Scan Report: 192.168.134.137

Scan results for 192.168.134.137

Generated: 2025-09-22

Scanner: kali@kali

Commands used: nmap -sV -p1-1000, nmap --script=..., nc, ssh -v

```
------------------------------------------------------------

== Nmap basic scan (command: nmap -sV -p1-1000) ==
Host is up (0.0000040s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0p2 Debian 5 (protocol 2.0)

------------------------------------------------------------

== Nmap SSH enumeration (banner + algos + vuln scripts) ==
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0p2 Debian 5 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_10.0p2 Debian-5
...

------------------------------------------------------------

== Banner grab (nc 192.168.134.137 22) ==
SSH-2.0-OpenSSH_10.0p2 Debian-5

------------------------------------------------------------
```

== ssh -v debug snippet (aborted) ==

```
debug1: OpenSSH_10.0p2 Debian-5, OpenSSL 3.5.0 8 Apr 2025

debug1: Reading configuration data /etc/ssh/ssh_config

...
```

== Findings summary ==

Host: 192.168.134.137

Ports discovered: 22/tcp (OpenSSH 10.0p2 Debian-5)

Banner: SSH-2.0-OpenSSH_10.0p2 Debian-5

Nmap vuln scripts: no CVEs reported by automated NSE during this scan

Notes: Server supports modern ciphers but also advertises legacy MACs and compression.

Recommendation: Check patches, verify admin config, enforce key-based auth, disable compression if possible.