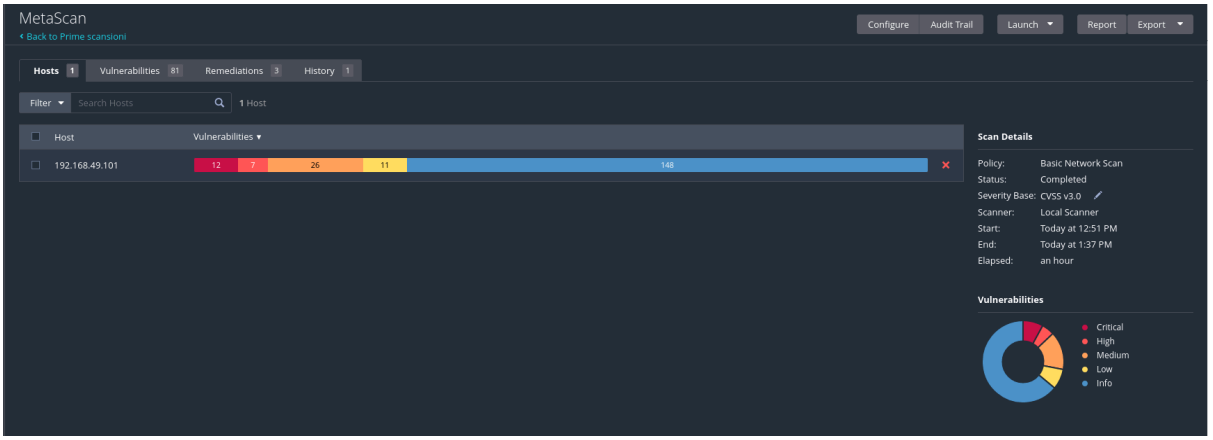
Esercizio 22-02-24

Nell'ambito della sicurezza informatica **Nessus** è un software di tipo client-server di scansione delle vulnerabilità. Costituito da **nessusd** - il demone - che effettua la scansione, e da nessus - il client - che fornisce all'utente i risultati della scansione, tramite lo scan e l'abilitazione di plugin appositamente configurabili a seconda della tipologia di host e vulnerabilità che si andrà ad analizzare, rileva le vulnerabilità presenti suggerendo le possibili soluzioni attraverso dei report di analisi in vari formati. Tuttora Nessus con le sue tante opzioni per la scansione, la possibilità di scrivere plugin e per il tipo di reportistica prodotta rimane uno dei migliori strumenti per la vulnerability assessment.



Vulnerabilities Total: 133

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	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	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	5.9	10205	rlogin Service Detection
HIGH	7.5*	5.9	10245	rsh Service Detection
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted

192.168.49.101

MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	6.1	3.8	10815	Web Server Generic XSS

MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	5.3	2.9	58751	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)
MEDIUM	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	4.5	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking

LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	4.5	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	4.5	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.1	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

192.168.49.101

LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	N/A	-	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	-	26194	Web Server Transmits Cleartext Credentials
LOW	2.6*	-	34850	Web Server Uses Basic Authentication Without HTTPS
LOW	2.6*	-	10407	X Server Detection

Le immagini allegate rappresentano alcune delle vulnerabilità rilevate da Nessus con diversi livelli di criticità: 10 critical, 6 high, 20 medium, 10 low.
Inoltre, questo strumento ci permette anche di visualizzare alcune delle soluzioni possibili per risolvere le criticità rilevate.

Apache Tomcat AJP connector request injection (Ghostcat) ad esempio è una vulnerabilità che permette l'esecuzione di codice remoto in alcune circostanze. Apache Tomcat include il connettore AJP, che è abilitato per impostazione predefinita e ascolta tutti gli indirizzi sulla porta 8009. Questa connessione viene trattata con più fiducia di una connessione come HTTP, consentendo a un utente malintenzionato di sfruttarla per eseguire azioni che non sono destinate a un utente non attendibile. La popolarità di Apache Tomcat rende questa vulnerabilità grave. Più di 1 milione di server attivamente raggiungibili su internet sono in esecuzione Apache Tomcat.

Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password: 'password'. Un attaccante remoto non autenticato potrebbe sfruttare questa vulnerabilità per prendere il controllo del sistema. Una soluzione molto semplice può essere proteggere il servizio con una password più forte e conforme allo standard GDPR.