

Cyber Security and Ethical Hacking Program

Information Gathering on Websites Using Linux

Introduction

Information gathering means collecting different kinds of information about the target. It is basically, the first step or the beginning stage of Ethical Hacking, where the penetration testers or hackers (both black hat and white hat) try to gather all the information about the target, in order to use it for Hacking.

Hacking is all about finding creative shortcuts, being limitless and you can apply it as a technique when approaching a target. In order to call yourself a hacker, you need to have the mindset of one and should be able to identify system weaknesses that require logical reasoning and the ability to think about all possible actions, alternatives, and potential conclusions.

Requirements

- Recommended operating system Kali Linux
- Nmap, macchanger, and Wireshark must be installed
- Separate Windows machine

Goal

- To demonstrate the understanding of the tools.
- Candidate should be able to gather valuable information from targets to test.

Scenario

You have been assigned as a network administrator in a company and have been given the task to inspect their network infrastructure. Find out what machines are running on the network and scan the individual devices to find out what services are running, open ports, operating systems, and if there is a firewall. Analyze the packets passing through the network and identify if there is a breach in the company network.

NAME : GAURAV UTTAM GHANDAT

Lab 1: Nmap Description

Network Mapper is referred to as **Nmap**. A network's IP addresses and ports can be scanned with this free and open-source Linux command-line tool in order to find installed programs. Network administrators can use Nmap to identify the devices that are connected to their network, find open ports and services, and find security holes. Nmap, for starters, makes it simple to quickly map out a network without the need for complex commands or configurations. Additionally, it allows complex programming using the Nmap scripting engine as well as basic commands (such checking is to see if a host is up). One of Nmap's strongest features is its ability to swiftly identify every device on single or several networks, including switches, routers, mobile devices, servers, and so on.

Task

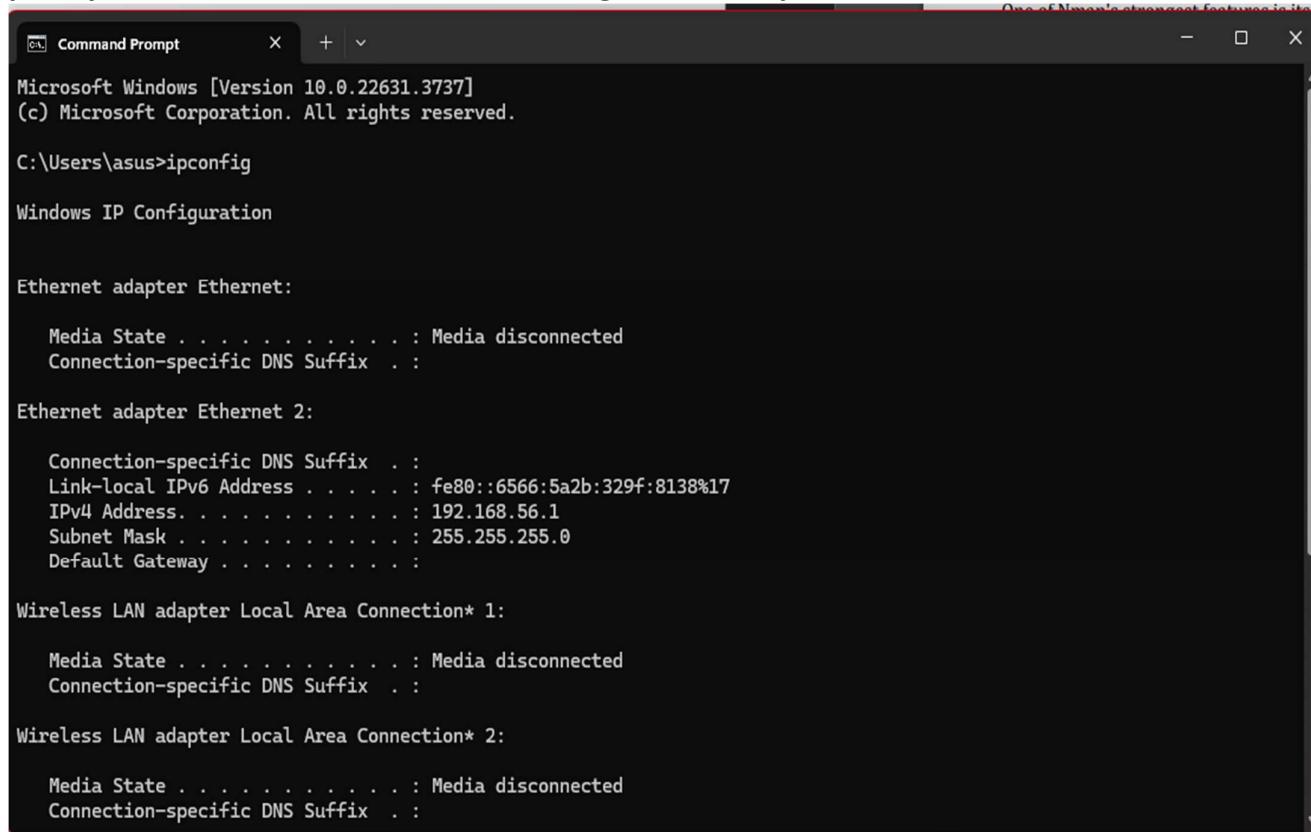
Find the—

- IP address of your Windows machine. (Target)**
- OS Details of your target machine.**
- port details of your target machine.**
- service details of your target machine.**

SOLUTION :

Task 1 :

In the first task we have to get ip address of windows machine using ipconfig in command prompt of windows machine for scanning in the nmap .



```
Microsoft Windows [Version 10.0.22631.3737]
(c) Microsoft Corporation. All rights reserved.

C:\Users\asus>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::6566:5a2b:329f:8138%17
    IPv4 Address . . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:

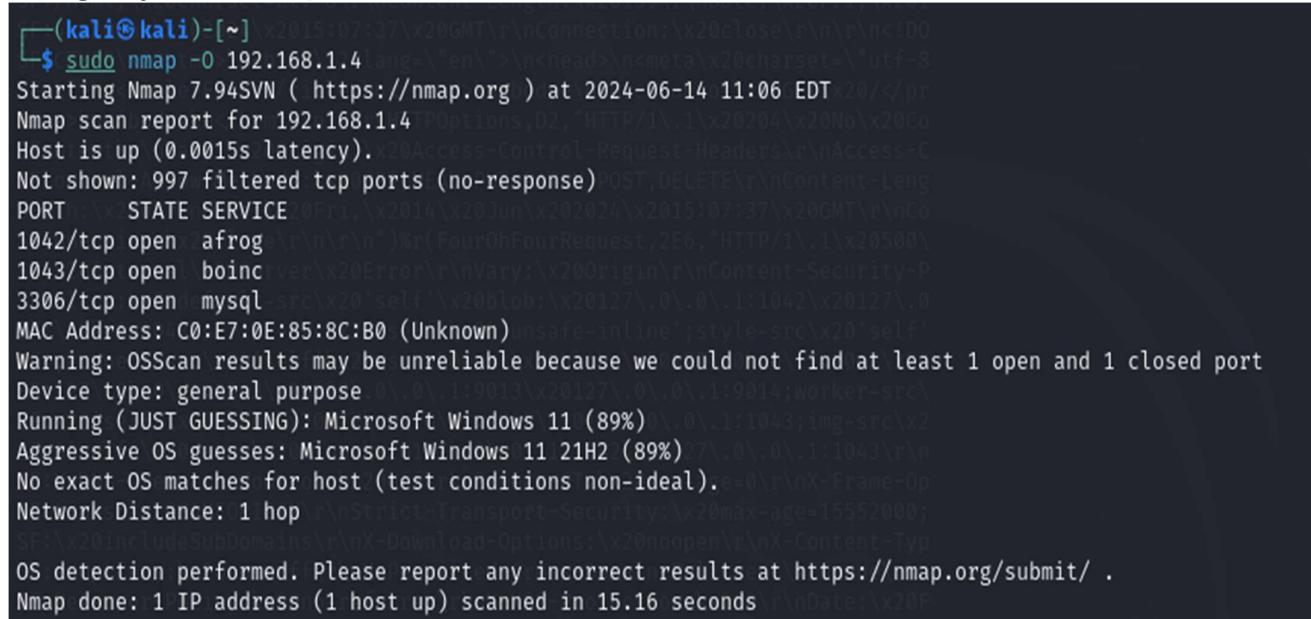
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
```

Task 2 :

In the second task we have to find OS details of your target machine using the nmap and ip address of the windows. We use nmap command to get the OS details using [nmap -o <target ip address>] with this command we can find the OS details.



```
(kali㉿kali)-[~] ~ % sudo nmap -o 192.168.1.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 11:06 EDT
Nmap scan report for 192.168.1.4
Host is up (0.0015s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
1042/tcp  open  afrog
1043/tcp  open  boinc
3306/tcp  open  mysql
MAC Address: C0:E7:0E:85:8C:B0 (Unknown)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11 (89%)
Aggressive OS guesses: Microsoft Windows 11 21H2 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.16 seconds
```

Task 3 :

In the third task we have to find the port details of your target machine using the nmap and ip address of the windows. We use the nmap command to get the port details using [nmap -p- <target ip address>] with this command we can find the port details.

```
(kali㉿kali)-[~]
$ sudo nmap -p- 192.168.1.4
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 11:03 EDT
Nmap scan report for 192.168.1.4
Host is up (0.0013s latency).
Not shown: 65520 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
1042/tcp   open  afrog
1043/tcp   open  boinc?inc?
3306/tcp   open  mysql      MySQL (unauthorized)
7250/tcp   open  unknown    despite returning data. If you know the service/version
7680/tcp   open  pando-pubg/cgi-bin/submit.cgi?new-service :
9012/tcp   open  unknown    ICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
9013/tcp   open  unknown    VNXI=7%D=6/14%Time=666C5BD8%P=x86_64-pc-linux-gnu%R
9014/tcp   open  unknown    P/1\.\1\x20404\x20Not\x20Found\r\nVary:\x20Origin\r\
33060/tcp  open  mysqlx    policy:\x20default-src\x20'self'\r\nX-DNS-Prefetch-Co
49696/tcp  open  unknown    nect-CT:\x20max-age=0\r\nX-Frame-Options:\x20SAMEORI
49697/tcp  open  unknown    port-Security:\x20max-age=15552000;\x20includeSubDom
49700/tcp  open  unknown    nctions:\x20noopen\r\nX-Content-Type-Options:\x20nos
49704/tcp  open  unknown    Cross-Domain-Policies:\x20none\r\nReferrer-Policy:\x20no
49707/tcp  open  unknown    XSS-Protection:\x200\r\nContent-Type:\x20text/html;
49714/tcp  open  unknown    Content-Length:\x20139\r\nDate:\x20Fri,\x2014\x2013
MAC Address: 4C:0:E7:0E:85:8C:B0 (Unknown)
SF:<x20html>\n<html>\x20lang=\\"en\\">\n<head>\n<meta>\x20charset=\\"utf-8\\">>\n<
Nmap done: 1 IP address (1 host up) scanned in 119.70 seconds
```

Task 4 :

In the fourth task we have to find the service details of your target machine using the nmap and ip address of the windows. We use the nmap command to get the service details using [nmap -sV <target ip address>] with this command we can find the service details.

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

SF-Port1043-TCP:V=7.94SVN%T=SSL%D=7%I=7%D=6/14%Time=666C5D2F%P=x86_64-pc-linux
SF:-gnu%r(GetRequest,27E,"HTTP/1\.1\x20404\x20Not\x20Found\r\nVary:\x20ri
SF:gin\r\nContent-Security-Policy:\x20default-src\x20'self'\r\nX-DNS-Prefe
SF:tch-Control:\x20off\r\nExpect-CT:\x20max-age=0\r\nX-Frame-Options:\x20S
SF:AMEORIGIN\r\nStrict-Transport-Security:\x20max-age=15552000;\x20include
SF:SubDomains\r\nX-Download-Options:\x20noopen\r\nX-Content-Type-Options:\x20n
SF:x20nosniff\r\nX-Permitted-Cross-Domain-Policies:\x20none\r\nReferrer-Po
SF:licy:\x20no-referrer\r\nX-XSS-Protection:\x200\r\nContent-Type:\x20text
SF:/html;\x20charset=utf-8\r\nContent-Length:\x20139\r\nDate:\x20Fri,\x201
SF:4\x20Jun\x202024\x2015:09:36\x20GMT\r\nConnection:\x20close\r\n\r\n<!Do
SF:CTYPE\x20html\r\n<html\x20lang=\\"en\\">\n<head>\n<meta\x20charset=\\"utf-8
SF:\">"\n<title>Error</title>\n</head>\n<body>\n<pre>Cannot \x20GET\x20/<pr
SF:er>\n</body>\n</html>\n")%r(HTTPOptions,D2,"HTTP/1\.1\x20204\x20No\x20Co
SF:ntent\r\nVary:\x20Origin,\x20Access-Control-Request-Headers\r\nAccess-C
SF:ontrol-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nContent-Leng
SF:th:\x200\r\nDate:\x20Fri,\x2014\x20Jun\x202024\x2015:09:36\x20GMT\r\nCo
SF:nnection:\x20close\r\n\r\n")%r(TerminalServerCookie,2F,"HTTP/1\.1\x2040
SF:0\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(FourOhFourReque
SF:st,2E6,"HTTP/1\.1\x20500\x20Internal\x20Server\x20Error\r\nVary:\x20ri
SF:gin\r\nContent-Security-Policy:\x20default-src\x20'self'\x20blob:\x2012
SF:7\.\.\.\.1:1042\x20127\.\.\.\.1:1043;script-src\x20'self'\x20'unsafe-in
SF:line';style-src\x20'self';connect-src\x20'self'\x20ws:\x20wss:\x20blob:
SF:\x20127\.\.\.\.1:1042\x20127\.\.\.\.1:1043\x20127\.\.\.\.1:9013\x20127\
SF:.\.\.\.1:9014;worker-src\x20'self'\x20blob:\x20127\.\.\.\.1:1042\x20127
SF:.\.\.\.1:1043;img-src\x20'self'\x20data:\x20blob:\x20127\.\.\.\.1:1042
SF:\x20127\.\.\.\.1:1043\r\nX-DNS-Prefetch-Control:\x20off\r\nExpect-CT:\x20
SF:20max-age=0\r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Transport-Secur
SF:ity:\x20max-age=15552000;\x20includeSubDomains\r\nX-Download-Options:\x20
SF:20noopen\r\nX-Content-Type-Options:\x20nosniff\r\nX-Permitted-Cross-Dom
SF:ain-Policies:\x20none\r\nReferrer-Policy:\x20no-referrer\r\nX-XSS-Prote
SF:ction:\x200\r\nDate:\x20Fri,\x2014\x20Jun\x202024\x2015:09:37\x20GMT\r\n
SF:nnection:\x20close\r\n\r\n");
MAC Address: C0:E7:0E:85:8C:B0 (Unknown)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 33.15 seconds

Lab 2 :Macchanger :

Task

- Change your mac address to any random Mac address

SOULTION :

We use the various macchanger command in kali linux terminal to change the mac address. We use [macchanger eth0] OR [macchanger -s eth0] with this command we can get the current and permanent mac address of the Machine . If we want to generate any random Mac address. We use [macchanger -r eth0] OR [macchanger -a eth0]with this command we can generate the random mac address.

```
(root㉿kali)-[~/home/kali]
└─# macchanger eth0
Current MAC: ea:43:56:0d:c4:af (unknown)
Permanent MAC: 08:00:27:7d:c2:56 (CADMUS COMPUTER SYSTEMS)

(root㉿kali)-[~/home/kali]
└─# macchanger -s eth0
Current MAC: ea:43:56:0d:c4:af (unknown)
Permanent MAC: 08:00:27:7d:c2:56 (CADMUS COMPUTER SYSTEMS)

(root㉿kali)-[~/home/kali]
└─# macchanger -s eth0
Current MAC: ea:43:56:0d:c4:af (unknown)
Permanent MAC: 08:00:27:7d:c2:56 (CADMUS COMPUTER SYSTEMS)

(root㉿kali)-[~/home/kali]
└─# macchanger -r eth0
Current MAC: ea:43:56:0d:c4:af (unknown)
Permanent MAC: 08:00:27:7d:c2:56 (CADMUS COMPUTER SYSTEMS)
New MAC: fe:3e:4a:5d:e1:74 (unknown)

(root㉿kali)-[~/home/kali]
└─# macchanger -a eth0
Current MAC: fe:3e:4a:5d:e1:74 (unknown)
Permanent MAC: 08:00:27:7d:c2:56 (CADMUS COMPUTER SYSTEMS)
New MAC: 00:16:7a:bf:cb:cd (Skyworth Overseas Development Ltd.)

Tor Browser
(root㉿kali)-[~/home/kali]
└─#
```

Lab 3: Netstat

Task

- Enumerate all the ports in the Windows machine.
- Display routing table of Windows machine.

SOULTION :

TASK 1 :

Enumerate all the ports in the Windows machine. Using netstat command in the windows command prompt [netstat -a].

```
Microsoft Windows [Version 10.0.22631.3737]
(c) Microsoft Corporation. All rights reserved.

C:\Users\asus>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135           LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:445           LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:554           LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:1042          LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:1043          LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:2869          LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:3306          LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:3790          LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:5040          LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:9012          LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:9013          LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:9014          LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:10243         LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:33060         LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:49664         LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:49665         LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:49666         LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:49667         LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:49668         LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:49690         LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:49696         LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:49697         LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:49700         LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:49704         LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:49707         LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    0.0.0.0:49714         LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    127.0.0.1:1042        LAPTOP-EHJ3QFJI:51626   ESTABLISHED
  TCP    127.0.0.1:1042        LAPTOP-EHJ3QFJI:52265   TIME_WAIT
  TCP    127.0.0.1:1042        LAPTOP-EHJ3QFJI:52276   TIME_WAIT
  TCP    127.0.0.1:1042        LAPTOP-EHJ3QFJI:52280   TIME_WAIT
  TCP    127.0.0.1:1042        LAPTOP-EHJ3QFJI:52281   TIME_WAIT
  TCP    127.0.0.1:1042        LAPTOP-EHJ3QFJI:52289   ESTABLISHED
  TCP    127.0.0.1:3001        LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    127.0.0.1:5354        LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    127.0.0.1:7337        LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    127.0.0.1:9012        LAPTOP-EHJ3QFJI:51624   ESTABLISHED
  TCP    127.0.0.1:13010       LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    127.0.0.1:13030       LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    127.0.0.1:13030       LAPTOP-EHJ3QFJI:49669   ESTABLISHED
  TCP    127.0.0.1:13031       LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    127.0.0.1:13032       LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    127.0.0.1:17532       LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    127.0.0.1:17532       LAPTOP-EHJ3QFJI:51606   ESTABLISHED
  TCP    127.0.0.1:17945       LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    127.0.0.1:22112       LAPTOP-EHJ3QFJI:0      LISTENING
  TCP    127.0.0.1:27339       LAPTOP-EHJ3QFJI:0      LISTENING
```

Command Prompt			
TCP	127.0.0.1:49669	LAPTOP-EHJ3QFJI:13030	ESTABLISHED
TCP	127.0.0.1:49686	LAPTOP-EHJ3QFJI:49687	ESTABLISHED
TCP	127.0.0.1:49687	LAPTOP-EHJ3QFJI:49686	ESTABLISHED
TCP	127.0.0.1:49688	LAPTOP-EHJ3QFJI:49689	ESTABLISHED
TCP	127.0.0.1:49689	LAPTOP-EHJ3QFJI:49688	ESTABLISHED
TCP	127.0.0.1:50505	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	127.0.0.1:51596	LAPTOP-EHJ3QFJI:65001	ESTABLISHED
TCP	127.0.0.1:51606	LAPTOP-EHJ3QFJI:17532	ESTABLISHED
TCP	127.0.0.1:51608	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	127.0.0.1:51608	LAPTOP-EHJ3QFJI:51962	ESTABLISHED
TCP	127.0.0.1:51624	LAPTOP-EHJ3QFJI:9012	ESTABLISHED
TCP	127.0.0.1:51626	LAPTOP-EHJ3QFJI:1042	ESTABLISHED
TCP	127.0.0.1:51962	LAPTOP-EHJ3QFJI:51608	ESTABLISHED
TCP	127.0.0.1:52289	LAPTOP-EHJ3QFJI:1042	ESTABLISHED
TCP	127.0.0.1:65001	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	127.0.0.1:65001	LAPTOP-EHJ3QFJI:51596	ESTABLISHED
TCP	192.168.41.59:139	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	192.168.41.59:51939	91.108.56.121:https	ESTABLISHED
TCP	192.168.41.59:51966	20.249.186.67:https	ESTABLISHED
TCP	192.168.41.59:51972	a23-196-14-50:https	CLOSE_WAIT
TCP	192.168.41.59:52247	204.79.197.222:https	ESTABLISHED
TCP	192.168.41.59:52248	152.195.38.76:http	ESTABLISHED
TCP	192.168.41.59:52259	40.126.212.197:https	ESTABLISHED
TCP	192.168.41.59:52268	ec2-52-89-255-138:https	TIME_WAIT
TCP	192.168.41.59:52270	ec2-52-89-255-138:https	TIME_WAIT
TCP	192.168.41.59:52282	20.189.173.25:https	ESTABLISHED
TCP	192.168.41.59:52283	ec2-52-89-255-138:https	TIME_WAIT
TCP	192.168.41.59:52284	ec2-52-89-255-138:https	TIME_WAIT
TCP	192.168.41.59:52288	20.17.11.191:https	ESTABLISHED
TCP	192.168.56.1:139	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:135	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:445	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:554	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:1042	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:1043	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:2869	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:3306	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:9012	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:9013	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:9014	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:10243	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:33060	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:49664	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:49665	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:49666	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:49667	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:49668	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::]:49690	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::1]:7337	LAPTOP-EHJ3QFJI:0	LISTENING
TCP	[::1]:7337	LAPTOP-EHJ3QFJI:49920	ESTABLISHED
TCP	[::1]:7337	LAPTOP-EHJ3QFJI:49924	ESTABLISHED
TCP	[::1]:7337	LAPTOP-EHJ3QFJI:50148	ESTABLISHED
TCP	[::1]:7337	LAPTOP-EHJ3QFJI:50491	ESTABLISHED
TCP	[::1]:49920	LAPTOP-EHJ3QFJI:7337	ESTABLISHED

C:\ Command Prompt			
TCP	[::1]:49924	LAPTOP-EHJ3QFJI:7337	ESTABLISHED
TCP	[::1]:50148	LAPTOP-EHJ3QFJI:7337	ESTABLISHED
TCP	[::1]:50491	LAPTOP-EHJ3QFJI:7337	ESTABLISHED
TCP	[2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:49414	[2603:1040:a06:6::2]:https	ESTABLISHED
TCP	[2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:51934	[2603:1040:a06:6::2]:https	ESTABLISHED
TCP	[2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:51948	g2600-140f-0004-0d9b-0000-0000-0000-1011:https	CLOSE_WAIT
TCP	[2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52246	g2600-140f-1e00-0000-0000-0000-17c4-e80:https	ESTABLISHED
TCP	[2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52253	[2620:1ec:bdf::68]:https	ESTABLISHED
TCP	[2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52256	[2603:1063:2000::254]:https	ESTABLISHED
TCP	[2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52262	g2600-140f-1e00-0000-0000-0000-17c4-0ec9:https	ESTABLISHED
TCP	[2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52263	[2603:1046:900:2c::2]:https	ESTABLISHED
TCP	[2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52279	[2600:9000:2600:1800:5:c033:1800:93a1]:https	ESTABLISHED
TCP	[2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52285	[2620:1ec:bdf::254]:https	ESTABLISHED
TCP	[2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52286	[2603:1063:27:2::254]:https	ESTABLISHED
TCP	[2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52293	[2803:f800:53::3]:https	TIME_WAIT
TCP	[2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52294	[2803:f800:53::3]:https	TIME_WAIT
TCP	[2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52295	[2803:f800:53::3]:https	TIME_WAIT
UDP	0.0.0.0:123	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	0.0.0.0:5004	*:*	
UDP	0.0.0.0:5004	*:*	
UDP	0.0.0.0:5005	*:*	
UDP	0.0.0.0:5005	*:*	
UDP	0.0.0.0:5050	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5355	*:*	
UDP	0.0.0.0:50289	*:*	
UDP	0.0.0.0:51310	*:*	
UDP	0.0.0.0:53561	*:*	
UDP	0.0.0.0:56684	*:*	
UDP	0.0.0.0:58546	*:*	
UDP	0.0.0.0:60714	*:*	
UDP	0.0.0.0:63306	*:*	
UDP	127.0.0.1:1900	*:*	
UDP	127.0.0.1:10020	*:*	
UDP	127.0.0.1:28363	*:*	
UDP	127.0.0.1:57252	*:*	
UDP	127.0.0.1:59005	*:*	
UDP	127.0.0.1:60716	127.0.0.1:60716	
UDP	192.168.41.59:137	*:*	
UDP	192.168.41.59:138	*:*	
UDP	192.168.41.59:1900	*:*	
UDP	192.168.41.59:5353	*:*	
UDP	192.168.41.59:5353	*:*	
UDP	192.168.41.59:59004	*:*	
UDP	192.168.56.1:137	*:*	
UDP	192.168.56.1:138	*:*	
UDP	192.168.56.1:1900	*:*	
UDP	192.168.56.1:5353	*:*	

Command Prompt

X + v

```
UDP 192.168.56.1:5353    *:*
UDP 192.168.56.1:5353    *:*
UDP 192.168.56.1:59003   *:*
UDP [::]:123              *:*
UDP [::]:500              *:*
UDP [::]:4500             *:*
UDP [::]:5004             *:*
UDP [::]:5005             *:*
UDP [::]:5353             *:*
UDP [::]:5353             *:*
UDP [::]:5355             *:*
UDP [::]:50289            *:*
UDP [::]:51310            *:*
UDP [::]:53562            *:*
UDP [::]:56684            *:*
UDP [::]:58546            *:*
UDP [::]:60715            *:*
UDP [::]:63306            *:*
UDP [::1]:1900             *:*
UDP [::1]:5353             *:*
UDP [::1]:5353             *:*
UDP [::1]:59002            *:*
UDP [::1]:60721           [::1]:60721
UDP [fe80::6566:5a2b:329f:8138%17]:1900  *:*
UDP [fe80::6566:5a2b:329f:8138%17]:59000  *:*
UDP [fe80::6d2f:e856:9513:514%19]:1900  *:*
UDP [fe80::6d2f:e856:9513:514%19]:59001  *:*
```

C:\Users\asus>

TASK 2 :

Display routing table of Windows machine. Using the netstat command in windows command prompt [netstat -r].

```
C:\ Command Prompt X + ▾
Microsoft Windows [Version 10.0.22631.3737]
(c) Microsoft Corporation. All rights reserved.

C:\Users\asus>netstat -r
=====
Interface List
12...58 11 22 ea 3b a6 .....Realtek PCIe GbE Family Controller
17...0a 00 27 00 00 11 .....VirtualBox Host-Only Ethernet Adapter
13...2e 3b 70 6e ce 2f .....Microsoft Wi-Fi Direct Virtual Adapter
15...2e 3b 70 6e ce 3f .....Microsoft Wi-Fi Direct Virtual Adapter #2
19...28 ac 9d 87 4a f9 .....MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
 3...2c 3b 70 6e ce 2e .....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    192.168.41.86  192.168.41.59    55
         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
        192.168.41.0    255.255.255.0  On-link     192.168.41.59    311
        192.168.41.59    255.255.255.255  On-link     192.168.41.59    311
        192.168.41.255    255.255.255.255  On-link     192.168.41.59    311
        192.168.56.0    255.255.255.0  On-link     192.168.56.1    281
        192.168.56.1    255.255.255.255  On-link     192.168.56.1    281
 192.168.56.255  255.255.255.255  On-link     192.168.56.1    281
          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     192.168.56.1    281
          224.0.0.0      240.0.0.0        On-link     192.168.41.59    311
 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     192.168.56.1    281
 255.255.255.255  255.255.255.255  On-link     192.168.41.59    311
=====
```

Persistent Routes:

None

IPv6 Route Table

=====
Active Routes:

If	Metric	Network	Destination	Gateway
19	71	::/0		fe80::28c1:bfff:fec9:fd70
1	331	::1/128		On-link
19	71	2405:204:922d:3cad::/64		On-link
19	311	2405:204:922d:3cad:53aa:ffbf:5857:8e9/128		On-link
19	311	2405:204:922d:3cad:c8cd:6e4d:fa57:b575/128		On-link
17	281	fe80::/64		On-link
19	311	fe80::/64		On-link
17	281	fe80::6566:5a2b:329f:8138/128		On-link
19	311	fe80::6d2f:e856:9513:514/128		On-link
1	331	ff00::/8		On-link
17	281	ff00::/8		On-link
19	311	ff00::/8		On-link

=====

Persistent Routes:

None

C:\Users\asus>

Lab 4: Wireshark

Description

Wireshark is an open-source packet analyzer used for monitoring networks by network or security administrators. This tool lets you see traffic passing through the network and helps you to inspect the traffic, troubleshoot the network, and even understand how communication between network devices takes place. Wireshark is built into Linux distributions like Kali Linux and is also available on OS X and Windows. Before opening Kali make sure you have the network settings on the bridged network. Select your Kali VM to go to settings and change the following settings. This will put your windows machine and Kali VM in the same network.

Things to know before performing the lab

Protocols

An established set of guidelines that govern how data is exchanged across various devices connected to the same network is known as a network protocol.

TCP stream

You can monitor a specific TCP discussion between two or more hosts using this capability. It locates all the TCP packets between a specific source and destination and puts the data sent during that exchange back together in a parseable form.

Task

- Identify the main types of protocols that could be found.**
- Find the protocol through which data is passed.**
- Create a column to identify TCP Streams.**
- Find the actual data that's passed in the TCP Streams.**

SOLUTION :

TASK 1 :

Identify the main types of protocols that could be found.

The screenshot displays the Wireshark interface with the following details:

- Packet List:** Shows 130 total packets, with 130 displayed (100.0% of the total). The list includes entries for ARP, TCP, and DHCP requests and responses.
- Protocol Hierarchy Statistics:**

Protocol	Percent Packets	packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	130	100.0	19420	555	0	0	0	130
Ethernet	100.0	130	11.0	2144	61	0	0	0	130
Internet Protocol Version 4	79.2	103	10.6	2060	58	0	0	0	103
User Datagram Protocol	3.1	4	0.2	32	0	0	0	0	4
Dynamic Host Configuration Protocol	3.1	4	11.3	2192	62	4	2192	62	4
Transmission Control Protocol	76.2	99	63.0	12236	349	64	6517	186	99
Malformed Packet	5.4	7	0.0	0	0	7	0	0	7
Data	21.5	28	23.6	4592	131	28	4592	131	28
Address Resolution Protocol	20.8	27	5.6	1080	30	27	1080	30	27

TASK 2 :

Find the protocol through which data is passed.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000316	192.168.56.1	192.168.56.101	TCP	72	63668 → 5555 [PSH, ACK] Seq=1 Ack=1 Win=4117 Len=6 Tsv=572920157 ...
15	37.945479	192.168.56.1	192.168.56.101	TCP	91	63668 → 5555 [PSH, ACK] Seq=7 Ack=1 Win=4117 Len=25 Tsv=572957937 ...
18	58.986071	192.168.56.1	192.168.56.101	TCP	99	63668 → 5555 [PSH, ACK] Seq=32 Ack=1 Win=4117 Len=33 Tsv=57297891 ...
49	123.228746	192.168.56.1	192.168.56.101	TCP	73	63677 → 5555 [PSH, ACK] Seq=1 Ack=1 Win=131744 Len=7 Tsv=57304286 ...
43	123.239956	192.168.56.101	192.168.56.1	TCP	71	5555 → 63677 [PSH, ACK] Seq=1 Ack=8 Win=29056 Len=5 Tsv=216254 TS ...
46	128.125666	192.168.56.1	192.168.56.101	TCP	73	63677 → 5555 [PSH, ACK] Seq=8 Ack=6 Win=131744 Len=7 Tsv=57304774 ...
47	128.137334	192.168.56.101	192.168.56.1	TCP	195	5555 → 63677 [PSH, ACK] Seq=8 Ack=16 Win=29056 Len=128 Tsv=217479 ...
50	135.829191	192.168.56.1	192.168.56.101	TCP	69	63677 → 5555 [PSH, ACK] Seq=15 Ack=135 Win=131616 Len=3 Tsv=57305 ...
51	135.833048	192.168.56.101	192.168.56.1	TCP	178	5555 → 63677 [PSH, ACK] Seq=136 Ack=18 Win=29056 Len=112 Tsv=2194 ...
54	146.021575	192.168.56.1	192.168.56.101	TCP	83	63677 → 5555 [PSH, ACK] Seq=18 Ack=247 Win=131520 Len=17 Tsv=5730 ...
55	146.025155	192.168.56.101	192.168.56.1	TCP	1514	5555 → 63677 [ACK] Seq=247 Ack=35 Win=29056 Len=1448 Tsv=221953 T ...
56	146.025166	192.168.56.101	192.168.56.1	TCP	635	5555 → 63677 [PSH, ACK] Seq=1695 Ack=35 Win=29056 Len=569 Tsv=221 ...
66	185.143394	192.168.56.1	192.168.56.101	TCP	83	63677 → 5555 [PSH, ACK] Seq=36 Ack=2264 Win=131072 Len=17 Tsv=573 ...
69	185.309961	192.168.56.101	192.168.56.1	TCP	132	5555 → 63677 [PSH, ACK] Seq=2264 Ack=53 Win=29056 Len=61 Tsv=2317 ...
72	185.385151	192.168.56.101	192.168.56.1	TCP	126	5555 → 63677 [PSH, ACK] Seq=2330 Ack=53 Win=29056 Len=60 Tsv=2317 ...
75	185.576331	192.168.56.101	192.168.56.1	TCP	146	5555 → 63677 [PSH, ACK] Seq=2399 Ack=53 Win=29056 Len=80 Tsv=2318 ...
78	205.927881	192.168.56.1	192.168.56.101	TCP	75	63677 → 5555 [PSH, ACK] Seq=53 Ack=2470 Win=131072 Len=9 Tsv=5731 ...
81	214.384283	192.168.56.1	192.168.56.101	TCP	75	63677 → 5555 [PSH, ACK] Seq=62 Ack=2470 Win=131072 Len=9 Tsv=5731 ...
84	214.412776	192.168.56.101	192.168.56.1	TCP	176	5555 → 63677 [PSH, ACK] Seq=2479 Ack=71 Win=29056 Len=110 Tsv=239 ...
88	215.776535	192.168.56.101	192.168.56.1	TCP	83	5555 → 63677 [PSH, ACK] Seq=2580 Ack=72 Win=29056 Len=17 Tsv=2393 ...
92	216.178502	192.168.56.101	192.168.56.1	TCP	82	5555 → 63677 [PSH, ACK] Seq=2597 Ack=72 Win=29056 Len=16 Tsv=2394 ...
96	216.216.178502	192.168.56.101	192.168.56.1	TCP	82	5555 → 63677 [PSH, ACK] Seq=2613 Ack=74 Win=29056 Len=16 Tsv=2395 ...

```

Frame 4: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: PCSSystemtec_fa:25:8e (08:00:27:fa:25:8e)
Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.101
Transmission Control Protocol, Src Port: 63668, Dst Port: 5555, Seq: 1, Ack: 1, URG: 0
Data (6 bytes)
0000 08 00 27 fa 25 8e 0a 00 27 00 00 08 00 45 00  ..%.'..E
0010 00 3a a7 55 40 00 40 06 a1 b1 c0 a8 38 01 c0 a8  ..@.8.
0020 38 65 f8 b4 15 b3 b9 a6 57 f9 8f f4 f2 95 80 18  8e .....W
0030 10 15 b7 a6 00 00 01 01 08 0a 22 26 11 5d 00 02  ....&].
0040 a3 48 68 65 6c 6c 6f 0a  .Hello.

```

TASK 3:

Create a column to identify TCP Streams.

No.	Time	Source	Destination	Protocol	Length	Info
82	214.385304	192.168.56.101	192.168.56.1	TCP	66	63677 → 5555 [ACK] Seq=2470 Ack=2471
83	214.385321	192.168.56.101	192.168.56.1	TCP	66	[TCP Dup ACK 82#1] 5555 → 63677
84	214.412776	192.168.56.101	192.168.56.1	TCP	176	5555 → 63677 [PSH, ACK] Seq=2471 Ack=2472
85	214.412794	192.168.56.101	192.168.56.1	TCP	176	[TCP Retransmission] 5555 → 63677
86	214.412846	192.168.56.1	192.168.56.101	TCP	66	63677 → 5555 [ACK] Seq=71 Ack=72
87	215.776197	192.168.56.1	192.168.56.101	TCP	67	63677 → 5555 [PSH, ACK] Seq=71 Ack=72
88	215.776535	192.168.56.101	192.168.56.1	TCP	83	5555 → 63677 [PSH, ACK] Seq=25555
89	215.776550	192.168.56.101	192.168.56.1	TCP	83	[TCP Retransmission] 55555 → 63677
90	215.776592	192.168.56.1	192.168.56.101	TCP	66	63677 → 5555 [ACK] Seq=72 Ack=73
91	216.176096	192.168.56.1	192.168.56.101	TCP	67	63677 → 5555 [PSH, ACK] Seq=72 Ack=73
92	216.178502	192.168.56.101	192.168.56.1	TCP	82	5555 → 63677 [PSH, ACK] Seq=255555
93	216.178519	192.168.56.101	192.168.56.1	TCP	82	[TCP Retransmission] 555555 → 63677
94	216.178598	192.168.56.1	192.168.56.101	TCP	66	63677 → 5555 [ACK] Seq=73 Ack=74
95	216.216.178598	192.168.56.1	192.168.56.101	TCP	67	63677 → 5555 [PSH, ACK] Seq=73 Ack=74
96	216.576573	192.168.56.101	192.168.56.1	TCP	82	555555 → 63677 [PSH, ACK] Seq=265555
97	216.576589	192.168.56.101	192.168.56.1	TCP	82	[TCP Retransmission] 555555 → 63677
98	216.576635	192.168.56.1	192.168.56.101	TCP	66	63677 → 5555 [ACK] Seq=74 Ack=75
99	217.272170	192.168.56.1	192.168.56.101	TCP	67	63677 → 5555 [PSH, ACK] Seq=74 Ack=75
100	217.272479	192.168.56.101	192.168.56.1	TCP	77	555555 → 63677 [PSH, ACK] Seq=26775555
101	217.272496	192.168.56.101	192.168.56.1	TCP	77	[TCP Retransmission] 555555 → 63677
102	217.272537	192.168.56.1	192.168.56.101	TCP	66	63677 → 5555 [ACK] Seq=75 Ack=76
103	219.240125	192.168.56.1	192.168.56.101	TCP	67	63677 → 5555 [PSH, ACK] Seq=75 Ack=76

```

Frame 92: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
Ethernet II, Src: PCSSystemtec_fa:25:8e (08:00:27:fa:25:8e), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)
Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.1
Transmission Control Protocol, Src Port: 5555, Dst Port: 63677, Seq: 1, Ack: 1, URG: 0
Data (16 bytes)
0000 0a 00 27 00 00 08 00 27 fa 25 8e 08 00 45 00  ..
0010 00 44 2d 0e 40 00 40 06 1b ef c0 a8 38 65 c0 a8  ..
0020 38 01 15 b3 f8 bd e9 55 79 ab 56 86 35 17 80 18  ..
0030 00 e3 c4 b4 00 00 01 01 08 0a 00 03 a7 8b 22 29  ..
0040 5a 30 09 57 6f 72 6b 20 50 68 6f 6e 65 20 5b 5d  ..
0050 8a 20

```

TASK 4 :

Find the actual data that's passed in the TCP Streams.

Wireshark - rogue_user.pcap

tcp.stream eq 1

No.	Time	Source	Destination	Protocol	Length	Info
82	214.385304	192.168.56.101	192.168.56.1	TCP	66	5555 → 63677 [ACK] Seq=2470 Ack=2531
83	214.385321	192.168.56.101	192.168.56.1	TCP	66	[TCP Dup ACK 82#1] 5555 → 63677 [PSH, ACK] Seq=2470 Ack=2531
84	214.412776	192.168.56.101	192.168.56.1	TCP	176	5555 → 63677 [PSH, ACK] Seq=2470 Ack=2531
85	214.412794	192.168.56.101	192.168.56.1	TCP	176	[TCP Retransmission] 5555 → 63677 [PSH, ACK] Seq=2470 Ack=2531
86	214.412846	192.168.56.1	192.168.56.101	TCP	66	63677 → 5555 [ACK] Seq=71 Ack=72
87	215.776197	192.168.56.1	192.168.56.101	TCP	67	63677 → 5555 [PSH, ACK] Seq=71 Ack=72
88	215.776535	192.168.56.101	192.168.56.1	TCP	83	5555 → 63677 [PSH, ACK] Seq=2531 Ack=2648
89	215.776550	192.168.56.101	192.168.56.1	TCP	83	[TCP Retransmission] 5555 → 63677 [PSH, ACK] Seq=2531 Ack=2648
90	215.776592	192.168.56.1	192.168.56.101	TCP	66	63677 → 5555 [ACK] Seq=72 Ack=73
91	216.176096	192.168.56.1	192.168.56.101	TCP	67	63677 → 5555 [PSH, ACK] Seq=72 Ack=73
92	216.178502	192.168.56.101	192.168.56.1	TCP	82	5555 → 63677 [PSH, ACK] Seq=2531 Ack=2648
93	216.178519	192.168.56.101	192.168.56.1	TCP	82	[TCP Retransmission] 5555 → 63677 [PSH, ACK] Seq=2531 Ack=2648
94	216.178598	192.168.56.1	192.168.56.101	TCP	66	63677 → 5555 [ACK] Seq=73 Ack=74
95	216.576056	192.168.56.1	192.168.56.101	TCP	67	63677 → 5555 [PSH, ACK] Seq=73 Ack=74
96	216.576573	192.168.56.101	192.168.56.1	TCP	82	5555 → 63677 [PSH, ACK] Seq=2648 Ack=2765
97	216.576589	192.168.56.101	192.168.56.1	TCP	82	[TCP Retransmission] 5555 → 63677 [PSH, ACK] Seq=2648 Ack=2765
98	216.576635	192.168.56.1	192.168.56.101	TCP	66	63677 → 5555 [ACK] Seq=74 Ack=75
99	217.272170	192.168.56.1	192.168.56.101	TCP	67	63677 → 5555 [PSH, ACK] Seq=74 Ack=75
100	217.272479	192.168.56.101	192.168.56.1	TCP	77	5555 → 63677 [PSH, ACK] Seq=2648 Ack=2765
101	217.272496	192.168.56.101	192.168.56.1	TCP	77	[TCP Retransmission] 5555 → 63677 [PSH, ACK] Seq=2648 Ack=2765
102	217.272537	192.168.56.1	192.168.56.101	TCP	66	63677 → 5555 [ACK] Seq=75 Ack=76
103	218.240105	192.168.56.1	192.168.56.101	TCP	67	63677 → 5555 [PSH, ACK] Seq=75 Ack=76

Frame 92: 82 bytes on wire (656 bits), 82 bytes captured 0000 0a 00 27 00 00 00 08 00 27 fa 25 8e 08 00 45 00
Ethernet II, Src: PCSSystemtec_fa:25:8e (08:00:27:fa:25:8e), Dst: 00:0c:00 (00:0c:00:00:00:00)
Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.1
Transmission Control Protocol, Src Port: 5555, Dst Port: 63677
Data (16 bytes) 0000 0a 00 27 00 00 00 08 00 27 fa 25 8e 08 00 45 00
0001 00 44 2d 0e 40 00 40 06 1b ef c0 a8 38 65 c0 a8
0020 38 01 15 b3 f8 bd e9 55 79 ab 56 86 35 17 80 18
0030 00 e3 c4 b4 00 00 01 01 08 0a 00 03 a7 8b 22 29
0040 5a 30 09 57 6f 72 6b 20 50 68 6f 6e 65 20 5b 5d
0050 3a 20

Wireshark - Follow TCP Stream (tcp.stream eq 1) - rogue_user.pcap

```
whoami
root
finger
Login      Name      Tty      Idle   Login Time   Office   Office Phone
root      root      tty2      19     Apr 21 12:08 (:1)
ls
Desktop
Documents
Downloads
index.html
index.html.1
Music
passhash.txt
Pictures
Public
Templates
Videos
VIP.txt
cat passhash.txt
root::16848:0:99999:7:::
daemon::16848:0:99999:7:::
bin::16848:0:99999:7:::
sys::16848:0:99999:7:::
sync::16848:0:99999:7:::
games::16848:0:99999:7:::
man::16848:0:99999:7:::
lp::16848:0:99999:7:::
mail::16848:0:99999:7:::
news::16848:0:99999:7:::
uucp::16848:0:99999:7:::
proxy::16848:0:99999:7:::
www-data::16848:0:99999:7:::
backup::16848:0:99999:7:::
list::16848:0:99999:7:::
irc::16848:0:99999:7:::
gnats::16848:0:99999:7:::
nobody::16848:0:99999:7:::
libuuid::16848:0:99999:7:::
syslog::16848:0:99999:7:::
messagebus::16848:0:99999:7:::
usbmux::16848:0:99999:7:::
dnsmasq::16848:0:99999:7:::
avahi-autoipd::16848:0:99999:7:::
kernoops::16848:0:99999:7:::
rtkit::16848:0:99999:7:::
saned::16848:0:99999:7:::
whoonsie::16848:0:99999:7:::
16 client pkts, 16 served pkts, 23 turns.
```

Entire conversation (4,535 bytes) Show data as ASCII Stream 1 Find Next

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