Phòng thí nghiệm An toàn Thông tin InsecLab

Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO THỰC HÀNH

Môn học: AN TOÀN MẠNG

Tên chủ đề: LAB 3 - QUÉT LỖ HỔNG BẢO MẬT

GVHD: Tô Trọng Nghĩa

Nhóm: 12

1. THÔNG TIN CHUNG:

Lớp: NT140.P11.ANTT.2

STT	Họ và tên	MSSV	Email
1	Thái Ngọc Diễm Trinh	22521541	22521541@gm.uit.edu.vn
2	Phan Nguyễn Nhật Trâm	22521501	22521501@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Nội dung	Tình trạng	Trang
1	Quét lỗ hổng sử dụng công cụ Nessus	100%	2 - 17
2	Bài tập nhóm	100%	18 - 20
Điểm tự đánh giá			**10/10**

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

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

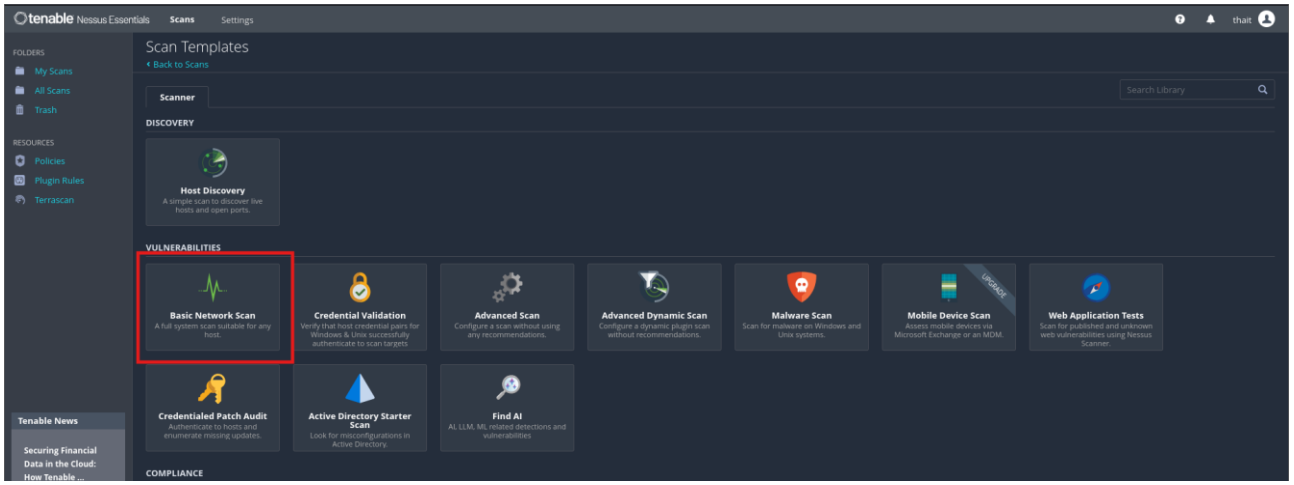
BÁO CÁO CHI TIẾT

A. Quét lỗ hổng sử dụng công cụ Nessus

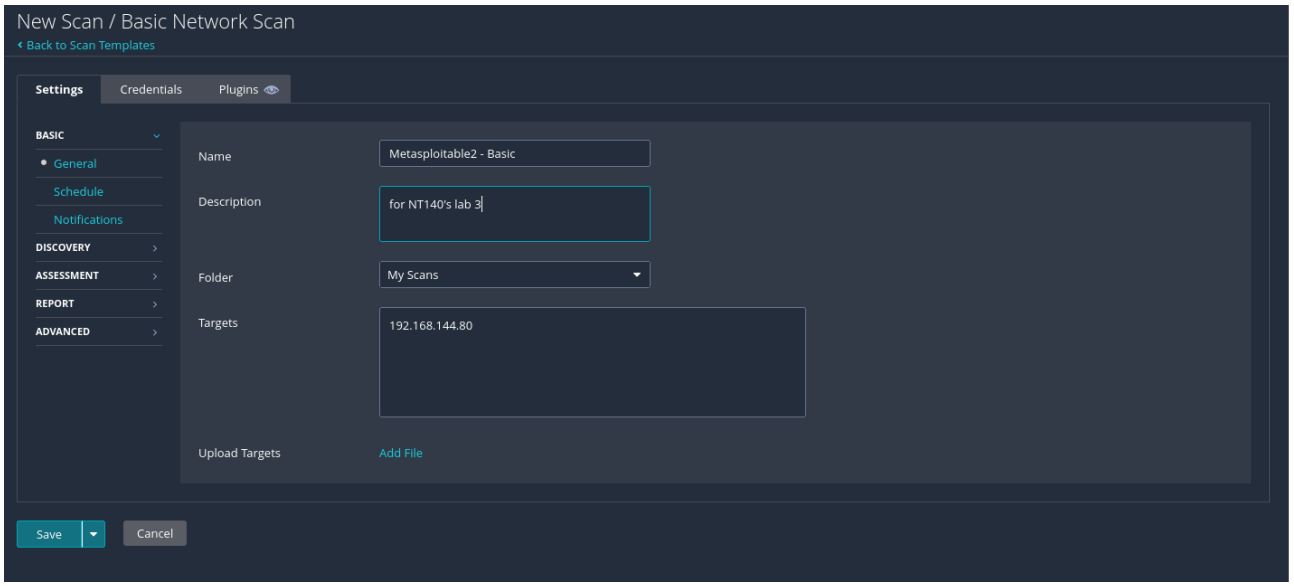
1. Quét lỗ hổng không sử dụng tài khoản chứng thực

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

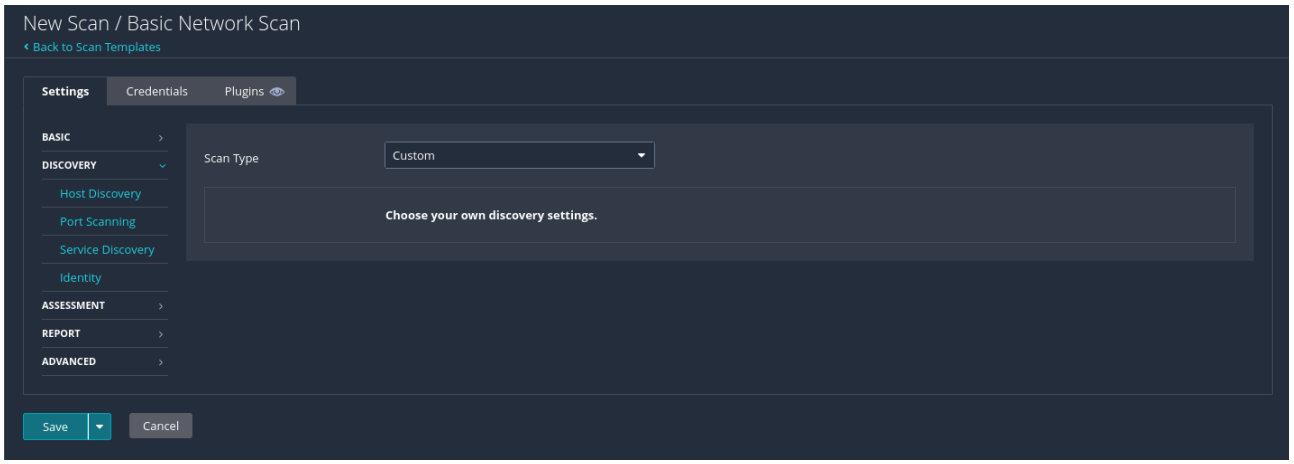
• **Bước 1:** Chọn ***New Scan*** ⇨ ***Basic Network Scan***



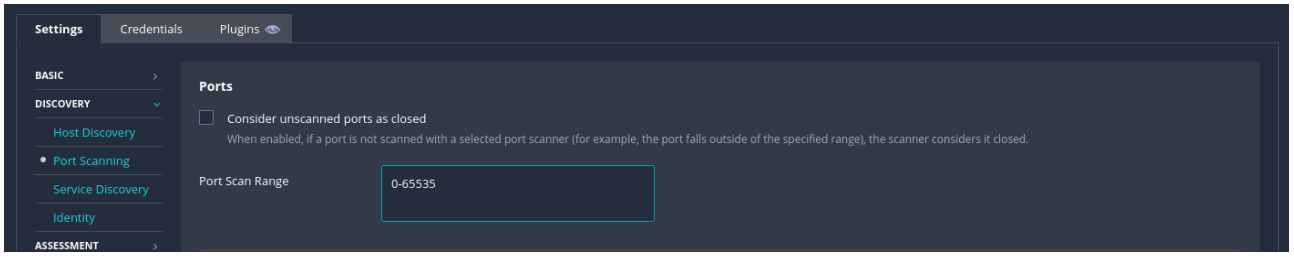
• **Bước 2:** Thiết lập các thông tin cơ bản như tên, địa chỉ IP của máy mục tiêu



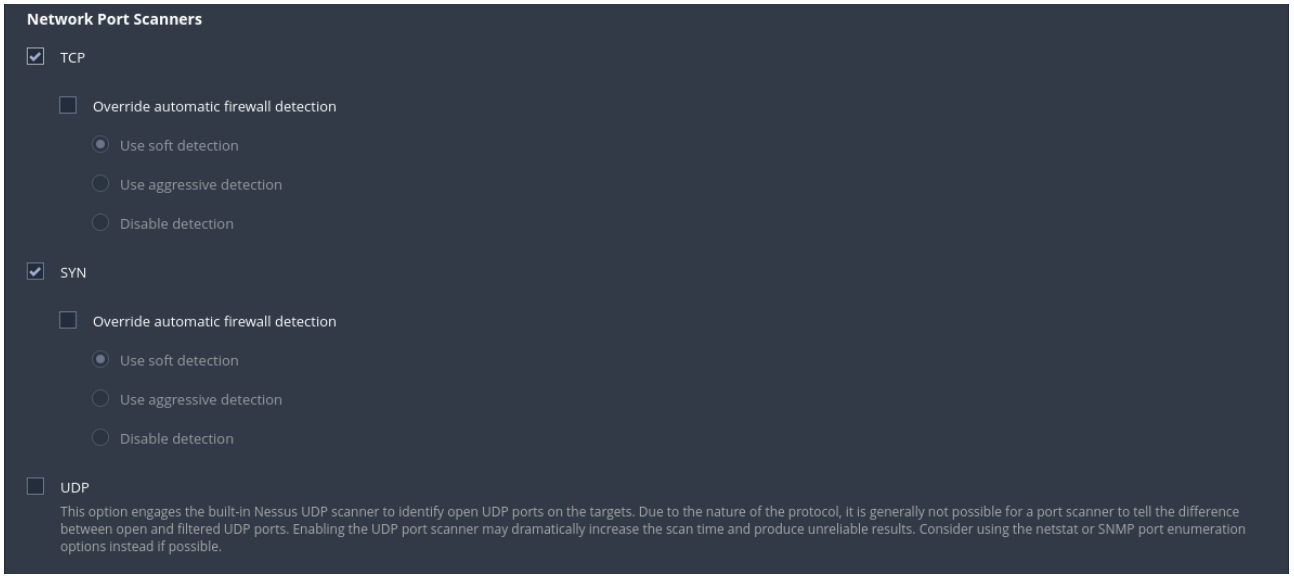
- **Bước 3:** Chọn ***Scan Type*** là ***Custom***



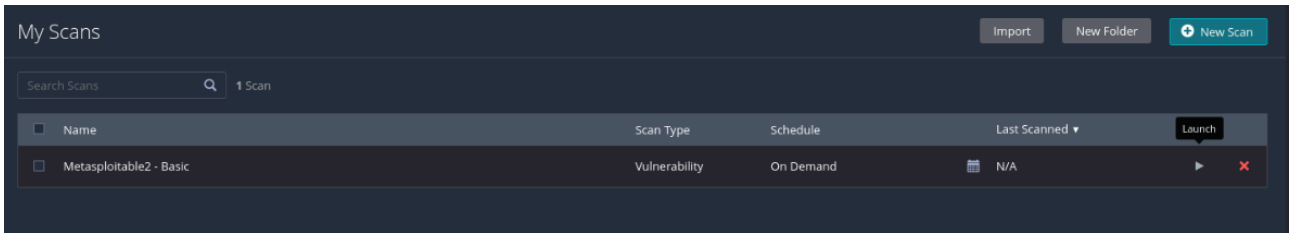
- **Bước 4:** Chọn ***Port Scanning***, sửa phạm vi port sẽ được scan thành ***0-65535***, nghĩa là sẽ scan tất cả các port



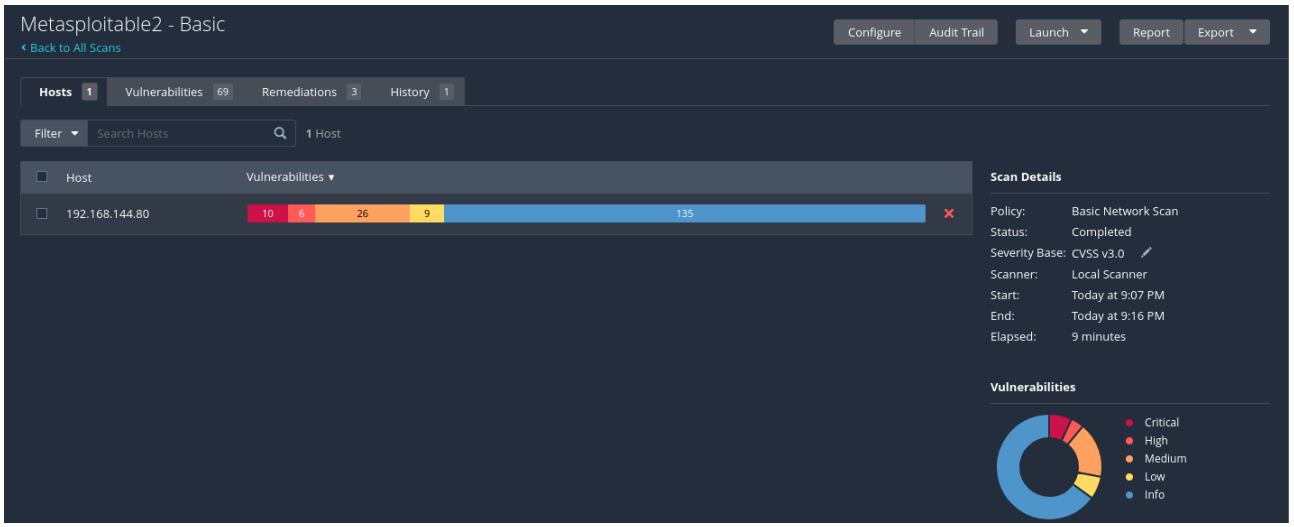
- **Bước 5:** Ở phần ***Network Poret Scanners***, chọn ***TCP*** và ***SYN***. Sau khi thiết lập xong nhấn ***Save*** để lưu các cài đặt



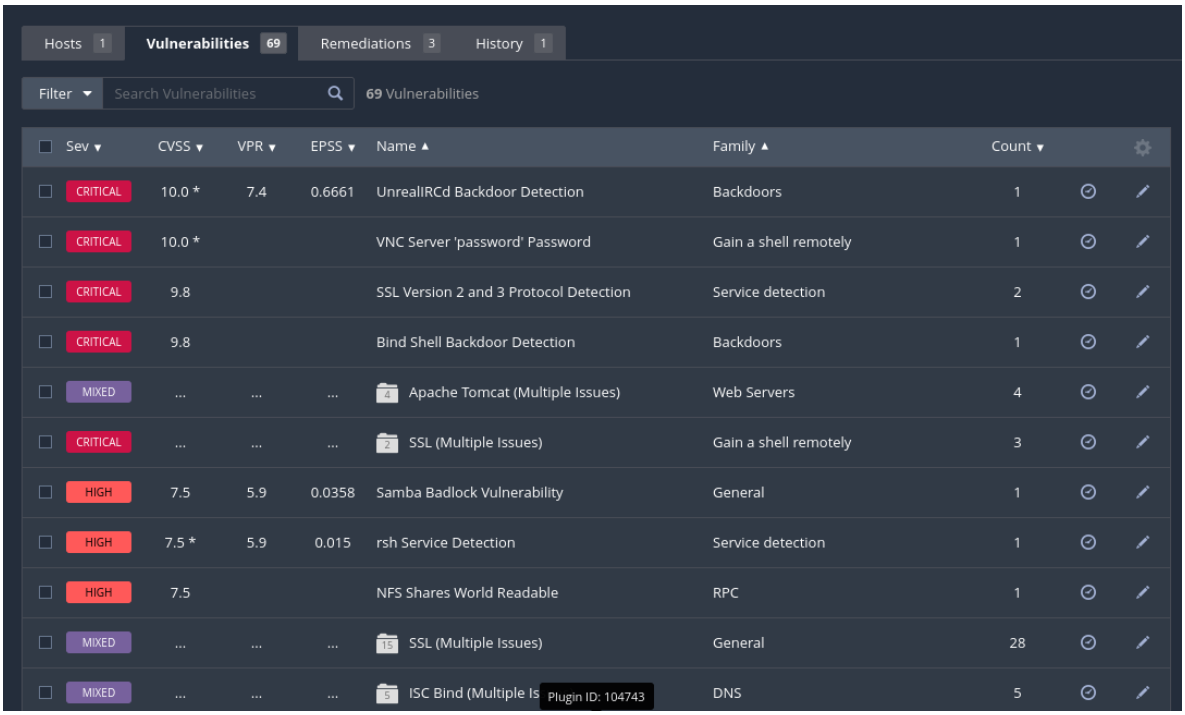
- **Bước 6:** Nhấn nút mũi tên (***Launch***) để tiến hành quá trình quét và chờ một lúc để quá trình quét hoàn tất



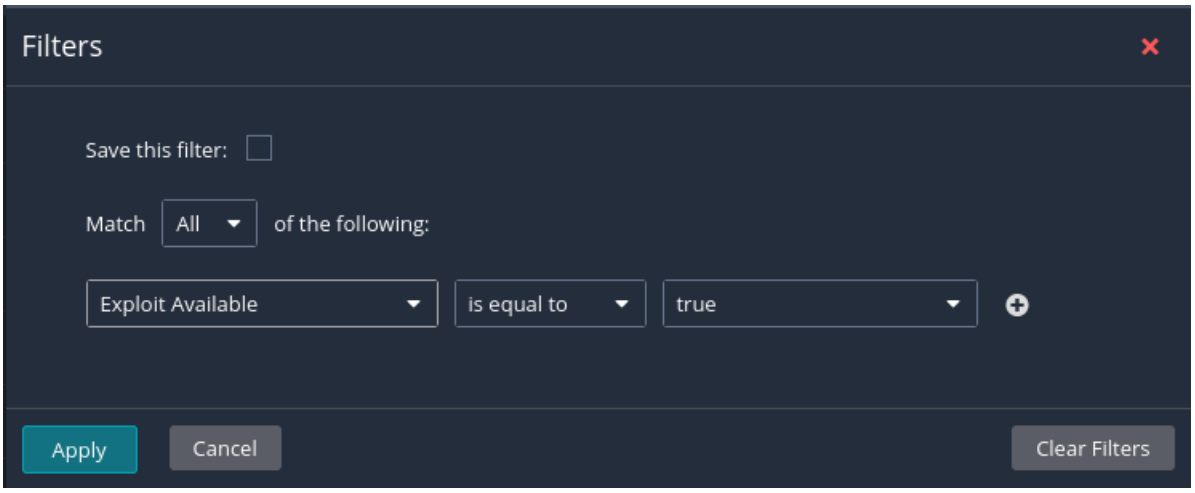
- **Bước 7:** Sau khi scan hoàn tất, click vào tên scan, "Metasploitable2 – Basic" để hiển thị danh sách các host được khám phá trong quá trình scan và tóm tắt các lỗ hổng tồn tại.



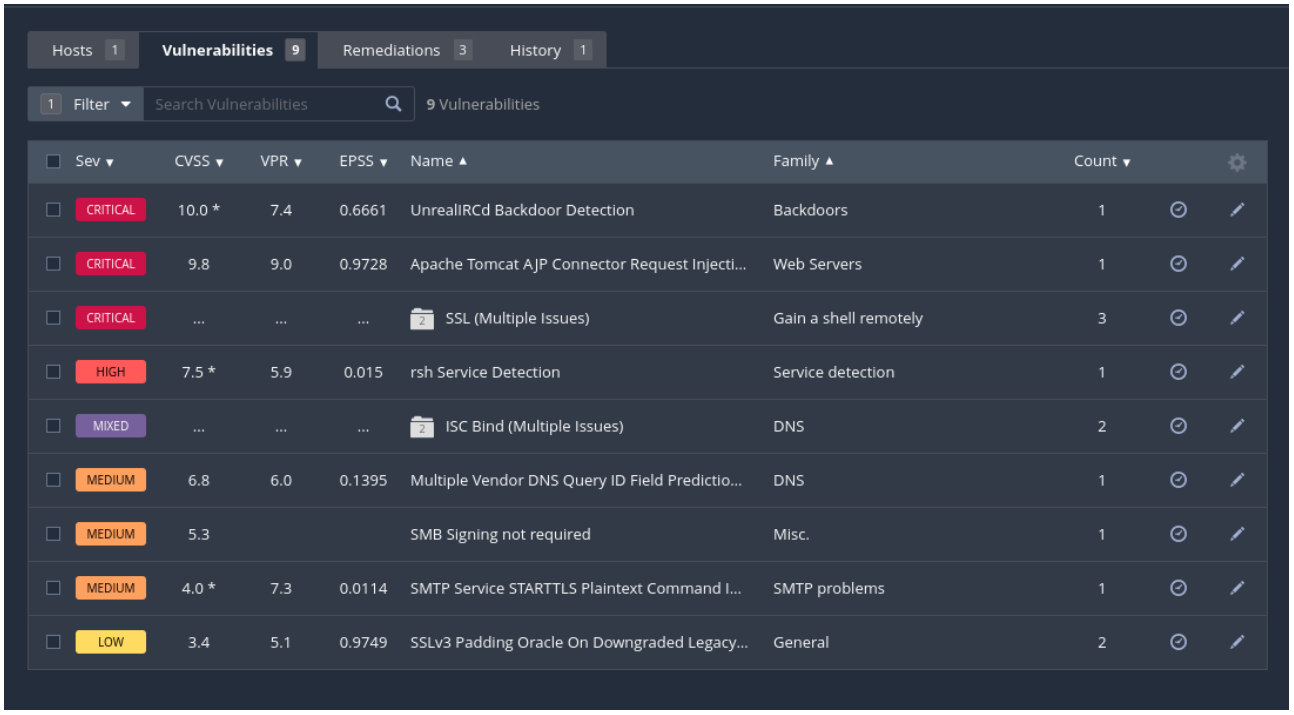
- Chọn ***Vulnerabilities*** để xem các lỗ hổng đã được phát hiện



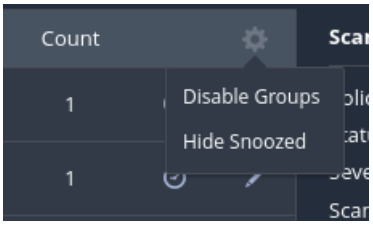
- Click ***Filter*** và thay đổi giá trị lọc thành ***Exploit Available***, giữ nguyên các giá trị mặc định của ***is equal to*** và ***true***. Sau khi cấu hình xong, click vào ***Apply***



- Danh sách lỗ hổng được phân loại theo nhóm



- Có thể vô hiệu hóa tính năng gom nhóm bằng cách nhấn vào hình răng cưa ⇨ ***Disable Groups***



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

- **Bước 1:** Tìm vị trí địa chỉ IP máy nạn nhân

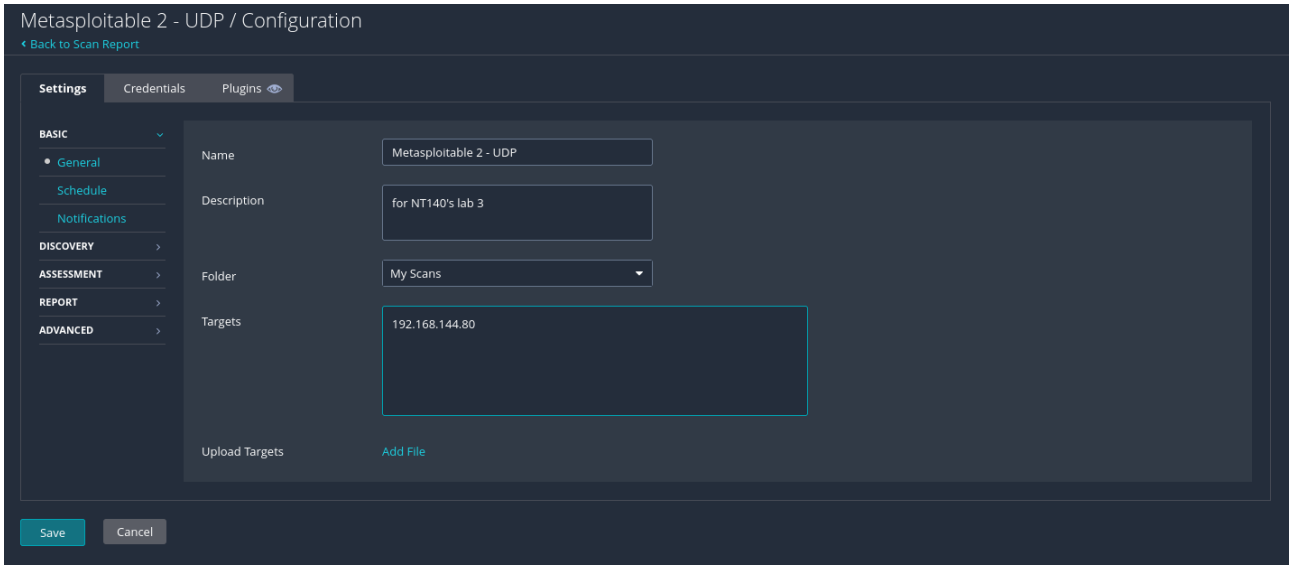
10	10.377472856	VMware_1b:a2:d2	Broadcast	ARP	60 Who has 192.168.144.80? Tell 192.168.144.196
11	10.378030390	VMware_49:2c:a6	VMware_1b:a2:d2	ARP	60 192.168.144.80 is at 00:0c:29:49:2c:a6

- **Bước 2:** Thực hiện kết nối trên các port của TCP sau đó quét các lỗ hỏng trên các port tìm được. Ví dụ với port 80:
  - Máy Kali Linux (192.168.144.196) gửi gói tin SYN đến máy Metasploitable 2 (192.168.144.80) để bắt đầu quá trình bắt tay 3 bước
  - Bên máy Metasploitable 2 gửi lại gói tin SYN ACK
  - Cuối cùng máy Kali Linux đã gửi gói tin ACK để hoàn thành quá trình bắt tay

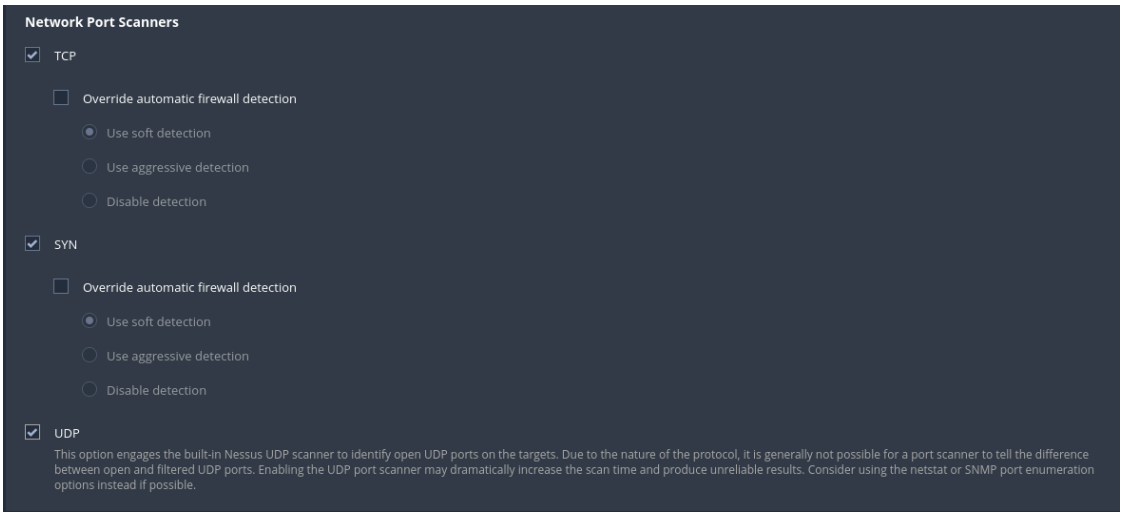
16	14.758042468	192.168.144.196	192.168.144.80	TCP	74 36246 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=786947447 …
17	14.758126696	192.168.144.196	192.168.144.80	TCP	74 35754 → 81 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=786947447 …
18	14.758157603	192.168.144.196	192.168.144.80	TCP	74 55308 → 8009 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=78694744…
19	14.758546998	192.168.144.80	192.168.144.196	TCP	74 80 → 36246 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=…
20	14.758547218	192.168.144.80	192.168.144.196	TCP	60 81 → 35754 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	14.758568037	192.168.144.196	192.168.144.80	TCP	66 36246 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=786947447 TSecr=82921
22	14.758655180	192.168.144.80	192.168.144.196	TCP	74 8009 → 55308 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSva…
23	14.758661502	192.168.144.196	192.168.144.80	TCP	66 55308 → 8009 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=786947447 TSecr=82921
24	14.808518947	192.168.144.196	192.168.144.80	HTTP	84 GET / HTTP/1.0
25	14.809077948	192.168.144.80	192.168.144.196	TCP	66 80 → 36246 [ACK] Seq=1 Ack=19 Win=5792 Len=0 TSval=82926 TSecr=786947497
26	14.819174380	192.168.144.80	192.168.144.196	HTTP	1152 HTTP/1.1 200 OK (text/html)
27	14.819174751	192.168.144.80	192.168.144.196	TCP	66 80 → 36246 [FIN, ACK] Seq=1087 Ack=19 Win=5792 Len=0 TSval=82927 TSecr=786…
28	14.819220246	192.168.144.196	192.168.144.80	TCP	66 36246 → 80 [ACK] Seq=19 Ack=1087 Win=64000 Len=0 TSval=786947508 TSecr=829…
29	14.819331169	192.168.144.196	192.168.144.80	TCP	66 36246 → 80 [RST, ACK] Seq=19 Ack=1088 Win=64128 Len=0 TSval=786947508 TSec…

3. Quét lại nhưng quét thêm port UDP.

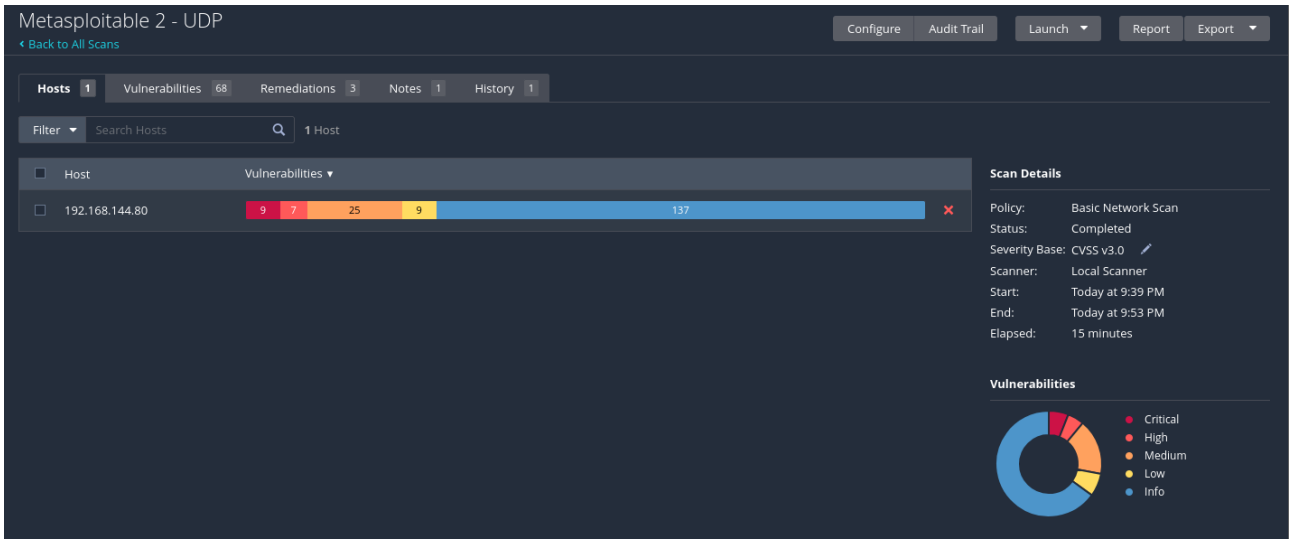
- **Bước 1:** Thực hiện lại từ bước 1 đến bước 4 giống bài 1



- **Bước 2:** Ở phần ***Network Port Scanners***, tick chọn thêm ***UDP***



- **Bước 3:** Tiến hành scan như bình thường. Kết quả sau khi scan



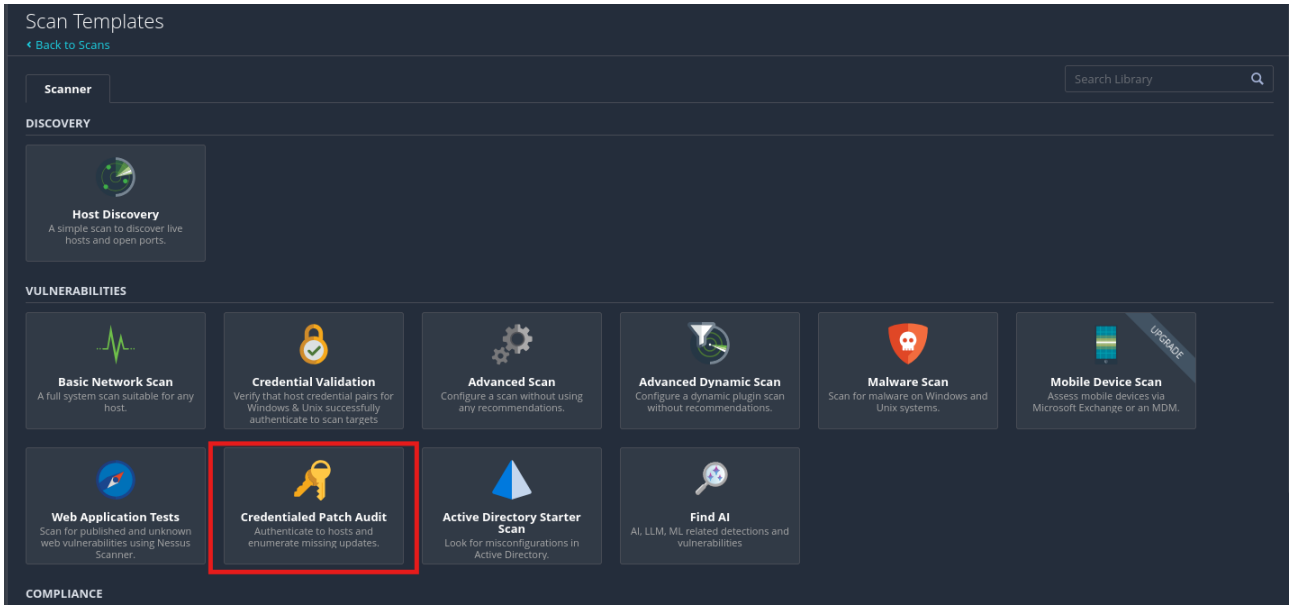
So sánh:

Tiêu chí	Không có UDP	Có UDP
Thời gian	9 phút	14 phút
Tổng số lỗ hổng	187	187
Critical	10	9
High	7	7
Medium	26	25
Low	9	9
Info	135	137

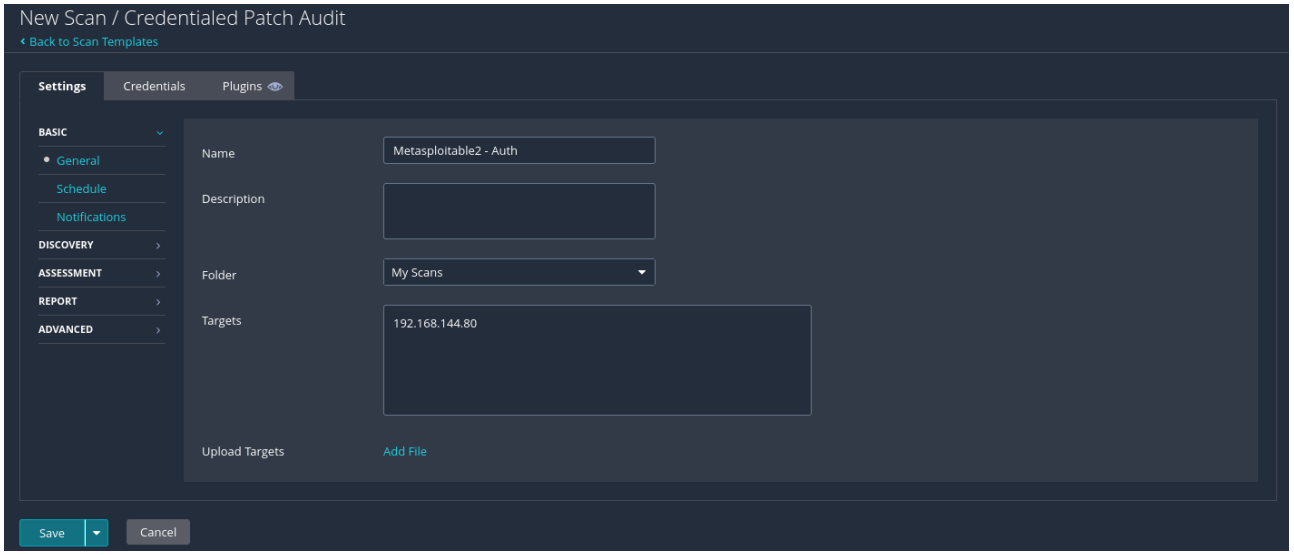
2. Quét lỗ hổng sử dụng tài khoản chứng thực

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

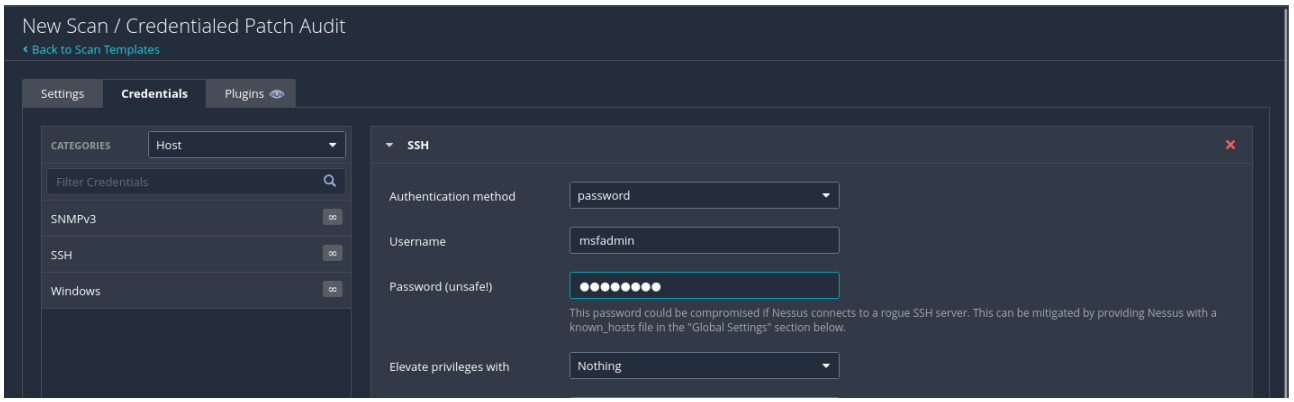
- **Bước 1:** Chọn ***New Scan*** ⇨ ***Credentialed Patch Audit***



- **Bước 2:** Thiết lập một số cấu hình cơ bản như tên, địa chỉ máy mục tiêu,...

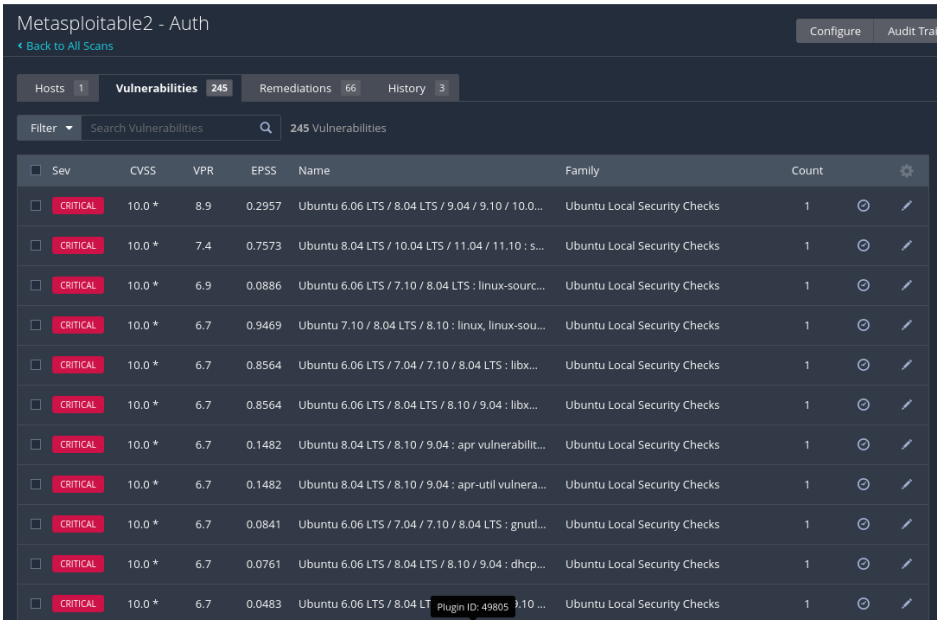


- **Bước 3:** Chọn ***Credentials*** ⇨ ***SSH*** ⇨ ***Authentication method*** chọn ***Custom***. Sau đó nhập thông tin đăng nhập là msfadmin:msfadmin và tiến hành lưu lại cài đặt



- **Bước 4:** Tiến hành quét và kết quả sau khi quét xong

- **Bước 5:** Danh sách một số lỗ hổng tìm được



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

- So sánh:

Tiêu chí	**Không có**	**Có**
Thời gian	9 phút	8 phút
Tổng số lỗ hổng	187	289
Critical	10	17
High	7	88
Medium	26	115
Low	9	9
Info	135	60

⇨ Quét có sử dụng tài khoản chứng thực nhanh hơn, cho thấy việc có tài khoản chứng thực giúp công cụ quét truy cập được nhiều tài nguyên hơn, từ đó giảm thời gian dò tìm. Việc sử dụng tài khoản chứng thực rõ ràng cải thiện đáng kể chất lượng quét, đặc biệt là trong việc phát hiện các lỗ hổng nghiêm trọng và quan trọng.

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

- So sánh:

	Không có	**Có**
Ưu điểm	Dễ triển khai: Không cần cấu hình tài khoản chứng thực, giúp việc triển khai đơn giản hơn. Nhanh chóng: Quá trình quét thường diễn ra nhanh hơn vì không yêu cầu thiết lập quyền truy cập nội bộ.	Hiệu suất cao hơn: Công cụ như Nessus có thể truy cập vào hệ thống bên trong, thu thập thông tin chi tiết về các ứng dụng, dịch vụ và lỗ hổng ⇨ cho phép tạo báo cáo chi tiết và chính xác hơn về tình trạng bảo mật. Phát hiện lỗ hổng ẩn: Có khả năng phát hiện các lỗ hổng không thể thấy khi quét bên ngoài.
Nhược điểm	Thông tin hạn chế: Chỉ thu thập được dữ liệu từ bên ngoài hệ thống, làm giảm khả năng phát	Đòi hỏi quyền truy cập: Cần quyền truy cập vào hệ thống, điều này có thể gây rủi ro bảo mật nếu tài

	hiện các lỗ hổng và cung cấp thông tin chi tiết. Nguy cơ sai sót cao: Báo cáo có thể thiếu chính xác hoặc bỏ sót các lỗ hổng nếu hệ thống được cấu hình để che giấu thông tin quan trọng.	khoản chứng thực bị lạm dụng hoặc không được bảo vệ đúng cách. Tốn thời gian và công sức: Yêu cầu cấu hình phức tạp hơn, bao gồm việc thiết lập tài khoản và mật khẩu chứng thực, dẫn đến mất thời gian.

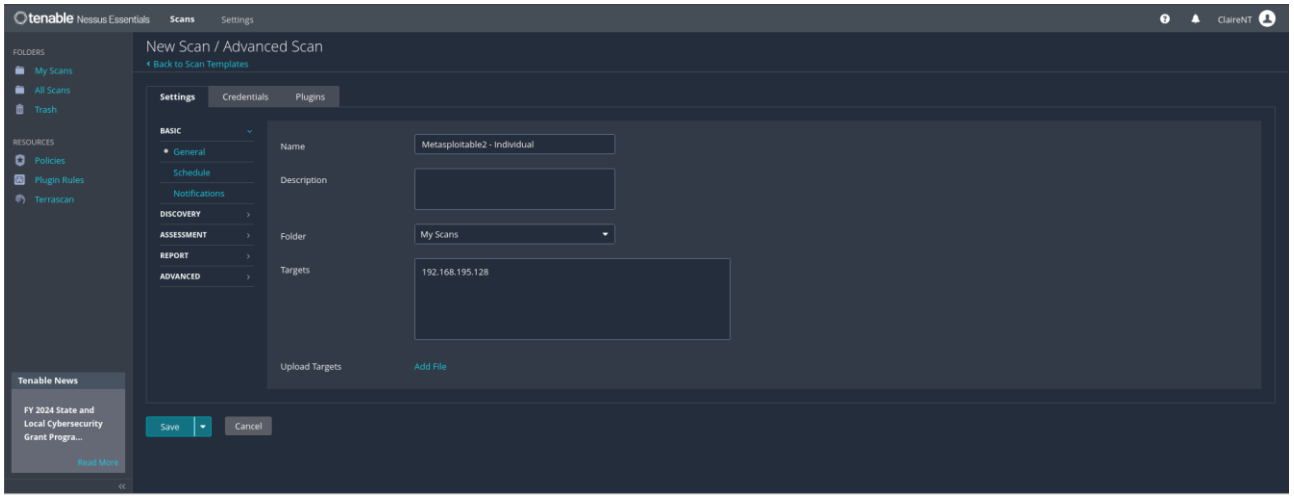
3. Quét với Plugin được chỉ định

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

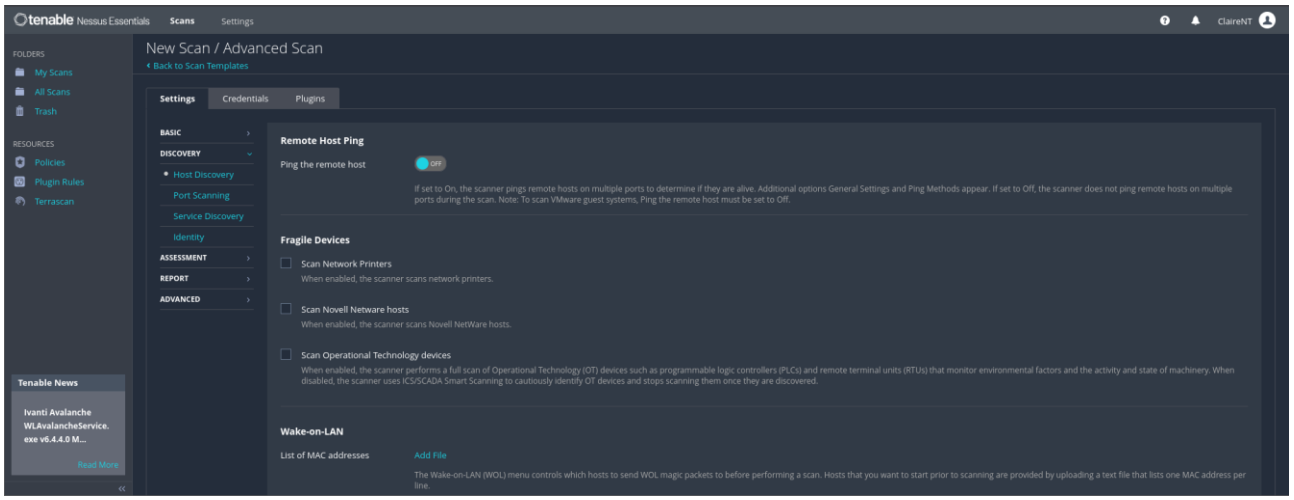
- IP metasploitable2

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:50:88:21
          inet addr:192.168.195.128  Bcast:192.168.195.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe50:8821/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:55 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6355 (6.2 KB)  TX bytes:7220 (7.0 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:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$
```

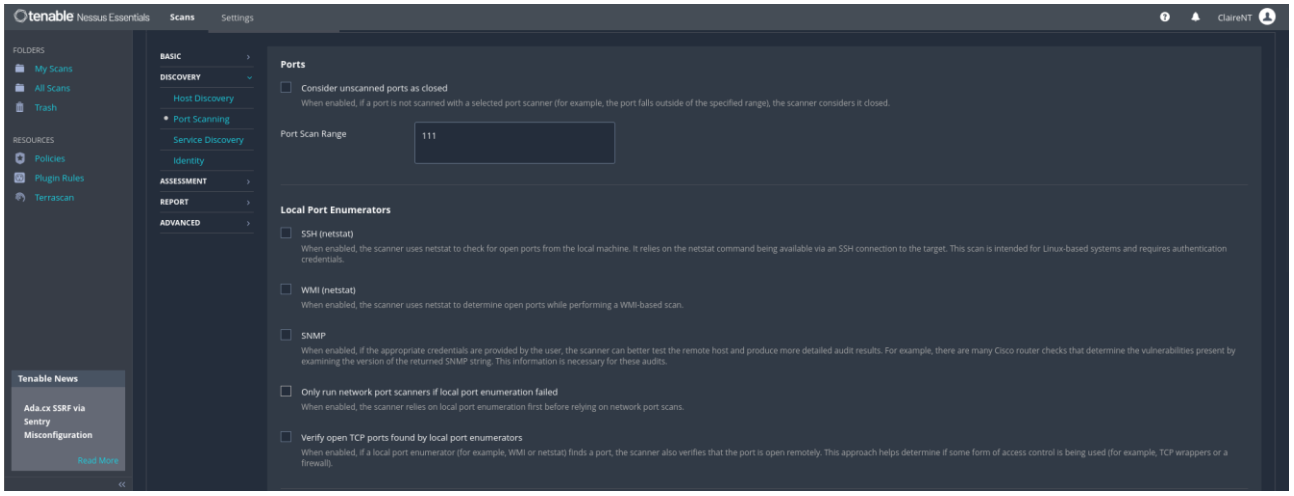
- Cấu hình quét: Chọn ***Advanced Scan*** ⇨ Thiết lập một số thông tin cơ bản như tên, địa chỉ máy mục tiêu,...



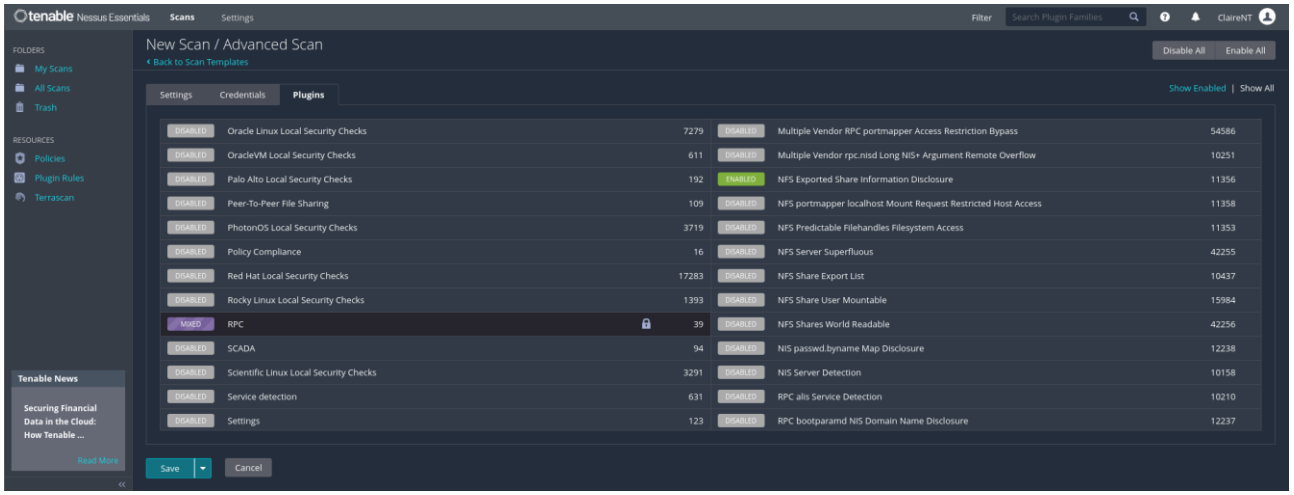
- Tắt ***Host Discovery*** để tiết kiệm thời gian



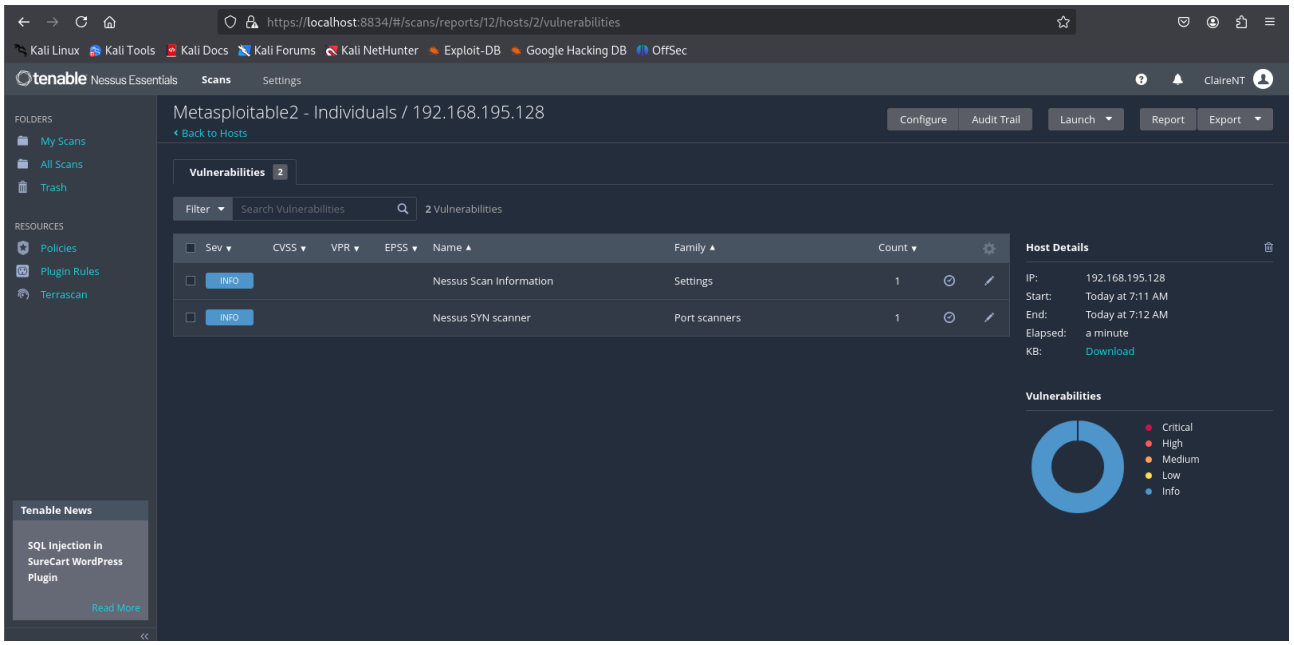
- Chọn scan port 111 – port của RPC



- Bật plugin NFS



- Kết quả quét



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?*

- Bật Wireshark và tiến hành thực hiện quá trình quét.

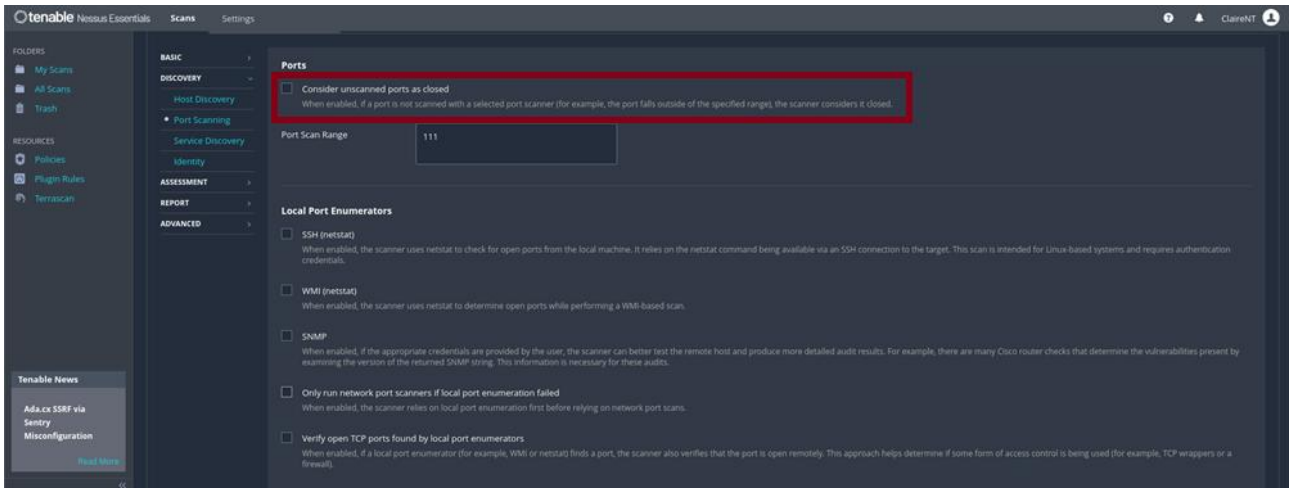
9	0.480965897	192.168.195.133	192.168.195.128	TCP	74	55198 → 8045 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2775261188 TSecr=0 WS=128
10	0.481991426	192.168.195.128	192.168.195.133	TCP	60	8045 → 55198 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12	0.501118071	192.168.195.133	192.168.195.128	TCP	74	34168 → 2810 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2775261208 TSecr=0 WS=128
13	0.501496682	192.168.195.128	192.168.195.133	TCP	60	2810 → 34168 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	0.540696298	192.168.195.133	192.168.195.128	TCP	74	56286 → 81 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2775261248 TSecr=0 WS=128
16	0.541230413	192.168.195.128	192.168.195.133	TCP	60	81 → 56286 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	0.554184582	192.168.195.133	192.168.195.128	TCP	74	41668 → 8009 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2775261262 TSecr=0 WS=128
19	0.554625895	192.168.195.128	192.168.195.133	TCP	74	8009 → 41668 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=347290 TSecr=2775…
20	0.554692096	192.168.195.133	192.168.195.128	TCP	66	41668 → 8009 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2775261262 TSecr=347290
21	0.566499233	192.168.195.133	192.168.195.128	TCP	377	41668 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=311 TSval=2775261274 TSecr=347290
22	0.567238654	192.168.195.128	192.168.195.133	TCP	66	8009 → 41668 [ACK] Seq=1 Ack=312 Win=6880 Len=0 TSval=347291 TSecr=2775261274
23	0.570349342	192.168.195.128	192.168.195.133	TCP	66	8009 → 41668 [FIN, ACK] Seq=1 Ack=312 Win=6880 Len=0 TSval=347291 TSecr=2775261274
24	0.575840899	192.168.195.133	192.168.195.128	TCP	66	41668 → 8009 [ACK] Seq=312 Ack=2 Win=64256 Len=0 TSval=2775261283 TSecr=347291
25	0.580214023	192.168.195.133	192.168.195.128	TCP	66	41668 → 8009 [RST, ACK] Seq=312 Ack=2 Win=64256 Len=0 TSval=2775261288 TSecr=347291
26	0.593981115	192.168.195.133	192.168.195.128	TCP	74	51650 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2775261301 TSecr=0 WS=128
27	0.594393827	192.168.195.128	192.168.195.133	TCP	74	80 → 51650 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=347294 TSecr=277526…
28	0.594462229	192.168.195.133	192.168.195.128	TCP	66	51650 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2775261302 TSecr=347294
29	0.615966642	192.168.195.133	192.168.195.128	HTTP	372	GET / HTTP/1.1
30	0.616709863	192.168.195.128	192.168.195.133	TCP	66	80 → 51650 [ACK] Seq=1 Ack=307 Win=6880 Len=0 TSval=347296 TSecr=2775261323
31	0.624801093	192.168.195.128	192.168.195.133	HTTP	1190	HTTP/1.1 200 OK (text/html)
32	0.624856595	192.168.195.133	192.168.195.128	TCP	66	51650 → 80 [ACK] Seq=307 Ack=1125 Win=66560 Len=0 TSval=2775261332 TSecr=347297
36	0.649856807	192.168.195.133	192.168.195.128	TCP	74	44886 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2775261357 TSecr=0 WS=128
37	0.650175316	192.168.195.128	192.168.195.133	TCP	74	445 → 44886 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=347299 TSecr=27752…
38	0.650245818	192.168.195.133	192.168.195.128	TCP	66	44886 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2775261358 TSecr=347299
43	0.655420765	192.168.195.133	192.168.195.128	SMB	241	Negotiate Protocol Request
44	0.655870178	192.168.195.128	192.168.195.133	TCP	66	445 → 44886 [ACK] Seq=1 Ack=176 Win=6880 Len=0 TSval=347300 TSecr=2775261363
45	0.656230288	192.168.195.128	192.168.195.133	SMB	197	Negotiate Protocol Response
46	0.656267989	192.168.195.133	192.168.195.128	TCP	66	44886 → 445 [ACK] Seq=176 Ack=132 Win=64128 Len=0 TSval=2775261364 TSecr=347300
48	0.660837719	192.168.195.133	192.168.195.128	TCP	66	44886 → 445 [RST, ACK] Seq=176 Ack=132 Win=64128 Len=0 TSval=2775261368 TSecr=347300
49	0.661340633	192.168.195.133	192.168.195.128	TCP	74	44236 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2775261369 TSecr=0 WS=128
50	0.661659342	192.168.195.128	192.168.195.133	TCP	74	139 → 44236 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=347301 TSecr=27752…
51	0.661725144	192.168.195.133	192.168.195.128	TCP	66	44236 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2775261369 TSecr=347301
56	0.672566853	192.168.195.133	192.168.195.128	NBSS	138	Session request, to Nessus171034070<20> from <20>
57	0.672884262	192.168.195.128	192.168.195.133	TCP	66	139 → 44236 [ACK] Seq=1 Ack=73 Win=5792 Len=0 TSval=347302 TSecr=2775261380
58	0.672893862	192.168.195.128	192.168.195.133	NBSS	70	Positive session response
59	0.672948864	192.168.195.133	192.168.195.128	TCP	66	44236 → 139 [ACK] Seq=73 Ack=5 Win=64256 Len=0 TSval=2775261380 TSecr=347302
60	0.682759244	192.168.195.133	192.168.195.128	TCP	66	44236 → 139 [RST, ACK] Seq=73 Ack=5 Win=64256 Len=0 TSval=2775261390 TSecr=347302

- Các port khác mà Nessus thực hiện scan: 8045, 2810, 8009, 80, 445…
- Nessus scan các port khác: vì nhiều plugin kiểm tra trạng thái của các cổng mặc định (được mã hóa cứng) trước khi kết nối với chúng
    - Các cổng ngoài phạm vi quét sẽ có trạng thái không xác định vì chúng không được quét

- Theo mặc định, hàm get_port_state() sẽ trả về TRUE khi trạng thái cổng không xác định, dẫn đến việc thử kết nối với các cổng đó

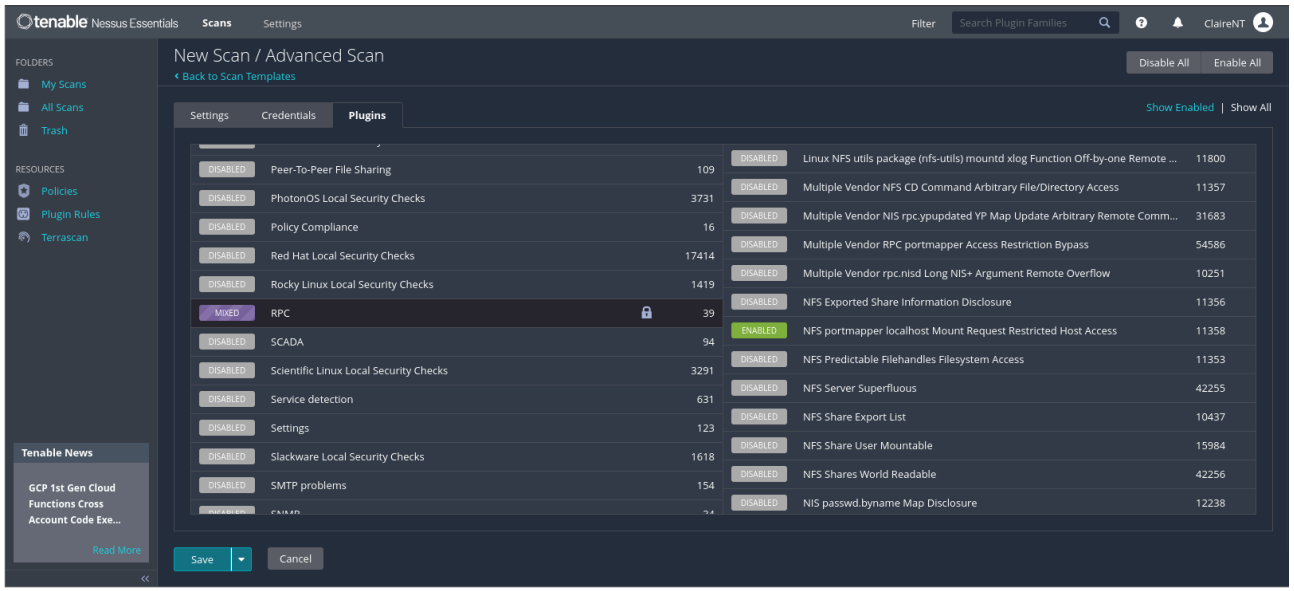
9. Mô tả cách làm để ngăn chặn việc Nessus scan port khác không phải là port được chỉ định?

- Kích hoạt tùy chọn ***Consider unscanned ports as closed***
- Tùy chọn này khiến get_port_state() trả về FALSE nếu trạng thái cổng không xác định, ngăn cản việc kết nối với các cổng ngoài phạm vi quét

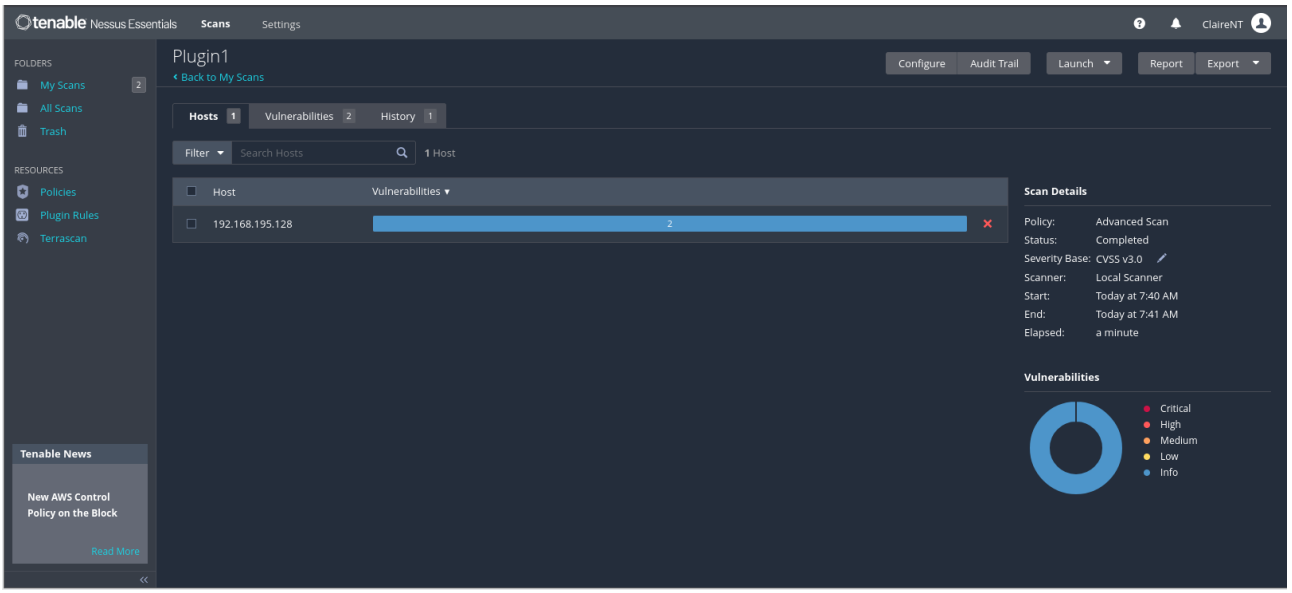


10. Thực hiện quét lại sử dụng 2 plugin khác.

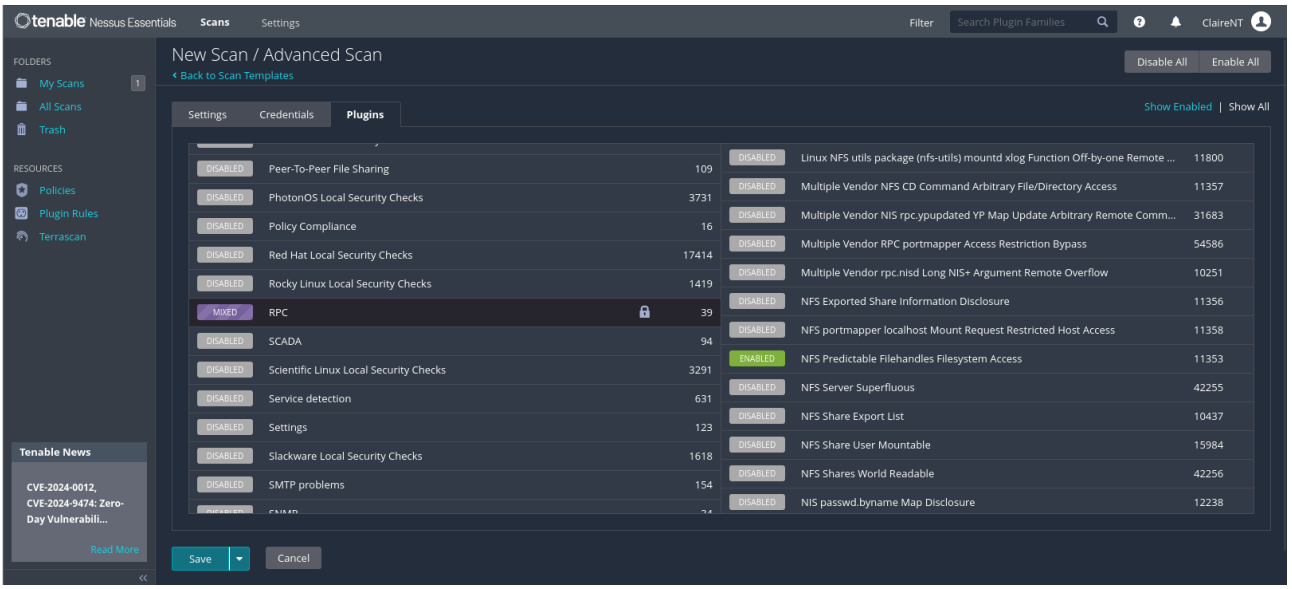
- Plugin 1:



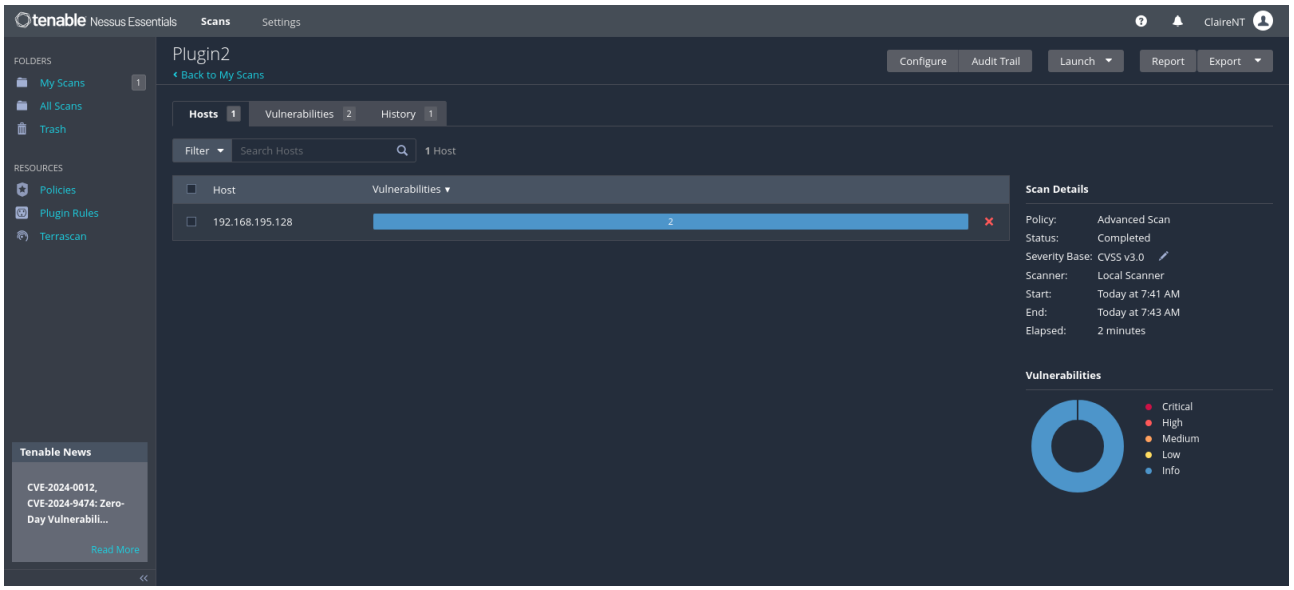
- Kết quả quét:



- Plugin 2



- Kết quả quét:


tenable Nessus Essentials
Scans
Settings
ClaireNT
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
CVE-2024-0012, CVE-2024-9474: Zero-Day Vulnerabili...
Read More
Plugin2
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 2
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.195.128
2
Scan Details
Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:41 AM
End: Today at 7:43 AM
Elapsed: 2 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

B. Bài tập nhóm

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:

- Công cụ: Tsunami
- Yêu cầu

```
┌──(nhattram1501㉿nhattram1501)-[~]
└─$ nmap --version
Nmap version 7.94SVN ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.6 openssl-3.3.2 libssh2-1.11.1 libz-1.3.1 libpcre2-10.42 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(nhattram1501㉿nhattram1501)-[~]
└─$ ncrack --version

Ncrack version 0.7 ( http://ncrack.org )
Modules: SSH, RDP, FTP, Telnet, HTTP(S), Wordpress, POP3(S), IMAP, CVS, SMB, VNC, SIP, Redis, PostgreSQL, MQTT, MySQL, MSSQL, MongoDB, Cassandra, WinRM, OWA, DICOM

┌──(nhattram1501㉿nhattram1501)-[~]
└─$ java --version
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
openjdk 23.0.1 2024-10-15
OpenJDK Runtime Environment (build 23.0.1+11-Debian-1)
OpenJDK 64-Bit Server VM (build 23.0.1+11-Debian-1, mixed mode, sharing)
```

- Cài đặt image docker của Jupyter Notebook chưa được xác thực để làm đối tượng quét

```
┌──(nhattram1501㉿nhattram1501)-[~]
└─$ sudo docker run --name unauthenticated-jupyter-notebook -p 8888:8888 -d jupyter/base-notebook start-notebook.sh --NotebookApp.token=''
[sudo] password for nhattram1501:
Unable to find image 'jupyter/base-notebook:latest' locally
latest: Pulling from jupyter/base-notebook
aece8493d397: Pull complete
fd92c719666c: Pull complete
088f11eb1e74: Pull complete
4f4fb700ef54: Pull complete
ef8373d600b0: Pull complete
77e45ee945dc: Pull complete
a30f89a0af6c: Pull complete
dc42adc7eb73: Pull complete
abaa8376a650: Pull complete
aa099bb9e49a: Pull complete
822c4cbcf6a6: Pull complete
d25166dcdc7b: Pull complete
964fc3e4ff9f: Pull complete
2c4c69587ee4: Pull complete
de2cdd875fa8: Pull complete
75d33599f5f2: Pull complete
Digest: sha256:8c903974902b0e9d45d9823c2234411de0614c5c98c4bb782b3d4f55b3e435e6
Status: Downloaded newer image for jupyter/base-notebook:latest
c181e071efa9a642557b2a75896a2cf5d07baa1050ffba29ae9a25aacbec9473
```

- Cài đặt

```
┌──(nhattram1501㉿nhattram1501)-[~]
└─$ bash -c "$(curl -sfL https://raw.githubusercontent.com/google/tsunami-security-scanner/master/quick_start.sh)"
```

- Cài đặt thành công

```
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true

BUILD SUCCESSFUL in 12s
5 actionable tasks: 5 executed

Building Tsunami scanner jar file ...
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Downloading https://services.gradle.org/distributions/gradle-6.5-bin.zip
.........10%.........20%.........30%.........40%.........50%.........60%.........70%.........80%.........90%.........100%

Welcome to Gradle 6.5!

Here are the highlights of this release:
 - Experimental file-system watching
 - Improved version ordering
 - New samples

For more details see https://docs.gradle.org/6.5/release-notes.html

Starting a Gradle Daemon (subsequent builds will be faster)

> Task :tsunami-common:compileJava
Note: /home/nhattram1501/tsunami/repos/tsunami-security-scanner/common/src/main/java/com/google/tsunami/common/net/http/OkHttpHttpClient.java uses unchecked or unsafe operations.
Note: Recompile with -Xlint:unchecked for details.

Deprecated Gradle features were used in this build, making it incompatible with Gradle 7.0.
Use '--warning-mode all' to show the individual deprecation warnings.
See https://docs.gradle.org/6.5/userguide/command_line_interface.html#sec:command_line_warnings

BUILD SUCCESSFUL in 11m 28s
19 actionable tasks: 19 executed

Build successful, execute the following command to scan 127.0.0.1:

cd /home/nhattram1501/tsunami && \
java -cp "tsunami-main-0.0.25-SNAPSHOT-cli.jar:/home/nhattram1501/tsunami/plugins/*" \
  -Dtsunami.config.location=/home/nhattram1501/tsunami/tsunami.yaml \
  com.google.tsunami.main.cli.TsunamiCli \
  --ip-v4-target=127.0.0.1 \
  --scan-results-local-output-format=JSON \
  --scan-results-local-output-filename=/tmp/tsunami-output.json

┌──(nhattram1501㉿nhattram1501)-[~]
└─$
```

- Lưu ý: sử dụng Java 11 để cài đặt vì Java > 16 sẽ không được hỗ trợ

```
┌──(nhattram1501㉿nhattram1501)-[~]
└─$ sudo update-alternatives --config java
There are 3 choices for the alternative java (providing /usr/bin/java).

  Selection    Path                                            Priority   Status
------------------------------------------------------------
* 0            /usr/lib/jvm/java-23-openjdk-amd64/bin/java   2311      auto mode
  1            /usr/lib/jvm/java-11-openjdk-amd64/bin/java   1111      manual mode
  2            /usr/lib/jvm/java-21-openjdk-amd64/bin/java   2111      manual mode
  3            /usr/lib/jvm/java-23-openjdk-amd64/bin/java   2311      manual mode

Press <enter> to keep the current choice[*], or type selection number: 1
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/java to provide /usr/bin/java (java) in manual mode

┌──(nhattram1501㉿nhattram1501)-[~]
└─$ java --version
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
openjdk 11.0.25-ea 2024-10-15
OpenJDK Runtime Environment (build 11.0.25-ea+5-post-Debian-1)
OpenJDK 64-Bit Server VM (build 11.0.25-ea+5-post-Debian-1, mixed mode, sharing)
```

- Kết quả scan

```
┌──(nhattram1501㉿nhattram1501)-[~]
└─$ cd /home/nhattram1501/tsunami && \
java -cp "tsunami-main-0.0.25-SNAPSHOT-cli.jar:/home/nhattram1501/tsunami/plugins/*" \
  -Dtsunami.config.location=/home/nhattram1501/tsunami/tsunami.yaml \
  com.google.tsunami.main.cli.TsunamiCli \
  --ip-v4-target=127.0.0.1 \
  --scan-results-local-output-format=JSON \
  --scan-results-local-output-filename=/tmp/tsunami-output.json
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Nov 19, 2024 9:36:01 AM com.google.tsunami.main.cli.TsunamiCli main
INFO: Full classpath scan took 10.15 s
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.config.ConfigModule configure
INFO: Found Tsunami config class: com.google.tsunami.common.net.http.HttpClientConfigProperties
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.config.ConfigModule configure
INFO: Found Tsunami config class: com.google.tsunami.plugin.TcsConfigProperties
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.config.ConfigModule configure
INFO: Found Tsunami config class: com.google.tsunami.plugins.detectors.credentials.genericweakcredentialdetector.GenericWeakCredentialDetectorConfigs
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.config.ConfigModule configure
INFO: Found Tsunami config class: com.google.tsunami.plugins.detectors.exposedui.phpunit.PHPUnitExposedEvalStdinDetectorConfigs
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.config.ConfigModule configure
INFO: Found Tsunami config class: com.google.tsunami.plugins.detectors.exposedui.spring.SpringBootExposedEndpointDetector$Configs
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.config.ConfigModule configure
INFO: Found Tsunami config class: com.google.tsunami.plugins.fingerprinters.web.WebServiceFingerprinterConfigs$WebServiceFingerprinterConfigProperties
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.config.ConfigModule configure
INFO: Found Tsunami config class: com.google.tsunami.plugins.portscan.nmap.NmapPortScannerConfigs
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.cli.CliOptionsModule configure
INFO: Found CliOption: com.google.tsunami.common.io.archiving.GoogleCloudStorageArchiver$Options
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.cli.CliOptionsModule configure
INFO: Found CliOption: com.google.tsunami.common.net.http.HttpClientCliOptions
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.cli.CliOptionsModule configure
INFO: Found CliOption: com.google.tsunami.main.cli.LanguageServerOptions
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.cli.CliOptionsModule configure
INFO: Found CliOption: com.google.tsunami.main.cli.ScanResultsArchiver$Options
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.cli.CliOptionsModule configure
INFO: Found CliOption: com.google.tsunami.main.cli.option.MainCliOptions
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.cli.CliOptionsModule configure
INFO: Found CliOption: com.google.tsunami.plugin.TcsClientCliOptions
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.cli.CliOptionsModule configure
INFO: Found CliOption: com.google.tsunami.plugins.detectors.credentials.genericweakcredentialdetector.GenericWeakCredentialDetectorCliOptions
Nov 19, 2024 9:36:02 AM com.google.tsunami.common.cli.CliOptionsModule configure
```

```
Nov 19, 2024 9:36:28 AM com.google.tsunami.common.net.http.OkHttpHttpClient parseResponse
INFO: Received HTTP response with code '200' for request to 'http://127.0.0.1:8888/static/logo/logo.png?v=a2a176ee3cee251ffddf5fa21fe8e43727a9e5f87a06f9c91ad7b776d9e9d3d5e0159c16cc188a3965e00375fb4bc336c16067c688f5040c0c2d4bfdb852a9e4'.
Nov 19, 2024 9:36:28 AM com.google.tsunami.plugins.fingerprinters.web.crawl.SimpleCrawlAction lambda$compute$0
INFO: SimpleCrawlAction visited target 'http://127.0.0.1:8888/static/logo/logo.png?v=a2a176ee3cee251ffddf5fa21fe8e43727a9e5f87a06f9c91ad7b776d9e9d3d5e0159c16cc188a3965e00375fb4bc336c16067c688f5040c0c2d4bfdb852a9e4' with method 'GET' at depth '1', response code: 200.
Nov 19, 2024 9:36:28 AM com.google.tsunami.plugins.fingerprinters.web.crawl.SimpleCrawlAction lambda$compute$0
INFO: SimpleCrawlAction visited target 'http://127.0.0.1:8888/static/favicon.ico?v=50afa725b5de8b00030139d09b38620224d4e7dba47c07ef0e86d4643f30c9bfe6bb7e1a4a1c561aa32834480909a4b6fe7cd1e17f7159330b6b5914bf45a880' with method 'GET' at depth '1', response code: 200.
Nov 19, 2024 9:36:28 AM com.google.tsunami.plugins.fingerprinters.web.crawl.SimpleCrawlAction lambda$compute$0
INFO: SimpleCrawlAction visited target 'http://127.0.0.1:8888/static/style/bootstrap-theme.min.css?v=8b2f045cb5b4d5ad346f6e816aa2566829a4f5f2783ec31d80d46a57de8ac0c3d21fe6e53bcd8e1f38ac17fcd06d12088bc9b43e23b5d1da52d10c6b717b22b3' with method 'GET' at depth '1', response code: 200.
Nov 19, 2024 9:36:28 AM com.google.tsunami.common.net.http.OkHttpHttpClient parseResponse
INFO: Received HTTP response with code '200' for request to 'http://127.0.0.1:8888/static/favicons/favicon.ico'.
Nov 19, 2024 9:36:28 AM com.google.tsunami.common.net.http.OkHttpHttpClient parseResponse
INFO: Received HTTP response with code '200' for request to 'http://127.0.0.1:8888/static/style/bootstrap.min.css?v=0e8a7fbd6de23ad6b27ab95802a0a0915af6693af612bc304d83af445529ce5d95842309ca3405d10f538d45c8a3a261b8cff78b4bd512dd9effb4109a71d0ab'.
Nov 19, 2024 9:36:28 AM com.google.tsunami.common.net.http.OkHttpHttpClient send
INFO: Sending HTTP 'GET' request to 'http://127.0.0.1:8888/static/favicons/favicon-busy-1.ico'.
Nov 19, 2024 9:36:28 AM com.google.tsunami.plugins.fingerprinters.web.crawl.SimpleCrawlAction lambda$compute$0
INFO: SimpleCrawlAction visited target 'http://127.0.0.1:8888/static/favicons/favicon.ico' with method 'GET' at depth '2', response code: 200.
Nov 19, 2024 9:36:28 AM com.google.tsunami.common.net.http.OkHttpHttpClient parseResponse
INFO: Received HTTP response with code '200' for request to 'http://127.0.0.1:8888/static/lab/main.b19b8a0b5c015351f92f.js?v=b19b8a0b5c015351f92f'.
Nov 19, 2024 9:36:28 AM com.google.tsunami.common.net.http.OkHttpHttpClient parseResponse
INFO: Received HTTP response with code '200' for request to 'http://127.0.0.1:8888/static/style/index.css?v=30372e3246a801d662cf9e3f9dd656fa192eebde9054a2282449fe43919de9f0ee9b745d7eb49d3b0a5e56357912cc7d776390eddcab9dac85b77bdb17b4bdae'.
Nov 19, 2024 9:36:28 AM com.google.tsunami.common.net.http.OkHttpHttpClient parseResponse
INFO: Received HTTP response with code '200' for request to 'http://127.0.0.1:8888/static/favicons/favicon-busy-1.ico'.
Nov 19, 2024 9:36:28 AM com.google.tsunami.plugins.fingerprinters.web.crawl.SimpleCrawlAction lambda$compute$0
INFO: SimpleCrawlAction visited target 'http://127.0.0.1:8888/static/style/bootstrap.min.css?v=0e8a7fbd6de23ad6b27ab95802a0a0915af6693af612bc304d83af445529ce5d95842309ca3405d10f538d45c8a3a261b8cff78b4bd512dd9effb4109a71d0ab' with method 'GET' at depth '1', response code: 200.
Nov 19, 2024 9:36:28 AM com.google.tsunami.plugins.fingerprinters.web.crawl.SimpleCrawlAction lambda$compute$0
INFO: SimpleCrawlAction visited target 'http://127.0.0.1:8888/static/style/index.css?v=30372e3246a801d662cf9e3f9dd656fa192eebde9054a2282449fe43919de9f0ee9b745d7eb49d3b0a5e56357912cc7d776390eddcab9dac85b77bdb17b4bdae' with method 'GET' at depth '1', response code: 200.
Nov 19, 2024 9:36:28 AM com.google.tsunami.plugins.fingerprinters.web.crawl.SimpleCrawlAction lambda$compute$0
INFO: SimpleCrawlAction visited target 'http://127.0.0.1:8888/static/lab/main.b19b8a0b5c015351f92f.js?v=b19b8a0b5c015351f92f' with method 'GET' at depth '2', response code: 200.
Nov 19, 2024 9:36:28 AM com.google.tsunami.plugins.fingerprinters.web.crawl.SimpleCrawlAction lambda$compute$0
INFO: SimpleCrawlAction visited target 'http://127.0.0.1:8888/static/favicons/favicon-busy-1.ico' with method 'GET' at depth '2', response code: 200.
Nov 19, 2024 9:36:28 AM com.google.tsunami.plugins.fingerprinters.web.WebServiceFingerprinter fingerprint
INFO: WebServiceFingerprinter discovered 12 different files on 'http://127.0.0.1:8888/'.
```