ANALISI REPORT

192.168.50.101

7	5	21	5	121
CRITICAL	HIGH	MEDIUM	LOW	INFO

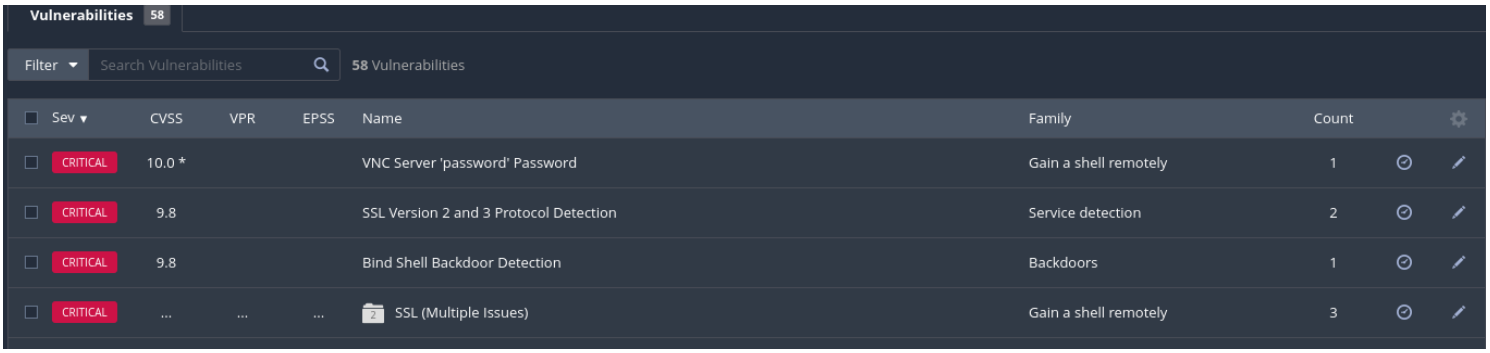
Scan Information

Start time:	Wed Dec 4 08:09:11 2024
End time:	Wed Dec 4 08:35:14 2024

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.101
MAC Address:	08:00:27:60:1E:3E
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

CRITICAL:



1.

Vulnerabilities

51988 - Bind Shell Backdoor Detection

Plugin Output

tcp/1524/wild_shell

Analizzando verifichiamo che è stata trovata una Bind shell attiva sulla porta 1524 senza che sia richiesta alcuna autenticazione. Una Bind Shell è un tipo di backdoor che apre una connessione in ascolto su una porta specifica del sistema compromesso. Quando un attaccante si collega a quella porta, può inviare comandi al sistema come se fosse un utente locale, senza autenticazione.

2.

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Plugin Output

Tcp/22/ssh

Analizzando verifichiamo che sulla porta 22 le chiavi SSH e SSL generate su sistemi affetti sono deboli e prevedibili, consentendo a un attaccante di:

1. Ricostruire le chiavi private partendo dalle chiavi pubbliche.
2. Compromettere la crittografia delle sessioni SSH, SSL/TLS, e VPN.
3. Condurre attacchi MITM (Man-In-The-Middle) o decrittare sessioni crittografate.

3. e 4.

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Plugin Output

Tcp/25/smtp

Analizzando verifichiamo che questa vulnerabilità riguarda certificati x509 SSL (utilizzati in connessioni HTTPS, SMTPS, etc.) generati su sistemi Debian o Ubuntu affetti dal bug nell'algoritmo RNG (Random Number Generator) di OpenSSL. Come nella vulnerabilità precedente, il problema è dovuto a una modifica errata da parte di Debian, che ha ridotto significativamente la casualità nella generazione di numeri casuali.

- Le chiavi SSL generate sono deboli e prevedibili.
- Un attaccante può calcolare facilmente la chiave privata partendo dalla chiave pubblica, compromettendo la sicurezza della crittografia.
- Può condurre attacchi Man-In-The-Middle (MITM) e decifrare il traffico crittografato

Plugin Output

Tcp/5432/postgresql

Questa vulnerabilità segnala che un certificato x509 SSL associato al servizio su porta 5432 (PostgreSQL) è stato generato su un sistema Debian o Ubuntu affetto dal noto problema dell'algoritmo RNG (Random Number Generator) di OpenSSL.

5. 6.

20007 - SSL Version 2 and 3 Protocol Detection

Plugin Output

Tcp/25/smtp

Plugin Output

Tcp/5432/postgresql

In questo caso, il servizio remoto accetta connessioni crittografate tramite SSL 2.0 e/o SSL 3.0 per i servizi SMTP (porta 25) e PostgreSQL (porta 5432) . Sia SSL 2.0 che 3.0 sono obsoleti e vulnerabili a diversi difetti crittografici, rendendo le comunicazioni crittografate suscettibili di attacchi.

7.

61708 - VNC Server 'password' Password

Plugin Output

Tcp/5900/vnc

Il server VNC (Virtual Network Computing) in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questo per prendere il controllo del sistema.