Part 4. 시스템 보안

Section 15. 클라이언트 보안 ★ (출제빈도 1.6%) ★

[1] 악성 소프트웨어

1. 분류

- 독립형/기생형 : 독립적으로 존재하지 못함
  - 독립형 : 웜, 좀비 바이러스
  - 기생형 : 바이러스, 논리폭탄, 백도어

2. 바이러스

3. 웜(worm)

- 주로 네트워크에서 연속적인 복사 기능을 수행함으로써 증식. 기억자잊를 소모하거나 저장된 데이터를 파괴하는 프로그램

  EX) 러브레터 바이러스, 조크 바이러스, 스테이지스 등

1. 분류

   1) MASS Mailer형 웜
      - 대량 메일 발송

   2) 시스템 공격형 웜
      - 운영체제 취약점 공략
      - svchost.exe 등의 파일을 설치

   3) 네트워크 공격형 웜

4. 트로이목마

- 원격 조정 / 패스워드 가로채기 / 키보드 입력 가로채기 / 시스템 파일 파괴
- 침임 행위의 시도를 위해 일정 기간 동안 위장하여 코드 형태로 시스템 특정 프로그램 내부에 존재한다 (O)
- 악성코드 전파(X)
- 자기복제 능력이 있다 (X)

5. 기타 악성 소프트웨어

- 스파이웨어(spyware) : 유용한 S/W를 제공하면서 설치된 시스템의 정보를 주기적으로 특정 서버로 보냄
- 루트킷(rootkit) : 컴퓨터 시스템에 침입 후 관리자(root) 수준의 접근 허락을 얻기 위해 사용하는 해킹 도구 모음
- 혹스(hoax) : 남을 속이거나 장난을 목적으로 퍼뜨리는 가짜 바이러스 (혹..시?)
- 익스플로잇(exploit) : 하나 혹은 여러 개의 취약점을 공격하기 위한 스크립트 혹은 프로그램
- Visual Basic 스크립트
  - 독립형으로 개발할 경우 파일 생성에 제한을 받아 웜형 악성코드를 만들지 못한다.

    → (X) VB 스크립트로 작성된 바이러스와 웜이 있음
  - 확장자는 VBA다.

→ (X) VBS

- 이메일에 첨부되어 전파될 수 있다.
  → (O)

[2] 웹 브라우저 보안

- 쿠키(cookie)
  - Set-Cookie : Server → Client\
    - 헤더에 키워드 secure를 표시하는 것은 쿠키 전송에 SSL을 사용하기 위해서이다. (O)
  - Cookie : Client → Server

Section 16. 윈도우 서버 보안

[1] 윈도우 개요

1. 윈도우 시스템의 구조

- 하드웨어 → HAL(Hadrware Abstraction Layer) → 마이크로 커널 → 각종 관리자 → 응용 프로그램

2. 윈도우의 특징

3. 윈도우 파일시스템

- FAT16 : 저용량(2GB이하) 하드디스크에 사용, DOS, Windows95 / 보안 취약
- FAT32 : 고용량(2GB이상) 하드디스크에 사용, Windows 95 OSR 이후 지원
- NFTS (New Technology File System)
  - 개별 폴더와 파일에 사용 권한 설정 가능
  - NFTS 보안의 기본 설정은 everyone그룹에 모든 권한이 '**허용**'
  - NFTS 클러스터의 크기는 512bye, 1KB, 2KB, 4KB까지 사용자 지정이 가능하다.
  - 결함관리(HotFixing)
  - 감사(auditing) 기능

NTFS File System

[NFTS 파일 시스템 구조]

- PBS(Partition Boot Sector) : 부팅에 필요한 최소한의 정보 저장
- MFT(Master File Table) : 모든 파일, 디렉터리에 대한 파일 이름, 크기, 생성 시간 등 파일에 대한 데이터 외의 모든 정보 저장
  - MFT 영역의 16개 엔트리는 파일시스템 자체의 메타 역할 및 추가적인 특성을 지원하기 위해 파일시스템 포맷 시 미리 할당된다.

    - $LogFile : 메타데이터(MFT)의 트랜잭션 저널 정보를 담고 있다.
    - $AttrDef : 속성의 식별자, 이름, 크기 등의 정보를 담고 있다.
  - 시스템 파일 : 파일 복사, 삭제 과정 中 시스템이 오류를 일으킬 때 복구하는데 사용할 디스크 사용에 대한 로그 파일, 디스크 불륨 이름 등
  - 파일 영역 : 각 파일에 대한 실제 데이터 저장

4. 윈도우 부팅 순서

1. POST(Power On Self Test) : 하드웨어 자체 점검, BIOS에 의해 실행됨
2. CMOS(Complementary Metal-Oxde Semiconductor) : BIOS는 CMOS 셋업에 저장한 정볼르 바탕으로 기본적인 설정사항을 읽음
3. MBR(Master Boot Record) : MBR에 부팅 매체에 대한 기본적인 파일시스템 정보가 들어가 있다.
4. NTLDR : 하드디스크의 부팅 파티션에 있는 프로그램으로, 윈도우 200이 부팅될 수 있도록 간단한 파일시스템을 실행하며, boot.ini 파이르이 내용을 읽어서 가능한 부팅 옵션을 보여줌
5. NTDETECT.com : 비디오 보드, 하드 드라이브와 같은 하드웨어를 검사함
6. NTOSKRNL.exe : HAL.DLL을 로드한다. (Hardware Abstraction layer)

[2] 윈도우 보안

1. 윈도우 설치

- 파티션 나누기

2. 윈도우 계정, 권한, 인증

1. 윈도우의 계정과 권한 체계
    - 기본 사용자와 그룹
    - SID(Security Identifier)

3. 공유자료 관리

1. 네트워크 드라이브의 이해
2. 파일과 폴더의 보안권한 설정
3. 디렉터리 및 파일에 대한 접근 권한 설정
4. 공유 자료 관리

   (가) 공유 폴더 숨기기

   (나) 윈도우 공유 폴더

   ① C$, D$

   ② ADMIN$

   ③ ★ IPC$(Inter Process Communication)

    - NULL 세션 공유 취약점을 가짐
    - 취약점을 이용해 사용자 계정과 암호 없이 시스템에 접속하여 계정 정보, 보안 정책, 네트워크 공유 현황 **불법 수집 가능**
    - $IPC를 제거하면 네트워크 서비스 일부에 문제 발생 가능
    - net share IPC$ /delete 명령어를 이용해 공유 해지 방법도 있지만, **레지스트리** 수정이 답

4. 암호 기능 사용

1. 폴더 및 파일 암호화(EFS, Encrypting File System))
   - 개별 파일 또는 특정 폴더 안에 있는 모든 파일 암호화 기능 제공
   - 사용자 계정 정보가 하드디스크에 저장 (보안 취약점)
   - NTFS 시스템에서만 사용 가능
2. 볼륨 암호화(BitLocker)
   - 드라이브 자체에 대한 암호화

5. 레지스트리 활용

1. 개요
2. 레지스트리 편집기
   - HKEY_CLASS_ROOT(HKCR) : 시스템에 등록된 파일 확장자, 애플리케이션에 대한 맵핑 정보, COM 오브젝트 등록 정보
   - HKEY_CURRENT_USER(HKCU) : 현재 시스템에 로그인하고 있는 사용자와 관련된 시스템 정보
   - HKEY_LOCAL_MACHINE(HKLM) : 컴퓨터에 설치된 하드웨어와 하드웨어를 구동시키는 드라이버 설정 사항
   - HKEY_USERS(HKU) : 시스템 내 계정과 그룹 정보
   - HKEY_CURRENT_CONFIG(HKCC) : 시스템이 시작할 때 사용하는 하드웨어 프로파일 정보를 저장
3. 레지스트리 공격 및 백업

   [공격]

   [백업]

   - 윈도우의 모든 시스템 정보를 백업하기 위해서는 USER.DAT, SYSTEM.DAT, SYSTEM.INI, WIN.INI를 백업해야 한다.

6. 윈도우 방화벽(PC 방화벽) 설정

[3] 윈도우 서버 보안 설정

1. 계정 및 패스워드 관리

1. 계정 및 패스워드 관리
2. 시스템 보안관리
3. 세션 관리

   (가) Session Timeout 설정

2. 시스템 보안관리

1. 파일시스템 체크
2. 불필요한 공유 제거
3. SAM(Security Account Manager) 파일 접근 통제

- 사용자 계정 및 패스워드 파일을 담고 있으므로 적절한 통제 필요
- 사용자 로그인 정보와 SAM 파일에 저장된 사용자 패스워드 정보를 비교해 인증 여부 결정
- 윈도우 암호 복구 시 사용되는 파일 (C:\Windows\System32\config)

3. 접근제어 관리

1. 접근제어 관리

   (가) Null Session 접근 차단

4. 세션 관리

1. Session Timeout 설정

[4] Winodws 네트워크 서비스

- 디렉토리 서비스 : 네트워크 리소스에 대한 정보를 저장하여 사용자와 응용 프로그램이 이 리소스에 액세스할 수 있게 만드는 네트워크 서비스

  → 네트워크의 여러 자원(사용자, 파일, 폴더, 프로그램, 프린터 등)을 편리하게 관리할 수 있도록 하는 서비스이다.

1. 디렉터리 데이터베이스

1. 네트워크 디렉터리 서비스
2. Active Directory
   - 네트워크상의 개체(object, 사용자, 컴퓨터, 프린터, 도메인, 서버, 사이트 등)에 대한 정보를 저장하며, 관리자와 사용자가 이 정보를 쉽게 찾아 사용할 수 있도록 함.
3. Active Directory 서버

> 💡 DC(Domain Controller) : 윈도우 서버 도메인 안에서 보안 인증 요청(로그인, 이용 권한 확인 등)에 응답하는 서버
> - Windows NT에서는 DC와 도메인 내의 각 컴퓨터가 각각 별도의 기반 비밀을 공유하고, 이 비밀값을 사용하여 암호화를 이용한 접속을 수행
> AD(Active Directory) : MS가 윈도우용 환경에서 사용하기 위한 LDAP 디렉터리 서비스. 주목적은 윈도우 기반의 컴퓨터를 위한 인증 서비스 제공

2. 윈도우즈 네트워크 방식

1. 워크그룹(Workgroup) 방식
   - 각각의 계정과 자원을 시스템별로 관리하는 방식으로 **소규모 네트워크**에 적합
   - P2P
   - 서버 관리자가 필요 없으며, 보안은 각 시스템 로컬 디렉터리 데이터베이스(SAM DB)에 의해 제공된다.
2. 도메인(Domain) 방식
   - 모든 계정과 자원을 특정 서버에서 관리하는 **중앙집중식** 방식

Section 17. UNIX 서버 보안

1. 유닉스(UNIX)

2. UNIX 기본 사용법

3. UNIX 시스템 관리

[부팅]

- 런 레벨(Run Level) : 시스템 운영 상태를 숫자 혹은 문자로 표현한 것

  0 : PROM(Programmable Read-Only Memory) 모드

  S, s : 시스템 싱글 유저 모드, 로컬 파일시스템이 마운트 되지 않은 상태

  1 : 시스템 싱글 유저 모드, 로컬 파일시스템이 마운트 된 상태

  2 : 멀티 유저 모드(NFS 클라이언트 모드)

  3 : 멀티 유저 모드(NFS 서버 모드) UNIX 기본 Run level)

  4 : 사용 안함

  5 : 시스템 power-off 모드

  6 : 시스템 리부팅

[파일시스템 관리]

[프로세스 스케줄 관리]

[cron]

- /etc/crontab : 파일에 처리할 작업 목록이 정의되고 저장
- /etc/default/cron : cron 데몬 프로세스가 실행괼 때 파일로서 변수를 저장 (CRONLOG, PATH 등)
- (리눅스) /var/log/cron : cron log파일

4. UNIX 서버 보안

[1] 시스템 보안

[passwd 파일]

[shadow 파일]

[파일 접근권한(umask)]

- 새롭게 생성되는 파일과 디렉토리의 기본 허용(default permission)을 결정

[권한 상승(SetUID, SetGID)]

- setUID 문자가 대문자 (-rwSr-r—) : SetUID는 설정되어있지만 파일소유자에게 실행권한(x)이 없음 (644)
- setUID 문자가 소문자 (-rwsr-r—) : SetUID는 설정되어있지만 파일소유자에게 실행권한(x)이 있음 (755)

```
* 패스워드 변경 명령어
ls -l /usr/bin/passwd

* 패스워드 보관 파일
ls -l /etc/passwd
-r-s--x--x   1   root   root   10704   Apr 15   1999   /usr/bin/passwd
```

[디렉토리 접근권한(sticky-bit)]

- sticky 비트를 이용해 디렉토리에 특별한 접근권한을 부여할 수 있음
- sticky 비트가 설정된 데릭터리는 시스템에 있는 모든 사용자가 파일이나 하위 디렉터리를 생성할 수 있지만 해당 디렉터리 `삭제`는 소유주나 root만 가능

[2] 네트워크 보안

[슈퍼 서버(inetd 데몬)]

- inetd 데몬은 슈퍼 데몬이라고 불리는데, 이는 데몬을 관리하는 데몬이기 때문

[접근 통제 TCP Wrapper)]

- TCP Wrapper가 설치되면, inetd 데몬은 TCP Wrapper 데몬인 `tcpd` 데몬에 연결을 넘겨준다. `tcpd` 데몬은 접속을 요구한 클라이언트가 적절한 접근권한이 있는지 확인한 뒤, 해당 데몬에 연결을 넘겨주며 연결에 대한 로깅을 실시한다.

5. 리눅스(Linux)

6. 유닉스/리눅스 서버 취약점 분석평가

PAM(Pluggable Authentication Modules)

- 리눅스에서 플러그인 방식으로 적용할 수 있는 인증 모듈
- 시스템 관리자가 응용프로그램들이 사용자를 인증하는 방법을 선택할 수 있도록 해주는 공유 라이브러리로, PAM을 사용하는 응용프로그램을 재컴파일 하지 않고 인증 방법을 변경할 수 있다.
- 관리자가 인증을 중앙에서 통제할 수 있게 해 준다.
- /etc/pam.conf 또는 /etc/pam.d 파일에서 각 시스템에 맞게 설정

Data Execution Prevention(DEP), No-eXecute

- 힙 스프레이 공격 방지
- MS 운영체제에 포함된 보안 기능. 실행 바잊 메모리 영역의 실행 코드에서 응용 프로그램이나 서비스가 실행되지 못하게 막기 위해 고안된 것.

Section 18. Linux 서버 보안

Section 19. 서버 보안 관리

1. 서버 관리자 업무

- 네트워크 관련 명령어

  ifconfig : 통신 디바이스(NIC) 상태

  netstat -an : 현 시스템에서 사용되는 통신 서비스 상태

  ps -elf : 현 시스템에서 수행 중인 프로그램과 데몬 상태

  snoop : 패킷을 캡쳐하여 분석

  inetd : 네트워크 슈퍼데몬 실행

2. 로그 설정과 관리

[윈도우 로그 분석]

- 응용 프로그램 로그
- 보안 로그 : 보안에 관한 내용을 가장 많이 담고 있음 (SecEvent.Evt) (파일 or 개체 만들기, 열기 또는 삭제, 리소스 사용 관련 이벤트 등)
- 시스템 로그
- 디렉터리 서비스 로그
- 파일 복제 서비스 로그
- DNS 서버 로그

[윈도우 감사 정책]

- 개체 액세스, 로그인/로그오프, 감사 정책 설정 변경 등의 보안 관련 로그를 기록.
- 종류 : 개체 액세스 감사, 계정 관리 감사, 계정 로그인 이벤트 감사, 권한 사용 감사, 로그인 이벤트 감사, 디렉터리 서비스 액세스 감사, 정책 변경 감사, 프로세스 추적 감사, 시스템 이벤트 감사

[유닉스/리눅스 로그 분석과 설정]

- **로그**
  - sulog : su 명령어를 사용한 경우, 변경 전 사용자 계정과 변경 후 사용자 계정 및 시간 정보가 저장되어 있는 파일

```
SU 04/18 18:41 + ttypd guard-wkshin
SU 04/18 18:44 + ttypb guard-wjshin
SU 04/19 00:50 + ttyp2 chester-guard
SU 04/19 06:27 - ttyp1 hacker-root (-의 경우 권한 변경 실패를 의미)
```

  - xferlog : FTP 로그파일로써 proftpd, vsftpd 데몬이 수행한 서비스를 기록하는 파일

```
Thu Feb 3 18:43:46 2011 1 192.168.1.1 861486 /tmp/12-67-ftp1.bmp b - o r algisa ftp 0 * c 861486 0
```

  - lastlog : 사용자가 최근에 언제 로그인했는지, 어떤 IP로 접속했는지 확인 가능
  - pacct : 사용자가 로그인한 후부터 로그아웃할 때까지 입력한 명령과 시간, 작동된 tty 등에 대한 정보
- **로그 설정 (/etc/syslog.conf)**

  `facility.priority; facility.priority  action(logfile-location)` ; A서비스 데몬에 의하여 B(메시지 우선순위)의 경우 C 로그파일에 그 기록을 남겨라

```
(예제1) Emergency 등급을 갖는 커널 이벤트 /var/log/emrge.log에 저장하기 위하여 /etc/syslog.conf에 추가해야 할 구문은 무엇인가?

kern.emerg /var/log/emerg.log

- 만약 모든 서비스(facility)를 의미하고 싶다면 kern이 아닌 '*'를 사용하면 된다.

(예제2) 모든 서비스에 대한 info 레벨 메시지와 mail,news 서비스는 메시지를 남기지 않는다. 로그는 /var/log/messages에 기록한다.

*.info ; mail.none ; news.none ; authpriv.none  /var/log/meesages
```

[응용 프로그램 로그 관리]

- IIS 웹 서버 로그

- Apache 웹 서버 로그

3. 공개 해킹도구에 대한 이해와 대응

[1] 트로이목마 S/W

- NetBus
- Back Office
- School Bus
- ackcmd
- rootkit : 자신과 다른 소프트웨어를 보이지 않게 숨기며, 사용자가 공격자의 소프트웨어를 인지하고 제거할 가능성을 피하는 것

[2] 크래킹 S/W

- 개요 : 크래킹은 해킹과 비교하여 특정 목적을 가지고 시스템에 침입하는 행위를 말하며, 다른 의미로 쉐어웨어 프로그램을 정식적으로 변환하는 행위
- John the Ripper
- pwdump
- L0phtCrack : 패스워드 취약점 점검도구로, 원격 및 로컬 서버나 PC에 대하여 패스워드를 점검하는데 유용
- ipccrack : 사용자 계정 패스워드를 원격지에서 추측하여 취약점을 점검하는 도구
- chntpw : 물리적 접근이 가능한 시스템에서 패스워드를 리셋하는 프로그램
- ERD COmmander

[3] 키로그 S/W

- 개요 : 키보드로 입력한 정보를 로그로 기록
- SK-Keylog
- Winhawk 등

[4] 로그 파일 변조 탐지 도구

- checklog
- chkwtmp : wtmpㅍ 파일에서 삭제된 부분을 검사하는 도구

4. 서버보안용 S/W 설치 및 운영

[1] 취약점 분석 도구

- SATAN (Security Analysis Tool for Auditing Networks) : 그래픽 모드로 개발되어있으며, 무료 사용 가능 (해커와 동일 방식으로 점검)
- SARA : SATAN 기반의 네트워크 기반의 컴퓨터, 서버, 라우터 IDS 취약점 분석
- SAINT : 유닉스 네트워크 취약점 점검도구(HTML 형식 보고 기능, 원격 취약점 점검)
- COPS : 유닉스 패스워드 취약점 점검도구

- Nessus : 유닉스 네트워크 취약점 점검도구

> 1. 공개소스 보안 도구
> 2. 스캔을 통해서 사용하지만 닫혀 있는(Closed) 포트, 서비스 취약점, 운영쳊 ㅐ종류 등이 가능
> 3. 네트워크 기반의 취약점 스캐너

- nmap : 포트 스캐닝 도구, stealth 모드 기능 포함
- hping : 사용자가 커스텀 패킷을 전송한 후 타깃으로부터 응답을 출력하는 툴로 TCP, UDP, ICMP 등 여러 프로토콜을 지원하며 사용 방법에 따라 DOS 공격도 가능
- PortQry : TCP/IP 연결 문제를 해결하는 데 사용할 수 있는 유틸리티.
- Acunetix : 상용 웹 취약점 스캐너로써 2005년 6월에 처음 발표된 이후 현재 가장 많이 사용되는 사용 웹 취약점 스캐너 (#526번)

[2] 무결성 점검

[시스템 백업]

- tar
- 이미지 백업

[파일 무결성 점검]

- tripwire : 다양한 해시 함수(MD5, SHA, CRC-32) 지원, 파일 DB를 만들어 변조 여부 판단
- MD5
- fcheck : perl 스크립트로 만들어짐
- AIDE
- Samhain : HIDS(호스트기반침입탐지) 기반으로 동작

[3] 스캔 탐지

[스캔 탐지 도구]

- mscan
- sscan
- portsentry : 실시간 포트 스캔, stealth 스캔 탐지 가능

> /etc/hosts.deny : 불법적인 접근 시도시 해당 경로로 파일에 실시간으로 추가됨

- nikto: (#509번)
- x-scan : (#509번)
- N-stealth : HTTP 웹 서버 취약점 및 웹 서비스의 content 취약점 점검 (#509번)

[4] 침임방지 및 방화벽

[네트워크 모니터링 및 침임탐지 도구]

- snort : 실시간 트래픽 분석과 공개 소스 네트워크 침입탐지시스템(IDS)

[방화벽]

- TCP-Wrapper
- IPchain/IPTable : IPchain/IPTable : rule 기반의 패킷 필터링, connection tracking(상태 추적), NAT 가능, 패킷 레벨 로깅, 확장 모듈 등

[5] iptable

```
    iptables  테이블명  체인명[A|I|D|F|P]  룰설정  타깃지정
                ①        ②                ③       ④

예제1) 목적지 IP 주소가 192.168.1.100 서버에 21번 포트를 통해 들어오는 TCP 패킷을 모두 차단(DROP) 하고자 함

    iptables -A INPUT -d 192.168.1.100 -p tcp -p 21 -j DROP

예제2) 외부 IP 172.20.0.1에서 들어오는 ICMP 패킷을 막는다

    iptables -A INPUT -s 172.20.0.1 -p icmp -j DROP
    * INPUT 체인 : 방화벽을 최종 목적지로 하는 체인
```

<테이블명>

- default : filter 테이블 (nat 가능)

<체인명>

- A : append, 해당 체인의 제일 마지막 룰을 추가
- I : insert, 해당 체인의 첫 행에 룰을 추가
- D : delete, 행 번호를 지정하여 특정 위치의 룰 삭제
- F : flush, 해당 체인의 모든 룰 삭제
- P : 해당 체인의 deafult 정책 설정

<룰설정>

- -p : 프로토콜 지정 (tcp, udp, icmp)
- -s : source IP 지정
- -d : destionation IP 지정
- —sport : source port ,출발지 포트 지정
- —dport : destination port, 목적지 포트 지정
- -i : 패킷이 들어오는 인터페이스(inbound interface)를 지정
- -o : 패킷이 나가는 인터페이스(outbound interface)를 지정

<타깃지정>

- -j : 룰에 매칭될 때 적용할 정책 또는 타깃체인을 지정
- ACCEPT(허용), DROP(차단), REJECT(차단), LOG(로깅)

Section 20. 각종 시스템 보안위협 및 대응책

1. 버퍼 오버플로우 공격

[프로세스 메모리 구조]

- Text : 프로그램 코드와 상수가 정의되어 있으며, 읽기(read)만 가능하기 때문에 데이터를 저장하려고 하면 분할 충돌을 일으켜 프로세스가 중지된다
- Data : 전역 변수와 정적 변수 저장
- Heap : 프로그래머 필요에 따라 동적 메모리 호출에 의해 할당되는 메모리 영역
- Stack : 함수 인자 값, 함수 내의 지역 변수, 함수의 반환 주소 등이 저장되는 영역

  [문제]

  프로그램 실행 중 함수 호출 시 생성되는 지역변수와 매개변수가 저장되었다가 함수가 종료되면 시스템에 반환되는 영역?

  [정답]

  Stack 영역

[1] 버퍼 오버플로우

- 유닉스 계열에서 버퍼 오버플로우 취약점이 발생하지 않도록 **/etc/system** 파일에 두 라인을 추가하여 방어 가능
  - set noexec_user_stack = 1
  - set noexec_user_stack_log = 1

[2] 스택 버퍼 오버플로우

- 보통 SetUID가 설정된 루트 권한의 프로그램을 공격
- 스택 영역에 할당된 버퍼 크기를 초과하는 데이터(실행가능코드)를 기록하고 저장된 **복귀주소를 변경**함으로써 임의의 코드를 실행
- 셸 코드(shellcode)

[3] 힙 오버플로우

- 스택오버플로우 공격과 다르게 실행 제어를 쉽게 이동시킬 수 있는 반환 주소가 없다. 그러나 할당된 공간이 함수에 대한 포인터를 포함하고 있다면 공격자는 이 주소를 변경가능.

[4] 버퍼 오버플로우 공격의 대응책

2. 포맷 스트링 공격

[1] 컴파일 시간 방어

- 새 프로그램 내에서 공격을 저지하도록 프로그램을 강화
  - EX) 고급 수준의 프로그래밍 언어 사용, 안전한 코딩기법(strncat, fgets, fscanf), Libsafe 라이브러리, 스택 보호 매커니즘(stack guard), 스택 쉴드(stack shield)

[2] 실행 시간 방어

- 존재하는 프로그램에서 공격을 발견하고 중지
  - EX) 실행가능 주소 공간의 보호(자바 런타임 시스템), 주소 공간의 임의 추출(ASLR, Address Space Layout Randomization)

3. 레이스 컨디션 공격

4. 백도어

- Trap Door라고도 하며, 트로이목마와 다르게 악의적인 해킹을 위한 것은 아님.
- 대응책 : 현재 동작 중인 프로세스 확인, H-IDS(Host-based Intrusion Detction System)

5. 시스템 자원 고갈 공격(=시스템 서비스 공격)

[1] 종류

1. 가용 디스크 자원 고갈 공격 : 파일 생성(write)후 1000바이트씩 while(1)
2. 가용 메모리 자원 고갈 공격 : malloc(1000)
3. 가용 프로세스 자원 고갈 공격 : fork()
4. 프로세스 죽이기 공격 : kill -15

문제

cron에 의해 수행된 작업에 관한 로그는 기본적으로 /etc/default/cron 파일에 저장된다.

(X)

- 로그 : /var/log/cron
- 경로 : /etc/cron
- 환경설정 파일 : /etc/default/cron

다음에서 설명하는 리눅스 명령어는?

```
리눅스 운영체제에서 원격 서버에 접속하기 위한 명령어로, 접속하고자 하는 호스트를 /etc/hosts.equiv 파일에 사전에 등록해 두어야 한다.
```

- ① telnet
- ② login
- ③ rlogin
- ④ talkd

정답 : 3번

윈도우의 SAM(Security Account Manager)에 대한 설명이다. 틀린 것을 고르시오.

- ① 사용자 계정의 비밀번호를 관리한다.
- ② 해시된 비밀번호는 한 번 더 암호화되어 저장된다.
- ③ SID를 이용해 사용자를 식별한다.
- ④ 액티브 디렉터리(AD)의 원격 사용자 인증에 사용된다.

정답 : 3번

- SAM(Windows Secutiry Account Manager) : 윈도우 운영체제에서 사용자의 비밀번호를 저장하는 DB 파일

취약점 탐지 도구가 아닌 것은?

1. SATAN
2. SAINT
3. Snort
4. NESSUS

→ 정답 : 3번, Snort는 침입탐지도구에 해당된다.