리눅스 보안 관리

(Linux 사용법 및 활용 I)

유닉스 보안 개요

- 보안 위협의 유형
  - 비 인가된 물리적 접근
  - 계정 도용
  - 파일 시스템의 비밀성 및 무결성 침해
  - 비 인가된 네트웍 접근
- 물리적 보안
  - 컴퓨터 열쇠
  - CMOS 암호
  - Boot loader 암호
  - xlock, vlock
- 계정 보안
- 파일 시스템 보안
- 네트워크 보안

물리적 보안

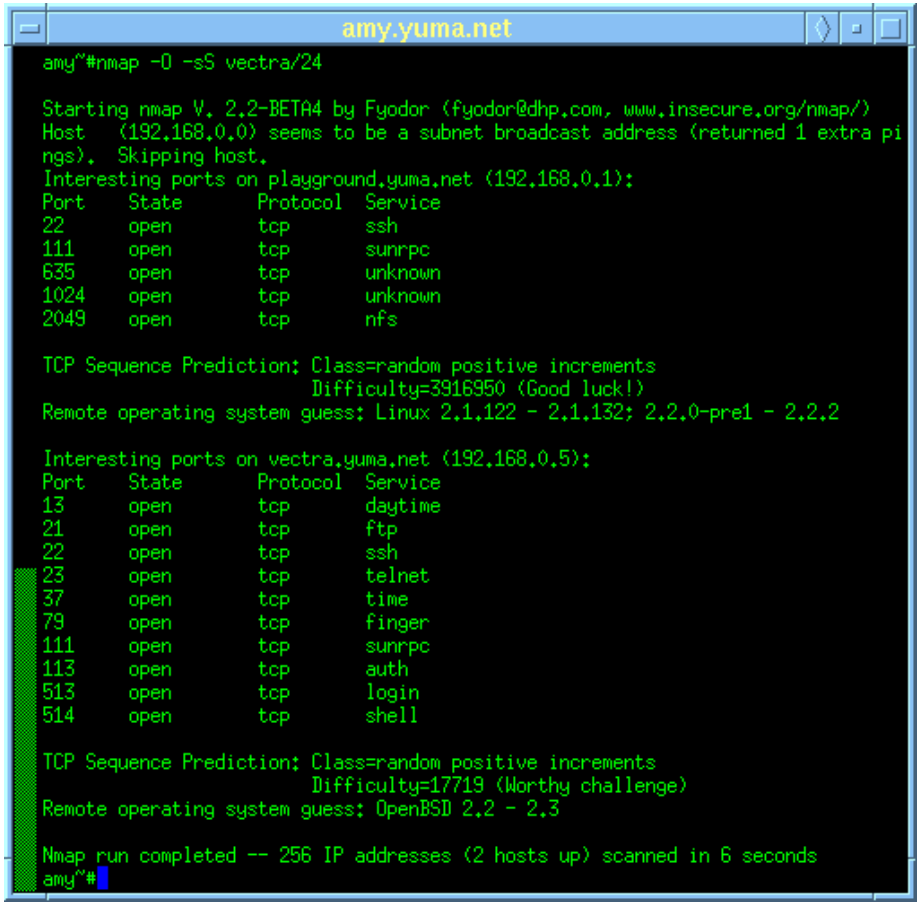
- **Boot loader 암호**
  - boot: linux single 부팅 시 root 권한 획득
  - /etc/lilo.conf 수정 (다음의 내용을 추가)
    - restricted
    - password=*pickyourpassword*
  - /etc/lilo.conf 수정 후 /sbin/lilo 실행
- **Login timeout 설정**
  - ~/.bashrc 또는 ~/.bash_profile에 TMOUT=*nn* 삽입
- **Logout시 화면 정리**
  - ~/.bash_logout에 clear 추가
- **xlock, vlock 이용**

정보 수집 (OS)

- 공격 목표의 OS 추측
  - ftp, telnet, http를 이용한 고전적 방법
  - TCP/IP fingerprint 이용 : nmap, queso
- OS 추측 방지
  - 고전적 방법에 대한 방지
    - /etc/inetd.conf 내용 수정
    - /usr/sbin/in.telnetd -h
  - nmap, queso 대응
    - 커넬 패치 이용
    - http://www.innu.org/~sean/

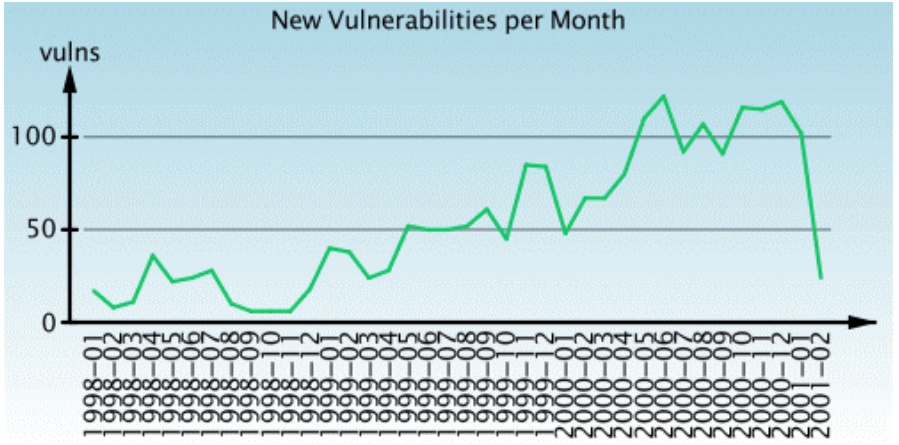
정보 수집 (Port scan)

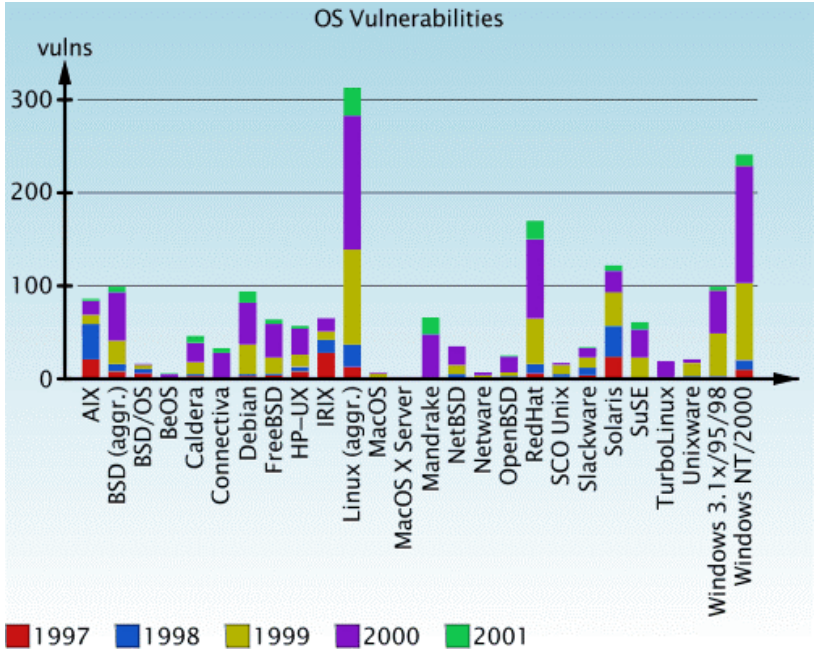
- 침투할 **Port** 및 버전 확인
  - nmap, strobe, nc
  - 침입에 사용할 ID 도용
  - 사용할 exploit 확정
- **Port scan** 대응책
  - 불필요한 서비스 제거
  - finger, telnet, login 등
  - /etc/inetd.conf 수정
  - 해당 서비스 #로 주석처리
  - snort : port scan detector



Exploits

- **Exploit**
  - 보안 취약점을 이용한 공격
  - remote/local attack으로 분류
  - 보안 포탈 사이트나 인터넷 상에서 쉽게 획득 가능
- 대응책
  - 빠른 보안 패치
  - 네트워 관련 서버 설정
  - 불필요한 계정 사용 금지
  - 커넬 업데이트





계정 보안

- 계정 보안 위협 및 취약점
  - 암호 관리 소홀
    - 암호 없는 계정
    - 추측 가능한 암호 사용
    - 장기간 사용하지 않는 계정
  - 암호 크랙
    - 사전 파일을 이용한 공격: ntucrack, John the Ripper
    - 무차별 공격 (Brute-force attack)
  - 네트워크 도청: tcpdump, snort, sniffit, ethereal

계정 보안

- **Shadow password 사용**
  - /etc/passwd 파일은 모든 사용자에게 읽기 가능
  - 암호 크래킹을 방지하기 위해 암호만 /etc/shadow에 보관
- **MD5 암호 사용**
  - 표준 DES 암호화 대신에 MD5 암호화 사용
  - /etc/pam.d/login과 /etc/pam.d/passwd 파일 수정
    - password required pam_unix.so nullok obscure min=4 max=8 md5
    - min과 max의 숫자를 높은 수를 이용함
- 사전 파일을 이용한 암호 크랙 방지
  - cracklib을 이용한 사용자 암호 검증
  - otp, makepasswd 등을 이용한 일회용 랜덤 암호 생성

계정 보안

- **root 계정 접속 제한**
  - /etc/securetty를 이용하여 root의 접속 제한
  - /etc/pam.d/login에 다음 내용 추가
    - auth requisite pam_securetty.so
- **특정 위치로부터의 특정 계정 및 그룹 접속 제한**
  - /etc/pam.d/login에 다음 내용 추가
    - account required pam_access.so
  - /etc/security/access.conf 내용 수정
    - -:wheel:ALL EXECEPT LOCAL .win.tue.nl
    - Local 또는 *.win.tue.nl 이외의 장소로부터의 wheel 그룹 멤버 접속 차단
- **접속 시간 제한**
  - /etc/pam.d/login과 /etc/security/time.conf 수정

계정 보안

- **chroot와 shell을 이용한 보안**
  - chroot를 이용한 shell jail
    - http://www.aarongifford.com/computers/chrsh.html
  - rbash (restricted bash)를 통한 제한
    - 상위 디렉터리로의 이동 불가
    - 일부 환경 변수의 변경 불가
    - redirection 제한
  - 불필요한 계정의 shell 항목 수정 및 삭제
    - root:x:0:0:root:/root:/bin/csh
    - xfs:x:101:234:X Font Server:/etc/X11/fs:/bin/false
    - ftp:x:14:50:FTP User:/home/ftp:

계정 보안

- **Resource 제한**
  - local DoS 방지
  - /etc/pam.d/login에 아래 내용 추가
    - session required pam_limits.so
  - /etc/security/limits.conf 내용 수정
    - core, rss, nproc 제한 필수
- **Super user 사용자 제한**
  - /etc/pam.d/su에 아래 내용 추가 또는 # 제거
    - auth sufficient pam_rootok.so
    - auth required pam_wheel.so group=wheel
  - wheel 그룹 생성
    - groupadd wheel
  - su 명령어 사용자 등록
    - usermod –G wheel *username*

계정 보안

- **sudo 사용자 및 명령어 설정**
  - 특정 일반 사용자에게만 특정 명령어만 root 권한으로 실행시킬 권한 부여
  - Shell로 빠질 수 있는 명령어의 경우 sudo 명령어 등록에서 제외
    - bash, csh, vipw, vigr, visudo, more
  - visudo 명령어로 /etc/sudoers 파일 수정
    - User_Alias FULLTIMERS = millert, mikef, dowdy
    - Host_Alias SERVERS = master, mail, www, ns
    - Cmnd_Alias SHUTDOWN = /usr/sbin/shutdown
    - FULLTIMERS SERVERS = NOPASSWD: SHUTDOWN

파일 시스템 보안

- 파일 시스템 보안 위협 및 취약점
  - 파일 및 디렉토리 소유권 및 허가권 설정 오류
  - root 소유의 SUID 프로그램의 보안 허점
    - race condition
    - buffer overflow
    - heap overflow
    - format string bug
  - 소프트웨어 설치 및 구성 설정 오류
    - ftp, http, sendmail, bind
    - NFS(Network File System)

파일 시스템 보안

- 파일 및 디렉터리의 소유권 및 허가권
  - 소유권 : 어떤 사용자나 그룹이 노드나 상위 노드의 허가권에 대한 조정을 할 수 있는 권한
    - user(u), group(g), other(o)
  - 허가권 : 특정 종류의 액세스가 가능하도록 정해주거나 변경할 수 있는 비트
    - read (r), write(w), execute(x)
  - 특수 목적용
    - sticky bit(t/T)
    - SUID/SGID (s/S)

파일 시스템 보안

- **SetUID/SetGID**
  - 일반 사용자에게 필요에 의해 잠시 특권을 부여할 경우 사용
    - 프로세스 생성 및 실행 시
    - 파일 및 디렉토리 생성 및 접근 시
      - passwd, chsh, chfn
        - /etc/passwd나 /etc/shadow 파일을 수정하기 위해서
      - su, sudo, mount, umount, ping, sendmail, traceroute, at, lpr
    - SUID가 설정된 프로그램을 실행시킬 경우 이 프로그램을 실행시키는 동안은 파일 소유자의 권한을 획득
    - 파일 소유자가 root인 SUID 프로그램은 backdoor, race condition, buffer overflow, format string bug등을 이용한 공격 대상
      - # find / -user root –perm –4000 –exec ls –l {} \; 2> /dev/null | more

파일 시스템 보안

- 파티션 분할
  - root 파티션 한 개만을 두는 것은 HDD 리소스 DoS의 취약점이 됨
- **/etc/fstab**을 이용한 파일 시스템 보안
  - /tmp, /var/tmp같은 디렉터리에는 noexec, nosuid 옵션 추가
    - 대부분의 exploit들이 /tmp와 같은 디렉터리에 실행 파일 생성
    - 실행 자체를 못하게 함으로서 exploit을 실행을 방지
  - Quota 설정
    - 사용자 또는 그룹 별로 하드 디스크의 사용량을 제한
    - 커넬 컴파일시
      - Quota support (CONFIG_QUOTA) [n] y
    - /etc/fstab에 해당 파티션에 usrquota 또는 grpquota 추가
    - 해당 파티션의 root에 quota.user, quota.group 파일 생성
    - edquota로 사용자별 또는 그룹별 사용량 기록

파일 시스템 보안

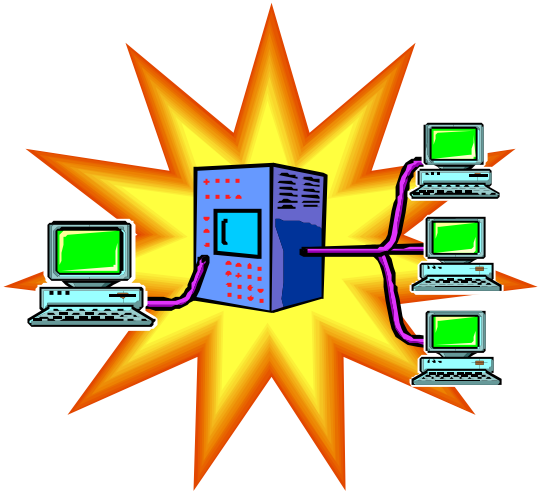
- **umask**를 이용한 파일 기본 퍼미션 조정
  - umask 077로 설정함으로써 본인 이외에는 다른 사람들은 파일을 읽을 수 없도록 설정
- 삭제된 파일 복원 방지
  - MFM(Magnetic Force Microscopy)에 의한 데이터 복원 방지
  - wipe와 같은 프로그램 이용하여 삭제
- **chattr**을 이용한 파일 수정 방지
  - ext2 파일 시스템에서만 적용
  - chattr +i *filename*

파일 시스템 보안

- 파일 시스템 보안 강화 대책
  - 주기적인 파일 시스템 무결성 검사
    - find, diff, cmp, strings, grep
      - root 소유의 SUID 파일 찾기
      - 기존의 파일과 신규 파일 간의 변화된 내용
      - 파일 내에서 특정 문자열 찾기
    - tripwire
      - 모든 파일에 대해서 MD5 메시지 다이제스트 생성
      - 파일 속성의 변화에 대하여 보고
  - 시스템 보안 취약점 및 보안 패치
  - 파일 시스템 암호화
    - CFS, TCFS, SFS, VS3FS
  - 파일 시스템 백업 및 복구
    - tar, dd, resotre

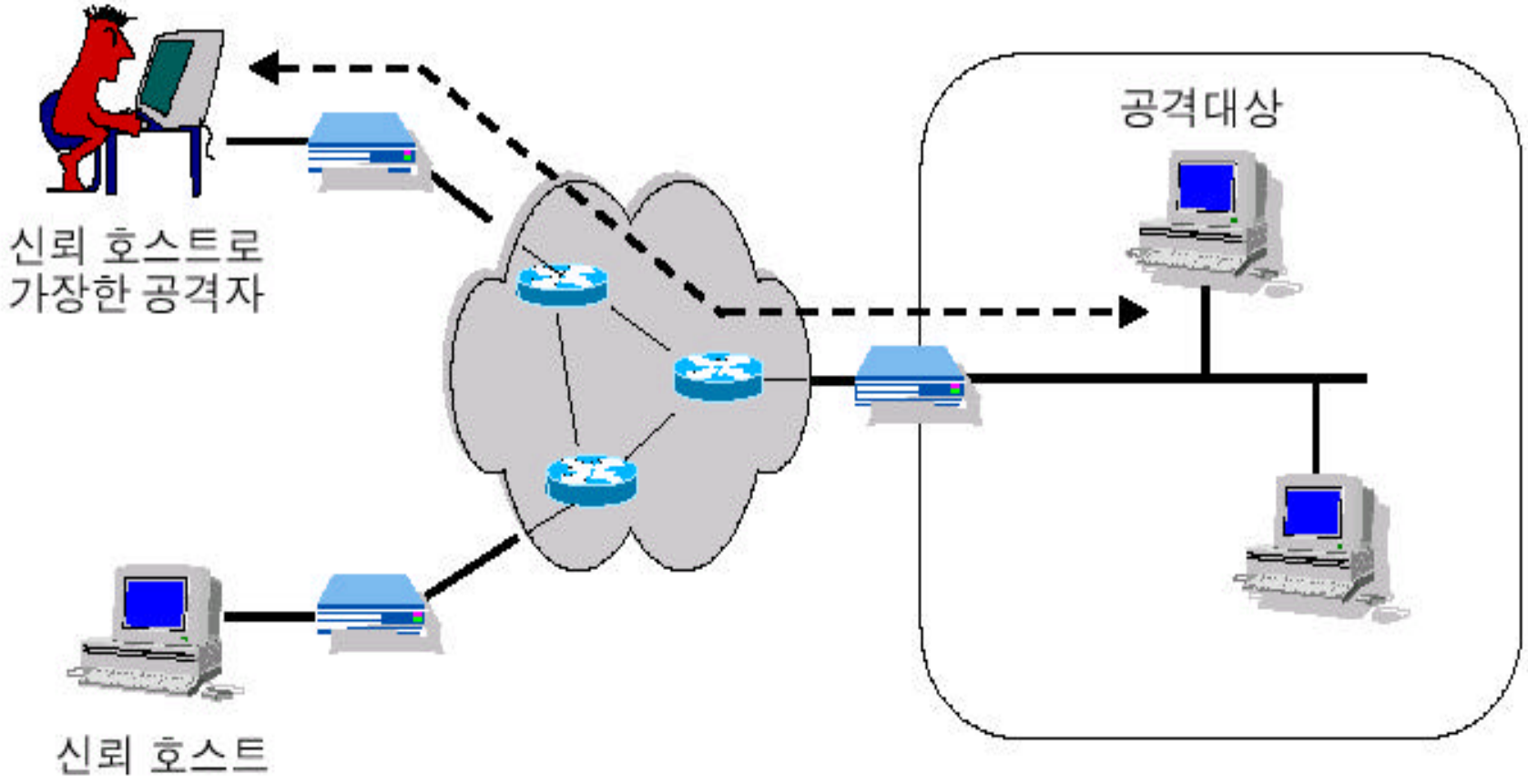
네트워크 보안

- 네트워크 보안 위협 및 취약점
  - 중요 시스템의 정보 노출
    - Network sniffing
    - Port scanning, OS detection, Remote vulnerabilities scanning
    - NFS 및 NIS 서비스 정보 수집
  - 네트워크 서버 공격
    - IP spoofing & session hijacking
    - ftp, http, sendmail, dns
      - Remote buffer overflow
  - 우회 접근
    - Backdoors, Reverse telnet, Bounce attack
  - DoS, DDoS 공격
    - Ping-of-Death, SYN flooding



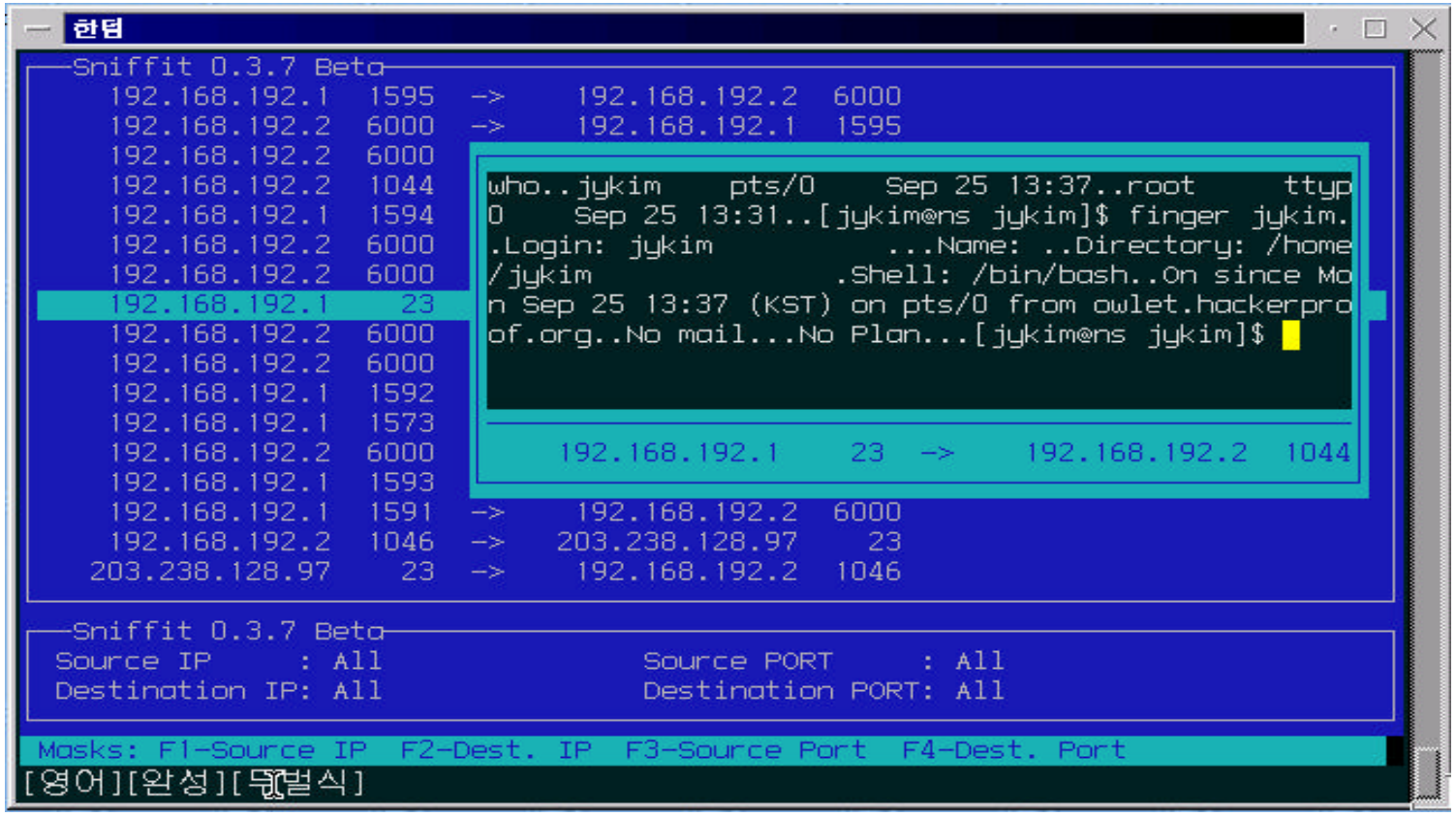
네트워크 보안

- **IP Spoofing & Session Hijacking**



네트워크 보안

- **sniffit을 이용한 암호 도청**



네트워크 보안

- **DoS/DDoS(Distributed Denial of Service)**
  - 여러 대의 컴퓨터가 한대의 서버를 공격하여 서비스를 하지 못하도록 방해하는 공격방법.

Victims in mid-February 2000

- Yahoo
- CNN Interactive
- Amazon.Com
- eBay
- Datek Online
- E*Trade
- ZDNet
- Buy.com

네트워크 보안

- 포트 및 서비스 확인
  - netstat –a | grep LISTEN | more
  - lsof | grep *portnumber* | more
- 서비스 제한
  - 필요 없는 서비스는 모두 제거 또는 서비스 명 앞에 # 삽입
  - /etc/inetd.conf 파일 수정
    - echo, chargen, daytime, discard, time 등 제거
    - finger - ID와 개인 신상 정보의 유출
    - telnet, ftp, talk, ntalk, auth, login, shell, imap, pop3 등 필요 없는 것은 전부 제거
  - /etc/init.d/inetd restart

네트워크 보안

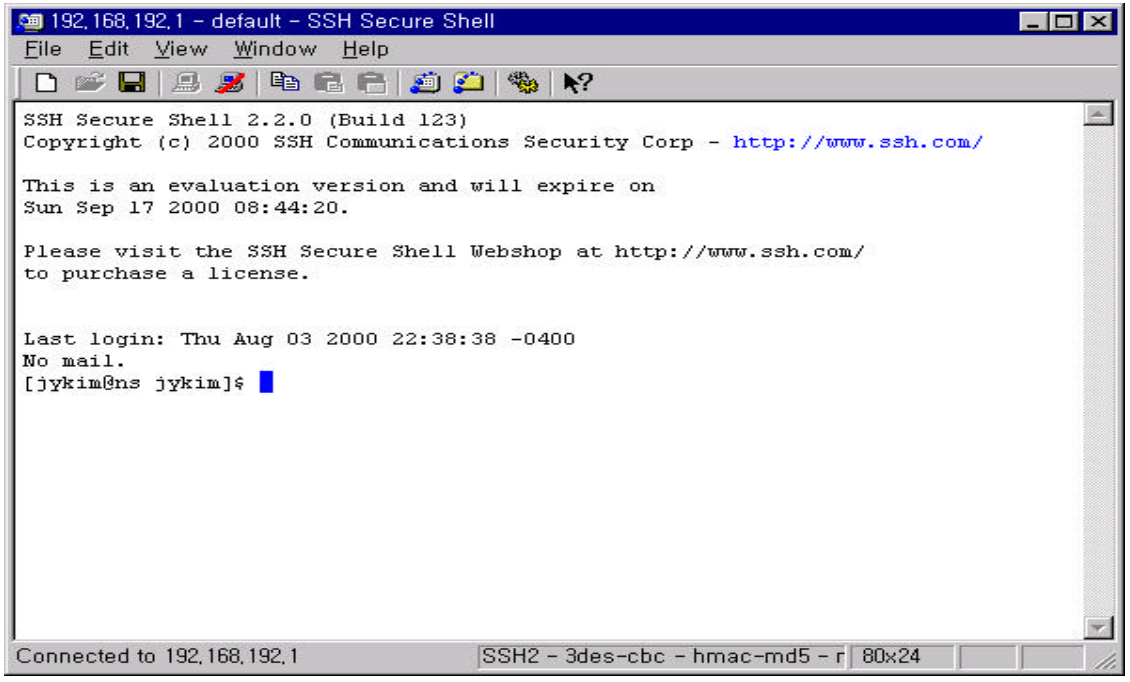
- **tcp wrapper를 이용한 서비스 접근 통제**
  - 호스트/네트워크 수준의 서비스 접근 통제
  - /etc/hosts.allow
    - 접근을 허용할 서비스와 호스트의 주소를 기록
    - in.fingerd, in.telnetd : 192.168.192.
  - /etc/hosts.deny
    - 접근을 거부할 서비스와 호스트의 주소를 기록
    - ALL : PARANOID
      - 모든 서비스에 대해서 호스트의 이름과 주소가 일치하지 않을 경우 서비스 거부
    - in.fingerd, in.rlogind, in.telnetd, in.ftpd: ALL : spawn (/usr/sbin/safer_finer –l @h \ | /bin/mail –s %d=%h root)&

네트워크 보안

- **IP spoofing 방지**
  - /etc/host.conf에 아래 내용 추가
    - nospoof on
  - /etc/network/options에서 아래 내용으로 수정
    - spoofprotect=yes
  - /etc/sysctl.conf에 아래 내용 추가
    - net/ipv4/conf/all/rp_filter=1
  - ipchain을 이용한 방법
    - # rules for standard unroutables
      - ipchains –A input –i eth0 –s 255.255.255.255/32 –b –j DENY
      - ipchains –A input –i eht0 –s 127.0.0.0/8 –b –j DENY
    - # rules for private(RFC1918) addresses
      - ipchains –A input –i eth0 –s 10.0.0.0/8 –b –j DENY
      - ipchains –A input –i eth0 –s 172.16.0.0/12 –b –j DENY
      - ipcahins –A input –i eth0 –s 192.168.0.0/16 –b –j DENY
    - # rules for reserved addresses(multicast)
      - ipchains –A input –i eth0 –s 240.0.0.0/5 –b –j DENY

네트워크 보안

- **IP spoofing 방지**
  - 기존의 telnet, rlogin, rcp 등은 스니핑을 당할 경우 입력문자가 쉽게 노출
  - ssh, scp, telnet-ssl, ssl-telnet, apache-ssl 등을 이용



네트워크 보안

- **SYN Attack 방어**
  - 커넬 컴파일 시에
    - IP: TCP syncookie support (CONFIG_SYN_COOKIES) [y/N] Y
  - /etc/network/options의 내용 수정
    - syncookies=yes
  - /etc/sysctl.conf 파일에 다음 내용 추가
    - net/ipv4/tcp_syncookies = 1
- **Ping flooding 방어**
  - /etc/sysctl.conf 파일에 다음 내용 추가
    - net/ipv4/icmp_echo_ignore_all = 1
      - ping에 반응하지 않아서 서버의 존재는 숨김
    - net/ipv4/icmp_echo_ignore_broadcasts = 1
      - 브로드캐스팅에서의 핑은 막고 직접 어드레스로의 핑은 가능

결론

- 완전 무결한 시스템은 존재하지 않는다
  - 지속적인 보안 관리가 요구됨
  - 위험 평가/분석
  - 적절한 보안대책

보안 관련 사이트

- http://www.securityfocus.com
- http://packetstorm.securify.com
- http://www.linuxsecurity.org
- http://www.phrack.com/
- http://www.insecure.org
- http://www.hack.co.za
- http://khdp.org
- http://cert.or.kr

참고문헌

- Filesystems HOWTO
- Firewall HOWTO
- IPChain HOWTO
- Net HOWTO
- NFS HOWTO
- NIS HOWTO
- Quota mini HOWTO
- Security HOWTO
- Secure POP+SSH HOWTO
- Shadow Password HOWTO
- Securing and Optimizing Linux RedHat Edition