Progetto M3

Fabrizio Meini

"Analisi di Vulnerabilità e Implementazione di Azioni di Rimedio su Metasploitable"

Ambiente:

-Macchina ATK:

VM Kali Linux - IP 192.168.1.100 - Scheda di rete bridged

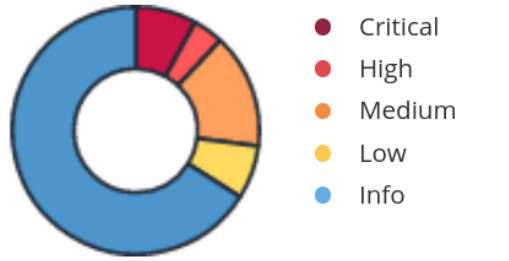
-Macchina Target:

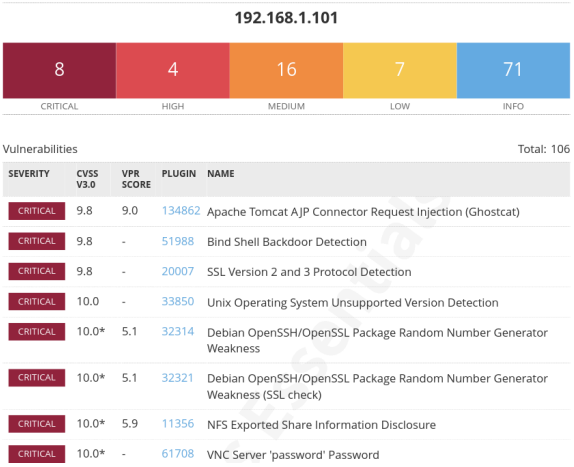
VM Metasploitable - IP 192.168.1.101 - Scheda di rete bridged

Strumenti utilizzati:

-Nessus

Report Iniziale:





192.168.1.101

8	4	16	7	71
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 106

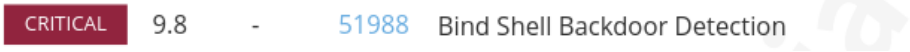
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Come possiamo notare sono presenti diverse vulnerabilità di cui circa il 6% risultano essere catalogate come Critiche. Proprio su quelle ci andremo a focalizzare per poter migliorare la stabilità e la tenuta della nostra VM.

Analisi delle Vulnerabilità:
Le vulnerabilità che prenderemo in considerazione per il progetto sono le seguenti:

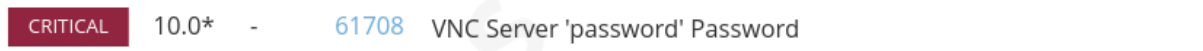
”At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.”

"NSF Exported Share Information Disclosure" è una vulnerabilità di informazione che si verifica quando le informazioni sensibili o riservate sono esposte attraverso la condivisione NFS (Network File System) non protetta. NFS è un protocollo di condivisione file di rete utilizzato comunemente in ambienti Unix e Linux. In particolare, questa vulnerabilità si verifica quando un server NFS espone in modo non sicuro l'elenco delle condivisioni NFS disponibili, consentendo agli attaccanti di ottenere informazioni sensibili sui file e sulle directory condivisi, incluso il loro percorso nel sistema di file.



“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.”

Il "bind shell backdoor" è un tipo di backdoor che consente a un attaccante di aprire una porta sul sistema compromesso e "vincolarla" a una shell di comando remota. Questo permette all'attaccante di connettersi al sistema e ottenere un accesso a livello di shell per eseguire comandi arbitrari.



“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.”

La stringa "vnc server password password" sembra indicare la configurazione di una password per il server VNC (Virtual Network Computing). Tuttavia, è importante notare che utilizzare una password così semplice come "password" è estremamente debole e non offre una protezione efficace per il server VNC.

CRITICAL 9.8 - 20007 SSL Version 2 and 3 Protocol Detection

“The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:
- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.
An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.”

La rilevazione dei protocolli SSL versione 2 e 3 è un processo volto a identificare se un server supporta o è configurato per utilizzare SSL versione 2 e/o SSL versione 3. Questi due protocolli sono considerati obsoleti e insicuri a causa delle loro vulnerabilità note, tra cui vulnerabilità di cifratura debole e attacchi di tipo POODLE (Padding Oracle On Downgraded Legacy Encryption).