TCP / UDP 통신

	TCP	UDP
연결 방식	연결지향형 서비스	비연결형 서비스
	3-Way Handshaking :데이터 전송 중 수신 확인	-
방향성	양방향 전송 (Full-Duplex)	단방향 전송 (Simplex)
전송 순서	전송 순서 보장	전송 순서 임의적
수신 여부	확인함	확인하지 않음
통신 방식	1:1 only	1:1, 1:n, n:n
신뢰성	신뢰성 통신 (높음)	비신뢰성 통신 (낮음)
속도	느림	빠름
특징	대용량 데이터를 주고받을 때 이용함 (메일, 파일전송 등) 헤더 필드에는 '발신/목적지 포트 주소, 순서 번호, 데이터 크기, 체크섬' 등이 포함됨	실시간으로 데이터를 주고받는 서비스에 이용 (온라인게임, 인터넷전화 등)

▷ 3-Way Handshaking

(1) 상대에게 통신을 하고 싶다는 메시지를 전송 (SYN)
[ex] SYN, Seq = 100
(2) 상대가 응답(통신 준비 완료)를 전송 (SYN-ACK)
[ex] SYN-ACK, Seq = 1000, Ack = 101
(3) [2]에서 받은 메시지에 응답을 전송 (ACK)
[ex] ACK, Seq = 101, Ack = 1001
* SYN: SYNchronization, ACK: ACKnowledgment

▷ UDP의 신뢰성을 높이는 방법

- 연결 유지를 위해 일정 시간마다 패킷을 전송하여, 일정 시간동안 해당 패킷이 도착하지 않는다면 전송이 되지 않는 것으로 판단하여 전송 중단.

Buffer Overflow (버퍼 오버플로우)

- 연속된 메모리 공간을 사용하는 프로그램에서 할당된 메모리의 범위를 넘어선 위치의 자료를 읽거나 쓰려고 할 때 발생
- 범위를 초과한 메모리의 데이터에 따라 공격자가 프로그램 및 시스템을 통제할 수 있는 권한을 획득할 수 있음

OSI 7-Layer (OSI 7 계층)

OSI Layer	Example	Protocol Layer
(7) Application	FTP, HTTP, SNMP	(4) Application
(6) Presentation	ASCII, 암호, 압축	
(5) Session	-	
(4) Transport	TCP, UDP	(3) Transport
(3) Network	IP, Routing Protocol	(2) Internet
(2) Data Link	PPTP, L2TP	(1) Device Driver
(1) Physical	광섬유, 케이블	

보안 시스템

▷ IDS (침입 탐지(Detection) 시스템)

- 시스템에 대한 원치 않은 조작을 탐지 후 로그 생성
- 시그니처 기반의 패턴을 탐지함.
- Firewall에서 탐지할 수 없는 영역까지 탐지함.
- 변형 패턴은 탐지가 어려움, 대응 능력 없음
- 네트워크 부하가 적음

데이터 수집 > 가공/축약 > 침입 분석/탐지 > 보고/대응

▷ IPS (침입 방지(Prevention) 시스템)

- 외부에서 내부로 침입 이전에 방지하기 위함.
- 네트워크 트래픽(패킷)을 감시하여 부정 패킷으로 판단한 경우 정책에 따라 차단함 (정책 DB 기반의 탐지)
- 실시간 대응, 오탐 발생 가능성
- 고가의 장비가 필요함
- 네트워크 부하가 발생할 수 있음 (모든 패킷을 검사하기 때문)

▷ Firewall (방화벽, 침입 차단 시스템)

- 접근을 통제하여 내부망을 보호하기 위함
- IP/PORT 기반의 차단 (패킷 감시가 아님)
- 내부자 공격에는 취약함

▷ NAC (네트워크 접근 제어)

- 네트워크망 내부에서 발생하는 문제에 대해서 감지 및 방어하기 위한 목적으로 나오게 된 장비 (IDS, IPS는 내부망 탐지가 불가능)

▷ UTM(통합 위협 관리, Unified Threat Management)

- IDS, IPS, Firewall 등 여러 보안 장비를 하나로 통합하여 관리하는 시스템
- 기본적인 IP/PORT 기반 접근 제어를 포함하여 트래픽 분석, 비정상 행위 탐지, 실시간 대응까지 모두 수행

√ IPS와 IDS를 동시에 사용하는 이유

- 오탐을 줄이기 위해
- IDS의 대응 능력 부족을 IPS를 통해 보완

공격 기법 (방어를 어떻게 하는가도 알아봐야 함)

▷ IP Spoofing

- IP의 취약점을 악용하여 자신의 IP 주소를 속여서 접속하는 공격.
- rlogin, rsh와 같이 IP 주소 기반으로 인증하는 서비스를 무력화할 수 있음

▷ DoS, DDoS (분산서비스거부)

- 수많은 클라이언트가 동시에 특정 서버에 접속하여, 공격당한 시스템의 리소스가 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격 방식

▷ Smurf Attack

- IP Spoofing 후 Echo Request를 다량 전송하면, 원래 IP 사용자에게 다량의 Echo Response 응답이 되돌아오는 것을 악용하여 시스템을 마비시키는 공격 방식

▷ Ping of Death

- Ping 패킷을 전송하면 똑같은 크기의 Ping 패킷을 상대에게 전송하는 방식을 악용한 것으로, 패킷을 최대한 길게 하여 수많은 좀비 PC가 공격 대상에 ping 패킷을 발송하면 이 패킷에 응답하다가 원래 기능을 수행하지 못하고 다운됨.

▷ SYN Flooding

- TCP 프로토콜의 3-way handshaking을 악용한 것으로, Request Queue에 SYN 패킷을 다량 발송하여 Queue가 가득 차면 정상적인 연결 요청의 SYN을 받을 수 없도록 하는 공격 기법

▷ Watering Hole

- 타겟 그룹의 서비스 이용 패턴을 분석하여, 해당 서비스를 감염시킨 후 타겟 그룹의 감염을 기다리는 공격 기법

▷ HTTP Session Hijacking

- HTTP 통신에서 사용자의 정보를 담은 Session ID 정보를 가로채는 방법으로, 직접 데이터를 중간에서 가로채거나 BruteForce를 통해 알아내는 공격 기법

▷ SQL Injection
- Input폼에 SQL문을 삽입하여 공격자가 SQL을 조작, 이후 정보를 열람하는 개인정보 탈취 공격 기법

▷ XSS (Cross Site Script)
- 게시물의 본문, 제목에 악성 스크립트를 삽입하여 이를 열람한 사용자의 PC에서 스크립트가 작동되도록 한 공격 방식
- Session ID(Cookie)를 탈취하거나, 특정 파일을 다운로드, 관리자 권한 탈취 등의 악성 행위를 수행할 수 있음

▷ APT
- 지속적으로 특정 타겟을 대상으로 행해지는 지능형 공격

▷ ARP Spoofing
- MAC 주소를 다른 컴퓨터의 MAC인 것처럼 속이는 공격 방식
- 다른 곳에 전달되어야 할 데이터 패킷을 가로챌 수 있음

▷ 0-Day (Zeroday)
- 패치가 나오지 않은 취약점을 악용한 공격 방식

▷ Race Condition
- 둘 이상의 프로세스가 공유 자원에 대해 동시에 접근하기 위해 경쟁하는 것을 활용하여 관리자 권한을 취득하는 공격 기법(또는 취약점)

▷ DLL Injection
- 다른 프로세스의 주소 공간 내에서 DLL을 강제로 로드시킴으로써 코드를 실행함

암호화 방식

▷ 대칭형 (비밀 키)
- 암호화와 복호화 시 같은 키를 사용함.
- 처리 속도가 빠름
- SEED, AES, DES, RC2 등의 방식
- n명의 사용자가 주고받는 경우 키는 $\frac{n(n-1)}{2}$개가 필요

▷ 비대칭형 (공개 키)
- 암호화와 복호화 시 사용하는 키가 다름.
- 대칭형 암호화 방식에 비해 더 안전함 (노출 위험 ↓)
- RSA, LUC, DSA, Diffie-Hellman 등의 방식
- n명의 사용자가 주고받는 경우 키는 $2n$개가 필요

▷ 키 분배 (KDC)
- 공개 키와 대칭 키 알고리즘을 사용하여 키 교환을 하는 방식에서 제 3자가 해당 공개 키로 인증할 수 있는 시스템

Linux Command

▷ chmod (Change Mode): 권한 설정을 변경함
- ex) chmod 755 ssogari.txt ¦ chmod 4755 ssogari.txt
  -rwxr-xr-x *-rwsr-xr-x*
- Read(r) = 4, Write(w) = 2, Execute(x) = 1
  -UUUGGGOOO > User(Owner) + Group + Others(Sticky Bit)
  ex) User: Read, Execute
  Group: Write → 624 (-r-x-w-r--)
  Others: Read
- User(4), Group(2), Sticky Bit(1): □___
  ex) 7___ : User, Group, Sticky Bit
  5___ : User, Sticky Bit
  → 4624(-r-s-w-r--) : 해당하는 소유권자의 마지막이 s로

▷ netstat (Network Statistics)
- LISTEN: 포트가 열림, 연결을 기다리는 중
- ESTABLISHED: 연결이 성립됨
- TIME_WAIT: 연결이 종료 또는 다음 연결을 기다리는 중
- CLOSE_WAIT: 연결 요청을 받고 연결 종료를 기다리는 중
- CLOSED: 포트가 닫힘, 연결이 종료됨

위협 탐지

▷ 정탐: TP(True Positive), TF(True Negative)
▷ 오탐: FP(False Positive) - 정상을 위협으로 탐지함
▷ 미탐: FN(False Negative) - 위협을 정상으로 탐지함

악성코드

▷ Virus
- 악의적인 목적으로 자기 자신 또는 자신의 데이터를 상대에게 복제, 감염, 전파함

▷ Worm
- 악의적인 목적으로 자신을 스스로(← 바이러스와의 차이점) 복제, 전파함

▷ Trojan
- 정상처럼 위장하여 전파되는 악성코드로, 주로 백그라운드에서 악의적인 동작을 수행함

▷ Ransomware
- 시스템을 감염시켜 시스템의 정상적인 접근 및 사용을 제한하고, 이를 인질로 하여 대가를 요구하는 악성코드
- WannyCry, PETYA 등이 있으며 DOS 때도 CASINO와 같은 랜섬웨어가 존재했음

▷ Backdoor
- 통상적으로 인증 절차를 우회할 목적으로 만들어진 악성코드. Trap Door 해킹도 이에 해당함.

▷ Rootkit
- 공격 후 공격 프로세스를 은닉할 목적으로 실행되는 프로그램, 잠복 후 재감염을 목표로 함.
- 관리자 권한을 탈취할 목적으로 감염되기도 함

▷ Spyware
- 사용자의 동의 없이 컴퓨터의 정보를 수집, 전송하는 악성 소프트웨어

▷ Cryptojacking
- 컴퓨터 시스템의 자원을 무단으로 사용하여 가상 화폐 등을 채굴하는 목적으로 제작된 악성코드

HTTP Response

▷ 100 Continue
▷ 200 OK
▷ 301 Moved Permanently
▷ 302 Found
▷ 304 Not Modified
▷ 400 Bad Request
▷ 401 Unauthorized
▷ 403 Forbidden
▷ 404 Not Found
▷ 408 Request Timeout
▷ 500 Internal Server Error
▷ 503 Service Unavailable

Linux File System

▷ Boot Block: 메모리에 올리는 운영체제의 부트 영역
▷ i-node Block: 파일의 기본 정보(크기, 유형, 권한 등)
▷ Super Block: 파일 시스템에 대한 정보
▷ Cylinder Group Block: 유효 블록에 대한 비트맵 정보, 통계를 기록함

전자 메일 프로토콜

▷ SMTP : 발신(전송) 프로토콜, TCP25

▷ POP3 : 사서함으로부터 직접 메일을 다운로드 받는 수신 프로토콜 (가져오고나면 원본은 삭제)
: 헤더(발신자 정보, 시간 등)와 본문을 모두 다운로드
: TCP 110

▷ IMAP : 이메일 서버와 동기화하여 수신받는 프로토콜
: 사용자의 요청이 있는 경우에만 다운로드 받아 빠르지만, 메일 확인 시마다 통신이 필요함 (오프라인 X)
: TCP 143

▷ PEM : 기밀성, 인증, 무결성, 부인방지를 지원하는 보안 프로토콜
: 기존 전자우편 프로토콜에 보안을 위한 정보를 추가

▷ PGP : 전자서명을 활용한 보안 프로토콜
: 평문 압축과 대칭 블록암호를 이용해 기밀성 제공

▷ S/MIME: ASCII가 아닌 데이터가 송신될 수 있도록 하는 보안 프로토콜, Non-ASCII를 ASCII로 변환 후 받는 측에서 역변환

2022. 1. 12.
blog.ssogari.dev