

Nessus

Nell'esercizio di oggi viene richiesto di fare una scansione delle vulnerabilità con il tool Nessus sulla macchina Meta e analizzarne le vulnerabilità.

CRITICAL

1. Canonical Ubuntu Linux 8.04.x – End of Life (EOL)

Descrizione:

Il sistema operativo non è più supportato dal vendor. Non riceve patch di sicurezza dal 2013.

Rischio:

Qualsiasi vulnerabilità nota negli ultimi 10+ anni è sfruttabile senza mitigazioni.

Soluzione:

Aggiornare a una versione supportata di Ubuntu (\geq 22.04 LTS).

2. VNC Server – Password “password” (Default Credential)

Descrizione:

Il servizio VNC utilizza credenziali predefinite.

Rischio:

Accesso remoto non autorizzato con privilegi dell'utente configurato.

Soluzione:

- Cambiare immediatamente password.
- Limitare VNC a utenti autorizzati.
- Abilitare cifratura (VNC over SSH).

3. Apache Tomcat AJP Connector Request Injection (Ghostcat – CVE-2020-1938)

Descrizione:

Il connettore AJP permette a un attaccante di leggere file sensibili o eseguire richieste non autorizzate.

Rischio:

Accesso remoto a file del server o esecuzione di codice arbitrario.

Soluzione:

- Disabilitare il connettore AJP se non necessario.
- Aggiornare Tomcat \geq 7.0.100, 8.5.51 o 9.0.31.

4. SSL Version 2 e Version 3 Abilitati (Protocol Obsolete)

Descrizione:

Il server accetta connessioni SSLv2/SSLv3, protocolli insicuri soggetti ad attacchi (POODLE, DROWN).

Rischio:

Decifrabilità del traffico HTTPS.

Soluzione:

- Disabilitare SSLv2/SSLv3.
- Abilitare solo TLS 1.2/1.3.

5. Bind Shell Backdoor Detection

Descrizione:

Rischio:

Comando remoto non autenticato.

Soluzione:

È presente un servizio di backdoor che apre una shell in ascolto su una porta fissa.
Rimuovere il servizio, reinstallare il sistema o isolarlo (VM da laboratorio).

6. SSL – Multiple Issues

Descrizione:

Weak cipher suite, protocolli deprecati, mancanza di Forward Secrecy.

Rischio:

Intercettazione e decifratura del traffico TLS.

Soluzione:

Aggiornare configurazione TLS, disabilitare cipher deboli (RC4, 3DES, null, anonymous).

HIGH

7. Samba Badlock Vulnerability (CVE-2016-2118)

Descrizione:

Vulnerabilità nel protocollo DCE/RPC su Samba.

Rischio:

Man-in-the-middle, esecuzione di codice o accesso non autorizzato.

Soluzione:

Aggiornare Samba all'ultima versione.

8. NFS Shares World-Readable

Descrizione:

Condivisioni NFS accessibili senza autenticazione.

Rischio:

Accesso non autorizzato a file sensibili.

Soluzione:

- Limitare l'accesso tramite /etc(exports).
- Usare root_squash.
- Abilitare autenticazione Kerberos (se necessario).

MIXED / MULTIPLE ISSUES

9. SSH – Weak Algorithms Enabled

Descrizione:

Sono presenti cipher obsoleti (es. CBC, MD5, DSA).

Rischio:

Debolezza nella confidenzialità o integrità della connessione SSH.

Soluzione:

Aggiornare sshd_config per consentire solo:

- aes256-gcm, chacha20-poly1305, MAC SHA2.

10. HTTP – Obsolete/Weak Configuration

Descrizione:

Header mancanti (X-Frame-Options, XSS-Protection), vecchie versioni, directory listing non protetto.

Rischio:

Esposizione informazioni, attacchi MITM, XSS.

Soluzione:

Aggiornare il web server e applicare best practice di hardening.

11. SMB – Multiple Issues (SMBv1 enabled)

Descrizione:

SMBv1 è attivo (protocollo vulnerabile a EternalBlue + altri).

Rischio:

Remote code execution, compromise completa del sistema.

Soluzione:

Raul Pastor

Disabilitare SMBv1, usare SMBv2/3.

12. TLS – Multiple Issues

Descrizione: Raul Pastor

Cifrari deboli, protocolli obsoleti, mancanza di protezione contro downgrade.

Soluzione:

Applicare hardening TLS e aggiornare OpenSSL.

13. ISC Bind – Multiple Issues

Descrizione:

Il DNS server contiene versioni vulnerabili e configurazioni insicure.

Rischio:

DNS spoofing, DoS, cache poisoning.

Soluzione:

Aggiornare Bind e configurare controllo accessi.

MEDIUM

14. TLS 1.0 Protocol Detection

Descrizione:

TLS1.0 è obsoleto.

Rischio:

Debolezze crittografiche note.

Soluzione:

Supportare solo TLS 1.2/1.3.

15. SSL Anonymous Cipher Suites Supported

Descrizione:

Cifrari senza autenticazione del server.

Rischio:

MITM totale.

Soluzione:

Disabilitare cipher suite anonime (aNULL).

16. SSL DROWN Attack Vulnerability

Descrizione:

Il server permette connessioni con protocolli compatibili con SSLv2.

Soluzione:

Disabilitare SSLv2, aggiornare OpenSSL.

LOW

17. X Server Detection

Descrizione:

È presente un server X esposto.

Rischio:

Accesso remoto al display o keylogging.

Soluzione:

Disabilitare accesso esterno, usare SSH con forwarding controllato.

18. ICMP Timestamp Disclosure

Descrizione:

Risponde a timestamp ICMP.

Rischio:

Informazioni sul clock per attacchi di fingerprinting.

Soluzione:

Filtrare ICMP timestamp nel firewall.