

Week 1: Reconnaissance, Information Gathering, and Scanning

INT302: Kali Linux Tools and System Security – Lab 4: Basic Port Scanning

Lab Steps

Step 1: Gather the IP Address of Your OWASP VM

Record the IP Address:

- OWASP VM IP Address: _____

You can access the web apps at <http://192.168.63.129/>

You can administer / configure this machine through the console here, by SSHing to 192.168.63.129, via Samba at \\192.168.63.129\\, or via phpmyadmin at <http://192.168.63.129/phpmyadmin>.

In all these cases, you can use username "root" and password "owaspbwa".

```
root@owaspbwa:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:59:62:f3
          inet addr:192.168.63.129  Bcast:192.168.63.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe59:62f3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:33 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3710 (3.7 KB)  TX bytes:11321 (11.3 KB)
          Interrupt:18 Base address:0x1400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:132 errors:0 dropped:0 overruns:0 frame:0
          TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:28673 (28.6 KB)  TX bytes:28673 (28.6 KB)

root@owaspbwa:~#
```

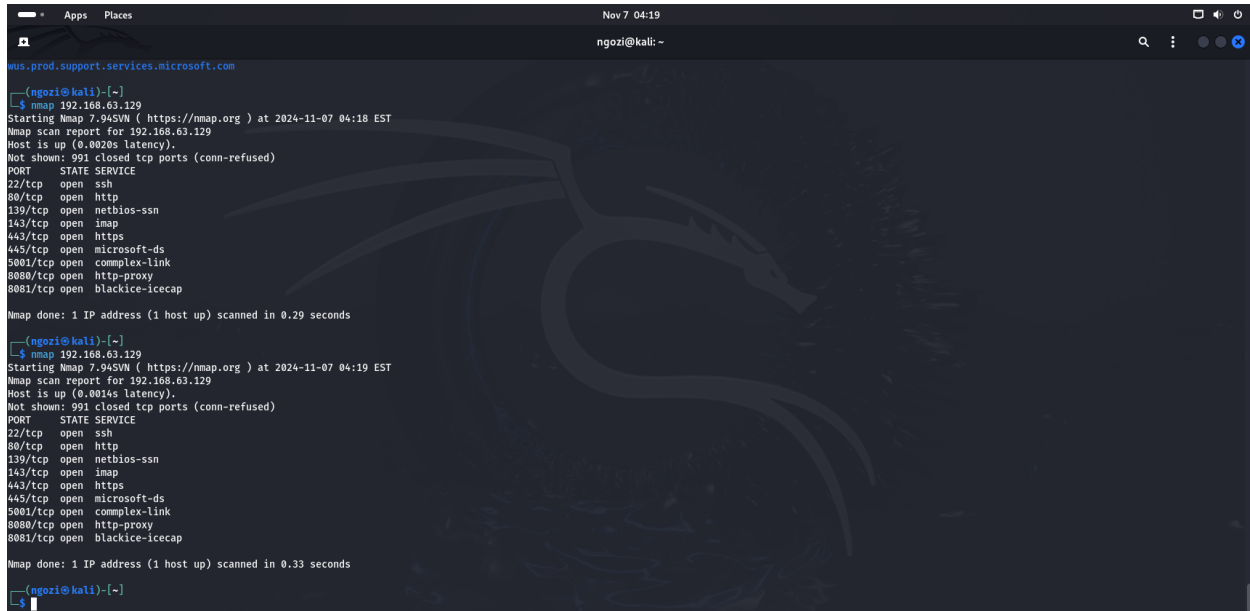
My OWASP VM IP Address is 192.168.63.129

Step 2: Basic Port Scanning with nmap

Exercise 1:

Perform a basic port scan on your OWASP VM IP address and record your findings:

- Open Ports:



```
wus.prod.support.services.microsoft.com
ngozikali:~$ nmap 192.168.63.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-07 04:18 EST
Nmap scan report for 192.168.63.129
Host is up (0.0020s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
5001/tcp  open  complex-link
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds

ngozikali:~$ nmap 192.168.63.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-07 04:19 EST
Nmap scan report for 192.168.63.129
Host is up (0.0014s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
5001/tcp  open  complex-link
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

ngozikali:~$
```

Open ports includes

22/tcp

80/tcp

139/tcp

143/tcp

443/tcp

445/tcp

5001/tcp

8080/tcp

8081/tcp

Step 3: Aggressive Scanning with nmap Aggressive scanning with nmap can reveal service versions and the operating system running on open port.

Exercise 2:

Perform an aggressive scan on your OWASP VM IP address and record your findings:

```
Nov 7 05:01
ngozi@kali: ~
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ /wordpress/#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 0001 requests: 1 error(s) and 41 item(s) reported on remote host
+ End Time: 2024-11-07 04:53:15 (GMT-5) (59 seconds)
-----
+ 1 host(s) tested

(ngozi@kali) ~
$ sudo nmap -sV -O 192.168.63.129
[sudo] password for ngozi:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-07 05:00 EST
Nmap scan report for 192.168.63.129
Host is up (0.00059s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http           Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL...)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap           Courier Imapd (released 2008)
443/tcp   open  ssl/http       Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL...)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-object    Java Object Serialization
8080/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http           Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Ports801-TCP:V=7.94SVNVI=7ND-11/7sTime=072CBFB1XP=x86_64-pc-linux-gnuXr
SF:(NULL,4,"\\xac\\xed\\0\\x05");
MAC Address: 00:0C:29:59:02:F3 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 14.72 seconds

(ngozi@kali) ~
$
```

- Service Versions:

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
--------	------	-----	--

80/tcp	open	http	Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL...)
--------	------	------	---

139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
---------	------	-------------	---

143/tcp	open	imap	Courier Imapd (released 2008)
---------	------	------	-------------------------------

443/tcp	open	ssl/http	Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL...)
---------	------	----------	---

445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
---------	------	-------------	---

5001/tcp	open	java-object	Java Object Serialization
----------	------	-------------	---------------------------

8080/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
----------	------	------	-------------------------------------

8081/tcp	open	http	Jetty 6.1.25
----------	------	------	--------------

- Operating System:

OS CPE: cpe:/o:linux:linux_kernel:2.6

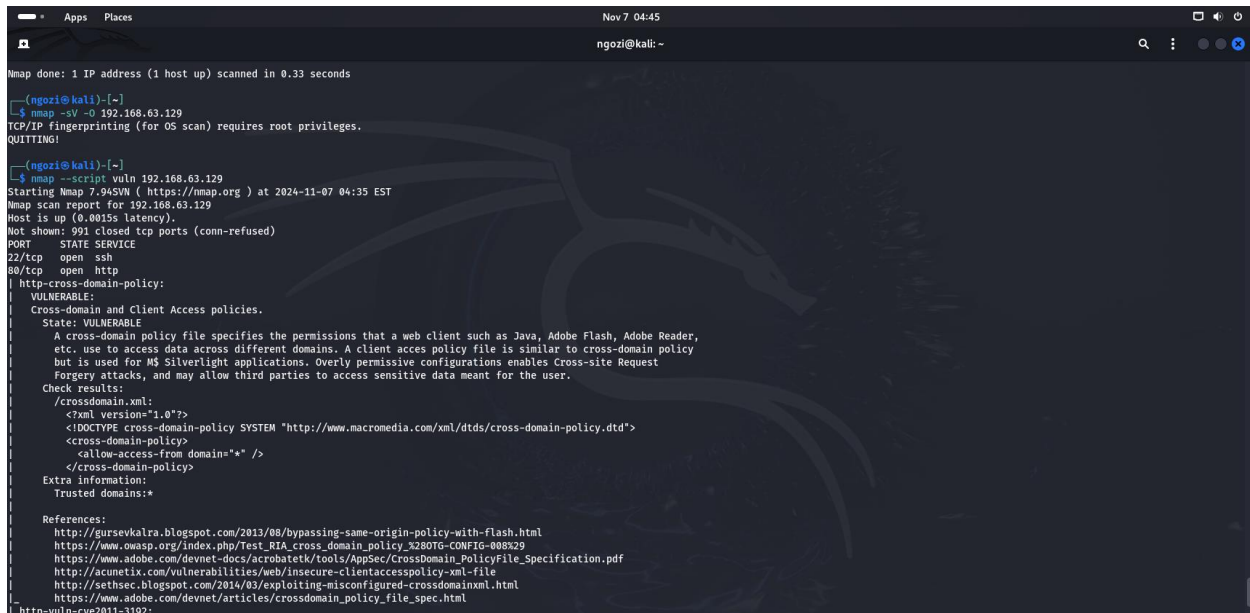
OS details: Linux 2.6.17 - 2.6.36

Step 4: Vulnerability Scanning with nmap

Exercise 3: Conduct a vulnerability scan on your OWASP VM IP address and record your findings:

- Vulnerabilities:

1. Cross-domain and Client Access policies.
2. SSL/TLS MITM vulnerability (CCS Injection)
3. Service regsvc in Microsoft Windows systems vulnerable to denial of service
4. Diffie-Hellman Key Exchange Insufficient Group Strength
5. SL POODLE information leak
6. Apache byterange filter DoS



```
Mmap done: 1 IP address (1 host up) scanned in 0.33 seconds
(ngozi@kali)-[~]
└─$ nmap -sV -O 192.168.63.129
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

(ngozi@kali)-[~]
└─$ nmap --script vuln 192.168.63.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-07 04:35 EST
Nmap scan report for 192.168.63.129
Host is up (0.0015s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
| http-cross-domain-policy:
|   VULNERABLE:
|     Cross-domain and Client Access policies.
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web client such as Java, Adobe Flash, Adobe Reader,
|       etc. use to access data across different domains. A client access policy file is similar to cross-domain policy
|       but is used for MS Silverlight applications. Overly permissive configurations enables Cross-site Request
|       Forgery attacks, and may allow third parties to access sensitive data meant for the user.
|     Check results:
|       /crossdomain.xml:
|       <?xml version="1.0"?>
|       <!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
|       <cross-domain-policy>
|       <allow-access-from domain="*" />
|       </cross-domain-policy>
|     Extra information:
|       Trusted domains:*
|
| References:
|   http://gurusekhalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html
|   https://www.owasp.org/index.php/Test_REA_cross_domain_policy_3260TG-CONFIG-008329
|   https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Specification.pdf
|   http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file
|   http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
|   https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
| http-vuln-cve2011-3192:
```

Step 5: Web Vulnerability Scanning with nikto

Exercise 4:

Perform a vulnerability scan on your OWASP VM and record your findings:

• Vulnerabilities Found:

```
Nov 7 04:52
ngozi@kali: ~
ngozi@kali:~$ nikto -h 192.168.63.129
-----
+ Target IP:      192.168.63.129
+ Target Hostname: 192.168.63.129
+ Target Port:    80
+ Start Time:     2024-11-07 04:52:16 (GMT-5)
-----
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
+ /: Server may leak inodes via ETags, header found with file /, inode: 286483, size: 28067, mtime: Thu Jul 30 22:55:52 2015. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scan-ner/vulnerabilities/missing-content-type-header/
+ /cgi-bin/: Directory indexing found.
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ /favicon.ico: Identifies this app/server as: omasp.org. See: https://en.wikipedia.org/wiki/Favicon
+ /images: IP address found in the 'location' header. The IP is '127.0.1.1'. See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is '127.0.1.1'. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649
+ /index: Uncommon header 'tcn' found, with contents: List.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.css, index.html. See: http://www.wise.c.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Python/2.6.5 appears to be outdated (current is at least 3.9.0).
+ Perl/v5.10.1 appears to be outdated (current is at least v5.32.1).
+ proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2).
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.11).
+ mod_ssl/2.2.14 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ mod_mono/2.4.3 appears to be outdated (current is at least 3.12).
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ Phusion_Passenger/4.0.38 appears to be outdated (current is at least 6.0.7).
+ PHP/5.3.2-1ubuntu4.30 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ mod_python/3.3.1 appears to be outdated (current is at least 3.5.0).
+ OpenSSL/0.9.8k appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell.
+ PHP/5.3 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ /phpBB2/search.php?search_id=1\:\: Cookie phpbb2owaspbwa_data created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /phpBB2/search.php?search_id=1\:\: Cookie phpbb2owaspbwa_sid created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /phpBB2/search.php?search_id=1\:\: Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.30.
```

```
Nov 7 04:55
ngozi@kali: ~
ngozi@kali:~$ nikto -h 192.168.63.129
-----
+ /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is '127.0.1.1'. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649
+ /index: Uncommon header 'tcn' found, with contents: List.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.css, index.html. See: http://www.wise.c.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Python/2.6.5 appears to be outdated (current is at least 3.9.0).
+ Perl/v5.10.1 appears to be outdated (current is at least v5.32.1).
+ proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2).
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.11).
+ mod_ssl/2.2.14 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ mod_mono/2.4.3 appears to be outdated (current is at least 3.12).
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ Phusion_Passenger/4.0.38 appears to be outdated (current is at least 6.0.7).
+ PHP/5.3.2-1ubuntu4.30 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ mod_python/3.3.1 appears to be outdated (current is at least 3.5.0).
+ OpenSSL/0.9.8k appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell.
+ PHP/5.3 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ /phpBB2/search.php?search_id=1\:\: Cookie phpbb2owaspbwa_data created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /phpBB2/search.php?search_id=1\:\: Cookie phpbb2owaspbwa_sid created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /phpBB2/search.php?search_id=1\:\: Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.30.
+ /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /icons/: Directory indexing found.
+ /images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /wordpress/readme.html: This WordPress file reveals the installed version.
+ /wordpress/wp-login/: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ /wordpress/wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 9061 requests: 1 error(s) and 41 item(s) reported on remote host
+ End Time:      2024-11-07 04:53:15 (GMT-5) (59 seconds)
-----
+ 1 host(s) tested
ngozi@kali:~$
```

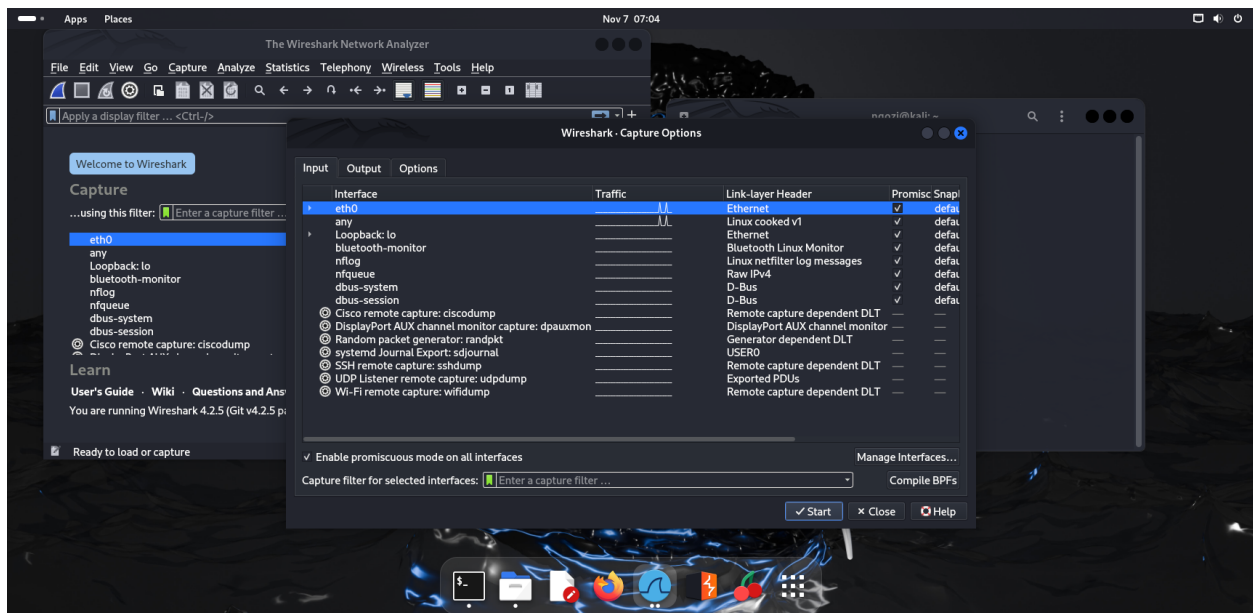
INT302: Kali Linux Tools and System Security – Lab 5: Wireshark

Lab Steps

Step 1: Launching Wireshark

Exercise 1:

- Explore the Wireshark GUI. Identify and list the main components you see, including where to find the Statistics menu



AppsPlaces

Nov 7 07:26

Capturing from eth0

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

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

No.	Time	Source	Destination	Protocol	Length	Info
5191	173.898208145	197.210.176.140	192.168.63.128	QUIC	1290	Protected Payload (KP0), DCID=fc6166
5192	173.898208207	197.210.176.140	192.168.63.128	QUIC	1290	Protected Payload (KP0), DCID=fc6166
5193	173.898208266	197.210.176.140	192.168.63.128	QUIC	1290	Protected Payload (KP0), DCID=fc6166
5194	173.898208329	197.210.176.140	192.168.63.128	QUIC	1290	Protected Payload (KP0), DCID=fc6166
5195	173.898208389	197.210.176.140	192.168.63.128	QUIC	1290	Protected Payload (KP0), DCID=fc6166
5196	173.898208453	197.210.176.140	192.168.63.128	QUIC	431	Protected Payload (KP0), DCID=fc6166
5197	173.898258624	197.210.176.140	192.168.63.128	QUIC	1290	Protected Payload (KP0), DCID=fc6166
5198	173.993605961	197.210.176.140	192.168.63.128	QUIC	1290	Protected Payload (KP0), DCID=fc6166
5199	174.032151673	192.168.63.128	197.210.176.140	QUIC	80	Protected Payload (KP0), DCID=fdff2c9bdb9ba375
5200	174.935616788	192.168.63.128	142.250.184.22	TLSv1.2	93	Application Data
5201	174.936064924	142.250.184.22	192.168.63.128	TCP	60	443 -> 57964 [ACK] Seq=367713 Ack=1015 Win=64240 Len=0
5202	175.122680492	142.250.184.22	192.168.63.128	TLSv1.2	93	Application Data
5203	175.122931267	192.168.63.128	142.250.184.22	TCP	54	57964 -> 443 [ACK] Seq=1015 Ack=367752 Win=65535 Len=0
5204	175.360841852	192.168.63.128	142.250.200.78	UDP	1134	51255 -> 443 Len=1092
5205	175.642657797	142.250.200.78	192.168.63.128	UDP	138	443 -> 51255 Len=96
5206	175.642658134	142.250.200.78	192.168.63.128	UDP	68	443 -> 51255 Len=26
5207	175.643226223	192.168.63.128	142.250.200.78	UDP	83	51255 -> 443 Len=41

> Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface eth0, id 0

> Ethernet II, Src: VMware_e4:4a:0d (00:50:56:e4:4a:0d), Dst: VMware_72:0b:bd (00:0c:29:72:0b:bd)

> Internet Protocol Version 4, Src: 142.250.200.131, Dst: 192.168.63.128

> User Datagram Protocol, Src Port: 443, Dst Port: 36090

> Data (42 bytes)

0000 00 06 29 72 0b bd 00 50 56 e4 4a 0d 08 00 45 00

0010 00 46 2e 24 00 00 00 11 b4 dc 8e fa c8 83 c0 a8

0020 3f 08 01 bb 8d 02 00 32 41 46 4d db ce 80 26 6b

0030 34 ea 61 d4 a8 00 d9 96 f3 e7 92 32 cd c6 4d 96

0040 f8 22 5a f7 80 52 0b 2f c7 ce 3f bf c9 98 65 04

0050 f6 5d 6f 55

...P V J...E

...F.\$... ..

...2 AFM...&k

4 a... ..2..W

...Z..Rk/...?..e

...joU

Bytes 0-5: Address (eth.addr)

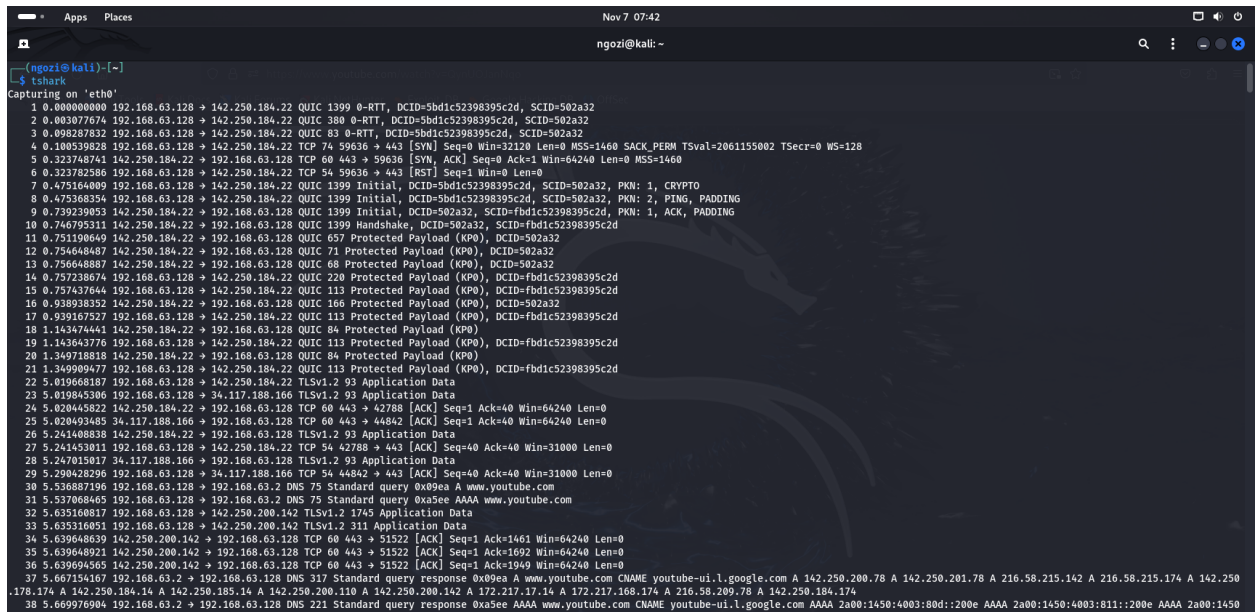
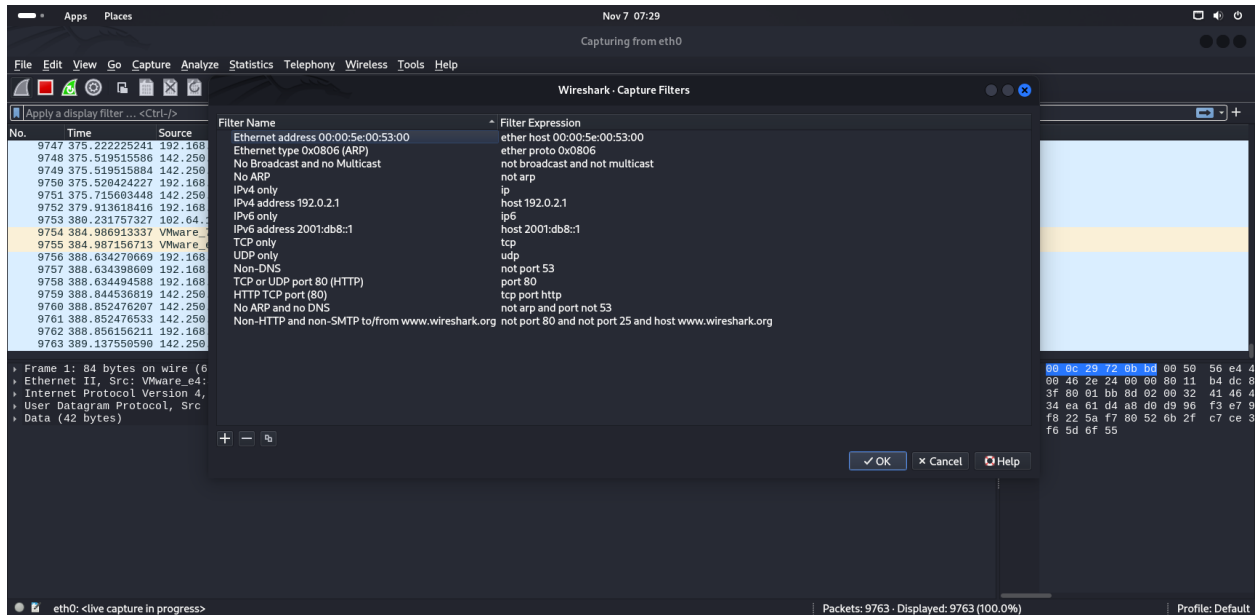
Packets: 5207 - Displayed: 5207 (100.0%)

Profile: Default

Step 2: Capturing Network Traffic

Exercise 2:

- Capture network traffic using both Wireshark and tshark. Compare the two methods and note any differences in the user experience



The first image is for wireshark and the second image is for tshark, the interface are different.

You work directly on the Kail terminal with the tshark but not the wireshark.

Step 3: Analyzing Captured Packet

Exercise 3:

- Use filters to analyze different types of traffic.

Record the following:

- o Number of HTTP packets captured: _____
- o Number of DNS packets captured: _____
- o Specific IP addresses you identified in the traffic: _____

Nov 7 07:52
*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
2361	14.235059883	192.168.63.128	197.210.176.140	UDP	75	60818 → 443 Len=33
2362	14.256744513	197.210.176.140	192.168.63.128	UDP	1290	443 → 60818 Len=1248
2363	14.265848056	197.210.176.140	192.168.63.128	UDP	1290	443 → 60818 Len=1248
2364	14.266505722	192.168.63.128	197.210.176.140	UDP	75	60818 → 443 Len=33
2365	14.296114038	197.210.176.140	192.168.63.128	UDP	1290	443 → 60818 Len=1248
2366	14.311850341	197.210.176.140	192.168.63.128	UDP	1290	443 → 60818 Len=1248
2367	14.311850647	197.210.176.140	192.168.63.128	UDP	1290	443 → 60818 Len=1248
2368	14.315345140	192.168.63.128	197.210.176.140	UDP	75	60818 → 443 Len=33
2369	14.317113767	197.210.176.140	192.168.63.128	UDP	1290	443 → 60818 Len=1248
2370	14.335963307	197.210.176.140	192.168.63.128	UDP	1290	443 → 60818 Len=1248
2371	14.336515989	192.168.63.128	197.210.176.140	UDP	75	60818 → 443 Len=33
2372	14.346618974	197.210.176.140	192.168.63.128	UDP	1290	443 → 60818 Len=1248
2373	14.346619305	197.210.176.140	192.168.63.128	UDP	1290	443 → 60818 Len=1248
2374	14.347296158	192.168.63.128	197.210.176.140	UDP	75	60818 → 443 Len=33
2375	14.357765796	197.210.176.140	192.168.63.128	UDP	1290	443 → 60818 Len=1248
2376	14.365801549	197.210.176.140	192.168.63.128	UDP	1290	443 → 60818 Len=1248
2377	14.369594298	192.168.63.128	197.210.176.140	UDP	75	60818 → 443 Len=33
2378	14.372875781	197.210.176.140	192.168.63.128	UDP	1290	443 → 60818 Len=1248

Frame 1: 1290 bytes on wire (10320 bits), 1290 bytes captured (10320 bits) on interface eth0, id 0
Ethernet II, Src: VMware_e4:4a:0d (00:50:56:e4:4a:0d), Dst: VMware_72:8b:bd (00:0c:29:72:0b:bd)
Internet Protocol Version 4, Src: 197.210.176.140, Dst: 192.168.63.128
User Datagram Protocol, Src Port: 443, Dst Port: 60818
Data (1248 bytes)

00f0 1a 64 dd 7a 30 19 c2 4c e4 d4 1b 30 7f 92 5a ea d:20:L...0-Z
0100 1b c5 4b cf 9a 81 98 31 89 ac 2c 38 d7 6c 34 18 K...1...8[4
0110 07 f5 0c da 98 ac 47 a0 6d 1c 81 7f 25 e5 00 326...X-2
0120 46 36 26 89 47 47 b9 78 ef fd 5e 4b 25 c4 7d 09 F66GGx...KX-
0130 83 d4 73 8b 8d 2a 66 02 86 87 53 5b cf db 14 5a s...f...S[...Z
0140 5f cd 66 83 fd b0 09 08 db dc 01 6c e1 6c f0 49 f...f...L.L.I
0150 df bd f9 1d 0f 10 f4 0b db 4d 43 e0 81 b3 7f 14MC....
0160 8d c2 dd 27 46 1b 3a 47 a8 88 ac d9 f2 1b 1e 71 ...F::G.....
0170 e2 a3 03 4d d8 72 db f1 0d 92 3c 94 6c 21 b9 4c ...M-r:...<L.L
0180 f8 24 d9 b5 39 46 d6 e7 df 35 99 05 18 04 01 98 \$.9F...5.....
0190 2e 62 26 2a 4c 45 f1 e9 21 cf 06 28 30 7a 48 02 b&*LE...l...{z0
01a0 15 ab 05 04 86 1c 5a f9 c3 50 c5 3c 81 14 98 73Z...V<...s
01b0 1c ac b4 86 43 a3 c2 89 bc e7 29 d6 37 8b 69 e9C...)-7-...
01c0 3b 5b 5f 54 7a 68 45 b5 15 45 b2 64 1a b4 36 8d p[TzhE...E;d...6
01d0 45 57 7c 72 7d fe d3 c4 69 ec 4f 53 39 08 41 4f EW[r]...1.0S9:AO
01e0 34 03 4d 7f fe 4a 9d 00 ff 36 b1 c9 1a 93 61 76 A[WJ...6...av
01f0 64 94 5d 63 0e e1 bc a7 b2 f5 28 db db 28 87 3d d[...W-m r]]-NT-
0200 c2 7b a9 a0 09 57 8d 6d 72 7c 7c a0 4e 54 c1 b1 {...u...b.....
0210 8d 83 73 eb e4 ad 75 8a 14 08 02 8d 84 eb 02 7e

Packets: 2390 - Displayed: 2390 (100.0%) - Dropped: 0 (0.0%) Profile: Default