



CHAPTER 17

NETWORK TRAFFIC MONITORING

CERTIFIED CYBERSECURITY TECHNICIAN

Copyrights @ 2022 EC-Council International Ltd.







Chapter 17: Network Traffic Monitoring

Exercise 1: Configure, View, and Analyze Windows Event Logs	05
Exercise 2: View and Analyze Windows Logs	18
Exercise 3: View and Analyze Linux Logs	23





Network monitoring helps security professionals identify possible issues before they affect business continuity. If an issue occurs in the network, the root cause can be determined easily through network monitoring. Subsequently, using network automation tools, the problem can be fixed automatically. Networking monitoring not only prevents outages but also provides visibility to potential issues. Continuous network monitoring minimizes downtime and increases the performance of the network.

Even when security tools are in place, attackers can find ways to bypass such security mechanisms to enter the network. Security tools generally use signature-based detection techniques, and it is difficult to identify continuously changing attack signatures/patterns. These tools are not designed to identify behavioural anomalies and are unable to detect attackers' activities that are initiated before and during attacks. Network monitoring tools provide the first level of security and help identify anomalous conditions in the network, that indicate attacker activity.

OBJECTIVE

The objective of this lab is to provide expert knowledge in network traffic monitoring. This includes knowledge of the following tasks:

- Intercepting network traffic using various tools such as Wireshark and tcpdump
- Exploring various filters in Wireshark
- · Analyzing and examining various network packet headers in Linux using tools such as tcpdump
- · Performing scan on network to identify machines in the local network

OVERVIEW OF NETWORK TRAFFIC MONITORING

Network monitoring is a retrospective security approach that involves monitoring a network for abnormal activities, performance issues, bandwidth issues, etc. It is an integral part of network security and is a demanding task within the network security operations of organizations. Continuous network traffic monitoring and analysis are critical for effective threat detection.

A proper analysis of log data enables actionable information to be identified, which helps the security professional in detecting and monitoring potential security breaches, internal misuse of information, operational issues, and other long-term issues. It also helps validate whether the end-user has followed all documented protocols to detect fraudulent activities and policy violations. It is also useful for internal investigations, security auditing and forensic analysis, determination of operational trends, and implementation of baselines.





LAB TASKS

Cyber security professional or a security professional use numerous tools and techniques to monitor network traffic. The recommended labs that will assist you in learning various aspects of network traffic monitoring include the following:



Intercept Network Traffic using Wireshark and tcpdump



Analyze and Examine Various Network Packet Headers in Linux using tcpdump



Apply Various Filters in Wireshark



Scan Network to Identify Hosts in the Local Network

Note: Turn on PfSense Firewall virtual machine and keep it running throughout the lab exercises.



EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND tcpdump

Network traffic monitoring is the process of capturing network traffic and inspecting it closely to determine what is happening on the network.

LAB SCENARIO

A security professional must have the required knowledge to intercept and interpret network traffic using various packet sniffing tools. The captured traffic can be used to identify malicious or suspicious packets hiding within traffic.

OBJECTIVE

This lab will demonstrate how to capture network traffic using Wireshark and tcpdump.

OVERVIEW OF TROJAN

The network monitoring process involves sniffing the traffic flowing through the network. For this purpose, network packets must be captured, and a signature analysis must be conducted to identify any malicious activity. Security professionals should constantly strive to maintain smooth network operation by monitoring network traffic. If the network goes down even for a small period, productivity within a company may decline. To be proactive rather than reactive, the traffic movement and performance must be monitored to ensure that no security breach occurs within the network.





Note: Ensure that the PfSense Firewall virtual machine is running.

- 1. Turn on Admin Machine-1, Web Server and Attacker Machine-2 virtual machines.
- 2. Log in with the credentials Admin and admin@123.

Note: If the network screen appears, click Yes.

3. Click on Type here to search field at the bottom right of the Desktop, type wireshark and select Wireshark from the results. The Wireshark app will appear. Click to open the Wireshark.









4. The main window of Wireshark appears.

Note: If Software Update Window appears, click on Skip this version.

5. Next, you need to select the interface of which you want Wireshark to capture traffic. To begin packet capture, select the Ethernet interface from the list and in the Enter a captured filter... field, enter ip.

Note: The ip filter captures only IPv4 traffic not IPv6.

6. Now, to begin packet capturing, click Start capturing packets icon (blue color shark fin icon) from the tool bar.

00		MAR	
	TRA	ESH	JMD
)RK	WIR	\mathcal{C}
		5 N	
		\mathbb{D}	NA

The Wireshark Network Analyzer		- D X
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help		
📶 🔳 🔬 💿 📴 🕱 🖆 🍳 🗢 🗢 🕾 🖗 🖢 🧮 🗮 🔍 Q, Q, Q, 🏛		
Apply a display filter <ctrl-></ctrl->		
Welcome to Wireshark		
Capture		
using this niter: 📕 (p)	All interfaces shown *	
Local Area Connection* 9		
Local Area Connection* 8		
Ethernet		
Local Area Connection* 7		
Adapter for loopback traffic capture /		



7. Wireshark begins to capture the traffic of the selected interface, as shown in the screenshot below.



a display filter < Time 1 0.000000 2 0.005308 3 8.576602 4 8.731673 5 8.778047	Source 10.10.1.2 10.10.1.1 10.10.1.2 20.197.71.89 10.10.1.2	Destination 10.10.1.1 10.10.1.2 20.197.71.89 10.10.1.2 20.197.71.89	Protocol L DNS DNS TLSv1.2 TLSv1.2	ength Info 76 Standard query 0xd996 A dns.msftncsi.com 92 Standard query response 0xd996 A dns.msftncsi.com A 131.107 155 Application Data
Time 1 0.000000 2 0.005308 3 8.576602 4 8.731673 5 8.778047	Source 10.10.1.2 10.10.1.1 10.10.1.2 20.197.71.89 10.10.1.2	Destination 10.10.1.1 10.10.1.2 20.197.71.89 10.10.1.2 20.197.71 20	Protocol L DNS DNS TLSv1.2 TLSv1.2	engh Info 76 Standard query 0xd996 A dns.msftncsi.com 92 Standard query response 0xd996 A dns.msftncsi.com A 131.107 155 Application Data
1 0.000000 2 0.005308 3 8.576602 4 8.731673 5 8.778047	10.10.1.2 10.10.1.1 10.10.1.2 20.197.71.89 10.10.1.2	10.10.1.1 10.10.1.2 20.197.71.89 10.10.1.2 20.197.71.89	DNS DNS TLSv1.2 TLSv1.2	76 Standard query 0xd996 A dns.msftncsi.com 92 Standard query response 0xd996 A dns.msftncsi.com A 131.107 155 Application Data
2 0.005308 3 8.576602 4 8.731673 5 8.778047	10.10.1.1 10.10.1.2 20.197.71.89 10.10.1.2	10.10.1.2 20.197.71.89 10.10.1.2 20.197.71.89	DNS TLSv1.2 TLSv1.2	92 Standard query response 0xd996 A dns.msftncsi.com A 131.10. 155 Application Data
3 8.576602 4 8.731673 5 8.778047	10.10.1.2 20.197.71.89 10.10.1.2	20.197.71.89 10.10.1.2 20.197.71.89	TLSv1.2 TLSv1 2	155 Application Data
4 8.731673 5 8.778047	20.197.71.89 10.10.1.2	10.10.1.2	TLSv1 2	
5 8.778047	10.10.1.2	20, 197, 71 89		225 Application Data
		20.157.71.05	TCP	54 50351 → 443 [ACK] Seq=102 Ack=172 Win=1028 Len=0
rnet II, Src: rnet Protocol Datagram Pro in Name System	WS-NLB-PhysServer- Version 4, Src: 10 tocol, Src Port: 50 m (query)	, 76 Dytes Carlot 21_5d:15:7d:7a (02 .10.1.2, Dst: 10.10 267, Dst Port: 53	a (eeo bits) on i 15:5d:15:7d:7a), a.1.1	Terrate upericeurrtousides-jour-40/E-3223-4305(22035047, 10 Dst: MS-NLB-PhysServer-21_5d:15:7d:76 (02:15:5d:15:7d:76)
2 15 5d 15 7d	76 02 15 5d 15 7d	1 7a 08 00 45 00	··]·}v··]·}z··E	
1 01 c4 5h 00	35 00 2a 16 52 de	9 96 01 02 0a 0a	·>·V····	
0 00 00 00 00	00 03 64 6e 73 08	3 6d 73 66 74 6e	······d ns msftr	n
53 73 69 03 63	6f 6d 00 00 01 00	9 01	csi.com	
53 73 69 0 3 63	6f 6d 00 00 01 00) 01	csi.com.	
	 1: 76 bytes met II, Src: met Protocol Datagram Protocol Datagram Protocol 10 Name Syster 10 15 5d 15 76 60 10 3e f9 56 60 10 16 45b 60 60 10 60 60 60 60 13 73 69 63 62 	2 1: 76 bytes on wire (608 bits) rnet II, Src: MS-NLB-PhysServer- rnet Protocol Version 4, Src: 10 Datagram Protocol, Src Port: 50 in Name System (query) 12 15 5d 15 7d 76 02 15 5d 15 7d 10 3e f9 56 00 08 08 11 00 00 01 10 1 c4 5b 00 35 00 2a 16 52 df 10 00 00 00 00 00 36 46 c7 30 01 37 36 90 36 36 f6 d0 00 00 01 01	2 1: 76 bytes on wire (608 bits), 76 bytes capture rnet II, Src: MS-NLB-PhysServer-21_5d:15:7d:7a (02 rnet Protocol Version 4, Src: 10.10.1.2, Dst: 10.11 Datagram Protocol, Src Port: 50267, Dst Port: 53 in Name System (query) 22 15 5d 15 7d 76 02 15 5d 15 7d 7a 08 00 45 00 10 3e f9 56 00 08 80 11 00 00 8a 0a 01 02 0a 0a 11 01 c4 5b 00 35 00 2a 16 52 d9 96 01 00 00 01 10 00 00 00 00 00 03 64 6e 73 08 6d 73 66 74 6e 13 73 69 03 63 6f 6d 00 00 01 00 01	2 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on in rnet II, Src: MS-NLB-PhysServer-21_5d:15:7d:7a (02:15:5d:15:7d:7a), rnet Protocol Version 4, Src: 10.10.1.2, Dst: 10.10.1.1 Datagram Protocol, Src Port: 50267, Dst Port: 53 in Name System (query) 12 15 5d 15 7d 76 02 15 5d 15 7d 7a 08 00 45 00 ···]·}v···]·}z··E 10 3e f9 56 00 00 80 11 00 00 0a 8a 01 02 0a 0a ···V····}·z··E 11 01 c4 5b 00 35 00 2a 16 52 d9 96 01 00 00 01 ···[·5* R.··· 13 73 69 03 63 6f 6d 00 00 01 00 01 ···[·5* R.···







8. Minimize the Wireshark window.

9. Open any web browser (here, Mozilla Firefox) and type http://www.moviescope.com in the url field and press Enter.









10. Now, switch back to the Wireshark window and click Stop capturing packets icon (red square icon) from the tool bar to stop capturing packets.

EXERCEPT Intercept Network traffic Using wireshark And topoump

6	Capturi	ng from Ethernet	(ip)			– Ø ×	
Eile	<u>E</u> dit	View Go C	apture <u>A</u> nalyze <u>S</u> tatisti	cs Telephony <u>W</u> ireless	Tools Help	5	
11			8 🖸 9 🗢 🕾 7	F 🕹 🚍 🔳 🔍 Q (Q. III		
	Appl Sto	n capturing nack	cets				F
No.	-	Time	Source	Destination	Protocol L	ength Info	^
	24700	271.601329	34.107.221.82	10.10.1.2	TCP	54 80 → 50595 [FIN, ACK] Seq=605 Ack=604 Win=67840 Len=0	
	24701	271.601366	10.10.1.2	34.107.221.82	TCP	54 50600 → 80 [ACK] Seq=608 Ack=442 Win=262656 Len=0	
	24702	271.601387	10.10.1.2	34.107.221.82	TCP	54 50595 → 80 [ACK] Seq=604 Ack=606 Win=262400 Len=0	
	24703	271.986889	104.95.180.134	10.10.1.2	TLSv1.2	85 Encrypted Alert	
	24704	271.986889	104.95.180.134	10.10.1.2	TCP	54 443 + 50642 [FIN, ACK] Seq=54003 Ack=1119 Win=64128 Len=0	
	24705	271.986962	10.10.1.2	104.95.180.134	TCP	54 50642 → 443 [ACK] Seq=1119 Ack=54004 Win=262656 Len=0	
	24706	271.987066	10.10.1.2	104.95.180.134	TCP	54 50642 → 443 [FIN, ACK] Seq=1119 Ack=54004 Win=262656 Len=0	
	24707	271.990017	104.95.180.134	10.10.1.2	TCP	54 443 → 50642 [ACK] Seq=54004 Ack=1120 Win=64128 Len=0	
	24708	278.617510	10.10.1.2	13.35.246.60	TLSv1.3	93 Application Data	
	24709	278.617742	10.10.1.2	13.35.246.60	TLSv1.3	78 Application Data	
	24710	278.617759	10.10.1.2	13.35.246.60	TCP	54 50616 + 443 [FIN, ACK] Seq=1343 Ack=15293183 Win=5592832 Len=0	
	24711	278.620942	13.35.246.60	10.10.1.2	TCP	66 [TCP Window Update] 443 → 50616 [ACK] Seq=15293183 Ack=1280 Wi…	





11. From the captured packets, select any DNS frame (they are light blue in colour), and observe the packet content displayed in the middle section, as shown in the screenshot below.

Note: Frame: Displays details regarding captured bytes.

CA CA

• Ethernet II: Displays details such as destination and source MAC addresses and type of network protocol used in the captured packet such as IPv4.

- Internet Protocol Version 4: Displays details such as source and destination IP addresses.
- User Datagram Protocol: Displays source and destination ports, length of the frame and checksum values.
- Domain Name System: Refers to the application protocol, there are two types of frame query and response.

00		A R K	
	RA	HSH/	
		$\sum_{i=1}^{n}$	

1 *	Ethernet (ip)				- 0 >
File	Edit View Go	Canture Analyze Sta	tistics Telephony Wirele	er Tools He	
-ne		Capture Analyze Sta			1P
4	🔳 🖉 💽 🛄 🛅	X 🖸 🤇 🗢 🖻	i 👔 🛓 📑 🔍 G		
A	pply a display filter <	Ctrl-/>			
lo.	Time	Source	Destination	Protocol	Length Info
	45 95.570173	40.127.86.76	10.10.1.2	TLSv1.2	741 Application Data
	46 95.570232	10.10.1.2	40.127.86.76	TCP	54 50588 → 443 [ACK] Seq=2087 Ack=7852 Win=261376 Len=0
	47 95.583930	10.10.1.2	40.127.86.76	TCP	54 50588 → 443 [FIN, ACK] Seq=2087 Ack=7852 Win=261376 Len=0
	48 95.819488	40.127.86.76	10.10.1.2	TCP	54 443 → 50588 [ACK] Seq=7852 Ack=2088 Win=525568 Len=0
+	49 96.835164	10.10.1.2	10.10.1.1	DNS	84 Standard query 0x3e08 A detectportal.firefox.com
	50 96.850472	10.10.1.2	10.10.1.1	DNS	88 Standard query 0xb61b A contile.services.mozilla.com
	51 96.864469	10.10.1.2	8.8.8	DNS	84 Standard query 0x3e08 A detectportal.firefox.com
	52 96.868096	8.8.8.8	10.10.1.2	DNS	195 Standard query response 0x3e08 A detectportal.firefox.com CN
	53 96.880706	10.10.1.2	10.10.1.1	DNS	97 Standard query 0xd341 A firefox.settings.services.mozilla.co
	54 96.882974	10.10.1.2	8.8.8	DNS	88 Standard query 0xb61b A contile.services.mozilla.com
	55 96.887897	8.8.8.8	10.10.1.2	DNS	104 Standard query response 0xb61b A contile.services.mozilla.co
	56 96.907210	10.10.1.2	34.107.221.82	TCP	66 50595 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_
	57 96.911120	34.107.221.82	10.10.1.2	TCP	66 80 → 50595 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 S
	58 96.911180	10.10.1.2	34.107.221.82	TCP	54 50595 → 80 [ACK] Seq=1 Ack=1 Win=262912 Len=0
	59 96.911363	10.10.1.2	34.107.221.82	HTTP	355 GET /canonical.html HTTP/1.1
	60 96.914555	10.10.1.2	10.10.1.1	DNS	102 Standard query 0x3c40 A prod.detectportal.prod.cloudops.mozg

Frame 49: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{26C51D69-3344-4B7E-9225-4309C2E8338A}, id 0 Ethernet II, Src: MS-NLB-PhysServer-21 5d:15:7d:7a (02:15:5d:15:7d:7a), Dst: MS-NLB-PhysServer-21 5d:15:7d:76 (02:15:5d:15:7d:76)

> Internet Protocol Version 4, Src: 10.10.1.2, Dst: 10.10.1.1

> User Datagram Protocol, Src Port: 54081, Dst Port: 53

Domain Name System (query)



12. Now, select first TCP packet (with light green color), to observe the packet content.

13. In the middle section, you can observe source and destination MAC addresses under Ethernet II, as shown in the screenshot below.

EXERCEPT NTERCEPT NETWORK TRAFFIC JSING WIRESHARK

4	Etherne	et (ip)				- 6		X
File	Edit	View Go	Capture Analyze Stat	istics Telephony Wirele	ss Tools He	lp		
4		🛞 📘 🔚	X C 9 0 0 0	T & 🗮 🔳 Q Q				
	Apoly a r	disolav filter <	Ctrl-/>					1+
Nie	appi) a	Time	Source	Destination	Protocol	Length Tafa		
vo.	AE	05 570172	40 107 96 76	10 10 1 2	TI Sul 2	741 Application Data		
-	45	95.570175	40.127.00.70	10.10.1.2	TCP	54 56588 + 442 [ACK] Sec-2087 Ack-7852 Min-261276 Lon-0		
-	40	95.570252	10.10.1.2	40.127.86.76	TCP	54 50500 + 445 [ACK] SEG-2007 ACK-7052 WIN-201370 LEN-0		
-	47	95.819488	49 127 86 76	10 10 1 2	TCP	54 50500 4 445 [FIR, ACK] Seq=2007 ACK=7052 WII-201570 Len-0	-	
	40	06 935164	10.10.1.2	10.10.1.1	DNS	S4 445 4 50500 [ACK] Seq-7052 ACK-2000 Mil-525500 Len-0		
	50	96 859472	10.10.1.2	10.10.1.1	DNS	88 Standard query 0x5606 A detection tal. Therox.com	-	
	51	96 864469	10.10.1.2	8 8 8 8	DNS	84 Standard query 0x3e08 A detectnortal firefox com		
	52	96 868096	8 8 8 8	10 10 1 2	DNS	195 Standard query response 0x3e08 A detection tal firefox com	CN	
	53	96.880706	10.10.1.2	10.10.1.1	DNS	97 Standard query 0xd341 A firefox settings services mozilla		
	54	96 882974	10 10 1 2	8 8 8 8	DNS	88 Standard query 0x651b A contile services mozilla com		-
	55	96.887897	8.8.8.8	10.10.1.2	DNS	104 Standard query response 0xb61b A contile services mozilla		
	56	96,907210	10.10.1.2	34,107,221,82	TCP	66 50595 → 80 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 WS=256 S4	CK	
	57	96,911120	34, 107, 221, 82	10.10.1.2	TCP	66 80 → 50595 [SYN, ACK] Seg=0 Ack=1 Win=65535 Len=0 MSS=143	10 S	
	58	96,911180	10.10.1.2	34,107,221,82	TCP	54 50595 → 80 [ACK] Seg=1 Ack=1 Win=262912 Len=0		=
	59	96,911363	10.10.1.2	34,107,221,82	HTTP	355 GET /canonical.html HTTP/1.1		-
	60	96,914555	10.10.1.2	10.10.1.1	DNS	102 Standard query 0x3c40 A prod.detectportal.prod.cloudops.m	IOZE	
								_
>	Frame	56: 66 byte	s on wire (528 bits)	, 66 bytes captured (528 bits) on	interface \Device\NPF_{26C51D69-3344-4B7E-9225-4309C2E8338A},	id 0	
~	Ethern	et II, Src:	MS-NLB-PhysServer-2	1 5d:15:7d:7a (02:15:	5d:15:7d:7a)	, Dst: MS-NLB-PhysServer-21_5d:15:7d:76 (02:15:5d:15:7d:76)		
	> Des	tination: M	S-NLB-PhysServer-21_5	5d:15:7d:76 (02:15:5d	:15:7d:76)			
	> Sou	rce: MS-NLB	-PhysServer-21_5d:15:	:7d:7a (02:15:5d:15:7	d:7a)			
	Тур	e: IPv4 (0x	0800)					
>	Intern	et Protocol	Version 4, Src: 10.	10.1.2, Dst: 34.107.2	21.82			
>	Transm	ission Cont	rol Protocol, Src Po	rt: 50595, Dst Port: 1	80, Seq: 0,	Len: 0		





14. Similarly, you can view all the other information under different sections such as Frame, Internet Protocol Version 4, Transmission Control Protocol.

15. Close all open windows.

16. Now, we will use tcpdump tool to intercept HTTP traffic.

17. Switch to the Web Server virtual machine.

18. Log in with the credentials Administrator and admin@123.

Note: The network screen appears, click Yes.

19. Click Start icon from the lower-left corner of the Desktop and from the options, select Server Manager.

20. The Server Manager window appears. Click Tools and select Internet Information Services (IIS) Manager option.

00			Dashboard	WELCOME TO SERVER MANAGER		Computer Management Defragment and Optimize Drives
	LL (Local Server All Servers	1 Configure	this local conver	Disk Cleanup Event Viewer
ΠΠΠ			File and Storage Services	Configure	this local server	Internet Information Services (IIS) Manager
				OUICK START		iSCSI Initiator
	$\left(\begin{array}{c} \\ \end{array} \right) \sum \\ \end{array} \right)$	$M \gg$	NO 113	2 Add role	s and features	Local Security Policy
$((\land \cap)$				2 Add foic.	s and reactives	Microsoft Azure Services
				3 Add othe	er servers to manage	ODBC Data Sources (32-bit)
				UNITE AUTO		ODBC Data Sources (64-bit)
				4 Create a	server group	Performance Monitor
(()) (Δ\						Print Management
	\bigcap^{1}	\geq 0		5 Connect	this server to cloud ser	Resource Monitor
						Services
				LEARN MORE		System Configuration
	\mathbf{Y}					System Information
				ROLES AND SERVER GROUPS		Task Scheduler
				Roles: 2 Server groups: 1 Servers total: 1		Windows Firewall with Advanced Security
		7/				Windows Memory Diagnostic
				File and Storage	IIS	Windows PowerShell
				Services		Windows PowerShell (x86)
				Manageability ①	Manageability	Windows PowerShell ISE
74				Events	Events	Windows PowerShell ISE (x86)





- 21. The Internet Information Services (IIS) Manager window appears; expand WEBSERVER (WEBSERVER\Administrator) node and Sites node under the Connections section from the left-hand pane. Select MovieScope site.
- 22. From the middle-pane, double-click on Authentication applet under IIS section.



ГГ

EC-Council

()





23. Authentication wizard appears, select Anonymous Authentication and click Disable from the right-pane under Actions section.

24. Similarly, select Basic Authentication and click Enable from the right-pane under Actions section.

Note: For demonstration purposes, here, we are using Basic authentication mechanism where plaintext credentials are used to authenticate and access the website which is not a safe practice. In real practice, it is advised to use Windows authentication which is considerably more secure than basic authentication.

Connections				Alerts
Q,• 🔒 🖄 IØ,	Authentication			SSL is not enabled for this site and enabled for this
Start Page	Group by: No Grouping -	sent in clear text over the		
- Application Pools	Name	Status	Response Type	wire.
V 👩 Sites	Anonymous Authentication	Disabled		Actions
> 🚯 Default Web Site	ASP.NET Impersonation	Disabled		Disable
> e Demor i Psite	Basic Authentication	Enabled	HTTP 401 Challenge	Edit
- monocope				
	Features View 🌇 Content View	4		







26. In the login page, the attacker username will be selected by default. Enter password as toor in the Password field and press Enter to log in to the machine.

Note: If a Parrot Updater pop-up appears at the top-right corner of Desktop, ignore and close it.

Note: If a Question pop-up window appears asking you to update the machine, click No to close the window.

27. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.

28. A Parrot Terminal window appears. In the terminal window, type sudo su and press Enter to run the programs as a root user.

29. In the [sudo] password for attacker field, type toor as a password and press Enter.

Note: The password that you type will not be visible.

30. Now, type cd and press Enter to jump to the root directory.

31. In the Terminal window, type tcpdump -vv dst 10.10.1.16 and port www -w test.pcap and press Enter to capture HTTP traffic of the target machine Web Server (10.10.1.16).

Note: --vv: Indicate a verbose output, dst: Indicate the destination, -w: To write raw packets to a file (here, test.pcap)

32. The tcpdump starts listening on eth0 interface to capture HTTP packets, as shown in the screenshot below.





33. Click the Firefox icon from the top section of Desktop to launch the Mozilla Firefox browser.

- 34. The Mozilla Firefox window appears; type http://www.moviescope.com into the address bar and press Enter.
- 35. Authentication Required pop-up appears; type Administrator and admin@123 as User Name and Password and click OK.

Note: If Would you like Firefox to save this login for moviescope.com? pop-up appears, click Don't Save.









36. You have now logged successfully to access the website, as shown in the screenshot below.

EXERCEPT INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP





37. Switch to terminal window and press Ctrl+C to terminate intercepting network traffic.

EXERCEPT INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP

🖲 🔵 🕘 Parro	ot Terminal		
File Edit View Search Terminal Help			
<pre>[attacker@parrot]-[~] \$sudo su</pre>			
[sudo] password for attacker:			
[root@parrot]+[/home/attacker]			
#cd			
[root@parrot]-[~]			
#tcpdump -vv dst 10.10.1.16 and port www -w tes	st.pcap		
tcpdump: listening on eth0, link-type ENIOMB (Etherr	iet), capture	size 262144	bytes
C/3 packets captured			
73 packets received by filter			
U packets dropped by kernel			





- 38. Type Is and press Enter.
- 39. You can observe a file name test.pcap has been created in the /root directory.



^C73 packets captured 73 packets received by filter 0 packets dropped by kernel [root@parrot]+[~] #ls avml Desktop lazys3 social-engineer-toolkit test.pcap buck-security-master DSSS shellphish Templates volatility-master [root@parrot]+[~] #





40. Now, type wireshark test.pcap and press Enter to open the file using Wireshark.

EXERCEPT INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP [root@parrot]+[~]
 #ls
avml Desktop lazys3 social-engineer-toolkit test.pcap
buck-security-master DSSS shellphish Templates volatility-master
 [root@parrot]-[~]
 #wireshark test.pcap]





41. Click to select any HTTP message with GET request.

42. From the middle-pane, expand Hypertext Transfer Protocol node. Under Hypertext Transfer Protocol node, expand Authorization node. Note: If you do not see Authorization node in the first block of HTTP packets then select HTTP GET packet from a different block of HTTP packets.

43. You can observe that the credentials are displayed because the HTTP packets are unencrypted which makes them vulnerable to packet sniffing. Close the Wireshark window.



File Ed	it <u>V</u> iew <u>G</u> o	Capture Analy	e <u>S</u> tatistics T	elephony	Wireless Tools	Help			
	20	i 🖹 🗎	्र 🔶	• 🖀	¥ 👤 🗌	Ð.		Π	
Apply	a display filter	<ctrl-></ctrl->							
No. 32 33 34 35 36	Time 312.454813 322.481456 322.526874 322.911579 323.079392 323.079510	Source 10.10.1.13 10.10.1.13 10.10.1.13 10.10.1.13 10.10.1.13 10.10.1.13	Destin 10.10 10.10 10.10 10.10 10.10 10.10	ation .1.16 .1.16 .1.16 .1.16 .1.16 .1.16	Protocol I TGP TCP HTTP TCP HTTP	ength Info 66 [TC 66 [TC 445 GET 66 539 421 GET 74 540	P Keep-Al P Keep-Al / HTTP/1 94 - 80 [/css/com	Live] 53994 80 [ACK] Seq=324 Ack= Live] 53994 80 [ACK] Seq=324 Ack= 1.1 ACK] Seq=704 Ack=6058 Win=62464 Ler mon.css HTTP/1.1 (SWI) Secretor Min=62404 Lerror MSS=146/	1510 Win 1510 Win
37 38 39	323.079810 323.079876 323.079957 34: 445 byte	10.10.1.13 10.10.1.13 10.10.1.13	10.10 10.10 10.10	.1.16 .1.16 .1.16	TCP TCP TCP	74 540 74 540 66 540	02 - 80 [04 - 80 [02 - 80 [[SYN] Seq=0 Win=64240 Len=0 MSS=1460 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TS	SACK_P SACK_P Sval=121
Etheri Interi Transi Hyper	net II, Src: net Protocol mission Contr text Transfer	MS-NLB-PhysSer Version 4, Src ol Protocol, S Protocol	ver-21_5d:20:4 : 10.10.1.13, rc Port: 53994	f:3e (02:1 Dst: 10.10 , Dst Port	15:5d:20:4f:3e), 0.1.16 1: 80, Seq: 325,	Dst: MS Ack: 151	NLB-Phys	Server-21_5d:20:4f:42 (02:15:5d:20: 379	4f:42)
► GE Hos Use Acc Acc DN Cor Upg ▼ Aut	/ HTTP/1.1 st: www.movie er-Agent: Moz sept: text/ht sept-Language sept-Encoding T: 1r\n nnection: kee grade-Insecur thorization:	r\n scope.com\r\n illa/5.0 (Winde ml,application : en-US,en;q=0 : gzip, deflate p-alive\r\n e-Requests: 1\n Basic QWRtaW5pd	wws NT 10.0; ry xhtml+xml,app 5\r\n 2\r\n 3NyYXRvcjphZG:	v:68.0) Ge lication/x 1pbkAxMjM=	cko/20100101 Fi ml;q=0.9,*/*;q=	refox/68. 0.8\r\n	0\r\n		
\r\ [Ft [H] [Ne	TP request U TP request 2 rev request 1 ext request 1	Administrator RI: http://www /7] n frame: 22] n frame: 36]	adming123 moviescope.com	<u>n/]</u>					
0040 fa 0050 00 0060 5 0070 20 0080 35 0090 31 00a0 65 00b0 72 00c0 70	1 55 47 45 54 1 0a 48 67 73 1 73 63 67 70 1 41 67 65 66 2 30 20 28 30 22 30 30 30 63 6b 67 78 2 50 66 67 78 2 74 3a 20 74	20 2f 20 48 5 74 3a 20 77 7 65 2e 63 6f 6 74 3a 20 40 6 57 69 6e 64 6 20 72 76 3a 3 32 30 31 30 32 327 38 38 2e 33 65 78 74 2f 6	4 54 50 2f 31 2 7 7 2e 6d 6f 7 4 0d 0a 55 73 6 6 7 7 3e 6 6c 6c 7 7 3e 9 6c 6c 6c 7 7 73 20 4e 5 53 2e 30 29 23 30 31 20 4e 5 5 3e 2e 31 30 31 20 4e 5 5 3e 2e 3i 3i 3i 3i 2i 4e 4i 3e 6i 3e 3e 3i 3i 3i 3i 3e 4e 3e 3e 3i 3i 3e <	2e 31 UU 16 69 - 15 72 23 11 2f -A 14 20 5.0 12 6 9 ecl 16 69 ecl 33 65 re 13 65 re 51 70 pt	SET / HTTP/1.1 Host: www.movi cope.c om User gent: Mozilla/ 0 (Win dows NT .0; rv :68.0) G ko/201 00101 Fi fox/68 .0 Acce : text /html,ap				h
07	Credentials (ht	tp.authbasic)						Packets: 171 · Displayed: 171 (100.0%)	Profile: Defau





44. Now, in a similar way, we will intercept SSH traffic and observe the packet content.

45. In the terminal window, type tcpdump -vv dst 10.10.1.79 and port ssh -w test2.pcap and press Enter to capture SSH traffic to the target machine Admin Machine-2 (10.10.1.79).

46. The tcpdump starts listening on eth0 interface to capture SSH traffic, as shown in the screenshot below.



#wi	reshark test.	pcap					
QStandar	dPaths: XDG R	UNTIME DIR no	t set, defa	ulting to '/	/tmp/runtime	-root'	
F[root@	parrot]-[~]						
L # <mark>tc</mark>	pdump -vv dst	10.10.1.79 a	nd port ssh	-w test2.pd	сар		
tcpdump:	listening on	eth0, link-t	ype EN10MB	(Ethernet),	capture size	e 262144	bytes
Got 0							





47. Now, click the MATE Terminal icon at the top of the Desktop window to open another Terminal window.

48. A Parrot Terminal window appears. In the terminal window, type sudo su and press Enter to run the programs as a root user.

49. In the [sudo] password for attacker field, type toor as a password and press Enter.

Note: The password that you type will not be visible.

50. Now, type cd and press Enter to jump to the root directory.

51. Type ssh sam@10.10.1.79 and press Enter to establish SSH connection with Admin Machine-2.

Note: If connection attempt prompt appears, type yes and press Enter.

52. In the password field, type admin@123 and press Enter.

53. You can observe that a remote connection has been established, as shown in the screenshot below.

					sam@sam-Virtual-Machine: ~	
\bigcirc			62	F	File Edit View Search Terminal Help	
					- attacker@parrot - ~]	
		Пп			\$sudo su	
				[[sudo] password for attacker:	
				\bigcirc	# # d	T
		Leγ				•
		\bigcirc	\overline{n}		#ssh sam@10.10.1.79 10.1.10 and port www.w.test.pree	
$\Box \Box$			U	/2, 1	The authenticity of host '10.10.1.79 (10.10.1.79)' can't be established.	
$(\cup /)$					ECDSA key fingerprint is SHA256:RM843/oUEthHrOcnTw6n0Us6WVfle2H1iaDhtuuXGa8.	
	п				Are you sure you want to continue connecting (yes/no/[fingerprint])? yes	
		\mathbb{N}			samala la 1 79's password.	
$\wedge \wedge$		\sum			Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-99-generic x86 64)	
	ΠΠΠ	<i>μ</i> Ωζ	>		* Documentation: https://help.ubuntu.com	
\bigcirc			\leq		* Management: https://landscape.canonical.com	
	()	(\bigcirc)		(\bigcirc)	* Support: https://ubuntu.com/advantage	
	<u> </u>					
ПпП	\bigcap	>>				
		\leq	\sim	Т	The programs included with the Ubuntu system are free software;	
		F -			the exact distribution terms for each program are described in the	
\bigtriangledown				1	individual files in /usr/share/doc/*/copyright.	
		ПоП			Ubuntu comes with ARSOLUTELY NO WARRANTY, to the extent permitted by	
				a a	applicable law.	
		\square				
		4		ι s	sam@sam-Virtual-Machine:~\$	
				1		





54. Type exit and press Enter to terminate the connection.



Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

sam@sam-Virtual-Machine:~\$ exit
logout
Connection to 10.10.1.79 closed.
[root@parrot]-[~]
#



55. Now, switch back to the previous terminal window and press Ctrl+C to terminate packet capturing by tcpdump.

EXERCEPT INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP

	Parrot Terminal
<u>File Edit View Search Terminal</u>	Help
<pre>[root@parrot]-[~] #wireshark test.pcap</pre>	
QStandardPaths: XDG_RUNTIME	_DIR not set, defaulting to '/tmp/runtime-root'
<pre>[root@parrot]-[~]</pre>	
<pre>#tcpdump -vv dst 10.10</pre>	.1.79 and port ssh -w test2.pcap
tcpdump: listening on eth0,	link-type EN10MB (Ethernet), capture size 262144 bytes
^C50 packets captured	
50 packets received by filt	erNO WARRANTY, to the extent permitted by
0 packets dropped by kernel	
[root@parrot]-[~]	
# Virtnel-Rednine5	



56. Type wireshark test2.pcap and press Enter to open the captured packet file using Wireshark.

57. The Wireshark window appears, displaying captured packets, as shown in the screenshot below.

EXERCEPT NTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP

ile <u>E</u> dit <u>V</u> iew <u>G</u>			(csterbrah	(as superaser)	
	o Capture Analyze	Statistics Telephony W	ireless Tools	Help	
			-		
		Y 🖛 🗭 🚟 🚹			
A . A			Summer of Street		
Apply a display filt	ter <ctri-></ctri->				len
Time	Source	Destination	Protocol	Length Info	
1 0.000000	10.10.1.13	10.10.1.79	TCP	74 53560 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
2 0.000335	10.10.1.13	10.10.1.79	TCP	66 53560 - 22 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=422
3 0.000939	10.10.1.13	10.10.1.79	SSHv2	98 Client: Prot	ocol (SSH-2.0-OpenSSH_8.3p1 Debian-1)
4 0.009973	10.10.1.13	10.10.1.79	TCP	66 53560 - 22 [ACK] Seq=33 Ack=42 Win=64512 Len=0 TSval=4
5 0.010119	10.10.1.13	10.10.1.79	SSHv2	1578 Client: Key	Exchange Init
6 0.010986	10.10.1.13	10.10.1.79	TCP	66 53560 - 22 [ACK] Seq=1545 Ack=1018 Win=64512 Len=0 TSv
7 0.012899	10.10.1.13	10.10.1.79	SSHv2	114 Client: Diff	ie-Hellman Key Exchange Init
8 0.017122	10.10.1.13	10.10.1.79	TCP	66 53560 - 22 [ACK] Seq=1593 Ack=1382 Win=64512 Len=0 TSv
9 19.327866	10.10.1.13	10.10.1.79	SSHv2	82 Client: New	Keys
10 19.369670	10.10.1.13	10.10.1.79	SSHv2	110 Client: Encr	ypted packet (len=44)
11 19.370332	10.10.1.13	10.10.1.79	TCP	66 53560 - 22 [ACK] Seg=1653 Ack=1426 Win=64512 Len=0 TSv
12 19.370432	10.10.1.13	10.10.1.79	SSHv2	126 Client: Encr	ypted packet (len=60)
13 19.371580	10.10.1.13	10.10.1.79	TCP	66 53560 - 22 [ACK] Seg=1713 Ack=1478 Win=64512 Len=0 TSv
0 02 15 5d 17	1b 3f 02 15 5d 17 11	a 40 08 00 45 00	-2 1- Ø-E		
0 02 15 5d 17 3 0 03 2 6b 0d 3	1b 3f 02 15 5d 17 11 40 00 40 06 b9 3f 02) 40 88 80 45 80 ··]. 1 8a 81 8d 8a a -<€	-?]-@-E @@?		
02 15 5d 17 0 00 3c 5b 0d 4 0 14 f 1 38 0	1b 3f 02 15 5d 17 11 40 00 40 06 b3 f 0; 00 16 54 15 ca 3e M	9 40 88 80 45 80 · .] • 88 81 84 88 80	?].@.E 0.0.? 		
 02 15 5d 17 00 3c 6b 6d 01 4f d1 38 fa f0 16 9e 	1b 3f 02 15 5d 17 11 40 00 40 06 b9 3f 0; 00 16 54 15 ca 3e 0; 00 00 02 04 05 b4 0;	0 49 98 99 45 99 ·] 1 9a 91 9d 9a 9a <k 9 99 99 90 a9 22 • 8 4 92 98 9a 10 12</k 	-?··]·@·E @@:?·· ·T·>···		
0 02 15 5d 17 0 03 36 04 01 4f 138 0 a f0 16 9e 0 5 2 90 90 90	1b 3f 02 15 5d 17 11 40 00 40 06 b9 3f 0; 00 16 54 15 ca 3e 0; 00 00 02 04 05 b4 0; 00 00 01 03 03 0a	0 40 88 60 45 60 ·] 1 8a 61 6d 8a 8a 66 69 69 a8 92 · 8 4 82 88 8a [D] 72	-?]-@-E @@-?- .T->		•
0 02 15 5d 17 0 00 3c 6b 0d 01 4f d1 38 0 fa f0 16 9e 0 15 2e 00 00	1b 3f 02 15 5d 17 11 40 00 40 06 b9 3f 0 00 16 54 15 ca 3e 0 00 06 02 04 05 b4 0 00 00 01 03 03 0a	0 40 98 90 45 90] 1 93 61 9d 9a 9a <k 9 69 90 90 92 08 4 92 98 9a 10 12 1 12 1</k 	-?]-@-E @@-? T->		Þ
02 15 5d 17 00 3c 6b 0d 01 4f d1 38 16 9e 16 9e 0 12 2e 00 00 0	1b 3f 02 15 5d 17 11 40 00 40 06 b9 3f 0; 00 16 54 15 ca 3e 0; 00 00 02 04 05 b4 0; 00 00 02 04 05 b4 0; 00 00 01 03 03 0a	0 40 08 00 45 00] 0 80 61 0d 0a 0a 0 90 60 00 a0 020 4 02 08 0a [b f 2]	-?]-@-E @@-? T->		•
02 15 5d 17 00 3c 6b 0d 01 4f d1 38 10 fa f0 16 9e 01 2e 00 00 0	1b 3f 02 15 5d 17 11 40 00 40 06 03 3f 0; 00 16 54 15 ca 3e 0 00 00 02 04 05 b4 0; 00 00 01 03 03 0a	0 40 88 80 45 80 ·] 0 80 81 80 88 80 · << 0 80 80 80 80 22 · 0 80 80 80 80 22 · 0 80 80 80 70 72 ·	?].@.E @.@.?. T.>		•
0 02 15 5d 17 0 00 3c 6b 6d 0 14 f d1 38 0 fa f0 16 9e 0 51 22 00 00 0	1b 3f 02 15 5d 17 11 40 00 40 06 b9 3f 0 00 16 54 15 ca 3e 0 00 00 02 04 05 b4 00 00 01 03 03 0a	0 40 98 00 45 00 1 0a 01 0d 0a 0a 0 00 00 00 a0 02 0 2 08 0a 10 12 1 02 08 0a	-?]-@-E @@? T->		•
02 15 5d 17 00 3c 6b 0d 01 4f d1 38 16 fa f0 16 9e 01 2c 00 00 0	1b 3f 02 15 5d 17 11 40 00 40 06 b9 3f 0; 00 16 54 15 ca 3e 0 00 00 02 04 05 b4 0 00 00 01 03 03 0a	0 40 08 00 45 00 1 0 1 0 0 0a 0a 0 0 0 0 0 0 0 0 2 1 0 2 08 0a (b f 2) (a b f f 2)	-?]-@-E @@-? T->		•
00 02 15 5d 17 00 03 C6 bd 03 01 4f dd 13 16 40 16 9e 10 01 22 00 00 0	1b 3f 02 15 5d 17 11 40 00 40 06 03 f 0; 00 16 54 15 ca 3e 0 00 06 02 04 05 b4 04 00 00 01 03 03 0a	0 40 08 00 45 00] 0 40 08 00 45 00] 0 00 00 00 00 2 0 00 00 00 00 02 1 02 08 0a 10 12 1 02 08 0a 10 12	?].@.E @@.? T.>		•
00 02 15 5d 17 00 3c 6b 0d 01 4f 138 30 fa f0 16 9e 01 25 00 00 0	1b 3f 02 15 5d 17 11 40 00 40 06 b3 f 0; 00 16 54 15 ca 3e 0 00 00 02 04 05 b4 04 00 00 01 03 03 0a	0 40 98 90 45 90 1 93 91 9d 9a 9a 9 69 90 90 a0 92 0 8 1 92 98 9a 10 12 1	?].@.E @@.? .T.>		Packata EQ. Displayed EQ.(100.0%)



58. Click to select SSHv2 protocol packet with Info as Client: Diffie-Hellman Key Exchange Init.

- 59. In the middle-pane expand SSH Protocol node. Under SSH Protocol node, expand SSH Version 2 node and Key Exchange node.
- 60. You can observe that the captured password is in encrypted form, as shown in DH client e option.

EXERCEPT INTERCEPT NETWORK TRAFFIC USING WIRESHARK

File	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>Analyze</u>	Statistics Telephony M	ireless <u>T</u> ools	Help		
1		🔁 🗙 🗋	۹ 🔶 🛸 🖀 🕯] 🛃 生 آ	€ Q	. €. Ⅲ	
	Apply a display filte	r <ctrl-></ctrl->					
lo.	Time	Source	Destination	Protocol	Length Info		
	1 0.000000	10.10.1.13	10.10.1.79	TCP	74 53560 -	- 22 [SYN] Seq=0 Win=64240 Len=0	MSS=1460 SACK_P
	2 0.000335	10.10.1.13	10.10.1.79	TCP	66 53560 -	- 22 [ACK] Seq=1 Ack=1 Win=64512	Len=0 TSval=422
	4 0 000939	10.10.1.13	10.10.1.79	TCD	98 Ctient:	22 [ACK] Seg=22 Ack=42 Win=6451	2 Lon-Q TSval-4
	5 0 010110	10.10.1.13	10.10.1.79	SSHv2	1578 Client:	Kev Exchange Init	c cen=o iSvat=4
	6 0.010986	10.10.1.13	10.10.1.79	TCP	66 53560	- 22 [ACK] Seg=1545 Ack=1018 Win=	64512 Len=0 TSv
	7 0.012899	10.10.1.13	10.10.1.79	SSHv2	114 Client:	Diffie-Hellman Key Exchange Ini	
	8 0.017122	10.10.1.13	10.10.1.79	TCP	66 53560 -	- 22 [ACK] Seg=1593 Ack=1382 Win=	64512 Len=0 TSv
	9 19.327866	10.10.1.13	10.10.1.79	SSHv2	82 Client:	: New Keys	
	10 19.369670	10.10.1.13	10.10.1.79	SSHv2	110 Client:	: Encrypted packet (len=44)	
	11 19.370332	10.10.1.13	10.10.1.79	TCP	66 53560 -	22 [ACK] Seq=1653 Ack=1426 Win=	64512 Len=0 TSv
	12 19.370432	10.10.1.13	10.10.1.79	SSHv2	126 Client:	: Encrypted packet (len=60)	
	13 19.371580	10.10.1.13	10.10.1.79	TCP	66 53560 -	- 22 ACK Seq=1/13 ACK=14/8 Win=	54512 Len=0 ISV
	Padding Leng	gth: 6 e Code: Diffie-Hellma	n Key Exchange Init (3	30)			
-	DH client	ecision integer Ler	gtn: 32 5h85e3h8d6h58a766f3d9r	ReeROAANROOR	21.5		
	Padding Str:	ing: 000000000000	505555566556476676456	.053000000aa0.			
	[Direction: cl	ient-to-server]					
082	0 01 4f d1 38 00	0 16 54 15 d0 47 7	bc 9b c7 80 18 0.8	3 · · T · · G · · · · ·			
	0 00 3f 16 c6 00	00 01 01 08 0a f	o f2 e1 3b 6e 49 ·?··	·····;nI			
904	0 9b 35 00 00 00	0 2c 06 1e 00 00 0	20 04 0e 92 38 5.	.,			
305	0 Ta 65 D9 50 85	e3 08 06 05 8a /	o 61 30 96 89 98 ·e·[
107	0 00 09 0a a8 85	J aJ 4/ 4/ 03 00 3					
	0000		11				
0	7 DH client o /c	sh dh e) 32 hyter				Packets: 50 - Displayed: 50 (100	0%) Profile: Defai
0	en clience (5:	smanler, 52 bytes				Tackets. 50 Displayed. 50 (100.	Fione. Dela





61. This concludes the demonstration showing how to intercept network traffic using various packet sniffing tools.

- 62. Close all open windows.
- 63. Turn off the Attacker Machine-2 virtual machine.





EXERCISE 2: APPLY VARIOUS FILTERS IN WIRESHARK

Wireshark provides numerous filters that can be applied to obtain only the required packets.

LAB SCENARIO

Wireshark filters traffic flowing through the entire network. This traffic contains various kinds of data packets associated with various protocols flowing between the source and destination. Therefore, searching for a specific packet, port, or an IP address manually is extremely difficult. In such cases, applying Wireshark filters helps a security professional track down a huge amount of traffic and discover the intended packets. A security professional must have a good knowledge of various Wireshark filters that help you narrow down the traffic and obtain the desired result.

OBJECTIVE

This lab will help you become familiar with various Wireshark filters.

OVERVIEW OF TROJAN

Wireshark has various filters that help you filter packets containing the following:

- Source IP address
- Destination IP address
- Internet Control Message Protocol (ICMP) traffic etc.







Note: Ensure that Admin Machine-1, Web Server and PfSense Firewall virtual machines are running.

1. In the Admin Machine-1 virtual machine, click Type here to Search field and type Wireshark. Select and open the Wireshark App.

2. The Wireshark main window appears.

Note: If Software Update Window appears, click on Skip this version.

3. Select Ethernet as interface and click the Start capturing packets fin icon to start capturing the network traffic.



The Wireshark Network Analyzer	-	đ	×
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp			
◢ ◼ ₫ ◉ <mark>-</mark> 🗅 🗙 🖻 ٩ ↔ ∞ ∞ 주 ⊉ 🚍 🔍 Q, Q, Q, 표			
Apply a display filter <ctrl-></ctrl->			• +
Welcome to Wireshark			
Carbon			
Capture			
using this filter: 📙 Enter a capture filter 💌 All interfaces shown	•		
Local Area Connection" 9			
Local Area Connection* 8			
Ethernet			
Local Area Connection* 7			
Adapter for loopback traffic capture / / / / / / /			





- 4. Next, in order to generate the network traffic between the local machine and Web Server machines, we will browse the website hosted on Web Server virtual machine.
- 5. Minimize the Wireshark window.
- 6. Open any web browser (here, Mozilla Firefox) and type http://www.luxurytreats.com in the url field and press Enter.

Note: If Default Browser pop-up appears, click Not now.

Note: Type the complete URL www.luxurytreats.com or http://www.luxurytreats.com as mentioned in the above instruction. Do not type an incomplete URL such as luxurytreats.com; otherwise, it will redirect you to some external website on the internet.









7. Now, navigate back to the Wireshark window and click Stop capturing packets icon (red color icon) in the tool bar (top-left corner) to stop the packet capturing.

EXERCEPT NTERCEPT NETWORK TRAFFIC USING WIRESHARK

11	r a display filter <c< th=""><th>trl-/></th><th></th><th></th><th></th></c<>	trl-/>			
	Time	Source	Destination	Protocol	Length Info
767	71 239.523078	10.10.1.2	192.168.1.12	TCP	66 [TCP Retransmission] 49824 + 7680 [SYN] Seq=0 Win=64240 Len=0
767	72 242.785659	10.10.1.2	142.250.187.195	TCP	55 [TCP Keep-Alive] 49822 → 80 [ACK] Seq=388 Ack=703 Win=262400 L
767	73 242.790014	142.250.187.195	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 80 → 49822 [ACK] Seq=703 Ack=389 Win=6681
767	74 244.522916	117.18.232.200	10.10.1.2	TLSv1.2	118 Application Data
767	75 244.522918	117.18.232.200	10.10.1.2	TLSv1.2	85 Encrypted Alert
767	76 244.522919	117.18.232.200	10.10.1.2	TCP	54 443 → 49807 [FIN, ACK] Seq=8459 Ack=949 Win=68096 Len=0
767	77 244.523059	10.10.1.2	117.18.232.200	TCP	54 49807 → 443 [ACK] Seq=949 Ack=8460 Win=260864 Len=0
Ethe Inte Use	ernet II, Src: ernet Protocol Datagram Prot	Microsot_08:cc:52 (0 Version 4, Src: 10.1 Dcol, Src Port: 5709	0:15:5d:08:cc:52), Dst 0.1.2, Dst: 8.8.8.8 12, Dst Port: 53	t: Microsof	_08:cc:4† (00:15:5d:08:cc:4†)
0	ain Name System	(query)			





- 8. The Filter field at the top of the Wireshark main window allows you to apply various filters that help narrow down the traffic including filter traffic by protocol.
- 9. To view the HTTP-specific traffic flowing in your network, type http in the filter field and press Enter. By applying this filter, Wireshark filters and displays HTTP traffic flowing through the network.

EXERCEPT INTERCEPT NETWORK TRAFFIC USING WIRESHARK *Cale and

-	ethernet				- 5	~
Eile	e <u>E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze Statis	stics Telephony <u>W</u> i	reless <u>T</u> ools <u>H</u>	elp	
4	🔳 🧟 💿 📙 📑	🗙 🖸 🭳 👄 📾 😫	Ŧ 🛓 📃 🗨	Q Q II		
	http					
No.	Time	Source	Destination	Protocol	Length Info	
4+	36 17.385165	10.10.1.2	34.107.221.82	HTTP	355 GET /canonical.html HTTP/1.1	
4-	38 17.392065	34.107.221.82	10.10.1.2	HTTP	356 HTTP/1.1 200 OK (text/html)	
1	64 17.954533	10.10.1.2	34.107.221.82	HTTP	357 GET /success.txt?ipv4 HTTP/1.1	
1	66 17.959135	34.107.221.82	10.10.1.2	HTTP	274 HTTP/1.1 200 OK (text/plain)	
8	210 19.385015	10.10.1.2	117.18.237.29	OCSP	435 Request	
1	218 19.463301	10.10.1.2	117.18.237.29	OCSP	435 Request	
E.	231 19.549016	117.18.237.29	10.10.1.2	OCSP	853 Response	
E.	232 19.549699	10.10.1.2	117.18.237.29	OCSP	435 Request	
	237 19.560006	10.10.1.2	117.18.237.29	OCSP	435 Request	
В.	244 19.620276	117.18.237.29	10.10.1.2	OCSP	853 Response	
	258 19.713498	117.18.237.29	10.10.1.2	OCSP	853 Response	
Ε.	262 19.721026	117.18.237.29	10.10.1.2	OCSP	853 Response	
8	330 24.463216	10.10.1.2	172.217.16.227	OCSP	441 Request	
1	345 24.548295	10.10.1.2	172.217.16.227	OCSP	441 Request	
1	348 24.567897	172.217.16.227	10.10.1.2	OCSP	755 Response	
	350 24.650930	172.217.16.227	10.10.1.2	OCSP	755 Response	
н.	476 38.730982	10.10.1.2	10.10.1.16	HTTP	395 GET / HTTP/1.1	
1	493 38.752079	10.10.1.16	10.10.1.2	HTTP	295 HTTP/1.1 200 OK (text/html)	
12	497 39.330712	10.10.1.2	10.10.1.16	HTTP	379 GET /App Themes/Default/00.reset.css HTTP/1.1	- 1
>	Frame 36: 355 byte	es on wire (2840 bits), 355 bytes capt	ured (2840 bit	s) on interface \Device\NPF_{26C51D69-3344-487E-9225-4309C2E8338A}, i	id 0
>	Ethernet II, Src:	Microsof_08:cc:52 (0	0:15:5d:08:cc:52)	, Dst: Microso	f_08:cc:4f (00:15:5d:08:cc:4f)	
>	Internet Protocol	Version 4, Src: 10.1	0.1.2, Dst: 34.10	7.221.82		
2	Transmission Contr	ol Protocol, Src Por	t: 49861, Dst Por	t: 80, Seq: 1,	Ack: 1, Len: 301	-
2	Hypertext Transfer	Protocol				
00	00 00 15 5d 08 cc	4f 00 15 5d 08 cc	52 08 00 45 00	· 1 · 0 · 1 · . R ·	E •	
00	10 01 55 ee 5f 40	00 80 06 00 00 0a	0a 01 02 22 6b	U. @	"k	- 11
66	20 dd 52 c2 c5 00	50 63 51 c2 fe 98	04 41 21 50 18	R····PcQ ·····A	P -	
00	30 04 03 0c 11 00	00 47 45 54 20 2f	63 61 6e 6f 6e	·····GE T /car	ion	
00	40 69 63 61 6c 2e	68 74 6d 6c 20 48	54 54 50 2f 31	Ical.htm 1 HTTP	/1	
00	2e 31 0d 0a 48	67 /3 /4 3a 20 64	65 /4 65 63 74	I Most : dete	(CT	
00	70 6f 6d 0d 0a 55	73 65 72 2d 41 67	65 6e 74 3a 20	m llser -Agent	1. E	
00	80 4d 6f 7a 69 6c	6c 61 2f 35 2e 30	20 28 57 69 6e M	lozilla/ 5.0 (1	lin	
0						



10. To view the TCP-specific traffic flowing in your network, type tcp in the filter field and press Enter. By applying this filter, Wireshark filters TCP traffic flowing through the network and displays.

EXERCEPT NTERCEPT JSING WIRESHARI

-	*Ethernet					- D	×
Eile	e <u>E</u> dit !	View Go Ca	pture <u>Analyze</u> <u>Statistic</u>	s Telephony <u>W</u> ireless	Tools Hel	p	
4		o 📘 🗅 🗙	C 9 0 0 0 7		TR		
	tcp						-+
No.	Tir	me	Source	Destination	Protocol	Length Info	-
	18 17	7.210128	10.10.1.2	13.35.199.113	TCP	54 49860 → 443 [ACK] Seg=1 Ack=1 Win=263424 Len=0	
	19 17	7.214825	10.10.1.2	13.35.199.113	TLSv1.3	571 Client Hello	
	20 17	7.217540	13.35.199.113	10.10.1.2	TCP	54 443 → 49860 [ACK] Sea=1 Ack=518 Win=43008 Len=0	-
	21 17	7.219540	13,35,199,113	10.10.1.2	TLSv1.3	1494 Server Hello, Change Cipher Spec, Application Data	
	22 17	7,219541	13,35,199,113	10.10.1.2	TCP	1494 443 → 49860 [PSH. ACK] Seg=1441 Ack=518 Win=67072 Len=1440_	
	23 17	7.219610	10.10.1.2	13.35.199.113	TCP	54 49860 + 443 [ACK] Sea=518 Ack=2881 Win=263424 Len=0	
	24 17	7.221639	13.35.199.113	10.10.1.2	TLSv1.3	1153 Application Data, Application Data, Application Data	-
	25 17	7.252641	10.10.1.2	13.35.199.113	TLSv1.3	118 Change Cipher Spec, Application Data	
	26 17	7.252835	10.10.1.2	13.35.199.113	TLSv1.3	340 Application Data	
	27 17	7.256361	13.35.199.113	10.10.1.2	TCP	54 443 → 49860 [ACK] Seq=3980 Ack=582 Win=67072 Len=0	
	28 17	7.256362	13.35.199.113	10.10.1.2	TCP	54 443 → 49860 [ACK] Seq=3980 Ack=868 Win=68096 Len=0	
	29 17	7.256943	13.35.199.113	10.10.1.2	TCP	1494 443 + 49860 [ACK] Seq=3980 Ack=868 Win=68096 Len=1440 [TCP	-
	30 17	7.256944	13.35.199.113	10.10.1.2	TLSv1.3	901 Application Data	
	31 17	7.256995	10.10.1.2	13.35.199.113	TCP	54 49860 → 443 [ACK] Seq=868 Ack=6267 Win=263424 Len=0	
E.	33 17	7.376305	10.10.1.2	34.107.221.82	TCP	66 49861 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC	-
	34 17	7.382071	34.107.221.82	10.10.1.2	TCP	66 80 → 49861 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430_	-
	35 17	7.382151	10.10.1.2	34.107.221.82	TCP	54 49861 + 80 [ACK] Seq=1 Ack=1 Win=262912 Len=0	
+	36 17	7.385165	10.10.1.2	34.107.221.82	HTTP	355 GET /canonical.html HTTP/1.1	
	37 17	7.392064	34.107.221.82	10.10.1.2	TCP	54 80 → 49861 [ACK] Sea=1 Ack=302 Win=66816 Len=0	~
>	Frame 36	5: 355 bytes	on wire (2840 bits),	355 bytes captured (2	2840 bits) on interface \Device\NPF_{26C51D69-3344-487E-9225-4309C2E8338A},	id 0
>	Ethernet	t II, Src: Mi	crosof_08:cc:52 (00:	L5:5d:08:cc:52), Dst:	Microsof	_08:cc:4f (00:15:5d:08:cc:4f)	
>	Internet	t Protocol Ve	rsion 4, Src: 10.10.	L.2, Dst: 34.107.221.8	32		
>	Transmis	ssion Control	Protocol, Src Port:	49861, Dst Port: 80,	Seq: 1, /	Ack: 1, Len: 301	
>	Hypertex	ct Transfer P	rotocol				
-							_
00	00 00 1	5 5d 08 cc 4	f 00 15 5d 08 cc 52	08 00 45 00].0.	·] · · R · · E		-
00	10 01 5	5 ee 51 40 0	0 80 06 00 00 0a 0a	01 02 22 6b ·U·_@··	o	'K	
	30 04 0	3 00 11 00 0	0 47 45 54 20 2f 63	61 6e 6f 6e	E T /canc		
00	40 69 6	3 61 6c 2e 6	8 74 6d 6c 20 48 54	54 50 2f 31 ical.ht	m 1 HTTP/	1	
69	50 2e 3	1 0d 0a 48 6	f 73 74 3a 20 64 65	74 65 63 74 .1 · Hos	t : detec	t	
00	60 70 6	if 72 74 61 6	c 2e 66 69 72 65 66	6f 78 2e 63 portal.	f irefox.	c	
00	70 6f 6d	d 0d 0a 55 7	3 65 72 2d 41 67 65	6e 74 3a 20 om Use	r -Agent:		
00	80 4d 61	f 7a 69 6c 6	c 61 2f 35 2e 30 20	28 57 69 6e Mozilla	/ 5.0 (Wi	in	*
0							



11. You can also filter traffic based on the source and destination IP addresses. To view traffic originating or destined to a specific IP address, apply the filter ip.addr==10.10.1.16 (the Web Server machine in which luxurytreat.com website is hosted (10.10.1.16)).

EXERCEPT NTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP

4	*Ethern	net				- 0	Х	1
Fil	e Edit	t View Go	Capture Analyze	Statistics Telephony Wirele	ss Tools H	Help		
	-							
-					· ~ #			
	ip.addr:	==10.10.1.16						۲
No.		Time	Source	Destination	Protocol	Length Info		^
	473	38.708137	10.10.1.2	10.10.1.16	TCP	66 49886 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC		
	474	38.709286	10.10.1.16	10.10.1.2	TCP	66 80 → 49886 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460		
	475	38.709366	10.10.1.2	10.10.1.16	TCP	54 49886 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0		
	476	38.730982	10.10.1.2	10.10.1.16	HTTP	395 GET / HTTP/1.1	-	
	477	38.751272	10.10.1.16	10.10.1.2	TCP	1514 80 → 49886 [ACK] Seq=1 Ack=342 Win=2102272 Len=1460 [TCP s	-	
	478	38.751273	10.10.1.16	10.10.1.2	TCP	1514 80 → 49886 [ACK] Seq=1461 Ack=342 Win=2102272 Len=1460 [TC	_	
	479	38.751275	10.10.1.16	10.10.1.2	TCP	1514 80 → 49886 [ACK] Seq=2921 Ack=342 Win=2102272 Len=1460 [TC		
	480	38.751276	10.10.1.16	10.10.1.2	TCP	1514 80 → 49886 [ACK] Seq=4381 Ack=342 Win=2102272 Len=1460 [TC		
	481	38.751277	10.10.1.16	10.10.1.2	TCP	1514 80 → 49886 [ACK] Seq=5841 Ack=342 Win=2102272 Len=1460 [TC		
	482	38.751278	10.10.1.16	10.10.1.2	TCP	1514 80 → 49886 [ACK] Seq=7301 Ack=342 Win=2102272 Len=1460 [TC	_	
	483	38.751279	10.10.1.16	10.10.1.2	TCP	1514 80 → 49886 [ACK] Seq=8761 Ack=342 Win=2102272 Len=1460 [TC		
	484	38.751280	10.10.1.16	10.10.1.2	TCP	1514 80 → 49886 [ACK] Seq=10221 Ack=342 Win=2102272 Len=1460 [T	-	
	485	38.751281	10.10.1.16	10.10.1.2	TCP	1514 80 → 49886 [ACK] Seg=11681 Ack=342 Win=2102272 Len=1460 [T		
	486	38.751282	10.10.1.16	10.10.1.2	TCP	1514 80 → 49886 [ACK] Seg=13141 Ack=342 Win=2102272 Len=1460 [T		
	487	38.751503	10.10.1.2	10.10.1.16	TCP	54 49886 → 80 [ACK] Seq=342 Ack=14601 Win=262656 Len=0		
	488	38.752067	10.10.1.16	10.10.1.2	TCP	1514 80 → 49886 [ACK] Seq=14601 Ack=342 Win=2102272 Len=1460 [T		
	489	38.752071	10.10.1.16	10.10.1.2	TCP	1514 80 → 49886 [ACK] Seq=16061 Ack=342 Win=2102272 Len=1460 [T		
	490	38.752073	10.10.1.16	10.10.1.2	TCP	1514 80 → 49886 [ACK] Seq=17521 Ack=342 Win=2102272 Len=1460 [T		
	491	38.752075	10.10.1.16	10.10.1.2	TCP	1514 80 → 49886 [ACK] Seg=18981 Ack=342 Win=2102272 Len=1460 [T		Y
>	Frame	473: 66 by	tes on wire (528 b	its), 66 bytes captured	(528 bits)	on interface \Device\NPF {26C51D69-3344-487E-9225-4309C2E8338A}, id @	9	1
>	Ether	net II, Sro	: Microsof 08:cc:5	2 (00:15:5d:08:cc:52), D	st: Microso	of 08:cc:55 (00:15:5d:08:cc:55)		
>	Inter	net Protoco	Version 4, Src:	10.10.1.2, Dst: 10.10.1.	16			
>	Trans	mission Con	trol Protocol, Src	Port: 49886, Dst Port:	80, Seq: 0,	, Len: 0		


12. You can also use various conditional operators on IP address filtering to filter traffic based on your preference/requirement. Symbol meaning:

- == Is equal to
- != Not equal to
- \> Is greater than
- < Is lesser than
- \>= Greater than or equal to
- <= Less than or equal to.

13. To view traffic higher than a specific IP address, use the > conditional operator in conjunction with IP address filtering. Apply the filter ip.dst > 10.10.1.16 to find the destination IP addresses greater than the specified IP address.

			ip.dst > 10.1	0.1.16				
	Пп		No. Time	e	Source	Destination	Protocol	Length Info
			443 29.	496923	10.10.1.2	44.239.250.14	TCP	54 49870 → 443 [ACK] Seq=2023 Ack=3993 Win=262144 Len=0
			444 29.	635121	10.10.1.2	117.18.237.29	TCP	55 [TCP Keep-Alive] 49875 → 80 [ACK] Seq=381 Ack=800 Win=2618
			445 29.	735435	10.10.1.2	117.18.237.29	TCP	55 [TCP Keep-Alive] 49874 → 80 [ACK] Seq=762 Ack=1599 Win=262
			446 29.	735477	10.10.1.2	117.18.237.29	TCP	55 [TCP Keep-Alive] 49878 → 80 [ACK] Seq=381 Ack=800 Win=2618
_			448 29.	813525	10.10.1.2	44.239.250.14	TCP	55 [TCP Keep-Alive] 49867 → 443 [ACK] Seq=1521 Ack=3723 Win=6
	\square	TO	451 29.	951703	10.10.1.2	44.239.250.14		55 [TCP Keep-Alive] 49876 → 443 [ACK] Seq=1183 Ack=3723 Win=6
			 452 29.	951734	10.10.1.2	44.239.250.14		55 [TCP Keep-Alive] 49871 → 443 [ACK] Seq=1151 Ack=3723 Win=6
)		Οų	453 29.	967320	10.10.1.2	44.239.250.14	TOP	55 [TCP Keep-Alive] 49877 → 443 [ACK] Seq=1183 Ack=3723 Win=6
			458 34.	170303	10.10.1.2	142.250.200.36	QUIC	1399 Initial, DCID=e9a13f7a9eae1892, SCID=7cf2bc
//			459 34.	170414	10.10.1.2	142.250.200.36	QUIC	1399 Initial, DCID=e9a13f7a9eae1892, SCID=7cf2bc
~			460 34.	570733	10.10.1.2	172.217.16.227	TCP	55 [TCP Keep-Alive] 49881 → 80 [ACK] Seq=387 Ack=702 Win=2624
		\square	462 34.	655451	10.10.1.2	172.217.16.227	TCP	55 [TCP Keep-Alive] 49883 → 80 [ACK] Seq=387 Ack=702 Win=2624
			464 35.	039373	10.10.1.2	192.168.1.100	TCP	66 49885 + 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 S
$\langle \rangle$			465 36.	.043427	10.10.1.2	192.168.1.100	TCP	66 [TCP Retransmission] 49885 → 7680 [SYN] Seq=0 Win=64240 Le
			466 37.	279077	10.10.1.2	13.35.199.113	TOP	55 [TCP Keep-Alive] 49860 → 443 [ACK] Seq=867 Ack=6267 Win=26
/ /	\sim		468 37.	422060	10.10.1.2	34.107.221.82	TCP	55 [TCP Keep-Alive] 49861 → 80 [ACK] Seq=301 Ack=303 Win=2626
			470 37.	985665	10.10.1.2	34.107.221.82	TCP	55 [TCP Keep-Alive] 49866 + 80 [ACK] Seq=303 Ack=221 Win=2626
			472 38.	054806	10.10.1.2	192.168.1.100	TCP	66 [TCP Retransmission] 49885 → 7680 [SYN] Seq=0 Win=64240 Le…
			495 39	257597	10.10.1.2	13.35.199.113	TCP	55 [TCP Keep-Alive] 49868 + 443 [ACK] Seg=2403 Ack=7274 Win=2
<u>с</u>	\bigcirc	(5)	<pre>> Frame 472 > Ethernet > Internet > Transmiss</pre>	: 66 bytes II, Src: № Protocol V ion Contro	; on wire (528 bi Nicrosof_08:cc:52 /ersion 4, Src: 1 Dl Protocol, Src	<pre>ts), 66 bytes capture (00:15:5d:08:cc:52), 0.10.1.2, Dst: 192.16 Port: 49885, Dst Port</pre>	d (528 bits) c Dst: Microsof 8.1.100 : 7680, Seq: 0	on interface \Device\WPF_{26C51D69-3344-487E-9225-4309C2E8338A}, id 0 f_08:cc:4f (00:15:5d:08:cc:4f) 0, Len: 0
	F	Z	0000 00 15 0010 00 34 0020 01 64 0030 fa f0 0040 04 02	5d 08 cc e7 7f 40 c2 dd 1e cd 3e 00	4f 00 15 5d 08 00 80 06 00 00 00 e6 a1 06 03 00 02 04 05 b4	cc 52 08 00 45 00 da 0a 01 02 c0 a8 4 do 00 00 00 80 02 c0 da 03 03 08 01 01 col] · O ·] · R · · • · @ · · · · · · · · · · · · · · · · ·	E.
			⊙ ♥ wires	hark Ethernet	: 20210629111644 a03	740.pcappg		Packets: 1263 • Disolaved: 332 (26, 3%) • Drooped: 0 (0, 0%)



14. To view traffic less than a specific IP address, use the < conditional operator in conjunction with IP address filtering. Apply the filter ip.dst < 10.10.1.16 to find the destination IP addresses less than the specified IP address.

EXERCEPT NTERCEPT VETWORK TRAFFIC JSING WIRESHARK

1 *	Etherne	t				- 0
File	Edit	View Go	<u>Capture</u> <u>Analyze</u> <u>Stati</u>	stics Telephony W	ireless <u>T</u> ools <u>H</u> elp	n
4		• E	X C 9 0 0 2	₹ 🕹 📜 🔳 🤅		
ic	.dst <	10.10.1.16				
No.		Time	Source	Destination	Protocol L	enath Infa
	433	28 795230	10 10 1 1	10 10 1 2	DNS	135 Standard query response By6ca4 AAAA way Juvurytreats com S
	435	29 201610	10.10.1.2	10.10.1.1	DNS	124 Standard query 0xf098 AAAA nineline-incoming-prod-elh-1491
2	436	29.202572	10.10.1.1	10.10.1.2	DNS	202 Standard query response 0xf098 AAAA pipeline-incoming-prod.
	438	29,249321	13, 35, 199, 113	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 443 + 49868 [ACK] Seg=7274 Ack=2404 W
8	439	29.352092	44.239.250.14	10.10.1.2	TCP	54 443 → 49870 [ACK] Seg=3723 Ack=2023 Win=31488 Len=0
£	442	29.449892	44.239.250.14	10.10.1.2	TLSv1.2	324 Application Data
	447	29.791388	117.18.237.29	10.10.1.2	тср	66 [TCP Keep-Alive ACK] 80 → 49875 [ACK] Seg=800 Ack=382 Win=
	449	29.893920	117.18.237.29	10.10.1.2	тср	66 [TCP Keep-Alive ACK] 80 → 49878 [ACK] Seq=800 Ack=382 Win=
	450	29.897608	117.18.237.29	10.10.1.2	ТСР	66 [TCP Keep-Alive ACK] 80 → 49874 [ACK] Seg=1599 Ack=763 Win
	454	29.968435	44.239.250.14	10.10.1.2	тср	54 [TCP Keep-Alive ACK] 443 → 49867 [ACK] Seg=3723 Ack=1522 W
	455	30.105843	44.239.250.14	10.10.1.2	TCP	54 [TCP Keep-Alive ACK] 443 - 49871 [ACK] Seg=3723 Ack=1152 W
	456	30.105843	44.239.250.14	10.10.1.2	TCP	54 [TCP Keep-Alive ACK] 443 > 49876 [ACK] Seq=3723 Ack=1184 W
	457	30.122448	44.239.250.14	10.10.1.2	TCP	54 [TCP Keep-Alive ACK] 443 → 49877 [ACK] Seq=3723 Ack=1184 W
	461	34.576810	172.217.16.227	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 80 → 49881 [ACK] Seq=702 Ack=388 Win=
	463	34.661665	172.217.16.227	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 80 → 49883 [ACK] Seq=702 Ack=388 Win=
	467	37.282957	13.35.199.113	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 443 + 49860 [ACK] Seq=6267 Ack=868 Wi
	469	37.428633	34.107.221.82	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 80 → 49861 [ACK] Seq=303 Ack=302 Win=
	471	37.990909	34.107.221.82	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 80 → 49866 [ACK] Seq=221 Ack=304 Win=
20	474	38.709286	10.10.1.16	10.10.1.2	TCP	66 80 → 49886 [SYN. ACK] Sea=0 Ack=1 Win=8192 Len=0 MSS=1460
> F	rame 4	471: 66 byt	es on wire (528 bits)	, 66 bytes captur	ed (528 bits) on	interface \Device\NPF_{26C51D69-3344-487E-9225-4309C2E8338A}, ic
> E	thern	et II, Src:	Microsof_08:cc:4f (6	0:15:5d:08:cc:4f)	, Dst: Microsof_(08:cc:52 (00:15:5d:08:cc:52)
> 1	ntern	et Protocol	Version 4, Src: 34.1	07.221.82, Dst: 1	0.10.1.2	
> T	ransm	ission Cont	rol Protocol, Src Por	t: 80, Dst Port:	49866, Seq: 221,	Ack: 304, Len: 0
000	0 00	15 5d 08 c	c 52 00 15 5d 08 cc	4f 08 00 45 00	··]··R··]··O··E·	
801	00 0	34 25 c5 0	0 00 37 06 53 36 22	6b dd 52 0a 0a	-4%7- S6"k-R	
002	0 01	02 00 50 C		50 5C de 60 10	X(
004	0 3c	de	0 00 01 01 03 08 00	50 SE 00 DE 50	<.	

38



15. You can also filter traffic based on the source and destination ports. To view traffic originating or destined to the TCP port, apply the filter tcp.port==80.

EXERCEPT NTERCEPT VETWORK TRAFFIC USING WIRESHARD

4		 Image: Image: Image:	🗙 🖸 🤉 👳 🕾 🔛	T 1 = = Q Q	Q II	
	tcp.port=	=80				
No.		Time	Source	Destination	Protocol	Length Info
	426	27.399679	10.10.1.2	34.107.221.82	TCP	55 [TCP Keep-Alive] 49861 → 80 [ACK] Seq=301 Ack=303 Win=2626
	427	27.405080	34.107.221.82	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 80 → 49861 [ACK] Seq=303 Ack=302 Win=
	428	27.966829	10.10.1.2	34.107.221.82	TCP	55 [TCP Keep-Alive] 49866 + 80 [ACK] Seq=303 Ack=221 Win=2626
	429	27.971059	34.107.221.82	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 80 + 49866 [ACK] Seq=221 Ack=304 Win=
	444	29.635121	10.10.1.2	117.18.237.29	TCP	55 [TCP Keep-Alive] 49875 + 80 [ACK] Seq=381 Ack=800 Win=2618
	445	29.735435	10.10.1.2	117.18.237.29	TCP	55 [TCP Keep-Alive] 49874 + 80 [ACK] Seq=762 Ack=1599 Win=262
	446	29.735477	10.10.1.2	117.18.237.29	TCP	55 [TCP Keep-Alive] 49878 → 80 [ACK] Seq=381 Ack=800 Win=2618
	447	29.791388	117.18.237.29	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 80 → 49875 [ACK] Seq=800 Ack=382 Win=
	449	29.893920	117.18.237.29	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 80 → 49878 [ACK] Seq=800 Ack=382 Win=
	450	29.897608	117.18.237.29	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 80 + 49874 [ACK] Seq=1599 Ack=763 Win
	460	34.570733	10.10.1.2	172.217.16.227	TCP	55 [TCP Keep-Alive] 49881 → 80 [ACK] Seq=387 Ack=702 Win=2624
	461	34.576810	172.217.16.227	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 80 + 49881 [ACK] Seq=702 Ack=388 Win=
	462	34.655451	10.10.1.2	172.217.16.227	TCP	55 [TCP Keep-Alive] 49883 + 80 [ACK] Seq=387 Ack=702 Win=2624
	463	34.661665	172.217.16.227	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 80 → 49883 [ACK] Seq=702 Ack=388 Win=
	468	37.422060	10.10.1.2	34.107.221.82	TCP	55 [TCP Keep-Alive] 49861 → 80 [ACK] Seq=301 Ack=303 Win=2626
	469	37.428633	34.107.221.82	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 80 → 49861 [ACK] Seq=303 Ack=302 Win=
+	470	37.985665	10.10.1.2	34.107.221.82	TCP	55 [TCP Keep-Alive] 49866 + 80 [ACK] Seq=303 Ack=221 Win=2626
	471	37.990909	34.107.221.82	10.10.1.2	TCP	66 [TCP Keep-Alive ACK] 80 + 49866 [ACK] Seq=221 Ack=304 Win=
10	473	38.708137	10.10.1.2	10.10.1.16	TCP	66 49886 → 80 [SYN] Sea=0 Win=64240 Len=0 MSS=1460 WS=256 SAC
> > >	Frame 4 Etherne Interne Transmi	F71: 66 byte et II, Src: et Protocol ission Contr	es on wire (528 bits) Microsof_08:cc:4f (0 Version 4, Src: 34.1 rol Protocol, Src Por	, 66 bytes captured (0:15:5d:08:cc:4f), D: 07.221.82, Dst: 10.10 t: 80, Dst Port: 4980	(528 bits) st: Microso 0.1.2 56, Seq: 2	on interface \Device\NPF_{26C51D69-3344-487E-9225-4309C2E8338A}, ic of_08:cc:52 (00:15:5d:08:cc:52) 21, Ack: 304, Len: 0

0006	00	15	5d	08	cc	52	00	15	5d	08	cc	4f	08	00	45	00	··]··R··] · · O · · E ·	
8010	00	34	25	c5	00	00	37	06	53	36	22	6b	dd	52	0a	Øa	-4%7-	56"k-R	
3620	01	02	00	50	c2	ca	5e	99	ed	a0	bc	58	3c	de	80	10	· · · P · · ^ ·	· · · X< · · ·	
9030	01	05	72	f6	00	00	01	01	05	0a	bc	58	3c	dd	bc	58	· · r · · · · ·	- · · X< · · X	
0040	3c	de															<.		

39



16. You can also filter traffic based on a specific string contained in the traffic. Apply the filter http contains www.luxurytreats.com to filter out the traffic that contains the mentioned string.

EXERCEPT INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP

intermed Edit Yiew Go Capture Analyze Statistics Telephony Wireless Jools Heip intermed Go Intermed Source Destination Protocol Length Info 476 38.73982 10.10.1.2 10.10.1.16 HTTP 395 GET // HTP/1.1 497 39.330712 10.10.1.2 10.10.1.16 HTTP 394 GET // App_Themes/Default/00.reset.css HTP/1.1 519 39.467420 10.10.1.2 10.10.1.16 HTTP 386 GET // App_Themes/Default/02.text.css HTP/1.1 523 39.464209 10.10.1.2 10.10.1.16 HTTP 380 GET / App_Themes/Default/02.text.css HTP/1.1 523 39.465943 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/02.text.css StattTP/1.1 523 39.458243 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/12/stotos.css HTP/1.1 523 39.4583343 10.10.1.2 10.10.1.16 HTTP 376								-	et	therne	•
Intervention Image: Colored State Image: Colored State Image: Colored State 2. Tree Surce Destination Protocol Length Info 476 38.730982 10.10.1.2 10.10.1.16 HTTP 395 GET / HTTP/1.1 497 39.330712 10.10.1.2 10.10.1.16 HTTP 394 GET / App_Themes/Default/00.reset.css HTTP/1.1 519 39.407482 10.10.1.2 10.10.1.16 HTTP 386 GET / App_Themes/Default/02.text.css HTP/1.1 523 39.46289 10.10.1.2 10.10.1.16 HTTP 386 GET / App_Themes/Default/02.text.css HTP/1.1 523 39.46299 10.30.1.2 10.10.1.16 HTTP 386 GET / App_Themes/Default/broms.css HTP/1.1 523 39.45231 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/state.css HTP/1.1 526 39.568336 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/state.css HTP/1.1 566	ols <u>H</u> elp		Tools <u>H</u> e	Wireless	tics Telephony	alyze <u>Statistic</u>	Capture A	Go	View	Edit	ile
International and the second			TR		T & 🗐 🗐		X C 9	-	•		1
Time Source Destination Protocol Length Info 447 38.730982 10.10.1.2 10.10.1.16 HTTP 395 GET / HTTP/1.1 497 39.337521 10.10.1.2 10.10.1.16 HTTP 395 GET / HTP_Themes/Default/00.reset.css HTTP/1.1 499 39.375241 10.10.1.2 10.10.1.16 HTTP 386 GET / App_Themes/Default/02.text.css HTTP/1.1 513 39.467482 10.10.1.2 10.10.1.16 HTTP 386 GET / App_Themes/Default/02.text.css HTTP/1.1 523 39.467482 10.10.1.2 10.10.1.16 HTTP 386 GET / App_Themes/Default/03.layout.css HTTP/1.1 523 39.485943 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/bruntons.css HTTP/1.1 524 39.6533428 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/spis.css HTTP/1.1 566 39.633428 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/spis.css HTTP/1.1 576 39.6557909 10.10.2							treats.com	w.luxur	tains www	tp cont	h
476 38.730982 10.10.1.2 10.10.1.16 HTTP 395 GET / App_Themes/Default/00.reset.css HTTP/1.1 497 39.330712 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/01.960_24_col.css HTTP/1.1 159 39.407482 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/02.text.css HTTP/1.1 523 39.464209 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/02.text.css HTTP/1.1 523 39.465429 10.10.1.2 10.10.1.16 HTTP 380 GET / App_Themes/Default/03.layout.css HTTP/1.1 523 39.455943 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/butons.css HTTP/1.1 543 39.66375 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/butons.css HTTP/1.1 563 39.56336 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/butons.css HTTP/1.1 564 39.653709 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/styles.css HTTP/1.1 578 39.665329 10.10.1.2 10.10.1.16 HTTP 376 GET / App_Themes/Default/styles.css HTTP/1.1 578 39.665329 10.10.1.2 10.10.1.16 HTTP 396 GET / App_Themes/Default/styles.css <td< td=""><td>ratocal Length Info</td><td>ath Info</td><td>Protocol</td><td></td><td>Destination</td><td></td><td>Source</td><td></td><td>Time</td><td></td><td>2.</td></td<>	ratocal Length Info	ath Info	Protocol		Destination		Source		Time		2.
497 39.330712 10.10.1.2 10.10.1.16 HTTP 379 GET /App_Themes/Default/00.reset.css HTTP/1.1 499 39.375241 10.10.1.2 10.10.1.16 HTTP 378 GET /App_Themes/Default/01.960_24_col.css HTTP/1.1 519 39.407482 10.10.1.2 10.10.1.16 HTTP 378 GET /App_Themes/Default/02.text.css HTTP/1.1 523 39.465249 10.10.1.2 10.10.1.16 HTTP 380 GET /App_Themes/Default/02.text.css HTTP/1.1 523 39.45543 10.10.1.2 10.10.1.16 HTTP 380 GET /App_Themes/Default/Breadcrumb.css HTTP/1.1 556 39.56336 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/breadcrumb.css HTTP/1.1 566 39.653428 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/lotros.css HTTP/1.1 576 39.653790 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/lotros.css HTTP/1.1 576 39.653729 10.10.1.2 10.10.1.16 HTTP 395 GET /App_Themes/Default/lotros.css HTTP/1.1 576 39.653729 10.10.1.2 10.10.1.16 HTTP 395 GET /App_Themes/Default/lotros.css HTTP/1.1 578 39.65329 10.10.1.2 10.10.1.16 HTTP 395 GET /App_Themes/Default/lotros.css HTTP/1.1 <	TTP 395 GET / HTTP/1.1	95 GET / HT	HTTP		10,10,1,16	2	10.10.1	0982	38.730	476	-
499 39.375241 10.10.1.2 10.10.1.16 HTTP 384 GET /App_Themes/Default/01.960_24_col.css HTTP/1.1 519 39.407482 10.10.1.2 10.10.1.16 HTTP 378 GET /App_Themes/Default/02.text.css HTTP/1.1 523 39.467482 10.10.1.2 10.10.1.16 HTTP 380 GET /App_Themes/Default/03.layout.css HTTP/1.1 523 39.465430 10.10.1.2 10.10.1.16 HTTP 381 GET /App_Themes/Default/Breadcrumb.css HTTP/1.1 523 39.455977 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/Portmos.css HTTP/1.1 563 39.568376 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/Portms.css HTTP/1.1 563 39.663328 10.10.1.2 10.10.1.16 HTTP 380 GET /App_Themes/Default/Jetr.menu.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 380 GET /App_Themes/Default/styles.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.6 HTTP 395 GET /App_Themes/Default/styles.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.6 HTTP 395 GET /App_Themes/Default/styles.css HTTP/1.1 578 39.663529 10.10.1.2 10.10.1.6 HTTP 395 GET /App_Themes/Default/styles.css HTTP/1.1 <	TTP 379 GET /App Themes/Default/00.reset.css HTTP/1.1	79 GET /App	HTTP		10.10.1.16	2	10,10,1	0712	39.330	497	
519 39.407482 10.10.1.2 10.10.1.16 HTTP 378 GET /App_Themes/Default/02.text.css HTTP/1.1 523 39.464209 10.10.1.2 10.10.1.16 HTTP 380 GET /App_Themes/Default/02.text.css HTTP/1.1 528 39.485943 10.10.1.2 10.10.1.16 HTTP 381 GET /App_Themes/Default/buttons.css HTTP/1.1 528 39.485943 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/buttons.css HTTP/1.1 556 39.56336 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/buttons.css HTTP/1.1 566 39.633428 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/grids.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/grids.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/styles.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 395 GET /App_Themes/Default/styles.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.6 HTTP 395 GET /App_Themes/Default/styles.css HTTP/1.1 576 39.659739 10.10.1.2 10.10.1.6 HTTP 395 GET /App_Themes/Default/styles.css HTTP/1.1 578 39.724398	TTP 384 GET /App Themes/Default/01.960 24 col.css HTTP	84 GET /App	HTTP		10.10.1.16	2	10.10.1	5241	39.375	499	
523 39.464209 10.10.1.2 10.10.1.16 HTTP 380 GET /App_Themes/Default/83.1ayout.css HTTP/1.1 528 39.4652943 10.10.1.2 10.10.1.16 HTTP 381 GET /App_Themes/Default/8readCrumb.css HTTP/1.1 528 39.465297 10.10.1.2 10.10.1.16 HTTP 378 GET /App_Themes/Default/8readCrumb.css HTTP/1.1 556 39.558376 10.10.1.2 10.10.1.16 HTTP 378 GET /App_Themes/Default/Forms.css HTTP/1.1 561 39.568336 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/Forms.css HTTP/1.1 566 39.638428 10.10.1.2 10.10.1.16 HTTP 380 GET /App_Themes/Default/spids.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 380 GET /App_Themes/Default/spids.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 390 GET /App_Themes/Default/spids.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 393 GET /App_Themes/Default/spids.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 393 GET /App_Themes/Default/spids.css HTTP/1.1 578 39.665329 10.10.1.2 10.10.1.16 HTTP 393 GET /App_Themes/Default/spids.css HTTP/1.1 693 9.977	TTP 378 GET /App Themes/Default/02.text.css HTTP/1.1	78 GET /Ann	HTTP		10.10.1.16	2	10,10,1	7482	39.407	519	
528 39.485943 10.10.1.2 10.10.1.16 HTTP 381 GET /App_Themes/Default/BreadCrumb.cs HTTP/1.1 532 39.525977 10.10.1.2 10.10.1.16 HTTP 378 GET /App_Themes/Default/Forms.css HTTP/1.1 563 9.568336 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/Forms.css HTTP/1.1 564 9.501375 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/Forms.css HTTP/1.1 565 9.601375 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/styles.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/styles.css HTTP/1.1 578 39.659729 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/styles.css HTTP/1.1 578 39.659729 10.10.1.2 10.10.1.16 HTTP 396 GET /Resources/juery-ui/juery-ui-1.8.16.custom.c 604 39.712630 10.10.1.2 10.10.1.16 HTTP 336 GET /Content/bootstrap.css HTTP/1.1 617 699 39.887152 10.10.1.2 10.10.1.16 HTTP 376 GET /Content/bootstrap.css HTTP/1.1 617 39.962566 10.10.1.2 10.10.1.16 HTTP 376 GET /Content/bootstrap.css HTTP/1.1 618 39.997821 10	TTP 380 GET /App Themes/Default/03.layout.css HTTP/1.1	80 GET /App	HTTP		10.10.1.16	2	10.10.1	4209	39.464	523	
532 39.525977 10.10.1.12 10.10.1.16 HTTP 378 GET /App_Themes/Default/buttons.css HTTP/1.1 556 39.568336 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/Forms.css HTTP/1.1 566 39.663375 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/grids.css HTTP/1.1 566 39.6533428 10.10.1.2 10.10.1.16 HTTP 380 GET /App_Themes/Default/styles.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 380 GET /App_Themes/Default/styles.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 395 GET /Resources/jquery-ui/jskautocomplete/styles.css 604 39.712630 10.10.1.2 10.10.1.16 HTTP 395 GET /Content/bootstrap.css HTTP/1.1 612 39.772034 10.10.1.2 10.10.1.16 HTTP 373 GET /Content/bootstrap.in.css HTTP/1.1 651 39.962566 10.10.1.2 10.10.1.16 HTTP 364 GET /Content/bootstrap.in.css HTTP/1.1 653 39.997821 10.10.1.2 10.10.1.16 HTTP 366 GET /Hotels/css/style.css HTTP/1.1 673 39.997821 10.10.1.2 10.10.1.16 HTTP 376 GET /Hotels/css/style.css HTTP/1.1 678 39.997821 10.10.1.2 </td <td>TTP 381 GET /App Themes/Default/BreadCrumb.css HTTP/1.</td> <td>81 GET /App</td> <td>HTTP</td> <td></td> <td>10.10.1.16</td> <td>2</td> <td>10,10,1</td> <td>5943</td> <td>39.485</td> <td>528</td> <td></td>	TTP 381 GET /App Themes/Default/BreadCrumb.css HTTP/1.	81 GET /App	HTTP		10.10.1.16	2	10,10,1	5943	39.485	528	
556 39.568336 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/Forms.css HTTP/1.1 561 39.568336 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/left-menu.css HTTP/1.1 565 39.563428 10.10.1.2 10.10.1.16 HTTP 380 GET /App_Themes/Default/left-menu.css HTTP/1.1 576 39.5659709 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/left-menu.css HTTP/1.1 578 39.655929 10.10.1.2 10.10.1.16 HTTP 395 GET /App_Themes/Default/left-menu.css HTTP/1.1 578 39.655929 10.10.1.2 10.10.1.16 HTTP 395 GET /App_Themes/Default/spise.css HTTP/1.1 604 39.712630 10.10.1.2 10.10.1.16 HTTP 395 GET /Content/bootstrap.cs HTTP/1.1 612 39.772034 10.10.1.2 10.10.1.16 HTTP 366 GET /Content/Sottstrap.min.css HTTP/1.1 657 39.687152 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/spise.css HTTP/1.1 671 39.962566 10.10.1.2 10.10.1.16 HTTP 376 GET /Content/Sottscs.st HTTP/1.1 672 40.966251 10.10.1.2 10.10.1.16 HTTP 376 GET /Hotels/css/style.css HTTP/1.1 672 40.966251	TTP 378 GET /App Themes/Default/buttons.css HTTP/1.1	78 GET /Ann	HTTP		10.10.1.16	2	10.10.1	5977	39.525	532	
561 39.601375 10.10.1.2 10.10.1.16 HTTP 376 GET /App_Themes/Default/grids.css HTTP/1.1 566 39.633428 10.10.1.2 10.10.1.16 HTTP 380 GET /App_Themes/Default/styles.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 377 GET /App_Themes/Default/styles.css HTTP/1.1 578 39.665329 10.10.1.2 10.10.1.16 HTTP 395 GET /Resources/jquery-ui/guery-ui-1.8.16.custom.c 604 39.712630 10.10.1.2 10.10.1.16 HTTP 395 GET /Resources/jquery-uibs/autocomplete/styles.css 606 39.734986 10.10.1.2 10.10.1.16 HTTP 396 GET /Content/bootstrap.css HTTP/1.1 632 39.772034 10.10.1.2 10.10.1.16 HTTP 373 GET /Content/Site.css HTTP/1.1 633 93.887152 10.10.1.2 10.10.1.16 HTTP 366 GET /Hotels/css/style.css HTTP/1.1 639 39.887152 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/style.css HTTP/1.1 649 39.79201 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/style.css HTTP/1.1 659 39.887152 10.10.1.2 10.10.1.16 HTTP 376 GET /Hotels/css/style.css HTTP/1.1 702 40.066251 10.10.1.2 10.10	TTP 376 GET /App Themes/Default/Forms.css HTTP/1.1	76 GET /App	HTTP		10.10.1.16	2	10.10.1	8336	39.568	556	
566 39.633428 10.10.1.2 10.10.1.16 HTTP 380 GET /App_Themes/Default/left-menu.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 397 GET /App_Themes/Default/left-menu.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 395 GET /Aep_Themes/Default/left-menu.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 395 GET /Aep_Themes/Default/left-menu.css HTTP/1.1 576 39.659709 10.10.1.2 10.10.1.16 HTTP 395 GET /Aep_Themes/Default/styles.css HTTP/1.1 606 39.734986 10.10.1.2 10.10.1.16 HTTP 393 GET /Content/bootstrap.css HTTP/1.1 632 39.772034 10.10.1.2 10.10.1.16 HTTP 366 GET /Hotels/css/style.css HTTP/1.1 659 39.887152 10.10.1.2 10.10.1.16 HTTP 368 GET /Hotels/css/style.css HTTP/1.1 671 39.962566 10.10.1.2 10.10.1.16 HTTP 376 GET /Motels/css/style.css HTTP/1.1 702 40.066251 10.10.1.2 10.10.1.16 HTTP 377 GET /Motels/css/style.css HTTP/1.1 702 40.066251 10.10.1.2 10.10.1.16 HTTP 377 GET /Motels/css/style.css HTTP/1.1 702 40.066251 10.10.1.2	TTP 376 GET /App Themes/Default/grids.css HTTP/1.1	76 GET /App	HTTP		10,10,1,16	2	10.10.1	1375	39,601	561	
576 39.659709 10.10.1.2 10.10.1.16 HTTP 377 GET /App_Themes/Default/styles.css HTTP/1.1 578 39.659709 10.10.1.2 10.10.1.16 HTTP 395 GET /Resources/jquery-ui/jquery-ui-1.8.16.custom.cc 604 39.712630 10.10.1.2 10.10.1.16 HTTP 393 GET /Resources/jquery-libs/autocomplete/styles.css 606 39.734986 10.10.1.2 10.10.1.16 HTTP 393 GET /Content/bootstrap.css HTTP/1.1 632 39.772034 10.10.1.2 10.10.1.16 HTTP 373 GET /Content/bootstrap.css HTTP/1.1 653 39.887152 10.10.1.2 10.10.1.16 HTTP 364 GET /Content/bootstrap.css HTTP/1.1 659 39.887152 10.10.1.2 10.10.1.16 HTTP 366 GET /Motels/css/style.css HTTP/1.1 671 39.962566 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/style.css HTTP/1.1 683 39.997821 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/style.css HTP/1.1 702 40.66251 10.10.1.2 </td <td>TTP 380 GET /App Themes/Default/left-menu.css HTTP/1.1</td> <td>80 GET /App</td> <td>HTTP</td> <td></td> <td>10.10.1.16</td> <td>2</td> <td>10.10.1</td> <td>3428</td> <td>39.633</td> <td>566</td> <td></td>	TTP 380 GET /App Themes/Default/left-menu.css HTTP/1.1	80 GET /App	HTTP		10.10.1.16	2	10.10.1	3428	39.633	566	
578 39.685329 10.10.1.2 10.10.1.16 HTTP 395 GET / Resources/jquery-ui/jquery-ui-1.8.16.custom.c 604 39.712630 10.10.1.2 10.10.1.16 HTTP 393 GET / Resources/jquery-libs/autocomplete/styles.css 606 39.734986 10.10.1.2 10.10.1.16 HTTP 369 GET / Content/bootstrap.css HTTP/1.1 632 39.772034 10.10.1.2 10.10.1.16 HTTP 373 GET / Content/bootstrap.css HTTP/1.1 659 39.887152 10.10.1.2 10.10.1.16 HTTP 366 GET / Hotels/css/style.css HTTP/1.1 671 39.962566 10.10.1.2 10.10.1.16 HTTP 368 GET /Hotels/css/style.css HTTP/1.1 698 39.997821 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/style.css HTTP/1.1 702 40.66251 10.10.1.2 10.10.1.16 HTTP 377 GET /Hotels/css/style.css HTTP/1.1 702 40.66251 10.10.1.2 10.10.1.16 HTTP 377 GET /Hotels/css/caterists/iouery-1.4.2.min.is Frame 476: 395 bytes	TTP 377 GET /App Themes/Default/styles.css HTTP/1.1	77 GET /App	HTTP		10.10.1.16	2	10.10.1	9709	39,659	576	
604 39.712630 10.10.1.2 10.10.1.16 HTTP 393 GET /Resources/jquery-libs/autocomplete/styles.css 606 39.734986 10.10.1.2 10.10.1.16 HTTP 369 GET /Content/bootstrap.css HTTP/1.1 632 39.772034 10.10.1.2 10.10.1.16 HTTP 373 GET /Content/bootstrap.min.css HTTP/1.1 659 39.887152 10.10.1.2 10.10.1.16 HTTP 376 GET /Content/bootstrap.min.css HTTP/1.1 671 39.96256 10.10.1.2 10.10.1.16 HTTP 366 GET /Hotels/css/style.css HTTP/1.1 698 39.997821 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/style.css HTTP/1.1 702 40.066251 10.10.1.2 10.10.1.16 HTTP 377 GET /Resources/client-scripts/iauerv-1.4.2.min.is Frame 476: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface \Device\NPF_{26C51D69-3344-487E-9225-4309 Ethernet II, Src: Microsof_08:cc:52 (00:15:5d:08:cc:52), Dst: Microsof_08:cc:55 (00:15:5d:08:cc:55) Internet Protocol Version 4, Src: 10.10.1.2, Dst: 10.10.1.16 Hypertext Transfer Protocol Sce Port: 49886, Dst Port: 80, Seq: 1, Ack: 1, Len: 341 Hypertext Transfer Protocol Set / HTTP/1.1\n Host: www.luxurytreats.com\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefo	TTP 395 GET /Resources/jauery-ui/jauery-ui-1.8.16.cust	95 GET /Res	HTTP		10.10.1.16	2	10.10.1	5329	39.685	578	
606 39.734986 10.10.1.2 10.10.1.16 HTTP 369 GET /Content/bootstrap.css HTTP/1.1 632 39.772034 10.10.1.2 10.10.1.16 HTTP 373 GET /Content/bootstrap.min.css HTTP/1.1 659 39.887152 10.10.1.2 10.10.1.16 HTTP 364 GET /Content/Site.css HTTP/1.1 671 39.962566 10.10.1.2 10.10.1.16 HTTP 368 GET /Hotels/css/style.css HTTP/1.1 698 39.97821 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/style.css HTTP/1.1 698 39.97821 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/style.css HTTP/1.1 702 40.066251 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/style.css HTTP/1.1 702 40.066251 10.10.1.2 10.10.1.16 HTTP 377 GET /Resources/client-scripts/jauery-1.4.2.min.is Frame 476: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface \Device\NPF_{26C51D69-3344-487E-9225-4309 Ethernet II, Src: Microsof_08:cc:52 (00:15:5d:08:cc:52) Internet Protocol Version 4, Src: 10.10.1.2, Dst: 10.10.1.16 Transmission Control Protocol, Src Port: 49886, Dst Port: 80, Seq: 1, Ack: 1, Len: 341 Hypertext Transfer Protocol ////////////////////////////////////	TTP 393 GET /Resources/iguery-libs/autocomplete/styles	93 GET /Res	HTTP		10.10.1.16	2	10.10.1	2630	39.712	604	
632 39.772034 10.10.1.2 10.10.1.16 HTTP 373 GET /Content/bootstrap.min.css HTTP/1.1 659 39.887152 10.10.1.2 10.10.1.16 HTTP 364 GET /Content/Site.css HTTP/1.1 671 39.962566 10.10.1.2 10.10.1.16 HTTP 368 GET /Hotels/css/style.css HTTP/1.1 698 39.997821 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/style.css HTTP/1.1 698 39.997821 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/style.css HTTP/1.1 702 40.066251 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/style.css Frame 476: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface \Device\NPF_{26C51D69-3344-4B7E-9225-4309 Ethernet II, Src: Microsof_08:cc:52 (00:15:5d:08:cc:52), Dst: Microsof_08:cc:55 (00:15:5d:08:cc:55) Internet Protocol Version 4, Src: 10.10.1.2, Dst: 10.10.1.16 Transmission Control Protocol, Src Port: 40886, Dst Port: 80, Seq: 1, Ack: 1, Len: 341 Hypertext Transfer Protocol Hypertext Transfer Protocol Set / HTTP/1.1\r\n Host: www.luxurytreats.com\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n Accept-Language: en-US,en;q=0.5\r\n	TTP 369 GET /Content/bootstrap.css HTTP/1.1	69 GET /Con	HTTP		10.10.1.16	2	10.10.1	4986	39.734	606	
659 39.887152 10.10.1.2 10.10.1.16 HTTP 364 GET /Content/Site.css HTTP/1.1 671 39.962566 10.10.1.2 10.10.1.16 HTTP 368 GET /Hotels/css/style.css HTTP/1.1 698 39.997821 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/style.css HTTP/1.1 702 40.066251 10.10.1.2 10.10.1.16 HTTP 377 GET /Resources/client-scripts/iduery-1.4.2.min.is Frame 476: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface \Device\NPF_{26C51D69-3344-4B7E-9225-4369 Ethernet II, Src: Microsof_08:cc:52 (00:15:5d:08:cc:55) 08:15:5d:08:cc:55) Internet Protocol Version 4, Src: 10.10.1.2, Dst: 10.10.1.16 Transmission Control Protocol, Src Port: 49886, Dst Port: 80, Seq: 1, Ack: 1, Len: 341 Hypertext Transfer Protocol Set: HTTP/1.1\r\n Host: www.luxurytreats.com\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0\r\n Vser-Agent: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n <td>TTP 373 GET /Content/bootstrap.min.css HTTP/1.1</td> <td>73 GET /Con</td> <td>HTTP</td> <td></td> <td>10.10.1.16</td> <td>2</td> <td>10.10.1</td> <td>2034</td> <td>39.772</td> <td>632</td> <td></td>	TTP 373 GET /Content/bootstrap.min.css HTTP/1.1	73 GET /Con	HTTP		10.10.1.16	2	10.10.1	2034	39.772	632	
671 39.962566 10.10.1.2 10.10.1.16 HTTP 368 GET /Hotels/css/style.css HTTP/1.1 698 39.997821 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/style.css HTTP/1.1 702 40.965251 10.10.1.2 10.10.1.16 HTTP 377 GET /Resources/client-scripts/fauery-1.4.2.min.is Frame 476: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface \Device\NPF_{26CS1D69-3344-487E-9225-4369 Ethernet II, Src: Microsof_08:cc:52 (00:15:5d:08:cc:52), Dst: Microsof_08:cc:55 (00:15:5d:08:cc:55) Internet Protocol Version 4, Src: 10.10.1, Dst: 10.10.1.16 Transmission Control Protocol, Src Port: 49886, Dst Port: 80, Seq: 1, Ack: 1, Len: 341 Hypertext Transfer Protocol > GET / HTTP/1.1\r\n Host: www.luxurytreats.com\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0\r\n Accept: text/Intl.application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n	TTP 364 GET /Content/Site.css HTTP/1.1	64 GET /Con	HTTP		10.10.1.16	2	10.10.1	7152	39.887	659	
698 39.997821 10.10.1.2 10.10.1.16 HTTP 373 GET /Hotels/css/extensions.css HTTP/1.1 702 40.066251 10.10.1.2 10.10.1.16 HTTP 377 GET /Resources/client-scripts/jauery-1.4.2.min.is Frame 476: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface \Device\NPF_{26C51D69-3344-487E-9225-4365 Ethernet II, Src: Microsof_08:cc:52 (00:15:5d:08:cc:52), Dst: Microsof_08:cc:55 (00:15:5d:08:cc:55) Internet Protocol Version 4, Src: 10.10.1.2, Dst: 10.10.1.16 Transmission Control Protocol, Src Port: 49886, Dst Port: 80, Seq: 1, Ack: 1, Len: 341 Hypertext Transfer Protocol > GET / HTTP/1.1\r\n Host: www.luxurytreats.com\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n	TTP 368 GET /Hotels/css/style.css HTTP/1.1	68 GET /Hot	HTTP		10.10.1.16	2	10.10.1	2566	39.962	671	
702 40.06625110.10.1.210.10.1.6HTTP377 GET /Resources/client-scripts/iduery-1.4.2.min.isFrame 476: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface \Device\NPF_{26C51D69-3344-4B7E-9225-4309Ethernet II, Src: Microsof_08:cc:52 (00:15:5d:08:cc:52), Dst: Microsof_08:cc:55 (00:15:5d:08:cc:55)Internet Protocol Version 4, Src: 10.10.1.2, Dst: 10.10.1.16Transmission Control Protocol, Src Port: 49886, Dst Port: 80, Seq: 1, Ack: 1, Len: 341Hypertext Transfer Protocol> GET / HTTP/1.1\r\nHost: www.luxurytreats.com\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0\r\nAccept-Language: en-US,en;q=0.5\r\n	TTP 373 GET /Hotels/css/extensions.css HTTP/1.1	73 GET /Hot	HTTP		10.10.1.16	2	10.10.1	7821	39,997	698	
<pre>Frame 476: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface \Device\NPF_{26C51D69-3344-487E-9225-4369 Ethernet II, Src: Microsof_08:cc:52 (00:15:5d:08:cc:52), Dst: Microsof_08:cc:55 (00:15:5d:08:cc:55) Internet Protocol Version 4, Src: 10.10.1.2, Dst: 10.10.1.16 Transmission Control Protocol, Src Port: 49886, Dst Port: 80, Seq: 1, Ack: 1, Len: 341 Hypertext Transfer Protocol > GET / HTTP/1.1\r\n Host: www.luxurytreats.com\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0\r\n Accept-Language: en-US,en;q=0.5\r\n</pre>	TTP 377 GET /Resources/client-scripts/jauery-1.4.2.min	77 GET /Res	HTTP		10.10.1.16	2	10.10.1	6251	40.066	702	
Hypertext Transfer Protocol > GET / HTTP/1.1\r\n Host: www.luxurytreats.com\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n Accept-Language: en-US,en;q=0.5\r\n	<pre>160 bits) on interface \Device\NPF_{26C51D69-3344-487E-9225- icrosof_08:cc:55 (00:15:5d:08:cc:55) eq: 1, Ack: 1, Len: 341</pre>	on interface :cc:55 (00:1 : 1, Len: 3	3160 bit Microsof Seq: 1,	captured 52), Dst: .10.1.16 Port: 80,), 395 bytes o :15:5d:08:cc:5 .1.2, Dst: 10. :: 49886, Dst f	(3160 bits) 3:cc:52 (00: Src: 10.10. L, Src Port:	tes on wire Microsof Version 4 rol Protoco	395 by Src: otocol	476: 3 net II, net Pro nission	rame thern ntern ransm	FEI
<pre>> GET / HTTP/1.1\r\n Host: www.luxurytreats.com\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n Accept-Language: en-US,en;q=0.5\r\n</pre>			remain in constitution	an chira sha chira			r Protocol	ansfe	ext Tr	ypert	H
Host: www.luxurytreats.com\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n Accept-Language: en-US,en;q=0.5\r\n							\r\n	P/1.1	/ HTT	GET	3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n Accept-Language: en-US,en;q=0.5\r\n						n\r\n	ytreats.co	.luxu	t: www	Hos	
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n Accept-Language: en-US,en;q=0.5\r\n	0) Gecko/20100101 Firefox/89.0\r\n	3100101 Fire	.0) Geck	64; rv:89	10.0; Win64; ×	lindows NT 1	zilla/5.0	nt: Mo	r-Agen	Use	
Accept-Language: en-US,en;q=0.5\r\n	<pre>9,image/webp,*/*;q=0.8\r\n</pre>	op,*/*;q=0.8	.9, image	on/xml;q=0	xml, applicatio	ion/xhtml+x	tml,applica	ext/h	ept: t	Acc	
						q=0.5\r\n	e: en-US,er	inguag	ept-La	Acc	
Accept-Encoding: gzip, deflate\r\n						late\r\n	g: gzip, de	codin	ept-En	Acc	
Connection: keep-alive\r\n						1	ep-alive\r	on: ke	nectio	Con	



Note: This can only be applied to characters and not numerals. It searches for a sequence of characters provided in the filter. 17. To view the HTTP traffic whose request header fields (host) contain a specific string, apply the http.host contains www.luxurytreats.com

filter.

EXERCEPT INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP

Ethernet					U
ile Edit View Go	Capture Analyze S	tatistics Telephony Wirele	ess Tools H	Help	
(🔳 🧟 🕥 📙 📑	🗙 🖸 🭳 👄 👄	🕾 🗿 🛓 🚍 🔳 🔍 🤅	2 9 1		
http.host contains www.k	uxurytreats.com				
). Time	Source	Destination	Protocol	Length Info	
476 38,730982	10.10.1.2	10.10.1.16	HTTP	395 GET / HTTP/1.1	
497 39, 330712	10.10.1.2	10.10.1.16	HTTP	379 GET /App Themes/Default/00.reset.css HTTP/1.1	
499 39, 375241	10.10.1.2	10.10.1.16	HTTP	384 GET /App Themes/Default/01.960 24 col.css HTTP/1.1	
519 39,407482	10.10.1.2	10.10.1.16	HTTP	378 GET /App Themes/Default/02.text.css HTTP/1.1	
523 39,464209	10.10.1.2	10.10.1.16	HTTP	380 GET /App Themes/Default/03.layout.css HTTP/1.1	
528 39,485943	10,10,1,2	10.10.1.16	HTTP	381 GET /App Themes/Default/BreadCrumb.css HTTP/1.1	
532 39,525977	10.10.1.2	10.10.1.16	HTTP	378 GET /App Themes/Default/buttons.css HTTP/1.1	
556 39,568336	10.10.1.2	10.10.1.16	HTTP	376 GET /App Themes/Default/Forms.css HTTP/1.1	
561 39,601375	10.10.1.2	10.10.1.16	HTTP	376 GET /App Themes/Default/grids.css HTTP/1.1	
566 39.633428	10.10.1.2	10.10.1.16	HTTP	380 GET /App Themes/Default/left-menu.css HTTP/1.1	
576 39.659709	10.10.1.2	10.10.1.16	HTTP	377 GET /App_Themes/Default/styles.css HTTP/1.1	
Ethernet II, Src: Internet Protocol Transmission Contr	Microsof_08:cc:52 Version 4, Src: 1 rol Protocol, Src	(00:15:5d:08:cc:52), [0.10.1.2, Dst: 10.10.1 Port: 49886, Dst Port:	Ost: Microso .16 80, Seq: 1,	of_08:cc:55 (00:15:5d:08:cc:55) L, Ack: 1, Len: 341	
Hypertext Transfer	r Protocol				
> GET / HTTP/1.1	\r\n				
Host: www.luxur	rytreats.com\r\n				
User-Agent: Moz	zilla/5.0 (Windows	NT 10.0; Win64; x64; r	v:89.0) Gec	cko/20100101 Firefox/89.0\r\n	
Accept: text/ht	tml,application/xh	tml+xml,application/xml	l;q=0.9,imag	ge/webp,*/*;q=0.8\r\n	
Accept-Language	e: en-US,en;q=0.5\	r\n			
Accept-Encoding	g: gzip, deflate\r	\n			
Connection: kee	ep-alive\r\n				
Upgrade-Insecur	re-Requests: 1\r\n				
\r\n					
[Full request L	URI: http://www.lu:	<pre>xurytreats.com/]</pre>			
[HTTP request 1	1/3]				
[Response in fr	came: 493]				
[Next request i	in frame: 497]				





18. Similarly, you may use various other filters to filter the required traffic.

- As described above, a security professional can specify one or more conditional and logical operators to find traffic based on their preference/requirement. Thus, Wireshark allows you to use a wide range of filters to filter traffic based on your preference/requirement.
 This concludes the demonstration showing how to apply various filters using Wireshark.
- 21. Close all open windows.
- 22. Turn off the Admin Machine-1 virtual machine.







EXERCISE 3: ANALYZE AND EXAMINE VARIOUS NETWORK PACKET HEADERS IN LINUX USING tcpdump

tcpdump is used to analyze TCP/IP and other packets on Linux host machine.

LAB SCENARIO

Each packet in a network contains control information and user data, known as the payload. The control information contains data for delivering the payload, which includes, for example, source and destination IP and MAC addresses and sequencing information. The header part of the packet stores this control information. Hence, the security professional needs to know how to examine the packet headers while examining the data packets.

OBJECTIVE

The objective of this lab is to learn how to inspect TCP/IP and other packet header fields of different network packets.

OVERVIEW OF TROJAN

Data packets traversing over a network can be intercepted using packet capture tools such as tcpdump. These captured packets are analyzed to determine whether proper network security policies are being followed.





Note: Ensure that Web Server and PfSense Firewall virtual machines are running.

- 1. Turn on the Admin Machine-2 virtual machine.
- 2. Type username as sam and password as admin@123 and click Log In.
- 3. Open a terminal by right-clicking on Desktop, and then click Open Terminal from the pop-up menu.









4. The Terminal window will appear. Type sudo tcpdump in Command Prompt and press Enter to capture the network packets of the machine. If you encounter a password prompt, type admin@123.
Note: The password that you type will not be visible.



		sam@sam-Virtual-Machine: ~	
-ile Edit View S	Search Terminal Help		



5. The tcpdump command shows the entire payloads captured packet.



Applications Places Terminal	Thu 03:59	4(1)	C
sam@sam-Virtual-Machine: ~	-	•	>
File Edit View Search Terminal Help			
<pre>355:02.000804 IP dms.google.domain > sam-Virtual-Machine.33089: 53577 1/0/0 PTR pugot.canonical.com. (75) 355:03.789457 IP sam-Virtual-Machine.ntp > ntp2.unix-solutions.be.ntp: NTPv4, Client, length 48 355:03.789457 IP sam-Virtual-Machine.ntp > ns2.vedur.is.ntp: NTPv4, Client, length 48 355:03.789451 IP sam-Virtual-Machine.s0965 / dms.google.domain / 41422 PTR 226.204.111.185.in-addr.arpa. (46) 35:03.789461 IP sam-Virtual-Machine.s0965 / dms.google.domain / 41422 PTR 226.204.111.185.in-addr.arpa. (44) 35:03.789461 IP sam-Virtual-Machine.s0965 / dms.google.domain / 41422 PTR 226.204.111.185.in-addr.arpa. (44) 35:03.789461 IP sam-Virtual-Machine.s0965 / dms.google.domain / asam-Virtual-Machine.s0965 / dms.google.domain / asam-Virtual-Machine.s0965 / dms.google.domain.edu.com.com.google.domain / asam-Virtual-Machine.s0964 / dms.google.domain / asam-Virtual-Machine.s010 / Dms.google.domain / asam-Virtual-Machine.s010 / Dms.google.domain / asam-Virtual-Machine.s010 / Dms.google.domain / asam-Virtual-Machine.s010 / Dms.google.domain: 20064 / Dms.google.domain / asam-Virtual-Machine.s010 / Dms.google.domain: 20074 / Dms.google.domain / asam-Virtual-Machine.s010 / Dms.google.domain: 23725 / Dms.google.domain / asam-Virtual-Machine.s010 / Dms.google.domain: 23725 / Dms.google.domain / asam-Virtual-Machine.s010 / Dms.google.domain / asam-Virtual-Machine.s010 / Dms.google.domain / addr.arpa. (43) 359:04.79354 IP nds.google.domain / asam-Virtual-Machine.ntp: NTPv4, Sciever, length 48 359:04.79354 IP nds.google.domain / asam-Virtual-Machine.ntp: NTPv4, Client, length 48 359:04.79354 IP nds.google.domain / asam-Virtual-Machine.ntp: NTPv4, Client, length 48 359:04.79354</pre>	18	Ι	
			.,
samesam surges - Machines			11







- 6. Press Ctrl + C to end the packet capture.
- 7. Type sudo tcpdump -i eth0 in the terminal and press Enter to capture the network packets from the machine's specific interface.



		sam@sam-Virtual-Machine: ~	
File Edit	View Search Terminal Help		
amfrom 1	(intus) Haching - C auda tandum	i etho	









plications Places Terminal Thu	04:00	40)	Ċ
sam@sam-Virtual-Machine: ~	-		,
<pre>e Edit View Search Terminal Help :00:05.910587 IP sam-Virtual-Machine.53471 > dns.google.domain: 22738+ PTR? 1.1.10.10.in-addr.arpa. (40) :00:05.924212 IP sam-Virtual-Machine.53271 > dns.google.domain: 36615 + PTR? 73.1.10.10.in-addr.arpa. (41) :00:05.924217 IP dns.google.domain > sam-Virtual-Machine.53271: 36615 NXDomain 0/4/0 (41) :00:05.931495 IP sam-Virtual-Machine.38306 > dns.google.domain: 36615 HYRP 78.1.8.8.8.in-addr.arpa. (38) :00:05.931495 IP sam-Virtual-Machine.38306 > dns.google.domain: 19055 HYRP 78.8.8.8.in-addr.arpa. (38) :00:05.931495 IP sam-Virtual-Machine.38306 > dns.google.domain: 10055 HYRP 48.8.8.1n-addr.arpa. (42) :00:07.7894051 IP sam-Virtual-Machine.39306 > dns.google.domain: 26002+ PTR? 1.200.155.162.in-addr.arpa. (44) :00:07.793307 IP dns.google.domain > sam-Virtual-Machine.33408: 26002 HYR? 1.200.155.162.in-addr.arpa. (44) :00:07.793377 IP dns.google.domain > sam-Virtual-Machine.stp: NTPV4, Client, length 48 :00:08.793516 IP time.cloudflare.com.ntp > sam-Virtual-Machine.th; NTPV4, Server, length 48 :00:08.793516 IP time.cloudflare.com.ntp > sam-Virtual-Machine.th; NTPV4, Server, length 48 :00:08.793517 IP dns.google.domain > sam Virtual-Machine.th; NTPV4, Server, length 48 :00:08.793517 IP dns.google.domain > sam-Virtual-Machine.th; NTPV4, Server, length 48 :00:08.793516 IP pugot.canonical.com.ntp > sam-Virtual-Machine.th; NTPV4, Server, length 48 :00:08.793517 IP dns.google.domain > sam-Virtual-Machine.4317: 37896 1/0/0 PTR time.rdg.uk.sa4574.net. (80) :00:09.793908 IP dns.google.domain > sam-Virtual-Machine.th; NTPV4, Client, length 48 :00:09.793908 IP dns.google.domain > sam-Virtual-Machine.ntp: NTPV4, Server, length 48 :00:01.789457 IP sam-Virtual-Machine.ntp > 10:01.com.ntp: NTPV4, Server, length 48 :00:01.789459 IP sam-Virtual-Machine.ntp > NTP4, Client, length 48 :00:01.789459 IP sam-Virtual-Machine.ntp > NTP4, Client, length 48 :00:01.789459 IP sam-Virtual-Machine.so77 and sgoogle.domain: 13923+ PTR7 15.01.189.01.in.addr.arpa. (44) :00:01.789459 IP s</pre>		I	
:80:11.799167 IP sam-Virtual-Machine.37926 > dns.google.domain: 47427+ PTR? 57.52.237.94.in-addr.arpa. (43) packets captured packets received by filter packets dropped by kernel mesam-Virtual-Machine:~\$			





9. Type sudo tcpdump -i eth0 tcp in the terminal and press Enter to capture only the TCP packets from the machine interface.



		sam@sam-Virtual-Machine: ~	
File Edit	View Search Termina	Help	
File Edit	view Search Termina	Пер	





10. Open another terminal and type dd if=/dev/urandom bs=1M count=1 | nc 10.10.1.50 9000 and press Enter; it generates the TCP packets of 1MB and sends them to destination 10.10.1.50.



			sam@sam-Virtual-Machine: ~	
File Edit	View	Search Termina	Help	
sam@sam-V sam@sam-V	irtual irtual	-Machine:~\$ d -Machine:~\$	d if=/dev/urandom bs=1M count=1 nc 10.10.1.50 9000	



11. Switch back to the first Terminal; here, you can see the traffic captured by the Tcpdump.



Applications Places Terminal	Thu 04:02	(1)	0
sam@sam-Virtual-Machine: ~	-		×
File Edit View Search Terminal Help sam@sam_Virtual-Machine:-\$ sudo tcpdump -i eth0 tcp tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on eth0, link-type EMIOM8 (Ethernet), capture size 262144 bytes 04:02:30-061098 IP sam-Virtual-Machine.39258 > 10.1.50.9000: Flags [5], seq 2650857465, win 65535, options JTS val 3334729349 ecr 0,nop,wscale 11], length 0 04:02:30-061402 IP 10.10.1.50.9000 > sam-Virtual-Machine.39258: Flags [R.], seq 0, ack 2650857466, win 0, leng	[mss 1460, th 0	sac	кок







- 12. Press Ctrl + C to end the packet capture.
- 13. Type sudo tcpdump -i eth0 port 80 in the terminal and press Enter to capture packets from the specific port on the machine interface.
- 14. Navigate to Applications Internet and select Chromium Web Browser.



Applications Places Ter	minal		Thu 04:04 🐠 🖒
		am-Virtual-Machine: ~	_ • ×
Favorites	Chromium Web Browser		
Accessories	Driftmat	protocol decode	
l Internet	Dinthet	ze 262144 bytes	
Other	Wireshark		
Sundry	Wireshark (GTK+)		
System Tools	-		
Utilities			
Activities Overview			
Activities over new			





15. The Chromium Web Browser opens. Type http://www.certifiedhacker.com as url and press Enter.

EXERCISE 3: ANALYZE AND EXAMINE VARIOUS NETWORK PACKET USING TCPDUMP





16. Switch back to the opened Terminal; you can observe that the tcpdump is capturing port 80 http traffic.



Applications Places Terminal			Thu 04	4:05	40)	C
sam@sam-Virtual-Machine: ~				-	•	×
File Edit View Search Terminal Help						
ptions [nop,nop,TS val 4153001220 ecr 3599564789,nop,nop,sack 1 {5093541:6723278}], lo 94:05:26.242350 IP 123.35.104.34.bc.googleusercontent.com.http > sam-Virtual-Machine.4/ 887 win 261 options [non non TS val 3596564789 ecr 415361211] lenoth 2840 HTTP	ength 0 2660: Flags [.], seq	4795341:47	79818	1,	ac
44:05:26.248708 IP 123.35.104.34.bc.googleusercontent.com.http > sam-Virtual-Machine.4/ 387. win 261. options [nop.nop.TS val 3599564795 er 4153001219]. length 19880: HTTP	2660: Flags [.], seq	4880541:49	90042	1,	ac
)4:05:26.248742 IP sam-Virtual-Machine.42660 > 123.35.104.34.bc.googleusercontent.com.h ptions [nop.nop.TS val 4153001227 ecr 3599564795.nop.nop.sack 1 {5093541:6723278}], h	http: Flags [ength 0	.], ack	4900421, 1	win 1	427	,
4:05:26.248749 IP 123.35.104.34.bc.googleusercontent.com.http > sam-Virtual-Machine.42 387, win 261, options [nop.nop.TS val 3599564796 ecr 4153001219], length 7100: HTTP	2660: Flags [.], seq	4900421:49	90752	1,	ac
)4:05:26.248758 IP sam-Virtual-Machine.42660 > 123.35.104.34.bc.googleusercontent.com.h pptions [nop,nop,TS val 4153001227 ecr 3599564796,nop,nop,sack 1 {5093541:6723278}], 10	http: Flags [ength 0	.], ack	4907521, v	win 1	424	,
4:05:26.249013 IP 123.35.104.34.bc.googleusercontent.com.http > sam-Virtual-Machine.42 x 387, win 261, options [nop.nop.TS val 3599564796 ecr 4153001219], length 7100: HTTP	2660: Flags [.], seq	4907521:49	91462	1,	ac
4:05:26.249027 IP sam-Virtual-Machine.42660 > 123.35.104.34.bc.googleusercontent.com.h options [nop,nop,TS val 4153001227 ecr 3599564796,nop,nop,sack 1 {5093541:6723278}], 1	http: Flags [ength 0	.], ack	4914621, 1	win 1	421	,
04:05:26.249082 IP 123.35.104.34.bc.googleusercontent.com.http > sam-Virtual-Machine.42 x 387, win 261, options [nop,nop,TS val 3599564796 ecr 4153001219], length 7100: HTTP	2660: Flags [.], seq	4914621:49	92172	1,	ac
4:05:26.250669 IP 123.35.104.34.bc.googleusercontent.com.http > sam-Virtual-Machine.42 x 387, win 261, options [nop.nop.TS val 3599564797 ecr 4153001219], length 9940: HTTP	2660: Flags [.], seq	4975681:49	98562	1,	ac
04:05:26.250881 IP 123.35.104.34.bc.googleusercontent.com.http > sam-Virtual-Machine.42 x 387, win 261, options [nop,nop,TS val 3599564797 ecr 4153001219], length 18460: HTTP	2660: Flags [.], seq	4985621:50	00408	1,	ac
04:05:26.250903 IP sam-Virtual-Machine.42660 > 123.35.104.34.bc.googleusercontent.com.h options [nop,nop,TS val 4153001229 ecr 3599564797,nop,nop,sack 1 {5093541:6723278}], le	http: Flags [ength 0	.], ack	5004081, 1	win 1	380	'
)4:05:26.251317 IP 123.35.104.34.bc.googleusercontent.com.http > sam-Virtual-Machine.42 & 387, win 261, options [nop,nop,TS val 3599564798 ecr 4153001219], length 7100: HTTP	2660: Flags [.], seq	5004081:50	01118	1,	ac
34:05:26.251336 IP sam-Virtual-Machine.42660 > 123.35.104.34.bc.googleusercontent.com.h pptions [nop,nop,TS val 4153001230 ecr 3599564798,nop,nop,sack 1 {5093541:6723278}], lr	http: Flags [ength 0	.], ack	5011181, 1	win 1	377	'
)4:05:26.251340 IP 123.35.104.34.bc.googleusercontent.com.http > sam-Virtual-Machine.42 & 387, win 261, options [nop,nop,TS val 3599564799 ecr 4153001220], length 1420: HTTP	2660: Flags [.], seq	5011181:50	01260	1,	ac
)4:05:26.251345 IP sam-Virtual-Machine.42660 > 123.35.104.34.bc.googleusercontent.com.t options [nop,nop,TS val 4153001230 ecr 3599564799,nop,sack 1 {5093541:6723278}], 1/	http: Flags [ength 0	.], ack	5012601, 1	Win 1	377	'
04:05:26.251682 IP 123.35.104.34.bc.googleusercontent.com.http > sam-Virtual-Machine.42 k 387, win 261, options [nop,nop,TS val 3599564799 ecr 4153001220], length 2840: HTTP	2660: Flags [.], seq	5012601:50	01544	1,	ac
J4:05:26.251694 IP sam-Virtual-Machine.42660 > 123.35.104.34.bc.googleusercontent.com.f pptions [nop,nop,TS val 4153001230 ecr 3599564799,nop,nop,sack 1 {5693541:6723278}], 1e	ength 0	.], ack	5015441, 1	win 1	376	'
4:05:20.251740 IP 123.35.104.34.0C.googleusercontent.com.nttp > sam-virtuai-Machine.4. < 387, win 261, options [nop.nop.TS val 3599564799 ecr 4153001220], length 14200: HTTP	2000: Flags [.], seq	5015441:50	02964	1,	ac
94:05:20.202903 IP 123.35.104.34.00.googleusercontent.com.nttp > sam-virtuai-machine.4, k 387, win 261, options [nop.nop.TS val 3599564800 ecr 4153001220], length 12780: HTTP	2000: Flags [.], seq	5072241:50	08502	245	ac
74:05:20.2029/7 1F Sam-Virtual Machine: 42000 > 123:35:104:34:05:googleuser content.com/ pptions [nop,nop,TS val 4153001231 ecr 3599564800,nop,nop,sack 1 {5093541:6723278}], 16	ength 0	. J, ack	5005021, 1	00354	1	1
x 387, win 261, options [nop,nop,TS val 3599564800 ecr 4153001221], length 8520: HTTP	http: Elage f	1 ack	6723278	win 4	212	aC
perior.co.233.29 in Sam-Virtual-Machine.42000 > 123.33.194.34.00.g00g1eUSerContent.com.t options [nop,nop,TS val 4153001232 ecr 3599564800], length 0	nich: Frags [J, ack	0123210, 1	with 1	213	'
III [sam@sam.Virtual_Machine: w]				_	1	14







- 17. Press Ctrl + C to end the packet capture.
- 18. Now, capture packets from specific source and destination IP.
- 19. Type sudo tcpdump -i eth0 src 10.10.1.16 in the terminal and press Enter to capture packets from the specific source on the machine interface.



	sam@sam-Virtual-Machine: ~	
File Edit View Search Terminal	Help	
sam@sam-Virtual-Machine:~\$ suc ccpdump: verbose output suppre Listening on eth0, link-type E	lo tcpdump -i eth0 src 10.10.1.16 essed, use -v or -vv for full protocol decode EN10MB (Ethernet), capture size 262144 bytes	



20. Open another Terminal and execute the command ping 10.10.1.16 to communicate with the machine. Leave the terminal open.

EXERCISE 3: ANALYZE AND EXAMINE VARIOUS NETWORK PACKET HEADERS IN LINUX USING TCPDUMP

Applications Places Terminal	
sam@sam-Virtual-Machine: ~	
File Edit View Search Terminal Help	
<pre>samPsam-Virtual-Machine:-\$ ping 10.10.1.16 PING 10.1.16 (10.10.1.16) 56(84) bytes of data. 64 bytes from 10.10.1.16: icmp_seq=1 ttl=128 time=2.72 ms 64 bytes from 10.10.1.16: icmp_seq=2 ttl=128 time=2.13 ms 64 bytes from 10.10.1.16: icmp_seq=3 ttl=128 time=2.13 ms 64 bytes from 10.10.1.16: icmp_seq=4 ttl=128 time=1.70 ms 64 bytes from 10.10.1.16: icmp_seq=5 ttl=128 time=1.58 ms 64 bytes from 10.10.1.16: icmp_seq=6 ttl=128 time=0.545 ms 64 bytes from 10.10.1.16: icmp_seq=7 ttl=128 time=1.84 ms</pre>	



21. Switch back to the first Terminal and observe the captured ICMP packets.



Applications Places Terminal Thu)4:07	40)	0
sam@sam-Virtual-Machine: ~	-	•	×
File Edit View Search Terminal Help			
am@sam-Virtual-Machine:-\$ sudo tcpdump -i eth0 src 10.10.1.16			
cpdump: verbose output suppressed, use -v or -vv for full protocol decode			
istening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes			
04:07:21.215181 ARP, Reply 10.10.1.16 is-at 02:15:5d:12:99:6a (oui Unknown), length 28			
04:07:21.216449 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, id 11191, seq 1, length 64			
04:07:22.216963 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, id 11191, seq 2, length 64			
14:07:23.218211 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, id 11191, seq 3, length 64			
14:07:24.218059 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, id 11191, seq 4, length 64			
14:07:25.218761 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, id 11191, seq 5, length 64			
14:07:26.078472 ARP, Request who-has sam-Virtual-Machine (02:15:5d:12:99:65 (oui Unknown)) tell 10.10.1.16, length	28		
14:07:26.218434 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, id 11191, seq 6, length 64			
14:07:27.221162 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, id 11191, seq 7, length 64			
14:07:28.221050 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, id 11191, seq 8, length 64			
14:07:29.238304 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, id 11191, seq 9, length 64			
14:07:30.238875 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, id 11191, seq 10, length 64			
14:07:31.240410 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, 1d 11191, seq 11, length 64			
14:07:32.237805 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, id 11191, seq 12, length 64			
14:07:33.269350 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, id 11191, seq 13, length 64			
14:07:34.268998 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, id 11191, seq 14, length 64			
4:07:35.268524 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, 1d 11191, seq 15, length 64			
4:07:36.275815 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, 1d 11191, seq 16, length 64			
4:07:37.300438 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, 1d 11191, seq 17, length 64			
4:07:38.301407 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, 1d 11191, seq 18, length 64			
4:07:39.301207 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, 1d 11191, seq 19, length 64			
14:07:40.308849 IP 10.10.1.16 > sam-Virtual-Machine: ICMP echo reply, 1d 11191, seq 20, length 64			
14:07:41.310118 IP 10.10.1.16 > sam-virtual-machine: ICMP echo reply, id 11191, seq 21, length 64			
14:07:42.311440 1P 10.10.1.10 > Sam-Virtual-Machine: ICMP echo reply, 1d 11191, seq 22, length 64			
14:07:43.312013 1P 10.101.10 > sam-virtual-machine: ICMP echo reply, 10 11191, seq 23, length 64			
14:07:44.310903 IP 10.10.1.10 > sam-virtuai-machine: ICMP echo reply, 10 11191, seq 24, length 64			





22. Close the second Terminal and press Ctrl + C in first Terminal to stop the packet capturing.

23. A security professional can use the tcpdump to capture the traffic.

24. This concludes the demonstration showing how to analyze and examine various network packet headers using tcpdump.

25. Close all open windows.





EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK

Network scanning is the process of gathering additional detailed information about the target by using highly complex and aggressive reconnaissance techniques.

LAB SCENARIO

A security professional must have the required knowledge to perform network scanning to identify active hosts in the entire network. Further, you must scan the machines for open ports and services running on them.

OBJECTIVE

This lab will demonstrate how to use Nmap to perform network scanning.

OVERVIEW NETWORK SCANNING

The purpose of scanning is to discover exploitable communication channels, probe as many listeners as possible, and keep track of the responsive ones.

Types of scanning:

- Port scanning: Lists open ports and services
- Network scanning: Lists the active hosts and IP addresses
- Vulnerability scanning: Shows the presence of known weaknesses



Note: Ensure that Admin Machine-2, Web Server and PfSense Firewall virtual machines are running.

1. Turn on, AD Domain Controller, Attacker Machine-1, Attacker Machine-2, Admin Machine-1, and Android Device virtual machines.

2. Switch to the Attacker Machine-2 virtual machine.

3. In the login page, the attacker username will be selected by default. Enter password as toor in the Password field and press Enter to log in to the machine.

Note: If a Parrot Updater pop-up appears at the top-right corner of Desktop, ignore and close it.

Note: If a Question pop-up window appears asking you to update the machine, click No to close the window.

4. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.

5. A Parrot Terminal window appears. In the terminal window, type sudo su and press Enter to run the programs as a root user.

6. In the [sudo] password for attacker field, type toor as a password and press Enter.

Note: The password that you type will not be visible.

7. Now, type cd and press Enter to jump to the root directory.

8. In the Terminal window, type ip a and press Enter to display information related to network configuration.

Note: Note down the IP address of the machine, here, 10.10.1.13.







9. Type ip route show and press Enter to display the IP address of the default gateway. **Note:** Note down the IP address of the default gateway, here, 10.10.1.1.



[root@parrot]-[~]
 #ip route show
default via 10.10.1.1 dev eth0 proto static metric 100
10.10.1.0/24 dev eth0 proto kernel scope link src 10.10.1.13 metric 100
[root@parrot]-[~]
 #

10. Now, type netdiscover -i eth0 -r 10.10.1.0/24 and press Enter to scan the local network and discover other hosts present in the network.
11. A total of 7 machines will be displayed with details such as MAC Address, Hostname, etc, as shown in the screenshot below.

EXERCISE 4: scan network to identify hosts in the local network

00			Pa	rrot Terminal	
<u>File Edit View</u>	<u>S</u> earch <u>T</u> erminal <u>H</u> elp				
Currently sca	nning: Finished!	Screen	View:	Unique Hosts	
7 Captured AR	P Req/Rep packets, fr	om 7 host	s. T	otal size: 294	
IP	At MAC Address	Count	Len	MAC Vendor / Hostname	
10.10.1.1	00:15:5d:03:02:6e	1	42	Microsoft Corporation	
10.10.1.2	00:15:5d:03:02:72	1	42	Microsoft Corporation	
10.10.1.11	00:15:5d:03:02:76	1	42	Microsoft Corporation	
10.10.1.16	00:15:5d:03:02:75	1	42	Microsoft Corporation	
10.10.1.19	00:15:5d:03:02:73	1	42	Microsoft Corporation	
10.10.1.50	00:15:5d:03:02:74	1	42	Microsoft Corporation	
10.10.1.79	00:15:5d:03:02:70	1	42	Microsoft Corporation	

- 12. Press Ctrl+C to terminate the scan.
- 13. Switch to the AD Domain Controller virtual machine.
- 14. Log in with the credentials CCT\Administrator and admin@123.
- Note: The network screen appears, click Yes.
- 15. Click Type here to search icon, type cmd and select Command Prompt from the results.
- 16. The Command Prompt window appears, type ipconfig and press Enter to display the details related to network configuration.

EXERCISE 4: scan network to identify hosts in the local network

Select Administrator: Com	mand Prompt
Microsoft Windows [Vo (c) 2018 Microsoft Co	ersion 10.0.17763.1397] orporation. All rights reserved.
C:\Users\Administrate	or.DOMAINCONTROLL.000.001.002>ipconfig
Windows IP Configura	tion
Ethernet adapter Eth	ernet 3:
Connection-specif: Link-local IPv6 Ad IPv4 Address Subnet Mask Default Gateway.	ic DNS Suffix .: ddress : fe80::b00f:ba58:f665:3ac5%10 : 10.10.1.19 : 255.255.255.0 : 10.10.1.1
C:\Users\Administrato	pr.DOMAINCONTROLL.000.001.002>_

17. Type pathping 10.10.1.13 and press Enter to check the connection between Attacker Machine-2 and AD Domain Controller machine. **Note:** It takes a while for the scan to finish.

18. From the results, you can observe that Attacker Machine-2 machine is just 1 hop count away from the AD Domain Controller machine with packet lost count being 0 and success rate is 100, as shown in the screenshot below.

.: \US	ers \Ad	ministrator.DOMA	INCONTROLL.000.001	.0023pathping 10.10.1.13
Traci	ng rou	te to 10.10.1.13	over a maximum of	30 hops
0 1	Domain 10.10.	Controll.CCT.com 1.13	[10.10.1.19]	
Compu	iting s	tatistics for 25 Source to Here	seconds This Node/Link	
Hop Ø	RTT	Lost/Sent = Pct	Lost/Sent = Pct 0/ 100 = 0%	Address DomainControll.CCT.com [10.10.1.19]
1	Øms	0/ 100 = 0%	0/ 100 = 0%	10.10.1.13
Trace	compl	ete.		
C:\Us C:\Us	ers\Ad	ministrator.DOMA ministrator.DOMA	INCONTROLL.000.001	.002>

Copyrights @ 2022 EC-Council International Ltd.

19. Now, we will use Nmap to discover hosts in the local network.

20. Switch back to the Attacker Machine-2 virtual machine.

21. In the terminal window, type nmap 10.10.1.0/24 and press Enter to run a basic scan to discover the hosts in the local network.

22. A result appears displaying hosts in the network along with their open ports and service running services, as shown in the screenshot below.

	Parrot Terminal
<u>File Edit View Search Terminal H</u> elp	
-[root@parrot]-[~]	
#nmap 10.10.1.0/24	
Starting Nmap 7.80 (https://nmap.org) at 2	021-08-20 08:42 EDT
Nmap scan report for 10.10.1.1	
Host is up (0.00065s latency).	
Not shown: 997 filtered ports	
PORT STATE SERVICE	
53/tcp open domain	
80/tcp open http	
443/tcp open https	
MAC Address: 00:15:5D:03:02:6E (Microsoft)	
	I
Nmap scan report for 10.10.1.2	
Host is up (0.00049s latency).	
Not shown: 997 closed ports	
PORT STATE SERVICE	
135/tcp open msrpc	
139/tcp open netbios-ssn	
445/tcp open microsoft-ds	
MAC Address: 00:15:5D:03:02:72 (Microsoft)	
and the second of the second second second	
Nmap scan report for 10.10.1.11	
Host is up (0.00034s latency).	
NOT SHOWN: 999 CLOSED POFTS	
FURI STATE SERVICE	
MAC Address, 00.15.5D.02.02.76 (Microsoft)	
MAC Address: 00.15:50.05:02:70 (MICTOSOIL)	
Nman scap report for MAN moviescope com (10	10 1 16)
Host is up (0.00082s latency)	10.1.107
host is up (0.000025 tatency).	

EC-Council

23. Type nmap -sn 10.10.1.0/24 and press Enter to scan for active machines in the network.

24. A result appears displaying active hosts in the entire network, as shown in the screenshot below.

Note: It takes a while for the results to display.

EXERCISE 4: scan network to identify hosts in the local Network

	Parrot Terminal
<u>File Edit View Search Terminal H</u> elp	
-[root@parrot]-[-]	
#nmap -sn 10.10.1.0/24	
Starting Nmap 7.80 (https://nmap.org) a	t 2021-08-20 09:03 EDT
Nmap scan report for 10.10.1.1	
Host is up (0.00048s latency).	
MAC Address: 00:15:5D:03:02:6E (Microsoft	
Nmap scan report for 10.10.1.2	
Host is up (0.00074s latency).	
MAC Address: 00:15:5D:03:02:72 (Microsoft	
Nmap scan report for 10.10.1.11	
Host is up (0.00045s latency).	
MAC Address: 00:15:5D:03:02:76 (Microsoft	
Nmap scan report for www.moviescope.com (10.10.1.16)
Host is up (0.00072s latency).	
MAC Address: 00:15:5D:03:02:75 (Microsoft	
Nmap scan report for 10.10.1.19	
Host is up (0.00062s latency).	
MAC Address: 00:15:5D:03:02:73 (Microsoft	
Nmap scan report for 10.10.1.50	
Host is up (0.00056s latency).	
MAC Address: 00:15:5D:03:02:74 (Microsoft	
Nmap scan report for 10.10.1.79	
Host is up (0.00072s latency).	
MAC Address: 00:15:5D:03:02:70 (Microsoft	
Nmap scan report for 10.10.1.13	
Host is up.	
Nmap done: 256 IP addresses (8 hosts up)	scanned in 2.04 seconds

25. Type nmap -p 10-300 10.10.1.0/24 and press Enter to scan the range of ports (10-300) in the entire network.26. A result appears displaying different machines with open ports along with the services running on them.

EXERCISE 4: scan network to identify hosts in the local network

	Parrot Terminal	
<u> Eile E</u> dit <u>V</u> iew <u>S</u> earch <u>T</u> erminal <u>H</u> elp		
-[root@parrot]-[-]		
#nmap -p 10-300 10.10.1.0/24		
Starting Nmap 7.80 (https://nmap.c	org) at 2021-08-20 08:59 EDT	
Nmap scan report for 10.10.1.1		
Host is up (0.00073s latency).		
Not shown: 289 filtered ports		
PORT STATE SERVICE		
S3/tcp open domain		
MAC Address: 00:15:50:03:02:65 (Mix	crosoft)	
MAC Address: 00.15.50.05.02.02 (MIC	CTOSOTE/	
Nmap scap report for 10,10,1,2		
Host is up (0.00049s latency).		
Not shown: 289 closed ports		
PORT STATE SERVICE		
135/tcp open msrpc		
139/tcp open netbios-ssn		
MAC Address: 00:15:5D:03:02:72 (Mic	crosoft)	
Nmap scan report for 10.10.1.11		
All 201 econped parts on 10 10 1 11	1 are closed	
MAC Address: 00:15:50:03:02:76 (Mid	resoft)	
MAC AUG1855, 00.15.50.05.02.70 (HIC	CTOSOTE/	
Nmap scan report for www.moviescope	e.com (10.10.1.16)	
Host is up (0.00052s latency).		
Not shown: 287 closed ports		
PORT STATE SERVICE	T	
21/tcp open ftp		
80/tcp open http		

27. Type nmap --top-port 20 10.10.1.0/24 and press Enter to scan for the twenty most common ports.

28. A result appears displaying different top 20 ports along with status as open/close/filtered, as shown in the screenshot below.

00			Parrot Terminal	
<u>File</u> <u>E</u> dit	View Searc	h <u>T</u> erminal <u>H</u> elp		
root@p	arrot]-[-	-] port 20 10.10.1.0/24		
Starting	Nmap 7.80	(https://nmap.org)	at 2021-08-20 09:01 EDT	
Host is u	report	or 10.10.1.1		
nust is u	ih (0.001	os tatency).		
PORT	STATE	SERVICE		
21/tcp	filtered	ftp		
22/tcp	filtered	ssh		
23/tcp	filtered	telnet		
25/tcp	filtered	smtp		
53/tcp	open	domain		
80/tcp	open	http		
110/tcp	filtered	pop3		
111/tcp	filtered	rpcbind		
135/tcp	filtered	msrpc		
139/tcp	filtered	netbios-ssn		
143/tcp	filtered	imap		
443/tcp	open	https		
445/tcp	filtered	microsoft-ds		
993/tcp	filtered	imaps		
995/tcp	filtered	pop3s		
1723/tcp	filtered	pptp		
3306/tcp	filtered	mysql		
3389/tcp	filtered	ms-wbt-server		
5900/tcp	filtered	vnc		
8080/tcp	filtered	http-proxy		
MAC Addre	ss: 00:15	:5D:03:02:6E (Microsof	ft)	
Mman ccan	report	for 10 10 1 2		

EC-Council

29. Type nmap -sn 10.10.1.0/24 and press Enter to scan for the active machines in the network.30. A result appears displaying active hosts in the entire network, as shown in the screenshot below.Note: It takes a while for the results to display.

Parrot Terminal
<u>Eile Edit View Search Terminal H</u> elp
-[root@parrot]-[~]
#nmap -sn 10.10.1.0/24
tarting Nmap 7.80 (https://nmap.org) at 2021-08-20 09:03 EDT
map scan report for 10.10.1.1
lost is up (0.00048s latency).
AC Address: 00:15:5D:03:02:6E (Microsoft)
map scan report for 10.10.1.2
ost is up (0.00074s latency).
AC Address: 00:15:5D:03:02:72 (Microsoft)
map scan report for 10.10.1.11
ost is up (0.00045s latency).
AC Address: 00:15:5D:03:02:76 (Microsoft)
map scan report for www.moviescope.com (10.10.1.16)
ost is up (0.00072s latency).
AC Address: 00:15:5D:03:02:75 (Microsoft)
map scan report for 10.10.1.19
ost is up (0.00062s latency).
AC Address: 00:15:5D:03:02:73 (M1Crosoft)
map scan report for 10.10.1.50
ost is up (0.00056s latency).
AC Address: 00:15:50:03:02:74 (Microsoft)
map scan report for 10.10.1.79
MC Address, 00.15.5D.02.02.70 (Microsoft)
AC AUDIESS: 00:13:30:02:70 (MICTOSOTE)
lost is up
man done: 256 TP addresses (8 hosts up) scanned in 2 04 seconds
map dolle. 200 IF addresses (o hosts up) scalined II 2.04 seconds




- 31. Now, we will perform a detailed scan on one host (here, AD Domain Controller machine (10.10.1.19)), to do so, type nmap -A 10.10.1.19 and press Enter.
- 32. Nmap scans the target machine and displays information such as open ports and services, device type, details of OS, etc., as shown in the screenshot below.

EXERCISE 4: scan network to identify hosts in the local Network

•••					Parrot Terminal			
<u>Eile</u> Edit	View S	earch <u>T</u> erminal <u>F</u>	<u>l</u> elp					
- [root@	parrot							
#nma	ap - A :	10.10.1.19						
Starting	Nmap	7.80 (https://	/nmap.org) at 2021	-08-20 08:51 EDT			
Nmap scar	n repoi	rt for 10.10.1	.19					
Host is u	up (0.0	00064s latency).					
Not shown	n: 984	closed ports						
PORT	STATE	SERVICE	VERSION					
53/tcp	open	domain?						
finger	print-s	strings:						
DNSVersionBindReqTCP:								
ve	rsion							
_ bir	nd							1.12
88/tcp	open	kerberos-sec	Microsoft	Windows	Kerberos (server t	time: 2021-08-	20 12:51:40)Z)
135/tcp	open	msrpc	Microsoft	Windows	RPC			
139/tcp	open	netbios-ssn	Microsoft	Windows	netbios-ssn			
389/tcp	open	ldap	Microsoft	Windows	Active Directory L	DAP (Domain:	CCT.com0.,	Site: Defaul
t-Mirst-Site-Name)								
445/tcp	open	microsoft-ds?						
464/tcp	open	kpasswd5?						
593/tcp	open	ncacn_http	Microsoft	Windows	RPC over HTTP 1.0			
636/tcp	open	tcpwrapped						
1801/tcp	open	msmq?						7 1
2103/tcp	open	msrpc	Microsoft	Windows	RPC			
2105/tcp	open	msrpc	Microsoft	Windows	RPC			
2107/tcp	open	msrpc	Microsoft	Windows	RPC			
3268/tcp	open	Ldap	Microsoft	Windows	Active Directory L	DAP (Domain:	CCI.com0.,	Site: Defaul
t-First-S	Site-Na	ame)						
3269/tcp	open	tcpwrapped						
3389/tcp	open	ms-wbt-server	Microsoft	Terminal	Services			
rdp-httm-info:								



33. In the terminal window, type nmap -sT -v 10.10.1.19 and press Enter.

Note: -sT: performs the TCP connect/full open scan and -v: enables the verbose output (include all hosts and ports in the output).

34. The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot below.

	Parrot Terminal
<u> Eile Edit View S</u> earch <u>T</u> erminal <u>H</u> elp	
-[root@parrot]-[~]	
#nmap -sT -v 10.10.1.19	
Starting Nmap 7.80 (https://nmap.org) at 2021	-08-23 05:17 EDT
Initiating ARP Ping Scan at 05:17	
Scanning 10.10.1.19 [1 port]	
Completed ARP Ping Scan at 05:17, 0.04s elapsed	(1 total hosts)
Initiating Parallel DNS resolution of 1 host. a	t 05:17
Completed Parallel DNS resolution of 1 host. at	05:17, 0.00s elapsed
Initiating Connect Scan at 05:17	
Scanning 10.10.1.19 [1000 ports]	
Discovered open port 53/tcp on 10.10.1.19	
Discovered open port 445/tcp on 10.10.1.19	
Discovered open port 3389/tcp on 10.10.1.19	
Discovered open port 139/tcp on 10.10.1.19	
Discovered open port 135/tcp on 10.10.1.19	
Discovered open port 3269/tcp on 10.10.1.19	
Discovered open port 2107/tcp on 10.10.1.19	
Discovered open port 2105/tcp on 10.10.1.19	
Discovered open port 389/tcp on 10.10.1.19	
Discovered open port 88/tcp on 10.10.1.19	
Discovered open port 464/tcp on 10.10.1.19	
Discovered open port 3268/tcp on 10.10.1.19	
Discovered open port 593/tcp on 10.10.1.19	
Discovered open port 636/tcp on 10.10.1.19	
Discovered open port 2103/tcp on 10.10.1.19	
Discovered open port 1801/tcp on 10.10.1.19	
Completed Connect Scan at 05:17, 2.35s elapsed	(1000 total ports)
whap scan report for 10.10.1.19	
Host is up (0.00036s latency).	
NOT SNOWN: 984 CLOSED DOFTS	











- 35. This concludes the demonstration showing how to perform network scan using Nmap.
- 36. Close all open windows.
- 37. Turn off all the running virtual machines.



EC-Council