The University of Texas at San Antonio™

IS 3423-005 Network Security

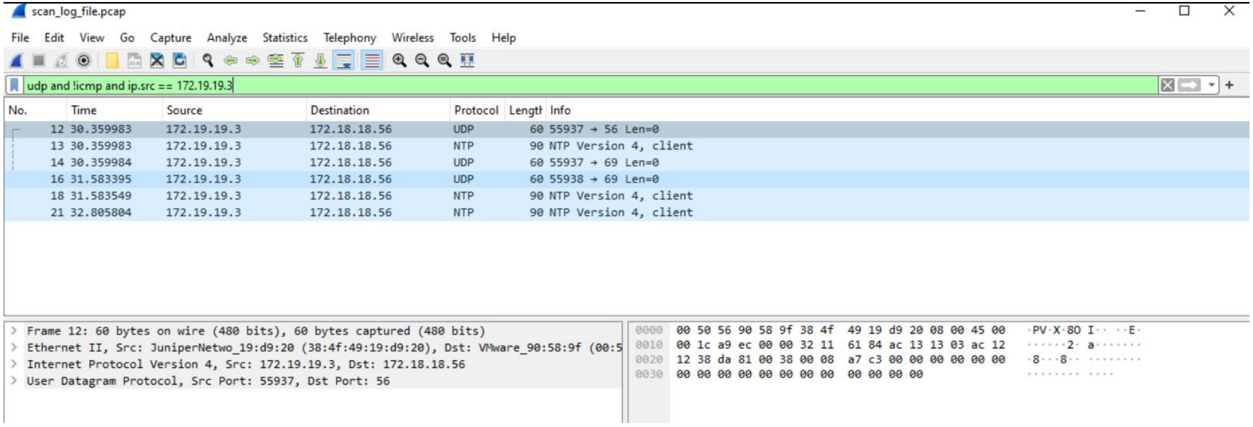
Wireshark Exercise – Win_10_t12

Student:

Dillen Dela Cruz, odv464

Prepared Network Security
03/05/2024
Professor: Natalie Sjelin

Part 2 - Analyzing and filtering capture files:


scan_log_file.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp and !icmp and ip.src == 172.19.19.3
```

```
No.  Time       Source       Destination   Protocol Length Info
  12 30.359983  172.19.19.3  172.18.18.56  UDP         60 55937 → 56 Len=0
  13 30.359983  172.19.19.3  172.18.18.56  NTP         90 NTP Version 4, client
  14 30.359984  172.19.19.3  172.18.18.56  UDP         60 55937 → 69 Len=0
  16 31.583395  172.19.19.3  172.18.18.56  UDP         60 55938 → 69 Len=0
  18 31.583549  172.19.19.3  172.18.18.56  NTP         90 NTP Version 4, client
  21 32.805804  172.19.19.3  172.18.18.56  NTP         90 NTP Version 4, client
```

```
> Frame 12: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: JuniperNetwo_19:d9:20 (38:4f:49:19:d9:20), Dst: VMware_90:58:9f (00:5
> Internet Protocol Version 4, Src: 172.19.19.3, Dst: 172.18.18.56
> User Datagram Protocol, Src Port: 55937, Dst Port: 56
```

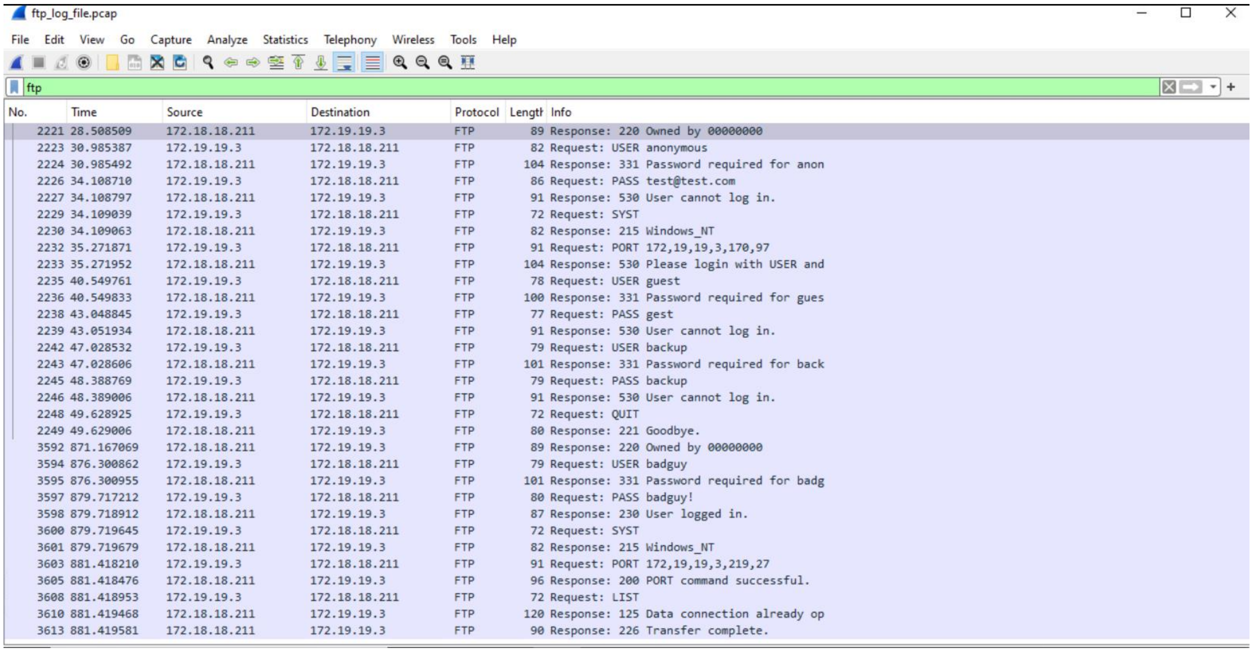
```
0000  00 50 56 90 58 9f 38 4f  49 19 d9 20 08 00 45 00   ·PV·X·8O I·· ··E·
0010  00 1c a9 ec 00 00 32 11  61 84 ac 13 13 03 ac 12   ······2· a·······
0020  12 38 da 81 00 38 00 08  a7 c3 00 00 00 00 00 00   ·8···8·· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Port 56 is assigned and uses the Xerox Network Systems Authentication Protocol. It is a protocol suite designed for easy, efficient, and rapid communication in both local and wide area networks (DevX).

Port 69 is assigned and uses the Trivial File Transfer Protocol. TFTP is a simplified file transfer protocol often used for transferring small files with no user authentication(IBM). It operates over UDP for simplicity and speed but lacks some of the security mechanisms found in other file transfer protocols like FTP (File Transfer Protocol).

Port 123 is assigned and is used for time synchronization. It uses the Network Time Protocol to ensure that various devices on a network have accurate and synchronized time, which is essential for various applications, including logging and coordination of events.

Part 3 - FTP Log File Analysis:



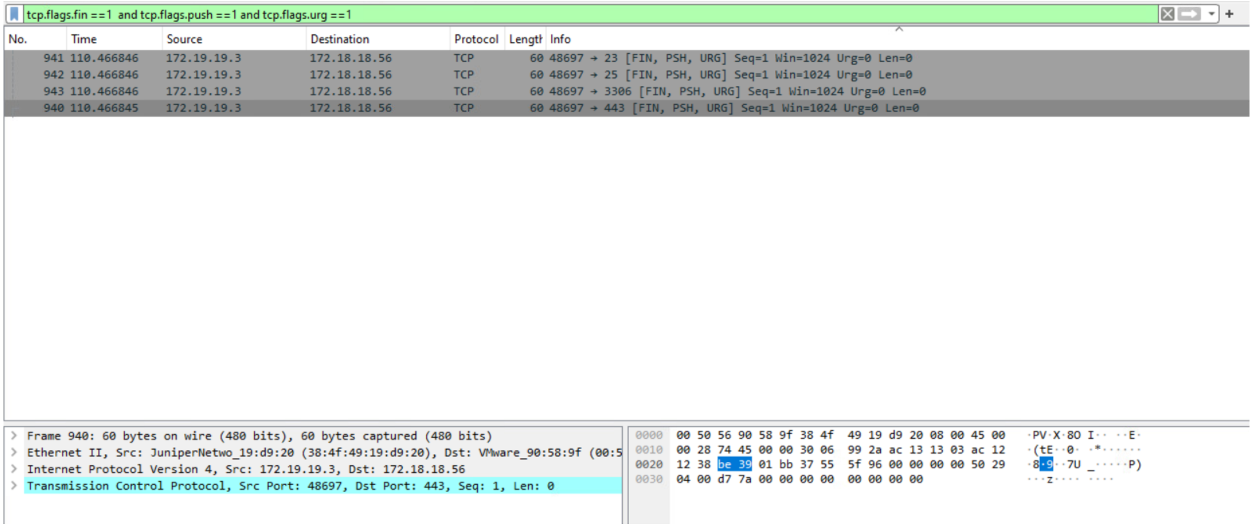
ftp_log_file.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

No.	Time	Source	Destination	Protocol	Length	Info
2221	28.508509	172.18.18.211	172.19.19.3	FTP	89	Response: 220 Owned by 00000000
2223	30.985387	172.19.19.3	172.18.18.211	FTP	82	Request: USER anonymous
2224	30.985492	172.18.18.211	172.19.19.3	FTP	104	Response: 331 Password required for anon
2226	34.108710	172.19.19.3	172.18.18.211	FTP	86	Request: PASS test@test.com
2227	34.108797	172.18.18.211	172.19.19.3	FTP	91	Response: 530 User cannot log in.
2229	34.109039	172.19.19.3	172.18.18.211	FTP	72	Request: SYST
2230	34.109063	172.18.18.211	172.19.19.3	FTP	82	Response: 215 Windows_NT
2232	35.271871	172.19.19.3	172.18.18.211	FTP	91	Request: PORT 172,19,19,3,170,97
2233	35.271952	172.18.18.211	172.19.19.3	FTP	104	Response: 530 Please login with USER and
2235	40.549761	172.19.19.3	172.18.18.211	FTP	78	Request: USER guest
2236	40.549833	172.18.18.211	172.19.19.3	FTP	100	Response: 331 Password required for gues
2238	43.048845	172.19.19.3	172.18.18.211	FTP	77	Request: PASS gest
2239	43.051934	172.18.18.211	172.19.19.3	FTP	91	Response: 530 User cannot log in.
2242	47.028532	172.19.19.3	172.18.18.211	FTP	79	Request: USER backup
2243	47.028606	172.18.18.211	172.19.19.3	FTP	101	Response: 331 Password required for back
2245	48.388769	172.19.19.3	172.18.18.211	FTP	79	Request: PASS backup
2246	48.389006	172.18.18.211	172.19.19.3	FTP	91	Response: 530 User cannot log in.
2248	49.628925	172.19.19.3	172.18.18.211	FTP	72	Request: QUIT
2249	49.629006	172.18.18.211	172.19.19.3	FTP	80	Response: 221 Goodbye.
3592	871.167069	172.18.18.211	172.19.19.3	FTP	89	Response: 220 Owned by 00000000
3594	876.300862	172.19.19.3	172.18.18.211	FTP	79	Request: USER badguy
3595	876.300955	172.18.18.211	172.19.19.3	FTP	101	Response: 331 Password required for badg
3597	879.717212	172.19.19.3	172.18.18.211	FTP	80	Request: PASS badguy!
3598	879.718912	172.18.18.211	172.19.19.3	FTP	87	Response: 230 User logged in.
3600	879.719645	172.19.19.3	172.18.18.211	FTP	72	Request: SYST
3601	879.719679	172.18.18.211	172.19.19.3	FTP	82	Response: 215 Windows_NT
3603	881.418210	172.19.19.3	172.18.18.211	FTP	91	Request: PORT 172,19,19,3,219,27
3605	881.418476	172.18.18.211	172.19.19.3	FTP	96	Response: 200 PORT command successful.
3608	881.418953	172.19.19.3	172.18.18.211	FTP	72	Request: LIST
3610	881.419468	172.18.18.211	172.19.19.3	FTP	120	Response: 125 Data connection already op
3613	881.419581	172.18.18.211	172.19.19.3	FTP	90	Response: 226 Transfer complete.

The password used in the successful FTP session was “badguy!”. How I got this answer is by typing “ftp” into the filter tab. I then looked at the “Info” tab to find information about that individual packet. I found that there were 2 unsuccessful logins and 1 successful login associated with the file transfer.

Part 4 – Scan File Analysis:



```
tcp.flags.fin ==1  and tcp.flags.push ==1 and tcp.flags.urg ==1

No.     Time        Source        Destination    Protocol Length Info
    941 110.466846  172.19.19.3   172.18.18.56   TCP        60 48697 → 23 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
    942 110.466846  172.19.19.3   172.18.18.56   TCP        60 48697 → 25 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
    943 110.466846  172.19.19.3   172.18.18.56   TCP        60 48697 → 3306 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
    940 110.466845  172.19.19.3   172.18.18.56   TCP        60 48697 → 443 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

> Frame 940: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: JuniperNetwo_19:d9:20 (38:4f:49:19:d9:20), Dst: VMware_90:58:9f (00:5
> Internet Protocol Version 4, Src: 172.19.19.3, Dst: 172.18.18.56
> Transmission Control Protocol, Src Port: 48697, Dst Port: 443, Seq: 1, Len: 0

0000  00 50 56 90 58 9f 38 4f  49 19 d9 20 08 00 45 00   ·PV·X·8O I··  ··E·
0010  00 28 74 45 00 00 30 06  99 2a ac 13 13 03 ac 12   ·(tE··0· ·*······
0020  12 38 be 39 01 bb 37 55  5f 96 00 00 00 00 50 29   ·8·9··7U _·····P)
0030  04 00 d7 7a 00 00 00 00  00 00 00 00               ···z····  ····
```

The XMAS Nmap scan is used for used for identifying if a port is open or closed. Why a network administrator or a security professional would find this scan useful is to overall enhance the security posture of their networks by identifying open ports, evaluate potential vulnerabilities, and ensure that only necessary ports are accessible. On the other hand, attackers could find this useful by probing a target network to identify open ports, which can serve as entry points for unauthorized access or exploitation of vulnerabilities.

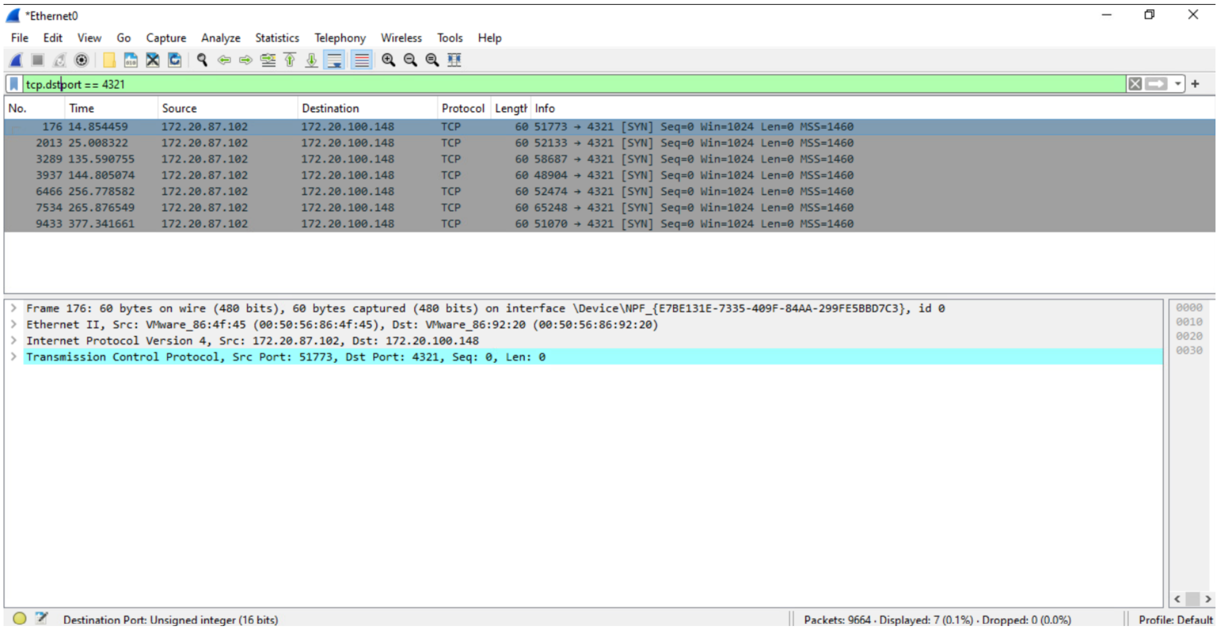
The destination ports found:

1. 23
2. 25
3. 3306
4. 443

* you can find the destination ports in the “Info” tab on the right side of the arrow

Part 5 – Capture Live Traffic:

Part A


*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.dstport == 4321

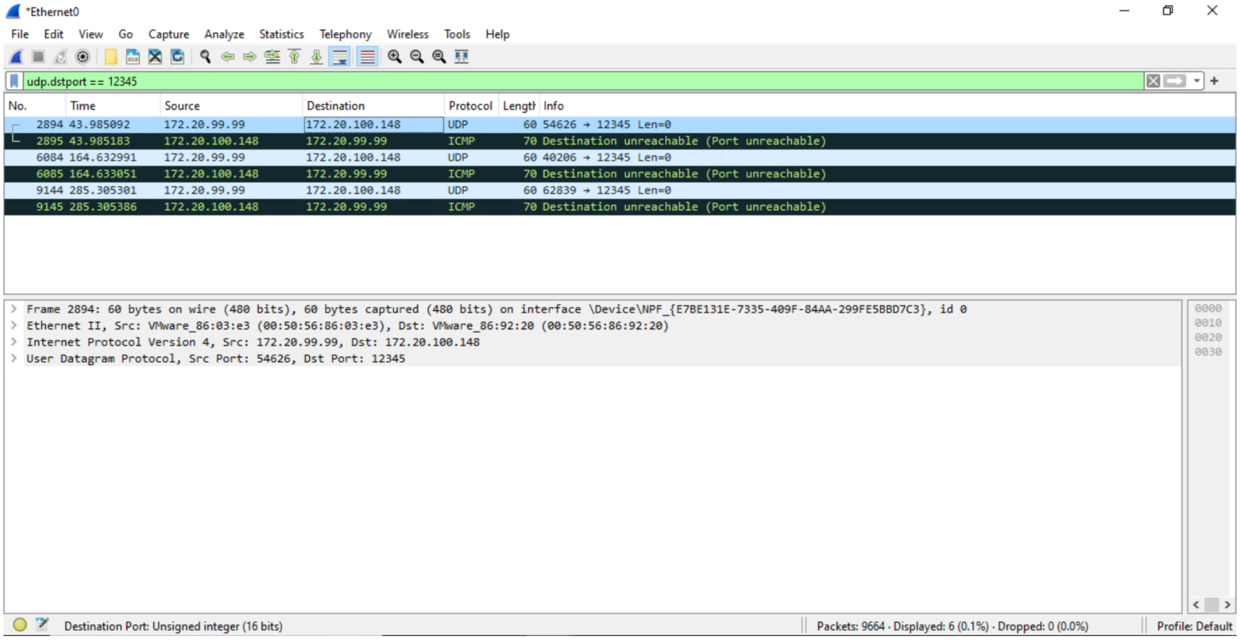
No.	Time	Source	Destination	Protocol	Length	Info
176	14.854459	172.20.87.102	172.20.100.148	TCP	60	51773 → 4321 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2013	25.008322	172.20.87.102	172.20.100.148	TCP	60	52133 → 4321 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3289	135.590755	172.20.87.102	172.20.100.148	TCP	60	58687 → 4321 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3937	144.805074	172.20.87.102	172.20.100.148	TCP	60	48904 → 4321 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6466	256.778582	172.20.87.102	172.20.100.148	TCP	60	52474 → 4321 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7534	265.876549	172.20.87.102	172.20.100.148	TCP	60	65248 → 4321 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9433	377.341661	172.20.87.102	172.20.100.148	TCP	60	51070 → 4321 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

```
> Frame 176: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{E7BE131E-7335-409F-84AA-299FE5BBD7C3}, id 0
> Ethernet II, Src: VMware_86:4f:45 (00:50:56:86:4f:45), Dst: VMware_86:92:20 (00:50:56:86:92:20)
> Internet Protocol Version 4, Src: 172.20.87.102, Dst: 172.20.100.148
> Transmission Control Protocol, Src Port: 51773, Dst Port: 4321, Seq: 0, Len: 0
```

Destination Port: Unsigned integer (16 bits) | Packets: 9664 · Displayed: 7 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

The source IP that is scanning for TCP port 4321 is 172.20.87.102. How I got this is by using the display “tcp.dstport == 4321”. Then I looked under the “Source” tab to find the IP address

Part B


*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.dstport == 12345

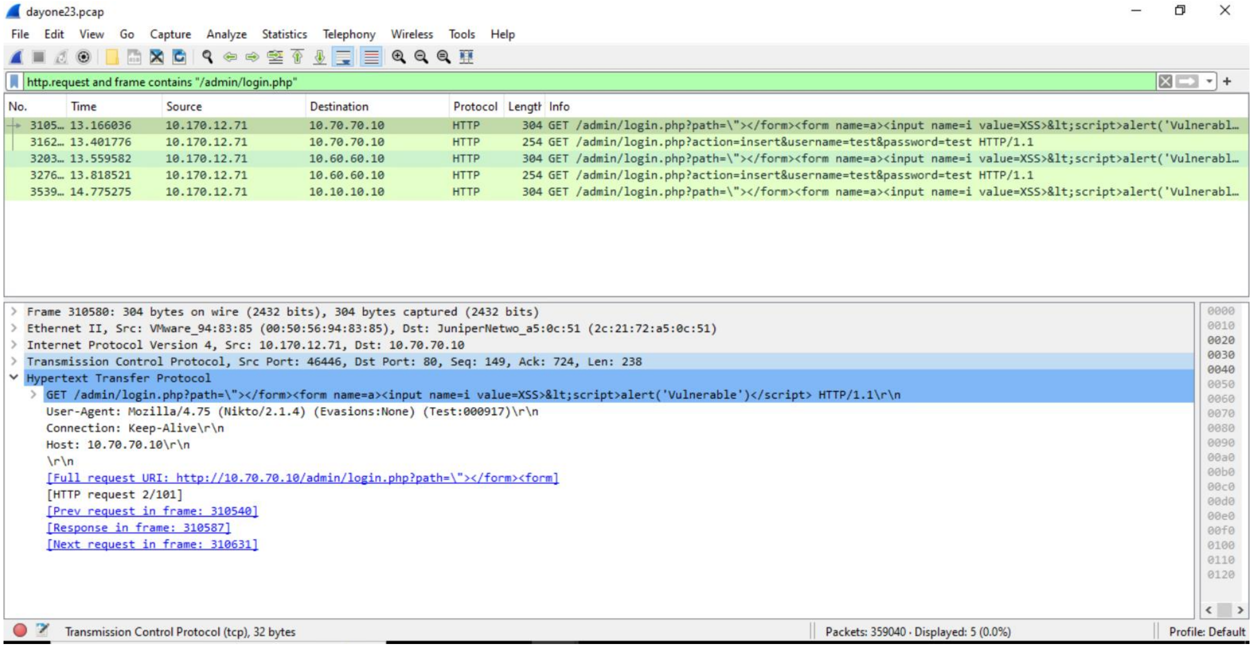
No.	Time	Source	Destination	Protocol	Length	Info
2894	43.985092	172.20.99.99	172.20.100.148	UDP	60	54626 → 12345 Len=0
2895	43.985183	172.20.100.148	172.20.99.99	ICMP	70	Destination unreachable (Port unreachable)
6084	164.632991	172.20.99.99	172.20.100.148	UDP	60	40206 → 12345 Len=0
6085	164.633051	172.20.100.148	172.20.99.99	ICMP	70	Destination unreachable (Port unreachable)
9144	285.305301	172.20.99.99	172.20.100.148	UDP	60	62839 → 12345 Len=0
9145	285.305386	172.20.100.148	172.20.99.99	ICMP	70	Destination unreachable (Port unreachable)

```
> Frame 2894: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{E7BE131E-7335-409F-84AA-299FE5BBD7C3}, id 0
> Ethernet II, Src: VMware_86:03:e3 (00:50:56:86:03:e3), Dst: VMware_86:92:20 (00:50:56:86:92:20)
> Internet Protocol Version 4, Src: 172.20.99.99, Dst: 172.20.100.148
> User Datagram Protocol, Src Port: 54626, Dst Port: 12345
```

Destination Port: Unsigned integer (16 bits) | Packets: 9664 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

The source IP that is scanning for UDP port 12345 is 172.20.99.99. How I got this is by using the display “udp.dstport == 12345”. Then I looked under the “Source” tab to find the IP address. Since there are Two IP addresses I had to inspect each packet which you see from the drop-down list named “User Datagram Protocol”, the destination port is 12345.

BONUS:


dayone23.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request and frame contains "/admin/login.php"
```

```
No.      Time       Source         Destination    Protocol Length Info
3105…  13.166036   10.170.12.71   10.70.70.10    HTTP     304 GET /admin/login.php?path=\"></form><form name=a><input name=i value=XSS>&lt;script>alert('Vulnerabl…
3162…  13.401776   10.170.12.71   10.70.70.10    HTTP     254 GET /admin/login.php?action=insert&username=test&password=test HTTP/1.1
3203…  13.559582   10.170.12.71   10.60.60.10    HTTP     304 GET /admin/login.php?path=\"></form><form name=a><input name=i value=XSS>&lt;script>alert('Vulnerabl…
3276…  13.818521   10.170.12.71   10.60.60.10    HTTP     254 GET /admin/login.php?action=insert&username=test&password=test HTTP/1.1
3539…  14.775275   10.170.12.71   10.10.10.10    HTTP     304 GET /admin/login.php?path=\"></form><form name=a><input name=i value=XSS>&lt;script>alert('Vulnerabl…
```

```
> Frame 310580: 304 bytes on wire (2432 bits), 304 bytes captured (2432 bits)
> Ethernet II, Src: VMware_94:83:85 (00:50:56:94:83:85), Dst: JuniperNetwo_a5:0c:51 (2c:21:72:a5:0c:51)
> Internet Protocol Version 4, Src: 10.170.12.71, Dst: 10.70.70.10
> Transmission Control Protocol, Src Port: 46446, Dst Port: 80, Seq: 149, Ack: 724, Len: 238
v Hypertext Transfer Protocol
  > GET /admin/login.php?path=\"></form><form name=a><input name=i value=XSS>&lt;script>alert('Vulnerable')</script> HTTP/1.1\r\n
    User-Agent: Mozilla/4.75 (Nikto/2.1.4) (Evasions:None) (Test:000917)\r\n
    Connection: Keep-Alive\r\n
    Host: 10.70.70.10\r\n
    \r\n
    [Full request URI: http://10.70.70.10/admin/login.php?path=\"></form><form]
    [HTTP request 2/101]
    [Prev request in frame: 310540]
    [Response in frame: 310587]
    [Next request in frame: 310631]
```

```
0000
0010
0020
0030
0040
0050
0060
0070
0080
0090
00a0
00b0
00c0
00d0
00e0
00f0
0100
0110
0120
```

```
Transmission Control Protocol (tcp), 32 bytes    Packets: 359040 · Displayed: 5 (0.0%)    Profile: Default
```

The source IP scanning multiple webservers for "/admin/login.php" is 10.170.12.71. What I did to obtain this IP address is by using the filter

http.request and frame contains "/admin/login.php"

"http.request" is used to find any requests for a webserver and the "frame contains" finds "/admin/login.php" within the packet

Works Cited

Cohen, Colin. “What is Port 123?” CBT Nuggets, 20 October 2023, https://www.cbtnuggets.com/common-ports/what-is-port-123. Accessed 5 March 2024.

DevX. “Xerox Network Systems.” DevX, 6 September 2023, https://www.devx.com/terms/xerox-network-systems/. Accessed 5 March 2024.

IBM. “Trivial File Transfer Protocol.” IBM, https://www.ibm.com/docs/en/i/7.1?topic=services-trivial-file-transfer-protocol. Accessed 5 March 2024.