정보보안론 4주차 강의

! 시험 !

Dos가 무엇인지?

공격 대상이 수용할 수 있는 능력 이상의 정보를 제공하거나 사용자 또는 네트워크 용량을 초과 시켜 정상적으로 작동하지 못하게 하는 공격 (공격대상에게 여러대의 pc가 공격하는 것)

ping이 무엇인지?

Ping of Death 공격

Ping을 이용하여 ICMP 패킷의 크기를 정상보다 아주 크게 만듦

■ 패킷 분할

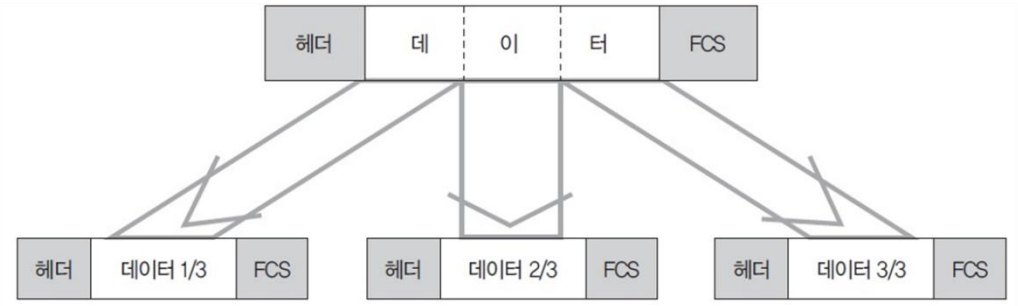

그림 11-3 패킷 분할도

- ICMP 패킷의 최대 길이를 65,500바이트로 임의로 설정
- 최대 크기인 65,500바이트로 네트워크에 ping을 보내면 패킷은 전송에 적절한 크기로 분할
- 패킷이 지나는 네트워크의 최대 전송 가능 길이가 100바이트라면 패킷 하나가 655개로 분할

! 시험 !

SYN Flooding(플러딩)

서버별로 한정되어 있는 접속 가능 공간에 존재하지 않는 클라이언트가 접속 한 것처럼 속여 다른 사용자가 서비스를 제공받지 못하게 하는 것

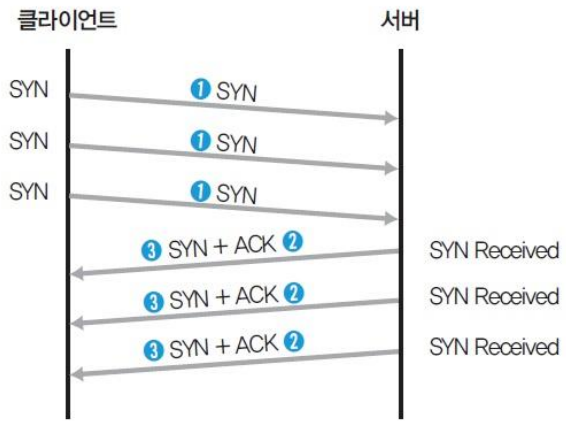

그림 11-8 SYN Flooding 공격 시 쓰리웨이 핸드셰이킹

① 공격자는 많은 숫자의 SYN 패킷을 서버에 보냄

② 서버는 받은 SYN 패킷에 대한

③ SYN/ACK 패킷을 각 클라이언트로 보냄.

④ 서버는 자신이 보낸 SYN/ACK 패킷에 대한 ACK 패킷을 받지 못함.

⑤ 서버는 세션의 연결을 기다리게 되고 공격은 성공함.

'SYN Received' 상태로 ACK 패킷을 기다리는 것을 '백로그Backlog에 빠졌다' 고 표현

Boink, Bonk, Teardrop

Boink(보잉크), Bonk(봉크), Teardrop(티어드랍)은 시스템의 패킷 재전송과 재조합에 과부하가 걸리도록 시퀀스 넘버를 속임.

Land

패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소의 값을 똑같이 만들어서 공격 대상에게 보냄(조작된 IP 주소 값은 공격 대상의 IP 주소여야 함).

서비스 거부 공격(DoS)

HTTP CC 공격

HTTP 1.1 버전의 CC 헤더 옵션은 자주 변경되는 데이터에 새로운 HTTP 요청 및 응답을 요구하기 위해 캐시 기능을 사용하지 않을 수 있음

서비스 거부 공격에 이를 응용하려면 'Cache-Control: no-store, must-revalidate' 옵션을 사용

이 옵션을 사용하면 웹 서버가 캐시를 사용하지 않고 응답해야 하므로 웹 서비스의 부하가 증가함

동적 HTTP 리퀘스트 플러딩 공격

특징적인 HTTP 요청 패턴을 확인하여 방어하는 차단 기법을 우회하기 위한 공격

지속적으로 요청 페이지를 변경하여 웹 페이지를 요청

슬로 HTTP 헤더 DoS(슬로로리스) 공격

서버로 전달할 HTTP 메시지의 헤더 정보를 비정상적으로 조작

웹 서버가 헤더 정보를 완전히 수신할 때까지 연결을 유지하도록 하는 공격

시스템 자원을 소비시켜 다른 클라이언트의 정상적인 서비스를 방해

슬로 HTTP POST 공격

웹 서버와의 커넥션을 최대한 오래 유지하여 웹 서버가 정상적인 사용자의 접속을 받아들일 수 없게 하는 공격

Smurf(스머프) 공격

ICMP Request를 받게 된 네트워크는 ICMP Request 패킷의 위조된 시작 IP 주소로 ICMP Reply를 다시 보냄.

공격 대상은 수많은 ICMP Reply를 받게 되고 Ping of Death처럼 수많은 패킷이 시스템을 과부하 상태로 만듦.

! 시험 !

표 11-3 3, 4계층 DoS 공격과 7계층 DoS 공격의 차이

	3, 4계층 DoS 공격	7계층 DoS 공격
주요 공격	• 대역폭 고갈 공격 • 세션 고갈 공격	• 서버의 자원 고갈 공격
주요 프로토콜	• TCP, UDP, ICMP	• HTTP, SMTP, FTP, VoIP 등
특징	• 단순한 Flooding 형태의 트래픽을 대량으로 발생시켜 공격 • Spoofed IP로 비정상적인 트래픽을 이용한 공격의 비율이 높음 • 보안 장비를 통해 방어 가능	• 정상 트래픽을 이용한 공격 • 소량의 트래픽을 이용한 공격 • 특정 어플리케이션의 취약점을 이용한 공격

! 시험 !

스푸핑과 스니핑이 무엇인지

스니핑 공격 == 스누핑(Snooping)

'기웃거리다, 염탐하다'라는 뜻을 가진 단어로 네트워크 상에 떠도는 중요 정보를 몰래 획득하는 행위를 말한다. (상대방의 패킷을 감청하는 행동)

스푸핑(Spoof) 공격

'속이다, 사기치다'의 뜻으로, 인터넷 프로토콜인 TCP/IP의 구조적 결함을 이용해 사용자의 시스템 권한을 획득한 뒤, 정보를 빼가는 해킹 수법을 말한다.

스니핑(Sniffing) 공격

프리미스큐어스(Primiscuous) 모드

스니핑을 위하여 랜카드를 스니핑 가능한 모드로 변경해야 한다. 일반적으로 랜카드로 입력되는 패킷은 자신의 IP주소와 MAC 주소가 일치할 경우 패킷을 받아들이고, 주소가 다른경우 패킷을 버리게 설계되어 있다. 프리미스큐어스 모드는 패킷의 IP 주소와 MAC 주소와 상관없이 모든 패킷을 수신할 수 있다.

! 시험 DNS 스푸핑 공격 !

DNS 스푸핑

실제 DNS 서버보다 빨리 공격 대상에게 DNS response 패킷을 보내어 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격

! 시험 ! – 무선 네트워크 (AP 보안)

SSID 브로드캐스팅 금지

SSID: 무선 랜 네트워크를 검색시 확인할 수 있는 AP목록 중 이름으로 표시된 것

무선 랜에서 AP의 존재를 숨기고 싶으면 SSID 브로드캐스팅을 막고 사용자가 SSID를 입력해야 AP에 접속할 수 있게 해야함

높은 수준의 보안 권한이 필요한 무선 랜은 대부분 SSID 브로드캐스팅을 차단

! 시험 ! – 무선 랜 통신의 암호화 (WEP)

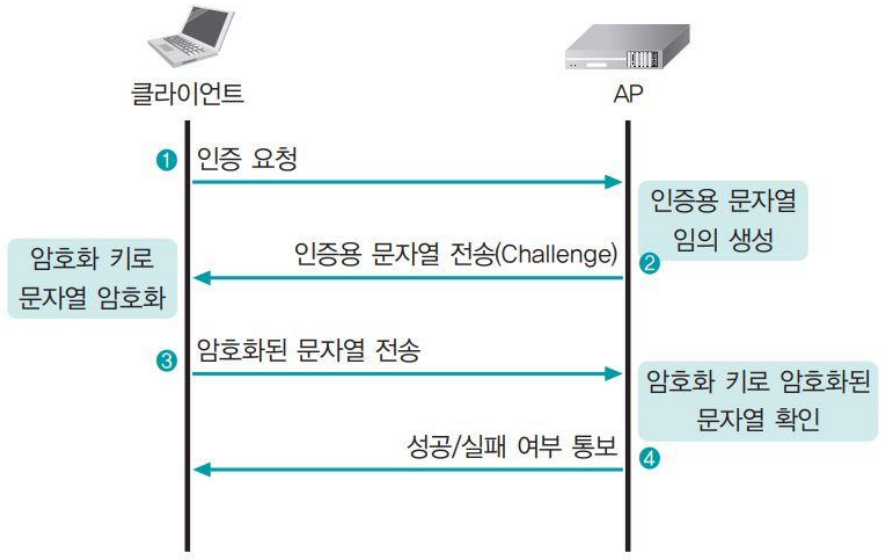

그림 3-51 WEP 암호화 세션의 생성

❶ 사용하려는 무선 랜 서비스의 SSID 값을 알아내어 무선 랜 AP에 연결 요청 메시지를 전송

❷ 사용자의 연결 요청 메시지를 받은 AP는 임의의 문장을 생성하여 원본을 저장하고 연결 요청 응답 메시지를 이용하여 암호화되지 않은 인증용 문자열을 전송

❸ 인증용 문자열을 받은 사용자는 자신이 가진 공유 키로 WEP 암호화를 적용하여 암호문을 만든 다음 AP에 전송

❹ 사용자가 공유 키로 만든 암호문을 전송받은 AP는 자신이 가진 공유 키로 암호문을 복호화, 복호화된 문장과 자신이 가진 원본 문장을 비교하여, 같으면 사용자를 같은 그룹원으로 인식해 연결 허용 메시지를 전송

! 시험 ! – 무선 랜 통신의 암호화

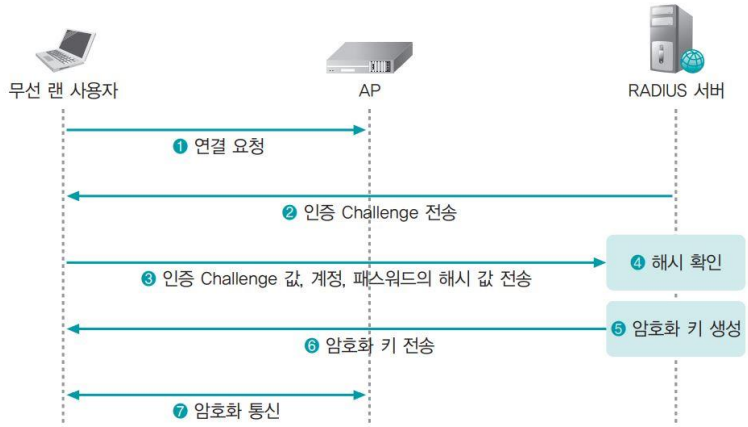

그림 3-54 RADIUS와 802.1x를 이용한 무선 랜 인증

❶ 클라이언트가 AP에 접속을 요청함, 이때 클라이언트와 AP는 암호화되지 않은 통신을 수행

클라이언트가 AP와 연결된 내부 네트워크로 접속하는 것은 AP에 의해 차단

❷ RADIUS 서버는 클라이언트에 인증 Challenge를 전송

❸ 클라이언트는 Challenge에 대한 응답으로 맨 처음 전송받은 Challenge 값, 계정, 패스워드에 대한 해시 값을 구하여 RADIUS 서버로 전송

❹ RADIUS 서버는 사용자 관리 DB 정보에서 해당 계정의 패스워드를 확인

연결 생성을 위해 최초로 전송한 Challenge의 해시 값을 구하여 클라이언트로부터 전송받은 해시 값과 비교

❺ 해시 값이 일치하면 암호화 키를 생성

❻ 생성한 암호화 키를 클라이언트에 전달

❼ 전달받은 암호화 키를 이용하여 암호화 통신을 수행