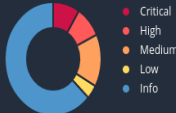


Vulnerability Scan con NISSUS

La scansione della macchina virtuale Metasploitable con Nessus ha permesso di identificare varie vulnerabilità. Questo processo non solo aiuta a comprendere le debolezze del sistema, ma è anche fondamentale per migliorare le difese e garantire la sicurezza dei sistemi.

Analisi delle vulnerabilità critiche:

Eseguendo una scansione di Metasploitable con NISSUS, ha rilevato diverse vulnerabilità critiche.

Sev	CVSS	VPR	EPSS	Name	Family	Count			Host Details
CRITICAL	10.0 *	7.4	0.6988	UnrealIRCd Backdoor Detection	Backdoors	1			IP: 192.168.1.40 DNS: Host-006.homenet.telecomitalia.it MAC: 08:00:27:F4:76:34 OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy) Start: Today at 12:02 PM End: Today at 12:11 PM Elapsed: 8 minutes KB: Download
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1			Vulnerabilities 
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			
HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1			
HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1			
HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1			
HIGH	7.5			NFS Shares World Readable	RPC	1			
MIXED	SSL (Multiple Issues)	General	28			
MIXED	ISC Bind (Multiple Issues)	DNS	5			

• UnrealIRCd Backdoor:

Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un aggressore di eseguire codice arbitrario sull'host interessato.

Risoluzione:

Scaricare nuovamente il software, verificarlo e reinstallarlo.

- **Password del server VNC: “Password”**

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password 'password'. Un aggressore remoto non autenticato potrebbe sfruttarla per prendere il controllo del sistema.

Soluzione

Proteggi il servizio VNC con una password forte.

- **Rilevamento del protocollo SSL versione 2 e 3:**

Il servizio remoto accetta connessioni crittografate tramite SSL 2.0 e/o SSL 3.0.

Queste versioni di SSL sono interessate da diversi difetti crittografici, un aggressore può sfruttare questi difetti per condurre attacchi man-in-the-middle o per decifrare le comunicazioni tra il servizio interessato e i client.

Soluzione

Utilizzare TLS anzichè SSL

- **Rilevamento backdoor della shell Bind:**

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un aggressore può utilizzarla connettendosi alla porta remota e inviando comandi direttamente.

Soluzione

Verificare se l'host remoto è stato compromesso e reinstallare il sistema, se necessario.

- **Debolezza del generatore di numeri casuali del pacchetto OpenSSH/OpenSSL di Debian (controllo SSL):**

Il certificato x509 remoto sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Un aggressore può facilmente ottenere la parte privata della chiave remota e usarla per decifrare la sessione remota o impostare un attacco man in the middle.

Soluzione

Considerare tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutto il materiale delle chiavi SSH, SSL dovrebbe essere rigenerato.