

# 수업 내용 정리 보고서

작성일: 2026년 6월 24일

## 챕터 구성

1. ARP 프로토콜과 트래픽 분석의 기초
2. Burp Suite를 활용한 중간자 공격(MITM)과 패킷 제어
3. 프록시 설정 자동화 및 모의해킹 환경 구축

## ARP 프로토콜과 트래픽 분석의 기초

네트워크 통신이 이루어지기 위해서는 데이터가 목적지까지 정확히 도달할 수 있도록 논리적 주소(IP)를 물리적 주소(MAC)로 변환하는 과정이 필수적입니다. 이 과정에서 핵심적인 역할을 하는 것이 **ARP(Address Resolution Protocol)**입니다. ARP는 단순히 주소를 찾는 것 외에도 다양한 변형 프로토콜을 통해 네트워크 환경에 대응합니다.

### ARP 프로토콜의 종류와 특징

ARP 프로토콜은 요청의 목적과 방식에 따라 크게 5가지 형태로 구분할 수 있습니다. 아래 표를 통해 각 프로토콜의 차이점을 정리합니다.

| 종류                    | 주요 기능 (방향) | 상세 설명 및 동작 원리                                                                      |
|-----------------------|------------|------------------------------------------------------------------------------------|
| ARP                   | IP → MAC   | 특정 IP 주소를 가진 호스트의 MAC 주소를 찾기 위해 요청을 보냅니다.                                          |
| RARP                  | MAC → IP   | 자신의 MAC 주소는 알지만 IP 주소를 모를 때, IP 주소를 알아내기 위해 사용합니다.                                 |
| Proxy ARP             | IP → MAC   | 라우터가 자신의 인터페이스에 연결된 다른 호스트를 대신하여 ARP 요청에 응답하는 방식입니다.                               |
| Inverse ARP           | DLCI 식별    | 자신의 DLCI(Data Link Connection Identifier)를 통해 FR(Frame Relay) 스위치에 정보를 물어보는 방식입니다. |
| GARP (Gratuitous ARP) | 정보 갱신      | 별도의 요청 없이 자신의 IP/MAC 정보를 네트워크에 뿌려 IP 충돌을 방지하거나 캐시를 업데이트합니다.                        |

### 네트워크 트래픽 분석 도구

네트워크 상에 흐르는 데이터 패킷을 확인하고 분석하는 기술을 **패킷 캡처(Packet Capture)**라고 하며, 이를 위해 **Pcap** 형식을 사용합니다. 실무에서는 목적에 따라 다음과 같은 도구를 활용합니다.

- **Wireshark**: 네트워크 패킷을 실시간으로 캡처하여 상세하게 분석할 수 있는 그래픽 기반 도구입니다.
- **tcpdump**: 커맨드 라인 환경에서 패킷을 캡처하고 덤프(Dump) 파일로 저장하는 데 주로 사용됩니다.
- **Sniffing(스니핑)**: 네트워크를 흐르는 패킷을 단순히 '보기만 하는' 행위입니다.
- **Spoofing(스푸핑)**: 가로챈 패킷을 단순히 보는 것에 그치지 않고, 내용을 조작하여 전달하는 공격 행위입니다.

## Burp Suite를 활용한 중간자 공격(MITM)과 패킷 제어

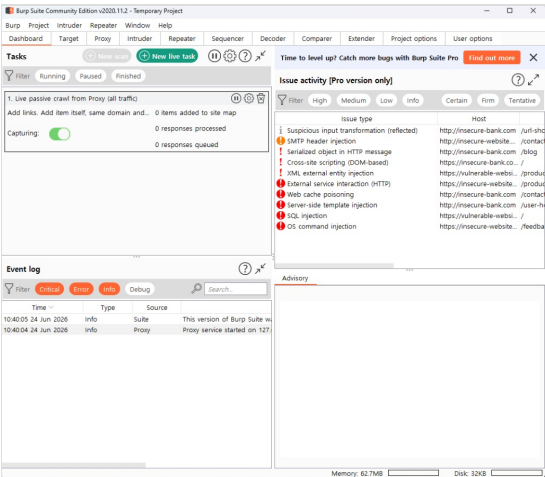
**MITM(Man-In-The-Middle, 중간자 공격)**은 클라이언트(A)와 서버(B) 사이의 통신 경로에 공격자가 개입하여 데이터를 가로채거나 조작하는 공격입니다. **Burp Suite**는 HTTP 트래픽을 대상으로 하는 프록시(Proxy) 서버 역할을 수행하여 이러한 환경을 구성하는 데 사용됩니다.

### 실습 환경 구성: MITM 시나리오

본 실습에서는 공격자 역할을 하는 Burp Suite를 중심으로, 피해자가 되는 클라이언트(Windows)와 타겟 서버(Metasploitable Linux)를 구성합니다. 공격자는 클라이언트가 보내는 HTTP 요청을 프록시 서버로 전달받아 내용을 검토한 후, 서버로 전달하거나 드랍(Drop)할 수 있습니다.

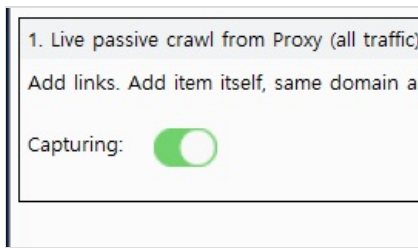
### Burp Suite를 이용한 패킷 제어 및 분석

Burp Suite의 핵심 기능은 트래픽을 가로채서 공격자가 원하는 대로 제어하는 것입니다. 'Intercept' 기능을 통해 패킷을 멈춰 세우고 내용을 수정할 수 있습니다. 먼저, Burp Suite의 대시보드를 통해 현재 수행 중인 작업과 탐지된 보안 취약점들을 확인할 수 있습니다. 패시브 크롤링(Passive Crawl)이 활성화되면 별도의 공격 없이도 사이트 구조를 파악하고 취약점을 탐지합니다.



Burp Suite 대시보드에서 패시브 크롤링이 실행 중이며 SQL Injection, XSS 등 다양한 보안 이슈가 탐지된 화면

패시브 크롤링이 활성화되어 있는지 확인하는 방법은 Tasks 영역의 상태를 보는 것입니다. Capturing 스위치가 녹색으로 켜져 있어야 트래픽 수집이 시작됩니다.

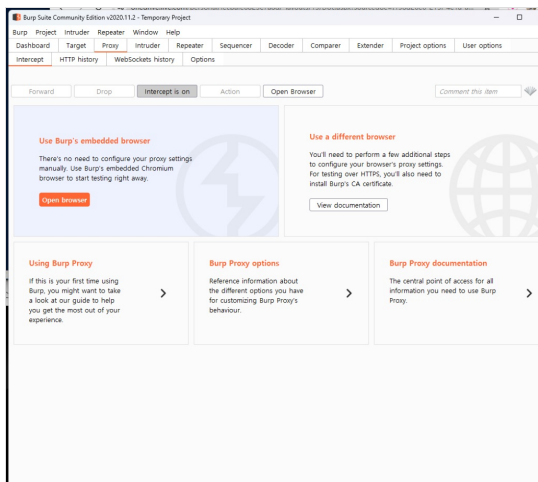


Live passive crawl 작업의 Capturing 상태 스위치가 녹색(On)으로 활성화된 모습

패킷 제어의 핵심인 **Intercept** 기능은 두 가지 상태를 가집니다.

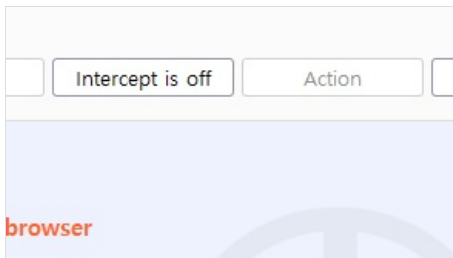
- **Intercept is on:** 브라우저에서 보내는 요청이 프록시 서버에 걸려 멈춥니다. 이때 공격자는 패킷을 확인하고 수정하거나, **Forward**를 눌러 전달하고, **Drop**를 눌러 버릴 수 있습니다.
- **Intercept is off:** 패킷을 가로채지 않고 그대로 통과시킵니다. 이를 **Bypassing** 상태라고 합니다.

실제로 Intercept 기능이 활성화되어 요청을 대기 중인 상태는 다음과 같습니다.



Proxy 탭의 Intercept 기능이 'Intercept is on' 상태로 활성화된 화면

반대로 패킷을 가로채지 않고 통과시키는 상태는 다음과 같이 표시됩니다.

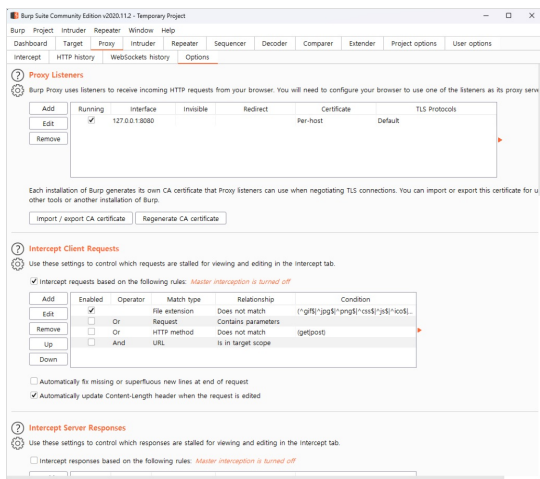


Proxy 탭의 Intercept 기능이 'Intercept is off' 상태로 비활성화된 화면

## 프록시 리스너(Proxy Listener) 설정

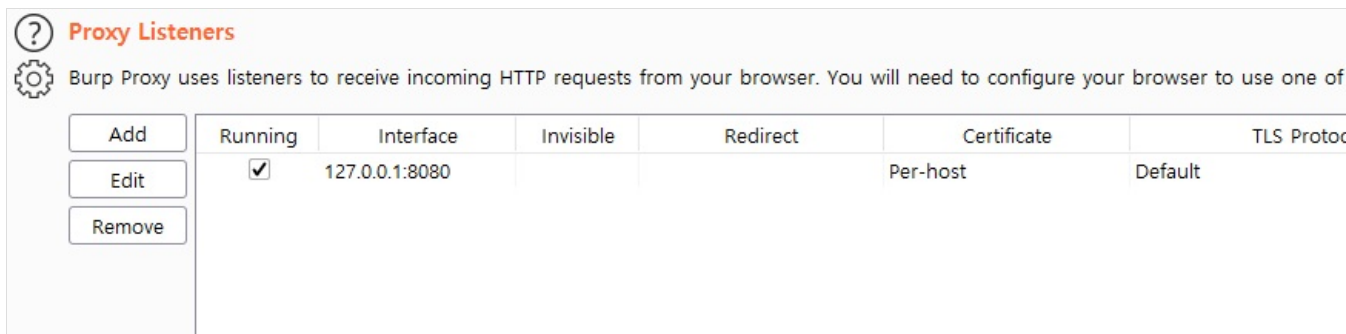
Burp Suite가 트래픽을 받으려면 특정 IP와 포트에서 대기하는 '리스너'가 설정되어 있어야 합니다. 기본적으로 127.0.0.1:8080 환경이 구성됩니다.

Proxy 옵션 메뉴에서는 현재 동작 중인 리스너의 인터페이스와 상태를 관리할 수 있습니다.



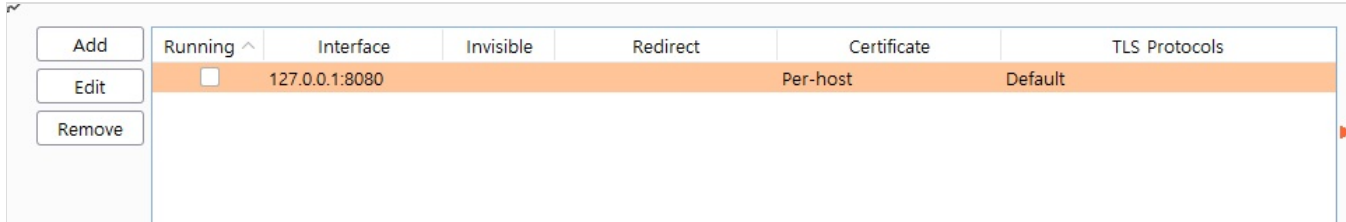
Burp Suite Proxy Options 탭에서 리스너 설정과 Intercept 규칙을 관리하는 화면

리스너 목록에서 현재 127.0.0.1:8080 포트가 정상적으로 실행(Running) 중인지 확인합니다.



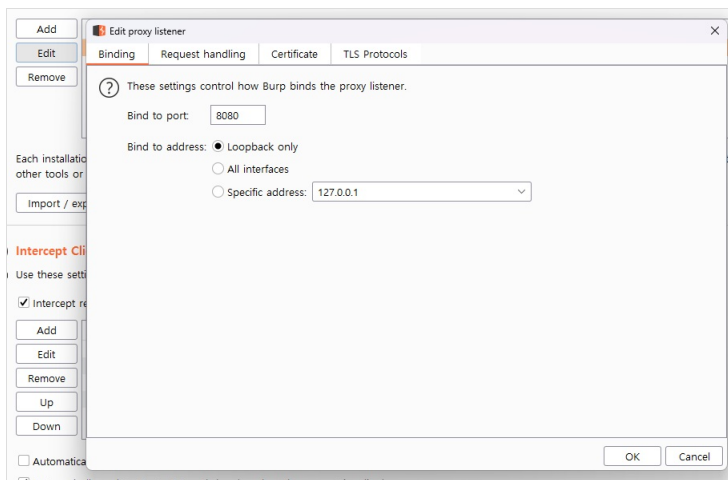
Proxy Listeners 목록에서 127.0.0.1:8080 인터페이스가 실행 중임을 보여주는 화면

특정 리스너 항목을 선택하여 상세 정보를 확인할 수 있습니다.



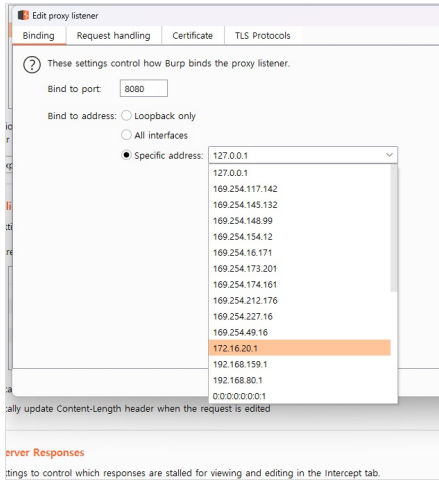
선택된 Proxy Listener의 인터페이스와 인증서 설정 정보를 보여주는 상세 행

리스너의 동작 주소를 변경하려면 'Edit' 버튼을 통해 바인딩(Binding) 설정을 수정해야 합니다. 예를 들어, 외부 호스트로부터의 접근을 허용하려면 Loopback only 옵션을 해제하고 특정 IP를 지정해야 합니다.



Edit proxy listener 창에서 Bind to address를 특정 주소로 설정하기 위한 Binding 탭 화면

사용 가능한 네트워크 인터페이스 목록에서 공격자가 사용할 IP 주소를 선택하는 과정입니다.



Edit proxy listener 창에서 Specific address 항목의 드롭다운을 통해 172.16.20.1 주소를 선택하는 화면

## 취약점 탐지 및 브루트포스 공격

Burp Suite의 **Intruder** 기능을 사용하면 브루트포스(Brute-force) 공격을 수행할 수 있습니다. 이는 사전(Dictionary) 파일에 있는 여러 아이디와 비밀번호를 자동으로 대입해보는 방식입니다. 이때 로그인 성공/실패 시 서버가 리턴하는 응답 패킷의 길이가 다를 경우, 이를 식별하여 유효한 계정을 찾아낼 수 있습니다.

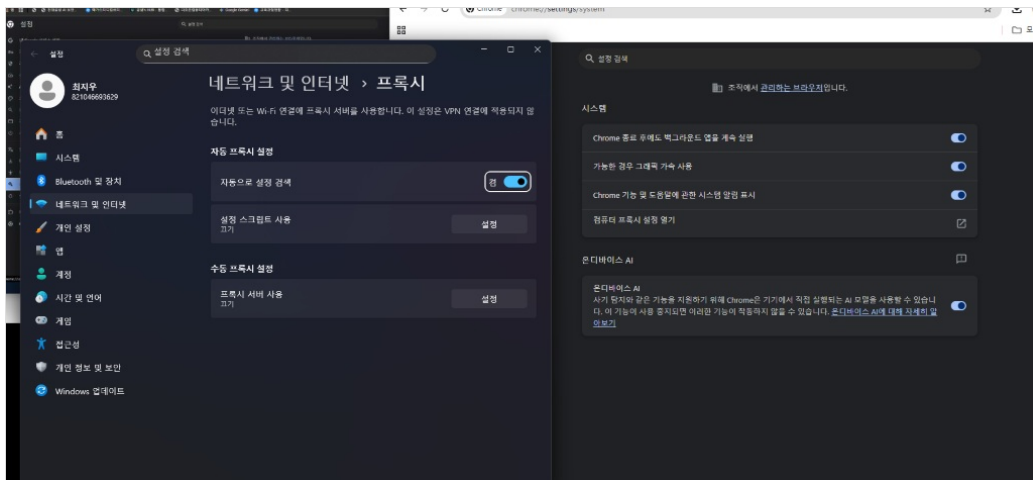
## 프록시 설정 자동화 및 모의해킹 환경 구축

모의해킹 실습을 위해 피해자 컴퓨터의 브라우저 프록시 설정을 일일이 수동으로 바꾸는 것은 비효율적입니다. 따라서 **윈도우 레지스트리(Registry)**를 조작하여 프록시 설정을 자동으로 변경하는 기법을 사용합니다.

### 레지스트리를 통한 프록시 강제 설정

윈도우 운영체제의 설정 저장소인 레지스트리 내 **Internet Settings** 경로를 수정하면 프록시 사용 여부와 서버 주소를 한 번에 제어할 수 있습니다.

먼저, 대상 컴퓨터(피해자)의 현재 프록시 설정 상태를 확인합니다. 수동 프록시 설정이 꺼져 있는 상태는 다음과 같습니다.



윈도우 설정의 네트워크 및 인터넷 메뉴와 크롬 설정 화면

수동 프록시 사용(Proxy Server) 스위치가 '끔(Off)' 상태인 일반적인 설정 화면입니다.



윈도우 네트워크 설정에서 프록시 서버 사용이 비활성화된 상태의 화면

프록시 서버 편집 창에서도 현재 설정된 IP나 포트가 없는 상태를 확인할 수 있습니다.

프록시 서버 편집

프록시 서버 사용

☐ 끄

프록시 IP 주소

포트

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 편집 창에서 사용 설정이 꺼져 있고 입력값이 비어 있는 화면

공격자가 준비한 프록시 서버 주소(예: 172.16.20.100:8080)로 설정을 변경하면 다음과 같이 활성화됩니다.

프록시 서버 편집

프록시 서버 사용

☒ 켜

프록시 IP 주소

포트

172.16.20.100

8080 ×

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

☐ 로컬(인트라넷) 주소에 프록시 서버 사용 안 함

저장

취소

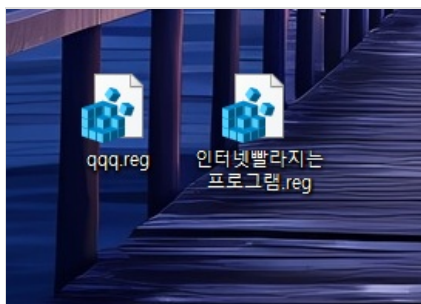
프록시 서버 편집 창에 공격자의 IP 172.16.20.100과 포트 8080이 입력되고 활성화된 화면

## 자동화 스크립트 활용 (.reg 및 .bat)

이 과정을 자동화하기 위해 두 가지 파일을 제작할 수 있습니다. **주의사항**으로, 레지스트리 파일은 반드시 **ANSI 인코딩**으로 저장해야 윈도우에서 정상적으로 인식됩니다.

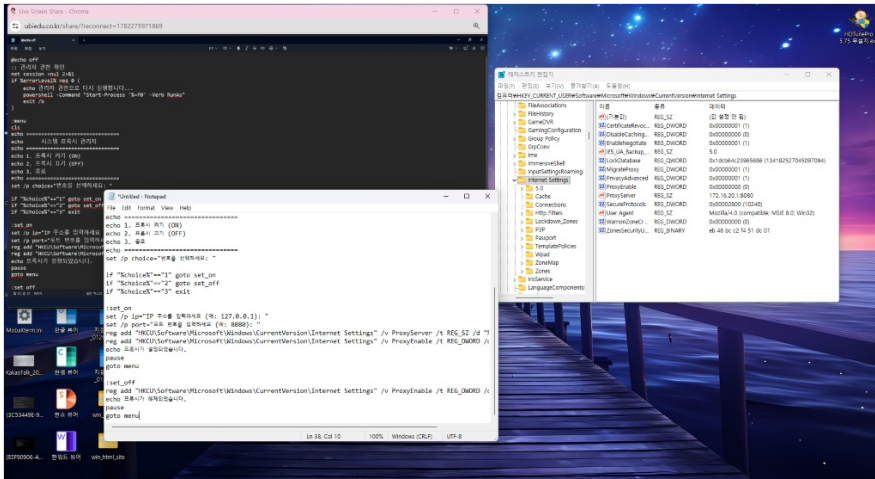
1. **.reg 파일**: 레지스트리 값을 직접 삽입하는 파일입니다. ProxyEnable을 1로, ProxyServer를 지정된 주소로 설정하는 텍스트를 포함합니다.
2. **.bat 파일**: 윈도우 명령 프롬프트(CMD)에서 실행되는 배치 파일입니다. reg add 명령어를 사용하여 명령줄에서 즉시 레지스트리를 수정합니다.

제작된 레지스트리 파일들이 바탕화면에 준비된 모습입니다.



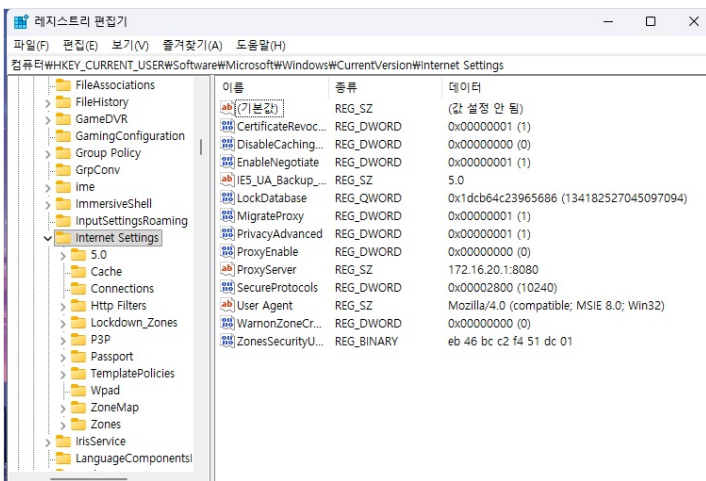
실습 화면에서 확인되는 설정-상태-검증 결과를 본문 근거로 활용합니다.

메모장으로 작성된 배치 파일(.bat)의 내부 코드는 다음과 같이 레지스트리 경로에 값을 추가하는 명령어를 담고 있습니다.



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

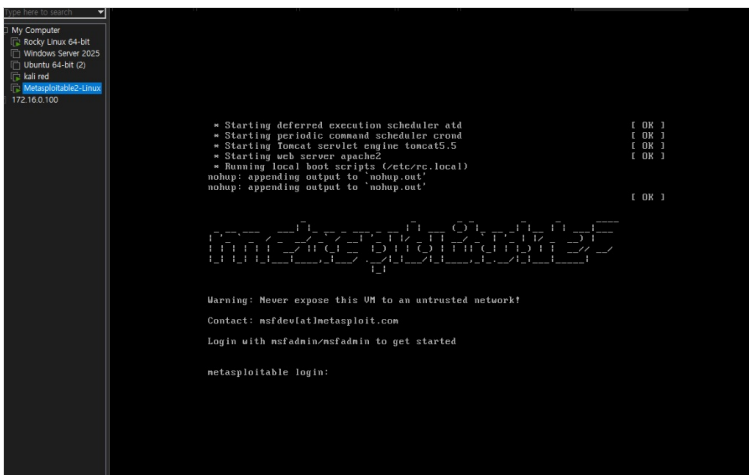
스크립트 실행 후, 레지스트리 편집기(regedit)를 통해 설정이 제대로 반영되었는지 검증합니다.



레지스트리 편집기에서 ProxyEnable이 1로, ProxyServer가 172.16.20.1:8080으로 변경된 것을 확인하는 화면

## 모의해킹 타겟: Metasploitable

실습의 대상이 되는 **Metasploitable**은 보안 취약점 테스트를 위해 의도적으로 많은 취약점을 노출시킨 리눅스 배포판입니다. 공격자는 이 서버의 서비스들을 대상으로 다양한 공격을 시도하게 됩니다.



Metasploitable2 리눅스 서버의 터미널 로그인 대기 화면

## 실습 및 점검 체크리스트

모의해킹 환경 구축 및 프록시 제어 실습을 마친 후, 다음 항목들을 통해 정상 작동 여부를 점검하십시오.

### 1. 프록시 환경 점검

- [ ] Burp Suite의 Listener가 지정한 포트(예: 8080)에서 **Running** 상태인가?

- [ ] 클라이언트 브라우저의 프록시 설정이 공격자의 IP로 올바르게 변경되었는가?
- [ ] Intercept 기능을 켜둘 때 브라우저의 요청이 Burp Suite에서 멈추는가?

## 2. 자동화 스크립트 검증

- [ ] .reg 또는 .bat 파일 실행 시 인코딩 문제(ANSI)로 인한 오류는 없는가?
- [ ] 레지스트리 편집기에서 ProxyEnable 값이 0x00000001 (1)로 변경되었는가?
- [ ] ProxyServer 값이 [공격자IP]:[포트] 형식으로 정확히 입력되었는가?

## 3. 문제 해결 (Troubleshooting)

- **프록시 설정 후 인터넷 연결이 안 될 경우:** Burp Suite의 Listener가 켜져 있는지, 혹은 클라이언트의 프록시 IP/Port가 리스너 설정과 일치하는지 확인하십시오.
- **레지스트리 적용이 안 될 경우:** 배치 파일 실행 시 관리자 권한이 필요한지 확인하고, 파일의 인코딩이 ANSI인지 반드시 재점검하십시오.
- **패킷이 가로채지지 않을 경우:** Burp Suite의 Intercept is on 상태인지, 그리고 브라우저의 프록시 설정이 127.0.0.1(로컬)이 아닌 공격자의 IP를 향하고 있는지 확인하십시오.

## 추가 실습 화면

---

본문에 포함되지 않은 기타 실습 관련 화면들입니다.