mestploi

Report generated by Nessus™ Wed, 10 May 2023 18:23:11 CEST

TABLE OF CONTENTS

192.168.49.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
3	3	3	1	80

Scan Information

Start time:	Wed May 10 18:13:56 2023
End time:	Wed May 10 18:23:11 2023

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.49.101
MAC Address:	08:00:27:B1:AA:58
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)

Vulnerabilities

Considerazioni generali

Dai risultati delle nostre operazioni ci risultano svariate vulnerabilità, molte anche particolarmente gravi, che comportano quindi seri rischi per i sistemi aziendali.

Alcune di esse permettono a potenziali malintenzionati di assumere il completo controllo dei sistemi aziendali, quindi avendo accesso a file e cartelle riservate, oppure il totale spegnimento ed eliminazione di qualsiasi servizio presente sul server analizzato.

Priorità di risoluzione

Si consiglia di risolvere prima le vulnerabilità critiche, in quanto sono sia quelle più comuni, e quindi più facili da trovare per un malintenzionato, che le più gravi, che comprometterebbero quindi la completa funzionalità dei sistemi aziendali.

Vulnerabilities Total: 50

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure

Alcune di esse sono molto semplici da risolvere, come per esempio l'ultima, cambiando la password di default del servizio.

Altre invece richiedono un intervento strutturale atto ad aggiornare il sistema operativo installato sulla macchina, in quanto così vecchio da non essere più supportato dalle patch di sicurezza.

Successivamente si andranno a risolvere le vulnerabilità di grado alto, che possono comportare una falla nella riservatezza dei dati, oppure un accesso non autorizzato ai dati aziendali.

HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	-	90509	Samba Badlock Vulnerability

In questo caso la risoluzione è meno strutturale e richiede l'utilizzo di servizi più appropriati per la condivisione di file e cartelle al interno del azienda. E l'aggiornamento di alcuni di quelli già presenti.

Procedendo poi con la risoluzione delle vulnerabilità, passiamo quindi a quelle di rischio medio:

Esse sono simili a quelle di grado alto come rischi, ma tuttavia presuppongono una conoscenza più avanzata dei sistemi informatici da parte di un potenziale attaccante.

MEDIUM	6.5	-	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	5.9	-	136808	ISC BIND Denial of Service
MEDIUM	4.0*	-	52611	SMTP Service STARTTLS Plaintext Command Injection

Per risolverle, alcune verranno risolte a cascata dal aggiornamento di alcuni servizi, per altre invece è necessaria la modifica di alcune configurazioni di alcuni servizi presenti. Poi vediamo che alcuni certificati presenti non sono validi, e vanno quindi aggiornati con fonti sicure, ciò è un rischio per la riservatezza delle informazioni che passano al interno dei canali cifrati.

Per ultimo verranno poi risolte le vulnerabilità di grado basso

LOW	2.6*	-	10407	X Server Detection

Esse sono vulnerabilità principalmente di crittografia e algoritmi deboli di cifratura, essi vanno disabilitati e/o aggiornati ove possibile.

Le vulnerabilità di tipo INFO sono semplici possibilità che si hanno per ottenere informazioni riguardo ai servizi e al sistema in uso, non sono di per se un rischio per la sicurezza se si mantengono tutti i servizi aggioranti, eventualmente con semplici regole di firewall o tramite particolari configurazioni dei servizi possono essere ridotte o eliminate.

Per sintesi ne elencheremo solo alcune:

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	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
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 (remote 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	-	66334	Patch Report
INFO	N/A	-	11111	RPC Services Enumeration
INFO	N/A	-	53335	RPC portmapper (TCP)
INFO	N/A	-	10263	SMTP Server Detection
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	-	25220	TCP/IP Timestamps Supported

INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	10342	VNC Software Detection
INFO	N/A	-	135860	WMI Not Available
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