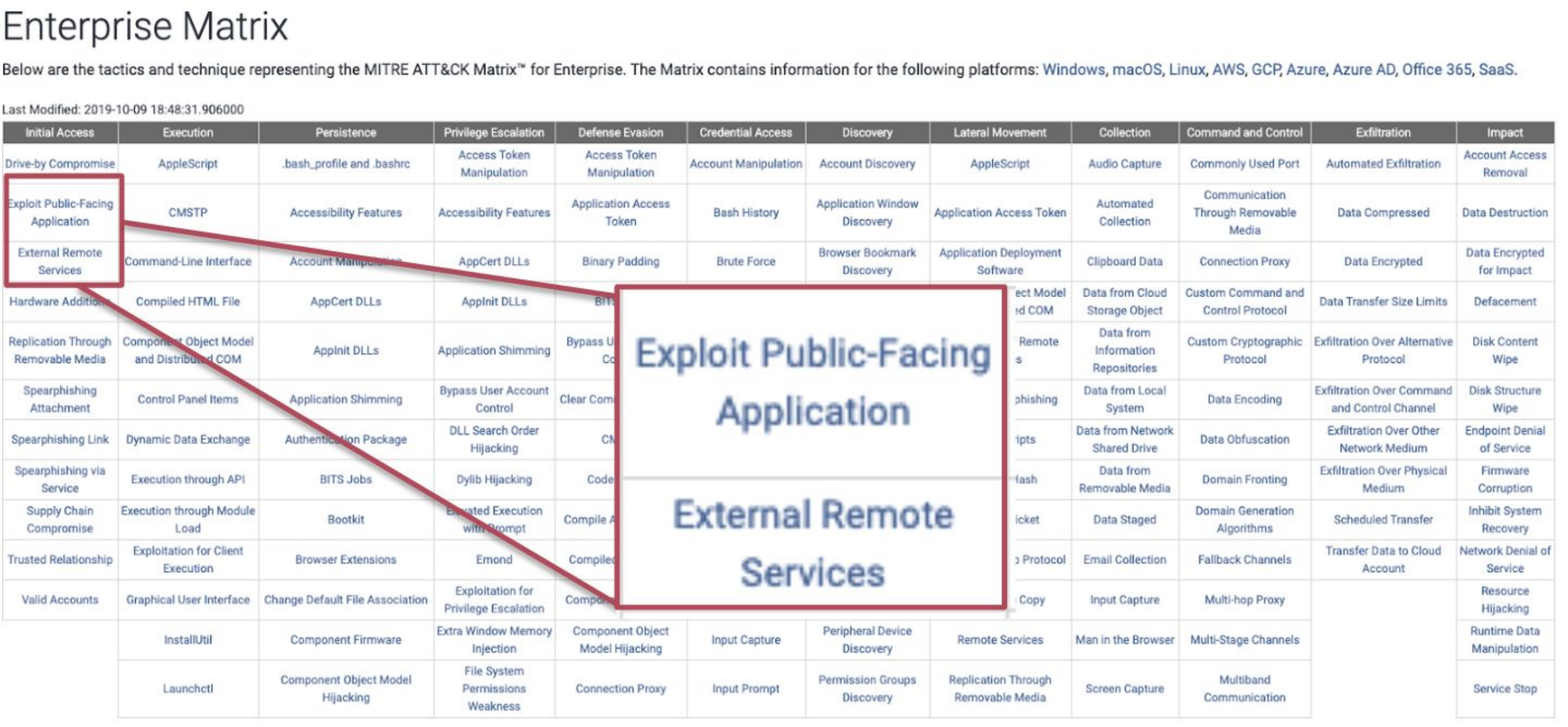
10.10.10.135 (tcp/23)

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------
router>

------------------------------ snip ------------------------------
```

MITRE ATT&CK



Enterprise Matrix

Below are the tactics and technique representing the MITRE ATT&CK Matrix™ for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additio	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS	[illegible]	[illegible]	ect Model ed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass U Co	[illegible]	[illegible]	Remote s	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Com	[illegible]	[illegible]	phishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CM	[illegible]	[illegible]	ipts	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code	[illegible]	[illegible]	lash	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compile A	[illegible]	[illegible]	icket	Data Staged	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Compiled	[illegible]	[illegible]	Protocol	Email Collection	Fallback Channels	Transfer Data to Cloud Account	Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Compo	[illegible]	[illegible]	Copy	Input Capture	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Screen Capture	Multiband Communication		Service Stop

Exploit Public-Facing Application

External Remote Services

Addressing Vulnerabilities:
The Wrong Way

- Many organizations address vulnerabilities by IP address
- For example: 1,000 IP addresses x ~25 vulnerabilities per IP = 25,000 issues to address
- This can be daunting
- Because of this we can see why so many companies focus on prioritization
- However, this approach is almost always wrong

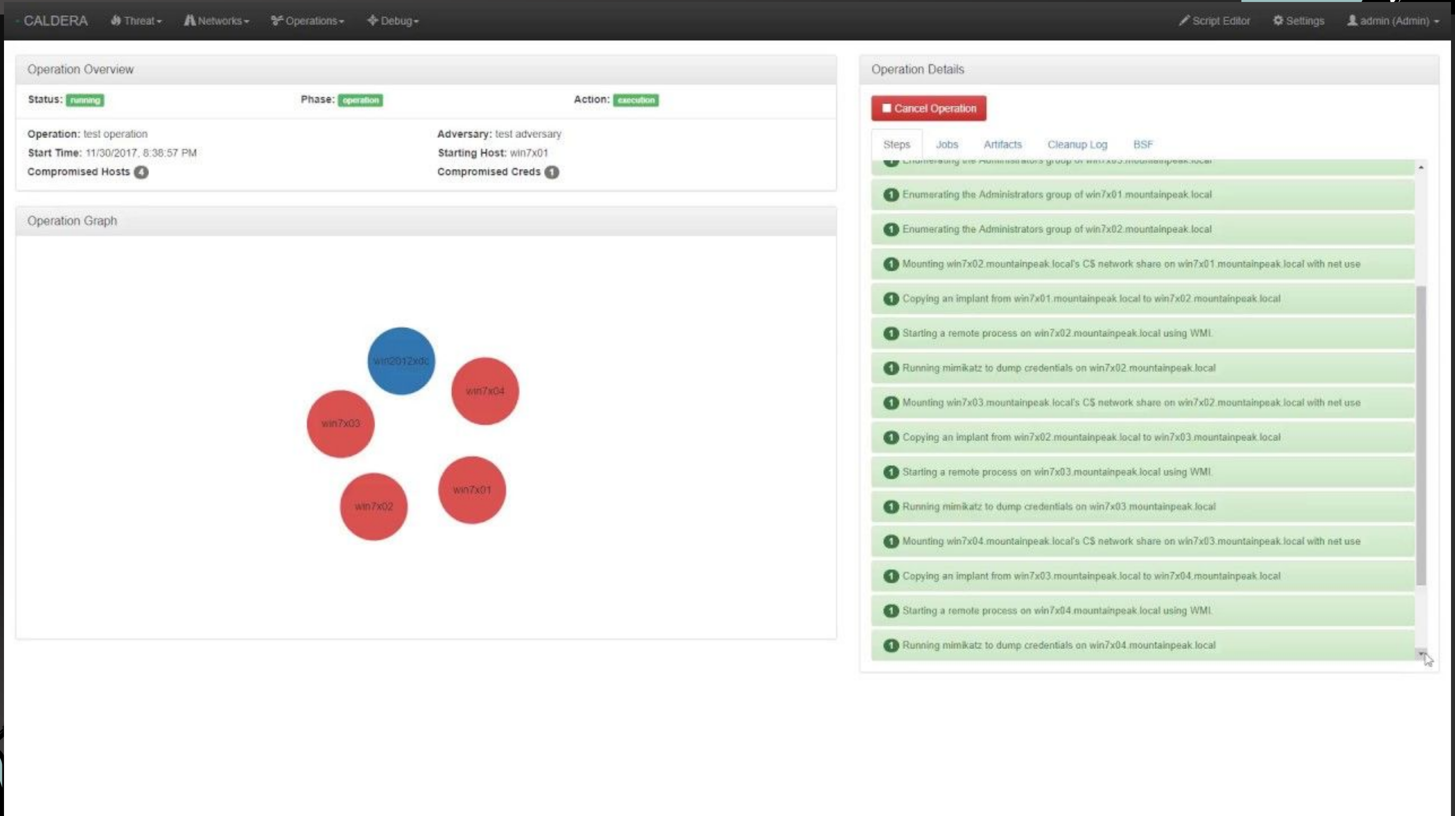
Addressing Vulnerabilities: The Correct Way

- Stop focusing on IP addresses and ranges
- Focus on the vulnerabilities
- Instead of 25,000 total vulnerabilities you will be dealing with a few hundred that repeat on multiple systems
- Use automation and address them as groups of issues
- This approach works regardless of the tool you use
- Consider it an “Open Source Technique”
- With this method IANS faculty have addressed over 1 million IP address, all vulnerabilities in less than 3 weeks

Threat Emulation

- Don’t just think of vulnerabilities as missing patches and misconfigurations on systems
- Think post exploitation
- What happens after an attacker gains access to a system
- There are a number of free tools that will automate parts of this process
- Currently, would take a bit of tuning and trial and error
- The collected data is invaluable

Open Source Tool Example: Caldera



Operation Overview

Status: running **Phase:** operation **Action:** execution

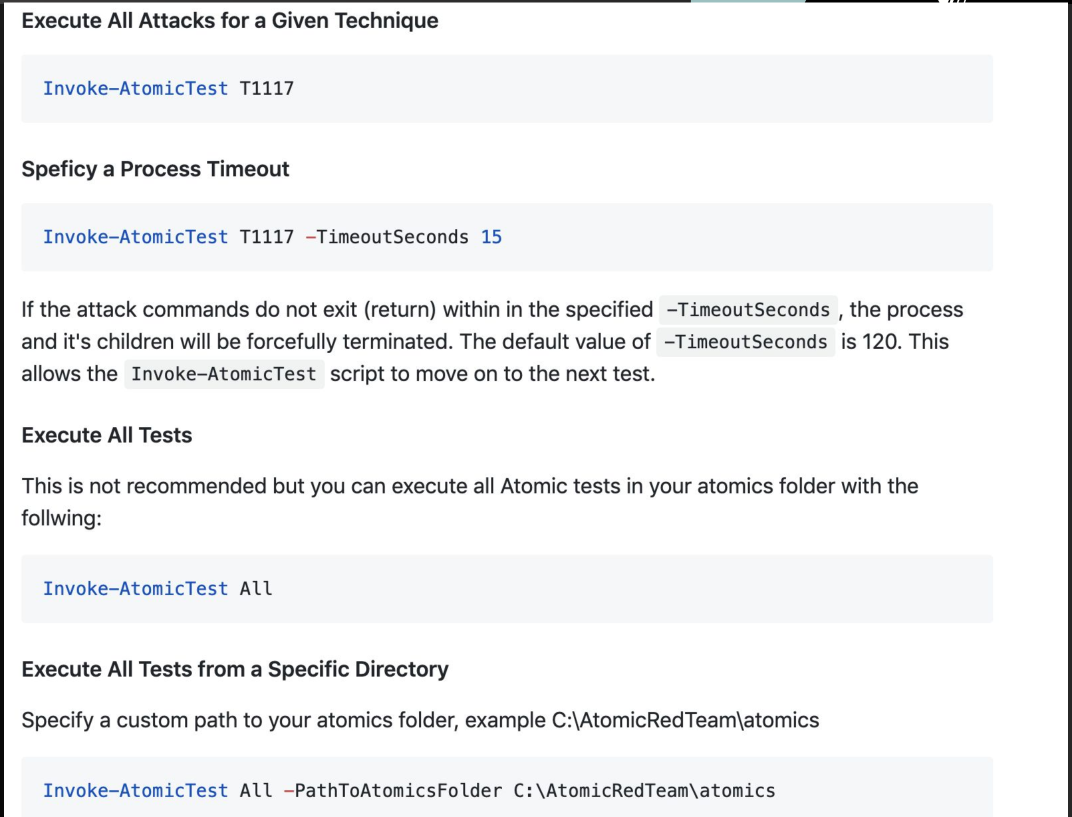
Operation: test operation **Adversary:** test adversary
Start Time: 11/30/2017, 8:38:57 PM **Starting Host:** win7x01
Compromised Hosts 4 **Compromised Creds** 1

Operation Graph

Operation Details

- 1 Enumerating the Administrators group of win7x03.mountainpeak.local
- 1 Enumerating the Administrators group of win7x01.mountainpeak.local
- 1 Enumerating the Administrators group of win7x02.mountainpeak.local
- 1 Mounting win7x02.mountainpeak.local's C$ network share on win7x01.mountainpeak.local with net use
- 1 Copying an implant from win7x01.mountainpeak.local to win7x02.mountainpeak.local
- 1 Starting a remote process on win7x02.mountainpeak.local using WMI.
- 1 Running mimikatz to dump credentials on win7x02.mountainpeak.local
- 1 Mounting win7x03.mountainpeak.local's C$ network share on win7x02.mountainpeak.local with net use
- 1 Copying an implant from win7x02.mountainpeak.local to win7x03.mountainpeak.local
- 1 Starting a remote process on win7x03.mountainpeak.local using WMI.
- 1 Running mimikatz to dump credentials on win7x03.mountainpeak.local
- 1 Mounting win7x04.mountainpeak.local's C$ network share on win7x03.mountainpeak.local with net use
- 1 Copying an implant from win7x03.mountainpeak.local to win7x04.mountainpeak.local
- 1 Starting a remote process on win7x04.mountainpeak.local using WMI.
- 1 Running mimikatz to dump credentials on win7x04.mountainpeak.local

Open Source Tool Example: Atomic Red Team



Execute All Attacks for a Given Technique

```
Invoke-AtomicTest T1117
```

Speficy a Process Timeout

```
Invoke-AtomicTest T1117 -TimeoutSeconds 15
```

If the attack commands do not exit (return) within in the specified `-TimeoutSeconds`, the process and it's children will be forcefully terminated. The default value of `-TimeoutSeconds` is 120. This allows the `Invoke-AtomicTest` script to move on to the next test.

Execute All Tests

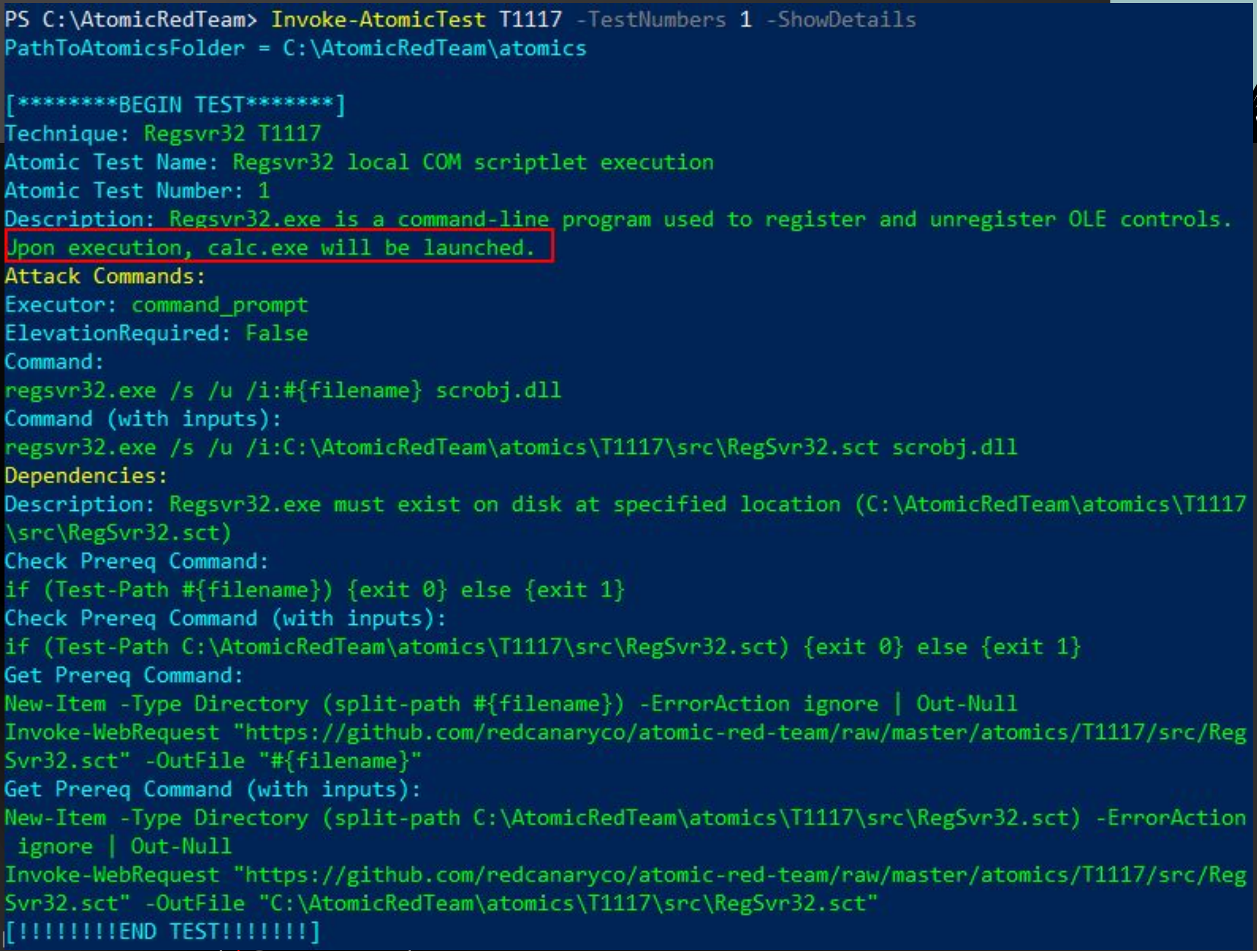
This is not recommended but you can execute all Atomic tests in your atomics folder with the follwing:

```
Invoke-AtomicTest All
```

Execute All Tests from a Specific Directory

Specify a custom path to your atomics folder, example C:\AtomicRedTeam\atomics

```
Invoke-AtomicTest All -PathToAtomicsFolder C:\AtomicRedTeam\atomics
```



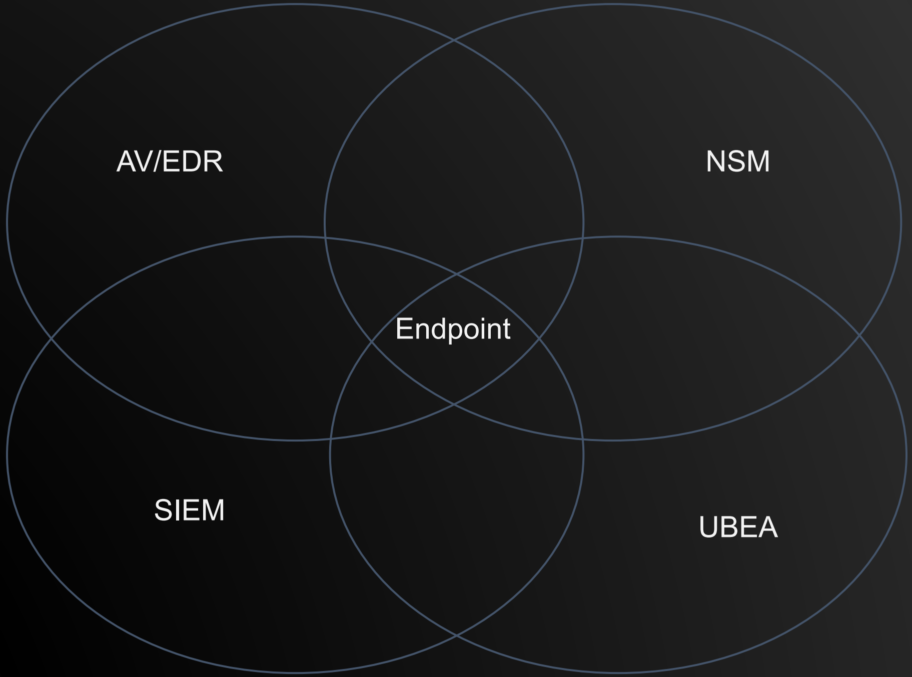
```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1117 -TestNumbers 1 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: Regsvr32 T1117
Atomic Test Name: Regsvr32 local COM scriptlet execution
Atomic Test Number: 1
Description: Regsvr32.exe is a command-line program used to register and unregister OLE controls.
Jpon execution, calc.exe will be launched.
Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
regsvr32.exe /s /u /i:#{filename} scrobj.dll
Command (with inputs):
regsvr32.exe /s /u /i:C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct scrobj.dll
Dependencies:
Description: Regsvr32.exe must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1117
\src\RegSvr32.sct)
Check Prereq Command:
if (Test-Path #{filename}) {exit 0} else {exit 1}
Check Prereq Command (with inputs):
if (Test-Path C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct) {exit 0} else {exit 1}
Get Prereq Command:
New-Item -Type Directory (split-path #{filename}) -ErrorAction ignore | Out-Null
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1117/src/Reg
Svr32.sct" -OutFile "#{filename}"
Get Prereq Command (with inputs):
New-Item -Type Directory (split-path C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct) -ErrorAction
 ignore | Out-Null
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1117/src/Reg
Svr32.sct" -OutFile "C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct"
[!!!!!!!!!END TEST!!!!!!!]
```

Things That Are Hard...

- Teaching people to “keep digging”
- Ping Port Parse
- Fighting Burnout
- Never “get stuck” pivot, try new things
- LMGTFY
- Drive….

Architecture



Questions?

BLACK HILLS
Information Security
• 2008 •