정보보안

목차

[정보보안 1](#_Toc53591877)

[1. 시스템보안 4](#_Toc53591878)

[1.1. 계정 4](#_Toc53591879)

[1.1.1. /etc/passwd 4](#_Toc53591880)

[1.1.2. /etc/group 4](#_Toc53591881)

[1.2. Unix 권한 관리 5](#_Toc53591882)

[1.2.1. SetUID, SetGID, Sticky bit 5](#_Toc53591883)

[1.2.2. umask 5](#_Toc53591884)

[1.2.3. chmod 5](#_Toc53591885)

[1.2.4. chown, chgrp 5](#_Toc53591886)

[1.3. Unix 파일 시스템 6](#_Toc53591887)

[1.4. 보안 솔루션 6](#_Toc53591888)

[1.5. 보안 운영체제 (Secure OS) 7](#_Toc53591889)

[1.6. 저작권 관리 7](#_Toc53591890)

[1.7. 도구 8](#_Toc53591891)

[1.7.1. TCP Wrapper 8](#_Toc53591892)

[2. 네트워크 보안 9](#_Toc53591893)

[2.1. 공격 기법 9](#_Toc53591894)

[2.1.1. 피싱, 파밍, 스미싱, 스피어 피싱 9](#_Toc53591895)

[2.1.2. DOS 공격 9](#_Toc53591896)

[2.1.3. DDOS 공격 10](#_Toc53591897)

[2.1.4. 스니핑 (Sniffing) 11](#_Toc53591898)

[2.1.5. 스푸핑 (Spoofing) 13](#_Toc53591899)

[2.1.6. 세션 하이재킹 14](#_Toc53591900)

[2.2. 무선 보안 15](#_Toc53591901)

[2.2.1. 공유기 15](#_Toc53591902)

[2.2.2. 워드라이빙 (Wardriving) 15](#_Toc53591903)

[2.2.3. 블루투스 15](#_Toc53591904)

[2.3. 주요 포트 번호 16](#_Toc53591905)

[3. 어플리케이션 보안 17](#_Toc53591906)

[3.1. Web 17](#_Toc53591907)

[3.1.1. GET/POST 17](#_Toc53591908)

[3.1.2. HTTP Response (상태 코드) 17](#_Toc53591909)

[3.1.3. 스크립트 종류 17](#_Toc53591910)

[3.1.4. Web 공격 (OWASP 10개 주요 취약점 중 발췌) 18](#_Toc53591911)

[3.1.5. Web 로그 18](#_Toc53591912)

[3.2. 코드 보안 19](#_Toc53591913)

[3.2.1. 버퍼 오버플로우 19](#_Toc53591914)

[3.2.2. 포맷 스트링 19](#_Toc53591915)

[4. 악성코드 20](#_Toc53591916)

[4.1.1. 웜 vs 바이러스 (자주 출제) 20](#_Toc53591917)

[5. 암호학 21](#_Toc53591918)

[5.1. 알고리즘 21](#_Toc53591919)

[5.1.1. 전치법, 대체법, 스테가노그래피 21](#_Toc53591920)

[5.1.2. 해시 21](#_Toc53591921)

[5.1.3. 대칭키, 비밀키 21](#_Toc53591922)

[5.1.4. 비대칭키, 공개키-개인키 22](#_Toc53591923)

[5.1.5. 공개키 기반 구조 (PKI, Public Key Infrastructure) 23](#_Toc53591924)

[5.2. 전자상거래 24](#_Toc53591925)

[5.2.1. 보안 요건 24](#_Toc53591926)

[5.2.2. ★ 전자서명, 전자봉투, 전자결재 24](#_Toc53591927)

# 시스템보안

## 계정

### /etc/passwd

|  |
| --- |
| root : x : 0 : 0 : root : /root : /bin/bash |
| 1. 계정명  2. 패스워드가 암호화되어 shadow 파일에 저장됨  3. 사용자 id  4. 그룹 id  5. 사용자 이름 (별명)  6. 홈 주소  7. 셸 종류 |

### /etc/group

|  |
| --- |
| root : x : 0 : root |
| 1. 그룹명  2. 패스워드가 암호화되어 shadow 파일에 저장됨  3. 그룹 id  4. 해당 그룹에 속한 계정 목록 |

## Unix 권한 관리

### SetUID, SetGID, Sticky bit

|  |  |  |
| --- | --- | --- |
| SetUID | chmod 4777 a.out  chmod u+s a.out | 해당 권한이 설정된 프로그램 실행 시,  파일 소유자의 권한으로 실행 (획득) |
| SetGID | chmod 2777 a.out  chmod g+s a.out | 해당 권한이 설정된 프로그램 실행 시,  파일 소유자의 Group 권한으로 실행 (획득) |
| Sticky bit | chmod 1777 /testdir  chmod u+t /testdir | 디렉터리 내 생성은 자유  수정, 삭제 불가  ex. 공용 디렉터리 관리 |

### umask

|  |
| --- |
| Directory 기본 접근권한 (Default) : 777  파일 기본 접근권한 (Default) : 666  **Q.** 디렉토리 접근 권한에 기본적으로 실행 권한이 포함된 이유?  해당 권한이 없으면 폴더 내부 접근 자체가 불가능하기 때문이다.  폴더 및 파일 생성 시 Default 권한에서 umask 값만큼을 빼고 생성됨  **$ umask 022** // 해당 값으로 설정 시 폴더는 755, 파일은 644로 설정된다. |

### chmod

|  |
| --- |
| a (all), g (group), u (user), o (other)  + 추가, - 제거  chmod g-w file.txt  chmod a=rw file.txt // 모든 (사용자, 그룹, others)에 읽기 쓰기 권한 부여  chmod g+w, o-x file.txt // 그룹에 쓰기 권한 추가, others 실행 권한 제거 |

### chown, chgrp

|  |
| --- |
| chown 사용자명:그룹명 file.txt // myfile1의 소유자와 그룹을 cand, cand 로 변경  chown 사용자명 file.txt // 만약 그룹을 입력하지 않으면 소유자만 변경된다 |
| chgrp 그룹명 file.txt |

## Unix 파일 시스템

파일 할당 과정

## 보안 솔루션

|  |  |
| --- | --- |
| 인증 | Something you know: 패스워드  Something you have: 생체정보  Something you are: 스마트 카드, 신분증, OTP  SSO (Single Sign On): 커버로스(Kerberos)를 이용한 윈도우 Active Directory |
| 방화벽 | 접근 제어 (룰셋 기반)  - 패킷 필터링 방식  - 프록시 방식  로깅과 감사 추적 |
| IDS | HIDS (Host-Based Intrusion Detection System)  NIDS (Network-Based Intrusion Detection System)  ★ 침입 탐지 기법  - 오용 탐지 기법 (Misuse Detection) : 사전에 패턴 입력 후 탐지  - 이상 탐지 기법 (Anomaly Detection) : 평상시와 다른 현상 탐지  ex. Snort, IPtable |
| IPS | 침입 탐지 기능을 수행하는 모듈이 패킷 하나하나를 검사하여 패턴을 분석한 뒤 정상적인 패킷이 아니면 차단 (능동적 대응) |
| VPN | Virtual Private Network  - 기업 내부 간 데이터 통신을 위한 가상 네트워크를 구현한 암호화 솔루션  - VPN을 이용한 터널링  - 원격의 두 지점 간을 내부 네트워크처럼 이용 가능  - 집에서도 회사 내의 서버를 보안된 상태로 접근 가능 |
| NAC | Network Access Control  - IP, MAC 주소 맵핑 정보 기반  - 사용자는 부여 받은 IP에 해당하는 MAC주소에 대해 관리자에게 알리고, 허가를 받아야함 (인증과정에서 백신이나 보안 패치 적절성 여부 검토)  - 라우터로 구분된 서브 네트워크마다 에이전트 시스템 설치(관리자) |
| 허니팟 | 해커를 **유인**해서 정보를 얻거나 잡으려고 설치 |

## 보안 운영체제 (Secure OS)

|  |
| --- |
| - 보안 커널  - 모든 프로세스 감시 (일정 수준의 CPU 점유로 성능 저하)  - TCB (Trust Computing Base) 핵심  - 참조 모니터  \* 모든 접근은 참조 모니터를 거쳐야 함  \* 격리성, 검증 가능성, 완전성  \* 참조모니터는 승인되지 않은 접근으로부터 객체를 보호하기 위해 객체에 대한 모든 주체의 접근을 통제하는 개념으로서 이를 실제로 구현한 하드웨어, 펌웨어, 소프트웨어로 구성된 것이 보안 커널이다.  - TPM (신뢰 플랫폼 모듈)  \* 하드웨어 칩으로 구현하는 것이 일반적이지만, 소프트웨어적으로 구현하기도 한다  \* 암호화 키 생성과 저장, 패스워드 저장, 무결성 검증 ㅡㅍㄹ랫폼  \* 인증된 부트 서비스, 암호화 서비스 |

## 저작권 관리

|  |  |
| --- | --- |
| DRM | Digital Right Management  - 운영체제의 커널에 DRM 모듈을 삽입해 문서에 대한 접근 권한을 설정, 통제  - 문서 보안, 파일 단위 암호화  - 파일 열람 시 사용자 권한 확인 후 파일 복호화 |
| 워터마크 | 저작권 정보를 디지털 콘텐츠에 삽입 |
| 핑거프린팅 | 디지털 콘텐츠 구매 시, 해당 컨텐츠에 구매자 정보를 삽입하여  유출 시 누구 유출하였는지 추적가능 |

## 도구

### TCP Wrapper

|  |
| --- |
| 클라이언트1 Telnet 서버  클라이언트2 🡪 inetd 🡪 tcpd 🡪 🡪 로그인  클라이언트3 FTP 서버 |
| **inetd (슈퍼 데몬)**은 클라이언트로부터 서비스 요청을 받아 FTP, Telnet에 해당하는 데몬을 활성화시켜 클라이언트와 연결시켜는 역할  TCP Wrapper를 설치하면 inetd 데몬은 TCPWrapper의 tcpd 데몬에 일괄적으로 넘겨준다.  tcpd 데몬은 접속을 요구한 클라이언트의 **접근 권한 확인** 후, 요청한 데몬(Telnet, ftp 등)에 연결한다. 또한 이때 관련 **로그를 생성**할 수 있다. |

tripwire 무결성 점검도구

여러 도구들에 관한 내용 금융결제원 2021 필기 객관식

# 네트워크 보안

## 공격 기법

### 피싱, 파밍, 스미싱, 스피어 피싱

|  |  |
| --- | --- |
| 피싱 | - 실제 사이트와 유사한 피싱 사이트를 제작 및 접근 유도 (주로 이메일)  - URL 다름 |
| 스피어 피싱 | 특정 인물 타깃으로 피싱 (관련된 사람들 정보 이용) |
| 파밍 | - 도메인 자체를 탈취 or DNS Spoofing 🡪 URL 동일  - 피싱 사이트로 유도 |
| 스미싱 | SMS + Phishing, 문자 메시지로 낚기 (피싱 사이트 링크 전송) |

### DOS 공격

|  |  |  |
| --- | --- | --- |
| 프로토콜 | 공격 기법 | 특징 |
| TCP | Boink  Bonk  TearDrop | TCP Sequence Number 조작 🡪 오류 제어 로직 공격  피해자는 풀 수 없는 문제로 처리 불가 에러   |  |  | | --- | --- | | Boink | **중간** seq 반복 | | Bonk | seq **1** 만 반복 | | TearDrop | seq 조합 엉망(무작위) |   \*해결: 패치 또는 과부하가 걸리거나 계속 반복되는 패킷 무시 |
| Land | SYN 패킷의 출발지 IP = 목적지 IP  피해자가 응답한 패킷은 피해자 자신에게 되돌아와 자원 고갈  \*해결: 패킷의 출발지 주소와 목적지 주소 검증 |
| SYN Flooding | 존재하지 않는 클라이언트가 서버 별로 한정되어 있는 접속 가능한 공간에 접속한 것처럼 속여 다른 사용자가 서비스를 제공받지 못하게함 🡪 3-way handshaking 악용  1. 공격자가 SYN 보냄  2. 피해자가 SYN+ACK 응답  3. 공격자는 고의적으로 응답하지 않음  4. 서버의 가용한 자원 상태를 전부 SYN Received 상태로 만듬  (**Half-Opened**)  \*해결: SYN Received 대기 시간 줄이기. IPS 사용 |
| 프로토콜 | 공격 기법 | 특징 |
| HTTP | HTTP Get Flooding | 정상 접속한 뒤 계속해서 요청  **특정한 페이지** http get method 반복 실행 |
| 동적  HTTP Request Flooding | 특정 페이지가 아닌 요청 페이지를 **지속해서 변경**  차단 기법을 우회하기 위함 |
| HTTP CC 공격 | **Cache Control**  헤더 옵션에서 캐시를 사용하지 않는 것으로 설정  서버에서는 캐시를 사용하지 않고 응답해야하므로 부하 증가 |
| ICMP  (Ping) | Smurf | ICMP Echo Request / Reply  다이렉트 브로드캐스트 (Direct Broadcast)  기본 브로드캐스트는 라우터를 넘어가지 못한다. 그러나 원격지의 네트워크에 브로드캐스트 하는 다이렉트 브로드캐스트 방법이 존재한다.  1. 공격자는 네트워크 상의 임의의 시스템에 송신자 IP를 피해자의 IP로 가장하여 ICMP Request 패킷을 다이렉트 브로드캐스팅한다.  2. ICMP Request 패킷을 받은 시스템들은 ICMP Reply 패킷을 피해자에게 보낸다.  3. 피해자는 다수의 ICMP Relpy를 받고 시스템이 과부하 된다. |
| - | 메일 폭탄 | Mail Bomb  메일 서버는 각 사용자에게 일정한 양의 디스크 공간을 할당하는데, 메일이 폭주하여 공간을 가득 채우면 정작 받아야 하는 메일을 받을 수 없다. |

### DDOS 공격

|  |  |
| --- | --- |
| 봇 | Bot  분산 서비스 공격에 사용되는 **악성코드** |
| 봇넷 | Botnet  좀비 PC(봇, 악성코드에 감염되는 PC)들이 이루는 네트워크 |

### 스니핑 (Sniffing)

#### Promiscuous 모드(무차별 모드)

기본 모드에서는 랜 카드에서는 자신의 MAC, IP 주소를 토대로 패킷을 필터링한다.

그러나, 무차별 모드에서는 필터링 없이 모든 패킷을 받아들인다.

#### 공격 기법

|  |  |
| --- | --- |
| 공격 종류 | 특징 |
| 스위치 재밍 | Switch Jamming  스위치 기능 마비 🡪 허브처럼 동작 🡪 모든 포트에 브로드캐스팅  스위치에 랜덤한 형태로 생성한 MAC 주소를 가진 패킷을 무한대로 보내면 스위치의 MAC 테이블은 저장 용량을 넘고, 스위치는 원래 기능을 잃고 더미 허브처럼 작동하게 된다. |
| SPAN 포트 태핑 | SPAN (Switch Port Analyzer)  포트미러링 (Port Mirroring)을 이용한 방법으로,  각 포트에 전송되는 데이터를 미러링하고 있는 포트에 동일하게 전달  네트워크 장비에서 간단할 설정으로 활성화되지만,  Splitter(Tapping 장비)를 통한 하드웨어적인 방법을 Tapping이라고 한다.  ex. IDS, 모니터링, 로그 시스템 설치 |
| Man in the Middle | 중간자 공격 |

#### 탐지 기법

|  |  |
| --- | --- |
| 이용 | 특징 |
| Ping  (ICMP Request) | 의심되는 호스트에 네트워크에 존재하지 않는 MAC주소를 목적지 주소로 설정한 ICMP Request를 보냈을 때 ICMP Reply가 오면 해당 호스트는 무차별 모드 사용 중 |
| ARP Request | ping과 유사한 방법으로 ICMP Request 대신 ARP Request 이용 |
| DNS | 테스트 대상 네트워크로 Ping Sweep을 보내고 들어오는 Inverse-DNS lookup을 검사한다.  스니핑 프로그램이 피해 시스템의 IP 주소에 DNS 정보를 얻기 위한 Inverse DNS Lookup 작업 사용하는 것을 이용 |
| Decoy(유인) | 가짜 ID, Password를 네트워크 상에 고의적으로 유출시키고,  해당 정보를 이용해 침입을 시도하는 공격자 감지 |
| ARP Watch | MAC, IP 주소 맵핑 값을 초기에 저장하고,  이후 ARP 트래픽을 모니터링하여 변경을 감지.  공격자가 위조된 ARP 사용하는 것을 탐지 가능 |

### 스푸핑 (Spoofing)

|  |  |
| --- | --- |
| 종류 | 특징 |
| ARP Spoofing | 서버 클라이언트에 위조된 IP, MAC 맵핑 정보 전달  서버: 클라이언트 IP 주소에 해당하는 가짜 MAC 주소(공격자 주소) 알림  클라이언트: 서버 IP 주소에 해당하는 가짜 MAC 주소(공격자 주소) 알림  받은 패킷들을 Relay 하여 눈치채지 못하도록 함  맵핑 값을 static 으로 설정하여 방어할 수 있다.  > arp -a (ARP 테이블 조회)  > arp -s 10.0.0.2 AA:BB:DD:DD:CC:EE (static 설정) |
| IP Spoofing | - 피해자가 쓰는 IP 주소를 이용하여 권한 획득  - 트러스트 관계  Trust 관계가 맺어져 있는 서버-클라이언트 관계에서,  클라이언트에 DoS 공격을 통해 서비스를 끊고,  서버 측에 피해자의 IP 주소를 가장하여 접속함으로써 패스워드 없이 권한 획득  유닉스: Trust 인증  윈도우: Active Directory 인증  **EX**. 유닉스 트러스트 설정 파일 (/etc/host.equiv)  200.200.200.200 root // 해당 IP 주소에서 root 계정으로 접속 시 패스워드 없이 접속 허용  201.201.201.201 + // 해당 IP 주소에서는 계정 상관없이 접속 허용  + + // IP와 계정 상관없이 접속 허용 |
| ICMP Redirect | 3계층 공격  한 네트워크 상에 두 개 이상의 라우터가 존재할 때,  더 효율적인 경로를 지닌 라우터를 알려주는 패킷 (ICMP Redirect) 이용  공격자는 피해자에게 ICMP Redirect 패킷을 통해 자신을 이용하는 것이 더 효율적인 경로라고 속임으로써 피해자가 자신에게 패킷을 보내도록 유도할 수 있다.  이후, 획득한 패킷을 기존 라우터로 릴레이하면 스니핑 가능 |
| DNS Spoofing | 실제 DNS 서버보다 DNS Response를 먼저 보냄으로써,  도메인과 맵핑되는 IP 주소를 조작하여, 잘못된 웹 주소로 접속 유도  DNS는 비신뢰성 비연결형 프로토콜로 패킷의 수신여부를 확인하지 않기 때문에 먼저 도착한 DNS Response가 처리되고 이후에 도착한 DNS Response 패킷은 버려진다.  사용자가 조작된 웹 페이지에서 계정정보를 입력하면, 원래 웹 사이트에 릴레이한 후 정상 로그인 페이지로 리다이렉트  cf. Webzip, Webstripper 웹 긁어오기 프로그램 🡪 피싱 사이트 제작 이용  \*해결: 중요 사이트 (도메인, IP) 맵핑 정보를 host 파일에 static 저장 |

### 세션 하이재킹

|  |
| --- |
| - 두 시스템 간 연결이 활성화된 상태, 즉 로그인된 상태 (로그인 세션)을 가로채는 것  - 순서 번호 조작으로 연결 끊고, RST 패킷으로 끼어들기 (연결 재설정)  1. 서버, 클라이언트 각각에 잘못된 TCP Sequence Number 전달로 세션 방해  2. 서버에 클라이언트 주소로 RST (Reset) 패킷을 보낸다.  3. 서버는 클라이언트의 Sequence Number가 재설정 된 것으로 판단하고,  공격자와 TCP 3-way Handshaking 진행  4. 공격자는 클라이언트가 연결을 맺고 있던 로그인 세션을 그대로 획득한다.  \*해결방안  - ssh 프로토콜을 사용하여 TCP Sequence Number 유출 방지  - 패킷 스니핑 방지 |

## 무선 보안

### 공유기

|  |  |
| --- | --- |
| SSID 브로드캐스팅 금지 | Service Set Identifier는 무선 랜을 구분하는 구분자이다.  무선랜 이름 |
| WEP | 128비트 암호화 키 |
| WPA, WPA-PSK | WEP 취약점 보완 |
| EAP 와 802.1x  (WPA Enterprise) | EAP (Extensible Authentication Protocol)  중앙 서버에서 사용자 인증 및 권한 관리  로그인 세션 별로 암호화키를 생성  🡪 암호화키를 탈취 공격 무력화  ex. 학교나 기관에서 개인 별 ID/PW로 접속하는 것 |

### 워드라이빙 (Wardriving)

무선랜의 경우 노트북에 수신율이 높은 안테나를 붙여서 차를 타고 보안이 취약한 무선 랜을 탐색하며 해킹을 시도하는 것

### 블루투스

|  |  |
| --- | --- |
| 블루프린팅  Blueprinting | - 탐색 활동  - SDP (Service Discovery Protocol) 이용  - 각 블루투스 장치는 고유의 블루투스 주소 존재 (6바이트)  6바이트 : 제조사(3), 장치고유(3) |
| 블루스나프  Bluesnarf | - 취약점을 이용하여 임의 파일 접근 및 다운로드  - 인증없이 정보 교환을 위해 개발된 프로토콜 OPP (OBEX Push Protocol)이용 |
| 블루버그  Bluebug | - 취약한 연결 관리 이용  - 공격대상에서 임의의 동작 실행  - 블루투스 기기는 한번 연결된 이후에는 다시 인증하지 않아도 연결 가능 |

## 주요 포트 번호

|  |  |
| --- | --- |
| 포트 번호 | 서비스 |
| 20 | FTP (데이터 채널) |
| 21 | FTP (제어 채널) |
| 23 | Telnet |
| 25 | SMTP |
| 53 | DNS |
| 69 | TFTP  부팅 프로그램 다운로드 등 단순한 파일 전송 |
| 80 | http |
| 110 | POP3  서버에서 메일 삭제 |
| 111 | RPC (Remote Procedure Call)  원격 함수 호출.  원격에서 서버의 프로세스 실행 |
| 138 | NetBIOS (Network Basic Input Output Service  윈도우에서의 네트워크 파일 공유 |
| 143 | IMAP  서버와 동기화 (메일 클라이언트 프로그램과 서버 둘다 존재) |
| 161 | SNMP |

# 어플리케이션 보안

## Web

### GET/POST

|  |  |
| --- | --- |
| GET | URL 에 정보 전송  URL의 ? 뒷 부분 ex. ?page=1&search=test |
| POST | HTTP Header에 정보 전송  HTTP 헤더 |

### HTTP Response (상태 코드)

금융결제원 2021 기출

|  |  |  |
| --- | --- | --- |
| 상태 코드 | 요약 | 설명 |
| 100 번대 | 정보 전송 | 요청을 받았으며 작업을 계속한다 |
| 200 번대 | 성공 |  |
| 300 번대 | 리다이렉션 | 클라이언트는 요청을 처리하기 위해,  사용자의 추가적인 동작 필요 |
| 400 번대 | 클라이언트 에러 |  |
| 500 번대 | 서버 에러 |  |

### 스크립트 종류

|  |  |
| --- | --- |
| Server Sids Script, SSS | ASP (Active Server Page)  JSP (Java Script Pages)  PHP (Personal Home Page) |
| Client Side Script, CSS | JSP  VBS (Visual Basic Script) |

cf. 금융결제원 2021 기출

스크립트 언어 고르는 것에서 Perl, ~~C#~~이 보기로 등장하였음

### Web 공격 (OWASP 10개 주요 취약점 중 발췌)

|  |  |
| --- | --- |
| 종류 | 내용 |
| Injection | SQL Injection 등 |
| XSS | Cross Site Scripting  1. 공격자는 게시판 등에 악의적인 스크립트를 업로드한다.  2. 피해자는 해당 게시클 클릭 후, 스크립트 자동 수행  3. 스크립트 수행 결과 공격자에게 전달 (정보 탈취) |
| CSRF | Cross-Site Request Forgery  XSS와 다른 점은 피해자의 권한으로 서버에 특정 요청을 하는 것이다.  ex. 다른 사람이 구매한 물품을 대신 결제하도록 유도 |
| 디렉터리 탐색  디렉터리 리스팅  Directory Listing | 서버의 디렉터리 경로가 URL에 노출되는 점을 이용하여,  특정 경로에 있는 파일을 다운로드 받을 수 있다. (/etc/passwd 등) |
| URL 접근 제한 실패 | 인증 없이 접근할 수 있는 관리자 페이지가 존재할 경우,  Brute Force 방식으로 URL 탐색으로 해당 페이지 접근 후 악용 |
|  |  |
|  |  |

### Web 로그

#### IIS (W3C 확장 로그 파일 형식)

|  |
| --- |
| 2012-06-03 08:53:12 192.168.137.128 GET  /XSS/GetCookie.asp?cookie=ASPSESSIONIDQQCAQDDA 80 - 192.168.137.1  Mozilla/5.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;) 200 0 0 255 |
| 날짜 시각 [**서버** IP] [http 요청 방식]  [접근 URL] [포트 번호] - [**클라이언트** IP]  브라우저 정보 [http 응답 코드]  [서버🡪클라이언트 데이터 전송 크기] [클라이언트🡪서버 데이터 전송 크기]  [처리 시간]  cf. 외울 때 서버 먼저로 외우면 쉽다. |

## 코드 보안

### 버퍼 오버플로우

데이터 사이즈 정의되지 않음 악용

|  |
| --- |
| int main(int argc, char\* argv[]){  char buffer[10];  strcpy(buffer, argv[1]);  printf(buffer);  } // 배열 크기보다 큰 문자열을 입력 받고 출력할 경우 허용되지 않은 메모리 영역을 침범  \*해결방안  1. 안전한 라이브러리 함수 사용  2. Stack Guard: 컴파일 시 canary 값 변조 여부 확인  3. Stack Shield: 리턴 주소값을 안전한 곳에 복사해두고 프로그램 종료 시 현재 스택의 리턴 주소와 일치 여부를 확인한다. |

### 포맷 스트링

데이터 형태에 대한 불명확한 정의 악용

|  |
| --- |
| int main(){  char \*buffer = "wishfree\n%x\n";  printf(buffer);  }  wishfree 문자열 외에 해당 문자열이 저장된 메모리의 다음 메모리 주소를 얻을 수 있음 |
| int main(){  long i=0x00000064, j=1;  printf("i 주소: %x \n", &i);  printf("i 값: %x \n", i);  printf("%64d %n \n", j, &i); // i에 64 입력 (%64d 는 64개 문자 지정 출력)  printf("변경된 i 값 : %x \n", i);  }  소스코드에서 변수에 데이터를 입력하는 동작이 나타나지 않았지만,  변수의 값을 변경할 수 있다.  %n: 유일하게 printf 함수 중 인자에 쓰기를 하는 녀석입니다.  %n 자리에 int 포인터를 넣어주면 그 자리에 지금까지 프린트 한 문자개수를 출력시켜줍니다. |

# 악성코드

보안기사 실기 책 참조

|  |  |
| --- | --- |
| 이름 | 특징 |
| 바이러스 | - 자가복제 O  - 감염 대상 필요  - 사용자가 감염된 파일을 옮김으로써 전파 |
| 웜 | - 자가복제 O  - 네트워크를 통해 스스로 전파  ex. Mass Mailer: 시스템에 계속 기생하면서 메일 주소를 수집해 대량의 메일을 계속해서 발송 |
| 트로이 목마 | 정상적인 인증을 우회하여 원격에서 접근  개발자의 의도가 아닌 해킹이 주 목적 |
| 백도어 | 정상적인 인증과정을 거치지 않고, 접근 가능한 통로.  개발 과정에서 개발자의 의도로 만들어며, 꼭 해킹이 목적은 아니다. |
| 스파이웨어 | - 자신이 설치된 시스템의 정보를 특정 서버에 주기적으로 전송  - 스파이 연상(Spy) 기밀 유출 |
| 애드웨어 | 자동으로 광고를 생성 |
| 다운로더 | Downloader  외부에서 악성코드를 다운로드 받음 |
| 드롭퍼 | Dropper  자기 자신이 보유하고 있던 악성코드를 설치 |
| RAT | Remote Access Trojan (유령쥐로 유명)  원격 조정이 가능한 트로이 목마 유형 |

### 웜 vs 바이러스 (자주 출제)

차이점 : 감염 대상 필요 여부

공통점 : 자가복제

# 암호학

## 알고리즘

### 전치법, 대체법, 스테가노그래피

|  |  |
| --- | --- |
| 전치법, Transposition | 자리 바꾸기, 위치 변경 |
| 대체법, Substitution | 다른 문자로 대체 |

cf. 스테가노그래피 : 메시지 은폐, 숨김. 초기 암호 유형

### 해시

|  |
| --- |
| 목적: 무결성 확보, 위변조 확인  특징:  **1. 단방향, 일방향 함수**  **2. 고정된 길이의 문자열 생성**  **3. 충돌저항성**  **4. 역상저항성**  MD (Message Digest), SHA (Secure Hash Algorithm)  MD5, SHA1, SHA256, SHA384, SHA512 |

### 대칭키, 비밀키

대칭키 문제점: **암호키 전달의 문제**

|  |  |
| --- | --- |
| 종류 | 특징 |
| DES | 64비트 블록 암호화  암호화키 크기 56비트 |
| 3DES | DES가 복호화가 가능해짐에 따라 AES 나오기 전까지 임시로 사용  DES와 달리 2개의 암호화키 사용 🡪 DES보다 2배의 암호화 강도 |
| AES | NIST 공모  128/192/256 암호화키 지원 |
| SEED | 한국인터넷진흥원 주도  128비트 블록 암호 알고리즘 |
| ARIA | 국가보안기술연구소, 국가정보원 주도  국가표준  128 비트 블록 암호화  128/192/256 암호화키 지원 |

### 비대칭키, 공개키-개인키

#### 종류

|  |  |
| --- | --- |
| 종류 | 특징 |
| Diffie–Hellman key exchange  디피 헬만 키 교환 알고리즘 | a: 공개된 정보  p, q: 각자 유지하고 있는 정보  1. 공개된 정보 a를 가지고 다음 정보 공유: ,  2. 받은 정보를 바탕으로 , 계산  3. 위 두 값은 동일함  서로 자신이 가진 키 정보를 전달하지 않고도,  같은 비밀키를 공유할 수 있음 |
| RSA 알고리즘 | 정수론, 소수  중요 정보를 2개의 소수로 표현한 후, 두 소수의 곱을 힌트와 함께 전송  1. 각자 고유한 공개키 N값 (두 소수의 곱)을 가짐  이때 개인키는 p, q 두 소수이다. |

#### 효과

|  |  |
| --- | --- |
| 기밀성 | A의 공개키로 암호환 내용은 A 비밀키를 가진 A만 볼 수 있음 |
| 부인방지 | A의 공개키로 복호화가 가능한 것은,  오직 A의 비밀키를 통해서 암호화했을 때임 |

### 공개키 기반 구조 (PKI, Public Key Infrastructure)

#### 개념

- 메시지의 암호화 및 전자서명을 제공하는 복합적인 보안 시스템 환경

- 인증서란? 인증서는 **공개키와 공개키의 소유자를 연결**시켜주는 전자 문서

- 공인인증서는 신뢰할 수 있는 기관(CA)이 전자서명하여 생성하며 공개키를 공증한다.

#### 기관 종류 (계층적 구조)

|  |  |
| --- | --- |
| 기관 | 내용 |
| PAA | - Policy Approval Authorities  - 정책 승인 기관  - 공인인증서에 대한 정책을 결정하고 하위 기관의 정책을 승인  - 미래창조과학부 담당 |
| PCA | - Policy Certification Authorities  - 정책 인증 기관  - **RootCA** 발급  - 한국정보보호진흥원 담당 |
| CA | - Certification Authorities  - 인증 기관  - 인증서 발급 및 취소  - yessign(금융결제원), NCA(한국 전산원) |
| RA | - Registration Authorities  - 등록 기관  - 사용자 신분 확인 및 CA 간 인터페이스 제공 |

#### 상호인증 (네트워크 구조)

- 두 인증 기관이 상대방의 공개키를 서로 인증해주는 인증서를 발급하여 사용하는 것

- 상호인증서 (**cross-certificate**)

#### 인증서 폐기목록

인증서 폐기목록 (CRL, Certification Revocation List)를 주기적으로 참조하여 해당 공인인증서의 유효성을 검증할 수 있다.

## 전자상거래

### 보안 요건

|  |  |
| --- | --- |
| 기밀성 | 거래 정보 유출 방지 |
| 무결성 | 거래 정보 조작 방지 |
| 부인 방지 | 거래 사실 부인 방지 |
| 효과적인 인증 수단의 확보 | 다른 사용자로 위장하는 것 방지 |

### ★ 전자서명, 전자봉투, 전자결재

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 전자서명 | Digital Signature  문서에 대해 개인키를 통해 생성한 해시값을 첨부  ★★ 효과   |  |  | | --- | --- | | 위조 불가 | 해시값 첨부를 통해 위조 불가 | | 인증 | 공개키를 통해 서명 검증 가능 | | 재사용 불가 | - **Salt** 개념  - 문서 + 개인키에 대한 해시값으로 다른 문서에 대해서는 다른 종류의 서명이 생성됨 | | 부인 방지 | 오직 서명자만이 서명 가능 (개인키 필요) | |
| 전자봉투 | - **암호문 + 전자봉투**  - **암호문**: 보내고자 하는 내용을 비밀키(대칭키)로 암호화하여 전달  - **전자봉투**: 비밀키 전달은 상대방의 공개키로 암호화 하여 전달 |
| 전자결재 | - 전자봉투 + 이중서명  - 전자봉투를 통해 비밀키 전달  - **이중서명**  \* 목적: **상점**이 사용자의 계좌번호와 같은 **지불정보**를 모르게 하고,  **은행**은 사용자가 구매한 물품 등 **구매정보**를 모르게 하기 위함  \* 구체적인 과정은 어려워서 생략함 |