



W12D3

REPORT VULNERABILITA'

La traccia

Traccia

A partire dal report di ieri:

- Analisi/studio delle vulnerabilità (PDF) - servirà sia per exploit che remediation
- Report PDF per «dirigente»
- Inteso come riassunto che va presentato ai dirigenti per l'approvazione a livello finanziario ecc. Non contiene troppi dettagli tecnici ma soltanto l'indicazione della vulnerabilità e soprattutto i grafici con la pericolosità delle varie vulnerabilità riscontrate

Report Vulnerabilità

Scan Information

Start time: Tue Jan 23 15:00:24 2024
End time: Tue Jan 23 15:10:45 2024

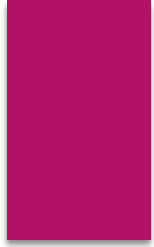
Host Information

Netbios Name: METASPLOITABLE
IP: 192.168.100.4
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Il presente lavoro evidenzia quelle che sono le principali vulnerabilità del sistema, sono riportate le principali criticità divise per livello di gravità.
Ad ogni vulnerabilità verrà attribuito un punteggio in decimi che indicherà il livello di gravità di quella specifica vulnerabilità.

Acronimi e definizioni

- Vulnerabilità:** la denominazione della vulnerabilità.
- Cvss:** lo score in decimi attribuito ad ogni vulnerabilità in modo da apprezzarne la severity.
- Tempistica risoluzione:** periodo di tempo richiesto per la remediation.
- Priorità:** la stima della priorità da attribuire alle vulnerabilità, in modo da capire quali risolvere prima



Vulnerabilità	CVSS(/10)	Tempistica risoluzione	Priorità
Apache Tomcat AJP Connector Request Injection (Ghostcat)	9.8	Lunga	Alta
Bind Shell Backdoor Detection	9.8	Breve	Alta
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	10	Media	Alta
61708 - VNC Server 'password' Password	10	Breve	Alta
136769 - ISC BIND Service Downgrade / Reflected DoS	10	Breve	Media
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	7.5	Media	Media
153953 - SSH Weak Key Exchange Algorithms Enabled	3.7	Media	Bassa