

192.168.1.103



Vulnerabilities

Total: 110

| SEVERITY | CVSS V3.0 | PLUGIN | NAME |
|----------|-----------|--------|-----------------------------------------------------------------------------|
| CRITICAL | 9.8 | 134862 | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| CRITICAL | 9.8 | 20007 | SSL Version 2 and 3 Protocol Detection |
| CRITICAL | 9.1 | 33447 | Multiple Vendor DNS Query ID Field Prediction Cache Poisoning |
| CRITICAL | 10.0 | 33850 | Unix Operating System Unsupported Version Detection |
| CRITICAL | 10.0* | 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICAL | 10.0* | 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| CRITICAL | 10.0* | 11356 | NFS Exported Share Information Disclosure |
| CRITICAL | 10.0* | 46882 | UnrealIRCd Backdoor Detection |
| CRITICAL | 10.0* | 61708 | VNC Server 'password' Password |
| CRITICAL | 10.0* | 10203 | rexecd Service Detection |
| HIGH | 8.6 | 136769 | ISC BIND Service Downgrade / Reflected DoS |
| HIGH | 7.5 | 42256 | NFS Shares World Readable |
| HIGH | 7.5 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 7.5 | 90509 | Samba Badlock Vulnerability |
| HIGH | 7.5* | 10205 | rlogin Service Detection |
| HIGH | 7.5* | 10245 | rsh Service Detection |
| MEDIUM | 6.8 | 78479 | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |

CRITICAL NFS Exported Share Information Disclosure:

è una vulnerabilità che riguarda il protocollo Network File System (NFS), un protocollo utilizzato per condividere file e directory su una rete. In particolare, questa vulnerabilità consente ad un attaccante di accedere alle informazioni condivise tramite NFS senza autorizzazione, inclusi i nomi delle condivisioni e gli indirizzi IP dei client che accedono a tali condivisioni. Per risolvere questa vulnerabilità, è necessario configurare correttamente le autorizzazioni di accesso alle condivisioni NFS, in modo che solo gli utenti autorizzati possano accedere alle informazioni condivise.

Comando usato per la risoluzione:

'sudo nano /etc/exports' e abbiamo aggiunto l'ip di kali

CRITICAL VNC Server 'password' Password:

è una vulnerabilità di sicurezza che riguarda il software di accesso remoto VNC (Virtual Network Computing). In particolare, questa vulnerabilità è causata dall'uso di password di accesso deboli o predefinite per il VNC Server. Tale vulnerabilità consente ad un attaccante di indovinare facilmente la password di accesso al VNC Server e di ottenere l'accesso non autorizzato al sistema remoto. Ciò può consentire all'attaccante di eseguire operazioni malevole sul sistema remoto, come il furto di dati, la modifica delle impostazioni di sistema o l'installazione di malware.

Per la risoluzione di questa vulnerabilità è necessario utilizzare password robuste e complesse per il VNC Server, evitando l'uso di password predefinite o facili da indovinare come "password" o "123456". Inoltre, è possibile configurare il software VNC per utilizzare l'autenticazione basata su certificati o altre tecniche di autenticazione più sicure.

Comando usato per la risoluzione:

'sudo iptables -A INPUT -p tcp --destination-port 5900 -j DROP'

CRITICAL rexecd Service Detection:

si riferisce alla rilevazione del servizio "rexecd" su una macchina virtuale o un dispositivo di rete durante una scansione di sicurezza. Questo servizio consente ad un utente remoto di eseguire comandi su una macchina remota. Tuttavia, poiché questo servizio è noto per essere vulnerabile a diversi tipi di attacchi, la sua presenza su una macchina può rappresentare un rischio per la sicurezza. Per risolvere questa vulnerabilità, è possibile disattivare il servizio "rexecd" o limitarne l'accesso solo a utenti autorizzati. Inoltre, è possibile utilizzare un firewall per bloccare l'accesso al servizio "rexecd" da fonti non autorizzate.

Comando usato per la risoluzione:

'sudo nano /etc/inetd.conf' e si modifica la configurazione del servizio per specificare l'elenco degli utenti autorizzati ad accedervi.

Risolvendo queste criticità si sono risolte in automatico anche le vulnerabilità *UnrealIRCd Backdoor Detection* (che permetteva all'attaccante di assumere il controllo del server compromesso e di accedere ai dati sensibili degli utenti) e *Multiple Vendor DNS Query ID Field Prediction Cache Poisoning* (che consentiva ad un attaccante di manipolare i dati di risoluzione dei nomi di dominio per indirizzare gli utenti verso siti malevoli o per bloccare l'accesso ai siti web legittimi).

Le 5 vulnerabilità rimanenti dopo la scansione (come si evince nella figura sottostante), si risolvono attraverso l'upgrade del sistema operativo.



Vulnerabilities

Total: 97

| SEVERITY | CVSS V3.0 | PLUGIN | NAME |
|----------|-----------|--------|---------------------------------------------------------------------------------------|
| CRITICAL | 9.8 | 134862 | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| CRITICAL | 9.8 | 20007 | SSL Version 2 and 3 Protocol Detection |
| CRITICAL | 10.0 | 33850 | Unix Operating System Unsupported Version Detection |
| CRITICAL | 10.0* | 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICAL | 10.0* | 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| HIGH | 8.6 | 136769 | ISC BIND Service Downgrade / Reflected DoS |
| HIGH | 7.5 | 42256 | NFS Shares World Readable |
| HIGH | 7.5 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 7.5 | 90509 | Samba Badlock Vulnerability |
| MEDIUM | 6.8 | 78479 | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |
| MEDIUM | 6.5 | 139915 | ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS |
| MEDIUM | 6.5 | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.5 | 57582 | SSL Self-Signed Certificate |
| MEDIUM | 6.5 | 104743 | TLS Version 1.0 Protocol Detection |
| MEDIUM | 5.9 | 136808 | ISC BIND Denial of Service |
| MEDIUM | 5.9 | 31705 | SSL Anonymous Cipher Suites Supported |
| MEDIUM | 5.9 | 89058 | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) |