Report scan su Metasploitable 2 W12D1

Vulnerabilità critiche

Totale vulnerabilità critiche trovate sull'host con IP 192.168.32.101: 8

1. VNC Server 'password' Password

- **Porta coinvolta:** 5900
- **Sinossi:** Server VNC ha una password debole
- **Descrizione vulnerabilità:** Il server VNC in esecuzione su host remoto ha una password debole. Nessus ha potuto eseguire il login usando l'autenticazione VNC e la password "password". Un attaccante remoto privo di autenticazione potrebbe usare questo metodo per prendere il controllo del sistema.
- **Remediation:** Cambiare la password con una più forte ed eseguire un password reset periodico.

2. Apache Tomcat AJP Connector Request Injection (Ghostcat)

- **Porta coinvolta:** 8009
- **Sinossi:** Trovato un connettore AJP vulnerabile in ascolto sull'host remoto
- **Descrizione vulnerabilità:** Una vulnerabilità lettura/inclusione sui file è stata trovata in un connettore AJP. Un attaccante remoto privo di autenticazione potrebbe sfruttare questa vulnerabilità per leggere file delle web applications da un server remoto vulnerabile. Nel caso in cui il server vulnerabile permetta il caricamento di file, un attaccante potrebbe caricare del codice malevolo JSP incluso in vari file e permettere così l'esecuzione remota del codice (RCE).
- **Remediation:** Aggiornare la configurazione AJP in modo che richieda l'autorizzazione oppure aggiornare il server Tomcat alle versioni 7.0.100, 8.5.51, 9.0.31 o successive.

3. SSL Version 2 and 3 Protocol Detection

- **Porta coinvolta:** 25, 5432
- **Sinossi:** Il servizio remoto cripta il traffico usando un protocollo con vulnerabilità note.
- **Descrizione vulnerabilità:** Il servizio remoto accetta connessioni criptate usando SSL 2.0 e/o SSL 3.0.
  Queste versioni di SSL sonno affette da diversi difetti crittografici, tra cui: un schema di riempimento non sicuro con cifrari CBC, schemi non sicuri di negoziazione e ripresa della sessione.
  Un attaccante potrebbe sfruttare queste vulnerabilità per eseguire attacchi man in the middle o per decifrare comunicazioni tra il servizio e i client.
  Anche se SSL/TLS hanno un meccanismo sicuro per scegliere la versione più recente supportata del protocollo (così che queste versioni vengano usate solo se il client o il server non supportano versioni più recenti), molti browser lo implementano in modo non sicuro, ciò permette ad un attaccante di eseguire un downgrade della connessione (come con POODLE).
  Si raccomanda quindi di disabilitare completamente questi protocolli.
  Il NIST ha determinato che SSL 3.0 non è più accettabile per comunicazioni sicure. A partire dall'entrata in vigore stabilita nel PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di crittografia forte del PCI SSC.
- **Remediation:** Consultare la documentazione dell'applicazione per disattivare SSL 2.0 e 3.0.
  Usare TLS 1.2 (con le approvate suite di cifratura) o versioni più recenti.

4. Bind Shell Backdoor Detection

- **Porta coinvolta:** 1524
- **Sinossi:** L'host remoto potrebbe essere stato compromesso.
- **Descrizione vulnerabilità:** Rilevata una shell in ascolto sulla porta remota senza nessun tipo di autenticazione richiesta.
  Un attacante potrebbe sfruttare la shell per connettersi alla porta remota ed eseguire direttamente comandi.
- **Remediation:** Verificare se l'host remoto è stato compromesso e reinstallare il sistema operativo se necessario.

5. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

- **Porta coinvolta:** 22
- **Sinossi:** Le chiavi host per l'SSH remoto sono deboli.
- **Descrizione vulnerabilità:** La chiave host per l'SSH remoto è stata generata da un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della libreria OpenSSL.
  Il problema è dovuto ad un packager Debian che ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.
  Un attaccante potrebbe facilmente ottenere la parte privata della chiave remota ed usarla per decifrare la sessione remota o avviare un attacco man in the middle.
- **Remediation:** Considerare come potenzialmente indovinabile tutto il materiale crittografico generato sull'host remoto.
  In particolare tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

6. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

- **Porta coinvolta:** 25, 5432
- **Sinossi:** Il cerfificato remoto SSL utilizza una chiave debole.
- **Descrizione vulnerabilità:** Il certificato remoto x509 per il server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.
  Il problema è dovuto ad un packager Debian che ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.
  Un attaccante potrebbe facilmente ottenere la parte privata della chiave remota ed usarla per decifrare la sessione remota o avviare un attacco man in the middle.
- **Remediation:** Considerare come potenzialmente indovinabile tutto il materiale crittografico generato sull'host remoto.
  In particolare tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

Facoltativo

Vulnerability assessment eseguito sulla VM di Metasploitable 2

Sommario

Informazioni generali sulla scansione:

- Rischio complessivo: critical
- Data e ora inizio scansione: Mer 14 Maggio 2025, 08:19:28
- Data e ora fine scansione: Mer 14 Maggio 2025, 08:46:37

Informazioni sull’host:

- Netbios name: METASPLOITABLE
- IP: 192.168.32.101
- MAC address: 08:00:27:EF:F5:CA
- OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardly)

Vulnerabilità trovate

Critical	High	Medium	Low	Info
8	4	23	8	121

Grafico a torta