**보안 컨설팅 프로젝트**

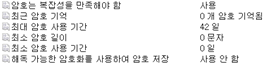
3조 [김동은, 곽준희, 유승호]

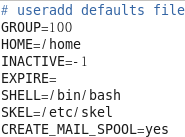
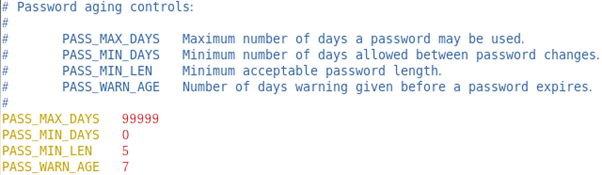
* **개요** [컨설팅 회사 소개, 조직 현황]

1. 회사 소개
2. 조직 현황

* **보안 취약점 점검**

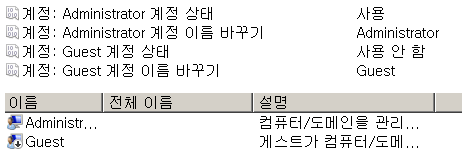
1. 보안 요구사항
2. 취약점 점검 리스트
3. 취약점 점검 일정
4. 점검 결과
5. 보안 점검
6. 계정 정책 [암호 정책 및 계정 잠금 정책]

 https://lh4.googleusercontent.com/Hg6vLIepMSQFn5U_oh0fXB7s6WVjiA67on_aEuehjXGwE5ZWOWa-PrqMTAYctEJrQO0e89lWlDaXM8r54UimntdPn6d7o5TG_xT6I3OKOjeNG1kazZYGZc-rcjmSDbEUZBmB5RlB



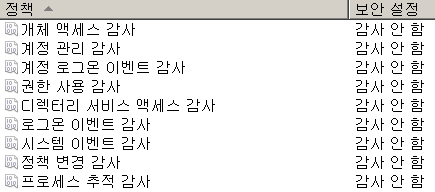
* 윈도우 OS 서버의 경우 암호 복잡성 정책만 사용, 최근 암호 기억 설정 없음, 최대 암호 사용기간 42일, 최소 암호 길이 제한 없음, 최소 암호 사용 기간 제한 없음, 계정 잠금 기간 및 임계 값 설정 없음
* CentOS 서버의 경우 /etc/pam.d/system-auth 파일 확인 결과 암호 복잡도 설정 없이 재시도 가능 횟수만 설정, 암호 사용 최대 최소 길이 설정은 기본값, 암호 만료 경고 일은 7일 전, 암호 최소 길이는 5로 설정, /etc/default/useradd 파일 확인결과 INACTIVE의 값이 -1로 계정 잠금 설정이 되어 있지 않음

1. 계정 정책 [계정 설정]

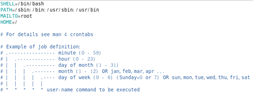
* 윈도우 서버는 관리자 계정 및 Guest 계정 명 그대로 사용, Guest 계정은 사용 안 함 상태, 원격 접속에 필요한 별도의 계정을 사용하지 않음
* CentOS 서버 /etc/passwd 파일 확인 결과 root 계정 이외에 user1 계정만 존재 사용자에 따른 구분이 보이지 않음

1. 감사 정책 [개체 액세스 및 이벤트 감사]



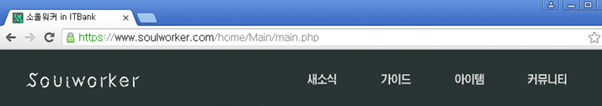
* 현재 설정된 감사 정책 없음, Linux의 로그 파일 경로 확인

1. 백업 일정 설정 및 확인

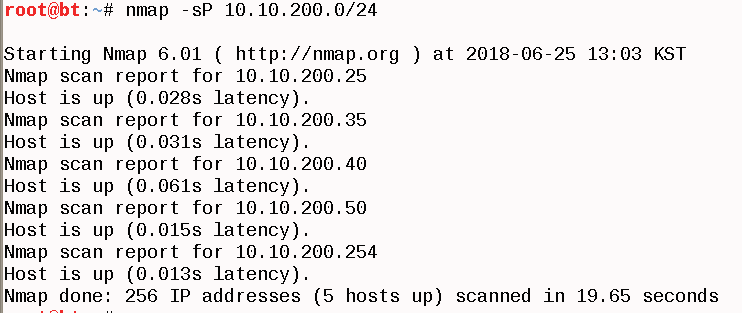
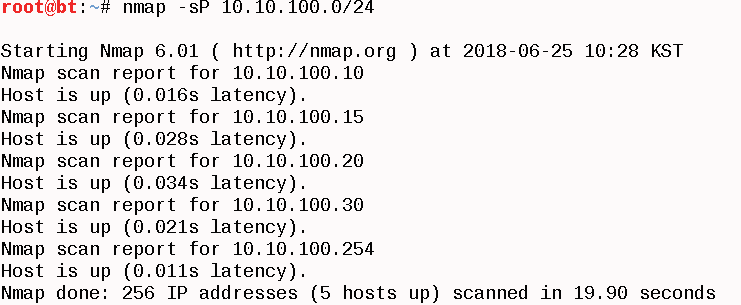
* 설정된 백업 일정 없음

1. 웹 서버 SSL 설정

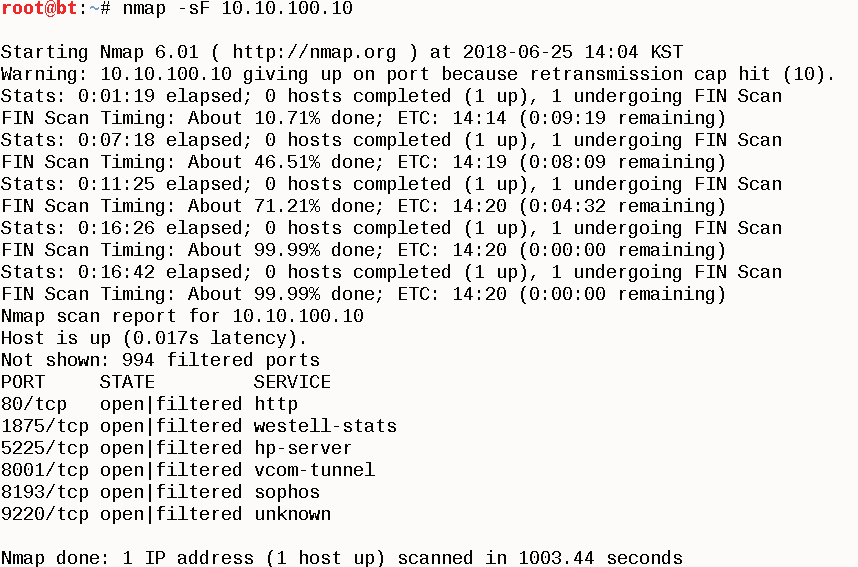
* 웹 서버 https 접속 설정 확인 및 http->https Redirect 확인

1. 시스템 보안
2. Host Scanning

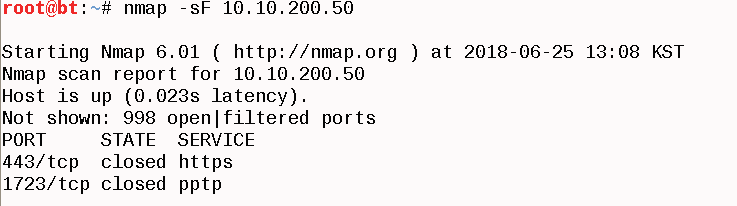
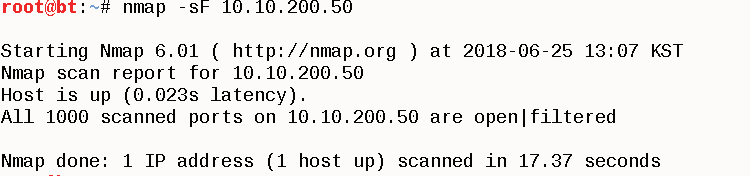


* Web, DNS[Primary], DHCP[Primary], DB, Game 서버가 있는 10.10.100.0/24 대역대와 DNS[Secondary], DHCP[Secondary], VPN, CA서버가 있는 10.10.200.0/24 대역대의 Host Scanning 결과 확인

1. Port Scanning

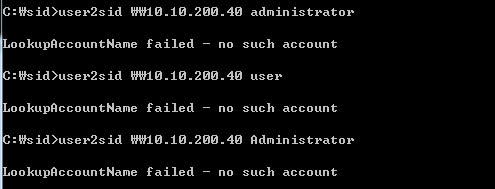


* 웹 서버[Linux, 10.10.100.10]를 대상으로 Fin Scanning을 시도했을 때의 결과



* VPN 서버[Window 2008 R2, 10.10.200.50]을 대상으로 Fin Scanning을 시도했을 때 방화벽이 있다면 Port Scanning이 되지 않고 방화벽이 없다면 열려 있는 Port들을 확인할 수 있다는 것을 알 수 있음

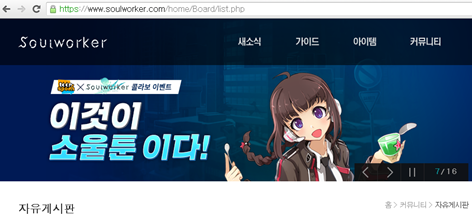
1. Null Session

* Window를 사용하는 CA서버에 Null Session은 연결이 되지만 연결된 Null Session으로는 서버의 접근할 수 없음, 아래 링크에서 확인 가능

[https://social.technet.microsoft.com/Forums/windowsserver/en-US/841523db-8c4b-43a0-9f28-be7270f92e2b/disable-server-2008-null-sessions?forum=winservergen]

1. 웹 보안
2. PUT, Delete Method 확인

 https://lh3.googleusercontent.com/OYPt-xyQrcKoQO3o4cH6yAzkhGshYTo4pY2hsbqrXrCy4dwTdxOMj61TwDt7d2a8E1zfOUSFvKdqwvDlq5JsowPtf6iL-APzvw7vh-XNI7nXhS7vVvKLVZ2HTdXCxTfkXAqXm6mg

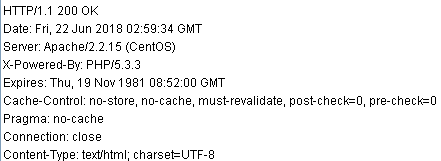
* 메인 페이지 접속 후 Paros를 통해 Packet을 확인하면 HTTP 버전이 1.1인 것을 확인할 수 있음

https://lh5.googleusercontent.com/lcuUwDfwLswBLdj1nQ668Zc8zP7sCaLQbLqhiI897H1l7CJPWM4jsIgXLzwVXX12MVBaaZJ2BvvzqgSGtzP9P-lC_NseU5bi40Eqy_8sctAmlVKBm_ndD1g2hCDwrWVJ3V6h2eWX 

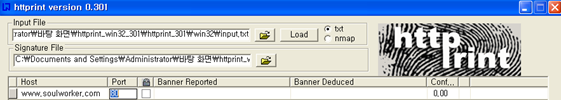
https://lh6.googleusercontent.com/KE8HfPOCUoDJ74MVobKJp5AN_RHBRbTOfA1PtZqJ6AQLekh2b2D3dMKTlCbjQBaI9aNijEgXgm-4BrUEsVrmIWl2ex2dR8nVfygCensh1UVwSwFPGiIq3_VWQA984XwDIXIVYKTd

* PUT, Delete Method 허용안됨

1. Banner Grabbing



* 현재 컨설팅 대상의 웹 페이지에 접속 후 Response Packet을 확인하면 헤더를 통해 HTTP의 버전, Apache 버전, OS 종류, PHP 버전 정보를 확인할 수 있음



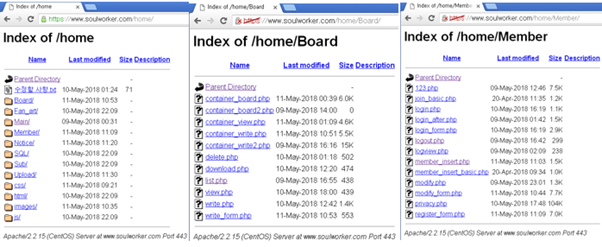
https://lh3.googleusercontent.com/SMrvEWqEBxNjyJjvz_4HfiOFwRN8Bi15NsvWssVkiEV4Gvr3RxV5VTEllkYlAAO1Nk_z65WO_U2Cd154tI6BNR-c2bvVGtoVsne4351AGleRjmyYj4CtiuhHr1zJrg9Rj84B22aX

* Httpint 툴을 이용하면 서버의 정보를 알아올 수 있는데 컨설팅 대상의 메인 페이지로 접속 시 https로 Redirect되는 것과 서버, OS의 정보가 노출되는 것을 볼 수 있음



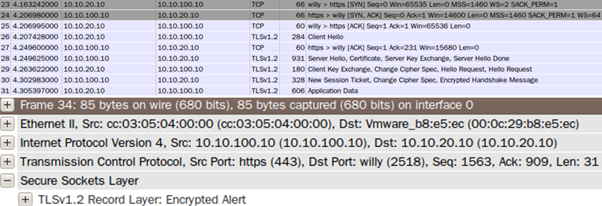
* 컨설팅 대상의 웹 페이지 접속 후 기본 페이지에서 가지고 있지 않을 만한 파일을 불러오면 웹 페이지에 오류 메시지가 출력됨, 이 오류 메시지를 확인해보면 서버와 OS의 정보를 확인할 수 있음

1. Directory Listing



* 현재 메인 페이지가 위치한 Main Directory 상위 Directory인 home으로 접속을 해보면 Directory Listing 이 실행되는 것을 확인, 이를 통해 기타 다른 Directory의 구조를 파악할 수 있음

1. Sniffing 을 통한 Session Hijacking



* ARP Spoofing을 이용한 MITM 공격으로 Sniffing에 성공 후 Packet을 확인할 수 있었지만, SSL을 이용한 암호화 통신을 하고 있었기 때문에 Packet의 내용에 포함되어 있을 세션 정보를 알아내지 못함

1. IP / Password Brute Forcing



* 모의해킹에 필요한 정상 로그인 정보를 확인하기 위해서 정상적인 방법으로 ID가 hacker이고 비밀번호가 hacker인 계정을 생성, 후에 Prose 툴을 이용해 Proxy 서버를 설정한 상태로 정상 로그인 시와 로그인 실패 시 응답 Packet 내용을 확인
* 로그인 실패 시에만 확인할 수 있는 문자열을 찾아내 Hydra 툴로 공격할 때 사용

https://lh6.googleusercontent.com/02r0W1ytGEse1x70ky6RcKyQtwFw_87bTR3FA2OEKT_VyNTCqVZeaX7Qp8ozjHE1Qjmst0vkitVUT-u6wY9J_NNvWEhQmugjtJHAVfejOV846Zzo-eHYGPNA6OUs4WWSAxdouK5A https://lh3.googleusercontent.com/HnqHVvp-ptm1qlmUn7BrjCJj7FbUUw-9u2yA4nLAZ6mcpEejpS97apVbZ7Epz6Vghi16ngaGFXRtiMIg-oMZ4cRq9D8JZeyfjgKkGVsYxBICq4vVQTb0-DH79_R0f6Povv85Vx7s

https://lh4.googleusercontent.com/dZgNuTMSNWe82wCVtImEuKrEpjy2XCib74Dvzjn6CiEbigT0_yysuiCBnisU1Wk_zg_KMW3Kz6C4tneLsQh8GHADfYE1wEZNIxqHUcR4Q8eecXdsqvGiRZtOHl9jBsxEybLqXGYt

* Hydra 툴을 사용해서 hacker 계정과 user1 계정에 대한 Brute Forcing 공격을 실시, DB에 저장된 비밀번호와 일치하는 Password를 찾아내는 것을 확인

1. XSS[Cross Site Script] 공격



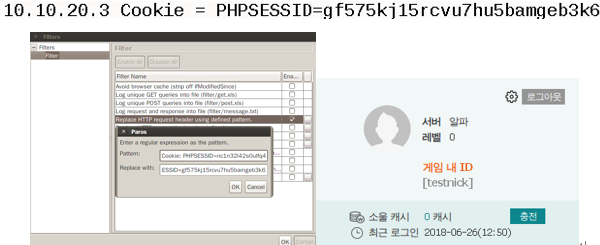
* XSS 공격을 이용해 게시 글에 Java script를 등록해 세션 쿠키 값 획득이 가능한지 확인



* 확인 후 BT으로 돌아와 웹 서비스를 실행 후 쿠키 값을 저장하기 위한 PHP파일 생성

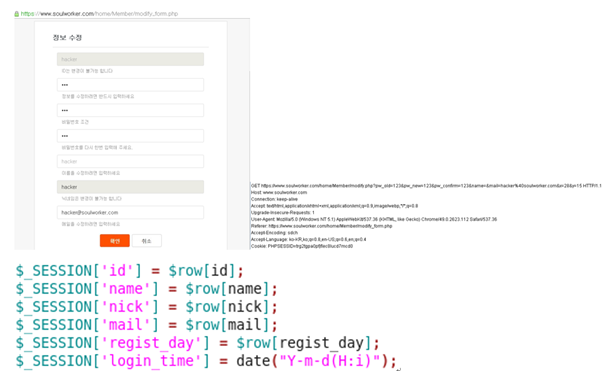


* XSS 공격 및 확인 유도 게시 글 업로드, 게시 글 확인 후 세션이 저장된 파일 확인

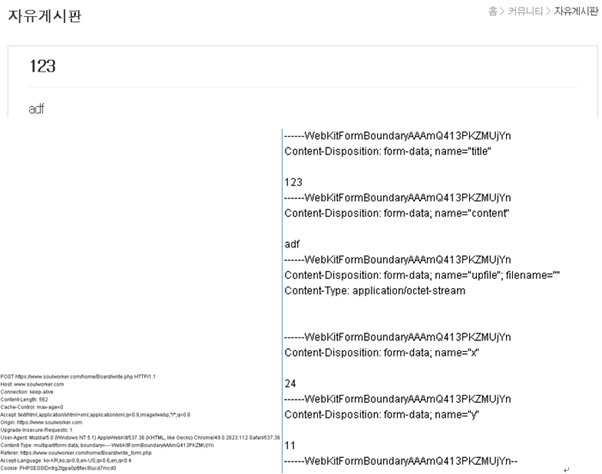


* 저장된 세션을 적용 후 세션이 유지되는지 확인

1. CSRF[Cross Site Request Forgery] 공격



* 회원 정보 수정에서 공격자가 의도한 비밀번호로 변경을 시도하려고 했으나 기존 비밀번호를 확인하는 과정이 포함되어 공격이 어려움





* 글을 게시할 때 넘어가는 Packet을 확인하고 자동 광고가 가능하도록 게시 글 작성 및 업로드



* 업로드 된 게시 글을 확인하면 공격자가 원하는 게시 글이 자동으로 등록되는 것을 볼 수 있음

1. SQL Injection [인증우회, Blind SQL Injection]

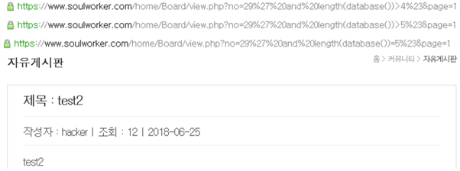
* 인증 우회 공격



* ‘ or ‘1’=’1’# 을 이용한 다른 인증 우회 공격은 실패, 단, DB 상에서 해당 SQL 쿼리를 실행했을 때 가장 상위에 위치한 레코드의 pw와 같은 값을 비밀번호로 입력하는 경우 해당 레코드 계정으로 접속됨
* Blind SQL Injection



* Injection Vector 확인



* Blind SQL Injection 공격을 통해 DB의 길이와 이름을 확인할 수 있음

and length((select table\_name from (select table\_name from information\_schema.tables where table\_schema=’SW\_db’ and table\_type=’base table’ order by table\_name limit 1) as vtable order by table\_name desc limit 1))=5%23

and substr((select table\_name from (select table\_name from information\_schema.tables where table\_schema='SW\_db' and table\_type='base table' order by table\_name limit 1) as vtable order by table\_name desc limit 1), 1, 1)=char(0x42)%23

(select table\_name from (select table\_name from information\_schema.tables where table\_schema=’SW\_db’ and table\_type=’base table’ order by table\_name limit 1) as vtable order by table\_name desc limit 1)=”board”%23

and length((select column\_name from (select column\_name from information\_schema.columns where table\_name='board' order by column\_name limit 1) as vtable order by column\_name desc limit 1))=7%23

and substr((select column\_name from (select column\_name from information\_schema.columns where table\_name='greet' order by column\_name limit 1) as vtable order by column\_name desc limit 1),1,1)=char(0x43)%23

(select column\_name from (select column\_name from information\_schema.columns where table\_name='board'\ order by column\_name limit 1) as vtable order by column\_name desc limit 1)=”content”%23

* 위 쿼리 문을 이용해 Table, Column의 이름을 확인

https://lh5.googleusercontent.com/DbNCB44fBsuTdZL1Te7mDQAu95q4kFLBwhLZJJQAs-2aX41Fh-EkMab3ollGTUnAC1pCfl2R9jmoUsu5p9-nP9TMvtfOLPWt22uB3dNwcX6D52W4krx-IshVVj7AKMylSiATkjRO

* DB가 가지고 있는 ID의 길이 및 내용 확인

https://lh5.googleusercontent.com/7zumQZIgOxYQcSPheNGTYRk3g61qV_QWRJGppoxvJ6KndlCrNFDkDxgZNzS8TeTIoaseHGts_lYlIVoJ532sjkq_1dxL5nrmbZjfwqRs0U1eOP-F44J7hhD4VLMPKt0RYpGUV4cZ

and length((select pw from (select id,pw from member order by id limit 1) as vtable order by id desc limit 1))=6%23

and substr((select pw from (select id,pw from member order by id limit 1) as vtable order by id desc limit 1), 1, 1)=char(0x42)%23

and (select pass from (select id,pw from member order by id limit 1) as vtable order by id desc limit 1)=”hacker”%23

and length(select pw from member where id =”hacker”)=6%23

and substr(select pw from member where id =”hacker”), 1, 1)=char(0x42)%23

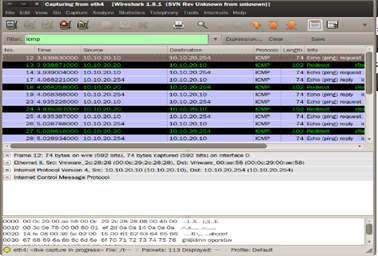
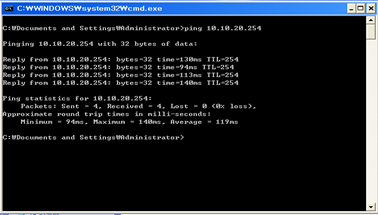
and (select pw from member where id =”hacker”)=”hacker”%23

* 비밀번호의 길이 및 내용 확인

1. 네트워크 보안
2. ARP Spoofing

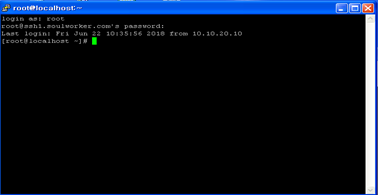
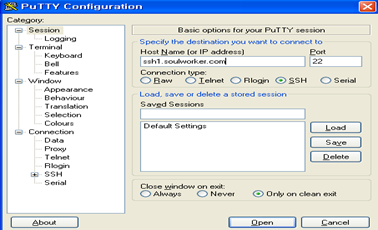


* 공격자가 경영기획부 네트워크에 침입해 BT으로 Gateway에 자신이 경영관리부 직원 PC[10.10.20.10]이라 속이고 경영관리부 직원 PC에 자신이 Gateway[10.10.20.254]라고 속임
* 공격대상 PC와 Gateway가 원활하게 통신할 수 있도록 Forwarding을 해주고 Sniffing 시작

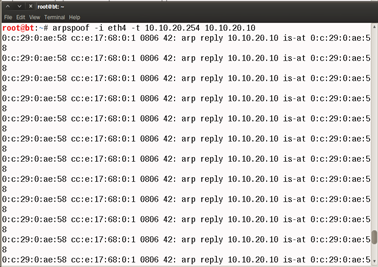
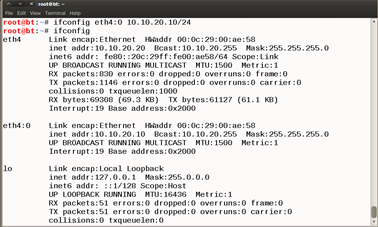


* 공격이 제대로 이루어졌는지 확인하기 위해 공격대상 PC에서 Gateway Ping test
* BT에서 공격대상 PC와 Gateway가 서로 Ping test하는 것을 Sniffing

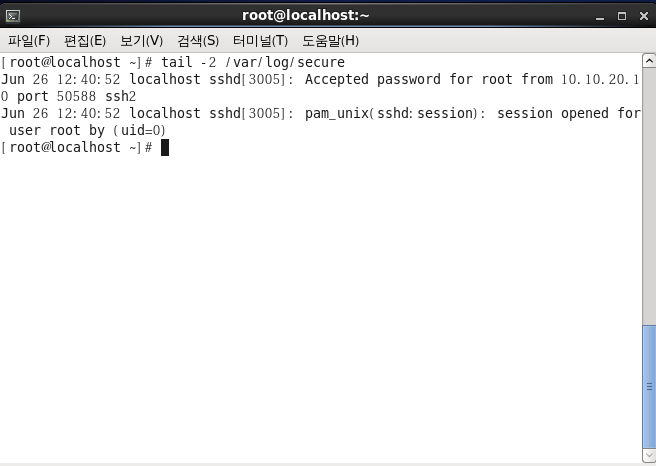
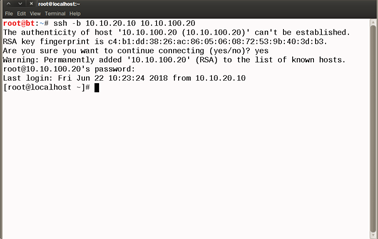
1. IP Spoofing



* 공격에 앞서 경영관리부 PC를 이용해 DNS서버[10.10.100.20]에 SSH로 접근이 가능한지 확인

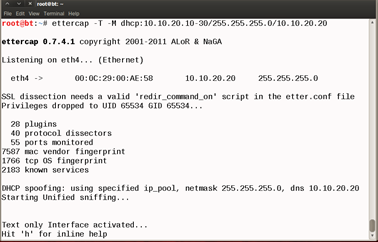
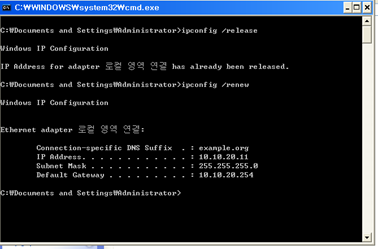


* BT에 경영기획부 PC[10.10.20.10]의 주소를 가상 인터페이스에 부여 후 공격을 위해 Gateway에게 자신이 경영기획부 PC[10.10.20.10]라고 속임

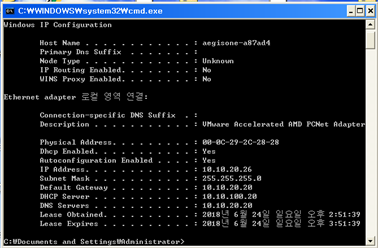
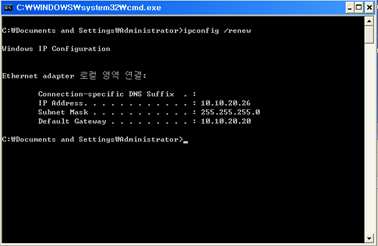


* BT에서 ssh –b 옵션을 이용해 가상 인터페이스에 부여한 경영기획부 PC[10.10.20.10] 아이피로 DNS서버[10.10.100.20]에 SSH로 접근하고 DNS 서버에서 SSH 접속 현황을 확인했을 때 경영기획부 PC [10.10.20.10]으로 로그인 되었다는 것을 볼 수 있음

1. DHCP Spoofing

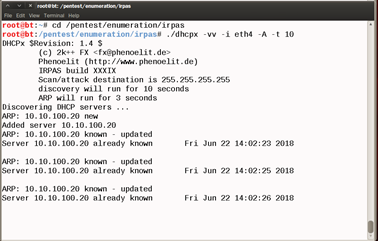
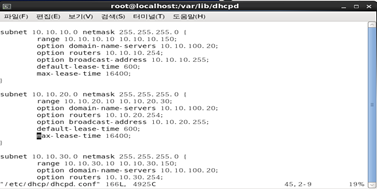


* 경영기획부 직원 PC에서 DHCP서비스를 이용해 아이피를 제대로 할당 받아오는지 확인 후 공격자가 BT에서 ettercap 툴을 이용해 DHCP Spoofing 공격 시도

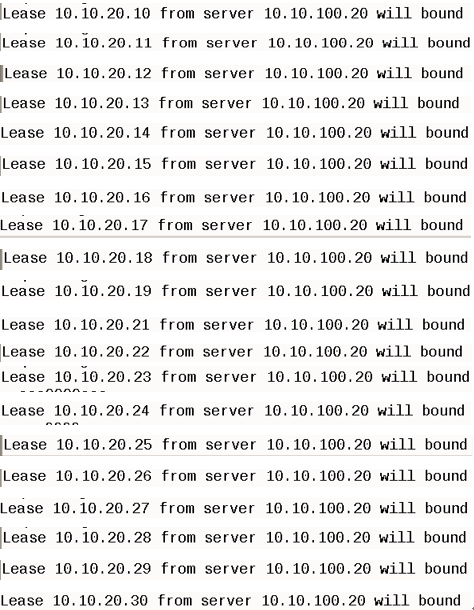


* 공격대상 PC에서 DHCP서버를 이용해 아이피를 할당 받으면 BT에서 설정한 대로 받아오는 것을 볼 수 있음

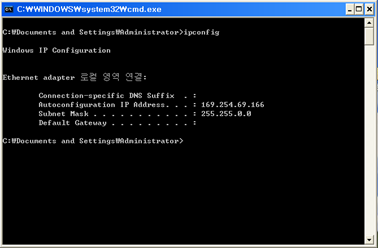
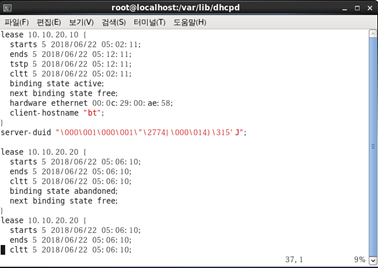
1. DHCP Starvation



* 공격을 한 뒤 확인을 위해 할당범위 재 설정을 하고 BT에서 Ettercap 툴을 이용해서 DHCP서버에 공격 시도

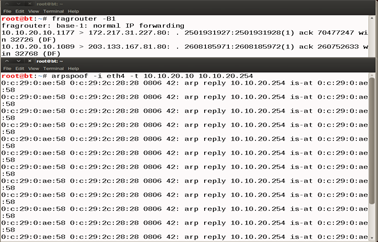
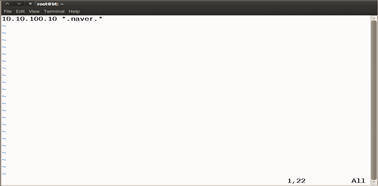


* BT에서 공격 내용 확인 시 BT이 가지고 있는 10.10.20.20을 제외한 나머지 주소들을 할당 받아 온 것을 볼 수 있음

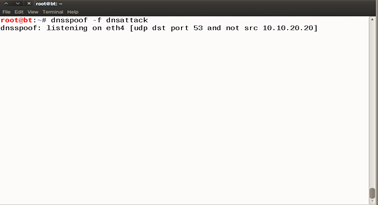


* DHCP서버로 이동해 아이피 할당 내역 확인을 한 뒤 XP에서 DHCP서버에게 아이피를 할당 받아보지만 DHCP서버가 더 이상 아이피를 할당하지 못해 아이피를 받아오지 않음

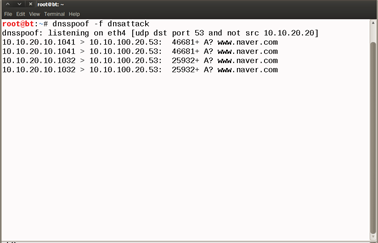
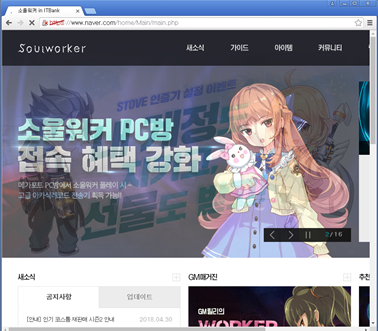
1. DNS Spoofing



* BT에서 DNS Spoofing 공격을 위한 파일 생성을 하고 경영기획부 PC를 대상으로 MITM 상태 만들기



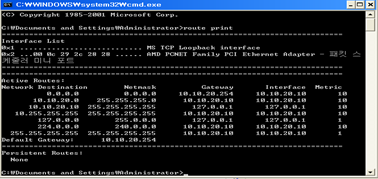
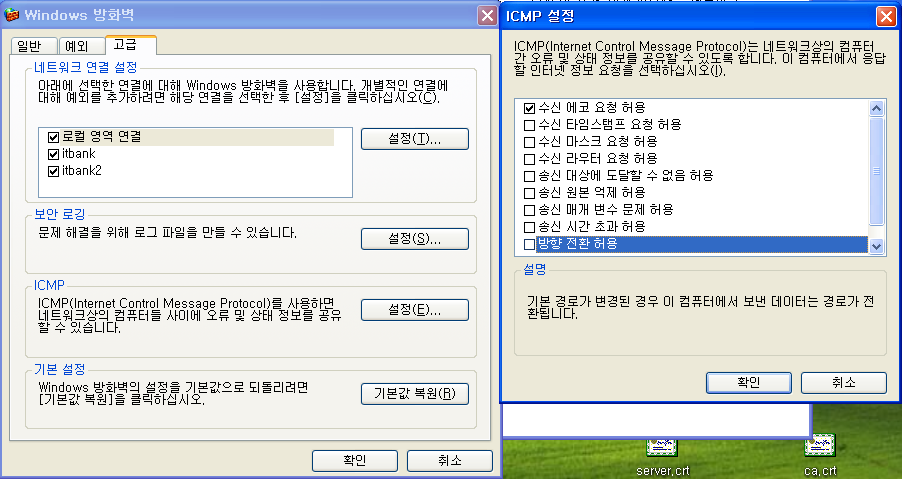
* dnsspoof 툴을 이용해 DNS Spoofing 공격 시도



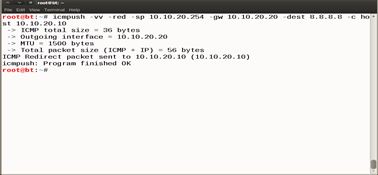
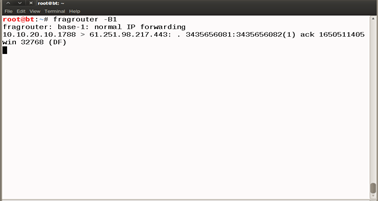
* 경영기획부 PC로 가서 공격이 제대로 이루어졌는지 확인 후 BT에서 공격이 진행된 내용 확인

1. ICMP Redirection

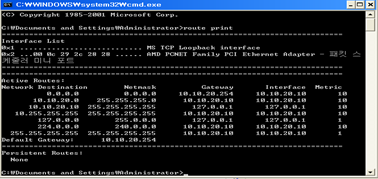
* 방향 전환 요청이 꺼져있을 경우



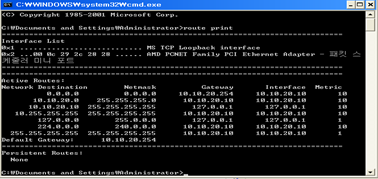
* 공격대상의 PC로 가서 방화벽 ICMP 설정에 방향 전환 요청에 체크가 되어 있는지 확인



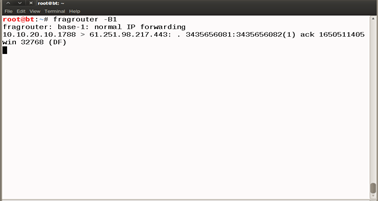
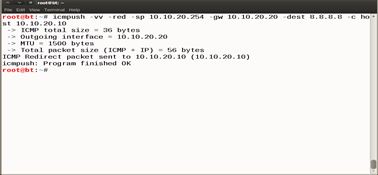
* BT으로 가서 Forwarding을 하고 icmpush 툴을 사용해 공격



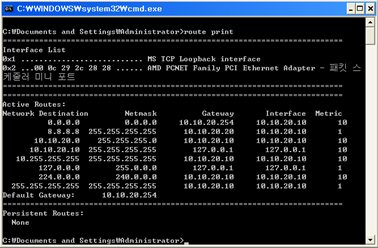
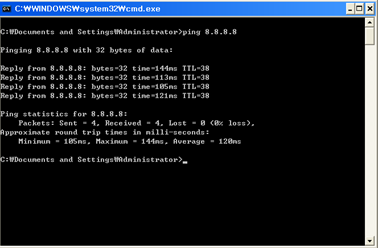
* 다시 공격대상의 PC로 돌아와 Routing Table을 확인해보면 변동이 없는 것을 볼 수 있음
* 방향 전환 요청이 켜져 있을 경우



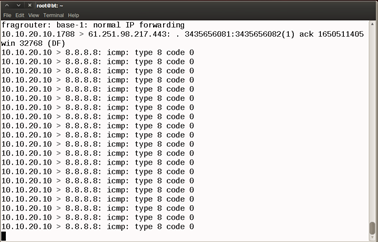
* 공격대상의 PC로 가서 방화벽 ICMP 설정에 방향 전환 요청에 체크가 되어 있는지 확인

* BT으로 가서 Forwarding을 하고 icmpush 툴을 사용해 공격

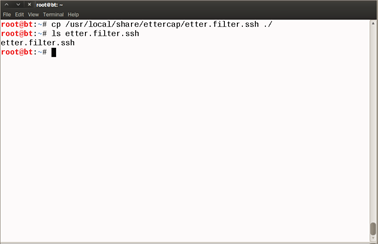
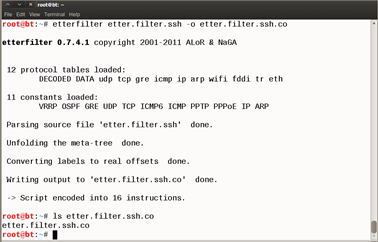
 

* 공격을 한 뒤 경영기획부 PC Routing Table을 확인했을 때 공격한 내용이 테이블에 추가된 것을 볼 수 있음, BT에서 Packet을 볼 수 있는지 확인하기 위해 공격대상 PC로 외부에 Ping test

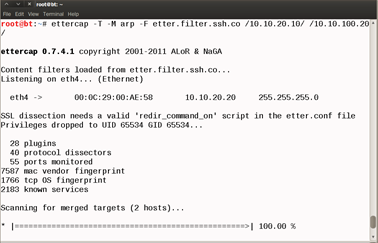
 

* BT으로 확인했을 때 Forwarding이 제대로 되는지, Wire Shark로 확인했을 때 Packet들이 제대로 잡히는지 확인

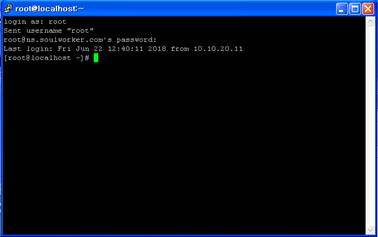
1. SSH 취약점

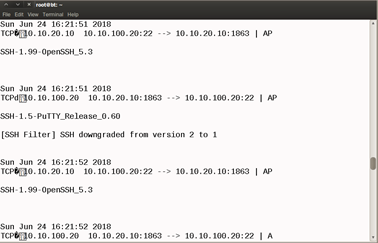
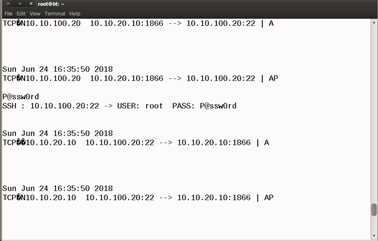
* SSH 버전 협상 시 버전 정보 변경을 하기 위한 filter파일 생성



* Ettercap 툴과 만든 etter.filter.ssh.co 필터 파일을 이용해 경영기획부 PC에 공격

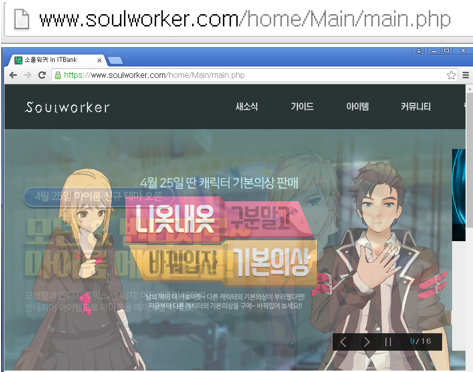
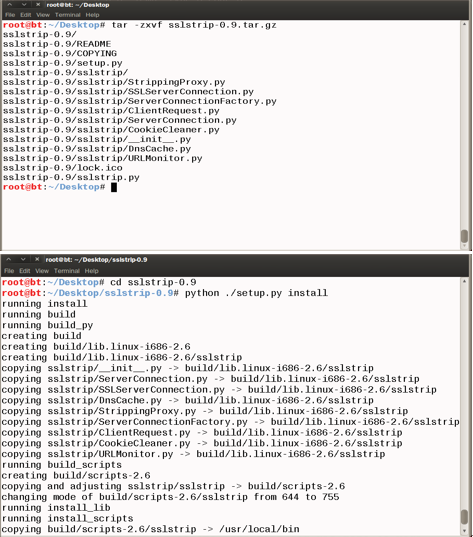
  

* 공격 확인을 위해 경영기획부 PC에서 DNS서버로 SSH 접속

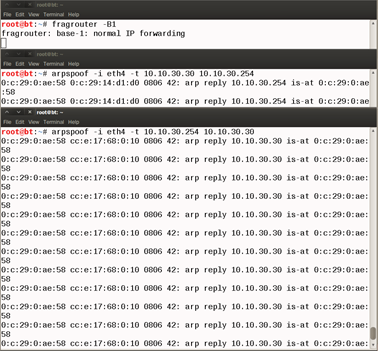
 

* BT에서 확인해보면 제대로 버전을 다운그레이드 했다는 것을 볼 수 있고 경영기획부 PC에서 DNS서버로 SSH 접속 시 사용했던 아이디와 비밀번호도 확인 가능

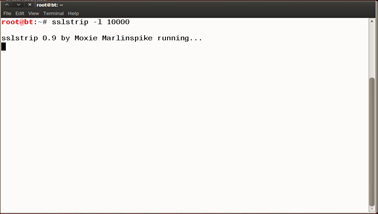
1. SSL Strip Attack

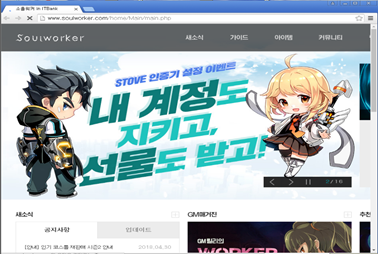
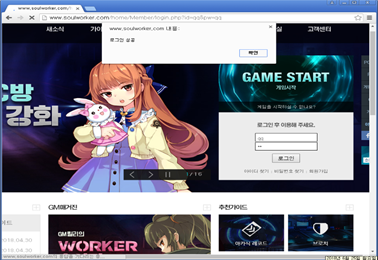
* 공격 시도에 앞서 TLS가 제대로 작동하는지 확인 후 SSL strip 공격을 위한 sslstrip 툴 설치

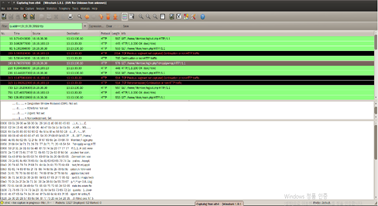
* Gateway와 개발관리부 PC에 MITM 상태를 만들고 80번 포트로 접근을 시도하면 10000번 포트로 Redirect 시키겠다는 방화벽 설정



* Sslstrip 툴 실행 –l 옵션으로 10000포트로 들어오는 요청에 대해 http로 접근하도록 설정

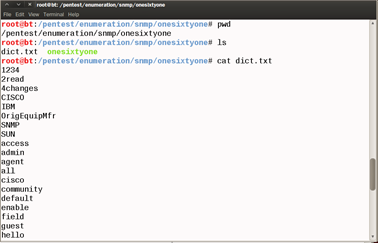
 

* 개발관리부 PC로 웹에 접근을 시도하면 https가 아닌 http로 접근하는 것을 확인 후 로그온 시도

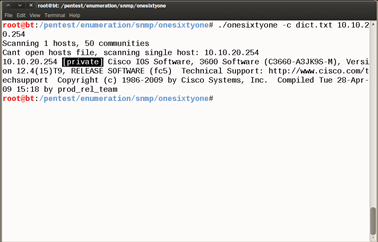


* BT으로 돌아와 Wire Shark를 확인해보면 아이디와 비밀번호가 노출된 것을 볼 수 있음

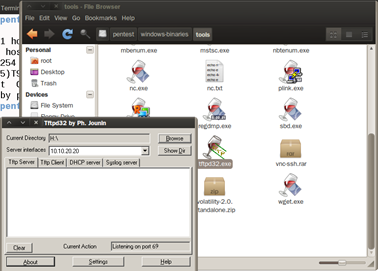
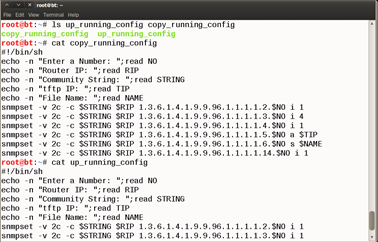
1. SNMP 취약점

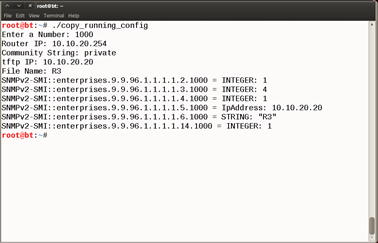
* 공격에 앞서 snmp서비스를 지원해주는지 nmap툴을 사용해 확인 후 Community String을 알아 오기 위해 사용할 dictionary 파일인 dict.txt파일 확인



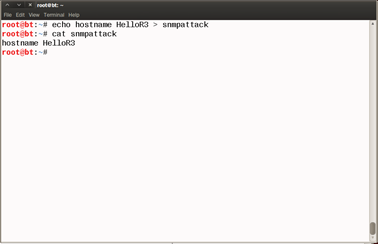
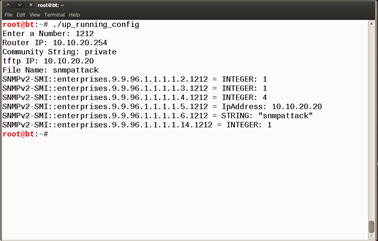
* Onesixtyone 툴과 dict.txt파일을 사용해 공격대상의 Community String 알아오기

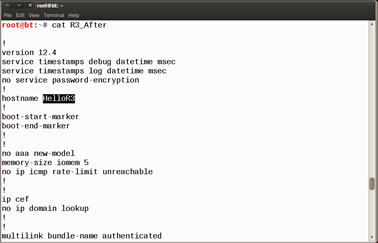
* 공격을 하기 위해 tftp을 실행하고 up\_running\_config, copy\_running\_config 파일 확인

* Copy\_running\_config 파일과 tftp를 이용해 공격대상의 running\_config 상태를 파일로 받고 제대로 running\_config 상태를 받아왔는지 확인

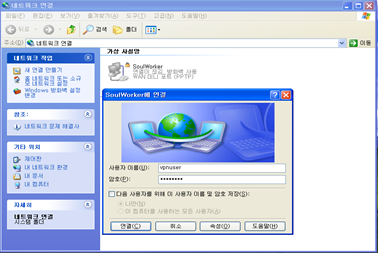
 

* 받아온 running\_config 상태 확인 후 바꾸고 싶은 내용을 파일로 만들고 Up\_running\_config 파일을 이용해 만든 공격파일을 공격대상에게 보내기

* 공격이 제대로 됐는지 확인하기 위해 다시 running\_config 상태를 파일로 받고 받아온 파일에서 내가 바꾼 내용이 제대로 적용 됐는지 확인

1. VPN Sniffing

* 지사의 컴퓨터를 이용해 본사 VPN 서버에 접속

https://lh6.googleusercontent.com/fGKzU8KLdTfnKbRyY1z7qAogzLBxFtb84LMbOKR0eB_RB3BetE0ZDd7crHO62FQSIs59M9cLpqeZaa4XtuNZylTauUuELe9Z4f_BY_iIFI-B-mgU8_iI9lNSX7O11wOnRsX2xOoT

* Wire Shark로 확인해보면 아이디와 컴퓨터 이름을 볼 수 있음