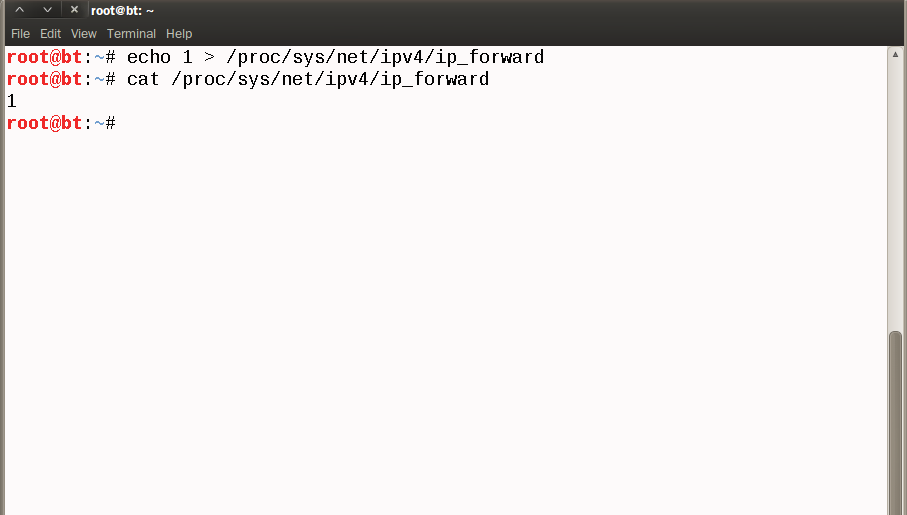
네트워크 보안

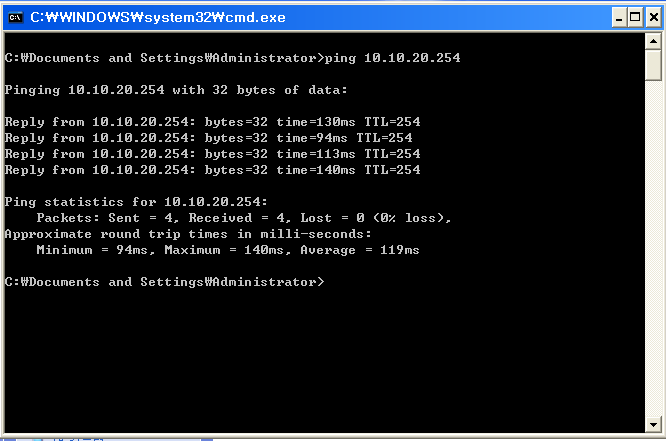
* ARP Spoofing



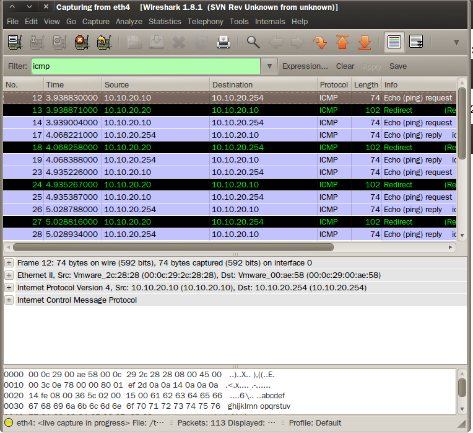
* 공격자가 경영기획부 네트워크에 침입해 BT으로 게이트웨이에 자신이 경영관리부 직원 PC[10.10.20.10]이라 속이고 경영관리부 직원 PC에 자신이 게이트웨이라 속임



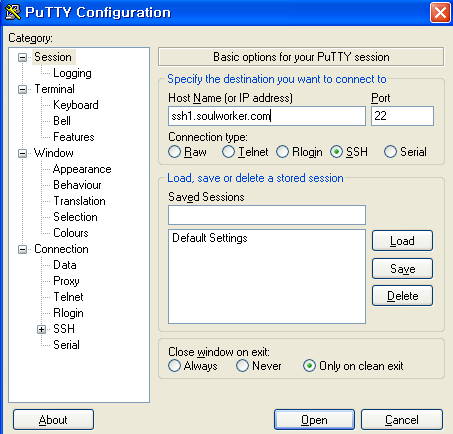
* 공격대상 PC와 게이트웨이가 통신하는 것을 Sniffing하기 위해 포워딩 시작

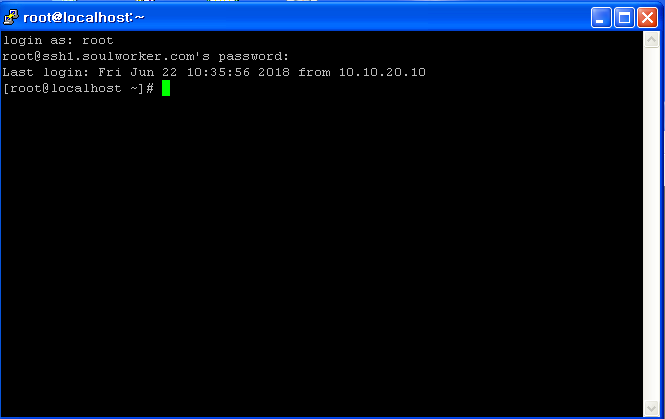


* 예시로 공격대상 PC가 게이트웨이에 Ping Test

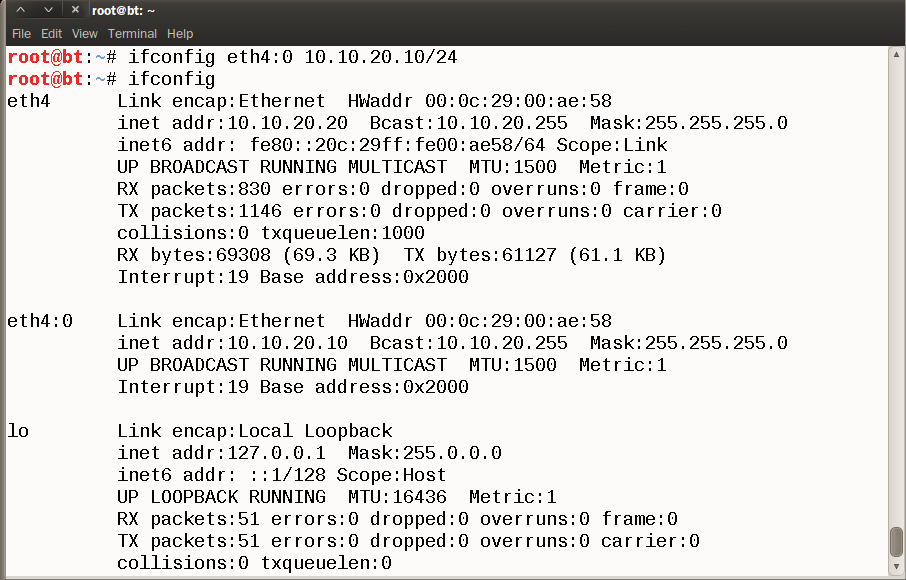


* BT 와이어샤크로 공격대상 PC와 게이트웨이가 Ping Test하는 것을 리다이렉트하면서 Sniffing하는 것을 확인
* IP Spoofing

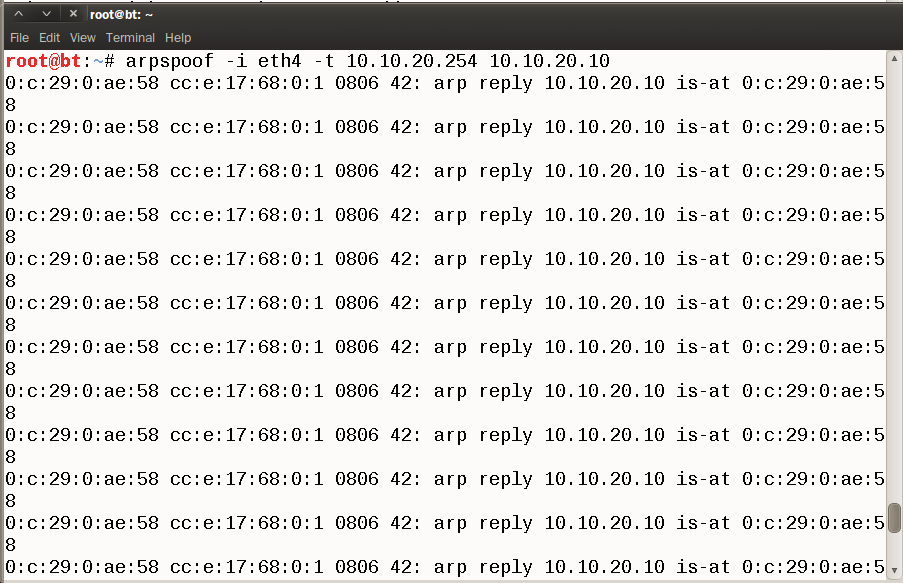




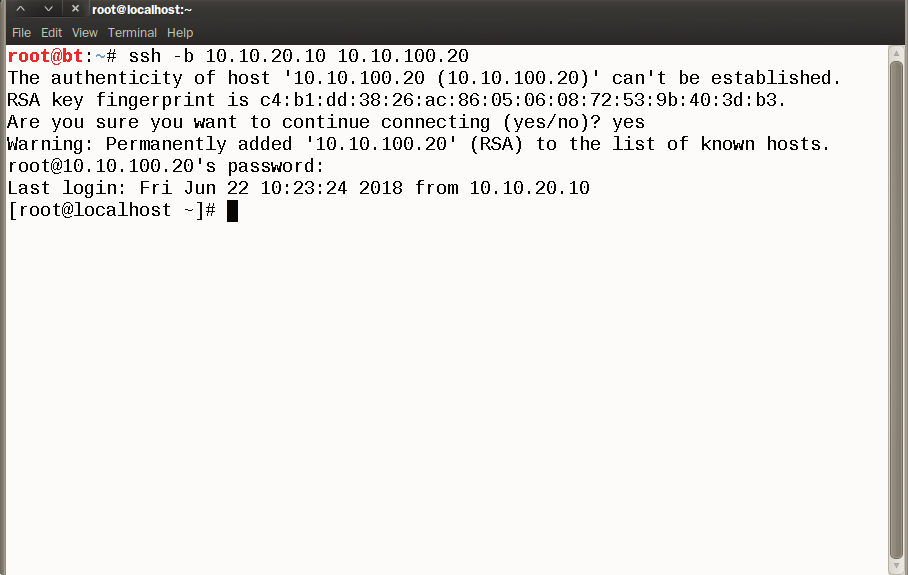
* 먼저 경영관리부 PC를 이용해 DNS서버[10.10.100.20]에 SSH로 접근이 가능한지 확인



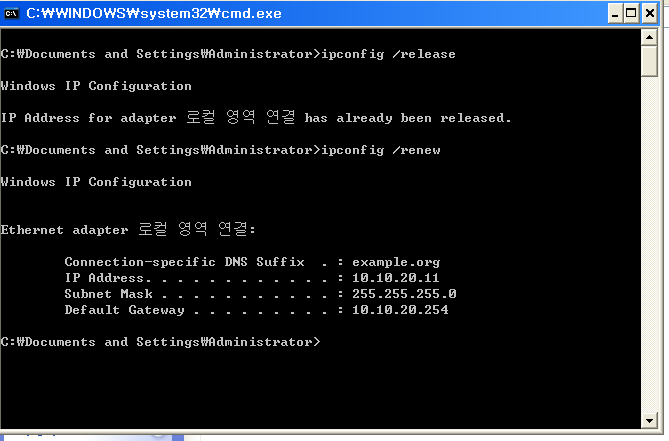
* BT에 경영기획부 PC[10.10.20.10]의 주소를 가상 인터페이스에 부여



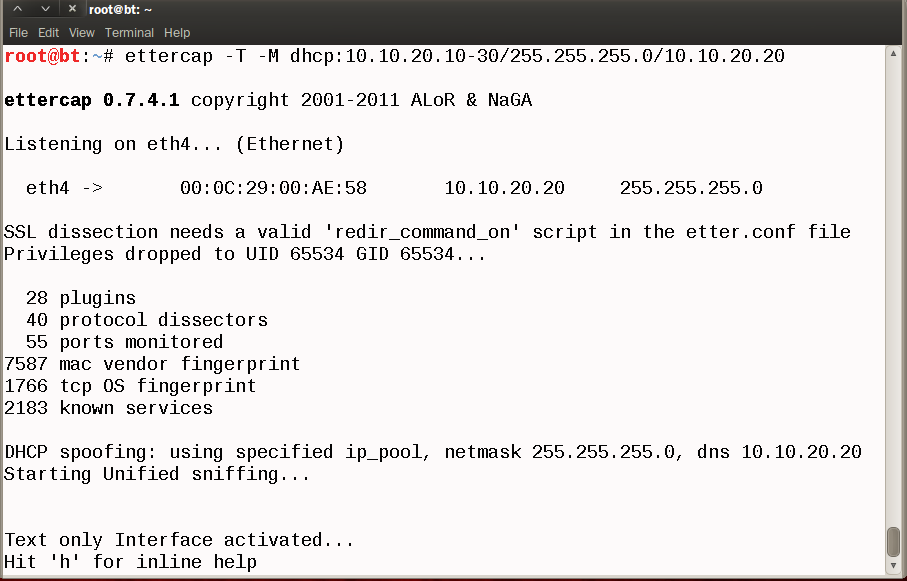
* 공격을 위해 게이트웨이에게 자신이 경영기획부 PC[10.10.20.10]라고 속임



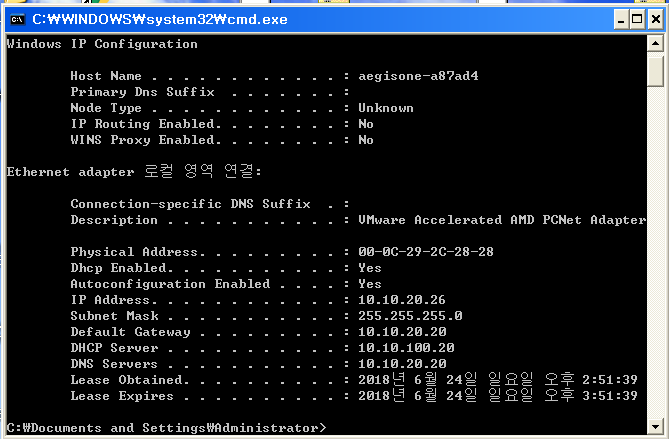
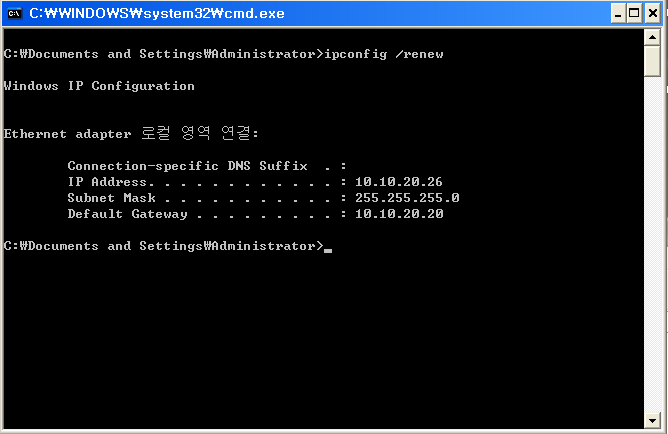
* BT에서 ssh –b 옵션을 이용해 가상 인터페이스에 부여한 경영기획부 PC[10.10.20.10] 으로 DNS서버[10.10.100.20]에 SSH로 접근
* DHCP Spoofing



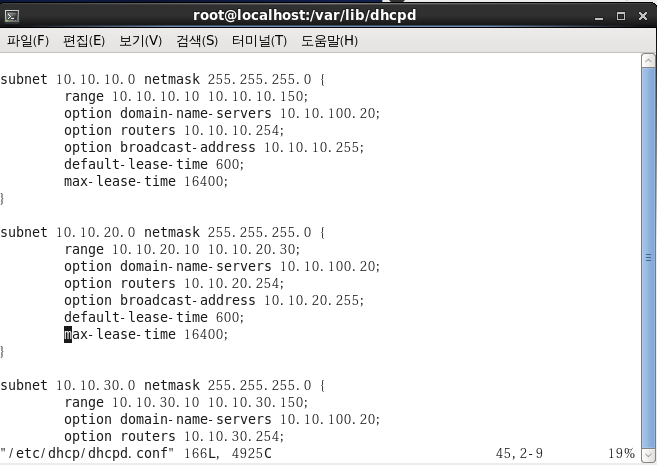
* 경영기획부 직원 PC에서 DHCP서비스를 이용해 아이피를 제대로 할당 받아오는지 확인



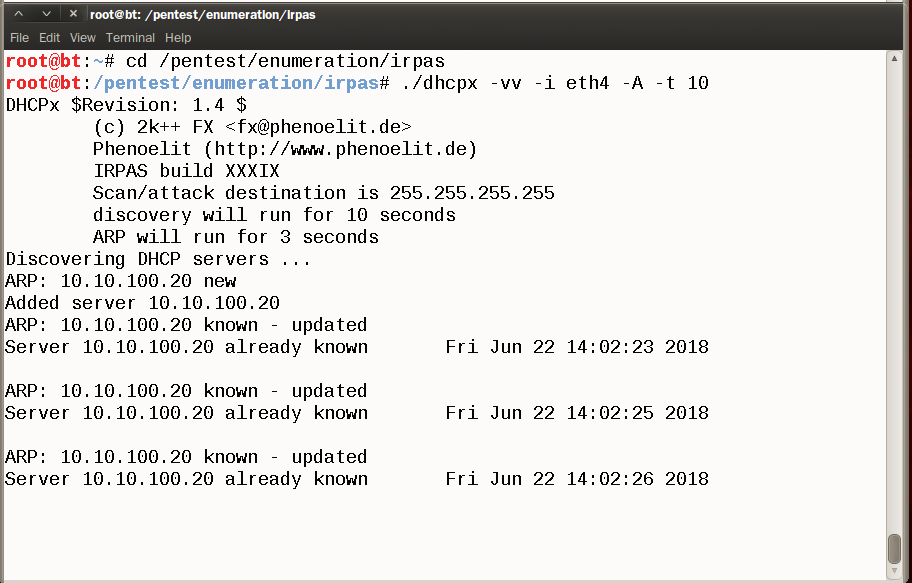
* 공격자가 BT에서 ettercap 툴을 이용해 DHCP Spoofing 공격 시도



* XP에서 DHCP서버를 이용해 아이피를 할당받으면 BT에서 설정한 대로 받아오는 것을 볼 수 있음
* DHCP Starvation



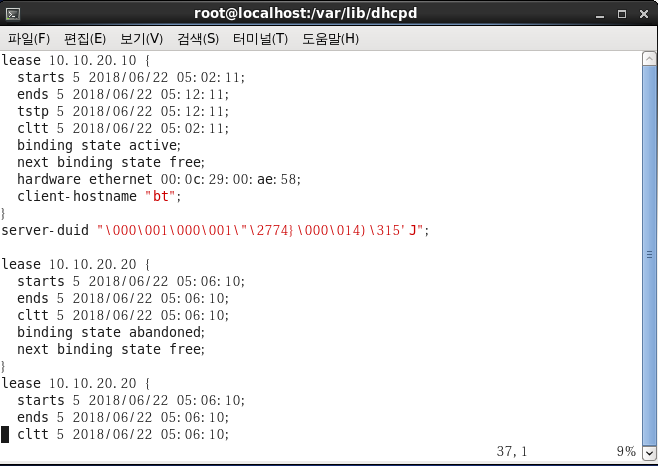
* 공격 후 확인을 위해 할당범위 재 설정



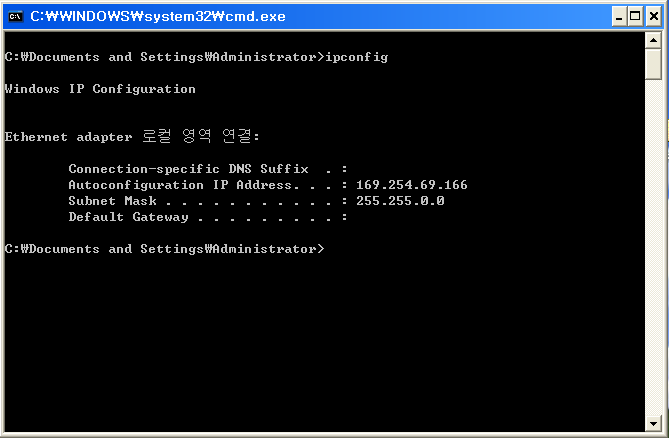
* BT에서 Ettercap 툴을 이용해서 DHCP서버에 공격 시도



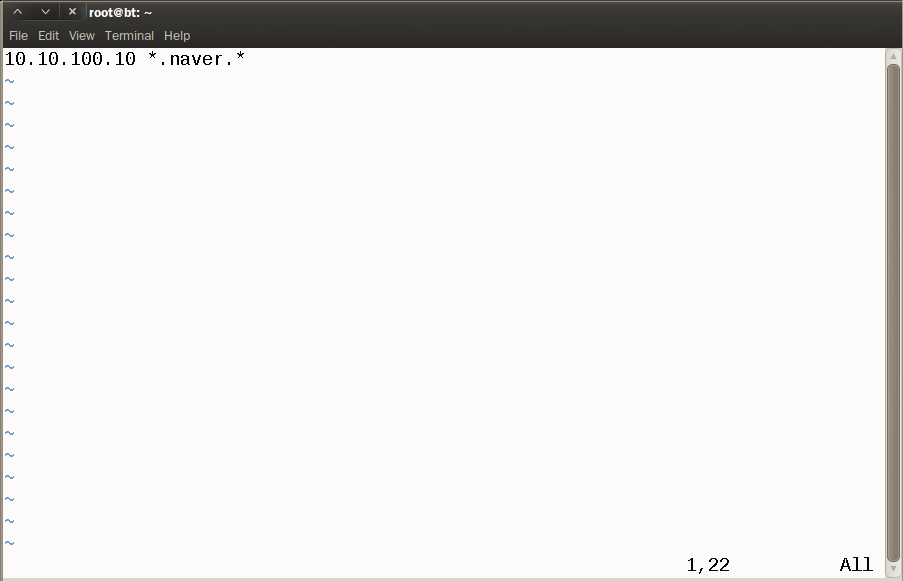
* BT에서 공격을 통한 아이피 할당 내용 확인



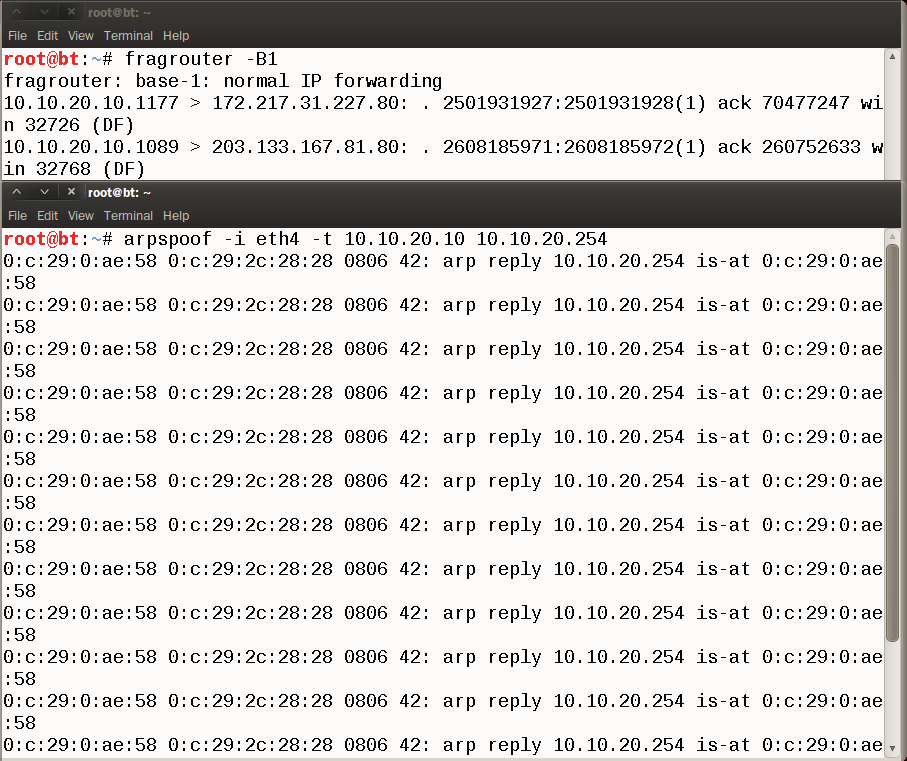
* DHCP서버로 이동해 아이피 할당 내역 확인



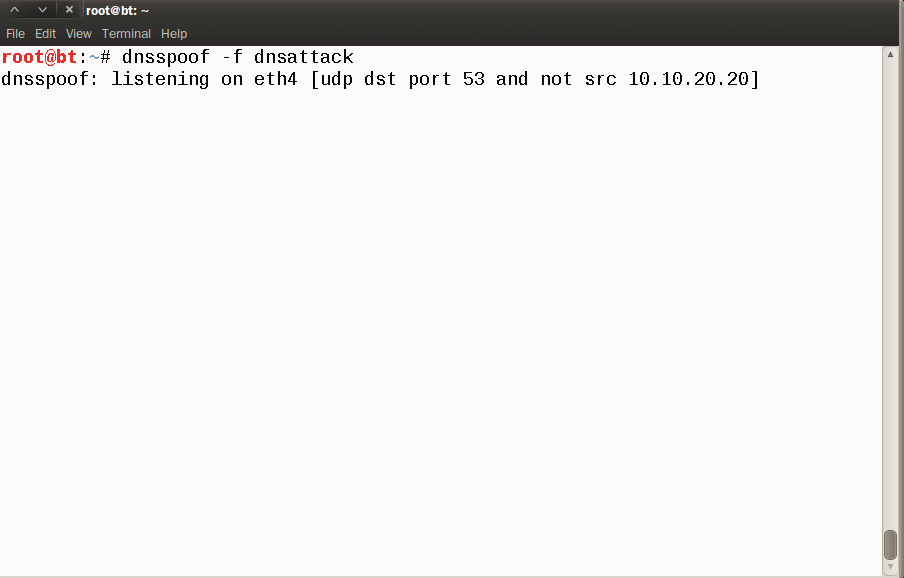
* XP에서 DHCP서버에게 아이피를 할당 받아보지만 DHCP서버가 더 이상 아이피를 할당하지 못해 아이피를 받아오지 않음
* DNS Spoofing



* DNSSpoofing 공격을 위한 파일 생성



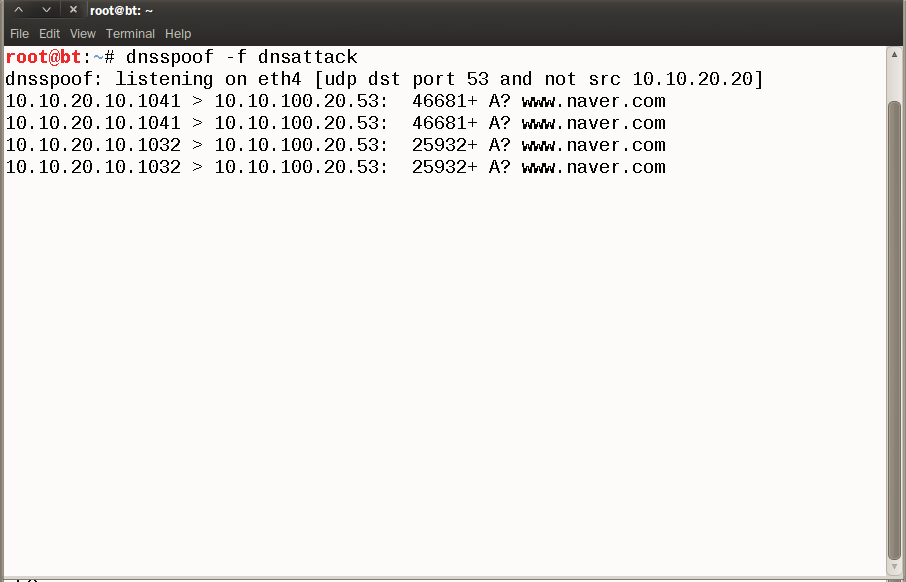
* 경영기획부 PC에게 MITM 상태 만들기



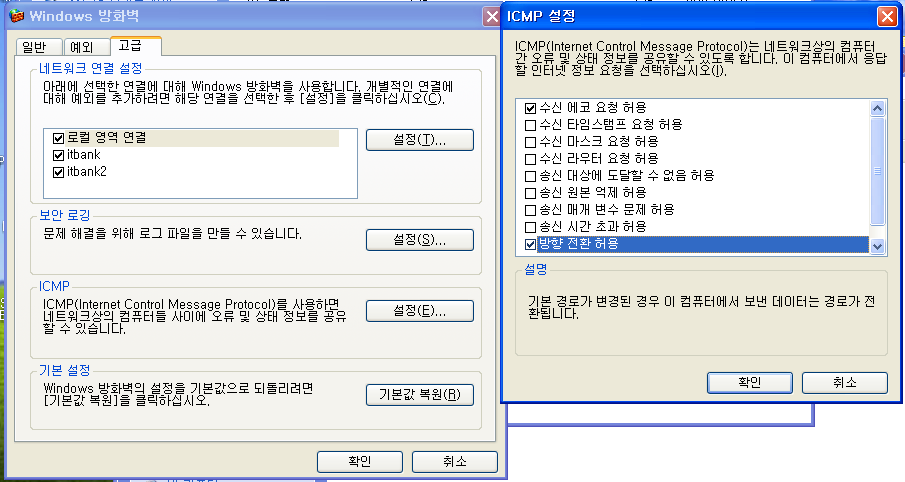
* Dnsspoof 툴을 이용해 DNS Spoofing 공격 시도

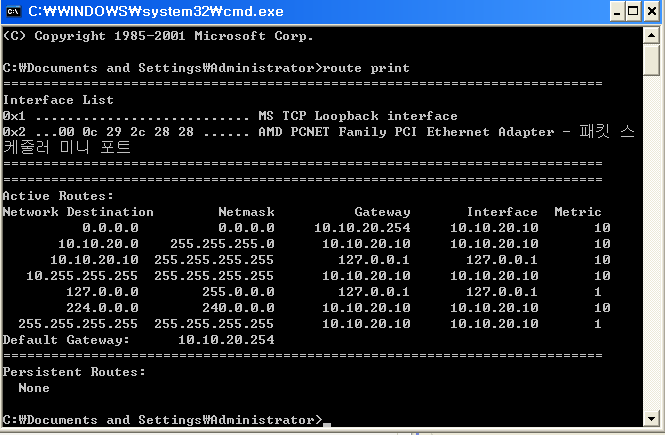


* 경영기획부 PC에서 공격이 제대로 이루어졌는지 확인

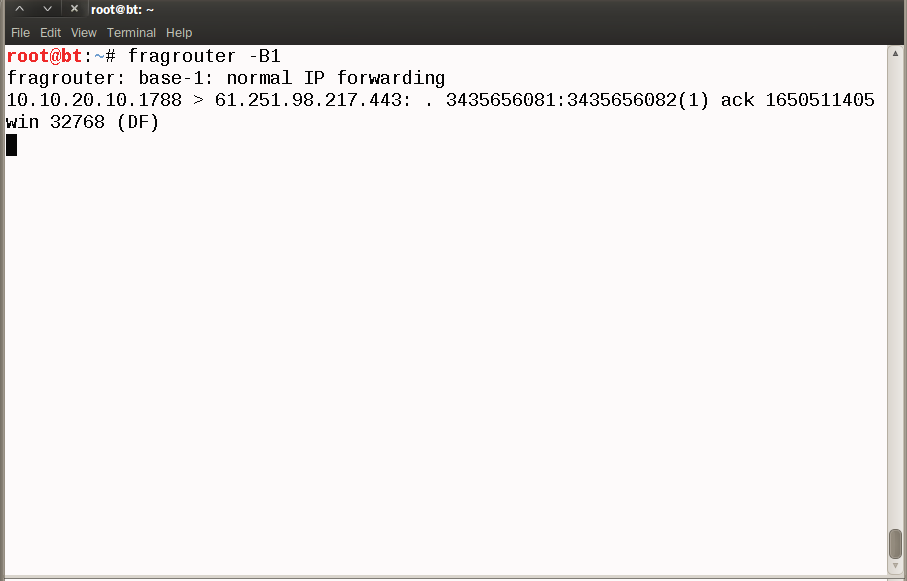


* BT에서 공격이 진행된 내용 확인
* ICMP Redirect

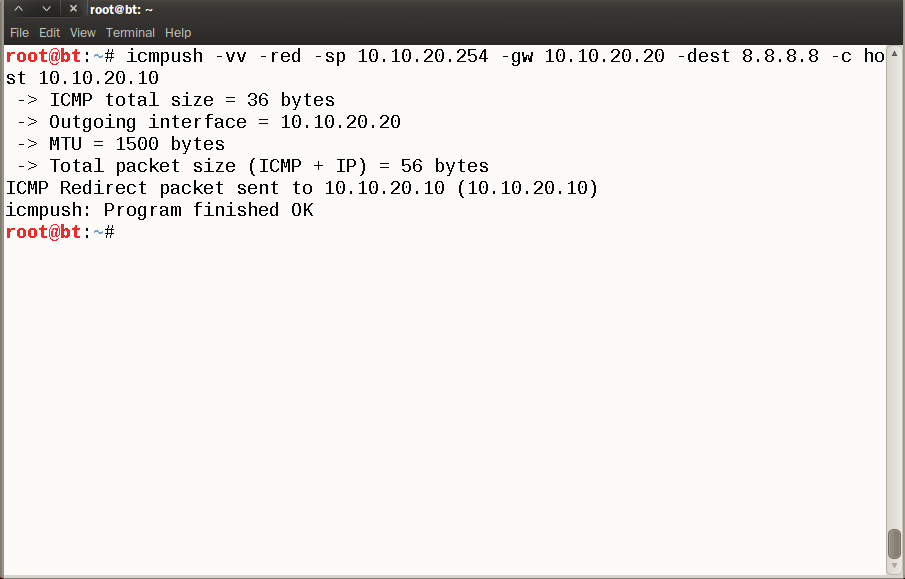




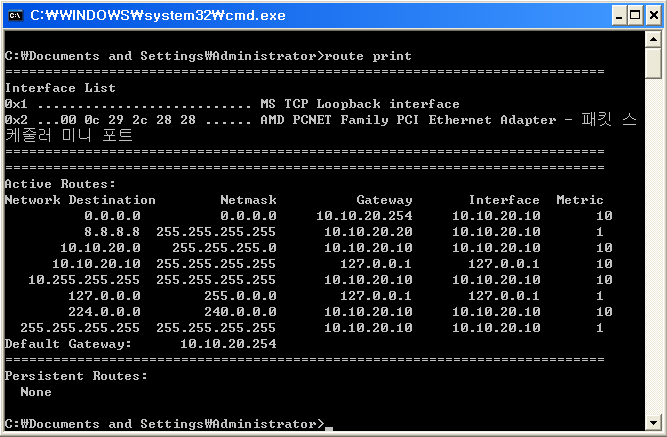
* 공격 확인을 위해 경영기획부 PC가 방향 전환 허용이 체크 되어 있는지와 라우팅 테이블 확인



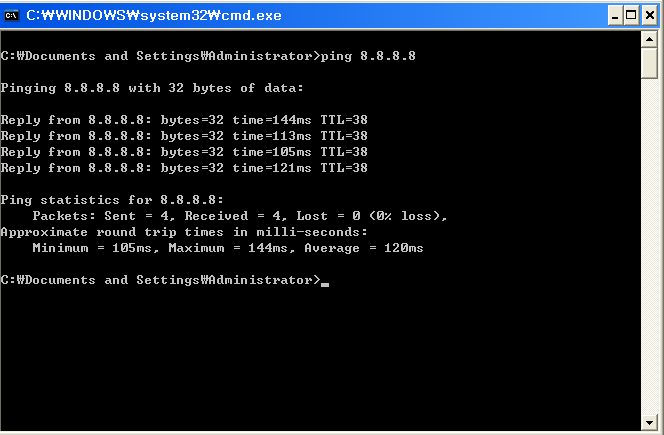
* 공격을 위해 BT에서 포워딩 시작



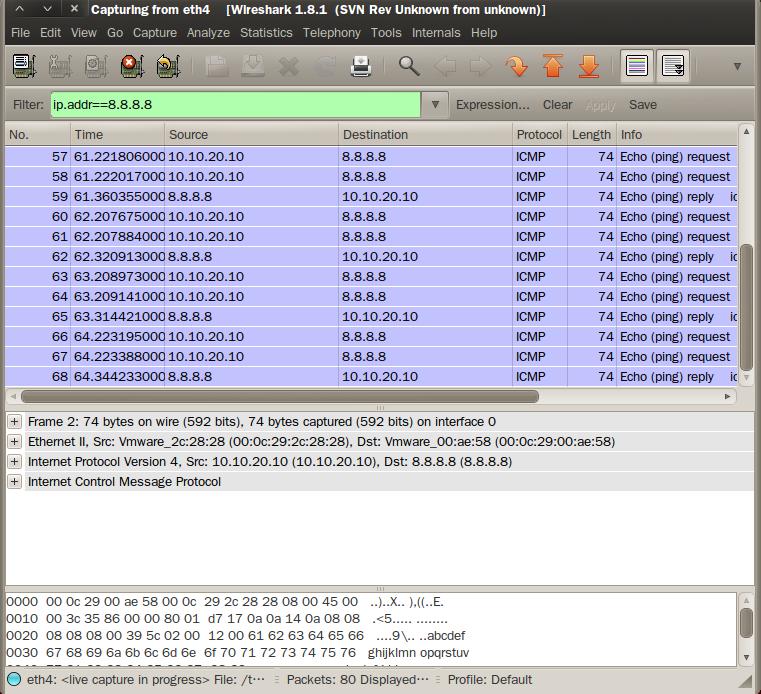
* Icmpush를 이용해서 BT으로 공격

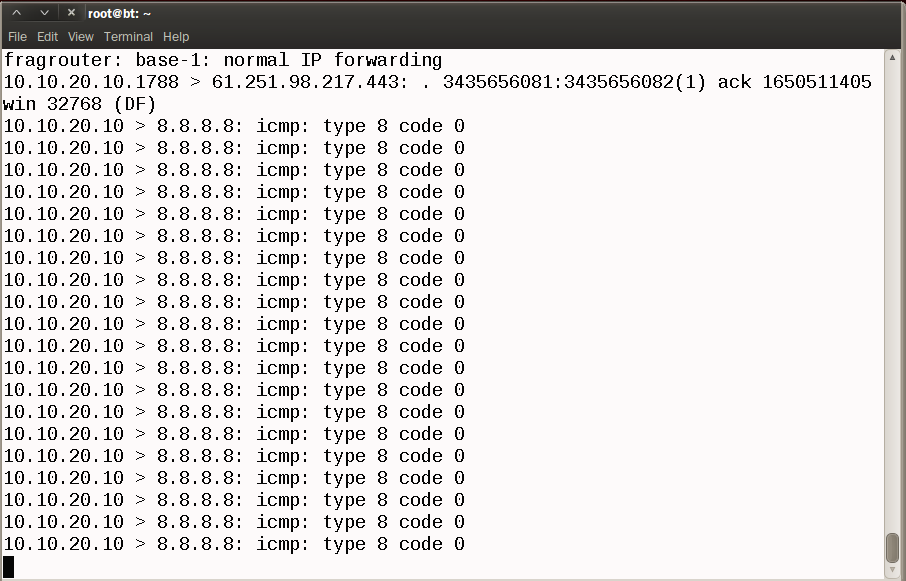


* 공격을 한 뒤 경영기획부 PC 라우팅 테이블을 확인했을 때 공격한 내용이 테이블에 추가된 것을 볼 수 있음

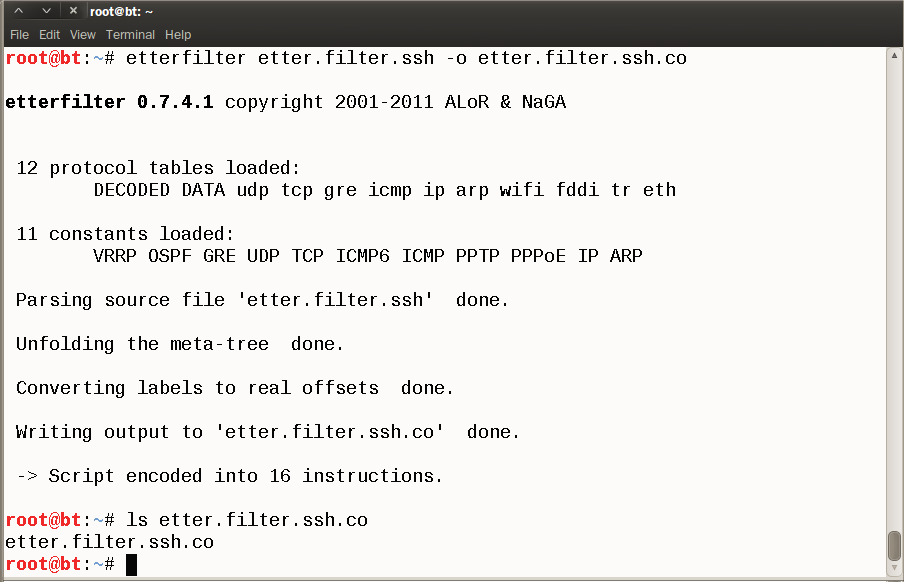
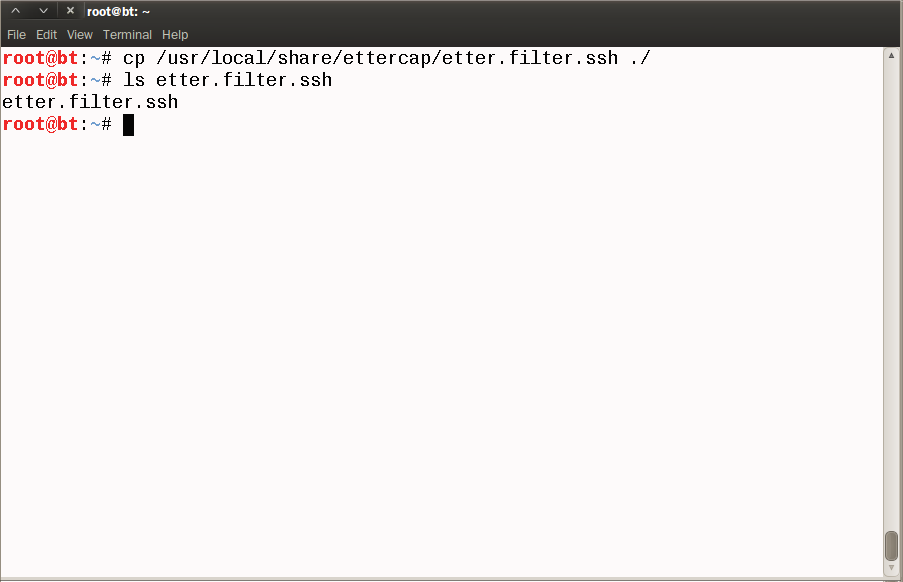


* BT에서 패킷을 볼 수 있는지 확인하기 위해 경영기획부 PC로 외부에 Ping test

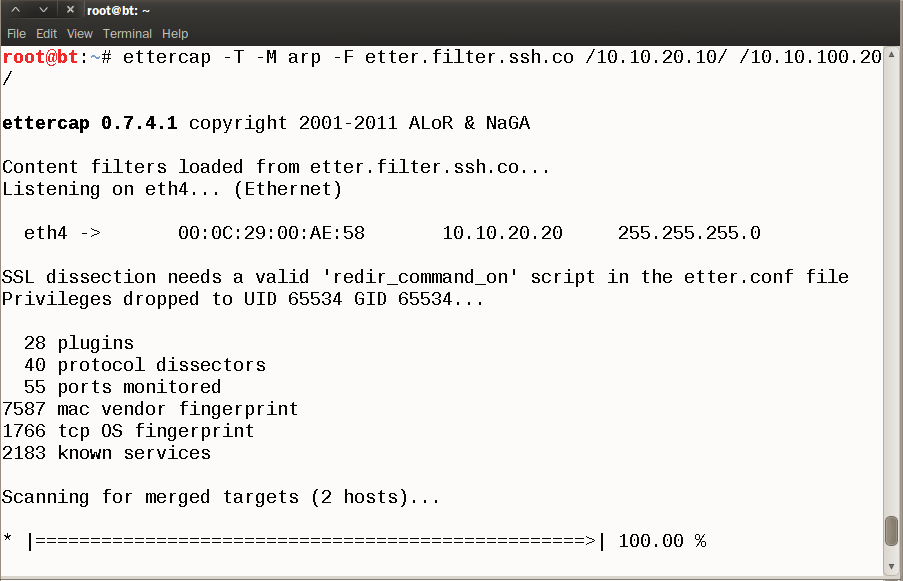




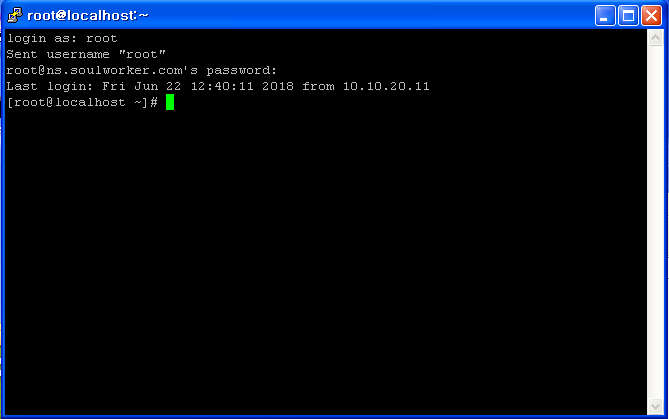
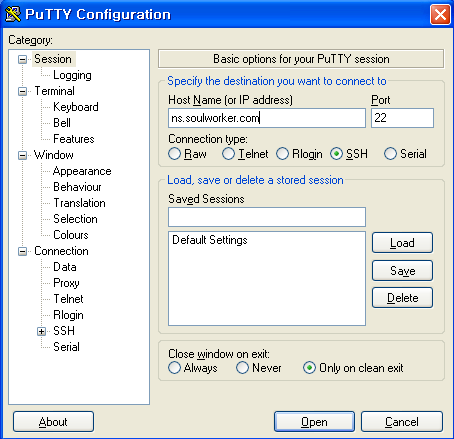
* BT으로 확인했을 때 포워딩이 제대로 되는지, 와이어샤크로 확인했을 때 패킷들이 제대로 잡히는지 확인
* SSH 취약점 공격



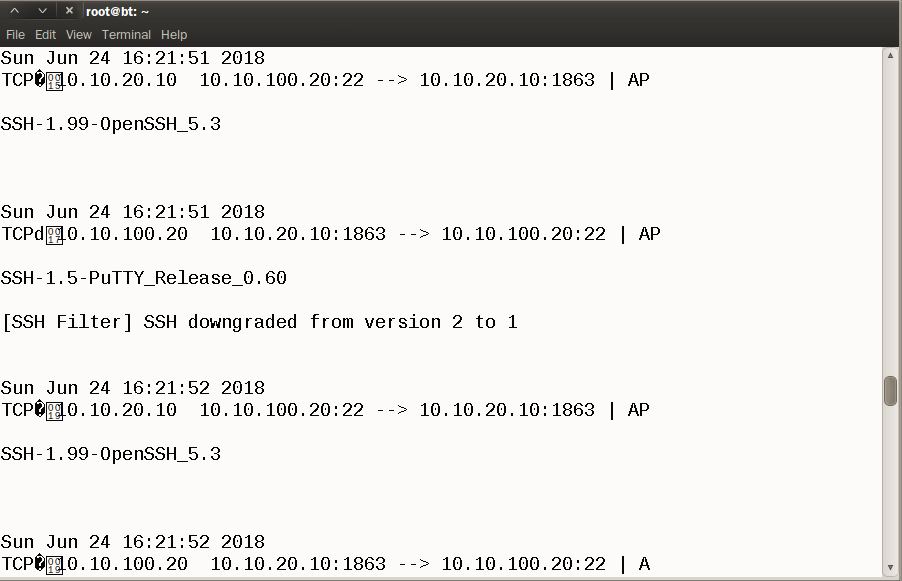
* SSH 버전 협상 시 버전 정보 변경을 하기 위한 filter파일 생성



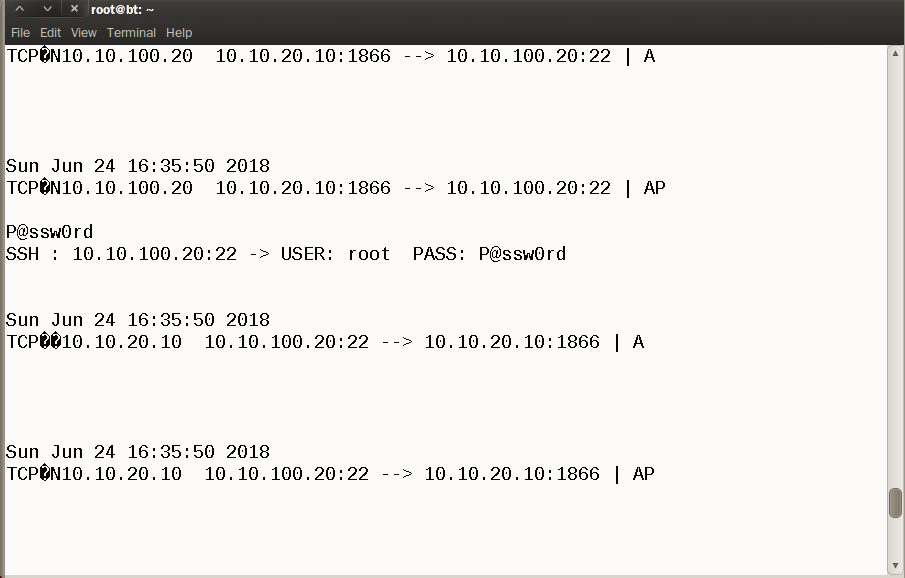
* Ettercap 툴과 만든 etter.filter.ssh.co 필터 파일을 이용해 경영기획부 PC에 공격



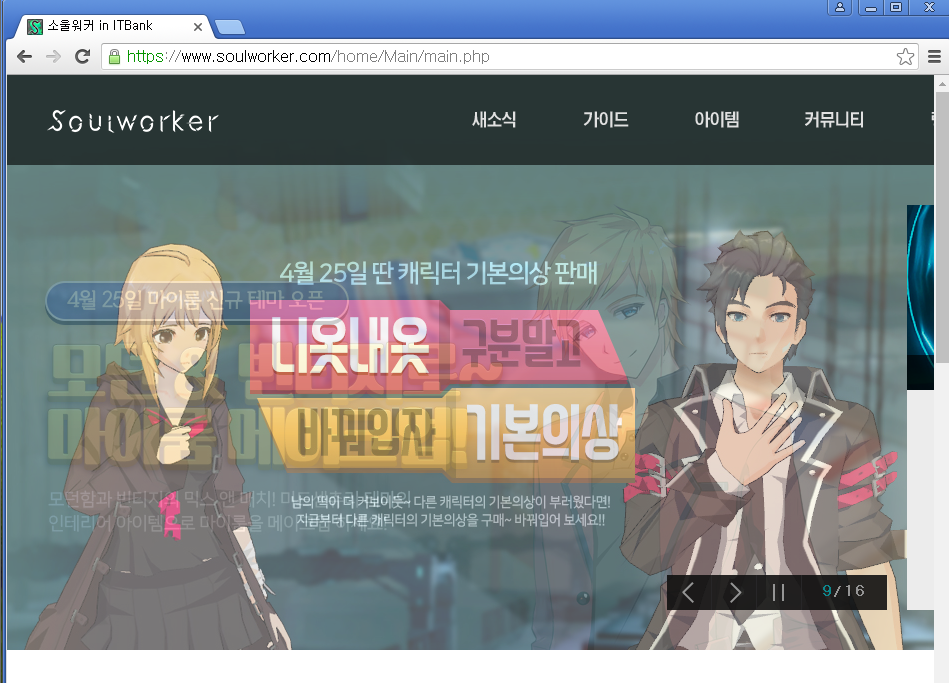
* 공격 확인을 위해 경영기획부 PC에서 DNS서버로 SSH 접속



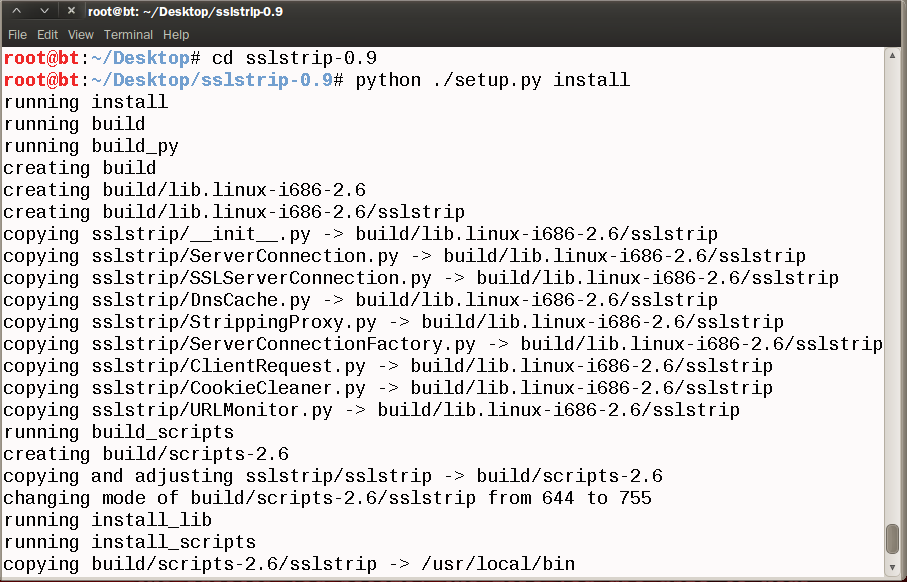
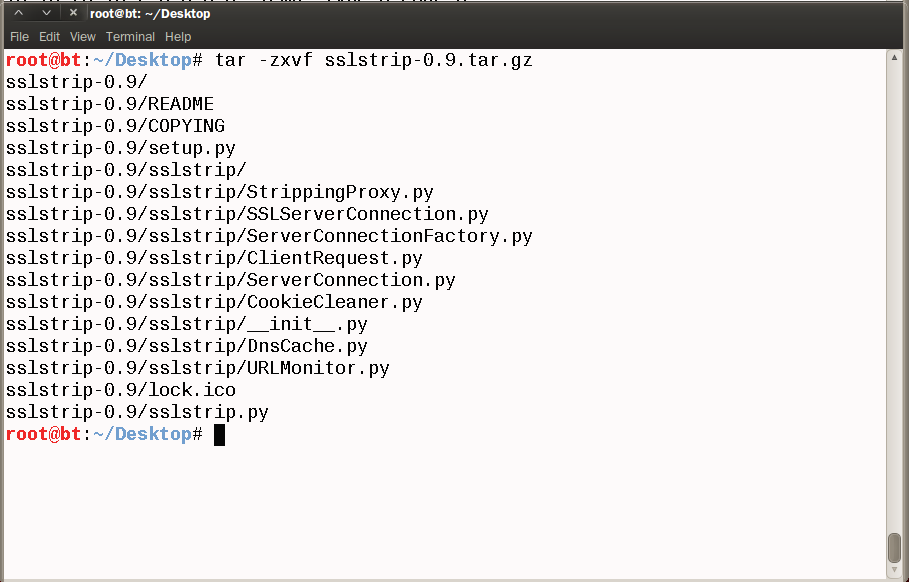
* BT에서 확인해보면 제대로 버전을 다운그레이드 했다는 것을 볼 수 있음



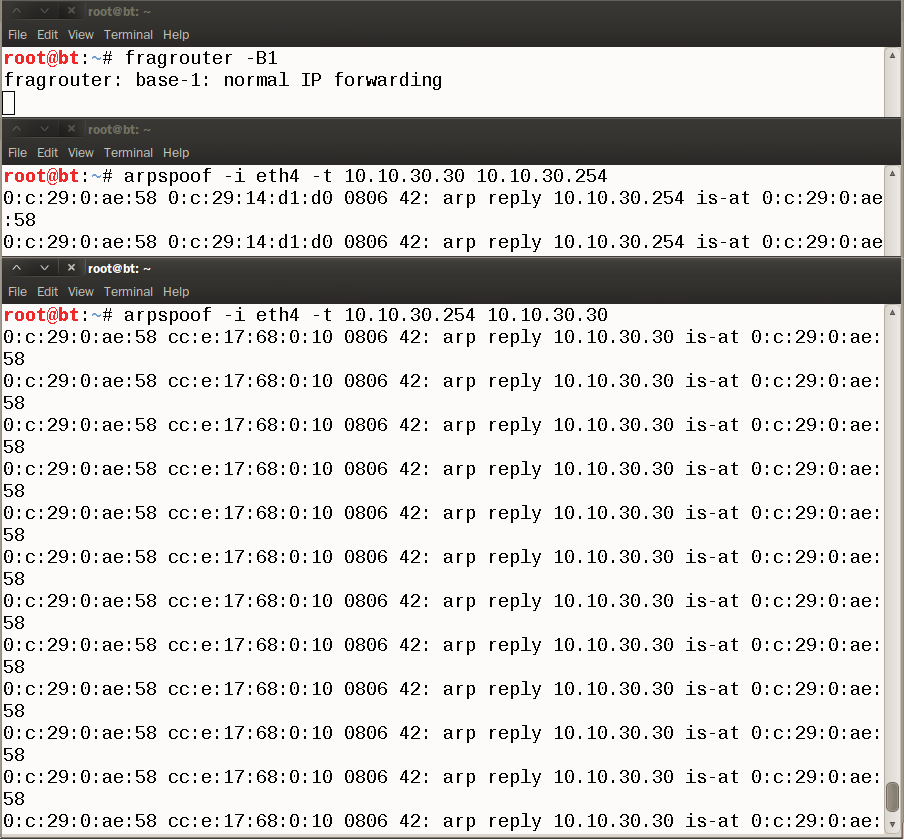
* 경영기획부 PC에서 DNS서버로 SSH 접속 시 사용했던 아이디와 비밀번호도 확인 가능
* SSL 취약점 공격 [SSL Strip Attack]



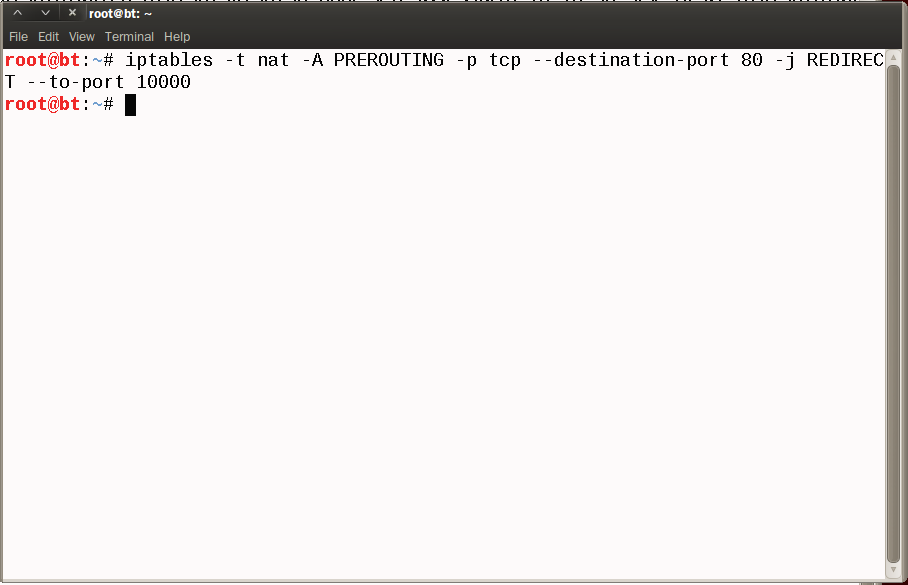
* 공격 시도에 앞서 TLS가 제대로 작동하는지 확인



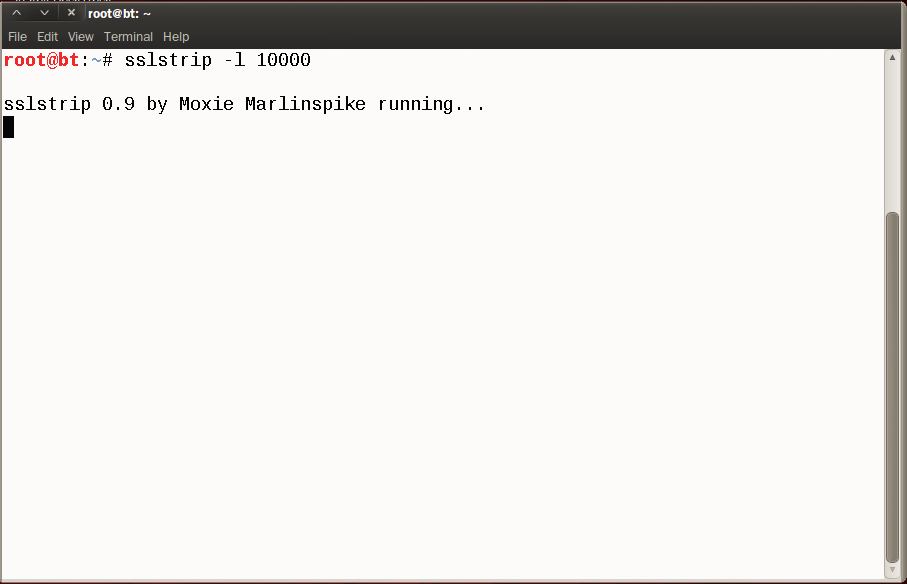
* Sslstrip 공격을 위한 sslstrip 툴 설치



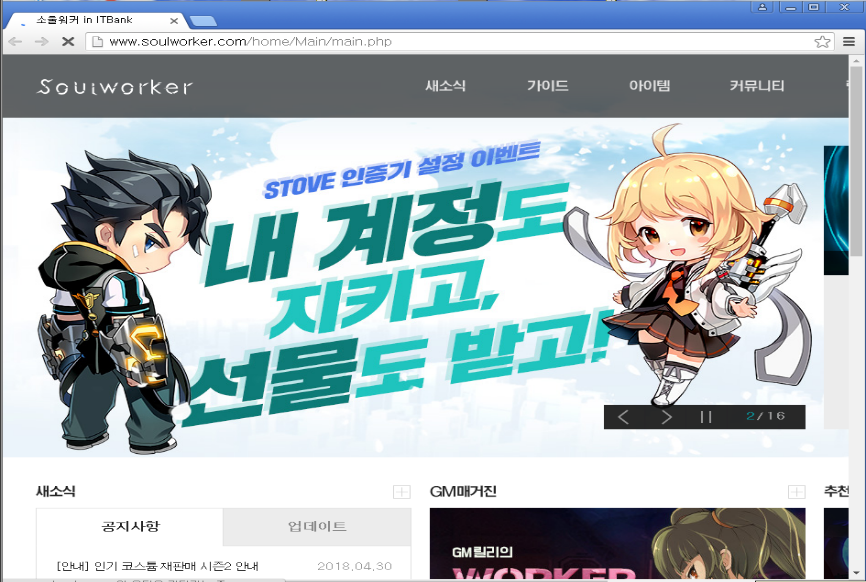
* 게이트웨이와 개발관리부 PC에 MITM 상태 만들기



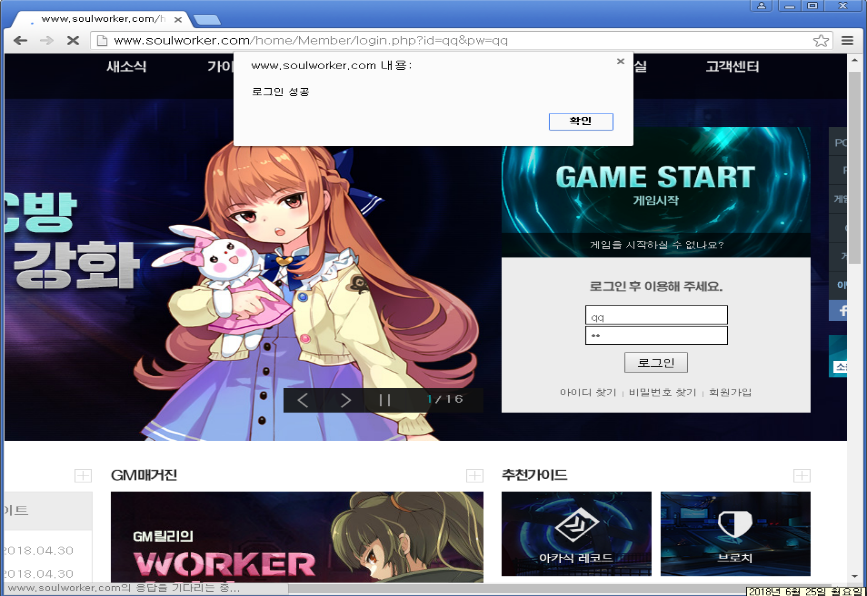
* 80번 포트로 접근을 시도하면 10000번 포트로 리다이렉트 시키겠다는 방화벽 설정



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



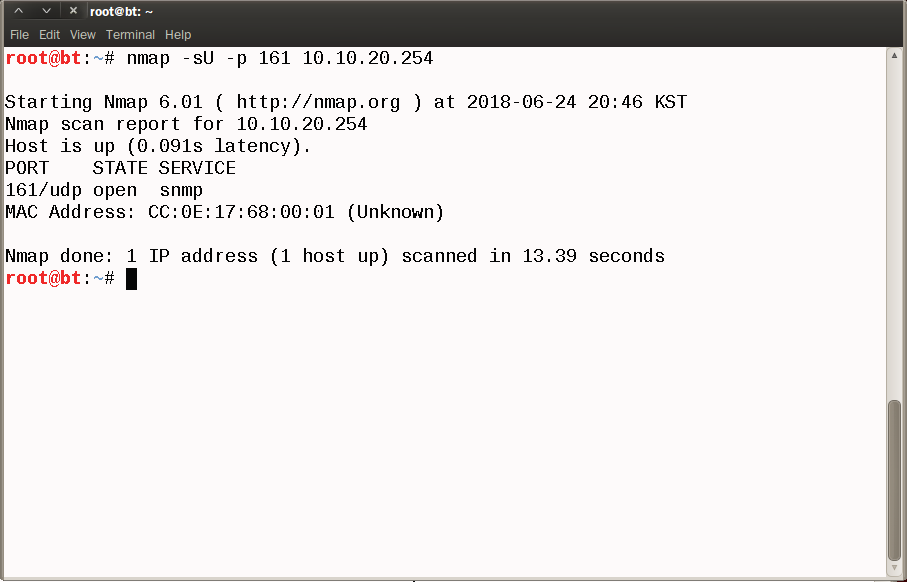
* 개발관리부 PC로 웹에 접근을 시도하면 https가 아닌 http로 접근하는 것을 볼 수 있음



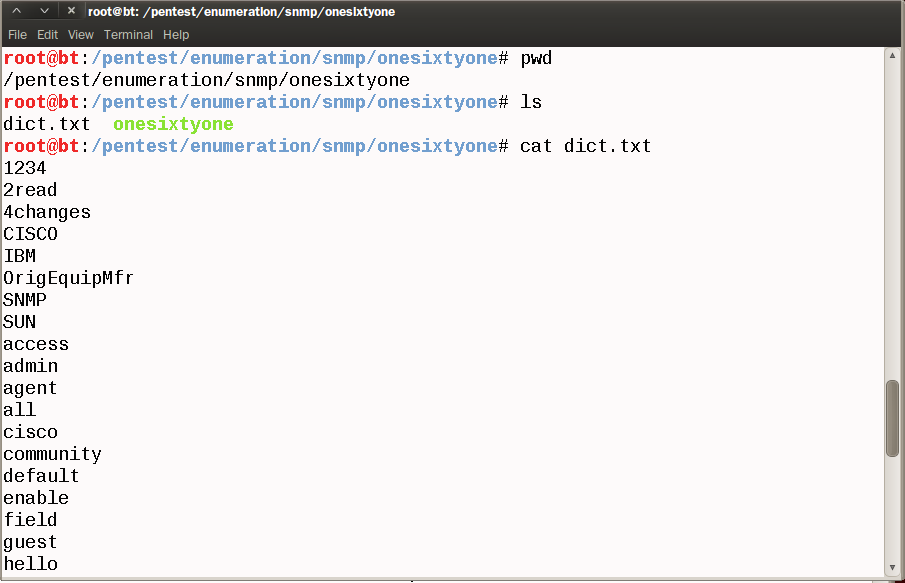
* 로그온 시도



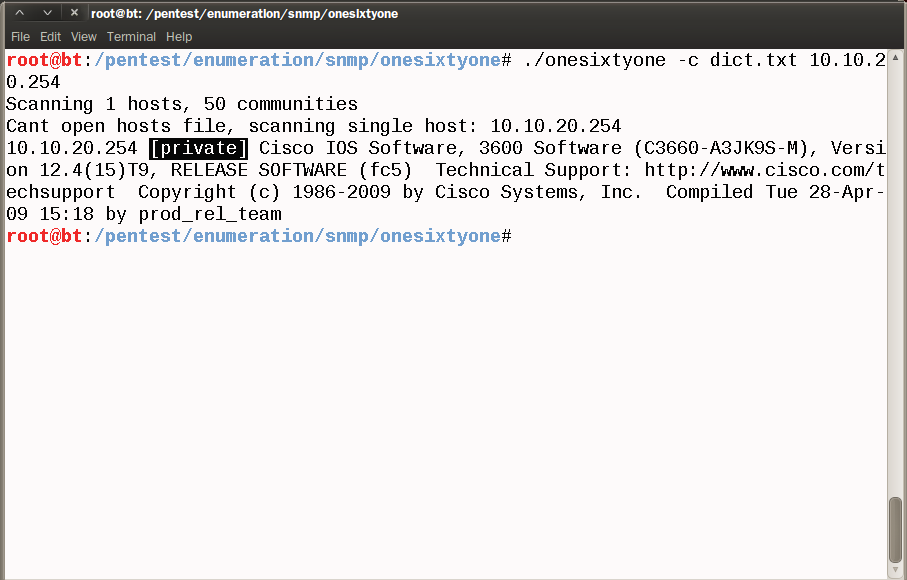
* 로그온 시도 후 BT으로 돌아와 와이어 샤크를 확인해보면 아이디와 비밀번호가 노출된 것을 볼 수 있음
* SNMP 취약점 공격



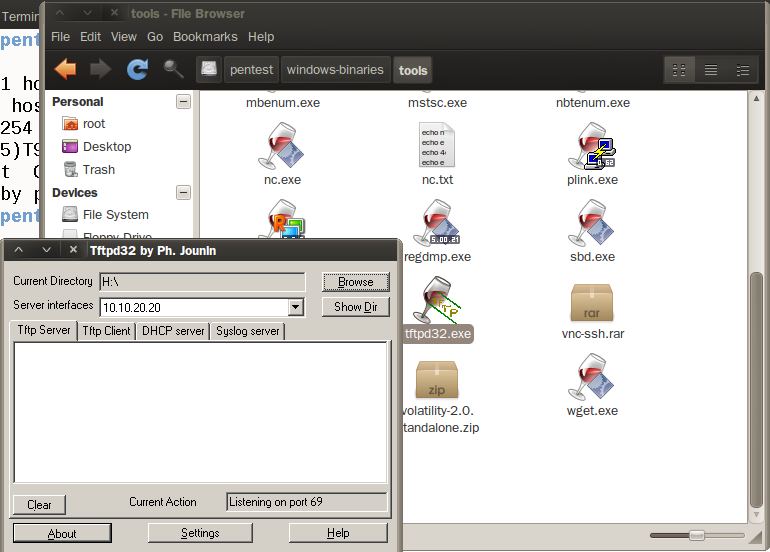
* 공격에 앞서 snmp서비스를 지원해주는지 nmap툴을 사용해 확인



* Community String을 알아오기 위해 사용할 dictionaty 파일인 dict.txt파일 확인

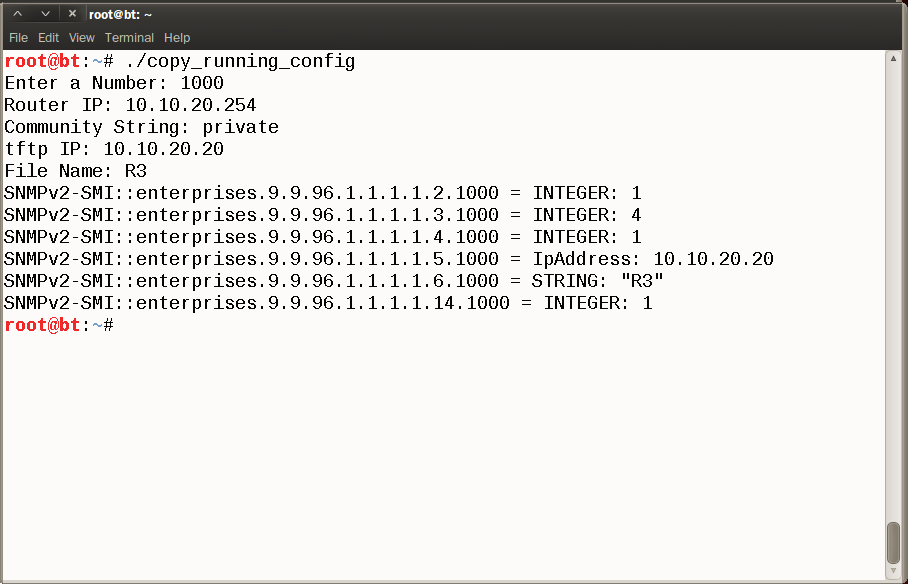


* Onesixtyone 툴과 dict.txt파일을 사용해 공격대상의 Community String 알아오기

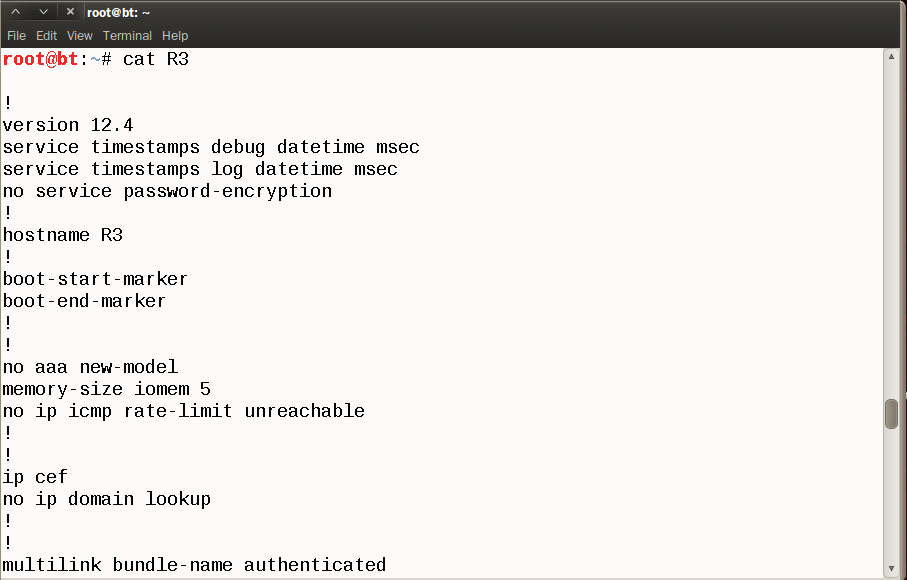




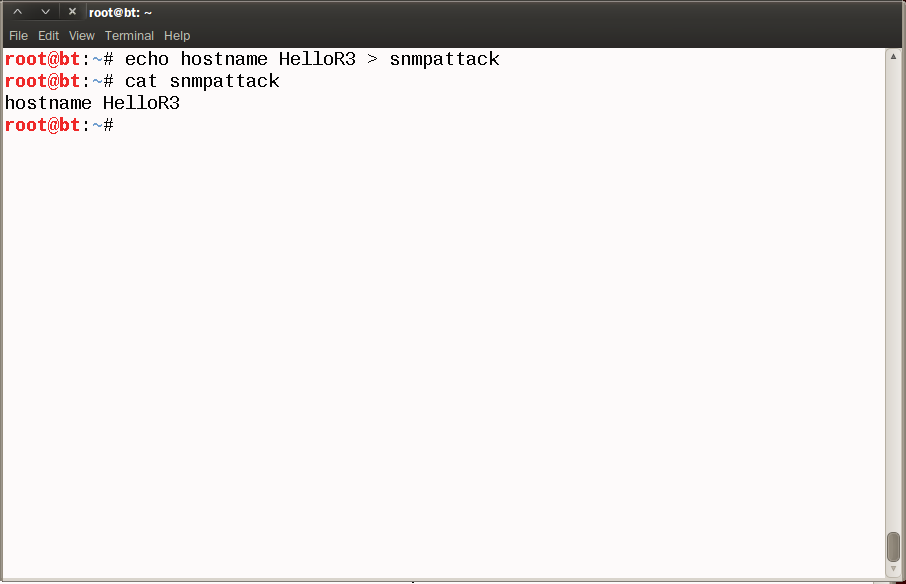
* 공격을 하기 위해 tftp을 실행하고 up\_running\_config, copy\_running\_config 파일 확인



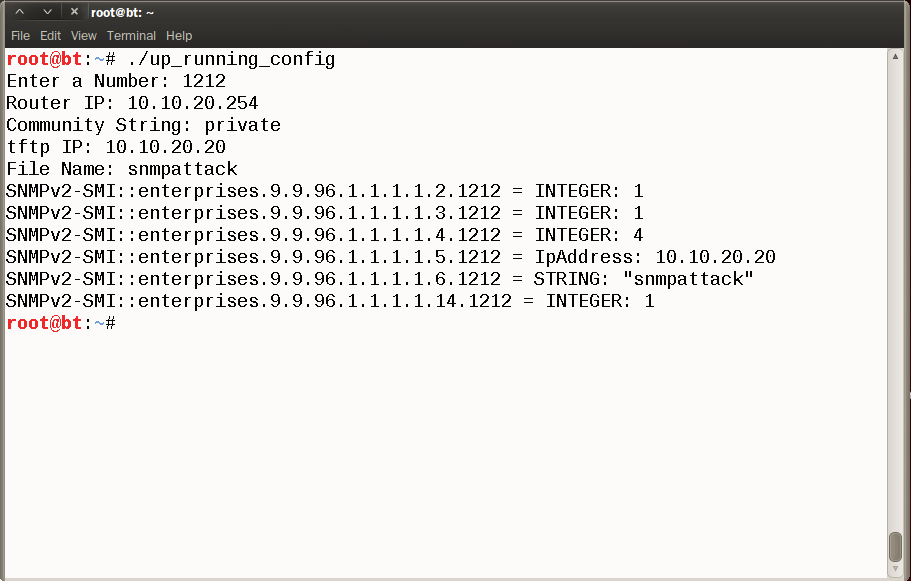
* Copy\_running\_config 파일과 tftp를 이용해 공격대상의 running\_config 상태를 파일로 받아보기



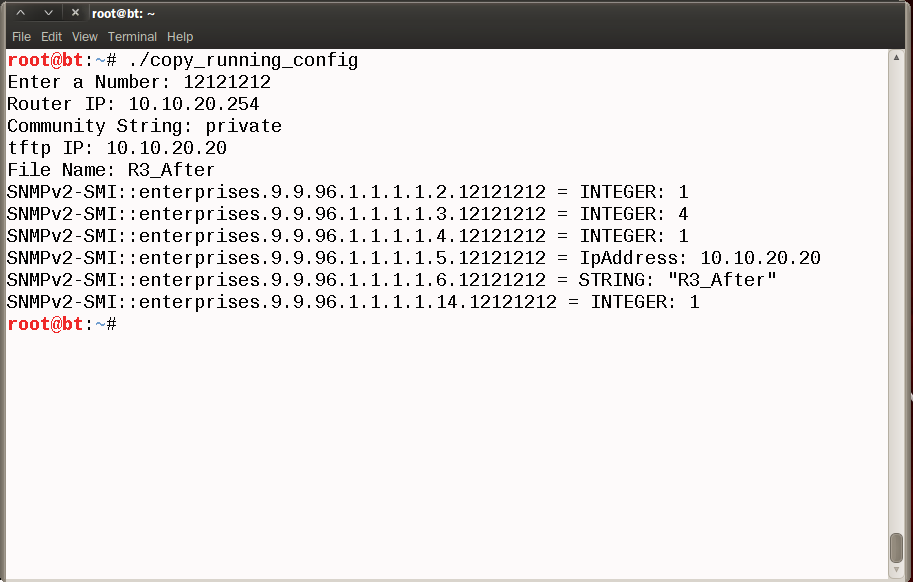
* 제대로 running\_config 상태를 받아왔는지 확인



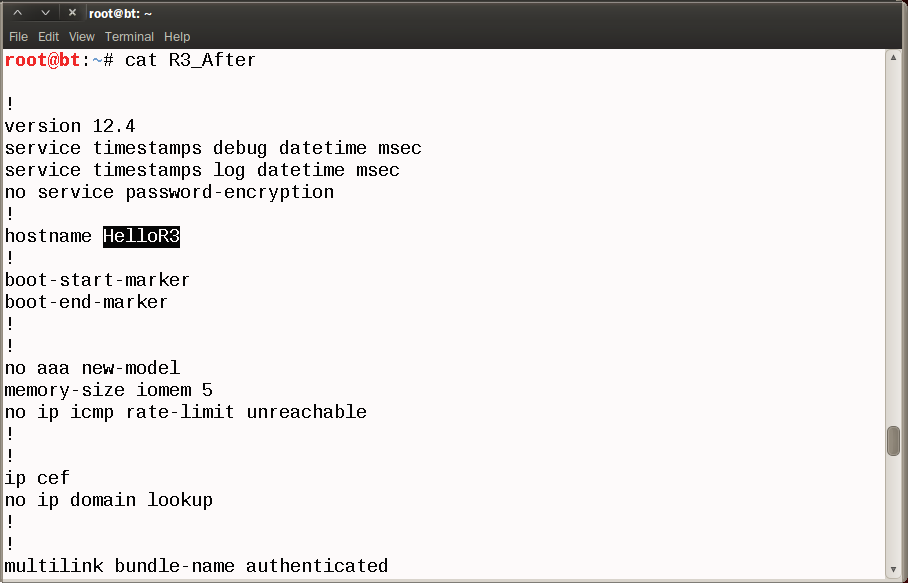
* 받아온 running\_config 상태 확인 후 바꾸고 싶은 내용을 파일로 만들기



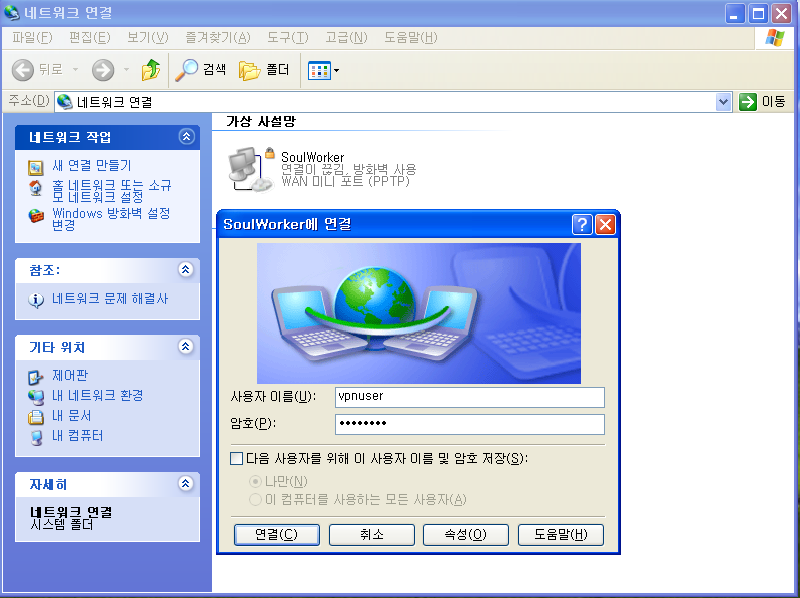
* Up\_running\_config 파일을 이용해 만든 공격파일을 공격대상에게 보내기

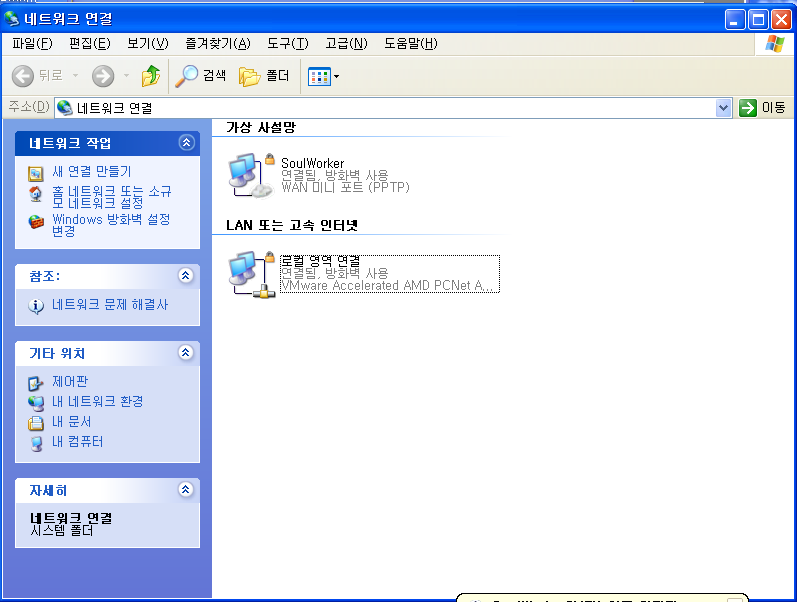


* 공격이 제대로 됐는지 확인하기 위해 다시 running\_config 상태를 파일로 받아보기



* 받아온 파일에서 내가 바꾼 내용이 제대로 적용 됐는지 확인
* VPN 취약점 [PPTP]



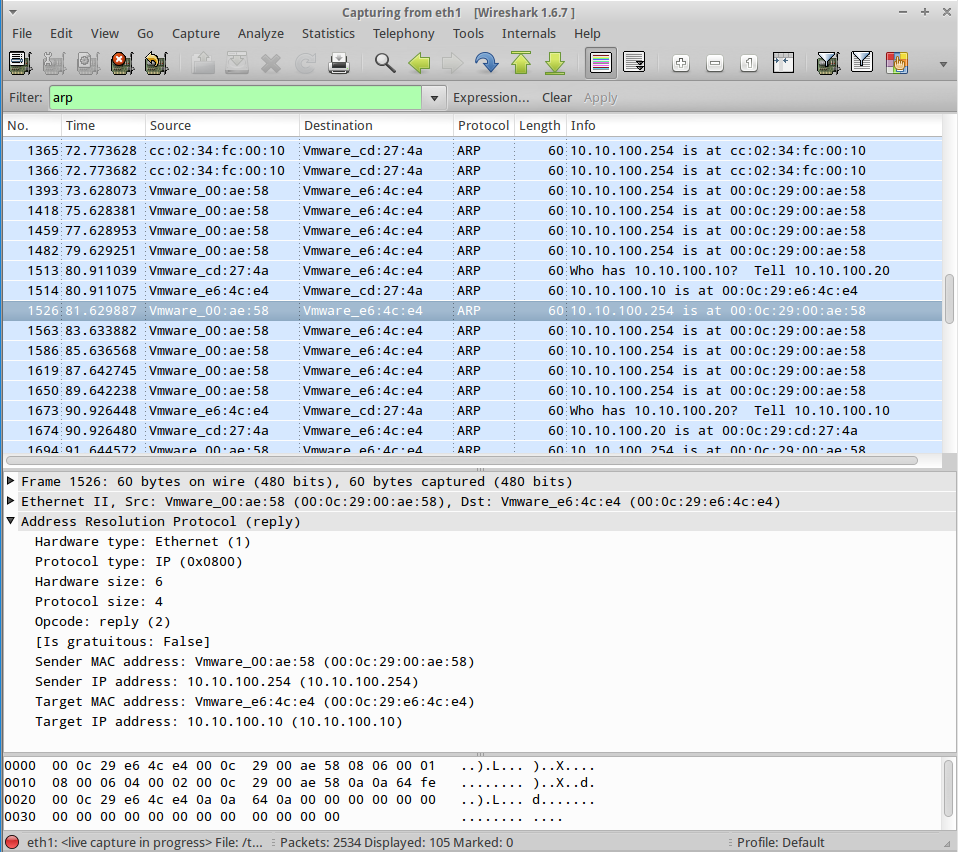
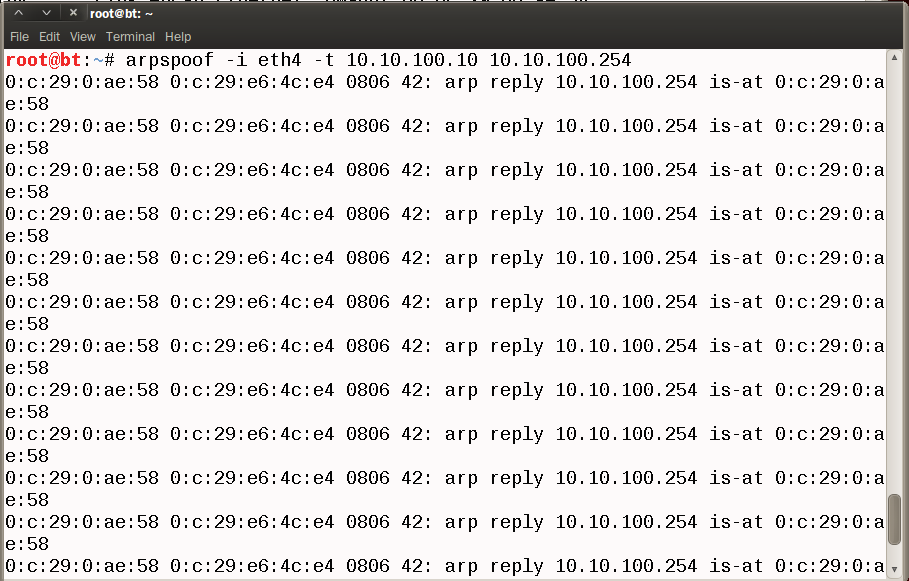


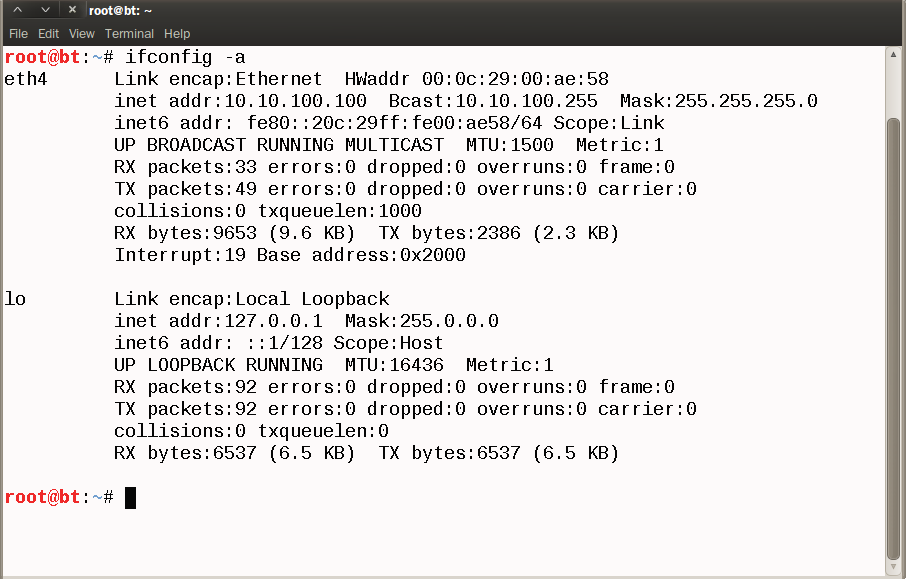
* 지사의 컴퓨터를 이용해 본사 VPN 서버에 접속



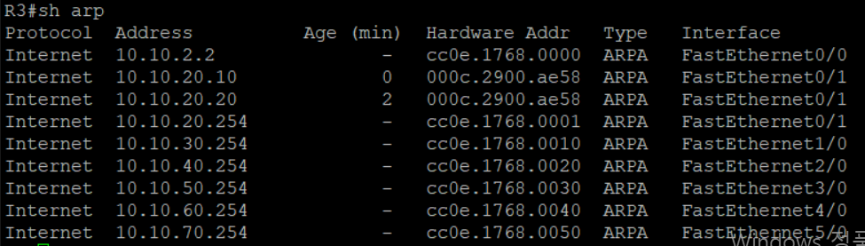
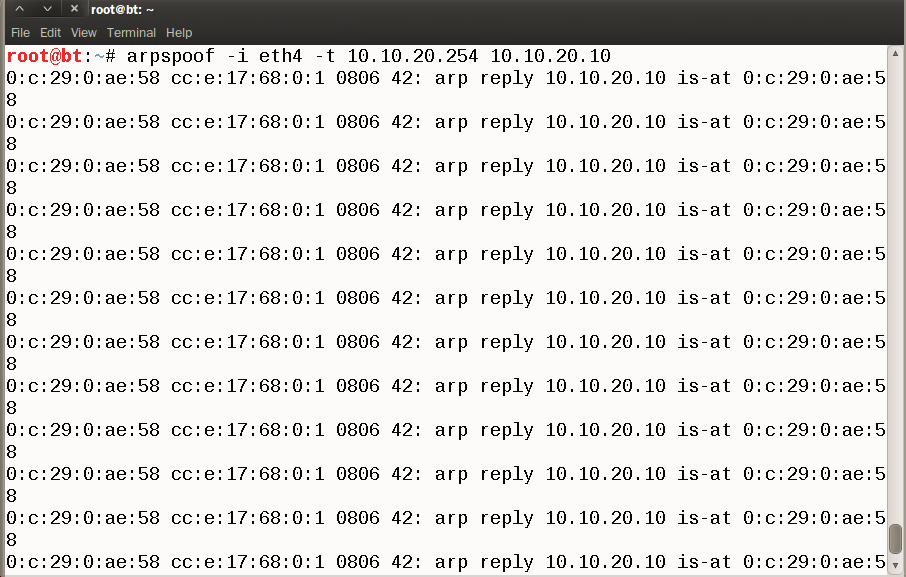
* 와이어 샤크로 확인해보면 아이디와 컴퓨터 이름을 볼 수 있음
* 대응책

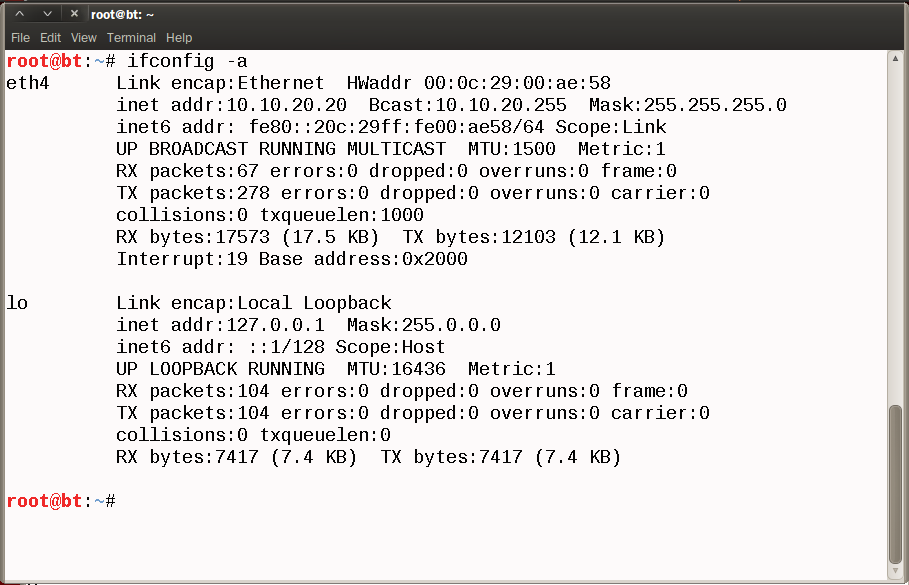
1. ARP Spoofing





* 탐지 방법으로는 IDS를 이용해 탐지 가능, 서버들과 같은 네트워크에서 ARP Spoofing 공격을 시도 했을 시 IDS에 들어오는 Packet들을 확인해보면 ARP Spoofing 공격을 확인할 수 있음

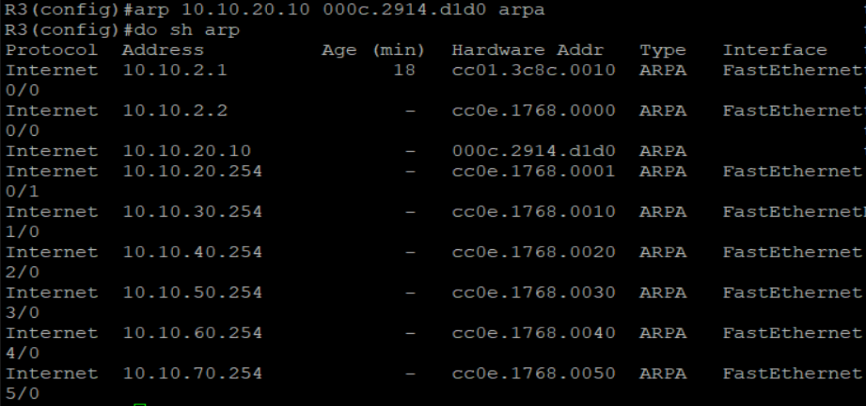
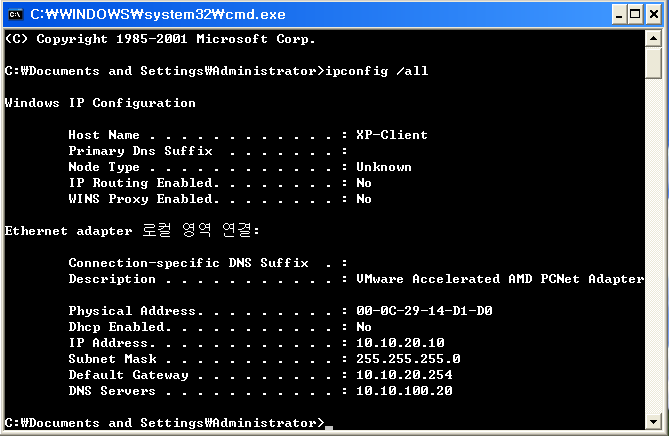




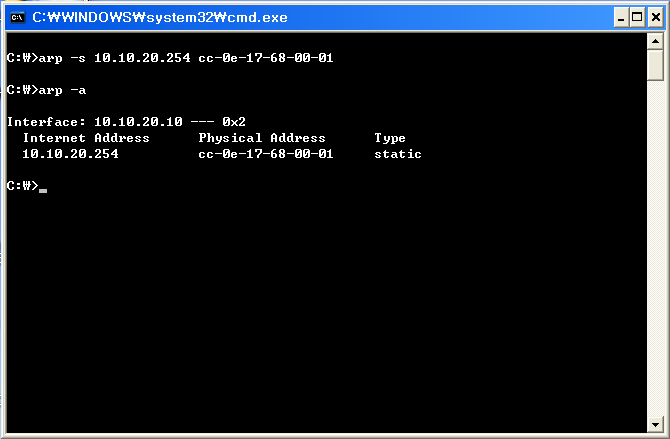
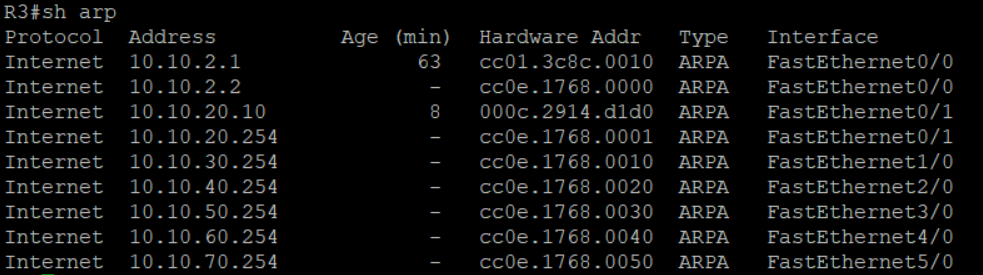
* IDS가 없는 네트워크라면 공격이 의심될 때 Router에서 ARP Table을 확인, 이 때 동일한 MAC주소를 가지고 있는 Host가 있다면 공격 의심 가능



* DAI [Dynamic ARP Inspection]을 사용해서 만들어진 DB와 비교해 매칭되는 아이피일 경우에만 Switch를 통과시키도록 하게 만들면 ARP Spoofing을 어느정도 방지할 수 있음

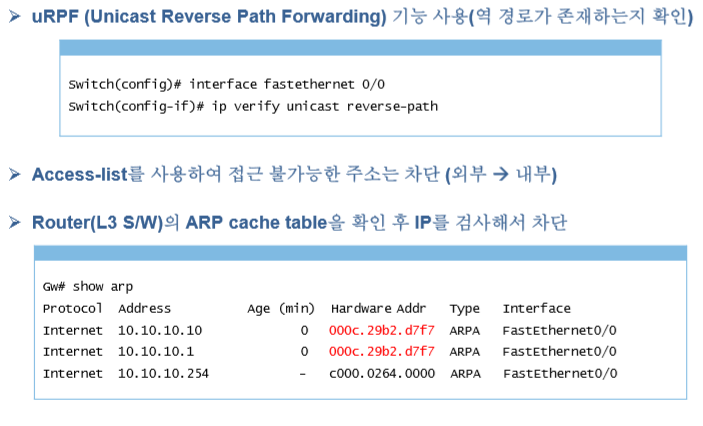


* Router에 Static으로 Routing Table을 등록하게 되면 ARP Spoofing을 방지 할 수 있음



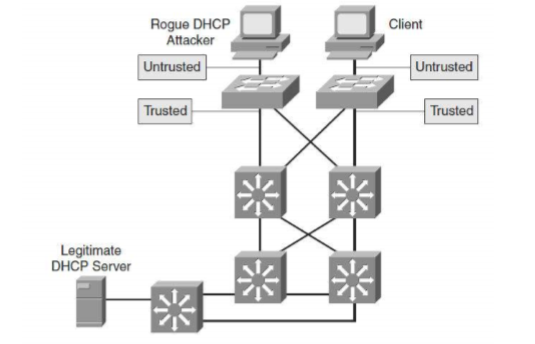
* 또는 Gateway의 MAC 주소를 확인하고 Client PC에 Static으로 ARP Table에 등록

1. IP Spoofing



* 공격이 의심된다면 먼저 ARP Spoofing 공격 탐지 방법을 이용해 탐지, 방어 방법으로는 ARP Spoofing공격에 대한 방어 방법을 사용하고 추가로 uRPF [Unicast Reverse Path Forwarding] 기능을 사용, uRPF [Unicast Reverse Path Forwarding] 기능은 출발지 주소를 확인했을 때 네트워크 내의 주소이지 않은 주소가 밖으로 나가는 것을 차단시켜 주는 기능을 하고 ARP Spoofing의 대응책을 설정해놓으면 어느 정도 차단 가능

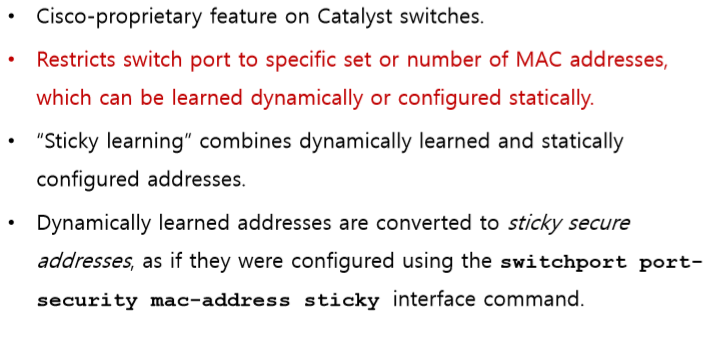
1. DHCP Spoofing



* DHCP Spoofing을 방어하는 방법으로는 DHCP Snooping을 사용하는 편이 좋음, Sniffing과 같이 Packet을 엿보지만 관리의 목적으로 사용

DHCP Snooping 설정은 관리자가 스위치상에 DHCP와 연결된 포트를 Untrusted포트로 설정을 해주고 반대되는 포트에 Trusted 포트로 설정

1. DHCP Starvation

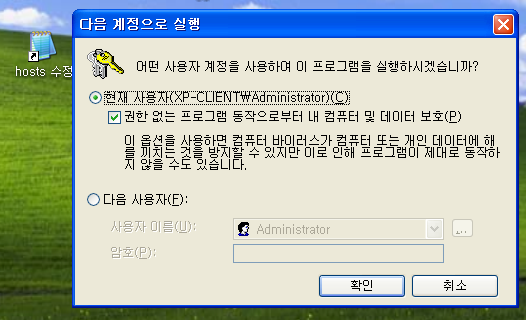
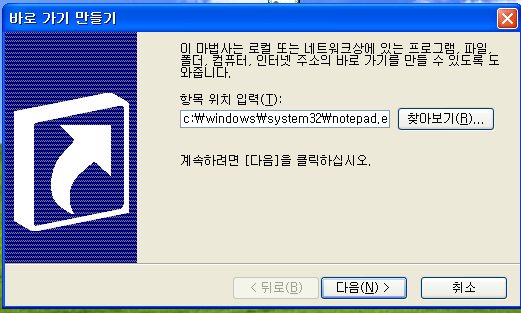
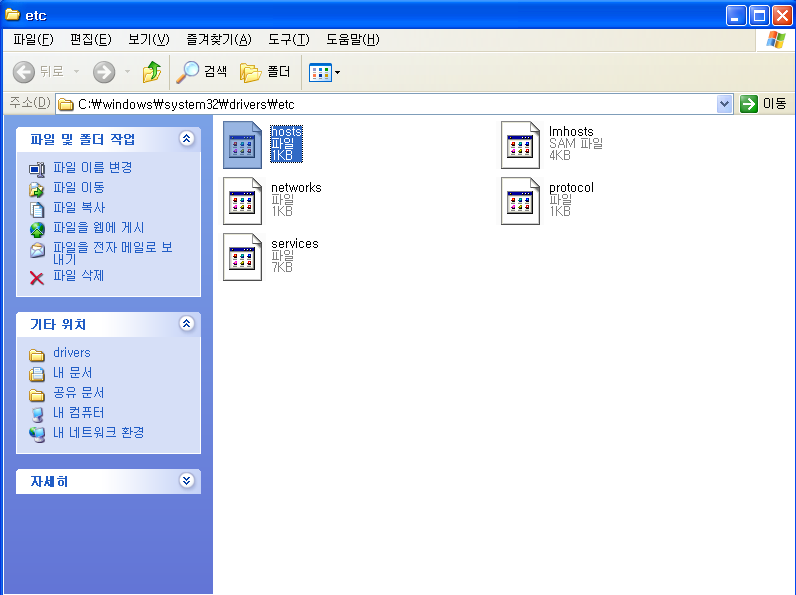


* DHCP Starvation은 Port Security를 사용해 어느 정도 방어가 가능

Port Security 설정은 먼저 switch port-security maximum [저장 갯수]를 사용해 학습 가능한 최대 MAC 주소를 설정해주고 switch port-security 명령을 사용해 활성화

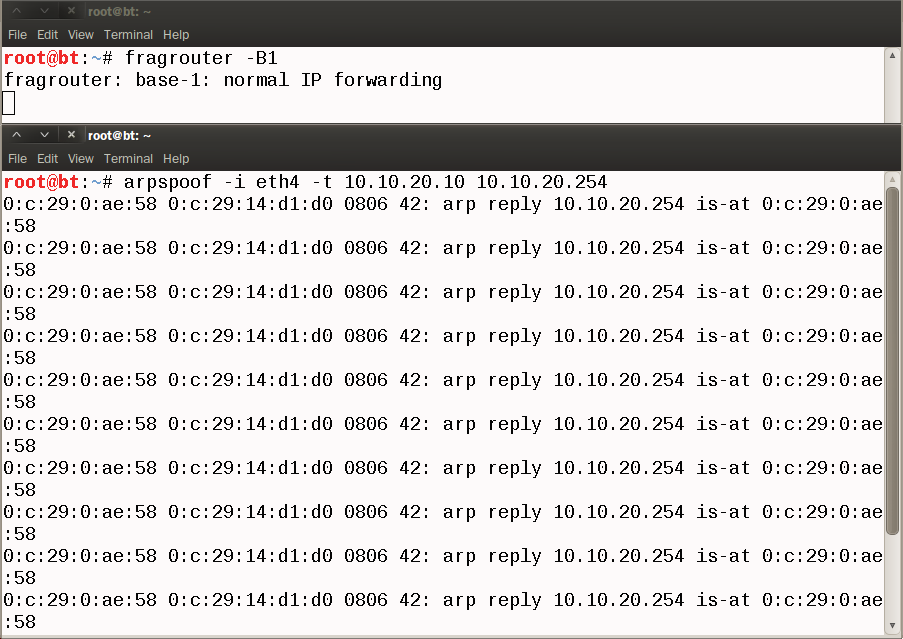
Switchport port-security mac-address sticky 명령어를 사용해 MAC 주소를 동적으로 학습되도록하고 학습한 주소를 저장할 수 있도록 설정

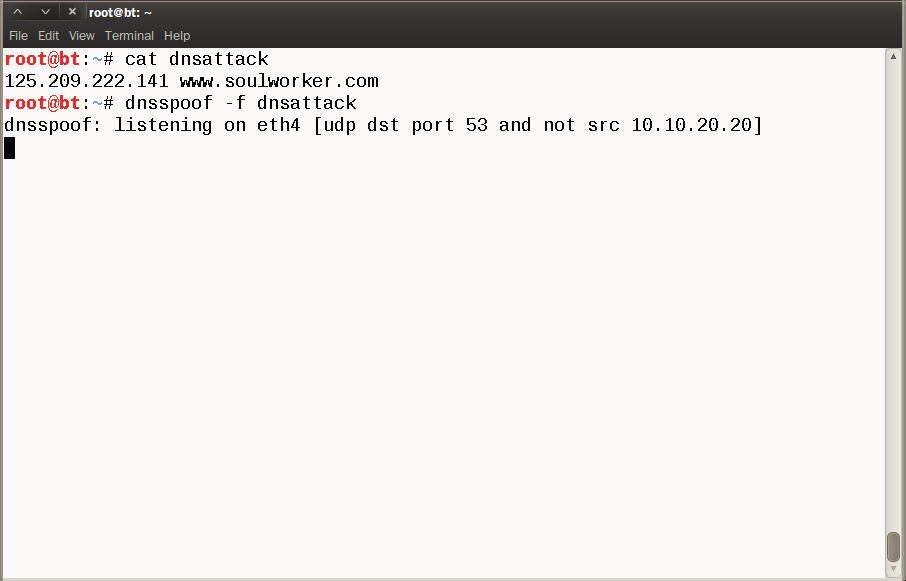
1. DNS Spoofing



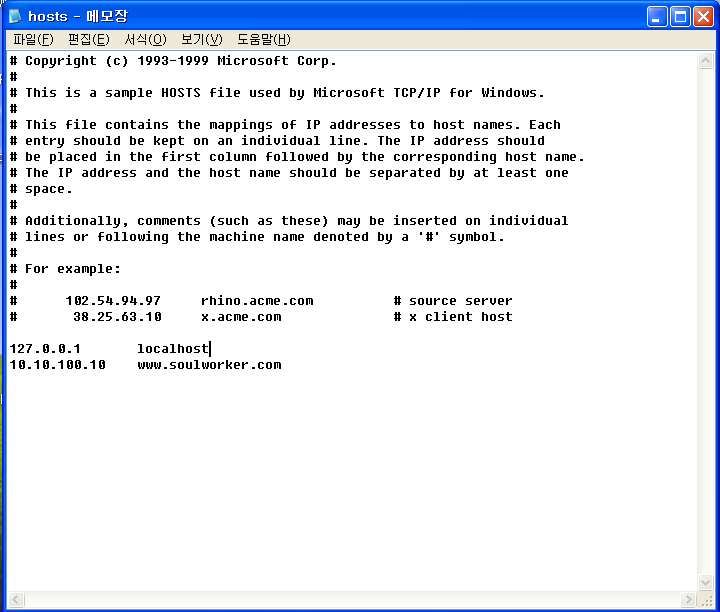
* Window의 경우 c:\windows\system32\drivers\etc 경로에 hosts파일이 있음, hosts파일은 관리자권한으로 수정해야 하는데 그를 위해 바로가기 생성

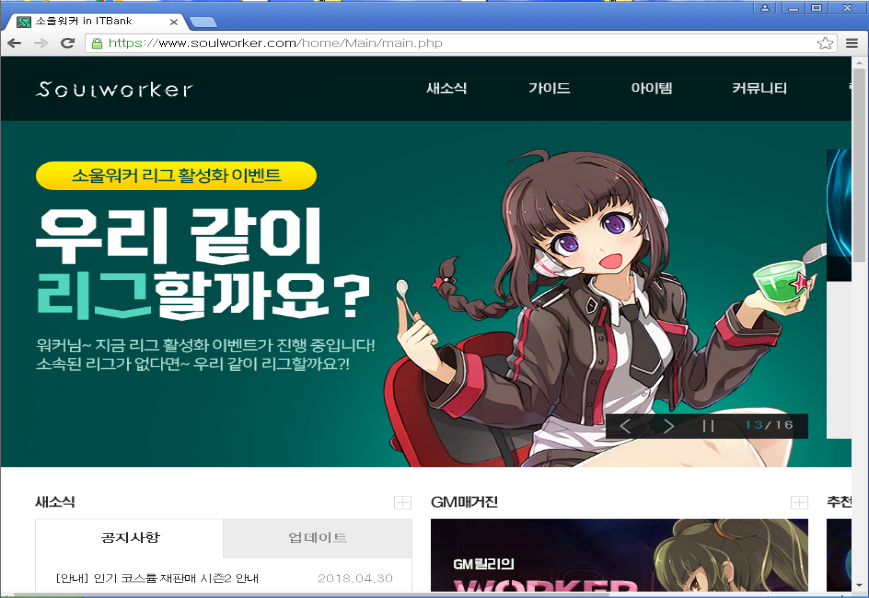
바로가기 생성 시 c:\windows\system32\notepad.exe c:\windows\system32\drivers\etc\hosts 라고 쳐주면 Notepad를 이용해 Hosts파일을 열어줌





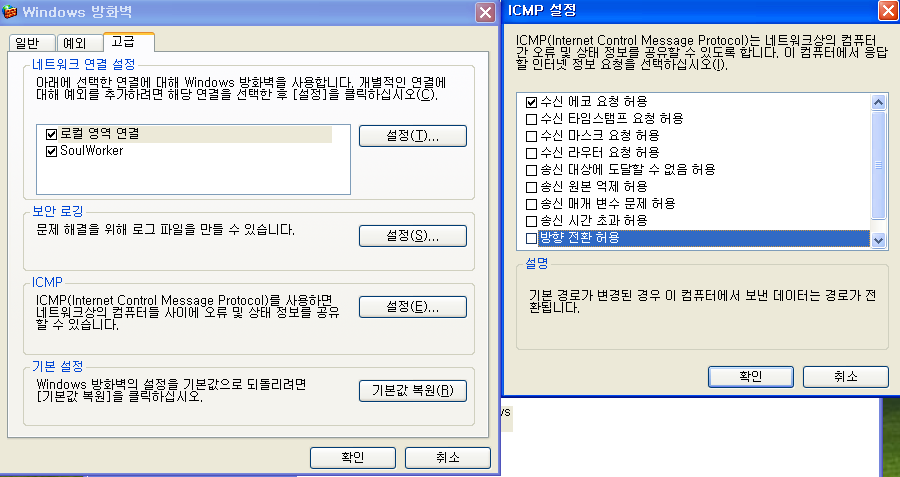
* Soulworker 페이지를 특정 페이지로 유도



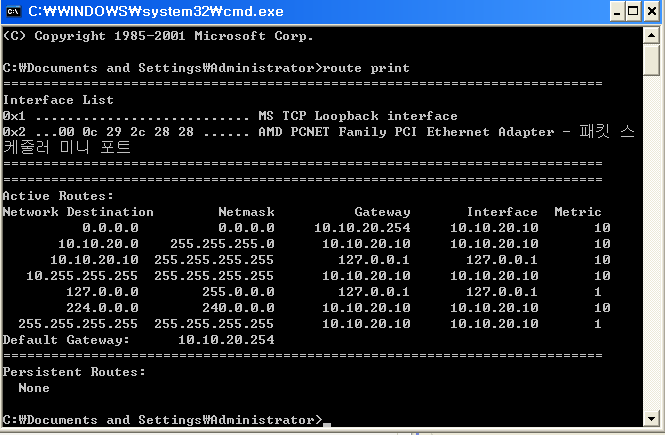


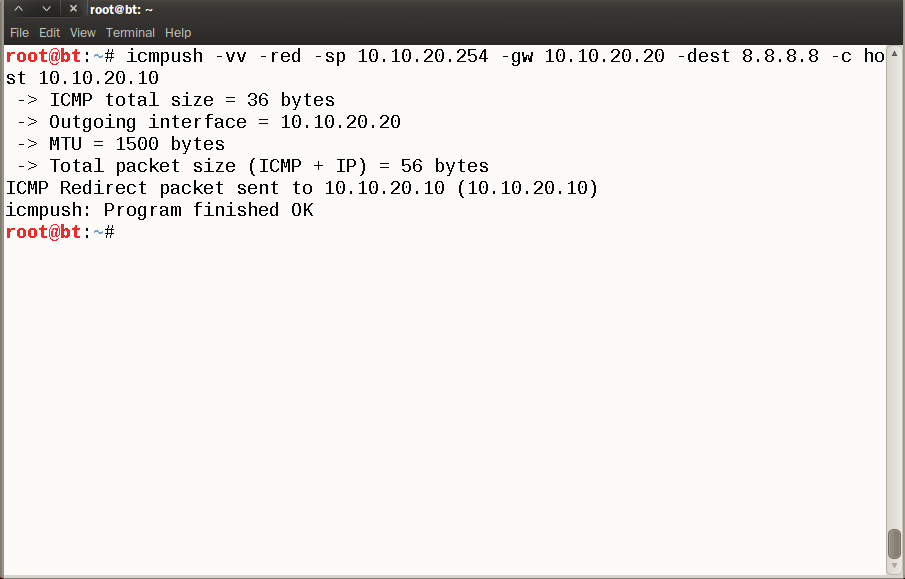
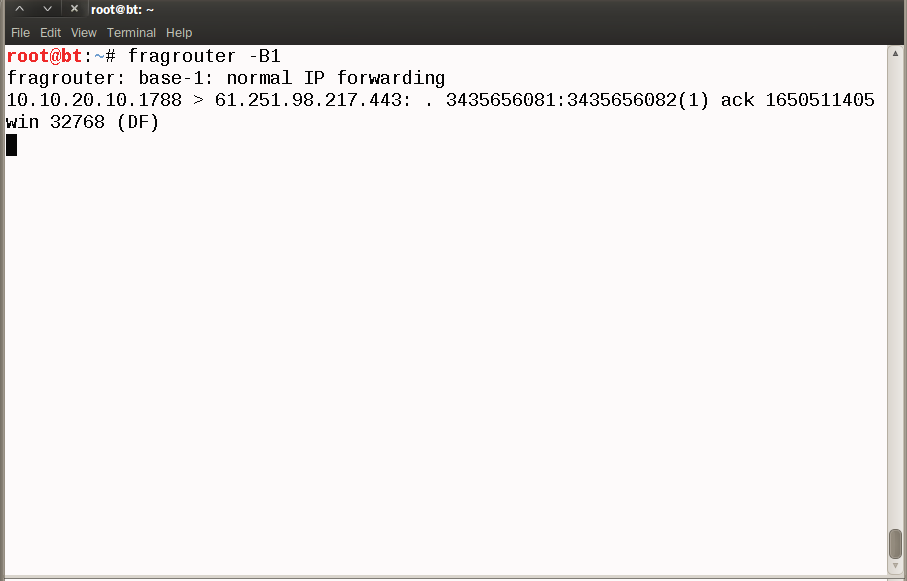
* Notepad를 이용해 Hosts를 열어 [아이피] [도메인]으로 도메인에 대한 아이피 주소를 고정 후 공격대상 PC에서 공격 당한 페이지를 열어보면 공격 실패
* ARP Spoofing 공격에 대한 방어 방법을 사용한다면 공격 방어 가능

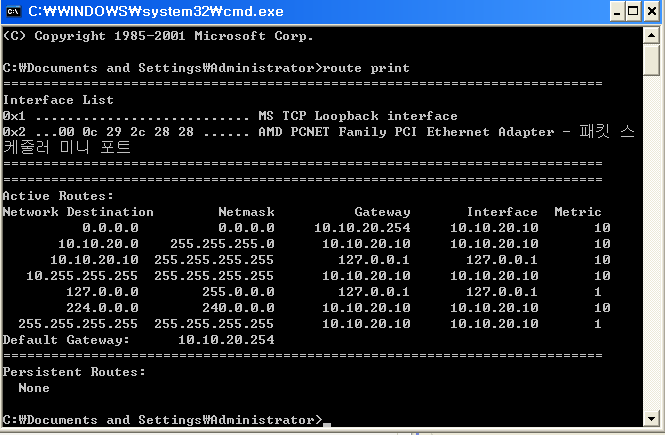
1. ICMP Redirect



* Window의 경우 방화벽에서 ICMP 설정을 눌러 방향전환요청을 체크 해제

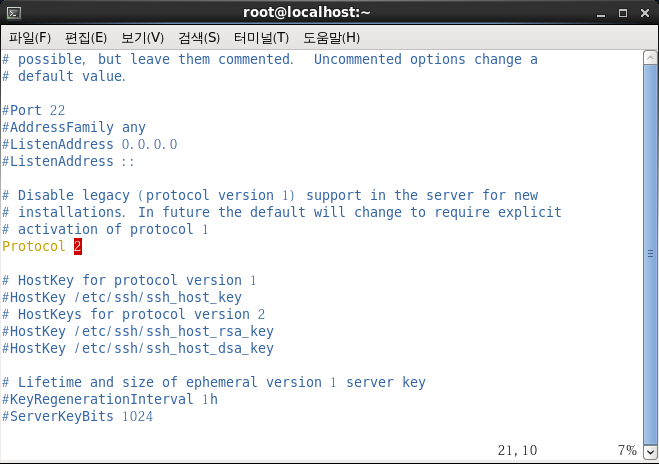




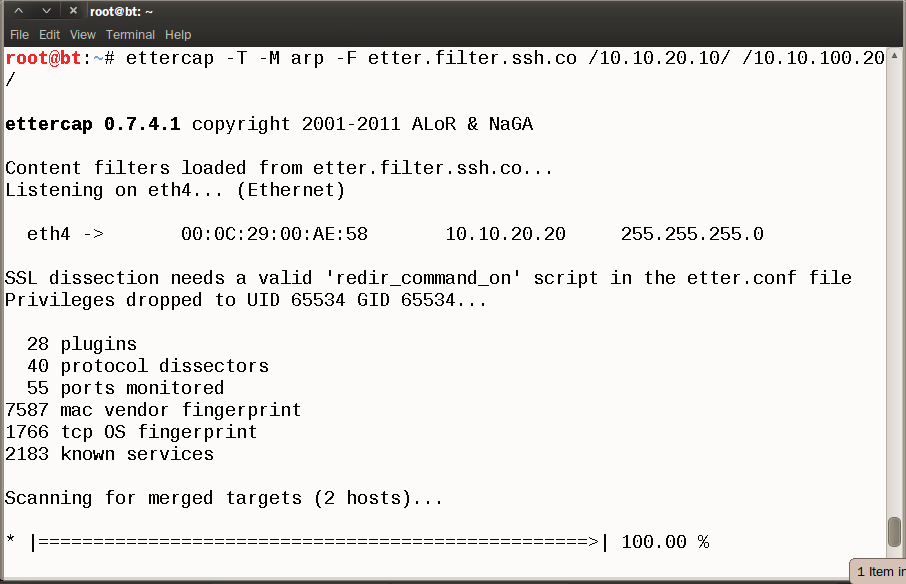


* Window의 경우 대응책 설정 후 다시 공격을 시도했을 때 공격이 되지 않는 것을 볼 수 있음

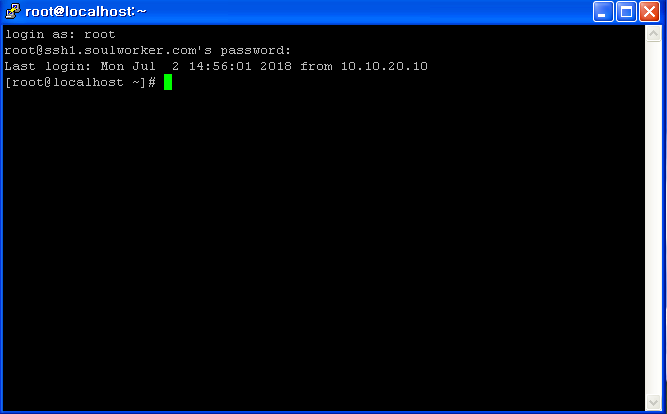
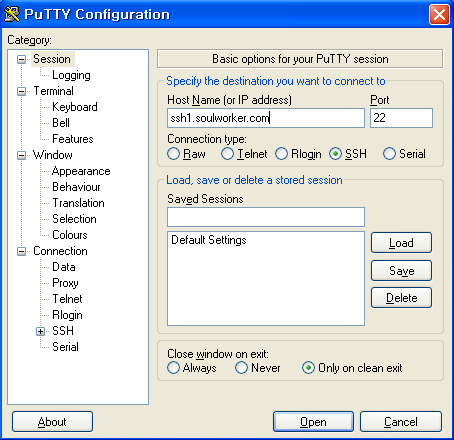
1. SSH 취약점 공격



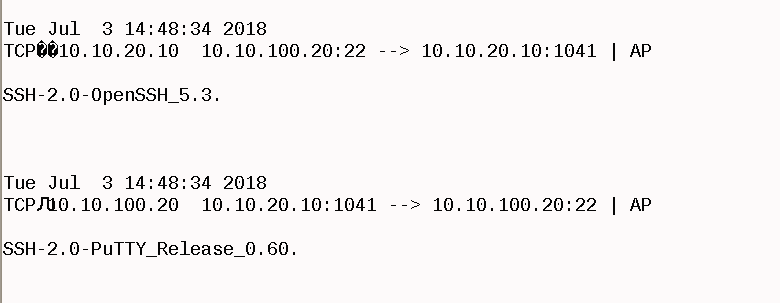
* SSH 취약점 공격에 대응하기 위해서는 Linux서버의 /etc/ssh/sshd\_config 파일을 열어 Protocol을 2로 수정, 수정 후에는 서비스 재 시작



* BT으로 돌아가 SSH 취약점 공격 시도



* 공격 대상 PC로 가서 DNS서버에 SSH로 접근 시도



* BT으로 돌아가서 확인해보면 버전이 2라서 읽어오지 못하는 것을 볼 수 있음



* Client PC에서 확인했을 때 Downgrade가 되지 않은 모습 확인 가능

1. SSL 취약점 공격

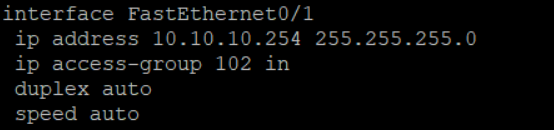
* MITM 상태가 되지 않도록 ARP Spoofing에 대한 방어 방법을 적용

1. SNMP 취약점 공격



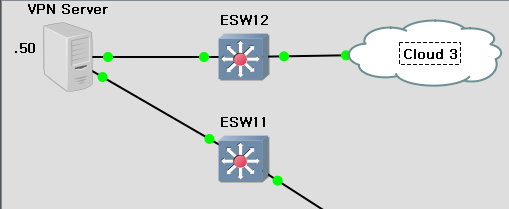
* Community String을 Dictionary Attack으로 쉽게 알아채지 못하도록 숫자와 문자, 기호를 포함하여 복잡하게 설정



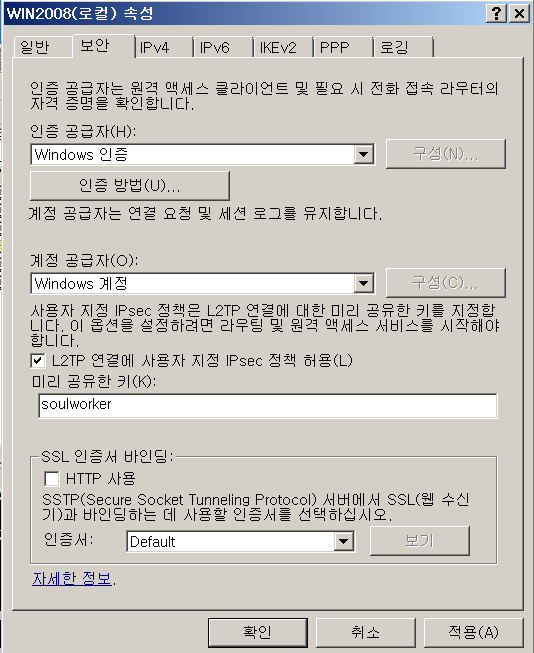


* 서버 관리부의 네트워크만 허용을 해주고 다른 네트워크에서 SNMP로 접근하게 되면 거부

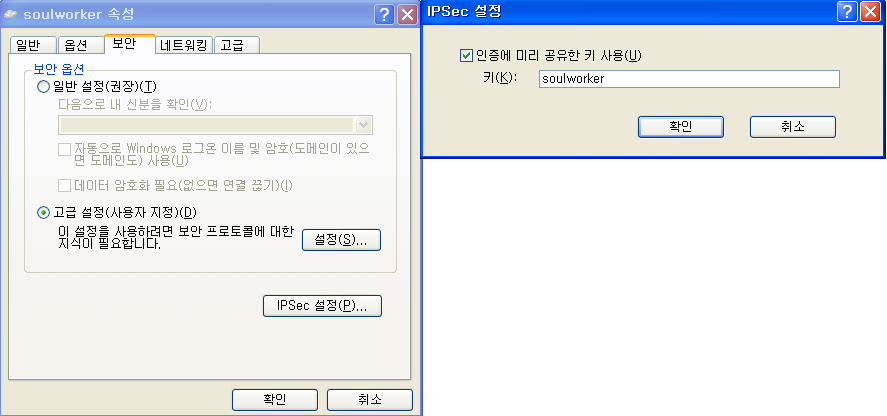
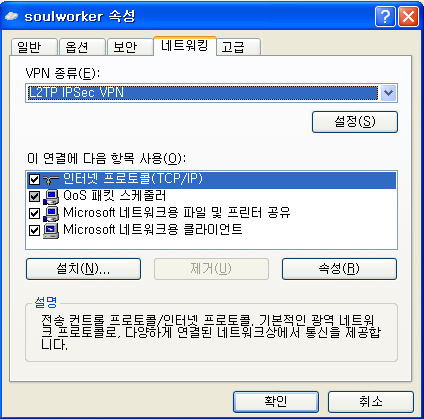
1. VPN 취약점



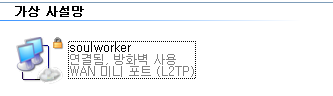
* 먼저 서버와 같은 네트워크에 구성되어 있던 VPN 서버를 별개의 네트워크로 구성



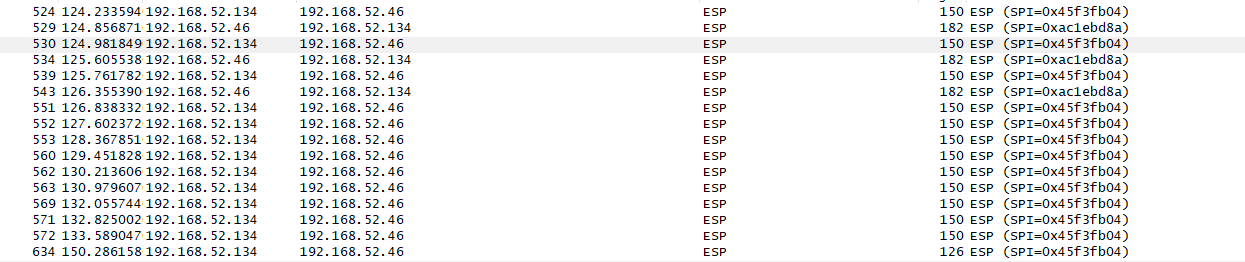
* L2TP 연결을 위해 VPN 서버 설정에서 L2TP 연결에 사용자 지정 IPsec 정책 허용 체크 후 미리 공유한 키 설정



* Client [지사] PC로 와서 사용하고 있던 가상 사설망 속성으로 들어가 VPN 종류를 L2TP로 설정 후 IPsec 설정에 미리 공유한 키 입력



* 설정 적용 후 VPN 연결 시도를 해보면 연결이 되는 것 확인 가능



* 연결 과정을 Wire Shark로 확인해보면 ESP로 암호화 통신 하는 것을 확인