Vulnerability Assessment Report

Target: Metasploitable2

Durata temporale dell'attività:
7 ore

Attività eseguita da:
Leonzio Emanuele

Indice generale Sommario

Esecutivo

Nel mese di novembre 2024 è stata eseguita un'attività di **Vulnerability Assessment** per verificare la postura difensiva dell'infrastruttura **Metasploitable2**. Il report si riferisce a uno scenario in cui sono presenti i seguenti elementi: il **target**, rappresentato dall'indirizzo IP di Metasploitable2 (192.168.1.7), e l'**attaccante**, Kali Linux, utilizzato per effettuare scansioni tramite **Nessus**.

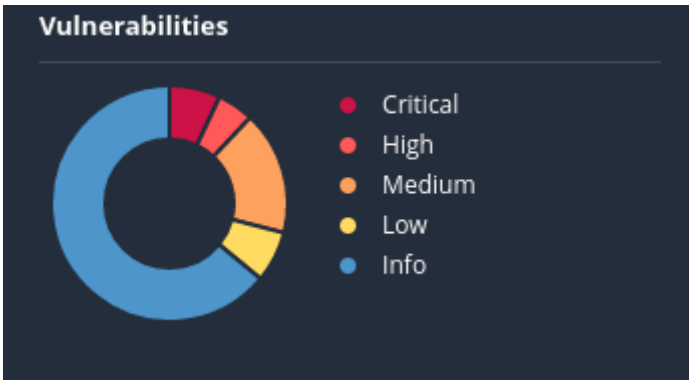
La descrizione dello scenario è la seguente: il test, condotto con Nessus, è stato finalizzato a eseguire una scansione di tutte le porte conosciute per individuare eventuali vulnerabilità critiche, così da poter implementare le necessarie azioni di rimedio e mitigare le criticità emerse.

Dall'analisi è emerso che il rischio complessivo dell'infrastruttura è **alto**. A causa della gravità di alcune vulnerabilità rilevate, è auspicabile un intervento immediato. Di seguito sono riportate le azioni consigliate da intraprendere al più presto:

1. **Configurare il servizio VNC** con una password più sicura e robusta.
2. **Aggiornare OpenSSL** e rigenerare i certificati SSL e SSH, implementando ulteriori configurazioni di sicurezza per abilitare esclusivamente protocolli sicuri.
3. Per la vulnerabilità **Bind Shell Backdoor Detection**, che segnala la presenza di una shell di comando in ascolto su una porta remota senza richiedere autenticazione, è necessario:
    - Individuare il processo responsabile;
    - Identificare la porta su cui è in ascolto;
    - Arrestare immediatamente il processo.

Queste misure sono fondamentali per rafforzare la sicurezza dell'infrastruttura e ridurre il rischio associato alle vulnerabilità riscontrate.

Grafico 1: Vulnerabilità



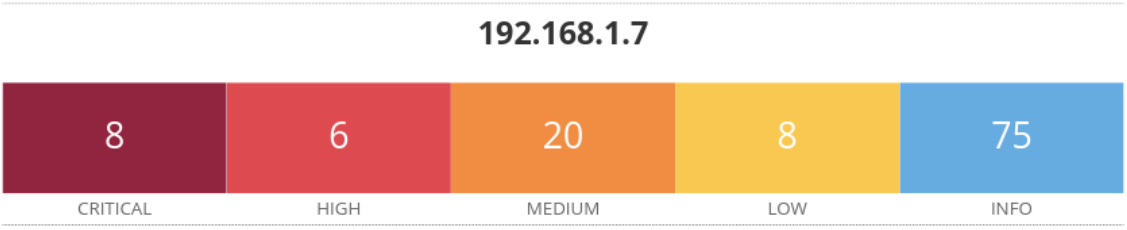
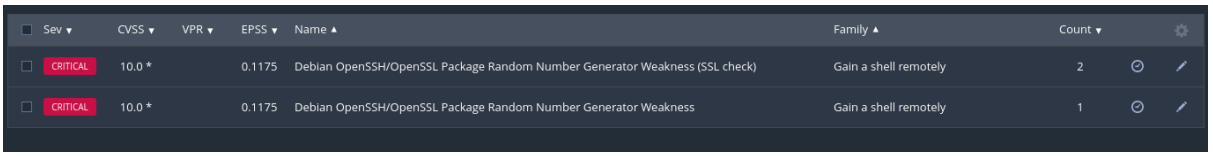


Tabella 1: Specifiche sulla scansione

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *		0.6661	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3



Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *		0.1175	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	Gain a shell remotely	2
CRITICAL	10.0 *		0.1175	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely	1

Elenco Vulnerabilità Metasploitable2 prese in esame

VNC Server 'password' Password

Description
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Bind Shell Backdoor Detection

Description
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Description
The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Description
The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.