# Intro to Linux

#### tcpdump vs Wireshark Lab



#### tcpdump vs Wireshark

- Materials needed
  - Ubuntu Linux Machine
  - Kali Linux Machine
- Software Tools used
  - tcpdump
  - Wireshark
  - JuiceShop





#### **Objectives Covered**

- Linux+ Objectives (XKO-005)
  - Objective 1.5 Given a scenario, use the appropriate networking tools or configuration files
    - Network Monitoring
      - tcpdump
      - Wireshark





#### tcpdump and Wireshark

- Tcpdump is a CLI-based packet analyzer.
  - Monitors incoming and outgoing packets
  - Lists source and destination details
- Wireshark is a GUI-based packet analyzer that offers a user-friendly interface.
  - Captures and analyzes network packets
  - It also offers advanced features, such as packet filtering, protocol decodes, and customizable display options.

#### DESCRIPTION

<u>Tcpdump</u> prints out a description of the contents of packets on a network interface that match the boolean <u>expres</u>-<u>sion</u>; the description is preceded by a time stamp, printed, by default, as hours, minutes, seconds, and fractions of a second since midnight. It can also be run with the -w flag, which causes it to save the packet data to a file for later analysis, and/or with the -r flag, which causes it to read from a saved packet file rather than to read packets from a network interface. It can also be run with the -V flag, which causes it to read a list of saved packet files. In all cases, only packets that match <u>expression</u> will be processed by <u>tcpdump</u>.

<u>Tcpdump</u> will, if not run with the -c flag, continue capturing packets until it is interrupted by a SIGINT signal (generated, for example, by typing your interrupt charac-Manual page tcpdump(8) line 23 (press h for help or q to quit)

#### ESCRIPTION

Wireshark is a GUI network protocol analyzer. It lets you interactively browse packet data from a live network or from a previously saved capture file. Wireshark's native capture file format is pcapng format, or pcap which is also the format used by tcpdump and various other tools.

Wireshark can read / import the following file formats:

- pcap captures from Wireshark/TShark/dumpcap, tcpdump, and various other tools using libpcap's/Npcap's/WinPcap's/tcpdump's/WinDump's capture format
- pcapng "next-generation" successor to pcap format





#### tcpdump vs Wireshark Overview

- 1. Start-up the JuiceShop web app on Kali
- 2. Capture network packets with tcpdump and Wireshark on Ubuntu
- 3. Interact with the JuiceShop web app
- 4. View the packets results from tcpdump and Wireshark





#### Setup Environments

- Log into your range
- Once logged in, right click on your browser's tab for the range and click duplicate to have two tabs or windows open
- Open the Ubuntu Linux Environment in one tab
  - You should be on your Ubuntu Linux Desktop
- Open the Kali Linux Environment in the other tab
  - You should be on your Kali Linux Desktop





#### Start the Juice Shop Application

- Move to your Kali machine
- You will need the Kali IP Address so use the command hostname -I or take note of it from the terminal or browser tab
- Open a terminal by clicking the white and black icon on the dashboard on the left.
- Use the following to start Juice Shop
- JuiceShop\_start





#### Move to Ubuntu for Wireshark Setup

- Move to your Ubuntu machine
- Open a terminal by clicking the white and black icon on the dashboard.
- Use the following to open Wireshark
- sudo wireshark





Leave this terminal window open





#### tcpdump Setup

- Open a new terminal by right clicking the white and black icon on the dashboard and selecting "New Window."
- Type the following command but do NOT hit [Enter] right now.
- sudo tcpdump -w tcpdump.pcap
- This commands starts capturing and writes the data to a file named "tcpdump.pcap."



## Open the Browser and Start Capturing

- Open Firefox by clicking the icon on the dashboard.
- While Firefox is opening, begin capturing packets:
  - Return to the Wireshark window and click the blue fin to start packet capturing there.
  - Return to terminal with the tcpdump command and hit [Enter] to start packet capturing there.
- Once the browser loads, navigate to <Kali\_IP\_Address>:3000
- After the page loads, click login under account on the top right side and login using the credentials admin@juice-sh.op and admin123 as the password.



\*Note this will be a fast-paced process. It is diagramed on the following slide to assist.



#### **Diagram of the Process**

Step 1: Click the blue fin to start capturing in Wireshark

| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help                               |            |
|--|------------|
| <u>File Edit Vie</u> 📕 🖉 🐵 🖮 🖹 🕅 🖓 🗣 🌧 🗺 🖉 🖢 🥃 🗐 🔍 🔍 🔍 🖬   |            |
| A pply a display filter <ctrl-></ctrl->  |            |
| No. Time Source Destination Protocol Lengt' Info   |            |
| 3456 35.501326565 10.15.21.107 10.15.128.194 VNC 488   |            |
| Apply a diep 3457 35.503530705 10.15.128.194 10.15.21.107 VNC 105  |            |
| Apply a disp 3458 35.518863140 10.15.21.107 10.15.128.194 VNC 2132                                       |            |
| 3459 35.519361017 10.15.128.194 10.15.21.107 VNC 105   |            |
| 3460 35.552539436 10.15.21.107 10.15.128.194 VNC 1651  |            |
| 3461 35.553323642 10.15.128.194 10.15.21.107 VNC 105   |            |
| 3462 35.595205286 10.15.21.107 10.15.128.194 TCP 66 5901 → 41174 [ACK] Seq=6630872 Ack=34585 Win=471 Lev | n=0 TSval= |

ubuntu@ip-10-15-21-107:

tcpdump: listening on ens5, link-type EN10MB (Ethernet), cap

ubuntu@ip-10-15-21-107:~\$ sudo tcpdump -w tcpdump.pcap

Step 2: Hit [Enter] to start capturing with tcpdump

Step 3: Navigate to <br/><Kali\_IP\_Address>:3000



ture size 262144 bytes

Step 4: Login to JuiceShop under Account using the credentials: admin@juice-sh.op admin123



Q ≣







## Stop Capturing

- In the terminal running tcpdump, use CTRL+C to stop the process and save the file.
- In the Wireshark window, click the red square to stop capturing the files.

ubuntu@ip-10-15-21-107:~\$ sudo tcpdump -w tcpdump.pcap tcpdump: listening on ens5, link-type EN10MB (Ethernet), cap ture size 262144 bytes ^C3826 packets captured 3831 packets received by filter 0 packets dropped by kernel ubuntu@ip-10-15-21-107:~\$







#### Packets, Bytes, & Protocols... Oh my!



#### Analyzing the Wireshark Capture

- Start off by clicking the protocol column to sort the packets alphabetically by protocol
- Scroll down until you see the http packets and try to find one that has "(JPEG JFIF image)" in the info section of the packet
- In the details of the packet, scroll down to JPEG File Interchange Format, right click and select "Show Packet Bytes..."
- What appears?



| (A reput of anisma) made in recently           | line company and       | Destagal *   | Langth lafa  |
|--|------------------------|--------------|--|
| 1527 11 725062 10 15 02                        | 25 10 15 82 20         |              | 420 GET /accots/public/imagos/products/applo_prossings_ing_HTTD/1      |
| 1520 11 726202 10 15 02                        | 25 10 15 82 20         | иттр         | 426 GET /assets/public/images/products/appie_pressings.jpg http://     |
| 1539 11.720292 10.15.92                        | 25 10.15.05.30         | UTTD         | 420 GET /assets/public/images/products/bahana_juice.jpg HTTP/1.1       |
|  | 25 10.15.03.30         | нттр         | 422 GET /assets/public/images/products/artwork2.jpg HTP/1.1            |
| 1543 11.727318 10.15.92                        | .35 10.15.03.30        | HITP         | 427 GET /assets/public/images/products/carfot_juice.jpeg HTTP/1.1      |
| 1545 11.727790 10.15.92                        | .35 10.15.03.30        | HITP         | 420 GET / ASSELS/ public/images/ products/ egginuit_juice.jpg Hilp/1.1 |
| 1548 11.734874 10.15.83                        | .30 10.15.92.35        | HTTP         | 15788 HTTP/1.1 200 OK (JPEG JFIF 1Mage)                                |
| 1550 11.735221 10.15.92                        | .35 10.15.83.30        | HITP         | 425 GET /assets/public/images/products/truit_press.jpg HTTP/1.1        |
| 1551 11.735675 10.15.83                        | .30 10.15.92.35        | нттр         | 20330 HTTP/1.1 200 OK (JPEG JFIF image)                                |
| 1554 11.736659 10.15.83                        | .30 10.15.92.35        | нттр         | 2813 HTTP/1.1 200 OK (JPEG JFIF 1mage)                                 |
| 1558 11.737175 10.15.83                        | .30 10.15.92.35        | нттр         | 9528 HTTP/1.1 200 OK (JPEG JFIF 1mage)                                 |
| 1560 11.737369 10.15.92                        | .35 10.15.83.30        | HTTP         | 428 GET /assets/public/images/products/green_smoothie.jpg HTTP/1.1     |
| 1561 11.737418 10.15.92                        | .35 10.15.83.30        | HTTP         | 424 GET /assets/public/images/products/permafrost.jpg HTTP/1.1         |
| 1563 11.738258 10.15.83                        | .30 10.15.92.35        | HTTP         | 19498 HTTP/1.1 200 OK (JPEG JFIF image)                                |
| 1565 11.740107 10.15.83                        | .30 10.15.92.35        | HTTP         | 15569 HTTP/1.1 200 OK (JPEG JFIF image)                                |
| 1567 11.743459 10.15.83                        | .30 10.15.92.35        | HTTP         | 17577 HTTP/1.1 200 OK (JPEG JFIF image)                                |
| 1569 11.744137 10.15.83                        | .30 10.15.92.35        | HTTP         | 16407 HTTP/1.1 200 OK (JPEG JFIF image)                                |
| <u> </u>                                       |                        |              |  |
| Transmission Control Proto                     | col, Src Port: 3000, 1 | Dst Port: 58 | 146, Seq: 35492, Ack: 1009, Len: 9462                                  |
| [ > [2 Reassembled TCP Segment                 | s (36309 bytes): #155  | 6(26847), #1 | 558(9462)]   |
| <ul> <li>Hypertext Transfer Protoco</li> </ul> | 1                      |              |  |
| <ul> <li>JPEG File Interchange Form</li> </ul> | at                     |              |  |
| Marker: Start of Image                         | Expand Subtrees        |              |  |
| Marker segment: Reserved                       | Collapse Subtrees      |              | FE0)   |
| Marker segment: Reserved                       | Expand All             |              | FE1)   |
| Marker segment: Define                         | Collapse All           |              |  |
| Marker segment: Define                         | Apply as Column        | Ctrl+Shift+I |  |
| Start of Frame header: .                       | Apply us column        | carronnerr   | uffman coding) - Progressive DCT (0xFFC2)                              |
| 01a0 3a 20 74 69 6d 65 6f                      | Apply as Filter        |              | ≥ou t=5  |
| 01b0 d8 ff e0 00 10 4a 46                      | Prepare as Filter      |              | IFI F·····,  |
| 01c0 2c 00 00 ff e1 00 75                      | Conversation Filter    | 1            | UE xif MM  |
| 01d0 2a 00 00 00 08 00 04                      | Colorize with Filter   | ,            |  |
| 01e0 00 00 4c 01 1b 00 05                      | Follow                 | ,            | , and an an arrange of the   |
| Frame (9528 bytes) Reassembled TCP (3          | Сору                   |              |  |
| 💛 🖉 JPEG File Interchange Format Image         | Show Packet Bytes      | Ctrl+Shift+O | Packets: 3872 · Displayed: 3872 (100.0%) · Dropped: 0 (0.0%            |
|  | Export Packet Bytes    | Ctrl+Shift+X |  |
|  | Wiki Protocol Page     |              | Best Juice Carrot Juice  |
|  | Filter Field Reference |              | Shop (1000ml) This website u   |
|  |                        |              |  |



## Locating the Login from Wireshark

- While the packets are still sorted by protocol, locate the http packet that is a POST and "/rest/user/login" in the info section of the packet
- In the details of the packet, scroll down to JavaScript Object Notation and expand the sections



CYBER.ORG

• What appears?



\*Note this appears because JuiceShop is meant to mimic a poorly secured web app. Hopefully, web apps use encryption and techniques to hide this information.

#### Analyzing the tcpdump Packets

- tcpdump packets can be viewed directly in the terminal using the command tcpdump -r tcpdump.pcap
- However, this is not user friendly, nor does it give you the details that Wireshark allows.
- In Wireshark, click File →
   Open → tcpdump.pcap

| 19:20.53.817859 IP 23.185.0.2.https > 10.15.50.118.43428: Flags [P.], seq 105683<br>1:1063076, ack 5904, win 312, options [nop,nop,TS val 179276001 ecr 1790035227],<br>length 6245   |
|---|
| 19:20:53.817869 IP 10.15.50.118.43428 > 23.185.0.2.https: Flags [.], ack 1063076<br>, win 11076, options [nop,nop,TS val 1790035229 ecr 179276001], length 0<br>19:20:53.880808 IP 10.15.50.118.5901 > 10.15.128.194.38574: Flags [.], seq 19398                            |
| 38:1948/8/, ack 60102, win 484, options [nop,nop,15 val 1908689/66 ecr 200395180<br>1], length 8949<br>19:20:53.902238 IP 10.15.50.118.5901 > 10.15.128.194.38574: Flags [.], seq 19487<br>87:1957736, ack 60102, win 484, options [nop,nop,TS val 1908689788 ecr 200395180 |
| 1], length 8949<br>19:20:53.902425 IP 10.15.128.194.38574 > 10.15.50.118.5901: Flags [.], ack 19577<br>36, win 443, options [nop,nop,TS val 2003952032 ecr 1908689766], length 0  |
| 19:20:53.907775 IP 10.15.50.118.5901 > 10.15.128.194.38574: Flags [.], seq 19577<br>36:1966685, ack 60102, win 484, options [nop,nop,TS val 1908689794 ecr 200395203  |

|                | Wi                 | iresh | ark · Open (  | Captu | re File         |           |        |     |     |     |
|----------------|--------------------|-------|---------------|-------|-----------------|-----------|--------|-----|-----|-----|
| Look in:       | 🚞 /home/ubuntu     |       |               |       | -               | 00        | 0 0    | G   | ::  |     |
| Computer       | Name               |       | *             | Size  | Туре            | Date Mo   | dified |     |     |     |
| -              | E Downloads        |       |               |       | Folder          | 15 Feb    | 7:54   | :15 |     |     |
| root           | E Music            |       |               |       | Folder          | 15 Feb    | 7:21   | :22 |     |     |
|                | Pictures           |       |               |       | Folder          | 17 Apr .  | 8:39   | 10  |     |     |
|                | E Public           |       |               |       | Folder          | 15 Feb    | 7:21   | :22 |     |     |
|                | 📄 pwndbg           |       |               |       | Folder          | 15 Feb    | 7:58   | :18 |     |     |
|                | 🚞 snap             |       |               |       | Folder          | 15 Feb    | 7:47   | :51 |     |     |
|                | Templates          |       |               |       | Folder          | 15 Feb    | 7:21   | :22 |     |     |
|                | thinclient_drives  |       |               |       | Folder          | 15 Feb    | 7:21   | :21 |     |     |
|                | 🚞 Videos           |       |               |       | Folder          | 15 Feb    | 7:21   | :22 |     |     |
|                | tcpdump.pcap       |       |               | 14    | MiB pcap File   | 9 May .   | .:21:0 | 1   |     |     |
| File name:     | tcpdump.pcap       |       |               |       |                 |           |        |     | Ope | en  |
|                |                    |       |               |       |                 |           |        | 2   | Can | cel |
| Files of type: | All Files          |       |               |       |                 |           | *      |     | Hel | lр  |
| Automatically  | / detect file type | *     | Format:       | W     | lireshark/tcpdu | mp/ p     | ocap   |     |     |     |
|                |                    |       | Size:         | 1     | 4 MiB, 6557 da  | ta record | i(s)   |     |     |     |
|                |                    |       | Start / elaps | ed: 2 | 024-05-09 19:2  | 20:22 / 0 | 0:00:3 | в   |     |     |
| Deed filters   |                    |       |               | 10.01 |                 |           |        |     |     |     |

CYB=R



#### Analyzing the tcpdump file with Wireshark

- Once the file is opened, notice it looks like the capture from Wireshark.
- You can find the same packets that exchanged data and information including images and the login credentials
- The main difference is tcpdump allows a quick way to start capturing packets through terminal

|      |  |  |  | tcpdu            | mp.pcap   |                        |
|------|--|--|--|------------------|---|------------------------|
| File | <u>Edit View Go</u>                                | Capture Analyze                            | Statistics Telephony                     | Wireless Tools   | Help  |                        |
|      |  | 🔁 🗶 🛅 📹                                    | ۹ 🔶 警                                    | r 🛓 🔲 🛛          |   |                        |
|      | Apply a display filte                              | r <ctrl-></ctrl->                          |  |                  |   |                        |
| Vo.  | Time<br>1066 11.426787                             | Source<br>10.15.21.107                     | Destination<br>10.15.18.9                | Protoc(*<br>HTTP | Length Info<br>540 GET /assets/public/images/products/melo  | n_bike.jpeg HTTP/1.1   |
|      | 1067 11.427807<br>1068 11.432238                   | 10.15.18.9<br>10.15.21.107                 | 10.15.21.107<br>10.15.18.9               | HTTP             | 458 HTTP/1.1 304 Not Modified<br>541 GET /assets/public/images/products/fan_1                             | facemask.jpg HTTP/1.1  |
|      | 1083 11.567389<br>1088 11.598623                   | 10.15.21.107<br>10.15.18.9                 | 10.15.18.9<br>10.15.21.107               | HTTP             | 455 GET /socket.io/?EI0=4&transport=polling<br>230 HTTP/1.1 200 OK (text/plain)                           | &t=OzPlbRl&sid=vgJlqaC |
|      | 1468 14.582589<br>1470 14.587838                   | 10.15.21.107<br>10.15.18.9                 | 10.15.18.9<br>10.15.21.107               | HTTP<br>HTTP     | 505 GET /rest/admin/application-configuration<br>372 HTTP/1.1 304 Not Modified                            | on HTTP/1.1            |
|      | 2319 36.110948<br>2321 36.118708<br>2322 36 128507 | 10.15.21.107<br>10.15.18.9<br>10.15.21.107 | 10.15.18.9<br>10.15.21.107<br>10.15.18.9 | HTTP             | 482 GET /rest/user/whoami HTTP/1.1<br>369 HTTP/1.1 304 Not Modified<br>482 GET /rest/user/whoami HTTP/1.1 |                        |
| •    | 2329 36.141628                                     | 10.15.21.107                               | 10.15.18.9                               | HTTP             | 567 POST /rest/user/login HTTP/1.1 (applic  | ation/json)            |
| -3   | 2331 30.140024<br>2339 36.233508<br>2241 26 242510 | 10.15.18.9                                 | 10.15.21.107                             | HTTP             | 309 HTTP/1.1 304 NOT MODIFied<br>1251 HTTP/1.1 200 OK (application/json)                                  |                        |
|      | 2345 36.249268<br>2349 36.259164                   | 10.15.21.107<br>10.15.21.107               | 10.15.18.9<br>10.15.18.9                 | НТТР             | 1978 GET /rest/user/whoami HTTP/1.1<br>1928 GET /rest/user/whoami HTTP/1.1                                |                        |
| F    | rame 2329: 567 b                                   | oytes on wire (4536                        | bits), 567 bytes cap                     | otured (4536 bi  | ts)<br>02:06:74 (02:07:45:02:05:74)   |                        |
| I    | internet Protocol                                  | Version 4, Src: 1                          | 0.15.21.107, Dst: 10.                    | 15.18.9          | Ack: 1 Lon: 501   |                        |
| H    | ypertext Transfe                                   | er Protocol                                | POIL: 48900, DSL POIL                    | 3000, 3eq. 1     | , ACK. 1, Len. 501  |                        |
| • •  | √avaScript Object<br>▼ Object                      | Notation: applica                          | tion/json                                |                  |   |                        |
|      | <ul> <li>Member Key:</li> <li>String va</li> </ul> | email<br>alue: admin@juice-s               | sh.op                                    |                  |   |                        |
|      | ✓ Member Key:<br>String va                         | password<br>alue: admin123                 |  |                  |   |                        |





#### Wrap-up

- Wireshark and tcpdump both allow packets to be captured and analyzes from a network
- Wireshark is GUI-based and has several built-in tools to assist in capturing and analyzing data
  - Clicking help and exploring the Manual pages gives you several additional options
- tcpdump is CLI-based and allows a quick method to capture packets in terminal
  - Use man tcpdump to look at additional options such as specifying connections, ports, or duration.



