

BÁO CÁO THỰC HÀNH

Môn học: An toàn Mạng máy tính

Tên chủ đề: Quét lỗ hổng bảo mật

GVHD: Tô Trọng Nghĩa

Nhóm: 18

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.011.ANTT.1

| STT | Họ và tên | MSSV | Email |
|-----|---------------------|----------|------------------------|
| 1 | Nguyễn Lê Thảo Ngọc | 21521191 | 21521191@gm.uit.edu.vn |
| 2 | Trần Lê Minh Ngọc | 21521195 | 21521195@gm.uit.edu.vn |

2. NỘI DUNG THỰC HIỆN:

| STT | Nội dung | Tình trạng | Trang |
|------------------|---------------------------|------------|-------|
| 1 | Làm 11 câu bài tập về nhà | 100% | |
| Điểm tự đánh giá | | | 9/10 |

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

I. Quét lỗ hổng sử dụng công cụ Nessus

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

Chạy máy ảo Metasploitable 2 với địa chỉ IP là 192.168.184.137

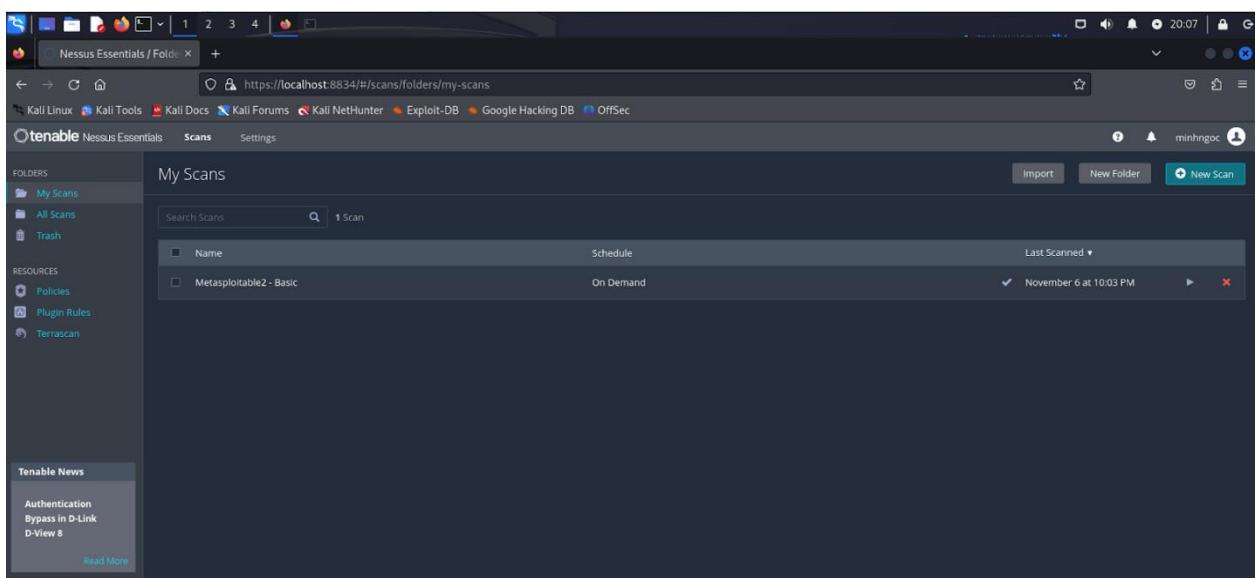
```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:dd:98:5e  
          inet addr:192.168.184.137 Bcast:192.168.184.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fedd:985e/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
          RX packets:51 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:62 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:5160 (5.0 KB) TX bytes:6668 (6.5 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:92 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)  
msfadmin@metasploitable:~$
```

a) Cài đặt Nessus

Khởi động dịch vụ Nessusd

```
(ngoc㉿ngoc) [~] $ /bin/systemctl start nessusd.service
Scans Settings
(ngoc㉿ngoc) [~] $ systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset>
   Active: active (running) since Tue 2023-11-07 20:02:18 +07; 16s ago
     Main PID: 4205 (nessus-service)
        Tasks: 19 (limit: 2216)
      Memory: 429.1M
         CPU: 39.240s
      CGroup: /system.slice/nessusd.service
              └─4205 /opt/nessus/sbin/nessus-service -q
              ├─4209 nessusd -q
Metasploitable2 - Basic Sched On De
Nov 07 20:02:18 ngoc systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
lines 1-12/12 (END)
```

Sau khi khởi động Nessus, mở trình duyệt và truy cập vào đường dẫn <https://localhost:8834/>.

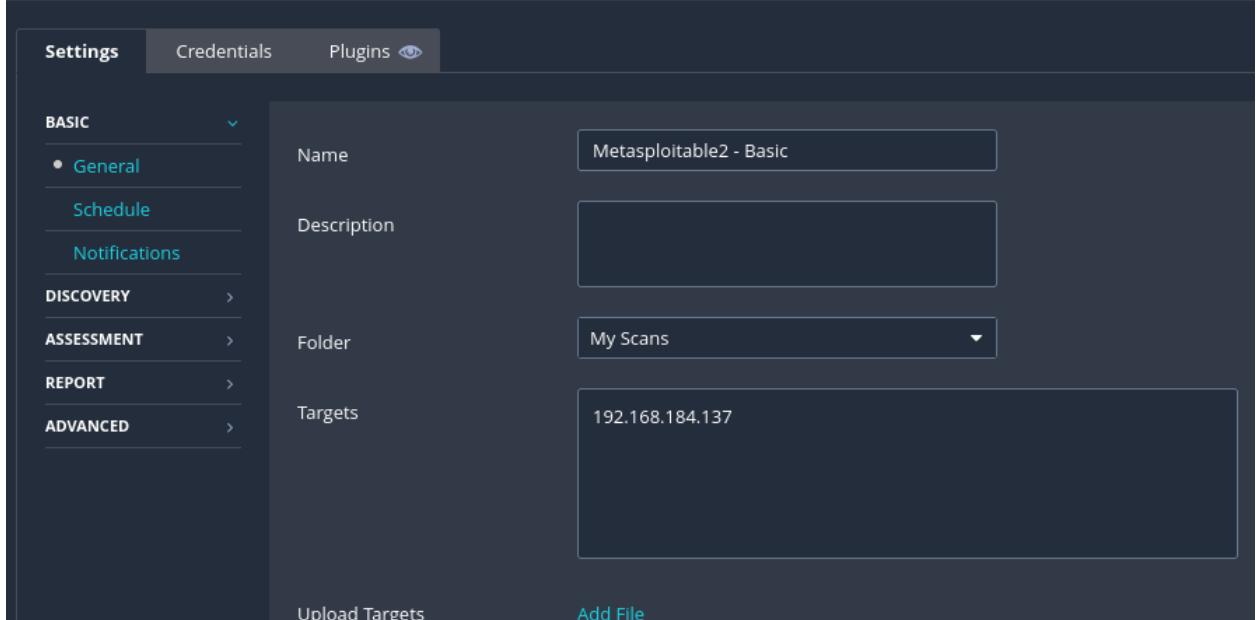


b) Khai báo đối tượng

Thực hiện quét máy Metasploitable2, có địa chỉ IP là 192.168.184.137. Chúng ta sẽ nhập “Metasploitable2 – Basic” trong trường Name và địa chỉ IP trong trường Targets:

Metasploitable2 - Basic / Configuration

[◀ Back to Scan Report](#)



c) Cấu hình các định nghĩa quét (Scan Definitions)

Thay đổi cấu hình trong mục Discovery để thực hiện quét tất cả các port.

Metasploitable2 - Basic / Configuration

[◀ Back to Scan Report](#)

Settings **Credentials** **Plugins**

BASIC >

DISCOVERY > **Scan Type** **Custom**

- [Host Discovery](#)
- [Port Scanning](#)
- [Service Discovery](#)
- [Identity](#)

ASSESSMENT >

REPORT >

ADVANCED >

Choose your own discovery settings.

Cấu hình Scanner sử dụng loại Custom Port

Metasploitable2 - Basic / Configuration

[◀ Back to Scan Report](#)

Settings **Credentials** **Plugins**

BASIC >

DISCOVERY > **Ports**

- [Host Discovery](#)
- Port Scanning**
- [Service Discovery](#)

Consider unscanned ports as closed

Port scan range: **0-65535**

Cấu hình Scanner để quét tất cả các port

d) Quét lỗ hổng không sử dụng tài khoản chứng thực

Sau khi quét hoàn tất, trạng thái sẽ chuyển sang Completed

| Name | Schedule | Last Scanned |
|-------------------------|-----------|-------------------|
| Metasploitable2 - Basic | On Demand | Today at 10:03 PM |

Quá trình scan hoàn tất

Sau khi scan hoàn tất, click vào tên scan, “Metasploitable2 – Basic” để hiển thị danh sách các host được khám phá trong quá trình scan và tóm tắt các lỗ hổng tồn tại.

Metasploitable2 - Basic

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: November 6 at 9:44 PM
- End: November 6 at 10:03 PM
- Elapsed: 20 minutes

Vulnerabilities

| Severity | Count |
|----------|-------|
| Critical | 13 |
| High | 7 |
| Medium | 25 |
| Low | 8 |
| Info | 144 |

Giao diện tổng quan

Chúng ta có thể nhấp vào địa chỉ IP hoặc tên máy chủ để hiển thị các lỗ hổng được phát hiện đối với mục tiêu đó.

Metasploitable2 - Basic / 192.168.184.137

Host Details

- IP: 192.168.184.137
- MAC: 00:0C:29:DD:98:5E
- OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- Start: November 6 at 9:44 PM
- End: November 6 at 10:03 PM
- Elapsed: 20 minutes
- KB: Download

Vulnerabilities

| Severity | Count |
|----------|---|
| Critical | 10.0 * |
| High | 6.7 |
| Medium | NFS Exported Share Information Disclosure |
| Low | General |
| Info | RPC |
| Critical | 10.0 |
| High | Unix Operating System Unsupported Version Detection |
| Medium | General |
| Low | Backdoors |
| Info | Gain a shell remotely |
| Critical | 10.0 * |
| High | 7.4 |
| Medium | UnrealIRCd Backdoor Detection |
| Low | Service detection |
| Info | VNC Server 'password' Password |
| Critical | 10.0 * |
| High | 9.8 |
| Medium | SSL Version 2 and 3 Protocol Detection |
| Low | General |
| Info | Bind Shell Backdoor Detection |
| Mixed | ... |
| High | ... |
| Medium | DNS (Multiple Issues) |
| Low | Backdoors |
| Info | DNS |
| Mixed | ... |
| High | ... |
| Medium | Apache Tomcat (Multiple Issues) |
| Low | General |
| Info | Web Servers |

Xem các lỗ hổng đã được phát hiện

Chúng ta có thể thực hiện lọc các lỗ hổng theo mức độ ảnh hưởng, CVE, khả năng khai thác, và nhiều hơn thế nữa. Để hiển thị các lỗ hổng có thể dẫn đến kiểm soát máy chủ mục tiêu, chúng ta có thể click Filter và thay đổi giá trị lọc thành "Exploit Available", giữ nguyên các giá trị mặc định của "is equal to" và "true". Sau khi cấu hình xong, click vào Apply.

Filters

Save this filter:

Match of the following:

Lọc các lỗ hổng với các lỗi khai thác

Nhóm 18

Kết quả lọc sẽ chỉ hiển thị các lỗ hổng theo nhóm được định nghĩa bởi Nessus

| Vulnerabilities 11 | | | | | | | | |
|--------------------|--------|------------------------|---|-----------------------|-------|-------|--------------------------|--------------------------|
| | Filter | Search Vulnerabilities | Q | 11 Vulnerabilities | | | | |
| Sev | CVSS | VPR | Name | Family | Count | Count | Disable Groups | Show Snoozed |
| □ CRITICAL | 10.0 * | 6.7 | NFS Exported Share Information Disclosure | RPC | 1 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| □ CRITICAL | 10.0 * | 7.4 | UnrealIRCd Backdoor Detection | Backdoors | 1 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| □ CRITICAL | 9.8 | 9.0 | Apache Tomcat AJP Connector Request Injection (Ghostcat) | Web Servers | 1 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| □ CRITICAL | 9.1 | 6.0 | Multiple Vendor DNS Query ID Field Prediction Cache Poisoning | DNS | 1 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| □ CRITICAL | ... | ... | SSL (Multiple Issues) | Gain a shell remotely | 3 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |

Danh sách lỗ hổng được phân loại theo nhóm

Trong khi việc gom nhóm có thể hữu ích, chúng ta sẽ click vào biểu tượng hình bánh răng bên góc phải của bảng và chọn Disable Groups.

| Vulnerabilities 11 | | | | | | | | |
|--------------------|--------|------------------------|---|--------------------|--------|-------|--------------------------------|--------------------------------|
| | Filter | Search Vulnerabilities | Q | 11 Vulnerabilities | Family | Count | Count | Disable Groups Show Snoozed |
| Sev | CVSS | VPR | Name | Family | Count | Count | Disable Groups Show Snoozed | |
| □ CRITICAL | 10.0 * | 6.7 | NFS Exported Share Information Disclosure | RPC | 1 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| □ CRITICAL | 10.0 * | 7.4 | UnrealIRCd Backdoor Detection | Backdoors | 1 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |

Vô hiệu hóa tính năng gom nhóm

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 tiến hành quét máy Metasploitable 2.

| No. | Time | Source | Destination | Protocol | Length Info |
|-----|-------------|-----------------|-----------------|----------|---|
| 52 | 6.485902613 | VMware_dd:98:5e | 192.168.184.137 | ARP | 62 192.168.184.137 is at 00:0c:29:d8:98:5e |
| 53 | 6.485913199 | 192.168.184.133 | 192.168.184.137 | TCP | 76 51128 - 80 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM Tsvl=1596450438 Tscr=0 WS=128 |
| 54 | 6.48591832 | 192.168.184.133 | 192.168.184.137 | TCP | 76 39698 - 81 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM Tsvl=1596450439 Tscr=0 WS=128 |
| 55 | 6.485989939 | 192.168.184.133 | 192.168.184.137 | TCP | 76 45572 - 8009 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM Tsvl=1596450439 Tscr=0 WS=128 |
| 56 | 6.486418162 | 192.168.184.137 | 192.168.184.133 | TCP | 76 80 - 51128 [SYN, ACK] Seq=0 Ack=1 Win=0 MSS=1460 SACK_PERM Tsvl=11437 Tscr=1596450438 WS=32 |
| 57 | 6.486418245 | 192.168.184.137 | 192.168.184.133 | TCP | 62 81 - 39698 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 58 | 6.486418581 | 192.168.184.137 | 192.168.184.133 | TCP | 76 8009 - 45572 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=11437 Tscr=1596450439 WS=32 |
| 59 | 6.486494792 | 192.168.184.133 | 192.168.184.137 | TCP | 68 51128 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=1596450439 Tscr=11437 |
| 60 | 6.486504226 | 192.168.184.133 | 192.168.184.137 | TCP | 68 45572 - 8009 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=1596450440 Tscr=11437 |
| 61 | 6.543895499 | 192.168.184.133 | 192.168.184.137 | HTTP | 88 GET / HTTP/1.0 |
| 62 | 6.543895212 | 192.168.184.137 | 192.168.184.133 | TCP | 68 80 - 51128 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 Tsvl=11443 Tscr=1596450437 |
| 63 | 6.548776362 | 127.0.0.1 | 127.0.0.1 | TCP | 76 56406 - 8834 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM Tsvl=2488759723 Tscr=0 WS=128 |
| 64 | 6.548798156 | 127.0.0.1 | 127.0.0.1 | TCP | 76 8834 - 56406 [SYN, ACK] Seq=0 Win=65493 Len=0 MSS=65493 SACK_PERM Tsvl=2488759723 Tscr=2488759723 |
| 65 | 6.548817294 | 127.0.0.1 | 127.0.0.1 | TCP | 68 56406 - 8834 [ACK] Seq=1 Ack=1 Win=65536 Len=0 Tsvl=2488759723 Tscr=2488759723 |
| 66 | 6.554276642 | 127.0.0.1 | 127.0.0.1 | TLSv1.3 | 585 Client Hello |

- Các bước mà Nessus đã thực hiện để hoàn tất quá trình quét.

Thực hiện kết nối trên các port của TCP sau đó quét các lỗ hổng trên các port tìm được. VD port 80

| No. | Time | Source | Destination | Protocol | Length Info |
|-----|-------------|-----------------|-----------------|----------|--|
| 53 | 6.485913199 | 192.168.184.133 | 192.168.184.137 | TCP | 76 51128 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=1596450438 Tscr=0 WS=128 |
| 54 | 6.485951832 | 192.168.184.133 | 192.168.184.137 | TCP | 76 39698 - 81 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=1596450439 Tscr=0 WS=128 |
| 55 | 6.485989939 | 192.168.184.133 | 192.168.184.137 | TCP | 76 45572 - 8009 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=1596450439 Tscr=0 WS=128 |
| 56 | 6.486418162 | 192.168.184.137 | 192.168.184.133 | TCP | 76 80 - 51128 [SYN, ACK] Seq=0 Ack=1 Win=0 MSS=1460 SACK_PERM Tsvl=11437 Tscr=1596450438 WS=32 |
| 57 | 6.486418245 | 192.168.184.137 | 192.168.184.133 | TCP | 62 81 - 39698 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 58 | 6.486418581 | 192.168.184.137 | 192.168.184.133 | TCP | 76 8009 - 45572 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=11437 Tscr=1596450439 WS=32 |
| 59 | 6.486494792 | 192.168.184.133 | 192.168.184.137 | TCP | 68 51128 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=1596450439 Tscr=11437 |
| 60 | 6.486504226 | 192.168.184.133 | 192.168.184.137 | HTTP | 88 GET / HTTP/1.0 |
| 61 | 6.543895499 | 192.168.184.133 | 192.168.184.137 | TCP | 68 80 - 51128 [SYN, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=1596450440 Tscr=11437 |
| 62 | 6.544225212 | 192.168.184.137 | 192.168.184.133 | TCP | 68 80 - 51128 [SYN, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=1596450440 Tscr=11437 |
| 63 | 6.717924126 | 192.168.184.137 | 192.168.184.133 | TCP | 68 49 - 51128 [PSH, ACK] Seq=1 Ack=1 Win=5792 Len=6 Tsvl=11443 Tscr=1596450497 [TCP segment of a retransmission] |
| 64 | 6.717924729 | 192.168.184.137 | 192.168.184.133 | TCP | 495 80 - 51128 [PSH, ACK] Seq=582 Ack=19 Win=5792 Len=6 Tsvl=11443 Tscr=1596450497 [TCP segment of a retransmission] |
| 65 | 6.717975159 | 192.168.184.133 | 192.168.184.137 | TCP | 68 51128 - 80 [ACK] Seq=19 Ack=582 Win=64128 Len=0 Tsvl=1596450671 Tscr=11469 |
| 66 | 6.718089721 | 192.168.184.133 | 192.168.184.137 | TCP | 68 51128 - 80 [ACK] Seq=19 Ack=99 Win=64128 Len=0 Tsvl=1596450671 Tscr=11469 |
| 67 | 6.718327835 | 192.168.184.137 | 192.168.184.133 | TCP | 135 80 - 51128 [PSH, ACK] Seq=99 Ack=19 Win=5792 Len=67 Tsvl=11460 Tscr=1596450671 [TCP segment of a retransmission] |
| 68 | 6.718340254 | 192.168.184.133 | 192.168.184.137 | TCP | 68 51128 - 80 [ACK] Seq=19 Ack=1866 Win=64128 Len=0 Tsvl=1596450671 Tscr=11468 |
| 69 | 6.724616662 | 192.168.184.137 | 192.168.184.133 | HTTP | 68 HTTP/1.1 200 OK (text/html) |
| 70 | 6.724712856 | 192.168.184.133 | 192.168.184.137 | TCP | 68 51128 - 80 [RST, ACK] Seq=19 Ack=1067 Win=64128 Len=0 Tsvl=1596450678 Tscr=11461 |

Port 445

| No. | Time | Source | Destination | Protocol | Length Info |
|-----|--------------|-----------------|-----------------|----------|--|
| 98 | 6.833171954 | 192.168.184.133 | 192.168.184.137 | TCP | 76 60092 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=1596450766 Tscr=0 WS=128 |
| 99 | 6.833833104 | 192.168.184.137 | 192.168.184.133 | TCP | 76 445 - 60092 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=11470 Tscr=15964 |
| 100 | 6.833874750 | 192.168.184.133 | 192.168.184.137 | TCP | 68 60092 - 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=1596450767 Tscr=11470 |
| 101 | 6.8314227195 | 192.168.184.133 | 192.168.184.137 | SMB | 243 Negotiate Protocol Request |
| 102 | 6.814492846 | 192.168.184.137 | 192.168.184.133 | TCP | 68 445 - 60092 [ACK] Seq=1 Ack=176 Win=6880 Len=0 Tsvl=11470 Tscr=1596450767 |
| 103 | 6.818141833 | 192.168.184.137 | 192.168.184.133 | SMB | 199 Negotiate Protocol Response |
| 104 | 6.818205382 | 192.168.184.133 | 192.168.184.137 | TCP | 68 60092 - 445 [ACK] Seq=176 Ack=132 Win=64128 Len=0 Tsvl=1596450771 Tscr=11470 |
| 105 | 6.818439431 | 192.168.184.133 | 192.168.184.137 | TCP | 68 60092 - 445 [RST, ACK] Seq=176 Ack=132 Win=64128 Len=0 Tsvl=1596450771 Tscr=11470 |
| 106 | 6.8206727807 | 192.168.184.133 | 192.168.184.137 | TCP | 76 33996 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=1596450774 Tscr=0 WS=128 |
| 107 | 6.821621977 | 192.168.184.137 | 192.168.184.133 | TCP | 76 139 - 33996 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=11470 Tscr=1596450774 |
| 108 | 6.821661341 | 192.168.184.133 | 192.168.184.137 | TCP | 68 33996 - 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=1596450774 Tscr=11470 |
| 109 | 6.821626115 | 192.168.184.133 | 192.168.184.137 | NBSS | 140 Session request, to Nessus112892840>30< from <20> |
| 110 | 6.821346226 | 192.168.184.137 | 192.168.184.133 | TCP | 68 139 - 33996 [ACK] Seq=1 Ack=73 Win=5792 Len=0 Tsvl=11470 Tscr=1596450774 |
| 111 | 6.823997780 | 192.168.184.137 | 192.168.184.133 | NBSS | 72 Positive session response |
| 112 | 6.824061678 | 192.168.184.133 | 192.168.184.137 | TCP | 68 33996 - 139 [ACK] Seq=73 Ack=5 Win=64256 Len=0 Tsvl=1596450777 Tscr=11471 |
| 113 | 6.824166366 | 192.168.184.133 | 192.168.184.137 | TCP | 68 33996 - 139 [RST, ACK] Seq=73 Ack=5 Win=64256 Len=0 Tsvl=1596450777 Tscr=11471 |

3. Quét lại nhưng quét thêm port UDP.

- Chọn thêm UDP trong phần Discovery.

The screenshot shows the Metasploit Framework's configuration interface. In the 'Discovery' section, the 'TCP' checkbox is checked, and the 'UDP' checkbox is also checked. Below each protocol section are four detection options: 'Override automatic firewall detection', 'Use soft detection' (selected), 'Use aggressive detection', and 'Disable detection'. At the bottom of the 'UDP' section, a note states: 'Due to the nature of the protocol, it is generally not possible to produce reliable results. Consider using the netstat or SNMP modules'.

| Name | Schedule | Last Scanned |
|-------------------------|-----------|------------------------|
| Metasploitable 2 - UDP | On Demand | Today at 9:22 PM |
| Metasploitable2 - Basic | On Demand | November 6 at 10:03 PM |

Quá trình scan hoàn tất

Sau khi scan hoàn tất, click vào tên scan, “Metasploitable 2 – UDP” để hiển thị danh sách các host được khám phá trong quá trình scan và tóm tắt các lỗ hổng tồn tại.

The screenshot shows the 'Scan Details' page for the 'Metasploitable 2 - UDP' scan. The scan was completed successfully on November 7 at 9:22 PM, using a Local Scanner, with a duration of 20 minutes. The 'Vulnerabilities' section shows a total of 144 vulnerabilities across 1 host, with a distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue). A pie chart visualizes this distribution.

Giao diện tổng quan



Chúng ta có thể nhấp vào địa chỉ IP hoặc tên máy chủ để hiển thị các lỗ hổng được phát hiện đối với mục tiêu đó.

Xem các lỗ hổng đã được phát hiện

- Thực hiện bắt wireshark

e) Quét lỗ hổng sử dụng tài khoản chứng thực

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

Chúng ta sẽ sử dụng template Credentialled Patch Audit, được cấu hình sẵn để thực hiện kiểm tra bảo mật cục bộ đối với máy mục tiêu. Tương tự như Basic Network Scan, chúng ta cần cung cấp tên và mục tiêu cần quét.

Cấu hình cơ bản của Authenticated Scan

Tiếp theo, chọn thẻ Credentials và chọn loại SSH. Trong mục Authentication method, chọn password, thiết lập username là “msfadmin” và password là “msfadmin”.

Nhập thông tin tài khoản SSH

Bắt đầu quá trình quét

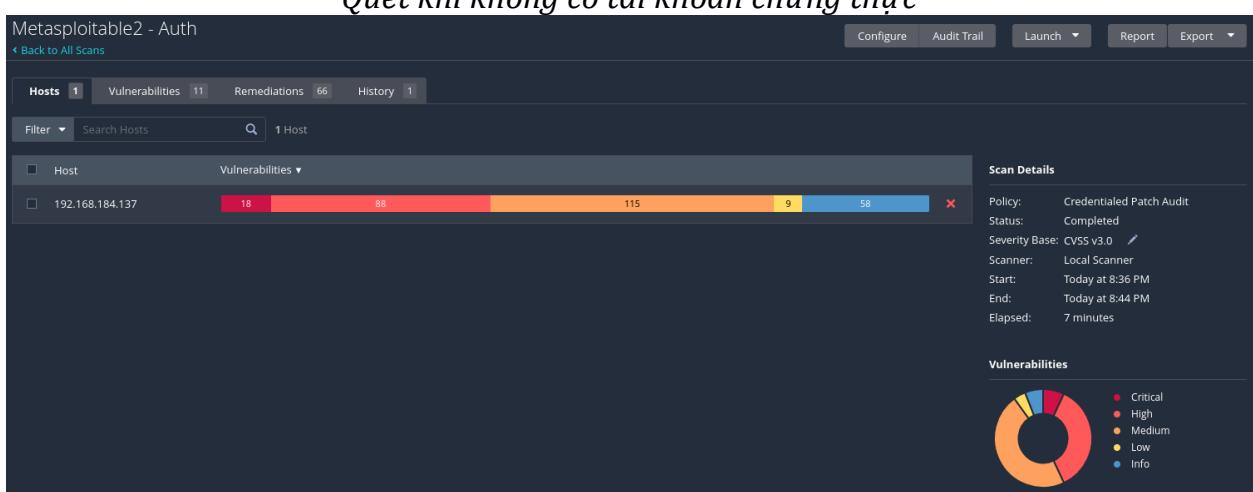
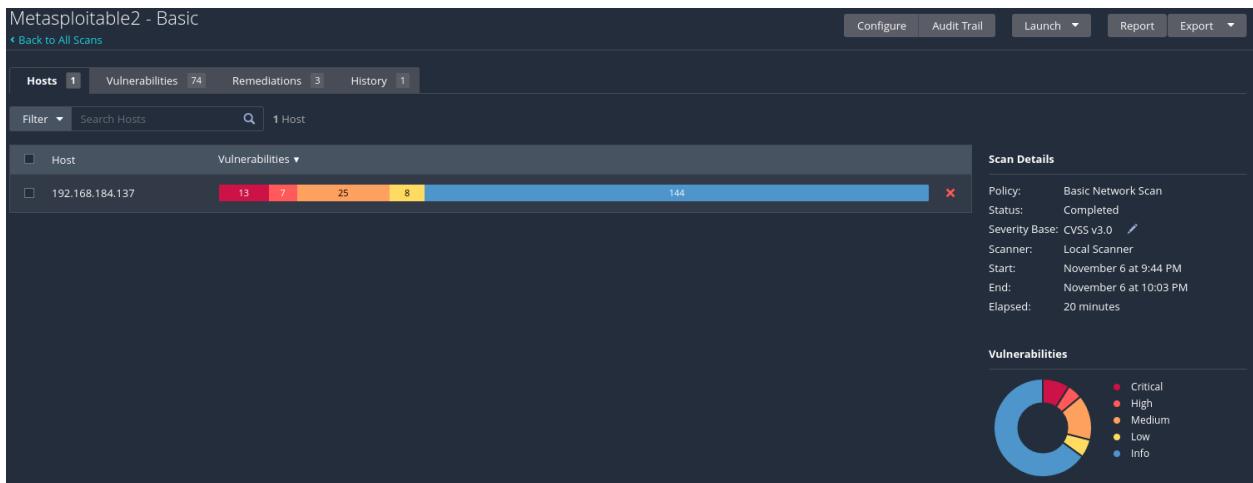
Thực hiện scan mục tiêu có sử dụng tài khoản chứng thực

Sau khi scan chuyển sang trạng thái “Completed”, chúng ta có thể click vào tên scan và mở danh sách các host và click vào địa chỉ IP của máy metasploitable 2, kết quả sẽ hiển thị danh sách các lỗ hổng được khai phá có thể được khai thác trên máy chủ.

Danh sách các lỗ hổng khi quét có tài khoản chứng thực

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

Nhóm 18



- Ta có thể dễ dàng nhìn thấy được khi quét máy Metasploitable 2 với tài khoản chứng thực, Nessusd quét được nhiều lỗ hỏng hơn nhiều so với không có tài khoản chứng thực.
 - Không có tài khoản chứng thực:
 - 13 critical
 - 7 high
 - 25 medium
 - 8 low
 - 144 info
 - Có tài khoản chứng thực:
 - 18 critical
 - 88 high
 - 115 medium
 - 9 low
 - 58 info
- Thời gian quét cũng nhanh hơn (không có tài khoản chứng thực: 20 phút, có tài khoản chứng thực: 7 phút).

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

Quét có tài khoản chứng thực:

- **Ưu điểm:**
 - Hiệu suất cao hơn: Nessus có thể truy cập vào hệ thống bên trong để thu thập thông tin chi tiết về các ứng dụng, dịch vụ và lỗ hổng. Điều này cho phép Nessus tạo ra báo cáo chính xác hơn và chi tiết hơn về lỗ hổng.
 - Phát hiện các lỗ hổng ẩn: Quét có tài khoản chứng thực có khả năng phát hiện các lỗ hổng ẩn mà không thể được phát hiện thông qua quét không chứng thực.
 - Phân loại lỗ hổng: Nessus có khả năng phân loại lỗ hổng theo mức độ nghiêm trọng.
- **Nhược điểm:**
 - Đòi hỏi quyền truy cập: Quét có tài khoản chứng thực yêu cầu quyền truy cập vào hệ thống, điều này có thể gây ra rủi ro an ninh nếu không được thực hiện cẩn thận.
 - Đòi hỏi thời gian và công sức: Quét có tài khoản chứng thực thường tốn nhiều thời gian hơn để cấu hình và thực hiện do cần phải xác định tài khoản và mật khẩu chứng thực.

Quét không có tài khoản chứng thực:

- **Ưu điểm:**
 - Dễ triển khai: Quét không chứng thực dễ dàng triển khai hơn vì không cần xác định tài khoản chứng thực.
 - Nhanh chóng: Quét không chứng thực nhanh chóng hơn vì không cần thiết lập quyền truy cập.
- **Nhược điểm:**
 - Thông tin hạn chế: Nessus sẽ chỉ thu thập thông tin mà có thể truy cập từ bên ngoài hệ thống, giới hạn khả năng phát hiện lỗ hổng và cung cấp thông tin chi tiết.
 - Khả năng sai sót cao: Quét không chứng thực có thể dẫn đến việc báo cáo lỗ hổng không chính xác hoặc thiếu sót nếu hệ thống được cấu hình đặc biệt để che giấu thông tin lỗ hổng.

f) Quét với Plugin được chỉ định

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

Lần này, chúng ta sẽ sử dụng template Advanced Scan. Tương tự, cũng đặt tên và đổi tượng cần scan

Nhóm 18

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Metasploitable2 - Individual

Description:

Folder: My Scans

Targets: 192.168.184.137

Thiết lập tên và đối tượng cần quét

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

Remote Host Ping

Ping the remote host

Tắt tính năng Host Discovery

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

BASIC

DISCOVERY

- Host Discovery
- Port Scanning (selected)
- Service Discovery
- Identity

ASSESSMENT

REPORT

ADVANCED

Ports

Consider unscanned ports as closed

Port scan range: 111

Local Port Enumerators

SSH (netstat)

WMI (netstat)

SNMP

Only run network port scanners if local port enumeration failed

Verify open TCP ports found by local port enumerators

Tắt hết các port không cần thiết

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

| STATUS | PLUGIN FAMILY | LOCKED | TOTAL | STATUS | PLUGIN NAME | PLUGIN ID |
|----------|------------------------------------|--------|-------|--------|-------------|-----------|
| DISABLED | AIX Local Security Checks | | 11532 | | | |
| DISABLED | Alma Linux Local Security Checks | | 1103 | | | |
| DISABLED | Amazon Linux Local Security Checks | | 3980 | | | |
| DISABLED | Backdoors | | 123 | | | |
| DISABLED | Brute force attacks | | 26 | | | |
| DISABLED | CentOS Local Security Checks | | 4270 | | | |
| DISABLED | CGI abuses | | 5374 | | | |
| DISABLED | CGI abuses : XSS | | 703 | | | |
| DISABLED | CISCO | | 2342 | | | |
| DISABLED | Databases | | 950 | | | |

Tắt hết tất cả các plugin

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 và Save

Nhóm 18

| New Scan / Advanced Scan | | | Disable All | Enable All |
|--------------------------|--|---------|--------------|--|
| < Back to Scan Templates | | | Show Enabled | Show All |
| Settings | Credentials | Plugins | | |
| DISABLED | Red Hat Local Security Checks | 11033 | DISABLED | IRIX rpc.ypasswd Unspecified Remote Overflow |
| DISABLED | Rocky Linux Local Security Checks | 765 | DISABLED | JetBrains TeamCity Agent XML-RPC Port RCE |
| MIXED | RPC | 39 | DISABLED | Linux Multiple statd Packages Remote Format String |
| DISABLED | SCADA | 52 | DISABLED | Linux NFS utils package (nfs-utils) mount xlog Function Off-by-one Remote Overflow |
| DISABLED | Scientific Linux Local Security Checks | 3291 | DISABLED | Multiple Vendor NFS CD Command Arbitrary File/Directory Access |
| DISABLED | Service detection | 595 | DISABLED | Multiple Vendor NIS rpc.ypupdated YP Map Update Arbitrary Remote Command Exec... |
| DISABLED | Settings | 121 | DISABLED | Multiple Vendor RPC portmapper Access Restriction Bypass |
| DISABLED | Slackware Local Security Checks | 1501 | DISABLED | Multiple Vendor rpc.nisid Long NIS+ Argument Remote Overflow |
| DISABLED | SMTP problems | 153 | ENABLED | NFS Exported Share Information Disclosure |
| DISABLED | SNMP | 33 | DISABLED | NFS portmapper localhost Mount Request Restricted Host Access |
| DISABLED | Solaris Local Security Checks | 3817 | DISABLED | NFS Predictable Filehandles Filesystem Access |

Bật plugin NFS

Sau khi trạng thái quét chuyển sang “Completed”, chúng ta có thể click vào tên scan, sau đó địa chỉ IP máy mục tiêu. Di chuyển đến lỗ hổng Critical duy nhất và click vào để hiển thị chi tiết thông tin lỗ hổng.

Metasploitable2 - Individual / Plugin #11356

< Back to Vulnerabilities

Vulnerabilities 3

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
- ...
more...
```

Xem kết quả scan với chỉ 1 plugin duy nhất

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?

- Port 111

| | | | | |
|------------------|-----------------|-----------------|-----|--|
| 72.8.380416005 | 192.168.184.133 | 192.168.184.137 | TCP | 64 2580 → 111 [SYN] Seq=0 Win=4896 Len=0 MSS=1460 SACK_PERM |
| 73.8.380767137 | 192.168.184.137 | 192.168.184.133 | TCP | 64 111 → 2580 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM |
| L 74.8.380804935 | 192.168.184.133 | 192.168.184.137 | TCP | 56 2580 → 111 [RST] Seq=1 Win=0 Len=0 |

- Ngoài port 111 còn có các port khác

Port 80

| | | | | |
|----------------|-----------------|-----------------|------|--|
| 90.8.685927442 | 192.168.184.133 | 192.168.184.137 | TCP | 76 52552 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2533974693 TSecr=0 WS=128 |
| 92.8.605277457 | 192.168.184.133 | 192.168.184.137 | TCP | 76 80 → 52552 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=248046 TSecr=2533974693 WS=32 |
| 92.8.605313431 | 192.168.184.133 | 192.168.184.137 | TCP | 68 52552 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2533974694 TSecr=248046 |
| 93.8.633981556 | 192.168.184.133 | 192.168.184.137 | HTTP | 374 GET / HTTP/1.1 |
| 94.8.634466874 | 192.168.184.133 | 192.168.184.137 | TCP | 68 80 → 52552 [ACK] Seq=1 Ack=307 Win=6880 Len=0 TSval=248048 TSecr=2533974722 |
| 95.8.655466687 | 192.168.184.137 | 192.168.184.133 | HTTP | 1192 HTTP/1.1 200 OK (text/html) |
| 96.8.655494374 | 192.168.184.133 | 192.168.184.137 | TCP | 68 52552 → 80 [ACK] Seq=307 Ack=1125 Win=64128 Len=0 TSval=2533974744 TSecr=248051 |

Port 81

Nhóm 18

| | | | | |
|-----------------|-----------------|-----------------|-----|---|
| 79 8. 514700362 | 192.168.184.133 | 192.168.184.137 | TCP | 76 49946 - 81 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsv=2533974603 Tscr=0 WS=128 |
| 80 8. 515080957 | 192.168.184.137 | 192.168.184.133 | TCP | 62 81 - 49946 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |

Port 445

| | | | | |
|------------------|-----------------|-----------------|-----|---|
| 104 8. 757599816 | 192.168.184.133 | 192.168.184.137 | TCP | 76 40146 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsv=2533974846 Tscr=0 WS=128 |
| 105 8. 757993241 | 192.168.184.137 | 192.168.184.133 | TCP | 76 445 - 40146 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsv=248061 Tscr=253 |
| 106 8. 758025278 | 192.168.184.133 | 192.168.184.137 | TCP | 68 40146 - 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=2533974846 Tscr=248061 |

Port 8009

| | | | | |
|------------------|-----------------|-----------------|-----|--|
| 81 8. 569609484 | 192.168.184.133 | 192.168.184.137 | TCP | 76 36508 - 8009 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsv=2533974658 Tscr=0 WS=128 |
| 82 8. 570180537 | 192.168.184.137 | 192.168.184.133 | TCP | 76 8009 - 36508 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsv=248042 Tscr=253 |
| 83 8. 570225269 | 192.168.184.133 | 192.168.184.137 | TCP | 68 36508 - 8009 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=2533974659 Tscr=248042 |
| 84 8. 579841426 | 192.168.184.133 | 192.168.184.137 | TCP | 76 58310 - 2810 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsv=2533974668 Tscr=0 WS=128 |
| 85 8. 580160015 | 192.168.184.137 | 192.168.184.133 | TCP | 62 2810 - 58310 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 86 8. 590638120 | 192.168.184.133 | 192.168.184.137 | TCP | 379 36508 - 8009 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=311 Tsv=2533974679 Tscr=248042 [TCP seq] |
| 87 8. 591171136 | 192.168.184.137 | 192.168.184.133 | TCP | 68 8009 - 36508 [ACK] Seq=1 Ack=312 Win=6880 Len=0 Tsv=248044 Tscr=2533974679 |
| 88 8. 599267041 | 192.168.184.137 | 192.168.184.133 | TCP | 68 8009 - 36508 [FIN, ACK] Seq=1 Ack=312 Win=6880 Len=0 Tsv=248045 Tscr=2533974679 |
| 89 8. 6606892880 | 192.168.184.133 | 192.168.184.137 | TCP | 68 36508 - 8009 [RST, ACK] Seq=312 Ack=2 Win=64256 Len=0 Tsv=2533974689 Tscr=248045 |

Và một số port khác nữa

Nessus lại scan các port khác, trong khi chúng ta đã chỉ định chỉ scan duy nhất 1 port là 111 là vì: để đảm bảo tính toàn vẹn và đáng tin cậy của kết quả quét lỗ hổng.

- Phát hiện lỗ hổng liên quan: Nessus quét nhiều cổng để phát hiện các lỗ hổng không chỉ trên cổng bạn đã chỉ định, mà còn trên các cổng khác mà ứng dụng hoặc dịch vụ đang chạy. Điều này giúp bạn xác định các lỗ hổng liên quan đến cấu hình hoặc phần mềm không chỉ ở cổng 111.
- Phát hiện lỗ hổng ẩn: Có thể có các lỗ hổng tiềm ẩn hoặc không rõ ràng không thể được phát hiện bằng cách quét một cổng cụ thể. Nessus quét nhiều cổng để kiểm tra xem có các lỗ hổng tiềm ẩn nào trên hệ thống.
- Quét toàn diện: Nessus thường quét nhiều cổng để đảm bảo rằng bạn có cái nhìn toàn diện về tình trạng bảo mật của hệ thống. Điều này giúp bạn không bỏ sót bất kỳ lỗ hổng nào.
- Tăng khả năng phát hiện lỗ hổng: Bằng cách quét nhiều cổng, Nessus tăng khả năng phát hiện các lỗ hổng và vượt qua các biện pháp an ninh cụ thể mà người quản trị hệ thống có thể đã áp dụng.

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 port khác không phải là port được chỉ định, ta vào chế độ configure ở phía bên phải



Vào phần Discovery, chọn Port Scanning và tick vào phần Consider unscanned ports as closed. Chế độ này là xem như tất cả các port khác ngoài port được chỉ định đều được đóng.

Metasploitable2 - Individual / Configuration

[Back to Scan Report](#)

| Settings | Credentials | Plugins |
|----------------------|-------------|---------|
| BASIC | | |
| DISCOVERY | | |
| Host Discovery | | |
| Port Scanning | | |
| Service Discovery | | |
| Identity | | |
| ASSESSMENT | | |
| REPORT | | |
| ADVANCED | | |

Ports

Consider unscanned ports as closed

Port scan range: 111

Local Port Enumerators

SSH (netstat)

WMI (netstat)

Thực hiện Launch để quét lại và bây giờ trên Wireshark ta chỉ thấy còn mỗi port 111.

| | | | | |
|------------------------|------------------------|------------------------|-------------|---|
| 157 9.641218276 | 192.168.184.133 | 192.168.184.137 | TCP | 64.12673 - 111 [SYN] Seq=0 Win=4096 MSS=1460 SACK_PERM |
| 153 9.641378691 | 192.168.184.133 | 192.168.184.133 | TCP | 64.111 - 12673 [SYN ACK] Seq=0 Ack=1 Win=8849 Len=0 MSS=1460 SACK_PERM |
| 154 9.641404976 | 192.168.184.133 | 192.168.184.137 | TCP | 56.12673 - 111 [RST] Seq=2 Win=0 Len=0 |
| 155 9.255546986 | 192.168.184.133 | 192.168.184.2 | DNS | 98 Standard query 0x0278 PTR 137.184.168.192.in-addr.arpa |
| 156 9.312558973 | 192.168.184.2 | 192.168.184.133 | DNS | 167 Standard query response 0x0279 No such name PTR 137.184.168.192.in-addr.arpa SOA prisoner.iana.org |
| 157 9.343102776 | 192.168.184.133 | 192.168.184.137 | SNMP | 97 get-next-request 1.3.6.1.2.1.1.1.6 |
| 158 9.343349938 | 192.168.184.137 | 192.168.184.133 | ICMP | 115 Destination unreachable (Port unreachable) |
| 159 9.3632843016 | 192.168.184.133 | 192.168.184.137 | SNMP | 87 get-next-request 1.3.6.1.2.1.1.1.9 |
| 160 9.363013031 | 192.168.184.137 | 192.168.184.133 | ICMP | 115 Destination unreachable (Port unreachable) |
| 161 9.381353921 | 192.168.184.133 | 192.168.184.133 | TCP | 76.33664 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2537809658 TSecr=0 WS=128 |
| 162 9.381558533 | 192.168.184.137 | 192.168.184.133 | TCP | 76.111 - 33664 [SYN ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=629156 TSecr=2537809658 WS=32 |
| 163 9.381577234 | 192.168.184.133 | 192.168.184.137 | TCP | 68.33664 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2537809658 TSecr=629156 |
| 164 9.395727172 | 192.168.184.133 | 192.168.184.137 | RPC | 236 Continuation |
| 165 9.396173531 | 192.168.184.137 | 192.168.184.133 | TCP | 68.111 - 33664 [ACK] Seq=1 Ack=169 Win=6880 Len=0 TSval=629158 TSecr=2537809672 |
| 166 9.396173880 | 192.168.184.137 | 192.168.184.133 | TCP | 68.111 - 33664 [FIN, ACK] Seq=1 Ack=169 Win=6880 Len=0 TSval=629158 TSecr=2537809672 |
| 167 9.418845749 | 192.168.184.133 | 192.168.184.137 | TCP | 68.33664 - 111 [ACK] Seq=169 Ack=2 Win=64256 Len=0 TSval=2537809687 TSecr=629158 |
| 168 9.411054212 | 192.168.184.133 | 192.168.184.137 | RPC | 75 Continuation |
| 169 9.411266056 | 192.168.184.137 | 192.168.184.133 | TCP | 62.111 - 33664 [RST] Seq=2 Win=0 Len=0 |
| 170 9.426588645 | 192.168.184.133 | 192.168.184.137 | TCP | 76.33676 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2537809703 TSecr=0 WS=128 |
| 171 9.427295996 | 192.168.184.137 | 192.168.184.133 | TCP | 76.111 - 33676 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=629161 TSecr=2537809703 WS=32 |
| 172 9.427238478 | 192.168.184.133 | 192.168.184.137 | TCP | 68.33676 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2537809704 TSecr=629161 |

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

Thực hiện tương tự như câu trên nhưng bây giờ chúng ta sẽ sử dụng 2 plugins khác

New Scan / Advanced Scan

[Back to Scan Templates](#)

| Settings | Credentials | Plugins |
|-----------------|--|---------|
| DISABLED | Debian Local Security Checks | 9085 |
| DISABLED | Default Unix Accounts | 172 |
| DISABLED | Denial of Service | 110 |
| MIXED | DNS | 231 |
| DISABLED | F5 Networks Local Security Checks | 1400 |
| DISABLED | Fedora Local Security Checks | 17981 |
| DISABLED | Firewalls | 405 |
| DISABLED | FreeBSD Local Security Checks | 5419 |
| DISABLED | FTP | 271 |
| DISABLED | Gain a shell remotely | 282 |
| DISABLED | General | 356 |
| DISABLED | DNS Sender Policy Framework (SPF) Enabled | 31658 |
| DISABLED | DNS Server BIND version Directive Remote Version Detection | 10028 |
| DISABLED | DNS Server Cache Snooping Remote Information Disclosure | 12217 |
| ENABLED | DNS Server Detection | 11002 |
| DISABLED | DNS Server DNSSEC Aware Resolver | 35373 |
| DISABLED | DNS Server Dynamic Update Record Injection | 35372 |
| DISABLED | DNS Server Fingerprinting | 11951 |
| DISABLED | DNS Server hostname.bind Map Hostname Disclosure | 35371 |
| DISABLED | DNS Server Recursive Query Cache Poisoning Weakness | 10539 |
| DISABLED | DNS Server Spoofed Request Amplification DDoS | 35450 |
| DISABLED | DNS Server UDP Querry Limitation | 18356 |

Scan Plugin DNS

| New Scan / Advanced Scan | | | | Back to Scan Templates | Disable All | Enable All |
|--------------------------|-----------------------------------|-------|-----------------------|--|------------------------------|----------------------------|
| | | | | | Show Enabled | Show All |
| DISABLED | Debian Local Security Checks | 9085 | DISABLED | CCProxy Application Proxy Detection | 15773 | |
| DISABLED | Default Unix Accounts | 172 | DISABLED | Cerbere HTTP Proxy Server Host: Header Remote DoS | 14640 | |
| DISABLED | Denial of Service | 110 | DISABLED | Check Point FireWall-1 4x Multiple Vulnerabilities (OF, FS) | 12084 | |
| MIXED | DNS | 231 | LOCKED | Check Point FireWall-1 HTTP Client Authentication Detection | 10676 | |
| DISABLED | F5 Networks Local Security Checks | 1400 | DISABLED | Check Point FireWall-1 ICA Service Detection | 22094 | |
| DISABLED | Fedora Local Security Checks | 17981 | ENABLED | Check Point FireWall-1 Identification | 10044 | |
| MIXED | Firewalls | 405 | LOCKED | Check Point FireWall-1 Open Web Administration | 11518 | |
| DISABLED | FreeBSD Local Security Checks | 5419 | DISABLED | Check Point FireWall-1 Spoofed UDP Packet Remote DoS | 11905 | |
| DISABLED | FTP | 271 | DISABLED | Check Point FireWall-1 Telnet Client Authentication Detection | 10675 | |
| DISABLED | Gain a shell remotely | 282 | DISABLED | Check Point FireWall-1 UDP Port 0 DoS | 10074 | |
| DISABLED | General | 356 | DISABLED | Check Point FireWall-1/VPN-1 Syslog Daemon Remote Overflow DoS | 11613 | |

Scan Plugin Firewalls

Kết quả scan được (không phát hiện lỗ hổng ở 2 plugins này)

Metasploitable2 - 2plugins / 192.168.184.137

[Back to Hosts](#)

| Vulnerabilities 4 | | | | Host Details | |
|-------------------|------|-----|---|---------------|-------|
| Sev | CVSS | VPR | Name | Family | Count |
| INFO | | | Nessus SYN scanner | Port scanners | 25 |
| INFO | | | DNS Server Detection | DNS | 2 |
| INFO | | | Nessus Scan Information | Settings | 1 |
| INFO | | | SSH Commands Require Privilege Escalation | Settings | 1 |

Host Details

- IP: 192.168.184.137
- MAC: 00:0C:29:DD:98:5E
- Start: Today at 11:40 PM
- End: Today at 11:44 PM
- Elapsed: 5 minutes
- KB: Download

Vulnerabilities

Critical
High
Medium
Low
Info

2. Bài tập nhóm

④ Bài tập về nhà (yêu cầu làm)

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:

Nhóm chọn công cụ quét OpenVAS

A) Cài đặt OpenVAS

- Trước khi cài đặt OpenVAS, cần phải thực hiện cập nhập và nâng cấp hệ điều hành bằng các lệnh sau:

\$ sudo apt update

\$ sudo apt -y upgrade

- Tải công cụ OpenVAS bằng lệnh

\$ sudo apt install openvas

- Cài đặt công cụ bằng lệnh

\$ sudo gvm-setup

- Sau đó thực hiện các lệnh sau để cập nhập signatures của OpenVAS scanning

```
(bun㉿kali)-[~]
$ sudo greenbone-feed-sync
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
  Downloading Notus files from
rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/notus/ to
/var/lib/notus
  Downloading NASL files from
rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/nasl/ to
/var/lib/openvas/plugins
Releasing lock on /var/lib/openvas/feed-update.lock

Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
  Downloading SCAP data from
rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/scap-data/ to
/var/lib/gvm/scap-data
  Downloading CERT-Bund data from
rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/cert-data/ to
/var/lib/gvm/cert-data
  Downloading gvmd data from rsync://feed.community.greenbone.net/community/data-feed/22.04/
to /var/lib/gvm/data-objects/gvmd/22.04
Releasing lock on /var/lib/gvm/feed-update.lock
```

```
(bun㉿kali)-[~]
$ sudo gvmd --rebuild
```

- Cuối cùng bắt đầu OpenVAS bằng lệnh sau (phải chờ nó chạy xong thì mới truy cập được vào trang web dùng để quét)

```
bun@kali: ~
File Actions Edit View Help Administration Help
└─(bun@kali)-[~]
$ sudo gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● gsad.service - Greenbone Security Assistant daemon (gsad)
   Loaded: loaded (/lib/systemd/system/gsad.service; disabled; preset: disabled)
   Active: active (running) since Wed 2023-11-08 19:08:41 +07; 42ms ago
     Docs: man:gsad(8)
           https://www.greenbone.net
   Main PID: 5994 (gsad)
      Tasks: 1 (limit: 4554)
     Memory: 1.7M
        CPU: 7ms
      CGroup: /system.slice/gsad.service
              └─5994 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

Nov 08 19:08:41 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Nov 08 19:08:41 kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
   Loaded: loaded (/lib/systemd/system/gvmd.service; disabled; preset: disabled)
   Active: active (running) since Wed 2023-11-08 19:08:36 +07; 5s ago
     Docs: man:gvmd(8)
   Process: 5847 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code-exited, status=0/SUCCESS)
   Main PID: 5849 (gvmd)
      Tasks: 2 (limit: 4554)
     Memory: 284.7M
        CPU: 779ms
      CGroup: /system.slice/gvmd.service
              ├─5849 "gvmd: Waiting" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
              ├─5945 "gvmd: Syncing" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
```

```
bun@kali: ~
File Actions Edit View Help Administration Help
CGroup: /system.slice/gvmd.service
└─5849 "gvmd: Waiting" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
    ├─5945 "gvmd: Syncing" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm

Nov 08 19:08:30 kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Nov 08 19:08:30 kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) after start: No such file or directory
Nov 08 19:08:36 kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).

● ospd-openvas.service - OSPD Wrapper for the OpenVAS Scanner (ospd-openvas)
   Loaded: loaded (/lib/systemd/system/ospd-openvas.service; disabled; preset: disabled)
   Active: active (running) since Wed 2023-11-08 19:07:49 +07; 52s ago
     Docs: man:ospd-openvas(8)
           man:openvas(8)
   Process: 4978 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf (code-exited, status=0/SUCCESS)
   Main PID: 5049 (ospd-openvas)
      Tasks: 6 (limit: 4554)
     Memory: 171.1M
        CPU: 15.468s
      CGroup: /system.slice/ospd-openvas.service
              ├─5049 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf
              ├─5053 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf
              └─5260 "openvas: openvas: Reloaded 5600 of 87199 NVTs (6% / ETA: 06:47)" NVIS by Severity Class (total: 153188)

Nov 08 19:07:41 kali systemd[1]: Starting ospd-openvas.service - OSPD Wrapper for the OpenVAS Scanner (ospd-openvas)...
Nov 08 19:07:49 kali systemd[1]: Started ospd-openvas.service - OSPD Wrapper for the OpenVAS Scanner (ospd-openvas).
[>] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...
└─(bun@kali)-[~]
```

- Trong quá trình thực thi lệnh gvm-setup, 1 tài khoản có tên “admin” và password là 1 chuỗi ngẫu nhiên đã được tạo ra. Nhưng nếu không thích thì ta có thể thay đổi chúng.

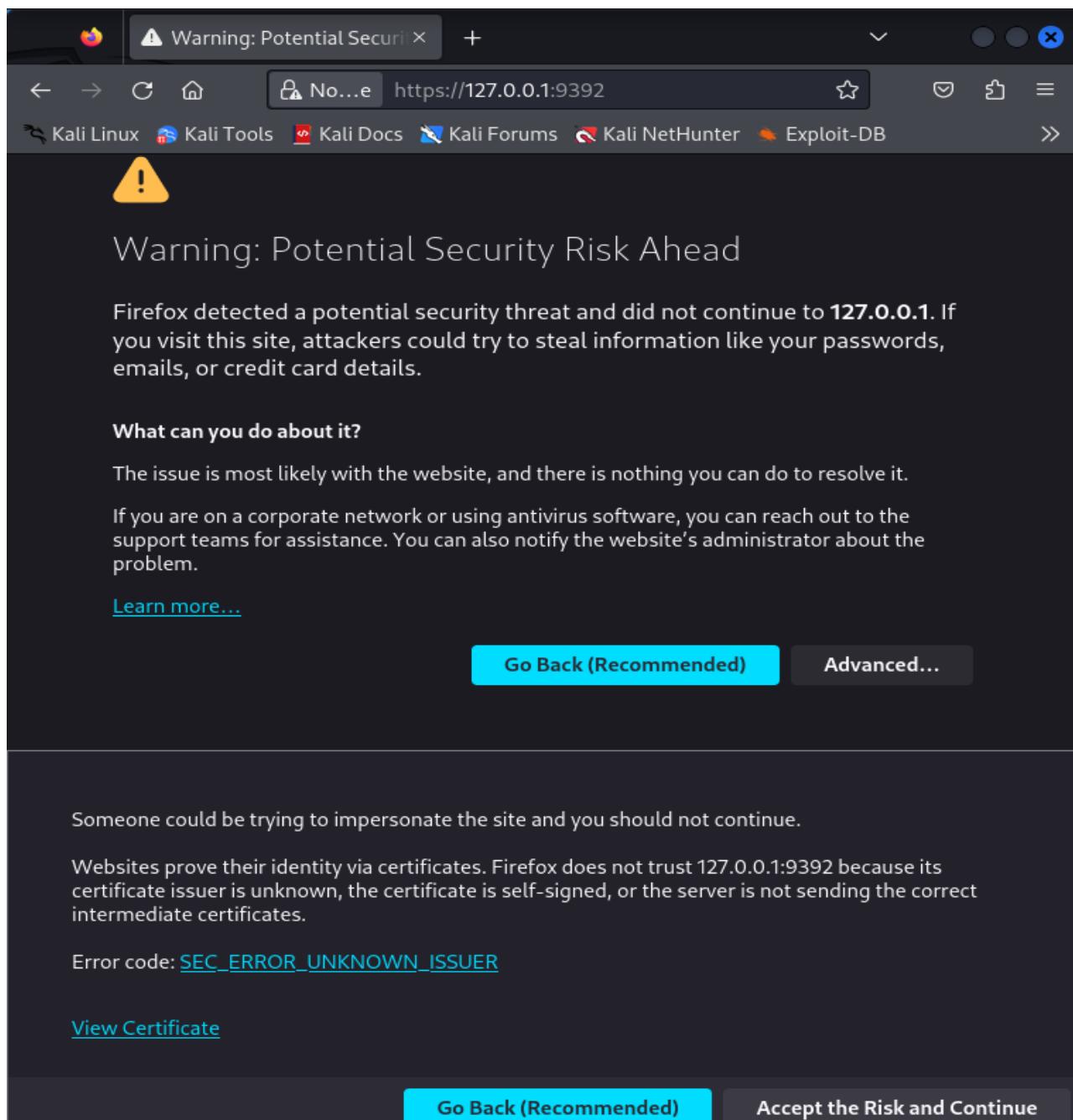
Ví dụ: dùng lệnh như bên dưới để thay đổi password sao cho dễ nhớ hơn



```
(bun㉿kali)-[~]
$ sudo runuser -u gvm -- gvmd --user=admin --new-password="pass"
(bun㉿kali)-[~]
$
```

- Truy cập URL: <https://127.0.0.1:9392/>

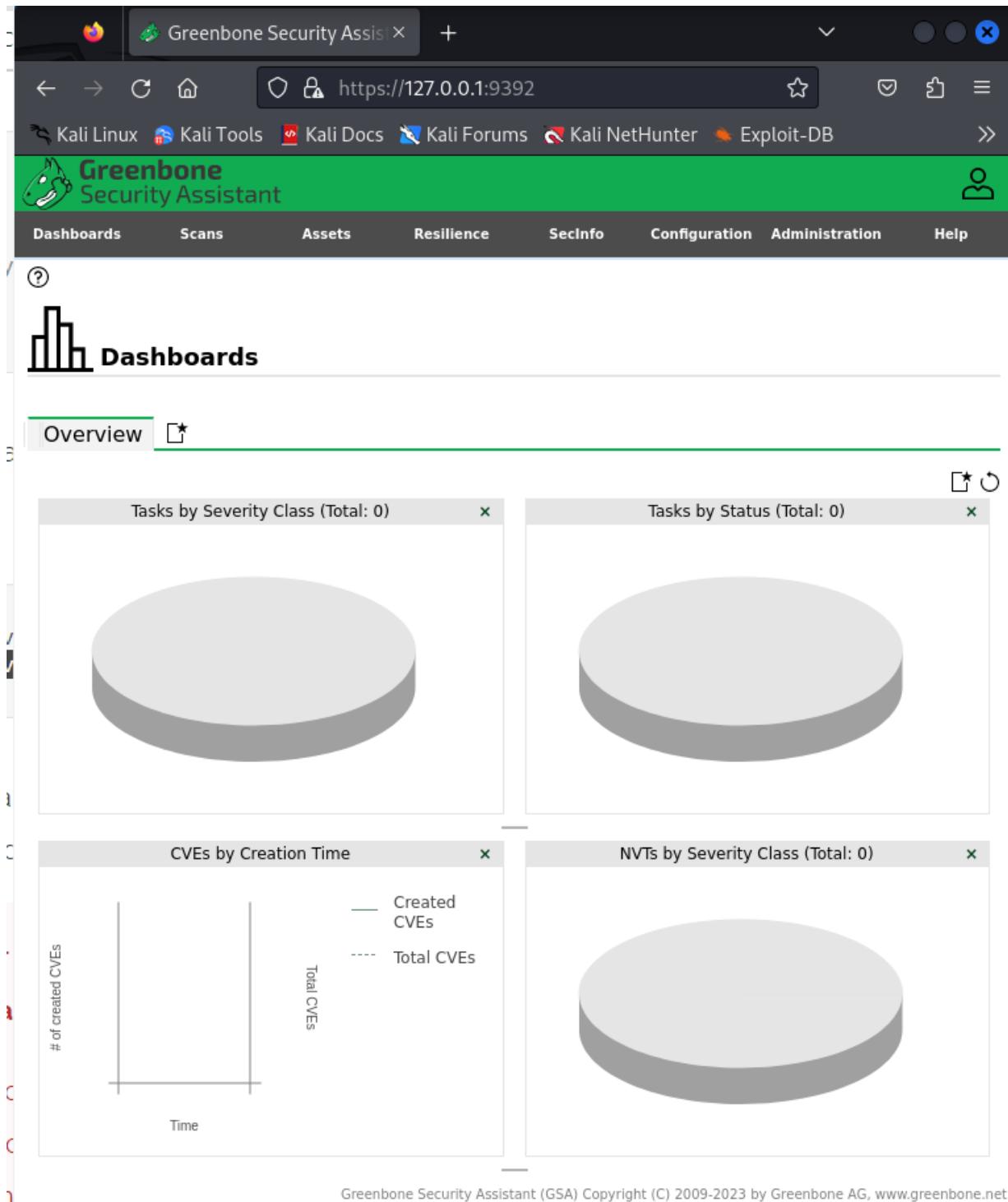
Để vào trang web chính



- Chọn “Accept the Risk and Continue” để vào trang web

Chờ trang web tải xong và hiện ra các đồ họa CVEs và NVTs trong Dashboards. Sau đó vô mục Administration -> chọn Feed Status để kiểm tra feeds.

Nếu status là “Current” thì lúc này các scanner đã sẵn sàng. Ngược lại thì sẽ không thực hiện việc quét được



- Có status="Current" => các scanner đã sẵn sàng để thực hiện scan

| Type | Content | Origin | Version | Status |
|-----------|---|-----------------------------|---------------|-----------------------|
| NVT | NVTs | Greenbone Community Feed | 20231108T0606 | Current |
| SCAP | CVEs CPEs | Greenbone SCAP Data Feed | 20231108T0504 | Update in progress... |
| CERT | CERT-Bund Advisories DFN-CERT Advisories | Greenbone CERT Data Feed | 20231108T0424 | Update in progress... |
| GVMD_DATA | Compliance Policies Port Lists Report Formats Scan Configs | Greenbone Data Objects Feed | 20231108T0505 | Update in progress... |

- Trước khi scan thì cần biết địa chỉ IP của target

Target của bài này là Metasploitable2 nên ta mở máy ảo Metasploitable2 rồi thực hiện lệnh ifconfig để xem IP của nó

```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:08:95:86
          inet addr:192.168.142.136 Bcast:192.168.142.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe08:9586/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4203 (4.1 KB) TX bytes:7112 (6.9 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:99 errors:0 dropped:0 overruns:0 frame:0
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21713 (21.2 KB) TX bytes:21713 (21.2 KB)

msfadmin@metasploitable:~$
```

Nhóm 18

- Thực hiện kết nối từ máy KaliLinux tới Metasploitable để kiểm tra kết nối giữa 2 máy đã ổn định chưa

```
(bun㉿kali)-[~]
$ ping 192.168.142.136
PING 192.168.142.136 (192.168.142.136) 56(84) bytes of data.
64 bytes from 192.168.142.136: icmp_seq=1 ttl=64 time=0.366 ms
64 bytes from 192.168.142.136: icmp_seq=2 ttl=64 time=0.405 ms
64 bytes from 192.168.142.136: icmp_seq=3 ttl=64 time=0.183 ms
^X64 bytes from 192.168.142.136: icmp_seq=4 ttl=64 time=0.715 ms
64 bytes from 192.168.142.136: icmp_seq=5 ttl=64 time=0.922 ms
^C
--- 192.168.142.136 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4067ms
rtt min/avg/max/mdev = 0.183/0.518/0.922/0.264 ms
```

B) Khai báo đối tượng

- Chọn mục Configuration -> chọn Targets

Trong trang hiện ra, truy cập vào biểu tượng New Target

The screenshot shows the Greenbone Security Assistant web interface. At the top, there's a navigation bar with links like Kali Linux, Kali Tools, Kali Docs, etc. Below it is a green header bar with the title 'Greenbone Security Assistant'. In the center, there's a main content area with a heading 'Targets 1 of 1'. Below this, there's a table with columns: Name, Hosts, IPs, Port List, Credentials, and Actions. A red circle highlights the 'New Target' button icon (a question mark inside a square) in the top-left corner of the table header.

- Trong bảng New Target, điền đầy đủ thông tin target như bên dưới.

Nhập tên target: “Metasploitable2” trong trường Name

Nhập địa chỉ IP của target trong trường Hosts(Manual)

Sau đó nhấn Save để lưu.

The screenshot shows the 'New Target' configuration dialog box. It has several sections:

- Name:** Metasploitable2
- Comment:** linux
- Hosts:** Manual (192.168.142.136), From file (No file selected)
- Exclude Hosts:** Manual (empty), From file (No file selected)
- Allow simultaneous scanning via multiple IPs:** Yes (selected)
- Port List:** All IANA assigned TCP
- Alive Test:** Scan Config Default
- Credentials for authenticated checks:** SSH (port 22), SMB (port 139)

 At the bottom right, there are 'Cancel' and 'Save' buttons, with 'Save' being highlighted.

Nhóm 18

- Sau khi save thì mục target có thêm 1 đối tượng mới

The screenshot shows the 'Targets' section of the Greenbone Security Assistant interface. At the top, there are navigation tabs: Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. Below the tabs is a search bar labeled 'Filter' with various search operators. The main area displays a table titled 'Targets 2 of 2'. The columns are 'Name', 'Hosts', 'IPs', 'Port List', 'Credentials', and 'Actions'. The first row shows 'Metasploitable2 (linux)' as the host, with IP 192.168.142.136 and port count 1. The 'Actions' column contains icons for delete, edit, and refresh.

C) Cấu hình các định nghĩa quét (Scan Definitions)

Yêu cầu đầu tiên sẽ chỉ quét các port TCP nên ta sẽ tạo ra danh sách port mới, chứ không dùng danh sách mặc định sẵn có

- Trong mục Configuration-> chọn Port Lists

Trong trang mới hiện ra, chọn biểu tượng New Port List

The screenshot shows the 'Portlists' section of the Greenbone Security Assistant interface. At the top, there are navigation tabs: Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. Below the tabs is a search bar labeled 'Filter' with various search operators. The main area displays a table titled 'Portlists 3 of 3'. The columns are 'Name', 'Port Counts' (Total, TCP, UDP), and 'Actions'. The three rows listed are 'All IANA assigned TCP (Version 20200827.)', 'All IANA assigned TCP and UDP (Version 20200827.)', and 'All TCP and Nmap top 100 UDP (Version 20200827.)'. The 'Actions' column contains icons for delete, edit, and refresh. At the bottom of the table, there is a link 'Apply to page contents' and a note '(Applied filter: sort=name first=1 rows=10)'.

- Trong bảng New Port List:

Nhập tên danh sách trong trường Name

Nhập chú thích (nếu có) trong trường Comment

Nhập các port muốn quét và loại port cần quét trong trường Port Ranges (Manual)

- Sau đó nhấn Save để lưu

Nhóm 18

New Port List

Name: start

Comment:

Port Ranges: Manual T:1-65535
 From file No file selected.

- Trong trang Portlists, danh sách port mới tạo ra đã được thêm vào

Portlists 4 of 4

| Name | Port Counts | Actions | |
|--|-------------|---------|--|
| Total | TCP | UDP | |
| All IANA assigned TCP (Version 20200827.) | 5836 | 5836 | <input type="button" value="trash"/> <input type="button" value="edit"/> <input type="button" value="refresh"/> |
| All IANA assigned TCP and UDP (Version 20200827.) | 11318 | 5836 | 5482 <input type="button" value="trash"/> <input type="button" value="edit"/> <input type="button" value="refresh"/> |
| All TCP and Nmap top 100 UDP (Version 20200827.) | 65635 | 65535 | 100 <input type="button" value="trash"/> <input type="button" value="edit"/> <input type="button" value="refresh"/> |
| start | 65535 | 65535 | 0 <input type="button" value="trash"/> <input type="button" value="edit"/> <input type="button" value="refresh"/> |

Applied filter: sort=name first=1 rows=10

- Thay đổi danh sách port sẽ quét của target

Chọn mục Configuration -> Chọn Targets -> Chọn biểu tượng Edit của đối tượng target muốn quét

Targets 1 of 1

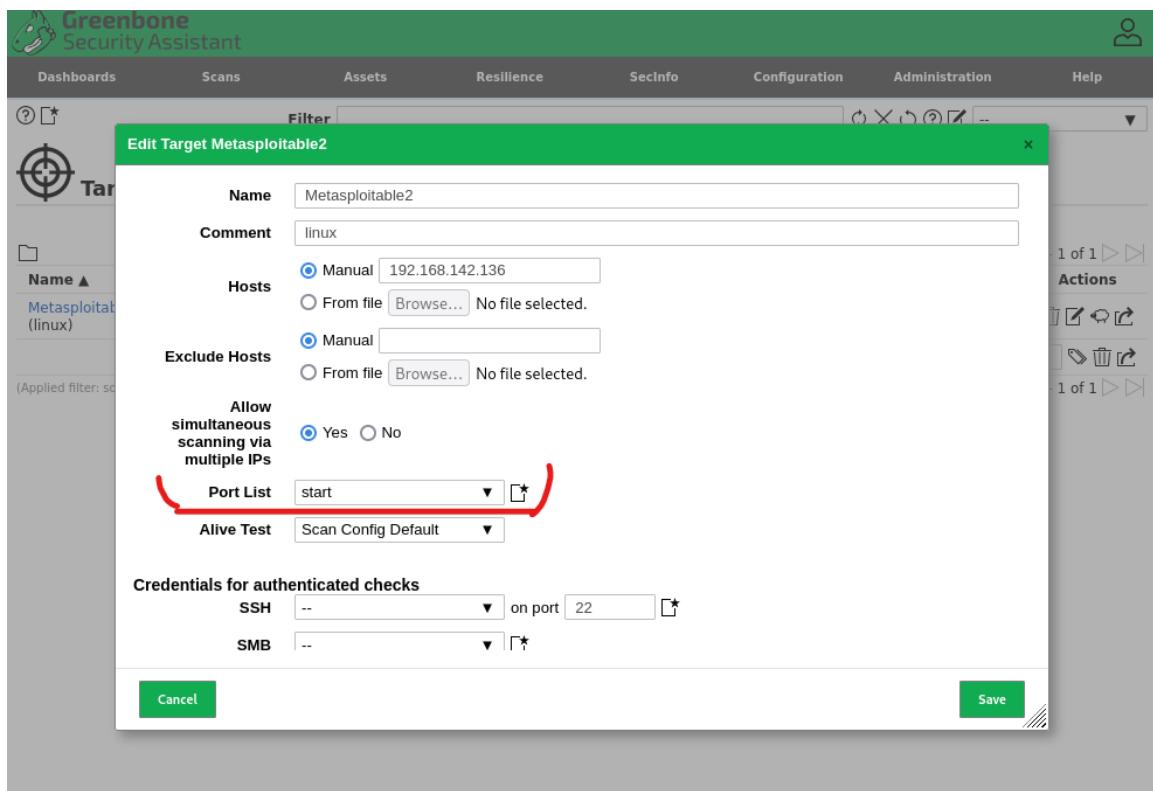
| Name | Hosts | IPs | Port List | Credentials | Actions |
|-------------------------|-----------------|-----|-----------------------|-------------|---|
| Metasploitable2 (linux) | 192.168.142.136 | 1 | All IANA assigned TCP | | <input type="button" value="trash"/> <input type="button" value="edit"/> <input type="button" value="refresh"/> |

Applied filter: sort=name first=1 rows=10

Nhóm 18

- Trong bảng Edit Target “target_name”, chọn danh sách port muốn quét trong trường Port List

Sau đó nhấn Save để lưu



- Kết quả sau khi lưu

| Name | Hosts | IPs | Port List | Credentials | Actions |
|-------------------------|-----------------|-----|-----------|-------------|---------|
| Metasploitable2 (linux) | 192.168.142.136 | 1 | start | | |

D) Quét lỗ hổng không sử dụng tài khoản chứng thực

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

- Truy cập mục Scans -> chọn Tasks

Trong trang hiện ra chọn biểu tượng New Task

The screenshot shows the Nessus interface with the 'Tasks' dashboard selected. The top navigation bar includes 'Dashboards', 'Scans', 'Assets', 'Resilience', 'SecInfo', 'Configuration', 'Administration', and 'Help'. Below the navigation is a search bar labeled 'Filter' with various search icons. The main area displays three cards: 'Tasks by Severity Class (Total: 0)', 'Tasks with most High Results per Host', and 'Tasks by Status (Total: 0)'. Below these cards, a message states 'No Tasks available' and provides a query log: '(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)'. The 'New Task' button is circled in red at the top left.

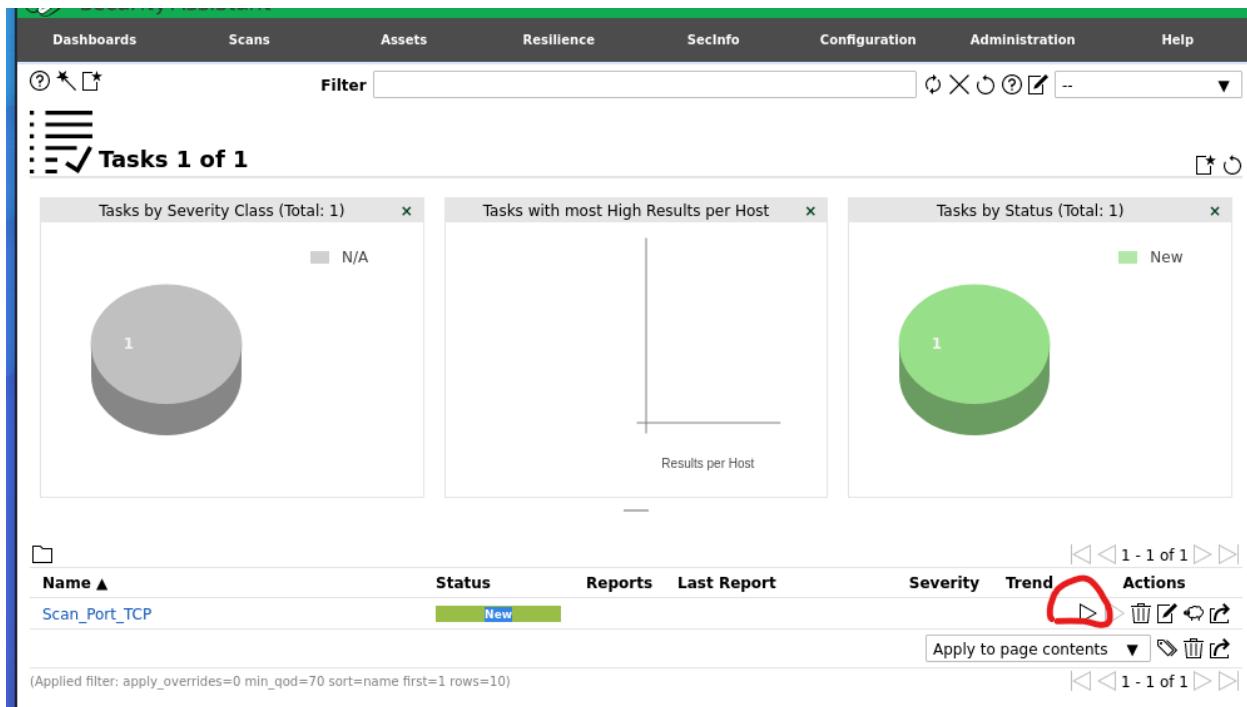
- Trong bảng New Task, nhập tên Task trong trường Name, chọn đối tượng quét trong trường Scan Targets, còn lại giữ như mặc định

Sau đó nhấn Save

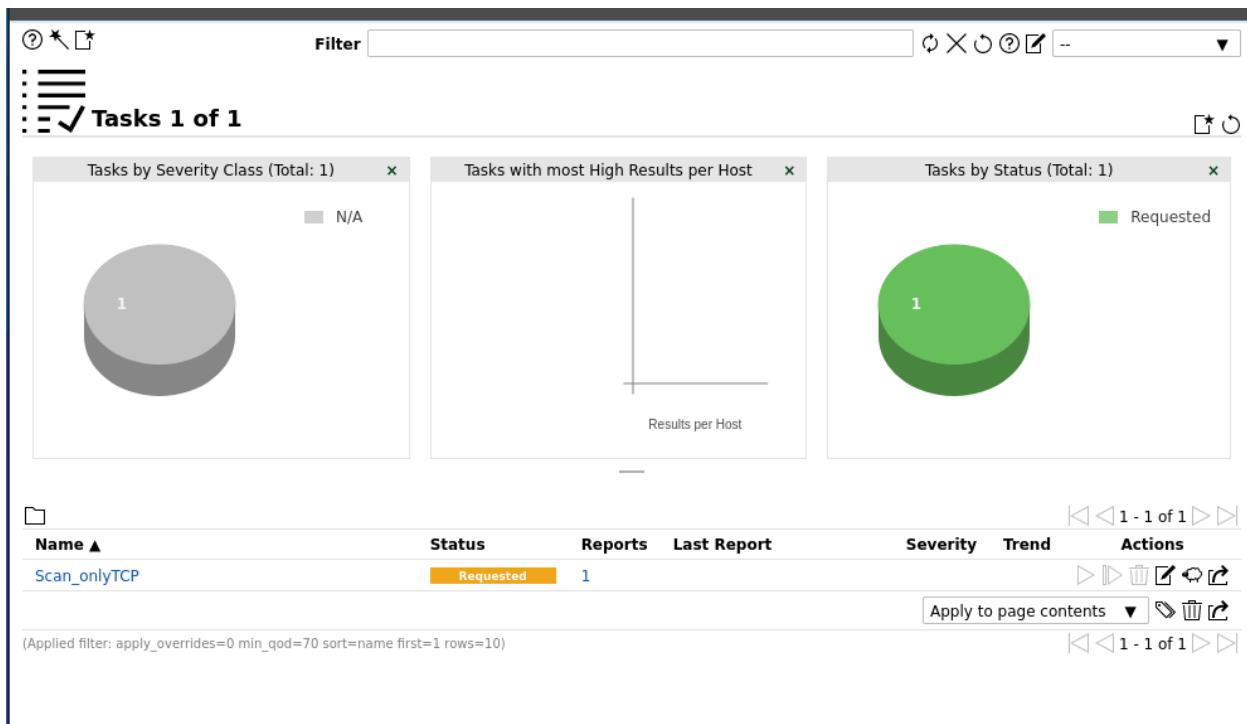
The screenshot shows the 'New Task' configuration dialog. The 'Name' field is filled with 'Scan_onlyTCP'. Other settings include 'Scan Targets' set to 'Metasploitable2', 'Alerts' empty, 'Schedule' empty, 'Add results to Assets' (radio button selected), 'Apply Overrides' (radio button selected), 'Min QoD' set to 70, 'Alterable Task' (radio button selected), 'Auto Delete Reports' (radio button selected), 'Scanner' set to 'OpenVAS Default', and 'Scan Config' set to 'Full and fast'. At the bottom are 'Cancel' and 'Save' buttons.

- Sau khi lưu thì trong danh sách Task xuất hiện tên Task mà ta mới tạo

Nhấn biểu tượng Start để bắt đầu quá trình quét

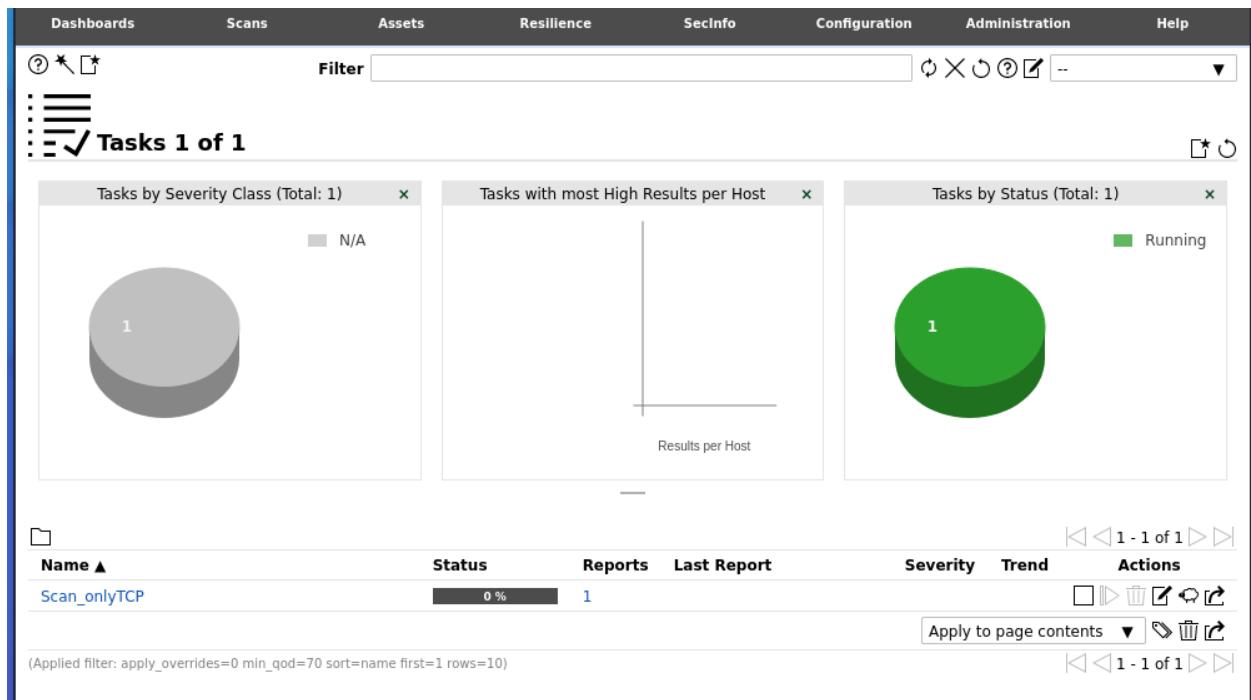


- Theo dõi cột Status để xem OpenVAS đang thực hiện giai đoạn nào
- Bắt đầu khởi tạo quá trình quét

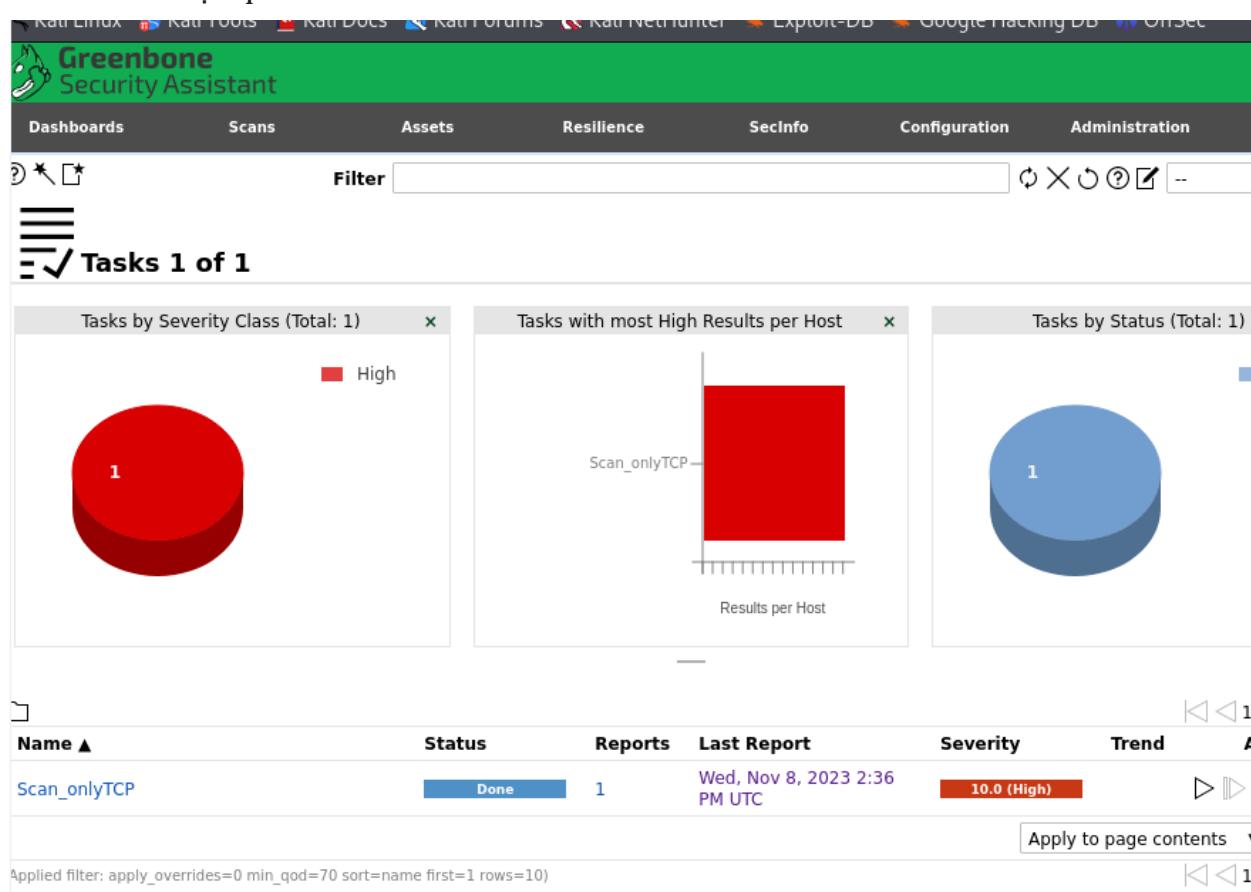


Đang thực hiện quét các lỗ hổng

Nhóm 18

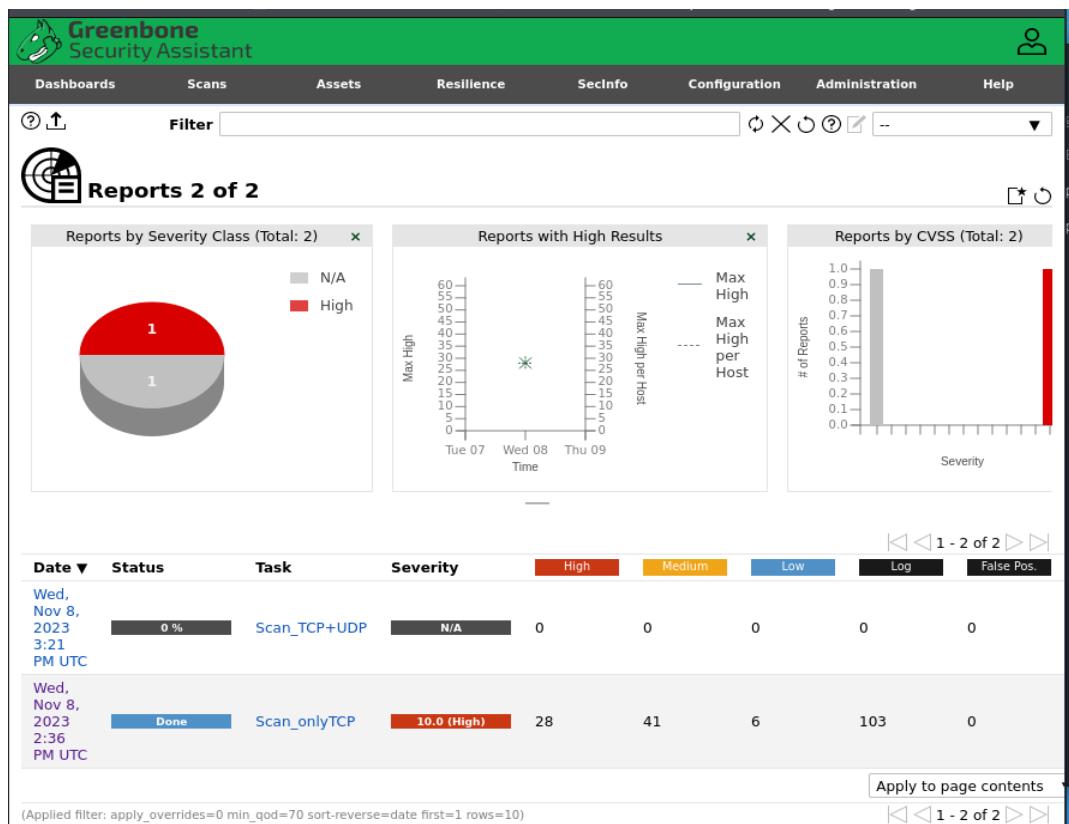


Hoàn thành việc quét

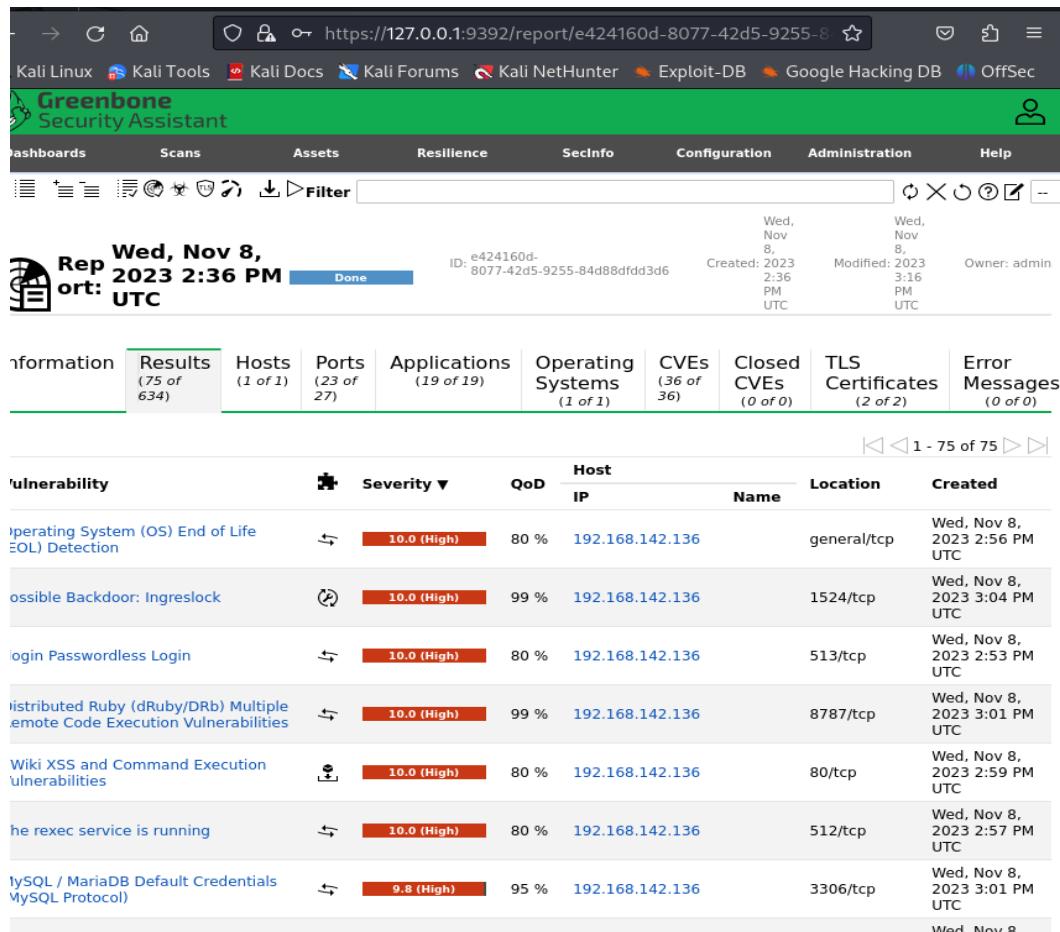


Nhóm 18

- Sau khi quét xong, vô mục Scan -> chọn Reports để xem các kết quả tìm được



- Nhấn vào đối tượng muốn xem report để hiện ra bản report chi tiết



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

Bước 1: OpenVAS thực hiện quá trình Requested

Nó sẽ gửi gói tin ARP để tìm địa chỉ MAC của target

| Capturing from eth0 | | | | | | |
|---------------------|-------------|-----------------|-----------------|----------|--------|---|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 1 | 0.000000000 | 192.168.142.129 | 34.107.243.93 | TLSv1.2 | 93 | Application Data |
| 2 | 0.000061191 | 192.168.142.129 | 34.149.100.209 | TLSv1.2 | 100 | Application Data |
| 3 | 0.000294252 | 34.107.243.93 | 192.168.142.129 | TCP | 60 | 443 → 41314 [ACK] Seq=1 Ack=40 Win=64240 Len=0 |
| 4 | 0.000294388 | 34.149.100.209 | 192.168.142.129 | TCP | 60 | 443 → 47300 [ACK] Seq=1 Ack=47 Win=64240 Len=0 |
| 5 | 0.044833436 | 34.107.243.93 | 192.168.142.129 | TLSv1.2 | 93 | Application Data |
| 6 | 0.044833655 | 34.149.100.209 | 192.168.142.129 | TLSv1.2 | 100 | Application Data |
| 7 | 0.044868042 | 192.168.142.129 | 34.107.243.93 | TCP | 54 | 41314 → 443 [ACK] Seq=40 Ack=40 Win=64028 Len=0 |
| 8 | 0.044892564 | 192.168.142.129 | 34.149.100.209 | TCP | 54 | 47300 → 443 [ACK] Seq=47 Ack=47 Win=64015 Len=0 |
| 9 | 5.166844461 | VMware_64:0b:77 | VMware_e8:21:21 | ARP | 42 | Who has 192.168.142.2? Tell 192.168.142.129 |
| 10 | 5.166927379 | VMware_e8:21:21 | VMware_64:0b:77 | ARP | 60 | 192.168.142.2 is at 00:50:56:e8:21:21 |

Bước 2: OpenVAS thực hiện quá trình Queue

Nó thực hiện ping tới target

| | | | | | | |
|----|--------------|-----------------|-----------------|------|----|---|
| 11 | 51.032696650 | 192.168.142.129 | 192.168.142.136 | ICMP | 98 | Echo (ping) request id=0xff7f, seq=0/0, ttl=64 |
| 12 | 51.033462213 | 192.168.142.136 | 192.168.142.129 | ICMP | 98 | Echo (ping) reply id=0xff7f, seq=0/0, ttl=64 |
| 13 | 51.308963495 | 192.168.142.129 | 192.168.142.2 | DNS | 88 | Standard query 0xb69 PTR 136.142.168.192.in-addr.arpa |
| 14 | 51.352340835 | 192.168.142.2 | 192.168.142.129 | DNS | 88 | Standard query response 0xb69 No such name P |

Bước 3: OpenVAS thực hiện quá trình Scanning

OpenVAS gửi hàng loạt các gói tin TCP đến target tại các port nằm trong danh sách Port List mà ta đã chọn

| | | | | | | |
|----|--------------|-----------------|-----------------|-----|----|---|
| 15 | 51.754488307 | 192.168.142.129 | 192.168.142.136 | TCP | 74 | 49872 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 |
| 16 | 51.754563350 | 192.168.142.129 | 192.168.142.136 | TCP | 74 | 53872 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 |
| 17 | 51.754627983 | 192.168.142.129 | 192.168.142.136 | TCP | 74 | 59338 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 |
| 18 | 51.754678035 | 192.168.142.136 | 192.168.142.129 | TCP | 74 | 3306 → 49872 [SYN, ACK] Seq=0 Ack=1 Win=5792 |
| 19 | 51.754687600 | 192.168.142.129 | 192.168.142.136 | TCP | 74 | 55894 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 |
| 20 | 51.754713530 | 192.168.142.129 | 192.168.142.136 | TCP | 66 | 49872 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1400 |
| 21 | 51.754739296 | 192.168.142.136 | 192.168.142.129 | TCP | 74 | 23 → 53872 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1400 |
| 22 | 51.754739369 | 192.168.142.136 | 192.168.142.129 | TCP | 60 | 8080 → 59338 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 23 | 51.754739388 | 192.168.142.136 | 192.168.142.129 | TCP | 60 | 199 → 55894 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 24 | 51.754751037 | 192.168.142.129 | 192.168.142.136 | TCP | 66 | 53872 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1400 |
| 25 | 51.754785504 | 192.168.142.129 | 192.168.142.136 | TCP | 74 | 58914 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 |
| 26 | 51.754856054 | 192.168.142.129 | 192.168.142.136 | TCP | 74 | 52116 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 |
| 27 | 51.754890795 | 192.168.142.136 | 192.168.142.129 | TCP | 60 | 135 → 58914 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 28 | 51.754910213 | 192.168.142.129 | 192.168.142.136 | TCP | 74 | 57288 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 |
| 29 | 51.754942173 | 192.168.142.136 | 192.168.142.129 | TCP | 60 | 143 → 52116 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 30 | 51.754959910 | 192.168.142.129 | 192.168.142.136 | TCP | 74 | 58118 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 |

Bước 4: OpenVAS hoàn tất quá trình quét (Done)

OpenVAS sẽ xuất ra bản report ghi lại chi tiết các lỗ hổng mà nó quét được.

3. Quét lại nhưng quét thêm port UDP.

- Tạo danh sách port mới để quét tất cả TCP port và UDP port

Nhập tên Port List trong trường Name

Nhập các port muốn quét trong trường Port Ranges (Manual)

Sau đó nhấn Save

Nhóm 18

New Port List

Name: start_TCP+UDP

Comment:

Port Ranges: Manual T:1-65535,U:1-65535

Actions: Save

| | 65635 | 65535 | 100 | |
|--|-------|-------|-----|--|
| All TCP and Nmap top 100 UDP (Version 20200827.) | 65635 | 65535 | 100 | Delete Edit Copy Run |
| start | 65535 | 65535 | 0 | Delete Edit Copy Run |

(Applied filter: sort=name first=1 rows=10)

- Sau khi lưu danh sách mới tạo, trong danh sách Portlists xuất hiện tên danh sách port mà ta vừa tạo ra

Portlists 5 of 5

| Name | Port Counts | Actions | |
|---|-------------|---------|--|
| Total | TCP | UDP | |
| All IANA assigned TCP (Version 20200827.) | 5836 | 5836 | 0 Delete Edit Copy Run |
| All IANA assigned TCP and UDP (Version 20200827.) | 11318 | 5836 | 5482 Delete Edit Copy Run |
| All TCP and Nmap top 100 UDP (Version 20200827.) | 65635 | 65535 | 100 Delete Edit Copy Run |
| start | 65535 | 65535 | 0 Delete Edit Copy Run |
| start_TCP+UDP | 131070 | 65535 | 65535 Delete Edit Copy Run |

(Applied filter: sort=name first=1 rows=10)

- Tạo 1 đối tượng quét mới dùng danh sách port mà ta đã tạo

Truy cập vô mục Configuration -> chọn Targets

Trong trang hiện ra, chọn biểu tượng New target

Targets 5 of 5

| Name | Hosts | IPs | Port List | Credentials | Actions |
|------|-------|-----|-----------|-------------|---------|
|------|-------|-----|-----------|-------------|---------|

- Trong bảng New Target, nhập thông tin cần thiết

Điền tên target trong trường Name

Điền IP address của target trong trường Hosts(Manual)

Chọn danh sách port muốn quét trong trường Port List

Sau đó nhấn Save

New Target

Name: Meta2

Comment:

Hosts: Manual 192.168.142.136

Exclude Hosts:

Allow simultaneous scanning via multiple IPs: Yes

Port List: start_TCP+UDP

Alive Test: Scan Config Default

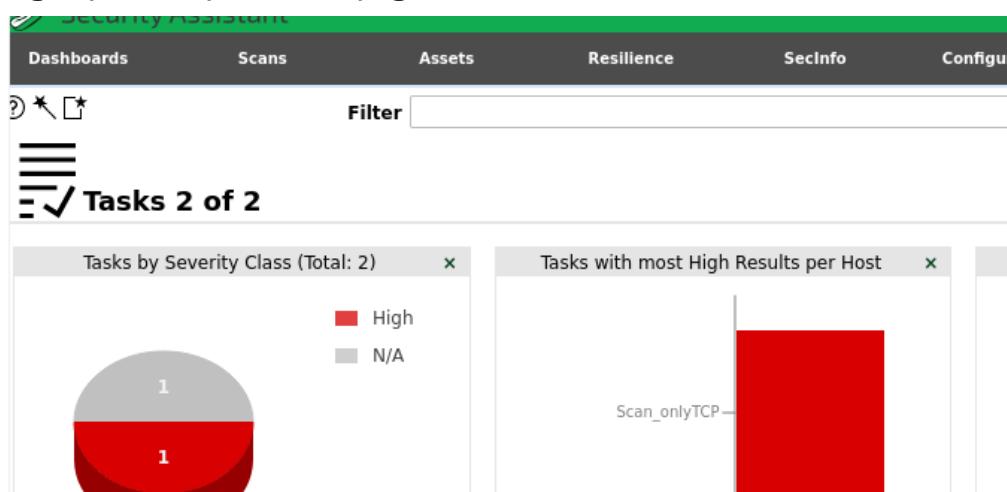
Credentials for authenticated checks:

- SSH: on port 22
- SMB:

Cancel Save

- Truy cập vô mục Scans -> chọn Tasks

Trong trang hiện ra chọn biểu tượng New Task



- Trong bảng New Task, nhập các thông tin cần thiết như ảnh bên dưới

Sau đó nhấn Save

Nhóm 18

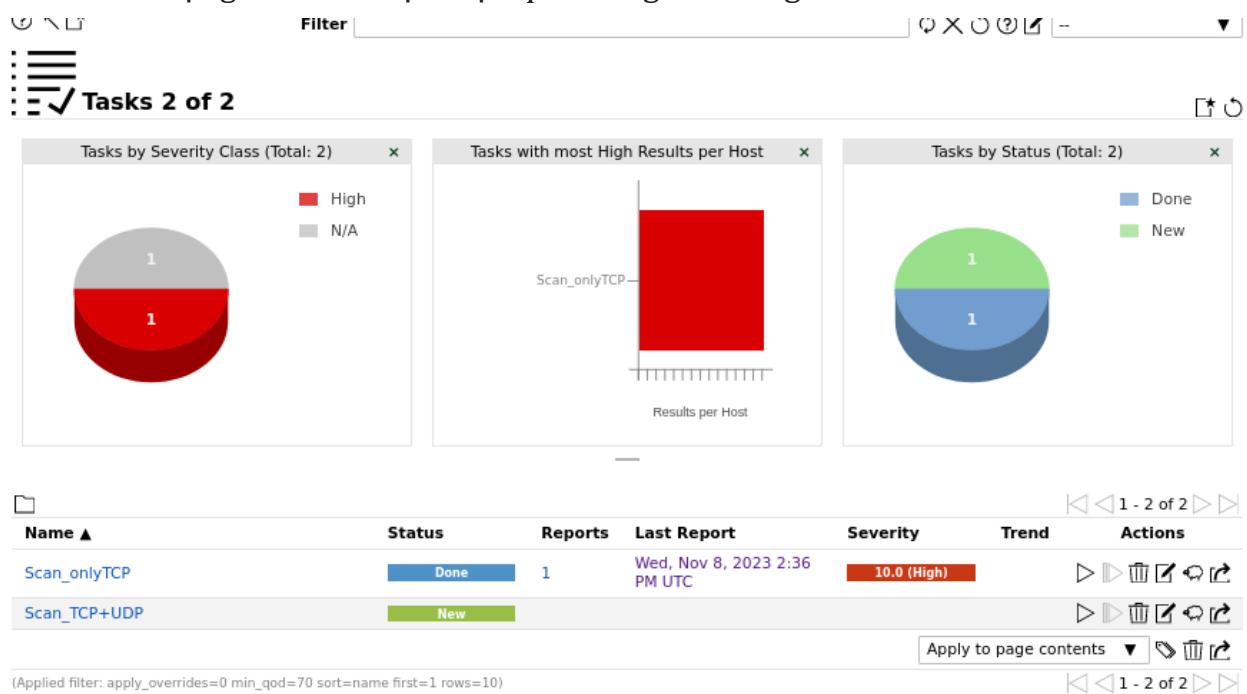
New Task

| | |
|-----------------------|--|
| Name | Scan_TCP+UDP |
| Comment | |
| Scan Targets | Meta2 |
| Alerts | |
| Schedule | -- |
| Add results to Assets | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Apply Overrides | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Min QoD | 70 |
| Alterable Task | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Auto Delete Reports | <input checked="" type="radio"/> Do not automatically delete reports <input type="radio"/> Automatically delete oldest reports but always keep newest <input type="radio"/> 5 reports |
| Scanner | OpenVAS Default |
| Scan Config | Full and fast |

Cancel **Save**

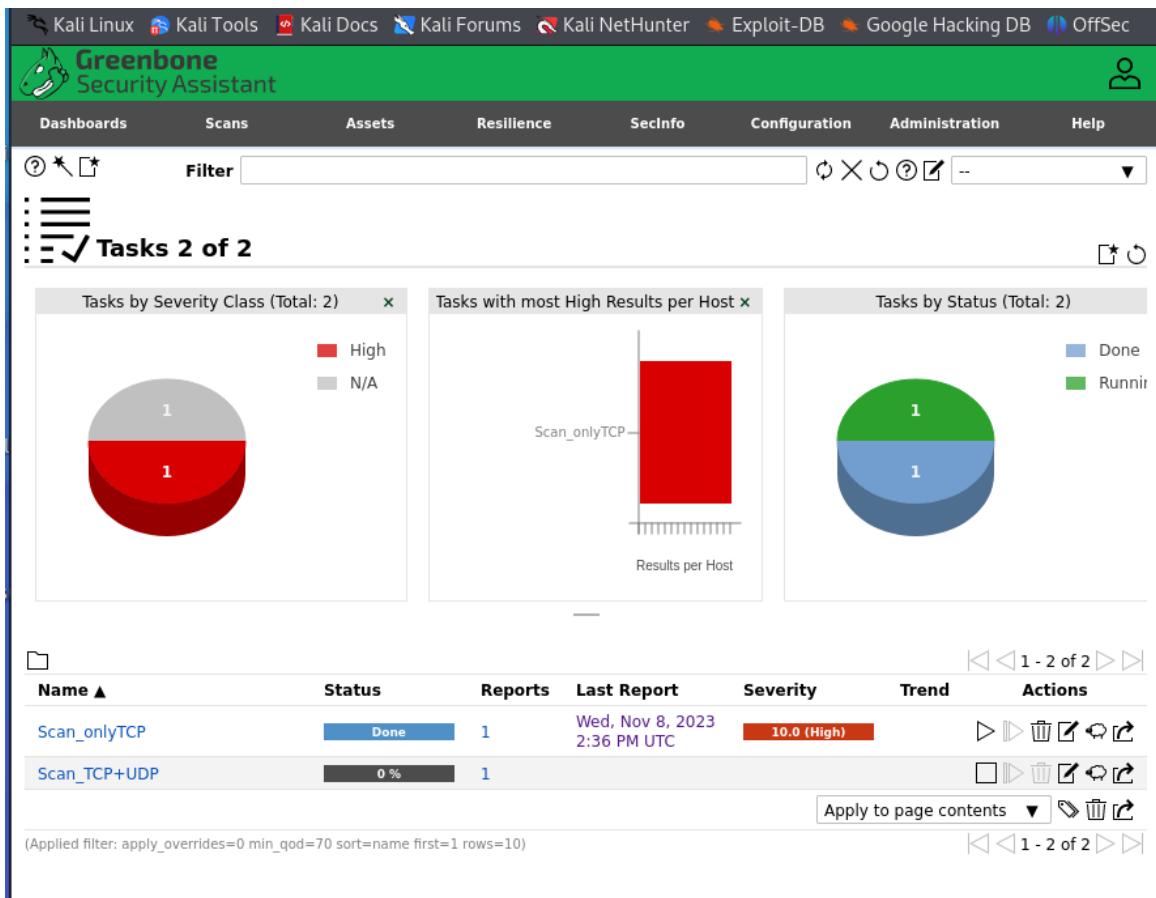
- Sau khi lưu trong danh sách Task xuất hiện tên Task vừa tạo

Nhấn biểu tượng Start để thực hiện quá trình Scanning

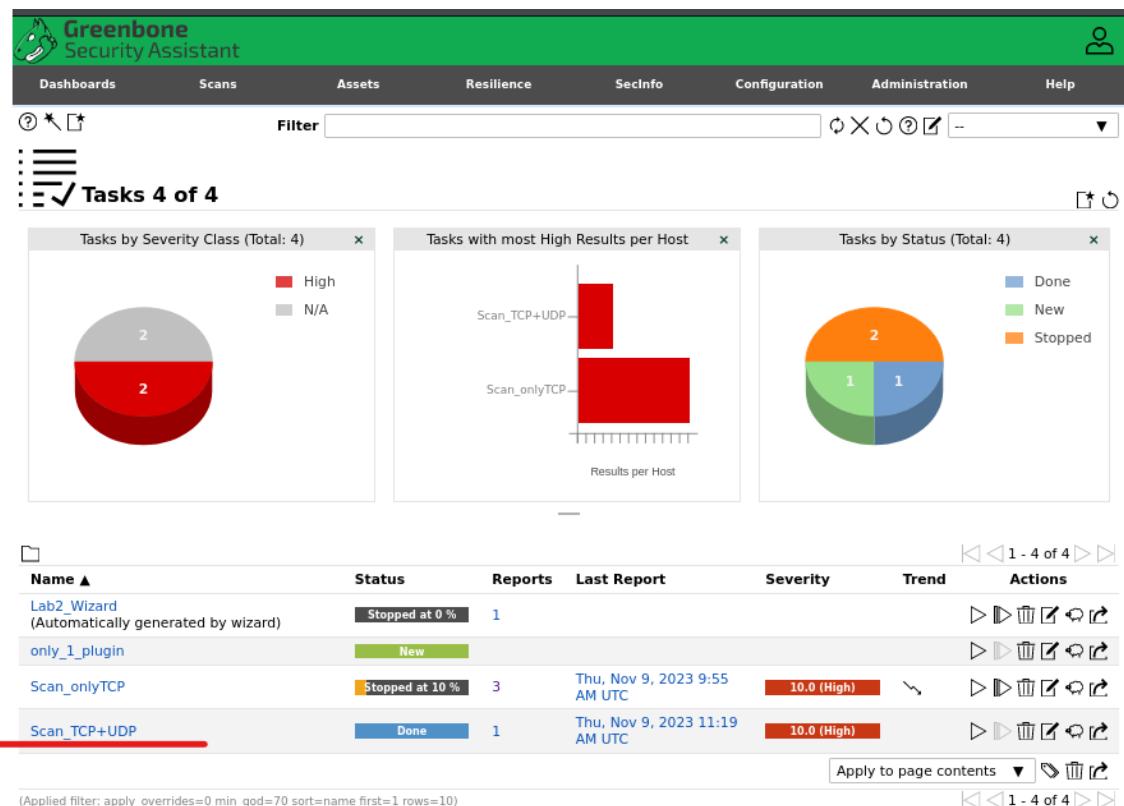


Đang quét

Nhóm 18



Hoàn thành quét target



- Sau khi quét xong, vô mục Scans -> chọn Reports để xem các kết quả tìm được

Nhóm 18

The screenshot shows the Greenbone Security Assistant web interface. At the top, there's a navigation bar with links for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. Below the navigation is a search/filter bar and a toolbar with various icons.

The main area displays three reports:

- Reports by Severity Class (Total: 5)**: A pie chart showing the distribution of severity levels: N/A (grey), Medium (orange), and High (red). The data is: N/A: 1, Medium: 1, High: 3.
- Reports with High Results**: A line graph showing the number of high-severity reports over time. The Y-axis is labeled "Max High" and ranges from 0 to 28. The X-axis shows dates: Wed 08, 12 PM, Thu 09. A dashed line shows the trend, with a peak at 28 on Wednesday afternoon.
- Reports by CVSS (Total: 5)**: A bar chart showing the number of reports per CVSS severity level. The Y-axis is labeled "# of Reports" and ranges from 0.0 to 3.0. The X-axis is labeled "Severity". The data is: Low: 1.0 (grey), Medium: 1.0 (orange), High: 3.0 (red).

Below the reports is a table of tasks:

| Date | Status | Task | Severity | High | Medium | Low | Log | False Pos. | Actions |
|-------------------------------|----------------|--------------|-------------|------|--------|-----|-----|------------|---------|
| Thu, Nov 9, 2023 11:23 AM UTC | Stopped at 0 % | Lab2_Wizard | N/A | 0 | 0 | 0 | 0 | 0 | Δ X |
| Thu, Nov 9, 2023 11:19 AM UTC | Done | Scan_TCP+UDP | 10.0 (High) | 8 | 30 | 5 | 59 | 0 | Δ X |

- Nhấn vào đối tượng muốn xem report để hiện ra bản report chi tiết

The screenshot shows a detailed report table with the following columns: Vulnerability, Severity, QoD, Host IP, Name, Location, and Created.

| Vulnerability | Severity | QoD | Host IP | Name | Location | Created |
|---|-------------|------|-----------------|----------------|-------------|-------------------------------|
| TWiki XSS and Command Execution Vulnerabilities | 10.0 (High) | 80 % | 192.168.142.136 | METASPLOITABLE | 80/tcp | Thu, Nov 9, 2023 11:35 AM UTC |
| Operating System (OS) End of Life (EOL) Detection | 10.0 (High) | 80 % | 192.168.142.136 | METASPLOITABLE | general/tcp | Thu, Nov 9, 2023 11:33 AM UTC |
| phpinfo() output Reporting | 7.5 (High) | 80 % | 192.168.142.136 | METASPLOITABLE | 80/tcp | Thu, Nov 9, 2023 11:35 AM UTC |
| vsftpd Compromised Source Packages Backdoor Vulnerability | 7.5 (High) | 99 % | 192.168.142.136 | METASPLOITABLE | 6200/tcp | Thu, Nov 9, 2023 11:37 AM UTC |
| vsftpd Compromised Source Packages Backdoor Vulnerability | 7.5 (High) | 99 % | 192.168.142.136 | METASPLOITABLE | 21/tcp | Thu, Nov 9, 2023 11:37 AM UTC |
| Test HTTP dangerous methods | 7.5 (High) | 99 % | 192.168.142.136 | METASPLOITABLE | 80/tcp | Thu, Nov 9, 2023 11:39 AM UTC |
| FTP Brute Force Logins Reporting | 7.5 (High) | 95 % | 192.168.142.136 | METASPLOITABLE | 21/tcp | Thu, Nov 9, 2023 11:37 AM UTC |

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

Bước 1: OpenVAS thực hiện quá trình Requested

Nó sẽ gửi gói tin ARP để tìm địa chỉ MAC của target

The figure shows a screenshot of the Wireshark application interface. At the top, there's a menu bar with File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for file operations like Open, Save, and Print, as well as search and selection tools. A status bar at the top right says "Capturing from eth0". The main area is a table representing network traffic. The columns are labeled No., Time, Source, Destination, Protocol, Length, and Info. The table contains several rows of data, with the first five rows highlighted in blue. The last row is highlighted in yellow. The "Info" column provides detailed information about each packet, such as port numbers and sequence numbers.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-----------------|-----------------|----------|--------|---|
| 1 | 0.000000000 | 192.168.142.129 | 34.107.243.93 | TLSv1.2 | 93 | Application Data |
| 2 | 0.000061191 | 192.168.142.129 | 34.149.100.209 | TLSv1.2 | 100 | Application Data |
| 3 | 0.000294252 | 34.107.243.93 | 192.168.142.129 | TCP | 60 | 443 → 41314 [ACK] Seq=1 Ack=40 Win=64240 Len=0 |
| 4 | 0.000294388 | 34.149.100.209 | 192.168.142.129 | TCP | 60 | 443 → 47300 [ACK] Seq=1 Ack=47 Win=64240 Len=0 |
| 5 | 0.044833436 | 34.107.243.93 | 192.168.142.129 | TLSv1.2 | 93 | Application Data |
| 6 | 0.044833655 | 34.149.100.209 | 192.168.142.129 | TLSv1.2 | 100 | Application Data |
| 7 | 0.044868042 | 192.168.142.129 | 34.107.243.93 | TCP | 54 | 41314 → 443 [ACK] Seq=40 Ack=40 Win=64028 Len=0 |
| 8 | 0.044892564 | 192.168.142.129 | 34.149.100.209 | TCP | 54 | 47300 → 443 [ACK] Seq=47 Ack=47 Win=64015 Len=0 |
| 9 | 5.166844461 | VMware_64:0b:77 | VMware_e8:21:21 | ARP | 42 | Who has 192.168.142.2? Tell 192.168.142.129 |
| 10 | 5.166927379 | VMware_e8:21:21 | VMware_64:0b:77 | ARP | 60 | 192.168.142.2 is at 00:50:56:e8:21:21 |

Bước 2: OpenVAS thực hiện quá trình Queue

Nó thực hiện ping tới target

| | | | | | | |
|----|--------------|-----------------|-----------------|------|----------------------------|--|
| 11 | 51.032696650 | 192.168.142.129 | 192.168.142.136 | ICMP | 98 Echo (ping) request | id=0xff7f, seq=0/0, ttl=64 |
| 12 | 51.033462213 | 192.168.142.136 | 192.168.142.129 | ICMP | 98 Echo (ping) reply | id=0xff7f, seq=0/0, ttl=64 |
| 13 | 51.308963495 | 192.168.142.129 | 192.168.142.2 | DNS | 88 Standard query | 0x8b69 PTR 136.142.168.192.in-addr.arpa. |
| 14 | 51.352340835 | 192.168.142.2 | 192.168.142.129 | DNS | 88 Standard query response | 0x8b69 No such name PTR |

Bước 3: Open VAS thực hiện quá trình Scanning

OpenVAS gửi hàng loạt các gói tin đến target tại các UDP port nằm trong danh sách Port List mà ta đã chọn

| | | | | | |
|----|-------------|-----------------|-----------------|------|---|
| 7 | 1.143792029 | 192.168.142.129 | 192.168.142.136 | UDP | 42 59308 → 81 Len=0 |
| 8 | 1.143848110 | 192.168.142.129 | 192.168.142.136 | UDP | 42 59308 → 162 Len=0 |
| 9 | 1.143879356 | 192.168.142.129 | 192.168.142.136 | UDP | 42 59308 → 147 Len=0 |
| 10 | 1.143916203 | 192.168.142.129 | 192.168.142.136 | UDP | 42 59308 → 130 Len=0 |
| 11 | 1.143951822 | 192.168.142.129 | 192.168.142.136 | UDP | 42 59308 → 120 Len=0 |
| 12 | 1.143975466 | 192.168.142.136 | 192.168.142.129 | ICMP | 70 Destination unreachable (Port unreachable) |
| 13 | 1.143975602 | 192.168.142.136 | 192.168.142.129 | ICMP | 70 Destination unreachable (Port unreachable) |
| 14 | 1.143986783 | 192.168.142.129 | 192.168.142.136 | UDP | 42 59308 → 166 Len=0 |
| 15 | 1.144012067 | 192.168.142.129 | 192.168.142.136 | UDP | 42 59308 → 79 Len=0 |
| 16 | 1.144025920 | 192.168.142.136 | 192.168.142.129 | ICMP | 70 Destination unreachable (Port unreachable) |
| 17 | 1.144025952 | 192.168.142.136 | 192.168.142.129 | ICMP | 70 Destination unreachable (Port unreachable) |
| 18 | 1.144036257 | 192.168.142.129 | 192.168.142.136 | UDP | 42 59308 → 154 Len=0 |
| 19 | 1.144037162 | 192.168.142.136 | 192.168.142.129 | ICMP | 70 Destination unreachable (Port unreachable) |
| 20 | 1.144060915 | 192.168.142.136 | 192.168.142.129 | ICMP | 70 Destination unreachable (Port unreachable) |
| 21 | 1.144063144 | 192.168.142.129 | 192.168.142.136 | UDP | 42 59308 → 173 Len=0 |
| 22 | 1.144087216 | 192.168.142.129 | 192.168.142.136 | UDP | 42 59308 → 14 Len=0 |
| 23 | 1.156199810 | 192.168.142.129 | 192.168.142.136 | UDP | 42 59308 → 44 Len=0 |
| 24 | 1.156248473 | 192.168.142.129 | 192.168.142.136 | UDP | 42 59308 → 25 Len=0 |
| 25 | 1.156278555 | 192.168.142.129 | 192.168.142.136 | UDP | 42 59308 → 60 Len=0 |

=> Có gói gửi thành công, có gói tin không được gửi thành công (VD: target gửi 1 gói tin tới port 81 trên máy tính thực hiện quét nhưng port này không hoạt động dẫn tới drop gói tin)

Sau khi gửi gói tin đến tất cả các UDP port thì OpenVAS sẽ tiến hành gửi hàng loạt gói tin tới TCP port của target

=> Quá trình này không xảy ra hiên tượng Destination unreachable

Bước 4: OpenVAS hoàn tất quá trình quét (Done)

OpenVAS sẽ xuất ra bản report ghi lại chi tiết các lỗ hổng mà nó quét được

E) Quét lỗ hổng sử dụng tài khoản chứng thực

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

- Truy cập vô mục Configuration -> chọn Credentials trong trang hiện ra chọn biểu tượng New Credential

The screenshot shows the Greenbone Security Assistant web interface. At the top, there's a navigation bar with links like Kali Linux, Kali Tools, Kali Docs, etc. Below the bar, the title 'Greenbone Security Assistant' is displayed next to a logo. The main area has tabs for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. A search bar labeled 'Filter' is present. Below the search bar, there's a large key icon and the text 'Credentials 0 of 0'. Underneath, it says 'No credentials available' and '(Applied filter: sort=name first=1 rows=10)'. A red circle highlights the 'New Credential' icon, which is a key icon with a plus sign.

- Trong bảng New Credential

Nhập tên Credential trong trường Name

Nhập comment (nếu thích)

Chọn loại xác thực trong trường Type

Sau đó nhập thông tin yêu cầu xác thực (ví dụ: username, password,...)

Cuối cùng nhấn Save

The screenshot shows the 'New Credential' dialog box. It has fields for Name (filled with 'Lab2'), Comment (filled with 'Metasploitable2'), Type (set to 'Username + Password'), Allow insecure use (radio button for 'No' is selected), Auto-generate (radio button for 'No' is selected), Username (filled with 'msfadmin'), and Password (redacted). At the bottom, there are 'Cancel' and 'Save' buttons.

Nhóm 18

- Sau khi lưu trong danh sách hiển thị các Credentials xuất hiện thêm tên Credential mới tạo xong

| Name | Type | Allow insecure use | Login | Actions |
|------------------------|--------------------------|--------------------|----------|---------|
| Lab2 (Metasploitable2) | Username + Password (up) | No | msfadmin | |

- Truy cập vô mục Configuration -> chọn Targets

Trong trang hiện ra chọn biểu tượng New Target



- Trong bảng New Target

Nhập tên target trong trường Name

Nhập Comment (không bắt buộc)

Nhập IP Address trong trường Hosts(Manual)

Chọn danh sách port muốn quét trong trường Port List

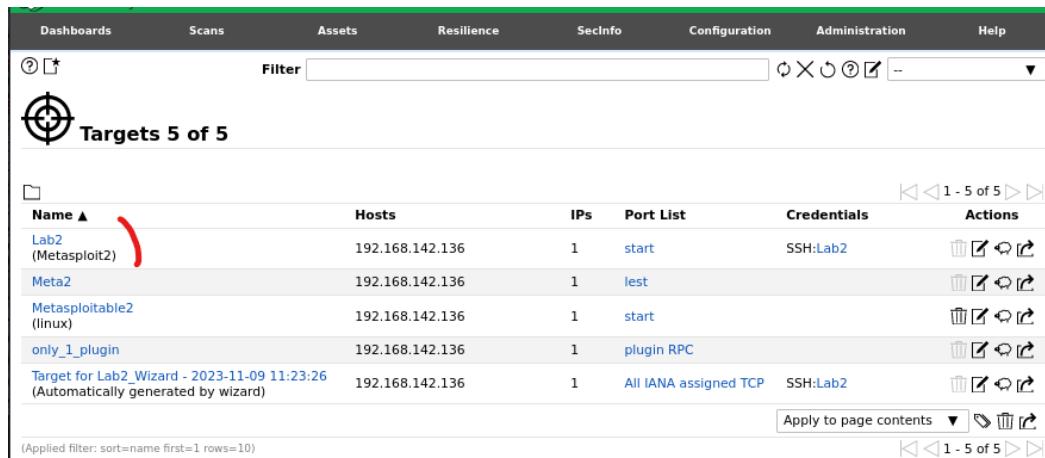
Chọn Credential trong trường SSH (mục Credentials for authenticated checks)

Sau đó nhấn Save để lưu

| | |
|--|--|
| Name | Lab2 |
| Comment | Metasploit2 |
| Hosts | <input checked="" type="radio"/> Manual 192.168.142.136 <input type="radio"/> From file <input type="button" value="Browse..."/> No file selected. |
| Exclude Hosts | <input checked="" type="radio"/> Manual <input type="text"/> <input type="radio"/> From file <input type="button" value="Browse..."/> No file selected. |
| Allow simultaneous scanning via multiple IPs | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Port List | <input type="button" value="start"/> <input type="button" value="stop"/> |
| Alive Test | <input type="button" value="Scan Config Default"/> |
| Credentials for authenticated checks SSH: Lab2 on port 22 <input type="checkbox"/> Elevate privileges | |
| <input type="button" value="Cancel"/> <input type="button" value="Save"/> | |

Nhóm 18

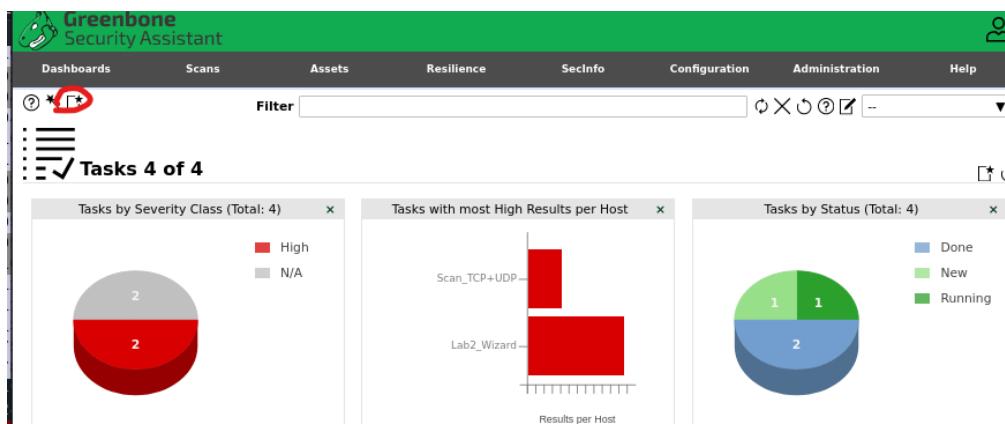
- Trong danh sách Targets xuất hiện tên target vừa mới tạo xong



| Name | Hosts | IPs | Port List | Credentials | Actions |
|---|-----------------|-----|-----------------------|-------------|---------|
| Lab2 (Metasploit2) | 192.168.142.136 | 1 | start | SSH:Lab2 | |
| Meta2 | 192.168.142.136 | 1 | test | | |
| Metasploitable2 (linux) | 192.168.142.136 | 1 | start | | |
| only_1_plugin | 192.168.142.136 | 1 | plugin RPC | | |
| Target for Lab2_Wizard - 2023-11-09 11:23:26 (Automatically generated by wizard) | 192.168.142.136 | 1 | All IANA assigned TCP | SSH:Lab2 | |

- Truy cập vô mục Scans -> chọn Task

Trong trang hiện ra chọn biểu tượng New Task



- Trong bảng New Task nhập các thông tin như trong ảnh dưới đây

Sau đó nhấn Save để lưu

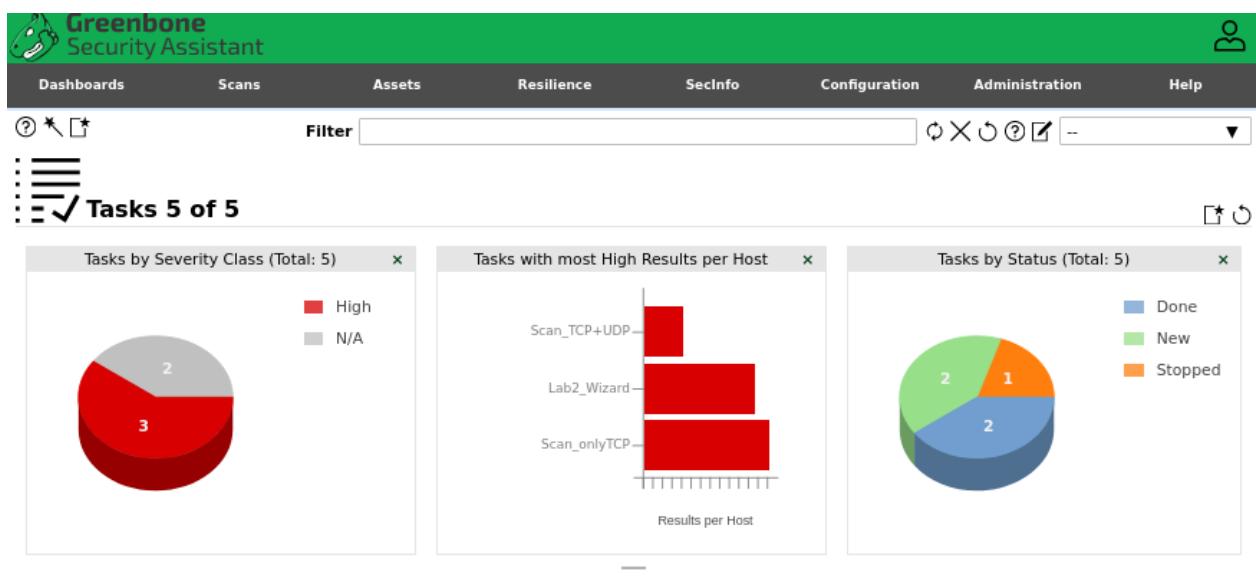
Nhóm 18

New Task

| | |
|-----------------------|--|
| Name | Credential |
| Comment | |
| Scan Targets | Lab2 |
| Alerts | |
| Schedule | -- |
| Add results to Assets | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Apply Overrides | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Min QoD | 70 % |
| Alterable Task | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Auto Delete Reports | <input checked="" type="radio"/> Do not automatically delete reports <input type="radio"/> Automatically delete oldest reports but always keep newest [5] reports |
| Scanner | OpenVAS Default |
| Scan Config | Full and fast |

Cancel **Save**

- Trong danh sách Tasks đã xuất hiện tên Task mới tạo



- Nhấn biểu tượng Start để bắt đầu quá trình quét

| Name | Status | Reports | Last Report | Severity | Trend | Actions |
|-------------|--------|---------|------------------------|----------|-------|---------|
| Credential | New | | | | | |
| Lab2_Wizard | New | | Thu, Nov 9, 2023 12:00 | | | |

- Hoàn thành quét target

| Name | Status | Reports | Last Report | Severity | Trend | Actions |
|------------|--------|---------|-------------------------------|-------------|-------|---------|
| Credential | Done | 1 | Thu, Nov 9, 2023 12:44 PM UTC | 10.0 (High) | | |

Nhóm 18

- Sau khi quét xong, vô mục Scans -> chọn Reports để xem các kết quả tìm được

The screenshot shows the 'Reports' section of the Greenbone Security Assistant. At the top, there are three charts: a pie chart for severity class (N/A: 3, Log: 1, High: 1), a line chart for high results over time, and a bar chart for CVSS. Below the charts is a table of scan results:

| Date | Status | Task | Severity | High | Medium | Low | Log | False Pos. | Actions |
|-------------------------------|--------|---------------|-------------|------|--------|-----|-----|------------|---------|
| Thu, Nov 9, 2023 1:35 PM UTC | Done | only_1_plugin | 0.0 (Log) | 0 | 0 | 0 | 1 | 0 | Δ X |
| Thu, Nov 9, 2023 12:44 PM UTC | Done | Credential | 10.0 (High) | 26 | 39 | 6 | 95 | 0 | Δ X |

- Nhấn vào đối tượng muốn xem report để hiện ra bản report chi tiết

The screenshot shows a detailed report for the scan on Nov 9, 2023, at 12:44 PM UTC. The report summary includes the date, ID, creation and modification times, and owner. Below the summary is a table of findings:

| Information | Results (71 of 601) | Hosts (1 of 1) | Ports (21 of 25) | Applications (17 of 17) | Operating Systems (1 of 1) | CVEs (33 of 33) | Closed CVEs (0 of 0) | TLS Certificates (2 of 2) | Error Messages (0 of 0) | User Tags (0) |
|---|---------------------|----------------|------------------|-------------------------|----------------------------|-----------------|----------------------|---------------------------|-------------------------|---------------|
| Vulnerability | | | | | | | | | | |
| Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities | 10.0 (High) | 99 % | 192.168.142.136 | | | | | | | |
| Operating System (OS) End of Life (EOL) Detection | 10.0 (High) | 80 % | 192.168.142.136 | | | | | | | |
| The rexec service is running | 10.0 (High) | 80 % | 192.168.142.136 | | | | | | | |
| rlogin Passwordless Login | 10.0 (High) | 80 % | 192.168.142.136 | | | | | | | |
| Possible Backdoor: Ingreslock | 10.0 (High) | 99 % | 192.168.142.136 | | | | | | | |
| TWiki XSS and Command Execution Vulnerabilities | 10.0 (High) | 80 % | 192.168.142.136 | | | | | | | |
| MySQL / MariaDB Default Credentials (MySQL Protocol) | 9.8 (High) | 95 % | 192.168.142.136 | | | | | | | |
| DistCC RCE Vulnerability (CVE-2004-2687) | 9.3 (High) | 99 % | 192.168.142.136 | | | | | | | |

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

- Quét sử dụng tài khoản chứng thực.

Nhóm 18

Report Date: Thu, Nov 9, 2023
Report Time: 12:44 PM UTC

| Vulnerability | Severity | QoD | Host IP | Name | Location | Created |
|---|-------------|------|-----------------|------|-------------|------------------------------|
| Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities | 10.0 (High) | 99 % | 192.168.142.136 | | 8787/tcp | Thu, Nov 9, 2023 1:11 PM UTC |
| Operating System (OS) End of Life (EOL) Detection | 10.0 (High) | 80 % | 192.168.142.136 | | general/tcp | Thu, Nov 9, 2023 1:05 PM UTC |
| The reexec service is running | 10.0 (High) | 80 % | 192.168.142.136 | | 512/tcp | Thu, Nov 9, 2023 1:08 PM UTC |
| rlogin Passwordless Login | 10.0 (High) | 80 % | 192.168.142.136 | | 513/tcp | Thu, Nov 9, 2023 1:03 PM UTC |
| Possible Backdoor: Ingreslock | 10.0 (High) | 99 % | 192.168.142.136 | | 1524/tcp | Thu, Nov 9, 2023 1:14 PM UTC |
| TWiki XSS and Command Execution Vulnerabilities | 10.0 (High) | 80 % | 192.168.142.136 | | 80/tcp | Thu, Nov 9, 2023 1:09 PM UTC |
| MySQL / MariaDB Default Credentials (MySQL Protocol) | 9.8 (High) | 95 % | 192.168.142.136 | | 3306/tcp | Thu, Nov 9, 2023 1:11 PM UTC |
| DistCC RCE Vulnerability (CVE-2004-2687) | 9.3 (High) | 99 % | 192.168.142.136 | | 3632/tcp | Thu, Nov 9, 2023 1:11 PM UTC |
| VNC Brute Force Login | 9.0 (High) | 95 % | 192.168.142.136 | | 5900/tcp | Thu, Nov 9, 2023 1:10 PM UTC |
| PostgreSQL Default Credentials (PostgreSQL Protocol) | 9.0 (High) | 99 % | 192.168.142.136 | | 5432/tcp | Thu, Nov 9, 2023 1:11 PM UTC |

- Quét không sử dụng tài khoản chứng thực

Report Date: Wed, Nov 8, 2023
Report Time: 2:36 PM UTC

| Vulnerability | Severity | QoD | Host IP | Name | Location | Created |
|---|-------------|------|-----------------|------|-------------|------------------------------|
| Operating System (OS) End of Life (EOL) Detection | 10.0 (High) | 80 % | 192.168.142.136 | | general/tcp | Wed, Nov 8, 2023 2:56 PM UTC |
| Possible Backdoor: Ingreslock | 10.0 (High) | 99 % | 192.168.142.136 | | 1524/tcp | Wed, Nov 8, 2023 3:04 PM UTC |
| rlogin Passwordless Login | 10.0 (High) | 80 % | 192.168.142.136 | | 513/tcp | Wed, Nov 8, 2023 2:53 PM UTC |
| Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities | 10.0 (High) | 99 % | 192.168.142.136 | | 8787/tcp | Wed, Nov 8, 2023 3:01 PM UTC |
| TWiki XSS and Command Execution Vulnerabilities | 10.0 (High) | 80 % | 192.168.142.136 | | 80/tcp | Wed, Nov 8, 2023 2:59 PM UTC |
| The reexec service is running | 10.0 (High) | 80 % | 192.168.142.136 | | 512/tcp | Wed, Nov 8, 2023 2:57 PM UTC |
| MySQL / MariaDB Default Credentials (MySQL Protocol) | 9.8 (High) | 95 % | 192.168.142.136 | | 3306/tcp | Wed, Nov 8, 2023 3:01 PM UTC |

Nhận xét: 2 cách quét cho kết quả tuy có nhiều chỗ giống nhau nhưng nhìn chung vẫn có độ chính xác cao

Nhưng khi quét có tài khoản chứng thực thì kết quả không chính xác giảm đáng kể so với khi quét không có 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.

| | Ưu điểm | Khuyết điểm |
|--------------------------|---|---|
| Credentialed Sscanning | <ul style="list-style-type: none"> + Cung cấp phân tích sâu và toàn diện về các lỗ hổng + Cung cấp các kết quả chính xác hơn. + Giúp xác minh các biện pháp bảo mật đang hoạt động hiệu quả. + Giúp nhận biết các lỗ hổng dựa trên mức độ nghiêm trọng và mức độ rủi ro của chúng. | <ul style="list-style-type: none"> + Thời gian quét khá lâu + Phải biết có quyền truy cập vào target (hay phải biết chính xác username và password) |
| Uncredentialed Sscanning | <ul style="list-style-type: none"> + Nó hữu ích trong việc xác định các lỗ hổng cơ bản có thể bị tấn công khai thác. + Cung cấp cái nhìn tổng quan nhanh về các lỗ hổng tiềm ẩn của hệ thống + Quét kể cả khi không có quyền truy cập quản trị vào target | <ul style="list-style-type: none"> + Bị giới hạn về phạm vi và cung cấp kết quả kém chính xác hơn so với kiểu quét được chứng nhận. |

F) Quét với Plugin được chỉ định

7. Thực hiện lại các bước trên để quét máy Metasploitable 2 sử dụng 1 plugin Nfs-utils rpc.rquotad Service Detection

Vì plugin này thuộc Family: RPC mà RPC chạy trên TCP port 111 nên chúng ta sẽ chỉ scan duy nhất 1 plugin tại port 111 này thôi.

- Truy cập vô mục Configuration -> Scan Configs

Trong trang hiện ra chọn biểu tượng New Scan Config để tạo chế độ quét mới

Nhóm 18

| Name ▲ | Family | | NVTs | | Actions |
|--|--------|-------|--------|-------|---|
| | Total | Trend | Total | Trend | |
| Base (Basic configuration template with a minimum set of NVTs required for a scan. Version 20200827.) | 2 | → | 3 | → | trash edit copy refresh |
| Discovery (Network Discovery scan configuration. Version 20201215.) | 10 | → | 3207 | ↗ | trash edit copy refresh |
| empty (Empty and static configuration template. Version 20201215.) | 1 | → | 1 | → | trash edit copy refresh |
| Full and fast (Most NVT's; optimized by using previously collected information. Version 20201215.) | 58 | ↗ | 133175 | ↗ | trash edit copy refresh |
| Host Discovery (Network Host Discovery scan configuration. Version 20201215.) | 2 | → | 2 | → | trash edit copy refresh |
| Log4Shell (Configuration with checks for Log4j and CVE-2021-44228. Version 20211227.) | 10 | → | 29 | → | trash edit copy refresh |
| System Discovery (Network System Discovery scan configuration. Version 20201215.) | 5 | → | 30 | → | trash edit copy refresh |

(Applied filter: sort=name first=1 rows=10) Apply to page contents trash refresh

◀◀ 1 - 7 of 7 ▶▶

- Trong bảng New Scan Config, nhập tên cấu hình trong trường Name, chọn loại cấu hình chung

New Scan Config

Name: only_1_plugin

Comment:

Base:

- Base with a minimum set of NVTs
- Empty, static and fast
- Full and fast
- OpenVAS Default

Cancel Save

- Trong danh sách Scan Configs, xuất hiện thêm tên cấu hình mới vừa tạo
Để thiết lập việc chỉ quét 1 plugin (được chỉ định), ta cần phải sửa lại chi tiết hơn
Chọn biểu tượng Edit Scan Config tại đối tượng muốn sửa

Nhóm 18

 Scan Configs 8 of 8

| Name | Family | NVTs | Actions | | |
|--|--------|-------|---------|-------|--|
| | Total | Trend | Total | Trend | |
| Base (Basic configuration template with a minimum set of NVTs required for a scan. Version 20200827.) | 2 | → | 3 | → | |
| Discovery (Network Discovery scan configuration. Version 20201215.) | 10 | → | 3207 | ↗ | |
| empty (Empty and static configuration template. Version 20201215.) | 1 | → | 1 | → | |
| Full and fast (Most NVT's; optimized by using previously collected information. Version 20201215.) | 58 | ↗ | 133175 | ↗ | |
| Host Discovery (Network Host Discovery scan configuration. Version 20201215.) | 2 | → | 2 | → | |
| Log4Shell (Configuration with checks for Log4j and CVE-2021-44228. Version 20211227.) | 10 | → | 29 | → | |
| only_1_plugin (Empty and static configuration template. Version 20201215.) | 1 | → | 1 | → | |
| System Discovery (Network System Discovery scan configuration. Version 20201215.) | 5 | → | 30 | → | |

Apply to page contents

(Applied filter: sort=name first=1 rows=10) 1 - 8 of 8

- Trong bảng Edit Scan Config của đối tượng được chọn

Nhấn vô ô vuông nếu muốn quét các plugin thuộc family đó

Chọn biểu tượng Edit Scan Config Family tại dòng có family của plugin mình muốn quét

Edit Scan Config only_1_plugin

| | | | | |
|---------------------------------|------------|---|-------------------------------------|--|
| Privilege escalation | 0 of 151 | → | <input type="checkbox"/> | |
| Product detection | 0 of 2934 | → | <input type="checkbox"/> | |
| RPC | 0 of 4 | → | <input checked="" type="checkbox"/> | |
| Red Hat Local Security Checks | 0 of 1853 | → | <input type="checkbox"/> | |
| Remote file access | 0 of 56 | → | <input type="checkbox"/> | |
| SMTP problems | 0 of 49 | → | <input type="checkbox"/> | |
| SNMP | 0 of 12 | → | <input type="checkbox"/> | |
| SSL and TLS | 0 of 85 | → | <input type="checkbox"/> | |
| Service detection | 0 of 253 | → | <input type="checkbox"/> | |
| Settings | 0 of 11 | → | <input type="checkbox"/> | |
| Slackware Local Security Checks | 0 of 1491 | → | <input type="checkbox"/> | |
| Solaris Local Security Checks | 0 of 1 | → | <input type="checkbox"/> | |
| SuSE Local Security Checks | 0 of 18348 | → | <input type="checkbox"/> | |
| Ubuntu Local Security Checks | 0 of 13309 | → | <input type="checkbox"/> | |
| Useless services | 0 of 16 | → | <input type="checkbox"/> | |
| VMware Local Security Checks | 0 of 57 | → | <input type="checkbox"/> | |

Apply to page contents

- Bảng Edit Scan Config Family tương ứng với family mình đã chọn hiện ra

Nó thể hiện các plugin thuộc family đó mà OpenVAS chạy scan được

Nhấn vô vuông của plugin mà mình muốn thực hiện

Sau đó nhấn Save để lưu

The screenshot shows the 'Edit Scan Config Family RPC' dialog box. It contains a table of network vulnerability tests (NVTs) with the following columns: Name, OID, Severity, Timeout, Prefs, Selected, and Actions. One row is selected, indicated by a checked 'Selected' checkbox in the Actions column. There are two 'Save' buttons at the bottom of the dialog.

- Tiếp tục nhấn Save trong bảng Edit Scan Config

Trong danh sách Scan Configs, Scan Config mà ta tạo ra xuất hiện sự thay đổi

The screenshot shows the 'Scan Configs' list in the Greenbone Security Assistant. The 'only_1_plugin' configuration is listed with the following details:

| Name | Family | NVTs | Actions |
|---------------|--------------------|--------------------|----------------------|
| only_1_plugin | Total: 1, Trend: → | Total: 4, Trend: → | [Delete, Edit, Copy] |

Below the table, there is a note: '(Empty and static configuration template. Version 20201215.)'.

- Vì chỉ quét tại 1 port duy nhất nên ta phải tạo danh sách port mới

Truy cập vô mục Configuration -> chọn Port Lists -> chọn biểu tượng New Port List

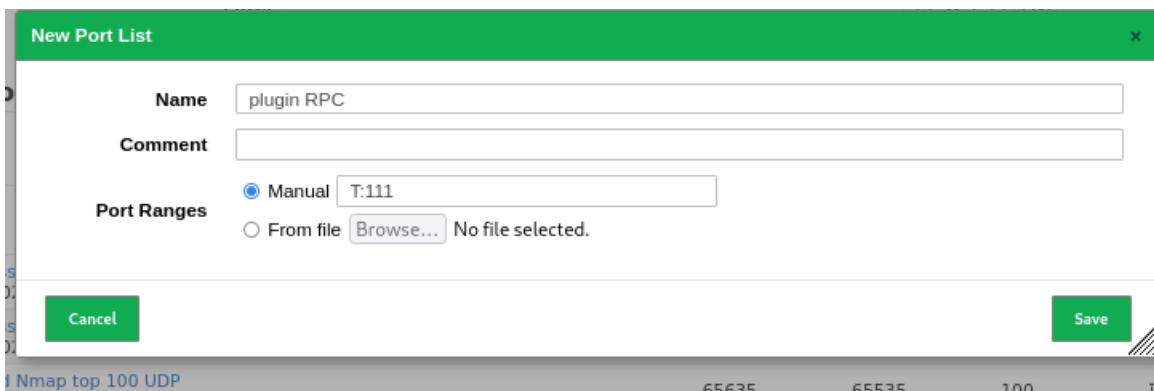
Nhập tên danh sách sẽ tạo trong trường Name

Nhập comment (không bắt buộc)

Chọn port muốn quét tại trường Port Ranges (Manual)

Nhóm 18

Sau đó nhấn Save để lưu



- Trong danh sách Portlists xuất hiện tên danh sách mới vừa tạo

| Name | Total | TCP | UDP | Actions |
|--|--------|-------|-------|---------|
| All IANA assigned TCP (Version 20200827.) | 5836 | 5836 | 0 | |
| All IANA assigned TCP and UDP (Version 20200827.) | 11318 | 5836 | 5482 | |
| All TCP and Nmap top 100 UDP (Version 20200827.) | 65635 | 65535 | 100 | |
| plugin RPC | 1 | 1 | 0 | |
| start | 65535 | 65535 | 0 | |
| start_TCP+UDP | 131070 | 65535 | 65535 | |

- Tạo 1 target mới với thiết lập portlist và scan config mới tạo

Truy cập vô mục Configuration -> chọn Targets

Trong trang Targets hiện ra, chọn biểu tượng New Target

- Trong bảng New Target, nhập các thông tin như ảnh bên dưới

Nhóm 18

The screenshot shows the 'Targets' section of the Metasploit Framework. A 'New Target' dialog box is open, prompting for target configuration. The 'Name' field is set to 'only_1_plugin'. The 'Hosts' section shows a manual entry of '192.168.142.136'. The 'Exclude Hosts' section is empty. The 'Allow simultaneous scanning via multiple IPs' option is set to 'Yes'. The 'Port List' is set to 'plugin RPC'. The 'Alive Test' is set to 'Scan Config Default'. Under 'Credentials for authenticated checks', there is a section for 'SSH' with a dropdown set to '--' and a port of '22'. A 'Save' button is visible at the bottom right of the dialog.

- Kiểm tra xem đã có tên target mới tạo trong danh sách Targets chưa

The screenshot shows the 'Targets' section of the Metasploit Framework. A table lists four targets: 'Lab2 (Metasploit2)', 'Meta2', 'Metasploitable2 (linux)', and 'only_1_plugin'. The table includes columns for 'Name', 'Hosts', 'IPs', 'Port List', 'Credentials', and 'Actions'. The 'Actions' column contains icons for delete, edit, refresh, and copy. The 'Port List' column shows values like 'start_TCP+UDP', 'All IANA assigned TCP and UDP', 'start', and 'plugin RPC'. The 'Credentials' column shows entries like 'SSH:Lab2'. The 'Targets' section header indicates 'Targets 4 of 4'.

- Tạo task thực hiện quét với 1 plugin cụ thể chỉ tại port 111

Truy cập vô mục Scans -> chọn Tasks

Trong trang Tasks hiện ra, chọn biểu tượng New Task

- Trong bảng New Task, điền các thông tin như ảnh bên dưới

Sau đó nhấn Save để lưu

New Task

Name: only_1_plugin

Comment:

Scan Targets: only_1_plugin

Alerts:

Schedule: -- Once

Add results to Assets: Yes

Apply Overrides: Yes

Min QoD: 70 %

Alterable Task: No

Auto Delete Reports: Do not automatically delete reports

Scanner: OpenVAS Default

Scan Config: only_1_plugin

Cancel Save

- Trong danh sách Task đã có tên task vừa tạo

Nhấn biểu tượng Start để bắt đầu Scanning

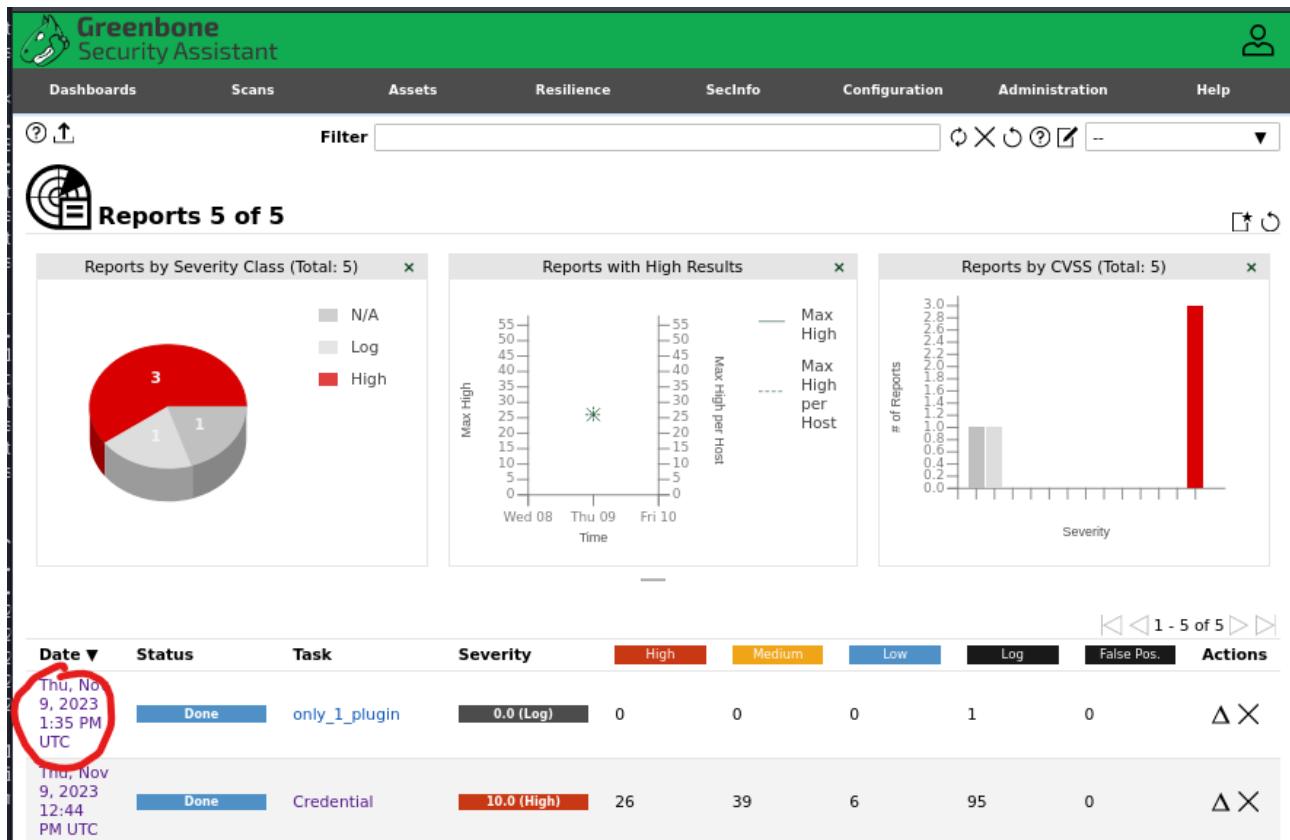
| Name | Status | Reports | Last Report | Severity | Trend | Actions |
|---------------|--------|---------|-------------------------------|-------------|-------|---------|
| Scan_TCP+UDP | Done | 1 | Thu, Nov 9, 2023 11:19 AM UTC | 10.0 (High) | | |
| only_1_plugin | New | | | | | |

- Hoàn thành quét target

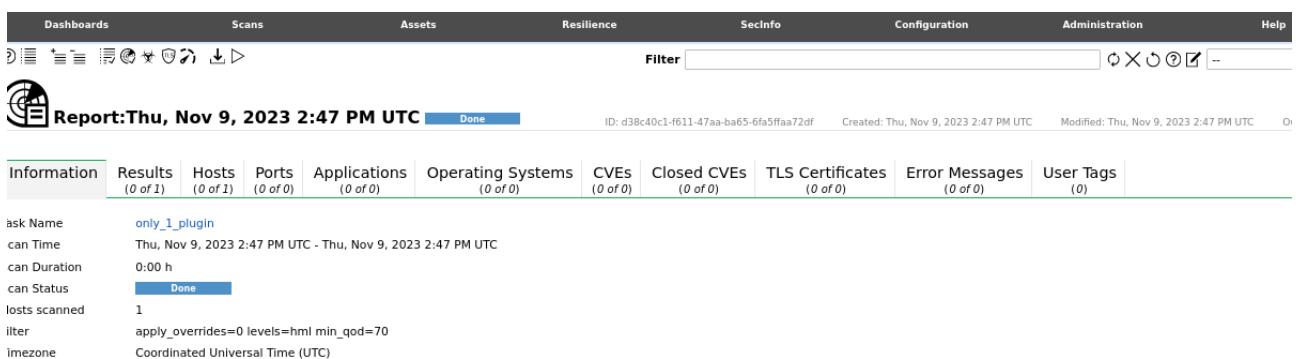
| Name | Status | Reports | Last Report | Severity | Trend | Actions |
|---------------|--------|---------|-------------------------------|-------------|-------|---------|
| Scan_TCP+UDP | Done | 1 | Thu, Nov 9, 2023 11:19 AM UTC | 10.0 (High) | | |
| only_1_plugin | Done | 1 | Thu, Nov 9, 2023 1:35 PM UTC | 0.0 (Log) | | |

Nhóm 18

- Sau khi quét xong, vô mục Scans -> chọn Reports để xem các kết quả tìm được



- Nhấn vào đối tượng muốn xem report để hiện ra bản report chi tiết



=> không phát hiện lỗ hổng nào khi chạy plugin Nfs-utils rpc.rquotad Service Detection

- Dùng Wireshark để kiểm tra

Nhóm 18

Wireshark Network Statistics

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-----------------|-----------------|----------|--------|--|
| 1 | 0.000000000 | 192.168.142.129 | 192.168.142.136 | ICMP | 98 | Echo (ping) request id=0xff7f, seq=0/0, ttl=64 |
| 2 | 0.000206590 | 192.168.142.136 | 192.168.142.129 | ICMP | 98 | Echo (ping) reply id=0xff7f, seq=0/0, ttl=64 |
| 3 | 0.474668721 | 192.168.142.129 | 192.168.142.2 | DNS | 88 | Standard query 0x2bbc PTR 136.142.168.192.in-addr.arpa |
| 4 | 0.528461691 | 192.168.142.2 | 192.168.142.129 | DNS | 88 | Standard query response 0x2bbc No such name PTR |
| 5 | 0.887388338 | VMware_64:0b:77 | Broadcast | ARP | 42 | Who has 192.168.142.136? Tell 192.168.142.129 |
| 6 | 0.887564809 | VMware_08:95:86 | VMware_64:0b:77 | ARP | 60 | 192.168.142.136 is at 00:0c:29:08:95:86 |
| 7 | 0.931263213 | 192.168.142.129 | 192.168.142.2 | DNS | 88 | Standard query 0xe0e6 PTR 136.142.168.192.in-addr.arpa |
| 8 | 0.943040861 | 192.168.142.2 | 192.168.142.129 | DNS | 88 | Standard query response 0xe0e6 No such name PTR |
| 9 | 2.055879788 | 192.168.142.129 | 192.168.142.136 | ICMP | 42 | Echo (ping) request id=0x56fa, seq=256/1, ttl=64 |
| 10 | 2.056693711 | 192.168.142.136 | 192.168.142.129 | ICMP | 60 | Echo (ping) reply id=0x56fa, seq=256/1, ttl=64 |
| 11 | 2.211855378 | 192.168.142.129 | 192.168.142.136 | ICMP | 66 | Timestamp request id=0x8193, seq=0/0, ttl=64 |
| 12 | 2.212272585 | 192.168.142.136 | 192.168.142.129 | ICMP | 60 | Timestamp reply id=0x8193, seq=0/0, ttl=64 |
| 13 | 2.365502496 | 192.168.142.129 | 192.168.142.136 | ICMP | 46 | Address mask request id=0x4bab, seq=0/0, ttl=64 |
| 14 | 3.517980207 | 192.168.142.129 | 192.168.142.136 | ICMP | 46 | Address mask request id=0x4bab, seq=0/0, ttl=64 |
| 15 | 4.686499992 | 192.168.142.129 | 192.168.142.136 | ICMP | 42 | Information request id=0x05e7, seq=0/0, ttl=64 |
| 16 | 5.824364475 | 192.168.142.129 | 192.168.142.136 | ICMP | 42 | Information request id=0x05e7, seq=0/0, ttl=64 |
| 17 | 7.099712121 | 192.168.142.129 | 192.168.142.136 | DNS | 112 | Unknown operation (11) 0x5858 [Malformed Packet] |
| 18 | 7.100069837 | 192.168.142.136 | 192.168.142.129 | ICMP | 140 | Destination unreachable (Port unreachable) |
| 19 | 40 398098522 | 192.168.142.129 | 34.117.237.239 | TLSv1.2 | 93 | Application Data |

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No. Time Source Destination Protocol Length Info

Frame 56: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0

Ethernet II, Src: VMware_64:0b:77 (00:0c:29:64:0b:77), Dst: VMware_e8:21:21 (00:0c:29:64:0b:77)

Internet Protocol Version 4, Src: 192.168.142.129, Dst: 34.107.243.93

Transmission Control Protocol, Src Port: 38496, Dst Port: 443, Seq: 0, Len: 74

0000 00 50 56 e8 21 21 00 0c 29 64 0b 77 08
0010 00 3c 78 52 40 00 40 06 5d 77 c0 a8 8e
0020 f3 5d 96 60 01 b1 a3 db 23 db 00 00 00
0030 fa f0 65 21 00 00 02 04 05 b4 04 02 08
0040 26 ed 00 00 00 00 01 03 03 07

Packets: 172 · Displayed: 172 (100.0%) · Profile: Default

=> Việc quét dien ra thuận lợi

8. Thực hiện quét lại sử dụng các plugin khác.

Truy cập vô Edit Scan Config của only_1_plugin -> chọn Edit Scan Config Family của RPC
 Nhấn vô hết các ô vuông để chạy tất cả các plugin thuộc RPC mà OenVAS có
 Sau đó nhấn Save để lưu

The screenshot shows the 'Edit Scan Config Family RPC' interface. At the top, it displays 'Config Family' as 'only_1_plugin' and 'RPC'. Below this is a section titled 'Edit Network Vulnerability Tests' containing a table with four rows of test details. At the bottom of this section are 'Cancel' and 'Save' buttons. Below this is another section titled 'Edit Local Security Checks' with three rows of check details. At the bottom of this section are 'Cancel' and 'Save' buttons.

| Name | OID | Severity | Timeout | Prefs | Selected | Actions |
|---|------------------------------|----------|---------|-------|-------------------------------------|-------------------------------------|
| CDE ToolTalk RPC Database Server Multiple Vulnerabilities | 1.3.6.1.4.1.25623.1.0.902477 | N/A | default | 0 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Calendar Manager Service rpc.cmsd Service Detection | 1.3.6.1.4.1.25623.1.0.802163 | N/A | default | 0 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Kcms Profile Server | 1.3.6.1.4.1.25623.1.0.10832 | N/A | default | 0 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Nfs-utils rpc.rquotad Service Detection | 1.3.6.1.4.1.25623.1.0.802137 | N/A | default | 0 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

| Category | Count | Status | Action |
|------------------------------|------------|--|-------------------------------------|
| Ubuntu Local Security Checks | 0 of 13309 | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> | <input type="checkbox"/> |
| Useless services | 0 of 16 | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> | <input checked="" type="checkbox"/> |
| VMware Local Security Checks | 0 of 57 | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> | <input checked="" type="checkbox"/> |

- Kiểm tra lại cấu hình của đối tượng trong danh sách scan configs

The screenshot shows a list of scan configurations. One configuration is selected, labeled 'only_1_plugin' with the note '(Empty and static configuration template. Version 20201215.)'. The number '4' is circled in red at the top right of the list area.

- Tạo lại 1 task mới với scan config mới tạo

Sau đó nhấn biểu tượng Start để scanning

The screenshot shows a list of tasks. One task is highlighted, labeled 'plugins_RPC' with the status 'New'. A red circle highlights the 'Start' button next to this task. The table includes columns for Name, Status, Reports, Last Report, Severity, Trend, and Action.

| Name | Status | Reports | Last Report | Severity | Trend | Action |
|--|----------------|---------|-------------------------------|-------------|-------|--|
| Scan_TCP+UDP | Done | 1 | Thu, Nov 9, 2023 11:19 AM UTC | 10.0 (High) | | <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |
| plugins_RPC | New | | | | | <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |
| Lab2_Wizard (Automatically generated by wizard) | Done | 2 | Thu, Nov 9, 2023 12:00 PM UTC | 10.0 (High) | | <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |
| Credential | Done | 1 | Thu, Nov 9, 2023 12:44 PM UTC | 10.0 (High) | | <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |
| 2_plugin | Stopped at 0 % | 1 | | | | <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |

- Kết quả sau khi hoàn tất scanning

The screenshot shows the task list again. The 'plugins_RPC' task now has a status of 'Done' and a report count of '1'. The report was generated on 'Thu, Nov 9, 2023 3:05 PM UTC'. A red circle highlights the 'View Log' button next to this task.

- Vào report của task này để xem chi tiết hơn

Report: Thu, Nov 9, 2023 3:05 PM UTC [Done]

ID: 3b3dc007-0292-46e6-87cf-e1d421abae86 Created: Thu, Nov 9, 2023 3:05 PM UTC Modified: Thu, Nov 9, 2023 3:06 PM UTC

| Information | Results (0 of 1) | Hosts (0 of 1) | Ports (0 of 0) | Applications (0 of 0) | Operating Systems (0 of 0) | CVEs (0 of 0) | Closed CVEs (0 of 0) | TLS Certificates (0 of 0) | Error Messages (0 of 0) | User Tags (0) |
|---------------|---|----------------|----------------|-----------------------|----------------------------|---------------|----------------------|---------------------------|-------------------------|---------------|
| Task Name | plugins_RCP | | | | | | | | | |
| Scan Time | Thu, Nov 9, 2023 3:05 PM UTC - Thu, Nov 9, 2023 3:06 PM UTC | | | | | | | | | |
| Scan Duration | 0.00 h | | | | | | | | | |
| Scan Status | Done | | | | | | | | | |
| Hosts scanned | 1 | | | | | | | | | |
| Filter | apply_overrides=0 levels=html min_qod=70 | | | | | | | | | |
| Timezone | Coordinated Universal Time (UTC) | | | | | | | | | |

=> Target này không có lỗi hỏng nào liên quan đến family RCP