Report di Sicurezza - Metasploitable2

Data della scansione: 26 Febbraio 2025 **Strumento di analisi:**Nessus **Host Analizzato:** 192.168.40.101 **Sistema Operativo:** Linux Kernel 2.6 su Ubuntu 8.04 (Hardy)

---

1. Riepilogo delle Vulnerabilità

Gravità	Numero Vulnerabilità
Critico	8
Alto	8
Medio	19
Basso	8
Informativo	119

---

2. Vulnerabilità Critiche

2.1 Apache Tomcat AJP Connector Request Injection (Ghostcat)

- **Descrizione:** Un attaccante remoto può sfruttare un connettore AJP vulnerabile per leggere file delle applicazioni web e, in alcuni casi, eseguire codice remoto (RCE).
- **Soluzione:** Aggiornare Apache Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successiva.
- **CVSS v3 Score:** 9.8 (Critico)
- **Riferimenti:** CVE-2020-1745

2.2 Bind Shell Backdoor Detection

- **Descrizione:** Un servizio shell remoto è in ascolto su una porta senza autenticazione, indicando una possibile compromissione del sistema.
- **Soluzione:** Verificare l'integrità del sistema e, se necessario, reinstallare l'OS.
- **CVSS v3 Score:** 9.8 (Critico)

2.3 Debian OpenSSH/OpenSSL Weak RNG

- **Descrizione:** La chiave SSH generata su questo sistema è prevedibile a causa di una vulnerabilità nell'implementazione Debian di OpenSSL.
- **Soluzione:** Rigenerare tutte le chiavi SSH, SSL e OpenVPN.
- **CVSS v3 Score:** 10.0 (Critico)

- **Riferimenti:** CVE-2008-0166

2.4 SSL Version 2 e 3 Protocol Detection

- **Descrizione:** Il sistema supporta SSL 2.0 e 3.0, protocolli deboli che possono essere sfruttati in attacchi Man-in-the-Middle (Poisoned Poodle).
- **Soluzione:** Disabilitare SSLv2 e SSLv3, utilizzare TLS 1.2 o superiore.
- **CVSS v3 Score:** 9.8 (Critico)

2.5 VNC Server con password debole

- **Descrizione:** Il servizio VNC accetta la password "password", permettendo l'accesso non autenticato.
- **Soluzione:** Impostare una password sicura per il servizio VNC.
- **CVSS v3 Score:** 10.0 (Critico)

2.6 Samba Badlock Vulnerability

- **Descrizione:** Samba è vulnerabile a un attacco Man-in-the-Middle (Badlock) che consente a un attaccante di modificare dati sensibili su Active Directory.
- **Soluzione:** Aggiornare Samba alla versione 4.2.11 o successiva.
- **CVSS v3 Score:** 7.5 (Alto)
- **Riferimenti:** CVE-2016-2118

2.7 NFS Shares senza restrizioni di accesso

- **Descrizione:** Il server NFS esporta condivisioni accessibili globalmente senza restrizioni.
- **Soluzione:** Applicare restrizioni di accesso alle condivisioni NFS.
- **CVSS v3 Score:** 7.5 (Alto)

---

3. Raccomandazioni Generali

1. **Aggiornare il sistema operativo**: Ubuntu 8.04 è obsoleto e non più supportato.
2. **Applicare le patch di sicurezza** per i servizi vulnerabili (Apache, SSH, Samba, NFS, VNC, OpenSSL).
3. **Disabilitare protocolli insicuri** come SSLv2, SSLv3 e RC4.
4. **Rinforzare le policy di accesso** per NFS, SMB e VNC con autenticazione forte.
5. **Monitorare il traffico di rete** per rilevare accessi sospetti.

---

4. Conclusione

L'host analizzato presenta diverse vulnerabilità critiche che possono essere sfruttate per ottenere accesso non autorizzato e compromettere la sicurezza della rete. Si consiglia un aggiornamento immediato del sistema e la messa in sicurezza dei servizi esposti per minimizzare i rischi identificati.
