

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: NT140.012.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.

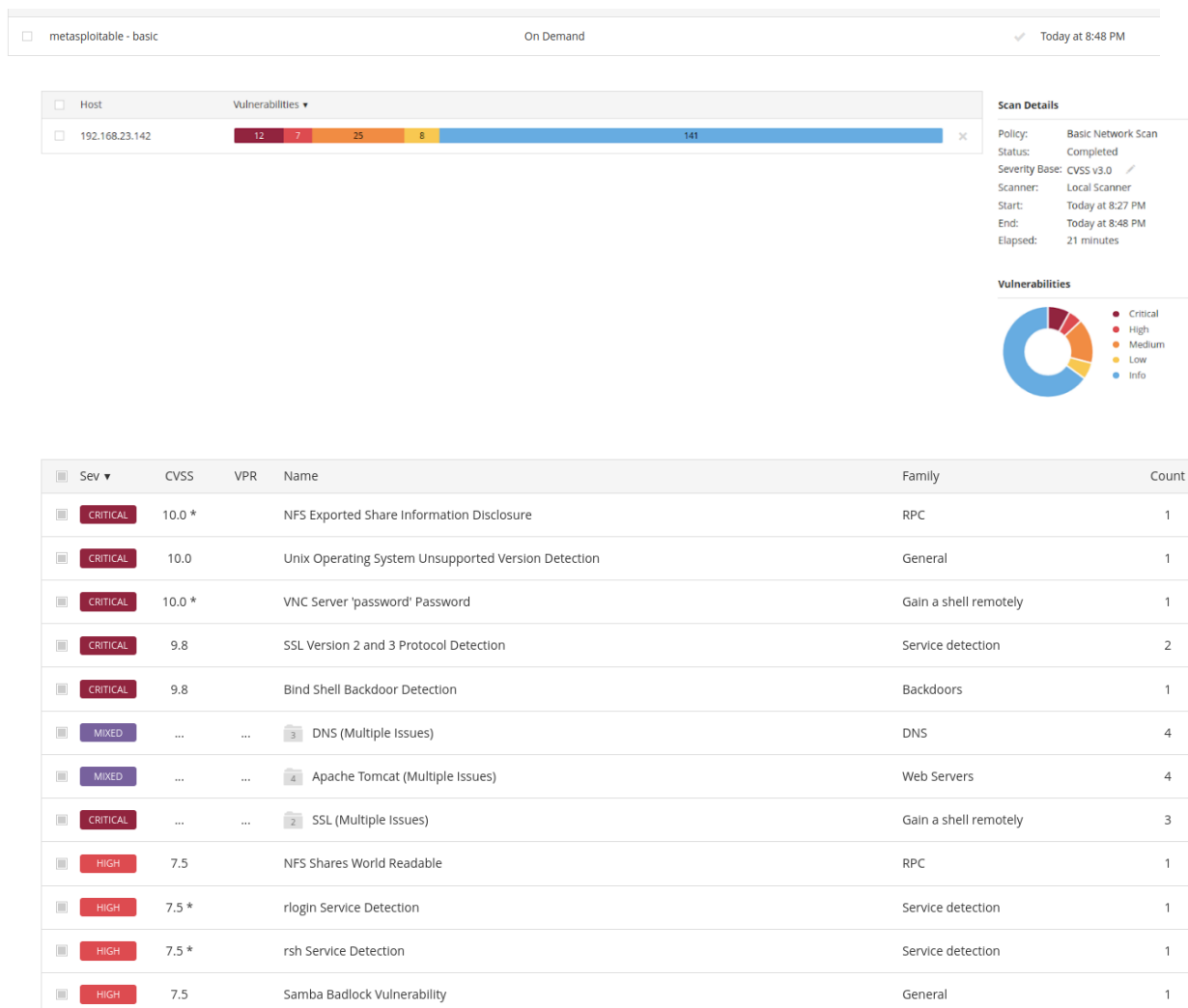
IP victim: 192.168.23.142

```
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:00:08:00:08  
          inet addr:192.168.23.142  Bcast:192.168.23.255
```

Ports

☐ Consider unscanned ports as closed

Port scan range:



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)
705	164.199100010	192.168.23.130	192.168.23.142	TCP	66 38668 → 22 [ACK] Seq=1 Ack=20 Win=64256 Len=0 TSval=31901

PortMap

1329...	86.986755652	192.168.23.130	192.168.23.142	TCP	66 47908 → 2121 [ACK] Seq=1 Ack=60 Win=64256 Len=0 TSval=31901
1329...	87.105990910	192.168.23.130	192.168.23.142	TCP	66 45056 → 111 [RST, ACK] Seq=844 Ack=1121 Win=0 Len=0
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=0
1329...	88.319805014	192.168.23.142	192.168.23.130	TCP	74 41101 → 43658 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0

DISTCC

298	5.064470460	VMware_47:0e:b9	VMware_ea:9c:fc	ARP	60 who has 192.168.23.142
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

Báo cáo môn học
HOC KỲ I – NĂM HỌC 2023-2024

<input type="checkbox"/>	CRITICAL	9.8	SSL Version 2 and 3 Protocol Detection	Service detection	2	⊖	✎
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell Backdoor Detection	Backdoors	1	⊖	✎
<input type="checkbox"/>	HIGH	7.5	NFS Shares World Readable	RPC	1	⊖	✎
<input type="checkbox"/>	HIGH	7.5 *	rlogin Service Detection	Service detection	1	⊖	✎
<input type="checkbox"/>	HIGH	7.5 *	rsh Service Detection	Service detection	1	⊖	✎
<input type="checkbox"/>	HIGH	7.5	Samba Badlock Vulnerability	General	1	⊖	✎
<input type="checkbox"/>	MEDIUM	6.5	TLS Version 1.0 Protocol Detection	Service detection	2	⊖	✎
<input type="checkbox"/>	MEDIUM	6.5	Unencrypted Telnet Server	Misc.	1	⊖	✎
<input type="checkbox"/>	MEDIUM	5.9	SSL Anonymous Cipher Suites Supported	Service detection	1	⊖	✎
<input type="checkbox"/>	MEDIUM	5.9	SSL DROWN Attack Vulnerability (Decrypting RSA w... Plugin ID: 11213 Weakened eNcrypt...	Misc.	1	⊖	✎
<input type="checkbox"/>	MEDIUM	5.3	HTTP TRACE / TRACK Methods Allowed	Web Servers	1	⊕	✎
<input type="checkbox"/>	LOW	3.7	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1	⊖	✎
<input type="checkbox"/>	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 08:00:06:27:00:00
          inet addr:192.168.10.135
```

Settings

Credentials

Plugins

CATEGORIES

Host

Filter Credentials

SNMPv3

SSH

Windows

SSH

User: msfadmin, Auth method: pa...

Authentication method

password

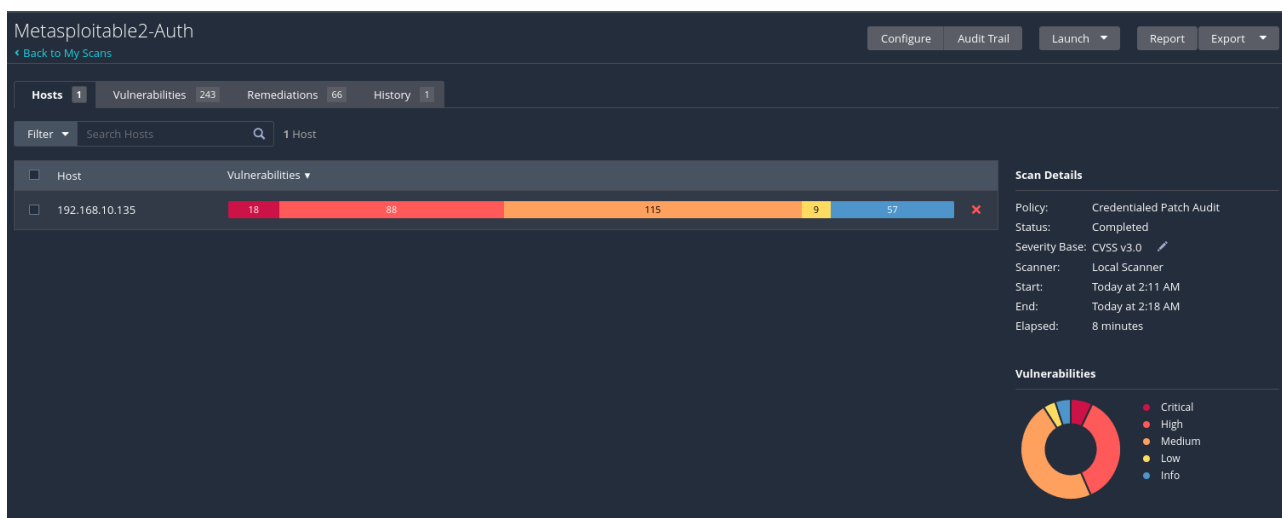
Username

msfadmin

Password (unsafe!)

●●●●●●●●

This password could be compromised if Nessus connects to a rogue SSH server. See the "Global Settings" section below.



Metasploit2-Auth

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 243 Remediations 66 History 1

Filter Search Vulnerabilities 243 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	8.9	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : linux, linux-ec2...	Ubuntu Local Security Checks	1
CRITICAL	10.0 *	7.4	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 : samba vulnerability (USN-142...	Ubuntu Local Security Checks	1
CRITICAL	10.0 *	6.9	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : linux-source-2.6.15/22, linux vulnerabili...	Ubuntu Local Security Checks	1
CRITICAL	10.0 *	6.7	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : gnutls12, gnutls13 vulnerabilities ...	Ubuntu Local Security Checks	1
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
CRITICAL	10.0 *	6.7	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : linux, linux-source-2.6.15/20/22 v...	Ubuntu Local Security Checks	1
CRITICAL	10.0 *	6.7	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : linux, linux-source-2.6.15 v...	Ubuntu Local Security Checks	1
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
CRITICAL	10.0 *	6.7	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : libx11 Plugin ID: 37337 5 (USN-815-1)	Ubuntu Local Security Checks	1
CRITICAL	10.0 *	6.7	Ubuntu 7.10 / 8.04 LTS / 8.10 : linux, linux-source-2.6.22 vulnerabilities (US...	Ubuntu Local Security Checks	1

Scan Details

Policy: Credentialed Patch Audit
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 2:11 AM
End: Today at 2:18 AM
Elapsed: 8 minutes

Vulnerabilities

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

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.

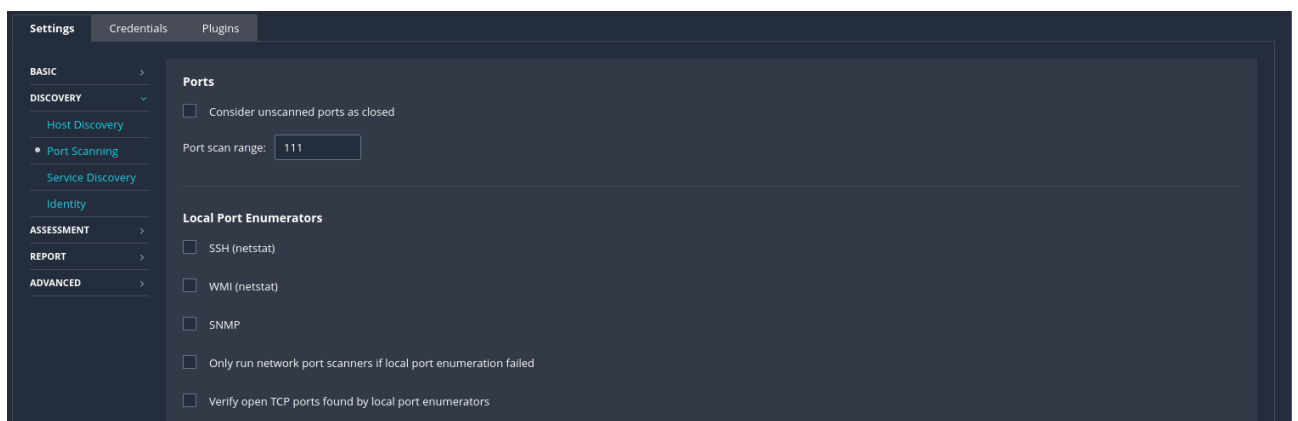
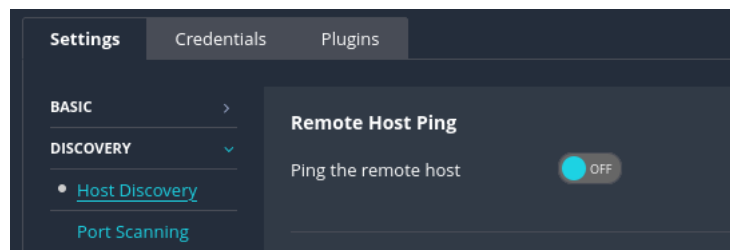
- **Nhược điểm:**
 - Thiếu chi tiết: Quét không thể cung cấp thông tin chi tiết như các lỗ hổng chưa được xác nhận do không có quyền truy cập đầy đủ.
 - Không hiệu quả với kiểm thử chứng thực: Không thể kiểm tra các lỗ hổng chỉ xuất hiện khi đăng nhập vào hệ thống.

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



Settings	Credentials	Plugins		Show Enabled	Show All
DISABLED	OracleVM Local Security Checks	601	DISABLED	Linux Multiple statd Packages Remote Format String	10544
DISABLED	Palo Alto Local Security Checks	164	DISABLED	Linux NFS utils package (nfs-utils) mountd xlog Function Off-by-one Remote Overflow	11800
DISABLED	Peer-To-Peer File Sharing	105	DISABLED	Multiple Vendor NFS CD Command Arbitrary File/Directory Access	11357
DISABLED	PhotonOS Local Security Checks	1895	DISABLED	Multiple Vendor NIS rpc.yppupdated YP Map Update Arbitrary Remote Command Exec...	31683
DISABLED	Policy Compliance	16	DISABLED	Multiple Vendor RPC portmapper Access Restriction Bypass	54586
DISABLED	Red Hat Local Security Checks	11281	DISABLED	Multiple Vendor rpc.nisd Long NIS+ Argument Remote Overflow	10251
DISABLED	Rocky Linux Local Security Checks	1059	ENABLED	NFS Exported Share Information Disclosure	11356
MIXED	RPC	39	DISABLED	NFS portmapper localhost Mount Request Restricted Host Access	11358
DISABLED	SCADA	52	DISABLED	NFS Predictable Filehandles Filesystem Access	11353
DISABLED	Scientific Linux Local Security Checks	3291	DISABLED	NFS Server Superfluous	42255
DISABLED	Service detection	598	DISABLED	NFS Share Export List	10437
DISABLED	Settings	121	DISABLED	NFS Share User Mountable	15984

Metasploitable2-Individual / Plugin #11356

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 3 History 2

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 / :
+ ..
+ .bit
+ boot
+ more...
```

To see debug logs, please visit individual host

Port 2049 / udp / rpc-nfs Hosts 192.168.10.135

Plugin Details

Severity: Critical
ID: 11356
Version: 1.21
Type: remote
Family: RPC
Published: March 12, 2003
Modified: August 30, 2023

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information
Vulnerability Priority Rating (VPR): 5.9

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 S
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?

Settings | Credentials | Plugins

BASIC >

DISCOVERY v

Host Discovery

• Port Scanning

Service Discovery

Ports

☒ Consider unscanned ports as closed

Port scan range: 111

No.	Time	Source	Destination	Protocol	Length	Info
9	0.869877	192.168.10.140	192.168.10.135	TCP	62	23410 → 111 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 S
10	0.870469	192.168.10.135	192.168.10.140	TCP	62	111 → 23410 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
11	0.870680	192.168.10.140	192.168.10.135	TCP	60	23410 → 111 [RST] Seq=1 Win=0 Len=0
18	0.984552	192.168.10.140	192.168.10.135	TCP	74	35380 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
19	0.984905	192.168.10.135	192.168.10.140	TCP	74	111 → 35380 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
20	0.985099	192.168.10.140	192.168.10.135	TCP	66	35380 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
21	0.990051	192.168.10.140	192.168.10.135	RPC	257	Continuation
22	0.990371	192.168.10.135	192.168.10.140	TCP	66	111 → 35380 [ACK] Seq=1 Ack=192 Win=6880 Len=0 TS
23	0.990625	192.168.10.135	192.168.10.140	TCP	66	111 → 35380 [FIN, ACK] Seq=1 Ack=192 Win=6880 Len=0
24	0.993070	192.168.10.140	192.168.10.135	TCP	66	35380 → 111 [ACK] Seq=192 Ack=2 Win=64256 Len=0 T
25	0.995750	192.168.10.140	192.168.10.135	RPC	73	Continuation
26	0.996011	192.168.10.135	192.168.10.140	TCP	54	111 → 35380 [RST] Seq=2 Win=0 Len=0
27	1.001333	192.168.10.140	192.168.10.135	TCP	74	35380 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460

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)*

Settings | Credentials | Plugins

BASIC >

DISCOVERY v

Host Discovery

• Port Scanning

Ports

☐ Consider unscanned ports as closed

Port scan range: 25

Plugin Name	Count	Status
FreeBSD Local Security Checks	5439	DISABLED
FTP	271	DISABLED
Gain a shell remotely	282	MIXED
General	356	DISABLED
Gentoo Local Security Checks	3473	DISABLED
HP-UX Local Security Checks	1983	DISABLED
Huawei Local Security Checks	9680	DISABLED
Junos Local Security Checks	619	DISABLED
MacOS X Local Security Checks	2240	DISABLED
Mandriva Local Security Checks	3641	DISABLED
MarinerOS Local Security Checks	557	DISABLED
Misc.	3572	DISABLED
Cyrus IMAP Server login Command Remote Overflow	11196	DISABLED
Darwin Streaming Server < 5.5.5 Multiple RCE Vulnerabilities	25214	DISABLED
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	32314	DISABLED
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	32321	ENABLED
Dell NetVault Backup 10.0.x < 10.0.5 RCE	84006	DISABLED
Digital Mappings Systems POP3 Server (pop3svr.exe) Multiple Field Remote Overflow	15783	DISABLED
Dropbear SSH Server DSS Verification Failure Remote Privilege Escalation	14234	DISABLED
Ebola AV Daemon < 0.1.5 Authentication Sequence Remote Overflow	11946	DISABLED
EMC AlphaStor Device Manager robotd RCE	33284	DISABLED
EMC AlphaStor Library Manager Remote Code Execution	33285	DISABLED
EMC AutoStart ftAgent Multiple Remote Code Execution Vulnerabilities (ESA-2012-020)	61491	DISABLED
EMC Legato Networker Remote Exec Service Stack Overflow RCE	94163	DISABLED

CRITICAL

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Description
 The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

 The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

 An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution
 Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

See Also
<http://www.nessus.org/u7107f9bdc>
<http://www.nessus.org/u7f14f4224>

Output
 No output recorded.

 To see debug logs, please visit individual host

Port	Hosts
5432 / tcp / postgresql	192.168.10.135
25 / tcp / smtp	192.168.10.135

Plugin Details

Severity: Critical
 ID: 32321
 Version: 1.27
 Type: remote
 Family: Gain a shell remotely
 Published: May 15, 2008
 Modified: November 16, 2020

VPR Key Drivers
 Threat Recency: No recorded events
 Threat Intensity: Very Low
 Exploit Code Maturity: Functional
 Age of Vuln: 730 days +
 Product Coverage: Low
 CVSSv3 Impact Score: 5.9
 Threat Sources: No recorded events

Risk Information
 Vulnerability Priority Rating (VPR): 7.4
 Risk Factor: Critical
 CVSS v2.0 Base Score: 10.0
 CVSS v2.0 Temporal Score: 8.3
 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

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

Settings

Credentials

Plugins

BASIC
DISCOVERY
 Host Discovery
 Port Scanning

Ports
☐ Consider unscanned ports as closed
 Port scan range: 25

Settings

Credentials

Plugins

Show Enabled | Show All

DISABLED	Rocky Linux Local Security Checks	1059	DISABLED	SSH Password Authentication Accepted	149334
DISABLED	RPC	39	DISABLED	SSH Server Type and Version Information	10267
DISABLED	SCADA	52	DISABLED	SSL Anonymous Cipher Suites Supported	31705
DISABLED	Scientific Linux Local Security Checks	3291	DISABLED	SSL Service Requests Client Certificate	35297
MIXED	Service detection	598	ENABLED	SSL Version 2 and 3 Protocol Detection	20007
DISABLED	Settings	121	DISABLED	ssllh Detection	42476
DISABLED	Slackware Local Security Checks	1510	DISABLED	StarTeam Server Detection	31355
DISABLED	SMTP problems	153	DISABLED	Strict Transport Security (STS) Detection	42822
DISABLED	SNMP	34	DISABLED	STUN Detection	45580
DISABLED	Solaris Local Security Checks	3817	DISABLED	Subversion Server Detection	12259
DISABLED	SuSE Local Security Checks	22829	DISABLED	Sun Java System ASP Server Detection	33438
DISABLED	Tenable.ot	1771	DISABLED	Sun Secure Global Software / Tarantella Detection	22478

CRITICAL

SSL Version 2 and 3 Protocol Detection

Description
 The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

 - An insecure padding scheme with CBC ciphers.

 - Insecure session renegotiation and resumption schemes.

 An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

 Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

 NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution
 Consult the application's documentation to disable SSL 2.0 and 3.0.
 Use TLS 1.2 (with approved cipher suites) or higher instead.

Plugin Details

Severity: Critical
 ID: 20007
 Version: 1.34
 Type: remote
 Family: Service detection
 Published: October 12, 2005
 Modified: April 4, 2022

Risk Information
 Risk Factor: Critical
CVSS v3.0 Base Score 9.8
 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
 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

```

Output

- SSLv2 is enabled and the server supports at least one cipher.

Low Strength Ciphers (<= 64-bit key)

Name           Code      KEX      Auth    Encryption      MAC
-----
EXP-RS2-CBC-MD5  RSA(512)  RSA      RC2-CBC(40)    MD5      export
EXP-RS4-MD5      RSA(512)  RSA      RC4(40)        MD5      export
more...

To see debug logs, please visit individual host
Port  Hosts
25/tcp/smtp      192.168.10.135

- SSLv3 is enabled and the server supports at least one cipher.
  Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name           Code      KEX      Auth    Encryption      MAC
-----
EXP-RS2-CBC-MD5  RSA(512)  RSA      RC2-CBC(40)    MD5      export
EXP-RS4-MD5      RSA(512)  RSA      RC4(40)        MD5      export
more...

To see debug logs, please visit individual host
Port  Hosts
5432/tcp/postgresql 192.168.10.135

```

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](https://github.com/1N3/Sn1per))

```

(root@kali)-[~]
# sniper --help
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]

  SNIPER

+ --=[ https://snipersecurity.com
+ --=[ Sniper v9.2 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>

[*] FULLPORTONLY SCAN MODE
sniper -t <TARGET> -fp

[*] WEB MODE - PORT 80 + 443 ONLY!
sniper -t <TARGET> -m web

[*] HTTP WEB PORT MODE
sniper -t <TARGET> -m webporthttp -p <port>

[*] HTTPS WEB PORT MODE
sniper -t <TARGET> -m webporthttps -p <port>

```

IP của máy Metasploitable 2: 192.168.10.135

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 82:00:00:08:00:08
          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] required:
[*] 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://snipersecurity.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: *[NT521.011.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