

BÁO CÁO BÀI TẬP

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

Tên chủ đề: Lab 1

GVHD: ThS. Đỗ Hoàng Hiển

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT204.O21.ATCL.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Đại Nghĩa	21521182	21521182@gm.uit.edu.vn
2	Hoàng Gia Bảo	21521848	21521848@gm.uit.edu.vn

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

BÁO CÁO CHI TIẾT

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.

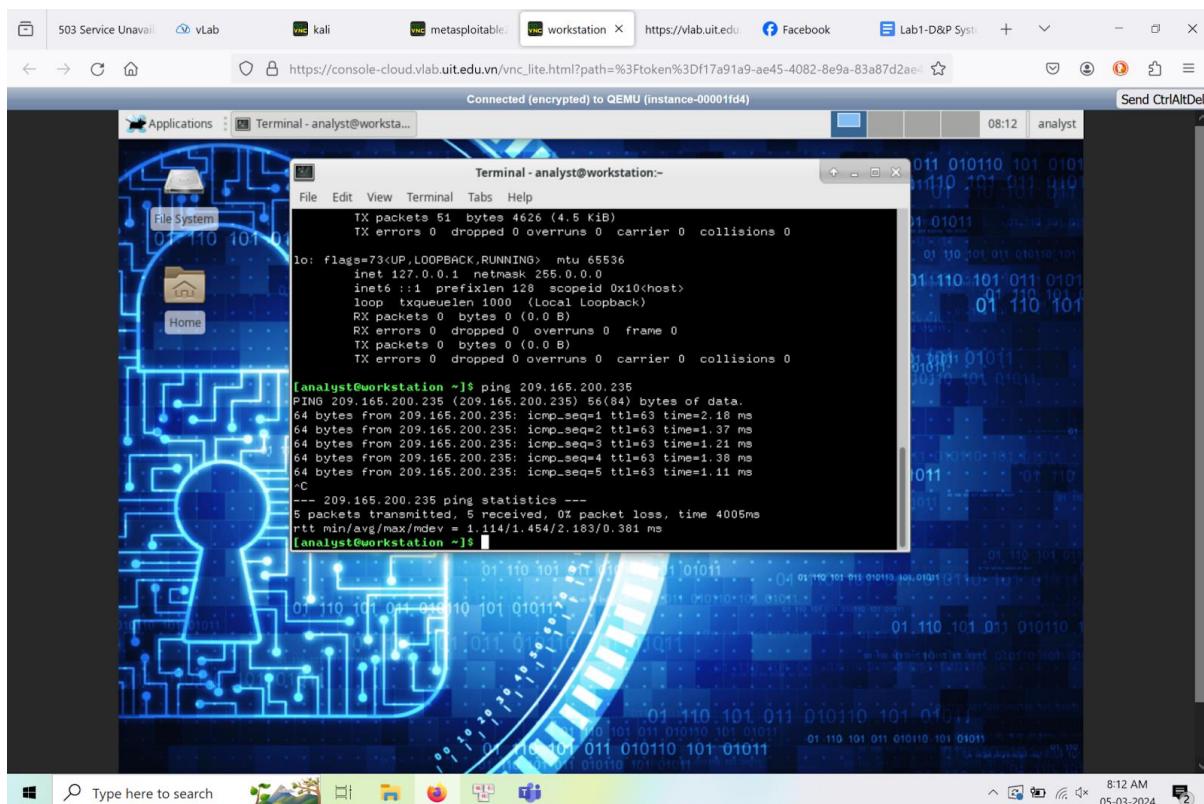
Địa chỉ ip của các máy:

CyberOps Workstation: 192.168.0.11

Metasploitable: 209.165.200.235

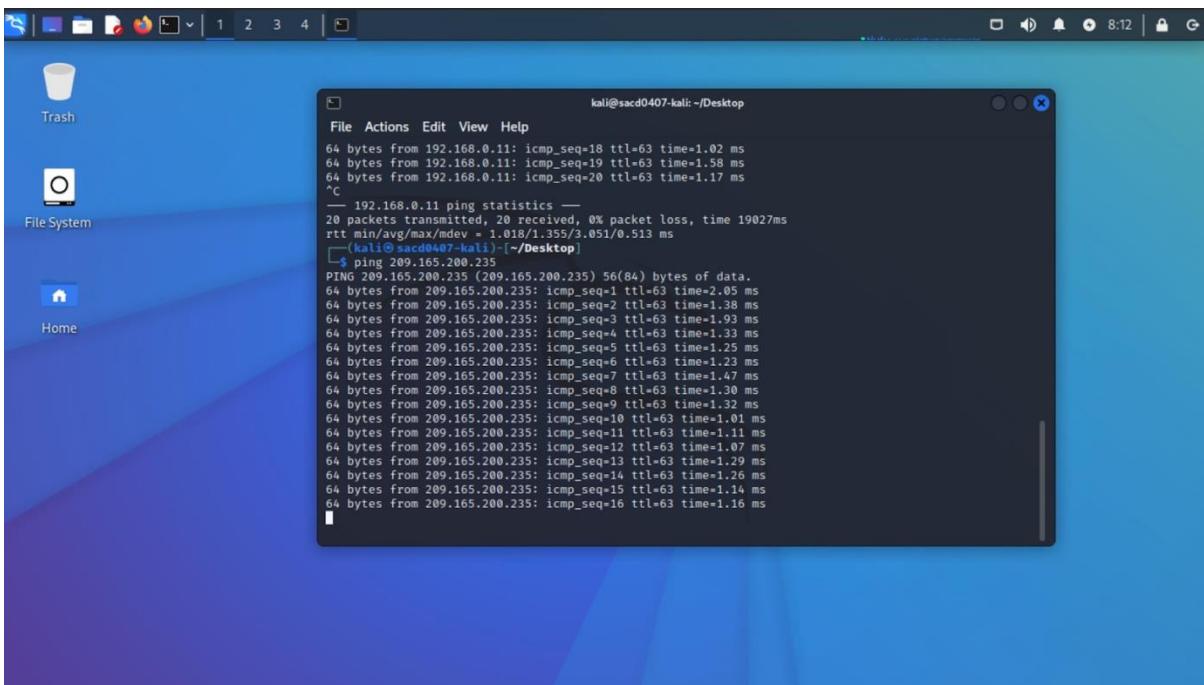
Kali: 209.165.201.17

CyberOps Workstation → Metasploitable

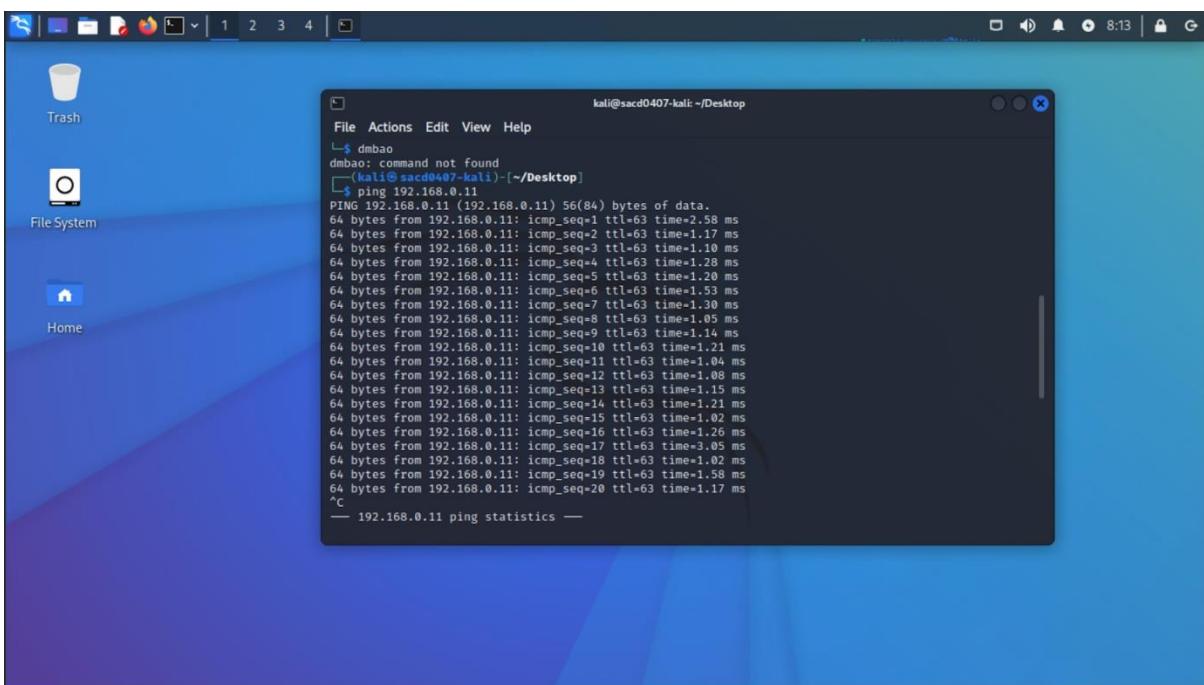


Kali → Metasploitable

Lab 01



Kali → CyberOps Workstation



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.

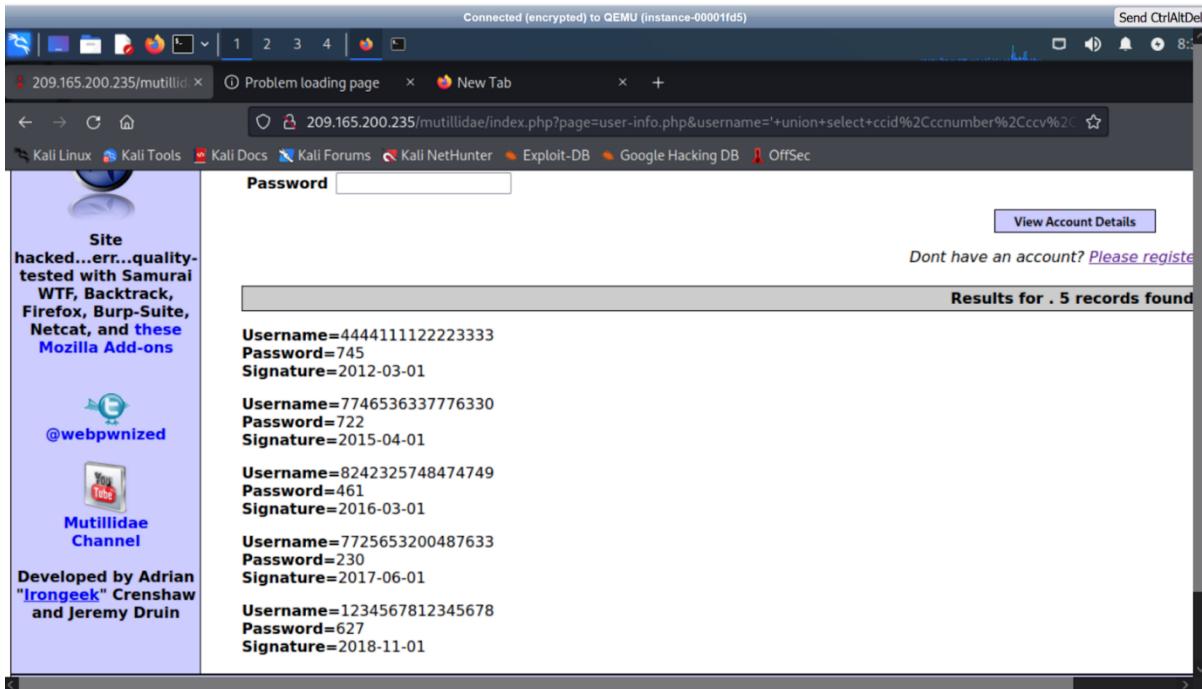
Đầu tiên nhóm em sẽ sửa đổi độ dài của input để có thể nhập vào lệnh phục vụ cho sql injection:

Lab 01

Size được chỉnh thành 200.

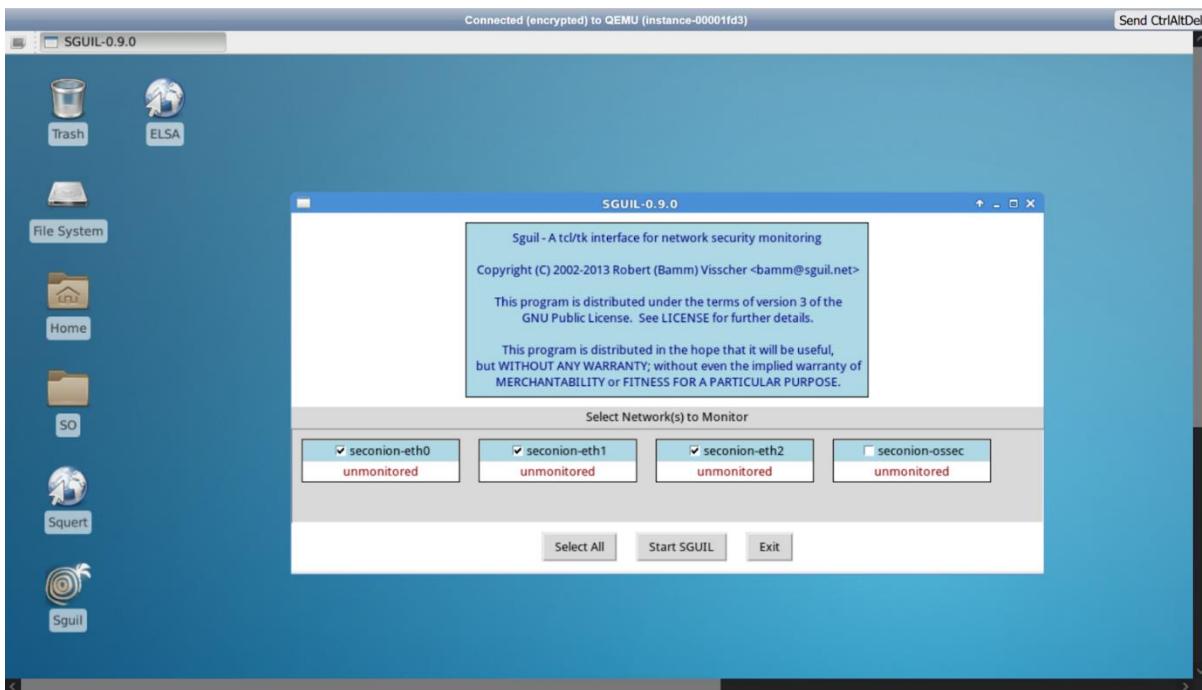
Nhập câu lệnh vào:

Và kết quả trả về được như sau:



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.

Khi vừa bật Sguil lên thì em kích hoạt 3 mạng sau để giám sát:



Kết quả nhận được như sau:

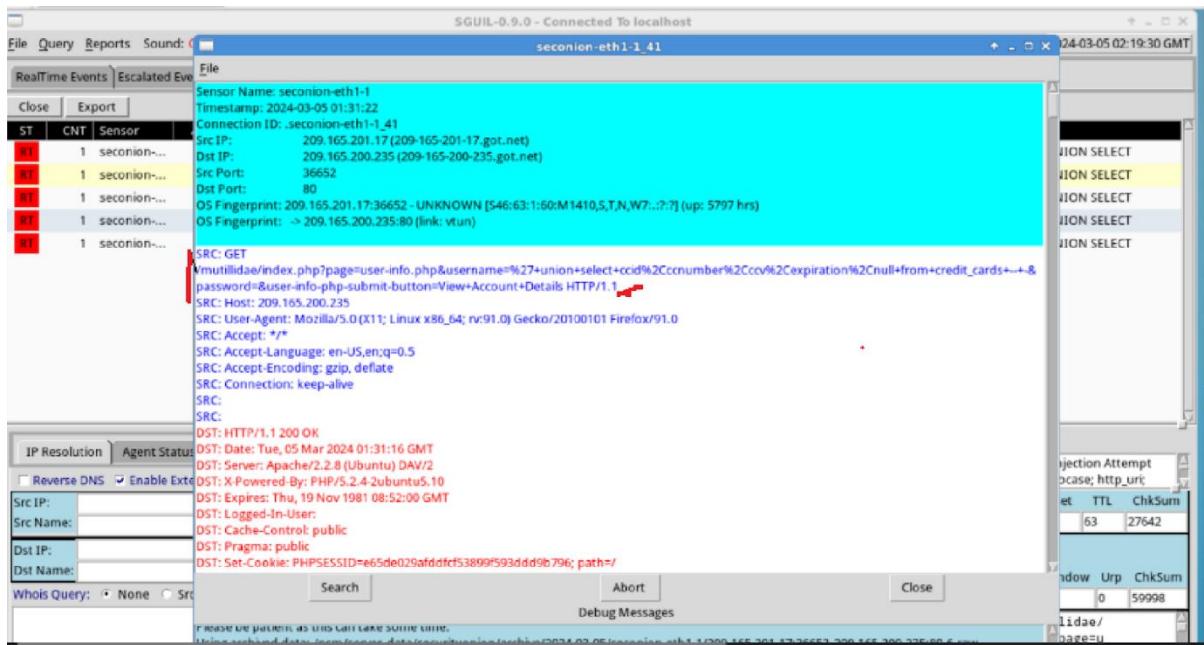
The screenshot shows the SGUIL-0.9.0 interface connected to QEMU. The main window displays a table of real-time events with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. Several rows are highlighted in yellow, indicating specific alerts related to SQL injection attempts. Below the event table is a packet capture window showing TCP and DATA layers with hex and ASCII representations. A rule definition for detecting UNION SELECT attacks is visible at the top of the packet list.

View Correlated Events để xem tất cả các cảnh báo có liên quan:

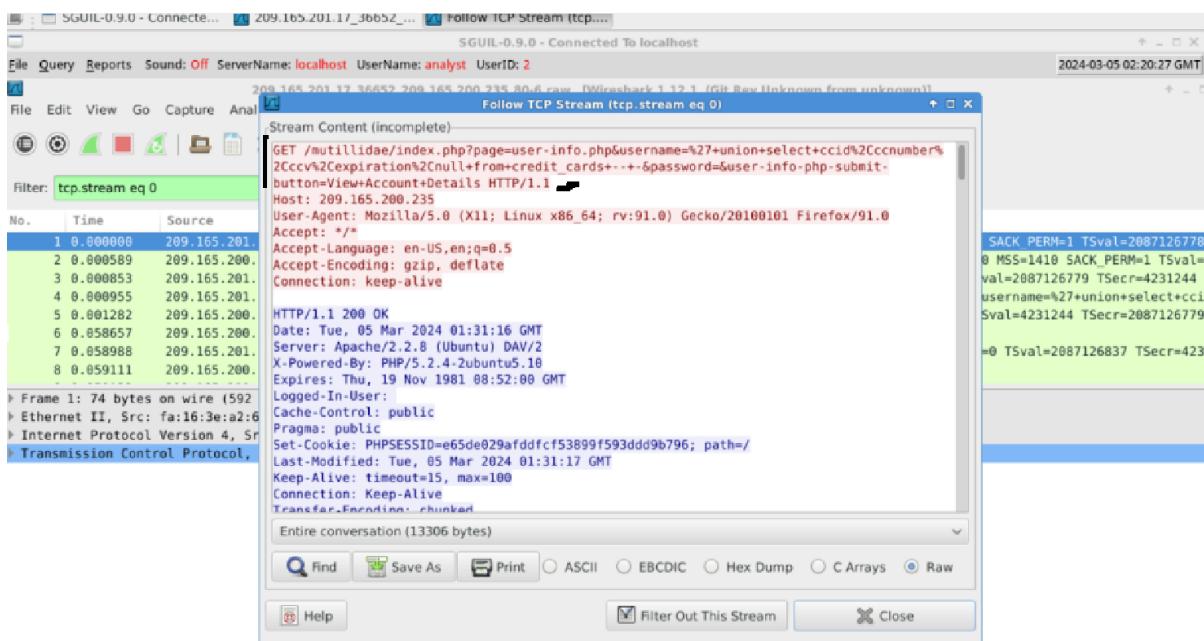
This screenshot shows the SGUIL-0.9.0 interface with a different set of correlated events. The event table shows multiple entries for alert ID 5.36, indicating a series of related SQL injection attempts. The packet capture window below shows the same TCP session and UNION SELECT attack rule as the previous screenshot.

Lab 01

Sau khi nhấp chuột phải trên 1 Alert ID và chọn Transcript thì nhận được payload sau:



Tiếp đến, nhấp chuột phải trên 1 Alert ID và chọn Wireshark và nhấp tiếp chuột phải trên 1 gói tin TCP và chọn Follow TCP Stream thì nhận được payload sau:



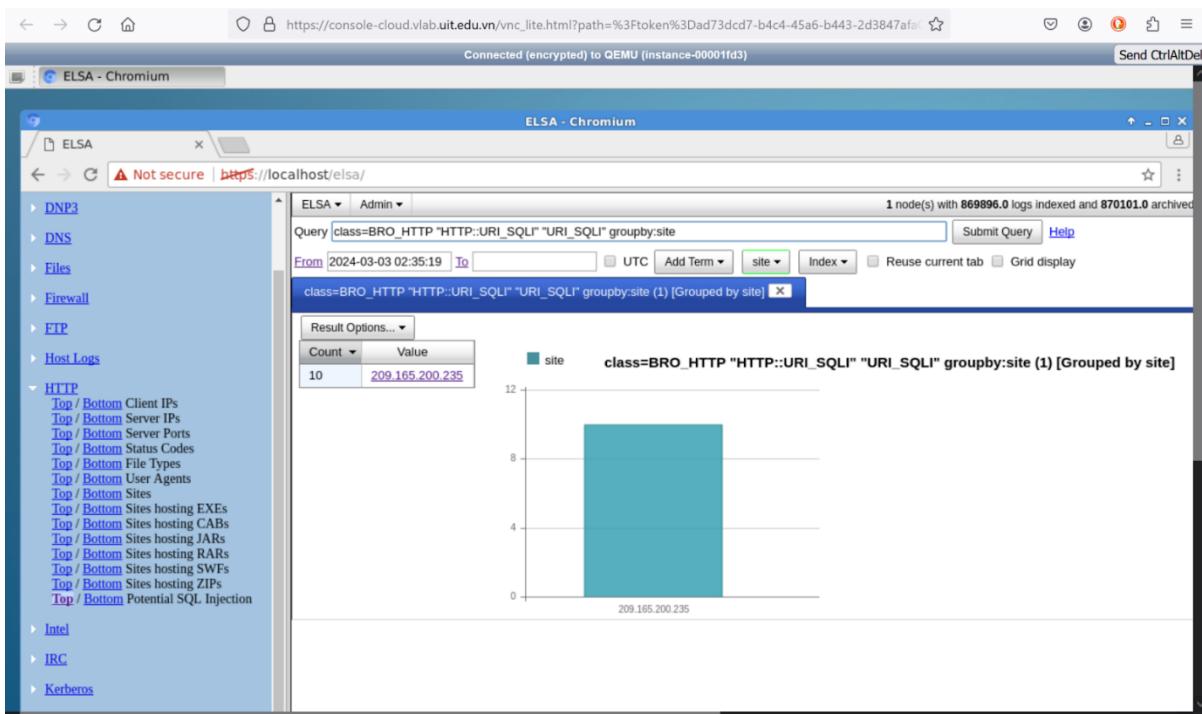


Yêu cầu 2.3. Sinh viên hãy tìm trên ELSA những sự kiện có thông tin liên quan đến tấn công SQL Injection đã thực hiện (payload tấn công, kết quả trả về...). Chụp lại các hình ảnh kết quả cho từng bước

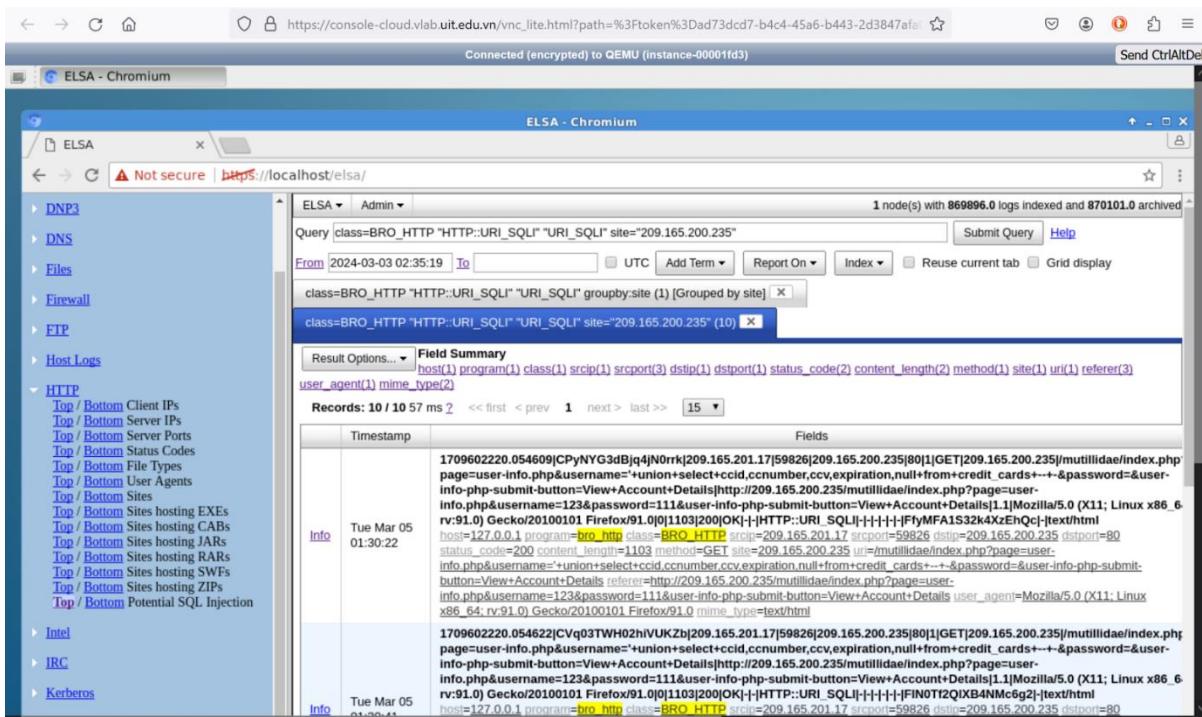
Sau khi đăng nhập vào ELSA thành công thì cửa sổ sau hiện ra:

Ở menu bên tay trái, chọn HTTP > Top Potential SQL Injection, nhận được kết quả sau:

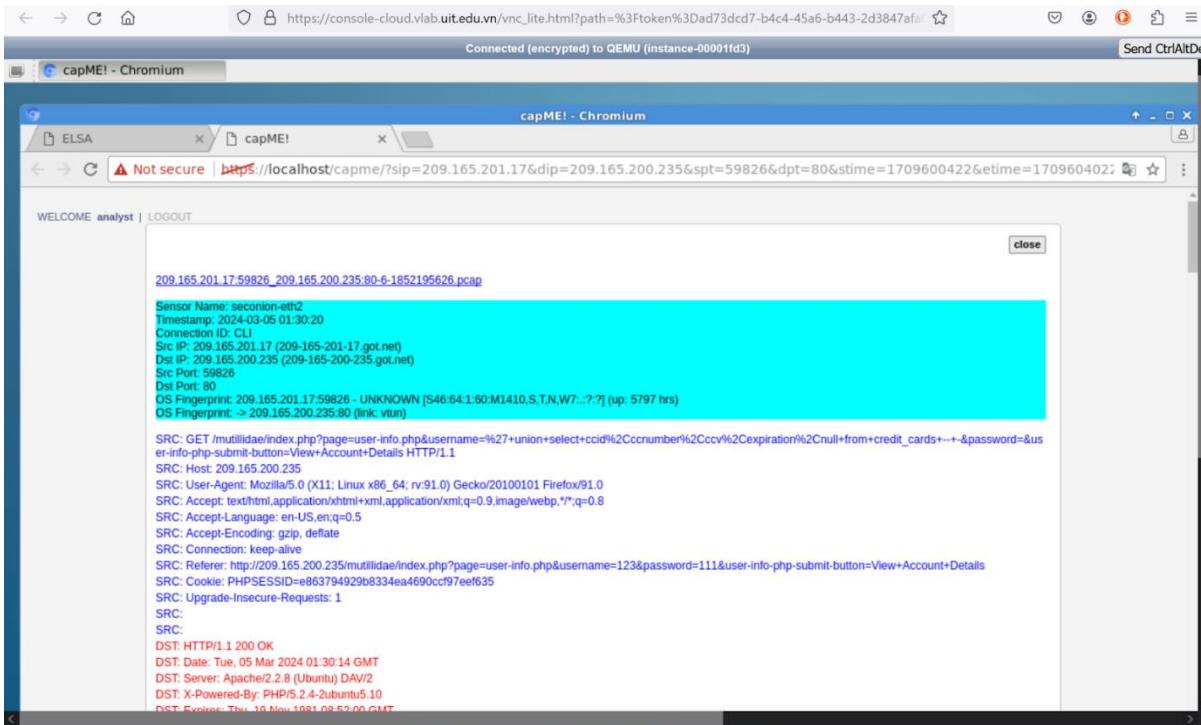
Lab 01



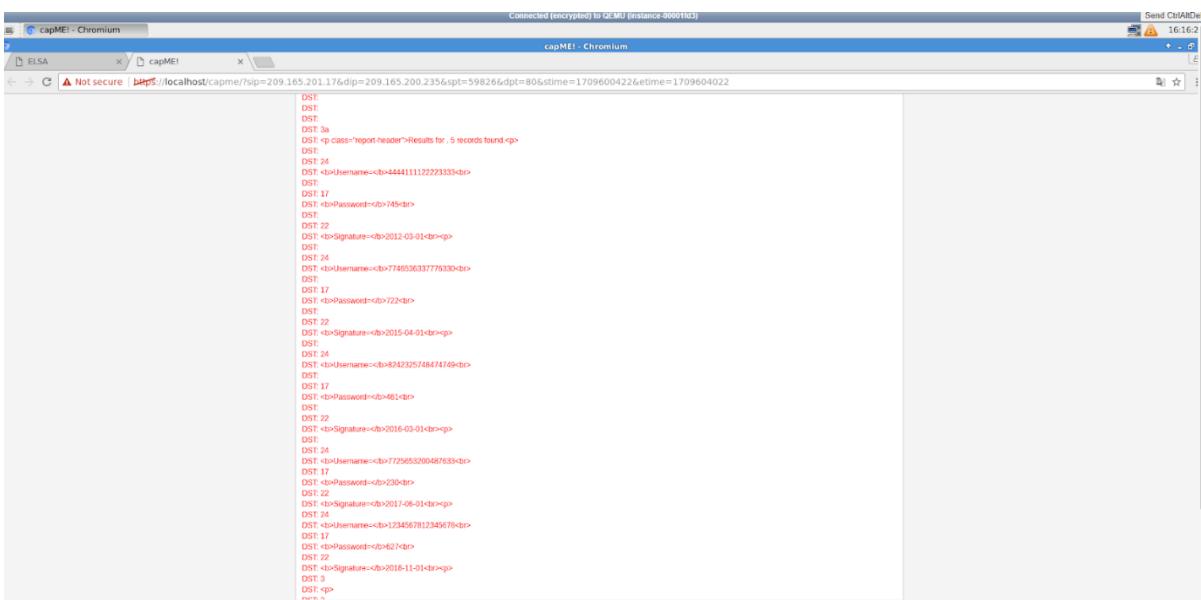
Khi nhấp vào địa chỉ IP 209.165.200.235:



Tiếp đến click vào Info, chọn Plugin > getPcap và đăng nhập vào, nhóm nhận được payload sau:



Dữ liệu sau là những dữ liệu đã bị đánh cắp:

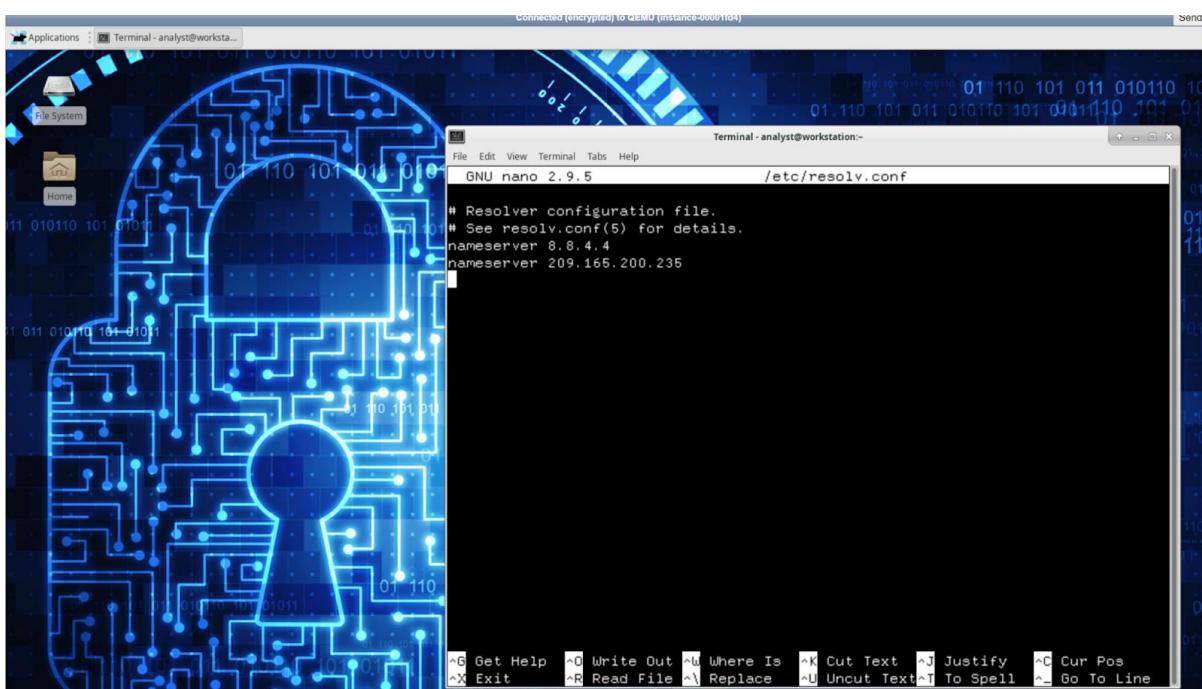


So sánh thông tin tìm được trên công cụ ELSA với thông tin tìm được trên công cụ SGUIL:

- ELSA mạnh mẽ hơn trong việc tìm kiếm dữ liệu log cụ thể và phân tích chi tiết, trong khi SGUIL tập trung hơn vào việc phát hiện sự kiện an ninh và phản ứng sự cố.
- SGUIL có ưu điểm trong việc tích hợp dữ liệu từ nhiều nguồn và quản lý sự kiện an ninh mạng, cung cấp cái nhìn tổng quan và hỗ trợ quy trình phản ứng sự cố. ELSA tập trung vào việc lưu trữ và phân tích log, cung cấp thông tin chi tiết cho việc điều tra và phân tích.
- SGUIL cung cấp một giao diện người dùng đồ họa trực quan, phù hợp với việc quản lý sự kiện và phản ứng sự cố. ELSA yêu cầu sự hiểu biết về cú pháp truy vấn để tìm kiếm và phân tích log, có thể là một thách thức đối với người dùng không chuyên.

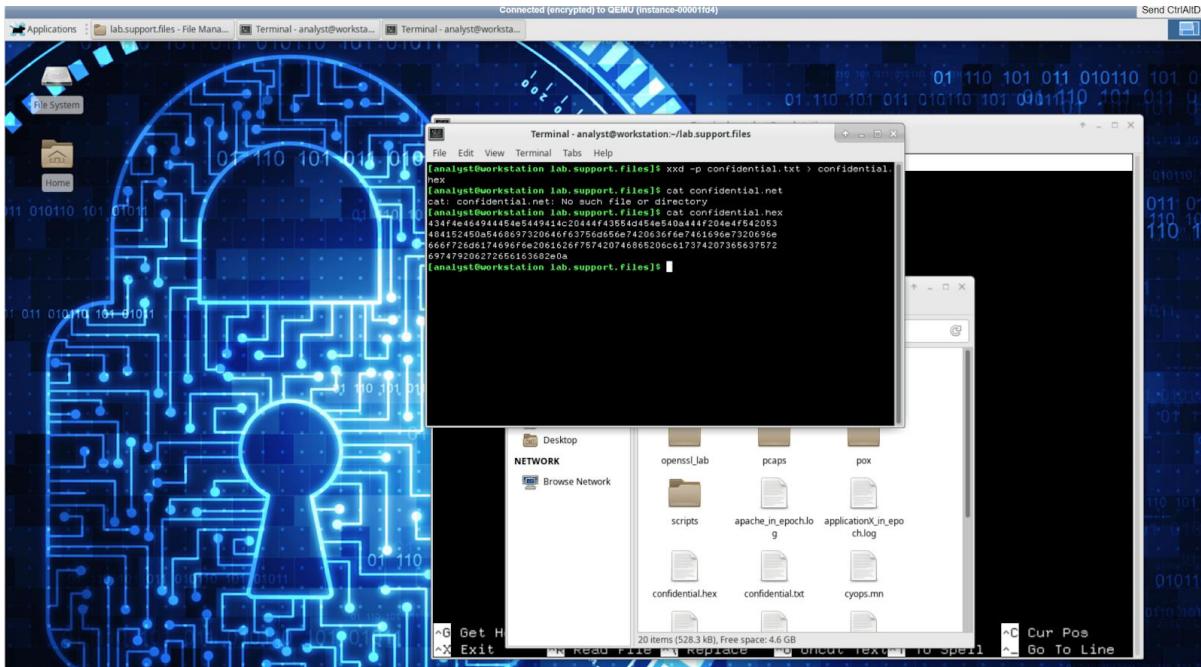
Yêu cầu 3.1. Thực hiện và báo cáo kết quả các bước tấn công lấy dữ liệu thông qua DNS như hướng dẫn. Minh chứng nội dung lấy được sau khi hoàn tất tấn công (file secret.txt)? Chụp lại các hình ảnh kết quả cho từng bước.

Mở file /etc/resolv.conf và kiểm tra danh sách các địa chỉ IP của DNS Server thì có xuất hiện địa chỉ IP của Metasploitable là 209.165.200.235:

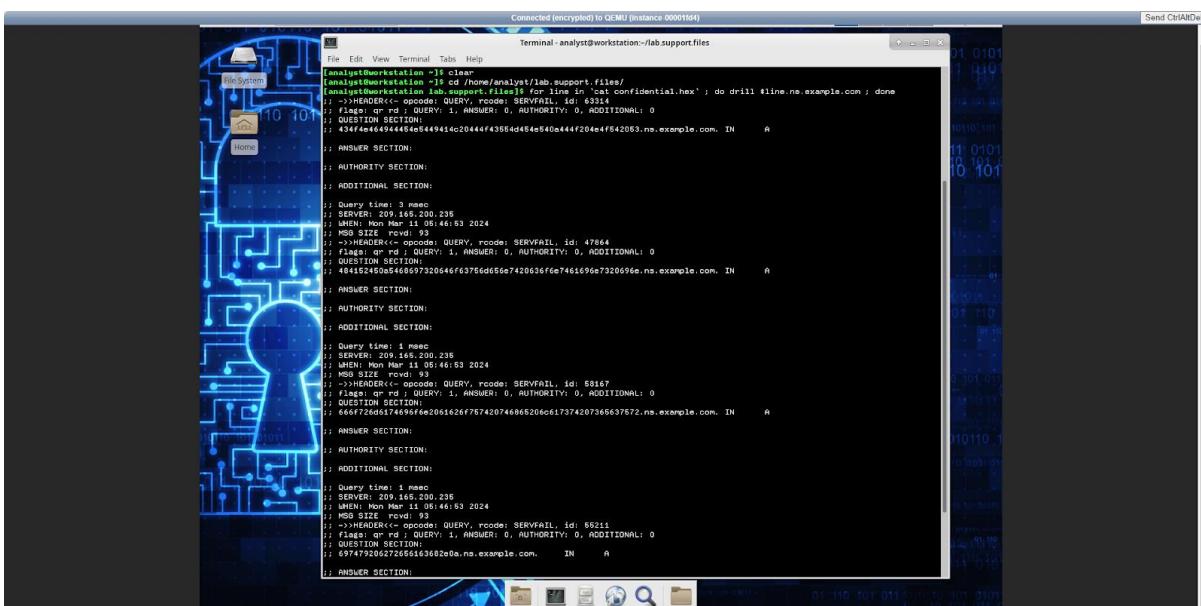


Lab 01

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:



Truy vấn URL tạo ra từ từng dòng hexan trong confidential.hex:



Mở file log /var/lib/bind/query.log trên máy Metasploitable sẽ có thấy được các entry tương ứng với truy vấn:

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

Bởi vì file confidential.hex có 4 dòng nên em có thể tạo ra được 4 URL như vậy từ file confidential.hex.

Từ máy Kali, kết nối SSH đến Metasploitable:

A screenshot of a Kali Linux desktop environment. A terminal window titled 'user@metasploitable-' is open, showing the following command and its output:

```
[user@metasploitable- ~]$ ssh -o StrictHostKeyChecking=ask root@209.165.200.235
Untracked connection to 209.165.200.235 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
[ user@metasploitable- ~]$
```

The terminal shows a warning about an untracked connection to the host '209.165.200.235'. It asks for confirmation to proceed with the connection, as the host key fingerprint is SHA256:80H5E0hXKGCIOLwVscegPLXO0sUpF9M/rJ84rK. The user responds with 'yes' to add the host to the known hosts file. The terminal then prompts for the root password 'root'. After entering the password, it shows the user's home directory: '/home/root'. Finally, it displays the system information: 'Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686'. The desktop background is a blue gradient, and the taskbar at the bottom shows icons for the terminal, file manager, and browser.

Phải thêm option là “-o HostKeyAlgorithms=ssh-rsa” thì mới kết nối SSH được.

Tiếp đến là đọc dữ liệu từ file /var/lib/bind/query.log và lọc ra các thông tin sẽ là nội dung hexan của file confidential.hex và sau đó đưa vào file secret.hex thay vì in ra màn hình:

```

Connected (encrypted) to GEMU (instance 000911d)
user@metasploitable: ~
File Actions Edit View Help
[sudo] password for kali:
-rsa,ssh-dss
File System
[home/kali]
# ssh user@209.165.200.235
ssh user@209.165.200.235
Unable to negotiate with 209.165.200.235 port 22: no matching host key type found. Their offer: ssh-
-rsa,ssh-dss
/home/kali
# ssh -o HostKeyAlgorithms=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 SHA256:4C90509C0GOLUVcepxDfQOsus+9d/rJBBArK.
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: [REDACTED]
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 | uniq > secret.hex
user@metasploitable:~$ 

```

Sau đó sử dụng câu lệnh scp để sao chép file secret.hex từ máy Metasploitable sang máy Kali:

```

Connected (encrypted) to GEMU (instance 000911d)
root@sad0407-kali: ~
File Actions Edit View Help
[root@sad0407-kali ~]
File System
[home/kali]
# ssh user@209.165.200.235
ssh 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 SHA256:4C90509C0GOLUVcepxDfQOsus+9d/rJBBArK.
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: [REDACTED]
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 | uniq > secret.hex
user@metasploitable:~$ exit
logout
Connection to 209.165.200.235 closed.
root@sad0407-kali: ~
# scp user@209.165.200.235:/home/user/secret.hex .
scp: user@209.165.200.235: No such file or directory
# ls
secret.hex
# scp user@209.165.200.235:/home/user/secret.hex ~/
user@209.165.200.235's password:
secret.hex
# ls
secret.hex
# 

```

Cuối cùng là sử dụng lại câu lệnh xxd với option -r -p để chuyển nội dung dạng hex về dạng text:

```

Connected [uncrypted] to GEMU (instance 00091165) Send CtrlAltDel
root@sacd0407-kali:~-
File Actions Edit View Help
root@sacd0407-kali:~/home/kali
└─# xxd -r -p secret.hex > secret.txt
xxd: secret.hex: No such file or directory
└─# find / -name secret.hex 2>/dev/null
/root/secret.hex
root@sacd0407-kali:~/home/kali
└─# cd /root
└─# root@sacd0407-kali:~/home/kali
└─# xxd -r -p secret.hex > secret.txt
root@sacd0407-kali:~/home/kali
└─# cat secret.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
└─#

```

Nhưng mà trước đó phải chuyển đến thư mục root rồi mới có thể sử dụng câu lệnh xxd được, vì file secret.hex nằm ở root.

Đọc nội dung trong file txt được kết quả sau:

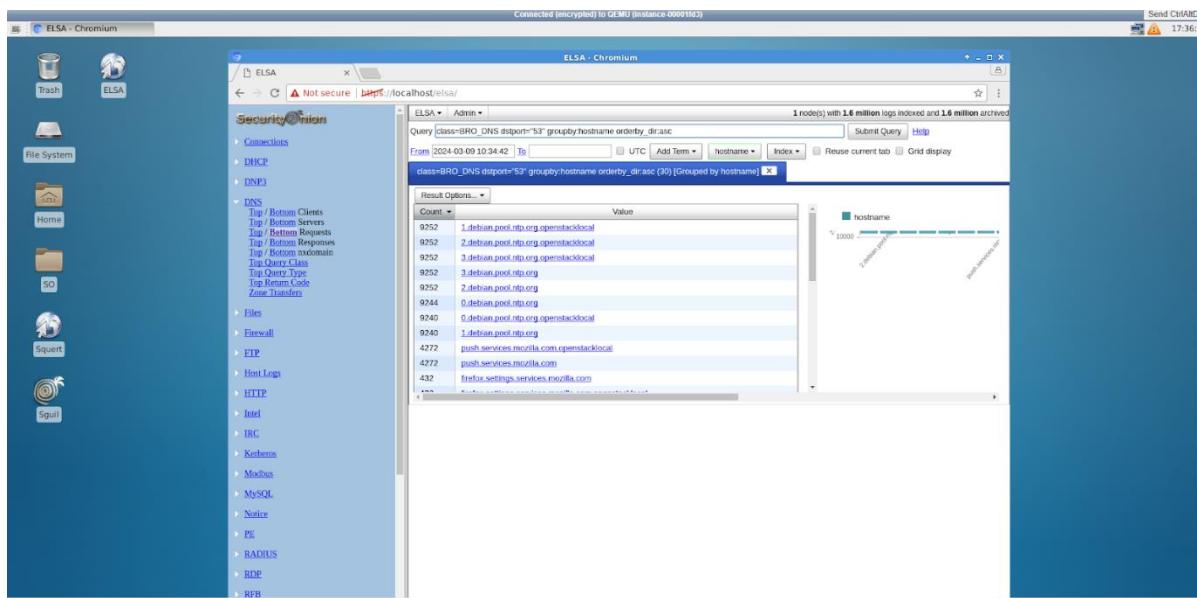
```

Connected [uncrypted] to GEMU (instance 00091165) Send CtrlAltDel
root@sacd0407-kali:~-
File Actions Edit View Help
root@sacd0407-kali:~/home/kali
└─# xxd -r -p secret.hex > secret.txt
xxd: secret.hex: No such file or directory
└─# find / -name secret.hex 2>/dev/null
/root/secret.hex
root@sacd0407-kali:~/home/kali
└─# cd /root
└─# root@sacd0407-kali:~/home/kali
└─# xxd -r -p secret.hex > secret.txt
root@sacd0407-kali:~/home/kali
└─# cat secret.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
└─#

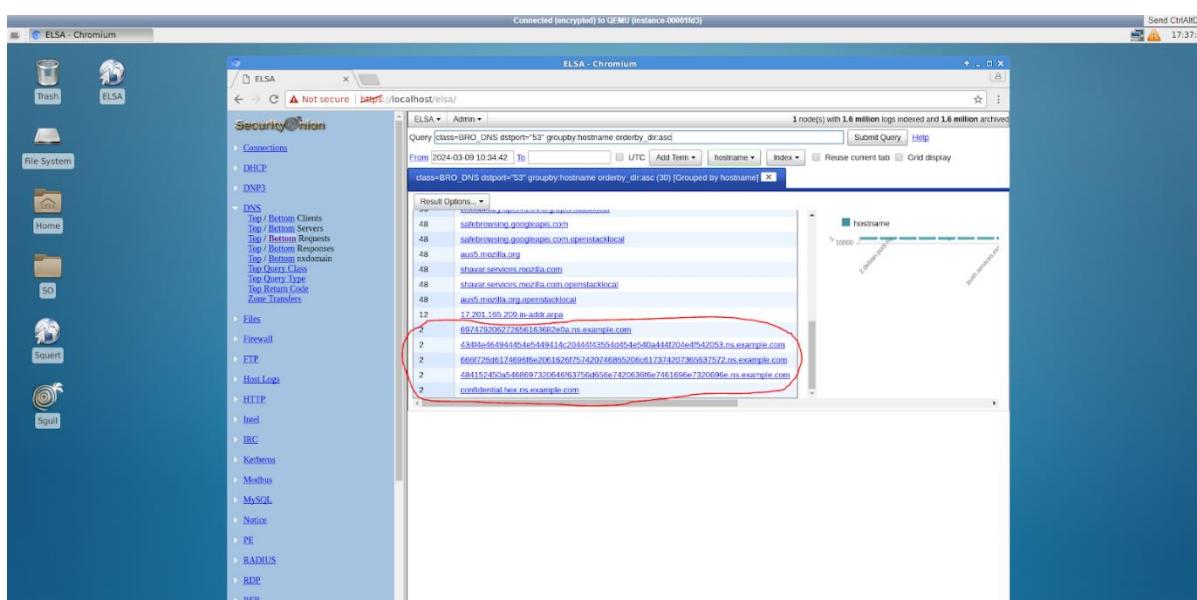
```

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 giải mã đoạn hex và so sánh với nội dung lấy được sau khi tấn công ở Yêu cầu 3.1?

Sau khi mở ELSA, ở menu bên trái và chọn DNS > Bottom Requests thì xuất hiện màn hình sau:



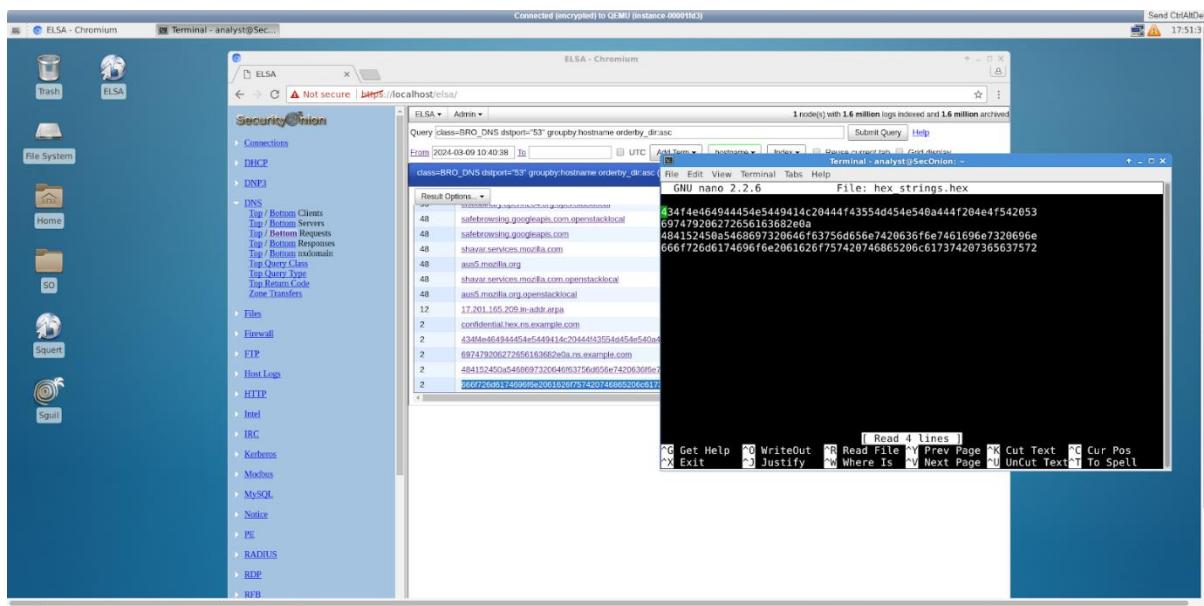
Trong đồng danh sách đó, có xuất hiện các entry có dạng ns.example.com bắt đầu bằng chuỗi hexan:



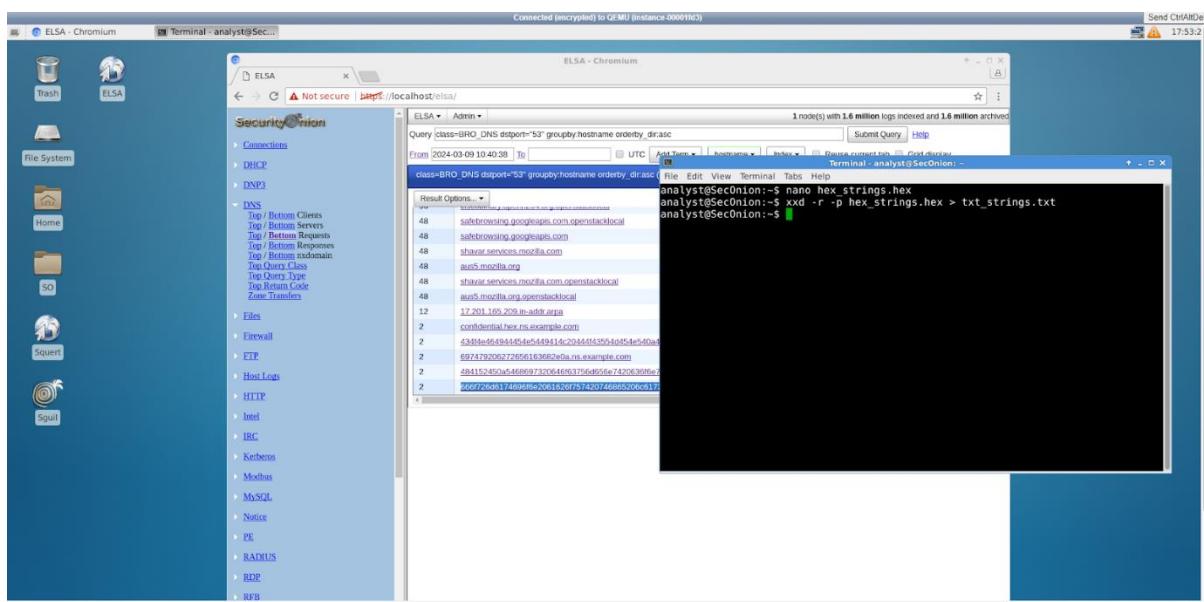
Lab 01

Và đây, chính các entry này là thứ mà cần phải thu thập và xem xét.

Để đọc nội dung của các đoạn hex này thì em mở terminal và đưa các đoạn này vào 1 file hex:



Sau đó lưu lại và sử dụng câu lệnh xxd để chuyển sang dạng text:



Cuối cùng là mở file txt lên để có thể đọc nội dung:

Lab 01

