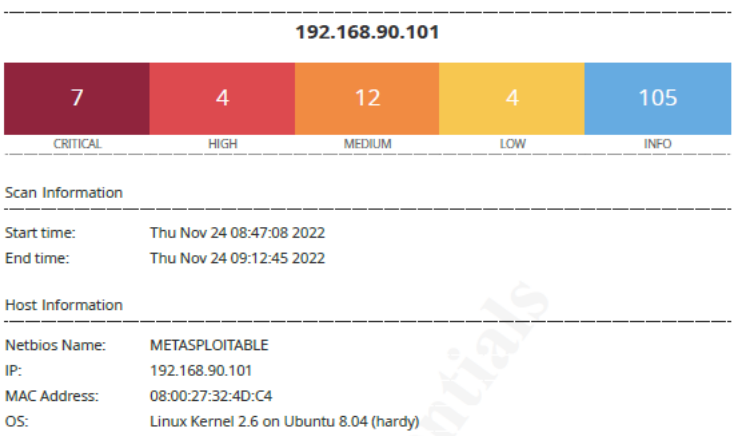
Scan meta

Report generated by Nessus™ Thu, 24 Nov 2022 09:12:45 EST

Scansione Iniziale



Adesso analizziamo le seguenti vulnerabilità:

51988 - Bind Shell Backdoor Detection:

• Descrizione: la shell di meta è in ascolto su una porta senza nessuna autenticazione richiesta. Un attaccante potrebbe connettersi alla porta e potrebbe mandare comandi direttamente alla shell.

• Soluzione: Verificare se meta fosse stato compromesso, reinstallare il sistema se necessario.

• Rischio: **Critico**

• Plugin Output: tcp/1524/wild_shell

11356 - NFS Exported Share Information Disclosure:

• Descrizione: Almeno un NFS può essere approcciato scannerizzando meta. Un attaccante potrebbe essere capace di leggere o scrivere i file di meta.

• Soluzione: Configurare l'NFS in modo che vi possano accedere solo host autorizzati.

• Rischio: **Critico**

• Plugin Output: udp/2049/rpc-nfs

61708 - VNC Server 'password' Password:

• Descrizione: Il server VNC in esecuzione su meta ha una password debole. Nessus è riuscito a fare il login nella VNC usando la password '**password'**. Un attaccante potrebbe usare questa cosa per prendere il controllo del sistema.

• Soluzione: Rendere più sicuro il servizio VNC con una password più sicura.

• Rischio: **Critico**

• Plugin Output: tcp/5900/vnc