모의 해킹_최종정리

모의해킹 (Penetration Testing)

> 학습 개요
>
> - **기간:** 2025.08 ~ 2025.11 (한국폴리텍대학 하이테크과정 2학기)
> - **환경:** Kali Linux(Attacker), Ubuntu/Windows(Victim), VMware NAT Network
> - **핵심 역량:** 정보 수집(Scanning) 기법 숙달, 네트워크 취약점(MITM) 공격 원리 이해 및 패킷 분석 능력 확보

⚔️ 상세 학습 내용 (Technical Skills & Attack Vectors)

1. 정보 수집 및 서비스 식별 (Information Gathering)

- **포트 스캔 및 배너 그래빙:** `nmap`을 활용하여 대상 서버(Ubuntu)의 활성 포트(22, 10000)를 식별하고, `sV` 옵션과 `nc`(Netcat), `telnet`을 통해 실행 중인 서비스의 구체적인 버전(Banner)을 확인하여 취약점 분석의 기초 데이터 확보.
- **서비스 상태 확인:** Webmin(10000/tcp) 등 특정 서비스의 데몬 상태(`systemctl status`)와 네트워크 연결 상태(`ss -lntp`)를 교차 검증하며 스캔 결과의 정확성 판단.

2. 네트워크 중간자 공격 (MITM & Sniffing)

- **ARP Spoofing:** `arpspoof` 도구를 사용하여 피해자(Victim)와 게이트웨이 사이의 ARP 테이블을 변조, 트래픽을 공격자(Kali)로 우회시키는 **중간자 공격(MITM)** 환경 구성.
- **트래픽 중계 및 스니핑:** 공격 수행 중 피해자의 네트워크가 단절되지 않도록 `fragrouter` 또는 `ip_forward` 설정을 통해 패킷을 정상적으로 릴레이(Relay)하고, `tcpdump`를 사용하여 Telnet과 같은 평문 통신 패킷 내의 **ID/Password를 감청(Sniffing)**.

3. 스푸핑 및 트래픽 조작 (Spoofing & Manipulation)

- **DNS Spoofing:** MITM 환경에서 피해자가 특정 도메인(google.com) 접속 시 공격자가 준비한 위조 웹페이지로 연결되도록 DNS 응답 패킷을 조작.
- **패킷 필터링 조작:** `iptables`를 활용하여 정상적인 DNS 응답 패킷을 차단(DROP)함으로써, 위조된 DNS 응답이 피해자에게 먼저 도달하도록 공격 성공률을 높이는 기법 적용.

💻 주요 활용 도구 및 명령어 (Key Tools & Commands)

- **Scanning:** `nmap -p [Port] -sS -sV -Pn [IP]`, `nc -v [IP] [Port]`, `telnet [IP] [Port]`
- **Sniffing & MITM:** `arpspoof -i [Interface] -t [Target] [Gateway]`, `sysctl -w net.ipv4.ip_forward=1`, `fragrouter -B1`
- **Packet Analysis:** `tcpdump -i [Interface] -A (ASCII) host [IP]`
- **Traffic Control:** `iptables -I FORWARD -p udp --sport 53 -j DROP` (DNS 차단 정책)

💡 학습 회고 (Learning Reflection)

> "방어자가 되기 위해서는 공격자의 방식을 알아야 한다는 점을 절감했습니다. 단순히 툴을 사용하는 것을 넘어, **ARP 프로토콜의 취약점(인증 부재)**이 어떻게 **중간자 공격(MITM)**으로 이어지고, 이것이 다시 DNS 스푸핑이나 계정 탈취로 확대되는지 공격의 연쇄 고리를 실습으로 확인했습니다. 특히 암호화되지 않은 Telnet 통신이 얼마나 쉽게 노출되는지 직접 눈으로 확인하며, 인프라 보안에서 **구간 암호화(SSH, TLS)**가 선택이 아닌 필수임을 확신하게 되었습니다."