‹ back to dashboard

Network Reconnaissance ♥ EXPIRED

Information gathering of live wireless and wired network data

`15-45 Minutes` `390 Points` `4/10 Difficulty`

Start Stop

✓ You have already completed this exercise.

Mission Statement Verify Flags Solution

Information gathering is the first and most important phase of penetration testing. Also known as the Reconnaissance phase. Penetration testing without information on the target host/network is like attacking in the dark. Gaining maximum information about the target host should be your purpose before diving into the exploitation phase of a pentest.

Reconnaissance is performed in 2 ways:

1. Active Reconnaissance
2. Passive Reconnaissance

Active recon is performed by directly probing the client and analysing the response, whereas Passive recon is rather simply sit and wait for the packets to arrive to you, either via MITM or simply sniffing promiscuously. In this lab, you'll learn both, Active and Passive Reconnaissance

Objective:

1. Identify servers running on non-TCP ports
2. Detect servers behind firewall
3. Identify wireless router manufacturer
4. Gather probing client's information

Note
This lab is an environment dedicated to you exclusively. That means this environment is never shared with any other student. So, no downtime or connection drops you would've faced in a shared-server CTF-like environment