OpenVAS Scan Analysis — Metasploitable2

1. Tools:
    - Nmap
    - GVM/OpenVAS

Scan Config: Full and Fast

2. Summary

- Scanned 1 host.
- Findings: 20 High, 32 Medium, 4 Low and 78 Log.

3. Findings (3 high)

- Operating System(OS) and End of life(EOL) detection –

  The operating system on the remote system has reached its end of life.

  Impact : An EOL version of an OS does not receiving any security updates from the vendor.

  Solution : Mitigation

- Possible backdoor ingreslock –

  A backdoor is installed on the remote host.

  Impact : Attackers can exploits this issues to execute arbitrary commands in the context of application. Successful attacks will compromise the infected system.

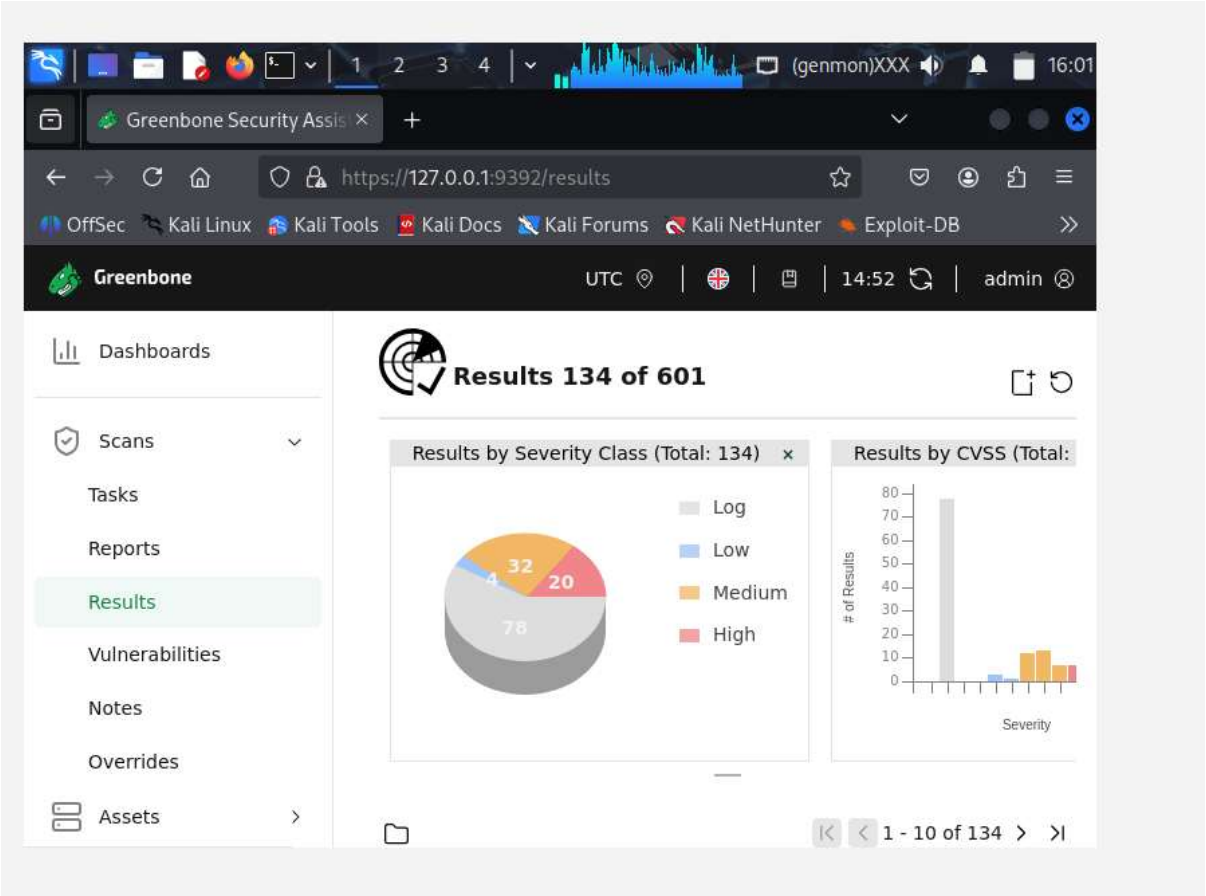
  Solution : Workaround – a whole cleanup of the affected system is recommended.

- rlogin passwordless login –

  The rlogin allows root access without a password.

Impact : This vulnerability allows an attacker to gain complete control over the attacker system.

Solution : Mitigation – Disable the rlogin services and use alternatives like SSH instead.



SCAN RESULT