

수업 내용 정리 보고서

작성일: 2026년 7월 16일

챕터 구성

- 모의해킹 정보수집 및 스캔 기술
- EIGRP 라우팅 프로토콜의 원리와 동작
- 웹 애플리케이션의 인증과 인가 취약점 실습
- 실습 체크리스트 및 보안 점검 포인트

모의해킹 정보수집 및 스캔 기술

모의해킹(Penetration Testing)은 실제 공격자의 관점에서 시스템의 취약점을 찾아내고 검증하는 과정입니다. 그 첫 번째 단계인 정보수집(Information Gathering)은 공격의 성공 여부를 결정짓는 가장 중요한 기초 작업입니다. 적절한 정보가 없으면 공격 대상을 정확히 파악할 수 없으며, 방어체계를 우회하기도 어렵습니다.

1. 정보수집과 네트워크 탐색(Net Discovery)

정보수집은 대상 네트워크의 구성을 파악하고, 열려 있는 포트와 서비스, 운영체제 등을 식별하는 과정입니다. Nmap(Network Mapper)은 네트워크 탐색을 위한 가장 강력한 도구로, 단순한 포트 스캔을 넘어 서비스의 버전 정보나 운영체제 탐지까지 수행합니다.

- 기본 스캔:** 단순히 호스트의 생존 여부와 열린 포트를 확인합니다.
- 운영체제 식별(Fingerprinting):** OS마다 다른 네트워크 패킷의 TTL(Time To Live) 값 등을 분석하여 운영체제를 추측합니다.
- 서비스 스캔(Banner Grabbing):** 서비스가 응답하는 배너를 통해 구체적인 버전 정보를 확인하여, 알려진 취약점(CVE)을 매칭할 근거를 마련합니다.

2. 주요 Nmap 스캔 기법과 작동 원리

Nmap은 네트워크 환경과 탐지 회피 전략에 따라 다양한 스캔 방식을 제공합니다.

- SYN Scan (-sS):** 'Stealth Scan'이라고도 불립니다. 3-way handshake를 완료하지 않고 SYN 패킷만 보내 응답을 확인하므로, 로그를 남기지 않거나 세션 기록을 최소화할 수 있습니다. (S → SYN, R → SYN+ACK, S → RST)
- TCP Connect Scan (-sT):** 전체 3-way handshake를 완료합니다. 안정적이지만 타겟 서버의 로그에 기록이 남을 확률이 높습니다.
- UDP Scan (-sU):** 서비스가 UDP 기반일 경우 사용합니다. 응답 속도가 느리며, 방화벽 설정에 따라 정확도가 낮을 수 있습니다.
- Comprehensive Scan (-A):** OS, 서비스 버전, 스크립트 실행 등을 한 번에 수행합니다. 정확도가 매우 높지만, 패킷량이 많아 DOS(Denial of Service)로 오인받을 수 있고 속도가 느립니다.

3. 스캔 시 고려사항 및 주의점

스캔 기술을 사용할 때는 기술적 효율성뿐만 아니라 탐지 가능성(Detection)을 항상 고려해야 합니다.

- 탐색 속도 조절 (-T):** T0(매우 느림)부터 T5(매우 빠름)까지 설정 가능합니다. 침입 탐지 시스템(IDS/IPS)의 시그니처 기반 탐지를 피하기 위해 의도적으로 속도를 늦추기도 합니다.
- Ping 생략 (-Pn):** 대상 시스템이 ICMP(Ping) 응답을 차단하도록 설정된 경우, 이를 생략하고 스캔을 강행할 때 사용합니다.
- DoS 오인 경계:** 65,535개의 전 포트를 대상으로 광범위한 스캔을 수행하면 서버의 CPU 부하가 증가하여 장애를 유발할 수 있으므로, 필요한 포트만 지정(-p)하는 것이 바람직합니다.

4. 실무 점검 포인트

모의해킹 현업에서는 다음과 같은 흐름으로 정보수집을 진행합니다.

- Passive Scanning:** 직접적인 패킷 전송 없이 공개된 도구(nslookup, 웹 레퍼런스 등)를 통해 정보를 수집합니다.
- Active Scanning:** Nmap 등을 사용하여 본격적인 네트워크 스캔을 수행합니다.
- 결과 분석:** 수집된 IP, 포트, 서비스 버전을 바탕으로 취약점 진단 단계에서 활용할 공격 벡터를 구체화합니다.

실무 주의사항: 정보수집 단계에서 과도한 스캔은 대상 서버의 서비스 가용성을 해칠 수 있습니다. 반드시 사전에 허용된 범위와 시간을 확인하고, 시스템 부하가 낮은 시간대를 활용하는 것을 권장합니다.

EIGRP 라우팅 프로토콜의 원리와 동작

EIGRP(Enhanced Interior Gateway Routing Protocol)는 시스코(Cisco) 환경에 최적화된 고급 거리 벡터(Advanced Distance Vector) 기반의 내부 게이트웨이 라우팅 프로토콜(IGP)입니다. 이전의 IGRP 프로토콜이 가진 클래스풀(Classful) 라우팅의 한계를 극복하고, 수렴 속도와 확장성을 대폭 개선하기 위해 탄생했습니다.

1. EIGRP의 핵심 동작 원리: DUAL 알고리즘

EIGRP는 DUAL(Diffusing Update Algorithm)이라는 알고리즘을 사용하여 네트워크 내에서 최적의 경로를 계산하고, 루프(Loop) 발생을 원천적으로 방지합니다. DUAL은 확산 업데이트 알고리즘의 약자로, 네트워크 변화 발생 시 모든 경로 정보를 다시 계산하는 대신 필요한 정보만 전파하여 수렴(Convergence) 속도를 극대화합니다.

- Successor:** 목적지 네트워크까지 가는 최적의 경로입니다. 라우팅 테이블에 즉시 등록됩니다.
- Feasible Successor:** 루프가 없음이 보장된 차순위 백업 경로입니다. Successor에 장애가 발생하면 즉시 전환하여 빠른 복구를 가능하게 합니다.
- DUAL의 상태:** 네트워크가 안정적이면 'Passive' 상태이며, 경로 재계산이 필요하면 'Active' 상태가 되어 이웃 라우터와 정보를 교환합니다.

2. 복합 메트릭(Composite Metric)의 계산

RIP이 단순히 홉 수(Hop Count)만을 기준으로 경로를 판단하는 것과 달리, EIGRP는 대역폭(Bandwidth)과 지연(Delay)을 핵심 기준으로 사용하는 복합 메트릭을 사용합니다. 이를 통해 네트워크의 물리적 성능을 보다 정확하게 반영합니다.

- **Bandwidth:** 경로상에서 가장 낮은 대역폭 값을 사용합니다. 대역폭이 높을수록 좋은 경로로 판단합니다.
- **Delay:** 경로에 포함된 모든 인터페이스 지연 시간의 합입니다. 지연 시간이 낮을수록 좋은 경로로 판단합니다.
- **기타 요소(K 상수):** 신뢰성(Reliability), 부하(Load), MTU 값을 사용할 수 있으나 기본 설정에서는 대역폭과 지연 값만 계산에 사용합니다.

3. 이웃 관계 형성 및 패킷 교환

EIGRP는 TCP/UDP를 사용하지 않고 IP 프로토콜 번호 88번을 사용하여 직접 통신합니다. 이웃 관계(Neighbor Relationship)를 유지하기 위해 5가지 패킷을 사용합니다.

- **Hello:** 이웃 라우터를 탐색하고 연결 상태를 유지합니다(기본 2초 주기). 멀티캐스트 주소 224.0.0.10을 사용합니다.
- **Update:** 라우팅 정보가 변경되었을 때 필요한 정보만을 부분적으로 전달합니다.
- **Query:** 대체 경로를 찾지 못할 때 이웃에게 경로를 질의합니다.
- **Reply:** Query에 대한 응답입니다.
- **Ack:** 업데이트, 질의, 응답 패킷의 수신을 확인합니다.

4. 실무 운영 시 주의사항 및 점검 포인트

EIGRP를 운영할 때 다음 조건이 일치하지 않으면 이웃 관계가 형성되지 않으므로 가장 먼저 확인해야 합니다.

- **AS 번호(Autonomous System Number):** 연결된 두 라우터의 AS 번호는 반드시 같아야 합니다.
- **K 값(Metric Weight):** 메트릭 계산에 사용하는 K 값 설정이 일치해야 합니다.
- **네트워크 인터페이스:** EIGRP 설정 범위에 해당 인터페이스가 포함되어 있어야 하며, passive-interface로 설정되어 있으면 안 됩니다.
- **인증(Authentication):** 인증을 사용하는 경우 비밀번호와 설정 방식이 동일해야 합니다.

흔한 실무 실수: 네트워크 변화가 잦은 환경에서 수렴 과정이 멈추지 않는 'Stuck In Active(SIA)' 현상이 발생할 수 있습니다. 이는 라우터가 경로를 찾지 못해 Query를 계속 보내고 응답을 기다리는 상태입니다. 네트워크 구조를 적절히 요약(Summarization)하여 Query의 확산을 방지하는 것이 예방책입니다.

5. 점검 및 확인을 위한 명령어

EIGRP 동작을 확인하기 위해 실무에서 가장 자주 사용하는 명령어는 다음과 같습니다.

- **show ip eigrp neighbors:** 이웃 라우터와의 관계 및 패킷 대기열을 확인합니다.
- **show ip route eigrp:** EIGRP를 통해 학습된 라우팅 테이블 정보를 확인합니다.
- **show ip protocols:** 현재 설정된 AS 번호, K 값, 타이머 등을 종합적으로 점검합니다.

웹 애플리케이션의 인증과 인가 취약점 실습

웹 애플리케이션 보안에서 가장 핵심적인 두 기둥은 인증(Authentication)과 인가(Authorization)입니다. 인증은 '사용자가 누구인가'를 확인하는 과정이며, 인가는 '확인된 사용자에게 어떤 자원 접근 권한을 줄 것인가'를 결정하는 정책입니다. 많은 보안 사고가 인증 단계의 결함보다, 일단 신원을 확인한 후의 인가 검증이 허술하여 발생하는 취약점에서 비롯됩니다.

인증과 인가의 구분

- **인증(Authentication):** 아이디와 비밀번호 등을 통해 사용자의 신원을 검증합니다.
- **인가(Authorization):** 로그인한 사용자가 특정 페이지를 보거나 데이터를 수정할 권한이 있는지 확인합니다.

실습 과정에서 다룰 4가지 주요 취약점(세션 하이재킹, IDOR, 기능 레벨 접근 제어 누락, 쿠키 위조)은 모두 인증은 통과했거나 우회 가능한 상태에서, 후속 인가 검증이 제대로 수행되지 않을 때 발생하는 문제들입니다.

실습 1: Hijack a Session (세션 하이재킹)

세션 쿠키는 사용자가 로그인한 상태를 서버에게 알리는 핵심 증명서입니다. 만약 이 쿠키 값이 예측 가능(Predictable)하다면, 공격자는 아이디와 비밀번호를 몰라도 다른 사용자의 세션을 가로챌 수 있습니다.

실습 목표는 hijack_cookie 값을 예측하여 시스템에 침투하는 것입니다. 세션 쿠키는 생성 알고리즘이 충분히 복잡하고 무작위(Random)여야 하는데, 단순히 순번이나 타임스탬프를 조합하여 만든 경우 보안에 취약합니다.

위 화면에서 쿠키 값을 예측하는 과정은 세션 식별자가 생성되는 패턴을 관찰하는 것에서 시작합니다. 서버가 쿠키를 생성하는 규칙을 파악할 수 있다면, 로그인 절차를 거치지 않고도 정상 사용자의 세션으로 접근할 수 있습니다. 이는 CWE-330(충분하지 않은 난수 값 사용) 취약점과 직결됩니다.

실습 2: IDOR (불안전한 직접 객체 참조)

IDOR(Insecure Direct Object Reference)은 사용자가 접근 권한이 없는 다른 사용자의 데이터를 URL 파라미터나 폼 값만 바꿔서 조회할 때 발생합니다. 공격자는 이미 자신의 계정으로 정상 로그인을 수행한 뒤, 요청에 포함된 객체 식별자(예: user_id, order_id)를 다른 값으로 변경하여 서버의 인가 검증이 우회되는지 확

인합니다.

이 실습은 '인가받지 않은 데이터 접근'이 핵심입니다. 개발자는 클라이언트 측에서만 특정 메뉴를 숨기거나 데이터를 제한하는 경우가 많은데, 공격자는 서버로 직접 요청을 보내 이러한 제한을 무력화합니다. 항상 서버 측에서 "현재 요청을 보낸 사람이 이 객체의 주인인가?"를 검증하는 로직이 필요합니다.

실습 3: Missing Function Level Access Control

관리자 페이지나 특정 기능이 메뉴에는 숨겨져 있어도, 해당 URL을 직접 호출했을 때 인가 검증이 이루어지지 않으면 일반 사용자도 관리자 기능을 수행할 수 있는 취약점입니다.

공격자는 관리자만 사용하는 URL 패턴을 추측하거나 디렉토리 브루트포싱을 통해 숨겨진 기능을 찾아냅니다. 단순히 UI에서 버튼을 숨기는 것은 보안 대책이 될 수 없으며, 반드시 서버 측에서 각 기능 호출 시마다 사용자의 권한을 재확인해야 합니다.

실습 4: Spoofing an Authentication Cookie

인증 쿠키를 위조하여 서버를 속이는 실습입니다. 서버가 쿠키 값의 무결성을 검증하지 않거나(예: 암호화되지 않은 쿠키), 쿠키 안에 사용자의 권한 정보를 평문으로 담고 있을 때 발생합니다.

학습 결과 요약 및 점검 포인트

오늘의 실습을 통해 우리는 "클라이언트를 믿지 말라"는 원칙을 '인가' 영역까지 확장해야 함을 확인했습니다. 다음은 실무 점검 시 확인해야 할 체크리스트입니다.

- **세션 관리:** 세션 쿠키는 예측 불가능한 강력한 무작위 값을 사용하는가?
- **인가 검증:** 모든 데이터 조회 및 기능 호출 시, 서버 측에서 사용자의 권한을 매번 체크하는가?
- **파라미터 오염:** URL 파라미터나 폼 값의 ID가 다른 사용자의 것으로 변경되었을 때 접근이 차단되는가?
- **쿠키 위조:** 쿠키 내에 권한 정보가 포함되어 있다면 암호화되거나 서버 측에서 재검증하는가?

이러한 취약점들은 대부분 OWASP Top 10의 '식별 및 인증 실패'와 '보안 설정 오류' 범주에 속하므로, 설계 단계부터 보안 모델을 적용하는 것이 필수적입니다.

실습 체크리스트 및 보안 점검 포인트

본 장에서는 모의해킹 및 네트워크 라우팅 프로토콜 실습 과정에서 반드시 수행해야 할 체크리스트와 보안 관점의 점검 포인트를 다룹니다. 시스템의 안전한 운영과 취약점 분석을 위해서는 기술적 절차 준수뿐만 아니라, 잠재적 위험 요소를 상시 식별하는 능력이 필요합니다.

1. 모의해킹 정보수집 단계 점검

정보수집은 공격의 성공 여부를 결정짓는 핵심 단계입니다. Nmap을 활용한 네트워크 탐색 시 서버의 가용성과 보안 정책을 동시에 고려해야 합니다.

- **기본 스캔 수행 여부:** nmap 192.168.0.1 명령어를 통해 대상 호스트의 열린 포트를 확인했는가?
- **종합 분석 전략:** -A 옵션을 통해 OS, 서비스 버전, 스크립트 정보를 확인했는가? (단, -A 스캔은 속도가 느리고 많은 트래픽을 유발하므로 네트워크 부하를 고려해야 함)
- **스캔 유형 선택:** 방화벽 탐지를 회피하기 위한 SYN 스캔(-sS)과 일반적인 TCP 연결 스캔(-sT)의 차이를 이해하고 상황에 맞게 적용했는가?
- **가용성 고려:** 광범위한 포트 스캔(-p 1-65000 등)은 서버가 DoS(서비스 거부) 공격으로 오인하여 차단할 수 있으므로, Top 1000 포트 위주의 -T4 -F 스캔 사용을 우선 고려했는가?

위 화면은 대상 시스템의 열린 포트와 서비스 버전을 배너 그래빙(Banner Grabbing)을 통해 확인하는 과정입니다. 버전 정보 획득은 특정 버전의 알려진 취약점(CVE)을 찾기 위한 필수적인 단계입니다.

2. EIGRP 네트워크 운영 및 보안 점검

EIGRP(Enhanced Interior Gateway Routing Protocol)는 대규모 네트워크에서 빠른 수렴을 제공하지만, 이웃 관계 설정 및 라우팅 정보 전파 시 보안적 결함이 발생할 수 있습니다.

- **이웃 관계 조건 확인:** AS 번호, K 값, 인증 설정 등이 양쪽 라우터에서 동일하게 설정되었는가?
- **인증(Authentication) 설정:** EIGRP 라우팅 정보의 무결성을 보장하기 위해 인증을 설정했는가? 인증이 설정되지 않으면 라우팅 정보 조작(Route Injection)에 취약해집니다.
- **불필요한 인터페이스 제어:** 라우팅 정보가 광고되지 않아야 할 인터페이스는 passive-interface를 사용하여 이웃 관계 형성을 방지하고 있는가?
- **부하 분산 전략:** 비균등 비용 부하 분산(Variance) 설정이 루프를 발생시키지 않는지 확인했는가?

3. 웹 애플리케이션 보안 점검 (WebGoat 실습)

인증(Authentication)과 인가(Authorization)의 구분은 웹 보안의 핵심입니다. 세션 관리와 객체 참조 취약점은 실무에서 가장 빈번하게 발생하는 문제 중 하나입니다.

- **세션 하이재킹(Session Hijacking) 점검:** 세션 쿠키 값이 예측 가능한 패턴(순번, 타임스탬프 등)으로 생성되고 있지는 않은가?
- **IDOR(Insecure Direct Object Reference) 점검:** 로그인된 사용자가 URL 파라미터나 쿠키 값을 변경하여 타인의 데이터에 접근할 수 있는가? 서버가 사용자별 권한을 확인하는지 반드시 검증해야 합니다.

- **기능 수준 접근 제어(Function Level AC) 점검:** 관리자 전용 페이지나 기능에 대해 인가되지 않은 일반 사용자가 직접 URL을 호출하여 접근할 수 있는가?
- **클라이언트 신뢰 금지:** 서버는 클라이언트가 전달한 모든 값(쿠키, 파라미터 등)을 조작 가능한 데이터로 간주하고 서버 측에서 재검증해야 합니다.

위 화면은 특정 사용자의 세션 쿠키를 가로채거나 예측하여 비정상적으로 접근하는 시나리오를 보여줍니다. 이러한 취약점은 강력한 난수 기반의 세션 ID 생성과 서버 측의 엄격한 인가 로직을 통해 방어해야 합니다.

4. 실습 결과 해석 및 주의사항

실습 과정에서 다음의 오답 포인트와 주의사항을 항상 염두에 두어야 합니다.

- **오답 포인트:** 화면에 데이터가 표시되지 않는다고 해서 데이터가 서버에서 오지 않은 것은 아닙니다. 네트워크 탭을 확인하여 원본 응답 데이터를 분석하는 습관이 중요합니다.
- **주의사항:** 정보수집이나 스캔 작업을 수행할 때 허가받지 않은 네트워크 대상에 대해 트래픽을 유발하는 것은 법적 문제가 될 수 있으므로, 반드시 실습 환경 내에서만 수행해야 합니다.
- **트러블슈팅:** 이웃 관계가 형성되지 않을 경우 `debug eigrp packets` 등을 통해 Hello 패킷 수신 여부와 설정 불일치 사항을 논리적으로 추적해야 합니다.