Moving From Threat Research To Threat Detection

Please sir, can I have some more detection?

SANS DFIR Summit

Agenda

- Who am I
- Stage 1- Research & Isolate
- Stage 2-Create The Attack
- Stage 3- Gathering Telemetry
- Stage 4- Attribute to Security Program

O’Shea Bowens

whoami

- Founder & CEO of Null Hat Security
- Technical Security Manager at DraftKings
- Founder of IDS Podcast
- Founder of SKICON
- Grew up in the SOC

Affiliations

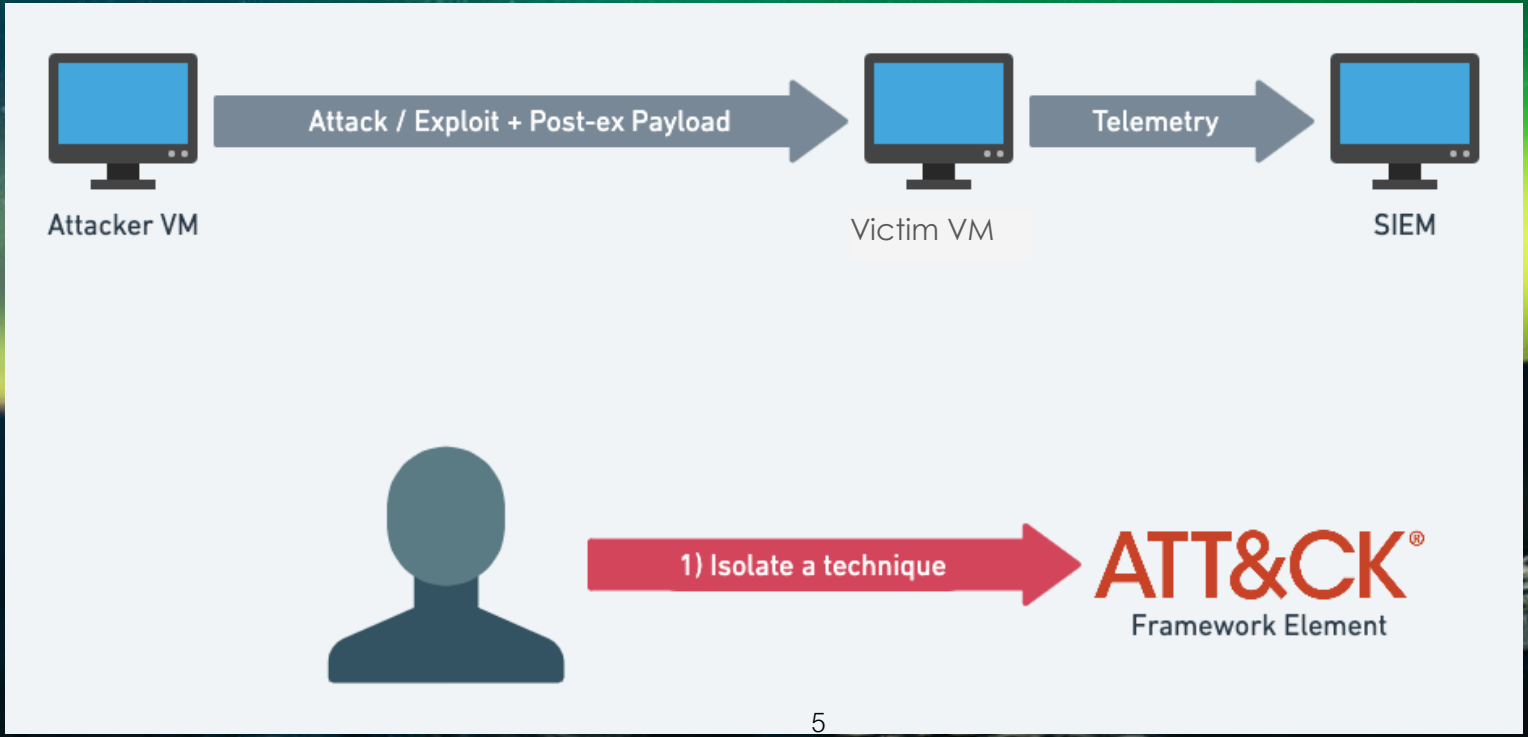
- Boston Security Meetup Organizer
- DC617
- ISSA NE- Board of Directors
- Blacks In Cyber- Board of Directors
- CSNP- Board of Directors

Twitter: @sirmudbl00d

WHO AM I ?

- DAD, lover of technology
- Captain in U.S. Army National Guard
- CND Manager on Cyber Protection Team and evangelist of raspberry pi
- I've been a tech hobbyist for about 12 years
- Part-time Pen tester and tinkerer
- Currently Sr Manager for a Sec Engineering Team with DOD
- Active volunteer at both B Sides Las Vegas and B Sides DC.
- I have taught intro to computing as an afterschool high school program within Chicago
- I worked as both a Defensive and Offensive analyst in the private sector and the military
- Three years leading Red Team engagements to support Blue Space Defenders
- I love to share when I can

Stage 1- Research



Stage 1- Research

- We need to know what we're concerned about before we can protect against it.
- This means reviewing your organization's tech stack and painting a picture of your vulnerabilities
- Dedicate time to research your attack vector and threat actors operating within it.

What's keeping your CISO up at night?

- Ransomware
- Phishing
- Web Application Attacks

Stage 1- Research

A little help from GRC

- If your organization is regulated, leverage your compliance documentation
- You've likely had to identify sensitive data, provide proof of security controls, create processes.
- Stay friendly with your compliance officer
- PCI DSS 10.x & 12.x

PCI requirements examples, because everyone loves PCI

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

Stage 1- Research

Threat Modeling

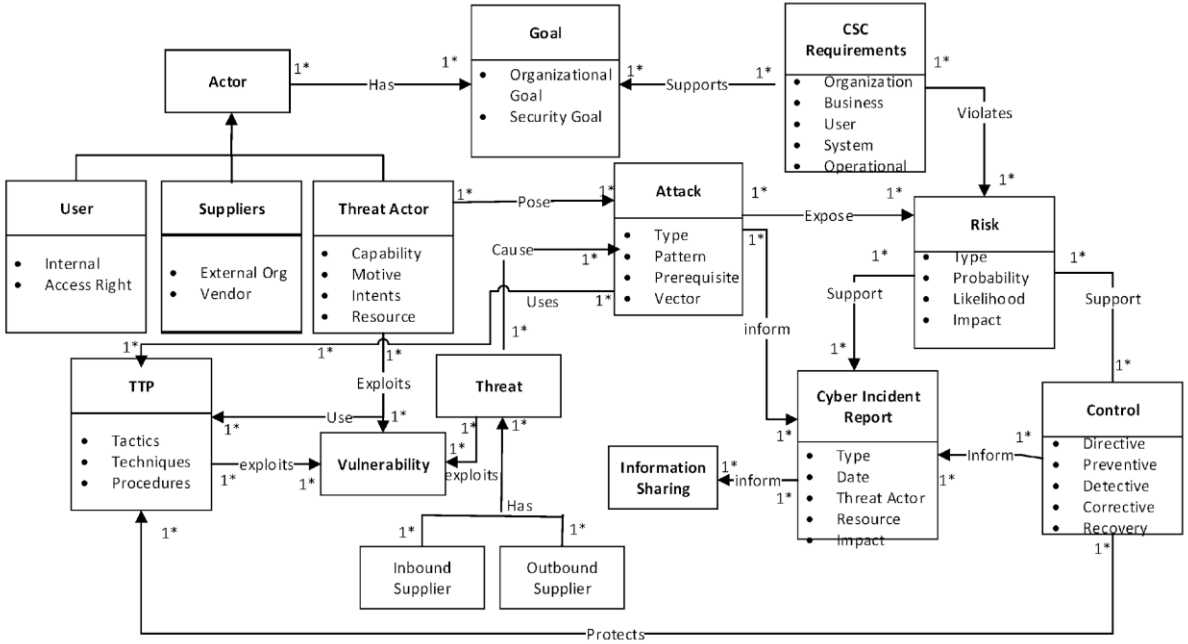
- The craftiness of threat actors and continuous development of advanced tactics, techniques and procedures (TTPs) has shifted the views of security practitioners.
- We must adapt and find vulnerabilities in similar methods as attackers.
- The end goal is the identification of threats and deploying countermeasures.

Threat Modeling Techniques

- System Centric or Risk Centric
- Microsoft's STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege) is system-centric, while
- PASTA (Process for Attack Simulation and Threat Analysis) is risk-centric.
- The challenge is both techniques are difficult to apply and don't reference addressing actual TTP's.

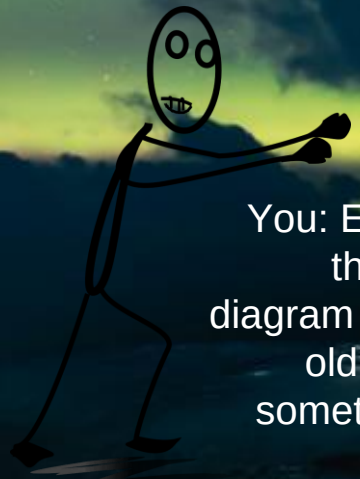
Threat Modeling

- Trust Boundaries
- Detection
- Logging



You: Hey, nice to meet you it's my first day. I'm the new security engineer. I was told to ping you, as I'd like an updated network diagram.

Them: Sure, here you go and welcome.

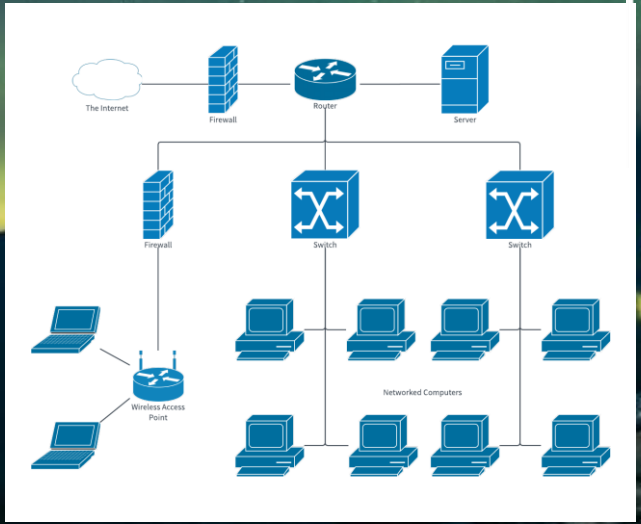


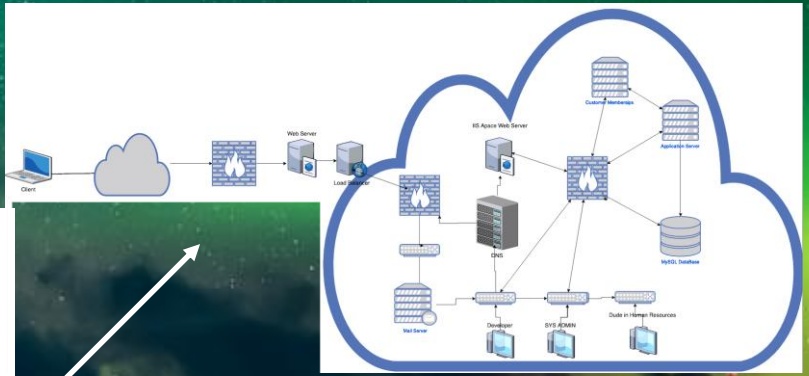
You: Excuse me but the date on this diagram is three years old. Do you have something from this year?

Them:!!!!!!!!!

Threat Modeling

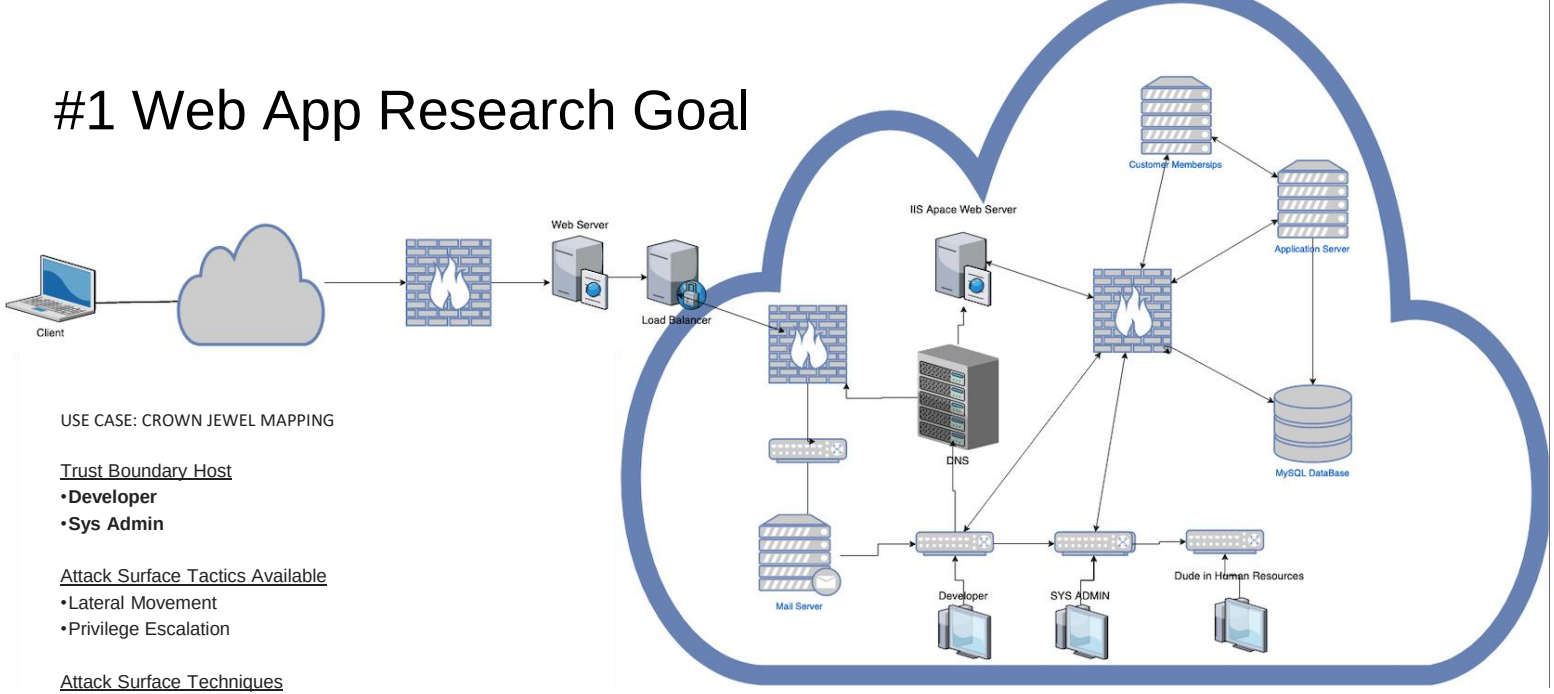
- Useful but lacks definition
- Helpful during an incident but not so much for our goals
- Lets go a bit deeper





- Somewhat better
- Positioned not only for layer3 reference but OS details. **It will come in handy later
- We're in security and need more relevant data
- Take note of the flow of data

#1 Web App Research Goal



USE CASE: CROWN JEWEL MAPPING

Trust Boundary Host
- **Developer**
- **Sys Admin**

Attack Surface Tactics Available
- Lateral Movement
- Privilege Escalation

Attack Surface Techniques
- Pash the Hash - T1075
  - mimikatz # kerberos::ptt #{user_name}@#{domain}

- SSH Hijacking- T1184
- Bypass User Account Control - T1088
  - New-Item "HKCU:\software\classes\ms-settings\shell\open\command" -Force

New-ItemProperty "HKCU:\software\classes\ms-settings\shell\open\command" -Name "DelegateExecute" -Value "" -Force

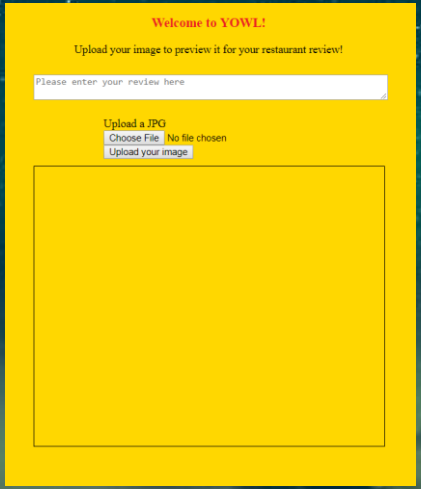
Set-ItemProperty "HKCU:\software\classes\ms-settings\shell\open\command" -Name "(default)" -Value "#{executable_binary}" -Force

Start-Process "C:\Windows\System32\fodhelper.exe"

Moving right of kill chain

Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques	Credential Access 13 techniques	Discovery 22 techniques	Lateral Movement 9 techniques	Collection 15 techniques	Command and Control 16 techniques	Exfiltration 8 techniques	Impact 13 techniques
Drive-by Compromise	Command and Scripting Interpreter (0/7)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/3)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/11)	Boot or Logon Autostart Execution (0/11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Phishing (0/3)	Scheduled Task/Job (0/5)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	File and Directory Discovery	Remote Services (0/6)	Data from Information Repositories (0/1)	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/1)	Network Service Scanning	Replication Through Removable Media	Data from Local System	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/2)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (0/3)	Network Share Discovery	Software Deployment Tools	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	File and Directory Permissions Modification (0/2)	Network Sniffing	Network Sniffing	Taint Shared Content	Data from Removable Media	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts (0/3)	User Execution (0/2)	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Group Policy Modification	OS Credential Dumping (0/8)	Password Policy Discovery	Use Alternate Authentication Material (0/2)	Data Staged (0/2)	Multi-Stage Channels		Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection (0/11)	Hide Artifacts (0/6)	Steal or Forge Kerberos Tickets (0/3)	Peripheral Device Discovery		Email Collection (0/3)	Non-Application Layer Protocol		Network Denial of Service (0/2)
		Hijack Execution Flow (0/11)	Scheduled Task/Job (0/5)	Hijack Execution Flow (0/11)	Steal Web Session Cookie	Permission Groups Discovery (0/2)		Input Capture (0/4)	Non-Standard Port		Resource Hijacking
		Office Application Startup (0/6)	Valid Accounts (0/3)	Impair Defenses (0/5)	Two-Factor Authentication Interception	Process Discovery		Man in the Browser	Protocol Tunneling		Service Stop
		Pre-OS Boot (0/3)		Indicator Removal on Host (0/6)	Unsecured	Query Registry		Man-in-the-Middle (0/1)	Proxy (0/4)		System Shutdown/Reboot
				Indirect Command Execution		Remote System Discovery		Screen Capture	Remote Access Software		
				Masquerading (0/6)		Software Discovery (0/1)		Video Capture			
						System Information					

The app!



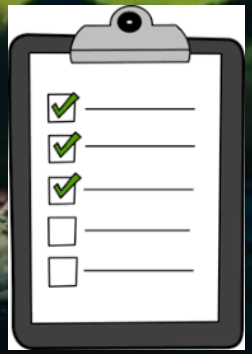
Yowl!

A restaurant review site that really shouldn't be in prod yet.

Allows you to register a user, add reviews, and search existing reviews.

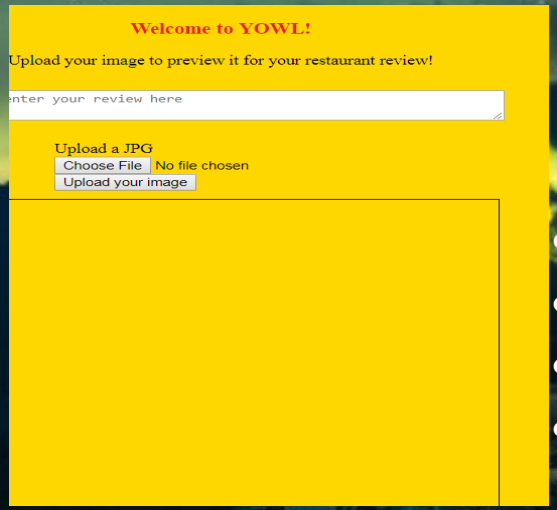
Based on our threat model ...

- What do we actually care about?
- What would need to be fixed to actually solve the problem?
- How would we fix it?



Does This Happen?

- Sort of.
- Actual vulnerabilities, not simulated.
- Doesn’t use modern frameworks or client side processing.



- Super small app
- Super vulnerable
- It intends to be an image upload
- Does it stop you from uploading something else?

What’s wrong with it?

?

And how do we find that out?

- Static Analysis
- Dynamic Analysis
- Code Review
- Manual testing

First, static findings

HIGH

	Static Scan
SQL Injection	2
Total	**2**

MEDIUM

	Static Scan
Credentials Management	1
Cross-Site Scripting	7
Cryptographic Issues	4
Directory Traversal	1
Total	**13**

LOW

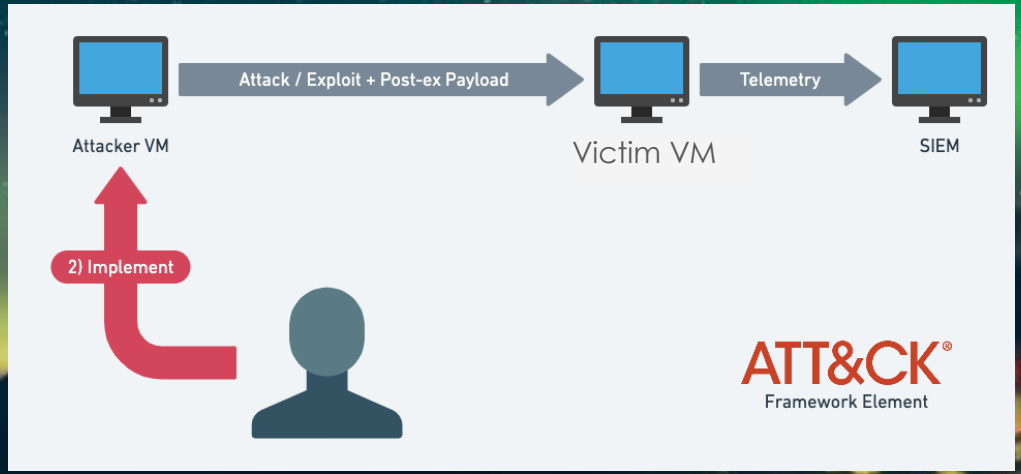
	Static Scan
Information Leakage	1
Total	**1**

Next, dynamic

- PHP code injection [2]
- Cross-site scripting (stored) [3]
- Cleartext submission of password [3]
- SQL injection
- Interesting input handling: Magic value: COM1 [2]
- Interesting input handling: MySQL injection [2]
- Password field with autocomplete enabled [3]
- Unencrypted communications
- XML injection
- Cross-site request forgery [2]
- Interesting input handling: String - doublequoted
- Cookie without HttpOnly flag set [2]
- Form action hijacking (reflected) [3]
- Input returned in response (stored) [2]
- Input returned in response (reflected) [300]
- File upload functionality
- HTTP TRACE method is enabled
- Content type is not specified
- Path-relative style sheet import [2]
- Frameable response (potential Clickjacking) [5]
- Link manipulation (reflected)

Not everything found by static is easily exploitable, and sometimes what's wrong with your app isn't visible in the code

Stage 2 - Creating The Attack



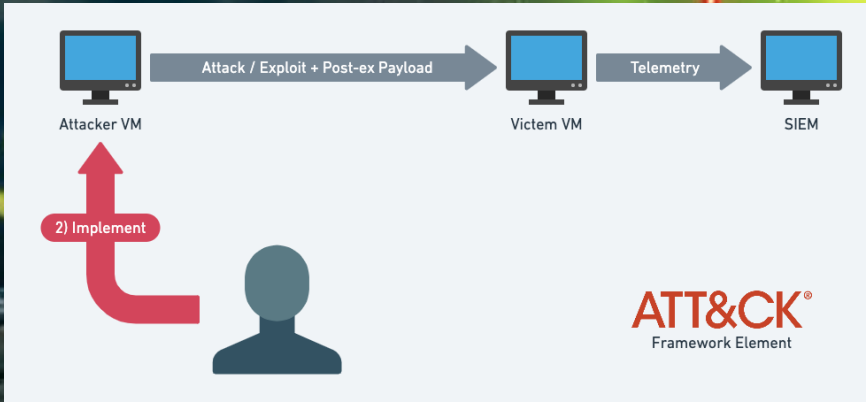
#OPSEC

- Stage 1-Local File Inclusion vulnerability running on Apache client for an organization. Upload payload
- Stage 2- Navigate to payload directory to leverage system calls for further exploitation. In our case, uploading backdoor. YAY
- Stage 3- Upload backdoor. Circumvent defensive tools
- Stage 4- Exfil of data

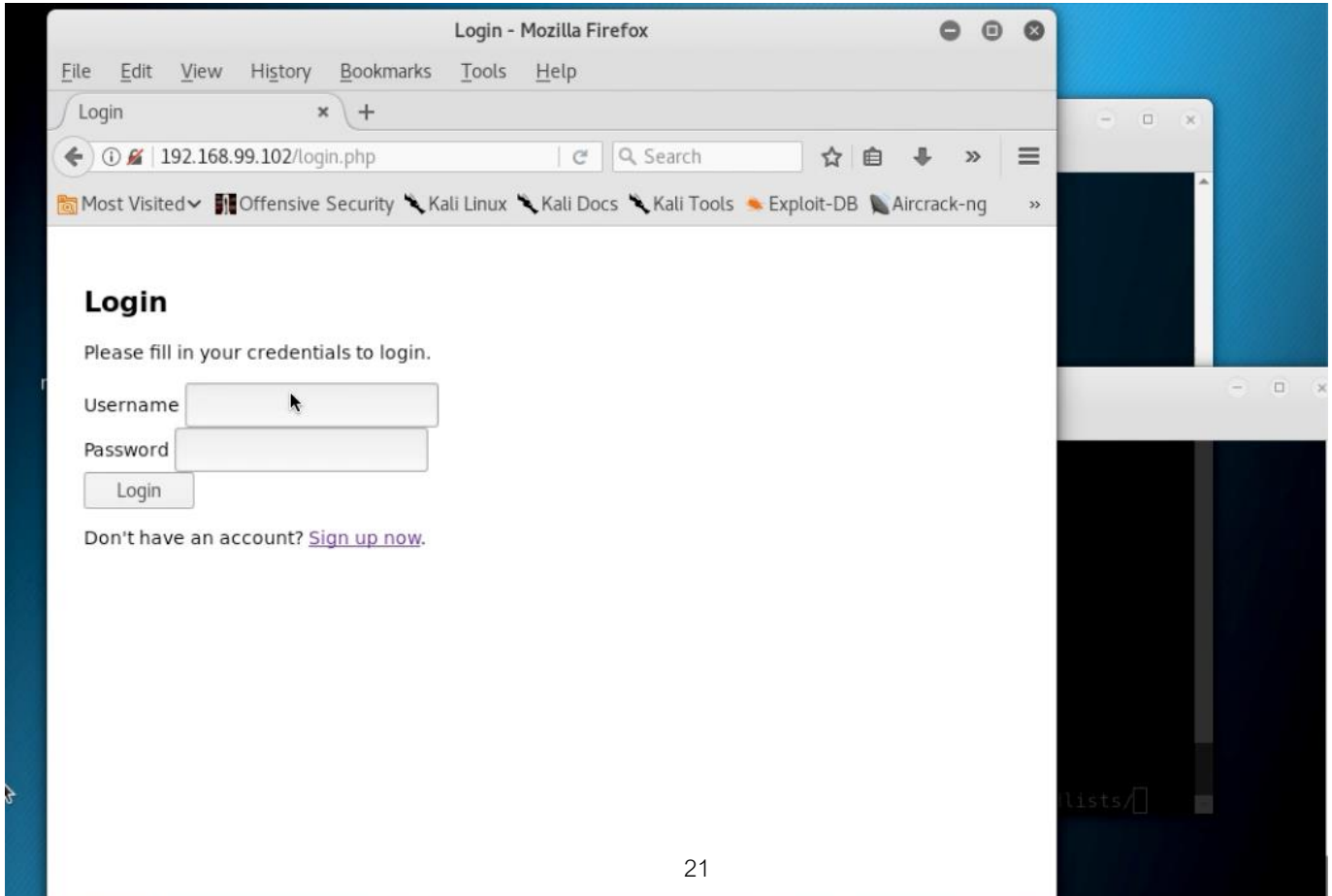
#OPSEC- Identify

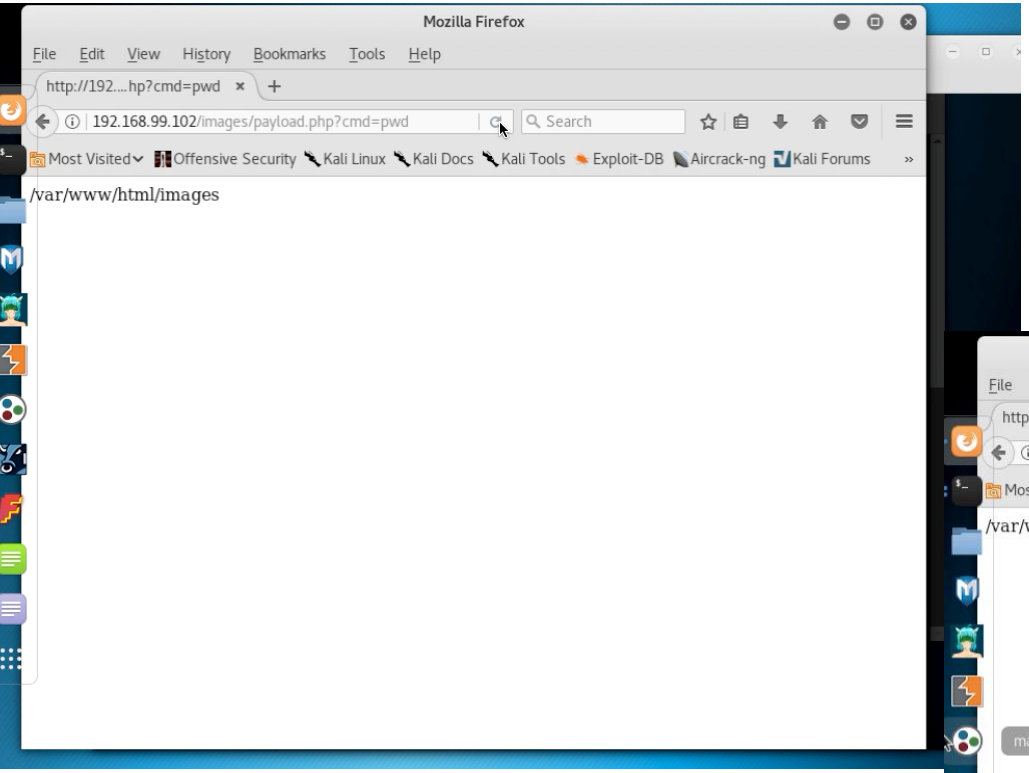
- What do we have here?
- Vulnerable PHP
- Does it stop you from uploading something else?

```php
$data = file_get_contents($_FILES["Upload"]["tmp_name"]);
if (file_put_contents($target_file, $data))
    {
        echo "<div class='centered'><img id='tada' src='/".
        $target_file ."'></div>";
    } else {
        echo "Sorry, there was an error uploading your file.";
    }
}
```

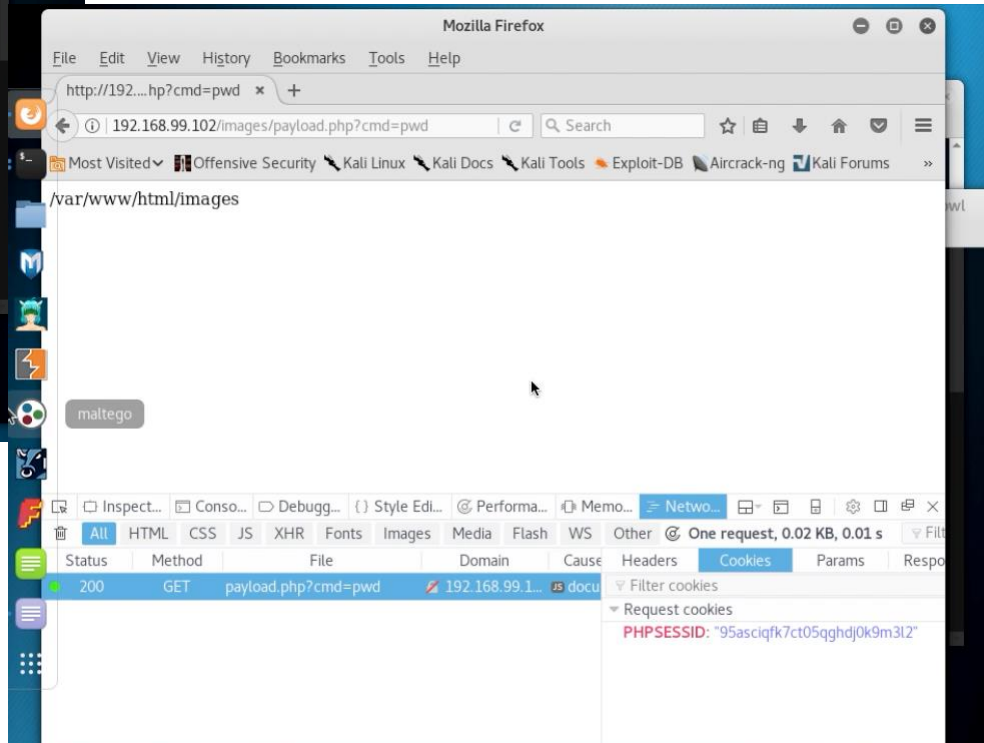


Can We Get In


Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Login
192.168.99.102/login.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Login
Please fill in your credentials to login.
Username
Password
Login
Don't have an account? Sign up now.

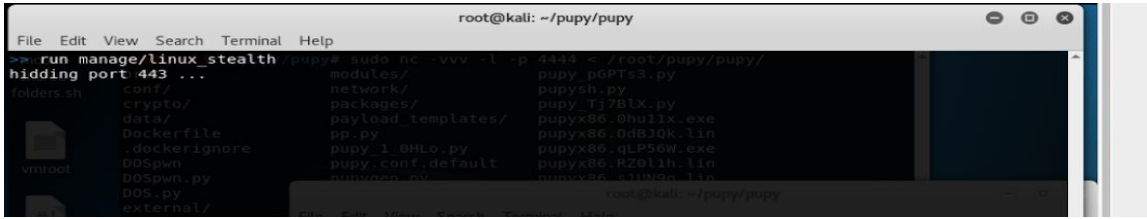


- Web server accepted the payload
- Time to grab hashes and dump'em
- Move to exfil, then leave
- Simple.



#OPSEC-Persistence

- Oh they're tricky and reboots don't always work
- So what can attackers rely upon to maintain access and not raise suspicious
- Check cron jobs

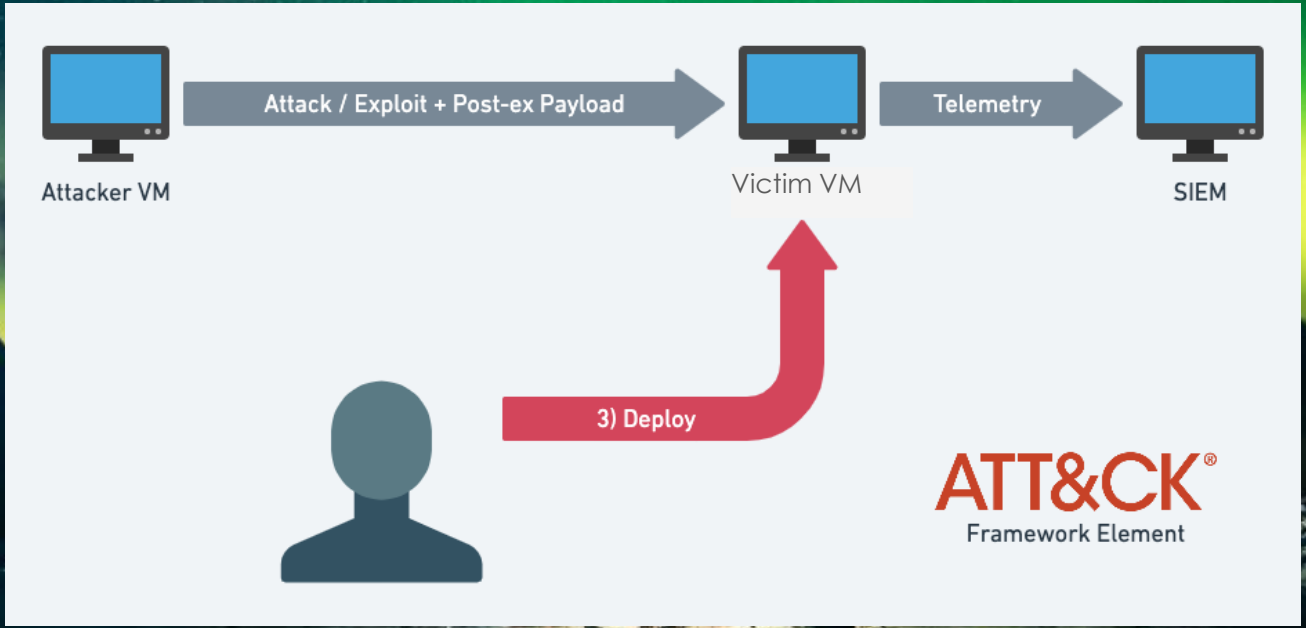


Internal Pupy call to hide process and ports

#OPSEC-Migration

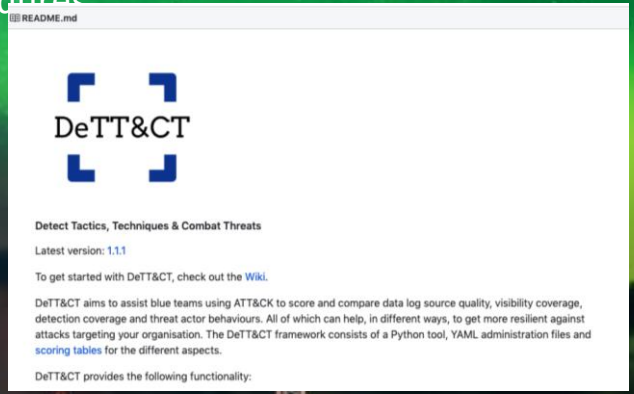
- Attacker methods to blend in
  - Odd cron jobs
  - Process hi-jacking
  - DLL Sideloading
  - Out of place powershell scripts
- Hint: Don't trust the timestamps

Stage 3 - Create & Deploy Detection



Hunt w/DeTT&CT

- How do we map our hypothesis to our to controls and procedures
- If you can't prove it, it doesn't exist
  - Except aliens. They are real
- Circling back to why we started
- At this stage you'll need a few things
  - Logs sources
  - Machine hostnames & ip address
  - EDR, IDS, SIEM information



README.md

DeTT&CT

Detect Tactics, Techniques & Combat Threats

Latest version: 1.1.1

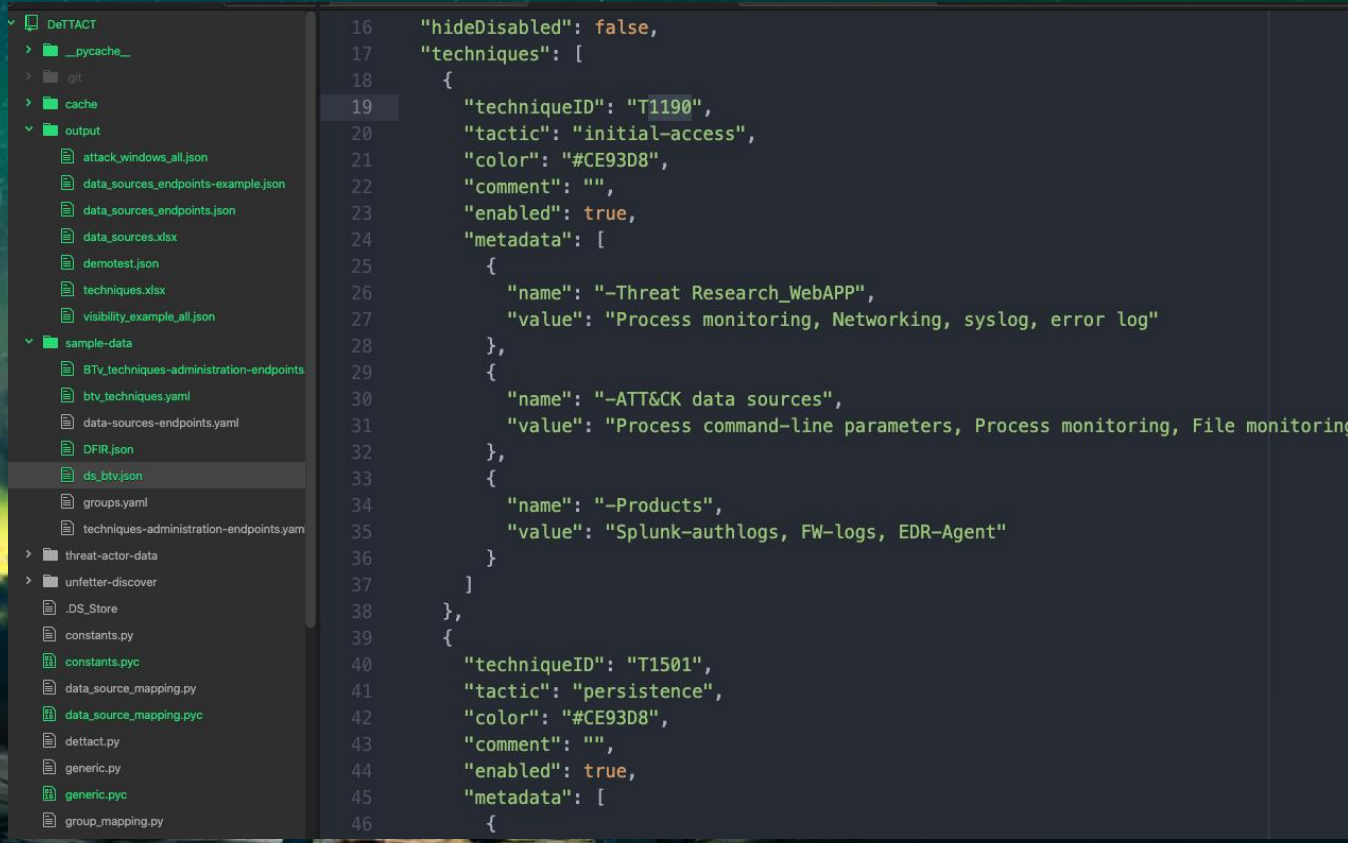
To get started with DeTT&CT, check out the Wiki.

DeTT&CT aims to assist blue teams using ATT&CK to score and compare data log source quality, visibility coverage, detection coverage and threat actor behaviours. All of which can help, in different ways, to get more resilient against attacks targeting your organisation. The DeTT&CT framework consists of a Python tool, YAML administration files and scoring tables for the different aspects.

DeTT&CT provides the following functionality:

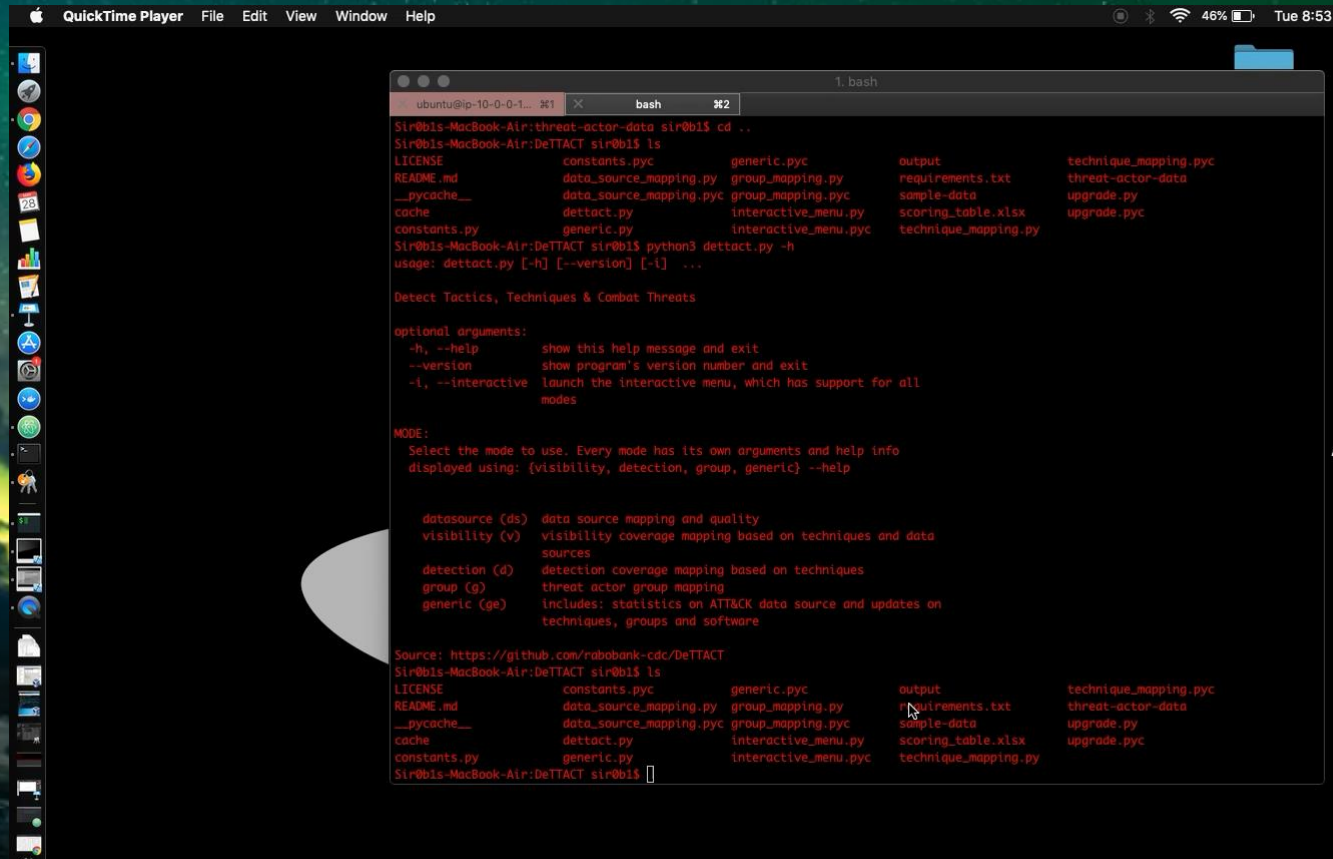
Define Data Sources w/ DeTTACT

- Start slow and build
- Only name relevant data
- Maintain consistency across the org
- Verify with IT



Hunt w/DeTT&CT

- Our Hypothesis
- Initial Access: Exploit Public-Facing Application
- Exfiltration: Data Compressed. Exfiltration C2 Channel



Mapping Data Sources

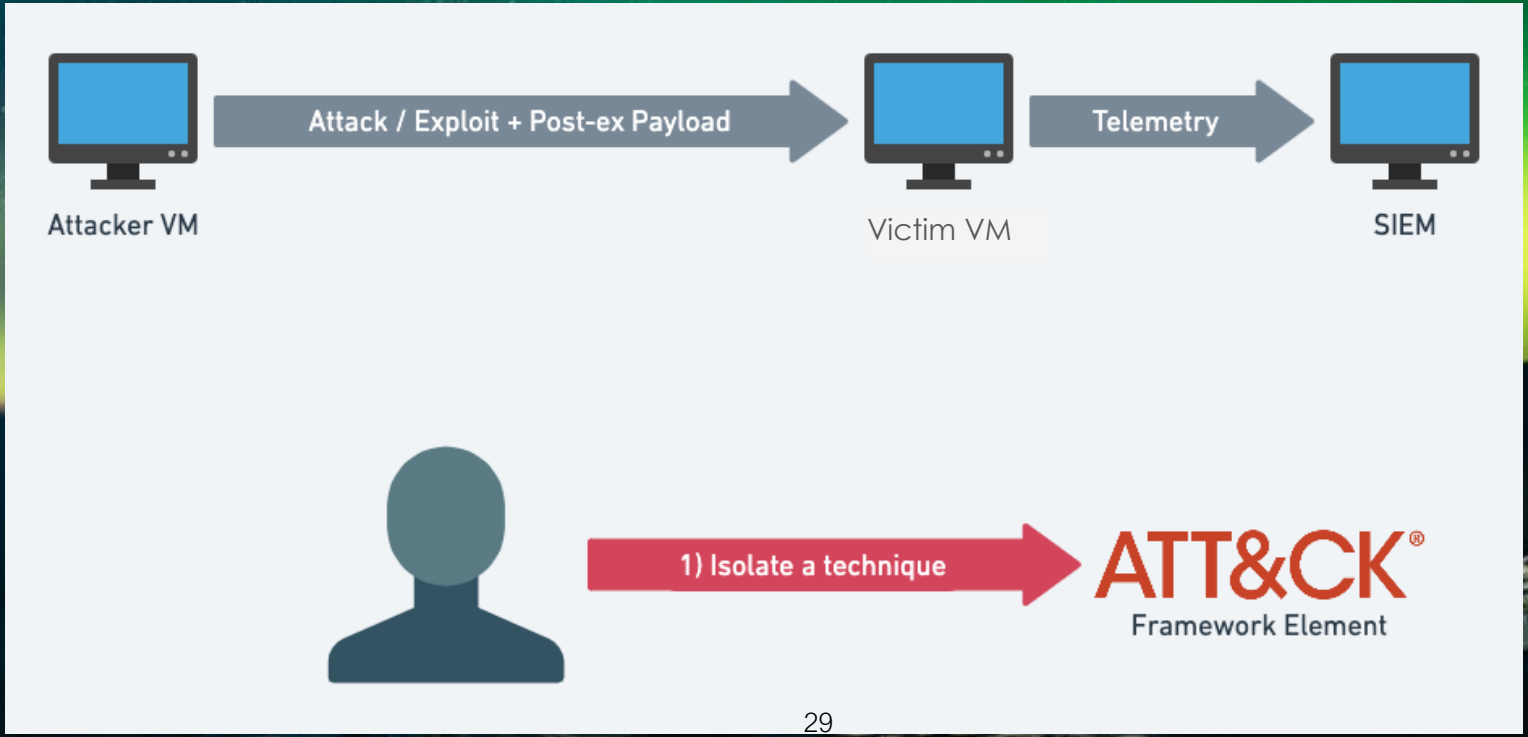
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
9 items	10 items	14 items	7 items	24 items	9 items	13 items	6 items	10 items	22 items	9 items	13 items
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Exploitation for Client Execution	Bootkit	Process Injection	Clear Command History	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
Hardware Additions	Graphical User Interface	Browser Extensions	Setuid and Setgid	Compile After Delivery	Credential Dumping	File and Directory Discovery	Remote File Copy	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Spearphishing Attachment	Local Job Scheduling	Create Account	Sudo	Disabling Security Tools	Credentials in Files	Network Service Scanning	Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Spearphishing Link	Scripting	Hidden Files and Directories	Sudo Caching	Execution Guardrails	Exploitation for Credential Access	Network Sniffing	SSH Hijacking	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing via Service	Source	Kernel Modules and Extensions	Valid Accounts	Exploitation for Defense Evasion	Input Capture	Password Policy Discovery	Third-party Software	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Supply Chain Compromise	Space after Filename	Local Job Scheduling	Web Shell	File Deletion	Network Sniffing	Permission Groups Discovery		Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
				File Permissions Modification	Private Keys						Inhibit System Recovery
					Two-Factor Authentication Interception						

T1022
Metadata:
-Available data sources: Process monitoring, syslog, error log, auditd
-ATT&CK data sources: File monitoring, Process monitoring, Process command-line parameters, Binary file metadata
-Products: Splunk, OSSEC

Initial Access	Exfiltration
1 items	2 items
Exploit Public-Facing Application	Data Compressed
	Data Encrypted

MITRE ATT&CK™ Navigator v2.2.1

Stage 1- Research



Sub-Techniques Are Here

Initial Access — 9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (3)
  - Compromise Software Dependencies and Development Tools
  - Compromise Software Supply Chain
  - Compromise Hardware Supply Chain
- Trusted Relationship
- Valid Accounts (4)
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts

Execution — 10 techniques

- Command and Scripting Interpreter (7)
  - PowerShell
  - AppleScript
  - Windows Command Shell
  - Unix Shell
  - Visual Basic
  - Python
  - JavaScript/JScript
- Exploitation for Client Execution
- Inter-Process Communication (2)
  - Component Object Model
  - Dynamic Data Exchange
- Native API
- Scheduled Task/Job (5)
  - At (Windows)
  - Scheduled Task
  - At (Linux)
  - Launchd
  - Cron
- Shared Modules
- Software Deployment Tools
- System Services (2)
  - Launchctl
  - Service Execution
- User Execution (2)
  - Malicious Link
  - Malicious File
- Windows Management Instrumentation

Persistence — 18 techniques

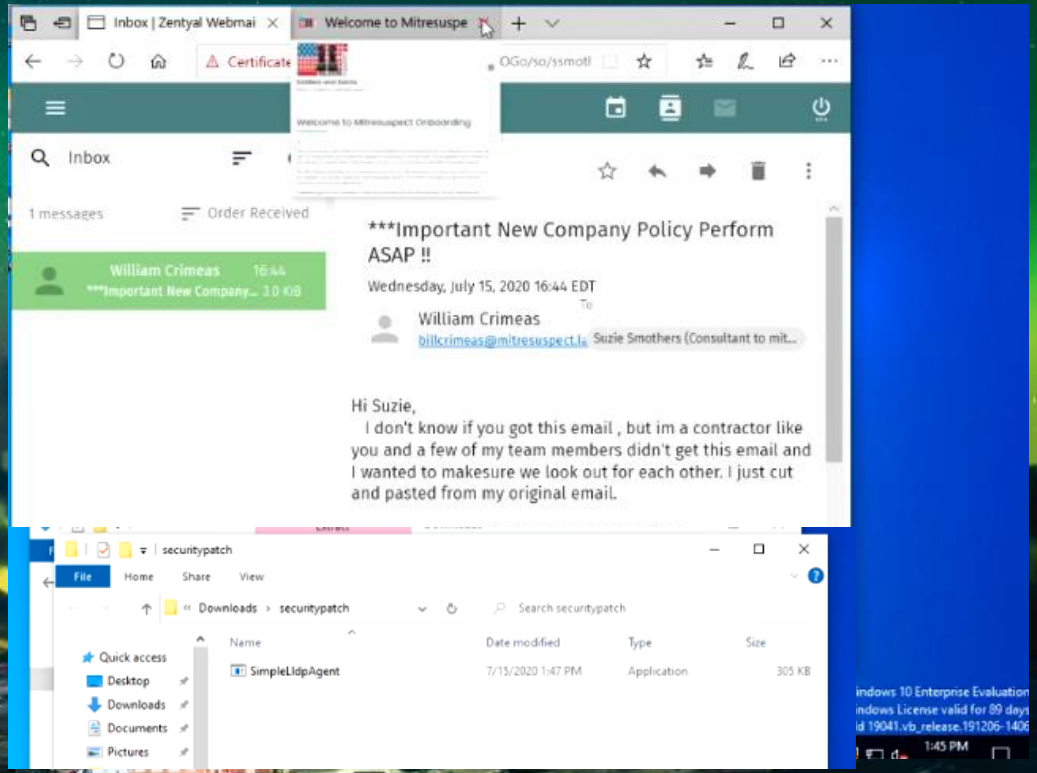
- Account Manipulation (4)
  - Additional Azure Service Principal Credentials
  - Exchange Email Delegate Permissions
  - Add Office 365 Global Administrator Role
  - SSH Authorized Keys
- BITS Jobs
- Boot or Logon Autostart Execution (11)
  - Registry Run Keys / Startup Folder
  - Authentication Package
  - Time Providers
  - Winlogon Helper DLL
  - Security Support Provider
  - Kernel Modules and Extensions
  - Re-opened Applications
  - LSASS Driver
  - Shortcut Modification
  - Port Monitors
  - Plist Modification
- Boot or Logon Initialization Scripts (5)
  - Logon Script (Windows)
  - Logon Script (Mac)
  - Network Logon Script
  - Rc.common
  - Startup Items
- Browser Extensions
- Compromise Client Software Binary

Privilege Escalation — 12 techniques

- Abuse Elevation Control Mechanism (4)
  - Setuid and Setgid
  - Bypass User Access Control
  - Sudo and Sudo Caching
  - Elevated Execution with Prompt
- Access Token Manipulation (5)
  - Token Impersonation/Theft
  - Create Process with Token
  - Make and Impersonate Token
  - Parent PID Spoofing
  - SID-History Injection
- Boot or Logon Autostart Execution (11)
  - Registry Run Keys / Startup Folder
  - Authentication Package
  - Time Providers
  - Winlogon Helper DLL
  - Security Support Provider
  - Kernel Modules and Extensions
  - Re-opened Applications
  - LSASS Driver
  - Shortcut Modification
  - Port Monitors
  - Plist Modification
- Boot or Logon Initialization Scripts (5)
  - Logon Script (Windows)
  - Logon Script (Mac)
  - Network Logon Script
  - Rc.common
  - Startup Items

#Phishing Execution

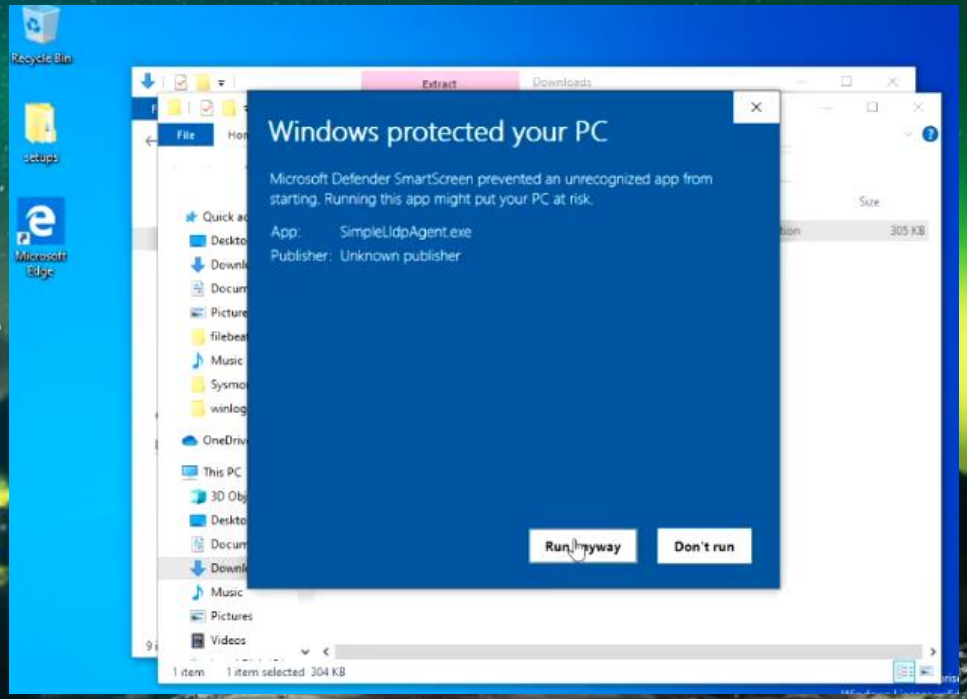
- Contractor Suzie Smothers receives the email and acts on the phishing campaign
- User bypasses security measures and installs the malicious software



#Phishing Execution

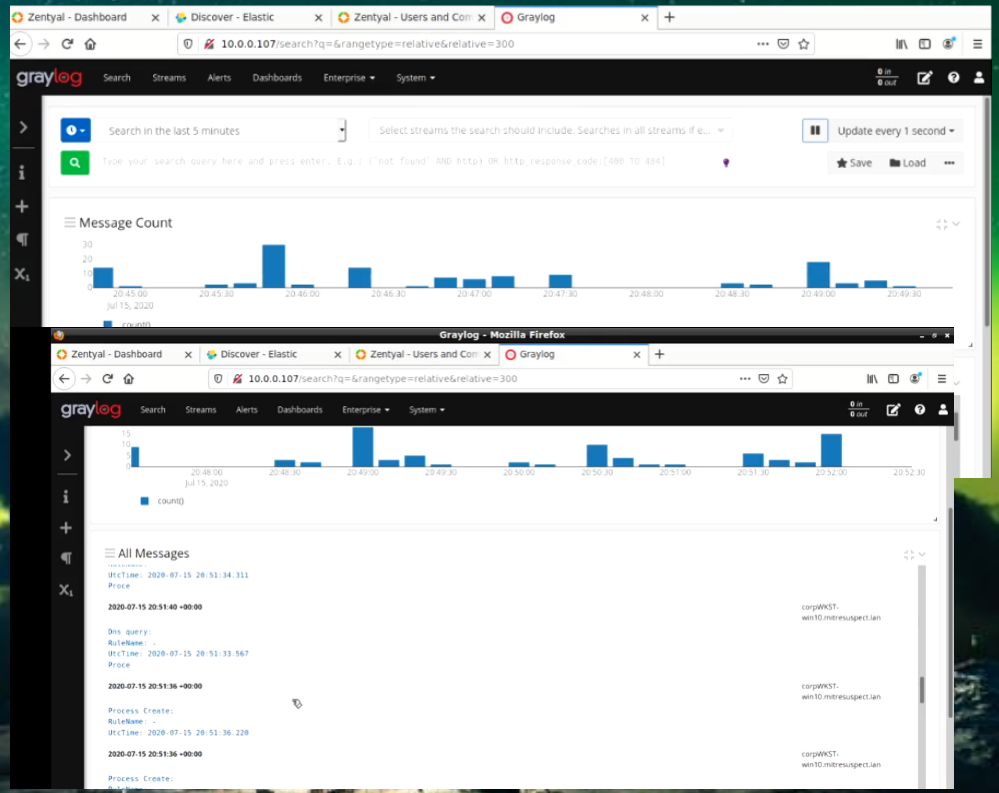
User bypasses security measures

and installs the malicious software

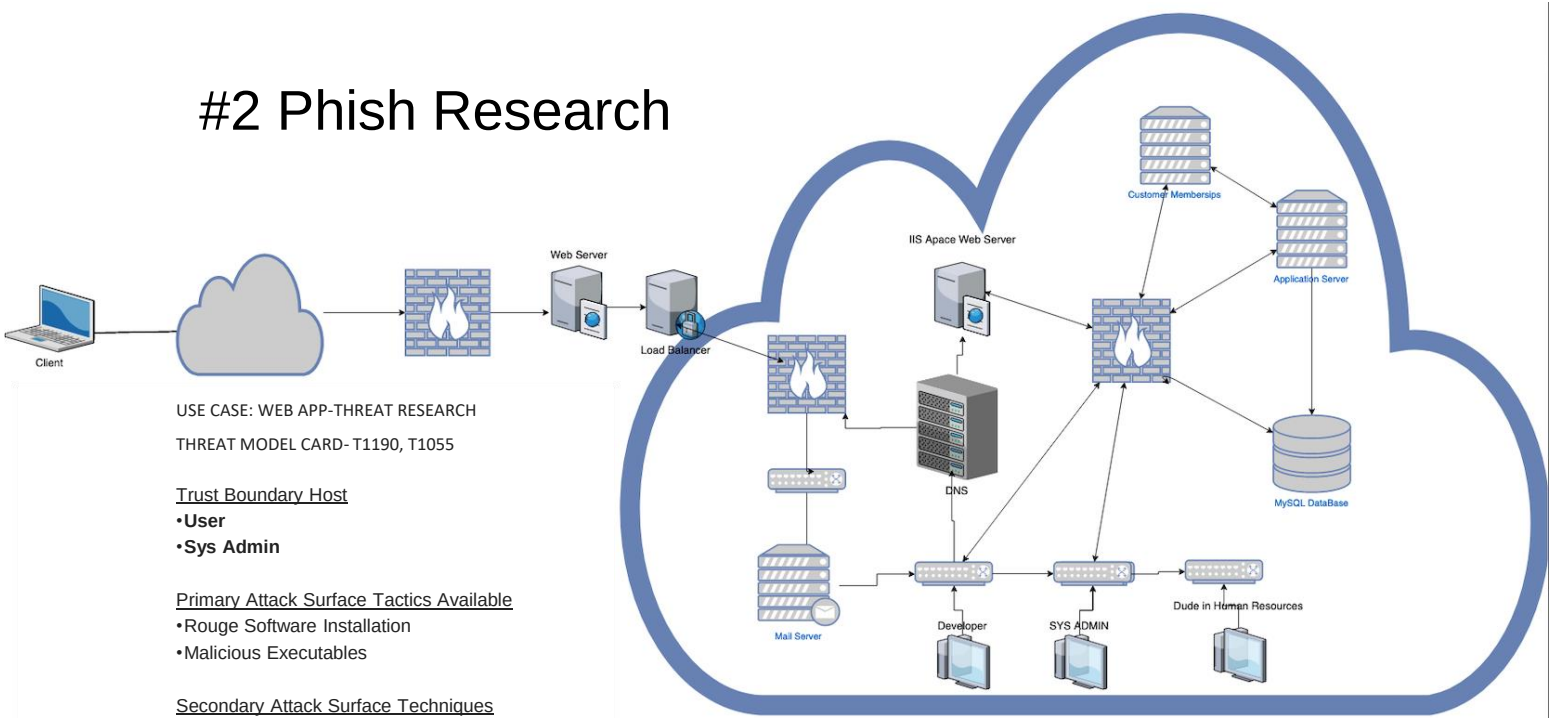


#Phishing Execution

Logs transition from normal to elevated reports on the machine corpWKST-win10 in response of repeated calls (every 30Sec beacon)



#2 Phish Research



USE CASE: WEB APP-THREAT RESEARCH

THREAT MODEL CARD- T1190, T1055

Trust Boundary Host
- **User**
- **Sys Admin**

Primary Attack Surface Tactics Available
- Rouge Software Installation
- Malicious Executables

Secondary Attack Surface Techniques
- WMI
  - Bypass User Account Control

- New-Item
- Start-Process “C\Windows\System32\simpleLldp.Agent.exe

Stage 4-
Attribute to Security Program

Attribute to Security Program

- After you've completed this cycle and created your threat cards, you'll need to consider how to leverage them
- Your use case is primarily driven by detection
  - How can we prove this?
  - Where does it count?
- After you've proven your use case, begin to think about metrics

ID	Use Case Category	Detection Name	Active Directory Auth	Proxy	CheckPoint MDS/ MLM	Internal NetFlow	SEP	DNS	Falcon Host	Suricata	D
UC001	Privileged User Monitoring	Unauthorized Privileged Account usage	x								
UC002	Malware	Ransomeware detected					x		x		
UC003	Authentication	Network traffic to known malicious destination	x								
UC047	Network Enumeration/ Reconnaissance	Internal system scanning (horizontal)				x					
UC048	Network Enumeration/ Reconnaissance	Internal system portscan				x					
UC005	Privileged User Monitoring	Use of a privileged account to log in locally to a workstation									
UC006	Privileged User Monitoring	Logging in as root in Linux/Unix environemnt									
UC007	Privileged User Monitoring	Domain Account created from unauthorized user ID	x								
UC009	Privileged User Monitoring	Local Server Account created from an unauthorized user ID									
UC010	Authentication	Successful login to honeyword account	x								
UC011	Authentication	Attempted login for dormant or inactive accounts	x								
UC012	Privileged User Monitoring	Network login to local account									
UC013	Privileged User Monitoring	Adding a network account to a privileged group from an unauthorized ID	x								
UC014	Privileged User Monitoring	Adding a local account to a privileged group on critical system	x								
UC015	Remote Authentication	Excessive Remote Failed Logon Attempts with same ID									
UC016	Remote Authentication	Excessive Remote Failed Logon Attempts from same Source IP							x	x	x
UC019	Authentication	Monitoring of default account login attempts	x								
UC020	Authentication	Attempted login for administratively disabled accounts	x								
UC021	Malware	Malware detected on critical system									
UC022	Malware	Antivirus software service stopped/disabled									
UC023	Malware	Malware detected on end-user workstation									
UC024	Malware	Servers and workstations with outdated virus definition									
UC025	Malware	Infected files not quarantined					x				
UC026	Malware	Top 50 Malware Infections		x			x				
UC027	Malware	Top 50 Infected hosts		x			x				
UC028	Traffic to Malicious Destination	Network traffic from critical systems to known malicious IP		x	x						
UC029	Traffic to Malicious Destination	Excessive firewall denies on perimeter firewalls by same Source IP			x						
UC030	Traffic to Malicious Destination	Excessive firewall denies on perimeter firewalls to same Dest IP			x						
UC031	Traffic to Malicious Destination	Excessive dropped requests by proxy		x							
UC032	Traffic to Malicious Destination	Top 50 Hosts for dropped traffic on perimeter firewalls			x						
UC033	Traffic to Malicious Destination	Top 50 Hosts for dropped proxy traffic		x							

Use Case Categories	UID Categories		Log sources	UID Log sources		Action	UID Action
Privileged User Monitoring	CA000001		Active Directory	LS000001		Alert	AC000001
Malware	CA000002		Proxy	LS000002		Report	AC000002
Traffic to Malicious Destination	CA000003		Internal NetFlow	LS000003		DashBoard	AC000003
Systems Monitoring	CA000004		EDR	LS000004			
Loss of Sensitive Data	CA000005		CheckPoint MDS/MLM	LS000005			
Network Enumeration/Reconnaissance	CA000006		DNS	LS000006			
Web Based Attacks	CA000007		DHCP	LS000007			
Remote Authentication	CA000008		DLP	LS000008			
Infrastructure Monitoring	CA000009		Web Server	LS000009			
Denial of Service	CA000010		WAF	LS000010			
Compliance	CA000011		Cisco ASA	LS000011			
Authentication	CA000012			LS000012			
Post-exploitation lateral movement	CA000013						
Mail	CA000014						
Database	CA000015						
Specific Application	CA000016						
Process Injection	CA000017						

Questions?

O’Shea Bowens-
email:ob@nullhatsecurity.org
Twitter:@sirmudbl00d

Nicolai Smith-
email:nicosmith312@gmail.com