Nell'esercitazione di oggi andremo ad effettuare una scansione tramite Nessus alla macchina Metasploitable per raccogliere informazioni sulle varie vulnerabilità.

Dalla scansione è risultato un totale di 10 vulnerabilità critiche, 7 di livello alto e 23 medie.

Sotto elencate ci sono le 10 più critiche tra cui anche una backdoor che semplicemente dal terminale di kali utilizzando il comando nc 192.168.1.17 1524 riusciamo ad avere accesso al root di metasploitable.

1. Apache Tomcat AJP Connector Request Injection (Ghostcat) – CVE-2020-1938
Una vulnerabilità in Tomcat consente la lettura di file tramite il connettore AJP. Se il server consente l'upload di file, un attaccante può ottenere l'esecuzione remota di codice caricando JSP malevoli. È sfruttabile da remoto senza autenticazione.
Gravità: Alta – CVSS 9.8

Soluzione: Aggiorna Tomcat a ≥ 7.0.100 / 8.5.51 / 9.0.31 e limita l'accesso al connettore AJP.
RedHat CVE-2020-1938 https://access.redhat.com/security/cve/CVE-2020-1745
Soluzione RedHat https://access.redhat.com/solutions/4851251

---

2. Bind Shell Backdoor Detection
Un backdoor è attivo sulla porta TCP 1524: accetta comandi senza autenticazione. È possibile che il sistema sia compromesso e usato per l'esecuzione remota di comandi come utente root.
Gravità: Critica – CVSS 10.0

Soluzione: Verifica compromissione e reinstalla il sistema da una sorgente affidabile.
NVD - CVE Entry http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-05020A%F0%9F%94%97-,NVD%20%2D%20CVE%20Entry,-(generico)

---

3. Canonical Ubuntu Linux 8.04 – End of Life
Il sistema operativo è fuori supporto dal 2013. Non riceve più patch di sicurezza, rendendo il sistema altamente vulnerabile a nuovi exploit.
Gravità: Critica – CVSS 10.0

Soluzione: Esegui upgrade a una versione LTS attualmente supportata, come Ubuntu 22.04.
Ubuntu Lifecycle https://wiki.ubuntu.com/Releases

---

4. Debian OpenSSL RNG Vulnerability – CVE-2008-0166

Un difetto nel generatore di numeri casuali in Debian causa chiavi SSH/SSL deboli e prevedibili. Attaccanti possono decifrare comunicazioni cifrate o impersonare host legittimi.

Gravità: Critica – CVSS 10.0

Soluzione: Rigenera tutte le chiavi crittografiche con una versione aggiornata di OpenSSL.

Debian Advisory

---

5. SSLv2/SSLv3 Enabled – POODLE & Protocol Flaws

Il sistema accetta protocolli SSL obsoleti (2.0 e 3.0), vulnerabili a downgrade e man-in-the-middle. Questi protocolli dovrebbero essere disabilitati in favore di TLS 1.2+.

Gravità: Critica – CVSS 9.8

Soluzione: Disabilita SSLv2/SSLv3 e usa TLS 1.2+ con cifrari sicuri.

RFC 7568 – Deprecation of SSLv3 https://tools.ietf.org/html/rfc7568

POODLE paper https://www.openssl.org/~bodo/ssl-poodle.pdf

---

6. UnrealIRCd Backdoor – CVE-2010-2075

Una versione compromessa di UnrealIRCd permette l'esecuzione remota di codice via porta 6667. È un malware noto incluso in copie modificate del software.

Gravità: Critica – CVSS 10.0

Soluzione: Scarica e reinstalla UnrealIRCd da fonte verificata con controllo checksum.

UnrealIRCd Advisory

---

7. VNC con password debole ("password")

Il server VNC utilizza una password debole e prevedibile. Un attaccante remoto può accedere facilmente al desktop remoto e prendere il controllo del sistema.

Gravità: Critica – CVSS 10.0

Soluzione: Configura una password robusta per il server VNC.

NIST VNC Guidance *(generico) https://nvd.nist.gov/vuln/detail/CVE-1999-0502*

---

8. ISC BIND – Reflected DoS / Service Downgrade – CVE-2020-8616

Una vulnerabilità in BIND permette a un attaccante remoto di sfruttare il DNS per causare un degrado del servizio o riflessione DoS, consumando risorse del server.

Gravità: Media – CVSS 8.6

Soluzione: Aggiorna BIND a versione ≥ 9.11.19.

ISC Advisory https://kb.isc.org/docs/cve-2020-8616

---

9. NFS con condivisioni world-readable

Condivisioni NFS sono accessibili da qualsiasi host, senza restrizioni. Questo espone potenzialmente file sensibili a letture non autorizzate.

Gravità: Media – CVSS 7.5

Soluzione: Limita l'accesso ai client autorizzati (IP o hostname) nel file /etc/exports.

NFS Security Best Practices http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

---

10. Samba Badlock Vulnerability – CVE-2016-2118

Un attacco man-in-the-middle può forzare un downgrade nell'autenticazione e invocare chiamate SMB con privilegi elevati, come modificare dati su Active Directory.

Gravità: Media – CVSS 7.5

Soluzione: Aggiorna Samba a ≥ 4.2.11 / 4.3.8 / 4.4.2.

Badlock.org http://badlock.org/

Samba Advisory https://www.samba.org/samba/security/CVE-2016-2118.html