

Vu Nguyen

UID: u1483046

Assignment 22 - Nmap and TCP or UDP Captures (Lab and Quiz)

1. Lab 9.3.8, Part 2, Step 1a:

David Eccles
School of Business
THE UNIVERSITY OF UTAH

Home Reservation u1483046@utah.edu

MyNETLAB > Cisco CyberOps Associate POD 3 > Reservation 70071 > 9.3.8 Lab - Exploring Nmap

Topology Content Status Workstation

Time Remaining
1 56
hrs. min.

Applications Terminal - analyst@secops

```
analyst@secops ~$ nmap -A -iL localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-22 20:53 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000041s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--  1 0      0      32 Aug 11 2020 Readme
|_rw-r--r--  1 0      0      8 Mar 26 2018 ftp_test
| ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 127.0.0.1
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_  At session startup, client count was 4
|_  vsFTPd 3.0.3 - secure, fast, stable
|_End of status
```

2. Lab 10.2.7, Part 2, Step 1c:

[illegible]

3. Lab 10.4.3, Part 1, Step 2b:

[illegible]

4. Lab 10.4.3, Part 1, Step 4:

The screenshot shows a Wireshark capture on the eth1 interface. The packet list pane displays several TCP and FTP packets. The selected packet is a TCP Reset (RST) with sequence number 39884 and destination port 21. The packet details pane shows the TCP header with RST=1 and Seq=39884. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000000	192.168.0.1	192.168.0.1	TCP	74	39884 → 21 [RST] Seq=39884 Win=0 Len=0
5	0.000000	192.168.0.1	192.168.0.1	TCP	60	39884 → 21 [ACK] Seq=1 Win=65536 Len=0 TSval=99237823 TSecr=391598708
6	0.000000	192.168.0.1	192.168.0.1	FTP	113	Response: 230 Welcome to Cisco CyberOps IP FTP service
7	0.000000	192.168.0.1	192.168.0.1	TCP	60	39884 → 21 [ACK] Seq=1 Win=65536 Len=0 TSval=99237826 TSecr=391598710
8	0.000000	192.168.0.1	192.168.0.1	FTP	82	Request: USER anonymous
9	0.000000	192.168.0.1	192.168.0.1	TCP	60	39884 → 21 [ACK] Seq=48 Win=65280 Len=0 TSval=991605392 TSecr=99244587
10	0.000000	192.168.0.1	192.168.0.1	FTP	180	Response: 331 Please specify the password.
11	0.000000	192.168.0.1	192.168.0.1	TCP	60	39884 → 21 [ACK] Seq=1 Win=65536 Len=0 TSval=99244507 TSecr=3915985392
12	0.000000	192.168.0.1	192.168.0.1	FTP	73	Request: PASS
13	0.000000	192.168.0.1	192.168.0.1	TCP	60	39884 → 21 [ACK] Seq=82 Win=65280 Len=0 TSval=391618229 TSecr=99249344
14	0.000000	192.168.0.1	192.168.0.1	FTP	89	Response: 230 Login successful.

5. Lab 10.6.7, Part 2, Step 1c:

The screenshot shows a Wireshark capture of an HTTP traffic file named httpdump.pcap. The packet list pane displays several HTTP and TLSv1.2 packets. The selected packet is a TLSv1.2 Application Data packet. The packet details pane shows the TLSv1.2 header and application data. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
27	2.490828	23.72.68.185	192.168.0.11	TLSv1.2	1083	Certificate Status, Server Key Exchange, Server
28	2.490841	192.168.0.11	23.72.68.185	TCP	54	38596 → 443 [ACK] Seq=193 Ack=5126 Win=39420 Len=0
29	2.490728	192.168.0.11	23.72.68.185	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypt
30	2.493133	23.72.68.185	192.168.0.11	TCP	60	443 → 38596 [ACK] Seq=5126 Ack=519 Win=64240 Len=0
31	2.494217	192.168.0.11	23.72.68.185	TLSv1.2	403	Application Data
32	2.494243	23.72.68.185	192.168.0.11	TCP	60	443 → 38596 [ACK] Seq=5126 Ack=482 Win=64240 Len=0
34	2.494532	23.72.68.185	192.168.0.11	TCP	60	443 → 38596 [ACK] Seq=5126 Ack=829 Win=64240 Len=0
35	2.515192	23.72.68.185	192.168.0.11	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypt
36	2.546885	23.72.68.185	192.168.0.11	TLSv1.2	131	Application Data