REPORT 1

Scansione Iniziale
M3W12-D4

22 / 11 / 2024

Cybersecurity Analyst

Scansione iniziale di Vulnerabilità (VA)
su Target Metasploitable

Matteo Madonia

SOMMARIO

1.Traccia e consegna

Effettuare una scansione completa sul target Metasploitable.
Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche e provate ad implementare delle azioni di rimedio. N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità. Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Consegna numero 1: Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (tecnico, già riassunto) - ScansioneInizio.pdf

2.Considerazioni iniziali

Per lo svolgimento di questo esercizio è necessario l'utilizzo del tool di scansione professionale di VA (Vulnerability Assessment): NESSUS, su macchina virtuale Kali Linux.

E necessario, in modo preliminare, l'installazione del tool (vedi istruzioni W11M3-D4) + l'avvio dello stesso da shell Linux e apertura da web browser (accesso con credenziali)

Macchina virtuale Metasploitable attiva (target), con indirizzo IP scheda di rete a scelta tra statico o dinamico.

3. Informazioni preliminari

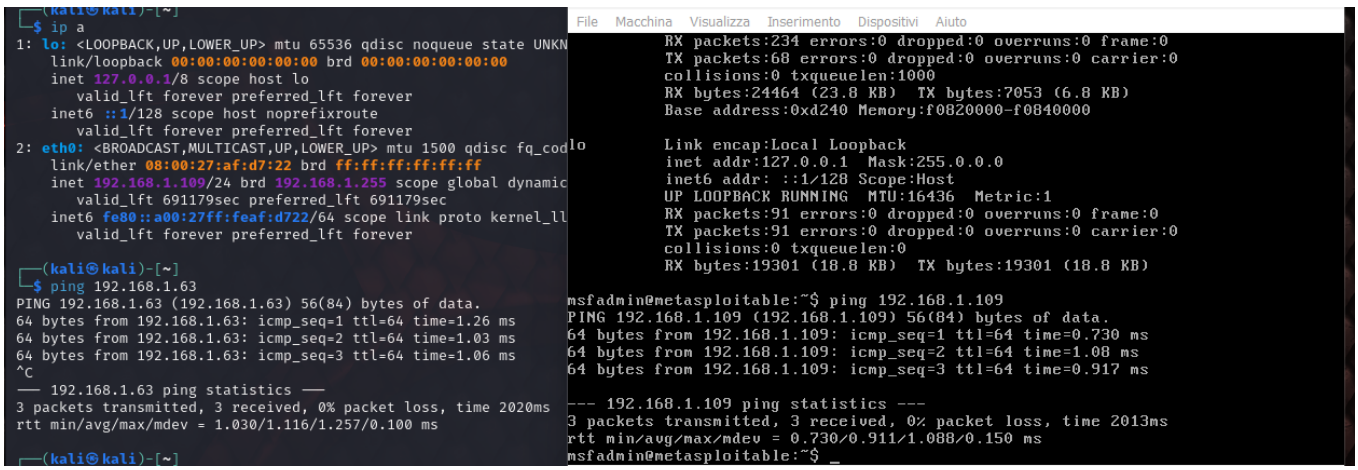
MV in esame:

- KALI LINUX: VM source per utilizzo tool NESSUS, scheda di rete in Bridge
- Metasploitable: VM target oggetto d'esame, scheda di rete in Bridge

TOOL di scansione vulnerabilità:

- Nessus (configurazioni e utilizzo mezzo su web browser)

PING per la verifica di comunicazione tra le due macchine: comunicazione avvenuta con successo

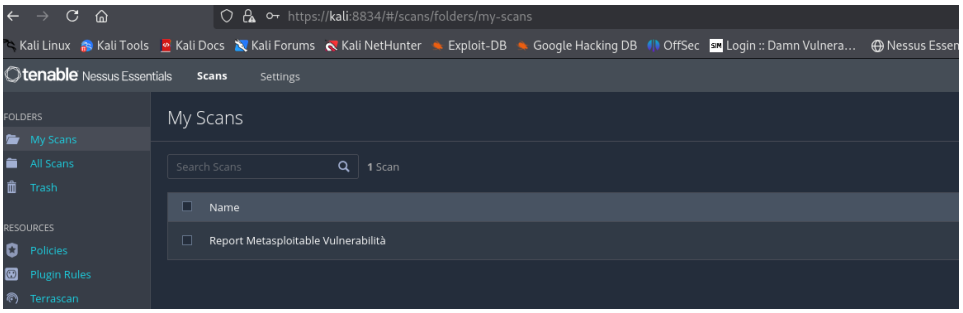


4. Tipologia di scansione e informazioni generali VM

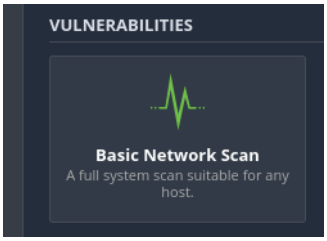
- Tool di scansione: Nessus
- Tipologia di scansione: Basic Network Scan
- IP VM target: 192.168.1.63/24 (Metasploitable) – rilasciato in DHCP
- IP VM source: 192.168.1.109/24 (Kali Linux) – rilasciato in DHCP
- Porte scansionate: 1-1024 (porte conosciute)
- Oggetto della scansione: vulnerabilità su porte aperte e servizi attivi

5. Fasi preliminari alla scansione

- Apertura Tool di scansione Nessus su Browser di Kali Linux



- Sezione “My Scans” -> “New Scan” -> Tipologia di scansione “Basic Network Scan”



- Procedere con la configurazione della scansione sopra indicata e infine avviarla (Launch)

6. Report della scansione

LEGENDA:
Richiesta Remediation su Vulnerabilità = ⇨

192.168.1.63

6	6	19	8	75
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 114

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0*	5.1	0.1175	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.1175	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	7.4	0.6661	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0164	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0358	90509	Samba Badlock Vulnerability
HIGH	7.5*	5.9	0.015	10205	rlogin Service Detection
HIGH	7.5*	5.9	0.015	10245	rsh Service Detection
MEDIUM	6.8	6.0	0.1395	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisonir
MEDIUM	6.5	4.4	0.0041	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	6.5	-	-	42263	Unencrypted Telnet Server

192.168.1.63 4

MEDIUM	5.9	4.4	0.9717	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.0031	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	0.9434	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsole and Weakened eNcryption)
MEDIUM	5.9	4.4	0.0076	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	-	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	4.0	0.0058	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*	7.3	0.0114	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	0.9488	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FRE
LOW	3.7	3.4	0.6115	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	3.9	0.9736	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	3.9	0.9736	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Suppor (Logjam)
LOW	3.4	5.1	0.9749	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	4.2	0.8808	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	-	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version

192.168.1.63 5

INFO	N/A	-	-	39519	Backported Security Patch Detection (FTP)
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	-	35373	DNS Server DNSSEC Aware Resolver
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	72779	DNS Server Version Detection
INFO	N/A	-	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11156	IRC Daemon Version Detection
INFO	N/A	-	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosur
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remo check)
INFO	N/A	-	-	10719	MySQL Server Detection
INFO	N/A	-	-	10437	NFS Share Export List

INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	50845	OpenSSL Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	10180	Ping the remote host
INFO	N/A	-	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	-	26024	PostgreSQL Server Detection
INFO	N/A	-	-	22227	RMI Registry Detection
INFO	N/A	-	-	11111	RPC Services Enumeration
INFO	N/A	-	-	53335	RPC portmapper (TCP)
INFO	N/A	-	-	10263	SMTP Server Detection
INFO	N/A	-	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported

192.168.1.63 7

INFO	N/A	-	-	62563	SSL Compression Methods Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	51891	SSL Session Resume Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	25240	Samba Server Detection
INFO	N/A	-	-	104887	Samba Version
INFO	N/A	-	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	17975	Service Detection (GET request)
INFO	N/A	-	-	11153	Service Detection (HELP Request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	11819	TFTP Daemon Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10281	Telnet Server Detection
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	19288	VNC Server Security Type Detection
INFO	N/A	-	-	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	-	-	10342	VNC Software Detection
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	11424	WebDAV Detection
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	52703	vsftpd Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

7. Analisi delle vulnerabilità – richiesta Remediation

- **61708 - VNC Server 'password' Password – Porta tcp/5900/vnc**

Synopsis
A VNC server running on the remote host is secured with a weak password.

Description
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution
Secure the VNC service with a strong password.

Risk Factor
Critical
CVSS v2.0 Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Output
tcp/5900/vnc

- **46882 - UnrealIRCd Backdoor Detection – Porta tcp/6667/irc**

Synopsis
The remote IRC server contains a backdoor.

Description
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

Risk Factor
Critical
0.6661
CVSS v2.0 Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS v2.0 Temporal Score
8.3 (CVSS2#E:F/RL:OF/RC:C)

Exploitable With
192.168.1.63 16
CANVAS (true) Metasploit (true)

Plugin Output
tcp/6667/irc

- **51988 - Bind Shell Backdoor Detection – Porta tcp/1524/wild_shell**

Synopsis
The remote host may have been compromised.

Description
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly. Nessus was able to execute the command "id" using the

Solution
Verify if the remote host has been compromised, and reinstall the system if necessary.

Risk Factor
Critical
CVSS v3.0 Base Score
9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSS v2.0 Base Score
192.168.1.63 4
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Output
tcp/1524/wild_shell

- **32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness Porta tcp/22/ssh**

E

- **32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)**

Synopsis
The remote SSH host keys are weak.

Description
The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.
The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.
An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Solution
Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor
Critical
VPR Score
5.1

EPSS Score
0.1175
CVSS v2.0 Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS v2.0 Temporal Score
8.3 (CVSS2#E:F/RL:OF/RC:C)

Exploitable With
Core Impact (true)

Plugin Output
tcp/22/ssh

8. Intervention priority timeline delle Vulnerabilità

➔

61708 - VNC Server 'password' Password – Porta tcp/5900/vnc	**46882 - UnrealIRCd Backdoor Detection – Porta tcp/6667/irc**	**32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness Porta tcp/22/ssh** **E** **32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)**	**51988 - Bind Shell Backdoor Detection – Porta tcp/1524/wild_shell**
CRITICA	CRITICA	CRITICA	CRITICA
Richiesto intervento immediato, nell'arco di pochi giorni	Richiesto intervento immediato, nell'arco di pochi giorni	Richiesto intervento immediato, nell'arco di pochi giorni	Richiesto intervento immediato, nell'arco di pochi giorni; precedenza ai primi 3 descritti

9. Quotazione tipo per interventi esposti in Timeline

La seguente quotazione, comprensiva dei costi da sostenere per la risoluzione delle criticità e vulnerabilità riscontrate, è da considerarsi EXTRA oltre totale sostenuto per il Vulnerability Assessment eseguito (comprensivo di scansione professionale sul target richiesto e reportistica).

Un **Cybersecurity Analyst Senior** o **Specialist,** data l'esperienza maturata nel corso degli anni, esegue interventi di questa entità ad un costo orario pari a € 60,00 i.e. / H

Si riporta di seguito un esempio di quotazione per le lavorazioni di remediation per la vulnerabilità CRITICA **Apache Tomcat AJP Connector Request Injection (Ghostcat)**

Importo unitario €/H	Tempo stimato	Descrizione	Lavorazione	TOTALE €
€ 60,00 i.e.	10,00 H	**REMEDIATION - Apache Tomcat AJP Connector Request Injection (Ghostcat) – CRITICITA' ALTA**	Valutazione della vulnerabilità, Applicazione della patch, Test post applicazione, Monitoraggio finale	€ 600,00 i.e.
€ 45,00 i.e.	Variabile	**Monitoraggio continuo post attività**	EVENTUALE LAVORAZIONE	\

ESCLUSIONI: sono da definirsi escluse tutte le attività non citate nella quotazione sopra esposta, eventuali interventi richiesti in loco e/o risoluzione di problematiche emerse al momento dell'intervento.

PAGAMENTO: anticipo 50% conferma lavori, saldo Bonifico Bancario ricevimento fattura

VALIDITA' QUOTAZIONE: 20/11/2024 – 30/11/2024

NOTE: L'azienda non si assume responsabilità circa eventuali attacchi hacker eseguiti prima dell'inizio dei lavori di risoluzione delle vulnerabilità.

Data

_____

Firma cliente per accettazione

_____

10. Considerazioni finali

Le vulnerabilità di sistemi operativi su porte aperte e servizi attivi in rete, sono al giorno d'oggi una tematica da non sottovalutare, da monitorare costantemente nel tempo e che richiede continuo aggiornamento di patch ecc.
Molte aziende sottovalutano questa tematica, perché magari ignare della reale e potenziale gravità economica, intellettuale, personale, finanziaria ecc. che un attacco Hacker potrebbe causare.

E' per questo che il ruolo del Cybersecurity Analyst e Specialist è di fondamentale importanza.