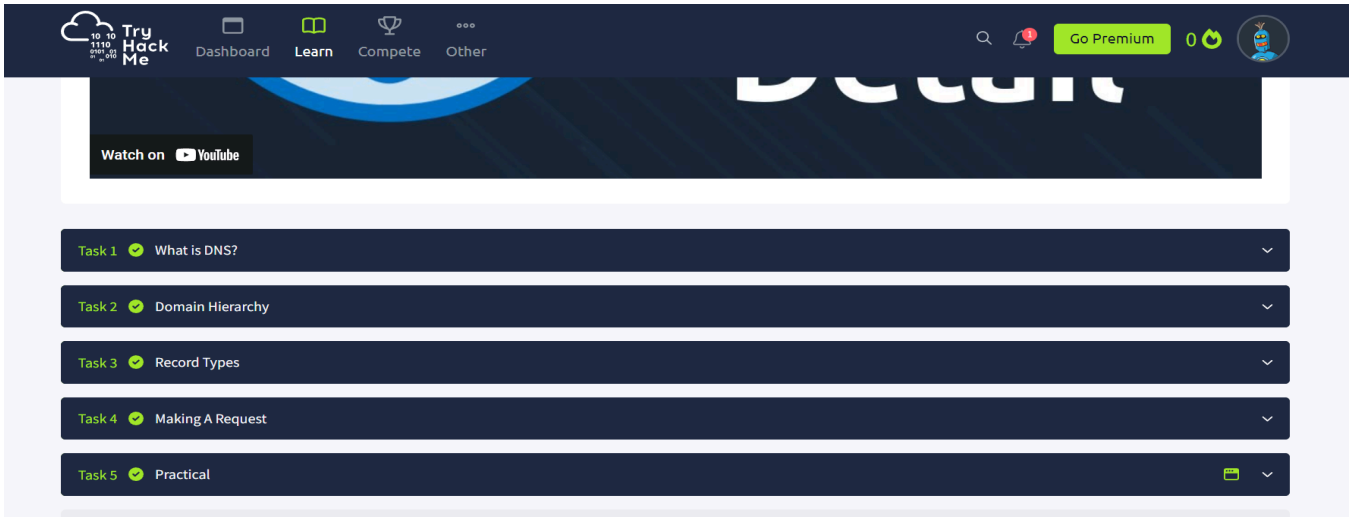
ACTIVE INFO GATHERING

DNS enumeration:

TryHackMe exercises:



1. What is the ip address of adlp-corp.com ?

Your response Your command:

```
└─$ nmap adlp-corp.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-10 05:41 EDT
Nmap scan report for adlp-corp.com (52.51.133.160)
```

```
└─$ host -t a adlp-corp.com
adlp-corp.com has address 52.51.133.160
```

Dig adlp-corp.com a : will also give the ip address

2. What is the TXT record of adlp-corp.com?

Your response Your command

```
└─$ host -t txt adlp-corp.com
adlp-corp.com descriptive text "BC{DESCRIPTIVE-DOMAIN-TXT}"
```

3. What are the MX records of becode.org ?

Your response Your command

```
└─$ host -t mx becode.org
becode.org mail is handled by 1 aspmx.l.google.com.
becode.org mail is handled by 5 alt2.aspmx.l.google.com.
becode.org mail is handled by 10 alt4.aspmx.l.google.com.
becode.org mail is handled by 5 alt1.aspmx.l.google.com.
becode.org mail is handled by 10 alt3.aspmx.l.google.com.
```

4. What are the MX records of adlp-corp.com ?

Your response Your command

```
└─$ host -t mx adlp-corp.com
adlp-corp.com mail is handled by 10 alt4.aspmx.l.google.com.
adlp-corp.com mail is handled by 1 aspmx.l.google.com.
adlp-corp.com mail is handled by 10 alt3.aspmx.l.google.com.
adlp-corp.com mail is handled by 5 alt2.aspmx.l.google.com.
adlp-corp.com mail is handled by 5 alt1.aspmx.l.google.com.
```

5. What is the first NS name server of adlp-corp.com?
Your response Your command

```
└─$ host -t ns adlp-corp.com
adlp-corp.com name server ns-1997.awsdns-57.co.uk.
```

6. Uses a brute force tool to find subdomains of adlp-corp.com. How many did you find?
Your response Your command

```
┌──(kali㉿kali)-[~]
└─$ dnsenum adlp-corp.com
dnsenum VERSION:1.3.1
```

```
Brute forcing with /usr/share/dnsenum/dns.txt:
_______________________________________________

admin.adlp-corp.com.                    300      IN    A        52.51.133.160
ftp.adlp-corp.com.                      300      IN    A        52.51.133.160
mail.adlp-corp.com.                     300      IN    A        52.51.133.160
mail2.adlp-corp.com.                    300      IN    A        52.51.133.160
smtp.adlp-corp.com.                     300      IN    A        52.51.133.160
```

```
┌──(kali㉿kali)-[~]
└─$ dnsmap adlp-corp.com
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for adlp-corp.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

admin.adlp-corp.com
IP address #1: 52.51.133.160

ftp.adlp-corp.com
IP address #1: 52.51.133.160
```

7. Use theHarvester tool at becode.org. How many Linkedin Users?
Your response Your command

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d becode.org -l 50 -b all
```

```
[*] LinkedIn Links found: 0
___________________________
```

Alternatively:

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d becode.org -b Linkedin

Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[!] Invalid source.
```

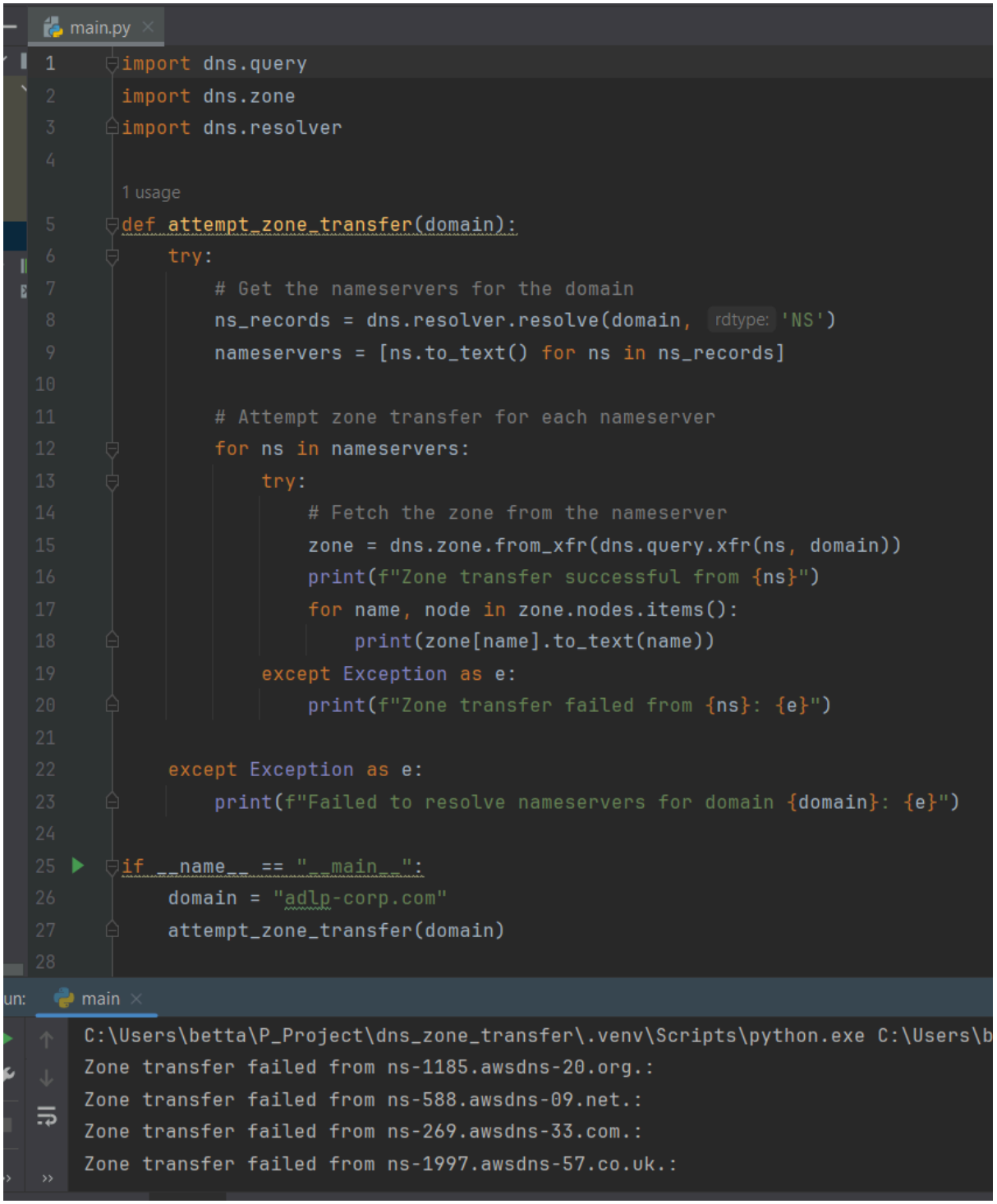
```
-b SOURCE, --source SOURCE
                      anubis, baidu, bevigil, binaryedge, bing, bingapi, bufferoverun, brave, censys,
                      certspotter, criminalip, crtsh, dnsdumpster, duckduckgo, fullhunt, github-code,
                      hackertarget, hunter, hunterhow, intelx, netlas, onyphe, otx, pentesttools,
                      projectdiscovery, rapiddns, rocketreach, securityTrails, sitedossier, subdomaincenter,
                      subdomainfinderc99, threatminer, tomba, urlscan, virustotal, yahoo, zoomeye
```

8. Use theHarvester tool at becode.org. How many ip addresses did you find?
Your response Your command

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d becode.org -l 50 -b all
```

```
[*] IPs found: 36
-------------------
104.19.244.91
104.19.245.91
108.129.32.135
109.197.246.221
18.200.133.185
185.199.108.153
185.199.109.153
```

9. Write a small script to attempt a zone transfer from adlp-corp.com using a higher-level scripting language such as Python, Perl, or Ruby
Your Script

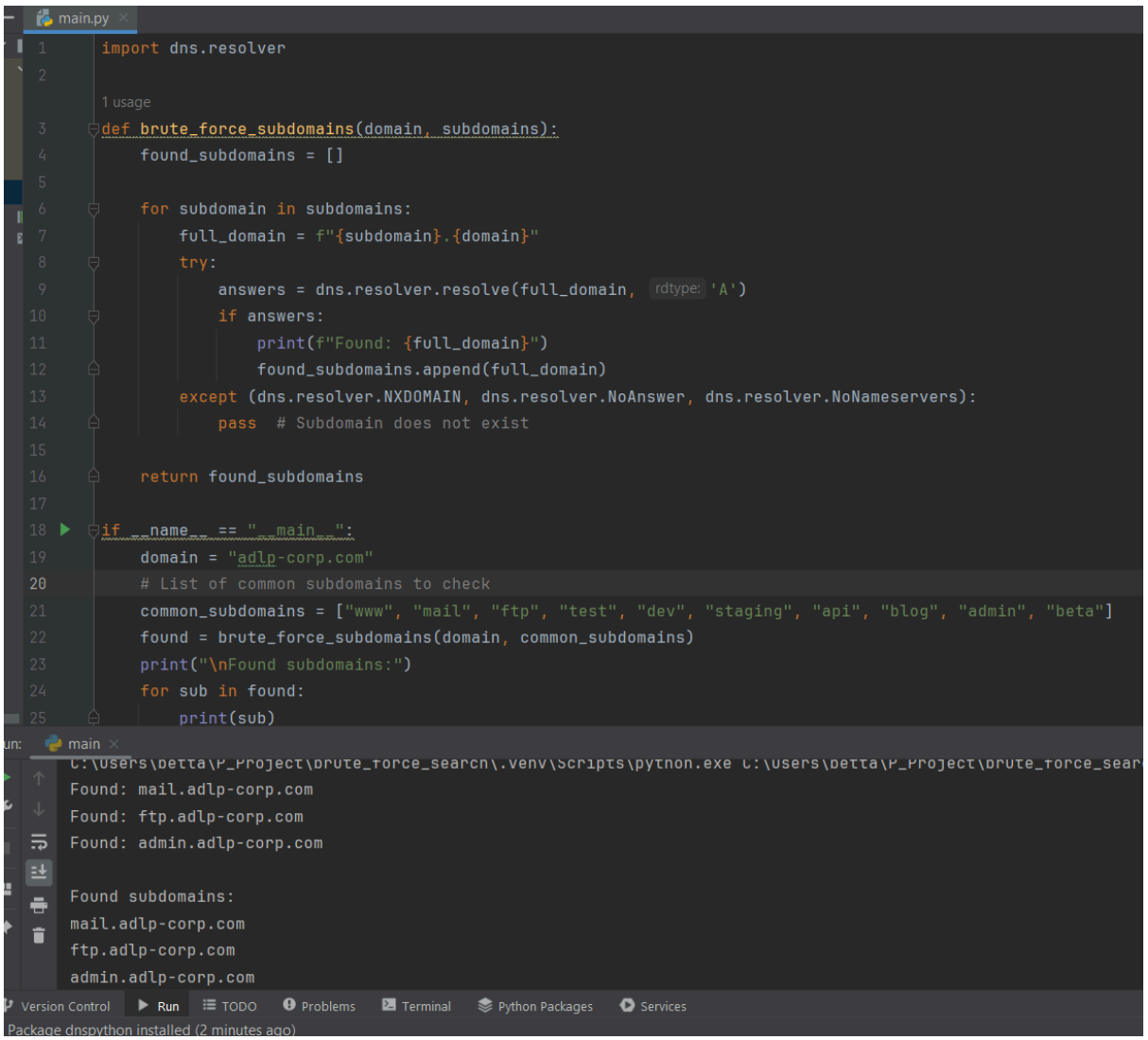


Important Notes

Performing a DNS zone transfer without permission is often considered unauthorized access and may violate policies or laws. Always ensure you have explicit permission to conduct such activities on a domain.

Many DNS servers are configured to disallow zone transfers for security reasons, so it's common for these attempts to fail even with legitimate permission.

10. Write a small script to attempt a brute force search for subdomains using a higher level scripting language such as Python, Perl or Ruby.
Your Script


main.py
import dns.resolver
1 usage
def brute_force_subdomains(domain, subdomains):
found_subdomains = []
for subdomain in subdomains:
full_domain = f"{subdomain}.{domain}"
try:
answers = dns.resolver.resolve(full_domain, rdtype: 'A')
if answers:
print(f"Found: {full_domain}")
found_subdomains.append(full_domain)
except (dns.resolver.NXDOMAIN, dns.resolver.NoAnswer, dns.resolver.NoNameservers):
pass # Subdomain does not exist
return found_subdomains
if __name__ == "__main__":
domain = "adlp-corp.com"
# List of common subdomains to check
common_subdomains = ["www", "mail", "ftp", "test", "dev", "staging", "api", "blog", "admin", "beta"]
found = brute_force_subdomains(domain, common_subdomains)
print("\nFound subdomains:")
for sub in found:
print(sub)
main
C:\Users\betta\P_Project\brute_force_search\.venv\Scripts\python.exe C:\Users\betta\P_Project\brute_force_sear
Found: mail.adlp-corp.com
Found: ftp.adlp-corp.com
Found: admin.adlp-corp.com
Found subdomains:
mail.adlp-corp.com
ftp.adlp-corp.com
admin.adlp-corp.com
Version Control
Run
TODO
Problems
Terminal
Python Packages
Services
Package dnspython installed (2 minutes ago)

HTTP Enumerator:

1. How many files could you find on port 80?

Your response: 16

```
┌──(kali㉿ntsapi)-[/opt/SecLists/Discovery/Web-Content]
└─$ sudo gobuster dir -u http://10.13.1.36:80 -w /opt/SecLists/Discovery/Web-Content/big
.txt -o gobuster_p80.txt
[sudo] password for kali:
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.13.1.36:80
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /opt/SecLists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 292]
/.htaccess            (Status: 403) [Size: 292]
/backup               (Status: 200) [Size: 51]
/caches               (Status: 301) [Size: 314] [--> http://10.13.1.36/caches/]
/cgi-bin/             (Status: 403) [Size: 291]
/dav                  (Status: 301) [Size: 311] [--> http://10.13.1.36/dav/]
/error_log            (Status: 301) [Size: 317] [--> http://10.13.1.36/error_log/]
/index                (Status: 200) [Size: 891]
/phpMyAdmin           (Status: 301) [Size: 318] [--> http://10.13.1.36/phpMyAdmin/]
/phpinfo              (Status: 200) [Size: 47969]
/server-status        (Status: 403) [Size: 296]
/stats                (Status: 301) [Size: 313] [--> http://10.13.1.36/stats/]
/test                 (Status: 301) [Size: 312] [--> http://10.13.1.36/test/]
/tikiwiki             (Status: 301) [Size: 316] [--> http://10.13.1.36/tikiwiki/]
/twiki                (Status: 301) [Size: 313] [--> http://10.13.1.36/twiki/]
/wp-contents          (Status: 301) [Size: 319] [--> http://10.13.1.36/wp-contents/]
Progress: 20476 / 20477 (100.00%)
===============================================================
Finished
===============================================================

┌──(kali㉿ntsapi)-[/opt/SecLists/Discovery/Web-Content]
└─$ cat gobuster_p80.txt | wc -l

16
```

2. What is the version of apache?

Your response

```
┌──(kali㉿ntsapi)-[/opt/SecLists/Discovery/Web-Content]
└─$ curl -I http://10.13.1.36
HTTP/1.1 200 OK
Date: Fri, 14 Jun 2024 07:34:44 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
```

3. What is the version of php ?

Your response

```
┌──(kali㉿ntsapi)-[/opt/SecLists/Discovery/Web-Content]
└─$ curl -I http://10.13.1.36
HTTP/1.1 200 OK
Date: Fri, 14 Jun 2024 07:34:44 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
```

4. What server extension is installed?

Your response: .php

```
┌──(kali㉿ntsapi)-[/opt/SecLists/Discovery/Web-Content]
└─$ gobuster dir -u http://10.13.1.36 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,js,css,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.13.1.36
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,js,css,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 288]
/index.php            (Status: 200) [Size: 891]
/index                (Status: 200) [Size: 891]
/stats                (Status: 301) [Size: 313] [--> http://10.13.1.36/stats/]
/stats.php            (Status: 200) [Size: 315]
/test                 (Status: 301) [Size: 312] [--> http://10.13.1.36/test/]
/backup               (Status: 200) [Size: 51]
/twiki                (Status: 301) [Size: 313] [--> http://10.13.1.36/twiki/]
Progress: 102370 / 1323366 (7.74%)
[!] Keyboard interrupt detected, terminating.
Progress: 102432 / 1323366 (7.74%)
===============================================================
Finished
```

5. What is the name of the file in testoutput?

Your response

6. Do a scan with Nikto on port 80.

Your response:

```
┌──(kali㉿ntsapi)-[~]
└─$ nikto -h http://10.13.1.36:80
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.13.1.36
+ Target Hostname:    10.13.1.36
+ Target Port:        80
+ Start Time:         2024-06-14 05:05:50 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer
.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to re
nder the content of the site in a different fashion to the MIME type. See: https://www.n
etsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to e
asily brute force file names. The following alternatives for 'index' were found: index.p
hp. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmclou
d.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34
 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false po
sitives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: http
s://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.o
rg/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive informat
ion via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informat
ion via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informat
ion via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informat
ion via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be p
rotected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMy
Admin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008. See: http:/
/cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be prote
cted or limited to authorized hosts.
+ /stats/: Directory indexing found.
+ /stats/: This might be interesting.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives
a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-ac
cess-to-iconsreadme/
+ /stats.php?vwar_root=http://blog.cirt.net/rfiinc.txt: Cookie PHPSESSID created without the ht
tponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be pro
tected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or li
mited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8911 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time:           2024-06-14 05:13:09 (GMT-4) (439 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

An informative file in php seems to be available, what is its name?

+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552

7. What application has a name that starts with T and ends with Y?

Your response:**TwikiHistory**

Welcome to TWiki

- readme.txt
- license.txt
- TWikiDocumentation.html
- TWikiHistory.html

8. What curl command can you use to see the server version?

Your response:

curl -I http://10.13.1.36

9. What tool for enumerating files does it do recursively? (By default)

Your response: ffuf

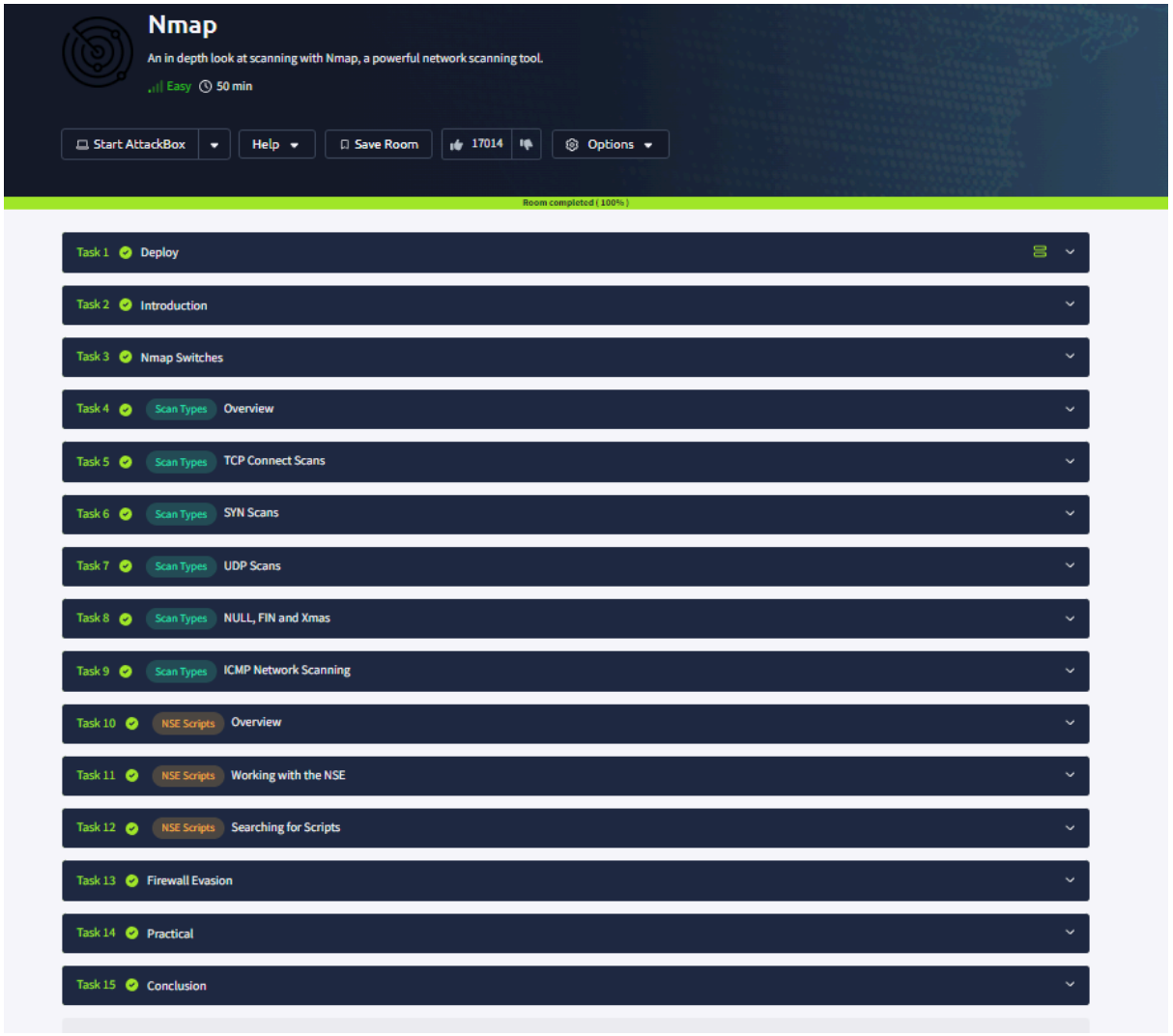
ffuf -w /opt/SecLists/Discovery/Web-Content/big.txt -u http://10.13.1.36/FUZZ -recursion -recursion-depth 1

10. What other administration application is currently also on port 80?

Your response:

```
+ /phpMyAdmin/: phpMyAdmin d
+ /phpMyAdmin/Documentation.
```

Nmap



1. How many tcp ports are open on the box? What command did you use?

Your response: 23

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -sT 10.13.1.36 | grep -c 'open'
23
```

2. How many udp ports are open on the box? What command did you use?

Your response: 0

```
┌──(kali㉿ntsapi)-[~]
└─$ sudo nmap -sU -p- 10.13.1.16 | grep -c 'open'
0
```

3. What is the version of ftp?

Your response

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -sV -p 21 10.13.1.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 10:09 EDT
Nmap scan report for 10.13.1.36
Host is up (0.038s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: OS: Unix
```

4. What is the version of ssh?

Your response

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -sV -p 22 10.13.1.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 10:11 EDT
Nmap scan report for 10.13.1.36
Host is up (0.041s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

5. What is the version of Apache?

Your response

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -sV -p 80,443 10.13.1.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 10:13 EDT
Nmap scan report for 10.13.1.36
Host is up (0.038s latency).

PORT    STATE  SERVICE VERSION
80/tcp  open   http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
443/tcp closed https
```

6. Is anonymous ftp access allowed on the box? What command did you use? (Use only nmap)

Your response: yes

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap --script ftp-anon -p 21 10.13.1.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 10:15 EDT
Nmap scan report for 10.13.1.36
Host is up (0.14s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

7. Do a SYN scan. Which command did you use?

Your response

```
┌──(kali㉿ntsapi)-[~]
└─$ sudo nmap -sS 10.13.1.36 | wc -l
30
```

8. Do a scan that bypasses a firewall. What command did you use?

Your response

- nmap -sT 10.13.1.36 **#WORKED**
- Sudo nmap -sI zombie_ip 10.13.1.36 **#BLOCKED**
- Sudo nmap -f 10.13.1.36 **#FILTERED**
- Sudo nmap -sS -Pn -D decoy1,decoy2,your_ip 10.13.1.36 **#WORKED**
- nmap -r 10.13.1.36 **#WORKED**

9. Run a scan with the default NSE scripts. Which flag do you use?

Your response:

-sC

10. What service occupies port 8180?

Your response

```
8180/tcp open  unknown
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
```

11. What is the salt of the mysql service?

Your response

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -p 3306 --script mysql-info 10.13.1.36
```

```
_  Salt: a)BRT/.:vh$wPf3i8{%B
```

12. What is the domain name ?

Your response:

nmap --script smb-os-discovery 10.13.1.36

Gave the below responses

localdomain

13. What is the FQDN of the box ?

Your response

metasploitable.localdomain

14. What is the os version ?

Your response

Unix

15. What is the version of Samba ?

Your response

3.0.20-Debian

16. Wat is the name of the box ?

Your response

Metasploitable

17. Do a scan on the subnet 10.xx.1.0/24. How many IP addresses respond? What command did you use? Charleroi : 10.11.0.1/24 Bruxelles : 10.12.0.1/24 Ghent : 10.13.0.1/24

Your response

Charleroi:

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -sP 10.11.0.1/24 | grep "Host is up" | wc -l
2
```

Bruxelles:

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -sP 10.12.0.1/24 | grep "Host is up" | wc -l
1
```

Ghent:

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -sP 10.13.0.1/24 | grep "Host is up" | wc -l
1
```

18. Do the same thing but with the top port option at 10. What command did you use?

Your response:

Scanning all 3 locations at once.

RPC

1. With the rpc protocol, how many users can you find ?

Your response Your command

```
┌──(kali㉿ntsapi)-[~]
└─$ rpcinfo -p 10.13.1.36 | wc -l
23
```

2. What is the rid of msfadmin?

Your response Your command

```
┌──(kali㉿ntsapi)-[~]
└─$ rpcclient -U "" -N 10.13.1.36
rpcclient $> enumdomusers
user:[games] rid:[0×3f2]
```

or

```
user_rid :      0×bb8
```

```
┌──(kali㉿ntsapi)-[~]
└─$ rpcclient -U "" 10.13.1.36
Password for [WORKGROUP\]:
rpcclient $> queryuser msfadmin
```

Password: enumdomusers

3. What is the path of msfadmin's profile?

Your response Your command

Same command on the screenshot:

Profile Path: \\metasploitable\msfadmin\profile

4. When did msadmin last change password?

Your response Your command

Same command on the screenshot

Password last set Time : Wed, 28 Apr 2010 02:56:18 EDT

5. When should msfadmin change its password?

Your response Your command

Same command on the screenshot

Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT

Details:

```
┌──(kali㉿ntsapi)-[~]
└─$ rpcclient -U "" 10.13.1.36
Password for [WORKGROUP\]:
rpcclient $> queryuser msfadmin
        User Name    :   msfadmin
        Full Name    :   msfadmin,,,
        Home Drive   :   \\metasploitable\msfadmin
        Dir Drive    :
        Profile Path:    \\metasploitable\msfadmin\profile
        Logon Script:
        Description :
        Workstations:
        Comment      :   (null)
        Remote Dial :
        Logon Time                :      Wed, 31 Dec 1969 19:00:00 EST
        Logoff Time               :      Wed, 13 Sep 30828 22:48:05 EDT
        Kickoff Time              :      Wed, 13 Sep 30828 22:48:05 EDT
        Password last set Time    :      Wed, 28 Apr 2010 02:56:18 EDT
        Password can change Time :       Wed, 28 Apr 2010 02:56:18 EDT
        Password must change Time:       Wed, 13 Sep 30828 22:48:05 EDT
        unknown_2[0..31]...
        user_rid :       0×bb8
        group_rid:       0×bb9
        acb_info :       0×00000010
        fields_present: 0×00ffffff
        logon_divs:      168
        bad_password_count:      0×00000000
        logon_count:     0×00000000
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $>
```

SMB:

1. What is the OS ?

Your response: **OS: Unix (Samba 3.0.20-Debian)**

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap --script smb-os-discovery 10.13.1.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-16 06:05 EDT
Nmap scan report for 10.13.1.36
```

```
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
```

2. What is the version of samba on the box?

Your response:

Samba 3.0.20-Debian

3. How many group names are there? (use nbtstat)

Your response: 4

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap --script nbstat.nse 10.13.1.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-16 06:12 EDT
```

```
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
```

4. What is the FQDN ?

Your response: **Metasploitable.localdomain**

```
|   FQDN: metasploitable.localdomain
```

5. What is the Netbios computer name?

Your response: **METASPLOITABLE:**

```
┌──(kali㉿ntsapi)-[~]
└─$ nbtscan 10.13.1.36
Doing NBT name scan for addresses from 10.13.1.36

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
10.13.1.36       METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
```

6. How many disks are shared?

Your response: 3

```
┌──(kali㉿ntsapi)-[~]
└─$ smbclient -L 10.13.1.36
Password for [WORKGROUP\kali]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
```

7. Which one is available for reading and writing?

Your response:

tmp Disk oh noes!

```
┌──(kali㉿ntsapi)-[~]
└─$ crackmapexec smb 10.13.1.36 -u '' -p '' --shares
SMB         10.13.1.36      445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE) (domain:localdoma
SMB         10.13.1.36      445    METASPLOITABLE   [+] localdomain\:
SMB         10.13.1.36      445    METASPLOITABLE   [+] Enumerated shares
SMB         10.13.1.36      445    METASPLOITABLE   Share           Permissions     Remark
SMB         10.13.1.36      445    METASPLOITABLE   -----           -----------     ------
SMB         10.13.1.36      445    METASPLOITABLE   print$                          Printer Drivers
SMB         10.13.1.36      445    METASPLOITABLE   tmp             READ,WRITE      oh noes!
SMB         10.13.1.36      445    METASPLOITABLE   opt
SMB         10.13.1.36      445    METASPLOITABLE   IPC$                            IPC Service (met
SMB         10.13.1.36      445    METASPLOITABLE   ADMIN$                          IPC Service (met
```

8. What flag did you find when you logged in?

Your response:

Not Found

9. What is the path that begins with `c:\` in this file?

Your response:

```
path:   C:\var\lib\samba\printers
```

10. How many users can you find ?

Your response: 5 or 49

```
┌──(kali㉿ntsapi)-[~]
└─$ rpcclient -U "" -N 10.13.1.36
rpcclient $> netshareenumall
netname: print$
        remark: Printer Drivers
        path:   C:\var\lib\samba\printers
        password:
netname: tmp
        remark: oh noes!
        path:   C:\tmp
        password:
netname: opt
        remark:
        path:   C:\tmp
        password:
netname: IPC$
        remark: IPC Service (metasploitable server (Samba 3.0.20-Debian))
        path:   C:\tmp
        password:
netname: ADMIN$
        remark: IPC Service (metasploitable server (Samba 3.0.20-Debian))
        path:   C:\tmp
        password:
rpcclient $>
```

Another possibility

```
┌──(kali㉿ntsapi)-[~]
└─$ enum4linux 10.13.1.36
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on
Sun Jun 16 14:44:14 2024
```

```
user:[games] rid:[0×3f2]
user:[nobody] rid:[0×1f5]
user:[bind] rid:[0×4ba]
user:[proxy] rid:[0×402]
user:[syslog] rid:[0×4b4]
user:[user] rid:[0×bba]
user:[www-data] rid:[0×42a]
user:[root] rid:[0×3e8]
user:[news] rid:[0×3fa]
user:[postgres] rid:[0×4c0]
user:[bin] rid:[0×3ec]
user:[mail] rid:[0×3f8]
user:[distccd] rid:[0×4c6]
user:[proftpd] rid:[0×4ca]
user:[dhcp] rid:[0×4b2]
user:[daemon] rid:[0×3ea]
user:[sshd] rid:[0×4b8]
user:[man] rid:[0×3f4]
user:[lp] rid:[0×3f6]
user:[mysql] rid:[0×4c2]
user:[gnats] rid:[0×43a]
user:[libuuid] rid:[0×4b0]
user:[backup] rid:[0×42c]
user:[msfadmin] rid:[0×bb8]
user:[telnetd] rid:[0×4c8]
user:[sys] rid:[0×3ee]
user:[klog] rid:[0×4b6]
user:[postfix] rid:[0×4bc]
user:[service] rid:[0×bbc]
user:[list] rid:[0×434]
user:[irc] rid:[0×436]
user:[ftp] rid:[0×4be]
user:[tomcat55] rid:[0×4c4]
user:[sync] rid:[0×3f0]
user:[uucp] rid:[0×3fc]
```

SMTP:

1. How many commands are allowed on port 25?

Your response: **10**

According to chatgpt

Or

9

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -p 25 --script smtp-commands 10.13.1.36 | wc -l
9
```

2. How many users can you enumerate via port 25?

Your response: **7**

```
┌──(kali㉿ntsapi)-[~]
└─$ nano users.txt

┌──(kali㉿ntsapi)-[~]
└─$ cat users.txt
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news

┌──(kali㉿ntsapi)-[~]
└─$ smtp-user-enum -M VRFY -U users.txt -t 10.13.1.36
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... users.txt
Target count ............. 1
Username count ........... 10
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Mon Jun 17 05:31:06 2024 #########
10.13.1.36: root exists
10.13.1.36: daemon exists
10.13.1.36: bin exists
10.13.1.36: lp exists
10.13.1.36: sync exists
10.13.1.36: mail exists
10.13.1.36: news exists
######## Scan completed at Mon Jun 17 05:31:09 2024 #########
7 results.

10 queries in 3 seconds (3.3 queries / sec)
```

3. Send a mail with the email admin@metasploitable.localdomain to root@metasploitable.localdomain by connecting to the smtp server.

Your response:

```
┌──(kali㉿ntsapi)-[~]
└─$ telnet 10.13.1.36 25
Trying 10.13.1.36 ...
Connected to 10.13.1.36.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
HELO local
250 metasploitable.localdomain
MAIL FROM:admin@metasploitable.localdomain
250 2.1.0 Ok
RCPT TO:root@metasploitable.localdomain
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Check ME with ssh
After creating this email, use ssh to check if the email exist.
.
250 2.0.0 Ok: queued as 1F5F0CC91
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

4. Connect to ssh with msfadmin:msfadmin creds and check if you have sent the mail

Your response:

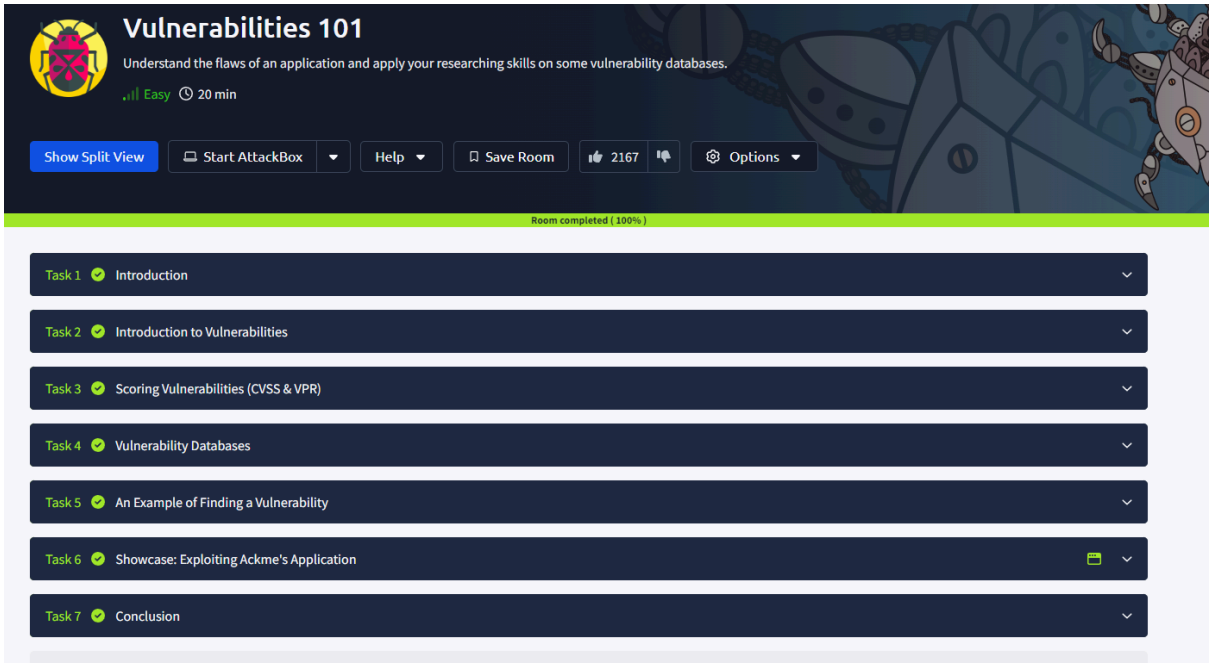
```
┌──(kali㉿ntsapi)-[~]
└─$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa msfadmin@10.13.1.36
msfadmin@10.13.1.36's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Tue Jun 18 03:47:50 2024 from 192.168.149.8
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ sudo grep "admin@metasploitable.localdomain" /var/log/mail.log
Jun 17 13:12:58 metasploitable postfix/qmgr[4580]: 9B4A2CC91: from=<admin@metasploitable.localdo
main>, size=436, nrcpt=1 (queue active)
Jun 18 02:47:44 metasploitable postfix/qmgr[4580]: 9FEDECC91: from=<admin@metasploitable.localdo
main>, size=427, nrcpt=1 (queue active)
Jun 18 03:08:07 metasploitable postfix/qmgr[4580]: 7347ECC91: from=<admin@metasploitable.localdo
main>, size=516, nrcpt=1 (queue active)
Jun 18 03:09:21 metasploitable postfix/qmgr[4580]: 12BBDCC91: from=<admin@metasploitable.localdo
main>, size=505, nrcpt=1 (queue active)
Jun 18 03:14:11 metasploitable postfix/qmgr[4580]: E59A2CC94: from=<admin@metasploitable.localdo
main>, size=481, nrcpt=1 (queue active)
Jun 18 03:17:48 metasploitable postfix/qmgr[4580]: 1F5F0CC91: from=<admin@metasploitable.localdo
main>, size=470, nrcpt=1 (queue active)
```

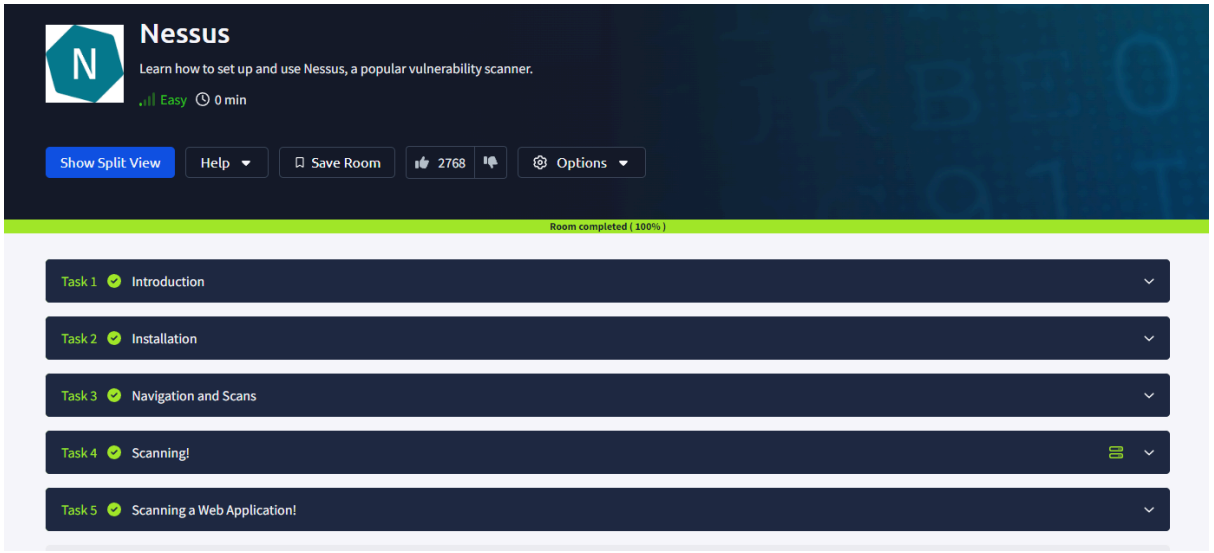
Vul_Scan:

1. Follow this room on try hack me

- https://tryhackme.com/room/vulnerabilities101



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

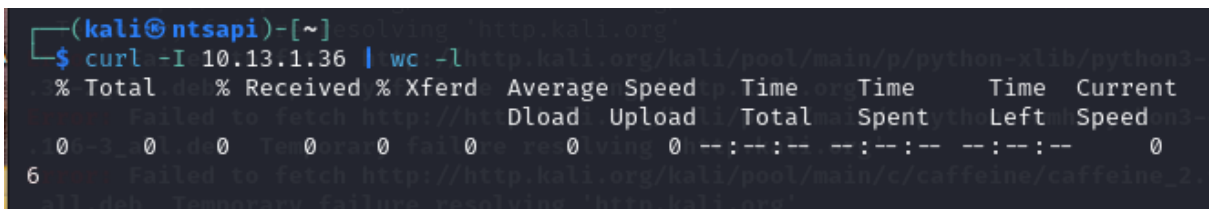


2. Questions :

2.1 Do a manual scan of the 10.13.1.36 box

- How many vulnerable services are there?

6



- What are these services?

```
 program vers proto   port  service
  100000    2   tcp    111  portmapper
  100000    2   udp    111  portmapper
  100024    1   udp  38611  status
  100024    1   tcp  43460  status
  100003    2   udp   2049  nfs
  100003    3   udp   2049  nfs
  100003    4   udp   2049  nfs
  100021    1   udp  51045  nlockmgr
  100021    3   udp  51045  nlockmgr
  100021    4   udp  51045  nlockmgr
  100003    2   tcp   2049  nfs
  100003    3   tcp   2049  nfs
  100003    4   tcp   2049  nfs
  100021    1   tcp  53711  nlockmgr
  100021    3   tcp  53711  nlockmgr
  100021    4   tcp  53711  nlockmgr
  100005    1   udp  38923  mountd
  100005    1   tcp  48817  mountd
  100005    2   udp  38923  mountd
  100005    2   tcp  48817  mountd
  100005    3   udp  38923  mountd
  100005    3   tcp  48817  mountd
```

3. 2.2 Do a vulnerability scan with nmap.
   - How many vulnerabilities did nmap find ?

     32

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -sV 10.13.1.36 | wc -l
32
```

   - What are these services?

```
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet       Linux telnetd
25/tcp   open  smtp         Postfix smtpd
53/tcp   open  domain       ISC BIND 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind      2 (RPC #100000)
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec         netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry?
1524/tcp open  bindshell    Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ftp          ProFTPD 1.3.1
3306/tcp open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13?
8180/tcp open  unknown
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:lin
ux: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 178.82 seconds
```

4. 3.3 Do a vulnerability scan with Nessus.
   - How many vulnerabilities did nessus find ?

After Launching Nessus and doing the setups.

- What are these services?