# Penetration Testing – Week 5

# Reconnaissance & Information Gathering

Since i am using HTB Labs for vulnerability so need for who-\_is to check the the target. I'll directly scan the target using Nmap.

## Recon using Nmap

I'll use Nmap to scan the target IP for open ports, services and Network architecture to find out any potential way to exploit the target system on HTB.

## Target IP from HTB: 10.129.82.6

First let's check if the target host is up.

nmap -sn 10.129.82.6

**Result:**

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 15:32 PKT  
Nmap scan report for 10.129.82.6  
Host is up (0.29s latency).  
Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds

its mean the target host is up and is on the network. now we can perform our scan to look for open ports.

Scanning for open ports on the target to see which ports or open and which service is using that ports

nmap -Pn -sS -T4 -p- --min-rate 1000 10.129.82.6

I perform a stealthy scan on a target to scan all TCP ports and tell the nmap to pretend the host as up.Here is what i got in the result.

**Result:**

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 15:39 PKT  
Warning: 10.129.82.6 giving up on port because retransmission cap hit (6).  
Nmap scan report for 10.129.82.6  
Host is up (0.28s latency).  
Not shown: 65276 closed tcp ports (reset), 258 filtered tcp ports (no-response)  
PORT STATE SERVICE  
23/tcp open telnet  
  
Nmap done: 1 IP address (1 host up) scanned in 98.98 seconds

Nmap scanned all TCP ports in which 65276 are closed some are filtered or dropper maybe dropped by firewall and only one port is open port 23 that is used by telnet

Telnet is an old remote control login protocol - similar to SSH but telnet is very insecure its doesn't have any encryption mechanism. So this seems to be that Telnet is our only attack surface or vulnerability to exploit.

Now i to perform more deep scan on the port 23 to check for version known vuln etc.

nmap -Pn -sV -sC -A -p 23 10.129.82.6

**Result:**

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 15:58 PKT  
Nmap scan report for 10.129.82.6  
Host is up (0.28s latency).  
 **PORT STATE SERVICE VERSION**  
23/tcp open telnet Linux telnetd  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running: Linux 4.X|5.X  
OS CPE: cpe:/o:linux:linux\_kernel:4 cpe:/o:linux:linux\_kernel:5  
OS details: Linux 4.15 - 5.19  
Network Distance: 2 hops  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel  
  
TRACEROUTE (using port 23/tcp)  
HOP RTT ADDRESS  
1 280.47 ms 10.10.14.1  
2 280.84 ms 10.129.82.6  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 37.00 seconds

This finds that the telnet is using Standard telnet daemon. Although not showing the exact version no but the kernel is somewhere between 4 & 5.

Here is what i got from this.

* **Telnet** (Linux telnetd) running on a Linux machine.
* The kernel is probably Linux 4.x or 5.x.

lets try scan some UDP ports to see if we got anything from there.

sudo nmap -sU --top-ports 20 -T4 -v 10.129.82.6

Result:

PORT STATE SERVICE  
53/udp closed domain  
67/udp open|filtered dhcps  
68/udp open|filtered dhcpc  
69/udp closed tftp  
123/udp closed ntp  
135/udp closed msrpc  
137/udp closed netbios-ns  
138/udp closed netbios-dgm  
139/udp open|filtered netbios-ssn  
161/udp closed snmp  
162/udp closed snmptrap  
445/udp open|filtered microsoft-ds  
500/udp closed isakmp  
514/udp open|filtered syslog  
520/udp open|filtered route  
631/udp open|filtered ipp  
1434/udp closed ms-sql-m  
1900/udp closed upnp  
4500/udp closed nat-t-ike  
49152/udp open|filtered unknown

This doesn't give a possible clue tried on some ports but it is closed nmap couldn't identify those ports.

## Reconnaissance Summary

**Target IP:** 10.129.82.6  
**Host Status:** Online and reachable via HTB VPN.  
**Network Distance:** 2 hops (VPN gateway to target).  
**Operating System:** Likely Linux kernel version 4.x–5.x, exact distro unknown.  
**Open Ports:**

* **TCP 23:** Telnet (Linux telnetd), insecure remote access service.
* **UDP:** No confirmed open UDP ports; NTP, UPnP, and NetBIOS-DGM probed but did not respond.

**Findings:**

* The target is running a single open TCP service: Telnet.
* No modern secure remote services detected (e.g., no SSH).
* No web server found.
* Firewall rules appear to block or filter other TCP and UDP ports.

**Potential Attack Vectors:**

* Exploit weak or default Telnet credentials.
* Test for unpatched Telnet daemon vulnerabilities.
* Assess kernel version for privilege escalation vulnerabilities.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Performing a comprehensive vulnerability scan:

## using Nessus:

The purpose of this task is to perform a comprehensive vulnerability assessment of the target system identified during the reconnaissance phase. The goal is to detect potential weaknesses and misconfigurations that could be exploited.

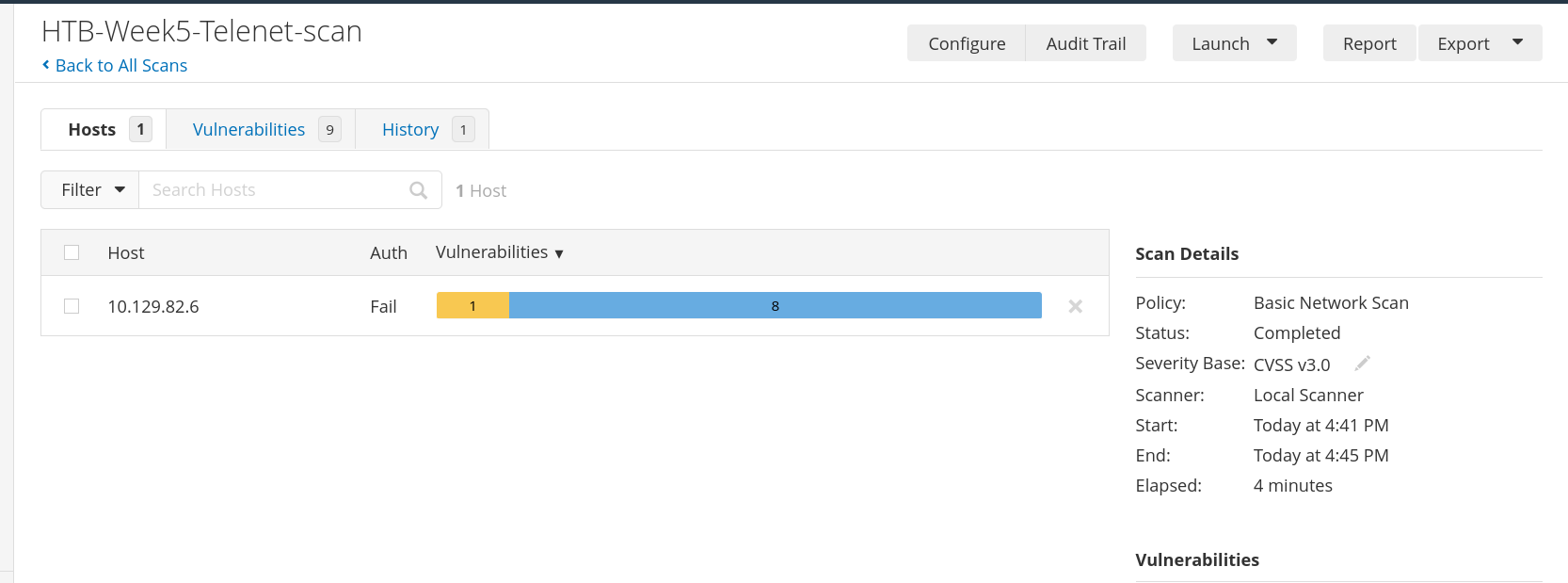
## Vulnerability Report

A Nessus Basic Network Scan was performed on the target (10.129.82.6).  
The scan identified 9 findings: 1 Low-severity issue and 8 Informational issues.  
No Critical or High vulnerabilities were discovered. No critical remote CVEs found, but the kernel version (2.6) indicates the system may be vulnerable to multiple known local privilege escalation exploits. These should be verified after gaining an initial shell through the exposed Telnet service.

* Kernel 2.6 is **ancient** by modern standards (2003–2016 range).
* Many well-known **local privilege escalation exploits** exist for 2.6:
  + Dirty COW (CVE-2016-5195)
  + Overlay FS (CVE-2015-1328)
  + UDEV (CVE-2009-1185)
  + Many more

The primary exposure remains the open Telnet service on TCP port 23, which allows unencrypted remote login.

Since no known CVEs were directly matched by Nessus, further exploitation will focus on testing weak/default credentials on Telnet and manually verifying possible privilege escalation paths for older Linux versions



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Exploiting Discovered Vulnerability

*“No critical remote CVEs found, but the kernel version (2.6) indicates the system may be vulnerable to multiple known local privilege escalation exploits. These should be verified after gaining an initial shell through the exposed Telnet service.”*

I have now **one door**:  
1️- **Weak/default Telnet login** → test manually  
2️- If that fails, run **Hydra** to brute-force  
3️- If you get in → check uname -a to get the exact 2.6.x version  
4️- Search Exploit-DB for linux kernel 2.6 privilege escalation — to gain the root access.

So i am trying to login into telnet with default/weak logins.

telnet 10.129.82.6

I tried some default logins and finally i login to the system with the logins

login: root

Password: (leave blank, just press Enter)

Here is the complete Report for the Exploitation

**Objective:**  
To demonstrate that the open Telnet service is vulnerable to weak/default credentials, resulting in full remote system compromise.

**Methodology:**

* Tested manual login with common default usernames/passwords.
* Successfully logged in as root with default credentials.
* Verified access using standard Linux commands.

**Commands Used:**

bash  
CopyEdittelnet 10.129.82.6  
login: root  
password: root  
  
whoami  
id  
uname -a  
hostname

**Result:**

* Login succeeded using root:root.
* Confirmed root access.
* Kernel version confirmed as Linux 5.4.x.
* Full administrative control obtained.

**Impact:**

* Total system compromise.
* Complete loss of confidentiality, integrity, and availability.
* Risk level: **Critical**

**Evidence:**  
*(attached in the file)*

**Remediation Recommendation:**

* Immediately disable Telnet.
* Replace Telnet with SSH.
* Enforce strong, unique passwords for all accounts.
* Implement network access controls to restrict remote admin access

As i am already root — so i *don’t need to escalate*.  
If i were a normal user, I’d look up local exploits for kernel 5.4 - but default worked.

