11. 악성코드 – II

담당교수: 차 영욱

ywcha@andong.ac.kr

목차

- 백도어
  - 유닉스 계열의 백도어
  - 윈도우 계열의 백도어: NetBus
- 스니핑: Wireshark
- 스푸핑
  - IP 스푸핑
  - ARP 스푸핑
  - DNS 스푸핑
- 패스워드 크래킹: Brutus AET2
- 봇넷과 DDOS

백도어

❑ 원래의 의미

- 프로그램 개발이나 유지 보수 및 유사 시의 문제 해결을 위해 관리자나 개발자가 정상적인 절차를 우회하여 시스템에 접속할 수 있게 만들어 놓은 비상문

❑ 해킹으로서의 백도어(Backdoor)

- 해커가 차후 접속을 위하여 시스템에 심어 놓은 프로그램
- 백도어의 주된 형태: 특정 포트를 시스템 관리자 몰래 열어 놓고 공격자의 명령을 기다림
- 시스템 관리자의 정상적인 보안 관리를 우회하여 동작 → 패스워드를 변경하더라도 지장을 받지 않음

유닉스 계열의 백도어

- 패스워드 크래킹 백도어: 패스워드가 취약한 사용되고 있지 않은 사용자 계정을 탐색하여 해당 시스템에 접속 → 어려운 패스워드로 바꾸므로 더 이상 취약한 패스워드가 아니며 공격자에 의해 백도어로 사용

- Rhosts + + 백도어: rsh, rlogin 등의 서비스에서 패스워드가 아닌 호스트 이름에 의해 인증이 이루어지는 점을 악용 → 침입자는 해당 시스템의 rhosts 파일에 "+ +" 기호를 추가함으로써 어떤 호스트의 사용자라도 공격할 호스트를 통해 접속

- Login 백도어: 텔넷 접속의 패스워드 인증 시스템에 대한 우회 방법을 이용 → login.c 프로그램을 수정하여 설정한 백도어 패스워드가 입력되면 관리자가 지정한 패스워드에 상관 없이 로그인을 허용

- Telnetd 백도어
  - 사용자의 텔넷 접속 → inetd 서비스가 텔넷 접속을 대기 → in.telnetd(사용자로 부터 터미널 종류 등 몇 가지 사항 점검) 에 연결 → login 프로그램 구동
  - 시스템 관리자가 수시로 login 프로그램을 점검하므로 침입자는 터미널 종류가 특수하게 설정되어 있는 경우에 인증과정 없이 로그인 되도록 in.telnetd를 수정

Windows 계열의 백도어

- 원격지에서의 윈도용 PC의 제어 및 관리 도구
  - 백오리피스(Back Orifice)
    - 1998년 해커들의 컨벤션인 DEFCON에서 MS 운영체제의 취약성을 소개하기 위하여 Sir Dystic에 의해서 소개된 프리웨어(freeware)
  - NetBus
    - 1998년 스웨덴 프로그래머인 Car-Fredrik Neikter가 개발한 쉐어웨어(shareware)
- 트로이목마 프로그램과 포트번호

포트번호	트로이목마 명
777	AimSpy
1080	SubSeven 2.2, WinHole
1243	BackDoor-G, SubSeven
5880	Y3K RAT
6000	The Thing
6666	Dark Connection Inside
12345	NetBus

백도어 툴 – 트로이 목마

- 트로이 목마(Trojan horse)는 악성 루틴이 숨어 있는 프로그램
  - 정상적인 프로그램으로 보이나 실행 시 악성 코드를 실행
  - 네트워크를 통한 원격 조정 가능
  - 컴퓨터 바이러스와 같이 시스템에 피해를 주지만 자기복제 능력이 없음
  - 시스템에 직접적인 피해와 더불어 사용자 몰래 정보를 빼오는 형태
  - 백신 프로그램을 이용해 진단 및 치료가 가능

- 서버 툴의 침입경로와 방법
  - 직접 침투: 해커가 직접 침투하여 설치
  - E-mail 침투: 전자 메일에 첨부된 서버 툴을 사용자가 실행함으로 설치
  - Windows 공유 폴더 침투: 읽기/쓰기가 모두 가능한 공유 폴더에 서버 툴을 설치

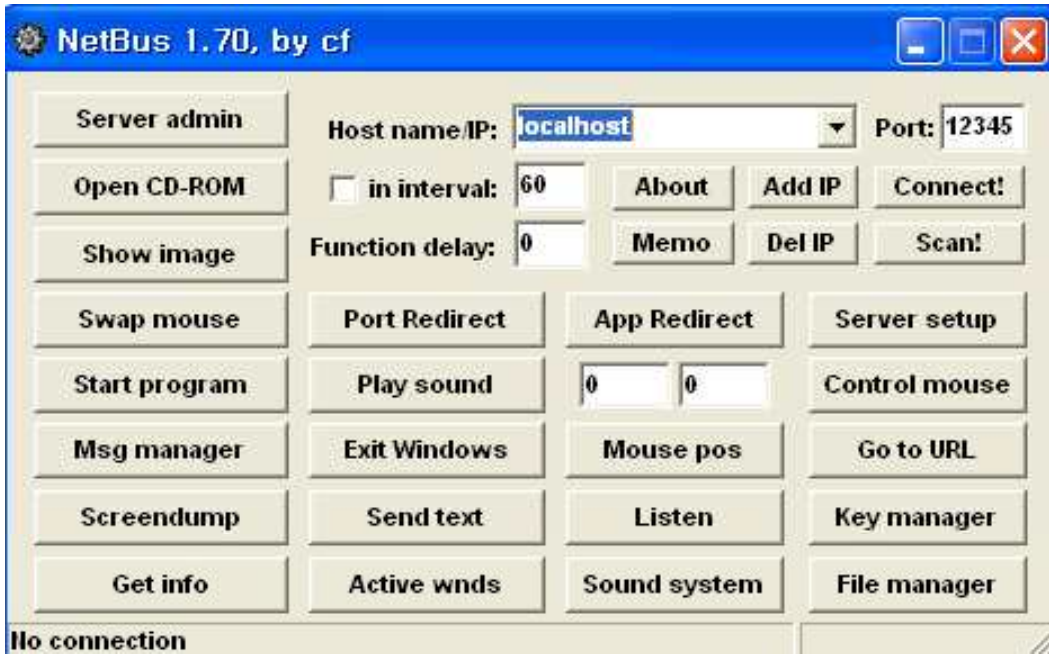
Netbus 프로그램

❑ 클라이언트 및 서버 프로그램

- Netbus.exe: 해커가 사용하는 클라이언트 프로그램
- Patch.exe: 공격 대상 시스템에 설치되는 서버 프로그램
- Netbus.rtf: 라이선스 등에 관련된 설명서

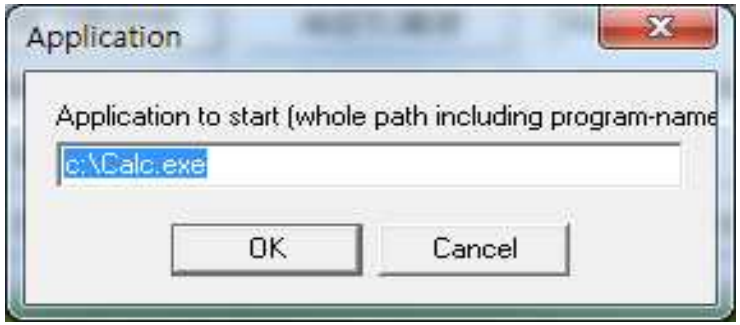
NetBus 기능 및 사용자 인터페이스

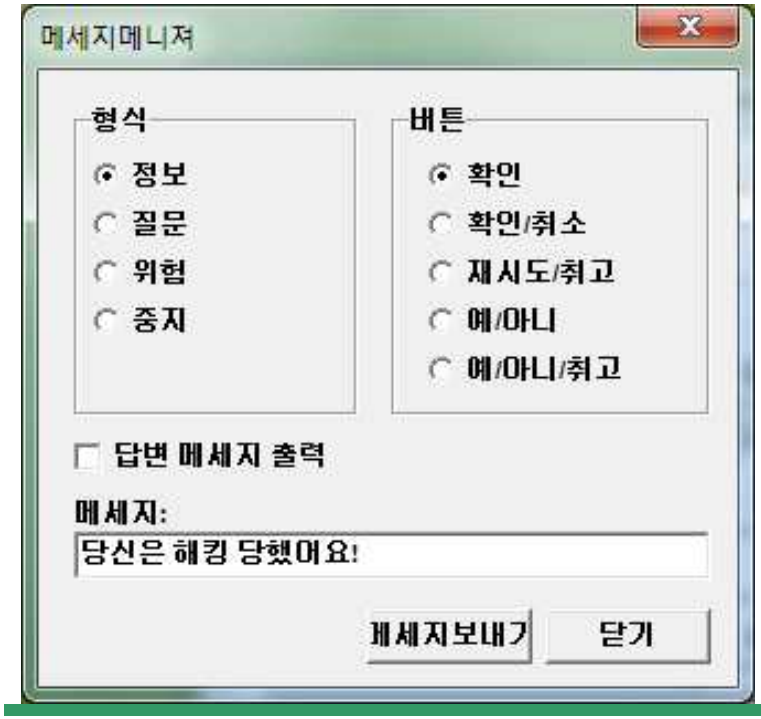
- Host name/IP: 접속할 타겟시스템(서버)의 IP 주소
- Port: 타겟 시스템의 포트번호(디폴트 값은 12345)
- Start program: 실행하려는 프로그램의 절대경로 입력
- Screendump: 타켓시스템의 현재 화면 캡쳐
- Active Wnds: 사용 중인 프로세스의 검색 및 종료
- Listen: 타겟시스템의 키 스트로크 저장
- Server setup: 서버의 설정 정보 세팅
- File manager: 타겟시스템 파일 검색/다운로드/업로드/삭제
- Open CD-ROM: 타겟시스템의 시디롬 개폐
- Swap mouse: 마우스 오른쪽과 왼쪽 버튼의 기능 스위치
- Exit Windows: 타겟시스템의 리부팅, 로그아웃 및 종료
- Sound system: 타겟시스템의 볼륨 조정 및 녹음 수행
- Control mouse: 공격자(클라이언트)의 마우스가 움직이는 대로 타켓시스템의 마우스 이동
- Go to URL: 특정 사이트의 URL 오픈
- Key manage: 타겟시스템의 키보드 관련사항 관리
- …

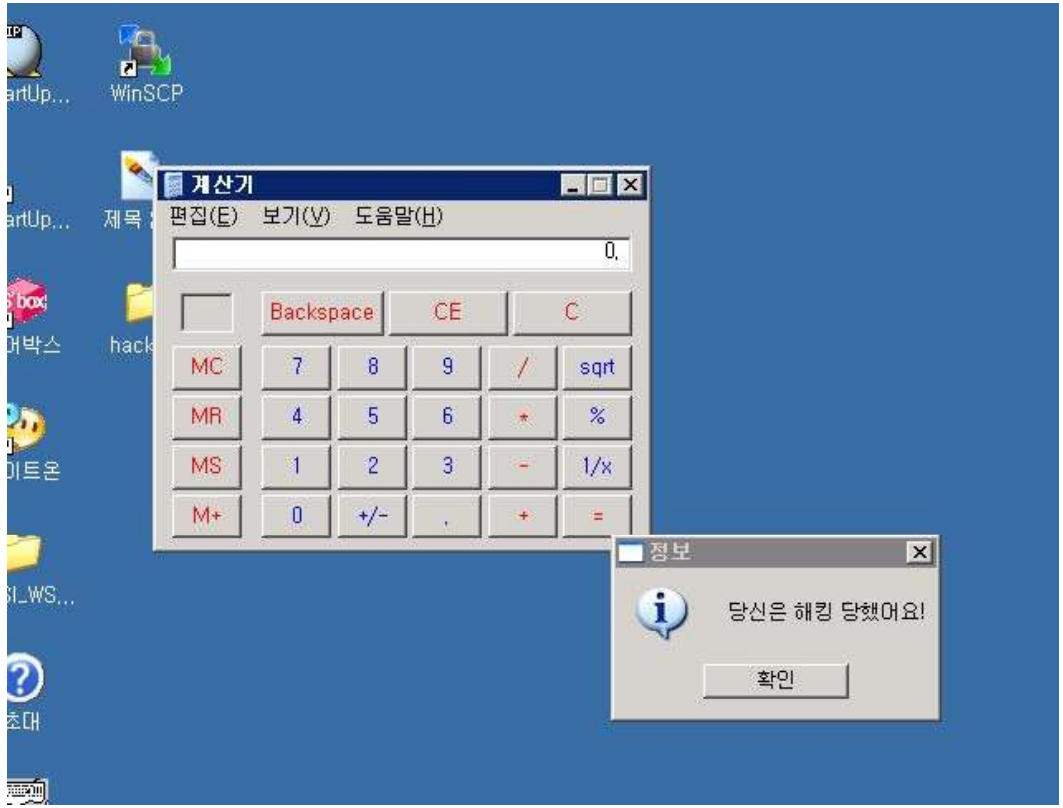


NetBus – 실행 화면(1/3)

❑ 프로그램 실행 및 경고창 띄우기

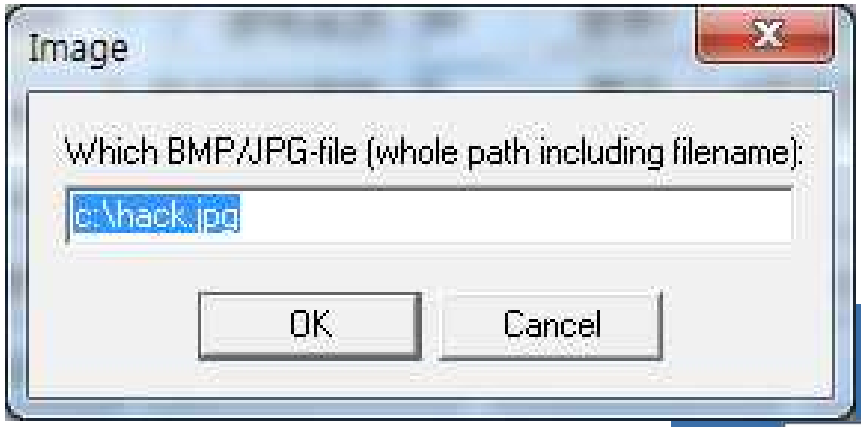


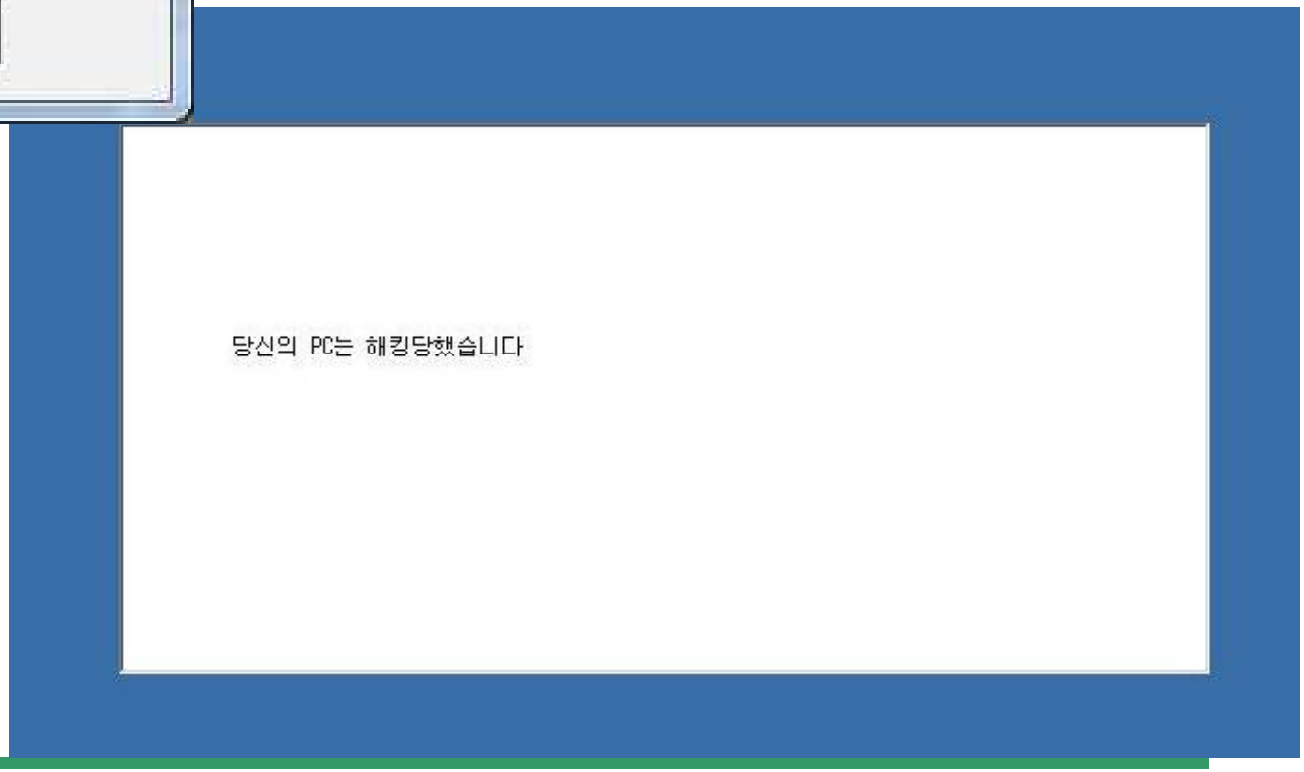




NetBus – 실행 화면(2/3)

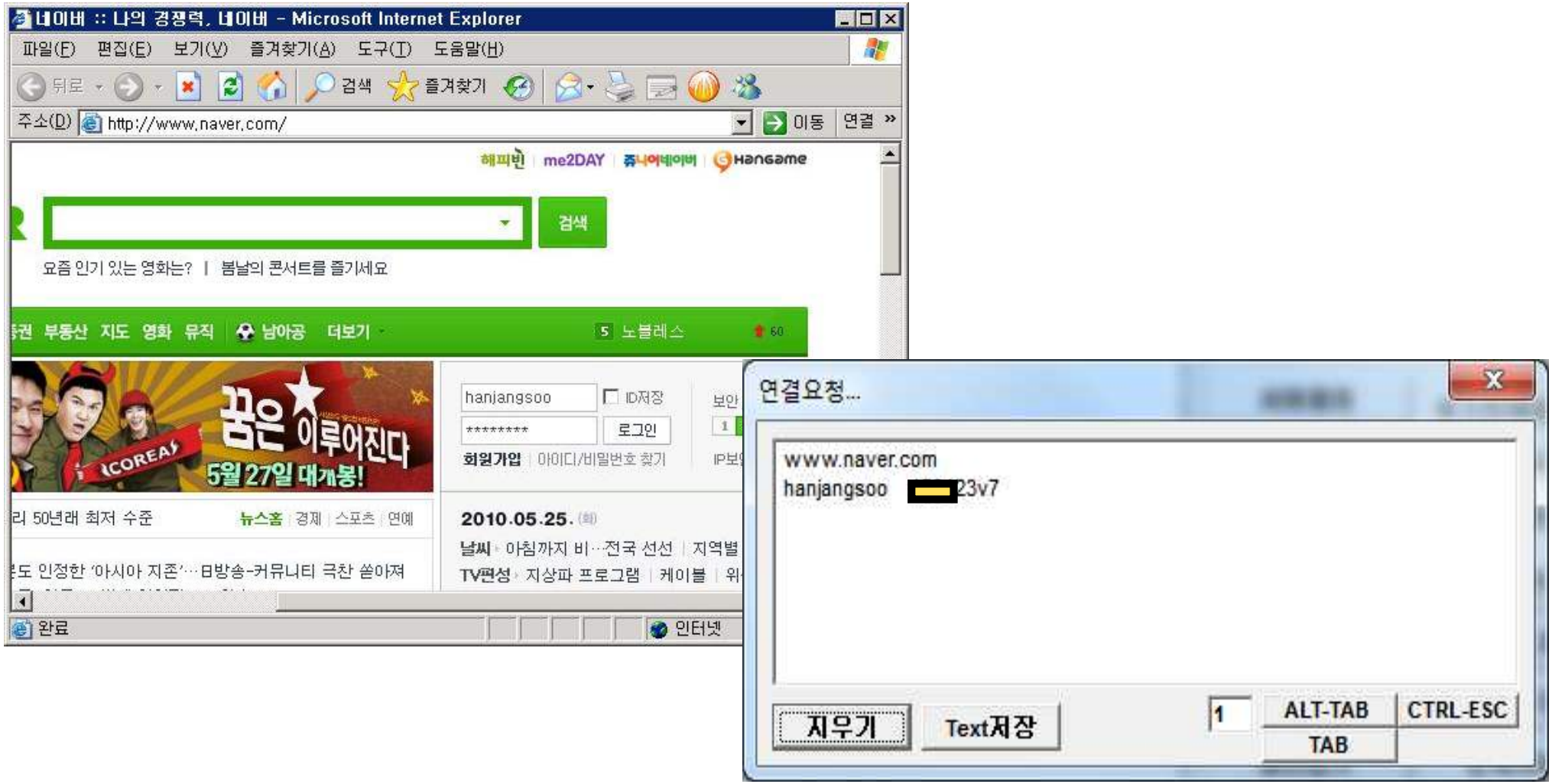
❑ 해킹 된 PC의 바탕화면에 이미지 나타내기





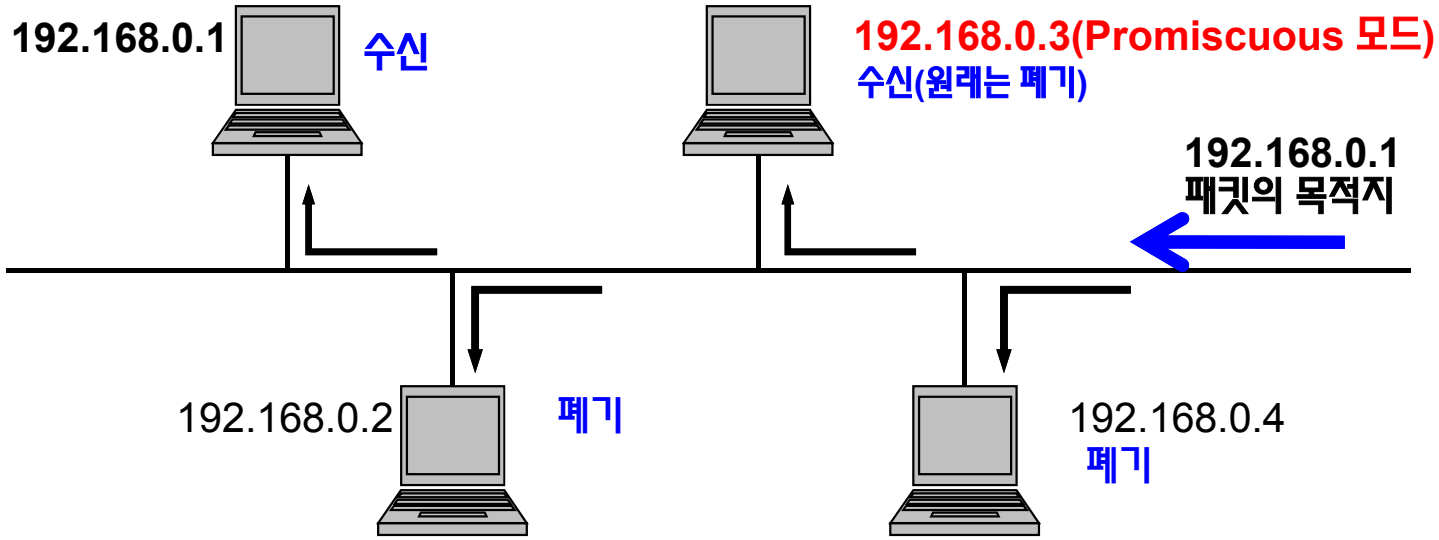
NetBus – 실행 화면(3/3)

❑ 키 로그 기능



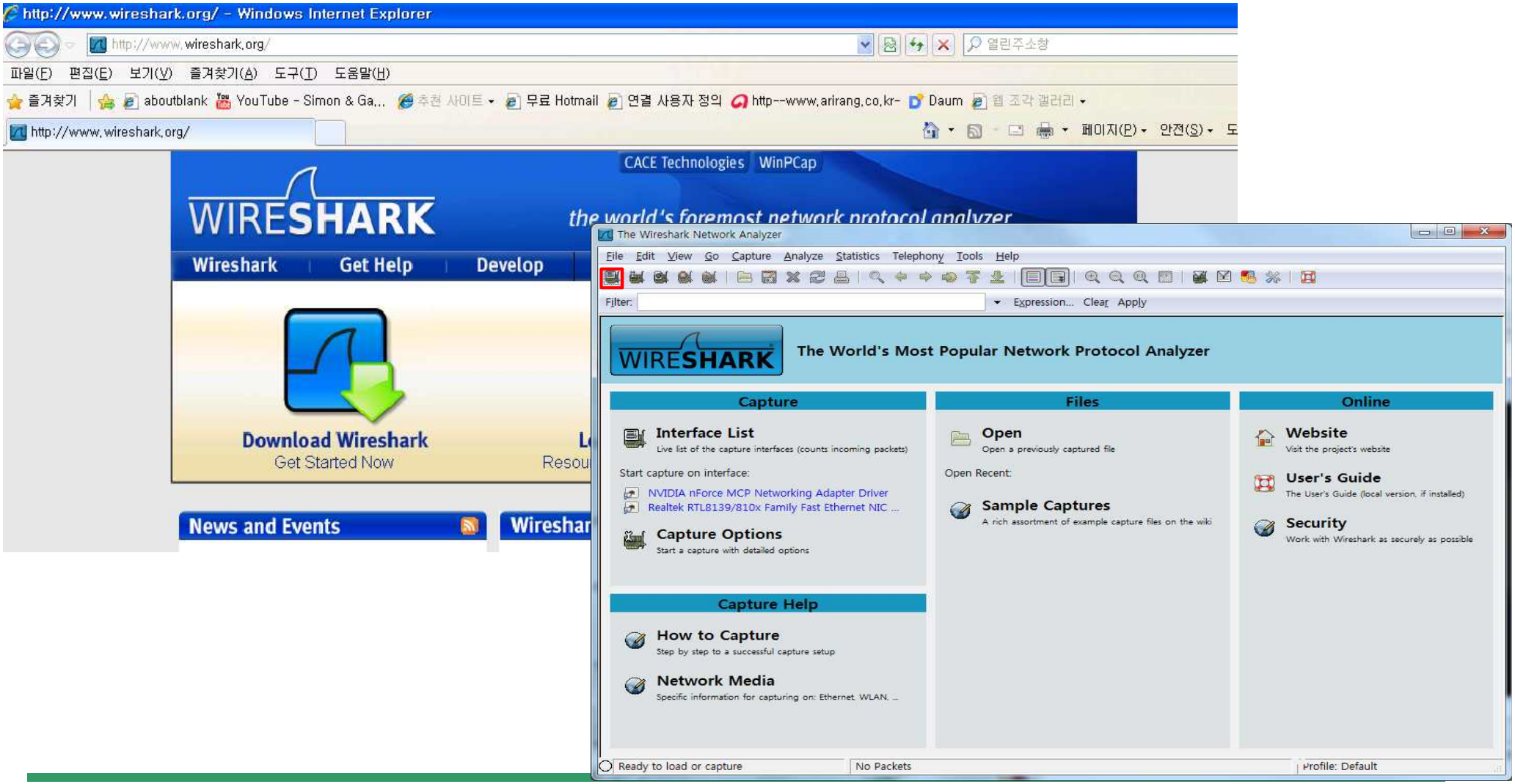
스니핑

- 스니퍼 프로그램을 이용하여 네트워크 상의 데이터를 몰래훔쳐 보는 행위
- 네트워크 카드의 프러미스큐어스(Promiscuous) 모드:
  - 네트워크의 모든 트래픽을 볼 수 있도록 하는 모드
  - 네트워크 카드의 프러미스큐어스 모드를 이용하여 스니핑 수행

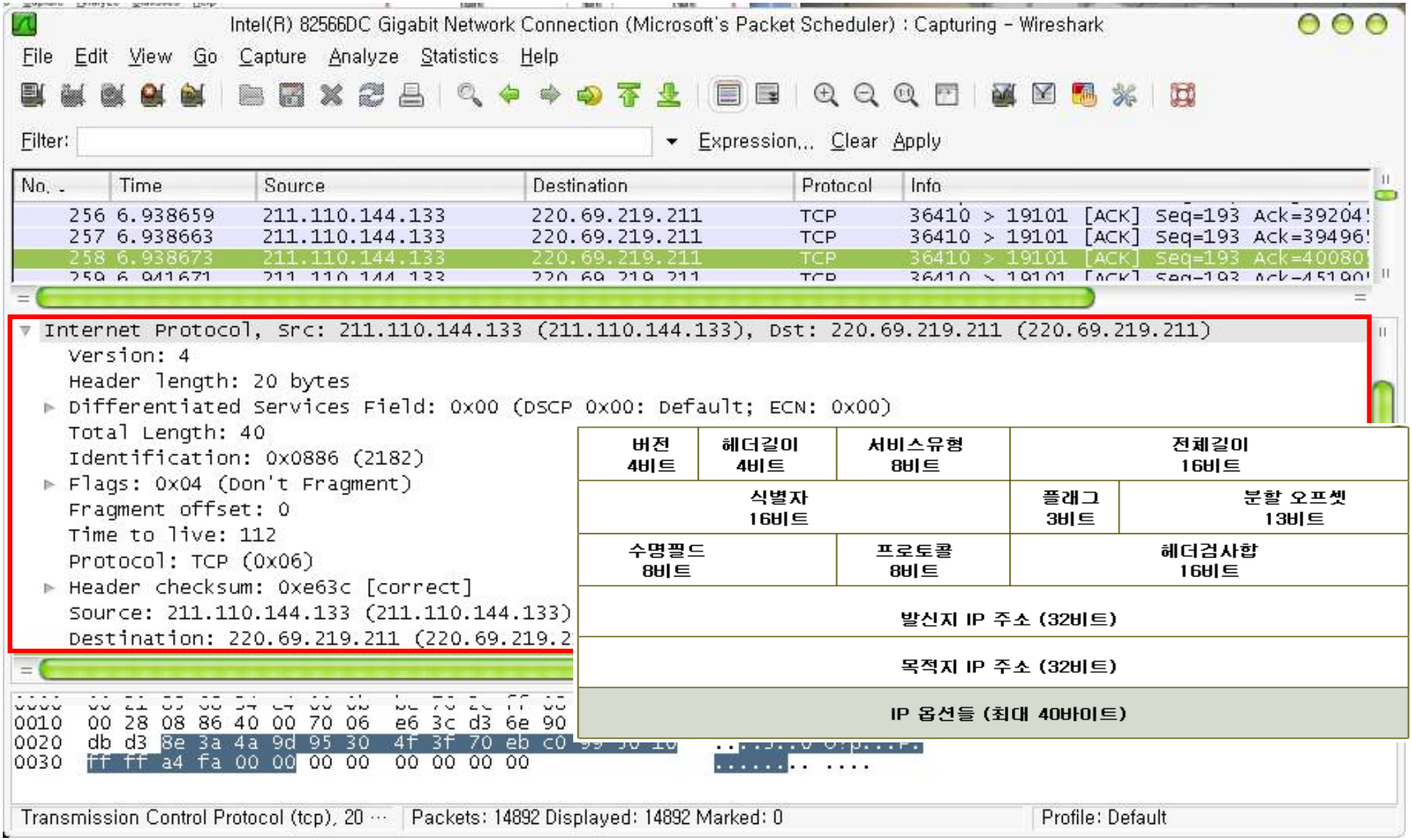


스니핑 툴 – Wireshark

- Wireshark 서버 접속: http://www.wireshark.org/



패킷 분석-IP 패킷



버전 4비트	헤더길이 4비트	서비스유형 8비트	전체길이 16비트
식별자 16비트		플래그 3비트	분할 오프셋 13비트
수명필드 8비트		프로토콜 8비트	헤더검사합 16비트
발신지 IP 주소 (32비트)			
목적지 IP 주소 (32비트)			
IP 옵션들 (최대 40바이트)			

패킷 분석-텔넷(1/2)

No.	Time	Source	Destination	Protocol	Info
94	7.457703	220.69.240.147	220.69.219.226	TCP	51154 > telnet [SYN] Seq=0 Win=8192 Len=0 MSS=1460
96	7.458089	220.69.240.147	220.69.219.226	TCP	51154 > telnet [ACK] Seq=1 Ack=1 Win=64240 Len=0
99	7.471923	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
101	7.472856	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
104	7.477211	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
106	7.516797	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
109	7.517570	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
111	7.557820	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
114	7.558305	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
121	7.756811	220.69.240.147	220.69.219.226	TCP	51154 > telnet [ACK] Seq=75 Ack=120 Win=64121 Len=0
125	8.081443	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
127	8.212948	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
135	8.385772	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
140	8.561916	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
143	8.760814	220.69.240.147	220.69.219.226	TCP	51154 > telnet [ACK] Seq=79 Ack=124 Win=64117 Len=0
156	9.809796	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
158	10.009771	220.69.240.147	220.69.219.226	TCP	51154 > telnet [ACK] Seq=80 Ack=126 Win=64115 Len=0
161	10.209776	220.69.240.147	220.69.219.226	TCP	51154 > telnet [ACK] Seq=80 Ack=136 Win=64105 Len=0
177	10.634893	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
179	10.813301	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
183	10.992105	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
189	11.158842	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
193	11.366780	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
197	11.566756	220.69.240.147	220.69.219.226	TCP	51154 > telnet [ACK] Seq=85 Ack=138 Win=64103 Len=0
200	11.766752	220.69.240.147	220.69.219.226	TCP	51154 > telnet [ACK] Seq=85 Ack=228 Win=64013 Len=0
786	67.483878	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
975	81.627469	220.69.240.147	220.69.219.226	TELNET	Telnet Data ...
978	81.647676	220.69.240.147	220.69.219.226	TCP	51154 > telnet [RST, ACK] Seq=96 Ack=247 Win=0 Len=0

telnet 접속

ID 패킷

PW 패킷

패킷 분석-텔넷(2/2)

❑ ID 패킷의 데이터

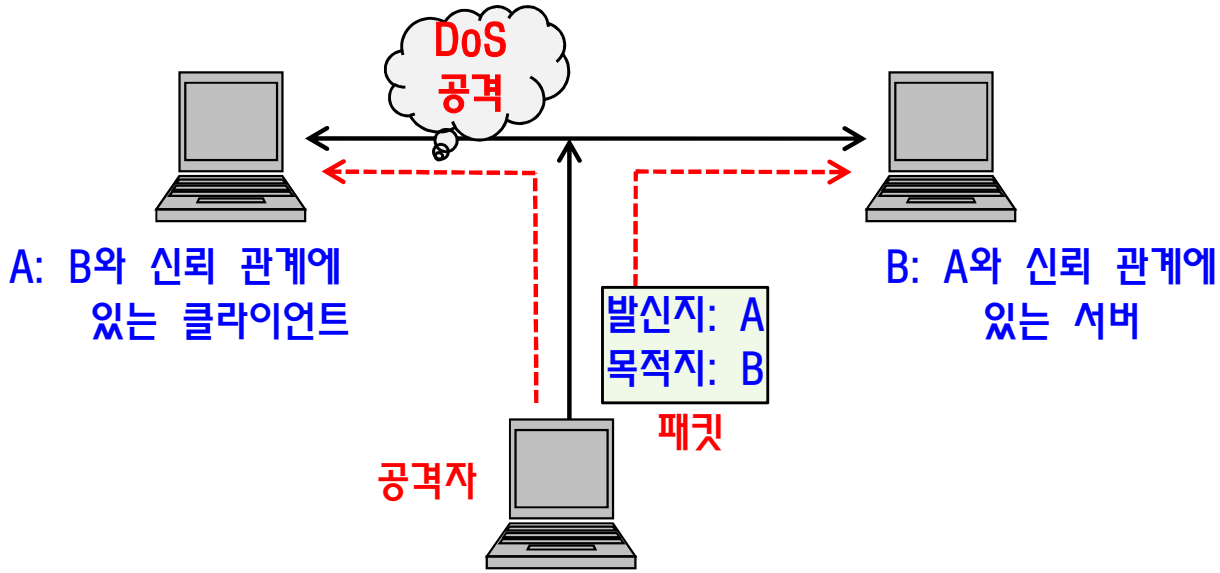
```
⊞ Transmission Control Protocol, Src Port: 51154 (51154), Dst Port: telnet (23), Seq: 75, Ack: 120, Len: 1
⊟ Telnet
    Data: t
⊞ Transmission Control Protocol, Src Port: 51154 (51154), Dst Port: telnet (23), Seq: 76, Ack: 121, Len: 1
⊟ Telnet
    Data: e
⊞ Transmission Control Protocol, Src Port: 51154 (51154), Dst Port: telnet (23), Seq: 77, Ack: 122, Len: 1
⊟ Telnet
    Data: s
⊞ Transmission Control Protocol, Src Port: 51154 (51154), Dst Port: telnet (23), Seq: 78, Ack: 123, Len: 1
⊟ Telnet
    Data: t
```

❑ PW 패킷의 데이터

```
⊞ Transmission Control Protocol, Src Port: 51154 (51154), Dst Port: telnet (23), Seq: 80, Ack: 136, Len: 1
⊟ Telnet
    Data: 1
⊞ Transmission Control Protocol, Src Port: 51154 (51154), Dst Port: telnet (23), Seq: 81, Ack: 136, Len: 1
⊟ Telnet
    Data: 2
⊞ Transmission Control Protocol, Src Port: 51154 (51154), Dst Port: telnet (23), Seq: 82, Ack: 136, Len: 1
⊟ Telnet
    Data: 3
⊞ Transmission Control Protocol, Src Port: 51154 (51154), Dst Port: telnet (23), Seq: 83, Ack: 136, Len: 1
⊟ Telnet
    Data: 4
```

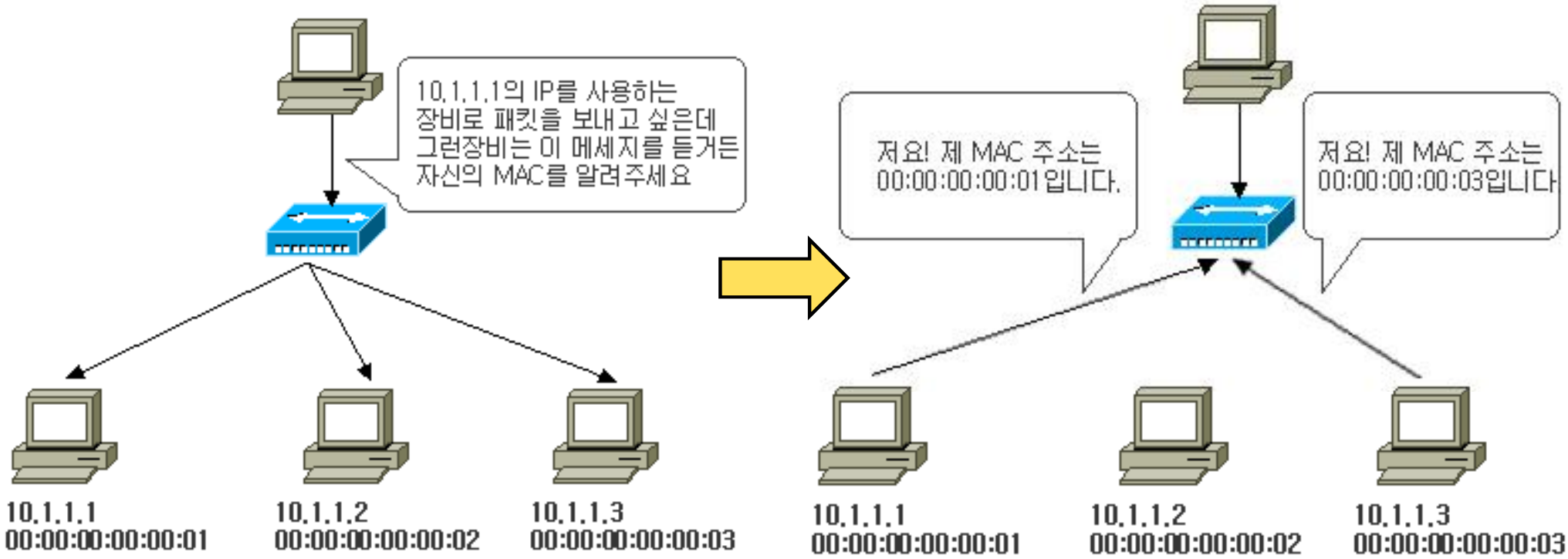
IP 스푸핑

- IP 스푸핑(Spoofing): IP 주소 및 패킷의 내용을 위조 및 변조하여 다른 시스템을 공격
  - 스머프 공격, LAND 공격, UDP 홍수, 과도한 TCP 연결설정 공격, …
  - 트러스트 관계의 서버 클라이언트를 확인 후, 클라이언트를 DoS 공격으로 무력화 시키고 공격자가 클라이언트의 IP 주소로 서버와 통신



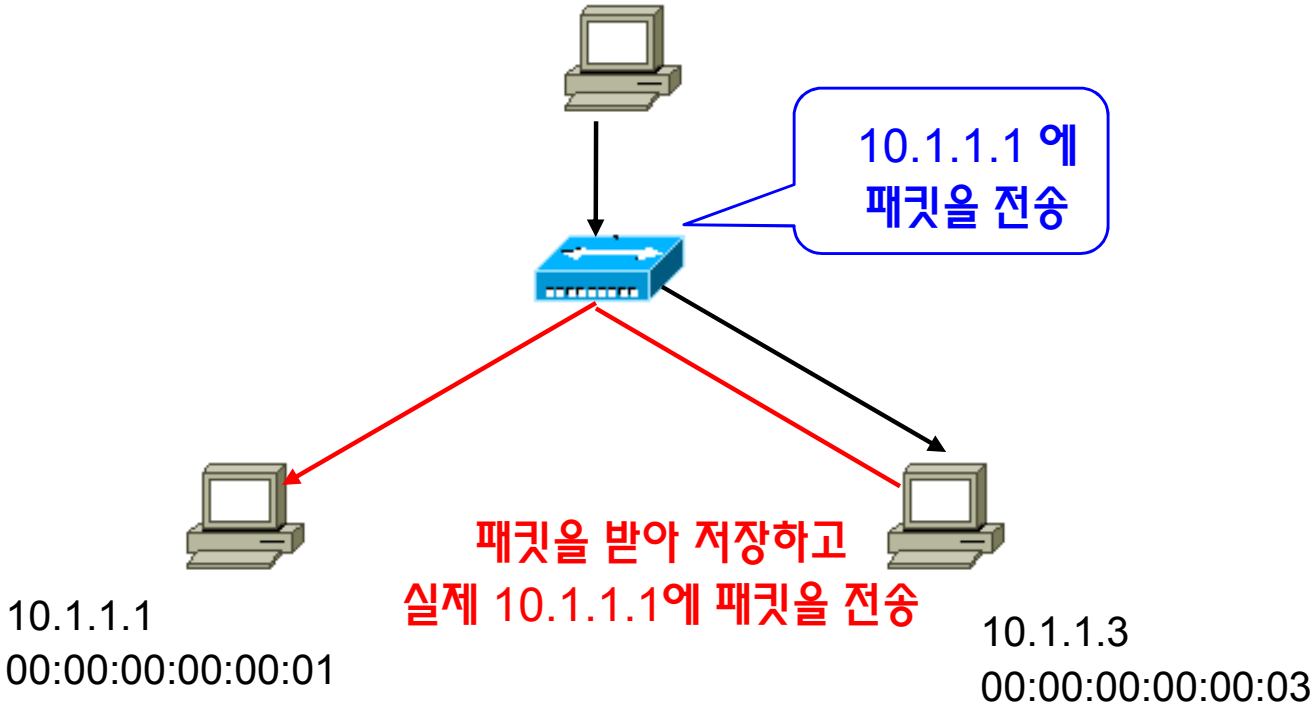
ARP 스푸핑(1/2)

- ARP(Address Resolution Protocol) 프로토콜: 32 비트 IP 주소를 48 비트의 물리주소로 대응시켜 주는 프로토콜
- 공격자는 공격 대상 시스템의 물리주소를 공격자 자신의 물리주소로 위장



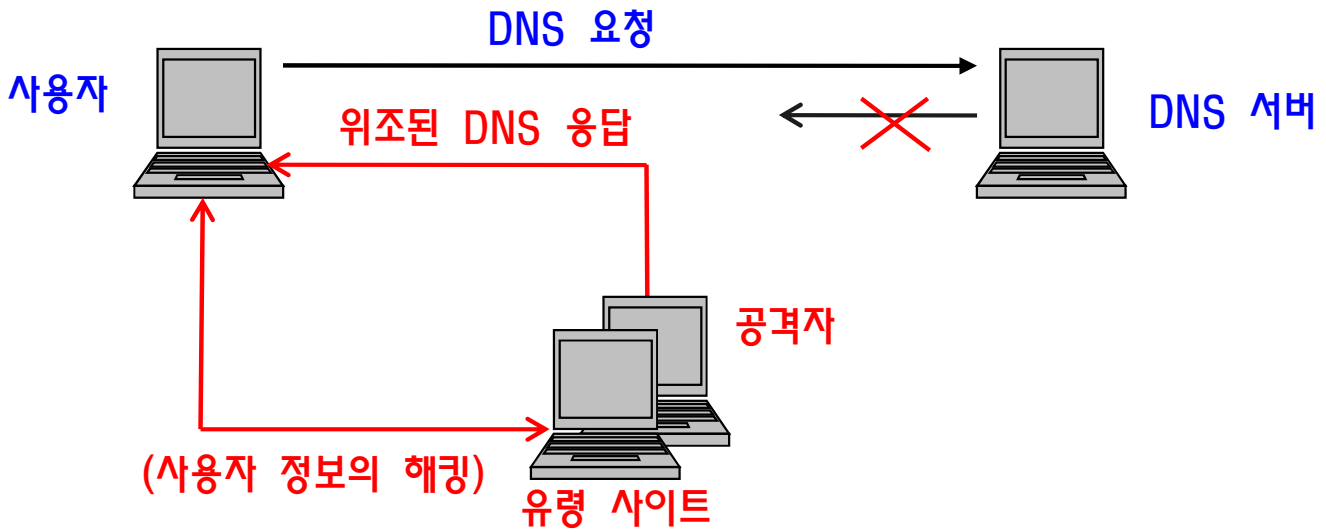
ARP 스푸핑(2/2)

- 공격자는 네트워크에 흐르는 패킷을 수신하여 정보를 훔침 → 실제 목적지로 패킷을 전달하여 스푸핑 및 스니핑을 은닉



DNS 스푸핑

- DNS(Domain Name System) 프로토콜: 도메인 주소를 IP 주소로 대응
- DNS 스푸핑
  - 클라이언트가 도메인 주소에 해당하는 IP 주소를 요청 시→ 공격자는 유령 사이트의 IP 주소를 갖는 위조된 DNS 응답 패킷을 전송
  - 사용자가 원하는 서비스(ex:인터넷 상거래)와 유사하게 만들어진 유령 사이트로 접속을 유도 → 사용자가 입력하는 개인정보를 해킹



패스워드 크래킹(1/2)

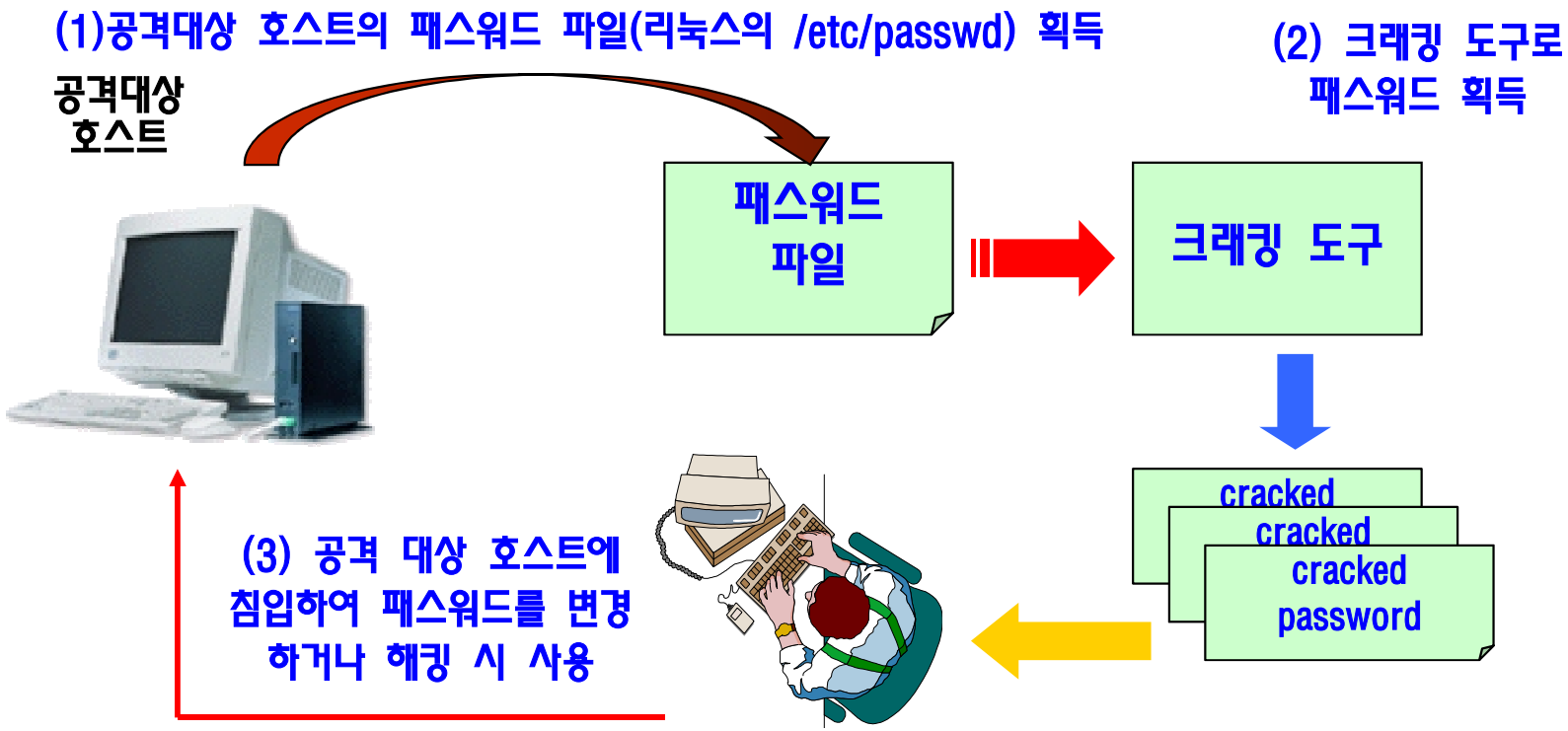
- 대상 프로그램이나 OS 자체를 크래킹하여 패스워드의 확인 단계를 거치지 않는 방법

- 예상되는 ID와 패스워드 목록을 가지고 패스워드를 추측하여 알아내는 방법
  - 목록을 가지고 있는 파일을 이용하는 방법(Brutus AET2)
    - 패스워드의 최소 길이를 설정해 놓지 않으면 무차별 공격에 당하기 쉽다.
    - /etc/login.defs 파일에 PASS_MIN_LEN 8 같이 최소 길이를 명시할 수 있다.
  - 크래킹 프로그램의 소스에 목록이 포함되는 방법

- 패스워드가 저장된 파일을 획득하여 패스워드를 알아내는 방법

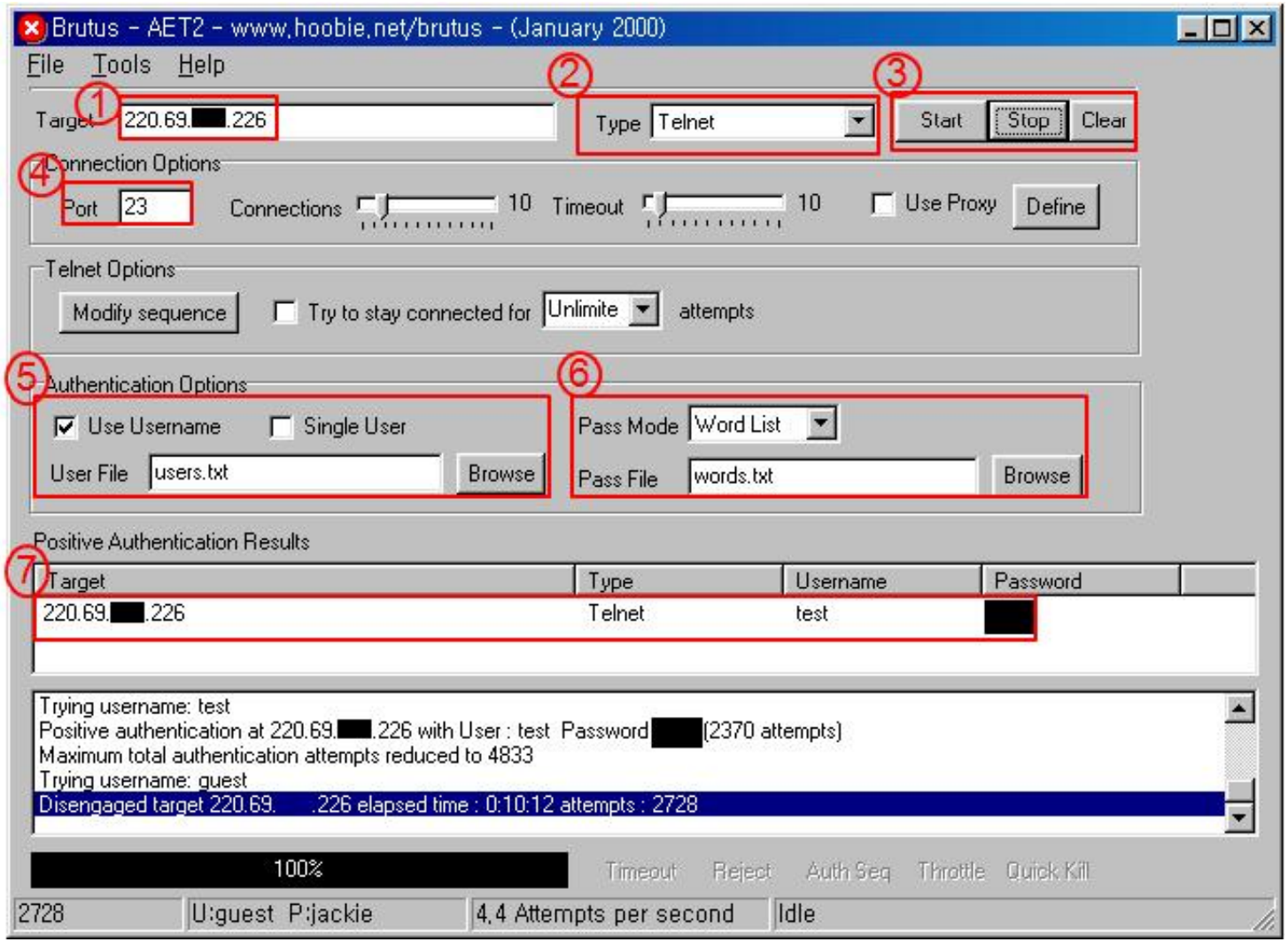
패스워드 크래킹(2/2)

- 패스워드가 저장된 파일을 획득하여 패스워드를 알아내는 방법



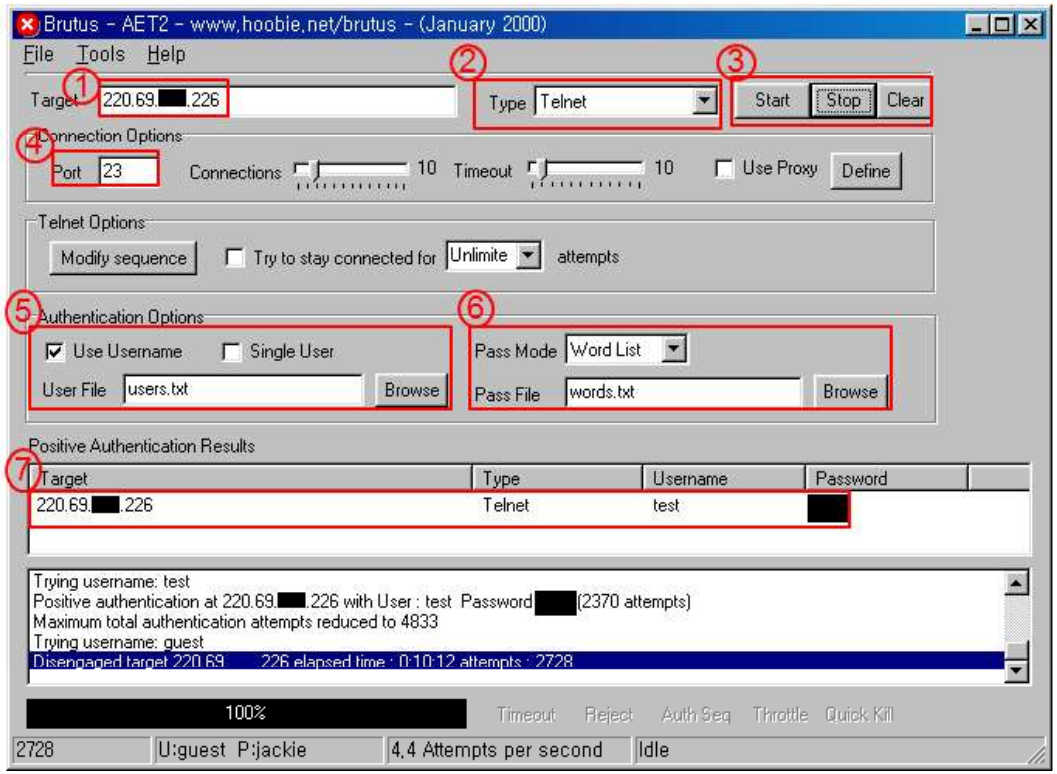
패스워드 크래킹 툴 – Brutus AET2(1/2)

- 예측되는 ID와 PW 조합을 이용하여 무차별 접속 시도를 하여 크래킹



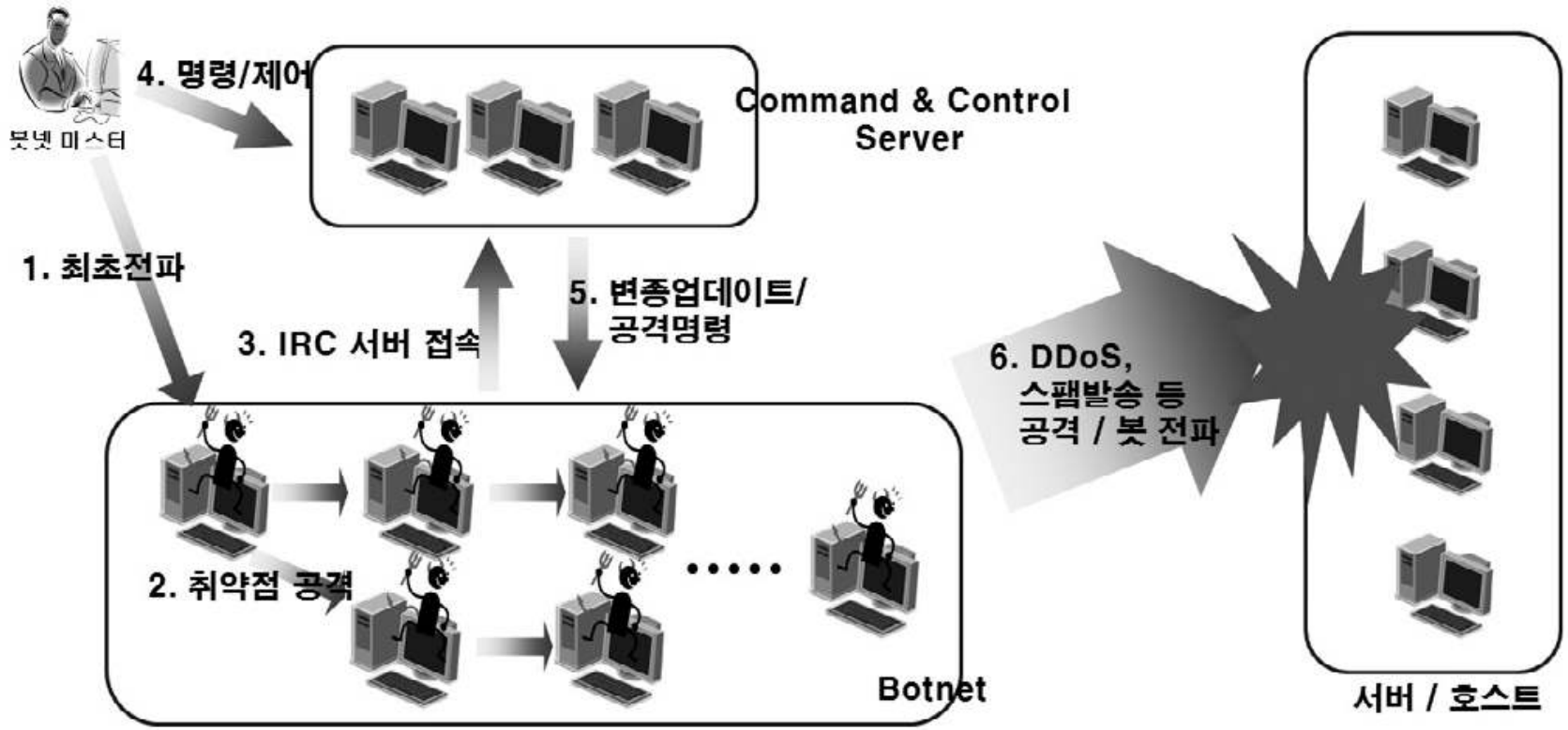
패스워드 크래킹 툴 – Brutus AET2(2/2)

① 공격 대상 시스템의 주소를 적는 곳
② 공격할 대상 서비스(Http, Telnet, Ftp 등) 선택
③ 툴의 시작 및 종료 버튼
④ 공격할 대상 서비스의 포트 번호
⑤ Users.txt : 예측되는 사용자 ID들의 목록 파일
⑥ Words.txt : 예측되는 PW들의 목록파일
⑦ 무작위 추출법으로 찾아 낸 공격 대상 시스템의 ID와 PW



봇넷(Botnet)(1/2)

- 봇넷: 악성소프트웨어인 봇(Bot)에 감염된 컴퓨터들이 네트워크로 연결되어 있는 형태
- 봇은 웜/바이러스, 백도어, 스파이웨어 등의 다양한 악성코드들의 특성을 통합적으로 지니며, 봇넷을 통해 DDoS, Ad-ware, Spyware, 스팸발송, 정보불법 수집과 같은 대부분의 사이버 공격이 가능



봇넷(Botnet)(2/2)

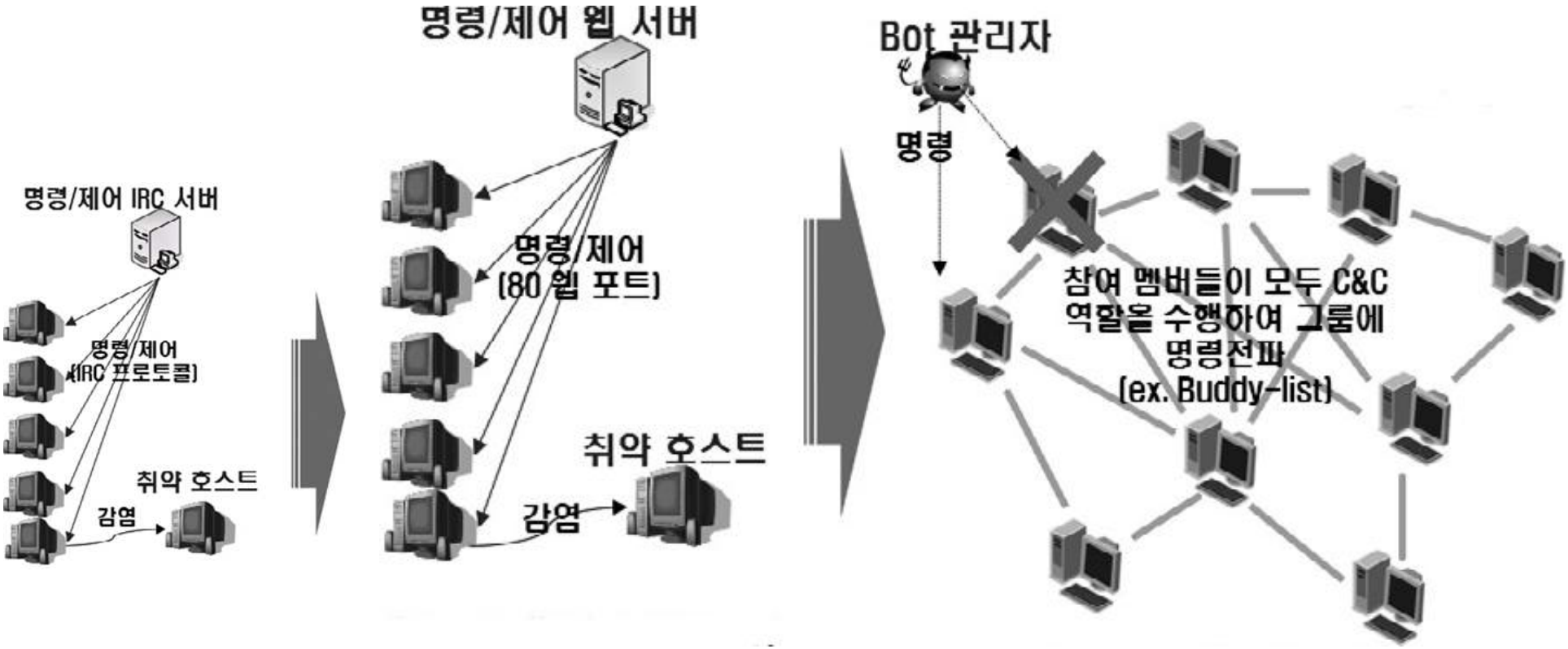
- 1993년 EggDrop으로 처음 나온 이후 DDoS와 더블어 가장 심각한 공격 유형으로 선정됨(Arbot, Networks, 2007)
  - EggDrop(http://www.eggheads.org/)은 가장 유명한 IRC 봇(EggDrop 1.6.21, 2011.8) 중의 하나

- 2007년 2월 미국의 루트 서버 2개가 봇넷을 통한 DDoS 공격으로 5시간 동안 서비스 장애 발생 -> 트래픽의 61%가 한국에서 발생
  - 초고속 인프라가 잘 갖추어진 한국은 봇넷 감염지로 선호되는 지역

- TCP/IP 프로토콜의 공동 창시자인 Vint Cerf: 전 세계 컴퓨터의 약 11%인 1억 5천 만 대 정도의 컴퓨터가 봇 악성코드에 감염되어 좀비 PC로 공격에 사용될 것으로 예상
  - 가장 큰 봇넷 중의 하나인 Storm 봇넷에는 230,000개의 좀비들이 연결되어 있음

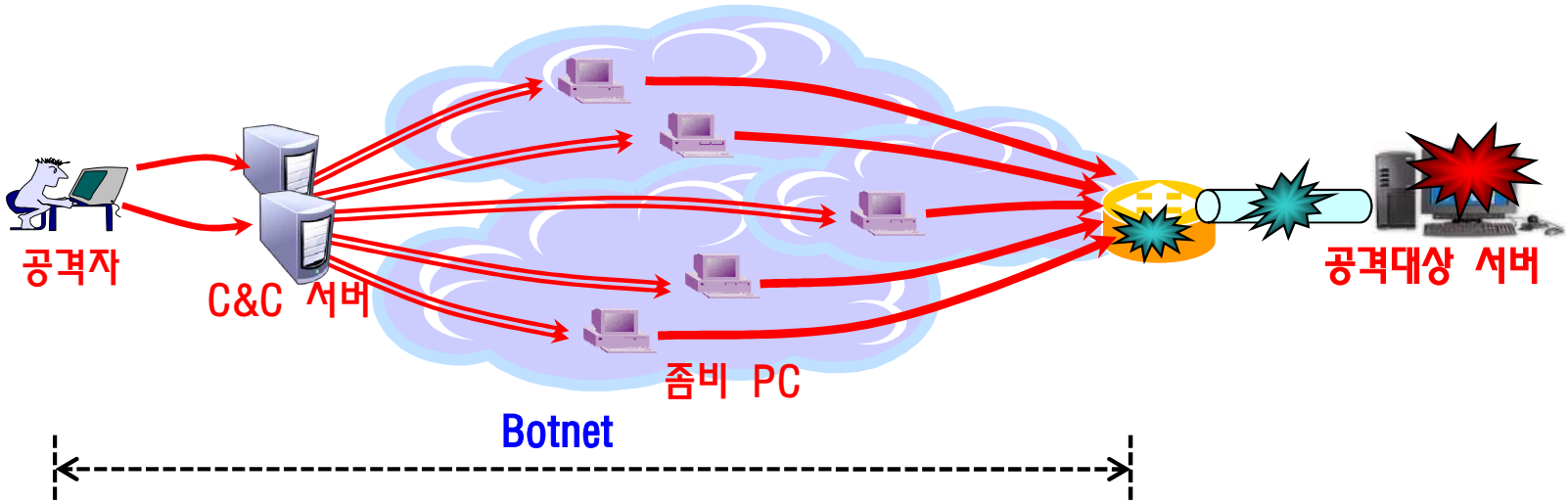
봇넷의 진화

- C&C 기반의 중앙집중형 제어 방식: 널리 사용되는 IRC(Internet Relay Chat)의 특성을 이용한 IRC 봇넷(Rbot)에서 탐지 및 대응을 보다 어렵게 하기 위하여 웹 서버를 해킹하여 C&C 서버로 악용하는 HTTP 기반의 봇넷(Robax)으로 진화
- 중앙 집중형에서 모든 좀비 PC들이 C&C가 될 수 있는 분산제어 방식(Storm)으로 진화



서비스 거부 공격(1/2)

- 서비스 거부(DOS: Denial of Service) 공격
  - 공격자가 시스템의 자원(예, 메모리, 테이블, 지원하는 연결의 수,…)을 모두 사용하거나 파괴함으로 다른 사용자들이 시스템의 서비스를 더 이상 사용할 수 없도록 만드는 공격
  - 분산 서비스 거부 공격(DDoS): 지역적으로 분산된 여러 좀비 시스템에 의한 공격



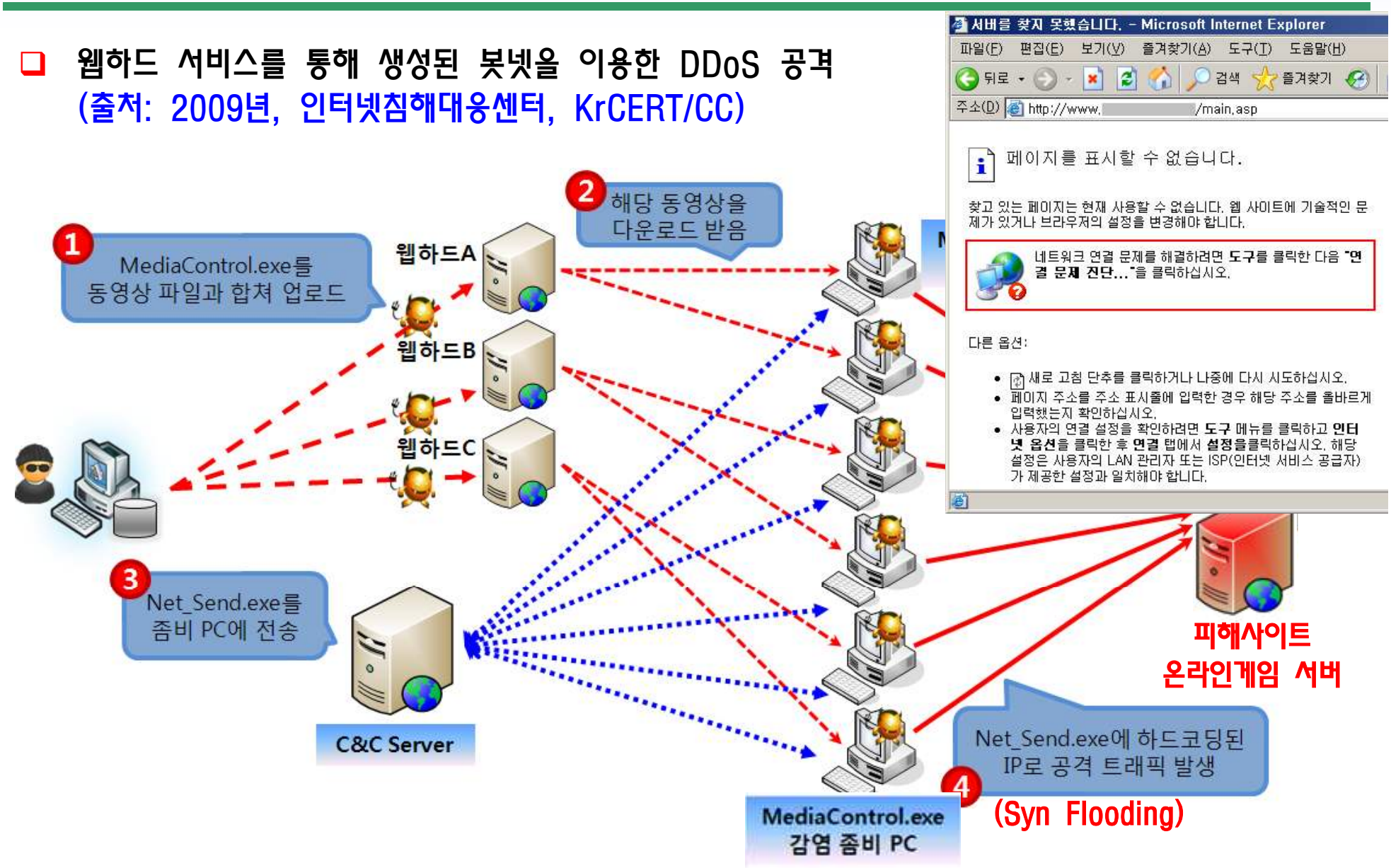
서비스 거부 공격(2/2)

- 헤더 검사합의 취약성을 이용한 서비스 거부 공격
  - 스머프(Smurf) 공격, LAND 공격, UDP 홍수(flood),
  - 동일 착.발신 주소/포트를 갖는 패킷 공격, 과도한 TCP 연결설정(TCP Syn) 공격, …

- DDoS의 대표적 사례
  - 7.7 DDoS(분산 서비스 공격) 대란: 2009년 7월 7일을 기점으로 한국과 미국 등의 주요 정부기관, 포털사이트, 은행 사이트 등의 DDoS 공격으로 서비스의 일시적인 마비 발생
  - 2002년 10월 22일과 2007년 2월 6일의 DNS 루트 서버에 대한 DNS 백본 DDoS 공격: 인터넷 URL 주소 체계를 무력화

DoS 피해 사례

- 웹하드 서비스를 통해 생성된 봇넷을 이용한 DDoS 공격
  (출처: 2009년, 인터넷침해대응센터, KrCERT/CC)



요점정리(1/2)

- 백도어: 해커가 차후 접속을 위해 시스템에 심어 놓은 프로그램
  - 유닉스 계열의 백도어: 패스워드 크래킹 백도어, Rhosts + + 백도어, Login 백도어, Telnetd 백도어, …
  - 윈도우 계열의 백도어: 백오리피스(Back Orifice), NetBus, SubSeven, …
- 스니핑: 스니퍼 프로그램(Wireshark)을 이용하여 네트워크 상의 데이터를 몰래훔쳐 보는 행위
- 스푸핑(Spoofing): 내용을 위조 및 변조하여 다른 시스템을 공격
  - IP 스푸핑: 스머프 공격, LAND 공격, UDP 홍수, 과도한 TCP 연결설정 공격, …
  - ARP 스푸핑
  - DNS 스푸핑

요점정리(2/2)

- 패스워드 크래킹
  - 대상 프로그램이나 OS 자체를 크래킹하여 패스워드의 확인 단계를 거치지 않는 방법
  - 예상되는 ID와 패스워드 목록을 가지고 패스워드를 추측하여 알아내는 방법(Brutus AET2)
  - 패스워드가 저장된 파일을 획득하여 패스워드를 알아내는 방법

- 봇넷: 악성소프트웨어인 봇(Bot)에 감염된 컴퓨터들이 네트워크로 연결되어 있는 형태
  - 봇은 웜/바이러스, 백도어, 스파이웨어 등의 다양한 악성코드들의 특성을 통합적으로 지니며,
  - 봇넷을 통해 DDoS, Ad-ware, Spyware, 스팸발송, 정보불법 수집과 같은 대부분의 사이버 공격이 가능

- 서비스 거부(DOS) 공격:공격자가 시스템의 자원을 모두 사용하거나 파괴함으로 다른 사용자들이 시스템의 서비스를 더 이상 사용할 수 없도록 만드는 공격
  - 분산 서비스 거부 공격(DDoS): 지역적으로 분산된 여러 좀비 시스템에 의한 공격