



BÁO CÁO THỰC HÀNH

Môn học: An toàn Mạng
Kỳ báo cáo: Buổi 03 (Session 03)
Tên chủ đề: Quét lỗ hổng bảo mật
GVHD: Nghi Hoàng Khoa

Nhóm: 08

1. THÔNG TIN CHUNG:
Lớp: NT140.O11.ANTN

STT	Họ và tên	MSSV	Email
1	Lưu Gia Huy	21520916	21520916@gm.uit.edu.vn
2	Nguyễn Vũ Anh Duy	21520211	21520211@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Câu 01	100%
2	Câu 04	100%
3	Câu 07	100%

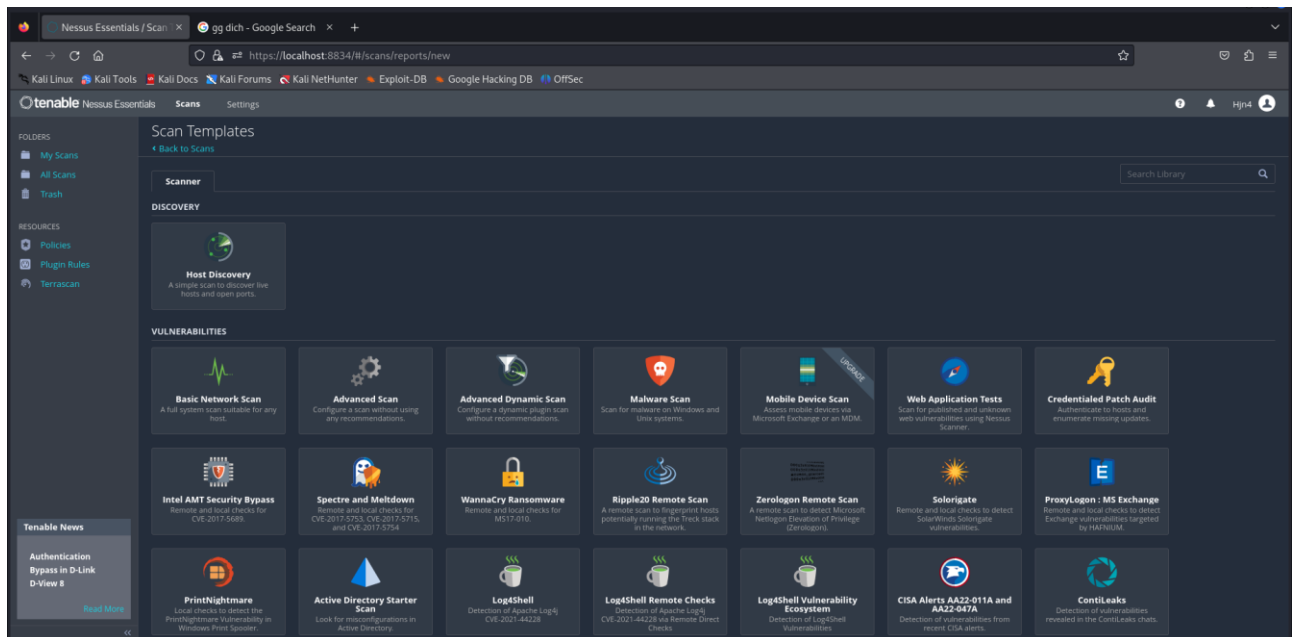
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

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

BÁO CÁO CHI TIẾT

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

- Sau khi bấm vào New scan:



- Ta sẽ đặt tên và ip mục tiêu:

New Scan / Basic Network Scan

[← Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name Metasploitable - Basic

Description

Folder My Scans

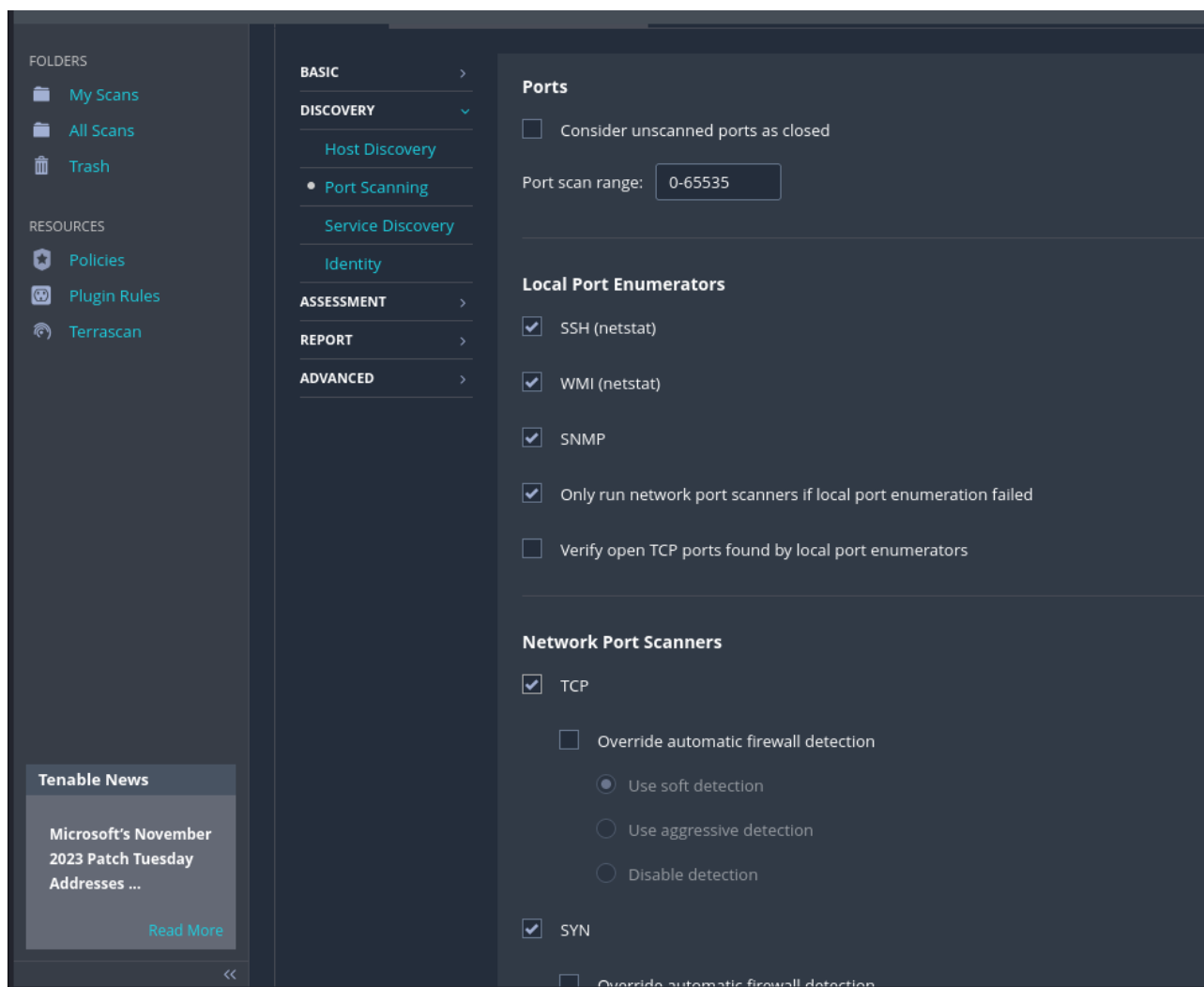
Targets

192.168.45.140

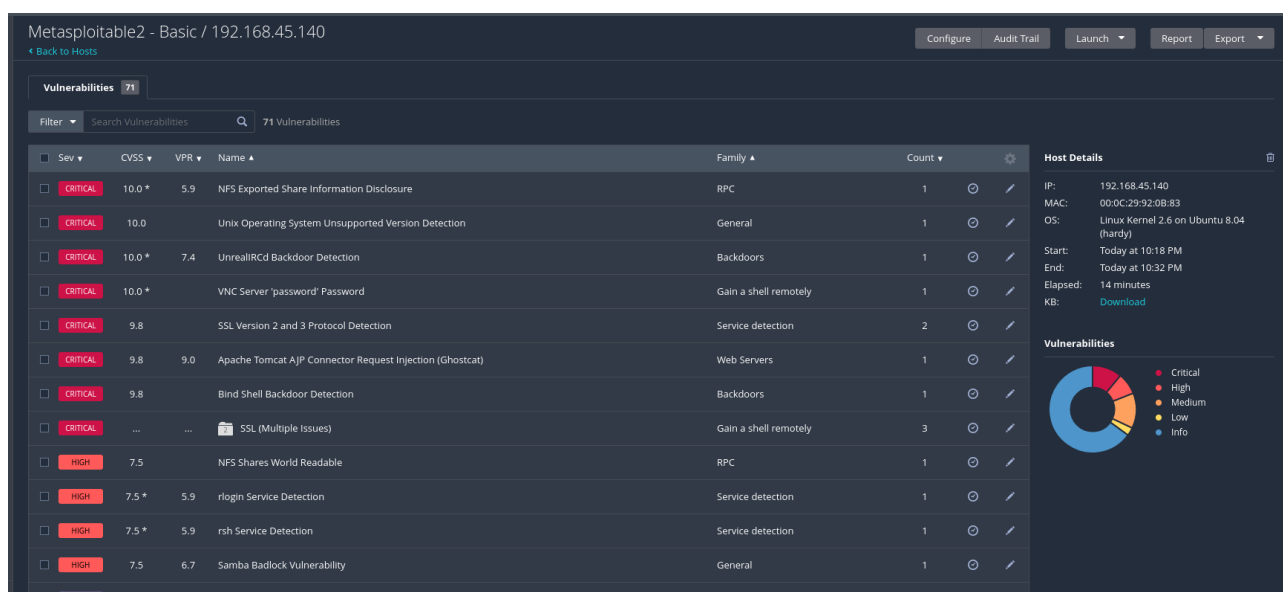
Upload Targets [Add File](#)

Save Cancel

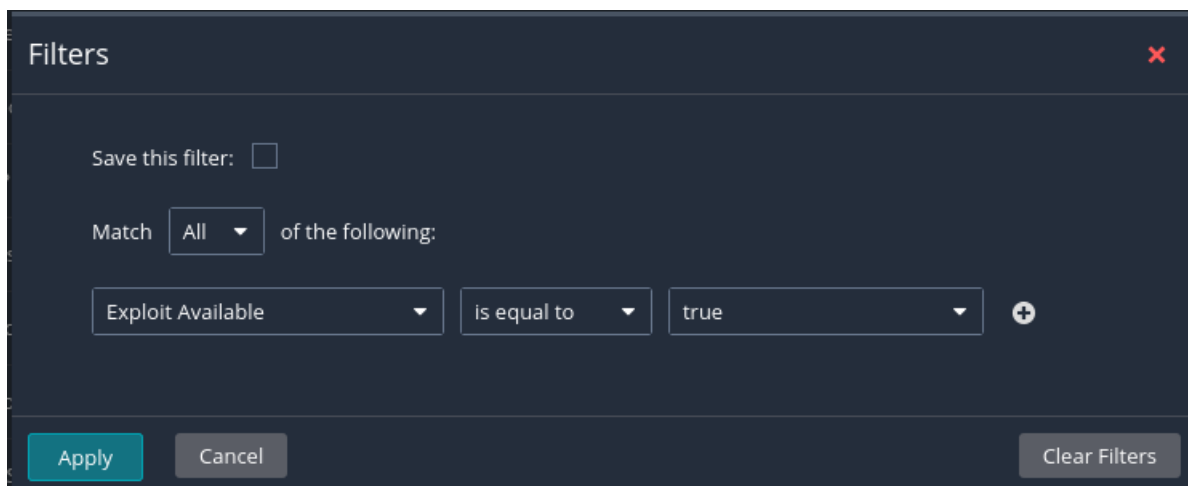
- Setup scan all port:



- Kết quả trước khi filter:



- Thực hiện filter:



Filters

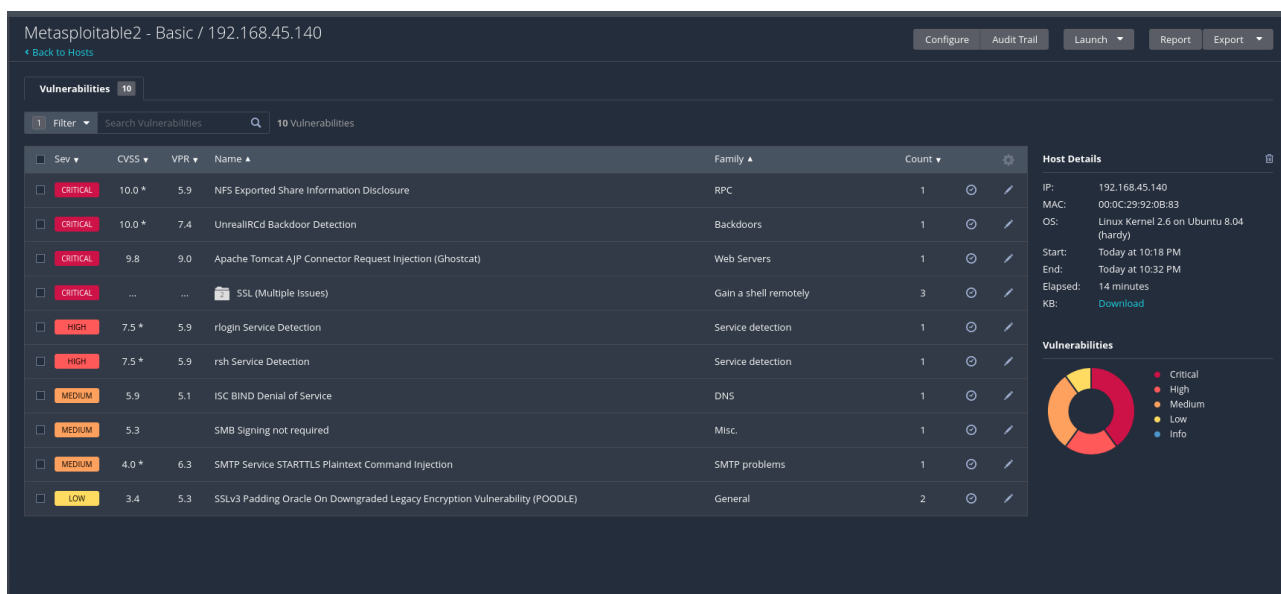
Save this filter: ☐

Match **All** of the following:

Exploit Available is equal to true

Apply Cancel Clear Filters

- Kết quả sau khi filter:



Metasploit2 - Basic / 192.168.45.140

Configure Audit Trail Launch Report Export

Vulnerabilities 10

Filter Search Vulnerabilities 10 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5 *	5.9	rlogin Service Detection	Service detection	1
HIGH	7.5 *	5.9	rsh Service Detection	Service detection	1
MEDIUM	5.9	5.1	ISC BIND Denial of Service	DNS	1
MEDIUM	5.3		SMB Signing not required	Misc.	1
MEDIUM	4.0 *	6.3	SMTP Service STARTTLS Plaintext Command Injection	SMTP problems	1
LOW	3.4	5.3	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	General	2

Host Details

IP: 192.168.45.140
MAC: 00:0C:29:92:08:83
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 10:18 PM
End: Today at 10:32 PM
Elapsed: 14 minutes
KB: Download

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

- Kết quả sau khi disable group:

Metasploitable2 - Basic / 192.168.45.140

Configure Audit Trail Launch Report Export

Vulnerabilities 11


Filter Search Vulnerabilities 11 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
CRITICAL	10.0 *	7.4	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	Gain a shell remotely	2	
CRITICAL	10.0 *	7.4	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely	1	
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1	
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	
HIGH	7.5 *	5.9	rlogin Service Detection	Service detection	1	
HIGH	7.5 *	5.9	rsh Service Detection	Service detection	1	
MEDIUM	5.9	5.1	ISC BIND Denial of Service	DNS	1	
MEDIUM	5.3		SMB Signing not required	Misc.	1	
MEDIUM	4.0 *	6.3	SMTP Service STARTTLS Plaintext Command Injection	SMTP problems	1	
LOW	3.4	5.3	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	General	2	

Host Details

IP: 192.168.45.140
MAC: 00:0C:29:92:08:83
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 10:18 PM
End: Today at 10:32 PM
Elapsed: 14 minutes
KB: [Download](#)

Vulnerabilities



Legend: Critical, High, Medium, Low, Info

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

- Đặt tên và ip mục tiêu:



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: 192.168.45.140

Upload Targets [Add File](#)

Save Cancel

- Nhập thông tin tài khoản SSH:

Settings

Credentials

Plugins

CATEGORIES

Host

Filter Credentials

Q

SNMPv3

∞

SSH

∞

Windows

∞

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 using a secure password.

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-pass'. Most standard password prompts.

Targets to prioritize credentials

Any hostnames or IPs or CIDR blocks (in a comma or space separated list in this field) that match a set of credentials

Global Credential Settings

known_hosts file

Add File

Preferred port

22

Client version

OpenSSH_5.0

• Kết quả:

Metasploitable2 - Auth / 192.168.45.140

Configure Audit Trail Launch Report Export

Vulnerabilities 244

Filter Search Vulnerabilities Q 244 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		Host Details
<input type="checkbox"/> CRITICAL	10.0 *	8.9	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : linux, linux-ec2, linux-source-2.6.15 vulnerabil...	Ubuntu Local Security Checks	1	⊙ ✎	IP: 192.168.45.140 MAC: 00:0C:29:92:08:83 00:0C:29:92:08:8D OS: Linux Kernel 2.6.24-16-server on Ubuntu 8.04 Start: Today at 10:32 PM End: Today at 10:40 PM Elapsed: 8 minutes KB: Download
<input type="checkbox"/> CRITICAL	10.0 *	7.4	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 : samba vulnerability (USN-1423-1)	Ubuntu Local Security Checks	1	⊙ ✎	<div>Vulnerabilities</div> <div><div></div><div><div>● Critical</div><div>● High</div><div>● Medium</div><div>● Low</div><div>● Info</div></div></div>
<input type="checkbox"/> CRITICAL	10.0 *	6.9	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : linux-source-2.6.15/22, linux vulnerabilities (USN-714-1)	Ubuntu Local Security Checks	1	⊙ ✎	
<input type="checkbox"/> CRITICAL	10.0 *	6.7	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : gnutils2, gnutils13 vulnerabilities (USN-613-1)	Ubuntu Local Security Checks	1	⊙ ✎	
<input type="checkbox"/> CRITICAL	10.0 *	6.7	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : libxml2 vulnerabilities (USN-644-1)	Ubuntu Local Security Checks	1	⊙ ✎	
<input type="checkbox"/> CRITICAL	10.0 *	6.7	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : linux, linux-source-2.6.15/20/22 vulnerabilities (USN-625-1)	Ubuntu Local Security Checks	1	⊙ ✎	
<input type="checkbox"/> CRITICAL	10.0 *	6.7	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : linux, linux-source-2.6.15 vulnerabilities (USN-894-1)	Ubuntu Local Security Checks	1	⊙ ✎	
<input type="checkbox"/> CRITICAL	10.0 *	6.7	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : dhcp3 vulnerability (USN-803-1)	Ubuntu Local Security Checks	1	⊙ ✎	
<input type="checkbox"/> CRITICAL	10.0 *	6.7	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : libxml2 vulnerabilities (USN-815-1)	Ubuntu Local Security Checks	1	⊙ ✎	
<input type="checkbox"/> CRITICAL	10.0 *	6.7	Ubuntu 7.10 / 8.04 LTS / 8.10 : linux, linux-source-2.6.22 vulnerabilities (USN-751-1)	Ubuntu Local Security Checks	1	⊙ ✎	
<input type="checkbox"/> CRITICAL	10.0 *	6.7	Ubuntu 8.04 LTS / 8.10 / 9.04 : apr vulnerability (USN-813-1)	Ubuntu Local Security Checks	1	⊙ ✎	
<input type="checkbox"/> CRITICAL	10.0 *	6.7	Ubuntu 8.04 LTS / 8.10 / 9.04 : apr-util vulnerability (USN-813-3)	Ubuntu Local Security Checks	1	⊙ ✎	

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

- Nhập tên và ip mục tiêu:

The screenshot shows the 'New Scan / Advanced Scan' window in the Metasploit Framework. The 'Settings' tab is selected, and the 'BASIC' section is expanded. The 'Name' field is filled with 'Metasploitable - Individual'. The 'Description' field is empty. The 'Folder' dropdown is set to 'My Scans'. The 'Targets' field contains the IP address '192.168.45.140'. At the bottom, there are 'Save' and 'Cancel' buttons.

- Để tiết kiệm thời gian và ít để lại dấu vết, chúng ta sẽ tắt Host discovery, vì chúng ta biết được host vẫn còn hoạt động.

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings | Credentials | Plugins

BASIC >

DISCOVERY ▾

- Host Discovery
- Port Scanning
- Service Discovery
- Identity

ASSESSMENT >

REPORT >

ADVANCED >

Remote Host Ping

Ping the remote host ☐ OFF

Fragile Devices

- ☐ Scan Network Printers
- ☐ Scan Novell Netware hosts
- ☐ Scan Operational Technology devices

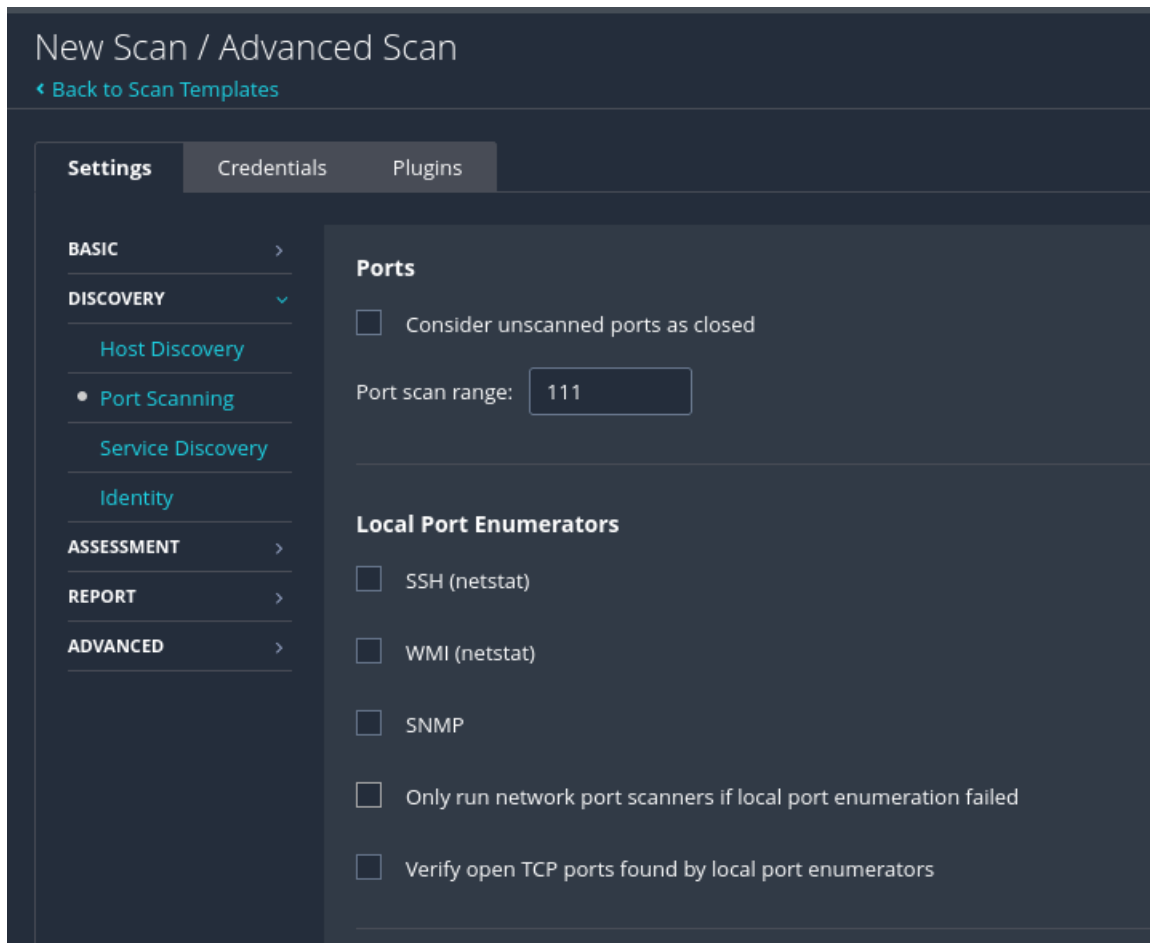
Wake-on-LAN

List of MAC addresses [Add File](#)

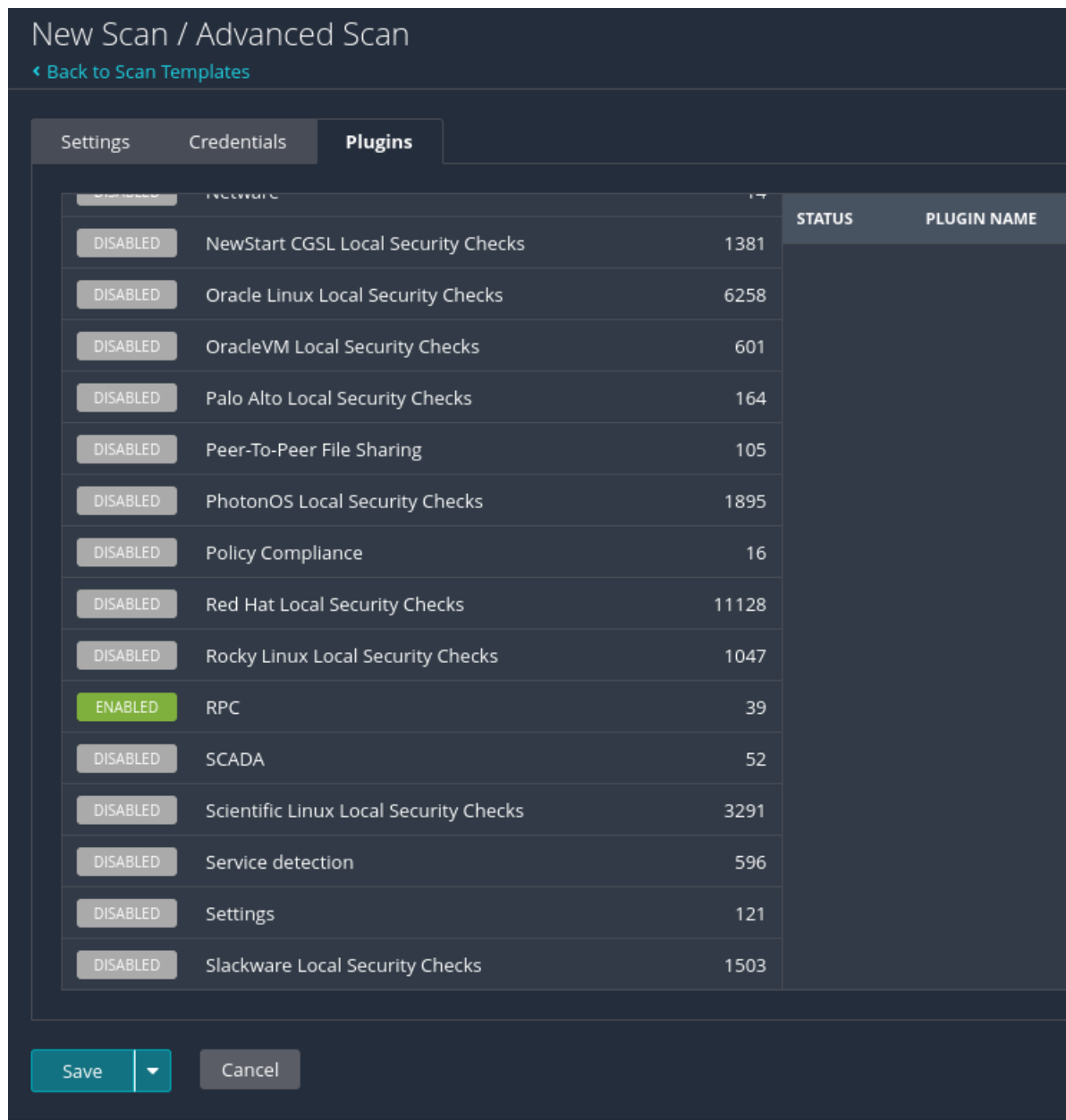
Boot time wait (in minutes)

Save | Cancel

- Vì chúng ta chỉ scan dịch vụ RPC và biết rằng RPC chạy trên TCP port 111, nên chúng ta chỉ scan duy nhất port này



- Sau khi giảm thiểu tối đa các tùy chọn scan, bây giờ tiến hành chọn plugin. Chọn thẻ Plugins và click vào Disable All ở góc phải. Sau đó để tiến hành quét NFS shares, chúng ta sẽ di chuyển đến “RPC” bên cột bên trái và thiết lập “NFS Exported Share Information Disclosure” ở cột bên phải thành Enabled



- Kết quả:

Metasploitable - Individual / 192.168.45.140

Configure Audit Trail Launch Report Export

Vulnerabilities 7


Filter Search Vulnerabilities 7 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	
<input type="checkbox"/> HIGH	7.5		NFS Shares World Readable	RPC	1	
<input type="checkbox"/> INFO			Nessus Scan Information	Settings	1	
<input type="checkbox"/> INFO			Nessus SYN scanner	Port scanners	1	
<input type="checkbox"/> INFO			NFS Share Export List	RPC	1	
<input type="checkbox"/> INFO			RPC portmapper (TCP)	RPC	1	
<input type="checkbox"/> INFO			RPC portmapper Service Detection	RPC	1	

Host Details

IP: 192.168.45.140
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 10:40 PM
End: Today at 10:41 PM
Elapsed: a minute
KB: [Download](#)

Vulnerabilities



● Critical
● High
● Medium
● Low
● Info

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

YÊU CẦU CHUNG

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

Báo cáo:

- File **.DOCX và .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 đã đăng ký với GVHD-TH).
Ví dụ: [NT101.K11.ATCL]-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 bài Lab.**
- 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 được bài thực hành. Khuyến khích:

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

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

HẾT