

## Lab 6 - Capturing and Analyzing Network Traffic Using a Sniffer

### **Objective:**

1. Starting the Sniffer
2. Generating the Traffic
3. Analysing the Traffic

### **Takeaways:**

1. Wireshark is a powerful network protocol analyzer used for capturing and inspecting network traffic in real-time. It allows users to examine data packets traversing a network, aiding in network troubleshooting, security analysis, and protocol development.
2. FTP, short for File Transfer Protocol, is a standard network protocol used for transferring files between a client and a server on a computer network. It enables users to upload, download, and manage files on a remote server over a network connection.
3. Telnet is a network protocol used to establish a remote connection and access resources or manage devices over a network, typically the internet. It allows users to log into and interact with a remote computer or server, but due to security vulnerabilities, its usage has declined in favor of more secure protocols like SSH (Secure Shell).
4. The "net group" command in Windows is a command-line utility used to manage groups within a network environment. It enables administrators to create, modify, view, and manage group memberships and permissions on a Windows system or domain.
5. A TCP stream refers to a sequence of data transmitted between two devices over a TCP (Transmission Control Protocol) connection. It represents the continuous flow of

information sent and received between the sender and receiver, maintaining the reliability and order of data delivery in a network communication session.

## Challenges:

The screenshot displays a web browser with multiple tabs. The active tab is titled "Capturing and Analyzing Network Traffic Using a Sniffer" and shows a challenge page from "Ethical Hacking and Systems Defense". The page contains instructions for Challenge 15: "Hover your mouse over the Picture icon. Notice the flag of 999818. Click on the Challenge icon and type the flag number into the answer box. This is just to show you how to capture Challenge Flags you will see throughout this lab." Below the instructions is a "SAMPLE CHALLENGE" button and a text input field containing "999818". A "Submit" button is also visible. Challenge 16 is partially visible below, stating: "Get the information for below Challenge Flag by using the same techniques from the previous steps."

Overlaid on the right side of the browser window is a console window titled "INT-WIN10-FINAL-INFOSEC-s". It shows a Windows Server 2008 desktop environment with a taskbar at the bottom. The desktop background features a Windows logo and the text "Windows Server 2008". A red box in the top right corner of the console window contains the text "FLAG: 999818". The console window also includes buttons for "View Fullscreen", "Send Ctrl+Alt+Delete", and "Reboot".

Sign in | saint peters blackboard - Search | Week 4-7: Malware Threats | Capturing and Analyzing Network Traffic Using a Sniffer | ChatGPT | port 443 - Search

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZUICEQRHFQ

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKitty.Net | untitled report | Introduction to Cry...

### Ethical Hacking and Systems Defense

#### Capturing and Analyzing Network Traffic Using a Sniffer

show you how to capture challenge flags you will see throughout this lab.

**SAMPLE CHALLENGE**

16 Get the information for below Challenge Flag by using the same techniques from the previous steps.

→ CHALLENGE #1

Get the flag number in the flag2.jpg file. Type the Flag number displayed.

808212

Submit Skip

DEVIATION

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZUICEQRHFQ

USD/CAD -0.35%

Search

10:27 AM 12/29/2023

Security of Sense FL... | Gmail... | YouTube... | Maps... | News... | Certified in Cybersec... | Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3605149/125

INT-WIN10-FINAL-INFOSEC-s View Fullscreen Send Ctrl+Alt+Delete Reboot

Registry: These

View all photos

FLAG-808212

Windows Server 2008

Sign in | saint peters blackboard - Search | Week 4-7: Malware Threats | Capturing and Analyzing Network Traffic Using a Sniffer | ChatGPT | port 443 - Search

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZUICEQRHFQ

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKitty.Net | untitled report | Introduction to Cry...

### Ethical Hacking and Systems Defense

#### Capturing and Analyzing Network Traffic Using a Sniffer

Logon hours allowed: All

Local Group Memberships: \*Domain Users

Global Group memberships: \*Domain Users

The command completed successfully.

25 Get the information for below Challenge Flag by using the same techniques from the previous steps.

→ CHALLENGE #2

Get the user information for the aquaman account. Type the Flag number displayed.

888221

Submit Skip

DEVIATION

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZUICEQRHFQ

43°F Mostly cloudy

Search

10:32 AM 12/29/2023

Security of Sense FL... | Gmail... | YouTube... | Maps... | News... | Certified in Cybersec... | Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3605149/125

INT-WIN10-FINAL-INFOSEC-s View Fullscreen Send Ctrl+Alt+Delete Reboot

PowerShell: net user aquaman aquaman

User name: aquaman

Full name: aquaman

Comment: Flag:888221

Country code: 000 (System Default)

Account active: Yes

Account expires: Never

Password last set: 2/26/2018 1:14:49 PM

Password expires: 4/2/2018 1:14:49 PM

Password changeable: 2/27/2018 1:14:19 PM

Password required: Yes

User may change password: Yes

Workstations allowed: All

Logon script:

User profile:

Home directory:

Last login: Never

Logon hours allowed: All

Local Group Memberships: \*Domain Users

Global Group memberships: \*Domain Users

The command completed successfully.

C:\Users\administrator\_

Sign in | saint peters blackboard - Search | Week 4-7: Malware Threats - | Capturing and Analyzing Net... | ChatGPT | port 443 - Search

https://lab.infoseclearning.com/course/WICWPYQVN/lab/ZUJCEQRHFQ

McAfee Security | Dell | Room GB 533-Fall... | HomeworkifyNet... | untitled report | Introduction to Cry... | Sec...

### Ethical Hacking and Systems Defense

#### Capturing and Analyzing Network Traffic Using a Sniffer

Automatic: WireShark/zip.pcap | Format: Wireshark/zip.pcap | Size: 60784 bytes | Packets: 612 | First Packet: 2018-02-26 13:40:35 | Elapsed time: 00:03:23

16 Get the information for below Challenge Flag by using the same techniques from the previous steps.

→ CHALLENGE #3

Use the ftp display filter to find the flag number. Type the Flag number displayed.

969776

Submit Skip

17

https://lab.infoseclearning.com/course/WICWPYQVN/lab/ZUJCEQRHFQ

44°F Cloudy

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3605145/123

INT-KALI-FINAL-INFOSEC-sni View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications | Ports | WireShark | Tue 10:48

File Edit View Help Capture Analyze Statistics HelpView Tools Internet Help

Filter: \*ftp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
2	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
3	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
4	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
5	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
6	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
7	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
8	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
9	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
10	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
11	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
12	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
13	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
14	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
15	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
16	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
17	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
18	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
19	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
20	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
21	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
22	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
23	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
24	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
25	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
26	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
27	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
28	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
29	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
30	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
31	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
32	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
33	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
34	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
35	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
36	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
37	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
38	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
39	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
40	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
41	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
42	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
43	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
44	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
45	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
46	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
47	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
48	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
49	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
50	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
51	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
52	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
53	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
54	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
55	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
56	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
57	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
58	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
59	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
60	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
61	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
62	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
63	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
64	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
65	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
66	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
67	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
68	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
69	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
70	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
71	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
72	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
73	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
74	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
75	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
76	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
77	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
78	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
79	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
80	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
81	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
82	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
83	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
84	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
85	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
86	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
87	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
88	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
89	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
90	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
91	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
92	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
93	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
94	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
95	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
96	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
97	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
98	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
99	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service
100	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Request: 330 Microsoft FTP Service

169776

170776

171776

172776

173776

174776

175776

176776

177776

178776

179776

180776

181776

182776

183776

184776

185776

186776

187776

188776

189776

190776

191776

192776

193776

194776

195776

196776

197776

198776

199776

200776

201776

202776

203776

204776

205776

206776

207776

208776

209776

210776

211776

212776

213776

214776

215776

216776

217776

218776

219776

220776

221776

222776

223776

224776

225776

226776

227776

228776

229776

230776

231776

232776

233776

234776

235776

236776

237776

238776

239776

240776

241776

242776

243776

244776

245776

246776

247776

248776

249776

250776

251776

252776

253776

254776

255776

256776

257776

258776

259776

260776

261776

262776

263776

264776

265776

266776

267776

268776

269776

270776

271776

272776

273776

274776

275776

276776

277776

278776

279776

280776

281776

282776

283776

284776

285776

286776

287776

288776

289776

290776

291776

292776

293776

294776

295776

296776

297776

298776

299776

300776

301776

302776

303776

304776

305776

306776

307776

308776

309776

310776

311776

312776

313776

314776

315776

316776

317776

318776

319776

320776

321776

322776

323776

324776

325776

326776

327776

328776

329776

330776

331776

332776

333776

334776

335776

336776

337776

338776

339776

340776

341776

342776

343776

344776

345776

346776

347776

348776

349776

350776

351776

352776

353776

354776

355776

356776

357776

358776

359776

360776

361776

362776

363776

364776

365776

366776

367776

368776

369776

370776

371776

372776

373776

374776

375776

376776

377776

378776

379776

380776

381776

382776

383776

384776

385776

386776

387776

388776

389776

390776

391776

392776

393776

394776

395776

396776

397776

398776

399776

400776

401776

402776

403776

404776

405776

406776

407776

408776

409776

410776

411776

412776

413776

414776

415776

416776

417776

418776

419776

420776

421776

422776

423776

424776

425776

426776

427776

428776

429776

430776

431776

432776

433776

434776

435776

436776

437776

438776

439776

440776

441776

442776

443776

444776

445776

446776

447776

448776

449776

450776

451776

452776

453776

454776

455776

456776

457776

458776

459776

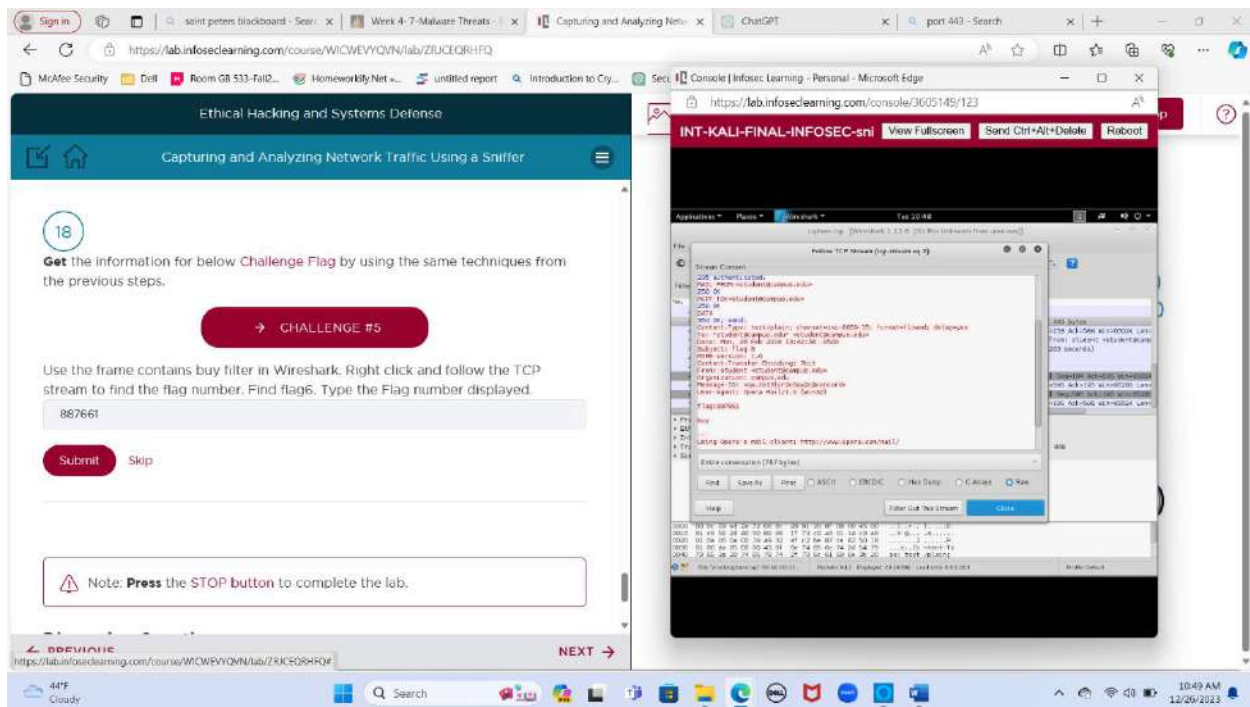
460776

461776

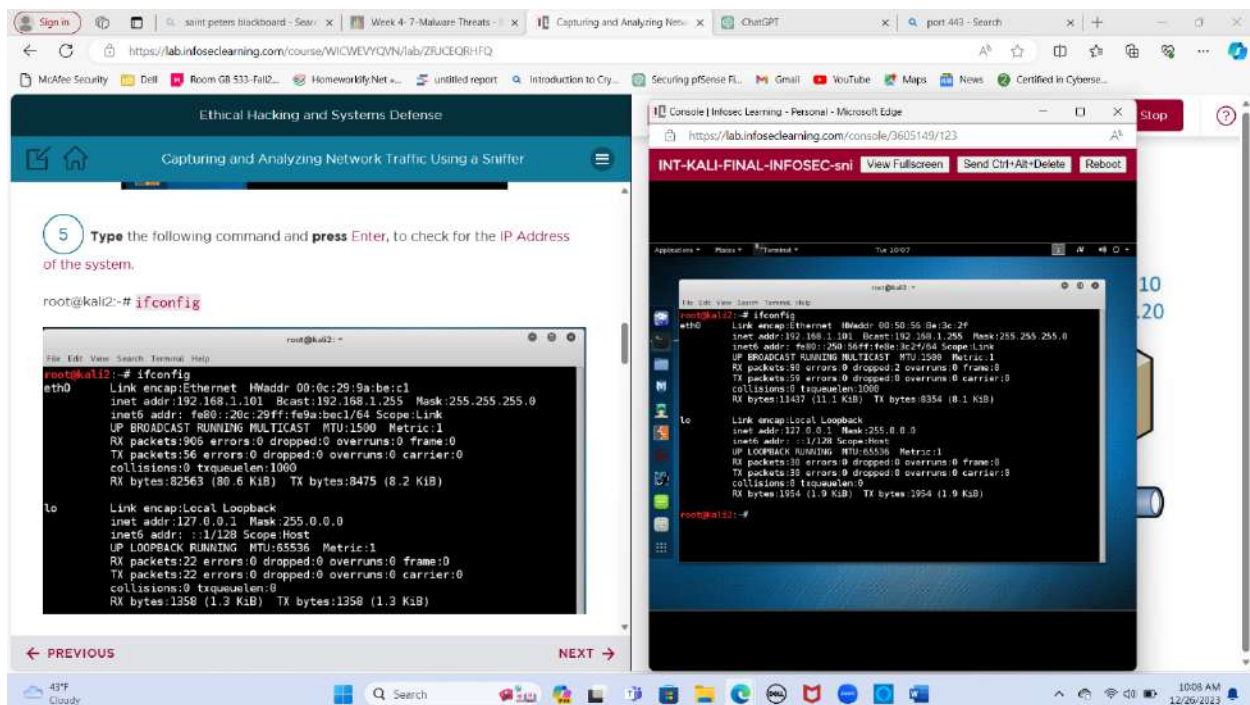
462776

463776

46477



## Screenshots:





## Removing the IP address:

**Ethical Hacking and Systems Defense**

**Capturing and Analyzing Network Traffic Using a Sniffer**

RX bytes:1358 (1.3 KiB) TX bytes:1358 (1.3 KiB)

6 Type the following command and **press** Enter, so your system will not have an IP Address.

```
root@kali2:~# ifconfig eth0 0.0.0.0 up
```

7 Type the following command and **press** Enter, to verify that no IPv4 address is listed for eth0.

```
root@kali2:~# ifconfig
```

```
root@kali2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9a:be:c1
          inet6 addr: fe80::20c:29ff:fe9a:bec1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:943 errors:0 dropped:0 overruns:0 frame:0
          TX packets:58 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:85927 (83.9 KiB)  TX bytes:8595 (8.3 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1954 (1.9 KiB)  TX bytes:1954 (1.9 KiB)
```

10:20

**Ethical Hacking and Systems Defense**

**Capturing and Analyzing Network Traffic Using a Sniffer**

7 Type the following command and **press** Enter, to verify that no IPv4 address is listed for eth0.

```
root@kali2:~# ifconfig
```

```
root@kali2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9a:be:c1
          inet6 addr: fe80::20c:29ff:fe9a:bec1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:58 errors:0 dropped:0 overruns:0 frame:0
          TX packets:58 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:85927 (83.9 KiB)  TX bytes:8595 (8.3 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1358 (1.3 KiB)  TX bytes:1358 (1.3 KiB)
```

8 Type the following command and **press** Enter, to open Wireshark.

10:20

## The screenshot captures a Windows 10 desktop environment during a network security training session. Two Microsoft Edge browser windows are open. The first window, titled "Ethical Hacking and Systems Defense", displays a lesson from "infoseclearning.com". The lesson title is "Capturing and Analyzing Network Traffic Using a Sniffer". A prominent instruction box contains a green circle with the number "10" and text stating: "If asked, click OK to the Running as 'root' user and group warning. Otherwise, proceed to the next step." Below this text is a small dialog box titled "Running as user 'root' and group 'root'. This could be dangerous." with a checkbox labeled "Don't show this message again." and an "OK" button. Navigation arrows for "PREVIOUS" and "NEXT" are visible at the bottom of the page. The second browser window shows the Wireshark application running on a Kali Linux virtual machine. The address bar indicates the URL "https://lab.infoseclearning.com/console/3605149/123". The Wireshark interface has several panels: "Interface List" on the left showing "eth0" as the selected interface; "Start" button below it; "Capture Options" panel showing settings for the selected interface; and a main pane displaying "Sample Captures" with a list of recent capture files. On the far right edge of the screen, a vertical sidebar with numbers "10" and "20" is partially visible. The Windows taskbar at the bottom shows the Start menu icon, search bar, and various pinned applications including File Explorer, Edge, and system tray icons for network, volume, and time (10:11 AM, 12/26/2023).

[illegible]

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZUICQIRHFG

### Ethical Hacking and Systems Defense

#### Capturing and Analyzing Network Traffic Using a Sniffer

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 Ethernet II, Src: Vmware\_80:19:9f (00:50:56:80:19:9f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 Address Resolution Protocol (request)

14 After a short while, packets should start appearing in the Packet List.

No.	Time	Source	Destination	Protocol	Length	Info
20	0.00000000	vmware_80:19:9f	192.168.1.100	ARP	60	Who has 192.168.1.100? Tell 192.168.1.100
30	0.00000000	192.168.1.100	192.168.1.100	ICMP	60	Standard query 0x7899 A new Live.com
40	0.00000000	vmware_80:19:9f	192.168.1.100	ARP	60	Who has 192.168.1.100? Tell 192.168.1.100
50	0.00000000	192.168.1.100	192.168.1.100	ICMP	60	Standard query 0x7899 A new Live.com
60	0.00000000	vmware_80:19:9f	192.168.1.100	ARP	60	Who has 192.168.1.100? Tell 192.168.1.100
70	0.00000000	192.168.1.100	192.168.1.100	ICMP	60	Standard query 0x7899 A new Live.com
80	0.00000000	vmware_80:19:9f	192.168.1.100	ARP	60	Who has 192.168.1.100? Tell 192.168.1.100
90	0.00000000	192.168.1.100	192.168.1.100	ICMP	60	Standard query 0x7899 A new Live.com
100	0.00000000	vmware_80:19:9f	192.168.1.100	ARP	60	Who has 192.168.1.100? Tell 192.168.1.100
110	0.00000000	192.168.1.100	192.168.1.100	ICMP	60	Standard query 0x7899 A new Live.com

Discussion Questions

← PREVIOUS NEXT →

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZUICQIRHFG

### Ethical Hacking and Systems Defense

#### Capturing and Analyzing Network Traffic Using a Sniffer

1 Click on the Windows 10 in the topology. After the machine boots up, right-click the cmd - Shortcut and select Run as administrator.

Kali 2 Linux 192.168.1.101 Windows Server 192.168.1.10 Windows 10 192.168.1.20

cmd - Shortcut

Open file location

Run as administrator

INT-WIN10-FINAL-INFOSEC-s

View Fullscreen Send Ctrl+Alt+Delete Reboot

Microsoft Windows [Version 10.0.19040]  
 (c) 2019 Microsoft Corporation. All rights reserved.  
 C:\Windows\system32\cmd.exe

← PREVIOUS NEXT →



# FTP

The screenshot shows a web browser with the URL <https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZUICEQRHFQ>. The page is titled "Ethical Hacking and Systems Defense" and "Capturing and Analyzing Network Traffic Using a Sniffer". It contains three numbered steps for connecting to an FTP server:

- 3 Type the following command and **press Enter**, to ftp to the Windows Server.  
`C:\> ftp 192.168.1.10`
- 4 For the User, type `ftp`. Then **press Enter**,  
`User (192.168.1.10:(none)): ftp`  
`131 Anonymous access allowed, send identity (e-mail name) as password.`
- 5 For the Password, type `zombie`. Then **press Enter**,  
`133 Anonymous user logged in.`

Below the steps are "PREVIOUS" and "NEXT" navigation buttons. To the right, a terminal window titled "INT-WIN10-FINAL-INFOSEC-s" shows the same commands and responses being executed in a Windows command prompt.

The screenshot shows the same web browser with the URL <https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZUICEQRHFQ>. It contains two more numbered steps for interacting with the FTP server:

- 6 Type the following ftp command and **press Enter**, to list all of the files and folders.  
`ftp> ls`
- 7 Type the following command and **press Enter**, to switch to binary mode to download the picture file.  
`ftp> bin`
- 8 Type the following ftp command and **press Enter**, to download the JPEG file

Below the steps are "PREVIOUS" and "NEXT" navigation buttons. To the right, the terminal window shows the execution of these commands, including the file listing and the switch to binary mode.







## Viewing accounts

Sign in | saint peters blackboard - Search | Week 4 - 7: Malware Threats | Capturing and Analyzing Network Traffic Using a Sniffer | ChatGPT | port 443 - Search

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZUCCQRHFQ

Ethical Hacking and Systems Defense

Capturing and Analyzing Network Traffic Using a Sniffer

24 There is another account on the system called superman. View the information about the superman account by typing the following command (Notice the flag of 999818).

C:\Users\Administrator> net user superman

```
C:\Users\Administrator>net user superman
User name      superman
Full Name      Flag:999818
Comment
User's comment 000 (System Default)
Country code   Yes
Account active  Never
Password last set  2/25/2018 9:48:13 PM
Password expires  4/8/2018 9:48:13 PM
Password changeable  Yes
Password required Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon      Never
```

PREVIOUS NEXT

43°F Mostly cloudy Search 10:31 AM 12/26/2023

INT-WIN10-FINAL-INFOSEC-s View Fullscreen Send Ctrl+Alt+Delete Reboot

https://lab.infoseclearning.com/console/3605149/125

Security of Sense Firewall | Gmail | YouTube | Maps | News | Certified in Cybersecurity

https://lab.infoseclearning.com/console/3605149/125

INT-WIN10-FINAL-INFOSEC-s View Fullscreen Send Ctrl+Alt+Delete Reboot

C:\Users\Administrator> net user superman

```
C:\Users\Administrator>net user superman
User name      superman
Full Name      Flag:999818
Comment
User's comment 000 (System Default)
Country code   Yes
Account active  Never
Password last set  2/25/2018 9:48:13 PM
Password expires  4/8/2018 9:48:13 PM
Password changeable  Yes
Password required Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon      Never
```

10:31 AM 12/26/2023

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZUCCQRHFQ

Ethical Hacking and Systems Defense

Capturing and Analyzing Network Traffic Using a Sniffer

33 The minecraft message should appear in the list.

Opera Mail

Unread (5) Mail Compose Search mail TODAY

All Messages

Unread

minecraft student 12:45 AM

34 Click Opera Mail and then select Exit.

My Public Key - Opera Mail

Page Print Mail Accounts Mail Contacts

PREVIOUS NEXT

43°F Mostly cloudy Search 10:34 AM 12/26/2023

INT-WIN10-FINAL-INFOSEC-s View Fullscreen Send Ctrl+Alt+Delete Reboot

https://lab.infoseclearning.com/console/3605149/125

Security of Sense Firewall | Gmail | YouTube | Maps | News | Certified in Cybersecurity

https://lab.infoseclearning.com/console/3605149/125

INT-WIN10-FINAL-INFOSEC-s View Fullscreen Send Ctrl+Alt+Delete Reboot

Unread (5) Mail Compose Search mail TODAY

All Messages

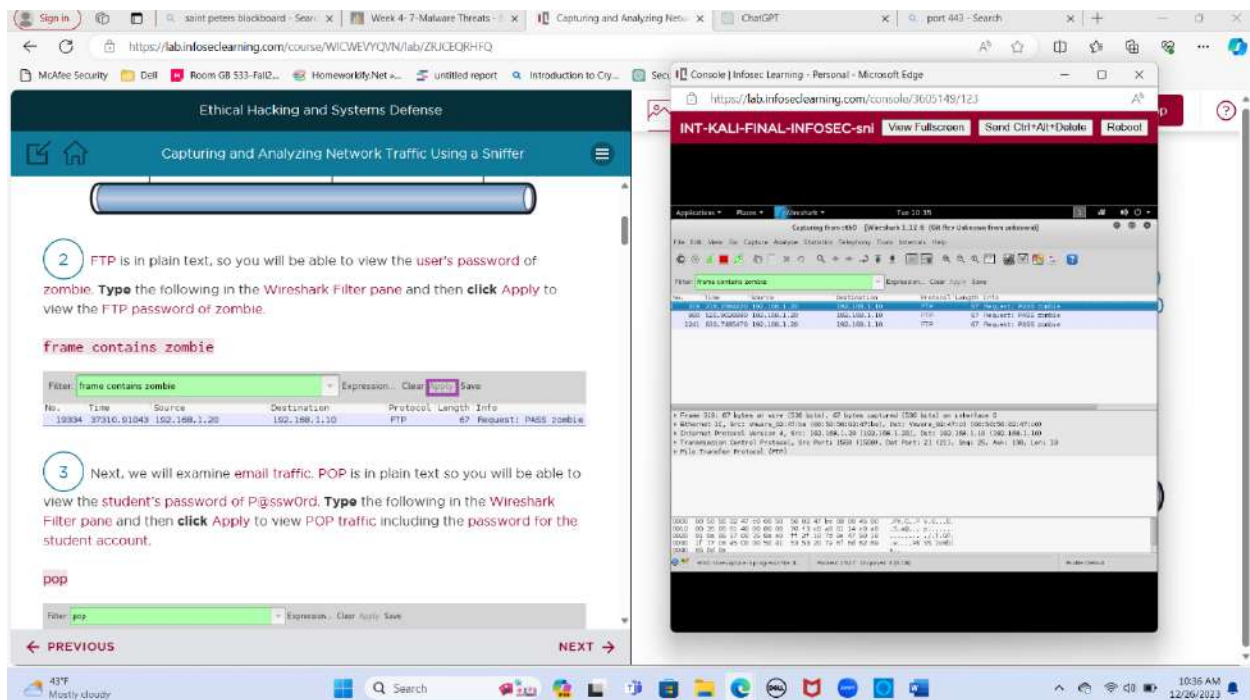
Unread

minecraft student 12:45 AM

10:34 AM 12/26/2023



## Frame contains zombie



2 FTP is in plain text, so you will be able to view the user's password of zombie. Type the following in the Wireshark Filter pane and then click Apply to view the FTP password of zombie.

frame contains zombie

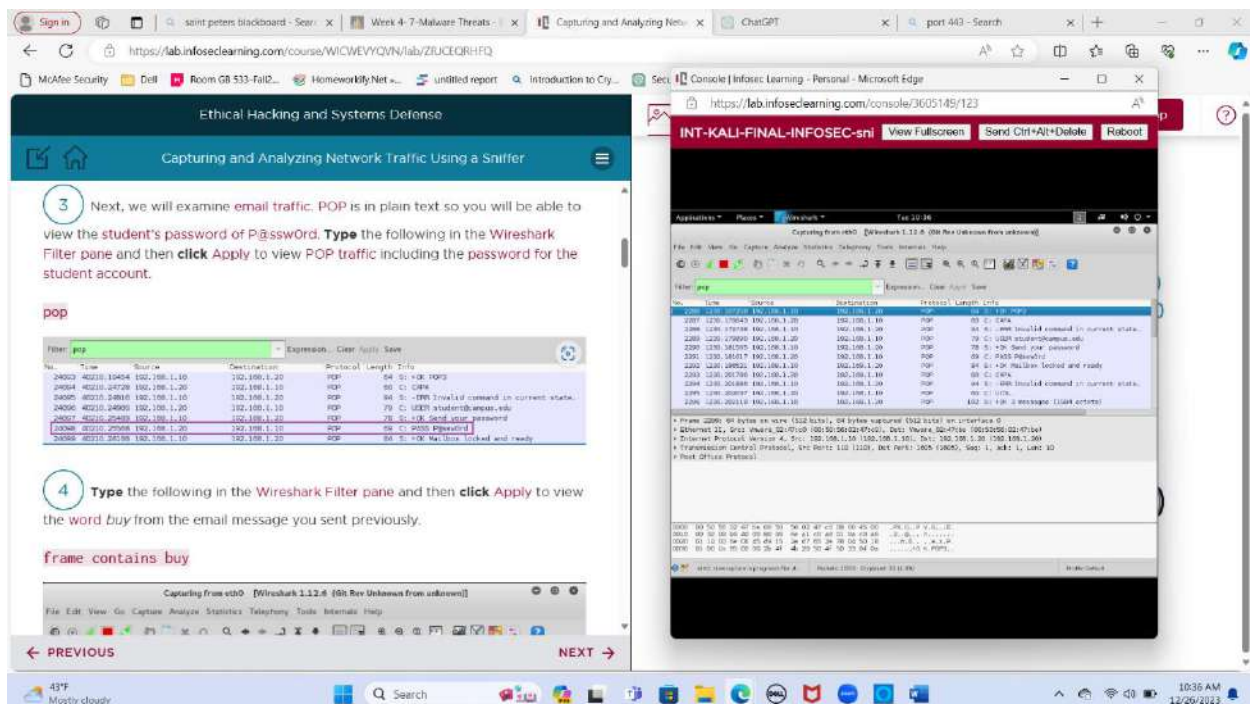
Filter: frame contains zombie

3 Next, we will examine email traffic. POP is in plain text so you will be able to view the student's password of P!ssw0rd. Type the following in the Wireshark Filter pane and then click Apply to view POP traffic including the password for the student account.

pop

Filter: pop

## pop



3 Next, we will examine email traffic. POP is in plain text so you will be able to view the student's password of P!ssw0rd. Type the following in the Wireshark Filter pane and then click Apply to view POP traffic including the password for the student account.

pop

Filter: pop

4 Type the following in the Wireshark Filter pane and then click Apply to view the word buy from the email message you sent previously.

frame contains buy

## Frame contains buy

The screenshot shows a web browser displaying a tutorial on 'Capturing and Analyzing Network Traffic Using a Sniffer'. The tutorial is titled 'Ethical Hacking and Systems Defense' and is part of a course on 'lab.infoseclearning.com'. The tutorial is divided into steps, with the current step being '4 Type the following in the Wireshark Filter pane and then click Apply to view the word buy from the email message you sent previously.' The filter 'frame contains buy' is entered in the Wireshark Filter pane. The packet list shows a single packet (No. 200) of type POP3. The packet details pane shows the 'Frame contains buy' filter applied. The packet bytes pane shows the raw data of the packet.

4 Type the following in the Wireshark Filter pane and then click Apply to view the word buy from the email message you sent previously.

frame contains buy

5 Right-click on the POP frame and select Follow TCP Stream.

## Telnet

The screenshot shows a web browser displaying a tutorial on 'Capturing and Analyzing Network Traffic Using a Sniffer'. The tutorial is titled 'Ethical Hacking and Systems Defense' and is part of a course on 'lab.infoseclearning.com'. The tutorial is divided into steps, with the current step being '7 Type the following in the Wireshark Filter pane and then click Apply to view telnet traffic.' The filter 'telnet' is entered in the Wireshark Filter pane. The packet list shows multiple packets of type TELNET. The packet details pane shows the 'Telnet' filter applied. The packet bytes pane shows the raw data of the packet.

7 Type the following in the Wireshark Filter pane and then click Apply to view telnet traffic.

telnet

8 Right-click on the first telnet frame in the list and select Follow TCP Stream.

## Stopping Wireshark

The screenshot displays a virtual machine environment with two windows. The left window is a tutorial titled "Ethical Hacking and Systems Defense" with the subtitle "Capturing and Analyzing Network Traffic Using a Sniffer". It contains two numbered steps: step 11, "click the red square to stop Wireshark," with a red arrow pointing to the stop button in the Wireshark interface, and step 12, "From the Wireshark Menu bar, select file and then select open," with a red box around the 'File' menu and 'Open...' option. The right window shows the Wireshark 1.12.6 interface. The 'File' menu is open, and 'Open...' is selected. The background shows a Windows taskbar with the time 10:40 AM on 12/09/2023.

11 click the red square to stop Wireshark.

12 From the Wireshark Menu bar, select file and then select open

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Open...

Open Recent

← PREVIOUS

NEXT →

10:40 AM 12/09/2023

This is the last screen before the end of this lab.