PURPLE TEAM
SUMMIT & TRAINING

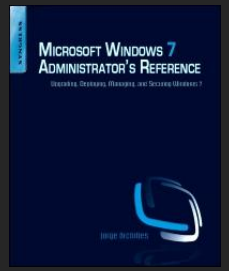
Work it Out: Organizing Effective Adversary Emulation Exercises

@JorgeOrchilles

#PurpleTeamSummit

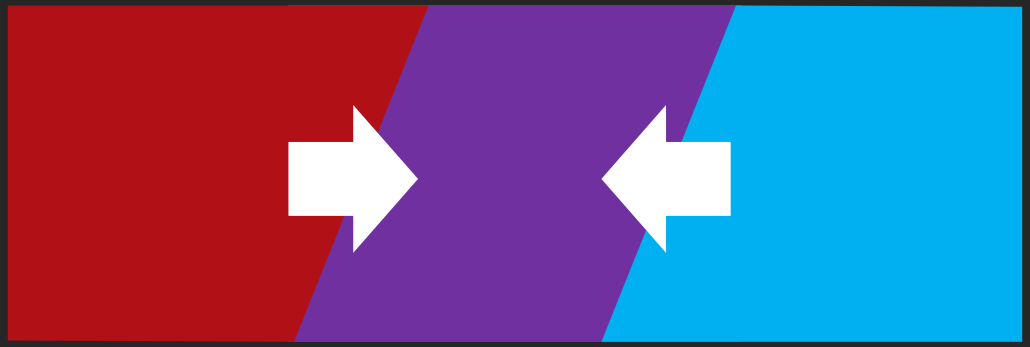
T1033 - System Owner/User Discovery

- 9+ years leading offensive team at Large Financial
- SANS Instructor & Author
- SEC564: Red Team Exercises and Adversary Emulation
- CVSSv3.1 Working Group Voting Member
- Author GFMA: Threat-Led Pen Test Framework
- Windows 7 Administrator's Reference (Syngress)
- South FL ISSA, Fellow, and Webinar Committee



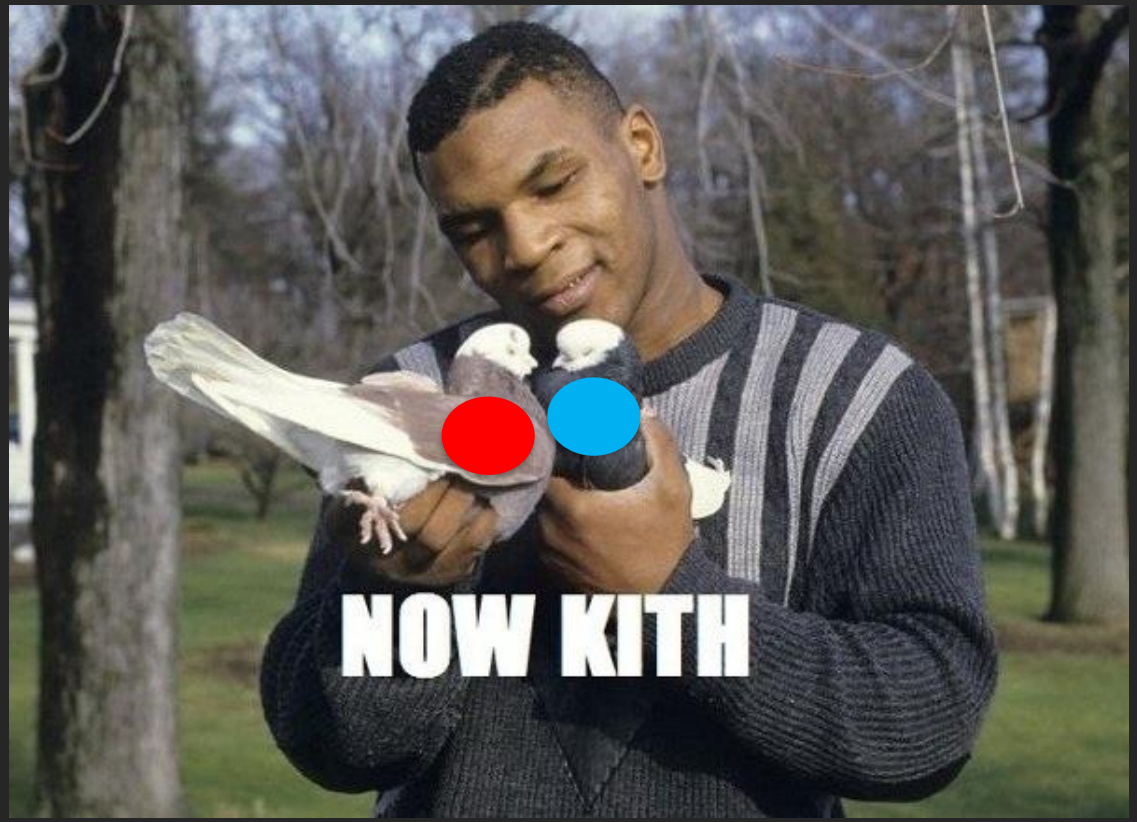
@jorgeorchilles

Purple… how hard can it be?



@jorgeorchilles

Lock Red and Blue in the same room

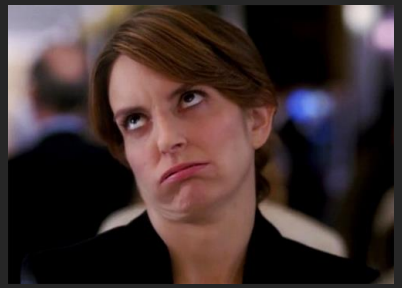


@jorgeorchilles

How you think it will go

@jorgeorchilles

How it may go



@jorgeorchilles

Agenda (because #structuredlife)

- How did we get here?
- Goals
- Sponsors and Roles
- Framework/Methodology
- TTPs
- Infrastructure Setup
- Team Prep

- Kick Off
- Exercise Flow
- Wrap Up
- Show Value

@jorgeorchilles

How did we get here?

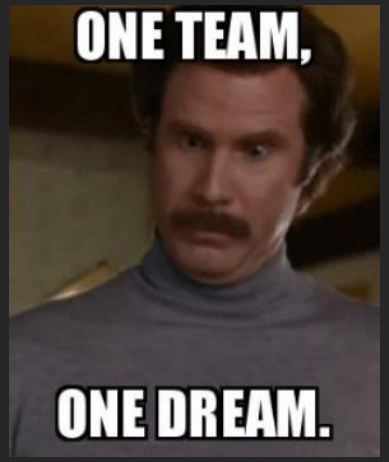
Adversary Emulation: effort to reproduce how an adversary operates, following the same Tactics, Techniques, and Procedures, to reach a similar objective

- Blind (Blue Team doesn't know of exercise)
  - Red Team Exercise || Threat-Led Penetration Test
- Non-Blind: Purple Team Exercise

Define: “In Person Purple Team Exercise”

‘Hands on keyboard’ engagement where:

- Red and Blue teams sit together
- Having an open discussion as one team
- While performing TTPs
- Review detective/preventive controls
- Perform live incident response
- Improve people, process, and technology



@jorgeorchilles

Adversary Emulation Goals

- Emulate an end to end attack against a target organization
- Obtain a holistic view of target organization
- Measure people, process, and technology
- When to do In Person Purple Team?
  - Prior to a blind Adversary Emulation
  - After a blind Adversary Emulation as “Replay”
  - To train new team members
  - Periodic training for certain operational locations
  - To chain TTPs (Attack Patterns) that have previously been documented
- Continuous Purple Team
  - Test new TTPs based on Threat Intelligence

We Need Sponsors aka $$$

- Approve the exercise, scope, and budget
- 2-3 members of each team:
  - Red Team
  - SOC
  - Incident Response

Time Requirements

- In-Person 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	Action Items
4-8 weeks	1 week	Undefined

Roles & Responsibilities

Title	Role	Responsibility
Head of Information Security	Sponsor	Approve Exercise and Budget
Red Team Manager	Sponsor & Attendee	Define Goals, Select Attendees, Select TTPs
SOC Manager	Sponsor & Attendee	Define Goals, Select Attendees, Select TTPs
Incident Response Manager	Sponsor	Define Goals, Select Attendees, Select TTPs
Threat Intelligence Analyst	Sponsor	Define Goals, Select TTPs
Red Teamers	1-3 Attendee(s)	Prepare, Attend, Action Items
SOC Analysts	2-5 Attendee(s)	Prepare, Attend, Action Items
Hunt Teamers	1-3 Attendee(s)	Prepare, Attend, Action Items
Incident Response Analysts	1-3 Attendee(s)	Prepare, Attend, Action Items
Exercise Coordinator	1-2	Operational Managers that lead Preparation Phase activities, participate in or observe the exercise, and responsible for the Lessons Learned document. Record minutes, notes, action items, and feedback. Send daily emails with those notes as well as plan for the next day.

Framework & Methodology

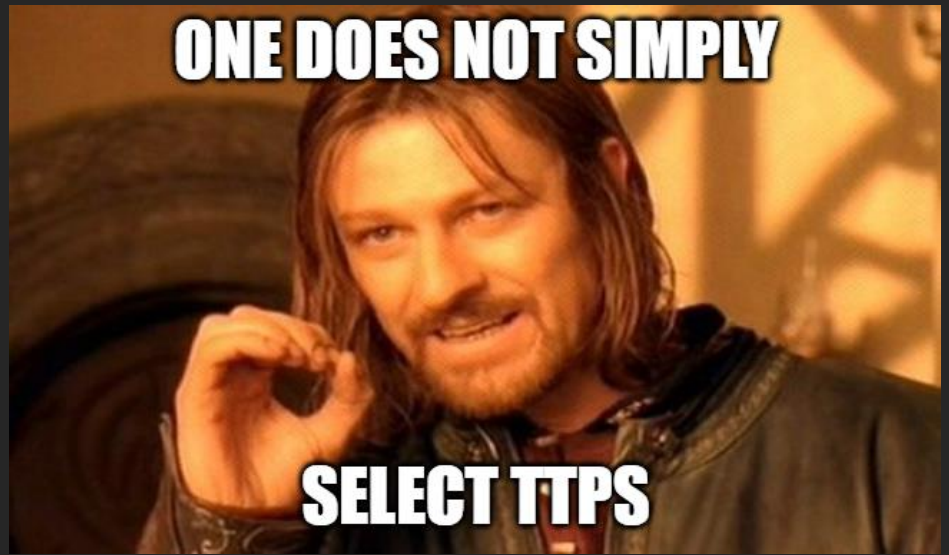
- Cyber Kill Chain – Lockheed Martin
- Unified Cyber Kill Chain – Paul Pols
- Financial/Regulatory Frameworks
  - CBEST Intelligence Led Testing
  - Threat Intelligence-Based Ethical Red Teaming
  - Red Team: Adversarial Attack Simulation Exercises
  - Intelligence-led Cyber Attack Simulation Testing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

Mandatory MITRE ATT&CK Slide

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	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption

Select TTPs

- Select TTPs at least 4 weeks in advance and based on goals
- TTPs chosen should be actively used by malicious actors targeting the organization



@jorgeorchilles

ATT&CK Navigator

https://mitre-attack.github.io/attack-navigator/enterprise/

Extract TTPs from CTI

T1068 – Exploitation for Privilege Escalation

T1086 – PowerShell

S0129 – AutoIT

S0194 – PowerSploit

The payload was an AutoIT downloader that retrieved and executed additional PowerShell from hxxps://85.206.161[.]216:8080/HomePage.htm. The follow-on PowerShell profiled the target system's architecture, downloaded the appropriate variant of PowerSploit (MD5: *c326f156657d1c41a9c387415bf779d4* or *0564706ec38d15e981f71eaf474d0ab8*), and reflectively loaded PUPYRAT (MD5: *94cd86a0a4d747472c2b3f1bc3279d77* or *17587668AC577FCE0B27842CB8EB72AC*). The actor leveraged a publicly available exploit for CVE-2017-0213 to escalate privileges, publicly available Windows SysInternals PROCDUMP to dump the LSASS process, and publicly available MIMIKATZ to presumably steal additional credentials. Managed Defense aided the victim in containing the intrusion.

T1003 – Credential Dumping

IP Address

S0002 – Mimikatz

S0192 – Pupy

Hash Value

FireEye Threat Intel: https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html

Discuss TTPs

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

Procedure	Technique	Tactic	Detection	SOC	Hunt	IR
<TTP1>	<Technique1>	<Tactic1>	<Control1>	x	x	x
<TTP2>	<Technique2>	<Tactic2>	<Control2>	x	x	
<TTP3>	<Technique3>	<Tactic3>	<Control3>	x		x
<TTP4>	<Technique4>	<Tactic4>	<Control4>		x	x

Use VECTR

https://vectr.io/

VECTR Dashboard

localhost:8081/sra-purpletools-webui/app/#/app/assessmentGroup/campaigns/full/phase/

SAMPLE_MITRE_ATTACK / MITRE ATTACK Q2 2018 / Full Assessment / Execution

New Test Case

Status: NotPerformed

Attack Start

Attack Stop

Source IPs

Red Team Details

Name: Test Case

Description: objective

Attack Pattern: method

Phase: Execution

Command: command

References

Attacker Tools

Target Assets

Blue Team Details

Outcome: TBD, Blocked, Detected, NotDetected

Outcome Notes: outcomeNotes

Tags

Rules

Detection Time

Expected Detection Layers

Prevention

Detection

Logistics

- Pick a physical location
  - 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 to show current screen to other participants

Target Systems

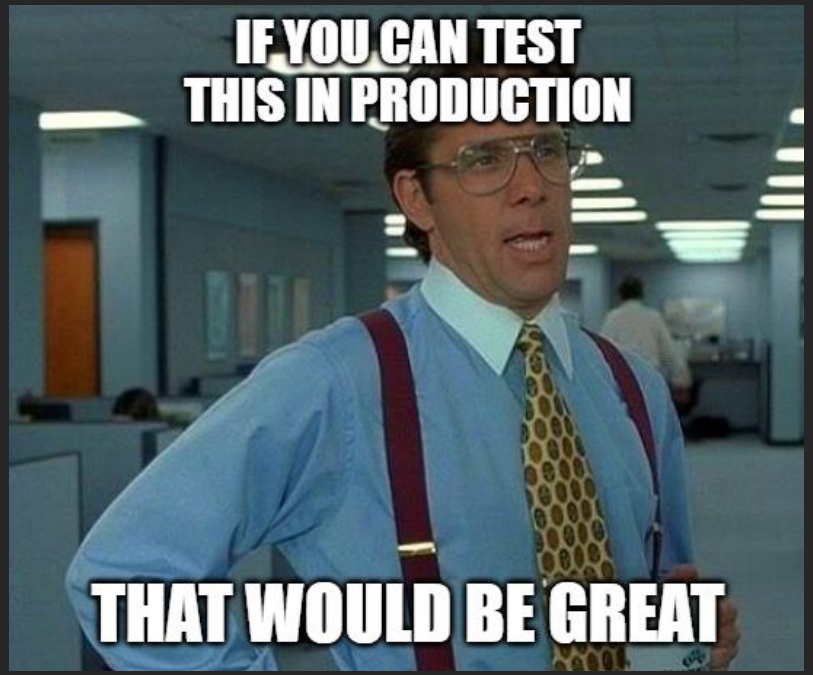
Provision production systems for exercise

- Endpoint Operation Systems in Environment
  - Windows 7 through 10 – multiple hosts
  - Terminal Services/Citrix
- Server Operating Systems in Environment
  - Windows Servers
  - *nix Servers
- Consider VDI, virtual, and cloud servers

Security Tools

Request the target systems have production security tools:

- Anti-Virus/Anti-Malware
- Anti-Exploit
- Endpoint Detection & Response
- Forensic Tools
  - Image acquisition
  - Live forensics



Target Accounts

Service or secondary accounts should be created for logging into systems, accessing Internet, receiving email, etc. and to ensure real production credentials are not compromised

- Request secondary account of a standard user
- Request Standard Email Access
- Request Internet Access
- Add accounts as local administrator of some target systems

Attack Infrastructure

- Choose and procure external hosting provider
- Create internal and Internet virtual machines
  - Only allow connection from organization proxies and Red Team IP addresses
  - Obtain and add external IP address of External Line of location of event
  - Build Credential theft site or Payload delivery sites
  - Setup C2 Infrastructure – based on payloads and TTPs
- Ensure SMTP servers allow sending emails into organization
- Purchase Domains and TLS Certificates
- Provide IP addresses and Domains to SOC for whitelisting
- Ensure white listed on any Network Access Controls

Red Team Prep

- Setup at least 2 laptops to show the attack activity live
- Ensure Attack Infrastructure is fully functional
- Ensure Target Systems are fully functional
- Document all commands required to emulate TTPs (Adversary Emulation Manual)
- 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 alike

SOC/Hunt Team Prep

- Validate security tools are reporting to SOC production tools from the target systems
- Ensure C2 whitelist of the Red Team domains
- Ensure TLS decryption for the Red Team domains
- Verify whitelisting
- Work with Red Team during testing of payloads and C2 prior to exercise
- Ensure laptop or workstations have access to all tools for showing on large screen in exercise location

Incident Response Prep

- Create an IR case/id
  - 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 correct forensic tools are deployed on the target systems
- Install Live Forensic Tools for efficiency
  - Sysmon
  - Processmon

Day of Exercise

- Exercise Coordinators should arrive early to ensure all systems are working:
  - Video conference
  - Presentation mode
  - External WiFi
  - Attack Infrastructure
  - Target Systems
- Purple Team Exercises should kick off in the afternoon in the event anyone is running late due to logistical issues

Kick Off

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

Exercise Flow

1. Red Team presents the TTP and technical details
   - Attack Vector
   - Delivery Method
   - User Interaction
   - Privilege gained
   - Tool or exploit used
2. Purple Team discussion of controls based on delivery method
   - SOC: Any logs or alerts for this TTP
   - Hunt Team: Any Hunt Cases for this TTP
   - Incident Response: Documented methods to identify if TTP was leveraged

Exercise Flow

3. Red Team executes the TTP
   - Provides attacker IP address
   - Provides target
   - Provides exact time
   - Shows the attack on projector
4. SOC, Hunt, and IR follow process to identify evidence of TTP
   - Time must 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

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
- [x] Detected
- [ ] NotDetected

Detecting Blue Tool(s):

McAfee ESM

McAfee Endpoint

What was the alert severity?

- [ ] Info
- [ ] Low
- [ ] TBD
- [ ] Med
- [x] 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. Show on screen if TTP was identified, received logs, alert, or forensic data
   - Time to detect and/or time to receive alert
   - Red Team stops TTP
6. Document what worked and what did not
7. Is there any short term adjustments that can increase visibility?
   - Implement adjustment
   - Red Team re-runs TTP
8. Document any Action Items
9. Repeat flow for the next TTP

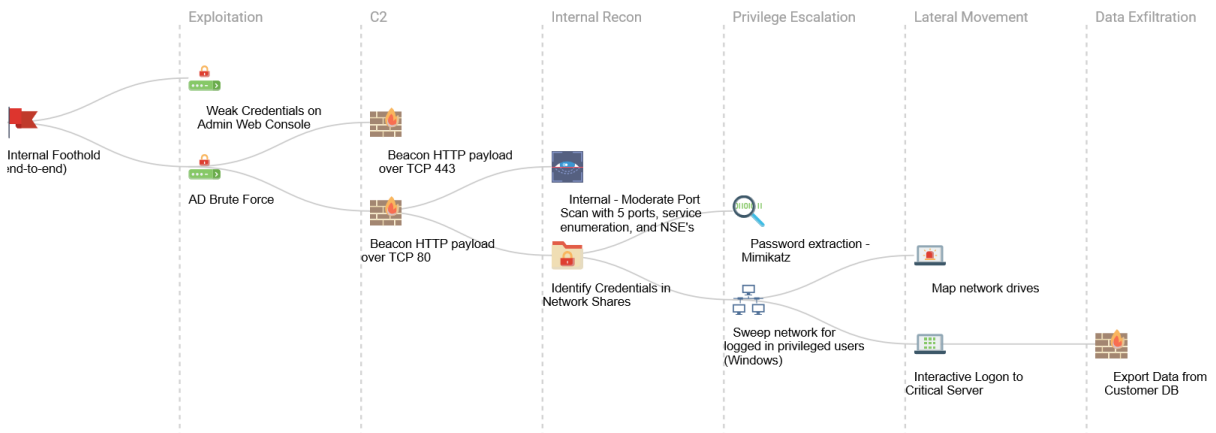
Wrap Up

- At least one dedicated Exercise Coordinator should be on site 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 also 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 30 days after the exercise has concluded

How to show value?

@jorgeorchilles

Internal Foothold (end-to-end): Escalation Path



Timeline

- 09/25/2018 07:43:31
  Password extraction - Mimikatz : outcome changed to Detected
- 02/02/2017 11:06:53
  Password extraction - Mimikatz : outcome changed to Blocked
- 02/02/2017 06:54:17
  Sweep network for logged in privileged users (Windows) : outcome changed to Detected
- 02/02/2017 05:22:55
  Interactive Logon to Critical Server : outcome changed to Detected
- 02/02/2017 04:16:07
  Map network drives : outcome changed to Detected
- 02/01/2017 06:23:18
  AD Brute Force : outcome changed to Detected
- 02/01/2017 04:38:04
  Beacon HTTP payload over TCP 80 : status changed to

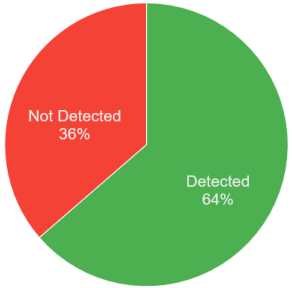
Test Cases

NEW

search filter ...

Phase	Method	Test Case	Status	Outcome	Action
Exploitation	App Server Exploitation	Weak Credentials on Admin Web Console	Completed	Not Detected	
Exploitation	Brute Force AD Account Credentials	AD Brute Force	Completed	Detected	
C2	C2 Channel	Beacon HTTP payload over TCP 443	Completed	Detected	
C2	C2 Channel	Beacon HTTP payload over TCP 80	Completed	Not Detected	
Privilege Escalation	Extract credentials	Password extraction - Mimikatz	Completed	Detected	
Privilege Escalation	Obtain Domain Admin Creds	Sweep network for logged in privileged users (Windows)	Completed	Detected	

Detection Status



2017 Q1 Purple Team

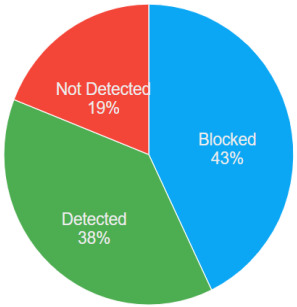
2017 Q1 Purple Team

Assessments Aggregated

Test Cases Completed:	126
Test Cases Passed:	102
Detected:	48
Blocked:	54
Test Cases Failed:	24
Not Detected:	24
Test Cases Not Completed:	0
To Be Determined:	0

Overall Score

Superior



Campaigns with Most Success

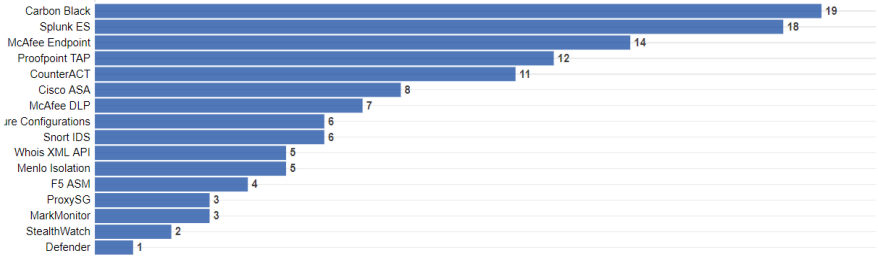
C2 Channels - Round 3	Superior (100.00%)
Windows Domain Enumeration	Superior (100.00%)
Network MiTM	Superior (100.00%)
Technical Defenses - Malicious Office Attachment	Superior (100.00%)
NAC Bypass	Superior (100.00%)

Campaigns with Least Success

External Port Scans	Lower (0.00%)
C2 Channels - Domain Fronting	Lower (0.00%)
Domain Controller Assault	Lower (25.00%)
Internal Web App Profiling	Average (50.00%)
Internal Foothold (end-to-end)	Above Average (63.64%)

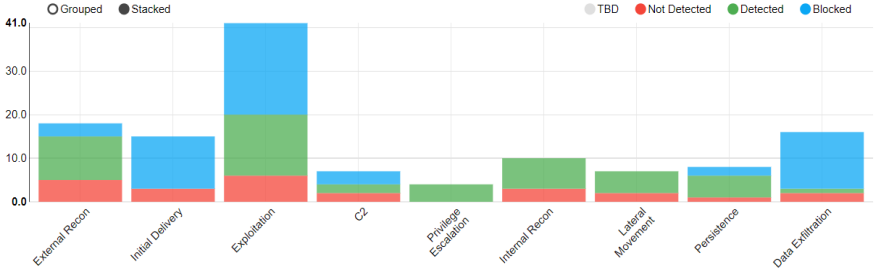
Statistics by Detection/Prevention Tool

Blocked and detected test cases for detection/prevention tools employed



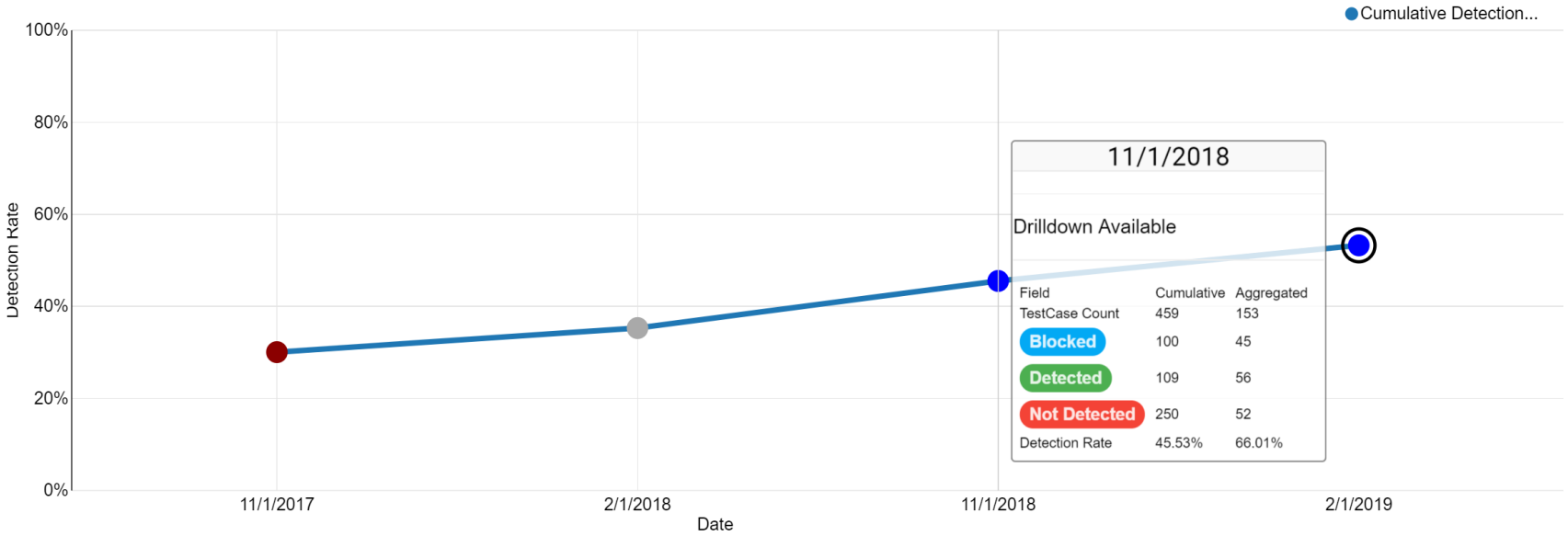
Statistics by Kill Chain Phase

Test case detection status distribution with respect to attack lifecycle phases



Report Type: Historical Trending
Assessments: ALL SELECTED
Campaigns: Malware Profile Simulation + 105 more
Outcomes: ALL SELECTED
Statuses: Completed + 3 more

Time Unit: Quarterly
Granularity: Data Only
Clicked Chart: Heat Map



1/1/2017 1/1/2019

Report Type: Heat Map
Assessments: Rogue One: A Star Wars Story
Campaig: ALL S
Outcomes: ALL SELECTED

Assessment HeatMap

Map Type: Latest
MITRE FILTERS
VE

No Test Coverage | Outcome TBD | Moderate

Initial Access	Execution	Persistence	Privileg Escalatio					Collection	Command and Control	Exfil
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Tol Manipulati					udio Capture	Commonly Used Port 3	Autom Exfiltra
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibili Features					utomated ollection	Communicatio n Through Removable Media	Data Compr
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DL					ipboard Data		Data Encryp
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLL					ata from formation epositories	Connection Proxy	Data T Size Li
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming					ata from ocal System	Custom Command and Control Protocol	Exfiltra Over Alterna Protoc
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass Use Account Control					ata from etwork hared Drive	Custom Cryptographic Protocol	Exfiltra Over Comm Contro Chann
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking					ata from emovable edia	Data Encoding	
	Execution through Module Load	BITS Jobs	Dylib Hijacking						Data Obfuscation	
	Exploitation for Client	Bootkit	Exploitation for Privilege	Compiled HTML File	Hooking	Network Share Discovery	Remote Desktop Protocol	Data Staged		Exfiltra
		Browser Extensions						Email		

Mitre Filters

Threat Groups

- [ ] APT1
- [ ] APT12
- [ ] APT16
- [ ] APT17
- [ ] APT18
- [ ] APT19
- [ ] APT28
- [ ] APT29
- [ ] APT3
- [ ] APT30
- [ ] APT32
- [ ] APT33
- [ ] APT34
- [ ] APT37

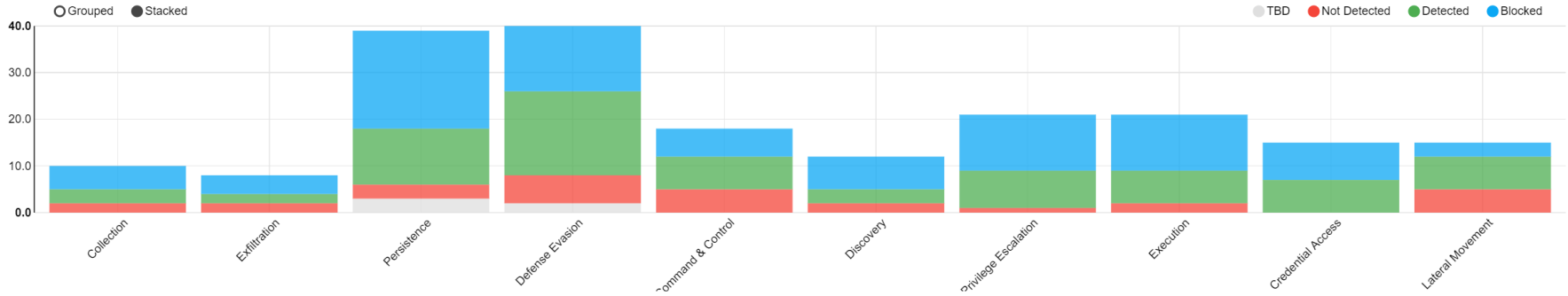
Malware

- [ ] 3PARA RAT
- [ ] 4H RAT
- [ ] ADVSTORESHELL
- [ ] ASPXSpy
- [ ] Agent Tesla
- [ ] Agent.btz
- [ ] Astaroth
- [ ] AuditCred
- [ ] AutoIt backdoor
- [ ] Azorult
- [ ] BACKSPACE
- [ ] BADCALL
- [ ] BADNEWS
- [ ] BBSRAT

Cancel | Done

Statistics by Kill Chain Phase

Test case detection status distribution with respect to attack lifecycle phases



Success Rates

CAMPAIGNS PHASES TECHNIQUES

Assessment	Campaign	Score
MITRE ATTACK Q2 2018	Credential Access	Superior (100.00%)
MITRE ATTACK Q2 2018	Privilege Escalation	Superior (95.24%)
MITRE ATTACK Q2 2018	Execution	Superior (90.48%)
MITRE ATTACK Q2 2018	Persistence	Superior (84.62%)
MITRE ATTACK Q2 2018	Discovery	Superior (83.33%)
MITRE ATTACK Q2 2018	Collection	Superior (80.00%)
MITRE ATTACK Q2 2018	Defense Evasion	Superior (80.00%)
MITRE ATTACK Q2 2018	Exfiltration	Above Average (75.00%)
MITRE ATTACK Q2 2018	Command & Control	Above Average (72.22%)

Report Type: Heat Map | Assessments: MITRE ATTACK Q2 2018 | Campaigns: ALL SELECTED | Outcomes: ALL SELECTED | Statuses: Completed + 3 more

Assessment HeatMap

No Coverage | TBD | Weakest | Minimal | Lower | Moderate | Strong

INACTIVE

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media (2)	AppleScript (2)	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript (2)	Audio Capture	Automated Exfiltration	Communication Through Removable Media
Valid Accounts (3)	Command-Line Interface	Accessibility Features	Accessibility Features	Bypass User Account Control	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Connection Proxy
	Dynamic Data Exchange	Account Manipulation	AppCert DLLs	Clear Command History	Brute Force	Network Service Scanning	Distributed Component Object Model	Clipboard Data	Data Encrypted	Custom Command and Control Protocol
	Execution through API	AppCert DLLs	AppInit DLLs (2)	Component Firmware	Credential Dumping	Network Sniffing	Logon Scripts (2)	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
	Execution through Module Load	AppInit DLLs (2)	Application Shimming (2)	Component Obje (2) Model Hijacking	Credentials in Files	Permission Groups Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
	Graphical User Interface	Application Shimming (2)	Bypass User Account Control	Deobfuscate/Decode Files or Information	Forced Authentication	Process Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Other Network Medium	Data Obfuscation
	InstallUtil (2)	Authentication Package	DLL Search Orde (3) Hijacking	Disabling Security Tools	Hooking (3)	Query Registry	Remote File Copy	Email Collection	Exfiltration Over Physical Medium	Domain Fronting
	Launchctl (3)	Bootkit	Exploitation for Privilege Escalation (4)	DLL Search Orde (3) Hijacking	Input Capture	Remote System Discovery	Remote Services	Input Capture	Scheduled Transfer	Fallback Channels
	Local Job Scheduling	Browser Extensions (2)	Extra Window Memory Injection (2)	DLL Side-Loading	Keychain	Security Software Discovery	Replication Through Removable Media (2)	Screen Capture		Multi-hop Proxy
	LSASS Driver (2)	Change Default File Association	File System Permissions Weakness	Extra Window Memory Injection (2)	LLMNR/NBT-NS Poisoning	System Network Configuration Discovery	Shared Webroot	Video Capture		Multi-Stage Channels
	Mshta (2)	Component Firmware			Network Sniffing	System Network Connections Discovery	SSH Hijacking			Multiband Communication
	PowerShell	Component Obje (2)			Private Keys		Taint Shared Content			Multilayer
	Regsvcs/Regasr (2)				Securityd Memory					

Don’t have a Red Team?

- “Breach and Attack Simulation” (BAS) Vendors
  - Control Validation
  - Red Team Automation
- Augments the *people* part of the “Red Team”
- May be more cost effective

Lots of tools and vendors

Free

- APTSimulator
- Atomic Red Team
- AutoTTP
- Blue Team Training Toolkit
- CALDERA
- InfectionMonkey
- DumpsterFire
- Invoke-Adversary
- NSA Unfetter
- Office 365 Attack Simulator
- Purple Team Automation
- Red Team Automation (RTA)
- Uber Metta

Commercial

- AttackIQ
- Cymulate
- SafeBreach
- SCYTHE
- Spirent CyberFlood
- Verodin
- vThreat
- XM-Cyber

@jorgeorchilles

SCYTHE

https://www.scythe.io/

INDUSTRY
ASSESSMENTS
Threat
Intelligence

THREAT
CATALOG
Real World

DEPLOYMENT
METHODS
Continuous

PRODUCTION
ENVIRONMENT
At Scale, Not a VM
Enterprise

SCYTHE
INFRASTRUCTURE
Reports for the
Business

@jorgeorchilles

THANK YOU FOR ATTENDING

Any Questions?