

BÁO CÁO BÀI TẬP

Môn học: An toàn mạng máy tính

Kỳ báo cáo: Buổi 03 (Session 01)

Tên chủ đề: Quét lỗ hổng bảo mật

GV: Nghi Hoàng Khoa

Ngày báo cáo: 30/11/2022

Nhóm: 12

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.N12.ATCL

STT	Họ và tên	MSSV	Email
1	Bùi Thị Trúc Nhận	20521692	20521692@gm.uit.edu.vn
2	Nguyễn Lê Trọng Nhân	20521699	20521699@gm.uit.edu.vn
3	Võ Lê Vũ	20522170	20522170@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

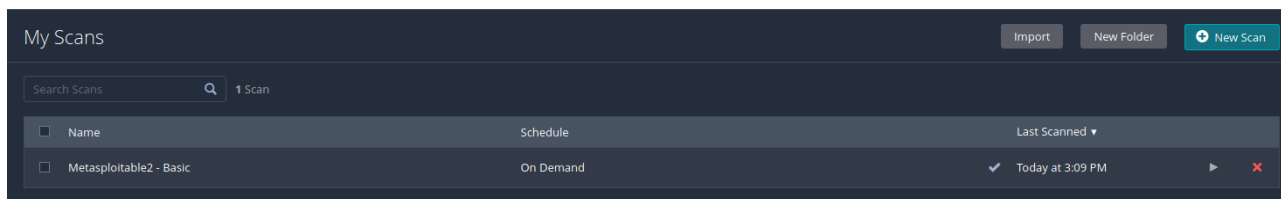
STT	Công việc	Kết quả tự đánh giá
1	Kịch bản 01/Câu hỏi 01	100%
2	Kịch bản 02	100%
3	Kịch bản 03	100%
4	Kịch bản 04	90%
5	Kịch bản 05	60%

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

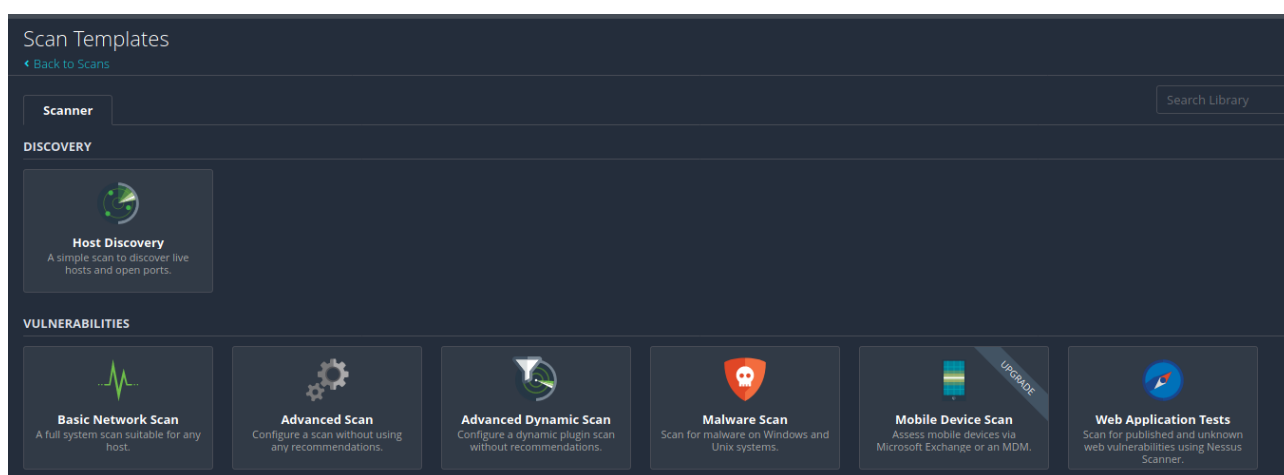
¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

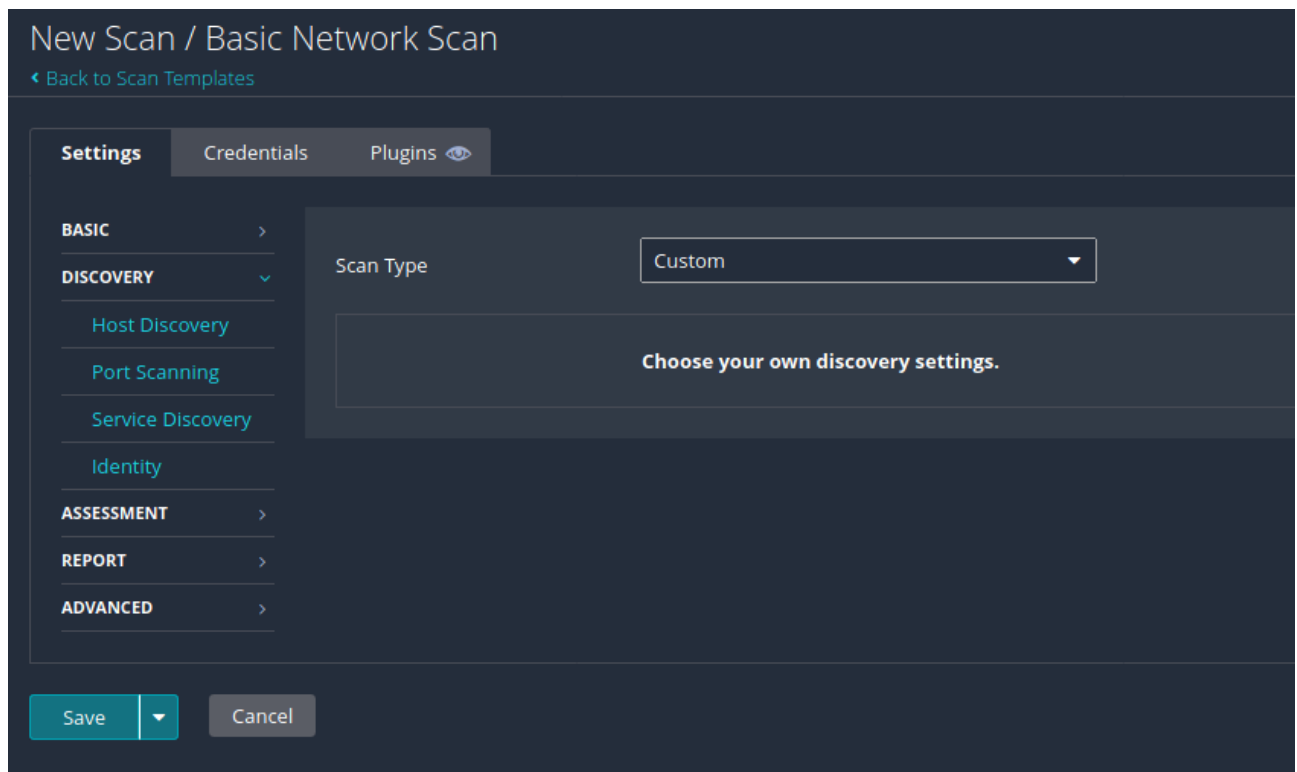
Câu 1: Thực hiện lại các bước trên để quét máy Metasploitable 2 không sử dụng tài khoản chứng thực.



Chọn *New Scan*



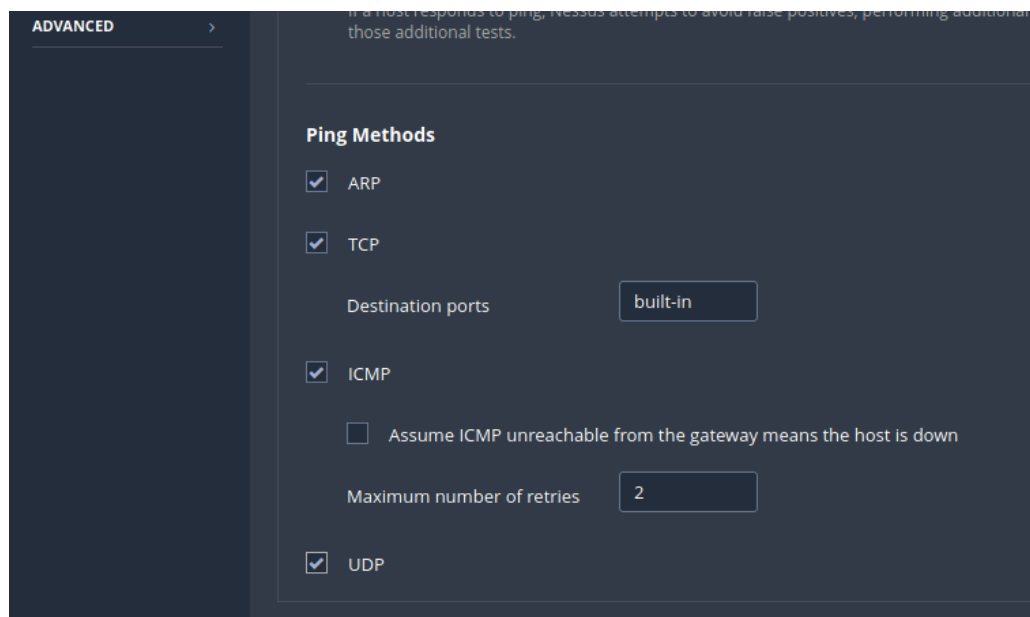
Chọn *Basic Network Scan*



Chọn *Discovery* và chỉnh *Scan type* thành *Custom*

Host Discovery

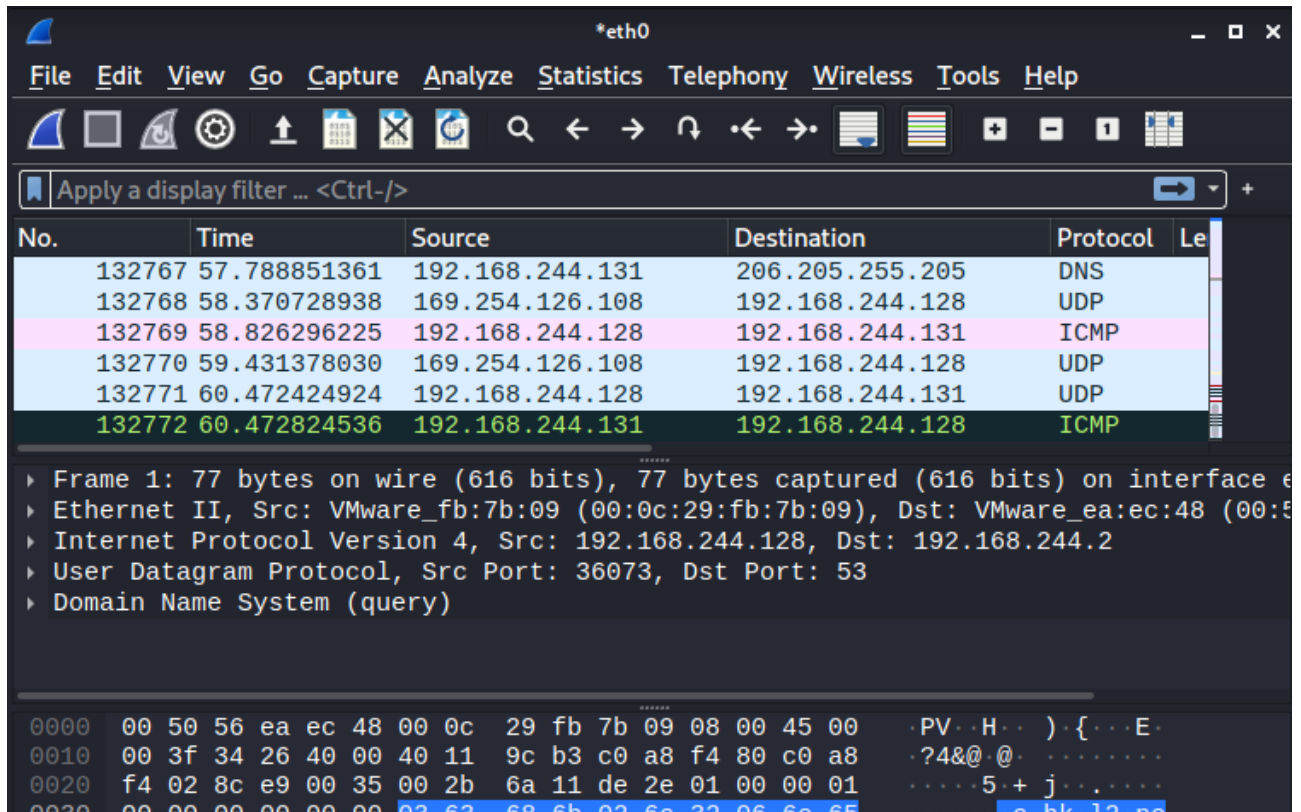
Chọn *Host Discovery* bên trái



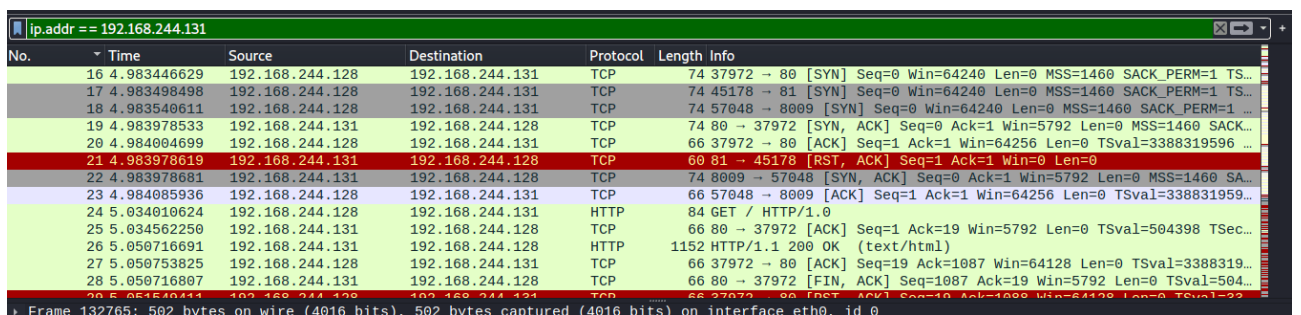
Kéo xuống và click vào checkbox UDP

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

- Bật wireshark và thực hiện bắt gói tin, sau đó cho Nessus bắt đầu quét



- Lọc gói tin theo ip máy metasploit 192.168.244.131



- Đầu tiên, Nessus sẽ tạo kết nối đến từng cổng ở máy mục tiêu, ví dụ đối với TCP thì Nessus sẽ tạo kết nối TCP bằng cách thực hiện bắt tay 3 bước (có thể thấy các gói tin SYN, ACK)

- Sau khi đã kết nối được, Nessus sẽ xác định dịch vụ chạy trên cổng đang quét và tiến hành gửi các gói tin đến cổng để thực hiện kiểm tra (DNS, UDP, TCP,...)

ip.addr == 192.168.244.131						
No.	Time	Source	Destination	Protocol	Length	Info
132753	56.713544660	192.168.244.128	192.168.244.131	DNS	71	Sta
132754	56.714082929	192.168.244.131	192.168.244.128	DNS	135	Sta
132755	56.837582874	192.168.244.128	192.168.244.131	ICMP	66	Tin
132756	56.838008467	192.168.244.131	192.168.244.128	ICMP	60	Tin
132757	56.876874153	192.168.244.128	192.168.244.131	ICP	89	Opc
132758	56.877591371	192.168.244.131	192.168.244.128	ICMP	117	Des
132759	56.880387866	192.168.244.128	192.168.244.131	UDP	82	411
132760	56.880752663	192.168.244.131	192.168.244.128	ICMP	110	Des
132761	56.882745079	192.168.244.128	192.168.244.131	UDP	48	499
132762	56.883117913	192.168.244.131	192.168.244.128	ICMP	76	Des
132763	56.994440460	192.168.244.128	192.168.244.131	ISAKMP	1458	Ide
132764	56.994796197	192.168.244.131	192.168.244.128	ICMP	590	Des
132765	57.174280737	192.168.244.128	192.168.244.131	ISAKMP	502	IKE
132767	57.788851261	192.168.244.131	206.205.255.205	DNS	82	Sta

Câu 3. Quét lại nhưng quét thêm UDP

- Tạo Scan mới, điền tên và IP máy cần quét

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Metasploitable - Cau3

Description

Cau 3

Folder

My Scans

Targets

192.168.244.131

- Ở phần Discovery, Scan Type chọn Custom

BASIC >

DISCOVERY ▾

- Host Discovery
- Port Scanning
- Service Discovery

ASSESSMENT >

Scan Type: Custom

Choose your own discovery settings.

- Nhập 0-65535 vào Port range để scan toàn bộ port

Ports

☐ Consider unscanned ports as closed

Port scan range: 0-65535

- Chọn mục UDP để quét kết nối UDP. Cuối cùng chọn Save

☐ Disable detection

☒ UDP

Due to the nature of the protocol, it is generally not possible for a port scanner to detect UDP connections. The port scanner may dramatically increase the scan time and may not be able to scan all ports.

Save Cancel

- Tiến hành quét

<input type="checkbox"/>	Name	Schedule	Last Modified ▾		
<input type="checkbox"/>	Metasploitable - Cau3	On Demand	Today at 10:38 PM		■
<input type="checkbox"/>	Metasploitable2 - Basic	On Demand	October 20 at 5:58 AM	▶	×

- Kết quả

Metasploitable - Cau3 Configure Audit Trail

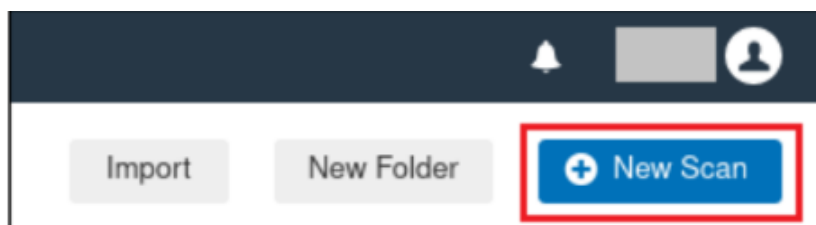
[← Back to My Scans](#)

Hosts 1 Vulnerabilities 72 Remediations 3 VPR Top Threats History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.244.131	8 7 30 6 140

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



Bắt đầu thì chọn nút New Scan

Scan Templates [← Back to Scans](#)

Scanner

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.

WannaCry Ransomware
Remote and local checks for MS17-010.

Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Chúng ta sử dụng template “*Credentialed Patch Audit*”

New Scan / Credentialed Patch Audit

[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: ques 4,5,6

Description:

Folder: My Scans

Targets: 192.168.1.134

Upload Targets Add File

Save Cancel

Điền thông tin của Target


Chọn thẻ “Credential” và “SSH” . Tại “Authentication method” chọn “password” , thiết lập “Username” và “password” là “msfadmin”

Save và Launch để quét

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

- Scan không chứng thực

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0 
Scanner:	Local Scanner
Start:	Today at 10:38 PM
End:	Today at 10:50 PM
Elapsed:	12 minutes

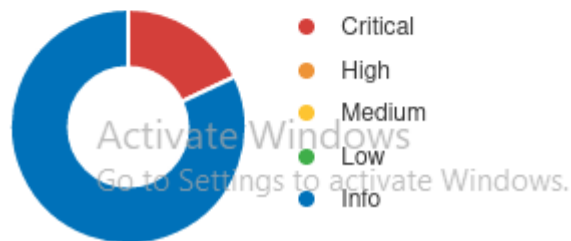
Vulnerabilities

- Scan chứng thực

Host Details

IP: 192.168.18.130
 OS: Linux Kernel 2.6.24-16-server on Ubuntu 8.04
 Start: Today at 2:18 AM
 End: Today at 2:23 AM
 Elapsed: 6 minutes
 KB: [Download](#)

Vulnerabilities



→ Scan chứng
nhiều lỗ hổng
critical hơn, vì có quyền truy cập sâu hơn vào hệ thống.

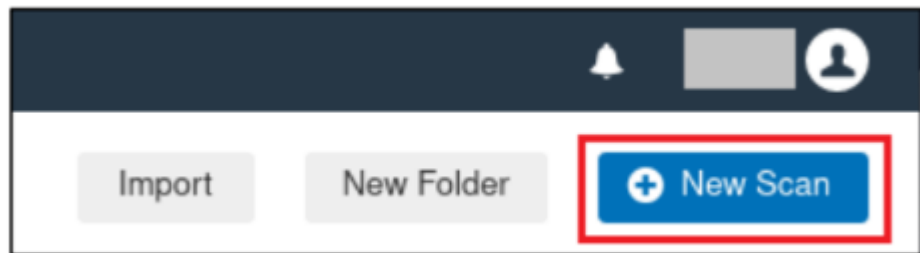
thực phát hiện được
nghiêm trọng mức

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

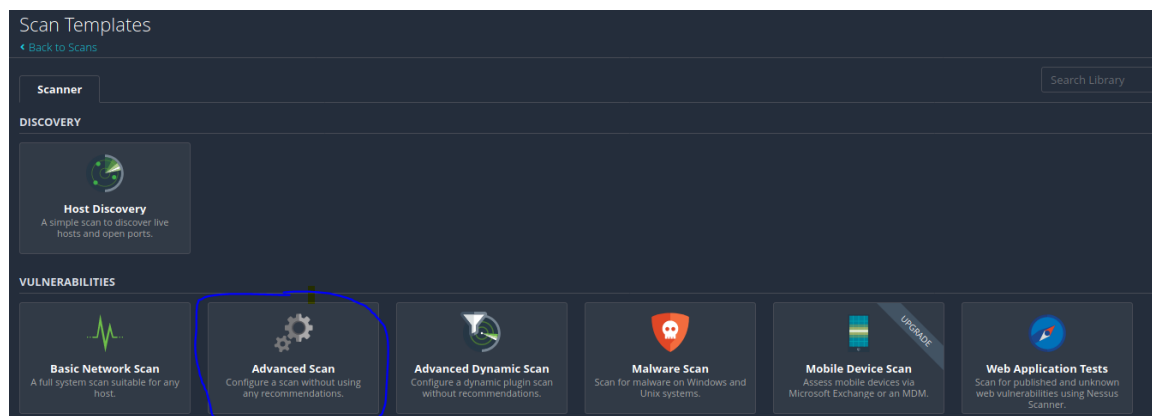
Scan không chứng thực (non-credentialed)	Scan có chứng thực (Credentialed)
Phương pháp scan thông thường, không có quyền truy cập vào hệ thống.	Phương pháp scan yêu cầu cung cấp credential để truy cập sâu hơn vào các file và ứng dụng hệ thống.
Ưu điểm: <ul style="list-style-type: none"> Thích hợp cho các lần scan có quy mô lớn Có thể thực hiện những quy trình cụ thể (brutefore credential) để tìm ra lỗ hổng 	Ưu điểm: <ul style="list-style-type: none"> Ít tiêu hao tài nguyên hơn so với scan không chứng thực, vì scan chứng thực sẽ thực hiện đăng nhập vào target (với tài khoản chứng thực đã cung cấp) và thực hiện scan ngay trên target (thay vì scan qua network) Cho ra kết quả chuẩn xác nhất và chuyên sâu hơn Phát hiện được lỗ hổng ở client-side
Nhược điểm: <ul style="list-style-type: none"> Có thể ảnh hưởng đến network 	Nhược điểm:

- | | |
|---|---|
| <ul style="list-style-type: none">Có thể bỏ sót những thiết bị không kết nối vào network tại thời điểm scan | <ul style="list-style-type: none">Có thể gây khó khăn trong việc kiểm soát và quản lý credentialKhó để thực hiện một lần scan chứng thực an toàn đối với những tổ chức lớn |
|---|---|

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



Chúng ta sẽ bắt đầu bằng



Chọn Advanced Scan để có thể cấu hình theo đề

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: ques 7,8,9,10

Description:

Folder: My Scans

Targets: 192.168.1.134

Điền thông tin đối tượng cần Scan

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

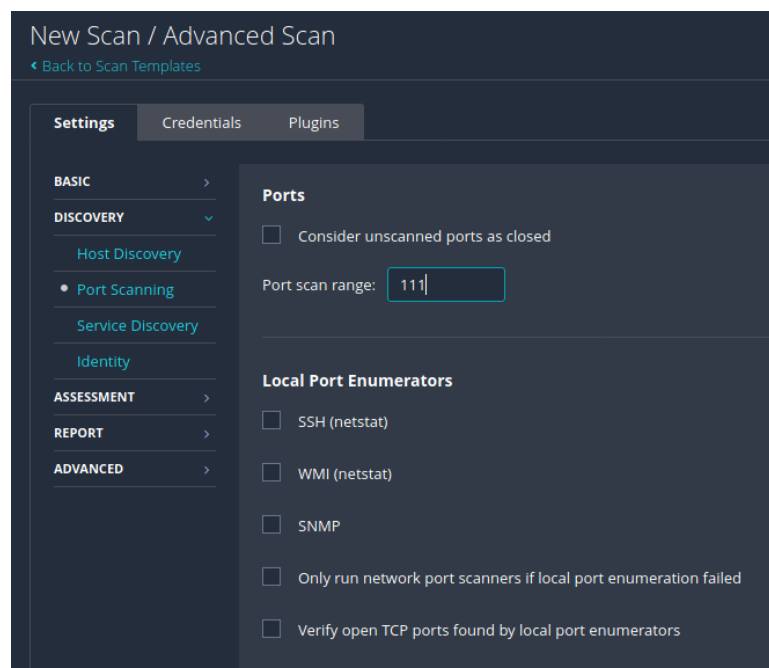
DISCOVERY

- Host Discovery

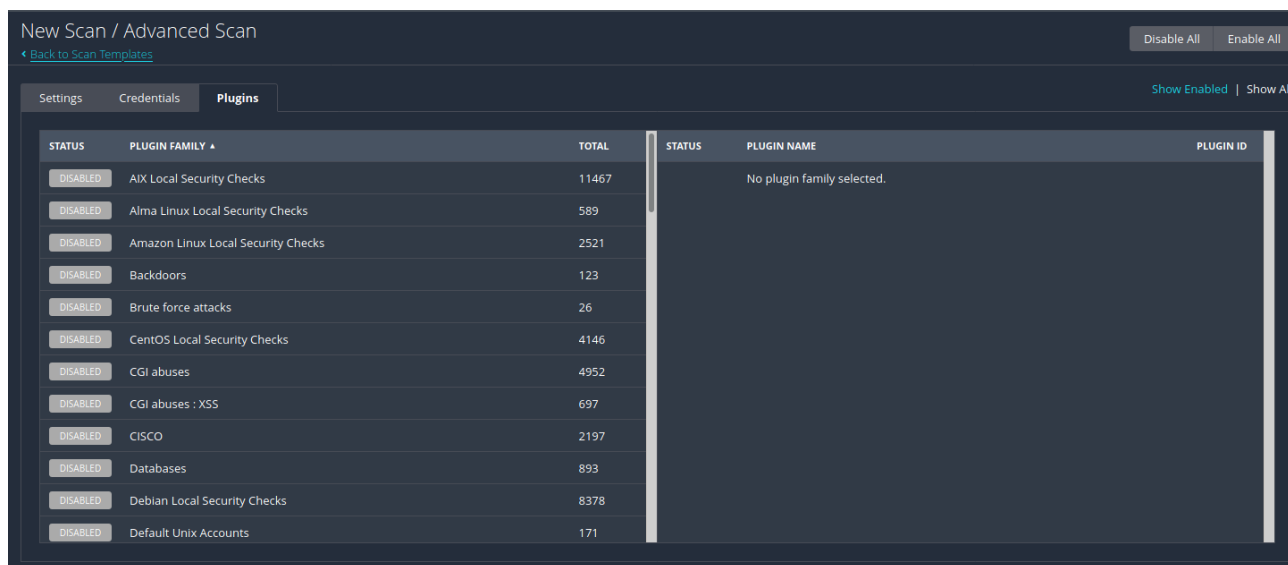
Remote Host Ping

Ping the remote host ☐ OFF

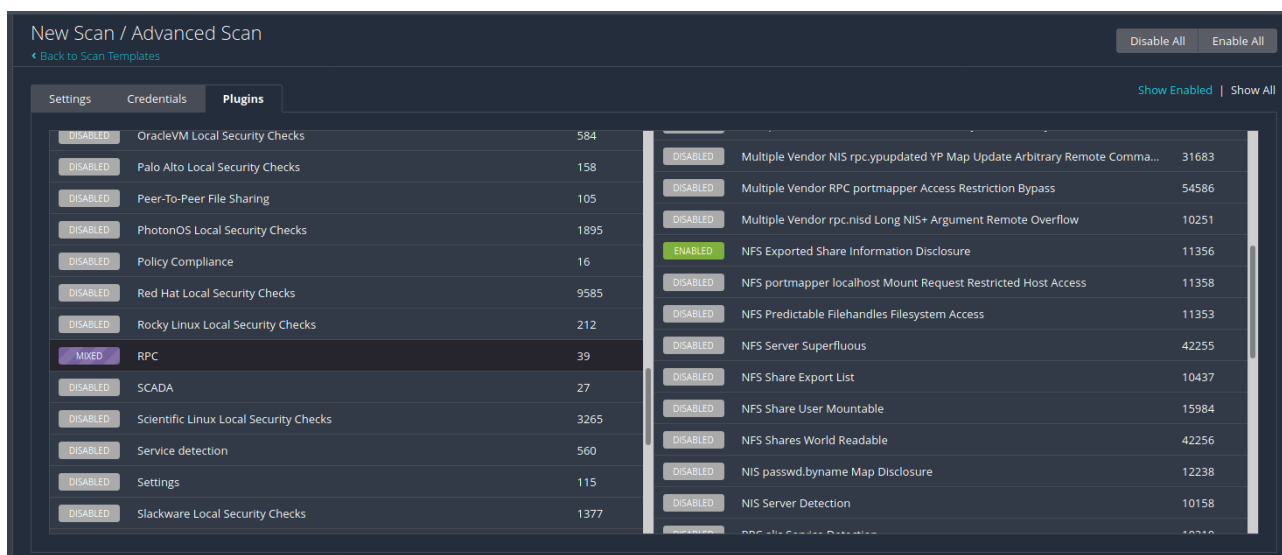
Chọn “Discovery” và vào “Host Discovery” , tắt tính năng “Ping the remote host”



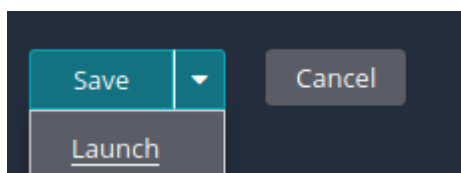
Tắt hết các port không cần thiết



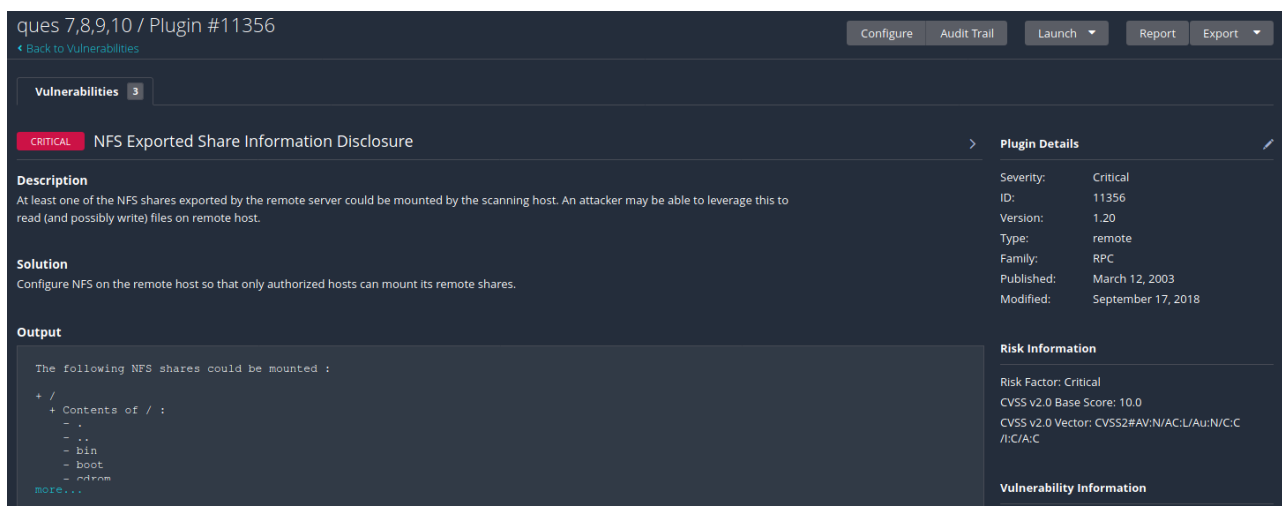
Chọn thẻ *Plugins* và click vào *Disable All* ở góc phải



Tìm “RFC” và click vào , đồng thời click vào “NFC Exported ..” ở cột phải



Cấu hình xong click vào *Save* và *Launch*



Kết quả scan với chỉ 1 lỗ hổng duy nhất

Câu 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?

- Thực hiện bắt gói tin với wireshark trong lúc thực hiện scan ở nessus (đã chỉ định port 111)

The screenshot shows a Wireshark capture of network traffic from 192.168.18.130. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
9	11.202352467	192.168.18.132	192.168.18.130	TCP	62	21164 → 111 [SYN] Seq=0 Win=4996 Len=0 MSS=1460 SACK_PERM=1
10	11.203297683	192.168.18.130	192.168.18.132	TCP	62	111 → 21164 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
13	11.337603852	192.168.18.132	192.168.18.130	TCP	74	51578 → 81 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2936570651 TSecr=0 WS=128
14	11.338090905	192.168.18.130	192.168.18.132	TCP	60	81 → 51578 [ACK] Seq=1 Ack=1 Win=0 Len=0
15	11.393070339	192.168.18.132	192.168.18.130	TCP	74	60216 → 8009 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2936570707 TSecr=0 WS=128
16	11.393726735	192.168.18.130	192.168.18.132	TCP	74	8009 → 60216 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=319477 TSecr=2
17	11.393809062	192.168.18.132	192.168.18.130	TCP	66	60216 → 8009 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2936570707 TSecr=319477
18	11.404885291	192.168.18.132	192.168.18.130	TCP	376	60216 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=310 TSval=2936570718 TSecr=319477 [TCP seq..
19	11.406186847	192.168.18.130	192.168.18.132	TCP	66	8009 → 60216 [ACK] Seq=1 Ack=311 Win=6880 Len=0 TSval=319479 TSecr=2936570718
20	11.419802673	192.168.18.130	192.168.18.132	TCP	66	8009 → 60216 [FIN, ACK] Seq=1 Ack=311 Win=6880 Len=0 TSval=319480 TSecr=2936570718
21	11.421027699	192.168.18.132	192.168.18.130	TCP	66	60216 → 8009 [ACK] Seq=311 Ack=2 Win=64256 Len=0 TSval=2936570734 TSecr=319480
22	11.424090418	192.168.18.130	192.168.18.132	TCP	66	8009 → 8009 [ACK] Seq=311 Ack=2 Win=64256 Len=0 TSval=2936570760 TSecr=319480
23	11.490909858	192.168.18.132	192.168.18.130	TCP	74	51468 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2936570803 TSecr=0 WS=128
24	11.490423935	192.168.18.130	192.168.18.132	TCP	74	80 → 51468 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=319487 TSecr=293
25	11.490462245	192.168.18.132	192.168.18.130	TCP	66	51468 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2936570804 TSecr=319487
26	11.528509165	192.168.18.132	192.168.18.130	HTTP	371	GET / HTTP/1.1
27	11.529078493	192.168.18.130	192.168.18.132	TCP	66	80 → 51468 [ACK] Seq=1 Ack=306 Win=6880 Len=0 TSval=319491 TSecr=2936570842
28	11.566451017	192.168.18.130	192.168.18.132	TCP	1204	80 → 51468 [PSH, ACK] Seq=1 Ack=306 Win=6880 Len=1138 TSval=319495 TSecr=2936570842 [TCP seq..
29	11.566451458	192.168.18.130	192.168.18.132	HTTP	71	HTTP/1.1 200 OK (text/html)
30	11.566519816	192.168.18.132	192.168.18.130	TCP	66	51468 → 80 [ACK] Seq=306 Ack=1139 Win=64128 Len=0 TSval=2936570880 TSecr=319495
31	11.566699883	192.168.18.132	192.168.18.130	TCP	66	51468 → 80 [ACK] Seq=306 Ack=1144 Win=64128 Len=0 TSval=2936570880 TSecr=319495
32	11.698935874	192.168.18.132	192.168.18.130	SNMP	85	get-next-request 1.3.6.1.2.1.1.1.0
33	11.698540020	192.168.18.130	192.168.18.132	ICMP	113	Destination unreachable (Port unreachable)
34	11.724847686	192.168.18.132	192.168.18.130	TCP	74	52414 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2936571038 TSecr=0 WS=128
35	11.726152560	192.168.18.130	192.168.18.132	TCP	74	445 → 52414 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=319511 TSecr=29
36	11.726234545	192.168.18.132	192.168.18.130	TCP	66	52414 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2936571040 TSecr=319511
37	11.746369321	192.168.18.132	192.168.18.130	SNMP	85	get-next-request 1.3.6.1.2.1.1.1.0
38	11.746755515	192.168.18.130	192.168.18.132	ICMP	113	Destination unreachable (Port unreachable)
39	11.775483692	192.168.18.132	192.168.18.130	SMB	241	Negotiate Protocol Request
40	11.775893088	192.168.18.130	192.168.18.132	TCP	66	445 → 52414 [ACK] Seq=1 Ack=176 Win=6880 Len=0 TSval=319516 TSecr=2936571089

Frame 9: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface ens33, id 0
 Ethernet II, Src: VMware_5b:5f:c9 (00:0c:29:5b:5f:c9), Dst: VMware_9a:54:44 (00:0c:29:9a:54:44)
 Internet Protocol Version 4, Src: 192.168.18.132, Dst: 192.168.18.130
 Transmission Control Protocol, Src Port: 21164, Dst Port: 111, Seq: 0, Len: 0

- IP máy meta là 192.168.18.130, ta có thể thấy ở đây dù đã chỉ định port scan là 111 nhưng Nessus vẫn kết nối đến những port khác của máy meta (No13: port 81; No15: port 8009;...)
- Giải thích: một số plugin kiểm tra trạng thái của các port ngoài những port được chỉ định. Những port ngoài phạm vi được chỉ định sẽ có trạng thái là “KHÔNG XÁC ĐỊNH” do chưa được scan. Mặc định, nếu port có trạng thái không xác định, hàm `get_port_state()` sẽ trả về đúng và nessus sẽ thử kết nối đến port.

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

- Để chặn việc Nessus scan port không được chỉ định, ở phần configure của scan, tích chọn **Consider unscanned ports as closed**

Metasploitable - Cau3 / Configuration

[← Back to Scan Report](#)

Settings | Credentials | Plugins

BASIC >
DISCOVERY v
Host Discovery
● Port Scanning
Service Discovery
ASSESSMENT >
REPORT >
ADVANCED >

Ports
☒ Consider unscanned ports as closed
Port scan range:
Local Port Enumerators
☒ SSH (netstat)

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

- Plugin thứ nhất

The screenshot shows the Nessus Scans page with the 'New Scan / Advanced Scan' configuration. The 'Plugins' tab is selected, displaying a list of plugins. The 'SNMP' plugin is highlighted with a 'MIXED' status.

STATUS	PLUGIN NAME	PLUGIN ID
DISABLED	Red Hat Local Security Checks	8164
DISABLED	RPC	38
DISABLED	SCADA	12
DISABLED	Scientific Linux Local Security Checks	3182
DISABLED	Service detection	526
DISABLED	Settings	111
DISABLED	Slackware Local Security Checks	1255
DISABLED	SMTP problems	149
MIXED	SNMP	33
DISABLED	Solaris Local Security Checks	3760
DISABLED	SuSE Local Security Checks	18125
DISABLED	ARRIS Touchstone DG950A SNMP Information ...	78921
ENABLED	ASG-Sentry SNMP Agent Detection	34396
DISABLED	BMC SNMP Agent Default Community Name (pu...	51160
DISABLED	Cisco CatOS VACM read-write Community String...	10688
DISABLED	Cisco Digital Media Manager < 5.3 Privilege Esc...	69948
DISABLED	D-Link DSL Broadband Modem SNMP Cleartext ...	11490
DISABLED	HP JetDirect Device SNMP Request Cleartext A...	11317
DISABLED	HP/H3C and Huawei SNMP User Data Informati...	62759
DISABLED	Microsoft Windows LAN Manager SNMP LanMa...	10547
DISABLED	Microsoft Windows LAN Manager SNMP LanMa...	10548

The screenshot shows the Nessus Scans page with the 'Metasploitable2 - Individual / Plugin #11219' configuration. The 'Vulnerabilities' tab is selected, displaying the 'Nessus SYN scanner' plugin details.

Plugin Details

Severity:	Info
ID:	11219
Version:	1.40
Type:	remote
Family:	Port scanners
Published:	February 4, 2009
Modified:	September 16, 2021

Risk Information

Risk Factor: None

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

Port 111/tcp was found to be open

Port	Hosts
111 / tcp / rpc-portma...	192.168.18.130

- Plugin thứ hai

New Scan / Advanced Scan [Back to Scan Templates](#) [Disable All](#) [Enable All](#)

[Settings](#) [Credentials](#) [Plugins](#) [Show Enabled](#) | [Show All](#)

STATUS	PLUGIN FAMILY ▲	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
DISABLED	AIX Local Security Checks	11409	DISABLED	4553 Parasite Mothership Backdoor Detection	11187
DISABLED	Amazon Linux Local Security Checks	2055	DISABLED	Agobot.FO Backdoor Detection	12128
MIXED	Backdoors	121	ENABLED	alya.cgi CGI Backdoor Detection	11118
DISABLED	CentOS Local Security Checks	3808	DISABLED	Arugizer Backdoor Detection	45005
DISABLED	CGI abuses	4560	DISABLED	ASUS Router 'infosvr' Remote Command Executi...	80518
DISABLED	CGI abuses : XSS	690	DISABLED	BackOffice Software Detection	10024
DISABLED	CISCO	1994	DISABLED	Bagle Worm Removal	12027
DISABLED	Databases	767	DISABLED	Bagle.B Worm Detection	12063
DISABLED	Debian Local Security Checks	7717	DISABLED	Bind Shell Backdoor Detection	51988
DISABLED	Default Unix Accounts	171	DISABLED	Bugbear Worm Detection	11135

[Read More](#) [Save](#) [Cancel](#)

Activate Windows
Go to Settings to activate Windows.

Metasploitable2 - Individual / Plugin #11219 [Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to Vulnerabilities](#)

Vulnerabilities 2

INFO Nessus SYN scanner

Description
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution
Protect your target with an IP filter.

Output

```
Port 21/tcp was found to be open
```

Port ▲	Hosts
21 / tcp / ftp	192.168.18.130

Plugin Details

Severity: Info
ID: 11219
Version: 1.40
Type: remote
Family: Port scanners
Published: February 4, 2009
Modified: September 16, 2021

Risk Information
Risk Factor: None

Activate Windows
Go to Settings to activate Windows.

Câu 11: Tìm hiểu công cụ Sn1per

- Cài đặt theo hướng dẫn từ github.

```
(kali@kali)-[~]
$ git clone https://github.com/1N3/Sn1per
Cloning into 'Sn1per' ...
remote: Enumerating objects: 2944, done.
remote: Counting objects: 100% (119/119), done.
remote: Compressing objects: 100% (93/93), done.
remote: Total 2944 (delta 64), reused 55 (delta 25), pack-reused 2825
Receiving objects: 100% (2944/2944), 44.03 MiB | 4.33 MiB/s, done.
Resolving deltas: 100% (2009/2009), done.

(kali@kali)-[~]
$ cd Sn1per

(kali@kali)-[~/Sn1per]
$ bash install.sh

  SN1PER

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

[>] This script will install Sn1per under /usr/share/sniper. Are you sure you want to continue? (Hit Ctrl+C to exit)
[ ]
```

```
⇒ https://www.kali.org/docs/general-use/python3-transition/

(Run: "touch ~/.hushlogin" to hide this message)
Creating configuration file in /usr/share/metasploit-framework/config/database.yml
Creating initial database schema
[*] Adding start menu and desktop shortcuts...
[>] Done!
[>] To run, type 'sniper'!

(kali@kali)-[~/Sn1per]
$
```

- Sniper có nhiều mode, ở đây sẽ scan thử Normal Mode với máy có ip là 45.122.249.68. Lệnh thực hiện sẽ là **sniper -t 45.122.249.68**

```
[*] Loaded configuration file from /root/.sniper.conf [OK]

Places
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos

+ -- ==[ https://snipersecurity.com
+ -- ==[ Sniper v9.0 by @xer0dayz

[*] NORMAL MODE
sniper -t <TARGET>

[*] SPECIFY CUSTOM CONFIG FILE
sniper -c /full/path/to/sniper.conf -t <TARGET> -m <MODE> -w <WORKSPACE>

[*] NORMAL MODE + OSINT + RECON
sniper -t <TARGET> -o -re

[*] STEALTH MODE + OSINT + RECON
sniper -t <TARGET> -m stealth -o -re

[*] DISCOVER MODE
sniper -t <CIDR> -m discover -w <WORKSPACE_ALIAS>

[*] SCAN ONLY SPECIFIC PORT
sniper -t <TARGET> -m port -p <portnum>
```

- Khi có dòng SCAN COMPLETE nghĩa là đã thực hiện quét xong

```
====
P4 - LOW, Clickjacking,http://45.122.249.68:80/,X-Frame-Options: DENY
=====
====
====•x[2021-11-01](06:24)x•
SCAN COMPLETE!
====•x[2021-11-01](06:24)x•
=====

[*] Opening loot directory /usr/share/sniper/loot/workspace/45.122.249.68 [OK]
+ -- ==[ Generating reports...
[|]
+ -- ==[ Sorting all files...
+ -- ==[ Removing blank screenshots and files...
+ -- ==[ Sniper Professional is not installed. To download Sniper Professional, go to https://snipersecurity.com.
+ -- ==[ Done!
ubuntu@ubuntu1804:~$
```

- Báo cáo về kết quả của lần scan sẽ được lưu ở /usr/share/sniper/loot/workspace/tên lần scan

```
ubuntu@ubuntu1804:/usr/share/sniper/loot/workspace/45.122.249.68$ ls
credentials  ips      notes  output  scans  vulnerabilities
domains     nmap     osint  reports  screenshots  web
ubuntu@ubuntu1804:/usr/share/sniper/loot/workspace/45.122.249.68$ cd vulnerabilities/
ubuntu@ubuntu1804:/usr/share/sniper/loot/workspace/45.122.249.68/vulnerabilities$ ls
critical_vulns_total.txt  scope-45.122.249.68-http-80-Clickjacking.txt
high_vulns_total.txt     scope-all-vulnerabilities-sorted.txt
info_vulns_total.txt     vulnerability-report-45.122.249.68.txt
low_vulns_total.txt      vulnerability-risk-45.122.249.68.txt
medium_vulns_total.txt   vuln_score_total.txt
ubuntu@ubuntu1804:/usr/share/sniper/loot/workspace/45.122.249.68/vulnerabilities$
```

- cat nội dung của một file để xem báo cáo

```
ubuntu@ubuntu1804:/usr/share/sniper/loot/workspace/45.122.249.68/vulnerabilities$ cat critical_vulns_total.txt
0
ubuntu@ubuntu1804:/usr/share/sniper/loot/workspace/45.122.249.68/vulnerabilities$ cat vulnerability-report-45.122.249.68.txt
=====
====
•?((~°...• Scope Vulnerability Report by @xer0dayz •._.°~))•
=====
====
Critical: 0
High: 0
Medium: 0
Low: 1
Info: 0
Score: 2
=====
====
P4 - LOW, Clickjacking,http://45.122.249.68:80/,X-Frame-Options: DENY
=====
====
ubuntu@ubuntu1804:/usr/share/sniper/loot/workspace/45.122.249.68/vulnerabilities$
```


Câu 11.2: Tìm hiểu công cụ OpenVAS

```
(root@kali)-[/home/kali/Desktop]
# sudo apt install openvas
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libgs9-common
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  doc-base dvisvgm fonts-lmodern fonts-texgyre fonts-texgyre-math
  ghostscript gnutls-bin greenbone-security-assistant gsad gvm gvm-tools
  gvmc gvmc-common icu-devtools libalgorithm-diff-xs-perl
  libapache-pom-java libapt-pkg-perl libbit-vector-perl libc-bin
  libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev libc6-i386
  libcarp-clan-perl libclone-perl libcommon-sense-perl
  libcommons-logging-java libcommons-parent-java libcrypt-rc4-perl
  libcrypt-ssleay-perl libdate-calc-perl libdate-calc-xs-perl
  libdbd-mariadb-perl libdbi-perl libdigest-perl-md5-perl libdlt2
  libfcgi-perl libfile-fcntllock-perl libfontbox-java libgnutls-dane0
  libgnutls30 libgs-common libgs10 libgs10-common libgs9-common libgvm22
  libhiredis0.14 libhtml-parser-perl libicu-dev libicu72 libjcode-pm-perl
  libjson-xs-perl libkpathsea6 liblist-moreutils-xs-perl
  liblocale-gettext-perl liblzfl libmath-random-isaac-xs-perl
  libmicrohttpd12 libmosquitto1 libnet-dbus-perl libnet-dns-sec-perl
  libnet-libidn-perl libnet-ssleay-perl libole-storage-lite-perl
```

Hình 11.1: Tiến hành cài đặt OpenVas

```
Processing triggers for nicolor-icon-theme (0.17-2) ...
Processing triggers for libc-bin (2.36-4) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for dbus (1.12.20-2) ...
Processing triggers for mailcap (3.69) ...
Processing triggers for fontconfig (2.13.1-4.2) ...
Processing triggers for tex-common (6.18) ...
Running updpmap-sys. This may take some time... done.
Running mktexlsr /var/lib/texmf ... done.
Building format(s) --all.
This may take some time... done.
```

Hình 11.2: Cài đặt hoàn tất

- Sau khi hoàn thành cài đặt ta restart máy để apply các setting mới của openvas
- Dùng lệnh gvm-setup để cài đặt gvm

```
(root@kali)-[~]
# gvm-setup
```

Hình 11.3: Lệnh gvm-setup

- Sau khi chạy lệnh trên ta được cấp password để login vào web của OpenVAS
- Tài khoản được cấp

User: admin

Pass: e9f9c388-58ef-47d1-ae4b-e117e37008a1

```
[+] GVM feeds updated
[*] Checking Default scanner
[*] Modifying Default Scanner
Scanner modified.

[+] Done
[*] Please note the password for the admin user
[*] User created with password 'e9f9c388-58ef-47d1-ae4b-e117e37008a1'.

[>] You can now run gvm-check-setup to make sure everything is correctly configured
```

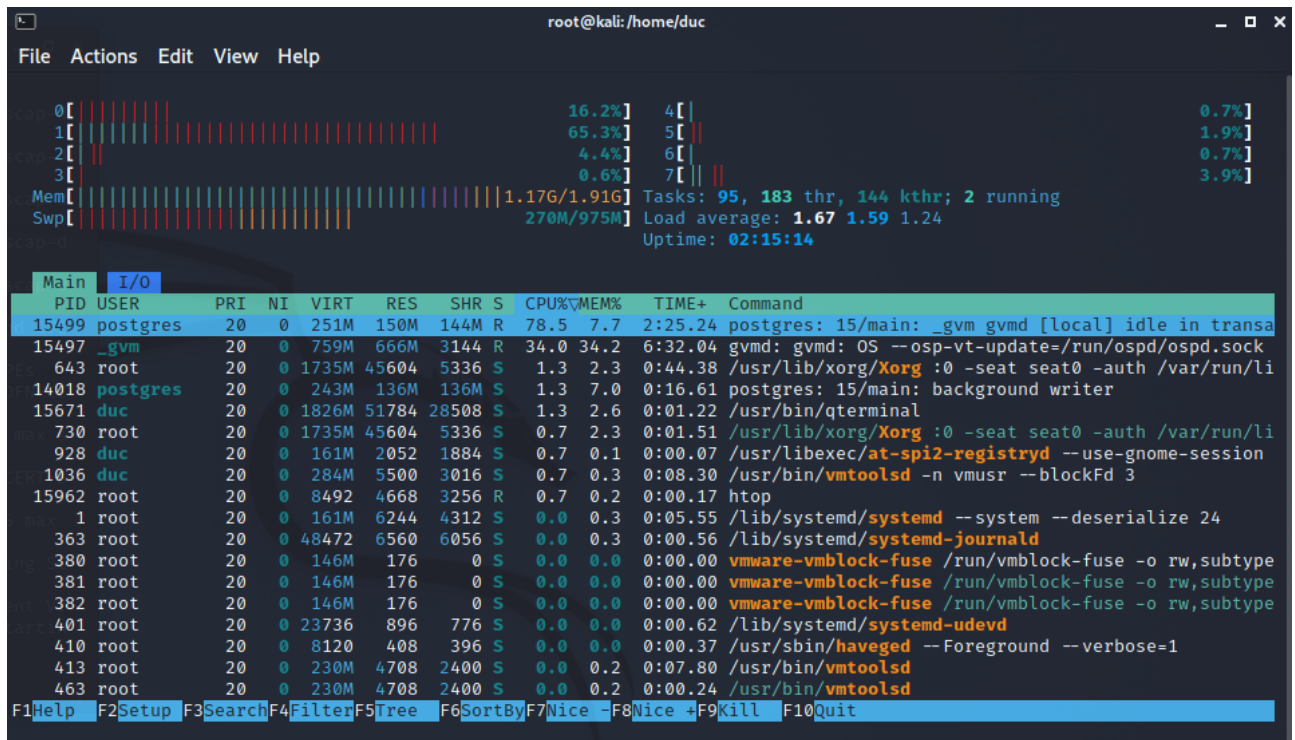
Hình 11.4: Tài khoản được cấp

```
(root@kali)~[/home/
# cd /var/log/gvm

(root@kali)~[/var/log/gvm]
# tail -f gvm.log
md manage: INFO:2022-11-20 04h29.25 UTC:15236: Updating /var/lib/gvm/cert-data/CB-K19.xml
md manage: INFO:2022-11-20 04h29.27 UTC:15236: Updating /var/lib/gvm/cert-data/CB-K15.xml
md manage: INFO:2022-11-20 04h29.31 UTC:15236: Updating /var/lib/gvm/cert-data/CB-K16.xml
md manage: INFO:2022-11-20 04h29.35 UTC:15236: SCAP database does not exist (yet), skipping CERT severity score update
md manage: INFO:2022-11-20 04h29.35 UTC:15236: sync_cert: Updating CERT info succeeded.
md manage: INFO:2022-11-20 04h30.46 UTC:15234: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2012.xml
md manage: INFO:2022-11-20 04h30.55 UTC:15234: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2018.xml
md manage: INFO:2022-11-20 04h31.36 UTC:15234: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2019.xml
md manage: INFO:2022-11-20 04h32.12 UTC:15234: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2009.xml
md manage: INFO:2022-11-20 04h32.24 UTC:15234: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2022.xml
```

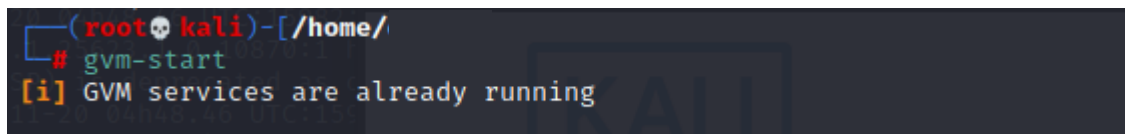
Hình 11.5: Log

- Sau khi hoàn tất ta sử dụng lệnh htop để quan sát tổng quát hệ thống



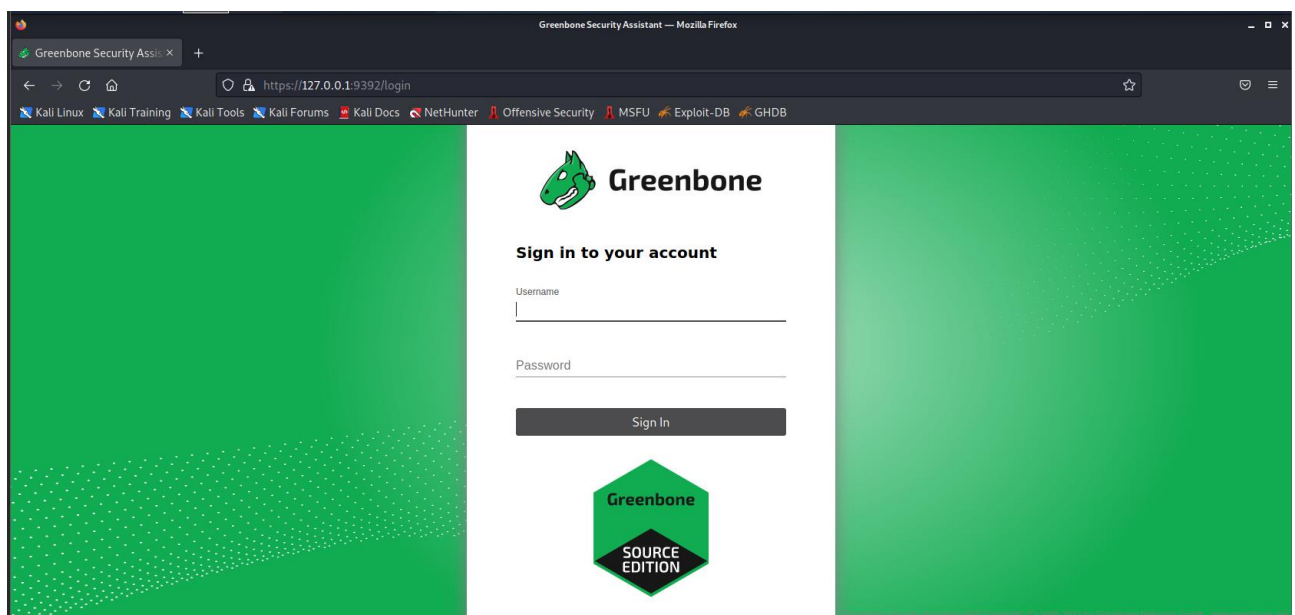
Hình 11.6: Kiểm tra hoạt động hệ thống

- Sau đó tiến hành khởi động OpenVAS



Hình 11.7: Start OpenVAS

- Mở Browser lên gõ : 127.0.0.1:9392 ta sẽ vào đc web của OpenVAS

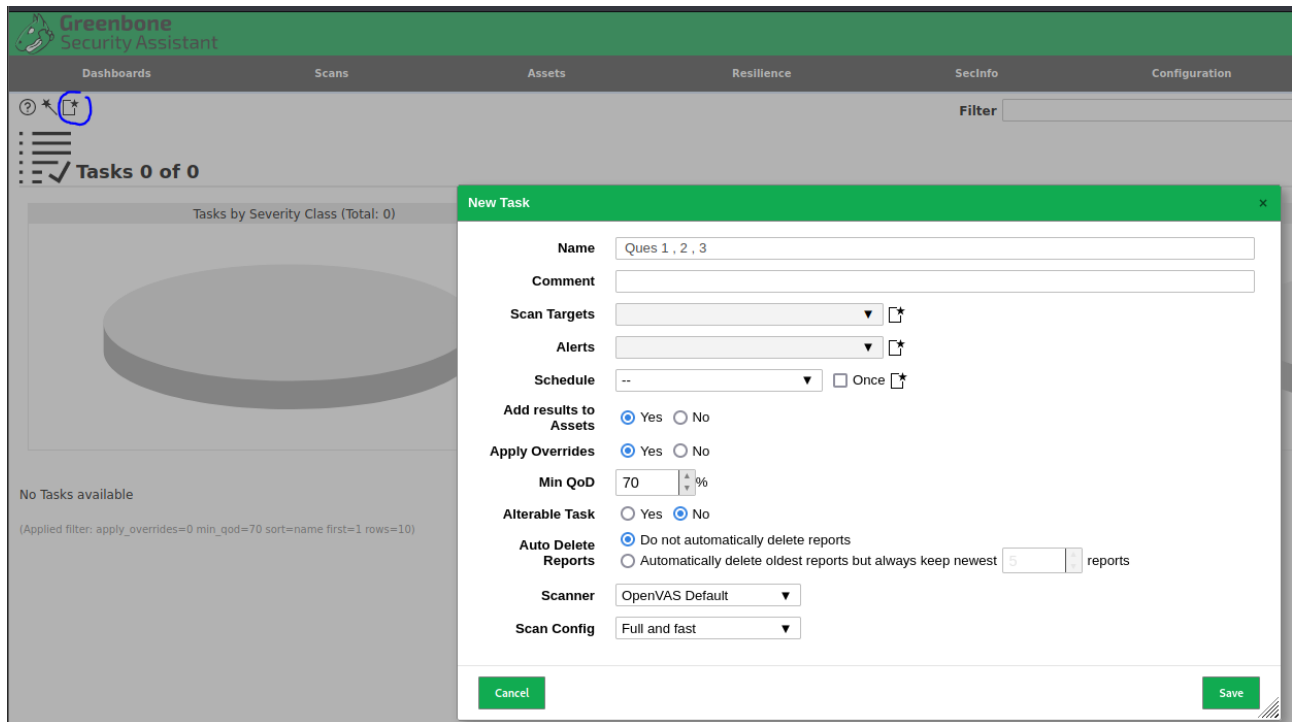


Hình 11.8: Trang đăng nhập OpenVAS

1. Quét máy Metasploitable2 không sử dụng tài khoản chứng thực

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

- Click vào button góc trái và chọn “New task”, 1 hộp thoại sẽ hiện ra để điền các thông tin để có thể quét



Hình 11.9: Setting để scan

- Click vào button bên cạnh combobox để cấu hình target

Scan Targets ▼ ★

Hình 11.10: Cài đặt target

- Điền các thông tin phù hợp với yêu cầu và ấn save để lưu các cài đặt

Hình 11.11: Thông số cần điền

- Sau đó tiến hành quét

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Ques 1, 2, 3	Done	1	Sun, Nov 20, 2022 5:55 AM UTC	10.0 (High)		▶ 🗑️ 🔄 🔍

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Apply to page contents [📄](#) [🗑️](#) [🔄](#)

1 - 1 of 1

Hình 11.12: Kết quả sau khi quét xong

- Sau đó tiến hành ping kiểm tra

55	59.687557022	192.168.1.136	192.168.1.134	ICMP	98 Echo (ping) request	id=0xc07f, seq=0/0, ttl=64 (reply in 56)
56	59.687839906	192.168.1.134	192.168.1.136	ICMP	98 Echo (ping) reply	id=0xc07f, seq=0/0, ttl=64 (request in 55)

Hình 11.13: Ping scanning

- Kiểm tra host có active hay không

63	61.240816563	192.168.1.134	192.168.1.136	TCP	74 23 → 40268 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=68739 TSecr=2025845694
64	61.240885286	192.168.1.136	192.168.1.134	TCP	66 40268 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2025845695 TSecr=68739

Hình 11.14: Active/Deactive Scanning

TCP scanning

- 3-way handshake
- Tạo kết nối TCP đến port trên remote system

2039...	1930.3153135...	192.168.1.136	192.168.1.134	HTTP	222 OPTIONS /twiki/pub/TWiki/TWikiTemplates/ HTTP/1.1
2039...	1930.3156178...	192.168.1.134	192.168.1.136	HTTP	306 HTTP/1.1 200 OK
2039...	1930.3171771...	192.168.1.136	192.168.1.134	HTTP	222 OPTIONS /twiki/pub/TWiki/TWikiTemplates/ HTTP/1.1
2039...	1930.3174757...	192.168.1.134	192.168.1.136	HTTP	306 HTTP/1.1 200 OK
2039...	1930.3189492...	192.168.1.136	192.168.1.134	HTTP	222 OPTIONS /twiki/pub/TWiki/TWikiTemplates/ HTTP/1.1
2039...	1930.3192311...	192.168.1.134	192.168.1.136	HTTP	306 HTTP/1.1 200 OK
2039...	1930.3206917...	192.168.1.136	192.168.1.134	HTTP	222 OPTIONS /twiki/pub/TWiki/TWikiTemplates/ HTTP/1.1
2039...	1930.3209705...	192.168.1.134	192.168.1.136	HTTP	306 HTTP/1.1 200 OK
2039...	1930.3224276...	192.168.1.136	192.168.1.134	HTTP	222 OPTIONS /twiki/pub/TWiki/TWikiTemplates/ HTTP/1.1
2039...	1930.3227279...	192.168.1.134	192.168.1.136	HTTP	306 HTTP/1.1 200 OK
2039...	1930.3246249...	192.168.1.136	192.168.1.134	HTTP	222 OPTIONS /twiki/pub/TWiki/TWikiTemplates/ HTTP/1.1
2039...	1930.3249322...	192.168.1.134	192.168.1.136	HTTP	306 HTTP/1.1 200 OK

Hình 11.15: Mã hóa thông tin giữa Kali và metasploitable2

- Ta tiến hành Half-open scanning

2045...	1931.5561814...	192.168.1.136	192.168.1.134	TCP	74 40365 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=20277160
2045...	1931.5563850...	192.168.1.134	192.168.1.136	TCP	74 80 → 40365 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval

Hình 11.16: Half-open scanning

- Chỉ gửi SYN từ scanner
- Reply là :
 - SYN/ACK
 ⇒ Port đang mở
- RST/ACK
- ⇒ Không có listening từ port

1069...	1340.4636018...	192.168.1.2	192.168.1.134	DNS	86 Standard query response 0x81ac No such name PTR 136.1.168.192.in-addr.arpa
1070...	1341.4969888...	192.168.1.134	192.168.1.2	DNS	86 Standard query 0x6ef5 PTR 136.1.168.192.in-addr.arpa
1070...	1341.5823610...	192.168.1.2	192.168.1.134	DNS	86 Standard query response 0x6ef5 No such name PTR 136.1.168.192.in-addr.arpa
1070...	1341.5858144...	192.168.1.134	192.168.1.2	DNS	86 Standard query 0xc905 PTR 136.1.168.192.in-addr.arpa

Hình 11.17: Metasploitable2 tìm remote host trong local LAN bằng “ARP pingging”

3. Quét lại nhưng quét thêm port UDP.

Làm tương tự câu 1 và 2 nhưng trong phần target thì sửa chỗ “Port list” thành “TCP and UDP”.

New Target

Name

ques3_real2

Comment

Hosts

☒ Manual 192.168.1.134
 ☐ From file Browse... No file selected.

Exclude Hosts

☒ Manual
 ☐ From file Browse... No file selected.

Allow simultaneous scanning via multiple IPs

☒ Yes
 ☐ No

Port List

All TCP and Nmap top 10 ▼

Alive Test

Scan Config Default ▼

Credentials for authenticated checks

SSH

--

on port 22

SMB

--

Cancel

Save

New Task

Name

Ques 3

Comment

Scan Targets

ques3 ▼

Alerts

Schedule

--

☐ Once

Add results to Assets

☒ Yes
 ☐ No

Apply Overrides

☒ Yes
 ☐ No

Min QoS

70 %

Alterable Task

☐ Yes
 ☒ No

Auto Delete Reports

☒ Do not automatically delete reports
 ☐ Automatically delete oldest reports but always keep newest 5 reports

Scanner

OpenVAS Default ▼

Scan Config

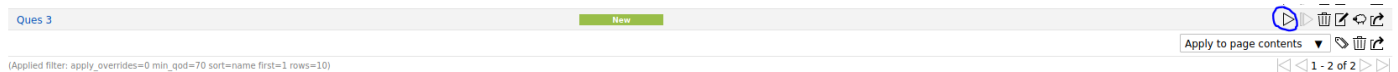
Full and fast ▼

Cancel

Save

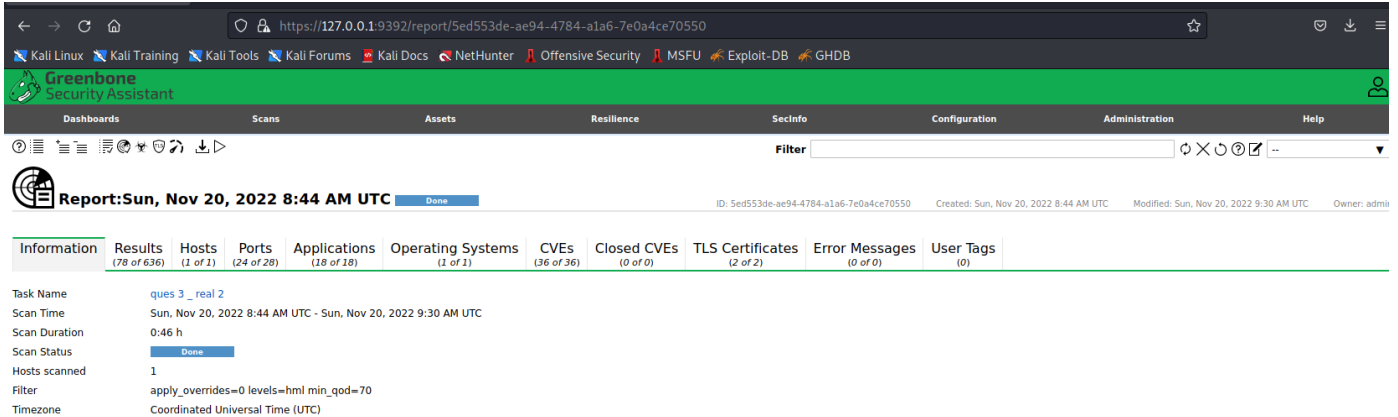
Hình 11.18: Các cài đặt như câu 1,2

- Tiến hành quét



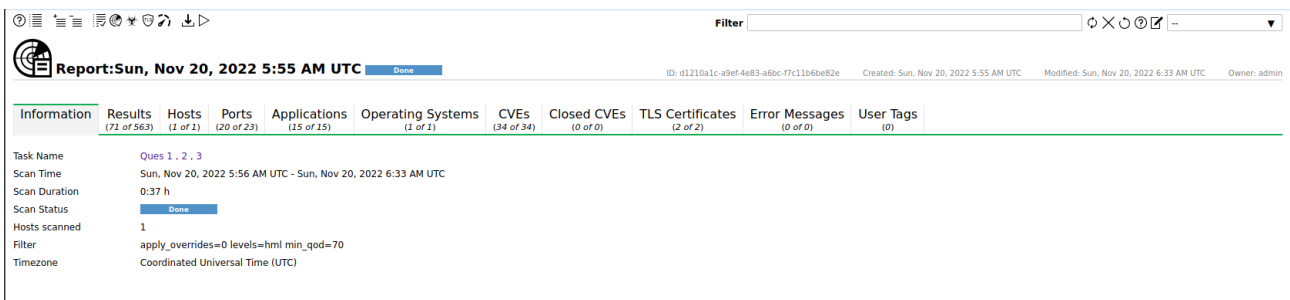
Hình 11.19: Quét

- Kết quả có UDP



Hình 11.20: Có UDP

- Kết quả không có UDP



Hình 11.21: Không có UDP

4. Thực hiện lại các bước trên để quét máy Metasploitable 2 có sử dụng tài khoản chứng thực.
5. Kiểm tra kết quả quét và so sánh với việc quét không sử dụng tài khoản chứng thực.
6. Hãy liệt kê các ưu, nhược điểm khi quét có tài khoản chứng thực và không có tài khoản chứng thực.

Vẫn cấu hình như cũ nhưng phần cấu hình target kéo xuống và click vào như hình dưới

Credentials for authenticated checks

SSH -- on port 22

SMB --

ESXi --

SNMP --

Hình 11.22: Cấu hình port

- Username và pass là : msfadmin. Sau đó bấm lưu lại

Create new SSH credential

Name msfadmin

Comment no comment

Type Username + Password

Allow insecure use ☐ Yes ☒ No

Auto-generate ☐ Yes ☒ No

Username msfadmin

Password

Cancel Save

Hình 11.23: Lưu lại tài khoản

New Target

simultaneous scanning via multiple IPs ☒ Yes ☐ No

Port List All IANA assigned TCP

Alive Test Scan Config Default

Credentials for authenticated checks

SSH msfadmin on port 22

Elevate privileges --

SMB --

ESXi --

SNMP --

Reverse Lookup Only ☐ Yes ☒ No

Reverse Lookup Unity ☐ Yes ☒ No

Cancel Save

New Task

Name ques 4.5.6

Comment

Scan Targets Unnamed

Alerts

Schedule -- ☐ Once

Add results to Assets ☒ Yes ☐ No

Apply Overrides ☒ Yes ☐ No

Min QoD 70 %

Alterable Task ☐ Yes ☒ No

Auto Delete Reports ☒ Do not automatically delete reports

Scanner OpenVAS Default

Scan Config Full and fast

Cancel Save

Hình 11.24: Các bước setting

Quét và kết quả có chứng thực

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration

Filter

Report: Sun, Nov 20, 2022 8:58 AM UTC Done ID: d90eff31-3d96-49fa-bd33-289c8c394294 Created: Sun, Nov

Information	Results (90 of 2789)	Hosts (1 of 1)	Ports (24 of 29)	Applications (42 of 42)	Operating Systems (1 of 1)	CVEs (47 of 47)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (1 of 1)	User Tags (0)
Task Name	quest 4.5.6_real									
Scan Time	Sun, Nov 20, 2022 8:58 AM UTC - Sun, Nov 20, 2022 9:56 AM UTC									
Scan Duration	0:58 h									
Scan Status	Done									
Hosts scanned	1									
Filter	apply_overrides=0 levels=hml min_qod=70									
Timezone	Coordinated Universal Time (UTC)									

Hình 11.25: Kết quả có chứng thực

Không có chứng thực

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration

Filter

Report: Sun, Nov 20, 2022 5:55 AM UTC Done ID: d1210a1c-a9ef-4e83-a6bc-f7c11b6be82e Created: Sun, Nov

Information	Results (71 of 563)	Hosts (1 of 1)	Ports (20 of 23)	Applications (15 of 15)	Operating Systems (1 of 1)	CVEs (34 of 34)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (0 of 0)	User Tags (0)
Task Name	Ques 1, 2, 3									
Scan Time	Sun, Nov 20, 2022 5:56 AM UTC - Sun, Nov 20, 2022 6:33 AM UTC									
Scan Duration	0:37 h									
Scan Status	Done									
Hosts scanned	1									
Filter	apply_overrides=0 levels=hml min_qod=70									
Timezone	Coordinated Universal Time (UTC)									

Hình 11.26: Kết quả không có chứng thực

Khi dùng tài khoản chứng thực

+ Ưu điểm :

- Có được nhiều thông tin chi tiết hơn
- Giảm thiểu các false positive
- Không chỉ quét các bản vá ở mức độ hệ điều hành mà còn quét các ứng dụng lỗi thời dễ bị tấn công

+ Nhược điểm :

- Có thể làm gián đoạn tới hệ thống của target

1. Kịch bản 01/Câu hỏi 01

2. Kịch bản 02

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

3. Kịch bản 03

- 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