데이터 링크 계층에서 수행하는 기능

회선 제어 : 데이터 통신 시스템에서 중앙 처리 장치와 복수의 통신 회선 사이에서 데이터의 상호 전송을 제어하는 것 / 보통 회선 제어장치에 의해 시분할 다중적 공통

흐름 제어 : 통신 당사자 간의 데이터 흐름을 규제하는 경우에는 송신 속도가 수신 측의 처리능력을 초과하지 않도록 데이터 흐름을 조정하는 것

오류 제어 : 전송 도중에 발생한 부호 오류를 검출하고, 정확한 정보를 재현하는 기술
: 오류제어 기술로는 오류 정정 부호에 의하여 오류를 정정하는 순방향 오류 정정(FEC)와 오류검출 부호를 사용하여 재송신하는 자동 재전송 요구(ARQ)등이

데이터 링크 계층의 세분화

1) LLC(Logical Link Control) 계층
- 장비 간 논리적 연결을 수립하고 제어하는 역할을 담당하는 계층
- 상위에 있는 네트워크 계층으로 서비스를 제공하고 다양한 LAN 기술/프로토콜에서 공통으로 필요한 회선제어, 흐름제어, 오류제어 등을 담당한다

2) MAC(Media Access Control) 계층
- 장비간 공유 매체(공유 회선/링크)에 대한 다중 접근 제어를 담당하는 계층
- 동일 채널을 공유하는 통신 방법을 제어하기 위한것

스위칭 허브의 기능과 동작 원리

: 더미 허브와 달리 유입된 프레임의 목적지 MAC 주소의 포트로만 프레임을 전달해주는 네트워크 장비

1) Learning(학습) 기능 : 특정 포트로 유입된 프레임의 출발지 MAC주소를 기반으로 MAC Address Table을 생성하여 포트별 연결된 장비의 MAC 주소를 식별

2) Forwarding(전달) 기능 : 생성된 MAC Address Table을 참조하여 전송할 프레임의 목적지 MAC 주소의 포트로 프레임을 전달

3) filtering(필터링) 기능 : 목적지 포트 외에는 프레임을 전송하지 않는다.

4) Flooding(플러딩) 기능 : MAC Address Table에 등록되지 않은 목적지 MAC 주소의 프레임은 더미 허브와 동일하게 모든 포트로 프레임을 전송

*Port Mirroring(포트 미러링) : 모니터링과 트래픽 분석을 위해 특정 포트로 전달되는 패킷 또는 VLAN의 모든 패킷을 다른 모니터링 포트로 복제하여 전달하는 기능

L2-스위치의 전송 방식

1) Store-and-Forward 방식
- 유입된 전체 프레임을 버퍼에 저장하고 CRC 등의 오류 검사를 수행한 후 목적지로 전송하는 방식
- 전체 프레임에 대한 오류 검사를 수행하기 때문에 신뢰성이 높다는 장점이 있지만 저장과 검사를 위한 지연시간이 발생한다는 단점이 있음

2) Fragment-Free 방식
- 유입된 프레임의 첫 64byte를 버퍼에 저장하고 충돌 등 오류 검사를 수행한 후 목적지로 전송하는 방식

3) Cut-Through 방식
- 유입된 프레임의 첫 6byte를 읽어 목적지 MAC 주소를 확인한 후 즉시 전송하는 방식으로 현재 대부분 스위치 전송 방식으로 사용됨
- 지연 시간이 줄어 빠른 전송이 가능하다는 장점이 있지만 프레임 오류 검사를 하지 않기 때문에 신뢰성이 낮은 단점이 있음

스위치 환경에서 스니핑

Switch Jamming / Mac Flooding
- Switch의 MAC address table을 모두 채워서 스위치가 허브처럼 동작하게 강제적으로 만들어 패킷을 스니핑하려는 기법을 말함
- 일반적으로 공격자는 MAC address table을 채우기 위해 변조한 MAC 정보를 담고 있는 ARP Reply패킷을 계속해서 전송한다

ARP Spoofing / ARP Cache Posioning
- 공격자가 특정 호스트의 MAC 주소를 자신의 MAC 주소로 위조한 ARP Reply 패킷을 만들어 희생자에게 지속해서 전송하면 희생자의 ARP cache table에 특정 호스트의 MAC 주소가 공격자의 MAC 주소로 변조됨

ARP Redirect
- 공격자가 자긴이 라우터인 것처럼 MAC주소를 위조한 ARP Reply 패킷을 해당 네트워크에 브로드캐스트하면 해당 네트워크에 연경된 모든 호스트의 ARP cache table에 라우터의 MAC주소가 공격자의 MAC주소로 변조됨

ICMP Redirect
- ICMP Redirect 메시지는 라우터에서 호스트 또는 라우터 간에 라우팅 경로를 재설정하기 위해 전송하는 메시지
- 공격자는 이를 악용하여 특정 IP 또는 대역으로 나가는 패킷의 라우팅 경로를 자기 주소로 위조한 ICMP Redirect 메싯지를 생성하여 희생자에게 전송함으로써 희생자의 라우팅 테이블에 공격자로 향하는 경로를 생성

Switch의 Span/Monitor Port를 이용(포트 미러링 기능 이용)
- 원래 Monitor Port란 스위치를 통과하는 모든 트래픽을 볼 수 있는 포트로 네트워크 관리 목적이지만 공격자가 트래픽들을 스니핑하는 좋은 장소를 제공한다.

스패닝 트리 프로토콜

스위치 이중화 시 루프가 생기는 것을 방지하기 위한 프로토콜
루프가 발생하는 것을 막기 위해서 이중화 구성된 라인을 논리적으로 한 부분만 포트를 막아줌 -> 무한 루핑 방지
만약 사용중인 라인에 문제가 발생하면 논리적으로 막은 포트를 다시 열어서 링크를 연결해준다

IPsec의 두가지 동작모드

1) 전송모드(Transport Mode)
(보호 범위) : ip 패킷의 페이로드를 보호하는 모드, 즉 IP 프로토콜의 상위 프로토콜 데이터를 보호하는 모드
: 원본 IP 헤더를 그대로 유지하기때문에 네트워크상 패킷 전송에 문제가 발생하지 않는다.
(보호 구간) : 일반적으로 종단 노드 구간의 IP 패킷 보호를 위해 사용한다

2) 터널모드(Tunnel Mode)
(보호 범위) : IP 패킷 전체를 보호하는 모드이다. IP 패킷 전체를 IP패킷 전체를 Ipsec으로 캡슐화하기 때문에 원본 IP 헤더를 식별할 수 없어 네트워크상 패킷 전송이 불가하므로 전송구간(터널 게이트웨이 구간) 주소 정보를 담은 New IP헤더를 추가한다

IPsec을 통해 제공되는 보안서비스

- 기밀성 : 보장하여도 그 내용을 알 수 없음을 보장
- 비연결 무결성 : 위변조되지 않았음을 보장
- 데이터 원천 인증(=송신처 인증) : 올바른 발신지로부터 온 메시지임을 보장
- 재현(재전송) 공격 방지 : 메시지가 재전송된 것이 아니고 현재 발신지로부터 송신권 실제 메시지임을 보장
- 접근 제어 :중요한 정보 및 시스템에 대하여 접근권한을 달리 부여하여 제어
- 제한적 트래픽 흐름의 기밀성 : 제한적으로 네트워크상 트래픽 흐름에 대한 정보의 기밀성을 보장

SSL/TLS 프로토콜의 구성

Handshake 프로토콜 : 종단 호스트 간 상호인증 및 보안 통신을 위해 필요한 보안 파라미터(보안 매개변수)를 협상하기 위한 프로토콜

Change Cipher spec 프로토콜 : 종단 호스트 간 협상한 보안 파라미터를 이후부터 적용(변경)함을 알리기 위한 프로토콜

Alert 프로토콜 : 통신 과정에서 오류 발생 시 이를 통보하기 위한 프로토콜

Application 프로토콜 : 응용 계층의 데이터를 전달하기 위한 프로토콜

Record 프로토콜

- 상위 계층 프로토콜의 데이터 전달 및 적용된 보안파라미터를 이용하여 애플리케이션 데이터에 대한 단편화 및 재조합, 암호화 및 복호화, 압축 및 압축해제, 메시지

SSL/TLS 레코드 프로토콜 동작방식

1) 단편화 : 애플리케이션 데이터를 일정 크기로 단편화한다

2) 압축 및 MAC 코드 생성 : 단편화된 데이터를 압축 알고리즘으로 압축한 후 MAC값을 계산하여 추가

3) 암호화 : 압축된 데이터와 MAC값을 암호 알고리즘으로 암호화한 후 recoed 헤더를 추가하여 전송

SSL/TLS 프로토콜이 제공하는 보안 서비스

데이터 기밀성 보장

- 정당하지 않은 자(권한 없는 자)에 의해 데이터가 노출되지 않도록 보장
- 대칭키 암호를 통해 송수신 데이터를 암호화하여 기밀성을 보장

데이터 무결성 및 인증 보장

- 정당하지 않은 자(권한 없는 자)에 의해 데이터가 위변조되지 않도록 보장해 주고, 수신한 데이터가 올바른 상대방이 보낸 데이터가 맞음을 보장해준다
- 메시지 인증 코드(MAC: Massage Authentication Code)를 통해 송수신 데이터에 대한 무결성과 인증을 보장

상호인증(상호 신원확인) 보장

- 통신하려는 상대방이 올바른 상대방이 맞음을 보장해 준다
- 공개키 인증서를 이용하여 클라이언드와 서버간 상호인증을 보장해 준다.

TLS 1.3 버전

1) 강화된 보안

- 협상(Handshake) 단계에서 인증서 암호화 및 무결성 검증을 수행함으로써 협상 단계의 다운그레이드(취약한 버전으로 낮추기) 공격 방어가 가능
- TLS 1.2 이하 버전에서 지원하는 불필요하고 안전하지 않은 암호화 알고리즘을 제거하여 보안성을 높임

2) 빨라진 성능

- TLS 1.2 이하 버전에서는 최조 세션 연결시(완전 협상) 2-RTT(Round Trip Time)을 거쳐야 했으나 TLS 1.3에서는 이 과정을 1-RTT로 단축하여 성능을 향상
- 세션 재연결 시(단축 협상)에도 TLS 1.2 이하 버전에서는 1-RTT을 거쳐야 했으나 TLS 1.3에서는 공유된 암호키를 로컬에 저장하여 바로 요청 메시지에 해당 키를 사

SSL/TLS의 취약점을 이용한 공격

1) BEAST 공격(Browser Exploit Against SSL/TLS)

- 사용자 브라우저의 취약점을 이용하여 HTTPS 쿠키를 훔쳐서 HTTPS 세션을 가로챌 수 있는 공격

2) CRIME 공격(Compression Ration Info-Leak Mass Exploitation)
- HTTPS의 압축에 따른 취약점을 이용하여 HTTPS 쿠키를 훔쳐서 HTTPS 세션을 가로챌 수 있는 공격

네트워크 스니핑 탐지 기법

1) ping을 이용한 스니핑 탐지 기법
- 의심스러운 호스트에 해당 네트워크에 존재하지 않는 MAC 주소로 위조한 ping 메시지(ICMP Echo Request 메시지)를 보내 응답 메시지(ICMP Rcho Reply 메시지)

2) ARP를 이용한 스니핑 탐지 기법
- 의심스러운 호스트에 해당 네트워크에 존재하지 않는 MAC 주소를 위조한 APR 요청 메시지를 보내(유니캐스트 전송) ARP 응답 메시지가 오면 무차별 모드로 스니

3) DNS를 이용한 스니핑 탐지 기법
- 일반적으로 스니퍼는 사용자 편의를 위해 ip 주소를 호스트명(도메인명)으로 변환하기 위한 역질의를 수행함, 따라서 네트워크의 모든 호스트에 ping수행 후 역질의

4) Decoy를 이용한 스니핑 탐지
- 스니핑 공격의 주요 목적은 계정과 패스워드를 획득하는 것 -> 가짜 계정과 패스워드를 네트워크에 계속 전송하여 유인한 계정을 이용해 접속을 시도하는 시스템을

5) Arpwatch도구를 이용한 스니핑 탐지 기법
- 초기 MAC 주소와 IP 주소의 매칭 값을 저장하고 ARP 트래픽을 모니터링하여 변화가 있는 ARP 패킷을 탐지하는 도구
- 대부분의 스니핑공격이 ARP Spoofing을 사용하기 때문에 이를 탐지할 수 있다

포트 스캔(port Scan)

TCP ACK 스캔 : 포트 오픈 여부를 확인하기 위한 스캔이 아니라 방화벽 룰셋(필터링 정책)을 테스트하기 위한 스캔

DRDoS

<공격 원리>
- 공격자가 출발지 IP를 공격 대상 IP로 위조하여 다수의 반서 서버로 요청정보를 전송하면 공격 대상은 반사 서버로부터 대량의 응답을 받아 서비스 거부상태가 되는

<공격 방식>
- TCP 연결 설정 과정(3way Handshake)의 취약점을 이용한 방식 : 출발지 IP를 희생자 IP로 위조한 다수의 SYN 요청을 반사 서버로 전달하여 대량의 SYN+ACK 응답이 희생자로 향하도록 한다
- ICMP 프로토콜을 이용한 방식 : 출발지 IP를 희생자 IP로 위조한 다수의 ICMP Echo Request 패킷을 반사 서버(증폭 네트워크)로 전달하여 대량의 ICMP Echo Reply

DDoS와의 차이점
- DDoS 공격은 공격자가 직접 공격을 수행하지만, DRDoS 공격은 출발지 IP주소를 위조한 후 수 많은 공개된 반사 서버(경유지 서버)를 경유하여 공격하기 때문에 공격 근원지 파악이 어렵다

<대응책>
- Unicast RPF 패킷 필터링 기법 : 라우터 인터페이스를 통해 유입괸 패킷의 출발지 IP에 대해 라우팅 테이블을 이용하여 들어온 인터페이스로 다시 전송되는지를 검

Resolving(cache) DNS 서버가 증폭공격의 Reflector가 되는 것을 방지 조치

1) 공개용이 아닌 내부 사용자용 DNS 서버라면 서버 설정을 통해 내부 사용자 주소만 재귀 쿼리가 가능하도록 제한

정) 한다.

HTTP 느림보 3형제

1) HTTP slow header DoS(slowloris) - 공격자가 다수의 HTTP 오청 시 요청 헤더를 조작하여 요청 헤더의 끝인 빈 라인(개행문자)을 전송하지 않고 불필요한 헤더 정보만 천천히 지속해서 전송함으로써 웹 서버와의 연결을 장시간 지속시켜 연결자원을 모두 소진시키는 형태의 Dos 공격 <대응 방안> - 방화벽을 이용하여 동시 연결에 대한 임계치 설정을 통해 동일한 출발지 IP에서 동시에 연결할 수 있는 연결개수를 제한한다 - 클라이언트와 웹서버 간 세션에 대한 연결 타임아웃을 적절히 설정하여 천천히 지속해서 발생하는 요청에 대응한다
2) HTTP slow post DoS(Rudy) - 다수의 HTTP POST 요청시 Content-Length 헤더를 매우 크게 조작한 후 소량의 데이터를 천천히 지속해서 전송하여 대상 웹서버와의 연결 상태를 장시간 지속시킴으로써 연결자원을 모두 소진시키는 형태의 서비스 거부 공격 <대응 방안> - 방화벽을 이용하여 동시 연결에 대한 임계치 설정을 통해 동일한 출발지 IP에서 동시에 연결할 수 있는 연결개수를 제한한다 - 클라이언트와 웹서버 간 세션에 대한 연결 타임아웃을 적절히 설정하여 천천히 지속해서 발생하는 요청에 대응한다
3) HTTP slow read DoS - 다수의 HTTP 요청에 대한 응답 시 조작된 'zero window packet'을 천천히 지속해서 전송하여 대상 웹서버와의 연결상태를 장시간 지속시킴으로써 연결 자원을 모두
NAT
있다
1) NAPT == PAT - NAPT(Network Address Port Translation), PAT(Port Address Translation) - 다수의 사설 IP와 Port 번호를 이용하여 하나의 공인 IP 주소로 변환하는 방식
2) 동적 NAT - 다수의 사설 IP와 소수의 공인 IP주소를 m:n 동적으로 변환하는 방식
3) 정적 NAT - 하나의 사설 IP와 하나의 공인 IP를 정적으로(고정적으로) 변환하는 방식 - 외부에서 공인 IP로 내부 네트워크의 특정 사설 IP 호스트에 고정적으로 접속할 수 있으므로 외부에 지속해서 서비스를 제공하는 웹서버 등에 주로 적용
라우터 명령어
패스워드 암호화를 활성화 => service password-encryption
패스워드를 암호화해서 저장하기 위한 설정 => enable secret + '사용자 패스워드'
패스워드를 평문으로 저장하기 위한 설정 => enable password
SNMP 서비스를 비활성화 -> no snmp-server
로깅 활성화 -> logging on
원격 로그 서버에 로그 저장 -> logging '원격 로그 서버ip주소'
무선랜 보안 기능

- 무선랜 접속을 허용할 단말의 MAC주소를 무선 AP에 사전 등록하여 등록된 단말에 대해서만 접속을 허용해주는 인증방식
(장단점)
- 접근 데어 방식이 간단하고 기본적인 공격을 효과적으로 방어할 수 있는 기술로 많은 종류의 무선 AP에서 지원하는 기법
- 공격자가 정자상 단말의 MAC주소를 위조함으로써 쉽게 무력화될 수 있다
(우회당하는 해킹 기법)
- 공격자는 자신의 접속요청이 제한되고 있음을 확인한 후 정상 사용자의 무선 AP 사이의 트래픽을 분석하여 정상 사용자의 MAC주소를 알아낸다
- 정상 사용자의 MAC주소를 확인한 공격자는 자신의 MAC주소를 정상 사용자의 MAC주소로 위조하여 접속을 재요청
- 이 경우 AP는 정상 사용자의 접속요청으로 여기고 접속을 허용하게 된다

무선랜 보안 기술

개인 모드	WEP	PSK	RC4(64bit/128bit)
	WPA	PSK	RC4-TKIP
	WPA2	PSK	AES-CCMP
기업 모드	WPA	IEEE 802.x/EAP	RC4-TKIP
	WPA2	IEEE 802.x/EAP	AES-CCMP

WEP

무선 AP와 무선 단말기 사이에 사전에 서로 동일하게 설정한 공유키를 이용하여 인증과 데이터 암호화 기능을 제공
무선 AP와 단말기 간에 40bit 또는 104 bit 공유키와 임의로 선택되는 24bit IV를 조합한 64bit 또는 128bit 키를 이용해 전송 데이터를 RC4 알고리즘으로 암호화하여

<암호화 방식의 특징>
- 랜덤하게 생성하는 24bit 초기벡터(IV)와 고정된 40bit(WEP-40) 또는 104bit의 WEP공유키를 조합하여 WEP 암호키를 생성한 후 RC4암호 알고리즘을 기반으로 한 난수발생기(PRNG)에 입력하여 스트림 암호를 위한 키스트림을 생성

<문제점>
- 짧은 길이의 초기벡터 값의 사용으로 인해 IV값이 재사용될 가능성이 높다
- 불완전한 RC4 암호 알고리즘 사용으로 인한 암호키 노출 가능성이 높다
- 짧은 길이의 암호키 사용으로 인한 공격 가능성이 높다
- 암호키 노출로 인한 무선 전송 데이터의 노출 위험성이 높다

WPA

WEP와 공일한 RC4알고리즘을 기반으로하며 48bit의 확장된 IV를 사용하는 TKIP 암호화 방식을 사용

WPA2

WPA와 키 관리의 유사성을 가지고 있지만 AES기반의 128bit 대칭키를 사용하고 블록암호모드로 CCM 모드를 사용하는 CCMP 암호화 방식을 사용

WPA3

을 제공하고 사전 대입 공격 및 무작위 대입공격을 방어할 수 있음

(기업모드 개선) 192비트 키 기반 암호화를 사용하여 이전세대(128비트 기반)보다 암호 강도를 향상

비밀번호가 없는 개방형 공공 네트워크에서 OWE 기반의 데이터 암호화를 제공하여 편리성 및 보안성 강화

NETBIOS(Network Basic Input/Output System)

LAN(근거리 통신망) 상에 있는 호스트 간에 서로 통신할 수 있도록 해주는 IBM PC를 위한 네트워크 인터페이스 체계로 이름 해석, 세션, 데이터그램의 세 가지 서비스를 제공

<서비스>

- RPC Endpoint Mapper : 애플리케이션에서 로컬 또는 원격 프로세스 호출 서비스(분산 서비스) -- 135/tcp
- NetBIOS 이름 해석 서비스 : 호스트의 NetBIOS 이름을 IP주소로 변환해 주는 서비스 -- 137/udp
- NetBIOS 데이터그램 서비스 : 연결 설정 없이 브로드캐스트 또는 유니캐스트 방식으로 데이터를 전송하는 서비스 -- 138/udp
- NetBIOS 세션 서비스 : 연결 기반 세션을 생성하고 데이터를 전송하는 서비스 / SMB/CIFS 서비스(장치 공유 서비스) -- 139/tcp
- Direct Host(SMB/CIFS over TCP/IP) : TCP/IP 기반의 SMB 서비스 -- 445/tcp,udp

<NetBIOS 바인딩이 취약한 이유>

- 인터넷에 직접 연결된 윈도우 시스템에서 NetBIOS TCP/IP 바인딩이 활성화되어 있으면 인터넷을 통해 외부 공격자가 윈도우 시스템의 네트워크 공유자원에 접근할

ngrep 분석도구

tcpdump/wireshark와 같이 패킷을 캡처하고 분석할 수 있는 도구

Ascii 형식으로 패킷의 데이터를 보고자 할 때 유용히 사용

<주요 옵션>

- I(영어 대문자 I) : pcap파일을 read
- t : 타임 스탬프를 출력
- W byline : 패킷을 라인 단위로 출력

tcpdump

네트워크 인터페이스를 거치는 패킷의 내용을 출력해주는 프로그램

스니핑 도구의 일종으로 자신의 컴퓨터로 들어오는 모든 패킷의 내용을 도청할 수 있으며, 공격자를 추적 및 공격 유형 분석을 위한 패킷 분석 시에 활용할 수 있는 도

<사용 예>

1) tcpdump -vX host [IP주소] : 출발지 또는 목적지 IP주소가 []인 패킷등의 헤더 정보까지 자세하게(v), hex-ascii(-X) 형식으로 출력

2) tcpdump -i eth0 host [IP주소] and port [port 주소] : eth0 인터페이스(-i)에서 출발지 또는 목적지 IP주소가 [ ]이고 목적지 혹은 출발지 포트가 [ ]인 패킷들을 출력

* 출발지 지정시 src를 앞에 추가, 목적지 지정시 dst를 앞에 추가
* 대역을 지정시 net [CIDR표기법]을 이용

Access-list

access-list : acl number로 1~99번까지 사용
(형식) access-list acl번호 permit | deny 프로토콜 출발지

extend access-list : acl number로 100~199번까지 사용
(형식) access-list acl번호 permit | deny 프로토콜 출발지 [출발지-wildcard] 목적지 [목적지-wildcard] [목적지 포트]

r계열 명령어(서비스)

인증 없이 신뢰관계에 있는 원격지 호스트를 접속할 수 있게 하는 명령어로 rlogin(513/tcp), rsh(514/tcp), rexec(512/tcp) 등이 있음
호스트 관리 등의 편리성을 제공하지만 보안상 매우 취약 -> 허용하지 않는 것이 권장이됨

(안전한 보안 설정) -> 불가피하게 사용시
- 접근권한을 600이하로 설정하여 소유자 이외에는 읽거나 수정할 수 없도록
- 설정 파일에서 모든 호스트 또는 계정의 원격 접속을 허용하는 "+"기호를 제거하고 접속을 허용할 호스트(IP 또는 도메인)와 계정만 등록하도록 한다.

Smurf 공격

비스 거부를 유발시키는 DoS공격 기법

(대응 방법)
- 다른 네트워크로부터 자신의 네트워크로 들어오는 Directed Broadcast 패킷을 허용하지 않도록 라우터 설정
- 브로드캐스트 주소로 전송된 ICMP Echo Request 메시지에 대해 응답하지 않도록 시스템 설정

블랙홀 필터링 기법(= Null 라우팅 기법)

보내 통신이 이루어지지 않도록 하는 필터링

(형식) ip route <차단하고자 하는 목적지 IP 또는 IP 대역> <netmask> Null 0

(문제점)
- 라우터는 패킷이 Null 인터페이스로 보내질 때마다 최초 출발지로 패킷 차단에 따른 ICMP Unreachable 메시지를 발송하게 되는데, 만약 필터링하는 패킷이 많으면 라우터에 과부하를 유발할 수 있음

SMB(Server Message Block)

유닉스/리눅스와 윈도우 컴퓨터간 공유가 가능

NetBIOS API에서 동작했으며 TCP 139번 포트 사용)

워너크라이 랜섬웨어, 워너마인 암호화폐 채굴 악성코드에 악용

멤캐시드(Memcached)

오픈소스 메모리 캐싱 시스템(메모리를 사용해 캐시 서비스를 제공해주는 데몬)으로 11211/tcp와 11211/udp 포트를 기본 포트로 사용

<동작 원리>
별도의 인증과정 없이 접근을 허용해주기 때문에 공격자가 멤캐시드 서버 IP주소의 기본 포트인 11211번 포트로 희생자의 IP주소로 위조한 특정 명령의 UDP 패킷을

<사례>
github대상의 디도스 공격

WSD(Web Service Discovery)

자동으로 장비를 검색해주는 기술 -> 자동으로 연결 설정을 완료

udp 3702번 포트를 기반으로 한 멀티캐스트 통신을 사용

는 공격기법

ARMS(Apple Remote Management Service)

애플 기기들의 원격제어 기능을 활성화할 때 사용되는 데스크톱 원격제어 프로토콜

TCP/UDP 3283번 포트를 사용

ARMS 증폭/반사 공격 -> 피해자의 IP로 출발지 IP를 위조한 후 취약한 애플 mac 컴퓨터를 대상으로 원격 접속요청을 보내 증폭된 응답이 가게 만드는 공격

CoAP(Constrained Application Protocol)

불안정한 네트워크상의 저전력 IoT기기들을 위한 일종의 애플리케이션 프로토콜

HTTP 형식과 유사하여 UDP 프로토콜의 5683번 포트를 사용

드는 공격기법

VLAN

물리적으로 LAN을 분리하는 것이 아니라 데이터링크 계층에서의 브로드캐스트 도메인을 논리적으로 나누기 위해 사용하는 기술

<사용하는 이유>

- 보안 강화 : 네트워크 관리자는 서로 다른 논리적인 그룹에 대하여 서로 다른 보안 정책을 적용할 수 있다
- 성능 향상 : 브로드캐스트 도메인의 크기/범위를 줄여 네트워크 성능향상을 기대할 수 있다

구성 방식

소를 전부 등록하고 관리해야 하는 어려움이 있음

을 사용

4) 프로토콜 기반 VLAN : 같은 통신 프로토콜(TCP/IP, IPX/SPX, Netview등)을 가진 호스트들 간에만 통신할 수 있도록 구성한 VLAN

IP 소스 라우팅

IP 패킷이 목적지에 도달하기 위한 경로는 라우터에 의해 결정된다.

패킷 자체는 목적지 주소만 가지고 있을 뿐 목적지에 도달하기 위한 경로에 대한 어떠한 정보를 가지고 있지 않는데 송신자쪽에서 IP옵션 헤더를 이용하여 라우팅 경

<IP 소스라우팅 허용시 보안상 문제점>

- IP 소스 라우팅을 허용하면 공격자가 정상적인 라우팅을 통해서는 외부에서 직접 접근이 불가능한 공격 대상 시스템을 IP 소스 라우팅을 통해 우회하여 접근할 수

netstat 명령

시스템의 네트워크 관련 다양한 상태정보를 확인할 수 있는 명령어 -> 현재 연결된 모든 세션의 상태를 확인할 수 도 있음

-a : 모든 상태의 소켓 정보 출력
-n : 네트워크 주소(IP, Port)를 숫자 형식으로 출력
-t 또는 u : -t는 TCP 소켓(연결) 정보, -u는 UDP 소켓 정보 출력 cf) 윈도우 -> -p '프로토콜이름'
-p : 해당 소켓의 PID/프로세스명 정보 출력 cf) 윈도우 -> -o : 연결의 소유자 프로세스 ID를 표시
-r : 라우팅 정보를 출력
-i : 네트워크 인터페이스에 대한 정보를 출력
-s : 각 네트워크 프로토콜에 대한 통계정보를 출력

TCP Syn Flooding 공격

TCP 연결 설정 과정에서 클라이언트의 유효성을 검증하지 않는(클라이언트를 인증하지 않는) 취약점을 이용
출발지 IP주소를 위조한 다수의 SYN 패킷(연결요청 패킷)을 공격 대상 호스트로 전송하여 공격 대상 호스트의 TCP 연결 자원(Backlog Queue)을 모두 소진시켜 서비

<공격 파악> -> netstat 명령을 통해
SYN 요청에 대한 SYN+ACK 응답 이후에 해당 클라이언트로부터 ACK응답이 없을 경우
*일부 RST응답이 있는 경우는 위조된 출발지 IP가 실제로 존재하는 IP일 때 발생할 수 있다

<대응 방안>
- 커널 파라미터 설정으로 TCP Backlog Queue(연결요청대기큐)의 크기를 늘린다(ex.1024로)
- 보안장비(디도스 대응 장비, 방화벽 등)를 이용한 임계치 기반 차단을 수행(ex. SYN 패킷에 대한 pps(초당 패킷 수) 임계치 설정 , 동시 연결개수에 대한 임계치를 설정)
- First SYN DROP 기능을 이용 -> 클라이언트 첫번째 SYN패킷을 폐기한 후 재요청이 오면 이를 허용하는 방식

안전한 무선랜 접속환경 구축을 위한 무선 AP(와이파이 공유기) 보안 설정

1) 무선 AP의 도난 및 공격자의 접근으로부터 보호할 수 있도록 보호 케이스 설치, AP 리셋 버튼 차단 등 물리적 보안대책을 확보
2) 무선 ap 관리자 모드 접속 비밀번호를 설정하고 주기적으로 변경하여 공격자가 AP 관리자 모드로 접속하는 것을 방지
3) SSID(Service Set Identifier)를 초기 설정값이 아닌 새로운 값으로 변경하여 곡격자가 쉽게 인지하지 못하도록 한다
4) SSID를 브로드캐스트하지 않고 숨김 모드로 설정하여 공격자에게 노출되는 것을 최소화한다
5) 공격자의 접속 방지 및 무선 구간에서의 데이터 기밀성과 무결성을 유지하기 위해 무선 AP에서 제공하는 안전한 인증 및 암호화 방식을 적용
6) 무선 AP에 접속을 허용할 무선 단말기 리스트를 등록하여(MAC 필터리) 임의 사용자 접근을 차단

hping3

TCP/IP프로토콜용 오픈소스 패킷 생성 및 분석 도구로 TCP, UDP, ICMP, IP등 다양한 프로토콜의 패킷을, 옵션을 이용하여 손쉽게 생성할 수 있다
네트워크 보안장비의 동작을 테스트하거나 디도스 모의훈련 시 모의 공격 패킷을 생성하기 위해 해당 도구가 주로 활용

예시)
1) TCP SYN Flooding -> hping3 [공격 대상 호스트 IP] --rand-source -p [포트번호] -S --flood
* --rand-source : 패킷 생성시마다 출발지 ip를 랜덤하게 설정
* -S : 제어비트 설정)
* --flood : 패킷 생성 속도를 의미, flood는 가능한 한 가장 빠른 속도로 패킷을 생성하라는 의미)

패킷 필터링 장비를 우회하는 공격 기법

1) Fragment Overlap 공격(단편 중첩 공격)
<공격 원리>
- 공격자는 공격용 IP패킷을 위해 두개의 단편을 생성, 첫번째 단편에서는 패킷 필터링 장비에서 허용하는 HTTP(TCP 80)과 같은 포트 번호를 설정, 두번째 단편에서는 offset을 조작해서 재조합될때 첫번째 단편의 일부분을 덮어쓰도록한다
- 일반적으로 공격자들은 첫 번째 단편의 포트 번호가 있는 부분까지 덮어씌운다. 침입 탐지/차단 시스템에서는 첫번째 단편은 허용된 포트 번호이므로 통과시키고,

2) Tiny Fragment 공격(헤더정보는 단편 공격)
<공격 원리>
- TCP 헤더(일반적으로 20바이트)가 2개의 단편에 나누어질 정도로 작게 쪼개서 목적지 TCP 포트가 두 번째 단편에 위치하게 한다
- 패킷 필터링 장비나 IDS는 필터링을 결정하기 위해 포트번호를 확인하는데, 포트 번호가 포함되지 않을 정도로 아주 작게 쪼개진 첫 단편을 그냥 통과시킨다
- 실제 포트 번호가 포함된 두 번째 단편은 첫 번째 단편이 허용되었으므로 통과된다
- 보호되어야할 목적지 서버에서는 이 단편들이 재조합되어 공격자가 원하는 포트로 연결된다

봇넷(Botnet)의 종류

1) 중앙 집중형 명령/제어방식의 봇넷 : IRC 프로토콜을 이용하는 IRC 봇넷, HTTP 프로토콜을 이용하는 HTTP 봇넷이 있다

2) 분산 명령/제어방식의 봇넷 : P2P봇넷(참여 멤버 모두 C&C 역할을 함으로 별도의 도메인과 C&C서버가 불필요, 대표적으로 Storm, Peacomm등이 있음)

악성 봇 또는 감염된 PC또는 서버가 도메인 명을 기반으로 C&C서버에 접속시 보안장비에 의해 차단되는 것을 우회하는 방법

1) Fast Flux 기법
- 하나의 C&C서버 도메인명에 미리 확보한 다수의 C&C 서버 IP 주소를 할당하는 기법
- IP 주소를 여러 개 할당하고 캐시 DNS 서버에 도메인 정보가 저장되는 시간인 TTL값을 매우 작게 설정하여 IP줓소가 질의 시마다 빠르게 변경되도록 한다
- 보안장비에 의해 Fast Flux IP중 어느 하나가 탐지 및 차단된다고 해도 다른 IP를 통해 지속적으로 C&C서버에 접속할 수 있다

2) DGA(Domain Generation Algorithm) 기법
- 새로운 C&C서버 도메인을 동적으로 다수 생성해 C&C서버가 노출되는 것을 숨기는 기법으로 도메인 기반으로 탐지하는 보안장비를 우회하기 위한 목적으로 사용
- 약속된 규칙에 따라 도메인명을 다수 생성하기 때문에 C&C서버를 운영하는 공격자는 해당 규칙에 따라 생성될 수 있는 도메인명 중 하나를 DNS서버에 새롭게 등

3) Domain Shadowing 기법
- 알려진 합법적인 도메인의 서브(하위) 도메인을 몰래 등록하여 C&C서버의 도메인으로 사용하는 기법
- 적법한 절차로 도메인을 소유하고 있는 도메인 관리자의 개인정보 등을 탈취하여 도메인 소유자 몰래 많은 서브(하위) 도메인을 등록시키는 방식
- 일반적으로 DBD공격에서 악성코드 유포지에 접근하기 위한 경유지 도메인들을 수많은 서브 도메인으로 구성하여 보안장비의 탐지 및 차단을 어렵게 한다

NMAP 스캐닝 도구의 옵션

1) sP 옵션 : ping 스캔(icmp/icmp echo 스캔)

2) sS 옵션 : TCP SYN(Half-Open) 스캔

3) sU 옵션 : UDP 스캔

4) sF 옵션 : TCP FIN 스캔

5) sN 옵션 : TCP NULL 스캔

6) O 옵션 : 대상 호스트의 운영체제 정보 출력

7) p 옵션 : 대상 호스트의 포트 지정

용어

충돌 도메인(collision Domain) : 매체를 공유하는 LAN에서 하나의 장비가 데이터를 보내고 있을 때 또 다른 장비가 데이터를 동시에 보내면 충돌이 발생, 이처럼 충돌이

브로드캐스트 도메인(broadcast Domain)
- 어떤 단말이 송신한 브로드캐스트 패킷이 전달되는 허용 영역
- 영역 내에 있는 단말은 직접 통신이 가능하며, 허용 영역은 라우터 사용을 기준으로 분할된다. 예외적으로 인터넷 프로토콜 브로드캐스트 시에는 라우터를 건너뛰는 경우가 있는데 일부 용도를 제외하고는 대부분 사용되지 않는다

CIDR IP 주소 할당방식
- 기존의 클래스 기반 주소 체계를 대체하여 클래스 구분없이 IPv4전체 bit에 대해 네트워크 ID와 호스트 ID를 설정하는 주소 할당 방식
- IP 주소와 서브넷 마스크를 이진 표기법으로 'IP 주소/ 연속된 1의 비트수(서브넷 비트수)'로 표현하여 기존의 고정크기 네트워크를 다양하고 세부적으로 나눈다.

uniq -c : 연속된 중복 행의 제거하는 명령, -c 옵션은 중복 횟수를 출력하고자 할 때 사용

DTLS(Datagram Transmission Layer Security) : 데이터그램 기반 응용프로그램(UDP 기반 응용 프로그램)의 통신 과정에서 도청, 변조 또는 메시지 위조를 방지하기 위하

소켓 : 호스트/프로세스 간에 통신을 위한 소프트웨어 모듈
: 특정 IP주소와 포트 번호의 조합으로서 같은 IP의 동일한 시스템이 동시에 특정 클라이언트의 복수 개의 응용 프로그램에 정확하게 통신할 수 있게 해주는 기반

DNS 싱크홀 서비스
- 악성 봇에 감염된 PC가 해커의 명령을 받기 위해 명령&제어 서버(C&C 서버)로 연결을 시도할 때 이를 싱크홀 서버로 우회시켜 더 이상 해커로부터 조종 명령을 받

PDU(Protocol Data Unit) - PCI와 SDU로 구성
- PCI(Protocol Control Information) : 프로토콜 제어 정보(일반적으로 헤더 또는 헤더와 트레일러로 구성)
- SDU(Service Data Unit) : 전송 데이터(페이로드)

워 드라이빙
- 무선랜 탐지 해킹
- 해커가 무선 네트워크를 찾기위해 무선 장치를 가지고 주위의 AP를 찾는 과정