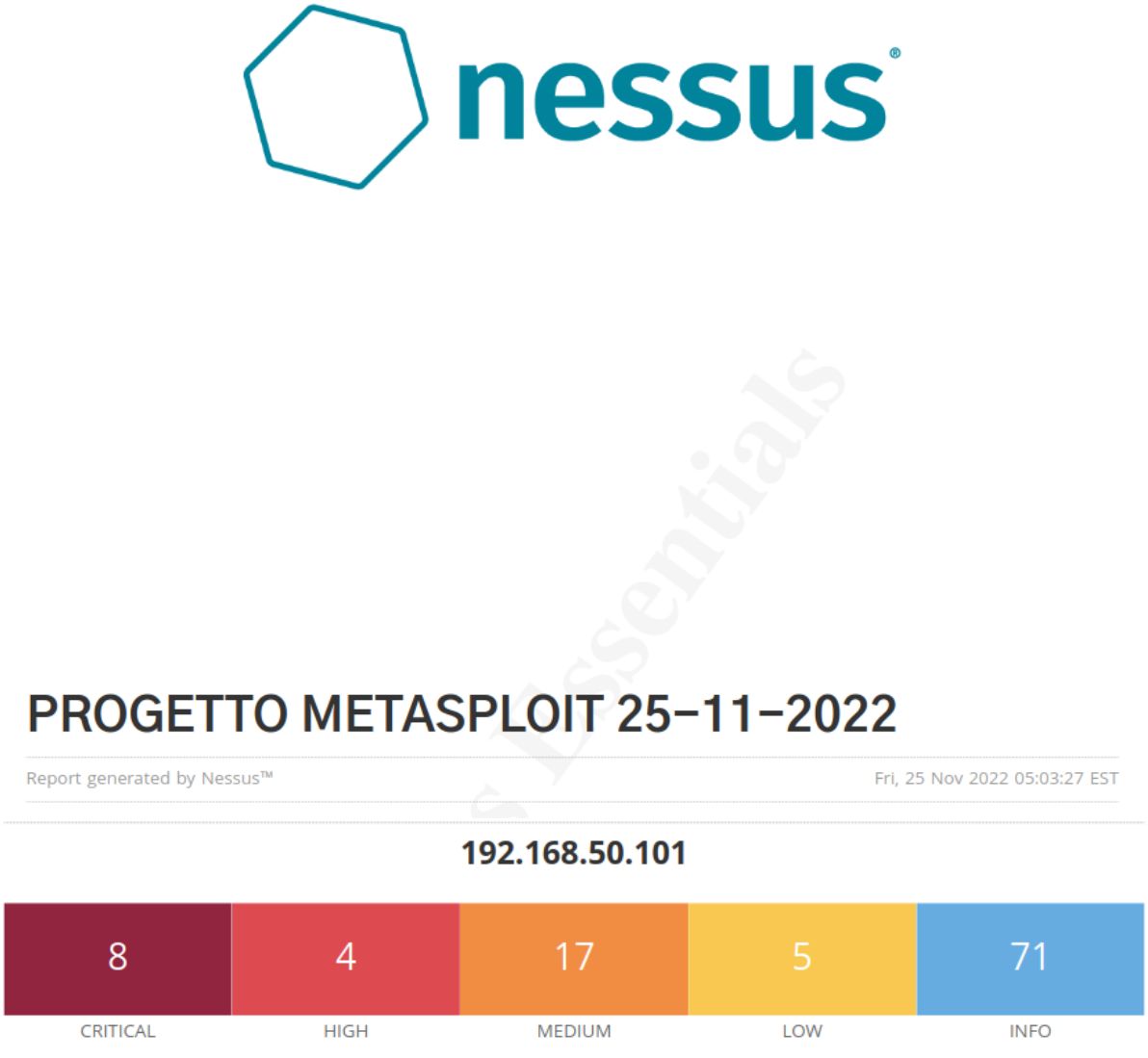
CUORE ANDREA

25-11-2022

VULNERABILITY ASSESSMENT:

	HOST	IP HOST	OS HOST
NESSUS	METASPLOIT	192.168.50.101	KALI LINUX



VULNERABILITA' RISCONTRATE:

Vulnerabilities Total: 105

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	61708	VNC Server 'password' Password
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	42256	NFS Shares World Readable
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	90509	Samba Badlock Vulnerability
MEDIUM	6.8	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

- NFS SHARES WORLD READABLE
  - Porta: 2049 TCP
  - Descrizione: Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base al nome dell'host, all'IP o all'intervallo IP).
  - Soluzione: Inserire le restrizioni appropriate su tutte le condivisioni NFS.

- VNC SERVER “PASSWORD” PASSWORD
  - **Porta:** 5900 TCP
  - **Descrizione:** Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di effettuare il login utilizzando l'autenticazione VNC e una password

di 'password'. Un aggressore remoto non autenticato potrebbe sfruttare questa situazione per prendere il controllo del sistema.
    - **Soluzione:** Proteggere il servizio VNC con una password forte.
    - **Fattore di rischio:** Critico

- BIND SHELL BACKDOOR DETECTION
    - **Porta:** 1524 TCP
    - **Descrizione:** Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla collegandosi alla porta remota e inviando direttamente i comandi.
    - **Soluzione:** Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.
    - **Fattore di rischio:** Critico

- NFS EXPORTED SHARE INFORMATION DISCLOSURE
    - **Porta:** 2049 UDP
    - **Descrizione:** Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttarla per leggere (ed eventualmente scrivere) i file sull'host remoto
    - **Soluzione:** Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.
    - **Fattore di rischio:** Critico