

Progetto Finale M3- Vulnerability Assessment (VA)

Introduzione

Obiettivo del test:

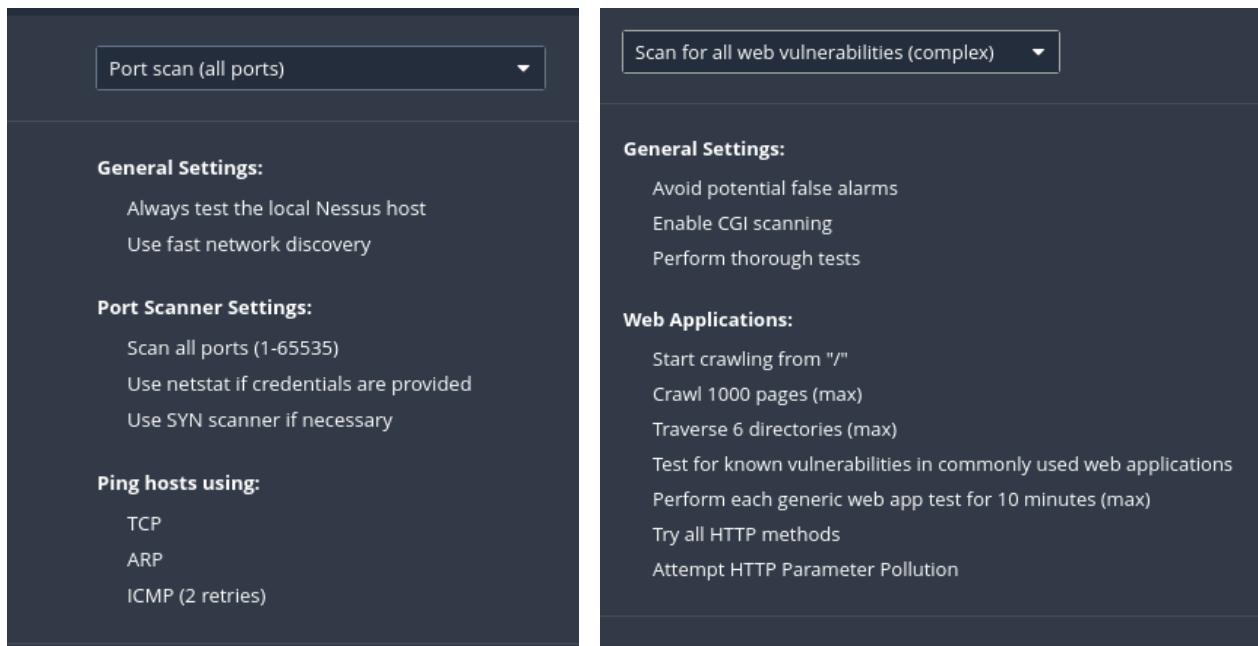
Il test ha l'obiettivo finale di identificare le 4 vulnerabilità più critiche della macchina virtuale (VM) Metasploitable 2.6 per garantirne la sicurezza e ridurre i rischi ad essa associati.

Ambito e Scope:

l'ambito del vulnerability assessment include solo la macchina virtuale Metasploitable 2.6.

Metodologia usata:

l'ambito del vulnerability assessment si basa sulla "Basic Network Scan", con range tutte le porte della macchina (le well-know ports 0-1.024, le registered ports 1.024-49.151 e le private ports 49.152-65.535) e con una scansione per tutte le vulnerabilità note complessa.



The image displays two side-by-side screenshots of the Nessus web interface, showing the configuration for a vulnerability scan. The left panel is titled 'Port scan (all ports)' and the right panel is titled 'Scan for all web vulnerabilities (complex)'. Both panels show a 'General Settings' section with options like 'Always test the local Nessus host' and 'Use fast network discovery'. The left panel also has a 'Port Scanner Settings' section with options like 'Scan all ports (1-65535)' and 'Use netstat if credentials are provided'. The right panel has a 'Web Applications' section with options like 'Start crawling from "/"' and 'Crawl 1000 pages (max)'. Both panels also have a 'Ping hosts using' section with options like 'TCP', 'ARP', and 'ICMP (2 retries)'.

Section	Option	Value
General Settings:	Always test the local Nessus host	Always test the local Nessus host
	Use fast network discovery	Use fast network discovery
	Use netstat if credentials are provided	Use netstat if credentials are provided
Port Scanner Settings:	Scan all ports (1-65535)	Scan all ports (1-65535)
	Use netstat if credentials are provided	Use netstat if credentials are provided
	Use SYN scanner if necessary	Use SYN scanner if necessary
Ping hosts using:	TCP	TCP
	ARP	ARP
	ICMP (2 retries)	ICMP (2 retries)

Strumenti utilizzati:

Nessus: è uno strumento di vulnerability assessment che permette di analizzare sistemi e reti informatiche per individuare vulnerabilità, falle di sicurezza, configurazioni errate o software non aggiornato che potrebbe essere sfruttato da un attaccante;

NMAP: è uno strumento open-source ampiamente utilizzato per la scansione ed analisi di reti informatiche, con lo scopo di mappare una rete, identificare i dispositivi collegati, scoprire le porte aperte, rilevare i servizi in esecuzione ed ottenere informazione sui sistemi operativi.

KALI linux: è una distribuzione Linux basata su debian progettata per la sicurezza informatica, il penetration testing e l'informatica forense grazie ai suoi oltre 600 strumenti preinstallati a scopo di sicurezza.

Sintesi dei risultati

La macchina come da previsione si è dimostrata molto debole e mal protetta da attacchi presentando 80 vulnerabilità di cui 6 critiche. Queste debolezze erano già previste in quanto metasploitable 2.6 è sviluppato con l'intento di voler essere "hackerabile" in quanto usato come materiale da esercitazione per ethical hacker e corsi di cybersecurity.

Come da Lei richiesto vi mostrerò la soluzione hai 5 problemi evidenziati nella sua richiesta:

1. SSL version 2/3 detection;
2. Shell Backdoors;
3. RPC;
4. VNC Server Password;
5. Canonical Ubuntu SEoL.

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	EPSS ▼	Family ▲
<input type="checkbox"/>	CRITICAL	10.0			General
<input type="checkbox"/>	CRITICAL	10.0 *			Gain a shell remotely
<input type="checkbox"/>	CRITICAL	9.8	8.9	0.9447	Web Servers
<input type="checkbox"/>	CRITICAL	9.8			Service detection
<input type="checkbox"/>	CRITICAL	9.8			Backdoors
<input type="checkbox"/>	MIXED	CGI abuses
<input type="checkbox"/>	CRITICAL	Gain a shell remotely

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	login?	
514/tcp	open	shell	Netkit rshd
1099/tcp	open	java-rmi	GNU Classpath grmiregistry
1524/tcp	open	bindshell	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ftp	ProFTPD 1.3.1
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

Per essere certi di questi dati ed evitare falsi positivi facciamo una scansione con nmp dal terminale di kali.

Come da immagine possiamo vedere i dati di Nessus sopra indicati coincidere con la scansione di kali nei seguenti punti:

1. Port 25/tcp = SSL version 2/3 detection
Port 1524/tcp = Shell Backdoors
2. Port 2049/tcp = RPC
3. Port 5900/tcp = VNC Server password
4. Port 80/tcp = Canonical Ubuntu SEoL

Dettaglio tecnico dei risultati

Titolo	Canonical Ubuntu Linux SEoL (8.04.x)	Gravità	Critical – 10
Host	192.168.50.101	Porta	80
Descrizione: Secondo Nessus è vulnerabile a numerose falle critiche, molte delle quali non sono più pubblicamente documentate perché la versione è fuori supporto. Qualsiasi utilizzo in ambienti produttivi o esposti in rete rappresenta un rischio di compromissione totale del sistema			
Impatto: Un aggressore che accede a questa porta può: <ul style="list-style-type: none">- Fare un'escalation di root- Sfruttare il sistema da remoto- Può effettuare un attacco DoS facendo collassare il sistema- Effettuare un furto di dati			
Soluzione: L'unica soluzione sicura è aggiornare a una versione di Ubuntu attualmente supportata. Continuare a utilizzare Ubuntu 8.04 espone il sistema a rischi elevati e non mitigabili con patch			

Titolo	VNC Server 'password' Password	Gravità	Critical – 10
Host	192.168.50.101	Porta	5900
Descrizione: Secondo Nessus la password usata per il VNC (Virtual Network Computing) è estremamente debole essendo una stringa letterale "password"			
Impatto: Un aggressore che accede a questa porta può effettuare un login diretto tramite brute force in maniera veramente semplice ed ottenere il controllo completo del desktop			
Soluzione: Cambiare la password per prima cosa e di conseguenza, fatto ciò si può pensare a limitarne l'accesso tramite firewall e se possibile, incapsularne la connessione in un tunnel cifrato SSH o VPN			

Titolo	SSL Version 2 and 3 Protocol Detection	Gravità	Critical – 9.8
Host	192.168.50.101	Porta	25
Descrizione: La vulnerabilità sta nei protocolli antiquati usati dal sistema che, essendo gravemente insicure e deprecate a causa delle innumerevoli falle critiche presenti in essi, risultano molto semplici da attaccare			
Impatto: un aggressore può facilmente intercettare e decifrare il traffico cifrato tra client e server ottenendo accesso a dati sensibili come credenziali e contenuti riservati (MitM)			
Soluzione: La soluzione migliore sarebbe disabilitare i protocolli SSLv2 e SSLv3 sul servizio SMTP per abilitare TLS 1.2 o TLS 1.3 e mantenerli aggiornati. Consigliata anche l'implementazione di HSTS e altre misure di hardening (impedisce l'accesso solo a comunicazioni sicure impedendo l'accesso a qualunque protocollo http)			

Titolo	Bind Shell Backdoor Detection	Gravità	Critical – 9.8
Host	192.168.50.101	Porta	1524
Descrizione: Secondo le scansioni vi è una backdoor che mette in ascolto una shell. La presenza di questa backdoor è un chiaro segnale che il sistema è stato già compromesso			
Impatto: un aggressore può collegarsi e lanciare comandi come se fosse davanti al terminale anche con privilegi di root senza dover neanche inserire una password. Ciò può portare a installazione di virus, il furto di dati e permettergli delle lateral move			
Soluzione: Controllare la presenza di file o processi sospetti per prima cosa. Successivamente disabilitare il servizio bind shell sulla porta 1524 e chiudere la porta			

Titolo	NFS Shares World Readable	Gravità	Critical – 7.5
Host	192.168.50.101	Porta	2049
Descrizione: Secondo le indagini ci sono uno o più file system condivisi tramite NFS, i quali sono accessibili senza restrizioni di accesso a chiunque dando la possibilità anche di leggerli, modificarli o caricarli senza alcun controllo di IP, hostname o autenticazione			
Impatto: un aggressore può accedere a dati sensibili, sovrascriverli o cancellarli. In alcune configurazioni può fare anche un'escalation di root creando direttamente file con tali permessi. Infine può copiare e/o crittare dati sensibili senza lasciare tracce evidenti			
Soluzione: Si consiglia di restringere l'accesso alle share NFS specificando che solo gli host possono accedervi, evitando permessi eccessivi. Inoltre si consiglia di mantenere il sistema operativo aggiornato e di configurare il firewall limitando l'accesso alla porta 2049. Si può anche pensare di isolare le share NFS su partizioni dedicate per limitare i danni in caso di abuso e di disabilitare SUID/SGID sulle directory esportate per evitare escalation di root			

Conclusioni

Alla base di quanto riportato sopra si possono stabilire i seguenti due punti

Punti di forza: come detto nell'introduzione Metasploitable è una macchina appositamente vulnerabile per fare pratica, infatti, come da report si possono notare tutte le debolezze volute in quanto molti problemi sono lì volutamente da macchina preimpostata come la backdoor o le porte più delicate già aperte

Punti di debolezza: il punto di forza è anche il punto di debolezza. Non si può minimamente pensare di usare meta come OS principale per fare alcunché in quanto sarebbe alla merce di tutti gli hacker. Anche nell'idea di volerlo sistemare andando ad aggiustare le vulnerabilità non ha il minimo senso in quanto esistono distribuzioni di linux "reali" e non da punching machine.