FINAL PROJECT

ACMEGRADE

Cyber Security (April'24)

Metasploitable

Submitted by: R.Yogeshram

Email: yogeshramr@gmail.com

Metasploitable IP : 192.188.29.129

The following steps to be carried out for the successful completion of the project

1. Set Up the Environment

- **Disable Windows Firewall:** Before beginning, ensure that the Windows firewall on the target machine is disabled to allow for unimpeded scanning and exploitation.
- **Ensure Tools are Installed:** Confirm that Nmap, Wireshark, and SQLMAP are installed and configured on your system.

2. Perform Network Scanning using Nmap Script Engines (NSE)

- **Initiate Nmap Scan:**

➢ Use Nmap with script engines (NSEs) to scan the target machine (Metasploitable).
➢ Focus on identifying database-related vulnerabilities.

- **Identify Loopholes:**

➢ Analyze the scan results to identify potential vulnerabilities in the target system.
➢ Pay attention to open ports, services running, and potential weak spots that can be exploited.

3. Analyze Packet Information using Wireshark

- **Capture Network Traffic:**

➢ Use Wireshark to capture the network traffic during the Nmap scan.
➢ Analyze the captured packets to gain insights into the network and identify any suspicious activity or vulnerabilities.

4. Exploit Vulnerabilities using SQLMAP

- **Target Database Vulnerabilities:**

➢ Based on the Nmap scan results, identify the databases that are potentially vulnerable.
➢ Use SQLMAP to perform SQL injection attacks on these databases to gain access.

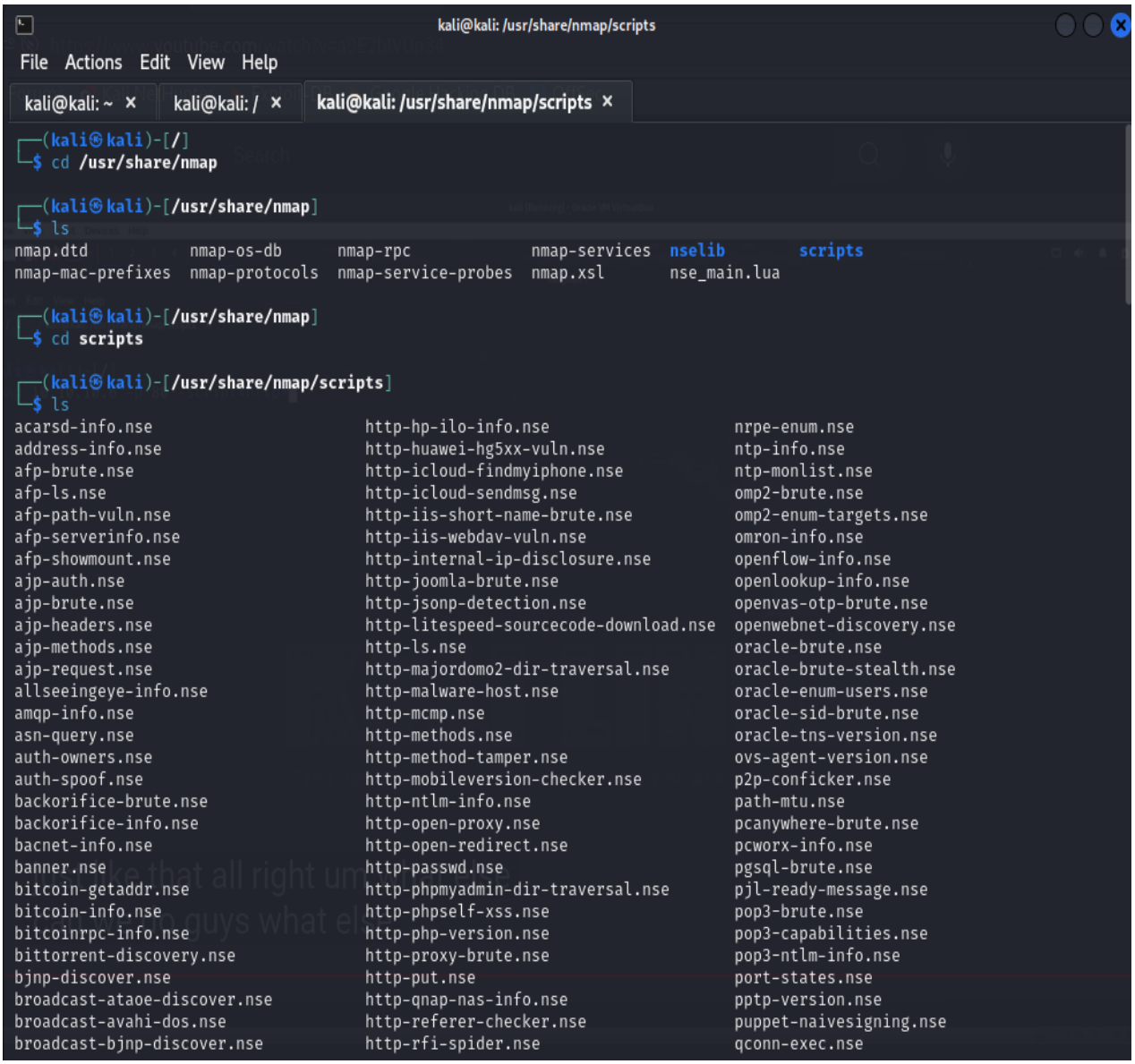
- **Extract Data:**

➢ Hover into the tables, columns, and retrieve useful information from the database.
➢ Make sure to extract and save any critical data that demonstrates the successful exploitation of the vulnerabilities.

Nmap Script Engines:

NSE scripts are categorized into different types such as:

- **auth**: Scripts related to authentication bypass.
- **broadcast**: Scripts that discover hosts by broadcasting messages.
- **brute**: Brute-force password auditing.
- **default**: A basic set of scripts run with -sC or --script=default.
- **dos**: Scripts for testing denial of service vulnerabilities.
- **exploit**: Scripts that target specific vulnerabilities.
- **intrusive**: Scripts that may be harmful to the target.
- **safe**: Scripts that are considered non-intrusive.



To view all the available scripts available on kali linux use the following command

cd /usr/share/nmap

Basic Nmap scanning with NSE

-sC it identifies the open ports with default scripts

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC 192.168.29.129
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 09:33 EDT
Nmap scan report for 192.168.29.129
Host is up (0.0042s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.29.134
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet
25/tcp   open  smtp
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BI
TMIME, DSN
|_ssl-date: 2024-09-04T13:33:46+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such
 thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
```

```
kali@kali: ~
File  Actions  Edit  View  Help
53/tcp   open  domain
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      42362/udp   mountd
|   100005  1,2,3      56512/tcp   mountd
|   100021  1,3,4      38345/udp   nlockmgr
|   100021  1,3,4      45089/tcp   nlockmgr
|   100024  1          42920/udp   status
|_  100024  1          51661/tcp   status
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 7
|   Capabilities flags: 43564
|   Some Capabilities: LongColumnFlag, SupportsTransactions, Support41Auth, SwitchToSSLAfterHandshake, SupportsCompres
sion, Speaks41ProtocolNew, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: 1[[6:^LBDmx5>w_Tg,CI
5432/tcp open  postgresql
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such
 thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2024-09-04T13:33:46+00:00; +1s from scanner time.
5900/tcp open  vnc
```

```
kali@kali: ~
File  Actions  Edit  View  Help
5900/tcp open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11
6667/tcp open  irc
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:02:28
|   source ident: nmap
|   source host: E652A892.E5C4C5A1.FFFA6D49.IP
|_  error: Closing Link: zewyacctl[192.168.29.134] (Quit: zewyacctl)
8009/tcp open  ajp13
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:0E:B5:8F (VMware)

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-09-04T09:33:31-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 1h00m01s, deviation: 2h00m00s, median: 0s

Nmap done: 1 IP address (1 host up) scanned in 73.58 seconds
```

Run Specific Scripts: To use specific NSE scripts, we can run some sample scripts like

nmap --script=http-vuln-cve2017-5638 -p 80 192.168.29.129

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80,443 --script=default 192.168.29.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 10:01 EDT
Nmap scan report for 192.168.29.129
Host is up (0.0028s latency).

PORT    STATE  SERVICE
80/tcp  open   http
|_http-title: Metasploitable2 - Linux
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

We can also target specific ports to speed up the scan or focus on known services:

The above images shows – port 80,443 are scanned using default script set

Run Multiple Scripts: we can also run multiple scripts by separating them with a comma

nmap --script=ssl-heartbleed,http-shellshock -p 443 192.168.29.129

this command checks the SSL heartbleed and shellshock vulnerabilities on port 443.

Advanced Scanning with NSE

Scan with a Category of Scripts:

nmap --script=auth 192.168.29.129

Use Wildcards for Script Names:

nmap --script "http-" -p 80 192.168.29.129*

Using Xsltproc to save the scanned port

This xsltproc converts the saved xml file report into a readable HTML report that be used for further analysis

```
kali@kali: /
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: / ×

┌──(kali㉿kali)-[/]
└─$ nmap --script=auth 192.168.29.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 09:59 EDT
Nmap scan report for 192.168.29.129
Host is up (0.0042s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
| ssh-publickey-acceptance:
|_  Accepted Public Keys: No public keys accepted
23/tcp   open  telnet
25/tcp   open  smtp
| smtp-enum-users:
|_  Method RCPT returned a unhandled status code.
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
|_mysql-empty-password: ERROR: Script execution failed (use -d to debug)
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
| http-default-accounts:
```

```
kali@kali: /
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: / ×
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
|_mysql-empty-password: ERROR: Script execution failed (use -d to debug)
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
| http-default-accounts:
|   [Apache Tomcat] at /manager/html/
|     tomcat:tomcat
|   [Apache Tomcat Host Manager] at /host-manager/html/
|_    tomcat:tomcat

Host script results:
| smb-enum-users:
|_  Domain: METASPLOITABLE; Users: backup, bin, bind, daemon, dhcp, distccd, ftp, games, gnats, irc, klog, libuuid, lis
t, lp, mail, man, msfadmin, mysql, news, nobody, postfix, postgres, proftpd, proxy, root, service, sshd, sync, sys, sys
log, telnetd, tomcat55, user, uucp, www-data

Post-scan script results:
| creds-summary:
|   192.168.29.129:
|     8180/nil:
|       tomcat:tomcat - Valid credentials
|_      tomcat:tomcat - Valid credentials
Nmap done: 1 IP address (1 host up) scanned in 31.11 seconds

┌──(kali㉿kali)-[/]
└─$
```

kali@kali: /

File Actions Edit View Help

kali@kali: ~ × | kali@kali: / × | kali@kali: /usr/share/nmap/scripts ×

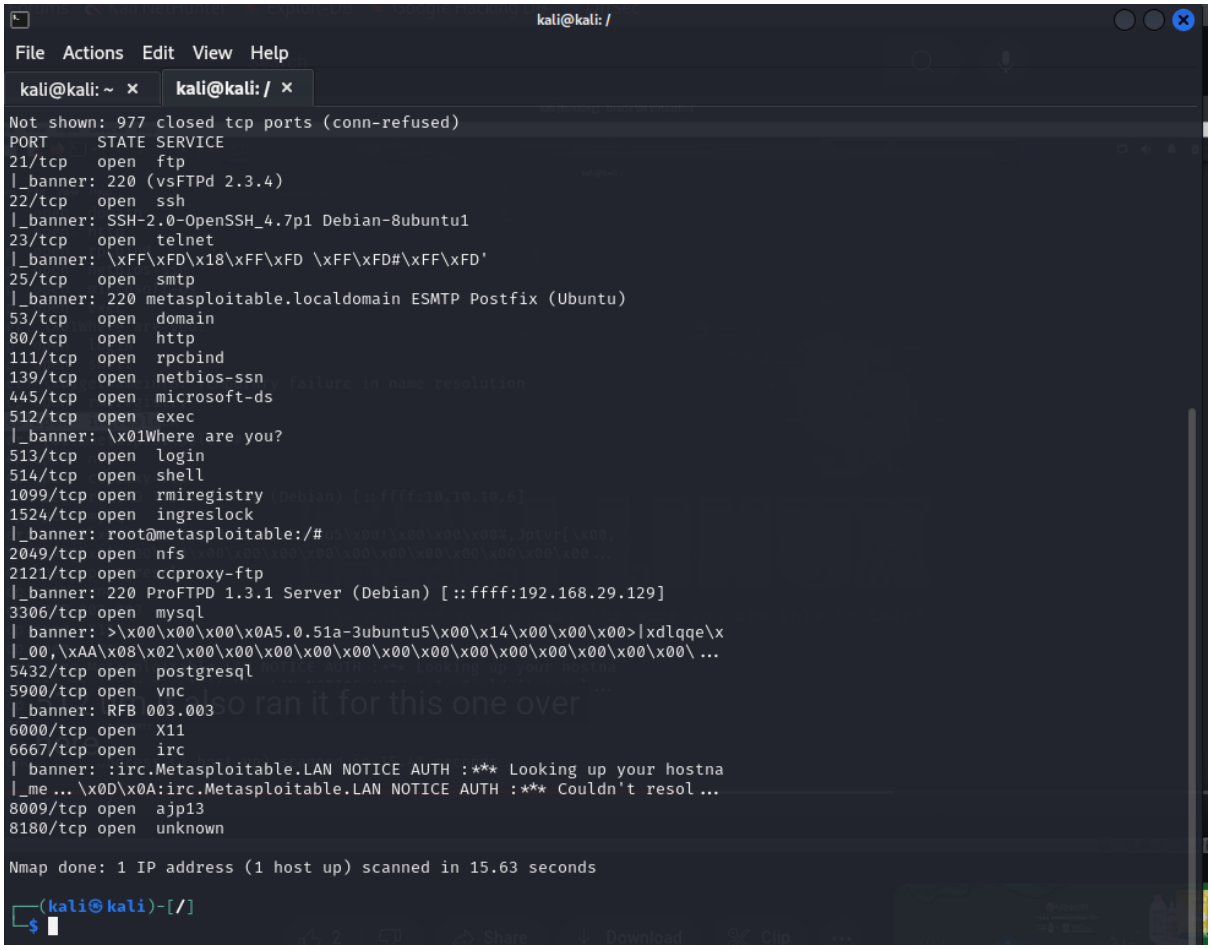
```
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

┌──(kali㉿kali)-[/]
└─$ nmap 192.168.29.129 -p 80 -script=metasploit-xmlrpc-brute.nse
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 09:52 EDT
Nmap scan report for 192.168.29.129
Host is up (0.0036s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

┌──(kali㉿kali)-[/]
└─$ nmap 192.168.29.129 -p 80 -script=http,banner
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 09:53 EDT
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:829: 'http' did not match a category, filename, or directory
stack traceback:
        [C]: in function 'error'
        /usr/bin/../share/nmap/nse_main.lua:829: in local 'get_chosen_scripts'
        /usr/bin/../share/nmap/nse_main.lua:1364: in main chunk
        [C]: in ?

QUITTING!
┌──(kali㉿kali)-[/]
└─$ nmap 192.168.29.129 -p 80 -script=http-title,banner
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 09:54 EDT
Nmap scan report for 192.168.29.129
Host is up (0.0029s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-title: Metasploitable2 - Linux

Nmap done: 1 IP address (1 host up) scanned in 10.36 seconds

┌──(kali㉿kali)-[/]
└─$
```

kali@kali: /

File Actions Edit View Help

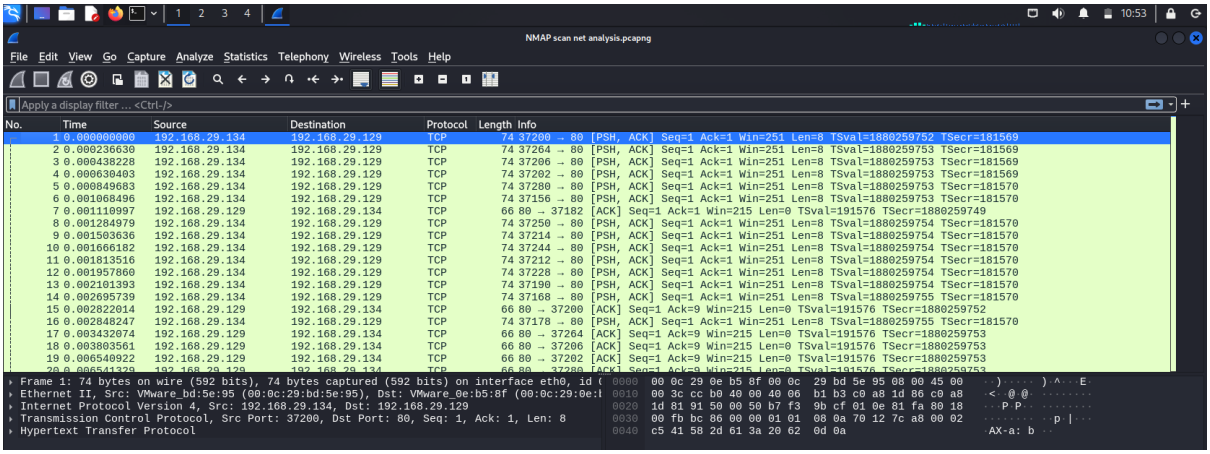
kali@kali: ~ × | kali@kali: / ×

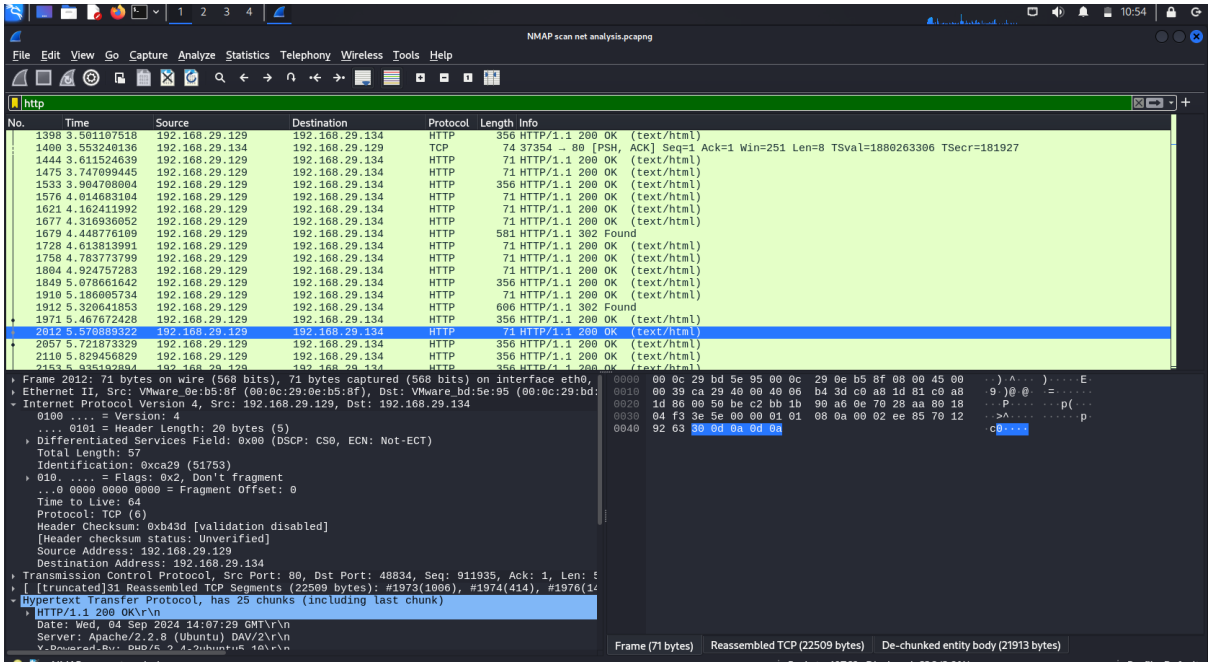
```
└─$ cd /

┌──(kali㉿kali)-[/]
└─$ ls
bin   dev  home        initrd.img.old  lib32  lost+found  mnt  proc  run   srv       sys  usr  vmlinuz
boot  etc  initrd.img  lib             lib64  media       opt  root  sbin  swapfile  tmp  var  vmlinuz.old

┌──(kali㉿kali)-[/]
└─$ nmap 192.168.29.129 -script=banner
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 09:43 EDT
Nmap scan report for 192.168.29.129
Host is up (0.0076s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
|_banner: 220 (vsFTPd 2.3.4)
22/tcp   open  ssh
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
23/tcp   open  telnet
|_banner: \xFF\xFD\x18\xFF\xFD \xFF\xFD#\xFF\xFD'
25/tcp   open  smtp
|_banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
|_banner: \x01Where are you?
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
|_banner: root@metasploitable:/#
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
|_banner: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.29.129]
3306/tcp open  mysql
| banner: >\x00\x00\x00\x0A5.0.51a-3ubuntu5\x00\x14\x00\x00\x00>|xdlqqe\x
|_00,\xAA\x08\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ ...
5432/tcp open  postgresql
5900/tcp open  vnc
```

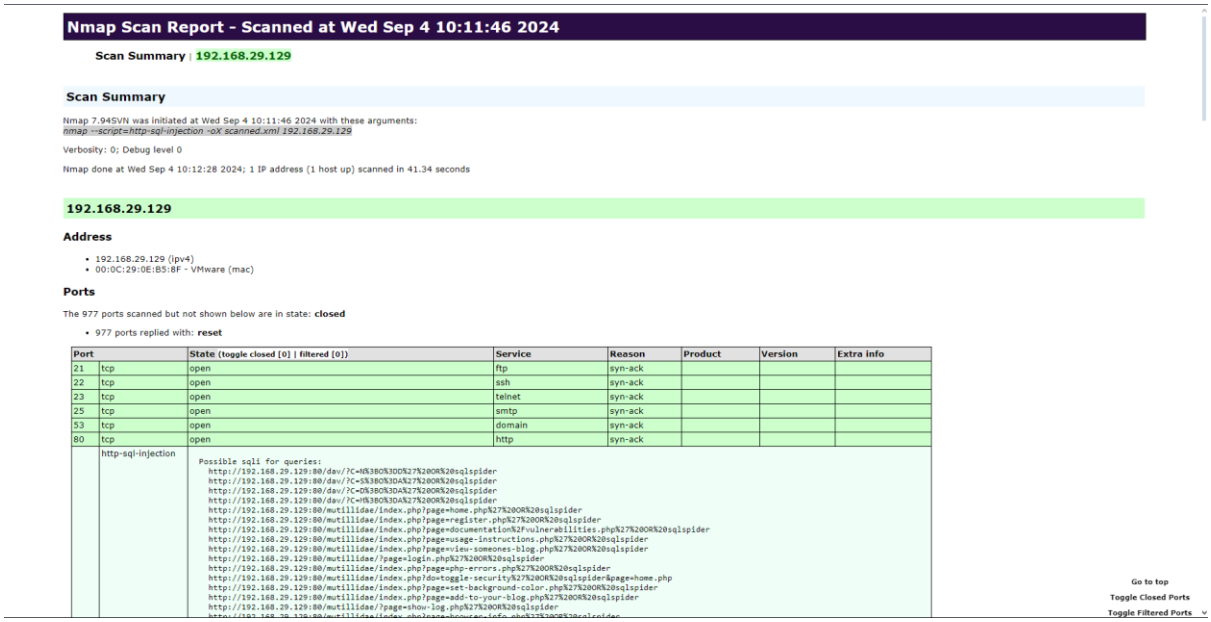


With the above carried out steps it is essential to run Wireshark to monitor the network traffic and also we can observe where each packages and frames have communicated and also analyse it based on the protocol it has communicated within a network environment and also it would help us better understand that the number of protocols used and the port number , start and destination port of each packets.

My drive link (public) in that I have posted the screenshots of the important scan and also the Wireshark file alongside with the Nmap scan report (https://drive.google.com/drive/folders/1mtAL3UEVkRjIoGYE0jJhK4AyKUOl4hnz?usp=sharing)



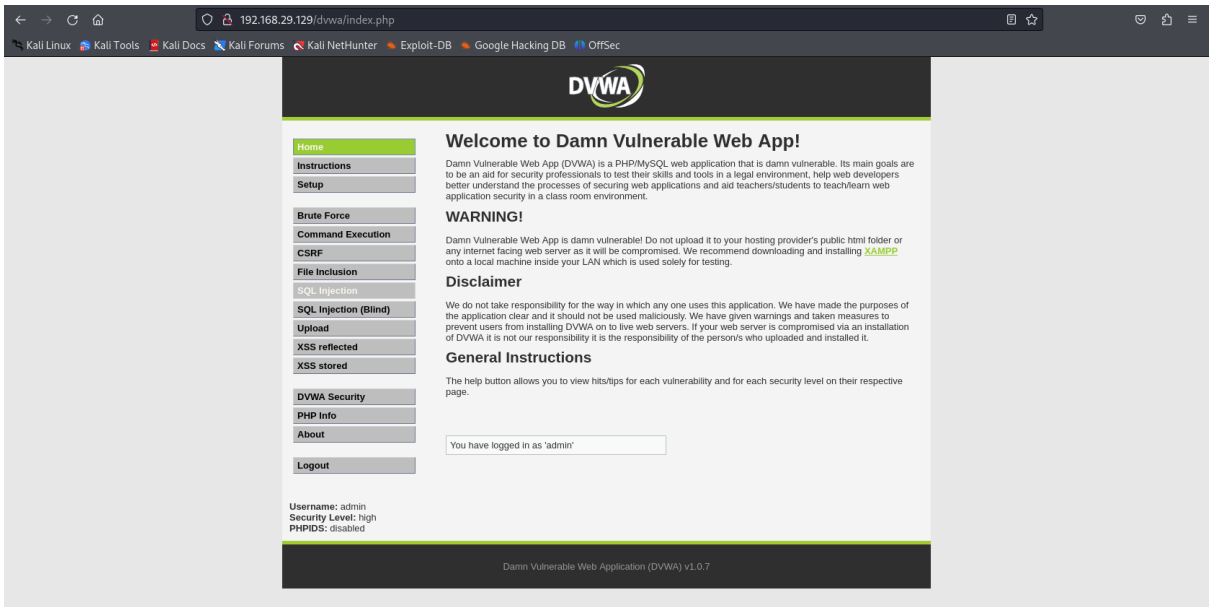




Accessing the DVWA:

DVWA – Damn Vulnerable Web Application

By using DVWA, we can practice various techniques and methodologies used in web application security testing. For example, we can use manual testing techniques to identify vulnerabilities, such as inspecting the source code, analyzing network traffic, and manipulating input fields.



SQL injection with SQLMAP

Identify a Vulnerable Web Application:

- Based on your Nmap scan, identify a web application running on the Metasploitable target that may be vulnerable to SQL injection (e.g., DVWA).

SQLMAP command:

sqlmap -u "http://192.168.29.129/vulnerable_page.php?id=1" --batch –dbs

-u: URL of the target.

--batch: Automatically handle user prompts.

--dbs: Enumerate databases.