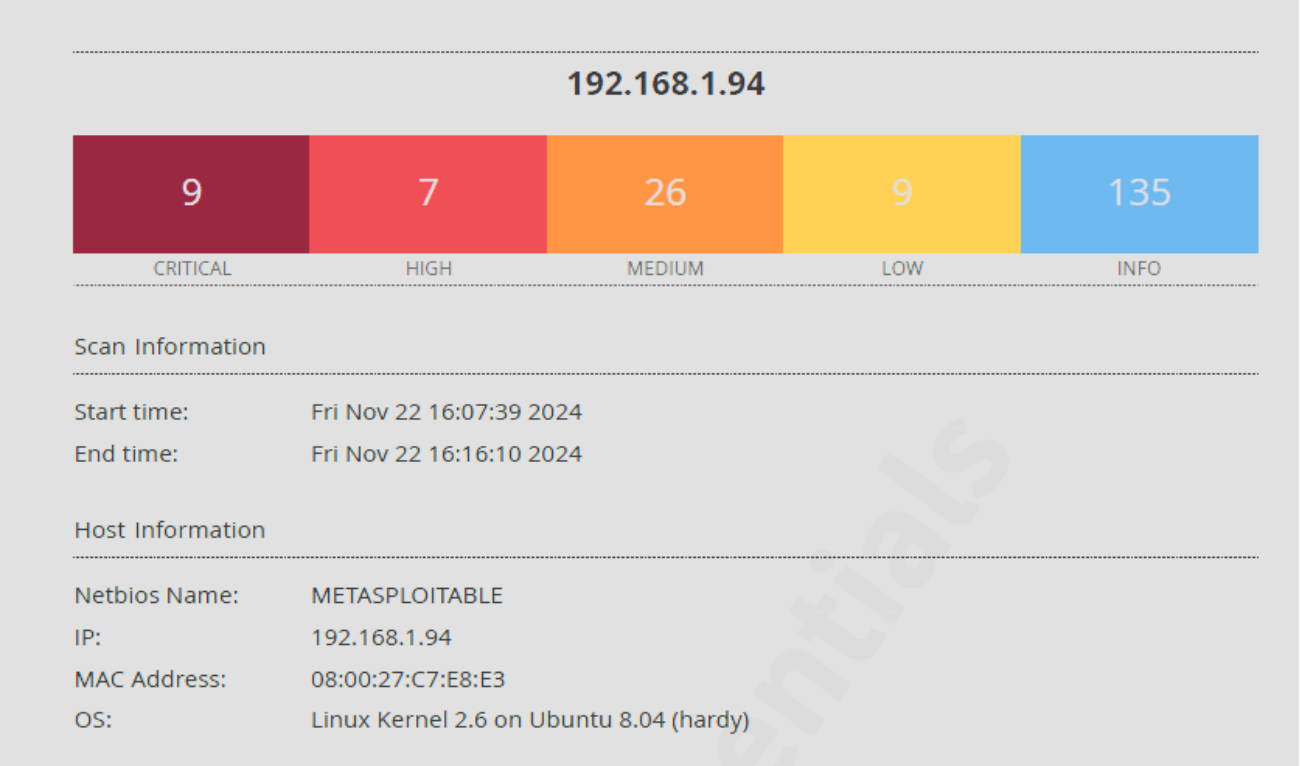
Analisi delle vulnerabilità e azioni di rimedio

Table of content

Introduzione

Scansione vulnerabilità Metasploitable con Nessus installato su macchina Kali. Entrambe le macchine sono sulla stessa rete

Grafico con tutte le vulnerabilità riscontrate



Dopo la scansione i risultati ci mostrano nove vulnerabilità critiche, si procederà con la risoluzione di quattro di esse.

Vulnerabilità scelte

61708 - VNC Server 'password' Password

Sinossi

Un server VNC in esecuzione sull'host remoto è protetto da una password debole.

Descrizione

Il server VNC in esecuzione sull'host remoto utilizza una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC con la password "password". Un attaccante remoto e non autenticato potrebbe sfruttare questa vulnerabilità per prendere il controllo del sistema.

Soluzione

Proteggi il servizio VNC con una password robusta.

Fattore di rischio

Critico

Punteggio CVSS v2.0 Base

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Informazioni sul plugin

Pubblicato: 29/08/2012, Modificato: 24/09/2015

Output del plugin

tcp/5900/vnc

46882 - UnrealIRCd Backdoor Detection

Sinossi

Il server IRC remoto contiene una backdoor.

Descrizione

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

Vedi anche:

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

Soluzione

Scarica nuovamente il software, verifica la sua integrità utilizzando gli MD5/SHA1 checksum pubblicati e reinstallalo.

Fattore di rischio

Critico

Punteggio VPR

7.4

Punteggio EPSS

0.6661

Punteggio CVSS v2.0 Base

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Sfruttabile con:

- 192.168.1.94 17
- CANVAS (true)
- Metasploit (true)

Informazioni sul plugin

Pubblicato: 14/06/2010, Modificato: 11/04/2022

Output del plugin

tcp/6667/irc

```
The remote IRC server is running as :

uid=0(root) gid=0(root)
```

51988 - Bind Shell Backdoor Detection

Sinossi

L'host remoto potrebbe essere stato compromesso.

Descrizione

Una shell sta ascoltando sulla porta remota senza richiedere alcuna autenticazione. Un attaccante potrebbe sfruttarla collegandosi alla porta remota e controllare il sistema.

Soluzione

Verifica se l'host remoto è stato compromesso e, se necessario, reinstalla il sistema.

Fattore di rischio

Critico

Punteggio CVSS v3.0 Base

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Punteggio CVSS v2.0 Base

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Informazioni sul plugin

Pubblicato: 15/02/2011, Modificato: 11/04/2022

Output del plugin

tcp/1524/wild_shell

```
Nessus was able to execute the command "id" using the
following request :


This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

------------------------------ snip ------------------------------
```

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Sinossi

Le chiavi host SSH remote sono deboli.

Descrizione

Le chiavi host SSH generate sull'host remoto sono state create su un sistema Debian o Ubuntu affetto da un bug nel generatore di numeri casuali della libreria OpenSSL.

Il problema è stato causato da un manutentore Debian che ha rimosso quasi tutte le fonti di entropia nella versione di OpenSSL utilizzata.

Un attaccante potrebbe facilmente ottenere la chiave privata del server remoto e usarla per decifrare le sessioni SSH o per organizzare un attacco *man-in-the-middle*.

Vedi anche:

- http://www.nessus.org/u?107f9bdc
- http://www.nessus.org/u?f14f4224

Soluzione

Considera tutto il materiale crittografico generato sull'host remoto come vulnerabile. In particolare, tutte le chiavi SSH, SSL e OpenVPN dovrebbero essere rigenerate.

Fattore di rischio

Critico

Punteggio VPR

5.1

Punteggio EPSS

0.1175

Punteggio CVSS v2.0 Base

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Punteggio CVSS v2.0 Temporale

8.3 (CVSS2#E:F/RL:OF/RC:C)

Riferimenti:

- **BID:** 29179
- **CVE:** CVE-2008-0166
- **XREF:** CWE:310

Sfruttabile con:

- Core Impact (true)

Informazioni sul plugin

Pubblicato: 14/05/2008, Modificato: 24/07/2024

Output del plugin

tcp/22/ssh

192.168.1.94