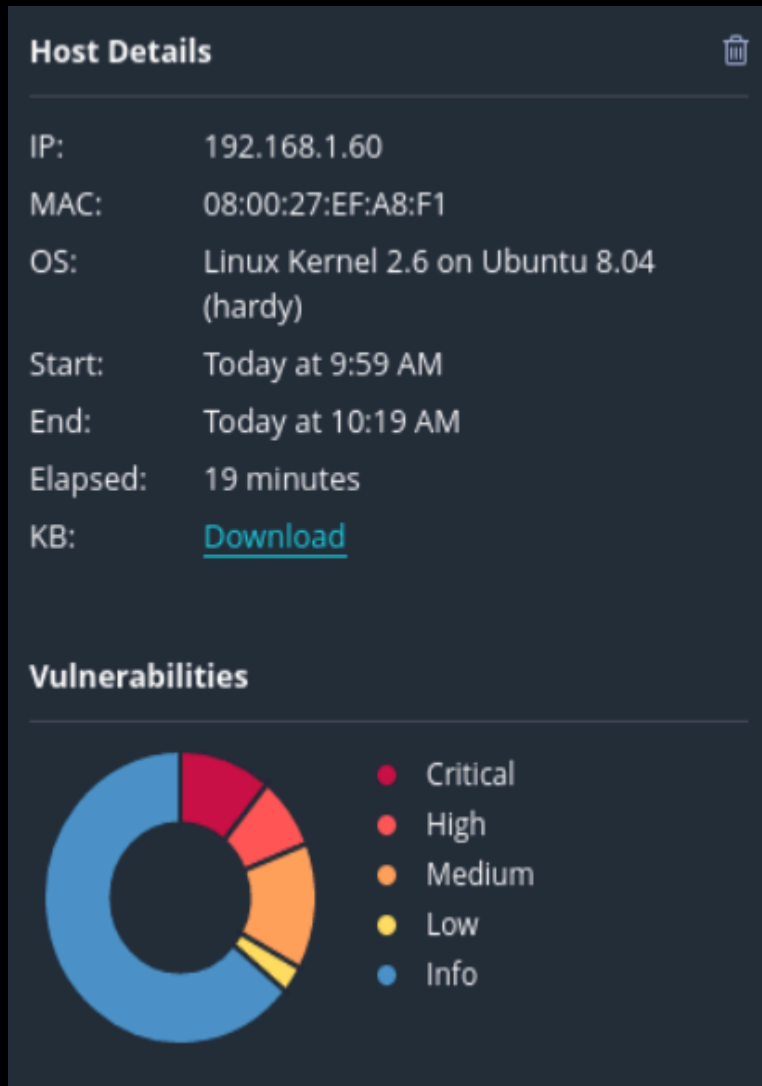


Nessus vulnerability scan

Target: Metasploitable

Risultato scansione



Analizziamo come richiesto 3 vulnerabilità, 2 critiche e 1 media.

Livello Critico

UnrealIRCd Backdoor Detection

Descrizione della Vulnerabilità

- **Natura:** Questa vulnerabilità è dovuta a una backdoor inserita nel codice sorgente del software. Fu scoperta che alcune versioni di UnrealIRCd erano distribuite con una backdoor, consentendo l'esecuzione di comandi arbitrari da parte di un attaccante remoto.
- **Versioni Interessate:** Generalmente, le versioni compromesse di UnrealIRCd sono quelle tra il 2009 e il 2010. È importante verificare la versione specifica per confermare la vulnerabilità.

Soluzione: Aggiornare all'ultima versione di UnrealIRCd che non contiene la backdoor.

Livello critico

SSL Version 2 and 3 Protocol Detection

Descrizione della Vulnerabilità

- **SSLv2 e SSLv3:** Sono versioni precedenti del protocollo SSL (Secure Sockets Layer), utilizzato per criptare il traffico su internet. Sono noti per avere diverse vulnerabilità, come "POODLE" (Padding Oracle On Downgraded Legacy Encryption) per SSLv3, che possono essere sfruttate per attacchi di man-in-the-middle.
- **Rischi:** L'uso di questi protocolli obsoleti espone le comunicazioni a rischi di intercettazione e decodifica da parte di malintenzionati.

Soluzione: Disabilitare SSLv2 e SSLv3 sui server e sui client. Installare la sua versione aggiornata "TLS" 1.2 o 1.3

Livello medio

Unencrypted Telnet Server

Descrizione della Vulnerabilità

- **Telnet:** È un protocollo di rete utilizzato per fornire comunicazione testuale bidirezionale. Una delle principali carenze di Telnet è che trasmette tutti i dati, comprese le credenziali di accesso, in chiaro, senza alcuna forma di crittografia.
- **Rischi:** Qualsiasi malintenzionato che abbia accesso alla rete può facilmente intercettare queste comunicazioni e ottenere informazioni sensibili, come username e password.

Soluzione: Sostituire Telnet con SSH (Secure Shell), che offre funzionalità simili ma con la comunicazione criptata.