1)PUNTI CHIAVE

- Configurazione scansione attraverso Nessus
- Filtraggio range di porte
- Avvio della scansione
- Approfondimento delle vulnerabilità incontrate

2)INTRODUZIONE

Nessus è un potente strumento di scansione di vulnerabilità dei sistemi informatici, evidenziando quest'ultime e suggerendo le possibili soluzioni per estinguerle.

3)PANORAMICA

Attraverso Nessus,è stato possibile configurare e avviare una scansione della macchina Target e restringere la stessa a porte specifiche.

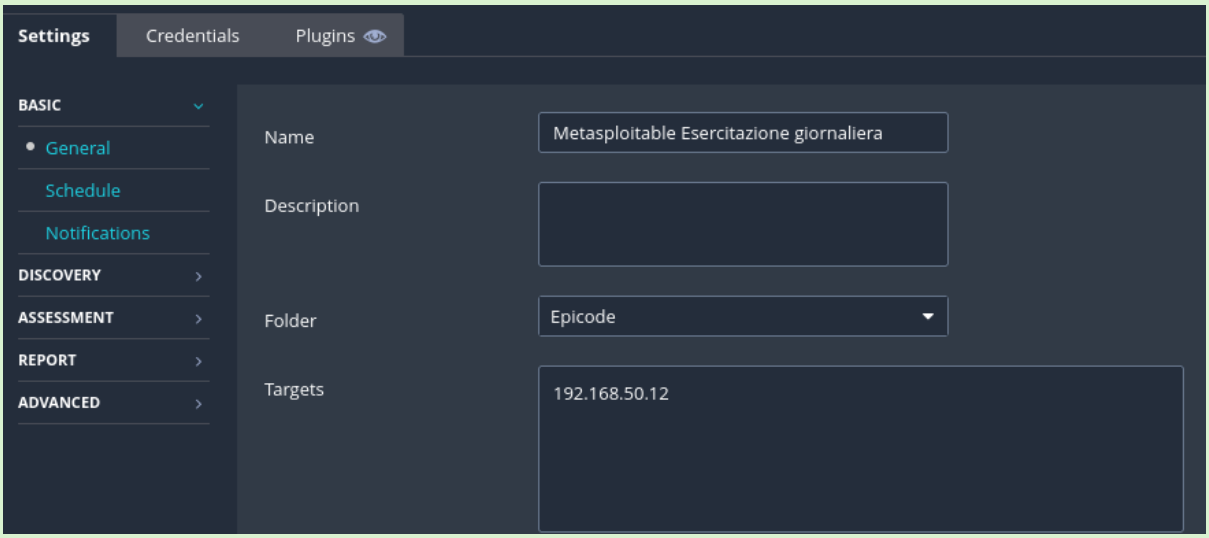
Tutte le vulnerabilità presentate alla fine della scansione, sono state approfondite dalle pagine Web presenti nei Link forniti.

4) IP METASPLOITABLE

**IP Metasploitable*

Tutte le scansioni di vulnerabilità descritte nel report hanno utilizzato come target l'indirizzo IP associato alla macchina ***Metasploitable*** al fine di identificare vulnerabilità specifiche .

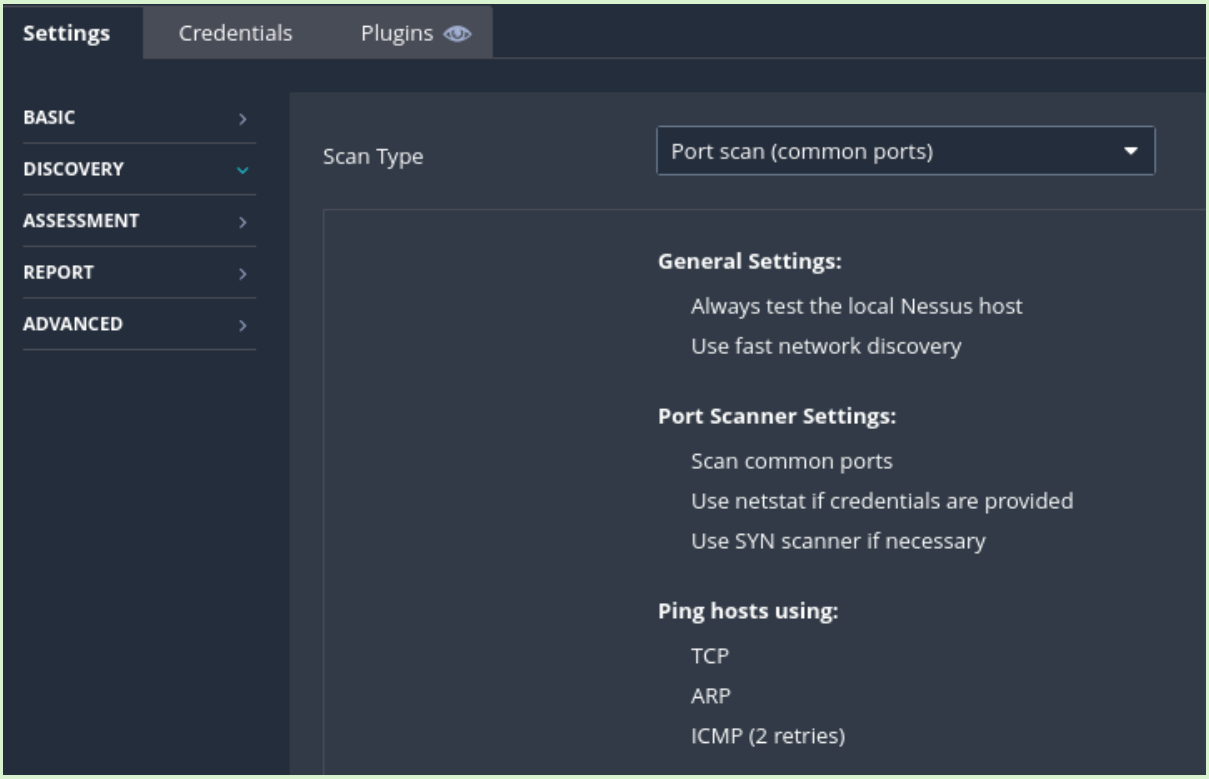
5)CONFIGURAZIONE SCANSIONE NESSUS



Configurazione scansione Metasploitable

In ***General*** è stato specificato il nome da dare alla scansione, la cartella dove verrà inserita e l'IP della macchina Target.

6)RESTRIZIONE RANGE PORTE

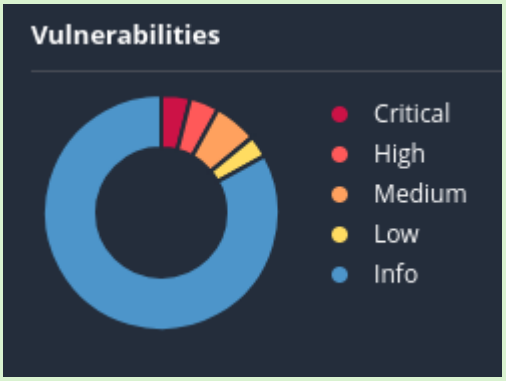


Restrizione range porte (solo comuni)

È stato richiesto di restringere la scansione solo alle porte comuni, serve a capire se il target è attivo e quali porte sono aperte.

7)AVVIAMENTO SCANSIONE

Selezionando il comando **Launch**, si avvia la procedura di scansione;la durata dell'operazione varia in base alla complessità del livello di sicurezza del target e dei plugin selezionati.



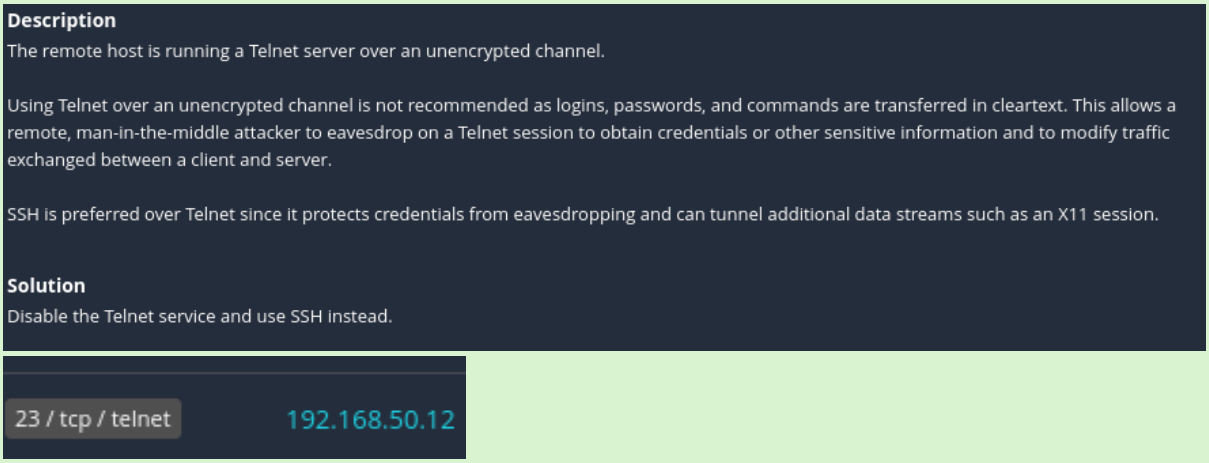
**Riepilogo vulnerabilità*

Il riepilogo presenta:

- **Vulnerabilità Critiche e Alte:** Rappresentano le falle più pericolose poiché potrebbero consentire a un utente malintenzionato di ottenere il controllo remoto del sistema;priorità più alta
- **Vulnerabilità Medie e Basse:** Spesso legate a configurazioni o servizi che possono fornire informazioni utili ; priorità bassa
- **Informazioni:** Forniscono dettagli come le porte aperte e i servizi attivi

8)ANALISI VULNERABILITÀ E APPROFONDIMENTO

8.1)Porta 23

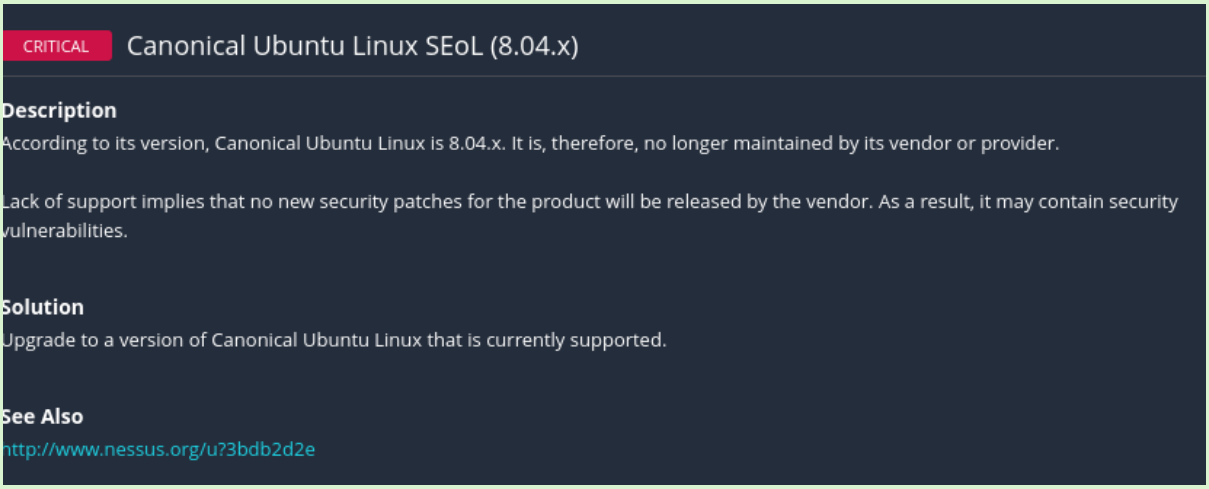


**Descrizione vulnerabilità e soluzione nella porta 23*

Nessus ha rilevato che nella porta 23 gira il servizio Telnet su un canale non crittografato, questo può aumentare il rischio di ***sniffing***.

Viene suggerito come soluzione di disabilitare il servizio Telnet e usare invece **SSH (Secure Shell)**, assicurando che la gestione remota avvenga in modo sicuro e protetto.

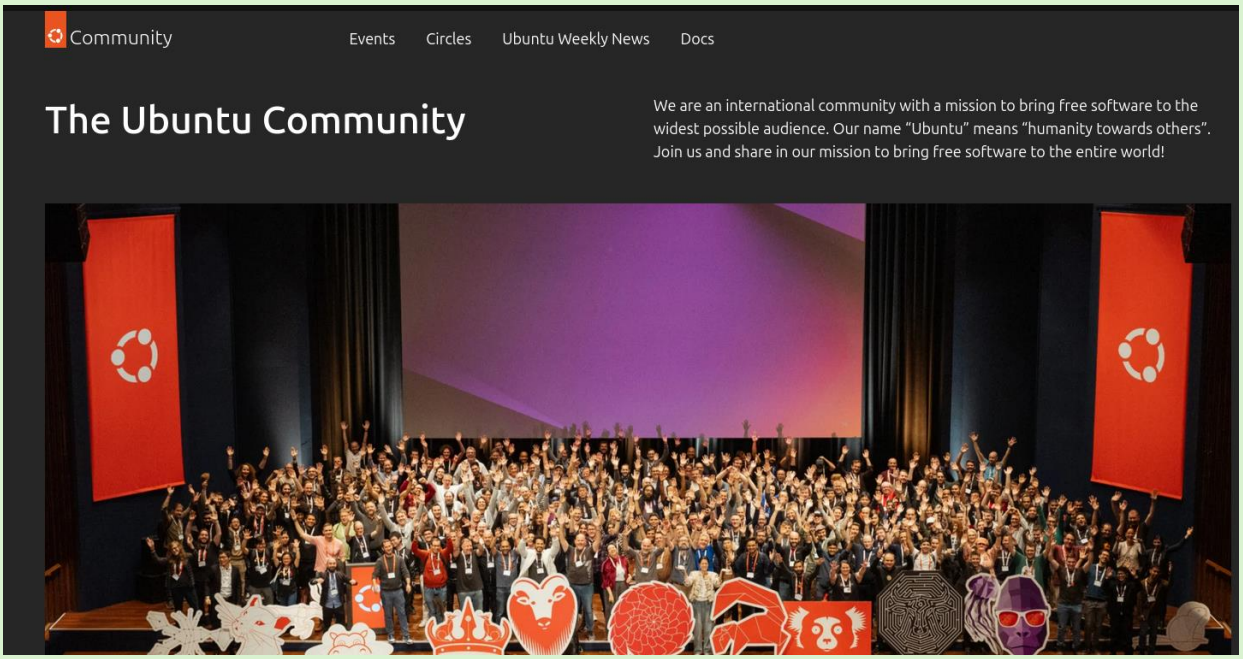
8.2)Porta 80



In questa porta,Nessus ha riscontrato una versione datata e **non più in manutenzione** da parte del provider Canonical(***Security End of Life(SEoL)***).

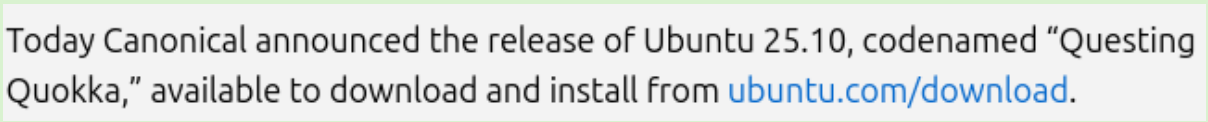
La soluzione è quella di aggiornare la versione di Canonical Ubuntu Linux ad una supportata e recente.

Per approfondire la vulnerabilità si accede al ***link*** sottostante alla soluzione che porta ad una pagina Web della ***community di Ubuntu*** .

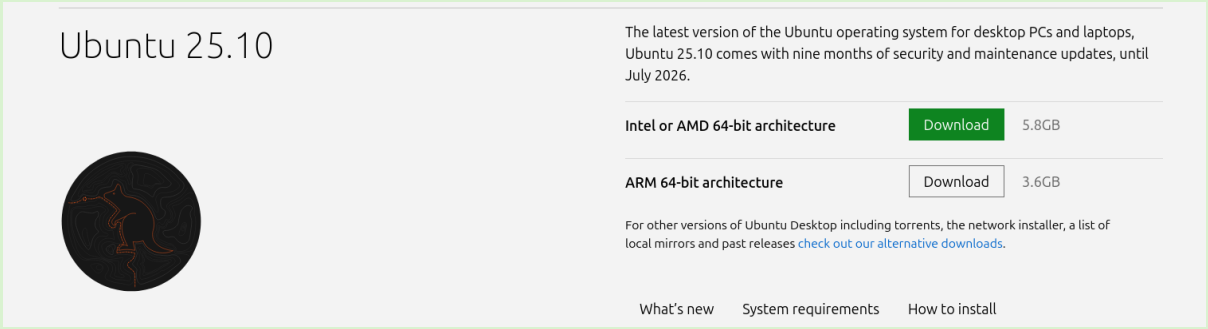


*Sito web Ubuntu Community accessibile dal link

*Notizia sul rilascio versione aggiornata di Canonical Ubuntu Linux



*Link download versione 25.10 nominata come Questing Quokka

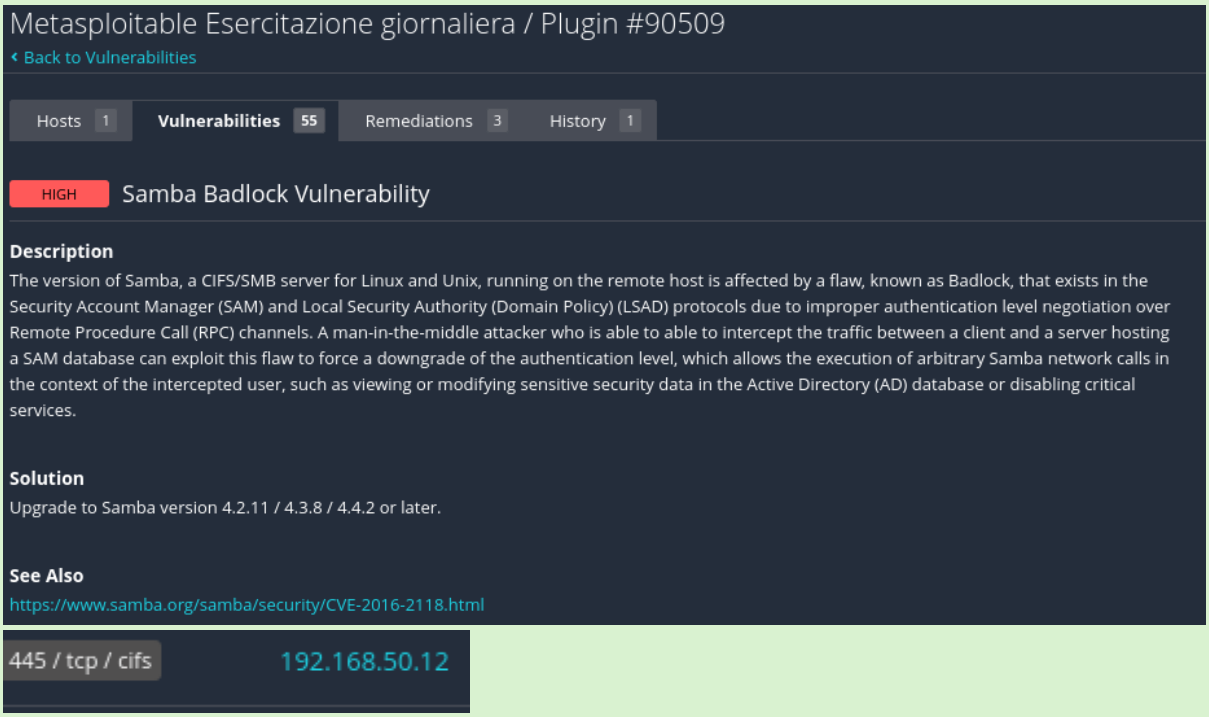


*Download Questing Quokka

Dalla sito web community di Ubuntu,è possibile ricercare notizie,patch etc.

In questo caso si è arrivati alla notizia del rilascio della versione recente (Questing Quokka) con download annesso.

8.3)Porta 445



In questo caso,Nessus ha individuato una versione di Samba (software che gestisce il protocollo SMB e CIFS) obsoleta e questo rende la Metasploitable esposta al Man In The Middle.

La soluzione è di aggiornarla alla versione più recente attraverso il link che porta ad una pagina Web dove fornisce ulteriori informazioni al riguardo con un collegamento alla pagina per le patch.

```
The Security Account Manager Remote Protocol [MS-SAMR] and the
Local Security Authority (Domain Policy) Remote Protocol [MS-LSAD]
are both vulnerable to man in the middle attacks. Both are application level
protocols based on the generic DCE 1.1 Remote Procedure Call (DCERPC) protocol.
```

**Vulnerabilità Samba*

```
A patch addressing this defect has been posted to

  https://www.samba.org/samba/security/
```

**Collegamento ipertestuale alla pagina web delle patches.*

Samba Security Releases

Security releases for Samba are listed below by their release date. The previously affected versions of Samba are listed alongside the appropriate security concern. For complete information, follow the link to full release notes for each release.

Samba's coordinated security release and disclosure process is followed and new versions of Samba are released for supported Samba versions.

A list of public Samba Security Bugs is available. Some minor issues will only be listed in The Samba Bugzilla and not here, if they did not result in a security release

Samba Security Releases

Date Issued	*Download*	*Known Issue(s)*	*Affected Releases*	*CVE ID #*	*Details*
15 October 2025	patch for Samba 4.23.2 patch for Samba 4.22.5 patch for Samba 4.21.9	CVE-2025-10230 and CVE-2025-9640. Please see announcements for details.	Please refer to the advisories.	CVE-2025-10230, CVE-2025-9640.	Announcement, Announcement
10 October 2023	patch for Samba 4.19.1 patch for Samba 4.18.8 patch for Samba 4.17.12	CVE-2023-3961, CVE-2023-4091, CVE-2023-4154, CVE-2023-42669, and CVE-2023-42670. Please see announcements for details.	Please refer to the advisories.	CVE-2023-3961, CVE-2023-4154, CVE-2023-4091, CVE-2023-42669, CVE-2023-42670.	Announcement, Announcement, Announcement, Announcement, Announcement

**Pagina download versioni Samba*

9)CONCLUSIONI

L'attività di analisi effettuata tramite Nessus ha permesso di mappare con precisione il livello di sicurezza della macchina Target, evidenziando criticità legate a sistemi obsoleti e non aggiornati.

Lo strumento si è dimostrato fondamentale non solo nell'individuazione dei rischi, ma anche nel fornire una roadmap chiara per la soluzione. Grazie ai link di approfondimento è possibile ridurre la superficie di attacco e proteggendo l'integrità dei dati del sistema.