Report dirigenziale
Target
Metasploitable

Sommario

Elenco vulnearbilità rilevanti

Criticità	Nome	Effort risoluzione
CRITICAL	Apache Tomcat A JP Connector Request Injection (Ghostcat)	MEDIO
CRITICAL	Bind Shell Backdoor Detection	MEDIO/ALTO
CRITICAL	SSL Version 2 and 3 Protocol Detection	BASSO
CRITICAL	Unix Operating System Unsupported Version Detection	MEDIO
CRITICAL	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	MEDIO
CRITICAL	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	MEDIO
CRITICAL	NFS Exported Share Information Disclosure	BASSO
CRITICAL	VNC Server 'password' Password	BASSO
HIGH	ISC BIND Service Downgrade / Reflected DoS	MEDIO
HIGH	NFS Shares World Readable	ALTO
HIGH	SSL Medium Strength Cipher Suites Supported (SWEET32)	MEDIO

HIGH	Samba Badlock Vulnerability	MEDIO
MEDIUM	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS	MEDIO
MEDIUM	SSL Certificate Cannot Be Trusted	BASSO
MEDIUM	SSL Self-Signed Certificate	BASSO
MEDIUM	TLS Version 1.0 Protocol Detection	BASSO
MEDIUM	ISC BIND Denial of Service	MEDIO
MEDIUM	SSL Anonymous Cipher Suites Supported	BASSO
MEDIUM	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	MEDIO
MEDIUM	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	BASSO
MEDIUM	HTTP TRACE / TRACK Methods Allowed	BASSO
MEDIUM	SMB Signing not required	BASSO
MEDIUM	SSL Certificate Expiry	BASSO
MEDIUM	SSL Certificate with Wrong Hostname	BASSO
MEDIUM	SSL Weak Cipher Suites Supported	BASSO
MEDIUM	SMTP Service STARTTLS Plaintext Command Injection MEDIUM 4.3*	ALTO
MEDIUM	SSH Weak Algorithms Supported	MEDIO

MEDIUM	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	MEDIO
LOW	SSH Server CBC Mode Ciphers Enabled LOW	BASSO
LOW	SSH Weak Key Exchange Algorithms Enabled	BASSO
LOW	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	BASSO
LOW	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	ALTO
LOW	SSH Weak MAC Algorithms Enabled	BASSO
LOW	X Server Detection	BASSO