

NESSUS ESSENTIALS

S 5 / L 4

Nell'esercitazione di oggi andremo a eseguire una scansione tramite Nessus Essential, a valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

Gli obiettivi dell'esercizio sono:

- Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.
- Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

<input type="checkbox"/>	CRITICAL	10.0 *	NFS Exported Share Information Disclosure	RPC	1			
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Configuration	General	1			
<input type="checkbox"/>	CRITICAL	10.0 *	UnrealIRCd Backdoor Detection	Backdoors	1			
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Server 'password' Password Disclosure	Gain a shell remotely	1			
<input type="checkbox"/>	CRITICAL	9.8	SSL Version 2 and 3 Protocol Detection	Service detection	2			
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell Backdoor Detection	Backdoors	1			
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3		
<input type="checkbox"/>	HIGH	9.8	Apache Tomcat AJP Connector Configuration	Web Servers	1			
<input type="checkbox"/>	HIGH	7.5 *	rlogin Service Detection	Service detection	1			
<input type="checkbox"/>	HIGH	7.5 *	rsh Service Detection	Service detection	1			

A seguito di una scansione con Nessus ci ritroveremo davanti una classificazione delle varie vulnerabilità che il nostro target presenta, se presenti, in modo da permetterci di andare ad agire tempestivamente su quelle che sono le problematiche più gravi.

Vulnerabilities 70

CRITICAL Unix Operating System Unsupported Version Detection < >

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Output

Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 23.04 / LTS 22.04 / LTS 20.04 .
For more information, see : <https://wiki.ubuntu.com/Releases>

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	192.168.1.104

Andando a controllare i vari errori uno ad uno possiamo notare la quantità di informazioni che Nessus è in grado di fornirci sul problema, in più ci fornisce dei consigli su come poter risolvere la falla di sicurezza. Inoltre questo software ci permette di andare a creare dei report più o meno dettagliati sulla situazione generale del nostro target.

Vulnerabilities 70

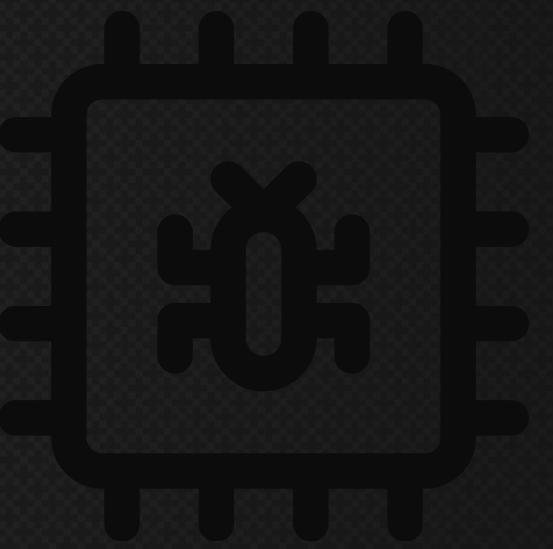
CRITICAL Unix Operating System Unsupported Version Detection

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Nella situazione che abbiamo preso in esempio in questa esercitazione il software ci segnala che il sistema operativo in uso è attualmente non supportato, il che vuol dire che eventuali falle di sicurezza non verranno risolte, questa è una situazione da evitare in quanto un sistema operativo che riceve supporto riceve costantemente dei miglioramenti man mano che determinate debolezze vengono scoperte.



Solution

Upgrade to a version of the Unix operating system that is currently supported.

Per quanto riguarda questa vulnerabilità la soluzione più semplice che possiamo andare ad attuare è quella di aggiornare il sistema operativo ad una versione attualmente supportata.