Powering Up Incident Response with

Power-Response

Drew Schmitt (@5ynax)
Matt Weikert (@5k33tz)
Gavin Prentice (@Valrkey)

Whois Drew Schmitt

- Senior Cyber Security Threat Hunter, Medtronic CSIRT
- Adjunct Professor, Metro State University (CSC Department)
- Metro State CCDC Coach
- Master's from University of Minnesota
- Certifications: GCIH, GCFA, GNFA

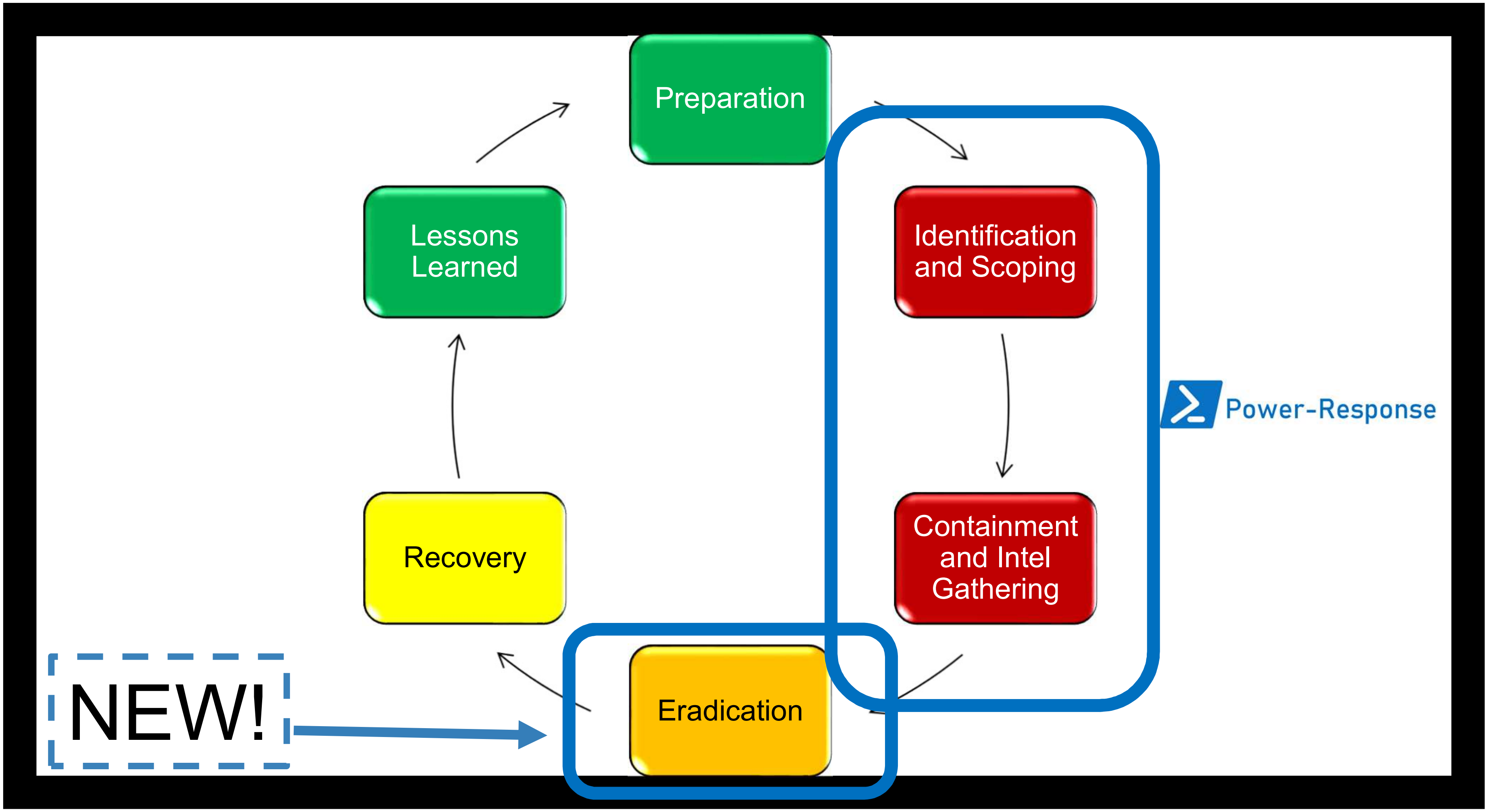
Whois Matt Weikert

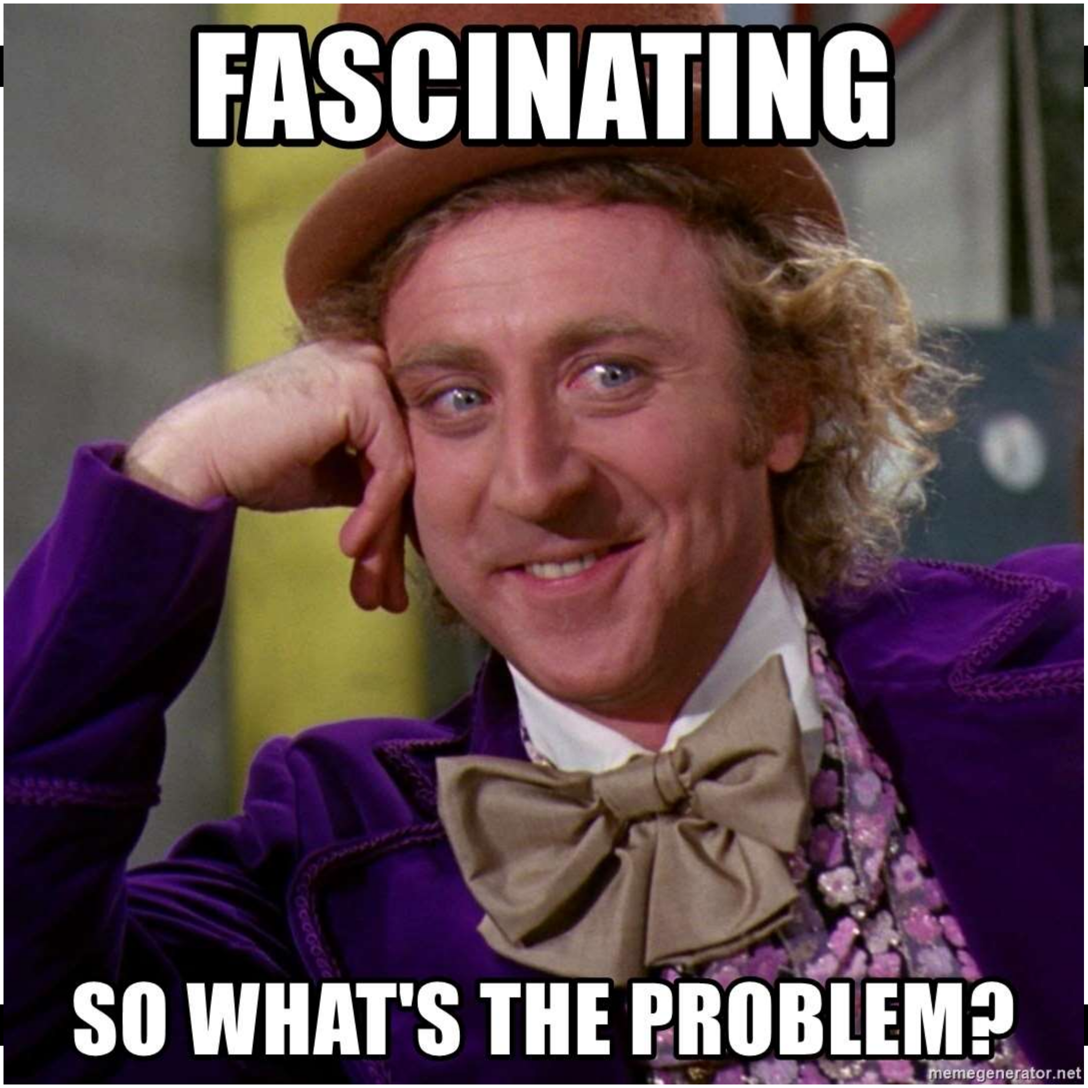
- Senior DFIR Consultant, Stroz Friedberg an Aon Company
- Adjunct Professor, Metro State University (CSC Department)
- Metro State CCDC Coach/Red Team Ops
- Bachelor’s in Computer Forensics from Metro State
- Certifications: GCIH, GCFA, GNFA, GREM, ACEv6

Whois Gavin Prentice

- Incident Responder, Medtronic CSIRT
- Not an Adjunct Professor at Metro State University
- Metro State CCDC Coach Therapist
- Bachelor’s in Computer Science from the U of M
- Certifications: GMON, GCIH

Our Incident Response Process


Preparation
Identification and Scoping
Containment and Intel Gathering
Eradication
Recovery
Lessons Learned
Power-Response
NEW!


FASCINATING
SO WHAT'S THE PROBLEM?
memegenerator.net

The Problems

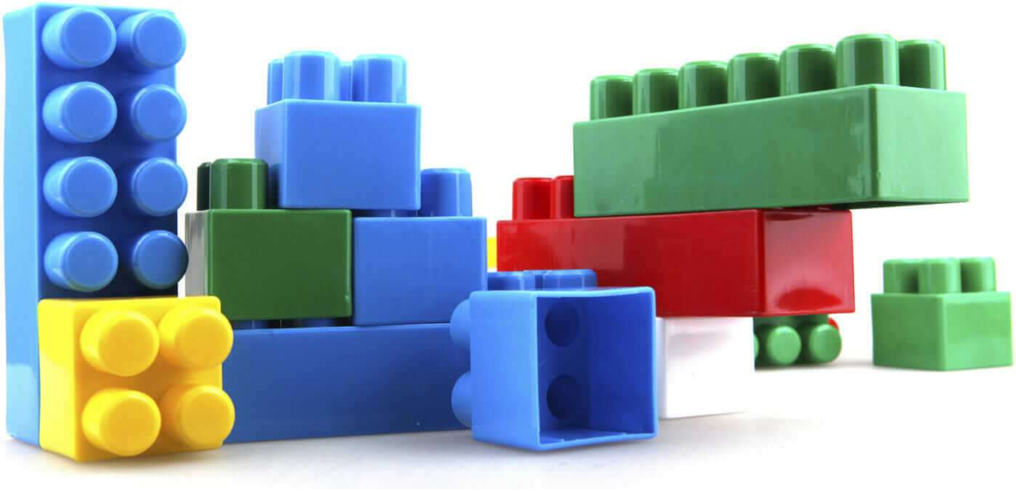
- One off scripts and one liner commands
- Tribal knowledge
  - One responder does it one way, another does it different
- Inconsistencies in data collection
  - We wanted certain parts of incident response to be repeatable when possible
- Time consuming data collection processes
  - Copy, paste, copy, paste, copy, paste

The Problems

- Lack of logging (knowing who did what, when, and how)
- Knowledge gaps
  - Analysts operate at different levels of IR knowledge
- Tunnel vision during the heat of the moment
  - Forgetting to collect certain kinds of data happens (kind of often)
- Individual (manual) data collection from hosts one at a time
  - All that typing and data management is not exactly fun
- Data collection and analysis are separate tasks

What is Power-Response

- Modular incident response framework built in PowerShell



The Goals of Power-Response

The Goals of Power-Response

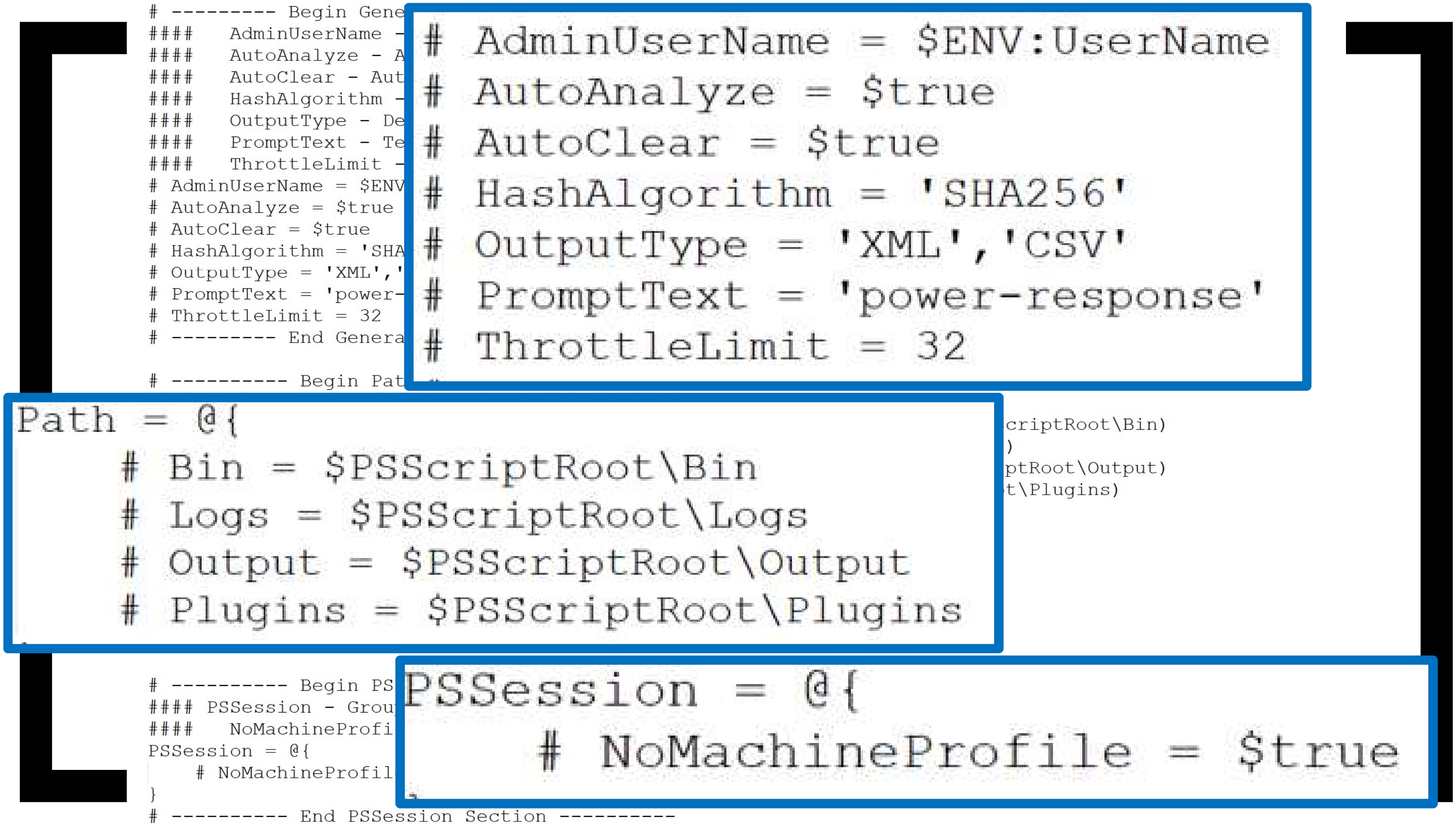
- Solve the problems
- Reduce the need for the memorization of commands run during investigations
- Fast, secure, and reliable data collection from remote Windows endpoints
- Improved logging and accountability during incidents
- A highly utilizable tool regardless of level of experience
- Automatic analysis of data collected

Framework Features of Power-Response

- Menu style navigation
- Persistent Parameters
- Fast and scalable data collection
- Consolidated and standardized output
  - □ Automatic Consolidated Output (Excel Spreadsheet w/ Multiple Tabs!) – New Feature
- Data integrity
- Logging and accountability during incidents
- Automatic analyzing of data collected

Customizing framework features

- The framework allows for the use of a configuration file that will enable the analyst to choose how they want the framework to handle specific framework features



```
# --------- Begin Gene
####    AdminUserName -
####    AutoAnalyze - A
####    AutoClear - Aut
####    HashAlgorithm -
####    OutputType - De
####    PromptText - Te
####    ThrottleLimit -
# AdminUserName = $ENV
# AutoAnalyze = $true
# AutoClear = $true
# HashAlgorithm = 'SHA
# OutputType = 'XML','
# PromptText = 'power-
# ThrottleLimit = 32
# --------- End Genera

# ---------- Begin Pat
```

```
# AdminUserName = $ENV:UserName
# AutoAnalyze = $true
# AutoClear = $true
# HashAlgorithm = 'SHA256'
# OutputType = 'XML','CSV'
# PromptText = 'power-response'
# ThrottleLimit = 32
```

```
Path = @{
    # Bin = $PSScriptRoot\Bin
    # Logs = $PSScriptRoot\Logs
    # Output = $PSScriptRoot\Output
    # Plugins = $PSScriptRoot\Plugins
```

```
criptRoot\Bin)
)
ptRoot\Output)
t\Plugins)
```

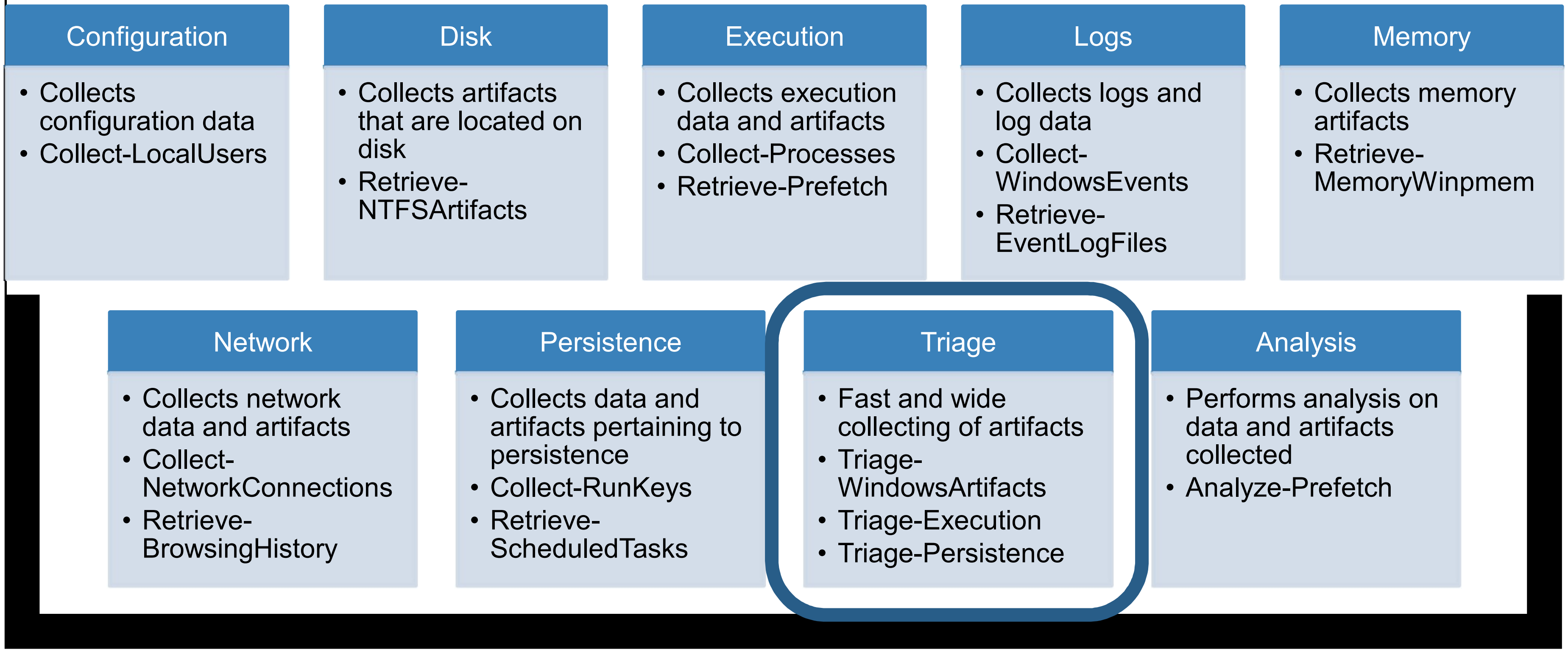
```
# ---------- Begin PS
#### PSSession - Grou
####    NoMachineProfi
PSSession = @{
    # NoMachineProfil
}
# ---------- End PSSession Section ----------
```

```
PSSession = @{
    # NoMachineProfile = $true
```

Power-Response Plugins

- Seven Plugin Types
  - □ Collect, Retrieve, Analyze, Triage, Hunt, Scope, Eradicate
- Currently 50+ plugins (for granularity)
- There's always room for more plugins
  - □ There really is no limitations to the plugins you can create (take a look at the wiki for more details on how to create custom plugins)
  - □ Consider sending pull requests for plugins you create
- Plugins always clean up after themselves
  - □ No leftover artifacts

Power-Response Plugins



Configuration

- Collects configuration data
- Collect-LocalUsers

Disk

- Collects artifacts that are located on disk
- Retrieve-NTFSArtifacts

Execution

- Collects execution data and artifacts
- Collect-Processes
- Retrieve-Prefetch

Logs

- Collects logs and log data
- Collect-WindowsEvents
- Retrieve-EventLogFiles

Memory

- Collects memory artifacts
- Retrieve-MemoryWinpmem

Network

- Collects network data and artifacts
- Collect-NetworkConnections
- Retrieve-BrowsingHistory

Persistence

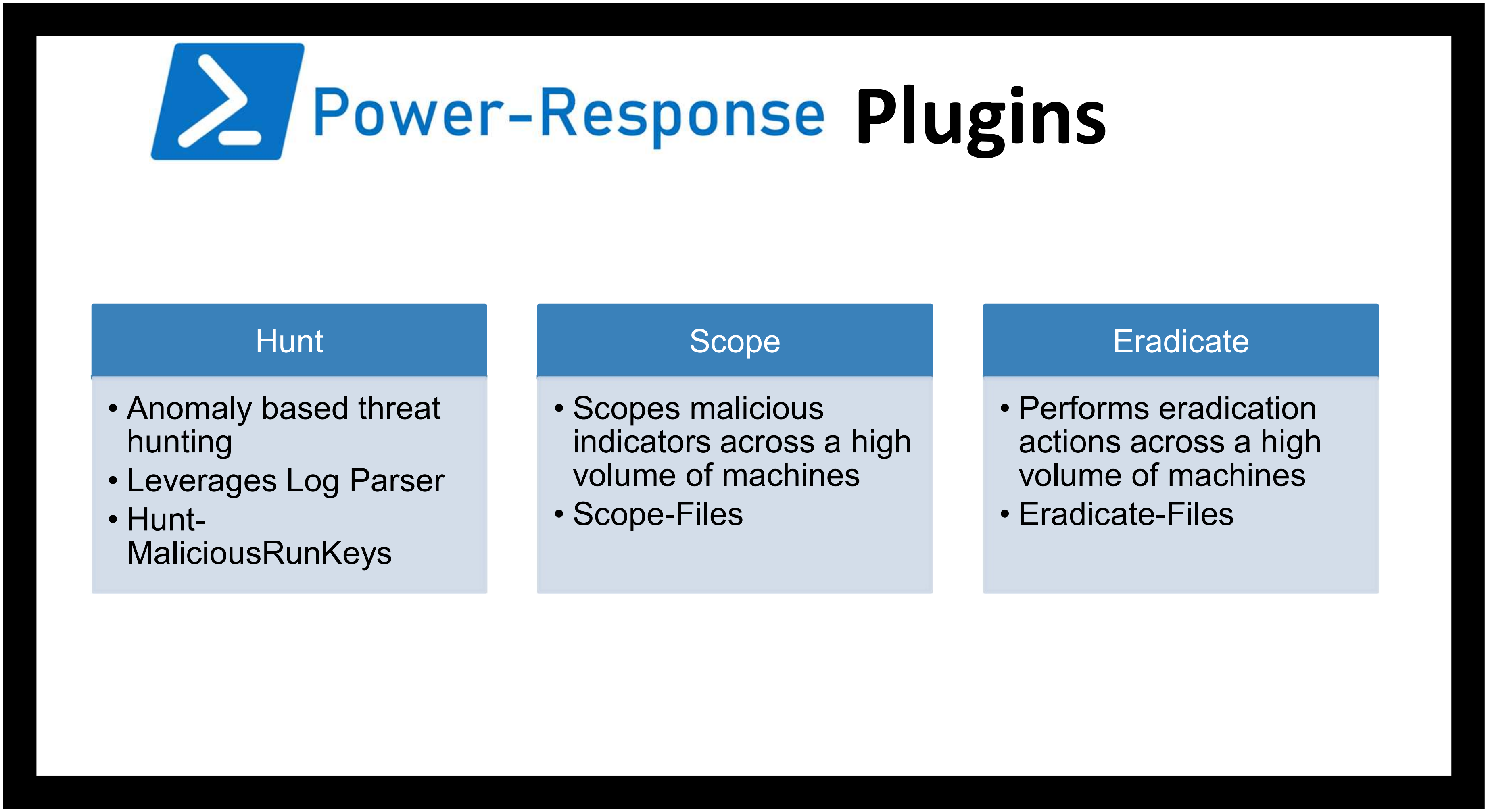
- Collects data and artifacts pertaining to persistence
- Collect-RunKeys
- Retrieve-ScheduledTasks

Triage

- Fast and wide collecting of artifacts
- Triage-WindowsArtifacts
- Triage-Execution
- Triage-Persistence

Analysis

- Performs analysis on data and artifacts collected
- Analyze-Prefetch



Power-Response Plugins

Hunt

- Anomaly based threat hunting
- Leverages Log Parser
- Hunt-MaliciousRunKeys

Scope

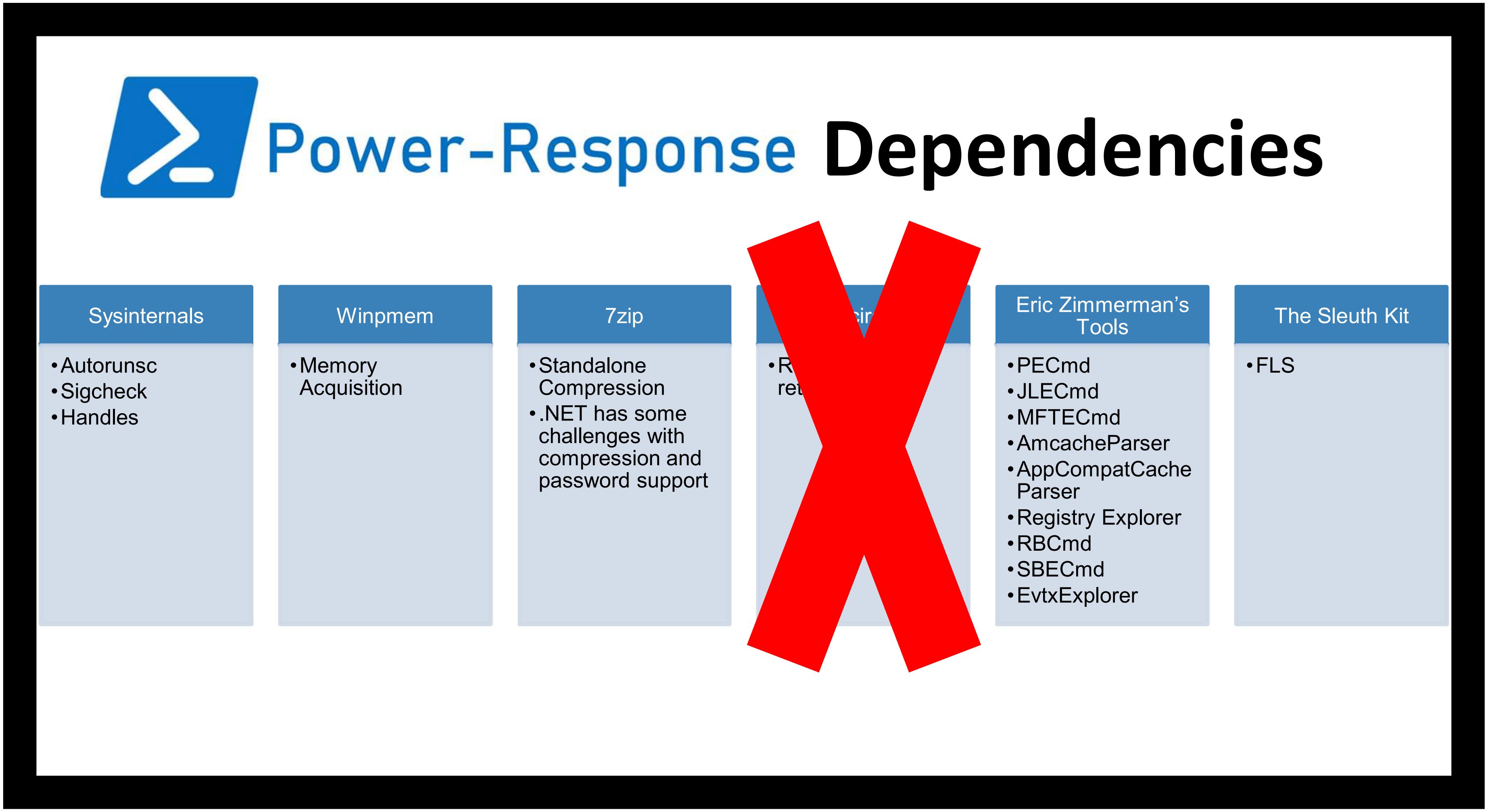
- Scopes malicious indicators across a high volume of machines
- Scope-Files

Eradicate

- Performs eradication actions across a high volume of machines
- Eradicate-Files

Power-Response Setup

- **Environment Dependency: PowerShell Remoting**
- Clone the repo
- (Unblock and) Run Setup.ps1
  - Satisfies dependencies
- Update the configuration file (if desired)
- Run it and collect all the dataz



Power-Response Dependencies

Sysinternals

- Autorunsc
- Sigcheck
- Handles

Winpmem

- Memory Acquisition

7zip

- Standalone Compression
- .NET has some challenges with compression and password support

cir

- R ret

Eric Zimmerman's Tools

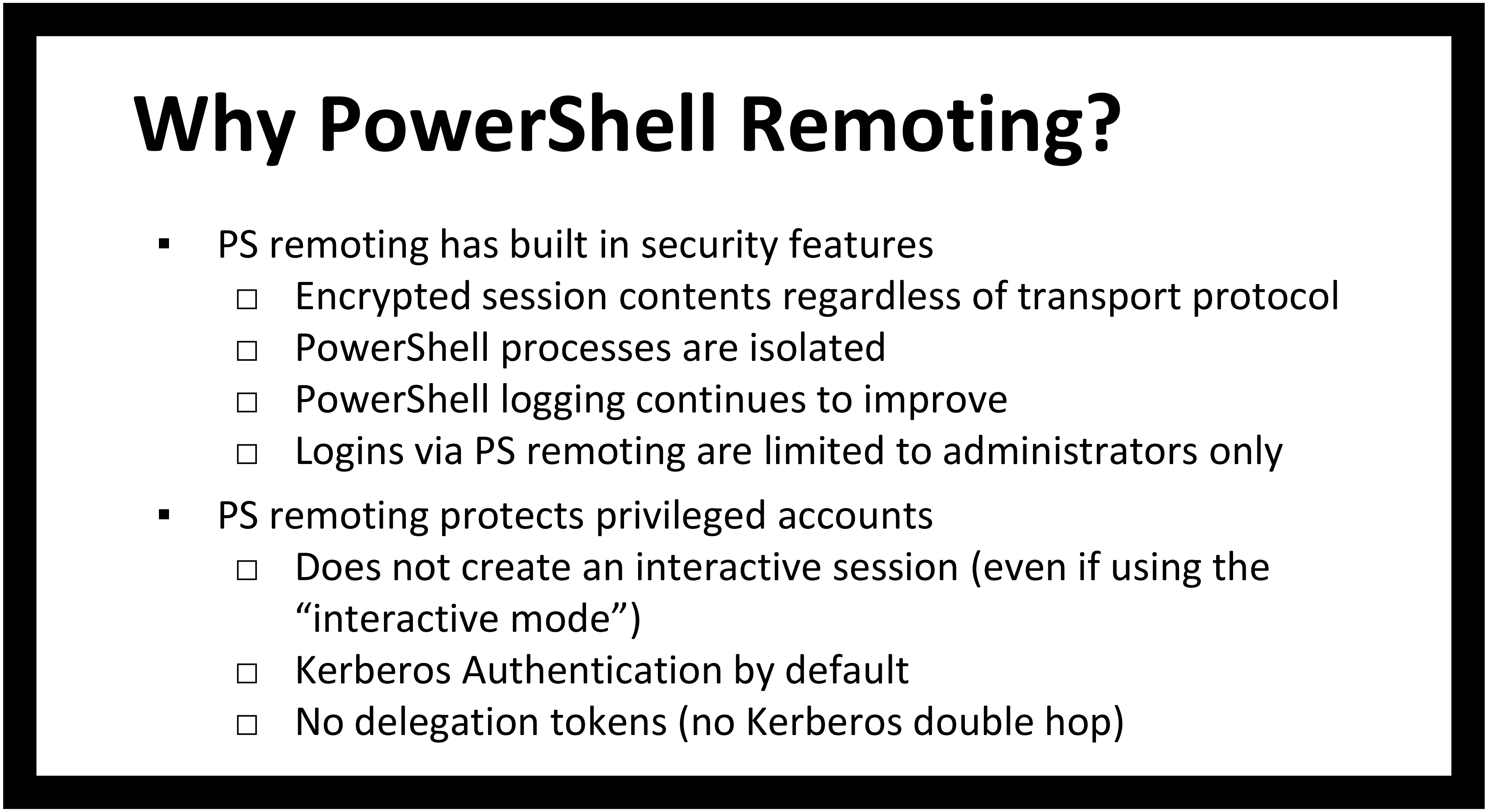
- PECmd
- JLECmd
- MFTECmd
- AmcacheParser
- AppCompatCacheParser
- Registry Explorer
- RBCmd
- SBECmd
- EvtxExplorer

The Sleuth Kit

- FLS

Why PowerShell Remoting?

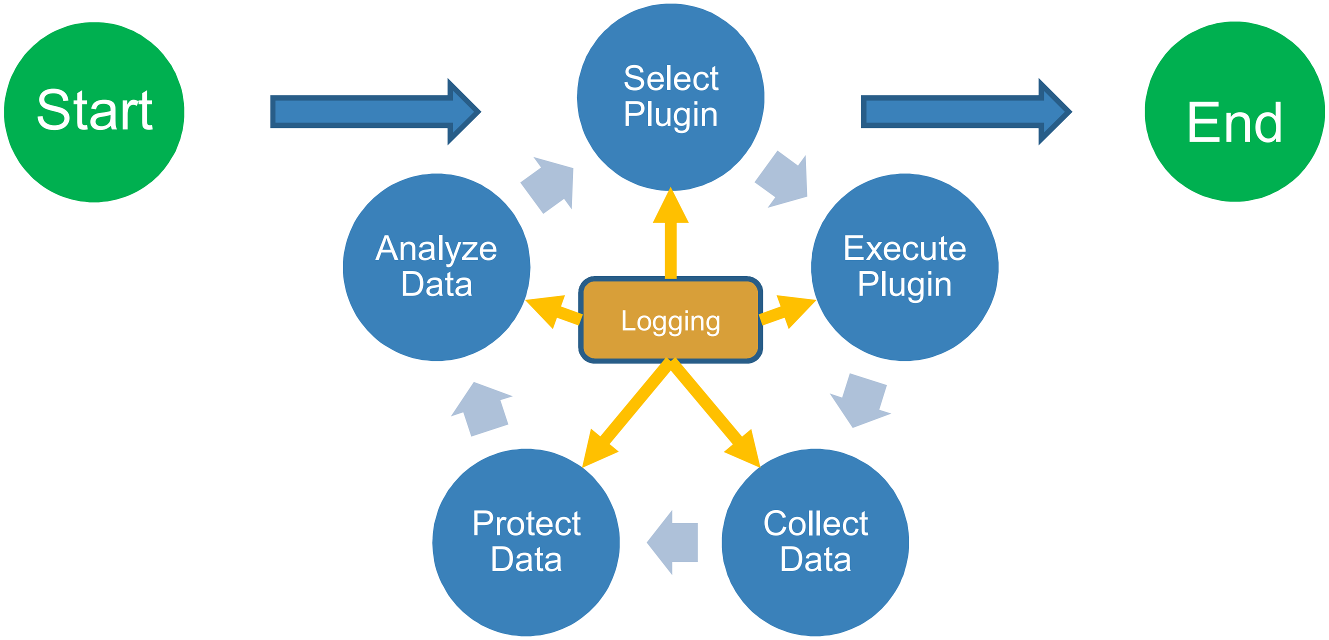
- Drawbacks of RDP and SMB
  - □ Interactive logons cache hash and ticket credentials on the target system
  - □ Tokens are vulnerable during interactive logons
  - □ NTLM hashes for authentication are more risky



Why PowerShell Remoting?

- PS remoting has built in security features
  - Encrypted session contents regardless of transport protocol
  - PowerShell processes are isolated
  - PowerShell logging continues to improve
  - Logins via PS remoting are limited to administrators only
- PS remoting protects privileged accounts
  - Does not create an interactive session (even if using the “interactive mode”)
  - Kerberos Authentication by default
  - No delegation tokens (no Kerberos double hop)

Power-Response Flow



Start

Select Plugin

Execute Plugin

Collect Data

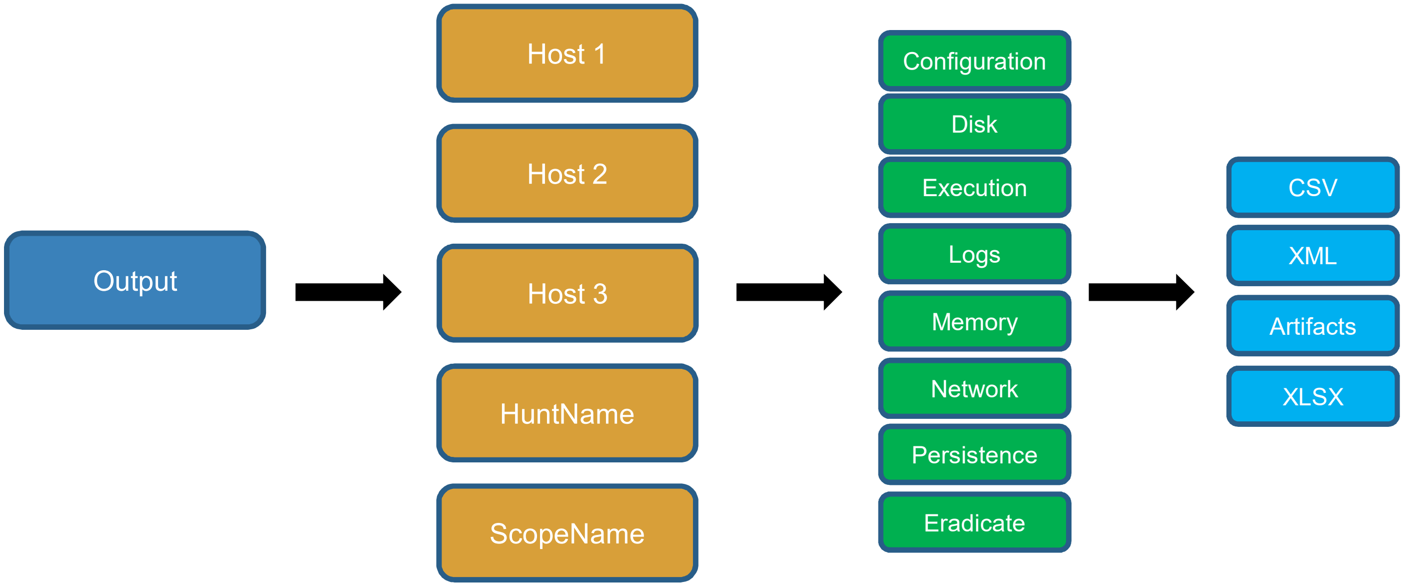
Protect Data

Analyze Data

Logging

End

Power-Response Output



Output

Host 1

Host 2

Host 3

HuntName

ScopeName

Configuration

Disk

Execution

Logs

Memory

Network

Persistence

Eradicate

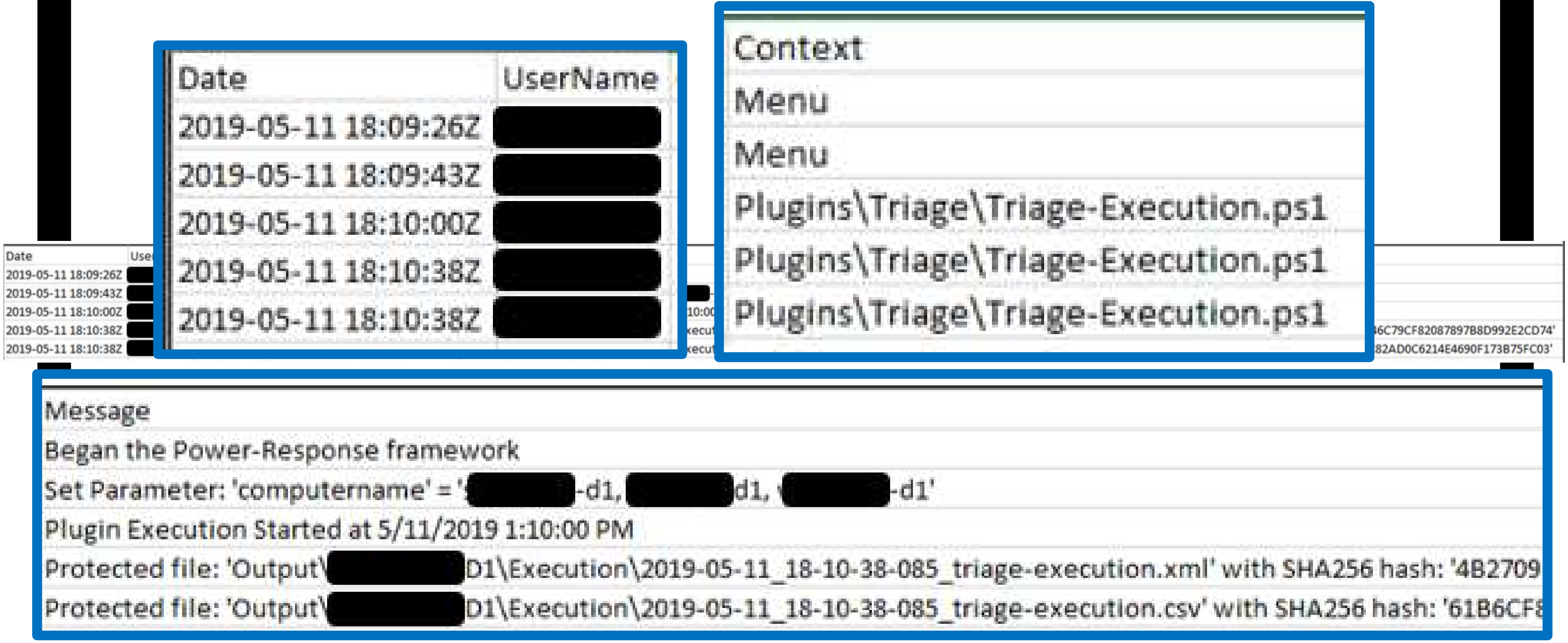
CSV

XML

Artifacts

XLSX

Power-Response Logging



Date	UserName
2019-05-11 18:09:26Z	[redacted]
2019-05-11 18:09:43Z	[redacted]
2019-05-11 18:10:00Z	[redacted]
2019-05-11 18:10:38Z	[redacted]
2019-05-11 18:10:38Z	[redacted]

Context
Menu
Menu
Plugins\Triage\Triage-Execution.ps1
Plugins\Triage\Triage-Execution.ps1
Plugins\Triage\Triage-Execution.ps1

Message
Began the Power-Response framework
Set Parameter: 'computername' = '[redacted]-d1, [redacted]d1, [redacted]-d1'
Plugin Execution Started at 5/11/2019 1:10:00 PM
Protected file: 'Output\[redacted]D1\Execution\2019-05-11_18-10-38-085_triage-execution.xml' with SHA256 hash: '4B2709
Protected file: 'Output\[redacted]D1\Execution\2019-05-11_18-10-38-085_triage-execution.csv' with SHA256 hash: '61B6CF8

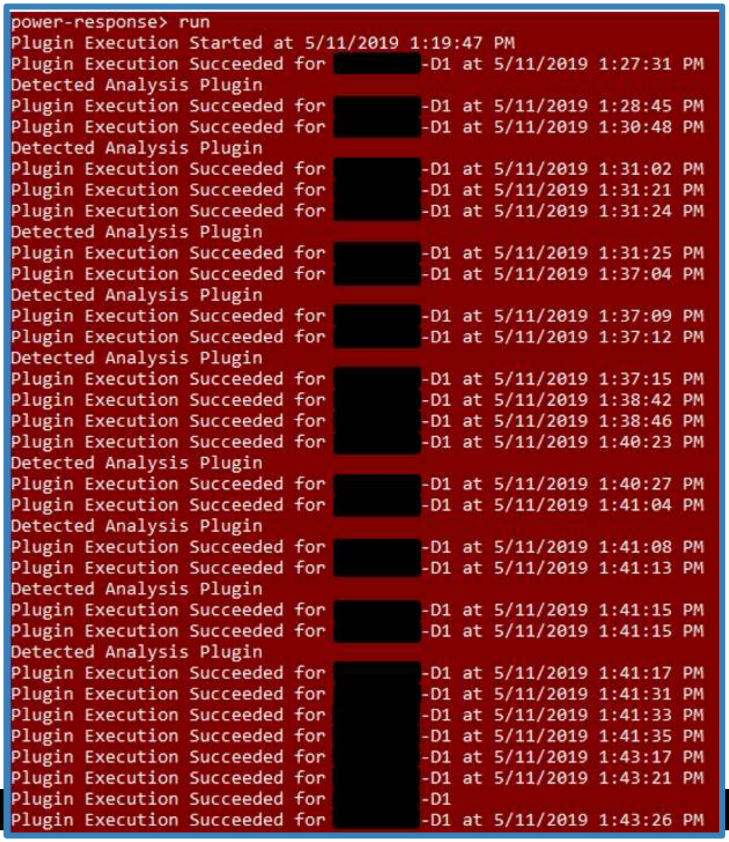
Date Use
2019-05-11 18:09:26Z [redacted]
2019-05-11 18:09:43Z [redacted]
2019-05-11 18:10:00Z [redacted]
2019-05-11 18:10:38Z [redacted]
2019-05-11 18:10:38Z [redacted]

6C79CF82087897B8D992E2CD74'
82AD0C6214E4690F173B75FC03'

Powering Up Incident Response With

Power-Response

Power-Response In the Real-World (I)



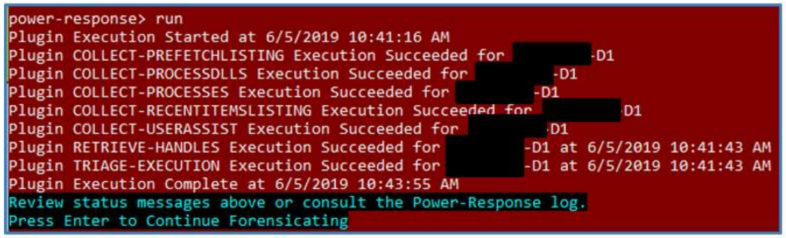
```
power-response> run
Plugin Execution Started at 5/11/2019 1:19:47 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:27:31 PM
Detected Analysis Plugin
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:28:45 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:30:48 PM
Detected Analysis Plugin
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:31:02 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:31:21 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:31:24 PM
Detected Analysis Plugin
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:31:25 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:37:04 PM
Detected Analysis Plugin
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:37:09 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:37:12 PM
Detected Analysis Plugin
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:37:15 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:38:42 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:38:46 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:40:23 PM
Detected Analysis Plugin
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:40:27 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:41:04 PM
Detected Analysis Plugin
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:41:08 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:41:13 PM
Detected Analysis Plugin
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:41:15 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:41:15 PM
Detected Analysis Plugin
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:41:17 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:41:31 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:41:33 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:41:35 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:43:17 PM
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:43:21 PM
Plugin Execution Succeeded for [redacted]-D1
Plugin Execution Succeeded for [redacted]-D1 at 5/11/2019 1:43:26 PM
```

Triage-WindowsArtifacts
Start: 1:19:47 PM
End: 2:17:21 PM
Total Run Time: ~58 Min
3 Machines
Average Data Collection per Machine: ~20 Min
Data Collection Over VPN

Plugins Completed per Host (26):

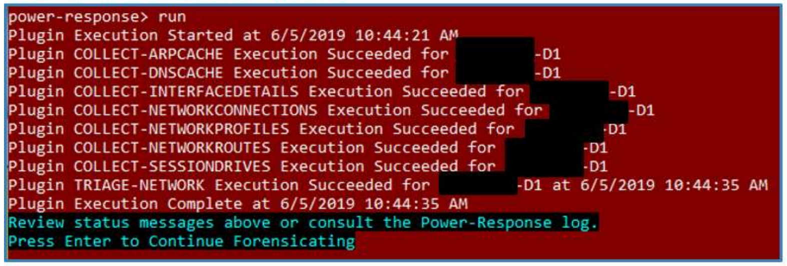
Retrieve-NTFSArtifacts, Analyze-NTFSArtififacts, Retrieve-RegistryHives, Analyze-RegistryHives, Retrieve-EventLogFiles, Retrieve-Amcache, Analyze-Amcache, Retrieve-Prefetch, Analyze-Prefetch, Retrieve-ShimCache, Analyze-Shimcache, Retrieve-ScheduledTasks, Retrieve-Startup, Retrieve-RecentItems, Analyze-RecentItems, Retrieve-JumpLists, Analyze-Jumplists, Retrieve-RecycleBin, Analyze-RecycleBin, Retrieve-Shellbags, Analyze-Shellbags, Retrieve-BrowsingHistory, Retrieve-HostsFile, Retrieve-WindowsSearchData, Retrieve-SRUMDB, Retrieve-PSReadLine

Power-Response In the Real-World (II)



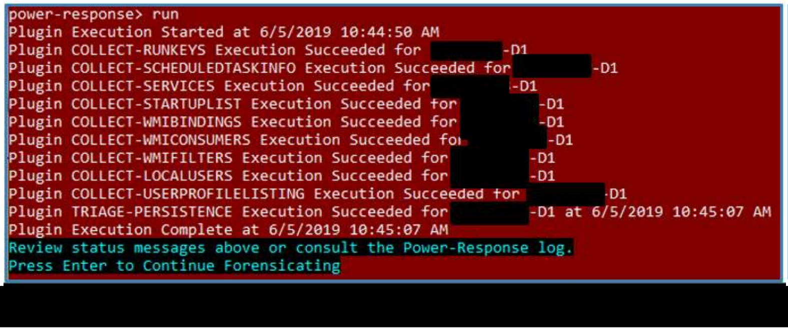
```
power-response> run
Plugin Execution Started at 6/5/2019 10:41:16 AM
Plugin COLLECT-PREFETCHLISTING Execution Succeeded for [redacted]-D1
Plugin COLLECT-PROCESSDLLS Execution Succeeded for [redacted]-D1
Plugin COLLECT-PROCESSES Execution Succeeded for [redacted]-D1
Plugin COLLECT-RECENTITEMSLISTING Execution Succeeded for [redacted]-D1
Plugin COLLECT-USERASSIST Execution Succeeded for [redacted]-D1
Plugin RETRIEVE-HANDLES Execution Succeeded for [redacted]-D1 at 6/5/2019 10:41:43 AM
Plugin TRIAGE-EXECUTION Execution Succeeded for [redacted]-D1 at 6/5/2019 10:41:43 AM
Plugin Execution Complete at 6/5/2019 10:43:55 AM
Review status messages above or consult the Power-Response log.
Press Enter to Continue Forensicating
```

Triage-Execution
Start: 10:41:16 AM
End: 10:43:55 AM
Total Run Time: ~3 Min
1 Machine
Data Collection Over LAN



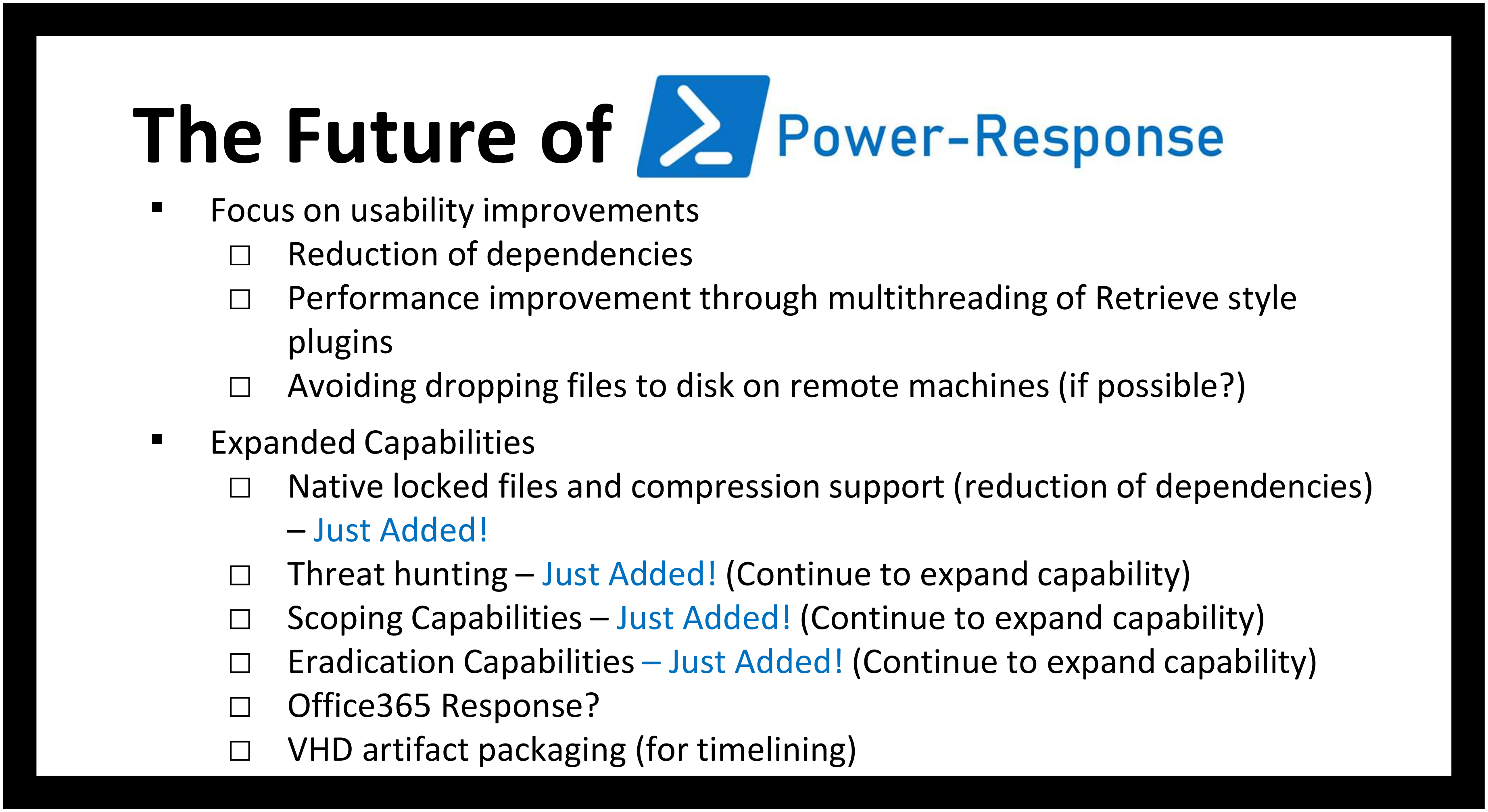
```
power-response> run
Plugin Execution Started at 6/5/2019 10:44:21 AM
Plugin COLLECT-ARPCACHE Execution Succeeded for [redacted]-D1
Plugin COLLECT-DNSCACHE Execution Succeeded for [redacted]-D1
Plugin COLLECT-INTERFACEDETAILS Execution Succeeded for [redacted]-D1
Plugin COLLECT-NETWORKCONNECTIONS Execution Succeeded for [redacted]-D1
Plugin COLLECT-NETWORKPROFILES Execution Succeeded for [redacted]-D1
Plugin COLLECT-NETWORKROUTES Execution Succeeded for [redacted]-D1
Plugin COLLECT-SESSIONDRIVES Execution Succeeded for [redacted]-D1
Plugin TRIAGE-NETWORK Execution Succeeded for [redacted]-D1 at 6/5/2019 10:44:35 AM
Plugin Execution Complete at 6/5/2019 10:44:35 AM
Review status messages above or consult the Power-Response log.
Press Enter to Continue Forensicating
```

Triage-Network
Start: 10:44:21 AM
End: 10:44:35 AM
Total Run Time: ~ 15 Sec
1 Machine
Data Collection Over LAN



```
power-response> run
Plugin Execution Started at 6/5/2019 10:44:50 AM
Plugin COLLECT-RUNKEYS Execution Succeeded for [redacted]-D1
Plugin COLLECT-SCHEDULEDTASKINFO Execution Succeeded for [redacted]-D1
Plugin COLLECT-SERVICES Execution Succeeded for [redacted]-D1
Plugin COLLECT-STARTUPLIST Execution Succeeded for [redacted]-D1
Plugin COLLECT-WMIBINDINGS Execution Succeeded for [redacted]-D1
Plugin COLLECT-WMICONSUMERS Execution Succeeded for [redacted]-D1
Plugin COLLECT-WMIFILTERS Execution Succeeded for [redacted]-D1
Plugin COLLECT-LOCALUSERS Execution Succeeded for [redacted]-D1
Plugin COLLECT-USERPROFILELISTING Execution Succeeded for [redacted]-D1
Plugin TRIAGE-PERSISTENCE Execution Succeeded for [redacted]-D1 at 6/5/2019 10:45:07 AM
Plugin Execution Complete at 6/5/2019 10:45:07 AM
Review status messages above or consult the Power-Response log.
Press Enter to Continue Forensicating
```

Triage-Persistence
Start: 10:44:50 AM
End: 10:45:07 AM
Total Run Time: ~15 Sec
1 Machine
Data Collection Over LAN

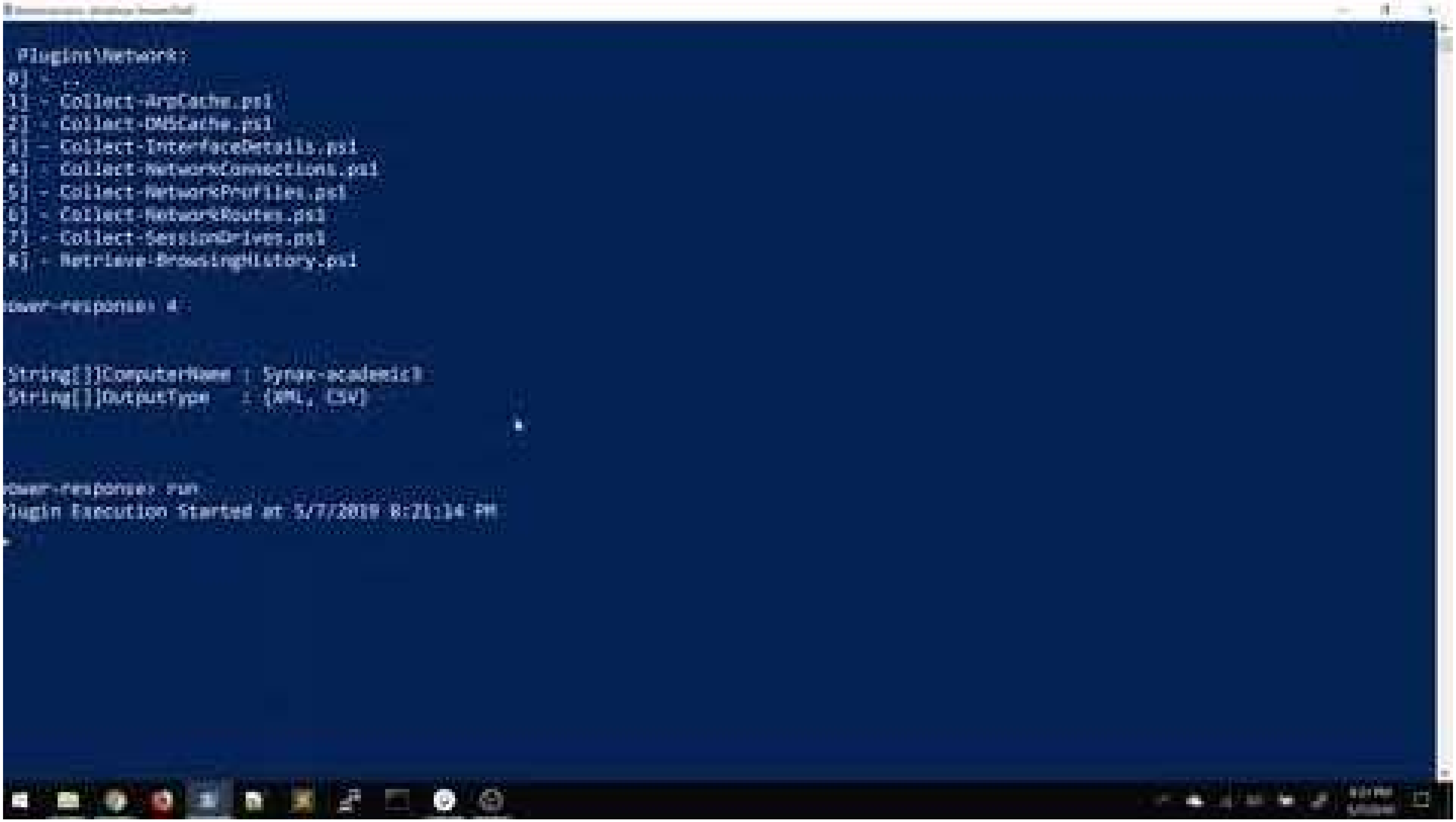


The Future of Power-Response

- Focus on usability improvements
  - □ Reduction of dependencies
  - □ Performance improvement through multithreading of Retrieve style plugins
  - □ Avoiding dropping files to disk on remote machines (if possible?)
- Expanded Capabilities
  - □ Native locked files and compression support (reduction of dependencies) – Just Added!
  - □ Threat hunting – Just Added! (Continue to expand capability)
  - □ Scoping Capabilities – Just Added! (Continue to expand capability)
  - □ Eradication Capabilities – Just Added! (Continue to expand capability)
  - □ Office365 Response?
  - □ VHD artifact packaging (for timelining)

The Power-Response Team

- Drew Schmitt, @5ynax
- Matt Weikert, @5k33tz
- Gavin Prentice, @Valrkey
- https://github.com/Asymmetric-InfoSec/Power-Response



```
 Plugins\Network:
0] - ..
1] - Collect-ArpCache.ps1
2] - Collect-DNSCache.ps1
3] - Collect-InterfaceDetails.ps1
4] - Collect-NetworkConnections.ps1
5] - Collect-NetworkProfiles.ps1
6] - Collect-NetworkRoutes.ps1
7] - Collect-SessionDrives.ps1
8] - Retrieve-BrowsingHistory.ps1

ower-response: 4


String[]]ComputerName : Synax-academic3
String[]]OutputType   : {XML, CSV}



ower-response: run
lugin Execution Started at 5/7/2019 8:21:14 PM
```