Report S5L3
Vulnerability assessment

Obiettivo:

Effettuare un vulnerability scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni.
Ho utilizzato il basic network scan con la configurazione di rete predefinita.

Configurazione della scansione:

Ho configurato la scansione sulle porte comuni, in questo caso:

-range port 21-23

-port 25

-port 80

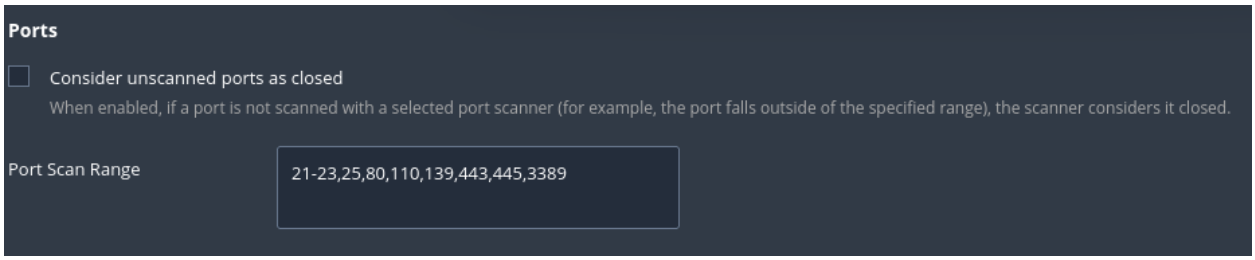
-port 110

-port 139

-port 443

-port 445

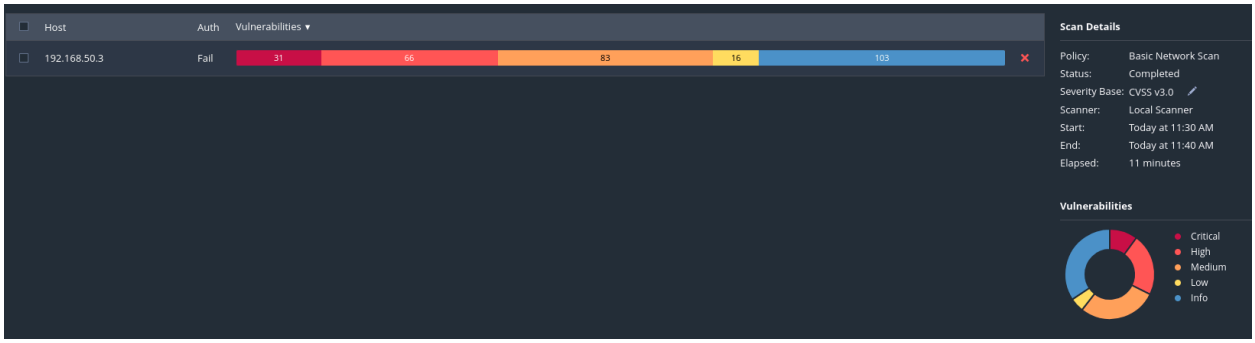
-port 3389



In assessment/accuracy ho selezionato l'opzione 'show potential false alarms', in report/processing 'report as much information as possible' e in advanced ho spuntato l'opzione 'vulnerability options' per scannerizzare le vulnerabilità non corrette.

Esecuzione della scansione:

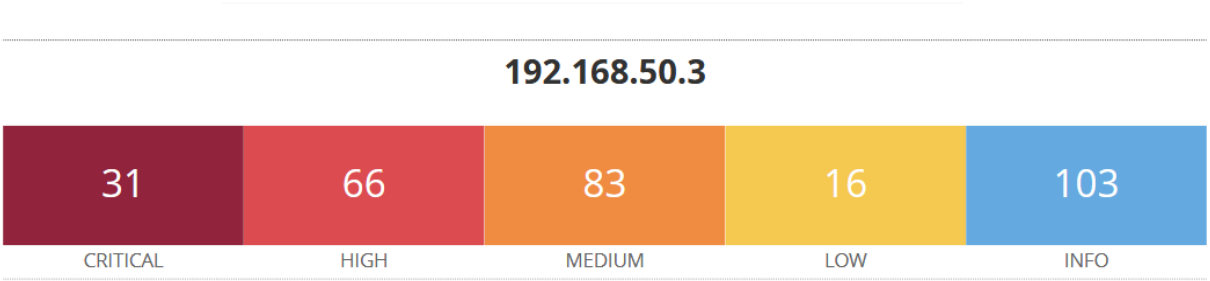
Una volta configurato tutto possiamo avviare la scansione cliccando sul triangolino sulla destra, durante la scansione vedremo in tempo reale le vulnerabilità trovate con tutti i dettagli e i link per avere maggiori informazioni riguardanti la stessa.



Analisi del report:

Una volta eseguita la scansione Nessus ci permette di scaricare un report più o meno dettagliato sulle vulnerabilità trovate, nel nostro caso abbiamo scelto “detailed vulnerabilities by host”.

A quel punto Nessus inizia a generare il report, una volta generato apre un file .pdf in un’altra scheda contenente il report.



Elenco vulnerabilità:

-Porta 22 (SSH):

1. OpenSSH < 7.2 Untrusted X11 Forwarding Fallback Security Bypass

Risk factor: critical

CVSS v3.0: 9.8

Descrizione:
Questa vulnerabilità permette a un attaccante di bypassare i meccanismi di sicurezza quando il forwarding X11 non trusted fallisce e viene fatto il fallback a trusted. Questo succede quando l'estensione SECURITY è disabilitata sul server X, permettendo connessioni X11 non affidabili che possono essere sfruttate per ottenere accesso non autorizzato.

Soluzione:
-Aggiornare OpenSSH alla versione 7.2 o superiore tramite il gestore pacchetti del sistema.
-Configurare il file sshd_config per disabilitare il forwarding X11 se non strettamente necessario.
-Implementare controlli di sicurezza aggiuntivi per le connessioni X11.
-Limitare l'uso del forwarding X11 solo a utenti autorizzati.

2. OpenSSH < 9.3p2 Vulnerability

Risk factor: critical

CVSS v3.0: 9.8

Descrizione:
Vulnerabilità critica nello ssh-agent quando viene utilizzato il supporto PKCS#11. Un attaccante può sfruttare librerie caricate tramite il supporto PKCS#11 per eseguire codice arbitrario in modalità remota, specialmente attraverso socket agent inoltrati. Questo rappresenta un rischio elevato per sistemi che utilizzano l'agent forwarding.

Soluzione:
-Aggiornare immediatamente OpenSSH alla versione 9.3p2 o superiore.
-Disabilitare l'agent forwarding nelle configurazioni se non essenziale.
-Implementare politiche restrittive per l'uso di PKCS#11.
-Limitare i privilegi dell'utente che esegue il servizio SSH.
-Monitorare le connessioni SSH per attività sospette.

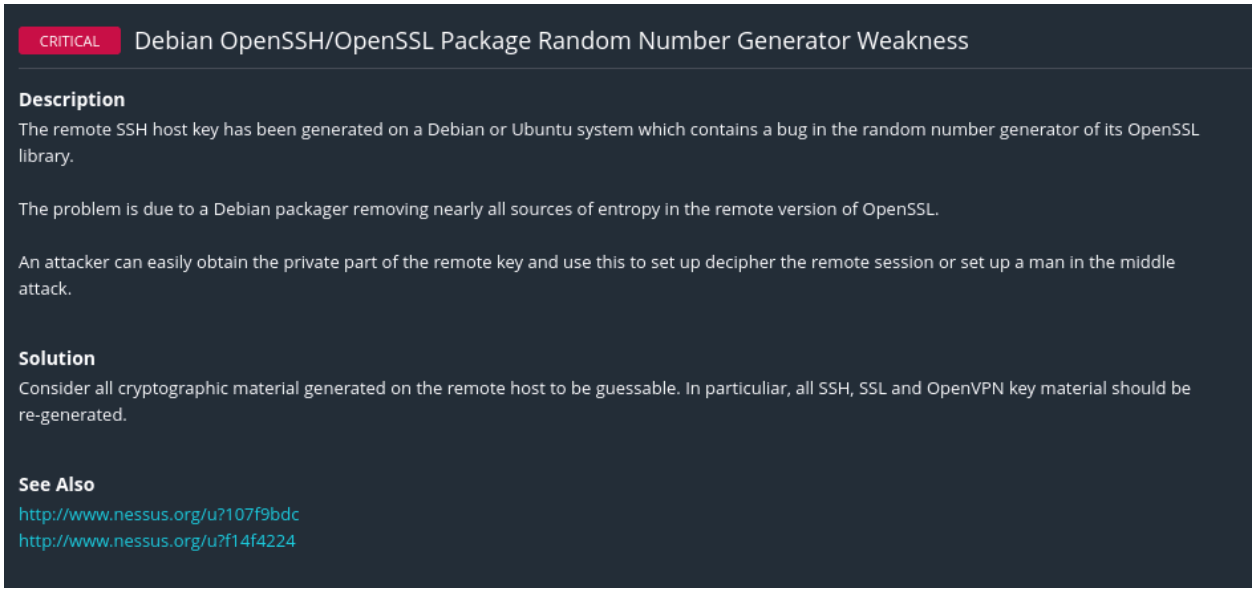
3. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Risk factor: critical

CVSS v2.0: 10.0

Descrizione:
Vulnerabilità storica ma critica nel generatore di numeri casuali di OpenSSL su sistemi Debian e Ubuntu. Il problema è causato dalla rimozione di quasi tutte le fonti di entropia, rendendo le chiavi crittografiche prevedibili e facilmente brute-forzabili. Questo compromette tutte le chiavi SSH e SSL generate sul sistema.

Soluzione:
-Rigenerare tutte le chiavi SSH host del sistema.
-Rigenerare tutti i certificati SSL/TLS.
-Sostituire tutte le chiavi di autenticazione utente SSH.
-Aggiornare OpenSSL alla versione più recente.
-Verificare che il sistema abbia sufficiente entropia disponibile.
-Implementare monitoraggio per identificare tentativi di sfruttamento.



PORTA 25 (SMTP)

1. SSL Version 2 and 3 Protocol Detection

Risk Factor: Critical

CVSS v3.0: 9.8

Descrizione:
Il servizio supporta versioni obsolete e vulnerabili del protocollo SSL (2.0 e 3.0). Queste versioni contengono vulnerabilità critiche come l'attacco POODLE che permette la decrittazione parziale del traffico, attacchi padding oracle, e meccanismi di renegotiation insicuri che possono portare a man-in-the-middle attack.

Soluzione:
-Disabilitare completamente SSL 2.0 e 3.0 in tutte le configurazioni.
-Utilizzare esclusivamente TLS 1.2 o superiore.
-Configurare cipher suite moderne e sicure.
-Implementare perfect forward secrecy.
-Aggiornare le librerie crittografiche.
-Eseguire test di verifica per confermare la disabilitazione.

PORTA 53 (DNS)

1. ISC BIND Unsupported Version Detection

Risk Factor: Critical

CVSS v3.0: 9.8

Descrizione:
La versione 9.4.2 di BIND è non supportata dal 2010 e contiene numerose vulnerabilità critiche tra cui denial of service, cache poisoning, e potenziali esecuzioni di codice remoto. Essendo EoL (End of Life), non riceve patch di sicurezza, esponendo il servizio DNS a multiple minacce.

Soluzione:
-Aggiornare BIND alla versione 9.16 o superiore.
-Configurare il servizio DNS per disabilitare la ricorsione pubblica.
-Implementare DNSSEC per la validazione delle risposte.
-Limitare le query DNS a reti autorizzate.
-Configurare response rate limiting.
-Implementare monitoring per query sospette.

PORTA 80 (HTTP)

1. Apache 2.2.x Multiple Critical Vulnerabilities

Risk Factor: Critical

CVSS v3.0: 9.8

Descrizione:

Apache versione 2.2.8 è affetto da multiple vulnerabilità critiche tra cui heap overflow nella libreria APR, attacchi TLS renegotiation, vulnerabilità in mod_proxy_ajp, e HTTP request smuggling. Queste vulnerabilità possono portare a denial of service, esecuzione di codice remoto, e bypass di controlli di sicurezza.

Soluzione:
-Migrare completamente ad Apache 2.4.x o superiore.
-Disabilitare moduli non necessari.
-Configurare header di sicurezza avanzati.
-Implementare limiti di richieste e timeout.
-Configurare correttamente i moduli proxy.
-Implementare Web Application Firewall.
-Abilitare logging esteso e monitoring.

2. PHP Unsupported Version Detection

Risk Factor: Critical

CVSS v3.0: 10.0

Descrizione:

PHP versione 5.2.4 è End of Life dal 2011 e contiene numerose vulnerabilità critiche tra cui remote code execution attraverso CGI argument injection, SQL injection, cross-site scripting, e multiple buffer overflow. Essendo non supportata, non riceve patch di sicurezza.

Soluzione:
-Migrare a PHP 8.1 o superiore.
-Rivedere tutto il codice applicativo per compatibilità.
-Disabilitare funzioni pericolose nel php.ini.
-Configurare direttive di sicurezza restrittive.
-Implementare input validation e output encoding.
-Utilizzare prepared statements per database.
-Implementare content security policy.

PORTA 445 (SMB)

1. Samba Multiple Critical Vulnerabilities

Risk Factor: Critical

CVSS v2.0: 10.0

Descrizione:
Samba versione 3.0.20 contiene multiple vulnerabilità critiche tra cui remote code execution (EternalRed), buffer overflow in nmbd, e vulnerabilità di autenticazione. Queste permettono a un attaccante di eseguire codice arbitrario, elevare privilegi, e compromettere completamente il sistema.

Soluzione:
-Aggiornare Samba alla versione 4.15 o superiore.
-Disabilitare protocolli SMB1 obsoleti.
-Implementare autenticazione strong.
-Limitare l'accesso per indirizzo IP.
-Configurare share permissions restrittive.
-Disabilitare account guest.
-Implementare monitoring per accessi sospetti.