REPORT 3

Scansione delle Vulnerabilità di Meta dopo la Remediation M3W12-D4

22 / 11 / 2024

Cybersecurity Analyst

Scansione delle Vulnerabilità su Metasploitable dopo la fase di Remediation

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 3: Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità (il grafico che mostra tutte le vulnerabilità) - ScansioneFine.pdf

2. Considerazioni iniziali – Post Remediation

In seguito alla fase di Remediation, nella quale prendiamo in analisi tutte le vulnerabilità critiche e la loro risoluzione per diminuire il fattore RISCHIO in RISCHIO RESIDUO accettabile, procediamo nuovamente con una scansione, tramite il tool di VA Nessus, che evidenzi effettivamente la corretta applicazione di tutte le remediation effettuate nel REPORT 2.

3. Informazioni preliminari

MV in esame:

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

4. Informazioni generali VM

- IP VM target: 192.168.1.109/24 (Metasploitable) – rilasciato in DHCP

- IP VM source: 192.168.1.103/24 (Kali Linux) – rilasciato in DHCP

  NOTA BENE: gli indirizzi IP delle schede di rete delle VM, sono cambiati durante il report, in quanto gli indirizzi rilasciati in DHCP, avendo eseguito i REPORT in luoghi fisici differenti, con reti quindi differenti.

5. Report della scansione dopo la fase di REMEDIATION

192.168.1.103

Vulnerabilities Total: 82

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9737	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0*	5.1	0.1175	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
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	5.9	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	-	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	4.4	0.9717	136808	ISC BIND Denial of Service
MEDIUM	5.3	-	-	12085	Apache Tomcat Default Files
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	4.3*	-	-	90317	SSH Weak Algorithms Supported
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	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	-	-	21186	AJP Connector Detection
INFO	N/A	-	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39446	Apache Tomcat Detection
INFO	N/A	-	-	39519	Backported Security Patch Detection (FTP)
INFO	N/A	-	-	84574	Backported Security Patch Detection (PHP)
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	-	-	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	-	-	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	-	-	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 (rem check)
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	-	-	48243	PHP Version Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	22227	RMI Registry Detection
INFO	N/A	-	-	11111	RPC Services Enumeration
INFO	N/A	-	-	53335	RPC portmapper (TCP)
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	-	-	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

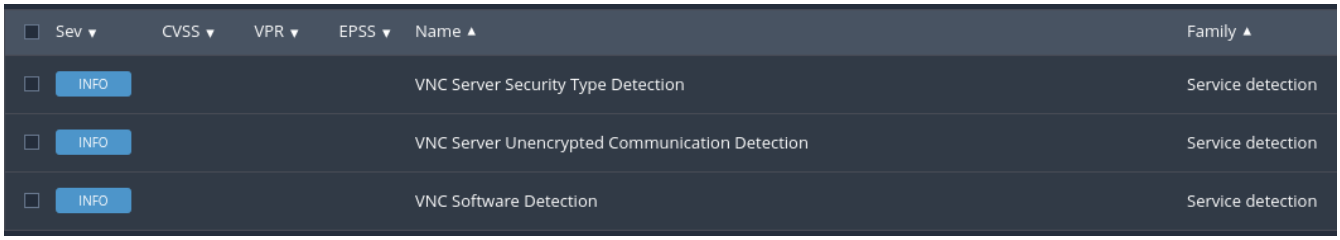
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	11819	TFTP Daemon Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10281	Telnet Server Detection
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	11154	Unknown Service 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	-	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	-	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	-	11424	WebDAV Detection
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	52703	vsftpd Detection

6. Analisi della Risoluzione delle vulnerabilità

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

Per il diminuire il fattore di RISCHIO CRITICO ad un livello di fattore di RISCHIO RESIDUO accettabile, è stata necessaria una remediation effettuando il cambio della password di accesso, che Metasploitable di default indica come 'password', in una più efficacie e sicura, con caratteri alfa-numerici; in sintesi, i lavori svolti sono i seguenti:

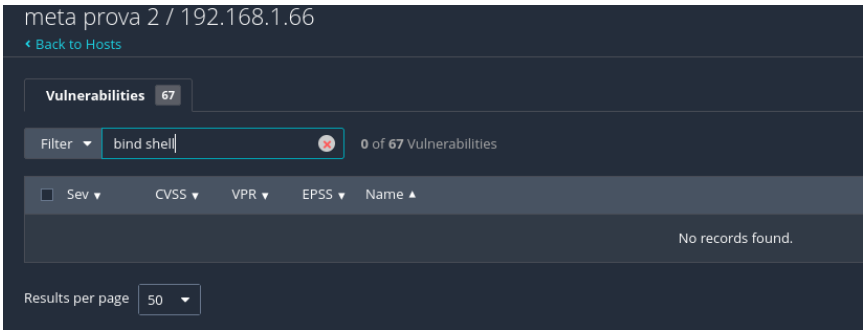
1. Verificato che il servizio VNC server sia attivo su Meta e in esecuzione
2. Verificata la connessione con il VNC Server sulla sessione :0 da Kali Linux
3. Eseguiti i successivi comandi come Root su Meta
4. Impostazione della nuova password
5. Terminato il processo VNC server
6. Riattivato il processo
7. Prova nuova connessione da Kali al server Meta con nuova password
8. Scansione di prova con tool Nessus per verifica applicazione Remediation



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

Per il diminuire il fattore di RISCHIO CRITICO ad un livello di fattore di RISCHIO RESIDUO accettabile, è stata effettuata la chiusura di tutte le porte non necessarie, come per la porta tcp/1524, tramite il firewall iptables presente sui sistemi Linux. Di seguito procedure eseguite:

1. Verificato lo stato aperto della porta 1524 e che il servizio sia attivo tramite scansione VA di Nessus
2. Verificata la presenza di una bindshell tramite tool Netcat da Kali Linux sulla porta 1524
3. Chiusura della porta in esame con il firewall iptables (eseguito comando come root)
4. Con tool Netcat da Kali Linux, verificata l'avvenuta chiusura della porta
5. Scansione di prova con tool Nessus per verifica applicazione Remediation



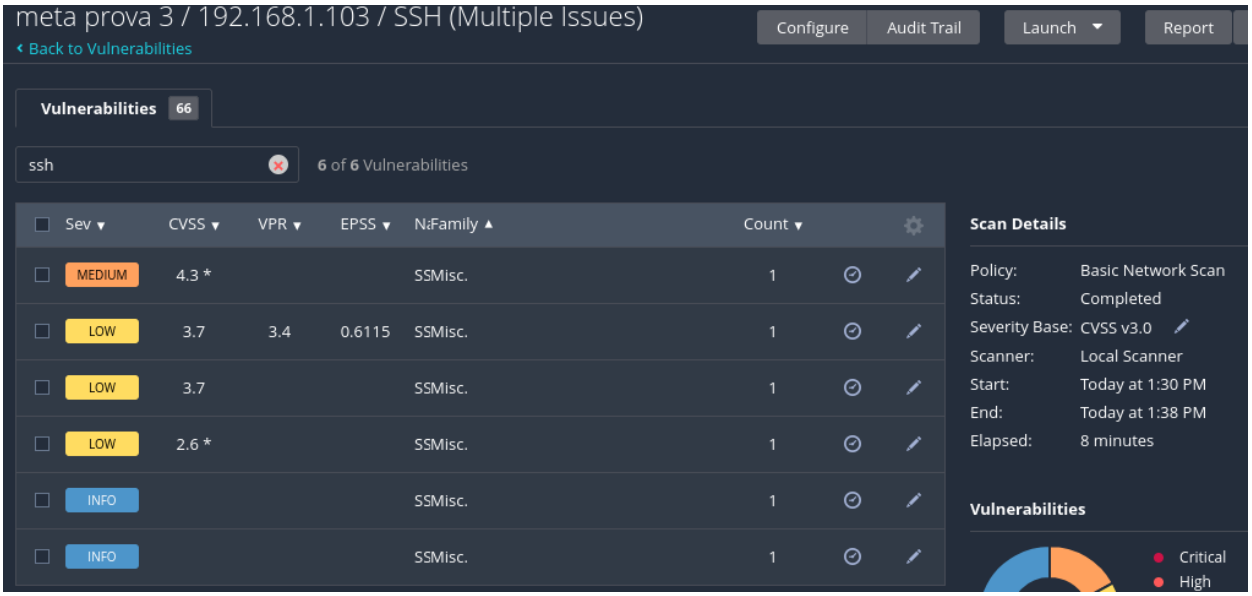
- **32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness Porta tcp/22/ssh** - **(NOTA BENE: questa vulnerabilità (che compare ancora nel report di scansione finale era stata risolta come da immagine sottostante, purtroppo con il cambio di postazione di lavoro e spegnimento MV Meta (che ha perso le configurazioni, non è più rientrata…)**

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

Il fattore rischio di queste vulnerabilità che presentano particolari problematiche circa l'RNG, il generatore di numeri casuali, utilizzato in OpenSSH e OpenSSL, protocolli utilizzati per l'invio sicuro di informazioni, è stato diminuito ad un fattore di rischio residuo, tramite l'aggiornamento delle Chiavi ssh Keygen. Di seguito le procedure eseguite:

8

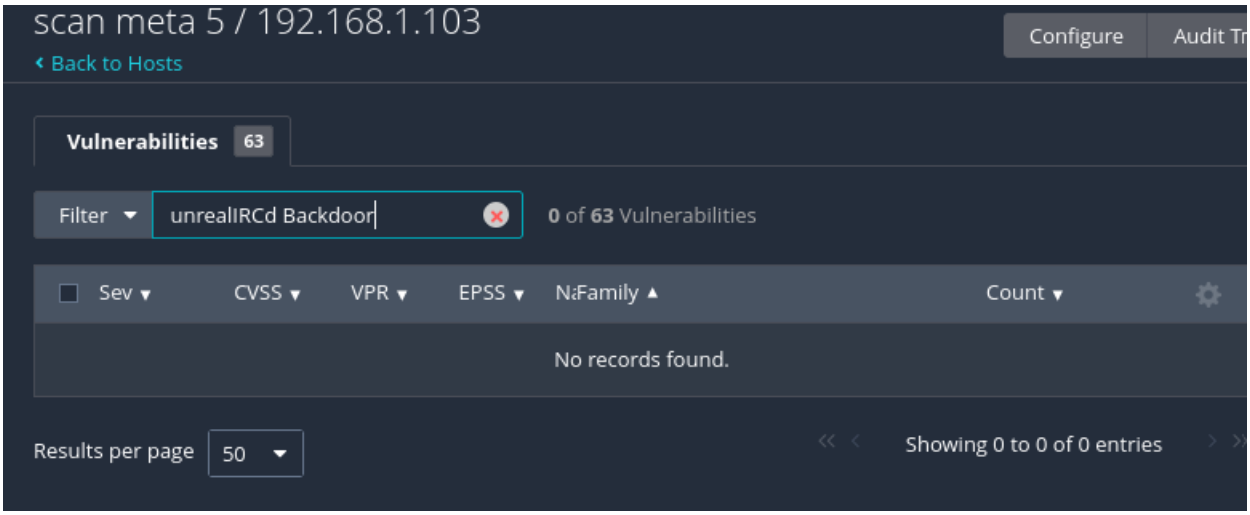
1. Sulla vm Meta eseguito un update degli aggiornamenti
2. Effettuato un upgrade dei pacchetti openssl
3. Effettuato il reboot della macchina
4. Esecuzione aggiornamento delle chiavi ssh Keygen
5. Scansione di prova con tool Nessus per verifica applicazione Remediation



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

Per il diminuire il fattore di RISCHIO CRITICO ad un livello di fattore di RISCHIO RESIDUO accettabile, è stata effettuata la chiusura della porta tcp/6667, tramite il firewall iptables presente sui sistemi Linux. Di seguito procedure eseguite:

1. Bloccaggio del servizio tramite apposito comando
2. Impostazione policy firewall di iptables sulla porta in esame
3. Scansione di prova con tool Nessus per verifica applicazione Remediation



7. 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.