REPORT NESSUS

Il report qui presente riporta in modo sintetico le principali vulnerabilità della macchina Metasploitable2 e accorgimenti da adottare per poter risolvere eventuali criticità.

192.168.64.3

CRITICAL	HIGH	MEDIUM	LOW	INFO
14	12	42	10	156

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.64.3
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)

192.168.64.3

12	11	34	8	89
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 154

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	9.1	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	34460	Unsupported Web Server Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Essentials

CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	61708	VNC Server 'password' Password
CRITICAL	10.0*	10203	rexecd Service Detection
HIGH	8.8	70728	Apache PHP-CGI Remote Code Execution
HIGH	8.8	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	42256	NFS Shares World Readable
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	90509	Samba Badlock Vulnerability

CRITICITA’ RISCONTRATA A LIVELLO CRITICO

VERSIONE DEL SISTEMA OPERATIVO UNIX NON SUPPORTATA

Questa voce ci indica che il sistema operativo non è più aggiornato e quindi altamente vulnerabile ad attacchi esterni.
Si consiglia di aggiornare o passare ad un’altra versione del sistema onde evitare questo genere di problematiche.

CRITICITA’ RISCONTRATA A LIVELLO HIGH

CODICE DI ESECUZIONE REMOTA PHP-CGI APACHE

Il protocollo server web PHP contiene un difetto che consente a chiunque l’accesso al server e ai comandi. Questo problema se abusato potrebbe portare a eventuali crash di sistema, pertanto si consiglia di aggiornare a versione PHP 5.4.3 o superiori.

Conclusione

Ci sono ulteriori vulnerabilità ovviamente, pero questo report ha come unico scopo di illustrare le vulnerabilità che vanno assolutamente risolte, al fine di evitare attacchi esterni.