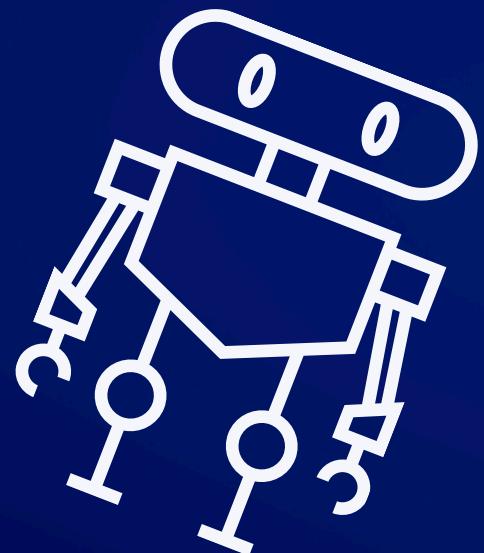
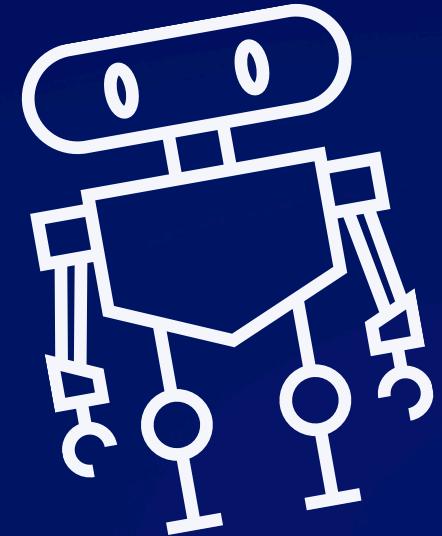




# Vulnerability Assessment

55/L4



Mara Dello Russo



# Cos'è un Vulnerability Assessment?

Una valutazione della vulnerabilità, Vulnerability Assessment, è un processo finalizzato a **identificare, quantificare e classificare** le vulnerabilità nei sistemi informatici, nelle reti, nelle infrastrutture o in altri asset. Questo processo può coinvolgere l'analisi delle vulnerabilità di sicurezza, dei rischi associati e delle possibili conseguenze di un'eventuale sfruttamento delle vulnerabilità. Inoltre, una valutazione delle vulnerabilità può includere raccomandazioni per mitigare o eliminare le vulnerabilità rilevate al fine di migliorare la sicurezza complessiva del sistema o dell'organizzazione. Un Vulnerability Assessment si può eseguire sia localmente che da remoto. Vista la numerosità di servizi noti, testare manualmente i sistemi per cercare le vulnerabilità sarebbe poco praticabile, quindi i penetration tester usano degli strumenti chiamati **Vulnerability Scanner** per automatizzare i test sui target. Nella scansione presentata in questo progetto utilizzeremo Nessus.

# Vulnerabilità

Le vulnerabilità sono catalogate dal SANS Institute attraverso dei codici chiamati CVE (Common Vulnerabilities and Exposures). Es. “Apache Tomcat AJP Connector Request Injection”, o Ghostcat, è identificata come CVE-2020-1938.

Alcune delle principali categorie di vulnerabilità trattate dal SANS Institute includono:

- **Vulnerabilità di software:** possono includere falle di sicurezza e errori di programmazione nei sistemi operativi, nelle applicazioni software e nei servizi di rete.
- **Vulnerabilità di configurazione:** le configurazioni errate o non sicure possono creare punti deboli nei sistemi e nelle reti. Possono includere password deboli, autorizzazioni eccessive, mancata installazione di patch di sicurezza.
- **Vulnerabilità di rete:** riguardano le debolezze nelle infrastrutture di rete, come router, switch, firewall e dispositivi di sicurezza.
- **Vulnerabilità web:** le applicazioni web possono essere vulnerabili a una varietà di minacce, come ad esempio injection di codice (SQL injection, XSS), autenticazione e gestione delle sessioni non sicure, esposizione di dati sensibili e altri problemi che possono compromettere la sicurezza e la privacy degli utenti.
- **Vulnerabilità mobile:** possono includere vulnerabilità di sicurezza nel software delle app, accesso non autorizzato ai dati dell'utente e problemi legati alla gestione remota dei dispositivi

# Nessus

Nessus è uno dei software più noti e utilizzati per la scansione e la valutazione della sicurezza dei sistemi informatici. Si tratta di uno **strumento di analisi delle vulnerabilità** che aiuta ad identificare e mitigare i rischi per la sicurezza nelle reti, nei sistemi e nelle applicazioni.

Nessus è in grado di eseguire scansioni automatiche dei dispositivi connessi in rete per individuare eventuali vulnerabilità note, come falle di sicurezza, configurazioni non sicure e altri problemi che potrebbero essere sfruttati da potenziali aggressori. Il software fornisce anche dettagliate relazioni sulle vulnerabilità rilevate, consentendo agli utenti di comprendere meglio i rischi e prendere misure correttive per migliorare la sicurezza del sistema.

Nessus è formato da:

- un client: viene utilizzato per configurare le scansioni: indicare i target IP, le modalità di scansione ed i test da lanciare.
- un server: si occupa di effettuare i veri e propri test sugli obiettivi specificati all'interno delle scansioni configurate dal client.

Dopo aver eseguito le scansioni il server confronta le risposte con il proprio database di vulnerabilità.

# Report delle vulnerabilità rilevate da Nessus con un Basic Network Scan

192.168.1.101 → IP Metasploitable

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	-	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*	-	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	5.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability
MEDIUM	6.8	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
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
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service

MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
			192.168.1.101	
MEDIUM	5.9	4.4	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	4.4	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
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	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
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	3.9	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)
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	10407	X Server Detection
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	21196	AIR Connector Detection

# Parametri Report

- **Severity:** La severità di una vulnerabilità indica il grado di rischio e di danno potenziale che una vulnerabilità può causare quando viene sfruttata
- **CVSS:** fornisce una valutazione numerica della gravità della vulnerabilità. il range numerico utilizzato è 0-10
- **VPR Score:** è un indice numerico che indica la priorità della minaccia, cioè aiuta a prioritizzare le azioni di mitigazione e risolvere le vulnerabilità più critiche in modo tempestivo.
- **Plugin:** sono identificatori univoci associati alle regole e ai controlli specifici eseguiti durante la scansione. ogni plugin è progettato per individuare una particolare vulnerabilità.
- **Nome:** nome della vulnerabilità rilevata.

GRAZIE PER  
L'ATTENZIONE

