Alessandro Azzolini
M3,W4,D1

INTRODUZIONE

In questo report sono mostrati i risultati del Vulnerability Assessment effettuato sulla macchina target 192.168.51.100 (Metasploitable). L'obiettivo era prendere confidenza con Nessus e analizzare le vulnerabilità di un sistema compromesso. Come richiesto dalla traccia, la scansione è stata configurata in modalità "Basic Network Scan" limitando l'analisi alle sole porte comuni (TCP). Questo ha permesso di individuare i servizi principali attivi e le relative criticità senza dover scansionare l'intero range di porte. Nel report verranno dettagliate le vulnerabilità trovate, classificate per gravità, accompagnate dalle relative soluzioni per la messa in sicurezza.

Target: 192.168.51.100
Tool: Nessus Essentials
Tipo di scansione: Basic Network Scan (Porte Comuni)ti

Canonical Ubuntu Linux SEoL (8.04.x) 10 CVSS

Gravità: Critica (CVSS 10.0)

Porta: 80/tcp (www)

Descrizione: Dall'analisi del sistema operativo in uso, si è riscontrato che la macchina esegue Canonical Ubuntu Linux versione 8.04.x. Questa versione è obsoleta e non è più mantenuta dal fornitore (End of Life). La mancanza di supporto ufficiale comporta l'assenza di nuove patch di sicurezza, lasciando il sistema esposto a qualsiasi vulnerabilità scoperta dopo la data di fine supporto.

Risoluzione: È indispensabile eseguire l'aggiornamento (upgrade) del sistema operativo a una versione di Ubuntu attualmente supportata (LTS) per garantire la ricezione degli aggiornamenti di sicurezza.

UnrealIRCd Backdoor Detection 10 CVSS

Gravità: Critica (CVSS 10.0)

Porta: 6667/TCP (irc)

Descrizione: Si è rilevato che il server IRC remoto utilizza una versione di UnrealIRCd contenente una backdoor. Questa vulnerabilità è particolarmente grave in quanto consente a un attaccante esterno di eseguire codice arbitrario sulla macchina (Remote Code Execution) sfruttando il servizio compromesso.

Risoluzione: È necessario scaricare nuovamente il software dal sito ufficiale. Si raccomanda di verificare l'integrità del pacchetto tramite i checksum (MD5/SHA1) pubblicati dal produttore prima di procedere alla reinstallazione

https://seclists.org/fulldisclosure/2010/Jun/277
https://seclists.org/fulldisclosure/2010/Jun/284
http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

VNC Server 'password' Password 10 CVSS

Gravità: Critica (CVSS 10.0)

Porta: 5900/TCP (vnc)

Descrizione: Il server VNC, utilizzato per l'amministrazione remota grafica, risulta protetto da una password debole. Dalla scansione è emerso che è possibile autenticarsi utilizzando semplicemente la password "password". Ciò permette a un attaccante remoto non autenticato di prendere il controllo del sistema.

Risoluzione: Si deve mettere in sicurezza il servizio VNC impostando una password forte e complessa.

SSL Version 2 and 3 Protocol Detection 9.8 CVSS

Gravità: Alta (CVSS 9.8)

Porte: 25/tcp (smtp), 5432/tcp (postgresql)

Descrizione: I servizi remoti accettano connessioni cifrate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni del protocollo sono affette da diversi difetti crittografici, tra cui schemi di padding insicuri con cifrari CBC e rinegoziazione della sessione insicura. Un attaccante può sfruttare tali falle per decifrare le comunicazioni. Inoltre, il NIST ha determinato che SSL 3.0 non è più accettabile per comunicazioni sicure e non soddisfa i requisiti PCI DSS.

Risoluzione: Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Si raccomanda di utilizzare TLS 1.2 o superiore.

Bind Shell Backdoor Detection 9.8 CVSS

Gravità: Critica (CVSS 9.8)

Porta: 1524/TCP (wild_shell)

Descrizione: È stata individuata una shell in ascolto sulla porta remota che non richiede alcuna autenticazione. Collegandosi a questa porta, è possibile inviare comandi direttamente al sistema con privilegi di root (uid=0), come dimostrato dall'output della scansione.

Risoluzione: La presenza di tale servizio indica che l'host potrebbe essere stato compromesso. Si consiglia di verificare l'integrità del sistema e, se necessario, procedere alla reinstallazione.

Apache Tomcat SEoL (<= 5.5.x) 10 CVSS

Gravità: Critica (CVSS 10.0)

Porta: 8180/tcp (www)

Descrizione: In base alla versione rilevata, l'installazione di Apache Tomcat risulta essere uguale o inferiore alla 5.5.x. Il software non è più mantenuto dal fornitore , essendo la data di "Security End of

Life" stimata al 30 settembre 2012. La mancanza di supporto implica che non verranno rilasciate nuove patch di sicurezza, esponendo il sistema a vulnerabilità.

Risoluzione: Si deve effettuare l'aggiornamento a una versione di Apache Tomcat attualmente supportata.

Debian OpenSSH/OpenSSL Package Random Number Generator 10 CVSS

Gravità: Critica (CVSS 10.0)

Porta: 22/tcp (ssh)

Descrizione: Si è rilevato che la chiave dell'host SSH remoto è stata generata su un sistema Debian o Ubuntu affetto da un grave bug nel generatore di numeri casuali della libreria OpenSSL. Il problema è causato dalla rimozione di quasi tutte le fonti di entropia da parte del pacchettizzatore Debian. Di conseguenza, un attaccante può facilmente ottenere la chiave privata remota e utilizzarla per decifrare la sessione o condurre attacchi "man-in-the-middle".

Risoluzione: Tutto il materiale crittografico generato sull'host deve essere considerato compromesso e indovinabile. È indispensabile rigenerare tutte le chiavi SSH, SSL e OpenVPN.

rsh Service Detection 7.5 CVSS / rlogin Service Detection 7.5 CVSS

Gravità: Alta (CVSS 7.5)

Porte: 513, 514

Descrizione: Sono stati rilevati i servizi rlogin e rsh attivi sull'host. Tali servizi sono considerati insicuri poiché trasmettono i dati (incluse le credenziali di accesso) in chiaro tra client e server, rendendo possibile l'intercettazione tramite sniffing.

Risoluzione: Si suggerisce di commentare le righe relative a 'login' e 'rsh' nel file di configurazione /etc/inetd.conf e riavviare il processo. In alternativa, si deve disabilitare il servizio e utilizzare esclusivamente SSH.

NFS Shares World Readable 7.5 CVSS

Gravità: Alta (CVSS 7.5)

Porta: 2049/tcp (rpc-nfs)

Descrizione: Il server NFS remoto esporta una o più condivisioni senza restrizioni di accesso basate su hostname o IP. Dalla scansione emerge che la condivisione / è accessibile a chiunque.

Risoluzione: È necessario configurare le restrizioni appropriate su tutte le condivisioni NFS.

Samba Badlock Vulnerability 7.5 CVSS

Gravità: Alta (CVSS 7.5)

Porta: 445/TCP (rpc-cifs)

Descrizione: La versione di Samba in esecuzione sulla macchina risulta affetta dalla vulnerabilità nota come "Badlock". Questo difetto nei protocolli SAM e LSAD espone al rischio di attacchi "Man-in-the-Middle", permettendo l'esecuzione di chiamate RPC arbitrarie nel contesto dell'utente intercettato.

Risoluzione: Si richiede l'aggiornamento di Samba alle versioni corrette (es. 4.2.11, 4.3.8 o successive).

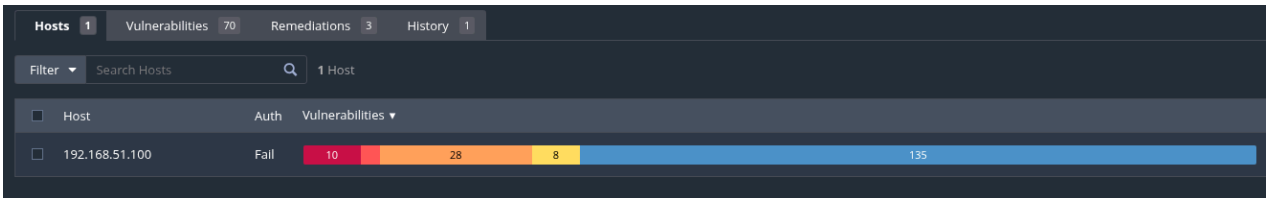
TLS Version 1.0 Protocol Detection 6.5 CVSS

Gravità: Media (CVSS 6.5)

Porta: 5432/tcp (postgresql)

Descrizione: Il servizio accetta connessioni cifrate tramite TLS 1.0, protocollo che presenta difetti di progettazione crittografica. Sebbene le implementazioni moderne mitighino alcuni problemi, versioni più recenti come TLS 1.2 e 1.3 dovrebbero essere preferite. Lo standard PCI DSS v3.2 richiede la disabilitazione totale di TLS 1.0.

Risoluzione: Abilitare il supporto per TLS 1.2 e 1.3 e disabilitare il supporto per TLS 1.0.



CONCLUSIONI

L'analisi effettuata tramite Nessus ha mostrato uno stato di sicurezza critico per la macchina target. Il sistema presenta numerose vulnerabilità di livello massimo (CVSS 10.0), causate principalmente da l'utilizzo di software ormai obsoleti e non più supportati e la presenza di configurazioni pericolose, come backdoor lasciate aperte e password di default. L'applicazione delle singole patch non sarebbe sufficiente a garantire la sicurezza: per un ripristino efficace, sarebbe necessario reinstallare il sistema operativo aggiornandolo a una versione supportata, chiudere i servizi non necessari e reimpostare tutte le credenziali di accesso.


license.
Vulnerabilities 70
Filter
Search Vulnerabilities
70 Vulnerabilities
Sev
CVSS
VPR
EPSS
Family
Count
CRITICAL 10.0 General 1
CRITICAL 10.0 * Backdoors 1
CRITICAL 10.0 * Gain a shell remotely 1
CRITICAL 9.8 Service detection 2
CRITICAL 9.8 Backdoors 1
MIXED ... ... Web Servers 4
CRITICAL ... ... Gain a shell remotely 3
HIGH 7.5 * Service detection 1
HIGH 7.5 * Service detection 1
MEDIUM 7.5 RPC 1
MEDIUM 7.5 General 1
MEDIUM 6.5 Service detection 2
MEDIUM 6.5 Misc. 1
MEDIUM 5.9 Misc. 1
MIXED ... ... General 26
MIXED ... ... Misc. 6
MIXED ... ... Web Servers 5
MIXED ... ... DNS 5
MIXED ... ... Misc. 2
MIXED ... ... Misc. 2
MIXED ... ... SMTP problems 2
LOW 5.9 Service detection 1
LOW 3.7 Misc. 1
LOW 2.6 * Service detection 1
LOW 2.1 * General 1
INFO ... ... Windows 7
INFO ... ... General 4
INFO ... ... DNS 3
st Details
192.168.51.100
Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
rt: December 11 at 10:23 AM
d: December 11 at 10:46 AM
psed: 23 minutes
Download
th: Fail
lnerabilities
Critical
High
Medium
Low
Info