

과정명	
04차시	네트워크 보안운영

<1> 네트워크 계층별 보안 프로토콜과 취약점

[1] 계층별 보안 프로토콜

- 네트워크 보안 프로토콜은 데이터 링크 계층, 네트워크 계층, 전송 계층, 응용 계층 보안 프로토콜로 분류 가능
- (1) 데이터 링크 계층
 - PPTP, L2TP, L2F
- (2) 네트워크 계층
 - IPSec
- (3) 전송 계층
 - SSL
- (4) 응용 계층
 - SSH VPN, MIME

[2] 네트워크 보안 취약점 분석

- (1) 대상 시스템 결정
 - 네트워크 관리자가 네트워크에서 목표로 하는 시스템의 IP(internal protocol)를 확인
 - 네트워크 관리자는 온라인 시스템들에 대응되는 IP 주소들 확인
- (2) 가동 시스템 탐색
 - 많은 핑거프린팅(Fingerprinting) 기술을 사용하여 그 중에서 살아 있는 호스트를 찾음
 - 핑거프린팅 기술은 간단한 네트워크 관리 프로토콜 쿼리에서부터 복잡한 TCP/IP 스택 기반의 운영 시스템 확인까지 포함
- (3) 서비스 목록 탐색
 - 네트워크 관리자는 살아 있는 각각의 호스트에 대하여 포트 스캐닝 실시
 - 포트 스캐닝은 취약점 분석에서 가장 중요한 단계
 - 포트 스캐닝을 통해 네트워크 관리자는 TCP와 UDP 서비스를 발견 가능
 - 방화벽이나 IDS를 우회할 수 있는 다양한 스캐닝 방법이 있으며 TCP ACK와 TCP 윈도우 스캐닝 기술이 많이 사용됨
 - 특정 포트가 오픈 되어 있다고 메시지를 받게 되면, 그 포트 번호는 로깅 되고 후의 공격을 위하여 저장
- (4) 서비스 인식
 - 모든 열린 포트의 서비스 확인
 - 테스트는 비슷한 쿼리를 반복적으로 전송, 분석 도구는 시그니처에 대한 응답 값 분석
 - 알려진 애플리케이션의 시그니처와 응답 값 사이에 일치성이 확인되면 데이터는 후의 공격을 위하여 저장되고 다른 서비스에 대한 테스트를 계속 수행
- (5) 애플리케이션 확인
 - 네트워크 관리자는 서비스를 확인하는 단계에서 모든 서비스의 유형과 벤더를 정확하게 알게 됨
 - 하나의 애플리케이션 취약점을 진단할 때는 다른 애플리케이션에 영향을 주지 않는지 아니면 충돌이 발생하는지를 알아야 함
- (6) 네트워크 취약점 확인
 - 시스템이 테스트를 실행하기 위한 준비
 - 네트워크에서 모든 오픈된 포트와 특정 애플리케이션에 대응되는 서비스도 확인

- 취약점 분석 진단이 시작되고 다음 액티브 구성 조사가 실행된 후 마지막에는 시스템에 존재하는 취약점에 대한 커스텀 공격도 실행

(7) 발견된 취약점 보고

- 보고서에는 발견된 취약점이 높은 위험도를 가지는지 여부와 그에 대한 보안 대책을 기술

[3] 네트워크 보안 주요 위협

(1) 비인가 침입 시도

- 비인가 접근 시도가 성공할 경우 주요 웹 및 DB 서버에 접근하여 중요 정보 및 개인정보 유출
- 웹 서버 등 외부 접속점에 대한 보안대책을 강화하고 외부 네트워크와 내부 네트워크를 분리하여 비인가자의 내부 네트워크에 대한 접근을 통제해야 하며, 방화벽 등을 통해 DMZ 구간에서 내부망으로 접근을 엄격히 통제하거나 네트워크 침입 탐지 기능을 강화
- 내부 네트워크는 외부에서 직접 접근이 불가능하도록 네트워크 주소변환 기술을 적용하여 구성

(2) 유해 트래픽 전송

- 침입차단, 침입탐지시스템 등의 정보보호시스템은 네트워크를 통해 전송되는 웜·바이러스 등의 악성코드를 차단하는 데 한계가 있으며, 이로 인해 정보유출이나 네트워크의 가용성이 침해될 수 있음
- 서버 및 네트워크 자원에 대한 다양한 형태의 침입 행위를 실시간 탐지, 분석 후 비정상적인 패킷을 차단하여야 하며 패킷 실시간 분석과 학습을 통해 알려지지 않은 공격에 대응할 수 있는 기능과 시스템 장애 시에도 네트워크서비스의 중단을 방지할 수 있는 Fallover 기능을 제공하는 침입 방지 시스템 등을 운영해야 함

(3) 잘못된 네트워크 설정

- 불안정한 구조의 잘못된 네트워크는 허가 없는 사용자들이 시스템에 침입할 수 있게 해주는 주요 시작점으로 작용
- 허브(hub)나 라우터는 수신자 노드가 데이터 패킷을 받아서 프로세스 할 때까지 데이터 패킷을 브로드캐스트 함
- 집중형 서버를 사용하는 경우, 중앙 서버가 손상되면 네트워크 전체가 정지되거나 데이터 조작 또는 도난 당하기 쉬움

<2> 네트워크 기반 공격의 이해

[1] 서비스 거부(DoS) 공격

- 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격
- DoS 공격의 원리는 공격자의 시스템부터 공격 대상 시스템과 그 시스템에 속한 네트워크에 과다한 데이터를 전송하여 대역폭, 프로세스, 처리능력, 기타 시스템 자원을 고갈시키고 정상적인 서비스가 불가능하도록 하는 것

- DoS 공격의 형태

(1) 시스템 과부하 형태

- 고갈 공격, 디스크 채우기 공격

(2) 네트워크 서비스 거부 형태

1) SYN Flooding

- TCP 프로토콜의 구조적인 문제를 이용한 각 서버의 동시 가용 사용자수를 SYN 패킷만 보내 점유하여 다른 사용자로 하여금 서버를 사용 불가능하게 하는 공격

2) UDP Flooding

- UDP 프로토콜을 이용하여 서버에 가상데이터를 연속적으로 보내 서버의 부하 및

네트워크 과부하 발생

- UDP의 비연결성 및 비신뢰성 특징을 이용한 공격

3) Teardrop 공격

- IP 헤더가 조작된 일련의 IP 패킷 조각들을 전송하는 공격으로 패킷을 겹치게 하거나 일정한 간격의 데이터가 빠지게 함. 이렇게 수신된 패킷은 재조립할 수 없어 시스템이 다운됨

4) Smurf 공격

- ICMP의 ping을 이용한 공격으로 위조된 패킷과 브로드 캐스트 주소의 사용으로 네트워크 사용을 불가능하게 만들

5) Ping of Death 공격

- ICMP Ping 패킷을 비정상적으로 크게 만들어서 전송하면 네트워크를 통해 라우팅 되어 공격 네트워크에 도달하는 동안 아주 작은 조각이 되는데, 공격대상 시스템은 조각화 된 패킷을 모두 처리해야 하기 때문에 정상적인 Ping의 경우보다 훨씬 많은 부하가 걸리게 되어 시스템의 성능이 저하됨

[2] 분산 서비스 거부(DDoS) 공격

- 목표물을 여러 장소에서 공격하기 위하여 분산해 다수의 공격 컴퓨터를 활용하는 것
- 대상시스템의 가용성과 합법적인 최종 사용자에게 악영향을 미치려는 악의적인 시도
- 일반적으로 공격자는 대량의 패킷 또는 요청을 생성하여 궁극적으로 대상 시스템을 마비 시킴
- 공격자가 여러 개의 손상된 또는 제어된 소스를 사용하여 공격을 생성하기도 함
- 일반적인 DDoS공격은 공격 대상인 OSI 모델의 계층에 따라 분리 되는데, DDoS 공격은 네트워크, 전송, 표현, 애플리케이션 계층에서 많이 나타나고 이들은 공격에 대응하는 완화 기법을 고려해 인프라 계층과 애플리케이션 계층으로 그룹화 할 수 있음

(1) 인프라 계층(네트워크, 전송 계층)

- 가장 일반적인 유형의 DDoS 공격
- Syn 플러드 같은 벡터와 UDP 플러드 같은 기타 반사 공격이 포함됨
- 볼륨이 상당히 크며, 네트워크 또는 애플리케이션 서버 용량에 과부하가 걸리는 것이 목표
- 징후가 분명하고 감지하기가 비교적 쉬움

(2) 애플리케이션 계층(표현, 애플리케이션 계층)

- 인프라 계층에 비해 덜 일반적이지만 조금 더 정교함
- 인프라 계층에 비해 볼륨은 작지만 애플리케이션에서 고가의 특정 부분을 집중적으로 공격하여 실제 사용자가 사용할 수 없게 만들

- DDoS 방지 기법

(1) 공격 대상 영역 줄이기

- 공격을 받을 수 있는 대상 영역을 최소화하여 공격자의 옵션을 제한하고 한 곳에서 보호 기능을 구축하는 것
- 컴퓨팅 리소스를 콘텐츠 전송 네트워크(CDN) 또는 로드 밸런서 뒤에 배치하고 인프라의 특정 부분에 인터넷 트래픽이 직접 접근하지 못하도록 제한
- 방화벽 또는 ACL(액세스 제어 목록)을 사용하여 애플리케이션에 도달하는 트래픽을 제어

(2) 규모에 대한 대비

- 대규모 볼륨의 DDoS 공격을 완화하기 위한 주요 고려 사항 두 가지는 공격을 흡수하고 완화할 수 있는 대역폭 용량과 서버 용량임

1) 전송 용량

- 애플리케이션을 설계할 때에는 호스팅 제공업체가 대량의 트래픽을 처리할 수 있도록 충분한 중복 인터넷 연결을 제공하는지 확인

2) 서버 용량

- 컴퓨팅 리소스를 신속하게 확장 또는 축소할 수 있는 기능이 중요

(3) 정상 및 비정상 트래픽 파악

- 호스트의 트래픽 발생 수준이 증가하는 것을 감지할 때마다 가용성에 영향을 주지 않고 호스트가 처리할 수 있는 만큼의 트래픽만 수용할 수 있어야 함

(4) 정교한 애플리케이션 공격에 대비한 방화벽 배포

- SQL 주입 또는 사이트 간 요청 위조와 같은 공격에 대비하려면 WAF(웹 애플리케이션 방화벽)를 사용하는 것이 좋음

[3] 스푸핑(Spoofing) 공격

(1) ARP 스푸핑

- 로컬에서 통신하고 있는 서버와 클라이언트의 IP 주소에 대한 MAC 주소를 공격자의 MAC 주소로 속여 클라이언트와 서버 간 패킷을 공격자에게 향하도록 변경함
- 공격자는 패킷을 확인하고 정상적인 목적지로 재전송하여 연결을 유지하도록 함
- ARP 테이블을 정적 지정하여 대응

(2) IP 스푸핑

- IP 주소를 위장하여 클라이언트가 서버로 가는 패킷이나 서버에서 클라이언트로 가는 패킷을 위조하여 IP라우팅을 가로채야 하므로 DoS 공격이나 ARP 스푸핑 등 두 가지 이상의 공격 기법을 동시에 활용
- 서버와 클라이언트간의 신뢰관계를 확인하고 신뢰관계의 호스트인 것처럼 서버를 속여 IP 스푸핑에 성공한 공격자는 서버로부터 패스워드 요구없이 접근이 가능
- 신뢰관계를 사용하지 않거나 신뢰 된 시스템의 MAC 주소를 정적 지정하고 각 시스템에서 TCpwrapper, SSH 등을 설치해서 운영하며 rlogin 등과 같이 패스워드의 인증 과정이 없는 서비스는 사용하지 않는 방법 등으로 대응

- IP 스푸핑 방식

1) Blind Spoofing

- A와 B 사이의 통신에서 순서 번호의 예측으로 중간에 끼어드는 방식
- 순서 번호가 증가하는 방식은 통신하는 운영체제별로 다름
- 일반적으로 일어나는 스푸핑 방법이지만 사용이 까다로움

2) Non-Blind Spoofing

- A와 B 사이의 통신을 스니핑하고 있다가 통신 중간에 끼어드는 방식
- 순서 번호를 예측하지 않아도 되기 때문에 간단하지만 Sniffing하고 있다는 것 자체가 LAN안에서 서버를 통제하고 있다는 것을 뜻함

(3) DNS 스푸핑

- 실제 동작 중인 DNS 서버를 마비시키고, 대체 질의응답을 하거나 질의 응답에 대해 좀 더 빠른 속도로 DNS 응답을 하여 공격
- 도메인 네임으로 접근 시 DNS 서버를 통해 해당 IP 주소를 얻어오는 방법을 이용하며 DNS 서버에 질의를 할 때 패킷을 탐지하여 실제 DNS 서버보다 빠른 응답으로 잘못된 IP로 접속하도록 유도하기도 함
- 2차 DNS와 여러 DNS서버를 두고 DoS 공격 등으로 무력화되지 않도록 시스템을 구성하거나 중요한 접속의 경우 IP주소를 직접 입력하거나 Hosts 파일에 저장하는 방법 등으로 대응

<3> 네트워크 보안 솔루션

[1] 방화벽

- 네트워크 기반의 보안 솔루션 중에서 가장 기본적인 솔루션 중 하나

- 방화벽의 주요 기능

(1) 접근 제어

- 외부에서 내부로 유입되는 메시지의 차단 또는 허용을 하는 기능

(2) 로그

1) 감사 로그

- 방화벽의 규칙 집합의 추가/변경/삭제를 한 자와 시기, 방화벽 서비스의 시작과 중지 등을 저장
- 보안 사고 발생 시 감사 증적에 기반하여 보안 사고 발생 사용자 추적 가능

2) 운영 로그

- 실제 방화벽이 운영되면서 차단, 허용 된 네트워크 메시지의 차단, 허용 시점을 알려줌
- 방화벽 기록을 이용해 해커의 사내 시스템 공격 시도 발견 가능

- 방화벽의 종류

(1) 하드웨어 방화벽

- 대규모의 네트워크 트래픽을 빠른 시간 안에 처리해야하기 때문에 대부분 네트워크의 제일 앞 단에서 동작하며 성능이 우수함
- 보안 정책 변경 사항을 중앙에서 한 번에 제어 가능

(2) 소프트웨어 방화벽

- 각각의 PC 혹은 서버 내에서 동작
- 사내 네트워크 내부에서 시도하는 침입에 대해서 차단 가능

[2] 침입탐지시스템과 침입방지시스템

- 침입탐지시스템(IDS)은 내부 시스템에서 악의적인 공격을 발견하고 이를 보고하는 보안 솔루션이며 여기서 공격(또는 침입)은 컴퓨터 및 네트워크 자원의 무결성, 비밀성, 가용성을 해치는 일련의 행위를 뜻함
- 방화벽이 단순히 IP주소와 포트 번호 등의 속성으로 차단을 결정하는 반면 침입 탐지 시스템은 전달되는 메시지 내용을 분석하여 차단을 결정
- 전통적인 방화벽이 탐지할 수 없는 스캐닝, 도스공격, 침투공격처럼 악의적인 네트워크 트래픽이나 컴퓨터 사용을 탐지하는 데 필요

- 침입탐지시스템 동작 원리

(1) 데이터 수집

- 네트워크 기반 침입 탐지 시스템은 네트워크상에서 일어나는 활동들을 감시하고 침입 시도를 탐지하기 위해 외부 네트워크에서 내부 네트워크로 전달되는 패킷을 수집하는데 전달되는 원본 패킷을 복사하고 이렇게 복사된 패킷을 분석에 사용하는 기법인 미러링 기법을 사용함

(2) 데이터 정제

- 데이터 수집 단계를 통해 구해진 정보는 침입 탐지 시스템이 실제 악의적 공격 여부를 탐지하기 위한 자료로 사용하기 위해 정제되어야하며, 보통 자료의 필터링과 축약으로 이루어짐

1) 필터링

- 내부 네트워크로 전달되는 매우 방대한 자료가 수집되기 때문에 이 중에서 분석에 필요 없을 것으로 예상하는 불필요한 정보는 제거하는 것

2) 축약

- 분석 대상이 되는 데이터의 양을 축소하고 분석에 걸리는 시간 감소

(3) 분석 및 탐지

1) 오용 탐지

- 패턴 매칭, 시그니처 기반, 지식 기반, 전문가 시스템 등으로 탐지
- 오탐률은 낮으나 새로운 공격 탐지가 불가능하고 시그니처 업데이트가 필요함

2) 이상 탐지

- 임계치 초과, 통계 기반, 행위 기반, 인공지능 등으로 탐지
- 새로운 공격의 탐지가 가능하나 오탐률이 높고 임계치 설정이 어려움

(4) 결과 리포트

- 발견된 실제 침입은 관리자에게 전달되며 관리자는 전달받은 침입에 대한 정보를 바탕으로 공격자에 대한 접근 통제 혹은 공격당한 시스템의 서비스 중지 등의 실제 대응행동을 수행함

- 네트워크 기반 침입탐지시스템 설치 위치

(1) 방화벽 내부(DMZ)

- 주로 DMZ내의 주요 공개 서비스 서버인 웹 서버 혹은 FTP 서버 등에 대한 공격을 탐지하는 목적으로 사용
- 방화벽을 통과한 패킷에 대해서 조사하여 방화벽에 대한 접근 통제 규칙의 정확성 평가 가능

(2) 내부 네트워크

- 내부 사용자의 악의적 사용 혹은 오남용을 감시 가능
- 내부 네트워크의 백본 네트워크에 설치한다면 비교적 대규모의 네트워크 트래픽에 대한 감시 기능이 필요

(3) 서브넷

- 비교적 소규모의 네트워크 트래픽에 대한 감시만 수행해도 되기 때문에 주로 보안적으로 중요한 시스템과 자원에 대한 침입 탐지를 하려 할 때 권장됨
- 해킹 당하기 쉬운 터미널 서버, 협력 업체 접속 네트워크 및 임시 직원 등의 사용자 이동이 많은 네트워크에 대한 침입 탐지 목적으로 사용될 수 있음

- 호스트 기반 침입탐지 시스템은 호스트의 자원 사용 실태를 분석하여 호스트에 대한 침입 여부 및 실제 침입이 성공했는지 여부 등을 식별하는 시스템으로 무결성 점검에 의해 실제 침입이 발생했는지 식별하는 시스템 무결성 체크 기능이 핵심 기능 중 하나임

- 침입방지시스템은 시스템 및 네트워크에 대한 다양한 불법 침입 행위를 실시간 탐지, 분석하여 비정상적인 패킷인 경우 자동으로 차단하는 시스템으로 룰 집합 기반의 패턴 매칭 기법으로 전달되는 데이터를 분석하여 침입 시도를 판단함

- 방화벽, 침입탐지시스템, 침입방지시스템의 비교

	방화벽	침입탐지시스템	침입방지시스템
패킷 차단	O	X	O
패킷 내용 분석	X	O	O
오용 탐지	X	O	O
오용 차단	X	X	O
이상 탐지	X	O	O
이상 차단	X	X	O