BÁO CÁO THỰC HÀNH

Môn học: An toàn mạng máy tính

Lab 3: Vulnerability Scanning

GVHD: Đoàn Minh Trung

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.O12.ATCL – Nhóm 03

STT	Họ và tên	MSSV	Email
1	Bùi Hoàng Trúc Anh	21521817	21521817@gm.uit.edu.vn
2	Lê Hoàng Oanh	21521253	21521253@gm.uit.edu.vn
3	Nguyễn Ngọc Trà My	21520353	21520353@gm.uit.edu.vn
4	Huỳnh Minh Tân Tiến	21521520	21521520@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Bài 1	100%
2	Bài 2	100%
3	Bài 3	100%
4	Bài 4	100%
5	Bài 5	100%
6	Bài 6	100%
7	Bài 7	100%
8	Bài 8	100%
9	Bài 9	100%
10	Bài 10	100%
11	Bài 11	100%

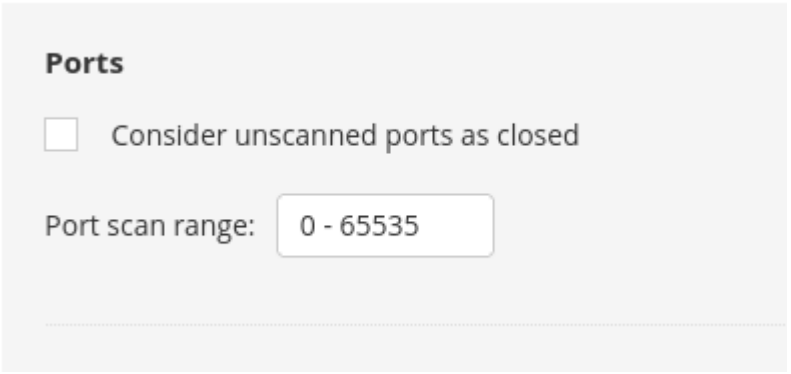
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

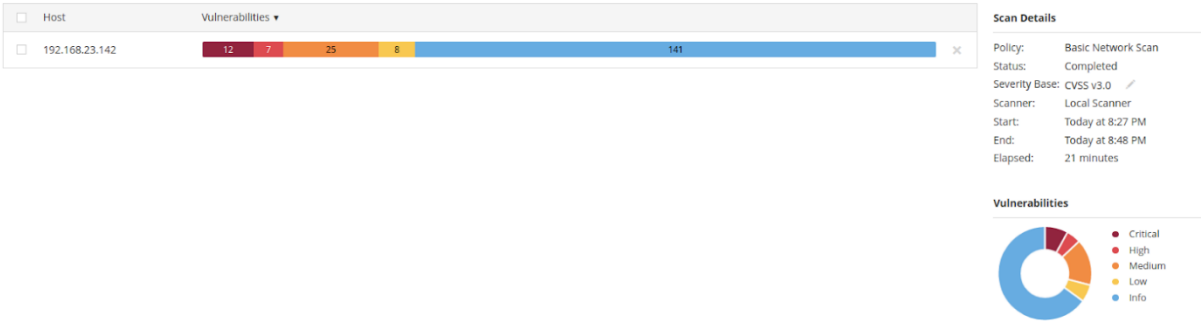
[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Thực hiện lại các bước trên để quét máy Metasploitable 2 không sử dụng tài khoản chứng thực.

IP victim: 192.168.23.142



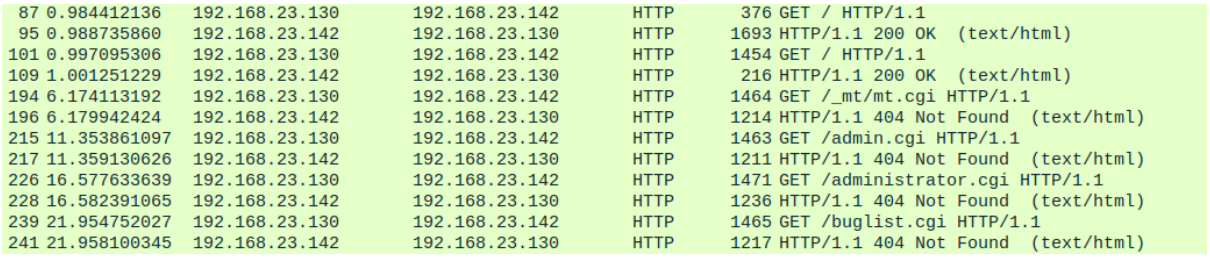


Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *		NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	DNS (Multiple Issues)	DNS	4
MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5 *		rlogin Service Detection	Service detection	1
HIGH	7.5 *		rsh Service Detection	Service detection	1
HIGH	7.5		Samba Badlock Vulnerability	General	1

2. Bật Wireshark sau đó tiến hành quét và xác định các bước mà Nessus đã thực hiện để hoàn tất quá trình quét.

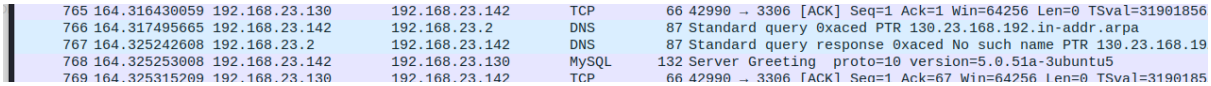
Nessus liên tục gửi các loại packet khác nhau đến máy victim

HTTP



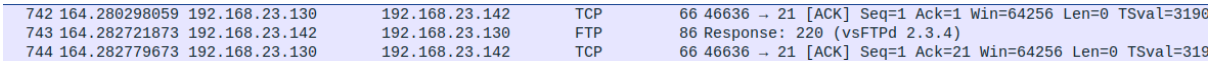
87	0.984412136	192.168.23.130	192.168.23.142	HTTP	376	GET / HTTP/1.1
95	0.988735860	192.168.23.142	192.168.23.130	HTTP	1693	HTTP/1.1 200 OK (text/html)
101	0.997095306	192.168.23.130	192.168.23.142	HTTP	1454	GET / HTTP/1.1
109	1.001251229	192.168.23.142	192.168.23.130	HTTP	216	HTTP/1.1 200 OK (text/html)
194	6.174113192	192.168.23.130	192.168.23.142	HTTP	1464	GET /_mt/mt.cgi HTTP/1.1
196	6.179942424	192.168.23.142	192.168.23.130	HTTP	1214	HTTP/1.1 404 Not Found (text/html)
215	11.353861097	192.168.23.130	192.168.23.142	HTTP	1463	GET /admin.cgi HTTP/1.1
217	11.359130626	192.168.23.142	192.168.23.130	HTTP	1211	HTTP/1.1 404 Not Found (text/html)
226	16.577633639	192.168.23.130	192.168.23.142	HTTP	1471	GET /administrator.cgi HTTP/1.1
228	16.582391065	192.168.23.142	192.168.23.130	HTTP	1236	HTTP/1.1 404 Not Found (text/html)
239	21.954752027	192.168.23.130	192.168.23.142	HTTP	1465	GET /buglist.cgi HTTP/1.1
241	21.958100345	192.168.23.142	192.168.23.130	HTTP	1217	HTTP/1.1 404 Not Found (text/html)

DNS ,MySQL



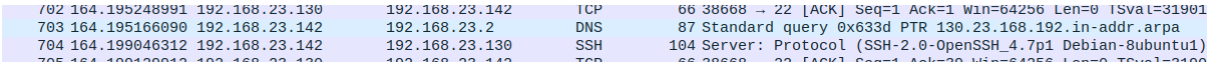
765	164.316430059	192.168.23.130	192.168.23.142	TCP	66	42990 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=31901856
766	164.317495665	192.168.23.142	192.168.23.2	DNS	87	Standard query 0xaced PTR 130.23.168.192.in-addr.arpa
767	164.325242608	192.168.23.2	192.168.23.142	DNS	87	Standard query response 0xaced No such name PTR 130.23.168.19
768	164.325253008	192.168.23.142	192.168.23.130	MySQL	132	Server Greeting proto=10 version=5.0.51a-3ubuntu5
769	164.325315209	192.168.23.130	192.168.23.142	TCP	66	42990 → 3306 [ACK] Seq=1 Ack=67 Win=64256 Len=0 TSval=3190185

FTP



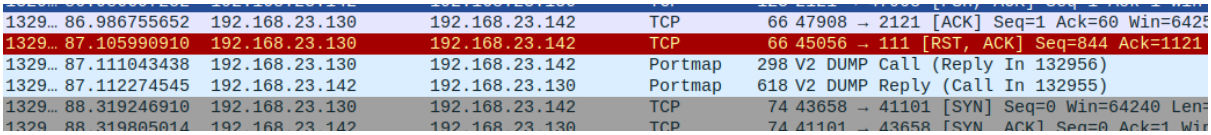
742	164.280298059	192.168.23.130	192.168.23.142	TCP	66	46636 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3190
743	164.282721873	192.168.23.142	192.168.23.130	FTP	86	Response: 220 (vsFTPd 2.3.4)
744	164.282779673	192.168.23.130	192.168.23.142	TCP	66	46636 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=319

SSH



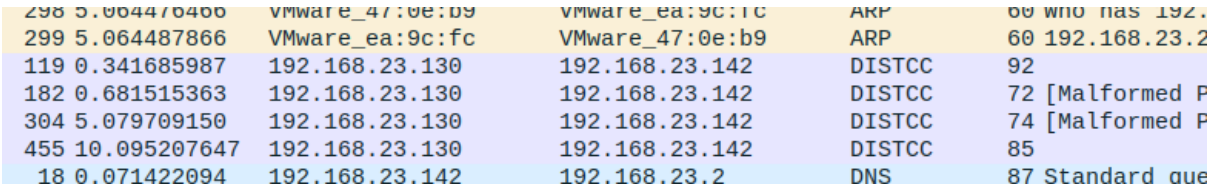
702	164.195248991	192.168.23.130	192.168.23.142	TCP	66	38668 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=31901
703	164.195166090	192.168.23.142	192.168.23.2	DNS	87	Standard query 0x633d PTR 130.23.168.192.in-addr.arpa
704	164.199046312	192.168.23.142	192.168.23.130	SSH	104	Server: Protocol (SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1)

PortMap



1329…	86.986755652	192.168.23.130	192.168.23.142	TCP	66	47908 → 2121 [ACK] Seq=1 Ack=60 Win=6425
1329…	87.105990910	192.168.23.130	192.168.23.142	TCP	66	45056 → 111 [RST, ACK] Seq=844 Ack=1121
1329…	87.111043438	192.168.23.130	192.168.23.142	Portmap	298	V2 DUMP Call (Reply In 132956)
1329…	87.112274545	192.168.23.142	192.168.23.130	Portmap	618	V2 DUMP Reply (Call In 132955)
1329…	88.319246910	192.168.23.130	192.168.23.142	TCP	74	43658 → 41101 [SYN] Seq=0 Win=64240 Len=
1329…	88.319805014	192.168.23.142	192.168.23.130	TCP	74	41101 → 43658 [SYN, ACK] Seq=0 Ack=1 Wi

DISTCC



298	5.064476466	VMware_47:0e:b9	VMware_ea:9c:fc	ARP	60	Who has 192.
299	5.064487866	VMware_ea:9c:fc	VMware_47:0e:b9	ARP	60	192.168.23.2
119	0.341685987	192.168.23.130	192.168.23.142	DISTCC	92	
182	0.681515363	192.168.23.130	192.168.23.142	DISTCC	72	[Malformed P
304	5.079709150	192.168.23.130	192.168.23.142	DISTCC	74	[Malformed P
455	10.095207647	192.168.23.130	192.168.23.142	DISTCC	85	
18	0.071422094	192.168.23.142	192.168.23.2	DNS	87	Standard que

SMB

```
5787 86.931449443  192.168.23.142  192.168.23.130  SMB   105 NT Create AndX Response, FID: 0x0000, Error: STATUS_OBJECT_NAME_NOT_FOUND
5786 86.930684439  192.168.23.130  192.168.23.142  SMB   318 NT Create AndX Request, Path: ${jndi:ldap://log4shell-smb-Gehu1ETe0HuXPS2gENqT${lower:ten}.w.nessus.or
5784 86.926836718  192.168.23.142  192.168.23.130  SMB   118 Tree Connect AndX Response
5783 86.926006713  192.168.23.130  192.168.23.142  SMB   164 Tree Connect AndX Request, Path: \\METASPLOITABLE\IPC$
1129 61.904570944  192.168.23.142  192.168.23.130  SMB   105 Tree Connect AndX Response, Error: STATUS_BAD_NETWORK_NAME
1128 61.887184148  192.168.23.130  192.168.23.142  SMB   318 Tree Connect AndX Request, Path: \\METASPLOITABLE\${jndi:ldap://log4shell-smb-Gehu1ETe0HuXPS2gENqT${lo
1127 61.883492528  192.168.23.142  192.168.23.130  SMB   192 Session Setup AndX Response
1126 61.882774424  192.168.23.130  192.168.23.142  SMB   328 Session Setup AndX Request, NTLMSSP_AUTH, User: \
1125 61.868386445  192.168.23.142  192.168.23.130  SMB   440 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
1124 61.867240338  192.168.23.130  192.168.23.142  SMB   306 Session Setup AndX Request, NTLMSSP_NEGOTIATE
1122 61.861892009  192.168.23.142  192.168.23.130  SMB   197 Negotiate Protocol Response
1120 61.860725382  192.168.23.130  192.168.23.142  SMB   324 Negotiate Protocol Request
 852 36.836840819  192.168.23.142  192.168.23.130  SMB   192 Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
```

Rlogin

```
7732 116.773700420 192.168.23.130  192.168.23.142  Rlogin  583 Data: \026\003\001\002\000\001\000\001f\003\003000f\027f\0300f3\026;p\005f
7726 116.766226479 192.168.23.130  192.168.23.142  Rlogin  375 Data: GET / HTTP/1.1\r\nHost: 192.168.23.142:513\r\nAccept-Charset: iso-8
5754 82.449996398  192.168.23.130  192.168.23.142  Rlogin  583 Data: \026\003\001\002\000\001\000\001f\003\003f0f\01600f\t`$j@'^ffLf\016f
 732 35.151391211  192.168.23.130  192.168.23.142  Rlogin  177 Data: \003\001\n\000\000\a\000\000\000;\000\000\000\000\000\000\000\000\0
 435 10.029853386  192.168.23.130  192.168.23.142  Rlogin   85 Data: \003\000\000\023\016f\000\000\000\000\000\001\000\b\000\000\000\000
 168 0.653794310   192.168.23.130  192.168.23.142  Rlogin   72 Data: HELP\r\n
  95 0.268281882   192.168.23.142  192.168.23.130  Rlogin   67 Data: \001
  72 0.167591825   192.168.23.130  192.168.23.142  Rlogin   92 Start Handshake
```

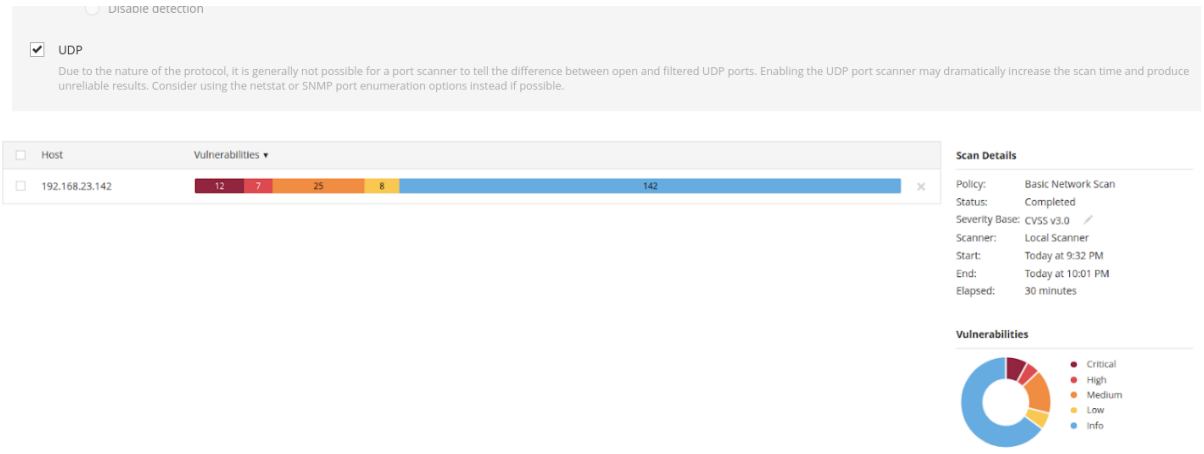
ICMP

```
1222 70.678981698  192.168.23.142  192.168.23.130  ICMP   82 Destination unreachable (Port unreachable)
1220 70.676994487  192.168.23.142  192.168.23.130  ICMP   82 Destination unreachable (Port unreachable)
1218 70.668124238  192.168.23.142  192.168.23.130  ICMP  106 Destination unreachable (Port unreachable)
1190 70.270652643  192.168.23.142  192.168.23.130  ICMP   71 Destination unreachable (Port unreachable)
1169 65.217088037  192.168.23.142  192.168.23.130  ICMP  124 Destination unreachable (Port unreachable)
1165 65.201892652  192.168.23.142  192.168.23.130  ICMP   87 Destination unreachable (Port unreachable)
1163 65.200598145  192.168.23.142  192.168.23.130  ICMP   87 Destination unreachable (Port unreachable)
1137 64.967902360  192.168.23.142  192.168.23.130  ICMP  358 Destination unreachable (Port unreachable)
1135 64.965571947  192.168.23.142  192.168.23.130  ICMP  358 Destination unreachable (Port unreachable)
1094 59.908277921  192.168.23.142  192.168.23.130  ICMP  118 Destination unreachable (Port unreachable)
```

RSH

```
   72 0.167591825   192.168.23.130  192.168.23.142  Rlogin   92 Start Handshake
   12 0.069337082   192.168.23.130  192.168.23.142  Rlogin   74 Data: I\000\000\000f\000\000\000
 7804 127.822308125 192.168.23.130  192.168.23.142  RSH     375 Client -> Server data
 6418 98.482505223  192.168.23.130  192.168.23.142  RSH     583 Client -> Server data
 5793 90.092783799  192.168.23.142  192.168.23.130  RSH     117 Server -> Client Data
 4741 80.094795593  192.168.23.130  192.168.23.142  RSH      85 Client -> Server data
 1109 60.187729064  192.168.23.130  192.168.23.142  RSH     177 Client -> Server data
  894 41.326698311  192.168.23.130  192.168.23.142  RSH      79 Session Establishment
  892 41.326282909  192.168.23.130  192.168.23.142  RSH      68 Session Establishment
  704 30.531611100  192.168.23.130  192.168.23.142  RSH      92 Client -> Server data
  695 30.117991916  192.168.23.130  192.168.23.142  RSH      74 Client -> Server data
  171 0.663764965   192.168.23.130  192.168.23.142  RSH      72 Client -> Server data
 7783 121.815347759 192.168.23.130  192.168.23.142  RMI     583 Continuation
```

3. Quét lại nhưng quét thêm port UDP

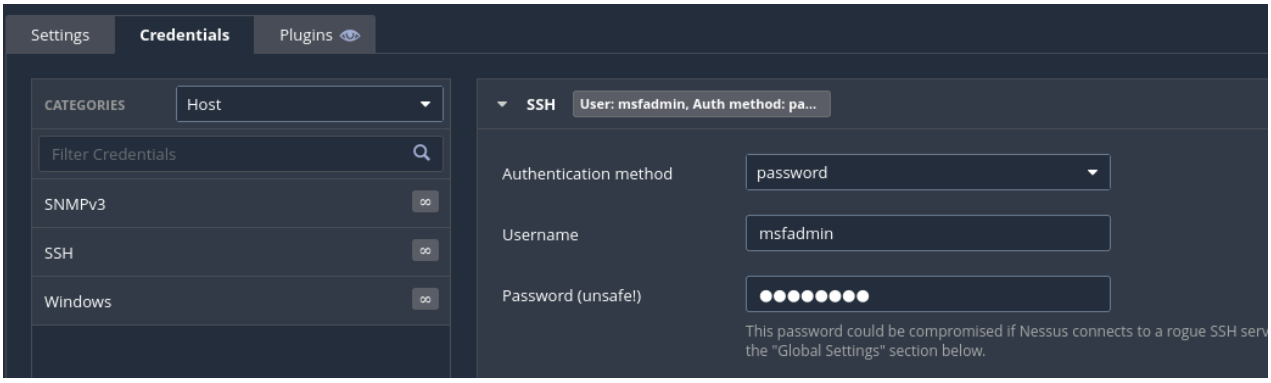


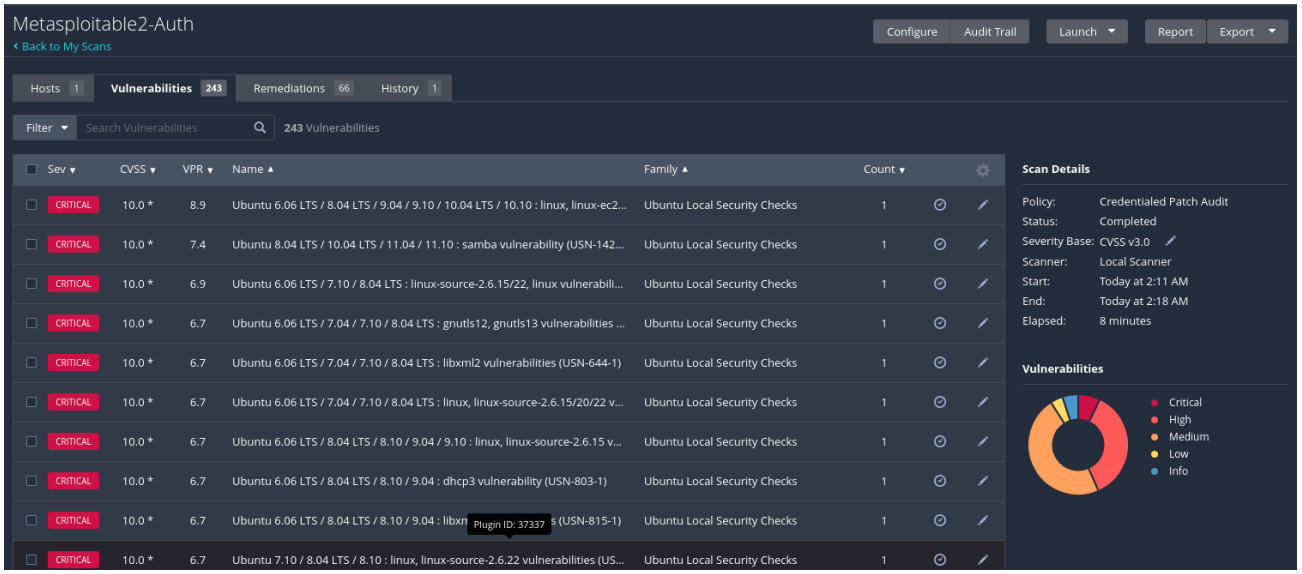
CRITICAL	9.8	SSL Version 2 and 3 Protocol Detection	Service detection	2		
CRITICAL	9.8	Bind Shell Backdoor Detection	Backdoors	1		
HIGH	7.5	NFS Shares World Readable	RPC	1		
HIGH	7.5 *	rlogin Service Detection	Service detection	1		
HIGH	7.5 *	rsh Service Detection	Service detection	1		
HIGH	7.5	Samba Badlock Vulnerability	General	1		
MEDIUM	6.5	TLS Version 1.0 Protocol Detection	Service detection	2		
MEDIUM	6.5	Unencrypted Telnet Server	Misc.	1		
MEDIUM	5.9	SSL Anonymous Cipher Suites Supported	Service detection	1		
MEDIUM	5.9	SSL DROWN Attack Vulnerability (Decrypting RSA w Plugin ID: 11213 Weakened eNcryp...	Misc.	1		
MEDIUM	5.3	HTTP TRACE / TRACK Methods Allowed	Web Servers	1		
LOW	3.7	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1		
LOW	2.6 *	X Server Detection	Service detection	1		

4. Thực hiện lại các bước trên để quét máy Metasploitable 2 có sử dụng tài khoản chứng thực.

IP victim: 192.168.10.135

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr
          inet addr:192.168.10.135
```





5. **Kiểm tra kết quả quét và so sánh với việc quét không sử dụng tài khoản chứng thực.**

Không sử dụng tài khoản chứng thực:

- Nessus thực hiện quét bằng cách gửi các gói tin đặc biệt tới các cổng mạng và phân tích các phản hồi từ máy chủ.
- Kết quả quét cung cấp thông tin về các lỗ hổng bảo mật, cấu hình hệ thống, các cổng mạng mở và các dấu vết tiềm ẩn trong hệ thống mục tiêu.
- Kết quả này có thể không cung cấp thông tin chi tiết về các lỗ hổng phức tạp và các vấn đề liên quan đến xác thực và ủy quyền.

Sử dụng tài khoản chứng thực:

- Nessus có thể truy cập sâu vào hệ thống mục tiêu và kiểm tra chi tiết hơn.
- Sử dụng tài khoản chứng thực, Nessus kiểm tra các lỗ hổng phức tạp hơn, cấu hình hệ thống, phân tích log, quét các ứng dụng phía máy chủ và sử dụng các công cụ phân tích bảo mật mạng.
- Kết quả quét cung cấp thông tin chi tiết về tình trạng bảo mật, cấu hình hệ thống, lỗ hổng phát hiện được, điểm yếu trong quản lý xác thực và ủy quyền, cũng như các vấn đề bảo mật sâu hơn trong hệ thống.

6. **Hãy liệt kê các ưu, nhược điểm khi quét có tài khoản chứng thực và không có tài khoản chứng thực.**

Không Sử Dụng Tài Khoản Chứng Thực (Unauthenticated):

- Ưu điểm:
  - Nhanh chóng: Quét không yêu cầu thông tin đăng nhập, do đó thực hiện nhanh chóng hơn.
  - Dễ triển khai: Không cần quản lý và bảo trì thông tin đăng nhập.

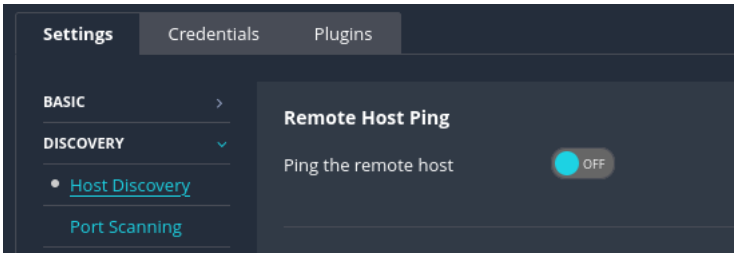
- Nhược điểm:
  - Thiếu chi tiết: Quét không thể cung cấp thông tin chi tiết như các lỗ hổng chưa được xác nhận do không có quyền truy cập đầy đủ.
  - Không hiệu quả với kiểm thử chứng thực: Không thể kiểm tra các lỗ hổng chỉ xuất hiện khi đăng nhập vào hệ thống.

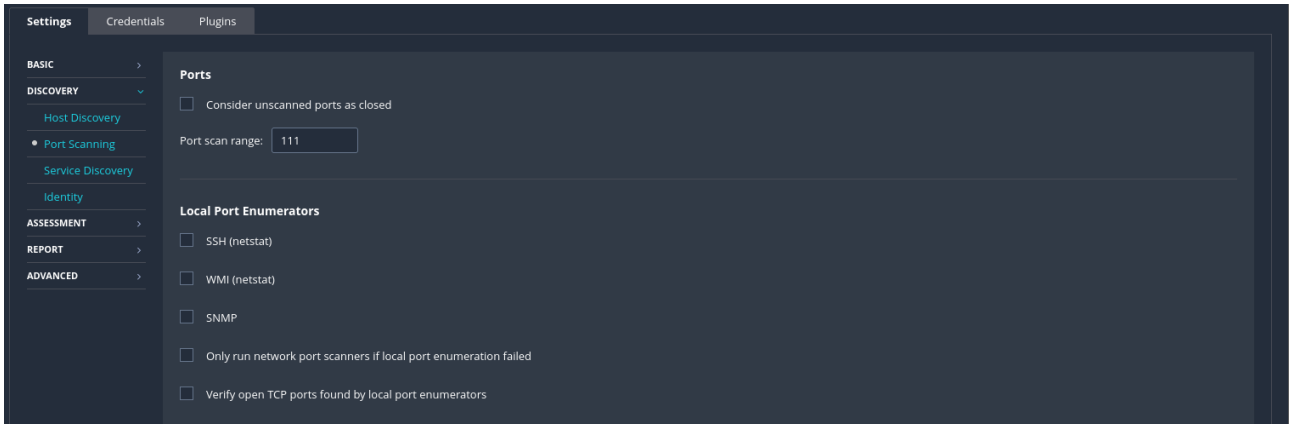
Sử Dụng Tài Khoản Chứng Thực (Authenticated):

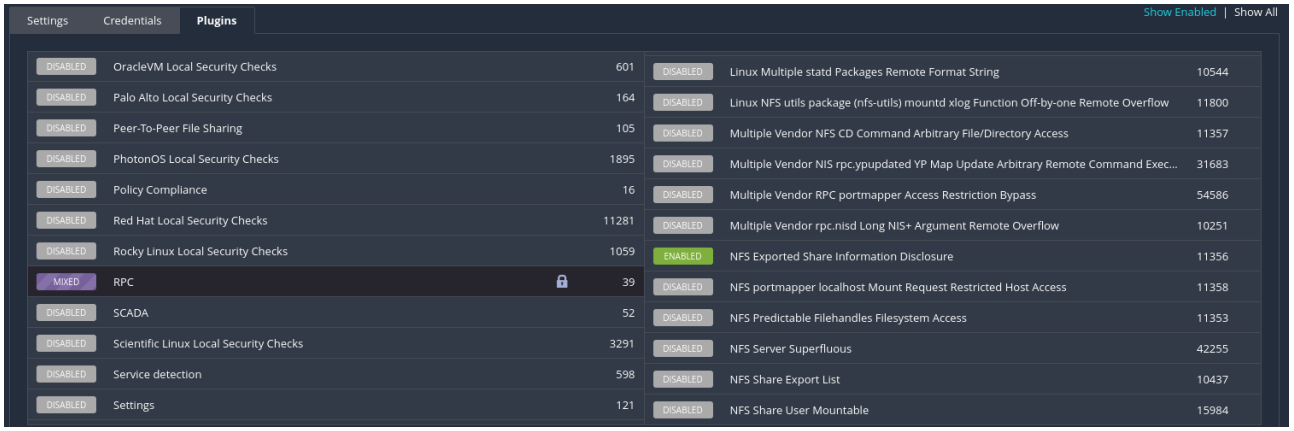
- Ưu điểm:
  - Chi tiết cao: Cung cấp thông tin chi tiết hơn về hệ thống, bao gồm các lỗ hổng có thể xuất hiện chỉ khi có quyền truy cập đầy đủ.
  - Hiệu quả với kiểm thử chứng thực: Có thể kiểm tra các lỗ hổng chỉ xuất hiện khi đăng nhập vào hệ thống.
- Nhược điểm:
  - Đòi hỏi thông tin đăng nhập: Yêu cầu thông tin đăng nhập hợp lệ để thực hiện quét.
  - Tăng độ phức tạp: Quản lý và duy trì thông tin đăng nhập có thể tăng độ phức tạp của quá trình.

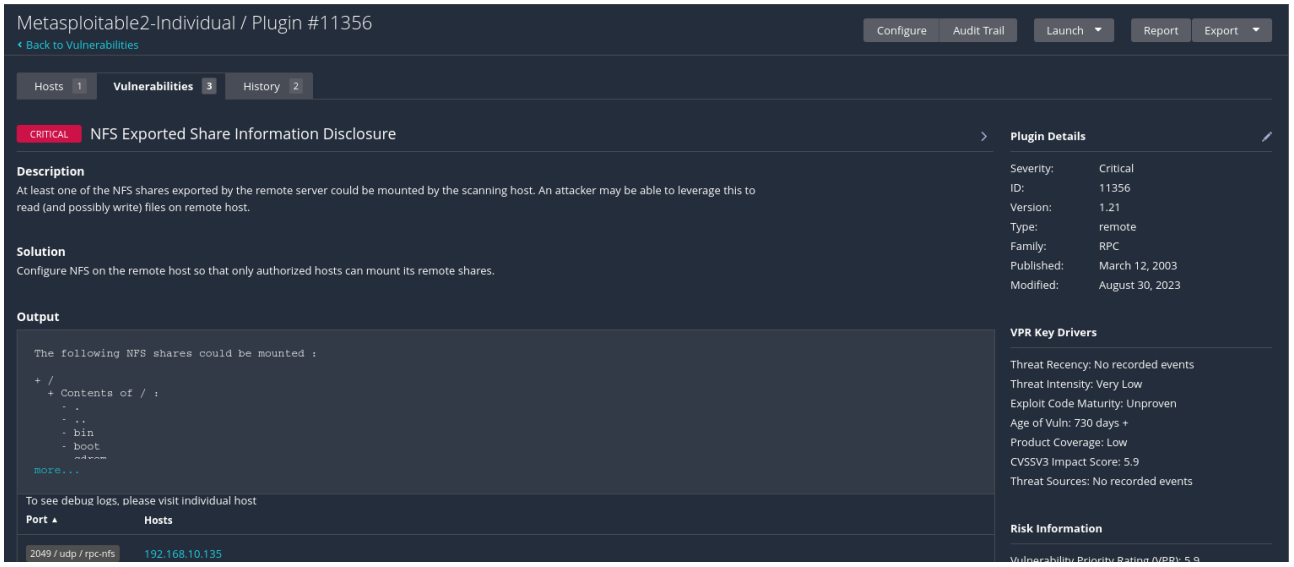
7. Thực hiện lại các bước trên để quét máy Metasploitable 2 sử dụng plugin NFS Exported Share Information Disclosure

IP victim: 192.168.10.135









8. Chạy Wireshark hoặc tcpdump trong suốt quá trình scan sử dụng 1 plugin duy nhất. Liệt kê các port khác mà Nessus thực hiện scan, mà không phải port 111? Tại sao Nessus lại scan các port khác, trong khi chúng ta đã chỉ định chỉ scan duy nhất 1 port là 111?

Các port khác: 21, 23

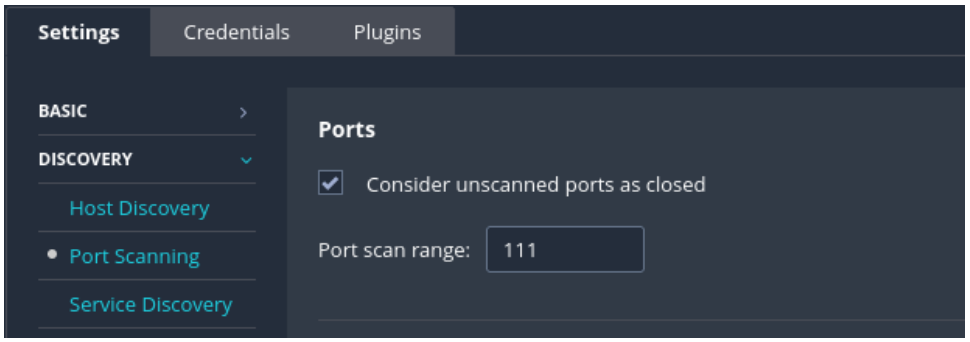
```
85 1.132037    192.168.10.140    192.168.10.135    TCP    74 49748 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
86 1.132207    192.168.10.135    192.168.10.140    TCP    74 21 → 49748 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
87 1.132271    192.168.10.140    192.168.10.135    TCP    74 40772 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
88 1.132426    192.168.10.135    192.168.10.140    TCP    74 23 → 40772 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
```

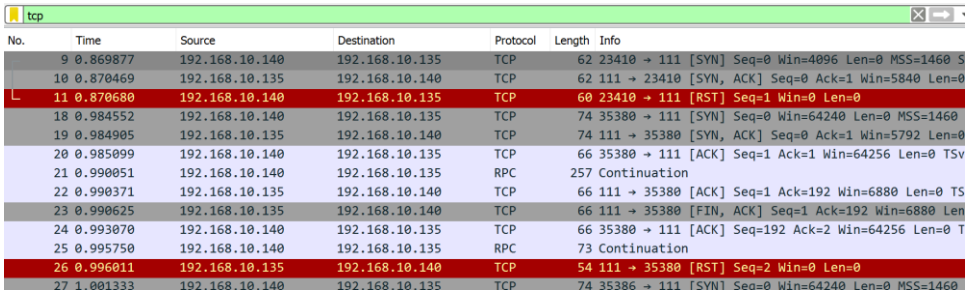
Nếu chỉ định Nessus để quét duy nhất một cổng (port) là 111 và Nessus vẫn quét các cổng khác, có một số lý do mà điều này có thể xảy ra:

- Dependency Ports: Một số plugin có thể yêu cầu quét các cổng phụ thuộc (dependency ports) để lấy thông tin chính xác hơn hoặc để kiểm tra các điều kiện tiên quyết. Trong trường hợp của NFS (Network File System), có thể có những cổng phụ thuộc khác cần được quét để đảm bảo tính toàn vẹn của dữ liệu.
- Service Detection: Nessus có thể tự động xác định các dịch vụ đang chạy trên cổng 111 và quyết định quét các cổng phụ thuộc dựa trên dữ liệu nhận được từ dịch vụ đó.

- Plugin Configuration: Một số plugin có thể được cấu hình để tự động mở rộng quét của chúng để bao gồm các cổng liên quan hoặc để lấy thông tin chi tiết hơn.

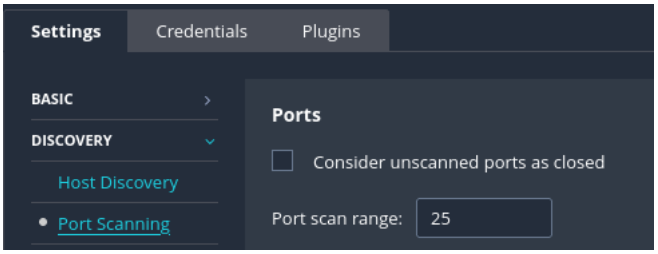
9. Mô tả cách làm để ngăn chặn việc Nessus scan port khác không phải là port được chỉ định?

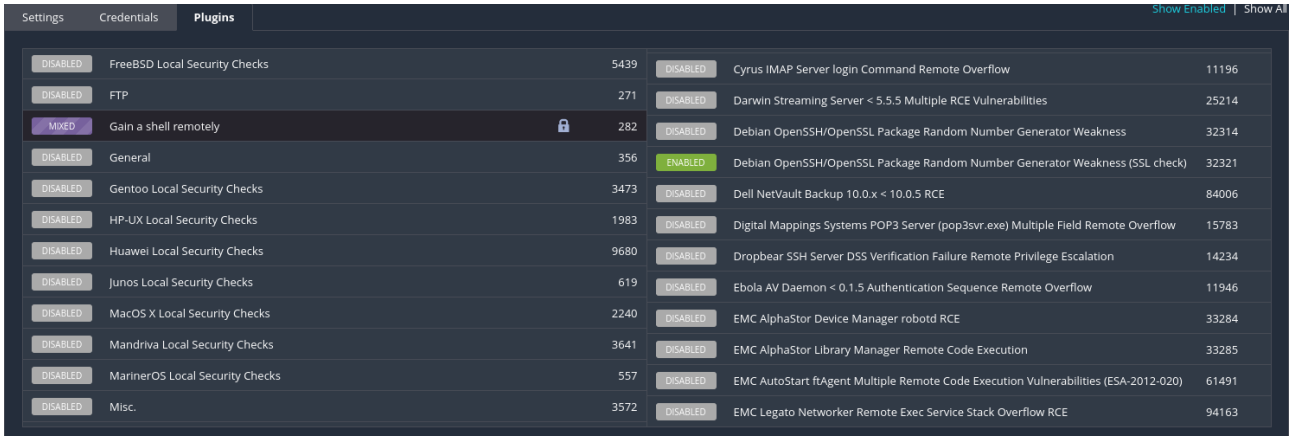


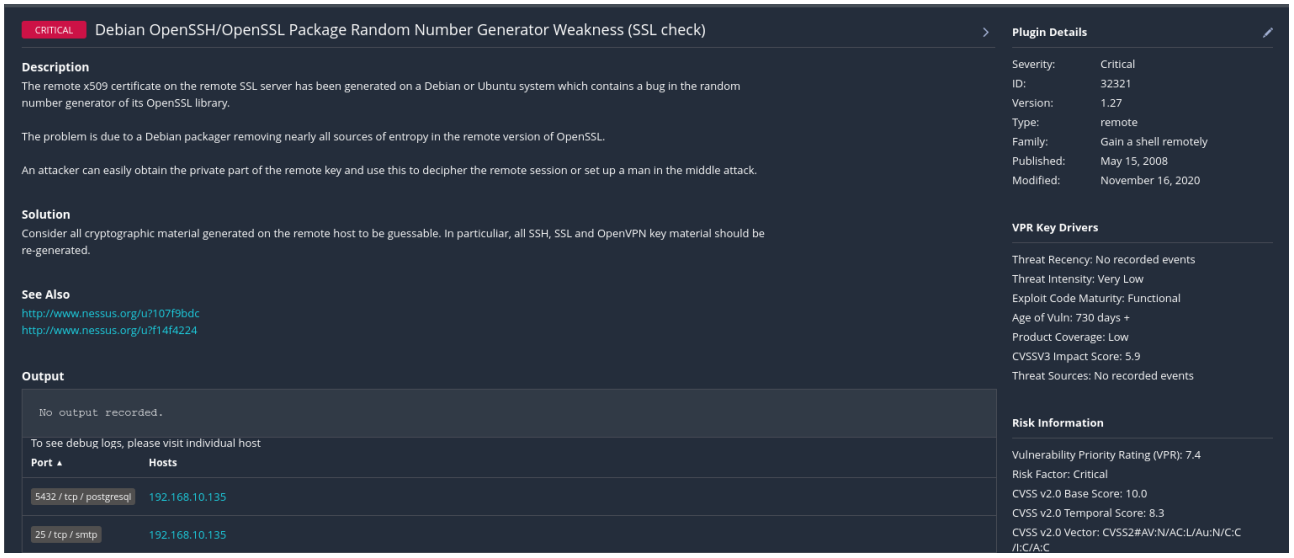


10. Thực hiện quét lại sử dụng 2 plugin khác.

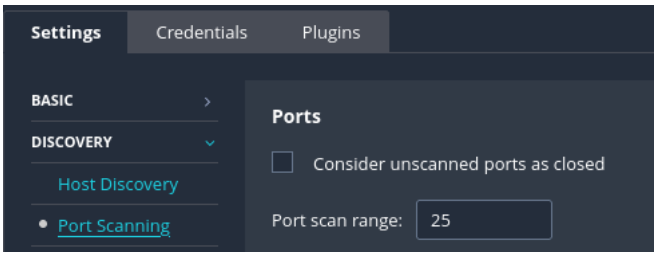
Quét lại sử dụng plugin *Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)*

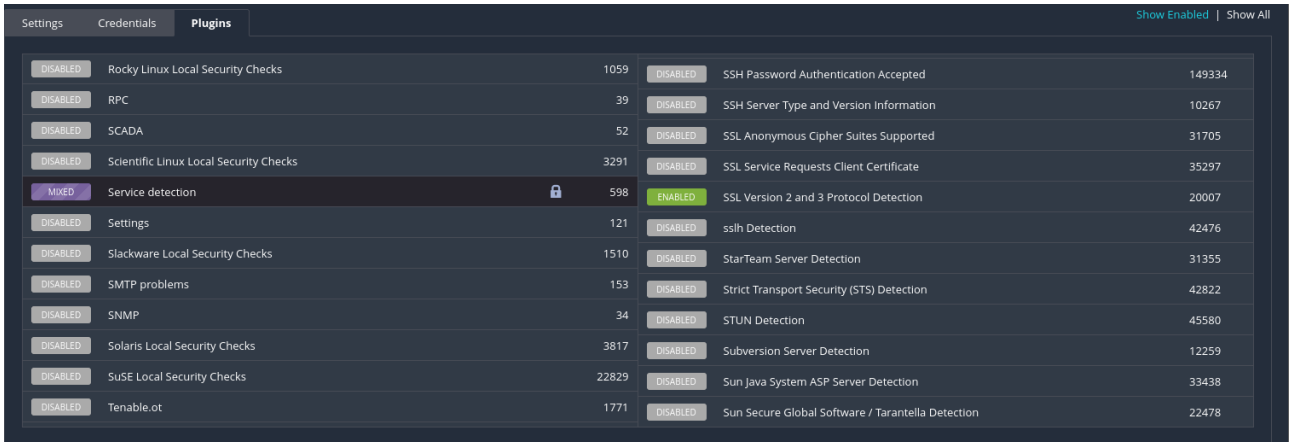


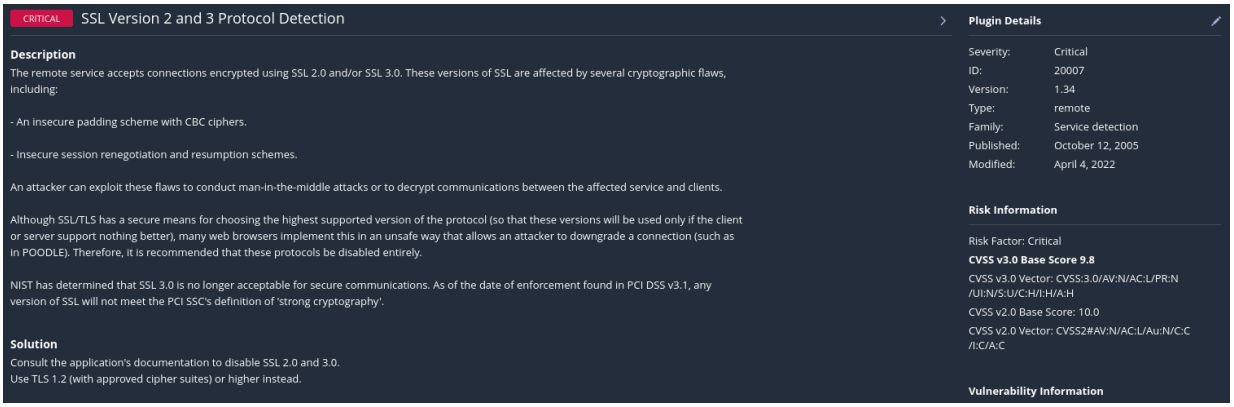




Quét lại sử dụng plugin *SSL Version 1 and 3 Protocol Detection*







11. Sinh viên/nhóm sinh viên tìm hiểu 1 trong các công cụ quét lỗ hổng tự động sau đây, và viết báo cáo kết quả theo như các phần đã chia ở bài tập 1:

Sn1per là một công cụ kiểm thử an ninh được phát triển bởi 1N3, thiết kế để quét lỗ hổng, thu thập thông tin, và kiểm tra tính bảo mật. Cung cấp nhiều chức năng như quét lỗ hổng tự động, tích hợp công cụ khác, và hỗ trợ đa nền tảng. Mã nguồn của Sn1per là mã nguồn mở và có sẵn trên GitHub. (GitHub - 1N3/Sn1per: Attack Surface Management Platform)

IP của máy Metasploitable 2: 192.168.10.135

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr
          inet addr:192.168.10.135
```

Scan máy Metasploitable với NORMAL MODE

Trước tiên thì Sn1per sẽ load Cấu Hình, rồi kiểm tra Host Active (Ping)

```
┌──(root㉿kali)-[~]
└─# sniper -t 192.168.10.135
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/ [OK]
[*] Scanning 192.168.10.135 [OK]
[*] Checking for active internet connection [OK]
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/192.168.10.135 [OK]
[*] Scanning 192.168.10.135 [OK]

 + -- --=[https://sn1persecurity.com
 + -- --=[Sn1per v9.2 by @xer0dayz

================================================================•x[2023-12-03](17:33)x•
 GATHERING DNS INFO
================================================================•x[2023-12-03](17:33)x•
================================================================•x[2023-12-03](17:33)x•
 CHECKING FOR SUBDOMAIN HIJACKING
================================================================•x[2023-12-03](17:33)x•

================================================================•x[2023-12-03](17:33)x•
 PINGING HOST
================================================================•x[2023-12-03](17:33)x•
PING 192.168.10.135 (192.168.10.135) 56(84) bytes of data.
64 bytes from 192.168.10.135: icmp_seq=1 ttl=64 time=1.53 ms

--- 192.168.10.135 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.533/1.533/1.533/0.000 ms
```

Sn1per chạy nmap để scan các TCP port

```
 RUNNING TCP PORT SCAN
================================================================•x[2023-12-03](17:33)x•
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-03 17:33 +07
Nmap scan report for 192.168.10.135 (192.168.10.135)
Host is up (0.00046s latency).
Not shown: 41 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgresql
5900/tcp open  vnc
6667/tcp open  irc
8180/tcp open  unknown
MAC Address: 00:0C:29:59:B0:62 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

Sn1per chạy các script để kiểm tra các lỗ hổng bảo mật (Vulnerability Scanning)

```
RUNNING METASPLOIT FTP VERSION SCANNER
RHOST ⇒ 192.168.10.135
RHOSTS ⇒ 192.168.10.135
[+] 192.168.10.135:21     - FTP Banner: '220 (vsFTPd 2.3.4)\x0d\x0a'
[*] 192.168.10.135:21     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
RUNNING METASPLOIT ANONYMOUS FTP SCANNER
RHOST ⇒ 192.168.10.135
RHOSTS ⇒ 192.168.10.135
[+] 192.168.10.135:21     - 192.168.10.135:21 - Anonymous READ (220 (vsFTPd 2.3.4))
[*] 192.168.10.135:21     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
RUNNING VSFTPD 2.3.4 BACKDOOR EXPLOIT
RHOST ⇒ 192.168.10.135
RHOSTS ⇒ 192.168.10.135
LHOST ⇒ 127.0.0.1
LPORT ⇒ 4444
[*] No payload configured, defaulting to cmd/unix/interact
[*] 192.168.10.135:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.10.135:21 - USER: 331 Please specify the password.
[+] 192.168.10.135:21 - Backdoor service has been spawned, handling...
[+] 192.168.10.135:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.10.131:36731 → 192.168.10.135:6200) at 2023-12-03 17:35:38 +0700
```

Sn1per tìm shell và mở nó để thực hiện remote command

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:59:b0:62
          inet addr:192.168.10.135  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe59:b062/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:174845 errors:4 dropped:14 overruns:0 frame:0
          TX packets:166770 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13671163 (13.0 MB)  TX bytes:19377143 (18.4 MB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1227 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1227 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:576333 (562.8 KB)  TX bytes:576333 (562.8 KB)
```

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

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, 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 nộp bài theo thời gian quy định trên course.

Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Đặt tên theo định dạng: **[Mã lớp]-AssignmentX_NhomY** (trong đó X là Thứ tự Assignment, Y là số thứ tự nhóm đồ án theo danh sách đã đăng ký).

  Ví dụ: [NT521.O11.ATCL]-Assignment01_Nhom03.pdf.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

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

HẾT