

1. 네트워크 관련 (총 13개)

[전반부: 7개]

1. **ARP Spoofing/Poisoning:** 위조된 ARP 응답을 보내 IP-MAC 매핑을 조작, 트래픽을 공격자 경유로 유도
2. **DNS Spoofing:** DNS 응답을 위조해 사용자를 가짜 IP(악성 사이트)로 유도
3. **IP Spoofing:** 패킷의 출발지 IP를 위조해 신원을 속이거나 필터를 우회
4. **MAC Flooding:** 스위치의 MAC 테이블을 위조 주소로 가득 채워 허브처럼 브로드캐스트하게 만들어 스니핑
5. **Man-in-the-Middle:** 통신 당사자 사이에 끼어들어 트래픽을 도청·조작
6. **DHCP Spoofing:** 가짜 DHCP 서버로 잘못된 게이트웨이/DNS 정보를 배포해 트래픽 가로채기
7. **VLAN Hopping:** 트렁크 프로토콜(802.1Q 등)을 악용해 원래 접근 불가능한 VLAN에 진입

[후반부: 6개]

8. **Smurf Attack:** 브로드캐스트 주소로 위조된 ICMP 요청을 보내 다수 호스트가 피해자에게 응답 폭주하게 만들
9. **Fraggle Attack:** Smurf와 유사하나 UDP(echo) 기반
10. **TCP SYN Flood:** SYN 패킷만 대량 전송해 half-open 연결로 서버 자원 고갈
11. **UDP Flood:** 대량 UDP 패킷으로 대역폭/자원 소진
12. **ICMP Flood:** 대량 ping(ICMP) 패킷으로 자원 소진
13. **Session Hijacking (네트워크):** 세션 토큰/시퀀스 번호를 탈취해 정상 세션을 가로챈

2. 웹 관련 (총 15개)

[전반부: 8개]

1. **Cookie/Session Hijacking:** 쿠키나 세션 ID를 탈취해 인증된 세션을 도용
2. **SQL Injection:** 입력값에 SQL 구문을 삽입해 쿼리 로직을 변조, DB 무단 조회/조작
3. **XSS:** 악성 스크립트를 웹페이지에 삽입해 다른 사용자 브라우저에서 실행
4. **CSRF:** 로그인된 사용자가 의도치 않은 요청을 보내게 유도
5. **Clickjacking:** 투명 레이어로 UI를 숨기고 클릭을 다른 동작으로 유도
6. **Path Traversal:** ../ 등을 이용해 웹 루트 밖 파일에 접근
7. **File Inclusion (LFI/RFI):** 서버가 사용자 입력을 파일 경로로 처리하게 해 로컬/원격 파일 실행
8. **Command Injection:** 입력값을 통해 시스템 명령을 삽입 실행

[후반부: 7개]

9. **XXE:** XML 파서가 외부 엔티티를 처리하게 해 파일 읽기/SSRF 등 유발
10. **SSRF:** 서버가 공격자가 지정한 내부/외부 URL로 요청을 보내게 만들

11. **HTTP Parameter Pollution:** 동일 파라미터를 중복 전달해 서버/필터 간 파싱 불일치 악용
12. **Open Redirect:** 검증 없는 리다이렉트 파라미터를 악용해 피싱 사이트로 유도
13. **Broken Authentication:** 세션 관리/인증 로직 결함으로 계정 탈취 가능
14. **IDOR:** 접근 권한 검증 없이 객체 참조값(ID 등)만으로 다른 사용자 데이터 접근
15. **LFI (시스템 레벨):** 웹 LFI와 개념 동일, 로컬 파일 강제 **include**로 코드 실행까지 이어지는 경우

3. 시스템 관련 (총 17개)

[전반부: 9개]

1. **Buffer Overflow:** 버퍼 크기를 초과하는 입력으로 인접 메모리를 덮어써 실행 흐름 변조
2. **Privilege Escalation:** 낮은 권한에서 관리자/루트 권한으로 상승
3. **DLL Injection:** 다른 프로세스에 악성 DLL을 강제 로드시켜 코드 실행
4. **Process Injection:** 정상 프로세스 내에 코드를 주입해 실행(탐지 회피 목적)
5. **Rootkit:** 시스템 깊은 곳에 숨어 존재/활동을 은폐하는 악성 소프트웨어
6. **Keylogger:** 키 입력을 기록해 자격증명 등을 탈취
7. **Reverse Shell:** 피해자 시스템이 공격자에게 먼저 연결을 걸어 셸 제공(방화벽 인바운드 우회)
8. **Bind Shell:** 피해자 시스템이 특정 포트를 열어 공격자의 접속을 대기
9. **Pass-the-Hash:** 평문 비밀번호 없이 탈취한 해시값으로 인증

[후반부: 8개]

10. **Pass-the-Ticket:** Kerberos 티켓을 탈취해 재사용, 인증 우회
11. **Kerberoasting:** 서비스 계정의 Kerberos 티켓을 요청해 오프라인으로 크랙
12. **AS-REP Roasting:** 사전 인증이 꺼진 계정의 응답을 받아 오프라인 크랙
13. **Golden/Silver Ticket:** 각각 KDC 자체 키(krbtgt), 서비스 계정 키를 위조해 임의 인증 티켓 생성
14. **Kernel Exploit:** 커널 취약점을 이용해 커널 권한(최고 권한) 획득

4. 정찰기법

1. Nmap
2. Gobuster
3. FFUF
4. Zenmap