

수업 내용 정리 보고서

작성일: 2026년 6월 24일

챕터 구성

- 네트워크 기초 및 ARP 프로토콜의 이해
- Burp Suite를 이용한 중간자 공격(MITM) 및 트래픽 분석
- 레지스트리 및 스크립트를 활용한 프록시 설정 자동화
- 실습 핵심 요약 및 운영 점검 리스트

네트워크 기초 및 ARP 프로토콜의 이해

네트워크 통신에서 장치 간에 데이터를 주고받기 위해서는 논리적인 주소인 IP 주소와 물리적인 주소인 MAC 주소를 연결하는 과정이 필수적입니다. 이 역할을 수행하는 핵심 프로토콜이 바로 **ARP(Address Resolution Protocol)**입니다. ARP는 네트워크 상에서 특정 IP 주소를 가진 장치의 MAC 주소를 알아내기 위해 사용됩니다.

ARP 프로토콜은 사용 목적과 동작 방식에 따라 크게 5가지 종류로 구분할 수 있습니다. 각 프로토콜의 차이점은 다음과 같습니다.

종류	주요 기능 (동작 방향)	상세 설명 및 특징
ARP	IP → MAC	가장 기본적인 형태로, 특정 IP 주소에 해당하는 MAC 주소를 요청하여 알아냅니다.
RARP	MAC → IP	자신의 MAC 주소를 알고 있을 때, 이에 대응하는 IP 주소를 서버에 요청합니다.
Proxy ARP	IP → MAC (대리 응답)	라우터가 대상 IP의 MAC 주소를 직접 알지 못하더라도, 마치 자신이 대상인 것처럼 대신 응답하여 통신을 중계합니다.
Inverse ARP	DLCI → IP	프레임 릴레이(Frame Relay) 환경에서 자신의 DLCI를 통해 상대방의 IP 주소를 식별합니다. (요청 정보가 없음)
GARP (Gratuitous ARP)	자기 정보 알림	상대방의 요청이 없더라도 자신의 IP/MAC 정보를 네트워크에 브로드캐스트하여 존재를 알립니다.

ARP의 동작 원리를 이해하는 것은 네트워크 트래픽을 분석하거나, 중간자 공격(MITM)과 같은 보안 위협을 탐지하는 데 있어 매우 중요한 기초가 됩니다.

Burp Suite를 이용한 중간자 공격(MITM) 및 트래픽 분석

중간자 공격(Man-In-The-Middle Attack, MITM)은 통신하는 두 당사자(클라이언트와 서버) 사이에 공격자가 끼어들어 데이터를 가로채거나 조작하는 공격 방식입니다. 이를 실습하기 위해 사용하는 도구가 **Burp Suite**입니다. Burp Suite는 HTTP 프로토콜을 대상으로 하는 **프록시(Proxy) 서버** 역할을 수행하며, 클라이언트와 서버 사이의 트래픽을 중계합니다.

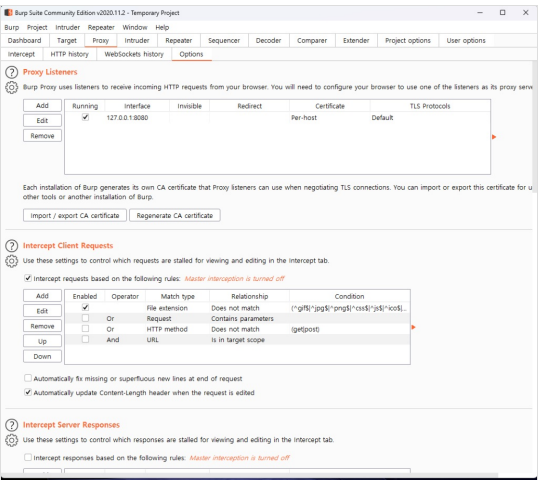
Burp Suite를 통한 트래픽 제어는 크게 세 가지 상태로 구분됩니다.

- **스니핑(Sniffing):** 흐르는 패킷을 단순히 관찰하고 내용을 읽는 행위입니다.
- **스푸핑(Spoofing):** 가로챈 패킷의 내용을 공격자의 의도대로 수정하여 전달하는 행위입니다.
- **바이패싱(Bypassing):** 가로챈 패킷을 아무런 수정 없이 그대로 전달하는 상태입니다.

프록시 서버 설정 및 리스너 구성

공격자가 클라이언트의 트래픽을 가로채기 위해서는 먼저 Burp Suite가 클라이언트의 요청을 기다릴 수 있도록 '리스너(Listener)'를 설정해야 합니다. 리스너는 특정 IP와 포트에서 들어오는 연결을 대기하는 설정입니다.

Burp Suite의 Proxy 메뉴 내 Options 탭에서는 현재 활성화된 리스너의 정보를 관리할 수 있습니다. 리스너가 정상적으로 구동 중인지 확인하는 것이 첫 번째 단계입니다.



Proxy Listeners 설정 메뉴에서 현재 활성화된 리스너의 인터페이스와 포트 정보를 확인

위 화면을 통해 현재 127.0.0.1:8080 주소에서 리스너가 동작하고 있음을 알 수 있습니다. 만약 외부 장치(피해자)의 트래픽을 받아야 한다면, 이 주소를 로컬 호스트(127.0.0.1)가 아닌 공격자의 실제 IP로 변경해야 합니다.

리스너의 상세 설정을 변경하기 위해 'Edit' 버튼을 누르면 바인딩(Binding) 설정을 할 수 있는 창이 나타납니다. 여기서 포트 번호와 바인딩할 주소를 지정합니다.

실습 화면 해석

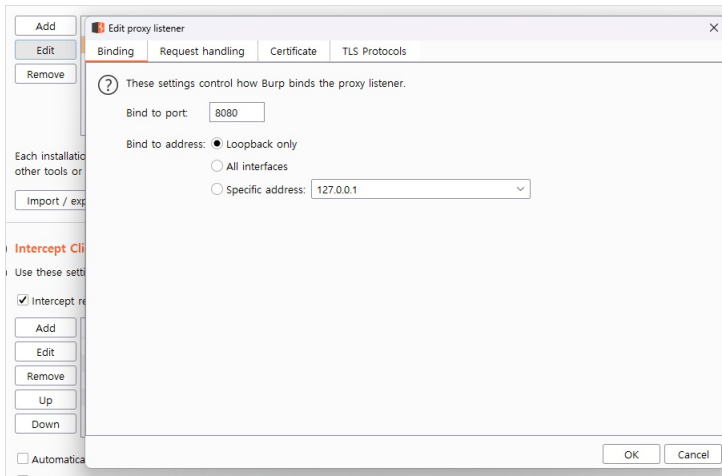
- Bind to port: 8080
- Bind to address: Specific address (127.0.0.1)

Add	Running ^	Interface	Invisible	Redirect	Certificate	TLS Protocols
Edit	☐	127.0.0.1:8080			Per-host	Default
Remove						

프록시 리스너의 바인딩 주소와 포트를 변경하기 위한 Edit Proxy Listener 창

설정 창에서 특정 주소를 선택하여 리스너를 바인딩할 수 있습니다. 외부 환경에서 접근 가능하도록 설정하는 것이 핵심입니다.

- Available Addresses: 127.0.0.1, 172.16.20.1 등



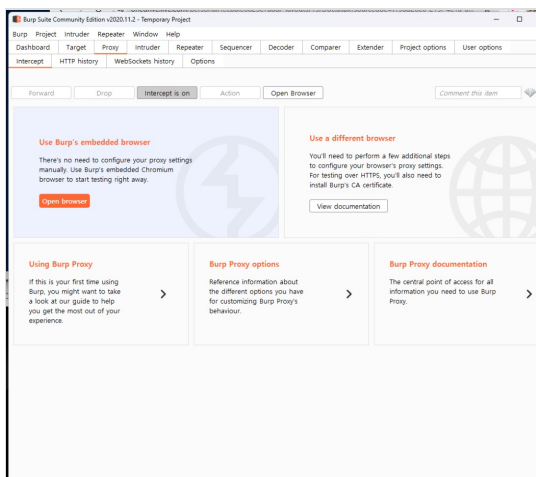
리스너의 바인딩 주소를 특정 IP(172.16.20.1)로 지정하여 외부 접근을 허용하는 과정

목록에서 공격자의 네트워크 IP(예: 172.16.20.1)를 선택함으로써, 동일 네트워크 내의 피해자가 공격자의 Burp Suite로 트래픽을 보내도록 유도할 수 있습니다.

패킷 가로채기(Intercept) 및 분석

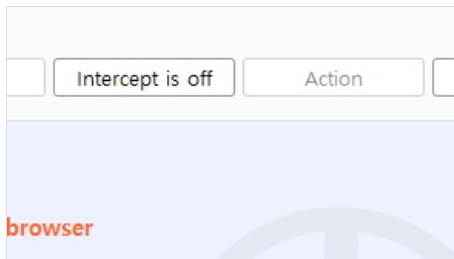
리스너 설정이 완료되면, 이제 실제 패킷을 가로채서 내용을 확인하거나 수정할 준비를 합니다. Burp Suite의 **Intercept** 기능은 클라이언트가 보낸 요청이 서버로 가기 전, 프록시 서버에서 멈춰 있게 만드는 기능입니다.

Intercept 기능의 상태에 따라 트래픽 흐름이 결정됩니다.



Intercept 기능이 켜져 있어 클라이언트의 요청을 일시 중단하고 가로챌 수 있는 상태

Intercept가 'On' 상태이면 패킷이 멈춰 있으며, 공격자는 내용을 확인한 뒤 **Forward**를 눌러 전달하거나 **Drop**를 눌러 버릴 수 있습니다.



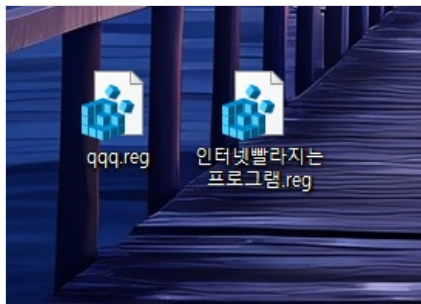
Intercept 기능이 꺼져 있어 패킷이 수정 없이 그대로 전달되는 바이패싱(Bypassing) 상태

Intercept가 'Off' 상태이면 패킷은 가로채지지 않고 그대로 통과(Bypassing)하게 됩니다.

가로채기에 성공하면 클라이언트가 보낸 실제 HTTP 요청의 Raw 데이터를 확인할 수 있습니다. 이를 통해 쿠키, 헤더, 파라미터 등을 분석하여 취약점을 찾을 수 있습니다.

실습 화면 해석

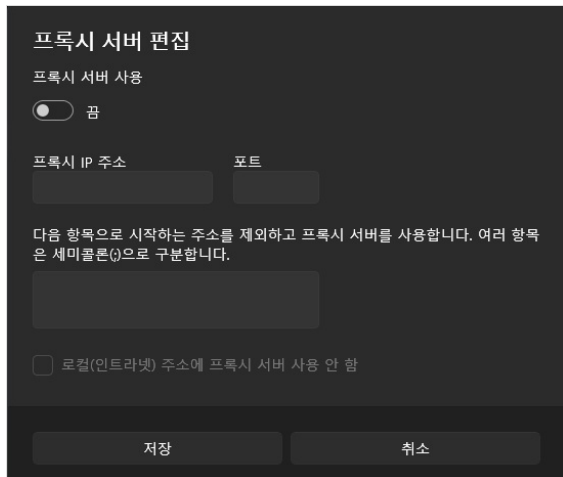
- Method: GET
- Host: 172.16.16.97
- Cookie: wp-settings-time-1=1779785750



가로채기(Intercept)를 통해 확인한 HTTP GET 요청의 헤더와 쿠키 정보

가로챈 패킷의 내용을 통해 클라이언트의 브라우저 정보(User-Agent)와 세션 정보(Cookie) 등을 정밀하게 분석할 수 있습니다.

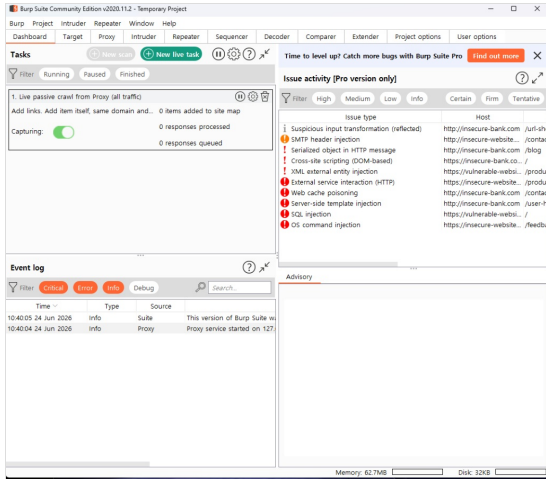
이러한 공격 실습을 위해서는 의도적으로 취약점을 노출시킨 환경이 필요합니다. 본 실습에서는 **Metasploitable** 리눅스를 사용합니다. 이는 모의 해킹 연습을 위해 다양한 취약점이 미리 설치된 훈련용 운영체제입니다.



모의 해킹 실습을 위한 Metasploitable 리눅스의 부팅 완료 및 로그인 대기 화면

Metasploitable이 정상적으로 부팅되면 로그인 프롬프트가 나타납니다. 지정된 계정(msfadmin/msfadmin)으로 접속하여 공격 대상 서버로 활용합니다.

전체적인 공격 흐름은 Burp Suite의 대시보드를 통해 실시간으로 모니터링하며, 수집된 데이터와 발견된 이슈를 종합하여 공격 전략을 수립합니다.



Burp Suite 대시보드에서 현재 실행 중인 태스크와 발견된 취약점 요약 정보를 확인

대시보드에서는 현재 진행 중인 크롤링 상태와 발견된 보안 이슈(SQL Injection, XSS 등)를 한눈에 파악할 수 있습니다.

레지스트리 및 스크립트를 활용한 프록시 설정 자동화

공격자가 피해자의 컴퓨터에 직접 접속할 수 없는 상황이라면, 어떻게 피해자의 브라우저 트래픽을 공격자의 프록시 서버로 보낼 수 있을까요? 정답은 **윈도우 레지스트리(Registry)**를 수정하는 것입니다. 레지스트리는 윈도우 운영체제의 모든 설정이 저장된 거대한 데이터베이스입니다.

피해자의 브라우저가 공격자의 프록시를 사용하도록 만들려면 레지스트리 내의 다음 경로를 수정해야 합니다.

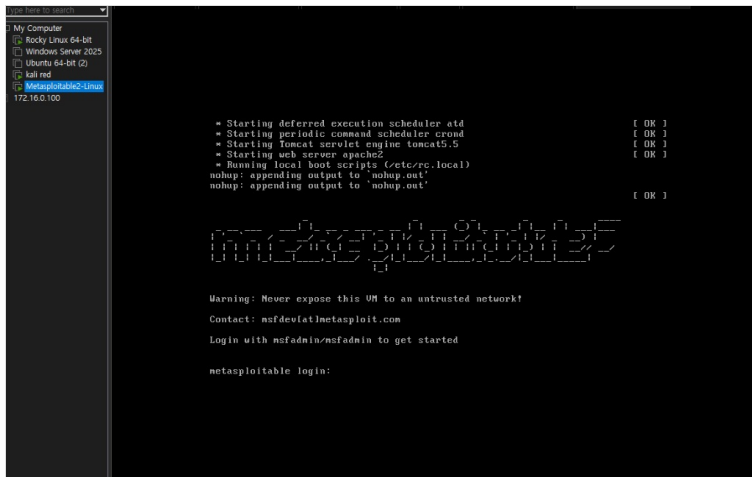
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

- **ProxyEnable**: 프록시 사용 여부 (1: 사용, 0: 미사용)
- **ProxyServer**: 프록시 서버의 주소와 포트 (예: 172.16.20.1:8080)

이 과정을 수동으로 하는 대신, 공격자는 **.reg** 파일이나 **.bat** 파일을 만들어 실행함으로써 피해자의 설정을 순식간에 변경할 수 있습니다.

자동화 스크립트 작성

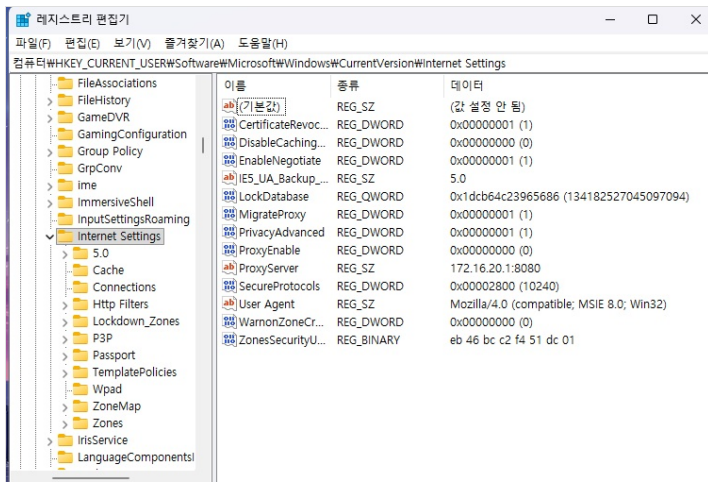
첫 번째 방법은 레지스트리 편집 파일인 **.reg** 파일을 사용하는 것입니다. 주의할 점은 파일 저장 시 반드시 **ANSI 인코딩** 형식을 사용해야 윈도우에서 정상적으로 인식됩니다.



실습 화면에서 확인되는 설정·상태·검증 결과를 본문 근거로 활용합니다.

작성된 .reg 파일을 실행하면 즉시 레지스트리 값이 변경됩니다.

두 번째 방법은 윈도우용 쉘 스크립트인 **배치 파일(.bat)**을 사용하는 것입니다. reg add 명령어를 사용하여 명령 프롬프트(CMD) 환경에서 레지스트리를 조작합니다.

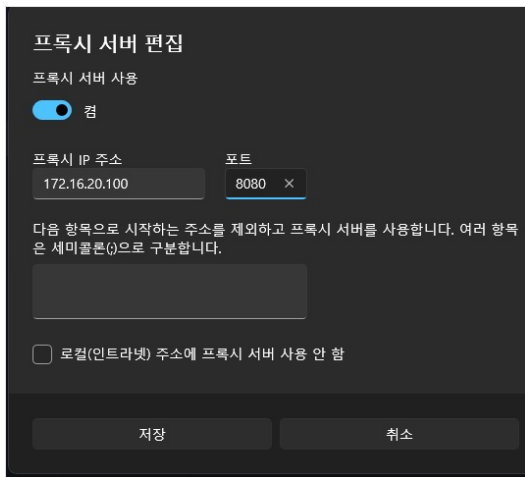


실습 화면에서 확인되는 설정·상태·검증 결과를 본문 근거로 활용합니다.

위 스크립트는 사용자가 IP와 포트를 입력하면 자동으로 'ProxyServer'와 'ProxyEnable' 값을 레지스트리에 등록하도록 설계되었습니다.

설정 결과 확인 및 검증

스크립트 실행 후에는 실제로 설정이 반영되었는지 확인해야 합니다. 가장 확실한 방법은 **레지스트리 편집기(Regedit)**를 직접 열어 데이터 값을 확인하는 것입니다.



레지스트리 편집기를 통해 ProxyServer와 ProxyEnable 값이 올바르게 수정되었는지 확인

확인 결과, 'ProxyServer'에 공격자의 IP와 포트가, 'ProxyEnable'에 1(사용)이 정상적으로 기록되어 있습니다.

또한, 일반 사용자가 확인하는 **윈도우 설정 UI**를 통해서도 확인할 수 있습니다. 설정이 성공하면 브라우저의 모든 트래픽은 공격자의 Burp Suite를 경유하게 됩니다.



윈도우 수동 프록시 설정에서 공격자의 IP와 포트가 성공적으로 적용된 화면

수동 프록시 설정 메뉴에 공격자의 IP(172.16.20.100)와 포트(8080)가 입력된 것을 확인할 수 있습니다. 이제 피해자의 모든 HTTP 요청은 공격자에게 전달됩니다.

실습 핵심 요약 및 운영 점검 리스트

이번 실습을 통해 네트워크 프로토콜의 기초부터 실제적인 중간자 공격 및 설정 자동화 과정까지 학습하였습니다. 실무 및 보안 점검 시 다음 사항을 반드시 유의하십시오.

핵심 요약

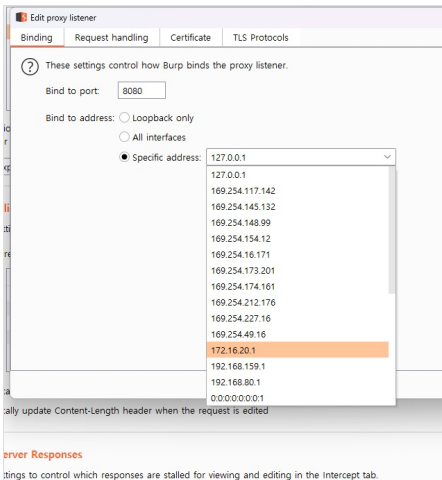
- **ARP 프로토콜:** IP와 MAC 주소를 매핑하는 과정에서 발생하는 특성(RARP, Proxy ARP 등)을 이해해야 네트워크 트래픽 흐름을 제어할 수 있다.
- **Burp Suite 활용:** Proxy 리스너를 적절한 IP/Port로 설정하고, Intercept 기능을 통해 패킷을 가로채고(Sniffing) 수정(Spoofing)하는 메커니즘을 숙지한다.
- **설정 자동화:** 윈도우 레지스트리 조작을 통해 클라이언트의 프록시 설정을 강제로 변경할 수 있으며, 이때 인코딩 방식(ANSI)과 명령어(reg add)의 정확성이 중요하다.

운영 및 보안 점검 리스트

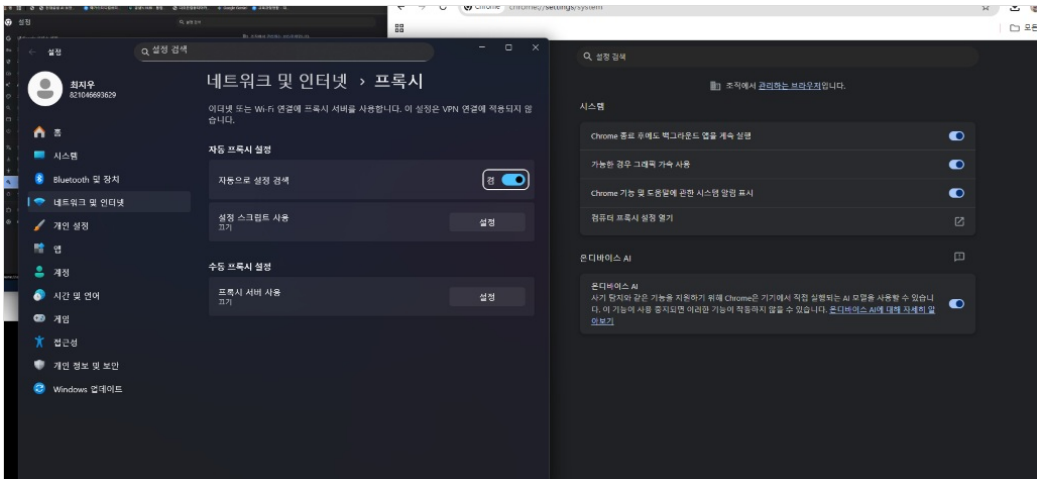
점검 항목	확인 사항	주의/조치
프록시 설정 임의 변경 여부	레지스트리 'Internet Settings' 경로의 값 확인	모르는 IP가 설정되어 있다면 즉시 제거 및 악성코드 검사
네트워크 리스너 상태	불필요한 포트(예: 8080)가 오픈되어 있는지 확인	비인가된 프록시 서비스 중단
스크립트 실행 주의	출처를 알 수 없는 .reg, .bat 파일 실행 금지	실행 전 반드시 스크립트 내용(명령어)을 검토할 것
인코딩 오류	.reg 파일이 적용되지 않을 경우	메모장에서 'ANSI' 인코딩으로 다시 저장하여 시도

추가 실습 화면

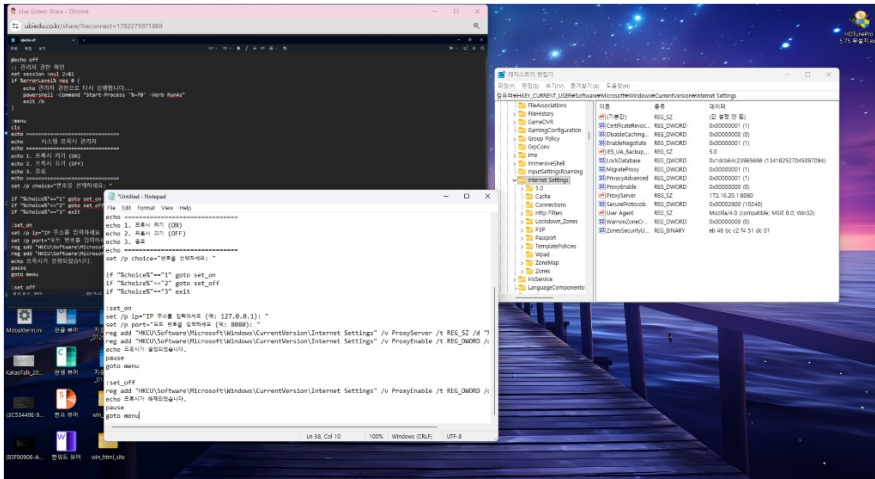
본문에서 주요하게 다루지 않았으나 실습 과정에서 확인된 화면들입니다.



윈도우 네트워크 설정에서 프록시 서버 사용 여부를 결정하는 기본 메뉴 화면

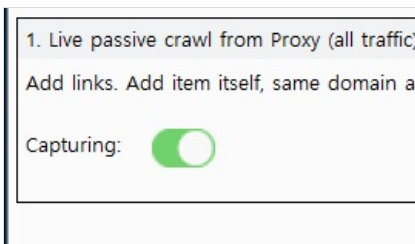


윈도우 수동 프록시 설정에서 프록시 사용이 꺼져 있는 상태

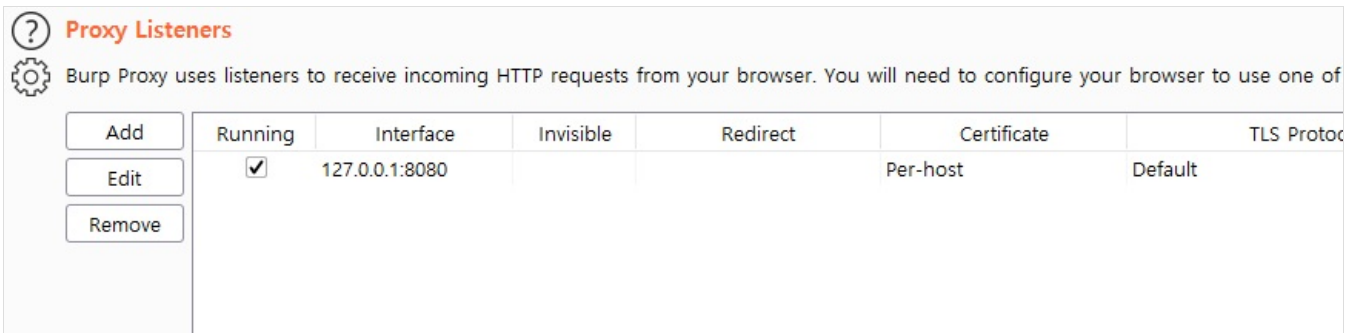


실습 화면에서 확인되는 설정·상태·검증 결과를 본문 근거로 활용합니다.

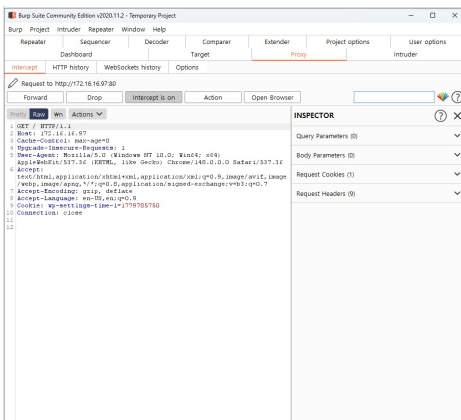
추가 실습 화면



본문 내용을 보충하는 실습 화면으로, 설정·상태·검증 결과를 함께 확인할 수 있습니다



본문 내용을 보충하는 실습 화면으로, 설정·상태·검증 결과를 함께 확인할 수 있습니다



본문 내용을 보충하는 실습 화면으로, 설정·상태·검증 결과를 함께 확인할 수 있습니다