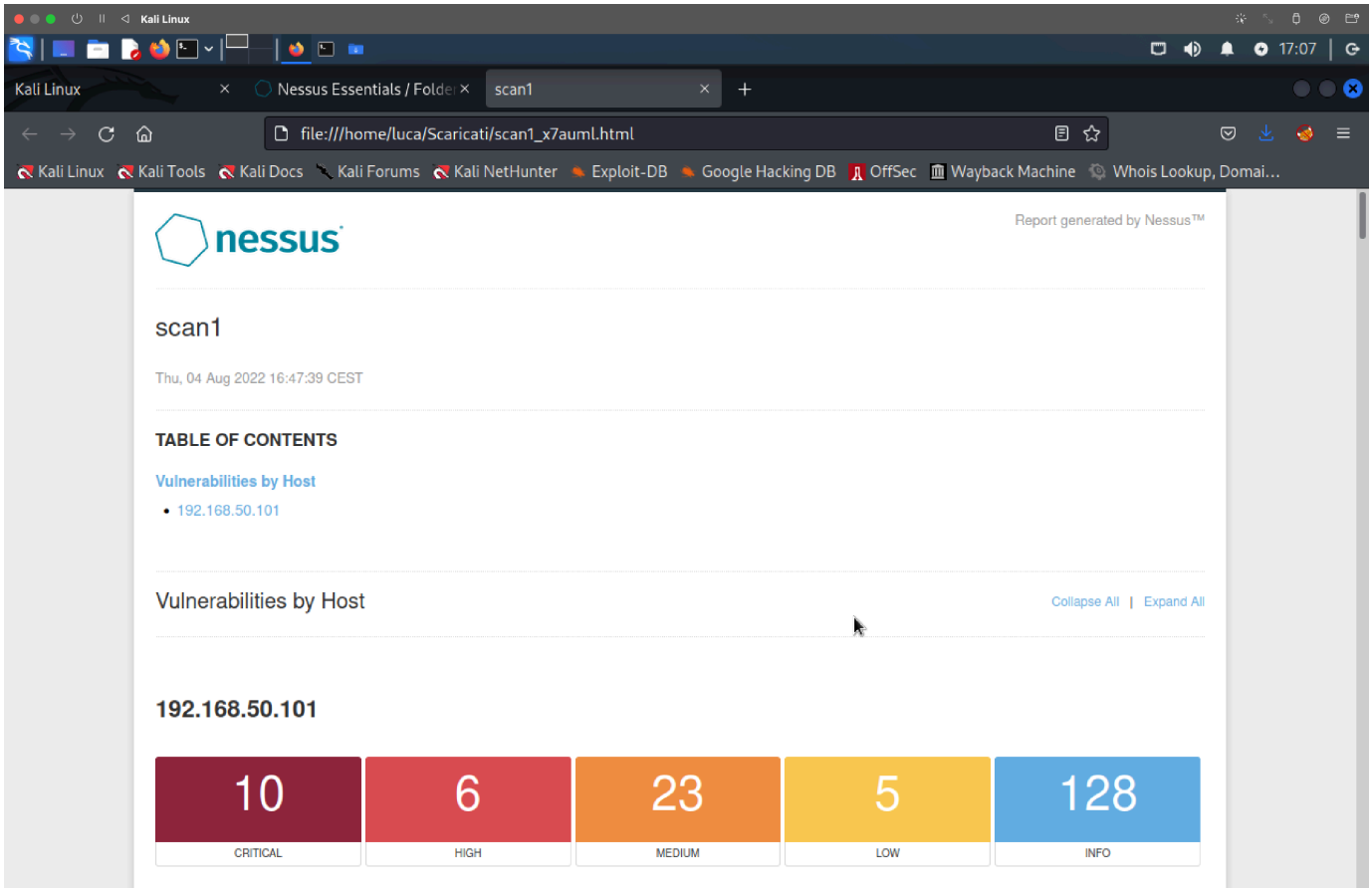
SCANSIONE DI METASPLOIT CON NESSUS ESSENTIALS VULNERABILITY SCANNER
REPORT CON SOLO LE VULNERABILITA CRITICAL, SE SI VOGLIONO AVERE PIU INFORMAZIONI RIVOLGERSI AL TECNICO DELL' AZIENDA CHE HA IL REPORT COMPLETO

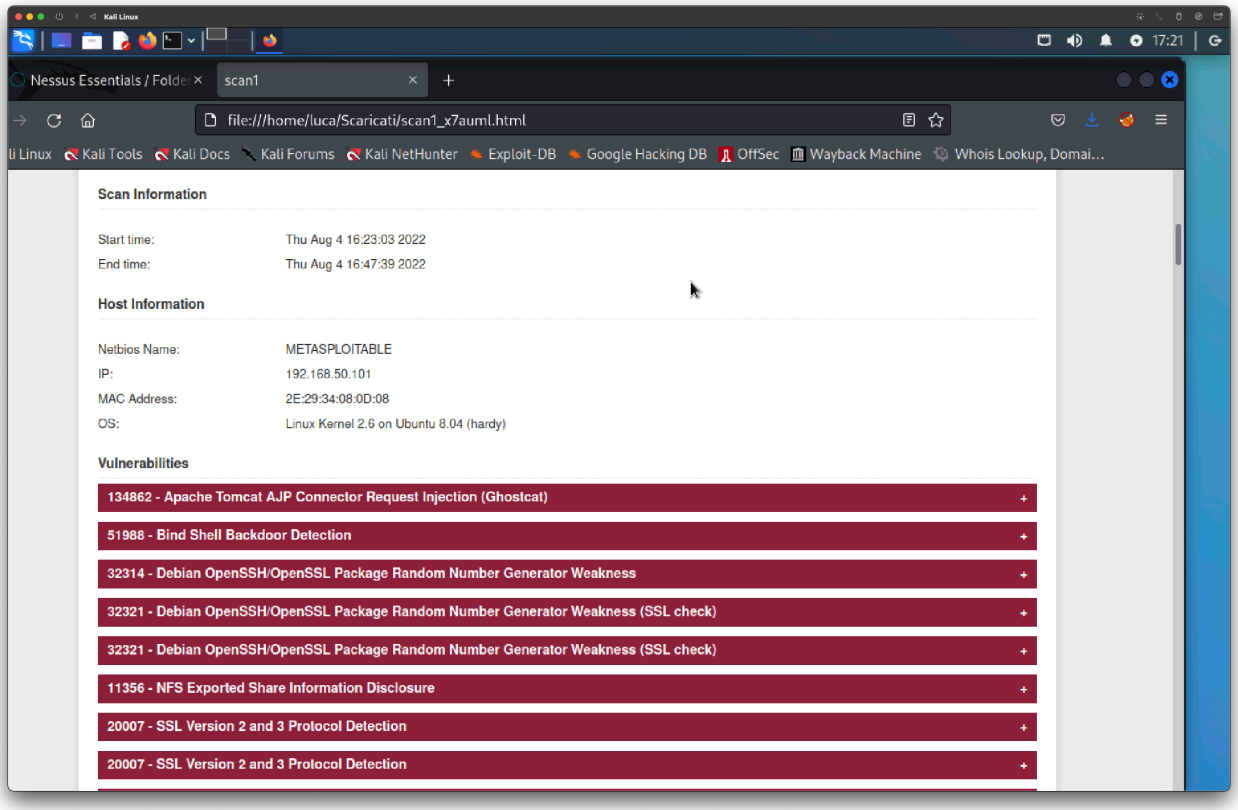


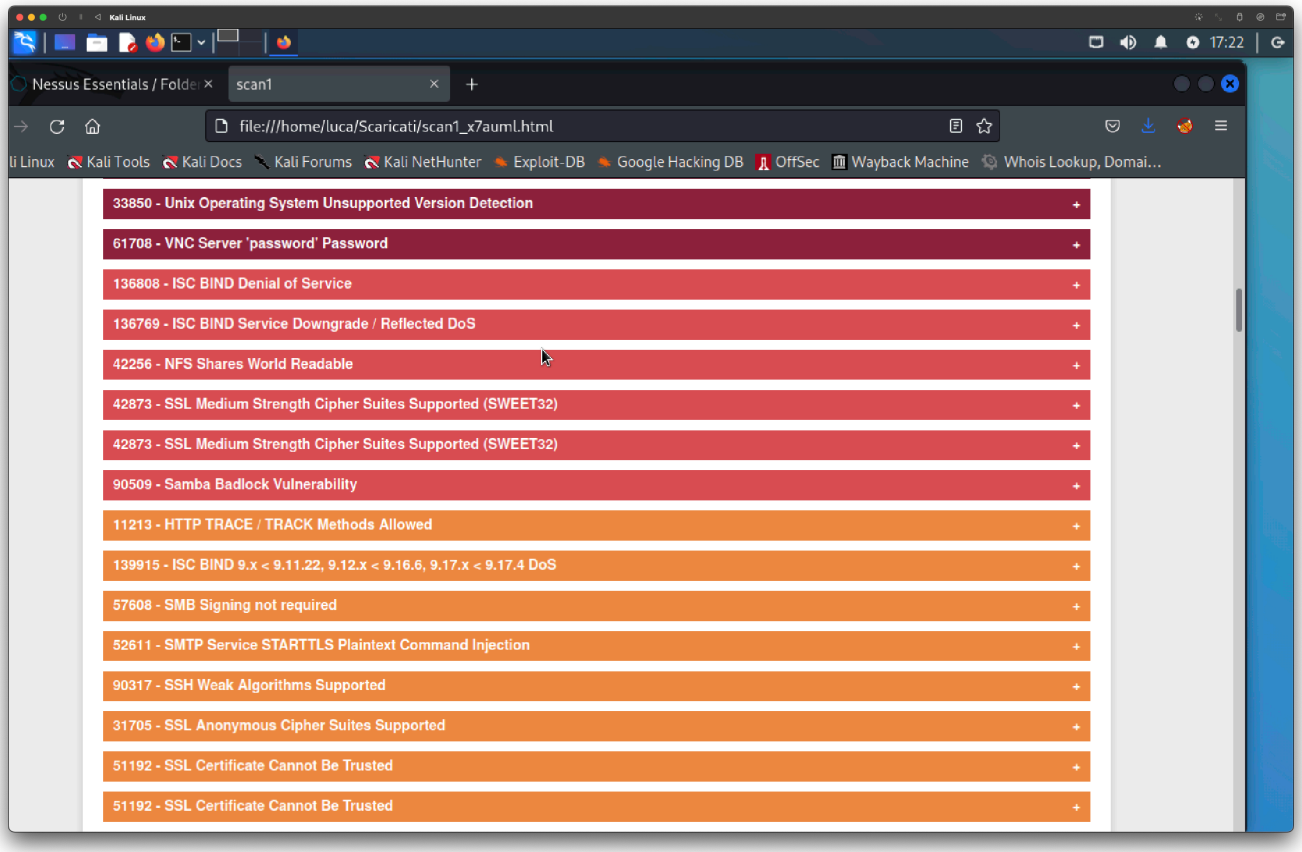
Come si può notare dalla foto sopra dopo la scansione sono state trovate:

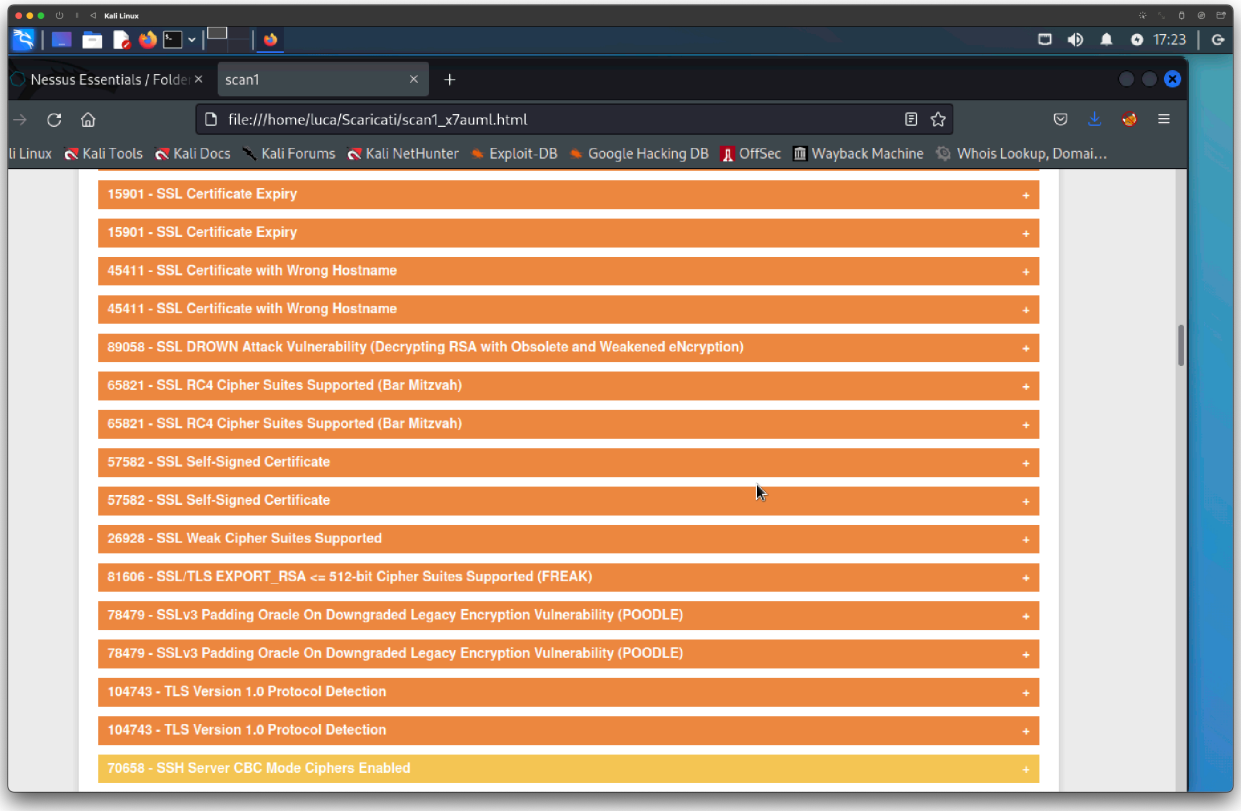
10 vulnerabilità CRITICAL

6 vulnerabilità HIGH

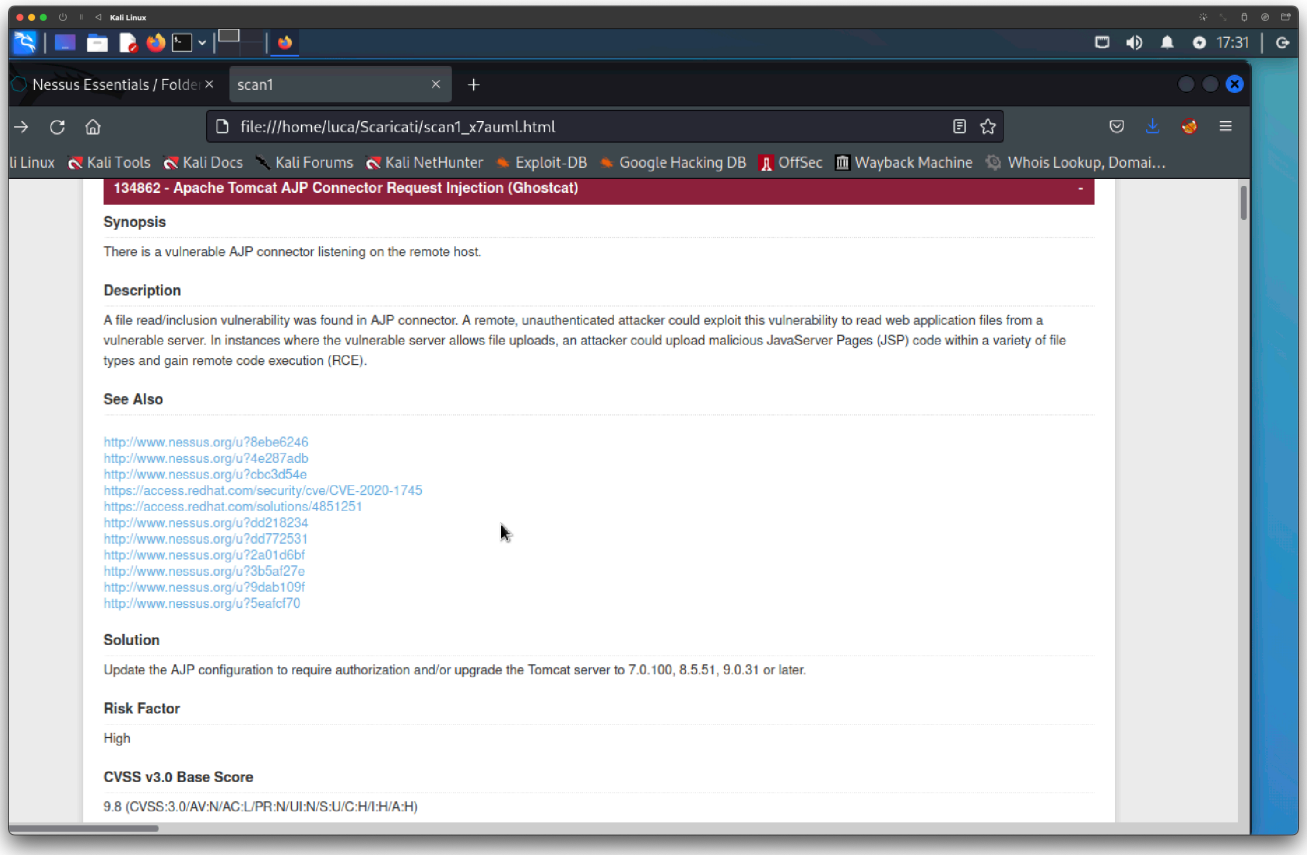
23 vulnerabilità MEDIUM




Kali Linux
17:22
Nessus Essentials / Folde
scan1
file:///home/luca/Scaricati/scan1_x7auml.html
li Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Wayback Machine
Whois Lookup, Domai...
33850 - Unix Operating System Unsupported Version Detection
61708 - VNC Server 'password' Password
136808 - ISC BIND Denial of Service
136769 - ISC BIND Service Downgrade / Reflected DoS
42256 - NFS Shares World Readable
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
90509 - Samba Badlock Vulnerability
11213 - HTTP TRACE / TRACK Methods Allowed
139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
57608 - SMB Signing not required
52611 - SMTP Service STARTTLS Plaintext Command Injection
90317 - SSH Weak Algorithms Supported
31705 - SSL Anonymous Cipher Suites Supported
51192 - SSL Certificate Cannot Be Trusted
51192 - SSL Certificate Cannot Be Trusted


Kali Linux
17:23
Nessus Essentials / Folde
scan1
file:///home/luca/Scaricati/scan1_x7auml.html
li Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Wayback Machine
Whois Lookup, Domai...
15901 - SSL Certificate Expiry
15901 - SSL Certificate Expiry
45411 - SSL Certificate with Wrong Hostname
45411 - SSL Certificate with Wrong Hostname
89058 - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
57582 - SSL Self-Signed Certificate
57582 - SSL Self-Signed Certificate
26928 - SSL Weak Cipher Suites Supported
81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
104743 - TLS Version 1.0 Protocol Detection
104743 - TLS Version 1.0 Protocol Detection
70658 - SSH Server CBC Mode Ciphers Enabled

DESCRIZIONE VULNERABILITA CRITICAL



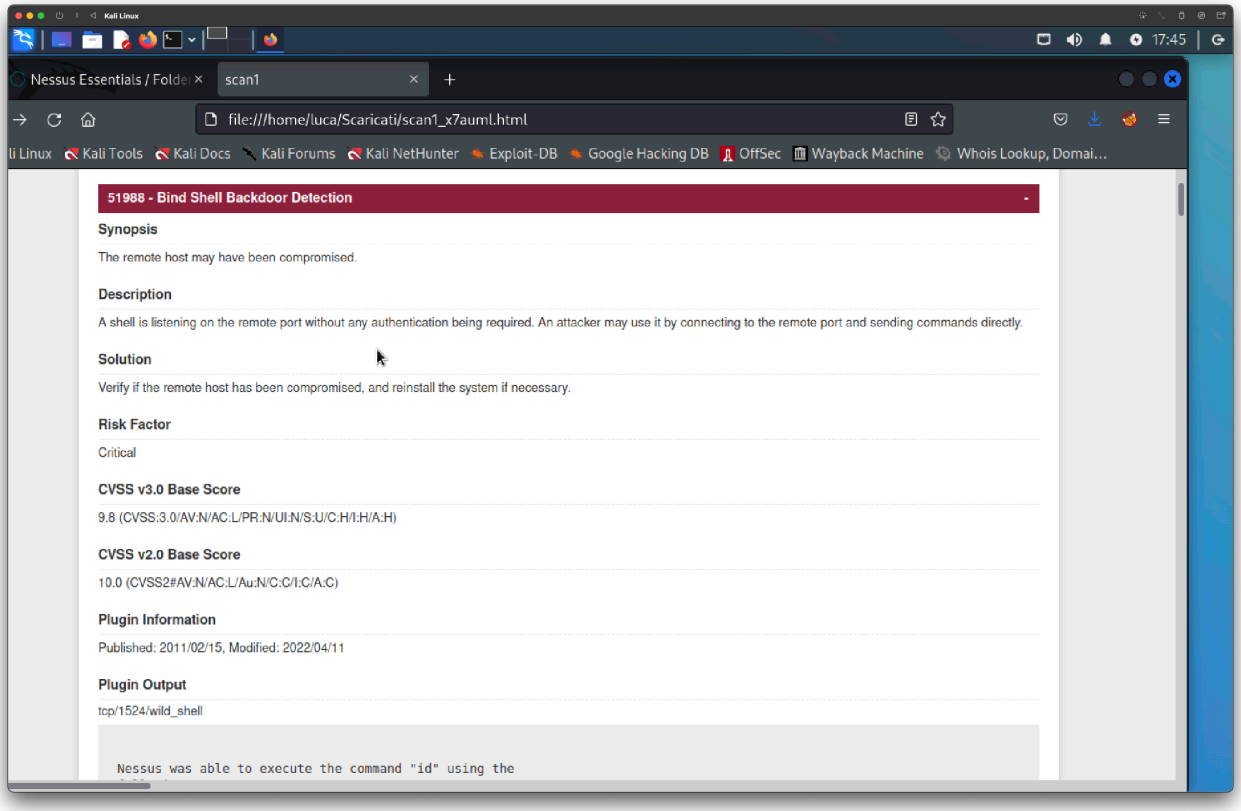
DESCRIZIONE VULNERABILITA

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JSP (JavaServer Pages) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

SOLUZIONE

Aggiorna la configurazione AJP per richiedere l'autorizzazione e/o aggiorna il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo.

PER MAGGIORI DETTAGLI GUARDA I SEGUENTI LINK

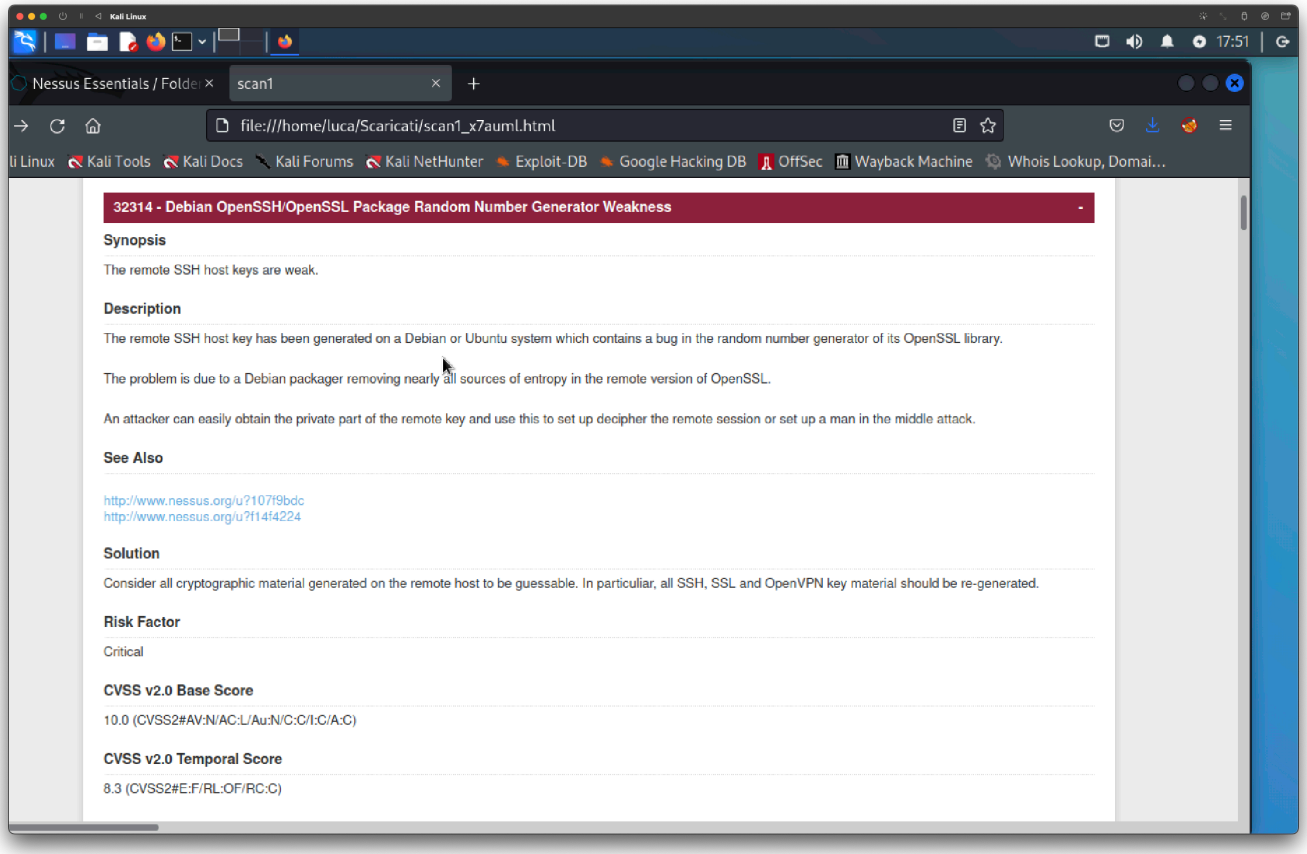


DESCRIZIONE VULNERABILITA

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

SOLUZIONE

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



DESCRIZIONE VULNERABILITA

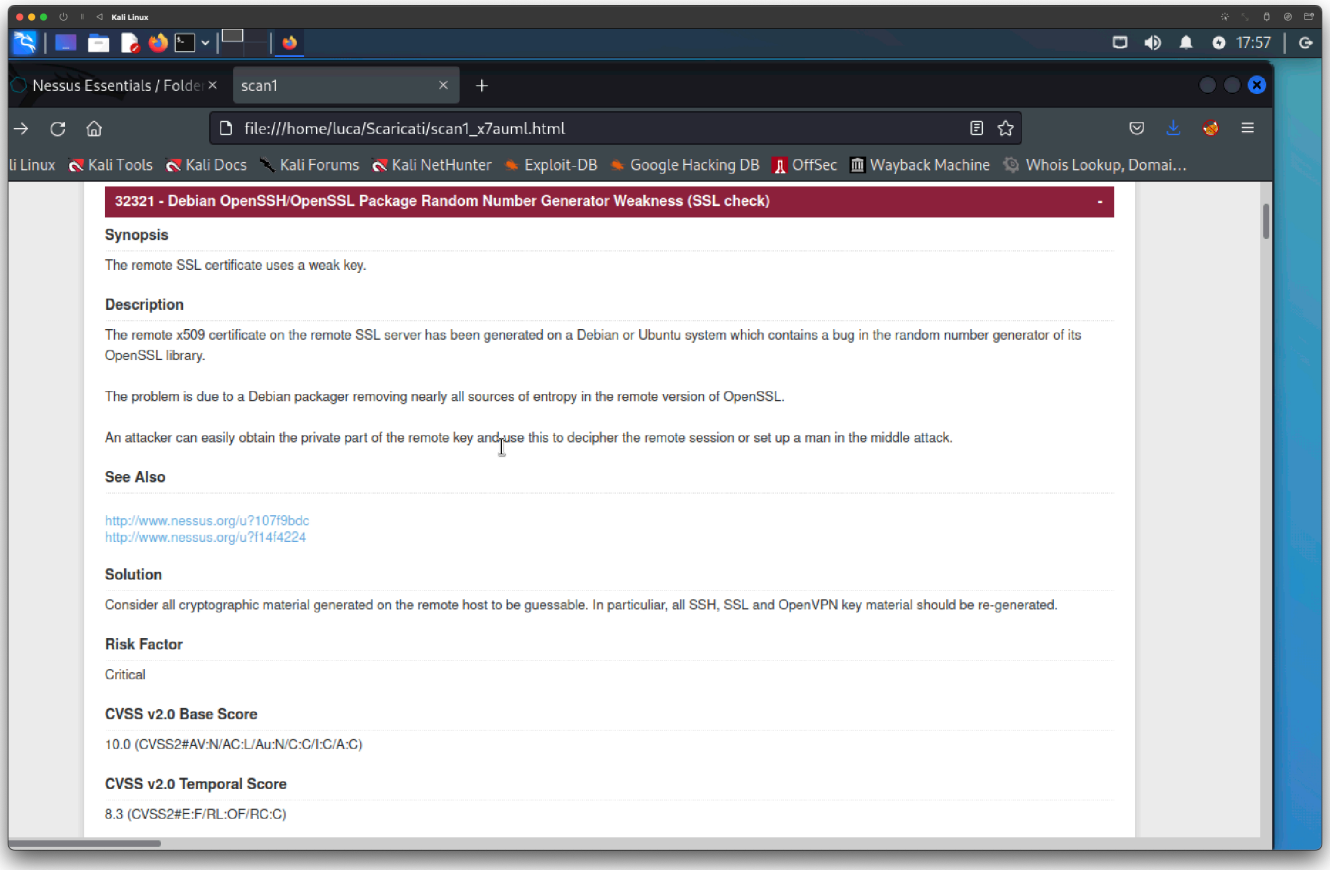
La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Il problema è dovuto a un packager Debian che rimuove quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per impostare la decifrazione della sessione remota o impostare un uomo nel mezzo dell'attacco.

SOLUZIONE

Considera che tutto il materiale crittografico generato sull'host remoto sia intuibile. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.



DESCRIZIONE VULNERABILITA

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.

Il problema è dovuto a un packager Debian che rimuove quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un uomo nel mezzo dell'attacco.

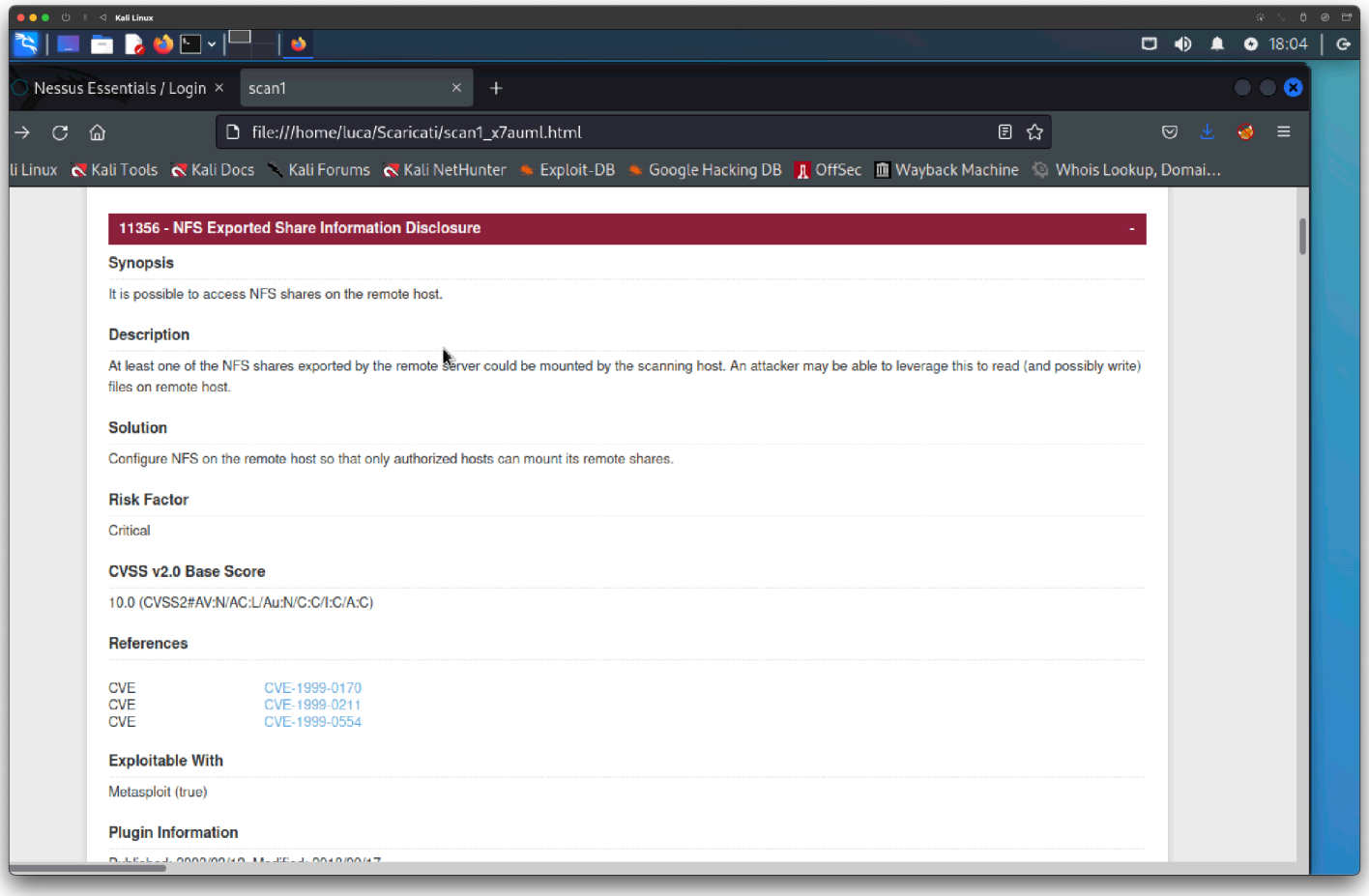
SOLUZIONE

Considera che tutto il materiale crittografico generato sull'host remoto sia intuibile. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

PER MAGGIORI DETTAGLI GUARDA I SEGUENTI LINK

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

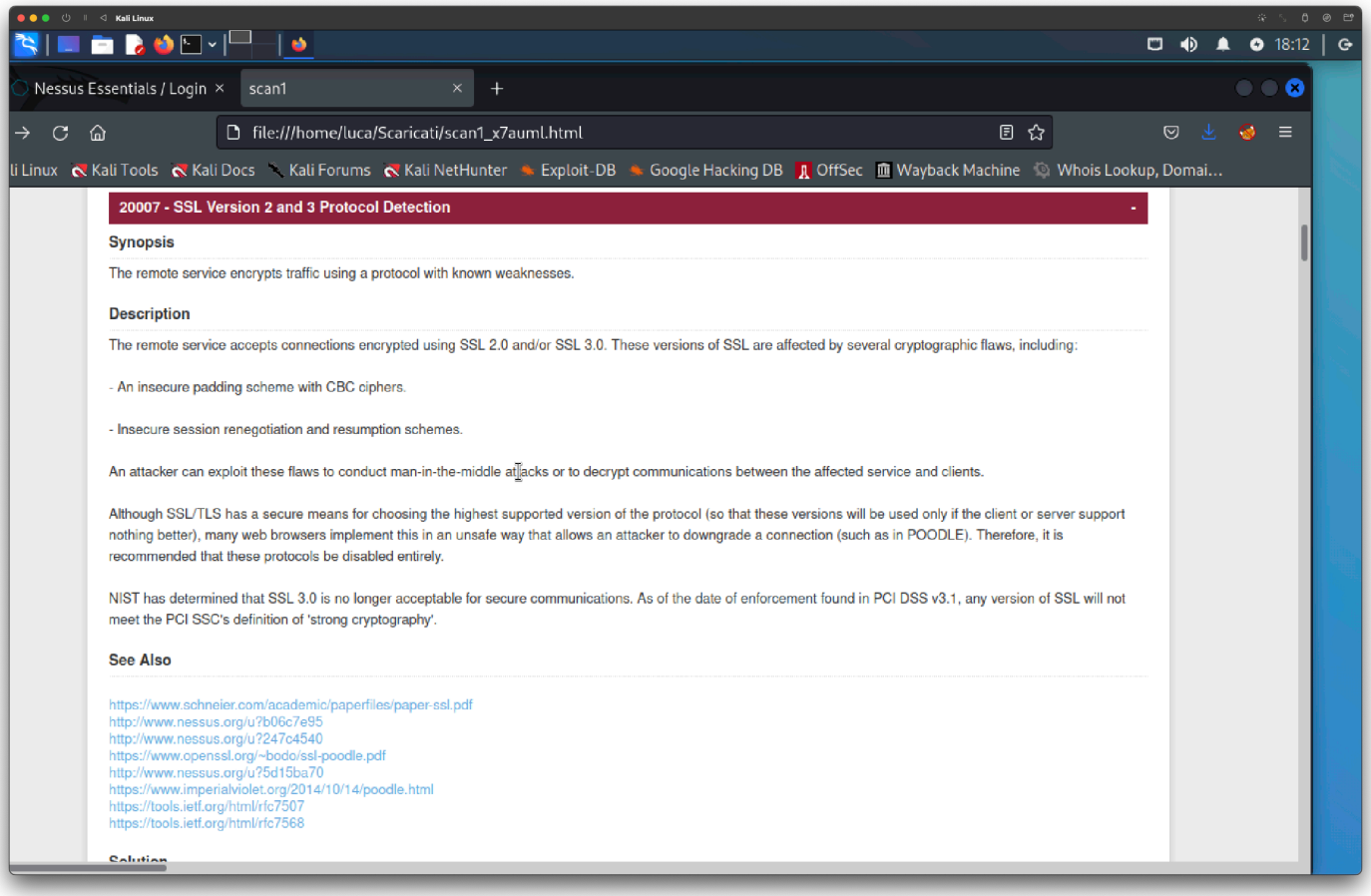


DESCRIZIONE VULNERABILITA

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttarlo per leggere (e possibilmente scrivere) file sull'host remoto.

SOLUZIONE

Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.



DESCRIZIONE VULNERABILITA

Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti di crittografia, tra cui:

- Uno schema di riempimento non sicuro con i codici CBC.

- Schemi di rinegoziazione e ripresa delle sessioni non sicuri.

Un utente malintenzionato può sfruttare questi difetti per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio interessato e i client.

Sebbene SSL/TLS disponga di un mezzo sicuro per scegliere la versione del protocollo più supportata (in modo che queste versioni vengano utilizzate solo se il client o il server non supportano nulla di meglio), molti browser Web lo implementano in un modo non sicuro che consente a un utente malintenzionato di eseguire il downgrade di una connessione (come in POODLE). Pertanto, si consiglia di disabilitare completamente questi protocolli.

Il NIST ha stabilito che SSL 3.0 non è più accettabile per comunicazioni sicure. A partire dalla data di applicazione trovata in PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di "crittografia avanzata" di PCI SSC.

SOLUZIONE

Consulta la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0.
Utilizzare invece TLS 1.2 (con suite di crittografia approvate) o versioni successive.

PER MAGGIORI DETTAGLI GUARDA I SEGUENTI LINK

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

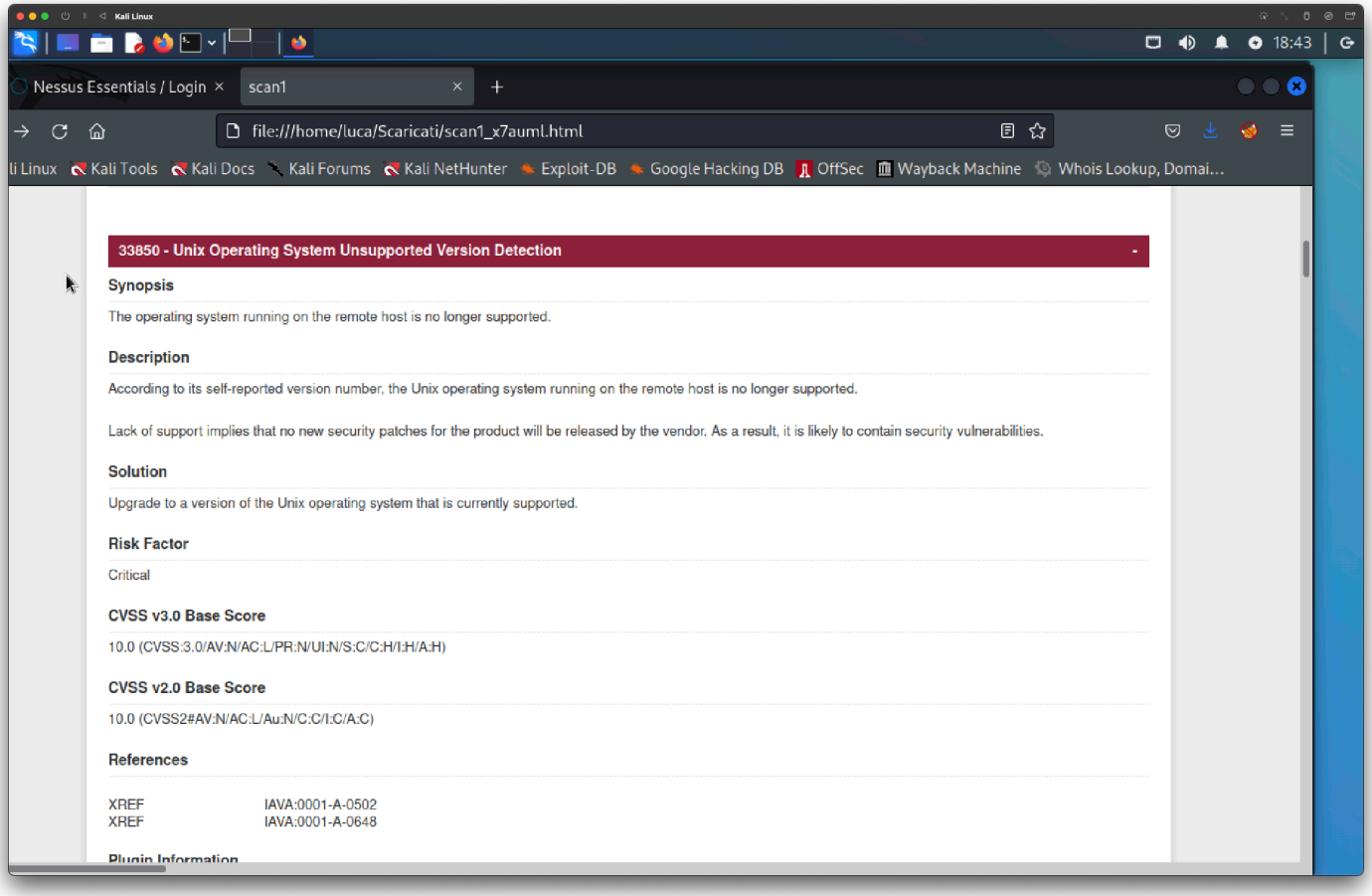
https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568



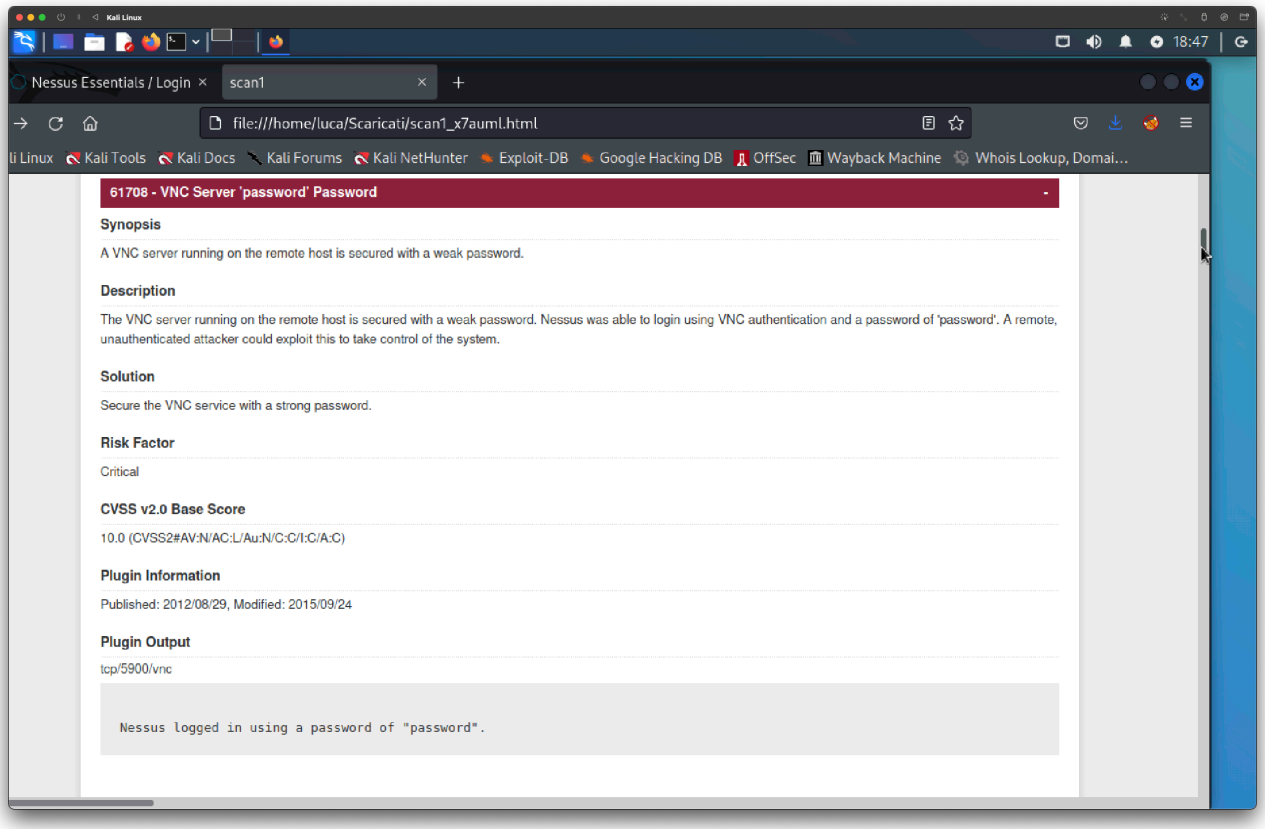
DESCRIZIONE VULNERABILITA

In base al numero di versione riportato automaticamente, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato.

La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

SOLUZIONE

Esegui l'aggiornamento a una versione del sistema operativo Unix attualmente supportata.



DESCRIZIONE VULNERABILITA

Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.

SOLUZIONE

Proteggi il servizio VNC con una password complessa.