Snort룰

형식 : action 프로토콜 출발지IP주소 출발지Port ->(방향) 목적지IP주소 목적지Port (msg : " "; content : " ";offset: ;depth: ; nocase;.. threshold:type <limit | thershold |

<패턴 매칭 방법>

1) 바이너리 비교 방법 : 속도가 빠름
2) 텍스트 비교 방법 : 속도가 느리지만 유연한 패턴 매칭을 제공

1) alert : 정해진 방식에 따라 alert를 발생시키고 패킷을 기록
2) log : 패킷을 로그로 남긴다
3) pass : 패킷을 무시한다
4) activate : alert를 발생시키고 대응하는 dynamic 시그니처를 유효하게 한다
5) dynamic : activate action에 의해 활성화 되면 log action과 동일한 액션을 취한다
6) drop : 탐지한 패킷을 차단하고 로그를 남긴 후 차단 메시지를 보내지 않는다.
7) reject : 탐지한 패킷을 차단하고 로그를 남긴 후 차단 메시지를 보낸다(TCP의 경우 TCP Reset을 UDP인 경우 ICMP Port Unreachable 메시지로 응답)
8) sdrop : 패킷을 차단하지만, 로그를 남기지 않는다

<type의 종류>

1) linit : 출발지(by_src) 또는 목적지(by_dst) IP를 기준으로 매 s초 동안 c번째 이벤트까지 액션을 수행한다
2) threshold : 출발지(by_src) 또는 목적지(by_dst) IP를 기준으로 매 s초 동안 c번째 이벤트마다 액션을 수행한다
3) both : 출발지(by_src) 또는 목적지(by_dst) IP를 기준으로 매 s초 동안 c번째 이벤트시 한번 액션을 수행한다

content 옵션에서 바이러니 형식의 데이터를 표현할 경우에는 파이프 기호(|) 사이에 핵사값으로 표현한다

수리카타

OISF 단체에서 오픈 소스 프로젝트로 개발한 IDS/IPS로 2010년에 발표
기존 Snort의 단일 스레드 방식에서 벗어나 대용량 트래픽을 실시간으로 처리할 수 있도록 멀티 코어/멀티 스레드를 지원하며 기존 스노트도 완벽하게 호환하는 장점

<주요 특징>

- 멀티 코어 및 멀티 스레드 지원
- 스노트 룰 완벽 호환 및 대부분 기능을 지원
- 하드웨어 벤더의 개발 지원으로 하드웨어 가속 지원
- 스크립트 언어(Lua) 지원

iptables

리눅스 커널에 내장된 패킷 필터링 기능을 제공하는 netfilter 기능을 관리하기 위한 툴로 rule기반의 패킷 필터링 기능등을 제공

<주요기능>
- 상태 검사 기능 제공
- NAT(네트워크 주소 변환) 기능 제공
- 패킷 레벨에서의 로긴 기능 제공
- 확장 모듈을 통한 다양한 추가 기능 제공

*추가옵션
--limit ?/s : 최대 초당 ?초까지
-m recent --update --seconds (초) --hitcount (개수) --name (목록이름) : 동일 IP로 -초 동안 -번이상 발생]
-m conlimit --conlimit-above (개수) : 개수를 초과하는 동시 연결을 제한한다
동일 IP 관련 대표적인 확장 모듈
- connlimit : 동일 출발지 IP의 동시 연결개수에 대한 제한 목적의 모듈
- recent : 지정한 시간 범위 내 동일 출발지 IP의 연결 요청개수에 대한 제한 목적의 모듈

(체인) 패킷이 이동하는 경로 -> 체인별로 룰(정책) 설정이 이루어짐
1) INPUT 체인 : 외부에서 방화벽 호스트를 목적지로 하여 들어오는 패킷이 이동하는 경로
2) OUTPUT 체인 : 방화벽 호스트를 출발지로 하여 외부로 나가는 패킷이 이동하는 경로
3) FORWARD 체인 : 방화벽 호스트를 거쳐서(경우해서) 나가는 패킷이 이동하는 경로로 네트워크 경로상에 방화벽 호스트를 별도로 구축해서 경유 트래픽을 필터링

(옵션)
-A : 체인의 마지막에 해당 룰(규칙)을 추가한다
-D : 체인에서 해당 룰(규칙)을 삭제한다(행 번호 지정 시 특정 위치의 룰삭제)
-I : 체인의 첫 행에 해당 룰(규칙)을 삽입한다(행 번호 지정 시 특정 위치에 삽입)
-n : 룰(규칙)의 주소 정보(IP, Port)를 숫자 형식으로 출력

iptables-save > "저장할 파일명" : 변경된 정책을 저장하고 종료할 수 있는 명령어
iptables-restore < "복원할 파일명" : 파일에 저장된 룰셋을 복원

침입차단시스템(방화벽) 구현 방식에 따른 구분

1) 패킷 필터링 방식
- 네트워크 계층의 출발지/목적지 IP 주소, 전송 계층의 출발지/목적지 port 번호, 프로토콜을 기반으로 방화벽 정책에 따라 패킷 필터링(허용/차단 등)을 수행하는 방식

2) 상태 검사(Stateful Inspection) 방식
- 프로토콜별 연결 상태 정보(세션 정보)를 추적하여 방화벽 정책에 따라 패킷 필터링을 수행하는 방식으로 패킷 필터링 방식에 상태 검사 기능이 추가된 형태
- 메모리상에 상태 흐름 테이블을 생성하여 모든 송수신 패킷의 연결 상태(세션) 정보를 일정 시간 동안 유지함으로써 보다 빠르고 높은 보안성을 제공
- 효율적인 방화벽 룰셋 설정과 연결된 상태의 패킷인 것처럼 위조한 패킷의 접근을 차단할 수 있으므로 보안상의 장점
- 연결된 상태의 패킷에 대해서는 추가적인 룰셋 검사를 수행하지 않으므로 성능상의 장점

3) 애플리케이션(응용) 게이트웨이 방식
- 응용 계층 서비스(HTTP, SSH, FTP등)에 대한 중계 역할(프록시 역할)을 하면서 방화벽 정책에 따라 서비스 제어, 사용자 인증, 로깅 및 감사추적 등의 기능을 수행하는 방식

4) 회선 게이트웨이 방식
- 전송 계층 트래픽(TCP, UDP등)에 대한 중계 역할을 하면서 방화벽 정책에 따라 연결 제어, 로깅 및 감사 추적 등의 기능을 수행하는 방식
- 전송 계층에서 동작하기 때문에 응용 계층 서비스에 대한 제어는 불가능함

침입차단시스템(방화벽) 구축 방식에 따른 구분

1) 스크리닝 라우터 방식
- 패킷 필터일 기능을 이용해 방화벽 기능을 함께 수행하는 라우터를 말함
- 일반적으로 외부 네트워크와 내부 네트워크 경계에 있는 경계 라우터를 주로 이용

2) 듀얼 홈드 게이트웨이 방식
- 두 개의 네트워크 인터페이스가 설치된 배스천 호스트로 하나의 인터페이스는 외부 네트워크와 연결되고 다른 하나의 인터페이스는 내부 네트워크와 연결되어 내부와 외부 사이의 접근 제어를 수행

3) 스크린드 호스트 게이트웨이 방식
- 스크리닝 라우터와 싱글 또는 듀얼 홈드 게이트웨이를 조합하여 구성한 방식으로 외부 네트워크에서 내부 네트워크로 들어오는 트래픽은 일차로 스크리닝 라우터에

4) 스크린드 서브넷 게이트웨이 방식
- 스크리닝 라우터들 사이에 듀얼 홈드 게이트웨이를 조합하여 구성한 방식으로 외부 네트워크와 내부 네트워크 사이에 DMZ이라는 네트워크 완충지역 역할을 하는

패킷 필터링 기술

- Ingress 필터링 : 외부에서 내부 네트워크로 들어오는 패킷에 대해 출발지 IP를 체크하여 위부에 존재할 수 없는 IP(사설 IP, 루프백 IP등)을 필터링

- Egress 필터링 : 내부에서 외부 네트워크로 나가는 패킷에 대해 출발지 IP를 체크하여 내부에서 관리하는 IP주소가 아니면 조작된 주소로 판단하여 필터링

proc 파일 시스템

- 유닉스/리눅스 커널이 사용 중인 프로세스 자원, 커널 파라미터 등에 대한 상태 정보를 관리하기 위해 파일 형식으로 정보를 보관하는 영역 -> 가상 파일시스템
- 물리적 디스크 영역이 아닌 메모리 영역에 존재하는 파일 시스템으로 부팅 시마다 새롭게 생성된다
- proc파일 시스템에 PID별로 디렉터리가 생성되어 있으며, 각 PID디렉터리를 보면 해당 프로세스 관련 상태정보들이 파일 형식으로 존재하고 있음
- 루트킷 참지 프로그램들은 ps를 실행하여 보이는 정보와 proc 디렉터리에 있는 프로세스 정보를 비교하여 숨겨진 프로세스가 있는 지 검사

NTP

- 네트워크상에 시스템들의 시간을 동기화하는 프로토콜로 UDP 123 포트를 사용
- 서버의 'monlist'기능을 이용해 DDoS를 발생시킬 수 있는 취약점이 발견되어 보안업데이트가 권고됨

* monlist기능 : NTP 서버에 최근 접속한 클라이언트 주소 정보를 전송해주는 기능

DLL 인젝션

DLL : Dynamic Link Library, 마이크로소프트 윈도우에서 구현된 동적 라이브러리로 여러 프로그램이 실행 중에 사용할 수 있는 공통적인 데이터와 함수들로 구성

개요 : 실행 중인 프로세스에 특정 DLL 파일을 강제로 삽입시키는 기법

용도 : 실행 중인 프로세스에 삽입된 DLL을 구현한 사용자가 원하는 작업(새로운 기능 추가, 백도어/키로깅 등의 악성 행위)을 해당 프로세스가 수행하도록 한다

구현 원리 : 외부에서 특정 DLL을 로드하여 실행하는 API를 호출하도록 실행 중인 프로세스에 명령을 전달하여 해당 DLL을 구현한 사용자가 우너하는 코드를 실행하도

쉘쇼크(Shell Shock)

취약점 : Bash 쉘이 제공하는 함수 선언 기능 -> () {로 시작하는 함수 선언문 끝에 임의의 명령어를 추가로 삽입하여 환경변수에 저장할 경우 삽입한 명령어까지 실행도

리버스 쉘 연결을 위한 공격으로 주로 이용이 됨

보안 관제 모니터링

보안장비 모니터링 : 위협관리시스템(TMS), 침입차단시스템, 침입탐지시스템, 등 네트워크 상황에 대한 실시간 감시 기능을 이용하여 실시간 공격 정보, 네트워크 트래

서버 모니터링 : 주요 시스템에 대한 health Check 모니터링 결과를 종합상황판에 표시하여 정기적으로 가용성을 확보

트래픽 모니터링 : 인터넷 주요 구간의 패킷에 대한 흐름 상태를 종합상황판에 제공하여 상태를 관리

악성코드

다운로더 : 악성코드에서 지정한 주소에 접속하여 추가 악성코드를 다운로드하여 실행시키는 악성코드 -> 드롭퍼와 같이 백신 프로그램을 우회하는 목적으로 사용

드롭퍼 : 다운로더와 유사하게 새로운 악성코드를 생성하지만, 다운로더가 외부에서 파일을 다운받는 것에 비해 드롭퍼의 경우 자신 내부에 포함된 데이터를 이용하여 악성코드를 생성한다는 차이점

인젝터 : 드롭퍼의 특수한 형태로 파일을 생성하지 않고 자신의 데이터를 이용해 바로 새로운 프로세스를 생성하여 메모리에 상주시키는 형태의 악성코드

취약점 표기 방법

CVE - (해당연도) - (취약점 번호)

ESM(Enterprise Security Mangement)

다양한 보안장비(솔루션)에서 발생하는 보안 정보를 단일 관제 환경에서 수집, 분석 및 대응함으로써 보안 장비(솔루션)간 상호연관분석과 일관성 있는 보안 정책 적용

상호연관분석 : 동종 또는 이기종의 여러 보안장비에서 발생하는 보안 정보 간에 연관성을 분석하는 것으로 보안 위협에 대한 보다 정확한 판단과 대응을 가능하게 한다

<구성요소>

- ESM 에이전트 : 관리 대상 보안장비에 설치되어 사전에 정의된 규칙에 따라 보안 정보를 수집하여 ESM매니저로 전달하는 기능을 수행
- ESM 메니저 : ESM 에이전트로부터 전달받은 보안 정보를 저장하고 이를 분석한 결과를 ESM 콘솔로 전달하는 기능을 수행
- ESM 콘솔 : ESM 매니저로부터 전달받은 분석 결과에 대한 시각화, 조회, 리포팅 등의 기능과 ESM 에이전트/매니저에 대한 제어 기능을 수행

SIEM(Security Information & Event Management)

보안장비뿐만 아니라 서버 장비, 네트워크 장비, 엔드 포인트, 애플리케이션 등 다양한 원천으로부터 보안 정보(이벤트, 로그등)를 수집하고, 빅데이터 기반의 상관관계 분석을 통해 보안 위협을 예측해내는 보안관제(운영/관리) 솔루션

1) 데이터 통합 : 다양한 원천에서 발생하는 보안 정보를 수집하여 통합
  - 정보(로그) 수집 : 관리 대상 장비에 설치된 에이전트 또는 SNMP, syslog 방식 등을 이용하여 정보(로그) 수집
  - 정보(로그) 변환 : 다양한 정보(로그) 표현형식을 표준으로 변환하는 과정
2) 상관관계 분석 : 수집한 정보를 유용한 정보로 만들기 위해 다양한 상관관계 분석 기능을 제공
  - 정보(로그) 분류 : 이벤트 발생 누적 횟수 등 유사한 정보를 기준으로 그룹핑하여 단일 정보로 취합하는 과정
  - 정보(로그) 분석 : 여러 개의 정보 간 연관성을 분석하는 과정
3) 알림 : 이벤트 발생 시 보안 담당자에게 자동으로 알린다
4) 대시보드 : 분석한 결과에 대한 시각화, 조회 등의 기능을 제공

SSL/TLS 관련 주요 취약점

1) HEIST 취약점
- 자바스크립트로 브라우저에 대한 사이드채널 공격을 통해 암호문의 정확한 크기를 알아냄

(대응 방안) 제3자 쿠키 비허용, 자바스크립트 사용 비활성화

2) DROWN 취약점
- SSL 2.0 취약점을 이용하여 TLS 연결 해독 가능

(대응 방안) SSL 2.0 사용 금지

3) FREAK 취약점
- 수출 등급 RSA 사용을 유도하여 brute-force 공격으로 키를 얻어냄

(대응 방안) RSA EXPORT Cipher Suites 비활성화

4) POODLE 취약점
- TLS 연결을 SSL 3.0으로 낮춰 SSL 3.0 취약점을 이용하여 암호문을 해독

(대응 방안) SSL 3.0 사용금지

OpenSSL 하트블리드 취약점

오픈소스 암호화 라이브러리의 취약점으로 서버에 저장된 중요 메모리 데이터가 노출됨 -> |18 03 ??| 패턴의 데이터가 SSL서비스 포트로 전송됨

보안장비를 이용하지 않고 취약점을 해결하는 방법
- OpenSSL 버전을 취약하지 않은 최신 버전으로 업데이트
- 서버 측 SSL 비밀키가 이미 유출되었을 가능성이 있으므로 SSL 서버인증서를 재발급받는다.

chattr(Change attribute) 명령어

리눅스 파일시스템에서 파일 속성을 설정(변경)하는 명령어

<주요 옵션>
형식 : chattr +-=[속성] [파일 or 디렉터리], 속성 추가 시 +, 속성 삭제 시 -, 속성 설정 시 =
chattr +I 파일명 : 해당 파일에 읽기 전용(immutable) 속성을 추가 -> 해당 파일은 읽기만 가능하고 내용 변경, 추가 및 삭제가 불가능
chattr +a 파일명 : 해당 파일에 내용 추가만(append) 허용 -> 로그파일 같은 경우 변경, 삭제는 못하게하고 추가만 가능하게 할 때 유용
chattr +A 파일명 : 해당 파일의 접근 시간(Access Time)을 변경하지 않는다. ->웹 사이트의 기본 페이지같이 빈번하게 접속하는 파일의 경우 접근시 마다 access time

lsattr 명령으로 chattr로 설정한 속성을 확인할 수 있다

악성코드 분석 방법

1) 동적 분석
- 악성 코드를 직접 실행시켜서 어떤 행위들이 나오는지 분석하고 의심스러운 행위가 보이면 악성코드로 진단하는 방식
- 가상의 이용자 PC환경을 구성하고 다양한 취약점에 노출시킨 후 점검 대상 홈페이지에 접속하여 비정상적인 레지스트리 변경, 악성코드 다운로드, C&C 서버 접속 등의 악성 행위를 분석하는 기법
- 이용 환경에 대한 행위분석이라고도하며 탐지 패턴을 이용하지 않기때문에 신종 악성코드 탐지가 가능하나 상대적으로 분석 속도가 느린 단점이 있음

2) 정적 분석
- 악성 코드를 실행하는 것이 아니라 실행파일에 대한 디버거를 통한 API 호출 관계 분석, 파일 헤더 및 바이너리 내 문자열 분석 등을 통해 악성코드 여부를 판단
- 점검대상 홈페이지 웹 프로그램 소스코드를 분석하여 알려진 악성코드 경유지/중계지/유포지 또는 악성 스크립트 문자열을 포함하는 악성 링크가 있는지를 탐지하는 방식

Log4j 취약점

- Apache 재단의 오픈 소스 JAVA 기반 로깅 라이브러리 사용 시 발생하는 취약점
- JAVA 기반의 JVM 호나경에서 해당 라이브러리를 사용하는 모든 서비스에서 발생할 수 있는 취약점으로 JNDI Lookup 메소드를 입력값 검증 없이 호출할 때 임의의

NTP 취약점 대응방안

*monlist 기능 : NTP 서버가 취근 접속한 서버정보를 요청하는 명령 -> DRDoS 공격으로 활용됨

1) ntpd --version : NTP 데몬의 버전을 확인하여 monlist 기능이 해제된 최신 버전으로 업그레이드 한다

2) disable monlist : NTP 데몬의 monlist 기능을 해제

3) ntpdc -c monlist "점검대상 NTP 서버 IP" : 점검 대상 NTP 서버가 monlist 명령을 허용하는지 여부를 점검

4) iptable -A OUTPUT -p udp --sport 123 -m length --length 100: -j Drop : iptable을 이용하여 100byte이상의 NTP 응답을 차단
(NTP 포트 : 123/udp) (통상적으로 정상적인 NTP 응답은 100byte이하이며 공격 패킷은 400byte 내외이기에 응답패킷의 크기를 제한

IDS(침입탐지 시스템)의 탐지방식에 따른 분류

1) 오용탐지
- 사전에 등록한 알려진 공격 패턴을 기반으로 공격 행위를 탐지하는 방식으로 '지식 기반 탐지' 또는 '시그니처 기반 탐지'라고도 한다

2) 이상 탐지
- 정상적이고 평균적인 상태를 기준으로 이를 벗어난 행위가 발생하면 탐지하는 방식으로 '행위 기반 탐지' 또는 ' 통계 기반 탐지'라고도 함다.

IDS(침입탐지시스템) 설취위치에 따른 장단점

1) 라우터를 통과하기 이전 트래픽을 탐지할 수 있는 위치
(장점) 외부(인터넷)에서 접근하는 모든 트래픽을 탐지할 수 있다
(단점) 라우터의 필터링 이전에 탐지하기 때문에 공격행위로 탐지한 트래픽이 라우터를 통과한 트래픽인지 판단하기 어렵고 대량의 트래픽으로 인하여 성능상의 문제

2) 라우터를 통과한 트래픽을 탐지할 수 있는 위치
(장점) 라우터를 통과하여 내부로 유입된 트래픽만을 효율적으로 탐지할 수 있다
(단점) 방화벽의 필터링(방화벽 룰셋) 이전에 탐지하기 때문에 공격행위로 탐지한 트래픽이 방화벽을 통과한 트래픽인지 판단하기 어렵고 방화벽 뒷단의 보호 구간내

3) 방화벽을 통과한 트래픽을 탐지할 수 있는 위치
(장점) 방화벽을 통과하여 보호 구간 내 공개 서버에 유입된 트래픽만을 효율적으로 탐지 할 수 있고 보호 구간 내에서 발생하는 트래픽에 대해서도 탐지할 수 있으므로 설치 우선순위가 가장 높다

NAC(Network Access Control)

과거 IP관리 시스템에서 네트워크에 대한 통제 기능을 더욱 강화한 보안 솔루션

윔 등의 보안 위협으로부터 안전한 단말기들로 이루어질 수 있도록 강제하는 역할

대표적이니 오픈소스 NAC 솔루션으로 PacketFence, FreeNAC등이 있다

DRM(Digital Right Management)

기술

<구성 요소>
1) 식별자(Identifier) : 컨텐츠를 식별할 수 있는 식별자
2) 메타데이터 : 컨텐츠 생명 주기 내에서 저작권 관리에 필요한 정보(저작권자 정보, 유통 정보등)
3) 패키저 : 컨텐츠를 메타데이터와 함께 배포할 수 있도록 묶어(패키징하여) 시큐어 컨테이너 포멧 구조를 만드는 프로그램
4) 시큐어 컨테이너 : 배포된 컨텐츠를 안전하게 유통하기 위해 전자적 보안 장치로 유통되는 컨텐츠의 배포 단위
5) DRM 제어기 : 배포된 컨텐츠의 이용 권한을 통제하는 프로그램

보안 솔루션(장비) 취약점 유형

1) 계정 관리
- 보안장비 기본 계정 변경 취약점 : 기본 계정은 장비 제조업체에서 출고 시 설정되어 나오는 기본 관리자 계정을 말한다 / 이를 변경하지 않고 사용할 경우 공격자의 불법적인 접근이 발생할 수 있다
- 보안장비 기본 패스워드 변경 취약점 : 기본 관리자 계정의 패스워드를 변경하지 않고 사용할 경우 공격자의 불법적인 접근이 발생할 수 있다
- 보안장비 계정별 권한설정 취약점 : 계정별 권한 설정이 미흡할 경우 권한 없는 자에 의해 보안장비 설정 변경이 발생할 수 있다.

2) 접근 관리
- 보안장비 원격관리 접근 통제 취약점 : 원격 접속 IP에 대해 접근 통제를 하지 않을 경우 공격자에 의한 계정 탈취가 발생했을 때 불법적인 접근이 발생할 수 있다 -> 관리자 IP 또는 특정 IP 및 계정에서만 접속할 수 있도록 조치
- 보안장비 보안 접속 취약점 : SSH, HTTPS 등의 보안 접속을 하지 않으면 공격자에 의한 스니핑 공격이 발생할 수 있다

주요 소프트웨어 보안 취약점 분류 체계 및 평가 체계

1) CVE(Common Vulnerabilities and Exposure)
- MITRE 사에서 운영하는 공개적으로 알려진 소프트웨어의 보안 취약점을 표준화한 식별자 목록으로 서로 유사한 취약점 정보가 관련 기관 및 보안 업계 간 상이하게

2) CVSS(Common Vulnerabilities Scoring System)
- MITRE 사에서 관리하는 보안 취약점 평가 체계로 기본 기준, 시간적 기준, 환경적 기준을 고려하여 취약점의 심각한 정도를 0.0부터 10.0까지 수치화하며 숫자가 높

3) CWE(Common Weakness Enumeration)
- MITRE 사가 중심이 되어 여러 업체와 연구기관이 협력하여 소프트웨어에서 공통으로 체계적으로 분류한 목록으로 소프트웨어 개발 생명주기에서 발생할 수 있는

4) CWSS(Common Weakness Scoring System)
- MITRE 사에서 관리하는 보안 취약점 평가 체계로 CWE에 등록된 취약점의 위험성을 정량화하기 위한 점수 체계를 말한다

SSDP(Simple Service Discovery Protocol)

네트워크상의 서비스나 정보를 검색하는 프로토콜로 프린터, 스캐너, IP 카메라 등 IoT 기기의 네트워크 탐색 용도로 사용된다.

1900/udp 포트를 사용하여 기기검색을 수행하며 검색 요청 대비 응답 패킷이 상대적으로 매우 크기에 증폭 반사 공격에 악용됨 -> SSDP 증폭 공격

네트워크 보안장비의 설치 모드(Ex. NAC, IDS, IPS, 방화벽 ..)

1) 미러링 모드
- 물리적인 네크워크 경로밖에 위치하여 미러링 장비(패킷을 복제해주는 장비)로부터 복제된 트래픽(패킷)을 받아서 처리하도록 설치하는 모드
(장단점)
- 물리적인 네트워크 경로밖에 위치하기 때문에 네트워크 구성 변경이 불필요하고 장비 장애시 전체 네트워크 장애를 유발하지 않는다는 장점
- 복제된 트래픽(패킷)을 받아서 탐지하기 때문에 실시간 차단이 어렵다는 단점

2) 인라인 모드
- 물리적인 네트워크 경로상에 위치하여 연결된 네트워크를 통과하는 모든 트래픽(패킷)이 장비를 거쳐가도록(통과하도록) 설치하는 모드
(장단점)
- 실제 트래픽(패킷)이 장비를 거쳐가기 때문에 실시간 탐지뿐만 아니라 차단까지 가능하다는 장점
- 물리적인 네트워크 경로상에 위치하기 때문에 네트워크 구성 변경이 필요하고 장비 장애 시 전체 네트워크 장애를 유발할 수 있는 단점

DLP(Data Loss Prevention) 솔루션

기관/조직의 중요한 데이터(정보)가 내부에서 외부로 유출되는 것을 방지하는 솔루션
HTTPS등 암호화 통신에서도 내부 중요 문서가 송수신되는 것을 탐지할 수 있다
데이터 보관/사용/전송 과정을 모두 모니터링하여 데이터가 유출되는 것을 감시하고 유출이 확인될 때 차단하는 방식으로 동작

1) 네트워크 DLP
- 내부에서 외부로 나가는 트래픽을 모니터링 하여 데이터 유출을 감시하고 제어하는 방식

2) 엔드포인트(단말) DLP
- 앤드포인트에 설치된 에이전트를 통해 데이터 유출 관련 이벤트를 감시하고 제어하는 방식

사이버 위기 경보 단계

1) 정상 단계 : 전 분야 정상적인 활동 단계

대한 탐지 활동 강화가 필요한 단계

3) 주의 단계 : 침해사고가 일부 기관에서 발생했거나 다수 기관으로 확산할 가능성이 증가하고 있는 상황으로 국가 정보시스템 전반에 보안 태세 강화가 필요한 단계

4) 경계 단계 : 침해사고가 다수 기관에서 발생 했거나 대규모 피해로 발전될 가능성이 증가하고 있는 상황으로 다수 기관의 공조 대응이 필요한 단계

5) 심각 단계 : 침해사고가 전국적으로 발생했거나 피해 규모가 대규모인 사고가 발생한 상황으로 국가적 차원에서 공동 대체가 필요한 단계

익스플로잇(Exploit)

소프트웨어나 하드웨어의 버그 또는 취약점을 이용하여 공격자가 의도한 동작이나 명령을 실행하도록하는 코드나 행위

(쉘 코드)

- 익스플로잇 수행 시 공격자가 의도한 명령을 담고 있는 어셈블리(기계어)로 작성된 작은 크기의 코드
- 쉘(바인드 또는 리버스 형태의 쉘)을 실행시키는 코드

(NOP 슬라이드)

- 아무 기능도 수행하지 않는 명령
- 기계어 코드의 헥사값 : 0x90
- 프로그램에서 NOP명령은 빈 영역을 채우기 위한 명령으로 해당 명령을 만나면 아무런 동작 없이 다음 명령으로 넘어감
- 익스플로잇 코드에서 NOP 명령을 삽입하는 이유
  -> 쉘 코드가 위치한 메모리상의 주소를 정확히 알 수 없으므로 실행 확률을 높이기 위해 다수의 NOP 명령을 쉘 코드 앞에 삽입하여 해당 영역을 가리키기만하면 NOP을 타고 최종적으로 쉘 코드가 실행되도록 하기 위함

(어셈블리어)

- 기계어와 1:1로 대응되는 저수준 프로그래밍 언어
- RET(Return Address) 명령은 CALL 명령을 통해 호출된 함수에서 수행을 마치고 원래 호출한 함수로 복귀하기 위해 사용하는 명령 / ESP 레지스터가 가리키는 값을 ELP 레지스터에 저장하는 기능

*ESP(Extended stack pointer) 레지스터 : 스택의 최상단 주소를 담고 있는 레지스터 / RET 수행 시점에 스택 포인터는 복귀주소 영역을 가리키고 있음

랜섬웨어 감염시 대응 절차

1) 증상 확인하기 : 파일 사용 불가, 파일의 확장자를 변경, 부팅 불가능 등

2) 피해 최소화를 위한 긴급조치 : 외부 저장장치 연결 해제, PC 전원 유지, 네트워크 차단, 복구 방법 확인 등

3) 신고하기 : 증거 남기기(감염 알림창과 암호화된 파일이 생성된 화면 캡처 및 저장), 신고기관에 신고하기

4) 데이터 복구하기 : 백업 매체 연결 및 데이터 복구

시스템의 함수 호출시 인수 저장 레지스터

64bit 리눅스 시스템에서 gdb를 통해 레지스터의 정보를 알수 있음

1) 64bit 리눅스 시스템

- 6개의 범용 레지스터 사용
- RDI, RSI, RDX, RCX, R8, R9 *첫번째인 RDI에는 인수의 주소가 저장되고 그 이후에 각각 코드값이 순서대로 저장
- 그 이상의 인수는 스택을 통해 전달

2) 64bit 윈도우 시스템
- 4개의 범용 레지스터
- RCX, RDX, R8, R9

권한 관리 솔루션(계정과 관련)

SSO : 한 번의 사용자 인증으로 여러 시스템에 접근할 수 있는 통합 인증(로그인) 솔루션으로 단일 인증을 통해 여러 시스템에 접근함으로써 사용자 편의성이 증대

EAM(Extranet Access Management) : 모든 사용자에 대한 통합인증(SSO)과 사용자별/그룹별 접근권한 통제를 담당하는 권한 관리 솔루션

IAM(Identity and Access Management)
EAM보다 포괄적으로 확장한 보안 솔루션으로 조직이 필요로 하는 보안 정책을 수립하고 자동으로 사용자에게 계정을 만들어주며, 사용자는 자신의 직무에 따라 적절

WireShark 필터

캡처 필터 : 실시간 패킷을 캡처할 때 사용하는 피리터로 BPF 구문을 사용

디스플레이 필터 : 캡처된 파일에서 원하는 패킷을 필터링할 때 사용하는 필터로 고유한 구문을 사용

(주요 필터 구문)
1) dns.flags.response==0 | 1 : 0은 질의를 의미, 1은 응답을 의미
2) dns.flags.authoritative==0 | 1 : 0은 recursive네임 서버의 캐시에 저장된 응답을 의미, 1은 authoritative 네임서버로부터의 응답을 의미
3) dns.flags.recdesired==0 | 1 : 0은 반복 질의/응답을 의미, 1은 재귀 질의/응답을 의미

윈도우 PE 파일(실행파일)의 섹션 헤더

각 섹션 데이터를 메모리에 로딩하고 속성을 설정하는데 필요한 정보를 담고 있음
* 섹션 : PE파일이 가상 주소 공간에 로드된 이후 프로그램 실행 코드, 데이터, 리소스 등 프로그램 실행에 필요한 정보를 배치한 영역을 말함
(주요 섹션)
- .text : 프로그램 실행 코드를 담고 있는 섹션
- .data : 읽기 쓰기가 가능한 데이터 섹션으로 전역변수와 정적변수 등이 위치
- .rdata : 읽기 전용 데이터 섹션으로 상수형 변수, 문자열 상수 등이 위치
- .bss : 초기화되지 않은 전역변수가 위치
- .idata : 임포트할 DLL과 그 API/함수들에 대한 정보를 담고 있는 섹션
- .edata : 익스포트할 DLL과 그 API/함수들에 대한 정보를 담고 있는 섹션
- .rsrc : 다이얼로그, 아이콘, 커서 등의 윈도우 애플리케이션 리소스 관련 데이터들을 담고 있는 섹션

MITRE ATT&CK(마이터 어택)

Adversairal(악의적인) Tactics(전술), Techniques(기법) and Common Knowledge의 약어
실제 사이버 공격 사례를 관찰한 후 공격자가 사용한 악의적인 행위에 대해서 공격 전술과 기법 관점으로 분석한 후 다양한 공격 그룹의 공격기법들에 대한 정보를 분

다양한 사이버 공격을 정의하고 설명하는 표준화된 프레임워크로 사이버 공격 분석에 공통으로 사용할 수 있다

다양한 사이버 공격의 전술, 기법, 그리고 절차를 설명한 프레임워크

보와의 연결고리가 없다는 한계점을 개선

공개 웹 방화벽

1) CATLE
- 한국인터넷진흥원(KISA)에서 제공하는 공개 웹 방화벽

2) WebKnight
- 아큐드로닉스(AQTRONIX)사에서 개발한 마이크로소프트사의 IIS 웹서버에서 동작하는 공개 웹 방화벽
- ISAP(Internet Server API) 필터 형태로 동작하며, IIS 웹서버 앞단에 위치하여 모든 웹 요청에 대해 필터 정책에 따라 웹 공격을 탐지 및 차단해주는 기능 제공

3) ModSecurity
- 트러스트웨이브(Trustwave)사의 SpiderLabs에 의해 개발된 Apache, IIS 등의 웹서버에서 동작하는 공개 웹 방화벽
- 웹 애플리케이션 공격에 대한 탐지 및 차단 기능뿐만이 아니라 웹 애플리케이션에 대한 실시간 모니터링 및 로그 분석 기능을 제공
- 일반적으로 OWASP의 RuleSet 또는 Trustwave사의 SpiderLabs 상용 RuleSet 적용이 가능

윈도우 레지스트리 최상위 루트키

1) HKCR : HKEY_CLASSES_ROOT
- 파일 확장명과 응용 프로그램의 연결 정보가 들어있고, 윈도우 시스템에 들어있는 개체들 및 응요 프로그램과 그 자동화에 대한 정보도 들어 있다
- 인터페이스 기능에 대한 바로가기 관련 키도 들어있다.

2) HKCU : HKEY_CURRENT_USER
- 현재 로그인 중인 사용자의 환경 설정(프로파일) 정보를 가지고 있다
- 주요 환경 설정 정보에는 제어판 설정, 네트워크 연결, 응용 프로그램 등이 있으며 HKU 루트키에 있는 해당 사용자 정보에 대한 링크를 가지고 있다

3) HKLM : HKEY_LOCAL_MACHINE
- 개별 사용자 단위가 아닌 시스템 전체에 적용되는 하드웨어(드라이버, 프린트, USB등)와 응용 프로그램의 설정 데이터를 저장

4) HKU : HKEY_USER
- 사용자별로 존재하는 하이브 파일인 ntuser.dat파일을 로드하여 생성
- 다중 사용자 환경에서 사용자별로 키 항목을 생성하여 환경 설정(프로파일) 정보를 저장

5) HKCC : HKEY_CURRENT_CONFIG
- 현재 사용 중인 윈도우의 하드웨어 프로필 정보(디스플레이 정보, 폰트 정보 등)을 가지고 있다

DDE(Dynamic Data Exchage)

사용자 편의를 위해 윈도우 운영체제에서 응용 프로그램(주로 오피스 프로그램) 간 데이터 전송을 위해 사용되는 기능

<공격자의 악용>
- 정상적인 엑셀, 위드 파일로 보이지만 실행 시 악의적인 시스템 명령을 수행하여 악성 프로그램 다운로드, 데이터 유출 등의 행위를 수행하는 파일을 만들어 유포

<대응 방법>
- 파일 열람 시 확장자와 알림창(팝업창)을 주의 깊게 확인하여 의심스러운 프로그램의 실행에 대해서는 허용하지 않도록 한다
- MS워드, 엑셀 등의 프로그램 옵션을 확인하여 DDE 기능에 대한 제한을 설정

루트킷 탐지

1) chrootkit : 루트킷을 탐지하기 위한 프로그램으로 위변조 의심파일이 있을 경우 "INFEXTED"메시지를 보여준다

2) rpm -V 패키지명 : 해당 패키지로 설치된 파일이 최초 설치시와 비교해 변경사항이 있는지 여부를 체크할 수 있다
(확인할 수 있는 정보)
- S : 파일 크기 변경, M : 파일 퍼미션 변경, 5 : MD5 체크섬 변경, D : 장치 정보 변경
- L : 심볼릭 링크 정보 변경, U : 소유자 정보 변경, G : 소유그룹 정보 변경
- T : 파일 수정시간 변경

보안 취약점 점검 도구

1) 트립와이어(Tripwire) 점검 도구
- 파일시스템의 무결성을 점검하는 대표적인 도구로 오픈소스 도구
- 파일시스템 무결성 점검이란 파일시스템의 상태 추적 및 허가를 받지 않은 변경여부를 주기적으로 점검하여 의심스러운 변화가 감지되면 이를 검사하고 복구하는

2) 네서스(Nessus) 점검 도구
- 미국 Tenable사가 개발/배포하는 도구
- 취약점 점검 도구(스캐너)로 로컬 또는 원격지에서 다양한 방법을 통해 시스템, 네트워크, 웹 애플리케이션 등의 알려진 취약점에 대한 점검을 수행하며 점검을 통해

3) 닉토(Nikto) 점검 도구
- 웹서버 또는 웹 애플리케이션 취약점을 점검할 수 있는 공개 점검 도구(스캐너)로 방대한 취약점 데이터베이스를 이용하여 다양한 형태의 취약점을 스캔할 수 있다

DBD(Drive By Download) 공격

사용자가 홈페이지에 접속만 해도 자신의 의도와 무관하게 악성코드가 다운로드되어 설치되는 공격

일반적으로 난독화된 악성 스크립트를 통해 다수의 경유지/중계지를 거쳐 최종 유포지로 접속하여 악성 코드를 다운로드하도록 유도
이때, 악성코드 다운로드를 위해 사용자 PC에 설치되어 있는 운영체제, 인터넷 브라우저, 문서 편집기, 뷰어 등의 응요프로그램 취약점을 익스플로잇하는 방식을 사용한다.

<예방 방안>
- 사용자 PC환경의 응용 프로그램, 웹 브라우저, OS등에 보안 취약점이 발생하지 않도록 최신 보안업데이트를 지속적으로 수행
- 업무 목적 이외의 신뢰할 수 없는 사이트(상대적으로 보안이 취약한 웹 사이트)에 대한 접근을 제한(통제)한다

SOAR(Security Orchestration, Automation & Response) 솔루션

보안 오케스트레이션, 자동화 및 대응 솔루션
- 숙련된 보안 인력이 부족한 상황에서 지속적으로 증가하는 사이버 위협에 대응하기 위한 자동화된(표준화된) 분석 및 대응 솔루션
- 자동화된 업무 프로세스를 통해 보안 인력을 효율적으로 운영하면서 분석 및 대응에 대한 정확도(품질)을 높이고 시간을 단축할 수 있는 장점
- 보안 오케스트레이션 : 다양한 보안장비와 IT기기들을 연동하여 관리한다는 의미
- 자동화 : 보안 인력을 통해 이루어지는 단순하고 반복적인 업무를 자동화하여 업무 처리 품질 및 시간을 향상시킬 수 있다
- 인시던트 대응 : 사이버 위협을 탐지하고 대응하기 위한 조직의 프로세스와 기술

멀웨어 분석을 어렵게 하기위한 기법

1) 다형성 : 악성코드 자체의 기능은 변하지 않지만, 실행 시마다 코드의 내용이 변경되도록하여 시그니처 기반의 탐지를 어렵게 하는 기법

2) 패킹 : 실행파일의 크기를 줄이고 내부 코드와 리소스를 감추기 위해 압축 또는 암호화하는 기법

단답 용어
EDR 솔루션 : Endpoint Detection and Response, 엔드포인트에서 발생하는 알려지지 않은 공격 행위를 실시간으로 탐지하고 탐지된 위협을 차단할(분석 및 대응하여 피해 확산을 막는) 수 있는 다양한 대응 도구를 제
사이버 위협 인텔리전스(CTI) : 단순한 위협 정보가 아닌 지능적 위협 정보를 말함 : 다양한 내/외부 조직에서 경험한 보안 위협정보를 전문가 집단이 수집 및 분석하여 만들어 내는 증거 기반 위협 정보로 공격자, 공격 절차, 공격 방법(도구), 업무 영향도, 공격 탐지 및 대응 방법 등 다양한 정보를 포함한다
UTM(통합 보안 시스템) : Unified Threat Management, 다양한 보안 기능을 통합한 장비로 단일 장비로 다양한 보안기능을 수행 -> 경제성과 보안 관리 및 운영을 편리
date 명령어 : 현재 호스트의 날짜와 시간을 확인
ntpdate 명령어 : 원격지 NTP 서버에 접속하여 현재 시스템의 날짜 및 시간을 동기화하는 명령어
트러스트 존 : 암(ARM)사에서 개발한 하드웨어 기반 보안기술로 하나의 하드웨어 장치에 분리된 두개의 환경을 제공하여 보안이 필요한 정보를 격리된 환경에서 안전하게 보호하는 기술
strace 명령어 : 유닉스/리눅스 시스템에서 특정 프로그램(실행파일)의 시스템콜과 시그널을 추적하는데 사용하는 디버깅 도구
YARA - 악성코드에 포함된 텍스트 또는 바이너리 패턴 정보(시그니처)를 이용하여 악성코드를 식별하고 분류할 수 있는 오픈소스 프로젝트 도구 - 단순히 텍스트 또는 바이너리 패턴뿐만이 아니라 파일이나 프로세스의 오프셋, 가상 메모리 주소 활용 및 정규표현식 등을 이용하여 다양한 룰을 생성할 수 있음
말버타이징 - 악성코드와 광고의 합성어로 온라인 광고를 통해 악성코드를 유포시키는 행위 - 상대적으로 보안이 취약한 광고 서버를 해킹하여 불특정 다수를 공격하는 기법으로 랜섬웨어 등 악성코드 유포 통로 중 하나 - 사용자 모르게 PC를 감염시키기 때문에 악성코드 최초 유포지를 파악할 수 없는 어려움이 있다.
혹스(Hoax) - 거짓 정보를 토대로 메일을 보내 사용자를 속이는 방식의 협박성 사기 메일 - 남을 속이거나 장난을 목적으로 퍼트리는 가짜 바이러스이며 일반적으로 허위 바이러스 경고 메일 형태 - 계정 정보가 해킹됐다거나 개인의 은밀한 영상을 지인들에게 유포하겠다며 비트코인을 송금하라는 내용으로 메일 수신자를 협박
조크(Joke) - 악성코드의 일종으로 사용자에게 데이터 파괴 등의 구체적인 피해를 입히는 것은 아니지만 유사한 증상으로 사용자들을 놀라게 하는 프로그램 - 작업 방해를 하는 것이 목적
공급망 공격 - 일반적으로 제품이나 서비스가 공급자로부터 소비자에게 전달되기까지의 조직, 사람, 정보, 자원 등에 대한 시스템에 침투하여 사용자에게 전달되는 S/W나 H/W를
풋프린팅 - 직접적인 해킬을 하기정에 침입 시스템에 대한 정보를 수집하는 사전 작업 - 침입하기 위한 공격 대상의 보안 취약점, 도메인 이름, IP주소, 침입탐지시스템 설치 여부, 사용자 목록, 시스템의 하드웨어 사양, 사용 중인 네트워크 프로토콜, 인증

AVT(Advanced Volatile Treats) 지능형 휘발성 위협
- 디스크 상에 악성코드를 남기지 않고 메모리상에서만 실행시키면서 시스템 피해를 입히는 파일리스 공격
- 디스크 내에 악성코드가 파일 형태로 존재하지 않기 때문에 AV(Anti virus) 솔루션을 통한 파일 스캔이 불가능하여 탐지가 어려운 특징이 있다

퍼징(Fuzzing)
- 소프트웨어 보안 테스트 기법
- 프로그램 실행 시 무작위 데이터를 입력하여 그 결과로 애플리케이션에 오류 등이 발생하면 보안 취약점이 존재할 가능성이 크다고 판단하는 테스트
- 테스트 분야에 따라 웹 퍼징, 네트워크 프로토콜 퍼징, 파일 포멧 퍼징, 메모리 퍼징으로 구분