

Analysis NMAP scans by potential adversary:

1. Number of TCP Connect is 1000

Wireshark packet capture showing a TCP SYN scan. The filter is `tcp.flags.syn==1 and tcp.flags.ack==0 and tcp.window_size <= 1024`. The packet list shows multiple SYN packets from 10.10.60.7 to 10.10.47.123. Packet 2042 is highlighted, showing a SYN packet to port 80.

No.	Time	Source	Destination	Protocol	Length	Info
2005	153.750287125	10.10.60.7	10.10.47.123	TCP	58	36044 → 445 [SYN]
2006	153.750287215	10.10.60.7	10.10.47.123	TCP	58	36044 → 1723 [SYN]
2007	153.750287365	10.10.60.7	10.10.47.123	TCP	58	36044 → 22 [SYN]
2008	153.750287375	10.10.60.7	10.10.47.123	TCP	58	36044 → 3306 [SYN]
2009	153.750287415	10.10.60.7	10.10.47.123	TCP	58	36044 → 995 [SYN]
2015	153.750366886	10.10.60.7	10.10.47.123	TCP	58	36044 → 111 [SYN]
2017	153.750378427	10.10.60.7	10.10.47.123	TCP	58	36044 → 135 [SYN]
2018	153.750378497	10.10.60.7	10.10.47.123	TCP	58	36044 → 8080 [SYN]
2019	153.750378537	10.10.60.7	10.10.47.123	TCP	58	36044 → 25 [SYN]
2023	153.750394477	10.10.60.7	10.10.47.123	TCP	58	36044 → 8888 [SYN]
2026	153.750676811	10.10.60.7	10.10.47.123	TCP	58	36044 → 143 [SYN]
2027	153.750685211	10.10.60.7	10.10.47.123	TCP	58	36044 → 5900 [SYN]
2028	153.750685281	10.10.60.7	10.10.47.123	TCP	58	36044 → 21 [SYN]
2032	153.750750092	10.10.60.7	10.10.47.123	TCP	58	36044 → 113 [SYN]
2033	153.750750222	10.10.60.7	10.10.47.123	TCP	58	36044 → 1720 [SYN]
2034	153.750750262	10.10.60.7	10.10.47.123	TCP	58	36044 → 53 [SYN]
2035	153.750753442	10.10.60.7	10.10.47.123	TCP	58	36044 → 199 [SYN]
2036	153.750753482	10.10.60.7	10.10.47.123	TCP	58	36044 → 554 [SYN]
2042	153.750818423	10.10.60.7	10.10.47.123	TCP	58	36044 → 80 [SYN]
2043	153.750824043	10.10.60.7	10.10.47.123	TCP	58	36044 → 443 [SYN]
2044	153.750824113	10.10.60.7	10.10.47.123	TCP	58	36044 → 993 [SYN]
2048	153.750879884	10.10.60.7	10.10.47.123	TCP	58	36044 → 139 [SYN]
2049	153.750882514	10.10.60.7	10.10.47.123	TCP	58	36044 → 1025 [SYN]
2050	153.750882564	10.10.60.7	10.10.47.123	TCP	58	36044 → 3389 [SYN]
2054	153.750953255	10.10.60.7	10.10.47.123	TCP	58	36044 → 110 [SYN]
2055	153.750953355	10.10.60.7	10.10.47.123	TCP	58	36044 → 256 [SYN]
2056	153.750953395	10.10.60.7	10.10.47.123	TCP	58	36044 → 587 [SYN]

Frame 2005: 58 bytes on wire (464 bits), 58 bytes captured on interface 0:00:00:00:00:00. Ethernet II, Src: 02:6d:30:b1:b9:69 (02:6d:30:b1:b9:69), Internet Protocol Version 4, Src: 10.10.60.7, Dst: 10.10.47.123, Transmission Control Protocol, Src Port: 36044, Dst Port: 445.

2. The type is used to scan the TCP port 80 and it's a open TCP port connection because of the full handshake

Wireshark packet capture showing a TCP port scan. The filter is `tcp.port==80`. The packet list shows a full TCP handshake sequence for port 80, including SYN, SYN-ACK, and ACK packets.

No.	Time	Source	Destination	Protocol	Length	Info
23	153.750818423	10.10.60.7	10.10.47.123	TCP	74	42026 → 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1
23	153.750818423	10.10.47.123	10.10.60.7	TCP	74	80 → 42026 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM=1
23	153.750818423	10.10.47.123	10.10.47.123	TCP	66	42026 → 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=1438484202
23	153.750818423	10.10.47.123	10.10.47.123	TCP	66	42026 → 80 [RST, ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=1438484202
23	153.750818423	10.10.47.123	10.10.47.123	TCP	58	36044 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	153.750818423	10.10.60.7	10.10.47.123	TCP	58	80 → 36044 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=8961 SACK_PERM=1
23	153.750818423	10.10.47.123	10.10.47.123	TCP	54	36044 → 80 [RST] Seq=1 Win=0 Len=0

3. The number of sys pacakets by the syn scan is 1000

tcp.flags.syn==1 and tcp.flags.ack==0 and tcp.window_size <= 1024

Time	Source	Destination	Protocol	Length	Info
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 1 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 100 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 1000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 10000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 10001 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 10002 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 10003 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 10004 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 10009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 1001 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 10010 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 10012 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 1002 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 10024 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 10025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 1007 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 10082 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 1010 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 1011 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 10180 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
0.000000	10.10.60.7	10.10.10.1	TCP	58	36044 → 1021 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Frame 2241: 58 bytes on wire (464 bits), 58 bytes capture
 Ethernet II, Src: 02:6d:30:b1:b9:69 (02:6d:30:b1:b9:69),
 Internet Protocol Version 4, Src: 10.10.60.7, Dst: 10.10.10.1,
 Transmission Control Protocol, Src Port: 36044, Dst Port: 10000

0000 02 46 92 ec ed bd 02 6d 30 b1 b9 69
 0010 00 2c 93 47 00 00 35 06 72 ef 0a 0a
 0020 2f 7b 8c cc 25 92 e5 48 41 32 00 00
 0030 04 00 3b b7 00 00 02 04 05 b4

Exercise.pcapng Packets: 6544 · Displayed: 1000 (15.3%) Profile: Default

=====+

ARP poisoning and MITM:

Scenario: The work is divided among your teammates and your teammates found some evidence of a potential attacker. Here is what they found.

Detection Notes	Findings	
IP to MAC matches.	3 IP to MAC address matches.	<ul style="list-style-type: none"> MAC: 00:0c:29:e2:18:b4 = IP: 192.168.1.25 MAC: 50:78:b3:f3:cd:f4 = IP: 192.168.1.1 MAC: 00:0c:29:98:c7:a8 = IP: 192.168.1.12
Attacker	The attacker created noise with ARP packets.	<ul style="list-style-type: none"> MAC: 00:0c:29:e2:18:b4 = IP: 192.168.1.25
Router/gateway	Gateway address.	<ul style="list-style-type: none"> MAC: 50:78:b3:f3:cd:f4 = IP: 192.168.1.1
Victim	The attacker sniffed all traffic of the victim.	<ul style="list-style-type: none"> MAC: 50:78:b3:f3:cd:f4 = IP: 192.168.1.12

What is the number of ARP requests crafted by the attacker? It's 284 packets.

eth.src==00:0c:29:e2:18:b4 and arp.opcode==1

No.	Time	Source	Destination	Protocol	Length	Info
3	17.626854996	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
5	17.637345249	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
6	17.647731835	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
7	17.658130017	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
8	17.668703449	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
9	17.679601294	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
10	17.690243597	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
11	17.700760790	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
12	17.711256788	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
13	17.721858036	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
14	17.732272555	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
15	17.742493934	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
16	17.752775894	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
17	17.763563411	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
18	17.774149379	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
19	17.784781470	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
20	17.795271846	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
21	17.805791112	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
22	17.816308046	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
23	17.826813382	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
24	17.837292051	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1
25	17.847816978	VMware_e2:18:b4	Broadcast	ARP	42	Who has 192.168.1.1

Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: VMware_e2:18:b4 (00:0c:29:e2:18:b4), Dst: 01:00:5e:00:00:00
Address Resolution Protocol (request)

```
0000  ff ff ff ff ff ff 00 0c 29 e2 18 b4
0010  08 00 06 04 00 01 00 0c 29 e2 18 b4
0020  00 00 00 00 00 00 00 c0 a8 01 01
```

Exercise.pcapng Packets: 2866 · Displayed: 284 (9.9%) Profile: Default

What is the number of HTTP packets received by the attacker? It's 90 packets

The image shows a Wireshark packet capture interface. The top toolbar includes icons for file operations, network analysis, and display filters. The display filter bar at the top shows 'eth.dst==00:0c:29:e2:18:b4 and http'. The packet list pane displays a table of captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
1107	107.294748849	192.168.1.12	44.228.249.3	HTTP	509	GET /login.ph
1116	107.524664472	44.228.249.3	192.168.1.12	HTTP	1350	HTTP/1.1 200
1122	107.544502796	192.168.1.12	44.228.249.3	HTTP	420	GET /style.cs
1123	107.546558129	192.168.1.12	44.228.249.3	HTTP	461	GET /images/lo
1137	107.767662150	44.228.249.3	192.168.1.12	HTTP	906	HTTP/1.1 200
1143	107.768836318	44.228.249.3	192.168.1.12	HTTP	1180	HTTP/1.1 200
1167	107.856353223	192.168.1.12	44.228.249.3	HTTP	457	GET /favicon.
1217	108.088537576	44.228.249.3	192.168.1.12	HTTP	948	HTTP/1.1 200
1226	112.878779336	192.168.1.12	44.228.249.3	HTTP	711	POST /userinfo
1232	113.105809063	44.228.249.3	192.168.1.12	HTTP	60	HTTP/1.1 200
1272	128.722212965	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo
1275	128.953703403	44.228.249.3	192.168.1.12	HTTP	1488	HTTP/1.1 200
1280	130.293866830	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo
1283	130.519826760	44.228.249.3	192.168.1.12	HTTP	1488	HTTP/1.1 200
1288	134.047286876	192.168.1.12	44.228.249.3	HTTP	587	GET /logout.pl
1291	134.271756279	44.228.249.3	192.168.1.12	HTTP	1180	HTTP/1.1 200
1298	136.609621027	192.168.1.12	44.228.249.3	HTTP	557	GET /login.ph
1301	136.829973665	44.228.249.3	192.168.1.12	HTTP	1350	HTTP/1.1 200
1306	137.855933795	192.168.1.12	44.228.249.3	HTTP	557	GET /signup.pl
1309	138.076887087	44.228.249.3	192.168.1.12	HTTP	1410	HTTP/1.1 200
1381	187.285689649	192.168.1.12	44.228.249.3	HTTP	849	POST /secured
1387	187.509053286	44.228.249.3	192.168.1.12	HTTP	844	HTTP/1.1 200

The packet details pane for the selected packet (No. 1107) shows the following structure:

- Frame 1107: 509 bytes on wire (4072 bits), 509 bytes captured
- Ethernet II, Src: VMware_98:c7:a8 (00:0c:29:98:c7:a8), Dst: 00:0c:29:e2:18:b4
- Internet Protocol Version 4, Src: 192.168.1.12, Dst: 44.228.249.3
- Transmission Control Protocol, Src Port: 49915, Dst Port: 80
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII format.

At the bottom, the status bar indicates: Packets: 2866 - Displayed: 90 (3.1%) Profile: Default

What is the number of sniffed username&password entries? Followed the HTTP stream and found vulnerable web FQDN and the 6 accounts were sniffed.

File Edit View

tcp.stream eq 4

No. Time

1100 107.06
1101 107.07
1104 107.29
1105 107.29
1106 107.29
1107 107.29
1108 107.36
1109 107.36
1114 107.52
1115 107.52
1116 107.52
1117 107.52
1118 107.52
1119 107.52
1120 107.52
1121 107.53
1122 107.54
1124 107.55
1138 107.76
1139 107.76
1140 107.76
1141 107.76

Frame 1107: Ethernet II, Internet Protocol, Transmission Control Protocol, Hypertext Transfer Protocol

GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.124 Safari/537.36
Edg/102.0.1245.44
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Tue, 21 Jun 2022 14:53:56 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBeginEditable name="/Templates/
main_dynamic_template.dwt.php" codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4
resized
if (init==true) with (navigator) {if
((document.location.protocol != "https:") && !navigator.isSecure()) {
document.location.reload(true);
}}
</script>

14 client pkt(s), 14 server pkt(s), 27 turn(s).

Entire conversation (74 kB) Show and save data as ASCII

Find: Find Next

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

http.host == testphp.vulnweb.com and http.request.method == "POST"

No. Time Source Destination Protocol Length Info

1226 112.878779336 192.168.1.12 44.228.249.3 HTTP 711 POST /userinfo.php
1272 128.722212965 192.168.1.12 44.228.249.3 HTTP 825 POST /userinfo.php
1280 130.293866830 192.168.1.12 44.228.249.3 HTTP 825 POST /userinfo.php
1381 187.285689649 192.168.1.12 44.228.249.3 HTTP 849 POST /secured/newus
1446 207.138156489 192.168.1.12 44.228.249.3 HTTP 726 POST /userinfo.php
1561 294.110756210 192.168.1.12 44.228.249.3 HTTP 722 POST /userinfo.php
1599 334.960960385 192.168.1.12 44.228.249.3 HTTP 726 POST /userinfo.php
1668 354.682038726 192.168.1.12 44.228.249.3 HTTP 728 POST /userinfo.php
1791 443.146852729 192.168.1.12 44.228.249.3 HTTP 726 POST /userinfo.php
2320 618.814163954 192.168.1.12 44.228.249.3 HTTP 787 POST /comment.php H

Frame 1226: 711 bytes on wire (5688 bits), 711 bytes captured on interface 0, from 192.168.1.12 to 44.228.249.3 on interface 0
Ethernet II, Src: VMware_98:c7:a8 (00:0c:29:98:c7:a8), Dst: 44:228:249:3
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 49915, Dst Port: 80
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "test"
Key: uname
Value: test
Form item: "pass" = "test"
Key: pass
Value: test

0000 00 0c 29 e2 18 b4 00 0c 29 98 c7 a8
0010 02 b9 40 c9 40 00 80 06 cf d9 c0 a8
0020 f9 03 c2 fb 00 50 06 90 7a a0 2c 7f
0030 04 02 d4 b2 00 00 50 4f 53 54 20 2f
0040 69 6e 66 6f 2e 70 68 70 20 48 54 5f
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 7f
0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6f
0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 6f
0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6f
0090 6e 67 74 68 3a 20 32 30 0d 0a 43 6f
00a0 43 6f 6e 74 72 6f 6c 3a 20 6d 61 7f
00b0 3d 30 0d 0a 55 70 67 72 61 64 65 2f
00c0 63 75 72 65 2d 52 65 71 75 65 73 7f
00d0 0d 0a 4f 72 69 67 69 6e 3a 20 68 7f
00e0 2f 74 65 73 74 70 68 70 2e 76 75 6f
00f0 2e 63 6f 6d 0d 0a 43 6f 6e 74 65 6f
0100 70 65 3a 20 61 70 70 6c 69 63 61 7f
0110 78 2d 77 77 72 6d 66 6f 72 6d 2d 7f
0120 63 6f 64 65 64 0d 0a 55 73 65 72 2f
0130 74 20 20 4d 6f 6f 6f 6f 6f 6f 6f 6f

Exercise.pcapng Packets: 2866 · Displayed: 10 (0.3%) Profile: Default

No.	Time	Source	Destination	Protocol	Length	Info
1226	112.878779336	192.168.1.12	44.228.249.3	HTTP	711	POST /userinfo.php
1272	128.722212965	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1280	130.293866830	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1381	187.285689649	192.168.1.12	44.228.249.3	HTTP	849	POST /secured/newus
1446	207.138156489	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1561	294.110756210	192.168.1.12	44.228.249.3	HTTP	722	POST /userinfo.php
1599	334.960960385	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1668	354.682038726	192.168.1.12	44.228.249.3	HTTP	728	POST /userinfo.php
1791	443.146852729	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
2320	618.814163954	192.168.1.12	44.228.249.3	HTTP	787	POST /comment.php

Frame 1446: 726 bytes on wire (5808 bits), 726 bytes captured on interface 0 (eth0) from 192.168.1.12 to 44.228.249.3 on interface 0 (eth0)		Ethernet II, Src: VMWare_98:c7:a8 (00:0c:29:98:c7:a8), Dst: 44.228.249.3		Internet Protocol Version 4, Src: 192.168.1.12, Dst: 44.228.249.3		Transmission Control Protocol, Src Port: 49915, Dst Port: 80		Hypertext Transfer Protocol		HTML Form URL Encoded: application/x-www-form-urlencoded		Form item: "uname" = "test_THM_test"		Key: uname		Value: test_THM_test		Form item: "pass" = "insecurepw"		Key: pass		Value: insecurepw		0000 00 0c 29 e2 18 b4 00 0c 29 98 c7 a8		0010 02 c8 40 e0 40 00 80 06 cf b3 c0 a8		0020 f9 03 c2 fb 00 50 06 90 85 d5 2c 70		0030 04 02 ab 4b 00 00 50 4f 53 54 20 2f		0040 69 6e 66 6f 2e 70 68 70 20 48 54 55		0050 31 0d 0a 48 6f 73 74 3a 20 74 65 77		0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d		0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 6d		0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6d		0090 6e 67 74 68 3a 20 33 35 0d 0a 43 6f		00a0 43 6f 6e 74 72 6f 6c 3a 20 6d 61 77		00b0 3d 30 0d 0a 55 70 67 72 61 64 65 20		00c0 63 75 72 65 2d 52 65 71 75 65 73 77		00d0 0d 0a 4f 72 69 67 69 6e 3a 20 68 77		00e0 2f 74 65 73 74 70 68 70 2e 76 75 6d		00f0 2e 63 6f 6d 0d 0a 43 6f 6e 74 65 6d		0100 70 65 3a 20 61 70 70 6c 69 63 61 77		0110 78 2d 77 77 77 2d 66 6f 72 6d 2d 77		0120 63 6f 64 65 64 0d 0a 55 73 65 72 2f	
---	--	--	--	---	--	--	--	-----------------------------	--	--	--	--------------------------------------	--	------------	--	----------------------	--	----------------------------------	--	-----------	--	-------------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

1226	112.878779336	192.168.1.12	44.228.249.3	HTTP	711	POST /userinfo.php
1272	128.722212965	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1280	130.293866830	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1381	187.285689649	192.168.1.12	44.228.249.3	HTTP	849	POST /secured/newus
1446	207.138156489	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1561	294.110756210	192.168.1.12	44.228.249.3	HTTP	722	POST /userinfo.php
1599	334.960960385	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1668	354.682038726	192.168.1.12	44.228.249.3	HTTP	728	POST /userinfo.php
1791	443.146852729	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
2320	618.814163954	192.168.1.12	44.228.249.3	HTTP	787	POST /comment.php

Frame 1561: 722 bytes on wire (5776 bits), 722 bytes captured on interface 0 (eth0) from 192.168.1.12 to 44.228.249.3 on interface 0 (eth0)		Ethernet II, Src: VMWare_98:c7:a8 (00:0c:29:98:c7:a8), Dst: 44.228.249.3		Internet Protocol Version 4, Src: 192.168.1.12, Dst: 44.228.249.3		Transmission Control Protocol, Src Port: 49918, Dst Port: 80		Hypertext Transfer Protocol		HTML Form URL Encoded: application/x-www-form-urlencoded		Form item: "uname" = "admin"		Key: uname		Value: admin		Form item: "pass" = "supersecret!"		Key: pass		Value: supersecret!		0000 00 0c 29 e2 18 b4 00 0c 29 98 c7 a8		0010 02 c4 40 e8 40 00 80 06 cf af c0 a8		0020 f9 03 c2 fe 00 50 d4 6e 9c dd d8 90		0030 04 02 a7 5c 00 00 50 4f 53 54 20 2f		0040 69 6e 66 6f 2e 70 68 70 20 48 54 55		0050 31 0d 0a 48 6f 73 74 3a 20 74 65 77		0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d		0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 6d		0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6d		0090 6e 67 74 68 3a 20 33 31 0d 0a 43 6f		00a0 43 6f 6e 74 72 6f 6c 3a 20 6d 61 77		00b0 3d 30 0d 0a 55 70 67 72 61 64 65 20		00c0 63 75 72 65 2d 52 65 71 75 65 73 77	
---	--	--	--	---	--	--	--	-----------------------------	--	--	--	------------------------------	--	------------	--	--------------	--	------------------------------------	--	-----------	--	---------------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

1226	112.878779336	192.168.1.12	44.228.249.3	HTTP	711	POST	/userinfo.php
1272	128.722212965	192.168.1.12	44.228.249.3	HTTP	825	POST	/userinfo.php
1280	130.293866830	192.168.1.12	44.228.249.3	HTTP	825	POST	/userinfo.php
1381	187.285689649	192.168.1.12	44.228.249.3	HTTP	849	POST	/secured/newu
1446	207.138156489	192.168.1.12	44.228.249.3	HTTP	726	POST	/userinfo.php
1561	294.110756210	192.168.1.12	44.228.249.3	HTTP	722	POST	/userinfo.php
1599	334.960960385	192.168.1.12	44.228.249.3	HTTP	726	POST	/userinfo.php
1668	354.682038726	192.168.1.12	44.228.249.3	HTTP	728	POST	/userinfo.php
1791	443.146852729	192.168.1.12	44.228.249.3	HTTP	726	POST	/userinfo.php
2320	618.814163954	192.168.1.12	44.228.249.3	HTTP	787	POST	/comment.php

Frame 1599: 726 bytes on wire (5808 bits), 726 bytes captured on interface 0, 726 bytes from 192.168.1.12 to 44.228.249.3 on interface 0				0000 00 0c 29 e2 18 b4 00 0c 29 98 c7 a1 2e 00 00 00			
Ethernet II, Src: VMware_98:c7:a8 (00:0c:29:98:c7:a8), Dst: 44:228:249:3 (00:0c:29:98:c7:a8)				0010 02 c8 40 eb 40 00 80 06 cf a8 c0 a1 2e 00 00 00			
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 44.228.249.3				0020 f9 03 c2 fe 00 50 d4 6e a1 89 d8 90 20 48 54 55			
Transmission Control Protocol, Src Port: 49918, Dst Port: 80				0030 04 02 e0 53 00 00 50 4f 53 54 20 20 48 54 55			
Hypertext Transfer Protocol				0040 69 6e 66 6f 2e 70 68 70 20 48 54 55 20 48 54 55			
HTML Form URL Encoded: application/x-www-form-urlencoded				0050 31 0d 0a 48 6f 73 74 3a 20 74 65 74 65 74 65 74			
Form item: "uname" = "client468"				0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 65 63 6f 6d			
Key: uname				0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 6d 65 63 6f 6d			
Value: client468				0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6d 65 63 6f 6d			
Form item: "pass" = "premiumsoda-_-"				0090 6e 67 74 68 3a 20 33 35 0d 0a 43 6f 6d 65 63 6f 6d			
Key: pass				00a0 43 6f 6e 74 72 6f 6c 3a 20 6d 61 74 65 63 6f 6d			
Value: premiumsoda-_-				00b0 3d 30 0d 0a 55 70 67 72 61 64 65 20 6d 61 74 65 20			
				00c0 63 75 72 65 2d 52 65 71 75 65 73 74 65 63 74 65			
				00d0 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 65 63 74 65			
				00e0 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 65 63 6f 6d			

No.	Time	Source	Destination	Protocol	Length	Info
1226	112.878779336	192.168.1.12	44.228.249.3	HTTP	711	POST /userinfo.php
1272	128.722212965	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1280	130.293866830	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1381	187.285689649	192.168.1.12	44.228.249.3	HTTP	849	POST /secured/newu
1446	207.138156489	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1561	294.110756210	192.168.1.12	44.228.249.3	HTTP	722	POST /userinfo.php
1599	334.960960385	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1668	354.682038726	192.168.1.12	44.228.249.3	HTTP	728	POST /userinfo.php
1791	443.146852729	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
2320	618.814163954	192.168.1.12	44.228.249.3	HTTP	787	POST /comment.php

Frame 1668: 728 bytes on wire (5824 bits), 728 bytes captured on interface 0, 728 bytes from 192.168.1.12 to 44.228.249.3 on interface 0				0000 00 0c 29 e2 18 b4 00 0c 29 98 c7 a1 2e 00 00 00			
Ethernet II, Src: VMware_98:c7:a8 (00:0c:29:98:c7:a8), Dst: 44:228:249:3 (00:0c:29:98:c7:a8)				0010 02 ca 40 ee 40 00 80 06 cf a3 c0 a1 2e 00 00 00			
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 44.228.249.3				0020 f9 03 c2 fe 00 50 d4 6e a6 39 d8 90 20 48 54 55			
Transmission Control Protocol, Src Port: 49918, Dst Port: 80				0030 04 02 8f 6d 00 00 50 4f 53 54 20 20 48 54 55			
Hypertext Transfer Protocol				0040 69 6e 66 6f 2e 70 68 70 20 48 54 55 20 48 54 55			
HTML Form URL Encoded: application/x-www-form-urlencoded				0050 31 0d 0a 48 6f 73 74 3a 20 74 65 74 65 74 65 74			
Form item: "uname" = "client986"				0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 65 63 6f 6d			
Key: uname				0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 6d 65 63 6f 6d			
Value: client986				0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6d 65 63 6f 6d			
Form item: "pass" = "clientnothere!"				0090 6e 67 74 68 3a 20 33 37 0d 0a 43 6f 6d 65 63 6f 6d			
Key: pass				00a0 43 6f 6e 74 72 6f 6c 3a 20 6d 61 74 65 63 6f 6d			
Value: clientnothere!				00b0 3d 30 0d 0a 55 70 67 72 61 64 65 20 6d 61 74 65 20			
				00c0 63 75 72 65 2d 52 65 71 75 65 73 74 65 63 74 65			

1226	112.878779336	192.168.1.12	44.228.249.3	HTTP	711	POST	/userinfo.php
1272	128.722212965	192.168.1.12	44.228.249.3	HTTP	825	POST	/userinfo.php
1280	130.293866830	192.168.1.12	44.228.249.3	HTTP	825	POST	/userinfo.php
1381	187.285689649	192.168.1.12	44.228.249.3	HTTP	849	POST	/secured/newu
1446	207.138156489	192.168.1.12	44.228.249.3	HTTP	726	POST	/userinfo.php
1561	294.110756210	192.168.1.12	44.228.249.3	HTTP	722	POST	/userinfo.php
1599	334.960960385	192.168.1.12	44.228.249.3	HTTP	726	POST	/userinfo.php
1668	354.682038726	192.168.1.12	44.228.249.3	HTTP	728	POST	/userinfo.php
1791	443.146852729	192.168.1.12	44.228.249.3	HTTP	726	POST	/userinfo.php
2320	618.814163954	192.168.1.12	44.228.249.3	HTTP	787	POST	/comment.php

Frame 1791: 726 bytes on wire (5808 bits), 726 bytes captured on interface 0 (eth0): Ethernet II, Src: VMware_98:c7:a8 (00:0c:29:98:c7:a8), Dst: 44:22:82:24:93:03, Protocol: HTTP, Src Port: 49921, Dst Port: 80				0000	00	0c	29	e2	18	b4	00	0c	29	98	c7	a8
Ethernet II, Src: VMware_98:c7:a8 (00:0c:29:98:c7:a8), Dst: 44:22:82:24:93:03, Protocol: HTTP, Src Port: 49921, Dst Port: 80				0010	02	c8	40	f6	40	00	80	06	cf	9d	c0	a8
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 44.228.249.3				0020	f9	03	c3	01	00	50	9a	69	5c	c8	3b	f9
Transmission Control Protocol, Src Port: 49921, Dst Port: 80				0030	04	02	b7	d4	00	00	50	4f	53	54	20	20
Hypertext Transfer Protocol				0040	69	6e	66	6f	2e	70	68	70	20	48	54	55
HTML Form URL Encoded: application/x-www-form-urlencoded				0050	31	0d	0a	48	6f	73	74	3a	20	74	65	77
Form item: "uname" = "tourist-audt"				0060	2e	76	75	6c	6e	77	65	62	2e	63	6f	66
Key: uname				0070	6e	6e	65	63	74	69	6f	6e	3a	20	6b	66
Value: tourist-audt				0080	6c	69	76	65	0d	0a	43	6f	6e	74	65	66
Form item: "pass" = "captainciso"				0090	6e	67	74	68	3a	20	33	35	0d	0a	43	66
Key: pass				00a0	43	6f	6e	74	72	6f	6c	3a	20	6d	61	77
Value: captainciso				00b0	3d	30	0d	0a	55	70	67	72	61	64	65	20
				00c0	63	75	72	65	2d	52	65	71	75	65	73	77
				00d0	0d	0a	4f	72	69	67	69	6e	3a	20	68	77

What is the password of the "Client986"? It's clientnothere!

1226	112.878779336	192.168.1.12	44.228.249.3	HTTP	711	POST	/userinfo.php
1272	128.722212965	192.168.1.12	44.228.249.3	HTTP	825	POST	/userinfo.php
1280	130.293866830	192.168.1.12	44.228.249.3	HTTP	825	POST	/userinfo.php
1381	187.285689649	192.168.1.12	44.228.249.3	HTTP	849	POST	/secured/newu
1446	207.138156489	192.168.1.12	44.228.249.3	HTTP	726	POST	/userinfo.php
1561	294.110756210	192.168.1.12	44.228.249.3	HTTP	722	POST	/userinfo.php
1599	334.960960385	192.168.1.12	44.228.249.3	HTTP	726	POST	/userinfo.php
1668	354.682038726	192.168.1.12	44.228.249.3	HTTP	728	POST	/userinfo.php
1791	443.146852729	192.168.1.12	44.228.249.3	HTTP	726	POST	/userinfo.php
2320	618.814163954	192.168.1.12	44.228.249.3	HTTP	787	POST	/comment.php

Frame 1668: 728 bytes on wire (5824 bits), 728 bytes captured on interface 0 (eth0): Ethernet II, Src: VMware_98:c7:a8 (00:0c:29:98:c7:a8), Dst: 44:22:82:24:93:03, Protocol: HTTP, Src Port: 49918, Dst Port: 80				0000	00	0c	29	e2	18	b4	00	0c	29	98	c7	a8
Ethernet II, Src: VMware_98:c7:a8 (00:0c:29:98:c7:a8), Dst: 44:22:82:24:93:03, Protocol: HTTP, Src Port: 49918, Dst Port: 80				0010	02	ca	40	ee	40	00	80	06	cf	a3	c0	a8
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 44.228.249.3				0020	f9	03	c2	fe	00	50	d4	6e	a6	39	d8	91
Transmission Control Protocol, Src Port: 49918, Dst Port: 80				0030	04	02	8f	6d	00	00	50	4f	53	54	20	20
Hypertext Transfer Protocol				0040	69	6e	66	6f	2e	70	68	70	20	48	54	55
HTML Form URL Encoded: application/x-www-form-urlencoded				0050	31	0d	0a	48	6f	73	74	3a	20	74	65	77
Form item: "uname" = "client986"				0060	2e	76	75	6c	6e	77	65	62	2e	63	6f	66
Key: uname				0070	6e	6e	65	63	74	69	6f	6e	3a	20	6b	66
Value: client986				0080	6c	69	76	65	0d	0a	43	6f	6e	74	65	66
Form item: "pass" = "clientnothere!"				0090	6e	67	74	68	3a	20	33	37	0d	0a	43	66
Key: pass				00a0	43	6f	6e	74	72	6f	6c	3a	20	6d	61	77
Value: clientnothere!				00b0	3d	30	0d	0a	55	70	67	72	61	64	65	20
				00c0	63	75	72	65	2d	52	65	71	75	65	73	77

What is the comment provided by the "Client354"? The message is nice work!

1226	112.878779336	192.168.1.12	44.228.249.3	HTTP	711 POST /userinfo.php
1272	128.722212965	192.168.1.12	44.228.249.3	HTTP	825 POST /userinfo.php
1280	130.293866830	192.168.1.12	44.228.249.3	HTTP	825 POST /userinfo.php
1381	187.285689649	192.168.1.12	44.228.249.3	HTTP	849 POST /secured/new
1446	207.138156489	192.168.1.12	44.228.249.3	HTTP	726 POST /userinfo.php
1561	294.110756210	192.168.1.12	44.228.249.3	HTTP	722 POST /userinfo.php
1599	334.960960385	192.168.1.12	44.228.249.3	HTTP	726 POST /userinfo.php
1668	354.682038726	192.168.1.12	44.228.249.3	HTTP	728 POST /userinfo.php
1791	443.146852729	192.168.1.12	44.228.249.3	HTTP	726 POST /userinfo.php
+	2320	618.814163954	192.168.1.12	HTTP	787 POST /comment.php



<ul style="list-style-type: none"> ▶ Frame 2320: 787 bytes on wire (6296 bits), 787 bytes captured ▶ Ethernet II, Src: VMware_98:c7:a8 (00:0c:29:98:c7:a8), Dst: 44.228.249.3 ▶ Internet Protocol Version 4, Src: 192.168.1.12, Dst: 44.228.249.3 ▶ Transmission Control Protocol, Src Port: 49927, Dst Port: 80 ▶ Hypertext Transfer Protocol ▼ HTML Form URL Encoded: application/x-www-form-urlencoded <ul style="list-style-type: none"> ▼ Form item: "name" = "client354" <ul style="list-style-type: none"> Key: name Value: client354 ▼ Form item: "comment" = "Nice work!" <ul style="list-style-type: none"> Key: comment Value: Nice work! ▼ Form item: "Submit" = "Submit" <ul style="list-style-type: none"> Key: Submit Value: Submit ▼ Form item: "phpaction" = "echo \$_POST[comment];" <ul style="list-style-type: none"> Key: phpaction Value: echo \$_POST[comment]; 		0200 62 70 2c 69 6d 61 67 65 2f 61 70 61 67 65 61 67 65 2f 61 70 61 67 65 0210 2a 3b 71 3d 30 2e 38 2c 61 70 70 61 67 65 61 67 65 2f 61 70 61 67 65 0220 69 6f 6e 2f 73 69 67 6e 65 64 2d 61 67 65 61 67 65 2f 61 70 61 67 65 0230 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 38 2c 61 70 70 61 67 65 0240 52 65 66 65 72 65 72 3a 20 68 74 70 61 67 65 61 67 65 2f 61 70 61 67 65 0250 74 65 73 74 70 68 70 2e 76 75 6c 61 67 65 61 67 65 2f 61 70 61 67 65 0260 63 6f 6d 2f 63 6f 6d 6d 65 6e 74 20 61 67 65 61 67 65 2f 61 70 61 67 65 0270 70 69 64 3d 37 0d 0a 41 63 63 65 70 61 67 65 61 67 65 2f 61 70 61 67 65 0280 63 6f 64 69 6e 67 3a 20 67 7a 69 70 61 67 65 61 67 65 2f 61 70 61 67 65 0290 66 6c 61 74 65 0d 0a 41 63 63 65 70 61 67 65 61 67 65 2f 61 70 61 67 65 02a0 6e 67 75 61 67 65 3a 20 65 6e 2d 5d 61 67 65 61 67 65 2f 61 70 61 67 65 02b0 3b 71 3d 30 2e 39 0d 0a 0d 0a 6e 61 67 65 61 67 65 2f 61 70 61 67 65 02c0 6c 69 65 6e 74 33 35 34 26 63 6f 61 67 65 61 67 65 2f 61 70 61 67 65 02d0 3d 4e 69 63 65 2b 77 6f 72 6b 25 30 2e 38 2c 61 70 70 61 67 65 02e0 62 6d 69 74 3d 53 75 62 6d 69 74 20 61 67 65 61 67 65 2f 61 70 61 67 65 02f0 63 74 69 6f 6e 3d 65 63 68 6f 2b 20 61 67 65 61 67 65 2f 61 70 61 67 65 0300 4f 53 54 25 35 42 63 6f 6d 6d 65 61 67 65 61 67 65 2f 61 70 61 67 65 0310 25 33 42
---	--	--