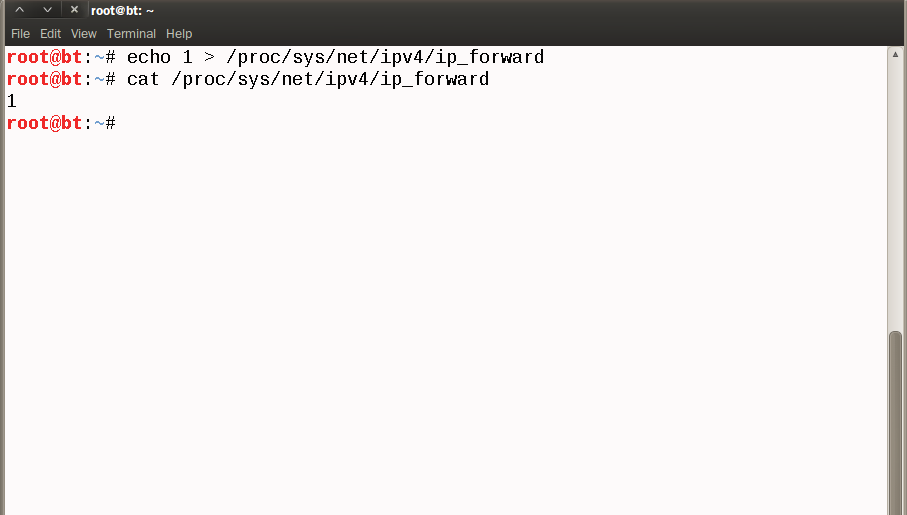
네트워크 보안

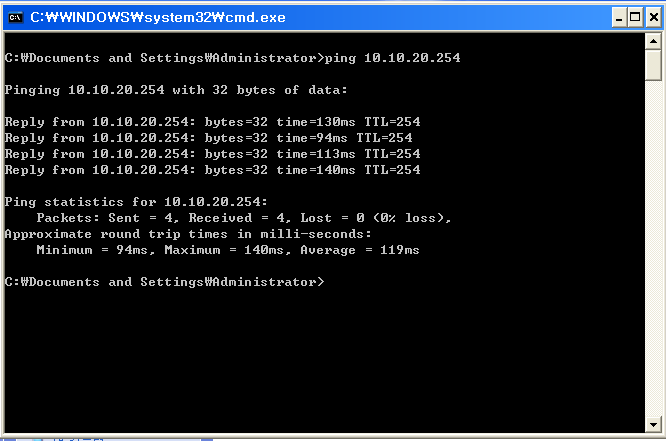
* ARP Spoofing



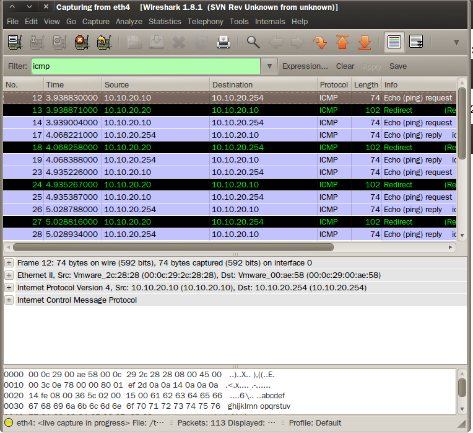
* 공격자가 경영기획부 네트워크에 침입해 BT으로 게이트웨이에 자신이 경영관리부 직원 PC[10.10.20.10]이라 속이고 경영관리부 직원 PC에 자신이 게이트웨이라 속임



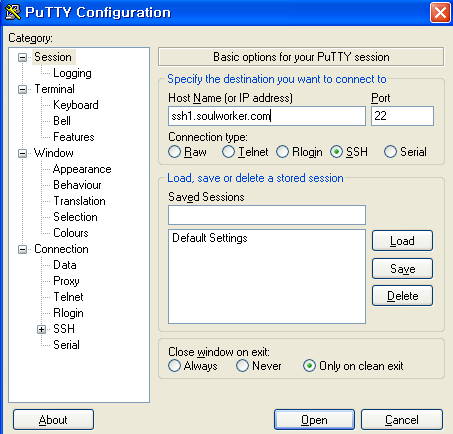
* 공격대상 PC와 게이트웨이가 통신하는 것을 Sniffing하기 위해 포워딩 시작

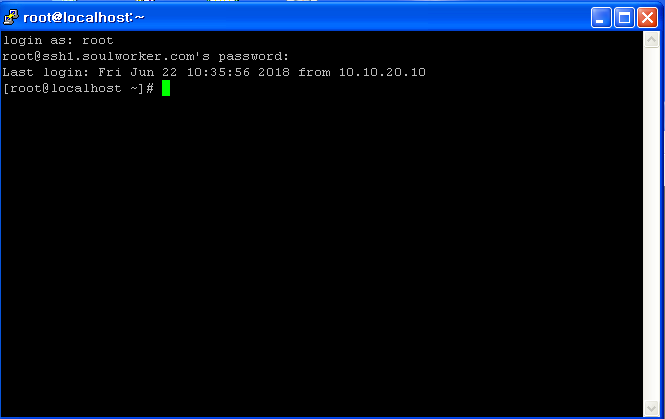


* 예시로 공격대상 PC가 게이트웨이에 Ping Test

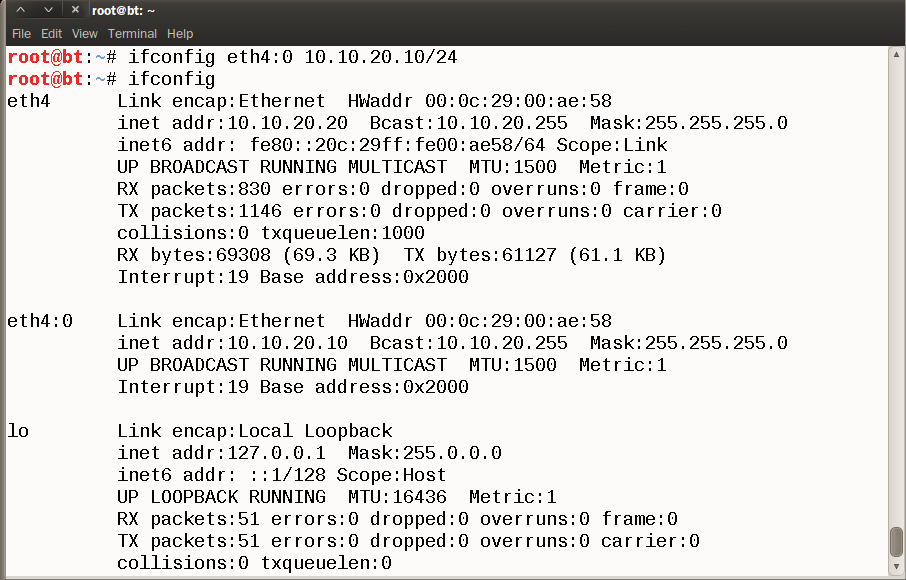


* BT 와이어샤크로 공격대상 PC와 게이트웨이가 Ping Test하는 것을 리다이렉트하면서 Sniffing하는 것을 확인
* IP Spoofing

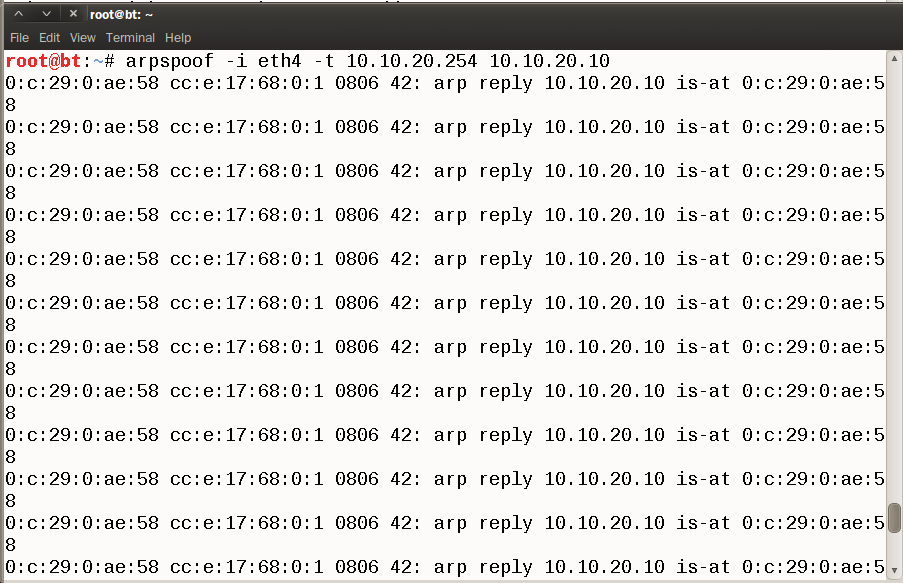




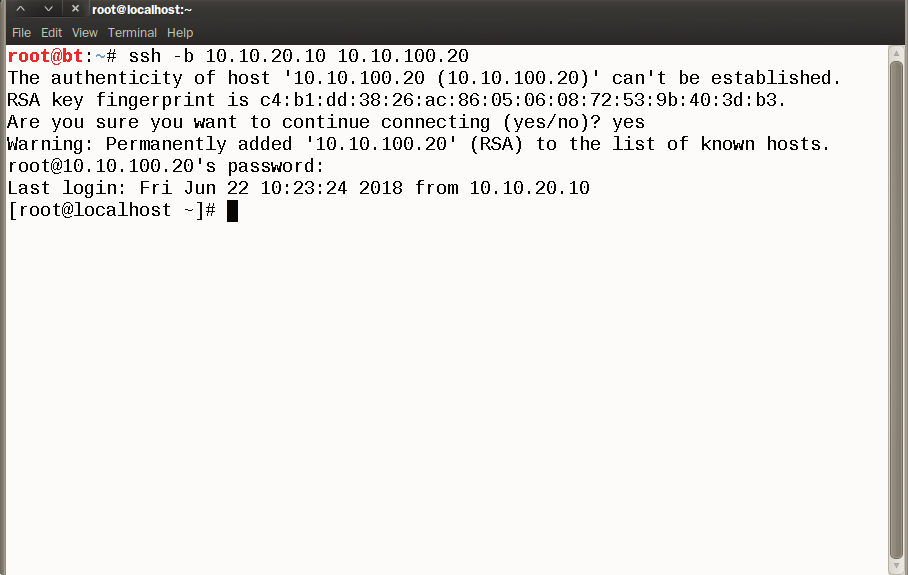
* 먼저 경영관리부 PC를 이용해 DNS서버[10.10.100.20]에 SSH로 접근이 가능한지 확인



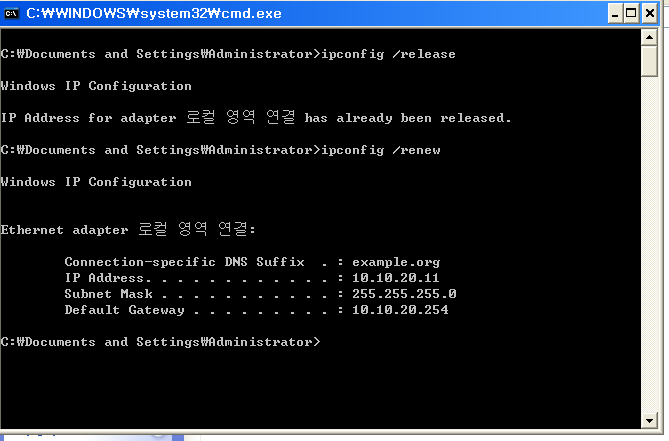
* BT에 경영기획부 PC[10.10.20.10]의 주소를 가상 인터페이스에 부여



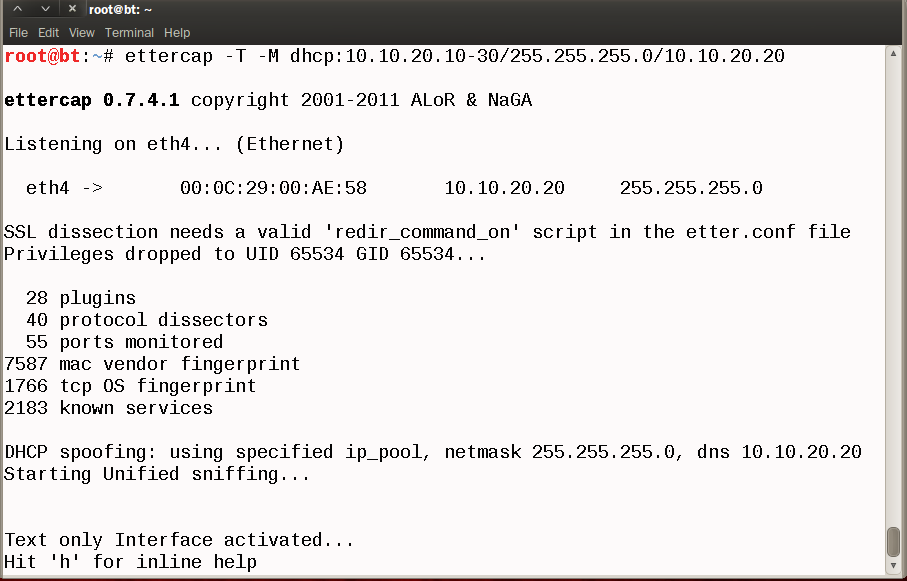
* 공격을 위해 게이트웨이에게 자신이 경영기획부 PC[10.10.20.10]라고 속임



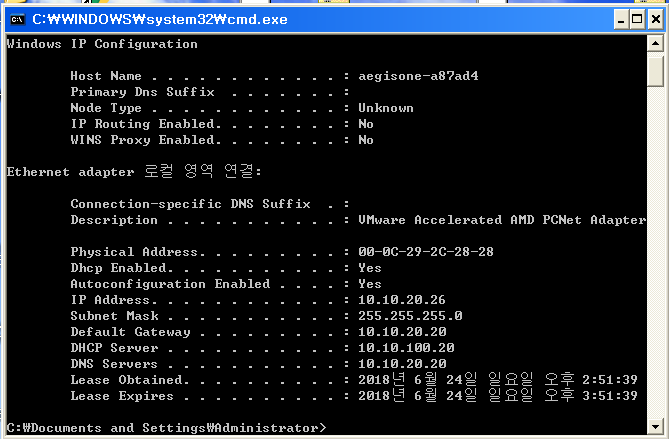
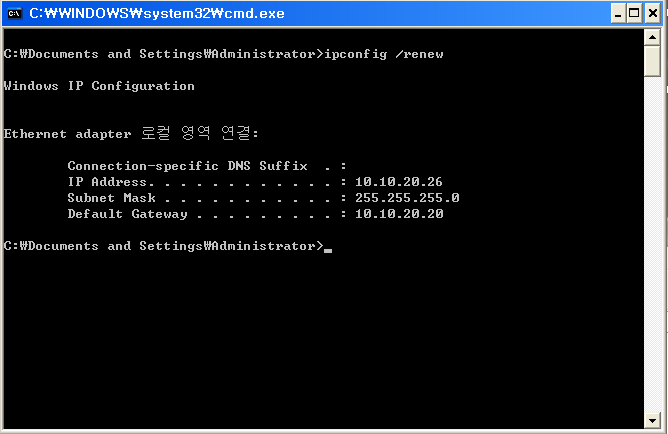
* BT에서 ssh –b 옵션을 이용해 가상 인터페이스에 부여한 경영기획부 PC[10.10.20.10] 으로 DNS서버[10.10.100.20]에 SSH로 접근
* DHCP Spoofing



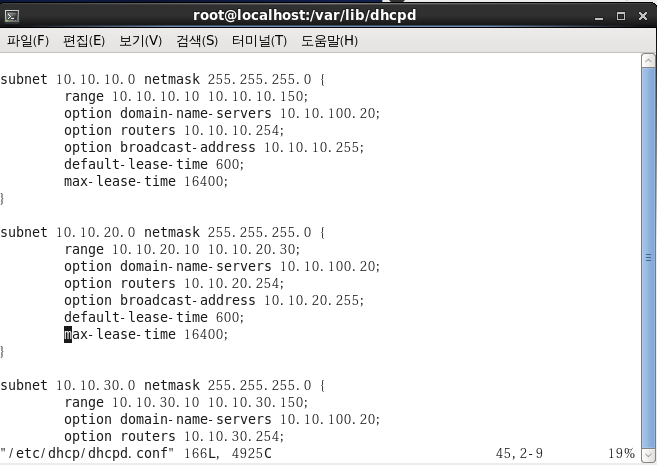
* 경영기획부 직원 PC에서 DHCP서비스를 이용해 아이피를 제대로 할당 받아오는지 확인



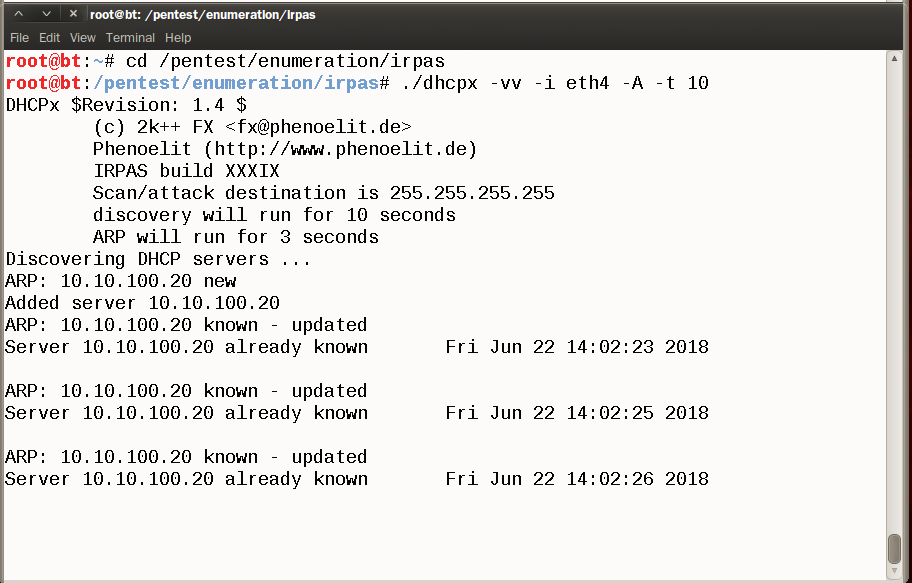
* 공격자가 BT에서 ettercap 툴을 이용해 DHCP Spoofing 공격 시도



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



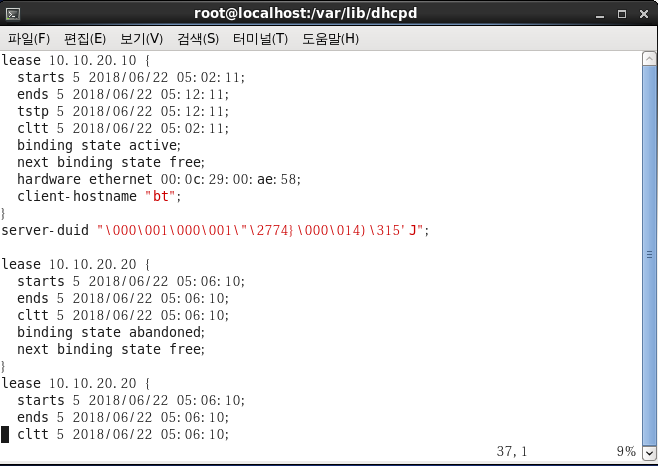
* 공격 후 확인을 위해 할당범위 재 설정



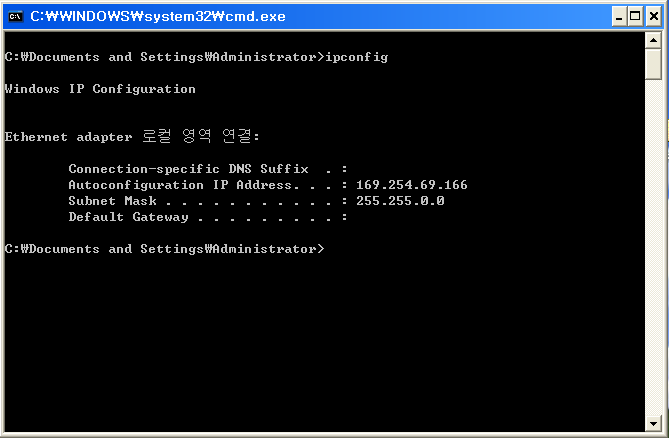
* BT에서 Ettercap 툴을 이용해서 DHCP서버에 공격 시도



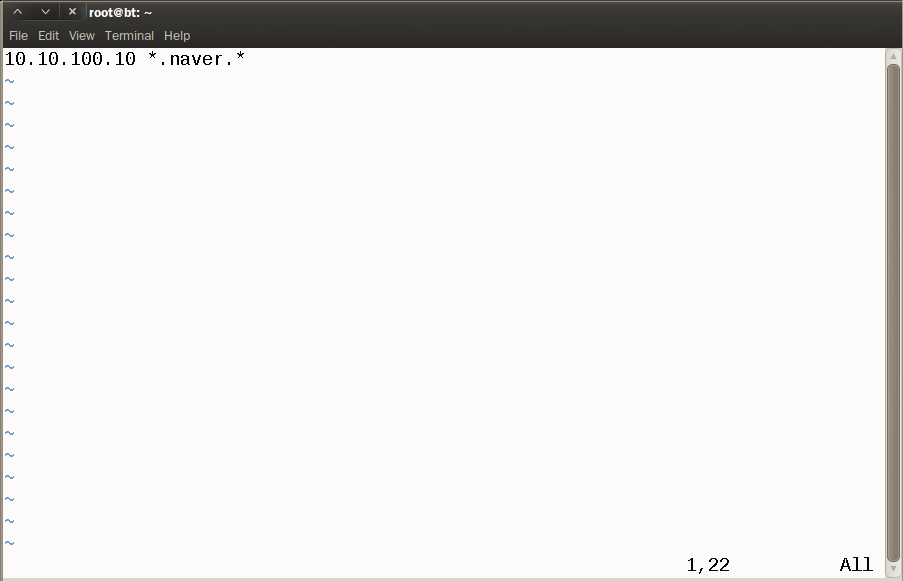
* BT에서 공격을 통한 아이피 할당 내용 확인



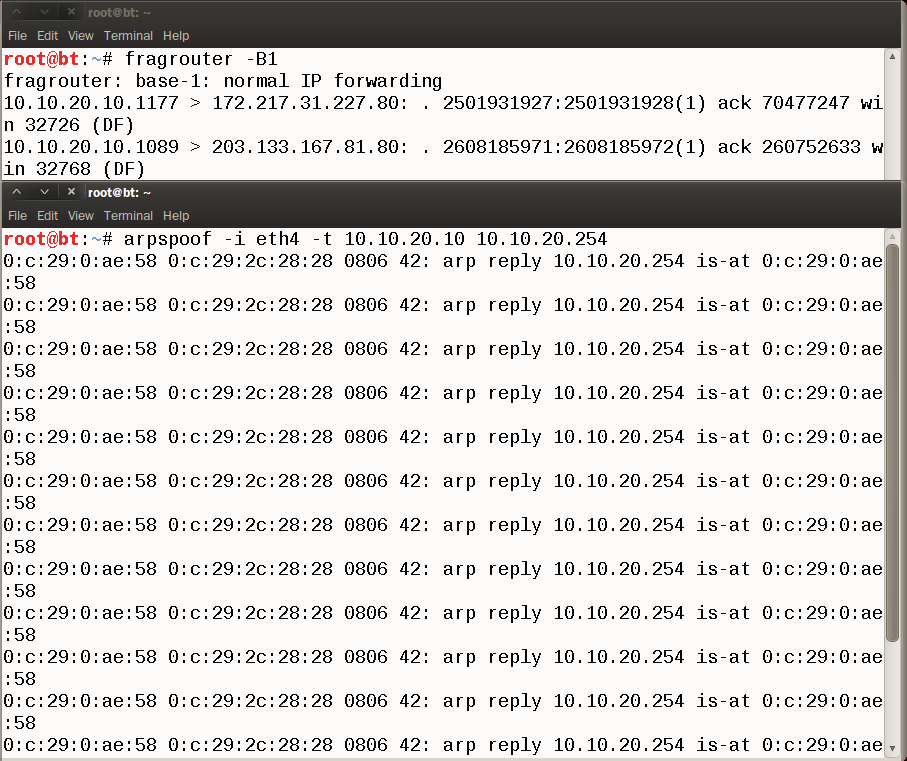
* DHCP서버로 이동해 아이피 할당 내역 확인



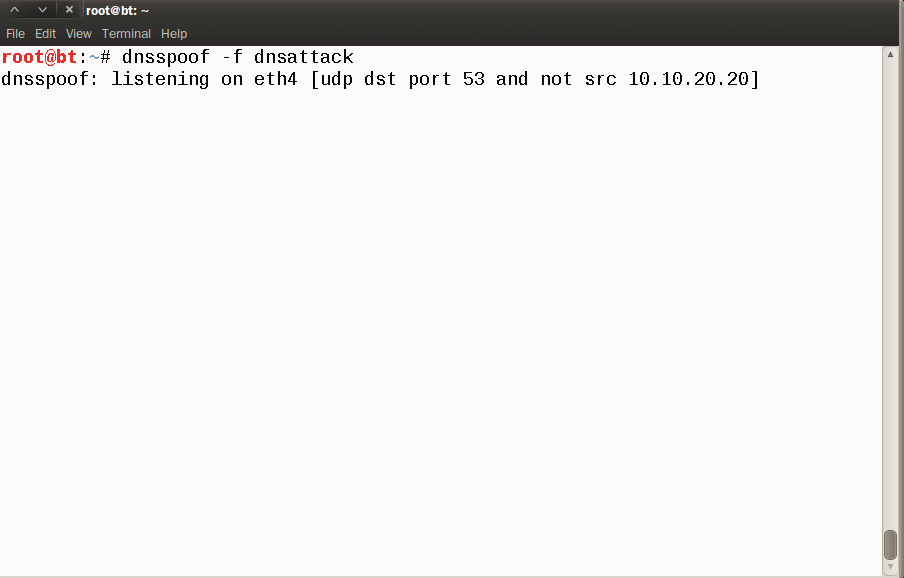
* XP에서 DHCP서버에게 아이피를 할당 받아보지만 DHCP서버가 더 이상 아이피를 할당하지 못해 아이피를 받아오지 않음
* DNS Spoofing



* DNSSpoofing 공격을 위한 파일 생성



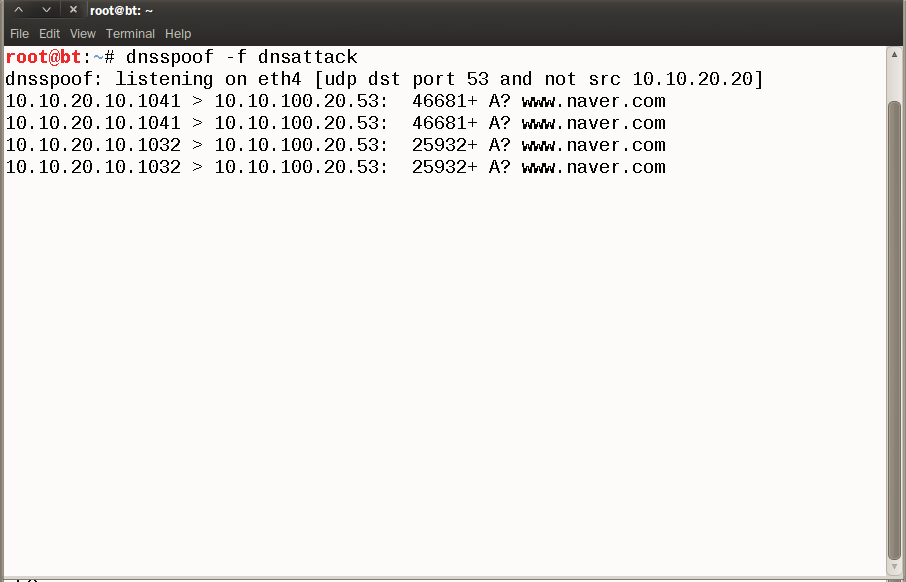
* 경영기획부 PC에게 MITM 상태 만들기



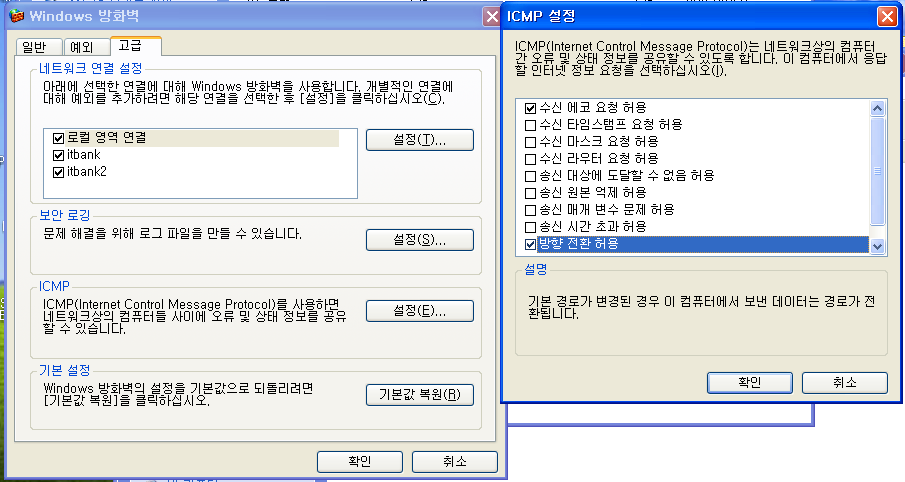
* Dnsspoof 툴을 이용해 DNS Spoofing 공격 시도

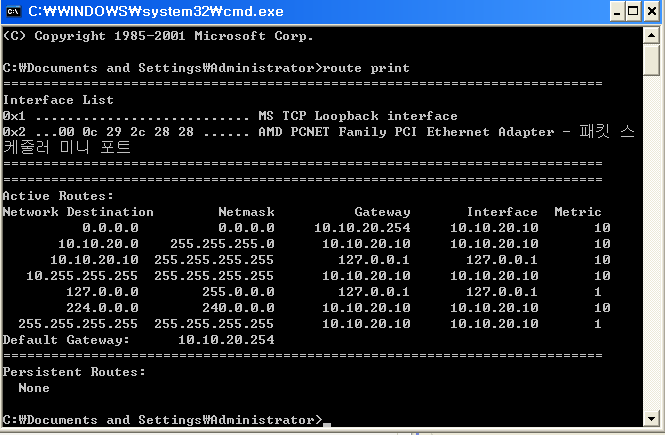


* 경영기획부 PC에서 공격이 제대로 이루어졌는지 확인

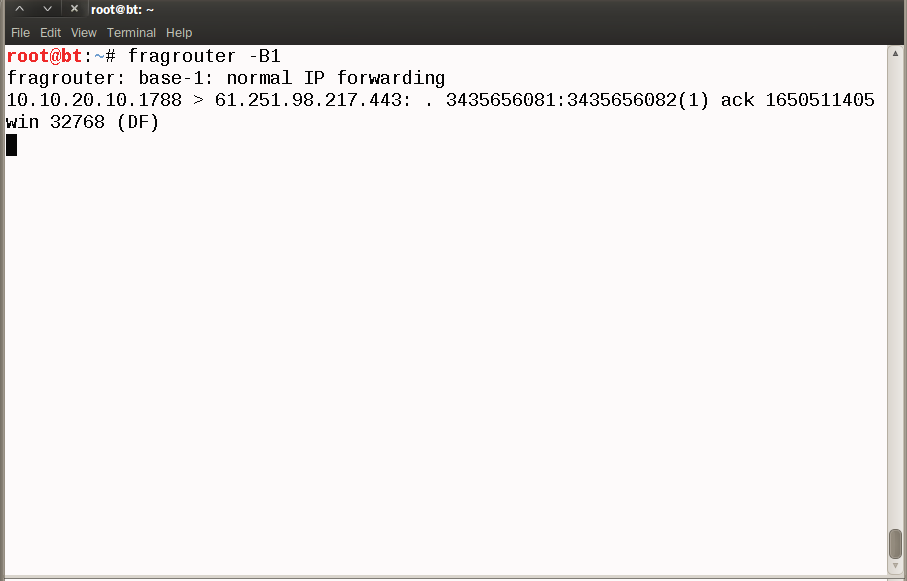


* BT에서 공격이 진행된 내용 확인
* ICMP Redirect

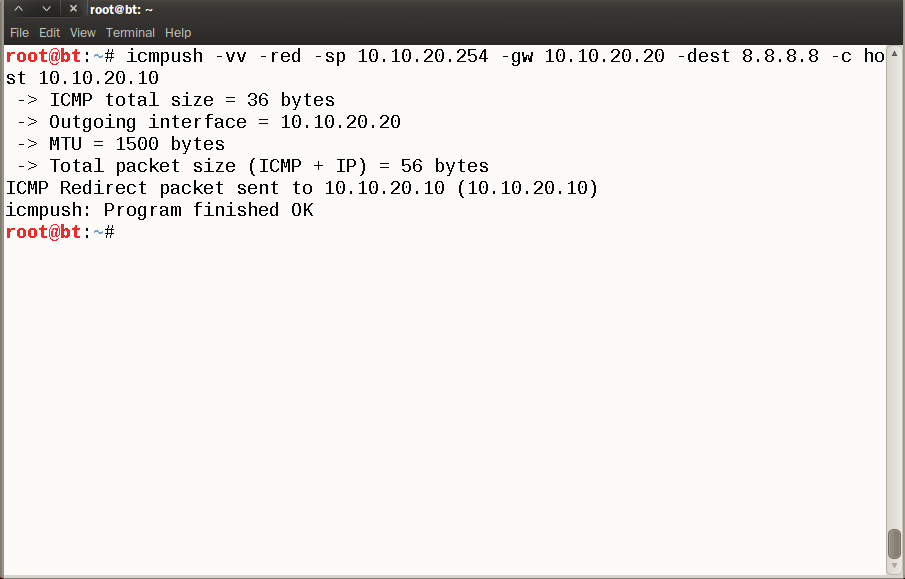




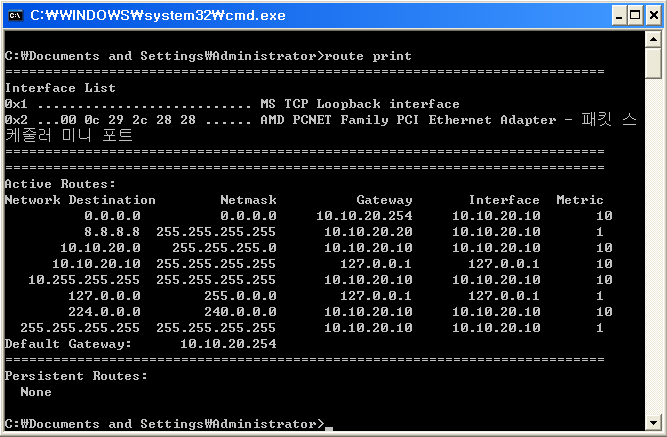
* 공격 확인을 위해 경영기획부 PC가 방향 전환 허용이 체크 되어 있는지와 라우팅 테이블 확인



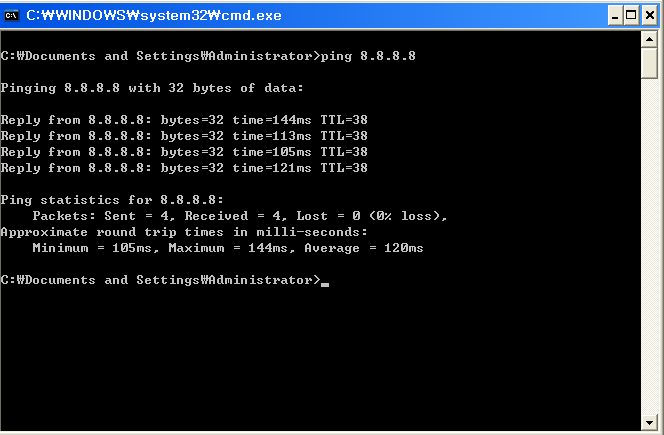
* 공격을 위해 BT에서 포워딩 시작



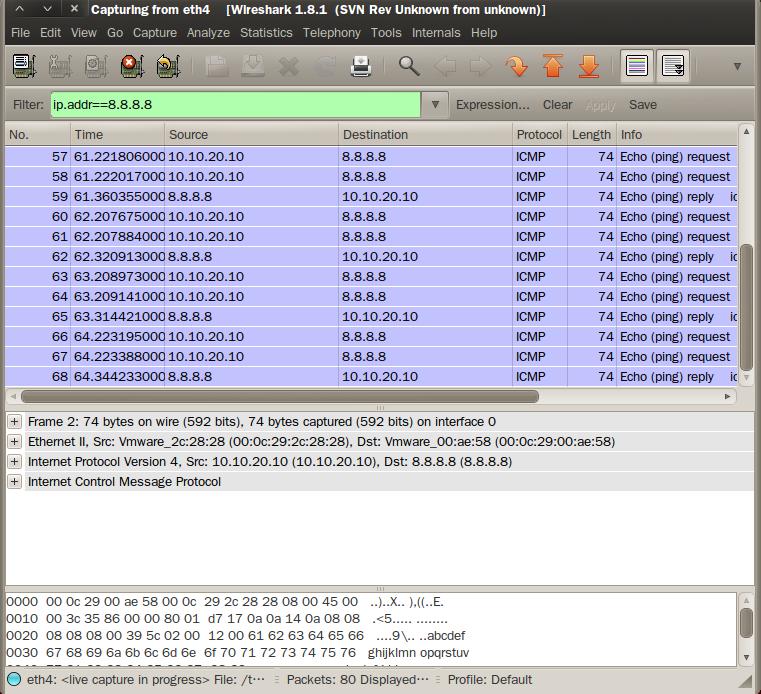
* Icmpush를 이용해서 BT으로 공격

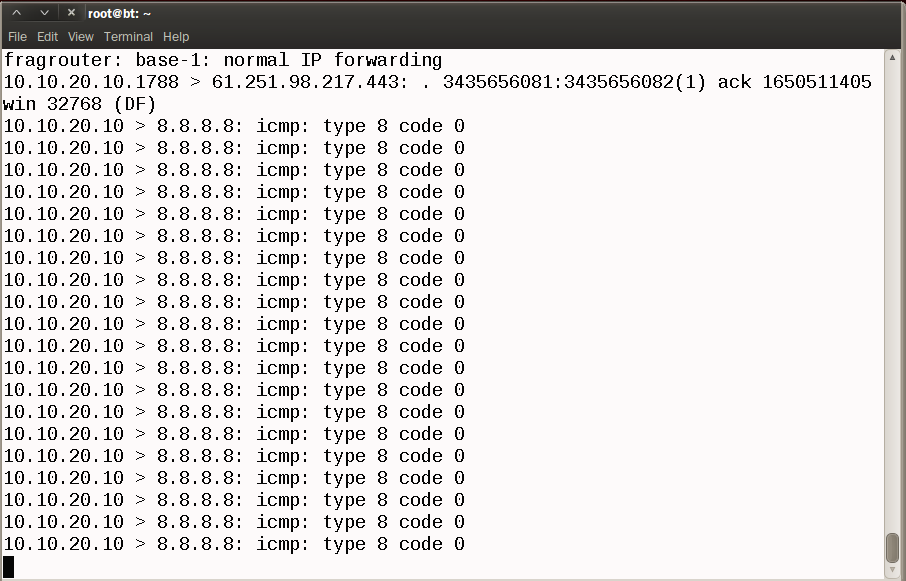


* 공격을 한 뒤 경영기획부 PC 라우팅 테이블을 확인했을 때 공격한 내용이 테이블에 추가된 것을 볼 수 있음

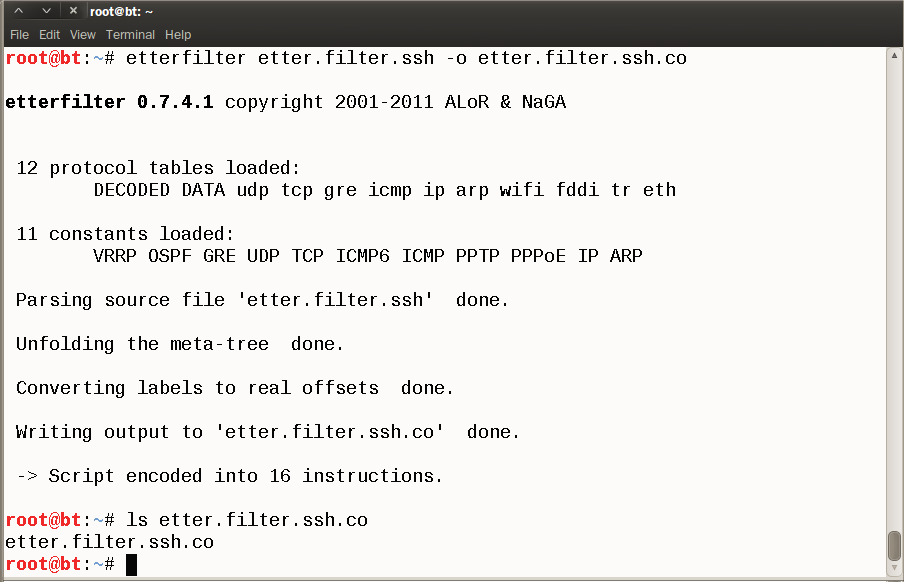
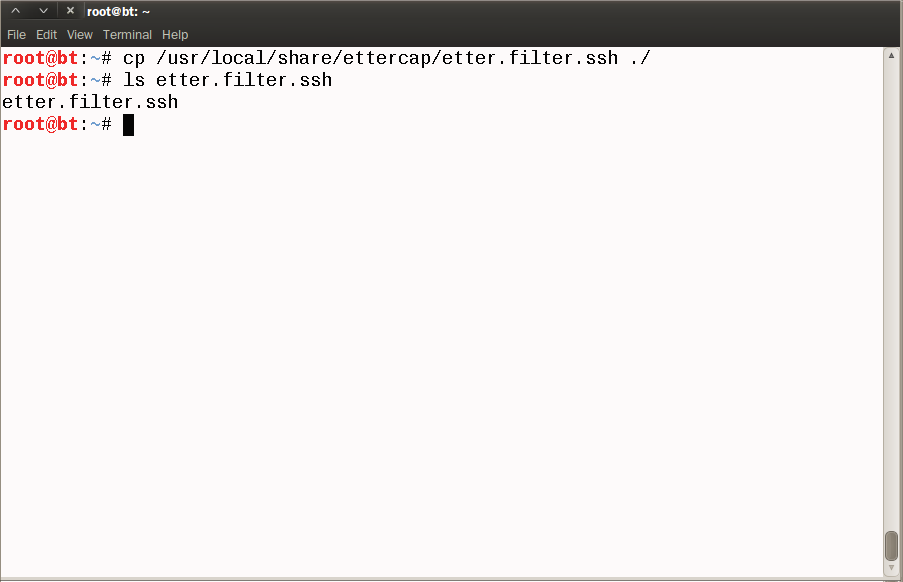


* BT에서 패킷을 볼 수 있는지 확인하기 위해 경영기획부 PC로 외부에 Ping test

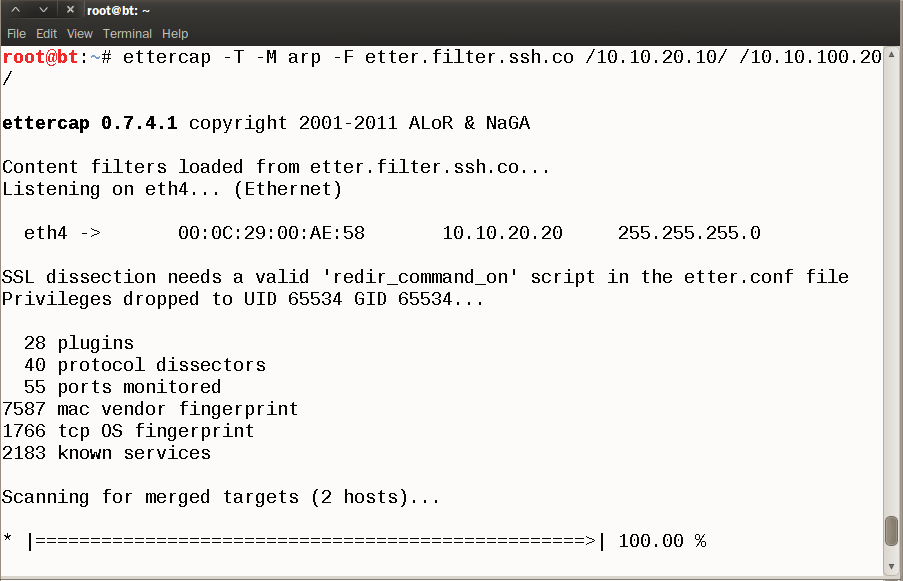




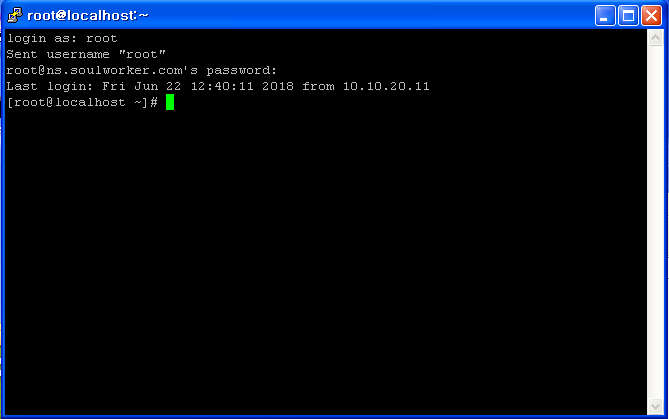
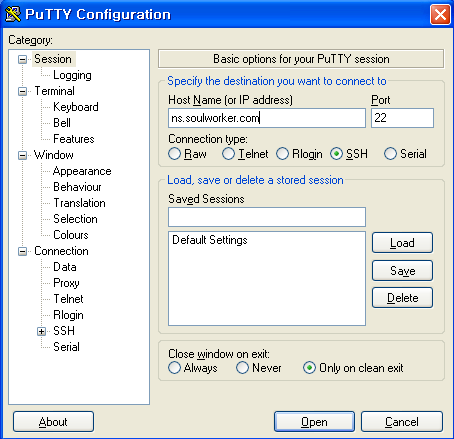
* BT으로 확인했을 때 포워딩이 제대로 되는지, 와이어샤크로 확인했을 때 패킷들이 제대로 잡히는지 확인
* SSH 취약점 공격



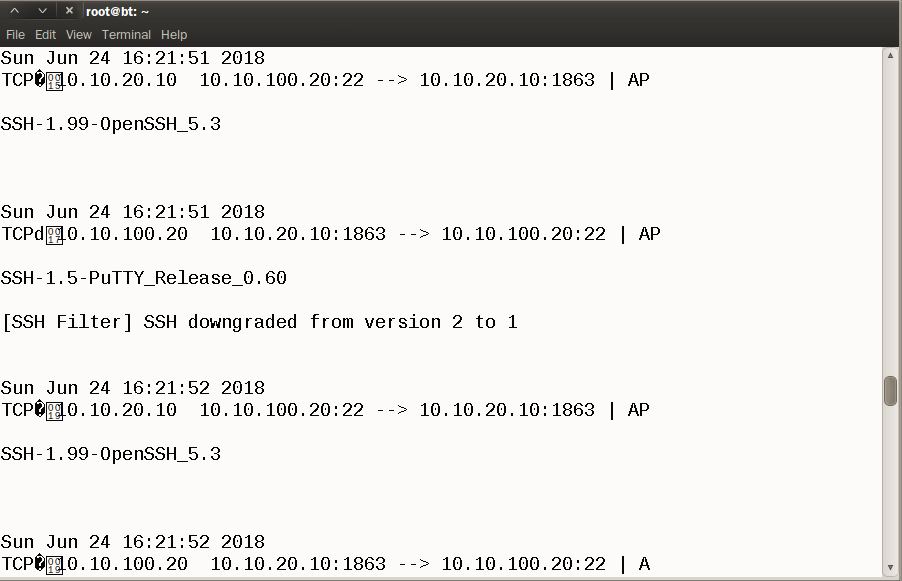
* SSH 버전 협상 시 버전 정보 변경을 하기 위한 filter파일 생성



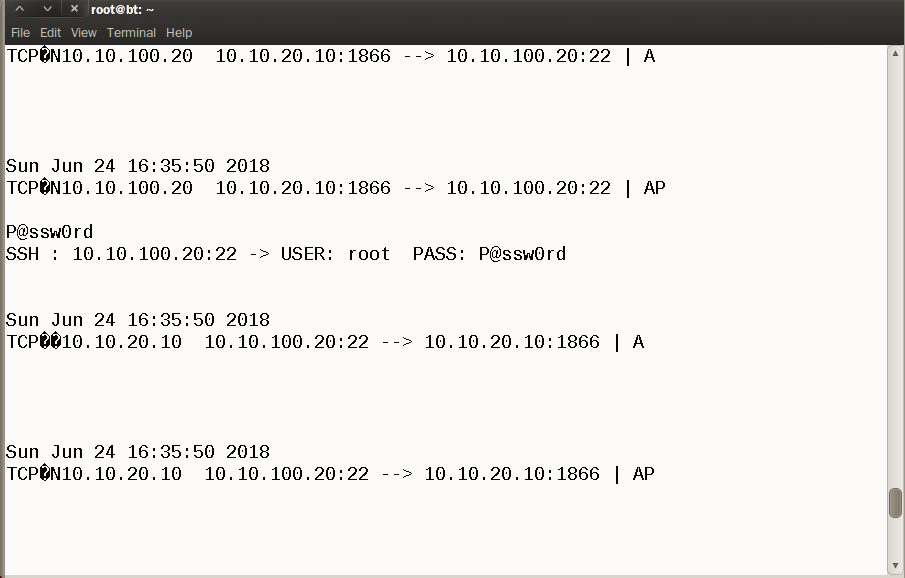
* Ettercap 툴과 만든 etter.filter.ssh.co 필터 파일을 이용해 경영기획부 PC에 공격



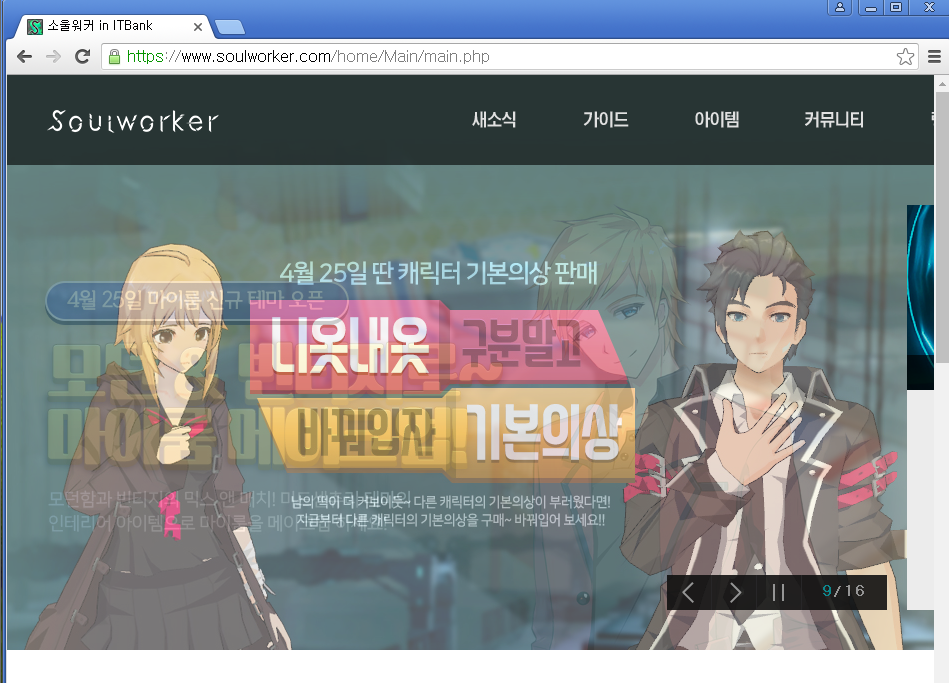
* 공격 확인을 위해 경영기획부 PC에서 DNS서버로 SSH 접속



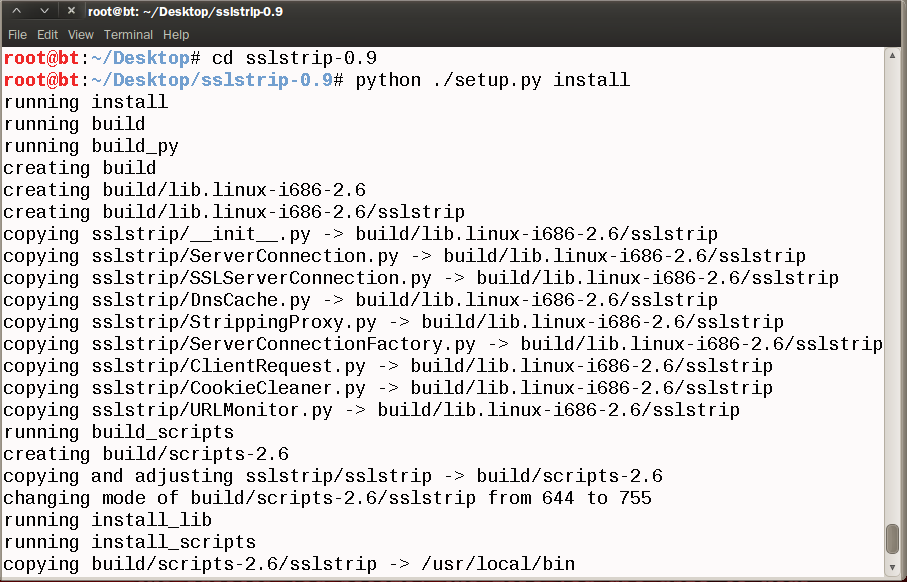
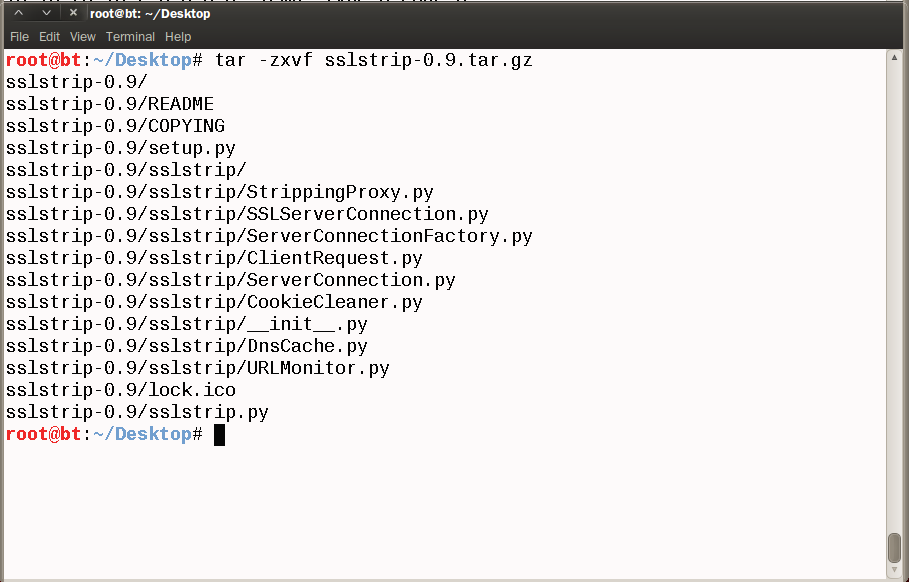
* BT에서 확인해보면 제대로 버전을 다운그레이드 했다는 것을 볼 수 있음



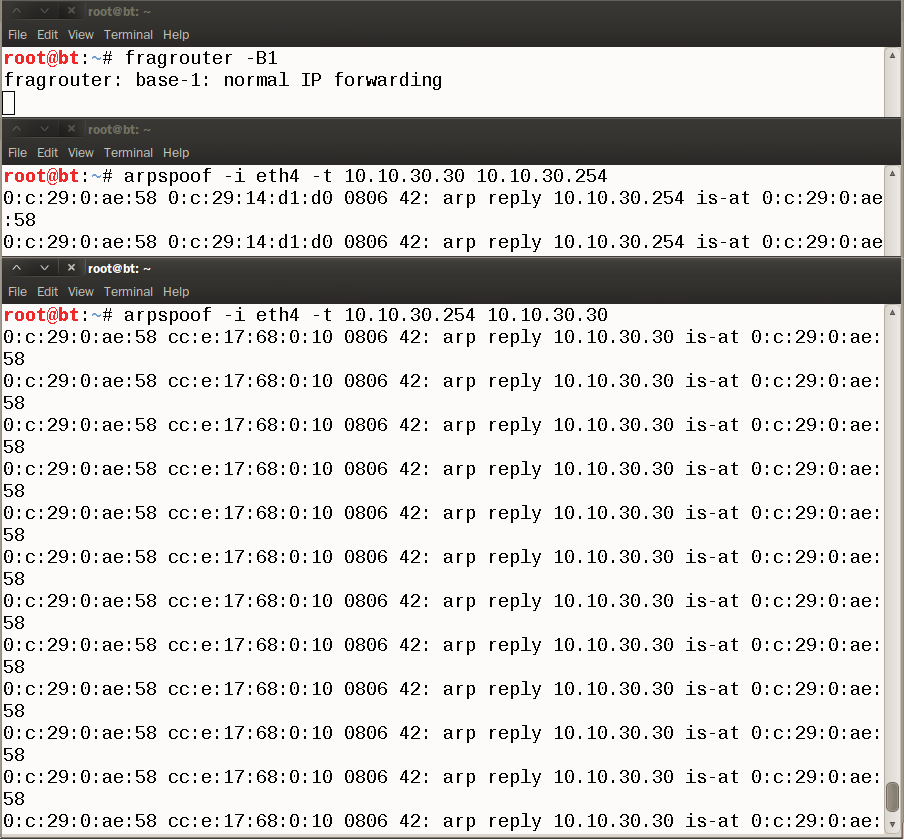
* 경영기획부 PC에서 DNS서버로 SSH 접속 시 사용했던 아이디와 비밀번호도 확인 가능
* SSL 취약점 공격 [SSL Strip Attack]



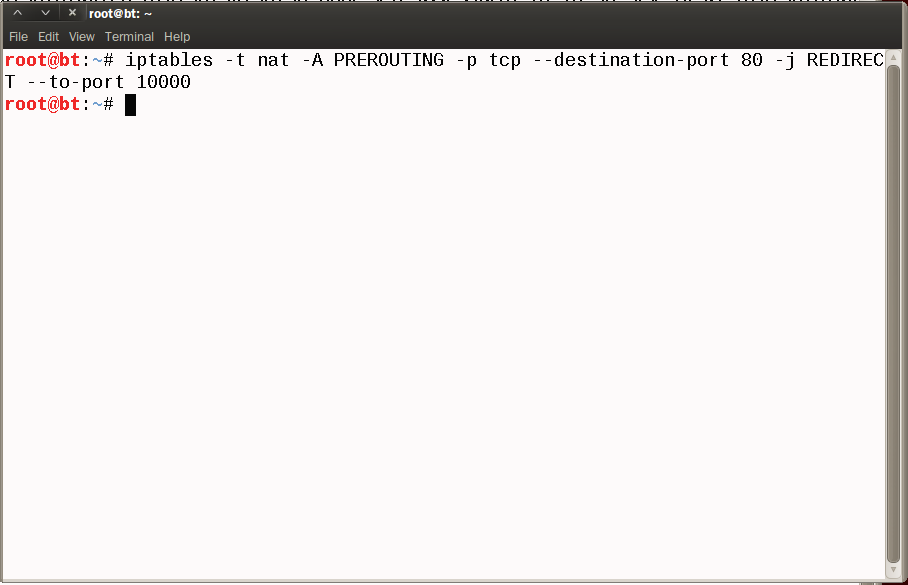
* 공격 시도에 앞서 TLS가 제대로 작동하는지 확인



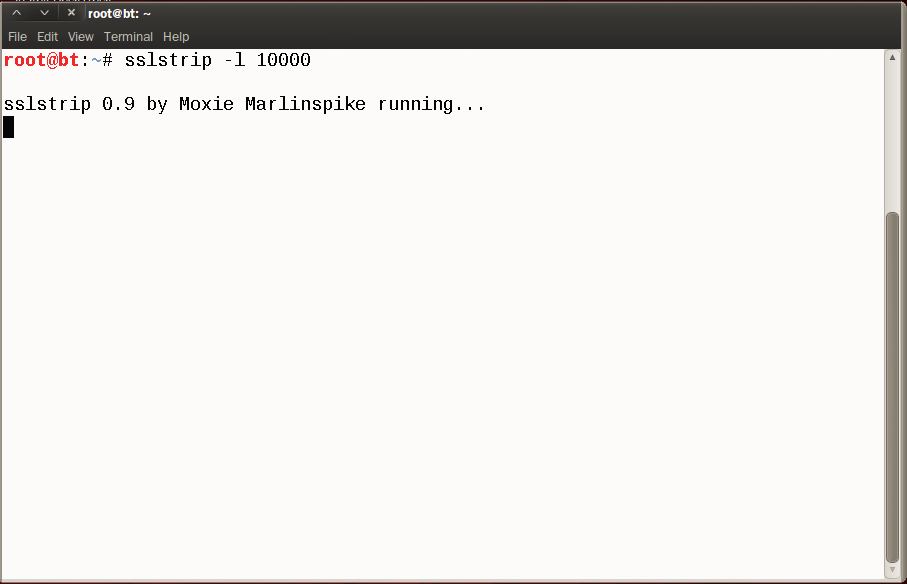
* Sslstrip 공격을 위한 sslstrip 툴 설치



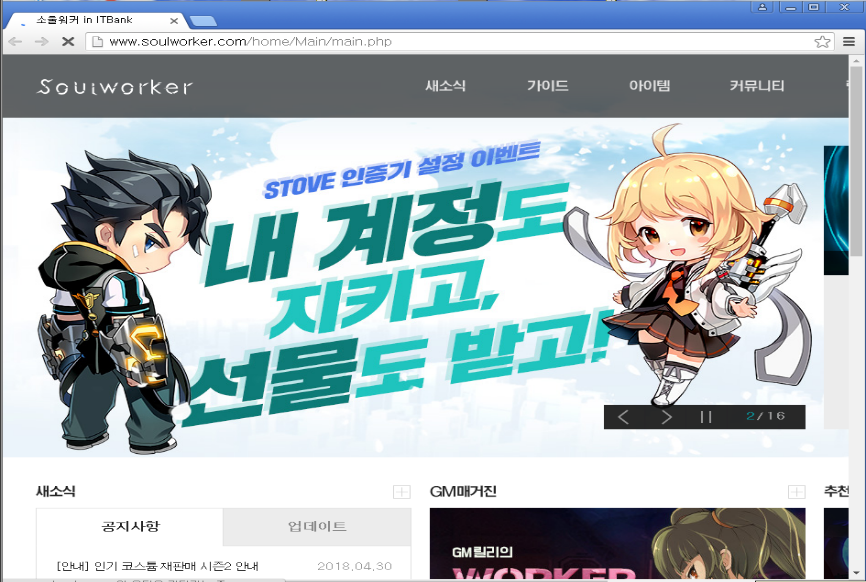
* 게이트웨이와 개발관리부 PC에 MITM 상태 만들기



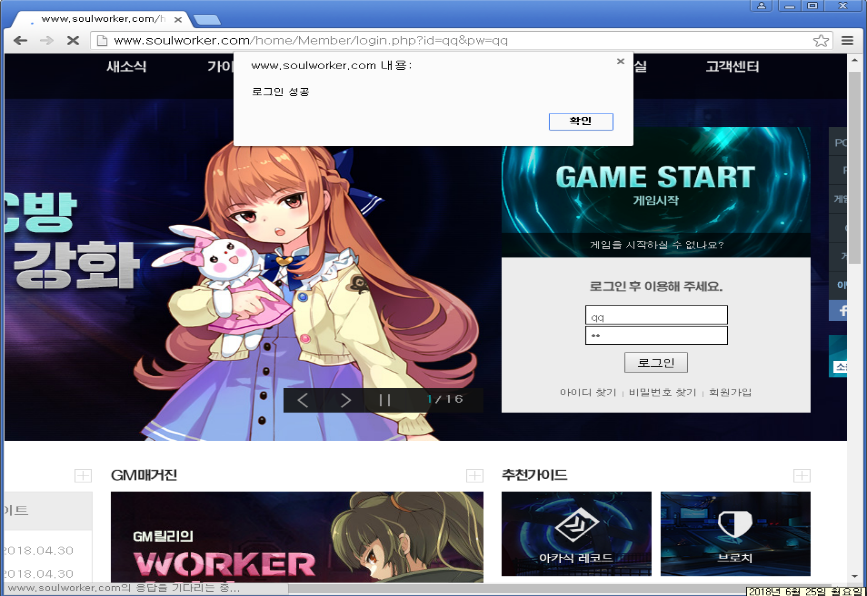
* 80번 포트로 접근을 시도하면 10000번 포트로 리다이렉트 시키겠다는 방화벽 설정



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



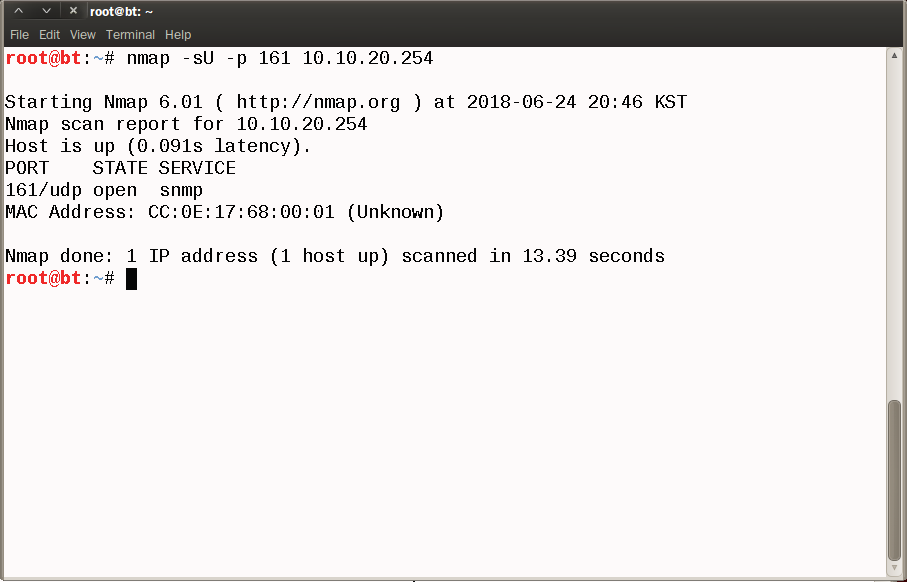
* 개발관리부 PC로 웹에 접근을 시도하면 https가 아닌 http로 접근하는 것을 볼 수 있음



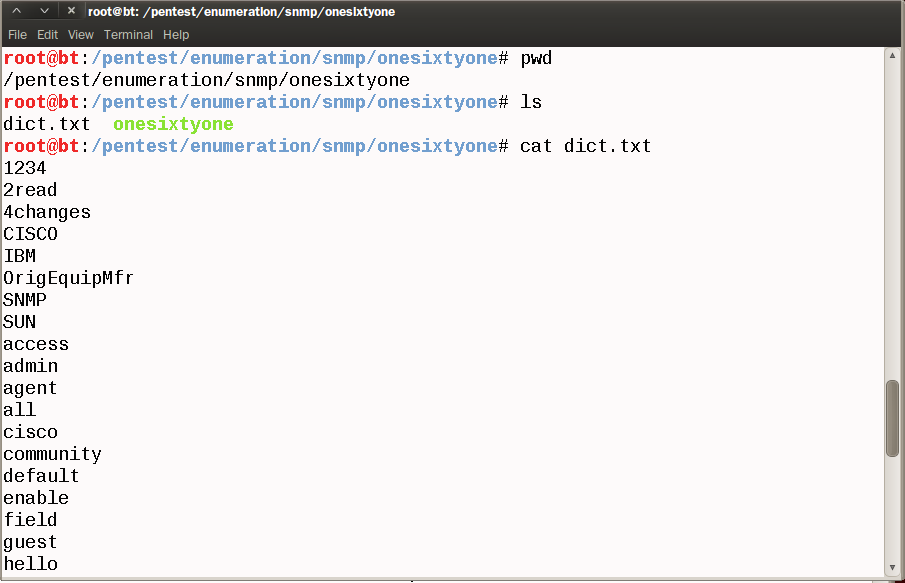
* 로그온 시도



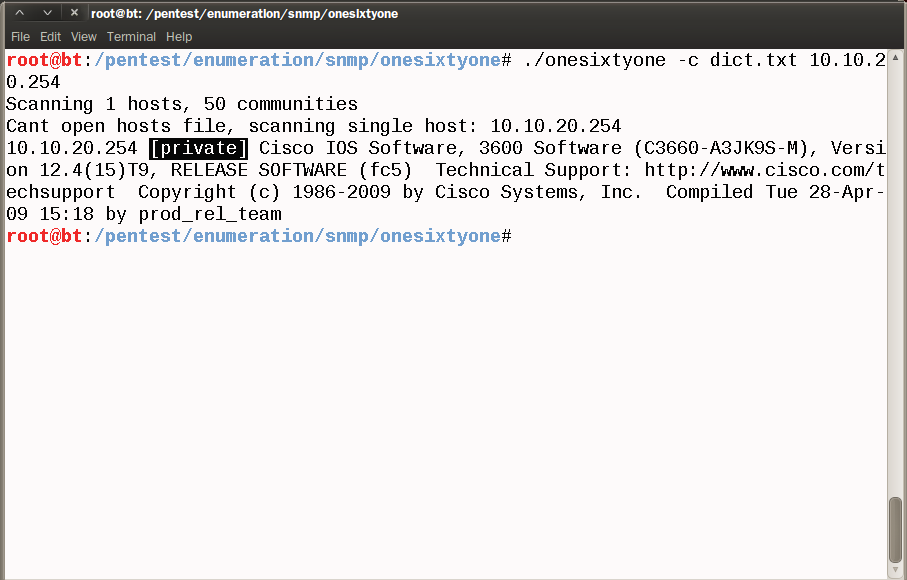
* 로그온 시도 후 BT으로 돌아와 와이어 샤크를 확인해보면 아이디와 비밀번호가 노출된 것을 볼 수 있음
* SNMP 취약점 공격



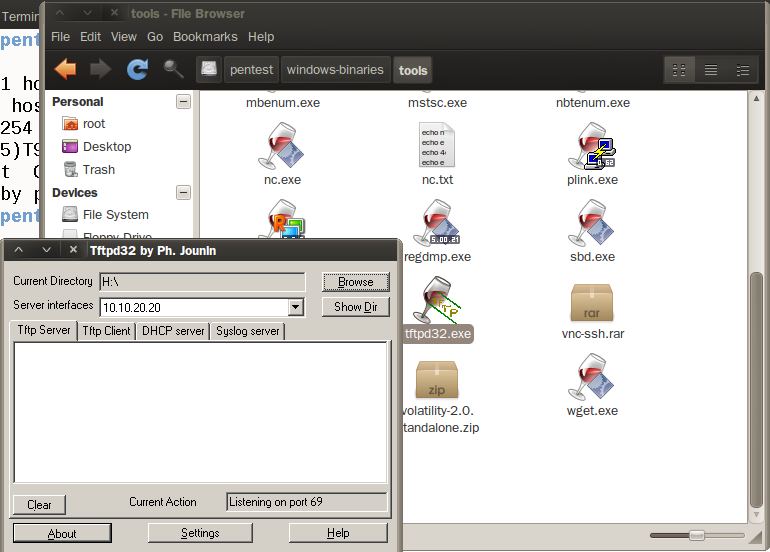
* 공격에 앞서 snmp서비스를 지원해주는지 nmap툴을 사용해 확인



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

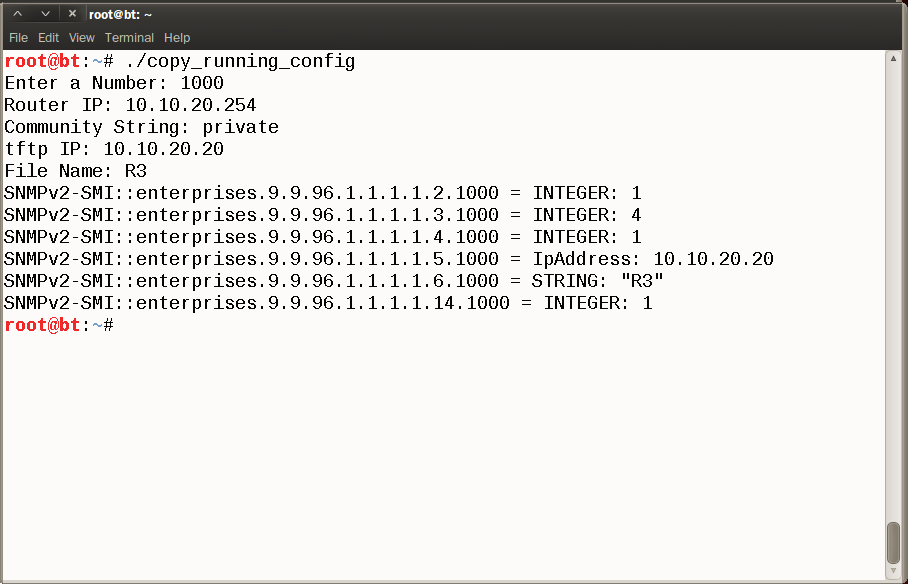


* Onesixtyone 툴과 dict.txt파일을 사용해 공격대상의 Community String 알아오기

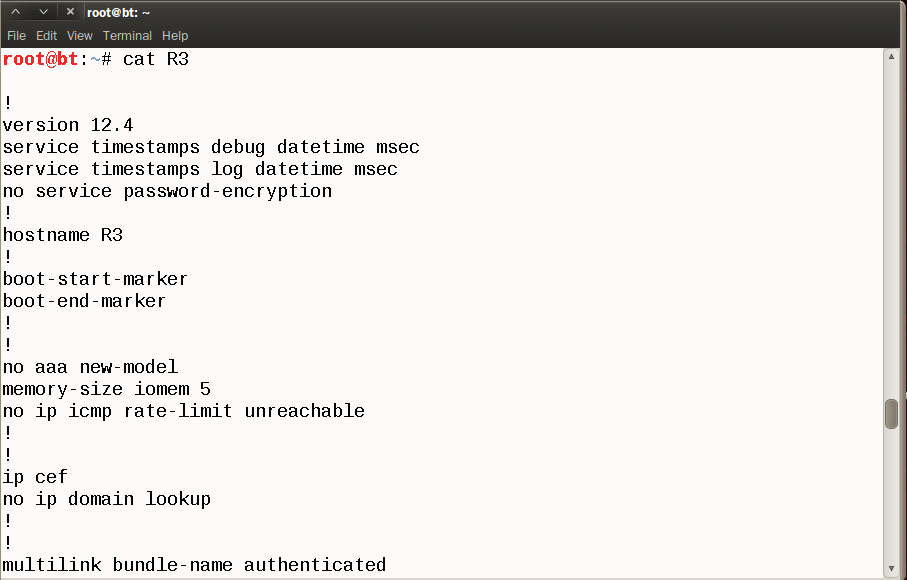




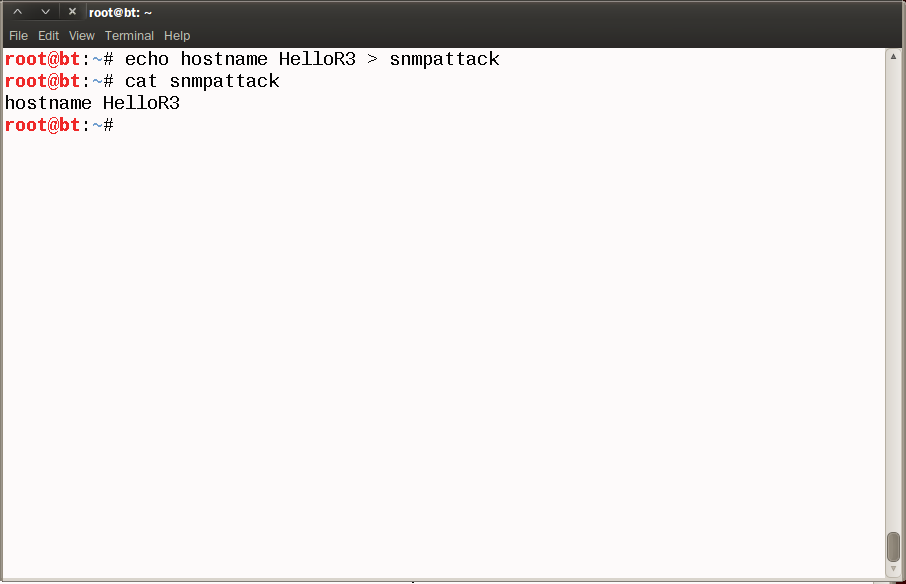
* 공격을 하기 위해 tftp을 실행하고 up\_running\_config, copy\_running\_config 파일 확인



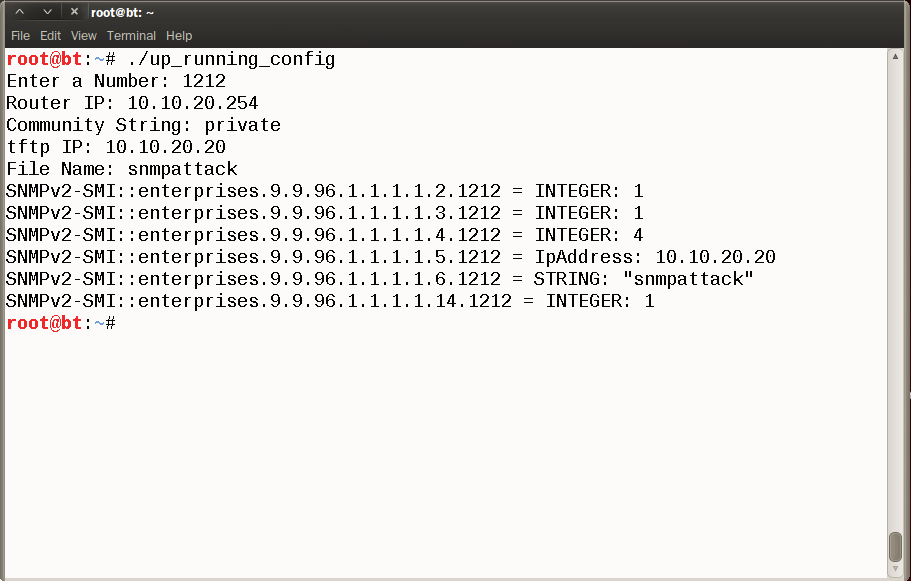
* Copy\_running\_config 파일과 tftp를 이용해 공격대상의 running\_config 상태를 파일로 받아보기



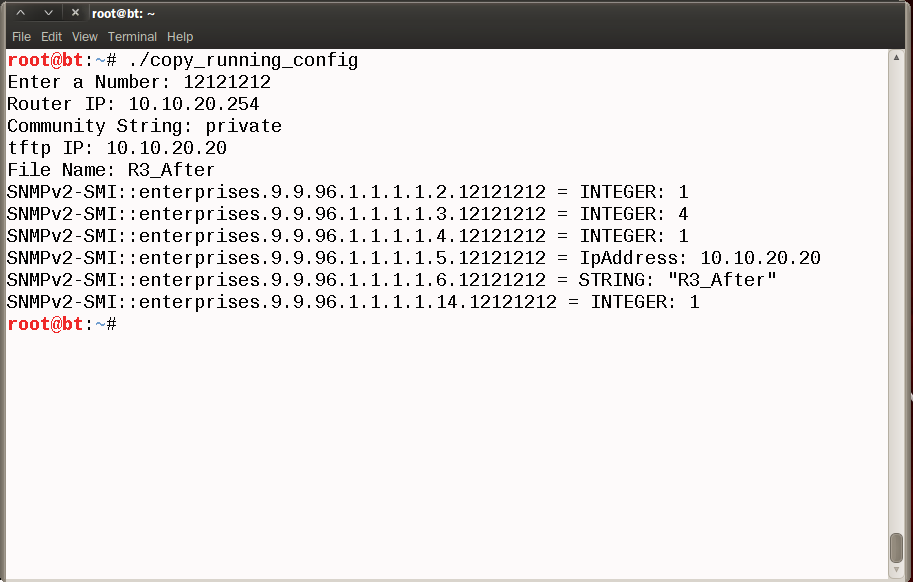
* 제대로 running\_config 상태를 받아왔는지 확인



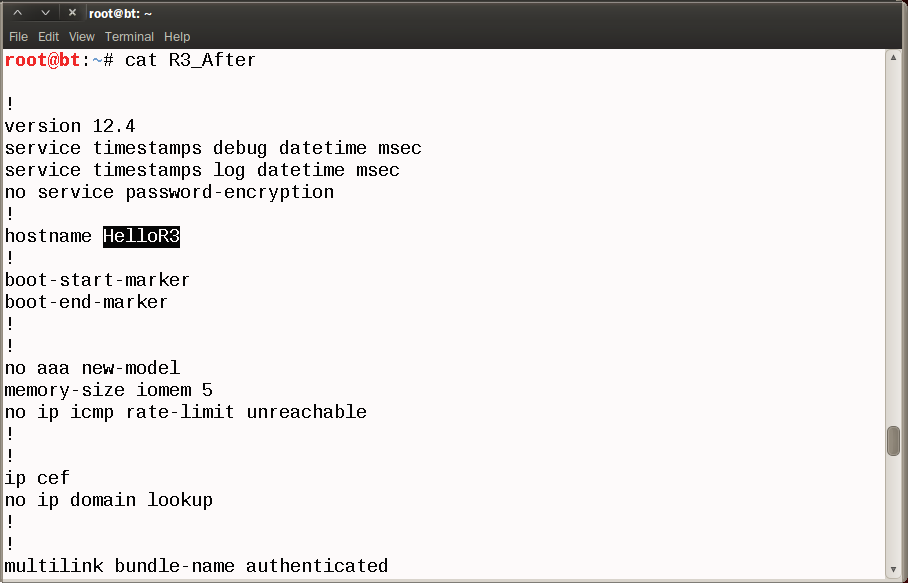
* 받아온 running\_config 상태 확인 후 바꾸고 싶은 내용을 파일로 만들기



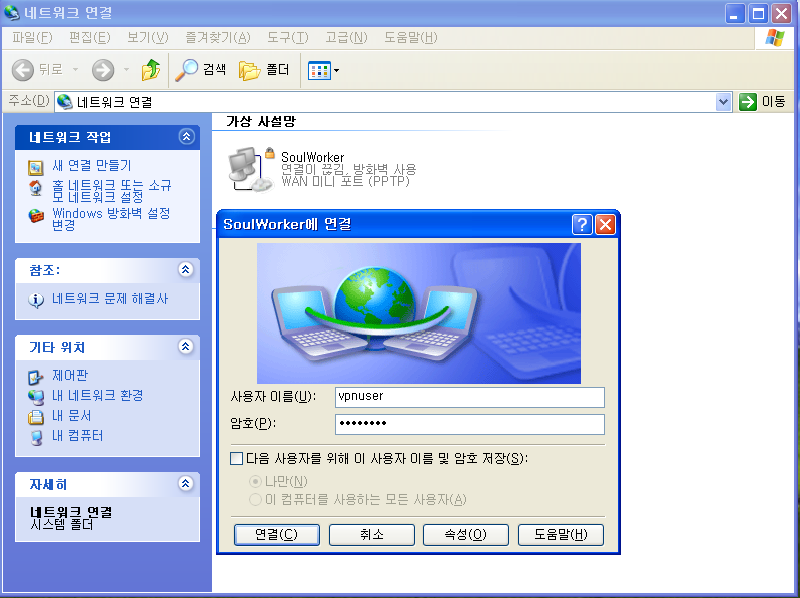
* Up\_running\_config 파일을 이용해 만든 공격파일을 공격대상에게 보내기

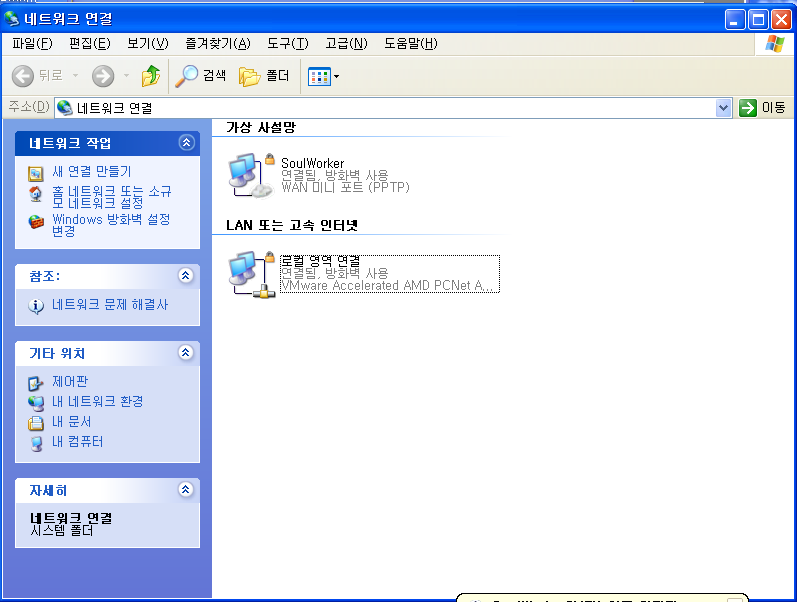


* 공격이 제대로 됐는지 확인하기 위해 다시 running\_config 상태를 파일로 받아보기



* 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