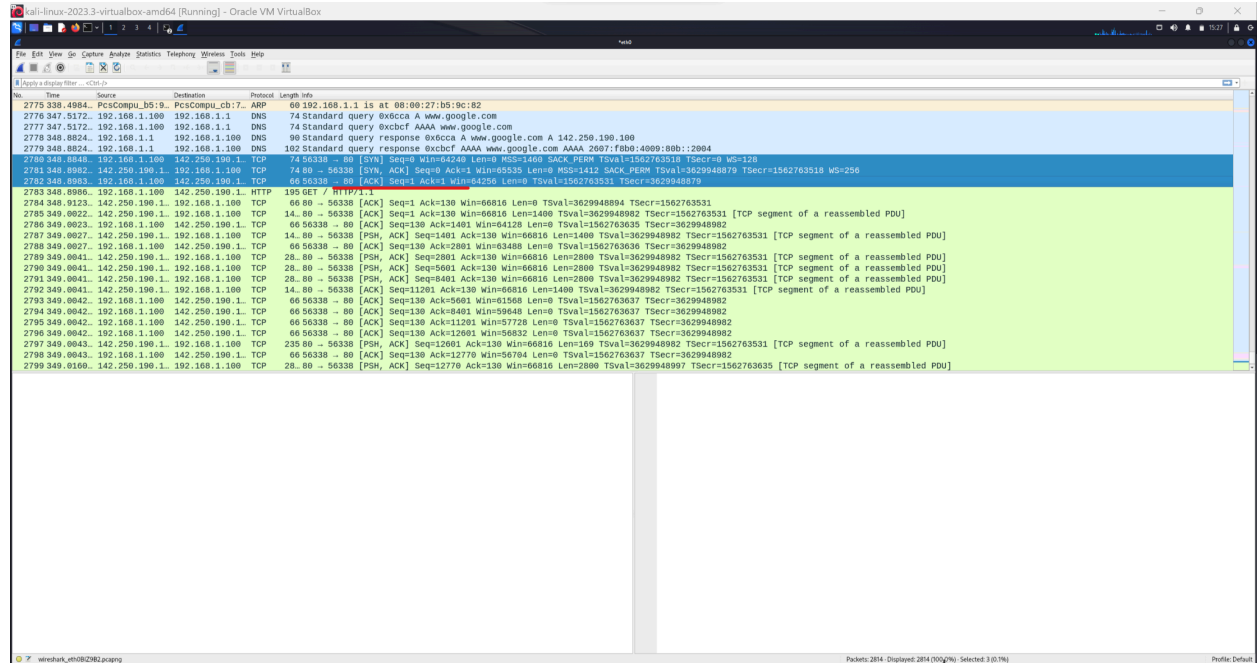
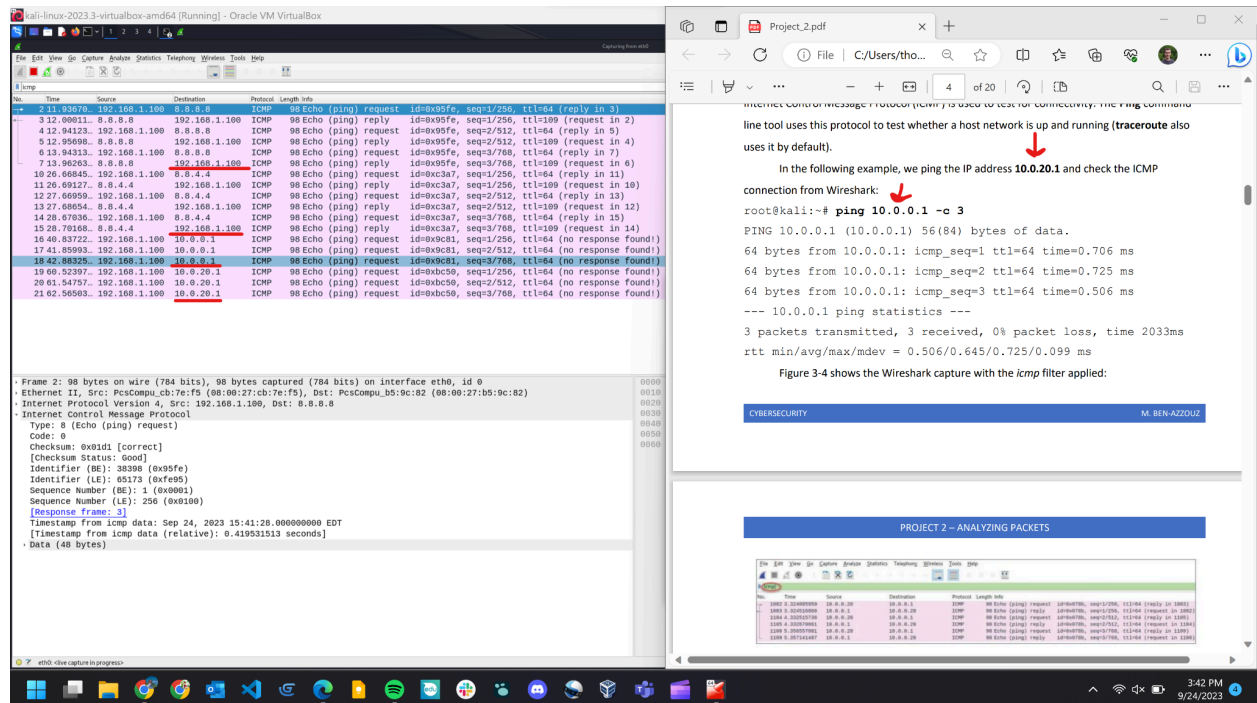


Analyze WireShark Captures:

Part 1: Analyze TCP networking protocols.



Part 2: Analyze UDP networking protocols.



The screenshot displays a Kali Linux virtual machine environment. The top bar indicates the system is running Oracle VM VirtualBox. The main window is divided into two primary sections: a packet capture analysis tool (Wireshark) and a terminal window.

Wireshark Interface:

- Filter:** Applied filter is `eth0`.
- Packet List:** Shows several captured packets. The selected packet (No. 6) is a DHCP request from `192.168.1.1` to `192.168.1.1` (Destination).
- Packet Details:** Displays the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query).
- Packet Bytes:** Shows the raw data of the selected packet, including the Ethernet frame header and payload.

Terminal Window:

- The terminal is running a `ping` command: `ping 10.0.0.1 -c 3`.
- The output shows the results of the ping command, including the IP address, the number of bytes of data, and the statistics for the ping (packets transmitted, received, and loss).
- The terminal also shows the output of the `arp` command, displaying the ARP table.

The screenshot shows a Kali Linux virtual machine with Wireshark open. The packet capture is on the 'eth0' interface, showing a list of packets. Packet 6192 is selected, which is an HTTP GET request from 192.168.1.101 to 192.168.1.102. The packet details pane shows the following information:

- Frame 6192: 490 bytes on wire (3920 bits)**
- Ethernet II, Src: PcsCompu, Dst: 192.168.1.102**
- Internet Protocol Version 4, Src: 192.168.1.101, Dst: 192.168.1.102**
- Transmission Control Protocol, Src Port: 54321, Dst Port: 80**
- Hypertext Transfer Protocol, Method: GET, URI: /, Status: 200 OK**

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII portion contains the following text:

```
Warning: Never expose this VM to an untrusted network!
Contact: nefar@cs.texasploit.com
Login with nefar@nefar@nefar to get started

</pre>
</body>
</html>
```

Exercise 1: Changed Password & Traffic Graphs

The screenshot displays the pfSense web interface within a Kali Linux virtual machine. The left sidebar provides system details: Version 2.7.0-RELEASE (amd64), built on Wed Jun 28 03:53:34 UTC 2023, Firmware 14.0-CURRENT. It also lists CPU Type (Intel(R) Core(TM) i7-10810U), Hardware crypto (Inactive), Kernel PTI (Disabled), MD5 Mitigation (Inactive), Uptime (01 Hour 27 Minutes 21 Seconds), Current date/time (Sun Sep 24 23:36:59 UTC 2023), DNS server(s) (127.0.0.1, 192.168.1.1, 192.168.1.1), Last config change (Sun Sep 24 23:36:41 UTC 2023), State table size (0% (20/96000)), MBUF Usage (0% (3556/1000000)), Load average (0.70, 0.67, 0.59), CPU usage (15%), Memory usage (27% of 961 MB), and SWAP usage (0% of 1024 MB). The main content area shows the 'System / User Manager / Users' page. A table lists users, with 'admin' having status 'checked' and group 'admins'. Below the table, there are traffic graphs for WAN and LAN interfaces, showing data over time from 35:00 to 37:00. The WAN graph shows a significant spike in traffic around 36:40.

Exercise 2: Method for getting deliverables.

The screenshot shows the Wireshark network protocol analyzer interface. The packet list pane displays a list of captured packets, with the selected packet being an ARP request from 192.168.1.104 to 192.168.1.105. The packet details pane shows the Ethernet II header, Internet Protocol Version 4 header, and ARP (Address Resolution Protocol) section. The ARP section shows the Sender MAC address as 08:00:27:5e:01:7c, Sender IP address as 192.168.1.1, Target MAC address as 08:00:27:b8:b7:58, and Target IP address as 192.168.1.104.

Deliverables:

Victim: 192.168.1.105 08:00:27:b8:f8:5a
Attacker: 192.168.1.104 08:00:27:b8:b7:58
Router: 192.168.1.1 08:00:27:5e:01:7c