Enter Mordor

Pre-recorded Security Events from Simulated Adversarial Techniques
@Cyb3rWard0g

- Creator of
  - @HunterPlaybook
  - @THE HELK
  - ATTACK-Python-Client
  - @OSSEM_Project
  - @Mordor_Project
  - Blacksmith & More

- Founder:
  - @HuntersForge

https://github.com/hunters-forge
Agenda

- What is the goal of Purple Teaming?
- Purple Teaming Challenges?
  - Planning vs Execution
- Are we being effective at purple teaming?
- The Mordor Project
- Purple Teaming - Mordor Style
- Enabling the community!
What is the Goal of Purple Teaming?

Or at least one of the goals! :)

4
What can we do together?
Remember: It is **NOT** a Competition!

Legolas! Two already!

I'm on seventeen!

I'll have no pointy-ear outscoring me!
A Few Goals!

- Validate current detections
- Build new detections
- Brainstorm new tradecraft
- Map data to adversary actions
- Improve Telemetry
- Learn from each other
  - Red improves Blue
A Few Goals!

- Validate current detections
- Build new detections
- Brainstorm new tradecraft
- Map data to adversary actions
- Improve Telemetry
- **Learn from each other**
  - Red improves Blue
  - Blue improves Red too!
Believe me! You will always learn something new..
Rubeus

- Rubeus is a C# re-implementation of some of the functionality from Benjamin Delpy's Kekeo project
  - Kerberos structures built by hand...
  - Rubeus works nicely with execute-assembly
  - So why not use Kekeo? Because ASN.1!
    - Requires a commercial ASN.1 library to customize/rebuild the Kekeo codebase
- **Author:** Will Schroeder @harmj0y
Rubeus: over-pass-the-hash

Mimikatz pth

- "sacrificial" logon session that doesn't interact with the current logon session.
- Opens the LSASS process
- Patches associated logon session with hash/key.
- Normal Kerberos authentication process Kicks off (Hash->TGT)

Rubeus asktgt (createnetonly)

- CreateProcessWithLogonW Function to create a sacrificial process/logon session
- Rubeus builds/crafts AS-REQ (w/ preauth)
- TGT request successful
- Imports TGT to logon session (Hash->TGT)

https://www.youtube.com/watch?v=QCDBjFJ_C3g
Rubeus askTGT does NOT touch LSASS!

Mimikatz pth

- "sacrificial" logon session that doesn't interact with the current logon session.
- **Opens the LSASS process**
- Opens the LSASS process
- Patches associated logon session with hash/key.
- Normal Kerberos authentication process Kicks off (Hash->TGT)

Rubeus asktgt (createsetonly)

- CreateProcessWithLogonW Function to create a sacrificial process/logon session
- Rubeus builds/crafts AS-REQ (w/ preauth)
- TGT request successful
- Imports TGT to logon session (Hash-TGT)

https://www.youtube.com/watch?v=QCDBjFJ_C3g
Mimikatz & Rubeus - Kerberos Authentication

https://www.youtube.com/watch?v=QCDBjFJ_C3g
Mimikatz & Rubeus - Kerberos Authentication

https://www.youtube.com/watch?v=QCDBjFJ_C3g
Purple Teaming Challenges
Purple Team Challenges?

- What techniques do we prioritize?
- What is the scope? (Production?)
- What is the risk?
- How long is it going to take?
- Do we use our own Tradecraft?
- How do we handle communications?
- What are the deliverables?
- How do we track findings?
- Who is in charge?
- How do we split the team?

- Do we need to update our audit policies?
- Are we collecting data from every endpoint in scope?
- Do we even know what events we are collecting?
- Do we write a report together?
- Do we do do a tabletop exercise?
- What metrics can we use?
- Who else should be included?
Purple Team Challenges? *(Strategy & Preparation)*

- What techniques do we prioritize?
- What is the scope? (Production?)
- What is the risk?
- How long is it going to take?
- Do we use our own Tradecraft?
- How do we handle communications?
- What are the deliverables?
- How do we track findings?
- Who is in charge?
- How do we split the team?

- Do we need to update our audit policies?
- Are we collecting data from every endpoint in scope?
- Do we even know what events we are collecting?
- Do we write a report together?
- Do we do do a tabletop exercise?
- What metrics can we use?
- Who else should be included?
Purple Team Challenges? (Strategy & Preparation)

- What techniques do we prioritize?
- What is the scope? (Production?)
- What is the risk?
- How long is it going to take?
- Do we use our own Tradecraft?
- How do we handle communications?
- What are the deliverables?
- How do we track findings?
- Who is in charge?
- How do we split the team?

- Do we need to update our audit policies?
- Are we collecting data from every endpoint in scope?
- Do we even know what events we are collecting?
- Do we write a report together?
- Do we do do a tabletop exercise?
- What metrics can we use?
- Who else should be included?
Purple Teaming Challenges

What about during the execution?
Purple Teaming: Ad-Hoc Execution! (I Love it!)

Just adding to the list of autorun evasions. Having some fun back and forth with @Cyb3rWard0g :)

https://twitter.com/tifkin_/status/953688435482652674
Purple Teaming: Basic Planned Execution

Plan Engagement

Emulate Adversary

Collect & Analyze Data

Enable Telemetry

Can I see it?

Yes

No

Document Results
Purple Teaming: Basic Planned Execution

Plan Engagement

Emulate Adversary

Collect & Analyze Data

Enable Telemetry

Can I see it?

No

Yes

Document Results
Planned Execution: Production Challenges

- How do you know what you need if you can't even see it?
- How long would it take to approve an audit policy change?
- How do you know the log volume that you are about to enable?
- How do you know it is not your data pipeline failing?
- What if your event logs are not parsed or standardized?
Planned Execution: Production Challenges

Emulate Adversary

Collect & Analyze Data

Can I see it?

Data Quality

No?
Planned Execution: Production Challenges

Emulate Adversary

Collect & Analyze Data

Can I see it?

Data Quality

Impacts Time Scope

No?
Planned Execution: Production Challenges
We all have busy schedules

https://dribbble.com/GraphicChendol
Purple Teaming: Ad-Hoc Execution! (I Love it!)

Just adding to the list of autorun evasions. Having some fun back and forth with @Cyb3rWard0g :)

https://twitter.com/tifkin_/status/953688435482652674
Planned Execution: A Lab Before Production

Plan Engagement

Emulate Adversary

Collect & Analyze Data

Enable Telemetry

Can I see it?

Yes

No

Document Results

Can I see it?
We can start improving this!
Purple Teaming Challenges

Can you run this technique variation one more time?
Execute -> Collect -> Analyze -> Repeat

Simulating Adversarial Technique

Data produced

Test Security Controls

Model Adversary Behavior

Plan Engagement

Emulate Adversary

Enable Telemetry

Collect & Analyze Data

Can I see it?

Document Results

No

Yes
Same Technique + Some Variations

Data produced

Model Adversary Behavior

Test Security Controls
Same Technique + Some Variations

Data produced

Same Data? Similar Events?

Test Security Controls

Model Adversary Behavior
Lateral Movement via WMI (Win32_Process Create)

- **wmic** /node:172.18.39.106 /user:Administrator /password:P1ls3n! process call create cmd.exe
- **Invoke-WmiMethod** -ComputerName 172.18.39.106 -Credential Administrator -Class Win32_Process -Name Create -ArgumentList notepad.exe
- **SharpWMI.exe** action=create computername=HR01.shire.com command="powershell.exe -enc ZQBj..."
- **./wmiexec** shire.com/pgustavo@172.18.39.106
Lateral Movement via WMI - Behavior

User → Host
Authentication
Logon Type (3)

Process
svchost.exe

Process
Wmiprvse.exe

Logon Session: Logon Type 3
creates

Process
?.exe
creates

Process
?.exe

https://twitter.com/HunterPlaybook/status/1171103081246969856
**Lateral Movement via WMI - Behavior**

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Event ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>4624</td>
</tr>
<tr>
<td>Sysmon</td>
<td>3</td>
</tr>
</tbody>
</table>

Logon Session: Logon Type 3
- Creates `svchost.exe`
- Creates `Wmiprvse.exe`
- Creates `?.exe`

User → Host
- Authentication
  - Logon Type (3)

https://twitter.com/HunterPlaybook/status/1171103081246969856
Lateral Movement via WMI - Behavior

Log Name | Event ID
---|---
Security | 4624
Sysmon | 3

Logon Session: Logon Type 3

- svchost.exe
- Wmiprvse.exe

Process

- creates
- creates

https://twitter.com/HunterPlaybook/status/1171103081246969856
Same Technique + Some Variations

- Wmic
- Invoke-WMIMethod
- SharpWMI
- Wmiexec

Data produced

Test Security Controls

Model Adversary Behavior
Can you run it again? Please!

- Wmic
- Invoke-WMIMethod
- SharpWMI
- Wmiexec

Data produced

Test Security Controls

Model Adversary Behavior
But... We are getting similar events...

Data produced

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Event ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>4624</td>
</tr>
<tr>
<td>Sysmon</td>
<td>3</td>
</tr>
<tr>
<td>Security</td>
<td>4688</td>
</tr>
<tr>
<td>Sysmon</td>
<td>1</td>
</tr>
</tbody>
</table>
Are we being effective at purple teaming?
Effective or Efficient Purple Teaming?

Efficiency ≠ Efficacy

Effectiveness

https://twitter.com/Cyb3rPandaH
Efficiency

The way resources are used (or wasted), How can I make the most of the resources I have.

Effectiveness

Accomplishes the goals (to be efficacious) employing the best and most economic methodology (to be efficient).

Efficacy

It doesn’t matter how we do it, but only on what we accomplish.
Efficiency

- Let’s prioritize specific techniques
- Can we automate adversary emulation plans?
- How do we replicate results?
- How do we expedite unit testing?
- How do I reduce the number of times a technique is executed for research?

Efficacy

- Let’s execute 5 techniques a week!
- At least 3 variations per technique!
- Let’s emulate all APT groups!
- Let’s test current security analytics!
We might be doing this over and over..
And we still get similar events..
What if we could save our output?

Plan Engagement

Emulate Adversary

Collect & Analyze Data

Enable Telemetry

Can I see it?

No

Yes

Document Results
What if we could save our output?

Plan Engagement

Emulate Adversary

Collect & Analyze Data

Enable Telemetry

Document Results

Can I see it?

Yes

No

Enable Telemetry

APT 3 Emulation Plan

Phase 1

Phase 2

Phase 3

Collect & Analyze Data

JSON

Plan Engagement

Emulate Adversary

Collect & Analyze Data
We could keep the momentum!
We could also train future purple teamers!
We could expedite analytic validation - Unit Testing

Mordor File

Validate Analytics

2 + 2 = 4
We could also help the community!
Enter Mordor
Mordor Project @Mordor_Project

- Pre-recorded security events generated by simulated adversarial techniques in the form of JavaScript Object Notation (JSON)
- Pre-recorded data categorized by platforms, adversary groups, tactics and techniques defined by the Mitre ATT&CK Framework.
- Data represents not only specific known malicious events but additional context/events that occur around it.

https://github.com/Cyb3rWard0g/mordor
Mordor Standard Environments

- Environment designed to replicate a small research network
- Standardized and documented setup
- Platforms
  - Windows
  - Linux
- Endpoints Telemetry
  - Windows Security Auditing
  - Event Tracing for Windows (ETW) (NEW!!)
- Network Telemetry
  - Network Logs
- Environments Available: Shire and Erebor deployed by BlackSmith!
Mordor Environments: The Shire
The Shire Design

HFDC01.shire.com
172.18.39.5
Administrator

WECServer.shire.com
172.18.39.102
Administrator

172.18.39.6
ubuntu

172.18.39.8
ubuntu

HR001.shire.com
172.18.39.106
nmartha

IT001.shire.com
172.18.39.105
pgustavo

ACCT001.shire.com
172.18.39.100
lrodriguez

FILE001.shire.com
172.18.39.103
Administrator
The Shire Telemetry: Win Logs & Sysmon

https://github.com/Cyb3rWard0g/OSSEM/tree/master/data_dictionaries/windows/sysmon
The Shire: Event Log -> WEC -> HELK

HR001.shire.com
172.18.39.106
nmartia

IT001.shire.com
172.18.39.105
pgustavo

WECServer.shire.com
172.18.39.102

ACCT001.shire.com
172.18.39.100
lrodriguez

kafka

HELK Server
172.18.39.6

https://mordor.readthedocs.io/en/latest/mordor_shire.html#
Mordor Environments: Erebor (Lonely Mountain)
Erebor Design

- **HFDC01.erebor.com**
  - 10.0.1.5
  - Administrator

- **WECServer.erebor.com**
  - 10.0.1.102
  - Administrator

- **10.0.1.6**
  - ubuntu

- **10.0.1.8**
  - ubuntu

- **HR001.erebor.com**
  - 10.0.1.106
  - bbaggins

- **IT001.erebor.com**
  - 10.0.1.105
  - toakenshield

- **ACCT001.erebor.com**
  - 10.0.1.100
  - kfili

- **FILE001.erebor.com**
  - 10.0.1.103
  - Administrator
Erebor Telemetry: ETW Events via SilkETW

XML
SilkServiceConfig.xml

Reads Config
SilkETW

Controller

Consumer

Real-Time Delivery

Enables ETW Providers

Microsoft-Windows-DotNETRuntime
Microsoft-Windows-DNS-Client
Microsoft-Windows-LDAP-Client
Microsoft-Windows-RPC

Creates Trace Sessions

Event Trace Sessions

Real-Time Delivery

SilkService-Log

Erebor: ETW Events -> Event Log -> WEC -> HELK

- HR001.erebor.com
  - 10.0.1.106
  - bbagins

- IT001.erebor.com
  - 10.0.1.105
  - toakenshield

- ACCT001.erebor.com
  - 10.0.1.100
  - kfili

- WEC
  - WECServer.erebor.com
    - 10.0.1.102

- HELK Server
  - 10.0.1.6
How do you export (consume) data?

- I use **Kafkacat**!
- kafkacat is a generic non-JVM producer and consumer for Apache Kafka >=0.8, think of it as a netcat for Kafka.

**In consumer mode**
- Kafkacat reads messages from a topic and prints them to standard output (stdout). You can also redirect it to a file.

**In producer mode**
- Kafkacat reads messages from standard input (stdin). You can also send data to kafkacat by adding data from a file.

https://github.com/edenhill/kafkacat
Consuming Data -> Creating Mordor File

Consuming Data (Taking a snapshot of data)

```
$ kafkacat -b <Kafka-IP>:9092 -t <kafka-Topic> -C -o end > file.json
```

- `-b` : Kafka broker
- `-t` : Topic to consume from
- `-C` : Consumer Mode
- `-o` : Offset to start consuming from
Producing Data (Injecting Adversary Dataset)
Producing Data (Injecting Adversary Dataset)

$ kafkacat -b <Kafka-IP>:9092 -t <kafka-Topic> -P -l file.json

- `-b`: Kafka broker
- `-t`: Topic to produce to
- `-P`: Producer Mode
- `-l`: Send messages from a file
Can I download all the available Mordor datasets?

```bash
$ git clone https://github.com/hunters-forge/mordor.git
$ cd mordor/small_datasets/
$ find . -type f -name "*.tar.gz" -print0 | sudo xargs -0 -I{} tar xf {} -C .
```
Purple Teaming - Mordor Style

One Adversarial Technique at the time!
Let’s do it!
Let's do it! (Demo)

```
Grunt: b1bde3dbff

Task
Assembly

AssemblyName

EncodedAssembly

Choose File
No file chosen

Parameters

ubuntu@ip-172-18-39-6:$
ubuntu@ip-172-18-39-6:$ ls -lh
total 0
ubuntu@ip-172-18-39-6:$ kafkacat -b localhost:9092 -t winlogbeat -C -o end > covenant_wmigrunt_powershell_$(date +%F%H%M%S).json
% Reached end of topic winlogbeat [0] at offset 1758940
% Reached end of topic winlogbeat [0] at offset 1758947
```
What about this other thing? (Demo)
Import and Analyze Mordor dataset (Demo)
Let’s do it! (Demo)
Purple Teaming - Mordor Style

Adversary Emulation Plans (Full Campaign)!
Emulating Adversary APT3

APT 3 Emulation Plan

Phase 1
- C2 Setup
- Software Packing
- Obfuscate Files
- Initial Access

Phase 2
- Compromise Host
- Defense Evasion
- Discovery
- Privilege Escalation
- Credential Access
- Persistence
- Lateral Movement
- Execution

Phase 3
- Collect Data
- Compress and Stage
- Exfiltrate

Figure 1 APT3’s Three Phases of Action

https://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf
## ATT&CK Evaluations: APT 3 Round 1

### Table:

|----------------|---------------------|-------------------|-----------|-------------------|------------|--------------------|--------------|--------------|----------|-----------|-----------|-----------|----------------|-----------|--------|
ATT&CK Evaluations: APT 3 Round 1 (Day 1 & 2)

Cobalt Strike

- Step 1 - Initial Compromise
- Step 2 - Initial Discovery
- Step 3 - Privilege Escalation
- Step 4 - Discovery for Lateral Movement
- Step 5 - Credential Access
- Step 6 - Lateral Movement
- Step 7 - Persistence
- Step 8 - Collection
- Step 9 - Exfiltration
- Step 10 - Execution of Persistence

Empire

- Step 11 - Initial Compromise
- Step 12 - Initial Discovery
- Step 13 - Discovery for Lateral Movement
- Step 14 - Privilege Escalation
- Step 15 - Credential Access
- Step 16 - Lateral Movement
- Step 17 - Persistence
- Step 18 - Collection
- Step 19 - Exfiltration
- Step 20 - Execution of Persistence
## ATT&CK Evaluations: APT 3 Round 1 Day 2

<table>
<thead>
<tr>
<th>ATT&amp;CK Eval Step</th>
<th>ATT&amp;CK Eval Phase</th>
<th>Tactic</th>
<th>Technique Id</th>
<th>Technique Name</th>
<th>Empire Commands / Notes</th>
<th>Source Endpoint</th>
<th>Source Username</th>
<th>Target Endpoint</th>
<th>Target Username</th>
<th>ATT&amp;CK Eval Scenario #2 Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.A.1</td>
<td>Initial Access</td>
<td>Defense Evasion Execution</td>
<td>T1064</td>
<td>Scripting</td>
<td>usetager windows\launchers_vbs set Listener https set OutFile \tmp\autoupdate.vbs execute user nmarta double click vbs script</td>
<td>HR001</td>
<td>nmarta</td>
<td>HR001</td>
<td>nmarta</td>
<td>Initial compromise was emulated via a malicious VBS script. A legitimate user executed a VBS script stager, which launched PowerShell to download and execute an Empire payload</td>
</tr>
<tr>
<td>11.B.1</td>
<td>Initial Access</td>
<td>Command and Control</td>
<td>T1043</td>
<td>Commonly Used Port</td>
<td>listeners use listener http set Name http set Host 10.0.10.106 set Port 443 set CertPath iopt/Empire/data execute</td>
<td>HR001</td>
<td>nmarta</td>
<td>HR001</td>
<td>nmarta</td>
<td>The executed Empire payload established an encrypted C2 channel over HTTPS on TCP port 443</td>
</tr>
<tr>
<td>11.B.1</td>
<td>Initial Access</td>
<td>Command and Control</td>
<td>T1071</td>
<td>Standard Application Layer Protocol</td>
<td>listeners use listener http set Name https set Host 10.0.10.106 set Port 443 set CertPath iopt/Empire/data execute</td>
<td>HR001</td>
<td>nmarta</td>
<td>HR001</td>
<td>nmarta</td>
<td>The executed Empire payload established an encrypted C2 channel over HTTPS on TCP port 443</td>
</tr>
<tr>
<td>11.B.1</td>
<td>Initial Access</td>
<td>Command and Control</td>
<td>T1032</td>
<td>Standard Cryptographic Protocol</td>
<td>listeners use listener http set Name https set Host 10.0.10.106 set Port 443 set CertPath iopt/Empire/data execute</td>
<td>HR001</td>
<td>nmarta</td>
<td>HR001</td>
<td>nmarta</td>
<td>The executed Empire payload established an encrypted C2 channel over HTTPS on TCP port 443</td>
</tr>
<tr>
<td>12.A.1</td>
<td>Initial Discovery</td>
<td>Discovery</td>
<td>T1016</td>
<td>System Network Configuration Discovery</td>
<td>shell route print</td>
<td>HR001</td>
<td>nmarta</td>
<td>HR001</td>
<td>nmarta</td>
<td>The route utility was executed via PowerShell to enumerate the local routing table.</td>
</tr>
<tr>
<td>12.A.2</td>
<td>Initial Discovery</td>
<td>Discovery</td>
<td>T1016</td>
<td>System Network Configuration Discovery</td>
<td>shell ipconfig /all</td>
<td>HR001</td>
<td>nmarta</td>
<td>HR001</td>
<td>nmarta</td>
<td>The ipconfig utility was executed via PowerShell to enumerate local TCP/IP network configuration information.</td>
</tr>
<tr>
<td>12.B.1</td>
<td>Initial Discovery</td>
<td>Discovery</td>
<td>T1033</td>
<td>System Owner/User Discovery</td>
<td>shell whoami /all /lo list</td>
<td>HR001</td>
<td>nmarta</td>
<td>HR001</td>
<td>nmarta</td>
<td>The whoami utility was executed via PowerShell to enumerate information about the current user.</td>
</tr>
<tr>
<td>12.C.1</td>
<td>Initial Discovery</td>
<td>Discovery</td>
<td>T1057</td>
<td>Process Discovery</td>
<td>shell procexp *</td>
<td>HR001</td>
<td>nmarta</td>
<td>HR001</td>
<td>nmarta</td>
<td>The process utility was executed via PowerShell to enumerate local running processes.</td>
</tr>
<tr>
<td>12.D.1</td>
<td>Initial Discovery</td>
<td>Discovery</td>
<td>T1007</td>
<td>System Service Discovery</td>
<td>shell net start</td>
<td>HR001</td>
<td>nmarta</td>
<td>HR001</td>
<td>nmarta</td>
<td>The net utility was executed via PowerShell to enumerate local active services.</td>
</tr>
<tr>
<td>12.E.1</td>
<td>Initial Discovery</td>
<td>Defense Evasion Execution</td>
<td>T1064</td>
<td>Scripting</td>
<td>usmodule situational_awareness/host\winenum</td>
<td>HR001</td>
<td>nmarta</td>
<td>HR001</td>
<td>nmarta</td>
<td>Empire: Built-in WinEnum module executed to programmatically execute a series of enumeration techniques.</td>
</tr>
<tr>
<td>12.E.1.1</td>
<td>Initial Discovery</td>
<td>Discovery</td>
<td>T1033</td>
<td>System Owner/User Discovery</td>
<td>usmodule situational_awareness/host\winenum</td>
<td>HR001</td>
<td>nmarta</td>
<td>HR001</td>
<td>nmarta</td>
<td>WinEnum: Get-Userinfo</td>
</tr>
<tr>
<td>12.E.1.2</td>
<td>Initial Discovery</td>
<td>Discovery</td>
<td>T1069</td>
<td>Permission Groups Discovery</td>
<td>usmodule situational_awareness/host\winenum</td>
<td>HR001</td>
<td>nmarta</td>
<td>HR001</td>
<td>nmarta</td>
<td>WinEnum: &quot;AD Group Memberships&quot;</td>
</tr>
<tr>
<td>12.E.1.3</td>
<td>Initial Discovery</td>
<td>Discovery</td>
<td>T1201</td>
<td>Password Policy Discovery</td>
<td>usmodule situational_awareness/host\winenum</td>
<td>HR001</td>
<td>nmarta</td>
<td>HR001</td>
<td>nmarta</td>
<td>WinEnum: &quot;Password Last Changed&quot;</td>
</tr>
</tbody>
</table>

[Link to GitHub repository](https://github.com/hunters-forge/mordor/blob/master/large_datasets/apt3/scope/apt3_mordor_playbook.xlsx)
Purple Teaming - Mordor Style

Automating Adversary Emulation Plans
Caldera: Automated Adversary emulation (ATT&CK)

Cyber Adversary Language and Decision Engine for Red Team Automation

I am a **blue-teamer**

As a blue-team operator, you should start by deploying one or many 54ndc47 (Sandcat) agents on remote computers you want to test. Then move into Chain mode to create adversary profiles and run operations against the deployed hosts.

I am a **researcher**

As a researcher, you should restart the server with the mock plugin, which deploys simulated agents. Then, go into Chain mode and run a few sample operations. Once familiar with how abilities link together, study the sequential.py module in the source code, which contains the automated decision-making logic.

I am a **red-teamer**

As a red-team operator, you should restart the server with the terminal plugin loaded. Then, deploy one or many 54ndc47 (Sandcat) agents on remote computers. Use the terminal to create and join reverse-shell sessions to manually compromise the hosts.

https://github.com/mitre/caldera
Caldera Installation

- git clone --recursive https://github.com/mitre/caldera.git
- cd caldera/
- pip3 install -r requirements.txt
- python -u server.py

- git clone https://github.com/Cyb3rWard0g/docker-caldera
- cd docker-caldera/
- docker-compose -f docker-compose-caldera.yml up --build -d
Caldera: Automated Adversary emulation (ATT&CK)

https://github.com/mitre/caldera
Is there a plugin for the ATT&CK evals?
Caldera ATT&CK Evals Plugin (NEW!)

ATT&CK | Evals

Initial Compromise

Manually execute the Remote Access Tool (RAT) on target machine (see Sandcat). Automated delivery is out of scope of this exercise and must be executed manually. Once this is completed, begin the evaluation by starting the ‘ATT&CK Eval APT3’ operation using Chain mode and include the “evals” fact sheet (see Chain).

2.A.1 - System Network Configuration Discovery (T1016)

2.A.2 - System Network Configuration Discovery (T1016)

https://github.com/mitre-attack/evals_caldera
Whaaat? You can just let the plugin do it all?
Caldera: APT3 ATT&CK Eval Round 1 Day 1

ATT&CK Eval APT3 - Full

full evaluation

Phase 1

2.A.2 - System Network Configuration Discovery (T1016)
The arp utility is executed via cmd to enumerate local ARP configuration information.
DISCOVERY | T1016 | SYSTEM NETWORK CONFIGURATION DISCOVERY

Phase 2

2.B.1 - System Owner / User Discovery (T1033)
The native echo command is executed via cmd to enumerate local environment variables associated with current user and domain.
DISCOVERY | T1033 | SYSTEM OWNER/USER DISCOVERY

https://attackevals.mitre.org/methodology/round1/scope.html
Phase 17

8.D.1 - Screen Capture (T1113)
Native API call(s) were used to collect a screenshot.
COLLECTION | T1113 | SCREEN CAPTURE

Phase 18

9.B.1 - Data from Network Shared Drive (T1039) and Exfiltration over C2 Channel (T1041)
Copy a target file from a remote file share through the existing C2 channel
EXFILTRATION | T1041 | EXFILTRATION OVER COMMAND AND CONTROL CHANNEL

Phase 19

EXECUTION | T1086 | POWERSHELL
Caldera: ATT&CK Evals Plugin Installation

- cd caldera/plugins
- git clone https://github.com/mitre-attack/evals_caldera.git
- Modify caldera/conf/local.yml file and add

  "- evals_caldera" under plugins
Can I do it at home?
Blacksmith Project & Mordor!

- git clone https://github.com/hunters-forge/Blacksmith
- Follow pre-requirements before deploying Shire Environment: https://blacksmith.readthedocs.io/en/latest/mordor_shire.html
- Update parameter RTODefaultC2 to caldera in cfn-parameters/shire/c2-server-parameters.json
- Update parameter RestrictLocation in cfn-parameters/shire/ec2-network-parameters.json
- Run ./deploy.sh -e ‘shire’
Blacksmith Project & Mordor!

https://github.com/hunters-forge/Blacksmith/blob/master/aws/mordor
Thank you so much Daniel!
Initial Compromise

Manually execute the Remote Access Tool (RAT) on target machine (see Sandcat). Automated delivery is out of scope of this exercise and must be executed manually. Once this is completed, begin the evaluation by starting the 'ATT&CK Eval APT3' operation using Chain mode and include the 'evals' fact sheet (see Chain).

2.A.1 - System Network Configuration Discovery (T1016)

2.A.2 - System Network Configuration Discovery (T1016)
What did we learn today?
Purple Teaming - Mordor Style

- Practice like you play before production!
- Be prepared and make sure you set rules of engagement!
- Keep the back and forth going and at the same time:
  - Take data snapshots of each technique or whole emulation plan (very very helpful and convenient!!)
  - Reuse pre-recorded data for additional deep research
  - Expedite analytic validations with the datasets
  - Train other purple teamers with re-recorded events
  - Learn from the data produced (Red & Blue)
Purple Teaming - Mordor Style

- Practice like you play before production!
- Be prepared and make sure you set rules
- Keep the back and forth going and at the same time:
  - Take data snapshots of each technique or whole emulation plan (very very helpful and convenient!!)
  - Reuse pre-recorded data for additional deep research
  - Expedite analytic validations with the datasets
  - Train other purple teamers with re-recorded events
  - Learn from the data produced (Red & Blue)
Purple Teaming - Mordor Style

- Practice like you play before production!
- Be prepared and make sure you set rules
- Keep the back and forth going and at the same time:
  - Take data snapshots of each technique or whole emulation plan (very very helpful and convenient!!)
  - Reuse pre-recorded data for additional deep research
  - Expedite analytic validations with the datasets
  - Train other purple teamers with re-recorded events
  - Learn from the data produced (Red & Blue)
- **Empower others and give back to the community!**
Threat Hunters Forge Community!

Threat Hunters Forge
Data Science, Threat Hunting & Open Source Projects
Threat Hunters Forge Slack Community!

ThreatHunting
Threat Hunters Forge

Join the Threat Hunters Forge Slack Community!

A community led effort to share detection strategies and to support open source projects to aid the development of security analytics and tooling for threat hunting!

https://launchpass.com/threathunting
Goal: Share and Empower the Community!
Let’s do it together!
Threat Hunters Forge References

- GitHub: https://github.com/hunters-forge
- Python Library: https://github.com/Cyb3rPanda/openhunt
- Slack Invitation: https://launchpass.com/threathunting
- Founders: @Cyb3rWard0g & @Cyb3rPandaH
- Official Twitter: @HuntersForge
- @HunterPlaybook
- @THE_HELK
- @OSSEM_Project, @Mordor_Project & More
Thank You! Muchas Gracias!