

BÁO CÁO BÀI TẬP

Môn học: An toàn mạng máy tính

Kỳ báo cáo: Buổi 03 (Session 03)

Tên chủ đề: Vuln Scaning

GV: Nghi Hoàng Khoa

Ngày báo cáo: 03/11/2022

Nhóm: 07 (nếu không có xóa phần này)

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.N11.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn
2	Nguyễn Bảo Phương	20520704	20520704@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	11 câu hỏi	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.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:18:b6:48
          inet addr:192.168.5.133  Bcast:192.168.5.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe18:b648/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:454 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:30359 (29.6 KB)  TX bytes:15278 (14.9 KB)
          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:275 errors:0 dropped:0 overruns:0 frame:0
          TX packets:275 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:108297 (105.7 KB)  TX bytes:108297 (105.7 KB)

msfadmin@metasploitable:~$ _
```

IP của metasploitable: 192.168.5.133

Đến vào nessus

<https://localhost:8834/>

Quét lỗ hổng không sử dụng tài khoản chứng thực

Khai báo đối tượng

The screenshot shows the 'New Scan / Basic Network Scan' configuration page in Metasploit. The left sidebar has tabs for 'Settings', 'Credentials', and 'Plugins'. Under 'Settings', there are sections for 'BASIC' (General, Schedule, Notifications), 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The 'General' section is active, showing fields for 'Name' (Metasploitable2 - Basic), 'Description', 'Folder' (My Scans), and 'Targets' (192.168.5.133). There are 'Upload Targets' and 'Add File' buttons at the bottom.

Cấu hình các định nghĩa quét

Cấu hình scanner để quét tất cả các port

The screenshot shows the 'Metasploitable2 - Basic / Configuration' page in Metasploit. The left sidebar has tabs for 'Settings', 'Credentials', and 'Plugins'. Under 'Settings', there are sections for 'BASIC', 'DISCOVERY' (Host Discovery, Port Scanning, Service Discovery, Identity), 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The 'Port Scanning' section is active, showing 'Ports' configuration with a checkbox for 'Consider unscanned ports as closed' and a 'Port scan range' of '0-65535'. Below this is the 'Local Port Enumerators' section with checkboxes for 'SSH (netstat)', 'WMI (netstat)', 'SNMP', 'Only run network port scanners if local port enumeration failed', and 'Verify open TCP ports found by local port enumerators'.

Metasploitable2 – Basic

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 70 Remediations 2 VPR Top Threats 1 History 1

Filter Search Hosts 1 Host

Host 192.168.5.133 12 7 27 5 140

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:56 AM
End: Today at 12:17 PM
Elapsed: 21 minutes

Vulnerabilities

Hosts 1 Vulnerabilities 8 Remediations 2 VPR Top Threats 1 History 1

Filter Search Vulnerabilities 8 Vulnerabilities

Sev	Score	Name	Family	Count		
CRITICAL	10.0 *	NFS Exported Share Information Disclosure	RPC	1		
CRITICAL	9.1	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS	1		
CRITICAL	...	SSL (Multiple Issues)	Gain a shell remotely	3		
HIGH	7.5 *	rlogin Service Detection	Service detection	1		
HIGH	7.5 *	rsh Service Detection	Service detection	1		
MEDIUM	5.9	ISC BIND Denial of Service	DNS	1		
MEDIUM	5.3	SMB Signing not required	Misc.	1		
MEDIUM	4.0 *	SMTP Service STARTTLS Plaintext Command Injection	SMTP problems	1		

Hosts 1 Vulnerabilities 9 Remediations 2 VPR Top Threats 1 History 1

Filter Search Vulnerabilities 9 Vulnerabilities

Sev	Score	Name	Family	Count		
CRITICAL	10.0 *	Debian OpenSSH/OpenSSL Package Random Number Generat...	Gain a shell remotely	2		
CRITICAL	10.0 *	Debian OpenSSH/OpenSSL Package Random Number Generat...	Gain a shell remotely	1		
CRITICAL	10.0 *	NFS Exported Share Information Disclosure	RPC	1		
CRITICAL	9.1	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS	1		
HIGH	7.5 *	rlogin Service Detection	Service detection	1		
HIGH	7.5 *	rsh Service Detection	Service detection	1		
MEDIUM	5.9	ISC BIND Denial of Service	DNS	1		
MEDIUM	5.3	SMB Signing not required	Misc.	1		
MEDIUM	4.0 *	SMTP Service STARTTLS Plaintext Command Injection	SMTP problems	1		

Sau khi set filter

Hosts	1	Vulnerabilities	8	Remediations	2	VPR Top Threats	1	History	1
1	Filter	Search Vulnerabilities	8 Vulnerabilities						
Sev	Score	Name	Family	Count					
CRITICAL	10.0 *	NFS Exported Share Information Disclosure	RPC	1					
CRITICAL	9.1	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS	1					
CRITICAL	...	SSL (Multiple Issues)	Gain a shell remotely	3					
HIGH	7.5 *	rlogin Service Detection	Service detection	1					
HIGH	7.5 *	rsh Service Detection	Service detection	1					
MEDIUM	5.9	ISC BIND Denial of Service	DNS	1					
MEDIUM	5.3	SMB Signing not required	Misc.	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.

Time	No.	Source	Destination	Protocol	Length	Info
8.424618024	15	192.168.5.129	192.168.5.133	TCP	74	48824 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=706597119 TSecr=0 WS=128
8.425035701	17	192.168.5.133	192.168.5.129	TCP	74	80 → 48824 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=228333 TSecr=706597119 WS=32
8.4254958141	18	192.168.5.129	192.168.5.133	TCP	66	48824 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=706597119 TSecr=228333
8.425497955	21	192.168.5.129	192.168.5.133	HTTP	84	GET / HTTP/1.0
8.425774607	23	192.168.5.133	192.168.5.129	TCP	66	80 → 48824 [ACK] Seq=1 Ack=19 Win=5792 Len=0 TSval=228333 TSecr=706597119
8.441093733	25	192.168.5.133	192.168.5.129	HTTP	1152	HTTP/1.1 200 OK (text/html)
8.441141296	26	192.168.5.129	192.168.5.133	TCP	66	48824 → 80 [ACK] Seq=19 Ack=1087 Win=64128 Len=0 TSval=706597135 TSecr=228335
8.444095409	27	192.168.5.133	192.168.5.129	TCP	66	80 → 48824 [FIN, ACK] Seq=1087 Ack=19 Win=5792 Len=0 TSval=228335 TSecr=706597135
8.444232675	28	192.168.5.129	192.168.5.133	TCP	66	48824 → 80 [RST, ACK] Seq=19 Ack=1088 Win=64128 Len=0 TSval=706597138 TSecr=228335

Có thể thấy được là quá trình bắt tay ba bước đã được diễn ra:

Địa chỉ 192.168.5.129 gửi gói tin SYN đến 192.168.5.133 để bắt đầu quá trình bắt tay 3 bước

Bên địa chỉ 192.168.5.133 gửi lại gói tin SYN ACK

Cuối cùng địa chỉ 192.168.5.129 đã gửi gói tin ACK để hoàn thành quá trình bắt tay

Ở một diễn biến khác:

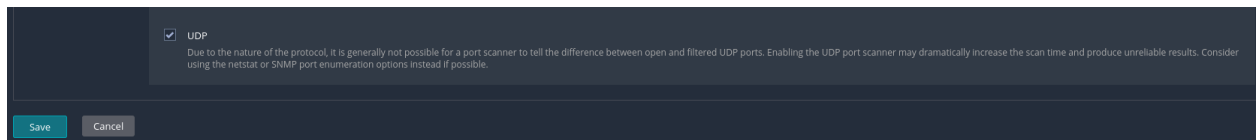
Time	No.	Source	Destination	Protocol	Length	Info
18.438596371	113513	192.168.5.129	192.168.5.133	TCP	62	55670 → 90 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
18.440200336	113547	192.168.5.133	192.168.5.129	TCP	60	90 → 55670 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Địa chỉ 192.168.5.129 gửi đến địa chỉ 192.168.5.133 gói tin SYN

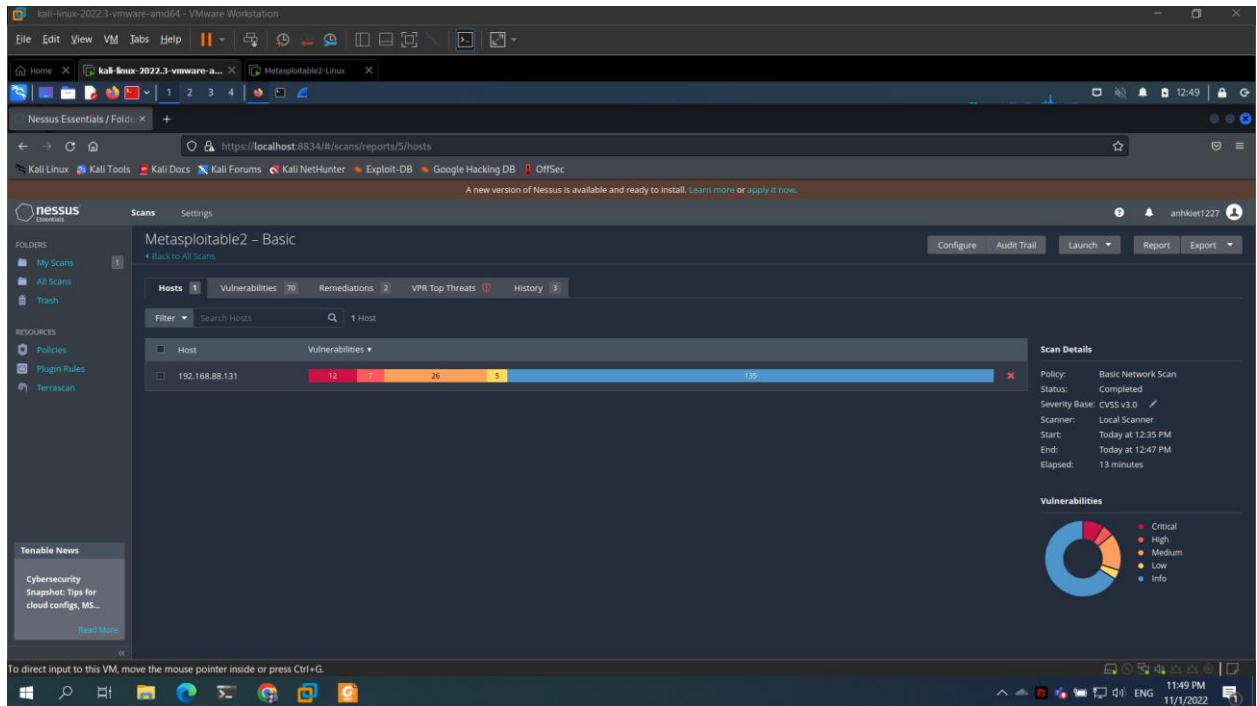
Địa chỉ 192.168.5.133 phản hồi gói tin RST ACK để yêu cầu đóng kết nối với flag RST cho thấy máy có địa chỉ 192.168.5.133 không mở port 90

3. Quét lại nhưng quét thêm port UDP

Add thêm UDP



Kết quả



Chỉ số low và chỉ số info có sự thay đổi so với câu 1: ít hơn 1 low và giảm 5 chỉ số info
=> số lỗ hổng tìm được tăng lên

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

Set up

New Scan / Credentialed Patch Audit

[Back to Scan Templates](#)

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Metasploitable2 - Auth

Description

Folder

My Scans

Targets

192.168.88.131

Upload Targets

Add File

Save

Cancel

Set up user và password

SSH

Authentication method

password

Username

msfadmin

Password (unsafe!)

●●●●●●●●

This password could be compromised if Nessus connects to a rogue SSH server. This can be mitigated by providing Nessus with a known_hosts file in the "Global Settings" section below.

Elevate privileges with

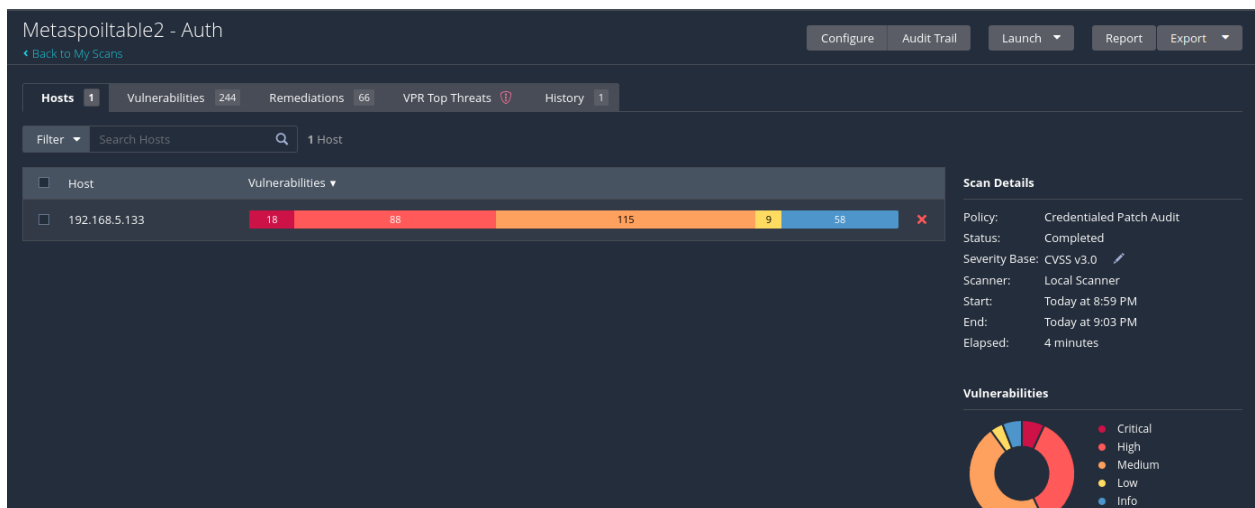
Nothing

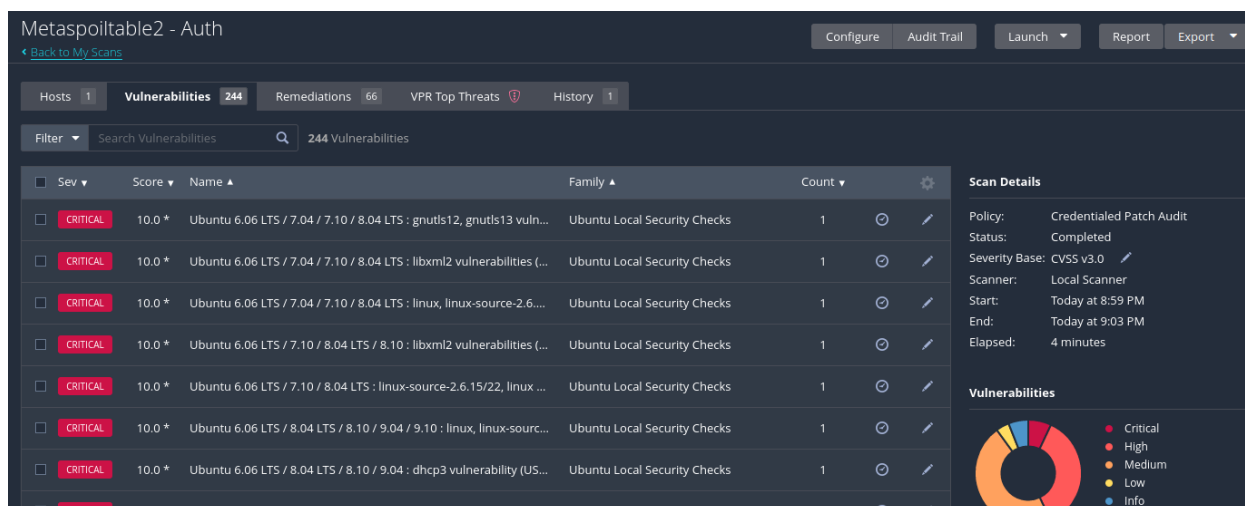
Custom password prompt

password:

Some devices are configured to prompt for a password with a non-standard string such as 'secret-passcode: '. This setting allows such prompts to be recognized. Leave this blank for most standard password prompts.

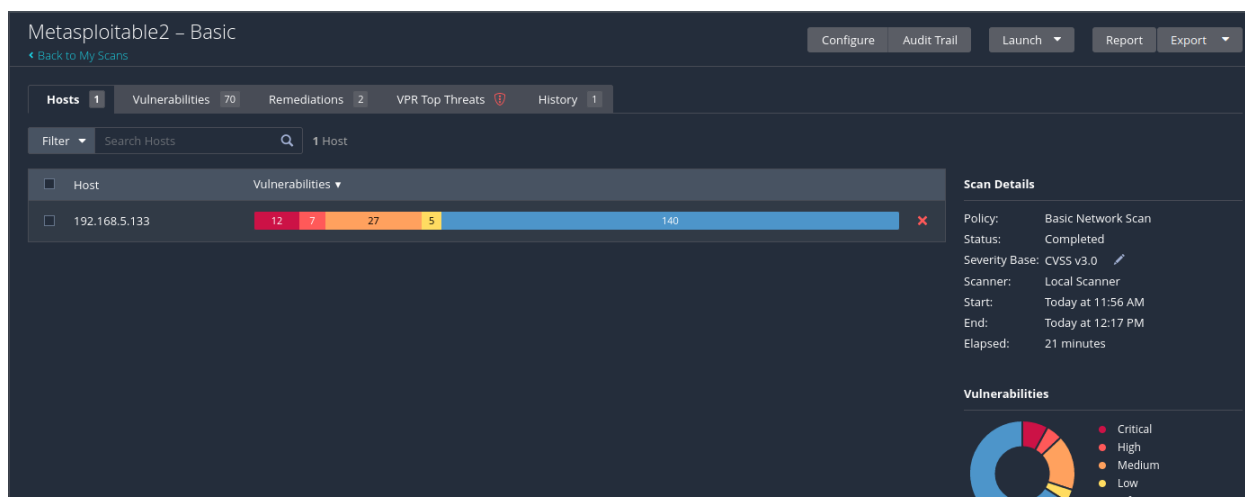
Kết quả



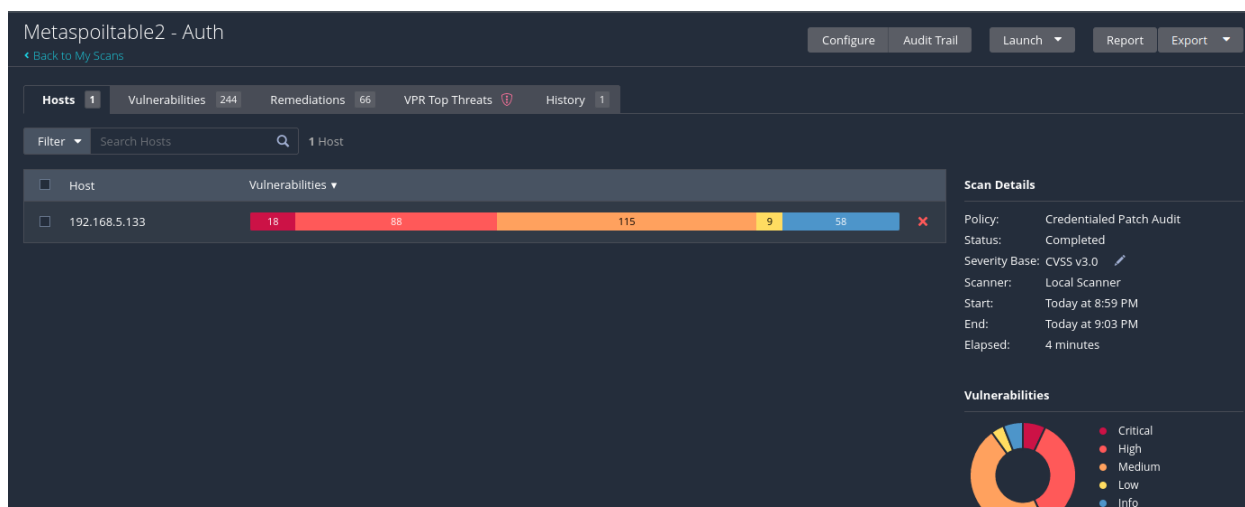


5. Kiểm tra kết quả quét và so sánh với việc quét không sử dụng tài khoản chứng thực.

Kết quả 1:



Kết quả 2



So sánh

Từ hai kết quả trên ta có thể thấy được rằng là được rằng là ở trường hợp 2 khi được cung cấp thêm user id và password thì ta có nhiều quyền truy cập hơn và từ đó có thể thực hiện quét được nhiều lỗi hơn. Có thể thấy được rằng chỉ số info thay đổi nhưng các chỉ số khác như critical, high, medium, low có sự tăng trưởng rõ rệt ở phần 2 so với phần 1. Điều này chứng tỏ được rằng việc được hỗ trợ user id và pass có thể hỗ trợ một phần nào đó tốt hơn trong việc phát hiện lỗi.

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

Không có tài khoản chứng thực:

Ưu điểm:

- + Không cần hỗ trợ userID và password
- + Có thể kiểm tra được các applications (plugin cục bộ)

Nhược điểm:

- + Không thể kiểm tra được các plugin ngoài cục bộ
- + Kiểm tra thấy được ít lỗi hơn việc không sử dụng tài khoản chứng thực

Có tài khoản chứng thực:

Ưu điểm:

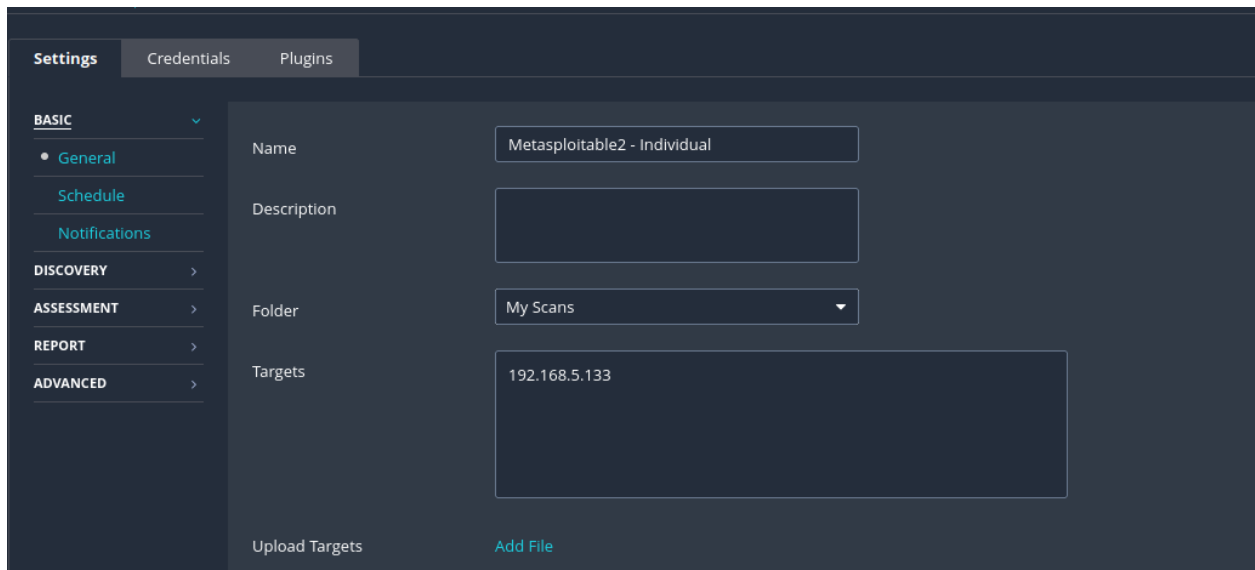
- + Có thể kiểm tra được các application ngoài cục bộ
- + Kiểm tra được nhiều lỗi hơn không có tài khoản chứng thực

Nhược điểm:

- + Cần phải có các cơ chế authenticate

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

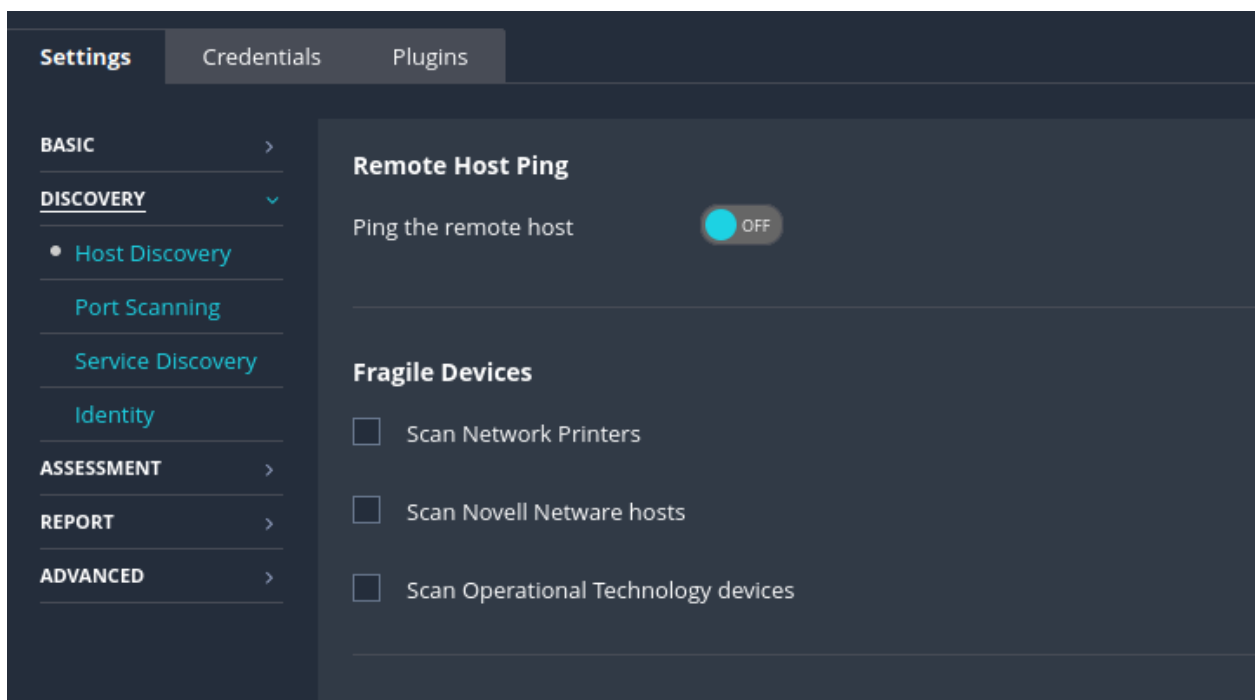
Cấu hình basic



The screenshot shows the 'Credentials' tab in the Metasploit settings interface. The left sidebar has a 'BASIC' section expanded, showing 'General', 'Schedule', and 'Notifications'. The main area contains fields for 'Name' (Metasploitable2 - Individual), 'Description', 'Folder' (My Scans), and 'Targets' (192.168.5.133). At the bottom, there are 'Upload Targets' and 'Add File' buttons.

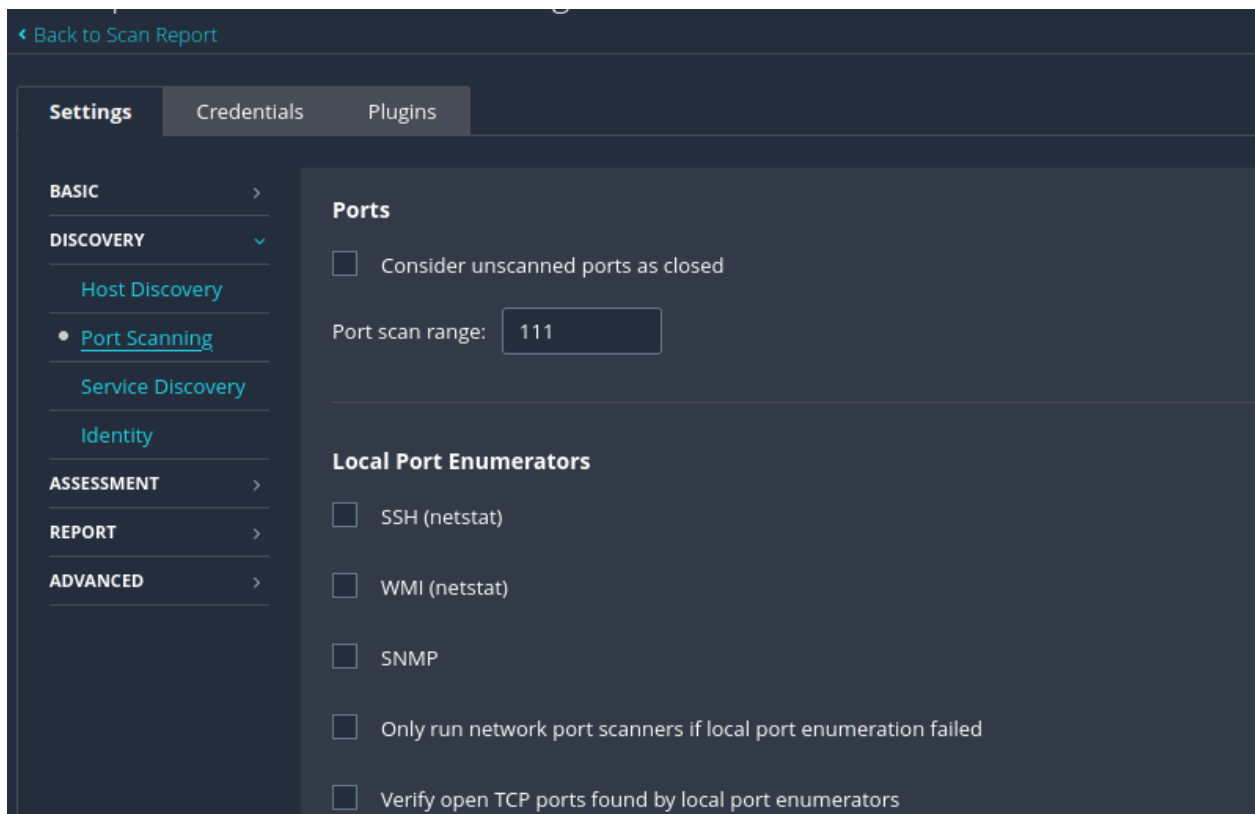
Field	Value
Name	Metasploitable2 - Individual
Description	
Folder	My Scans
Targets	192.168.5.133

Cấu hình discovery

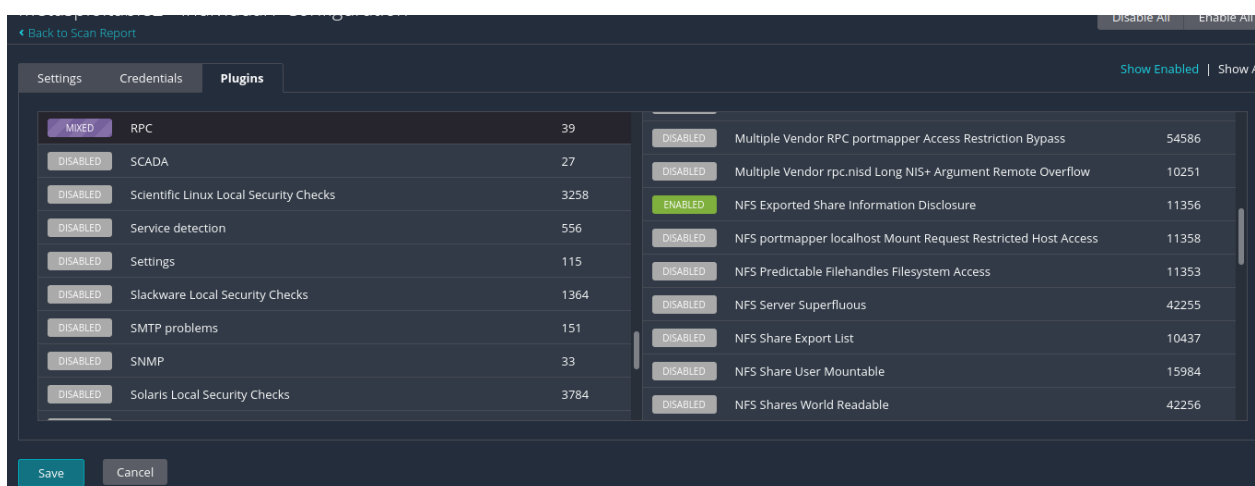
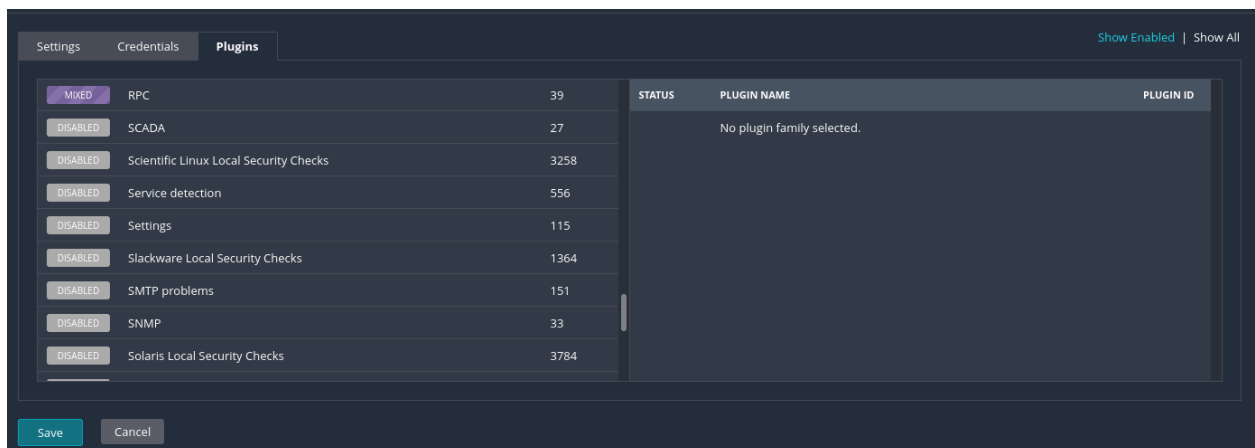


The screenshot shows the 'Discovery' tab in the Metasploit settings interface. The left sidebar has a 'DISCOVERY' section expanded, showing 'Host Discovery', 'Port Scanning', 'Service Discovery', and 'Identity'. The main area contains 'Remote Host Ping' (Ping the remote host, OFF) and 'Fragile Devices' (Scan Network Printers, Scan Novell Netware hosts, Scan Operational Technology devices).

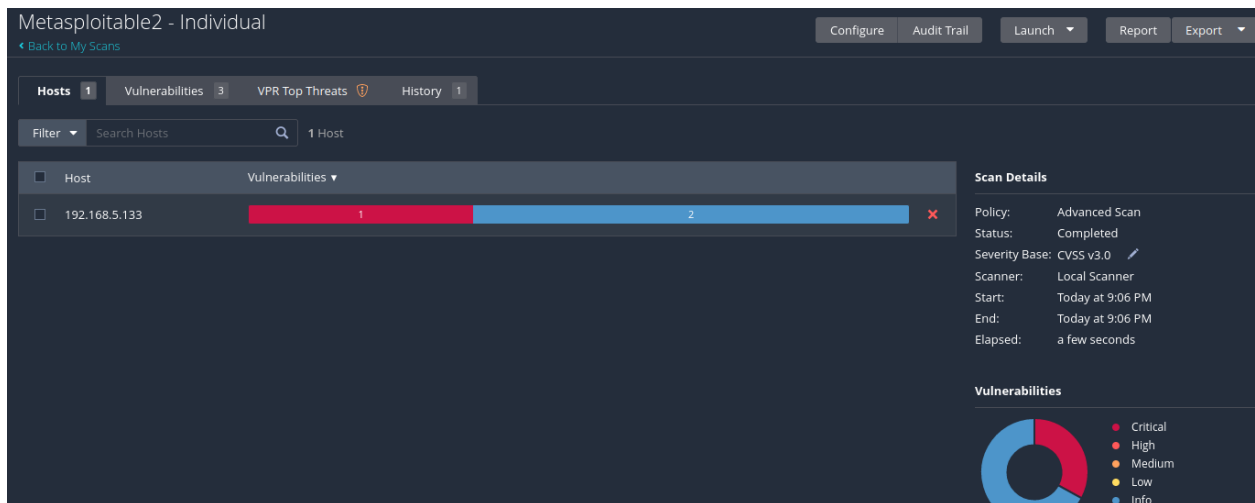
Section	Option	Value
Remote Host Ping	Ping the remote host	OFF
Fragile Devices	Scan Network Printers	<input type="checkbox"/>
	Scan Novell Netware hosts	<input type="checkbox"/>
	Scan Operational Technology devices	<input type="checkbox"/>



Cấu hình plugin



Kiểm tra kết quả chạy



CRITICAL NFS Exported Share Information Disclosure

Description
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

```
The following NFS shares could be mounted :
+ /
+ Contents of / :
- .
- ..
- bin
- boot
- cdrom
- dev
- etc
- home
- initrd
- initrd.img
- lib
- lost+found
- media
```

Plugin Details

Severity: Critical
ID: 11356
Version: 1.20
Type: remote
Family: RPC
Published: March 12, 2003
Modified: September 17, 2018

Risk Information

Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: January 1, 1985

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?

Wireshark:

192.168.88.128 là máy kali

192.168.88.131 là máy metasploitable

No.	Time	Source	Destination	Protocol	Length	Accept-Language	Info
7	1.1205671...	192.168.88.128	192.168.88.131	TCP	62		1619 → 111 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
9	1.1210908...	192.168.88.128	192.168.88.131	TCP	54		1619 → 111 [RST] Seq=1 Win=0 Len=0
12	1.1720286...	192.168.88.128	192.168.88.131	TCP	74		54790 → 81 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=335878776
14	1.1751020...	192.168.88.128	192.168.88.131	TCP	74		58044 → 8009 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787
16	1.1755334...	192.168.88.128	192.168.88.131	TCP	66		58044 → 8009 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3358787773 TSecr=13948
17	1.1847302...	192.168.88.128	192.168.88.131	TCP	376		58044 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=310 TSval=3358787782 TSecr=13948
20	1.1932166...	192.168.88.128	192.168.88.131	TCP	66		58044 → 8009 [RST, ACK] Seq=311 Ack=2 Win=64256 Len=0 TSval=3358787790 TSecr=13948
21	1.1950813...	192.168.88.128	192.168.88.131	TCP	74		48976 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=335878779
23	1.1960175...	192.168.88.128	192.168.88.131	TCP	66		48976 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3358787793 TSecr=13948
24	1.1988193...	192.168.88.128	192.168.88.131	HTTP	371	en	GET / HTTP/1.1
26	1.2018024...	192.168.88.128	192.168.88.131	SNMP	85		get-next-request 1.3.6.1.2.1.1.1.0
27	1.2024375...	192.168.88.131	192.168.88.128	ICMP	113		Destination unreachable (Port unreachable)
28	1.2040697...	192.168.88.128	192.168.88.131	TCP	74		42010 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=33587878
30	1.2046026...	192.168.88.128	192.168.88.131	TCP	66		42010 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3358787802 TSecr=13948
31	1.2074298...	192.168.88.128	192.168.88.131	SNMP	85		get-next-request 1.3.6.1.2.1.1.1.0
32	1.2078908...	192.168.88.131	192.168.88.128	ICMP	113		Destination unreachable (Port unreachable)
34	1.2117683...	192.168.88.128	192.168.88.131	TCP	66		48976 → 80 [ACK] Seq=306 Ack=1125 Win=64128 Len=0 TSval=3358787809 TSecr=13
35	1.2124073...	192.168.88.128	192.168.88.131	SMB	241		Negotiate Protocol Request
38	1.2134137...	192.168.88.128	192.168.88.131	TCP	66		42010 → 445 [ACK] Seq=176 Ack=132 Win=64128 Len=0 TSval=3358787811 TSecr=13
39	1.2188864...	192.168.88.128	192.168.88.131	TCP	66		42010 → 445 [RST, ACK] Seq=176 Ack=132 Win=64128 Len=0 TSval=3358787816 TSecr=13
40	1.2192280...	192.168.88.128	192.168.88.131	TCP	74		60904 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=33587878
41	1.2193502...	192.168.88.128	192.168.88.131	UDP	44		55032 → 9101 Len=2
41	1.2193502...	192.168.88.128	192.168.88.131	UDP	44		55032 → 9101 Len=2
43	1.2197186...	192.168.88.131	192.168.88.128	ICMP	72		Destination unreachable (Port unreachable)
44	1.2197337...	192.168.88.128	192.168.88.131	TCP	66		60904 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3358787817 TSecr=139488
45	1.2211117...	192.168.88.128	192.168.88.131	NBSS	138		Session request, to Nessus151820574<31> from <20>
46	1.2213107...	192.168.88.128	192.168.88.131	BJNP	58		Printer Command: Discover
48	1.2215414...	192.168.88.131	192.168.88.128	ICMP	86		Destination unreachable (Port unreachable)
49	1.2217046...	192.168.88.128	192.168.88.131	TCP	74		36088 → 8045 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787819 TSecr=0 WS=128
51	1.2218270...	192.168.88.128	192.168.88.131	TCP	66		60904 → 139 [ACK] Seq=73 Ack=5 Win=64256 Len=0 TSval=3358787819 TSecr=139488
53	1.2222639...	192.168.88.128	192.168.88.131	TCP	74		51350 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787820 TSecr=0 WS=128
54	1.2224197...	192.168.88.128	192.168.88.131	TCP	74		47784 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787820 TSecr=0 WS=128
55	1.2225065...	192.168.88.128	192.168.88.131	TCP	74		60816 → 2092 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787820 TSecr=0 WS=128
57	1.2227118...	192.168.88.128	192.168.88.131	TCP	66		51350 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3358787820 TSecr=139489
58	1.2228861...	192.168.88.128	192.168.88.131	TCP	74		58044 → 9000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787820 TSecr=0 WS=128
61	1.2230733...	192.168.88.128	192.168.88.131	TCP	66		47784 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3358787820 TSecr=139489
63	1.2232447...	192.168.88.128	192.168.88.131	TCP	74		46756 → 9200 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787821 TSecr=0 WS=128
64	1.2234049...	192.168.88.128	192.168.88.131	TCP	74		56290 → 10000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787821 TSecr=0 WS=128
67	1.2237751...	192.168.88.128	192.168.88.131	TCP	74		44584 → 79 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787821 TSecr=0 WS=128
68	1.2239227...	192.168.88.128	192.168.88.131	TCP	74		48980 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787821 TSecr=0 WS=128
69	1.2240642...	192.168.88.128	192.168.88.131	TCP	74		40766 → 280 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787821 TSecr=0 WS=128
72	1.2243951...	192.168.88.128	192.168.88.131	TCP	66		48980 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3358787822 TSecr=139489
74	1.2245642...	192.168.88.128	192.168.88.131	TCP	74		36488 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787822 TSecr=0 WS=128
75	1.2246718...	192.168.88.128	192.168.88.131	TCP	74		54510 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787822 TSecr=0 WS=128
76	1.2247775...	192.168.88.128	192.168.88.131	TCP	74		42434 → 7627 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787822 TSecr=0 WS=128
79	1.2249191...	192.168.88.128	192.168.88.131	TCP	74		59462 → 9100 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787822 TSecr=0 WS=128
82	1.2256223...	192.168.88.128	192.168.88.131	TCP	66		60904 → 139 [RST, ACK] Seq=73 Ack=5 Win=64256 Len=0 TSval=3358787823 TSecr=139488
84	1.2273436...	192.168.88.128	192.168.88.131	TCP	66		51350 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=3358787825 TSecr=139489
85	1.2278715...	192.168.88.128	192.168.88.131	TCP	74		58826 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787825 TSecr=0 WS=128
88	1.2303156...	192.168.88.128	192.168.88.131	TCP	74		42010 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3358787827 TSecr=0 WS=128

Các port mà Nessus quét ngoài port 111:

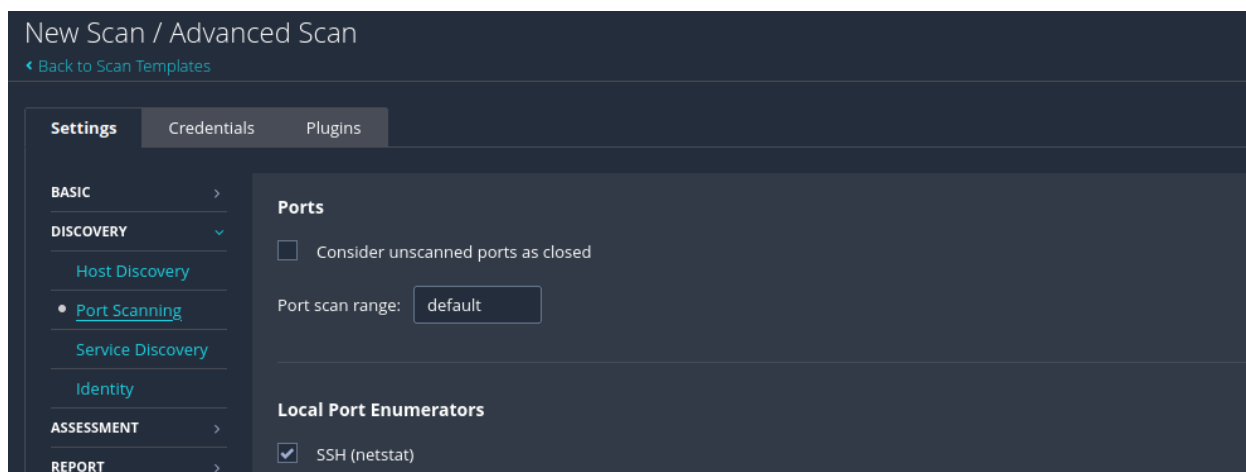
81, 8009, 80, 445, 1901, 139, 21, 23,...

Có nhiều plugins kiểm tra trạng thái của các cổng hardcoded mặc định, các port ngoài chỉ định chưa được quét sẽ có trạng thái chưa biết nên `get_port_state()` sẽ trả về `True` (mặc định). Điều này dẫn đến các port này sẽ bị kết nối thử.

(<https://community.tenable.com/s/article/Why-Is-Nessus-Scanning-Ports-Outside-Of-The-Port-Range>)

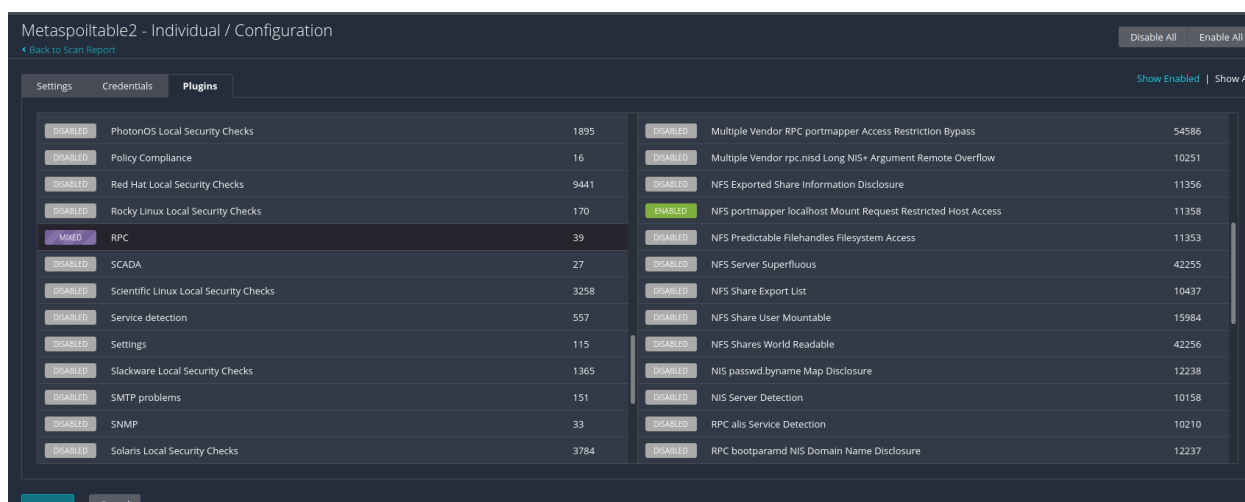
9. Mô tả cách làm để ngăn chặn việc Nessus scan port khác không phải là port được chỉ định?

Để ngăn chặn việc Nessus scan các port khác ngoài những port được chỉ định, ta đánh tick vào lựa chọn “Consider unscanned ports as closed”, khi làm vậy, đối với những port có trạng thái unknown, `get_port_state()` sẽ trả về `FALSE`

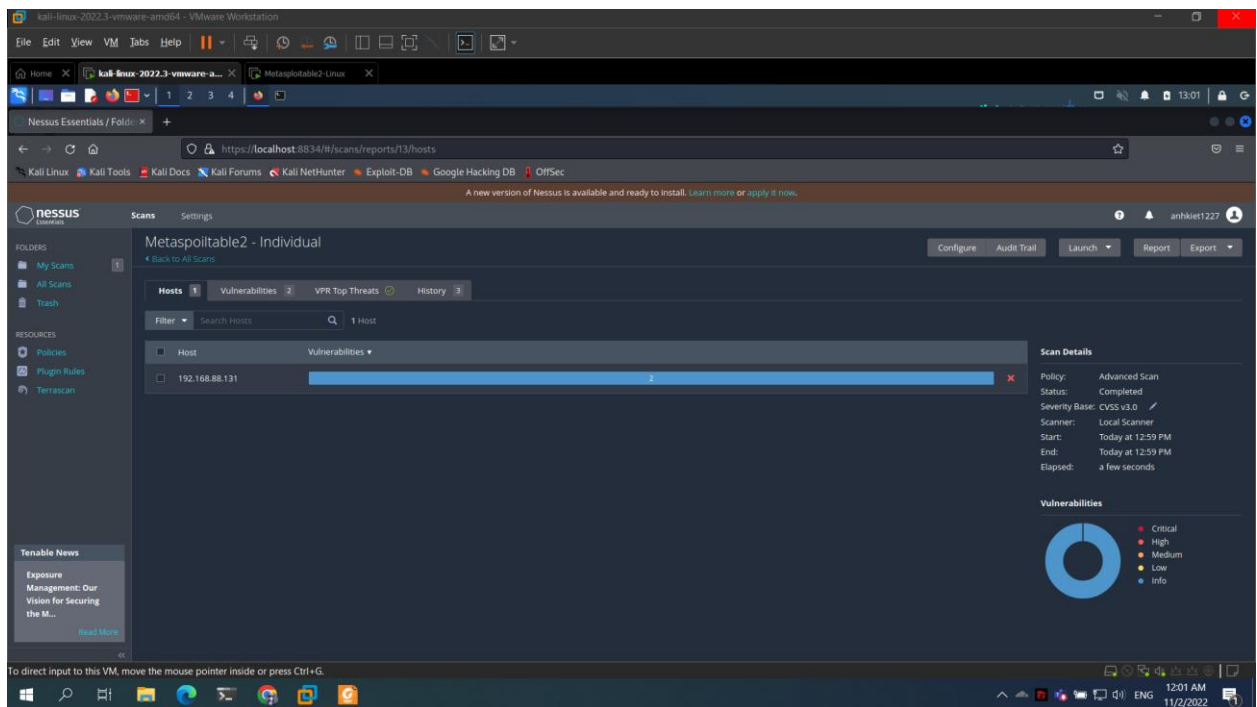


10. Thực hiện quét lại sử dụng 2 plugin khác.

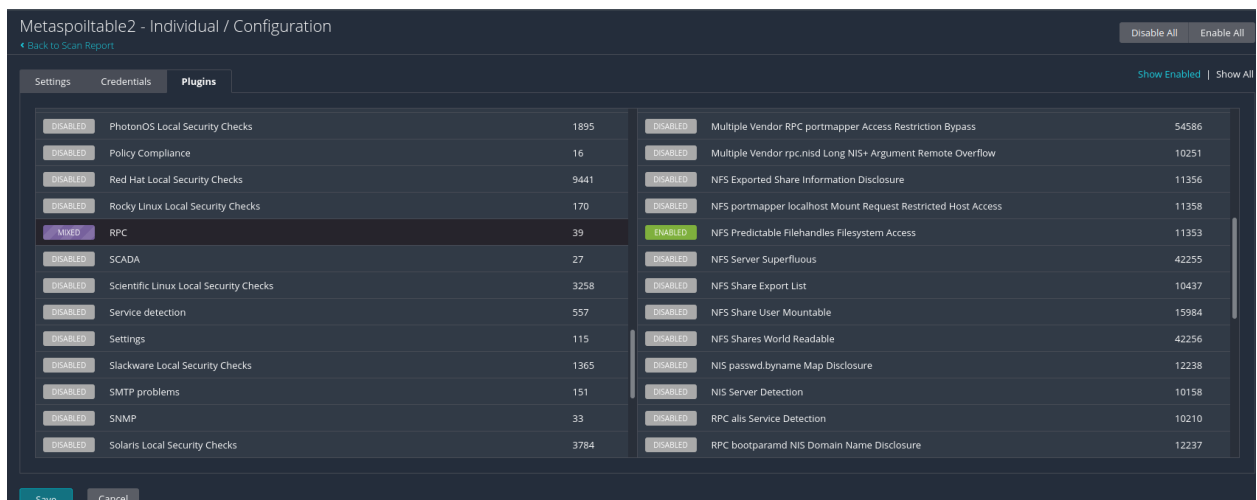
New plugin 1:



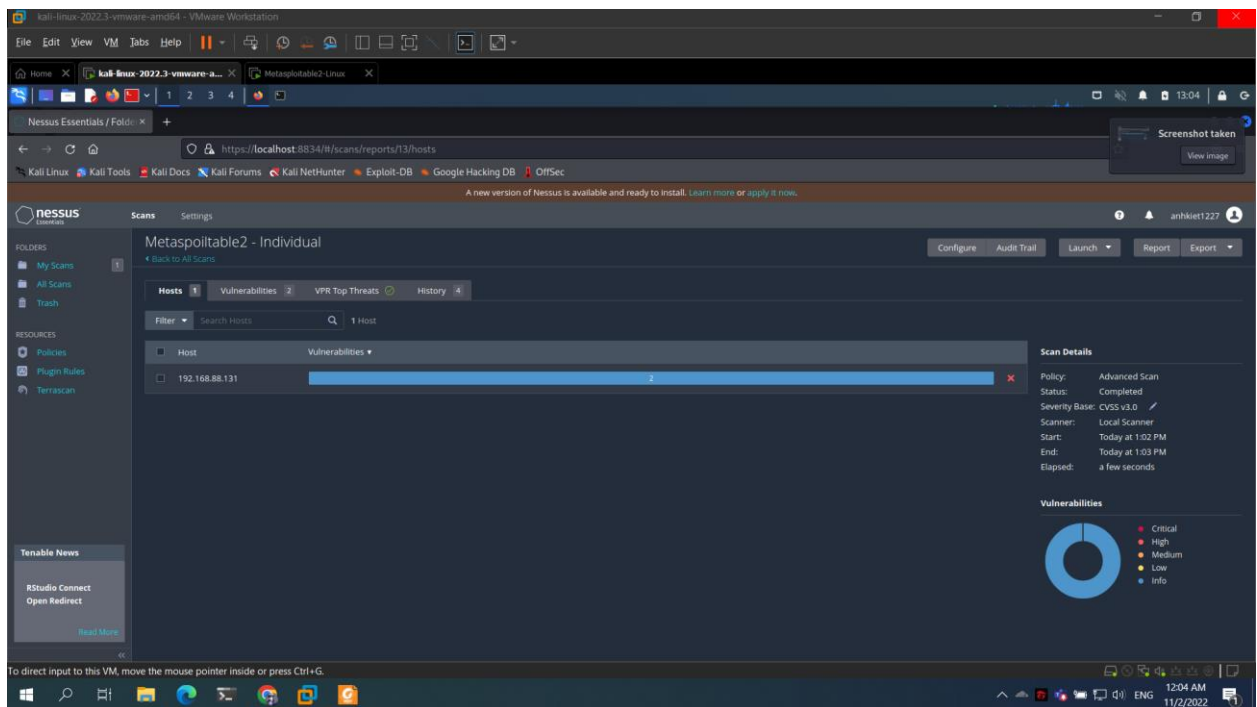
Kết quả:



New plugin 2:



Kết quả:



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:

Cài đặt

Ở đây ta sẽ clone chương trình từ github về sau đó vào file đã clone và chạy lệnh `./install.sh` và chờ cho file cài xong

```

root@kali: ~/Sn1per

File Actions Edit View Help

(root@kali)-[~]
# git clone https://github.com/1N3/Sn1per
Cloning into 'Sn1per'...
remote: Enumerating objects: 3036, done.
remote: Counting objects: 100% (211/211), done.
remote: Compressing objects: 100% (94/94), done.
remote: Total 3036 (delta 132), reused 172 (delta 116), pack-reused 2825
Receiving objects: 100% (3036/3036), 44.05 MiB | 6.35 MiB/s, done.
Resolving deltas: 100% (2077/2077), done.

(root@kali)-[~]
# ls
go  nuclei-templates  Sn1per  sniper  workspace

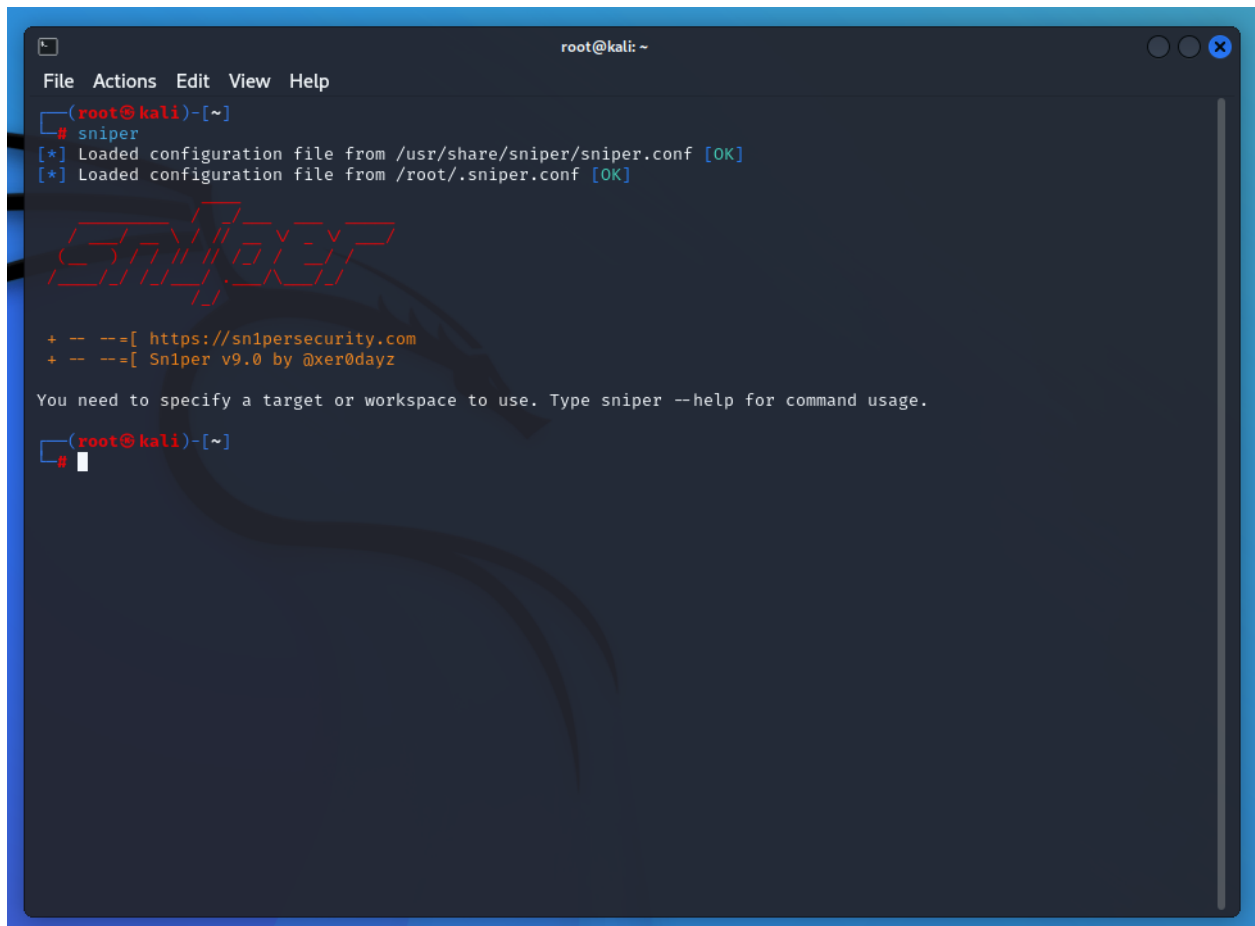
(root@kali)-[~]
# cd Sn1per

(root@kali)-[~/Sn1per]
# ls
bin          conf          install.sh    loot          pro          sn1per.desktop  sniper        templates      wordlists
CHANGELOG.md Dockerfile    LICENSE.md    modes         README.md     sn1per.png      sniper.conf   uninstall.sh

(root@kali)-[~/Sn1per]
# ./install.sh

```

Check sau khi cài đặt:



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)~[~]  
# sniper  
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]  
[*] Loaded configuration file from /root/.sniper.conf [OK]  
  
  sniper  
+ -- ==[ https://snlpersecurity.com  
+ -- ==[ Snlper v9.0 by @xer0dayz  
  
You need to specify a target or workspace to use. Type sniper --help for command usage.  
(root@kali)~[~]  
#
```

Đã cài đặt thành công

Chạy thử với ip được cung cấp





BỘ MÔN
AN TOÀN THÔNG TIN

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, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT