

수업 내용 정리 보고서

작성일: 2026년 6월 24일

챕터 구성

1. ARP 프로토콜의 유형과 동작 원리
2. Burp Suite를 이용한 프록시 제어 및 중간자 공격(MITM)
3. 레지스트리 기반 프록시 자동 설정 및 공격 환경 구축
4. Burp Suite Intruder를 활용한 브루트포스 공격 검증

ARP 프로토콜의 유형과 동작 원리

네트워크 통신에서 IP 주소(Logical Address)를 기반으로 실제 물리적인 장치의 주소인 MAC 주소(Physical Address)를 찾아내는 과정은 필수적입니다. 이 역할을 수행하는 프로토콜이 바로 **ARP(Address Resolution Protocol)**입니다. ARP는 데이터가 목적지 호스트에 도달하기 위해 필요한 계층 간의 매핑 정보를 제공합니다.

ARP는 단순히 주소를 찾는 기능 외에도 네트워크 환경과 목적에 따라 다양한 변형된 형태로 동작합니다. 주요 ARP 유형을 비교하면 다음과 같습니다.

종류	동작 방식 및 특징	주요 목적
ARP	IP 주소를 통해 대응하는 MAC 주소를 요청	표준 주소 결정 과정
RARP	MAC 주소를 통해 대응하는 IP 주소를 요청	IP 할당 및 식별 (Reverse ARP)
Proxy ARP	라우터가 대상 IP를 대신하여 자신의 MAC 주소로 응답	서로 다른 네트워크 간 통신 중계
Inverse ARP	자신의 DLCI(Data Link Connection Identifier)를 통해 정보를 물어봄	Frame Relay 환경에서의 식별
GARP (Gratuitous ARP)	상대방의 요청 없이 자신의 정보를 브로드캐스트함	ARP 테이블 업데이트 및 IP 충돌 감지

여기서 주의할 점은 **RARP**와 **Inverse ARP**처럼 요청 정보의 방향이 일반적인 ARP와 반대이거나, **Proxy ARP**처럼 중간 장비(라우터)가 개입하여 대리 응답을 하는 특수한 경우를 정확히 구분하는 것입니다. 이러한 프로토콜의 동작 원리를 이해하는 것은 네트워크 스니핑이나 스푸핑 공격을 분석할 때 매우 중요한 기초가 됩니다.

Burp Suite를 이용한 프록시 제어 및 중간자 공격(MITM)

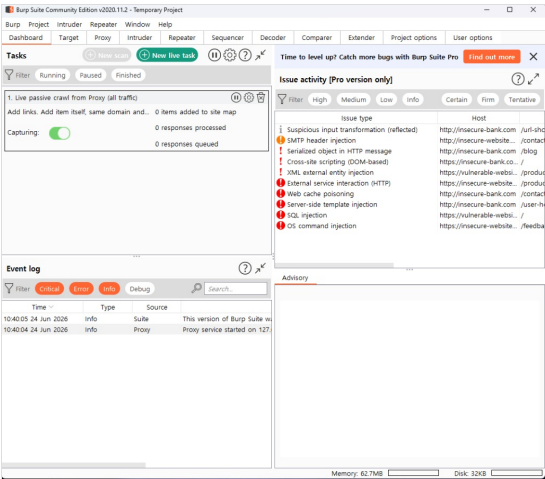
Burp Suite는 웹 애플리케이션 보안 테스트를 위한 핵심 도구로, 클라이언트와 서버 사이에서 트래픽을 가로채는 **프록시(Proxy) 서버** 역할을 수행합니다. 프록시란 '대리자' 또는 '경유지'를 의미하며, 모든 HTTP 통신이 이 서버를 거치게 함으로써 공격자는 데이터를 관찰하거나 수정할 수 있는 위치를 확보하게 됩니다.

1. 프록시 서버 및 대시보드 구성

Burp Suite를 실행하면 가장 먼저 대시보드를 통해 전체적인 작업 현황과 탐지된 취약점 이슈를 확인할 수 있습니다. 프록시를 활성화하면 실시간으로 패킷을 수집하는 **패시브 크롤링(Passive Crawl)**이 진행됩니다.

대시보드 상단에서는 수행 중인 Task의 상태와 탐지된 이슈들의 요약 정보를 볼 수 있습니다.

Dashboard 탭의 Tasks, Issue activity, Event log UI 구성 요소

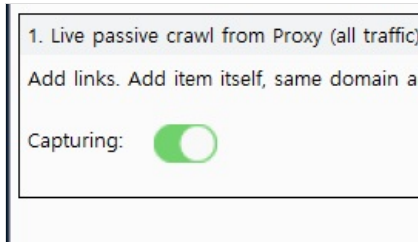


Burp Suite 대시보드에서 수행 중인 작업, 탐지된 취약점 이슈 및 이벤트 로그 현황 확인

이 화면을 통해 현재 시스템에서 실시간으로 탐지되고 있는 취약점 유형과 진행 중인 스캔 작업의 상태를 한눈에 파악할 수 있습니다.

프록시 탭의 Tasks 영역에서는 캡처링(Capturing) 스위치가 활성화되어 실시간으로 트래픽을 수집하고 있는지 확인할 수 있습니다.

Tasks 영역 내 Capturing 스위치가 녹색(ON)으로 표시됨



프록시를 통한 실시간 패시브 크롤링 작업의 캡처링 상태가 활성화된 모습

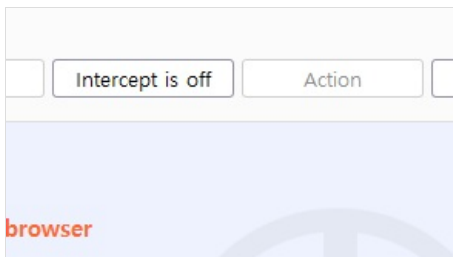
캡처링 상태가 녹색(ON)으로 표시되어야 프록시를 통과하는 트래픽이 정상적으로 기록됩니다.

2. 인터셉트(Intercept)를 통한 트래픽 제어

프록시의 핵심 기능은 **인터셉트(Intercept)**입니다. 인터셉트 기능이 켜져 있으면 클라이언트가 보낸 요청이 서버로 바로 전달되지 않고 Burp Suite 단계에서 멈추게 됩니다. 이때 공격자는 패킷의 내용을 확인하거나 조작할 수 있습니다.

인터셉트 버튼의 상태를 통해 현재 패킷 가로채기 기능이 작동 중인지, 아니면 단순히 통과시키고 있는지 확인할 수 있습니다.

Intercept is off 버튼의 텍스트 상태

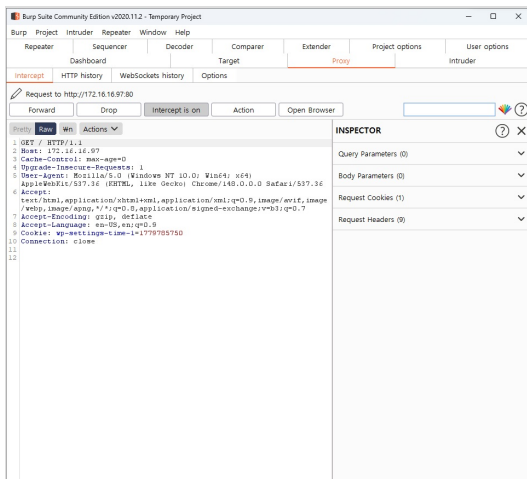


프록시 인터셉트 기능이 현재 비활성화(off) 상태임을 나타내는 버튼 UI

버튼이 'Intercept is off' 상태라면 패킷은 가로채지지 않고 그대로 통과(Bypassing)됩니다.

실제로 인터셉트가 활성화되면, 특정 호스트로 향하는 HTTP GET 요청이 가로채져 상세 헤더 정보가 표시됩니다.

Proxy 탭의 Intercept is on 상태 및 172.16.16.97 호스트를 대상으로 하는 HTTP 요청 헤더 정보



Burp Suite Intercept 기능을 통한 172.16.16.97 대상의 HTTP GET 요청 가로채기

이 화면을 통해 호스트, 머스트, 쿠키(Cookie), User-Agent 등 클라이언트가 서버에 보내는 모든 원본 데이터를 확인할 수 있습니다.

3. 중간자 공격(MITM)의 메커니즘

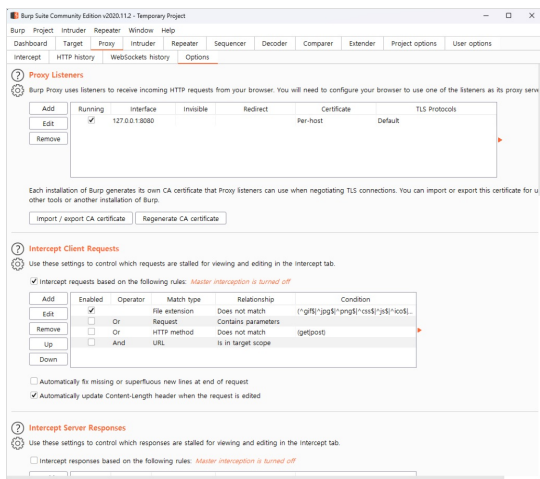
이러한 프록시 환경을 악용하여 클라이언트(A)와 서버(B) 사이의 통신 경로에 공격자(P)가 끼어드는 것을 **중간자 공격(Man-in-the-Middle Attack)**이라고 합니다. 공격자는 다음과 같은 세 가지 방식으로 트래픽을 다룹니다.

- **스니핑(Sniffing)**: 가로챈 패킷을 단순히 읽고 관찰하는 행위
- **스푸핑(Spoofing)**: 가로챈 패킷의 내용을 공격자가 원하는 대로 수정하여 전달하는 행위
- **바이패싱(Bypassing)**: 가로챈 패킷을 아무런 수정 없이 있는 그대로 전달하는 행위

공격자가 효율적으로 MITM을 수행하기 위해서는 프록시 서버의 **리스너(Listener)**를 적절히 설정해야 합니다. 리스너는 특정 IP와 포트에서 클라이언트의 요청을 기다리는 대기 상태를 의미합니다.

프록시 옵션 메뉴에서는 리스너의 구성과 클라이언트 요청을 필터링하는 규칙을 관리할 수 있습니다.

Proxy 탭의 Options 하위 메뉴와 Proxy Listeners, Intercept Client Requests 설정 영역

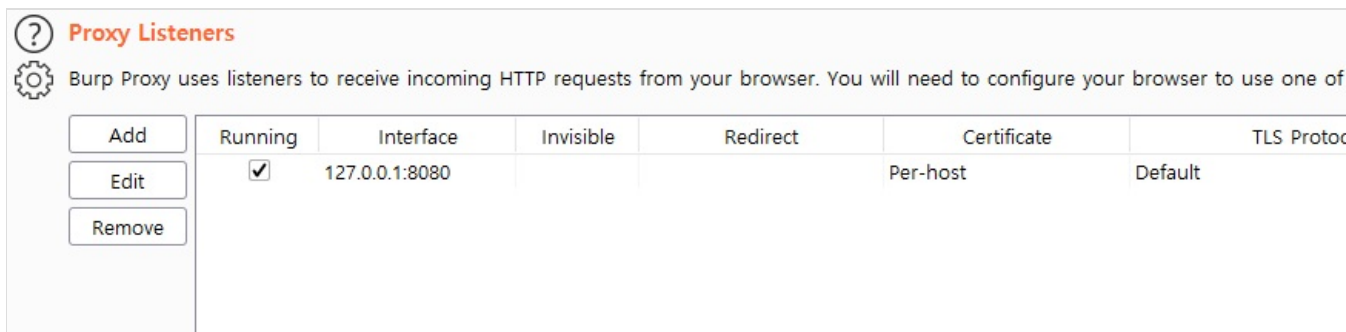


프록시 리스너 구성 및 클라이언트 요청 인터셉트 규칙을 관리하는 옵션 설정 화면

이 설정 창을 통해 특정 확장자(예: .jpg, .css)를 제외하고 인터셉트할 규칙을 정의할 수 있습니다.

기본적으로 리스너는 로컬 호스트(127.0.0.1:8080)에서 동작하도록 설정되어 있습니다.

Proxy Listeners 테이블 내 Interface 항목의 127.0.0.1:8080 값

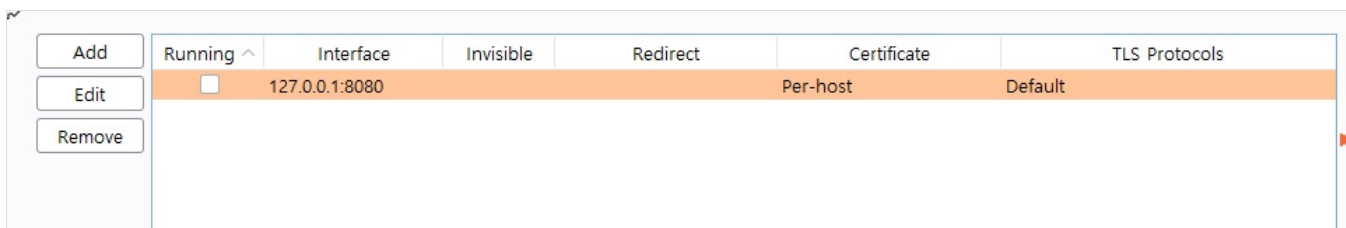


127.0.0.1:8080 포트에서 실행 중인 프록시 리스너의 인터페이스 정보

리스너가 올바른 인터페이스와 포트에서 실행 중인지 확인하는 단계입니다.

만약 리스너의 실행 여부가 불투명하다면, Running 체크박스를 통해 활성화 상태를 점검해야 합니다.

Running 열의 체크박스 미선택 및 선택된 행의 강조 표시

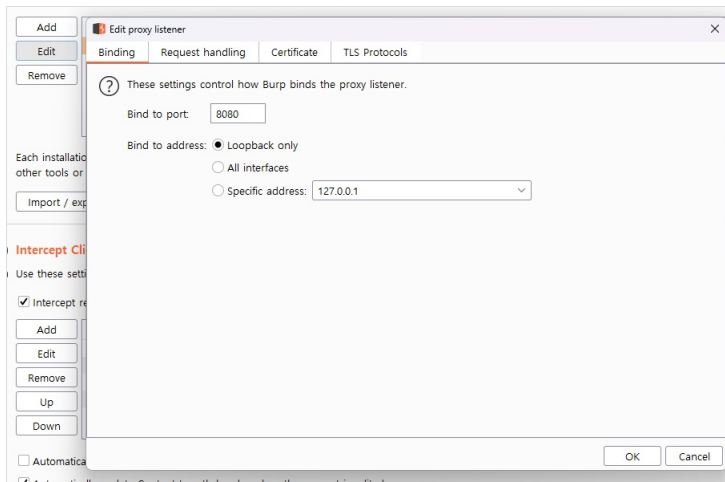


프록시 리스너의 Running 체크박스가 해제되어 리스너가 중지된 상태

체크박스가 해제되어 있다면 프록시 서버가 동작하지 않아 트래픽을 가로챌 수 없습니다.

외부 장치(피해자 컴퓨터)로부터 트래픽을 받기 위해서는 리스너의 속성을 수정하여 특정 IP에 바인딩해야 합니다.

Bind to port 8080 및 Bind to address Loopback only 설정창

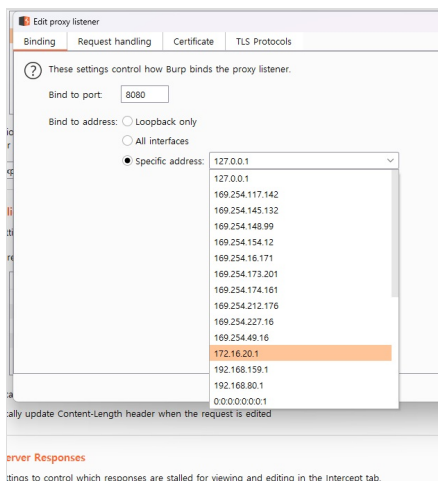


프록시 리스너의 포트 번호와 바인딩 주소를 변경하는 Edit proxy listener 대화상자

포트 번호와 바인딩할 주소를 변경하는 설정 과정입니다.

예를 들어, 포트를 8080으로 유지하면서 특정 IP(예: 172.16.20.1)를 지정하여 외부 접근을 허용할 수 있습니다.

Bind to port: 8080, Specific address: 172.16.20.1



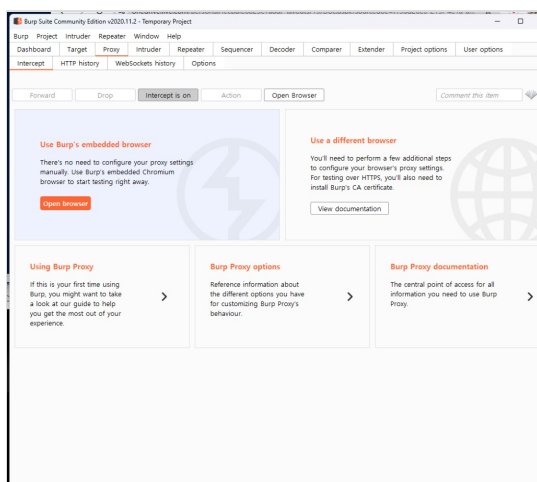
Burp Suite 프록시 리스너의 포트를 8080으로 지정하고 특정 IP를 바인딩하는 화면

특정 IP를 바인딩함으로써 외부의 피해자 컴퓨터가 공격자의 Burp Suite로 접속할 수 있는 통로를 만듭니다.

관련 실습 화면

브라우저와 프록시 간의 연동을 위해 내장 브라우저를 사용하거나 외부 브라우저의 설정을 변경해야 합니다.

Proxy 탭의 Intercept 하위 메뉴와 브라우저 선택 옵션 UI



프록시 설정을 위한 내장 브라우저 사용 및 외부 브라우저 연동 안내 화면

레지스트리 기반 프록시 자동 설정 및 공격 환경 구축

실제 공격 시나리오에서 해커는 피해자 컴퓨터에 일일이 접속하여 프록시 설정을 할 수 없습니다. 따라서 **윈도우 레지스트리(Registry)**를 수정하여 피해자의 브라우저가 자동으로 공격자의 프록시 서버를 거치도록 만드는 기법을 사용합니다.

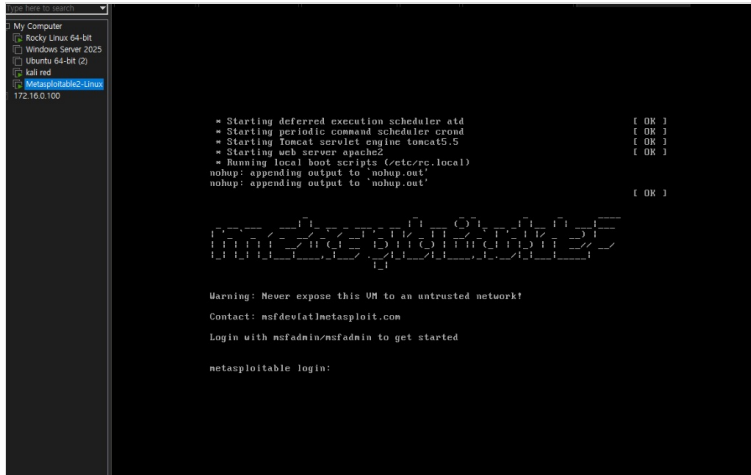
레지스트리는 윈도우 운영체제의 모든 설정 정보가 담긴 거대한 데이터베이스(DB)입니다. 이 중 인터넷 설정과 관련된 경로를 수정하면 시스템 전체의 프록시 동작을 강제할 수 있습니다.

1. 공격 환경 구성 (Metasploitable)

모의 해킹 실습을 위해 의도적으로 보안 취약점이 다수 존재하는 **Metasploitable 리눅스**를 공격 대상 서버로 구성합니다.

가상 머신 환경에서 Metasploitable2-Linux 서버가 선택된 상태입니다.

Metasploitable2-Linux 항목 선택됨

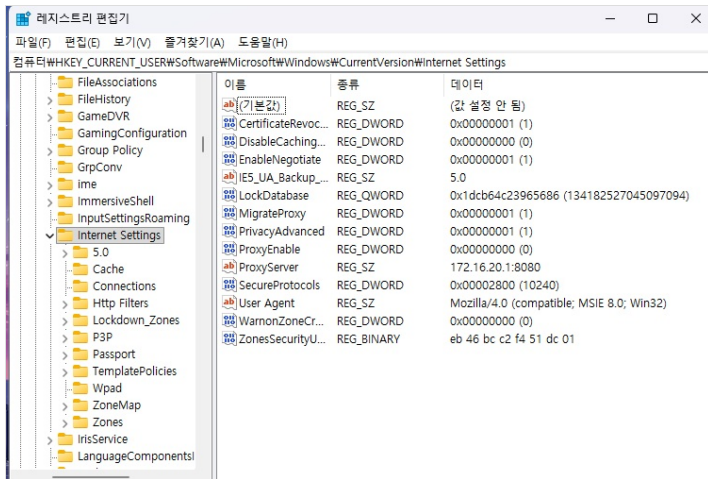


가상 머신 목록에서 Metasploitable2-Linux가 선택되어 있는 상태

공격 대상이 될 취약한 서버 환경을 준비하는 단계입니다.

서버가 정상적으로 부팅되어 로그인 프롬프트가 나타나면 공격 준비가 완료된 것입니다.

metasploitable login: 텍스트 표시



Metasploitable 리눅스 서버의 부팅이 완료되어 로그인 프롬프트가 나타난 상태

사용자 계정(msfadmin/msfadmin)을 통해 접속할 수 있는 상태임을 확인합니다.

2. 프록시 자동 설정 자동화 (Registry & Batch)

피해자의 프록시 설정을 자동화하기 위해 두 가지 방법을 사용할 수 있습니다.

방법 A: .reg 파일 사용

인코딩을 ANSI로 설정한 레지스트리 파일을 실행하여 설정을 주입합니다. 수정해야 할 경로는 다음과 같습니다.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

윈도우 설정 메뉴에서 현재 프록시가 꺼져 있는 상태를 확인합니다.

수동 프록시 설정 프록시 서버 사용 끄

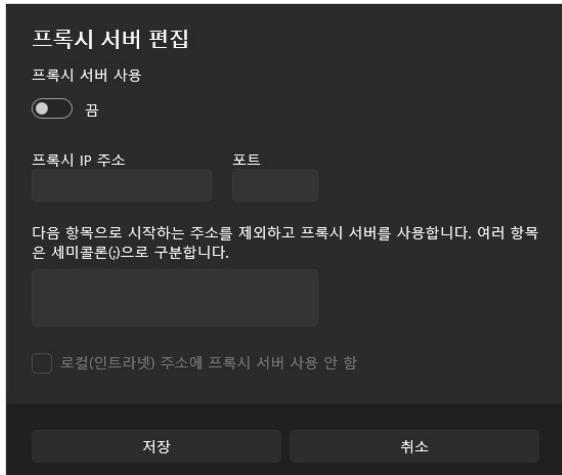


Windows 수동 프록시 설정 메뉴에서 프록시 서버 사용 항목이 꺼져 있는 상태

설정이 되어 있지 않은 초기 상태를 확인합니다.

프록시 설정 편집 창이 열려 있지만, 아직 정보가 입력되지 않은 상태입니다.

프록시 서버 사용 끄기 및 입력란 공란

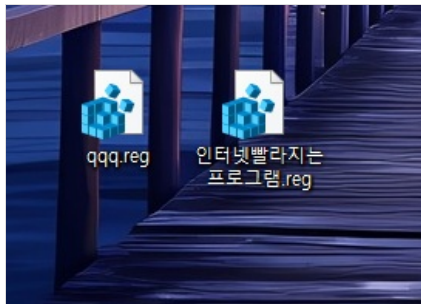


프록시 서버 편집 창에서 사용 설정이 비활성화되어 있고 정보가 입력되지 않은 상태

설정을 변경하기 전의 빈 상태를 나타냅니다.

레지스트리 편집기를 통해 직접 'ProxyEnable'과 'ProxyServer' 값이 설정되었는지 검증합니다.

ProxyEnable 0x00000001, ProxyServer 172.16.20.1:8080



레지스트리 편집기를 통해 ProxyEnable과 ProxyServer 값이 설정되었는지 확인한 결과

ProxyEnable이 1로, ProxyServer가 공격자의 IP(172.16.20.1:8080)로 정상 변경되었음을 확인합니다.

설정이 완료된 후 윈도우 설정 화면에서 프록시 서버가 활성화된 것을 확인합니다.

ProxyEnable 켜, IP 172.16.20.100, 포트 8080

프록시 서버 편집

프록시 서버 사용

컴

프록시 IP 주소
172.16.20.100

포트
8080

다음 항목으로 시작하는 주소를 제외하고 프록시 서버를 사용합니다. 여러 항목은 세미콜론(;)으로 구분합니다.

☐ 로컬(인트라넷) 주소에 프록시 서버 사용 안 함

저장

취소

프록시 서버 사용을 활성화하고 IP 172.16.20.100 및 포트 8080을 입력한 화면

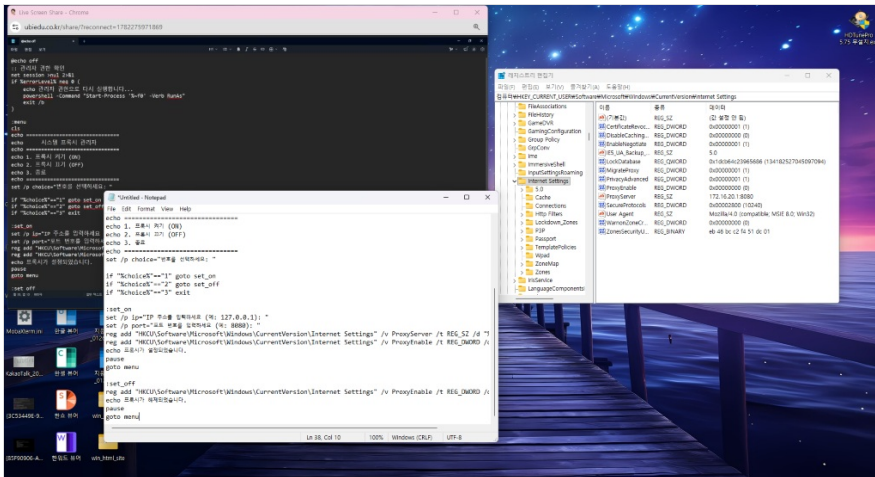
피해자의 트래픽이 이제 공격자의 프록시로 향하게 됩니다.

방법 B: .bat 파일(Batch File) 사용

명령 프롬프트(CMD)에서 실행되는 쉘 스크립트를 사용하여 더 빠르게 설정을 강제합니다. reg add 명령어를 사용하여 레지스트리를 직접 조작합니다.

배치 파일을 통해 레지스트리 명령어를 실행하면 시스템 설정이 즉각 반영됩니다.

ProxyEnable(1) 및 ProxyServer(172.16.20.1:8080) 레지스트리 값과 reg add 명령어가 포함된 배치 파일 소스



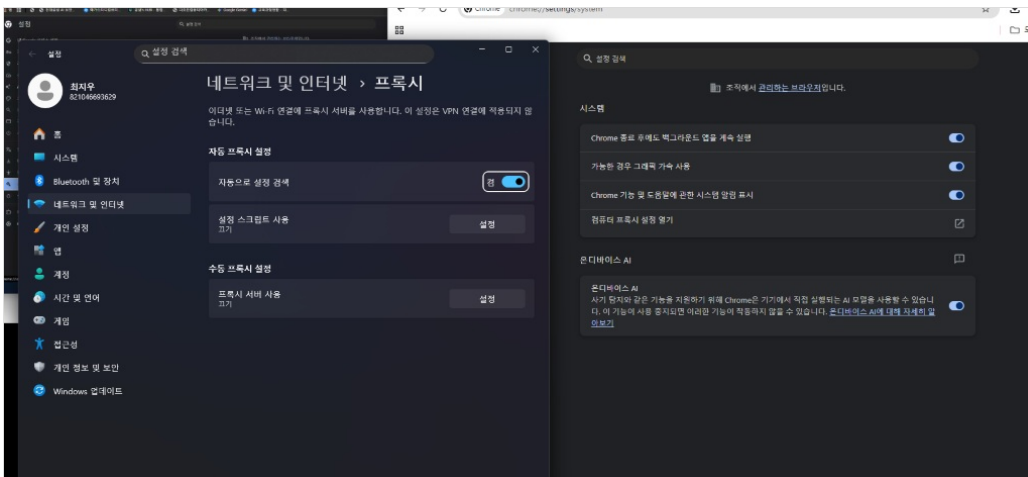
이 절차의 실습 결과를 확인하는 화면

배치 파일 코드와 함께 레지스트리 값이 성공적으로 주입된 환경을 보여줍니다.

관련 실습 화면

윈도우의 네트워크 및 인터넷 설정 메뉴를 통해 프록시 설정 페이지로 진입합니다.

네트워크 및 인터넷 > 프록시 메뉴 표시



Windows 설정 메뉴의 네트워크 및 인터넷 항목 내 프록시 설정 페이지

Burp Suite Intruder를 활용한 브루트포스 공격 검증

프록시를 통해 트래픽을 장악했다면, 다음 단계는 획득한 정보를 바탕으로 계정 탈취를 시도하는 것입니다. 가장 대표적인 방법이 **브루트포스(Brute Force)** 공격입니다.

브루트포스 공격이란 가능한 모든 문자열 조합이나 미리 준비된 사전(Dictionary) 파일을 이용하여 로그인을 시도하는 방식입니다. Burp Suite의 **Intruder** 기능을 사용하면 이 과정을 자동화할 수 있습니다.

실무/시험 포인트: 성공 여부 판단 기준

브루트포스 공격 시, 수많은 요청 중에서 어떤 것이 로그인에 성공했는지 어떻게 알 수 있을까요? 가장 쉬운 판단 기준은 **응답의 길이(Response Length)**를 확인하는 것입니다. 로그인 성공 시와 실패 시 서버가 리턴하는 메시지(예: "Welcome" vs "Invalid Password")의 길이가 다르기 때문에, 응답 길이를 기준으로 필터링하면 빠르게 정답을 찾을 수 있습니다.

실습을 통해 공격자가 브라우저의 요청 정보를 가로채고 이를 조작하여 공격을 수행하는 전체적인 흐름을 이해할 수 있습니다.

종합 점검 및 문제 해결 체크리스트

실습 중 발생할 수 있는 문제와 주요 점검 사항을 정리합니다.

1. 통신이 되지 않을 때 (Troubleshooting)

- 리스너 상태 확인:** Burp Suite의 Proxy → Options 탭에서 리스너의 **Running** 체크박스가 선택되어 있는지, 포트(8080)가 충돌하지 않는지 확인하십시오.
- 바인딩 주소 확인:** 외부 기기에서 접속하려면 리스너의 주소가 **127.0.0.1**이 아닌 **All interfaces** 또는 특정 외부 IP로 설정되어 있어야 합니다.
- 방화벽 확인:** 공격자 PC의 방화벽이 지정된 포트(8080)를 차단하고 있지 않은지 점검하십시오.

2. 프록시 설정이 적용되지 않을 때

- 레지스트리 경로 확인:** HKEY_CURRENT_USER\...\Internet Settings 경로가 정확한지 확인하십시오.
- 데이터 타입 확인:** ProxyEnable은 REG_DWORD 타입이어야 하며, ProxyServer는 REG_SZ 타입이어야 합니다.
- 인코딩 주의:** .reg 파일을 생성할 때는 반드시 **ANSI** 형식으로 저장해야 윈도우에서 정상적으로 인식됩니다.

3. 보안 실무 관점의 핵심 요약

구분	안전한 상태 (Safe)	위험한 상태 (At Risk)
프록시 설정	사용자 지정된 신뢰할 수 있는 서버만 사용	알 수 없는 IP/포트로 프록시가 자동 설정됨
ARP 동작	정적인 ARP 테이블 관리 및 GARP 모니터링	ARP 스푸핑을 통한 중간자 공격 노출
계정 보안	복잡한 비밀번호 및 2FA(2단계 인증) 사용	사전 공격(Dictionary Attack)에 취약한 단순 비밀번호

추가 실습 화면

실습 과정에서 확인된 추가적인 UI 구성 요소들입니다.

윈도우 수동 프록시 설정 창의 초기 상태입니다.

프록시 서버 정보를 입력하여 설정을 활성화하는 과정입니다.