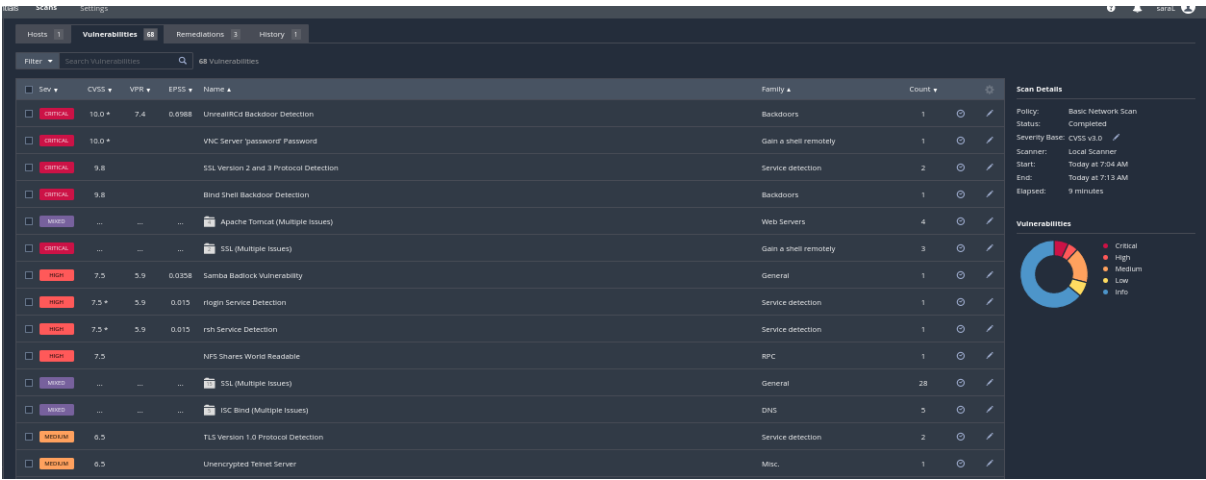


NESSUS PER SCANSIONARE LE VULNERABILITA':

Nel compito di oggi abbiamo installato Nessus su Kali e abbiamo fatto una scansione di un indirizzo IP target che era quello della nostra macchina di Metasploitable: 192.168.1.30.

In questa scansione quello che noi vogliamo sapere sono le vulnerabilità che ha Metasploitable, quindi impostando l'indirizzo IP e il range di porte (abbiamo scelto quelle comuni) abbiamo lanciato la scansione e questo è il risultato:



Come possiamo vedere dalla nostra scansione sono uscite fuori 68 vulnerabilità di diverso livello.

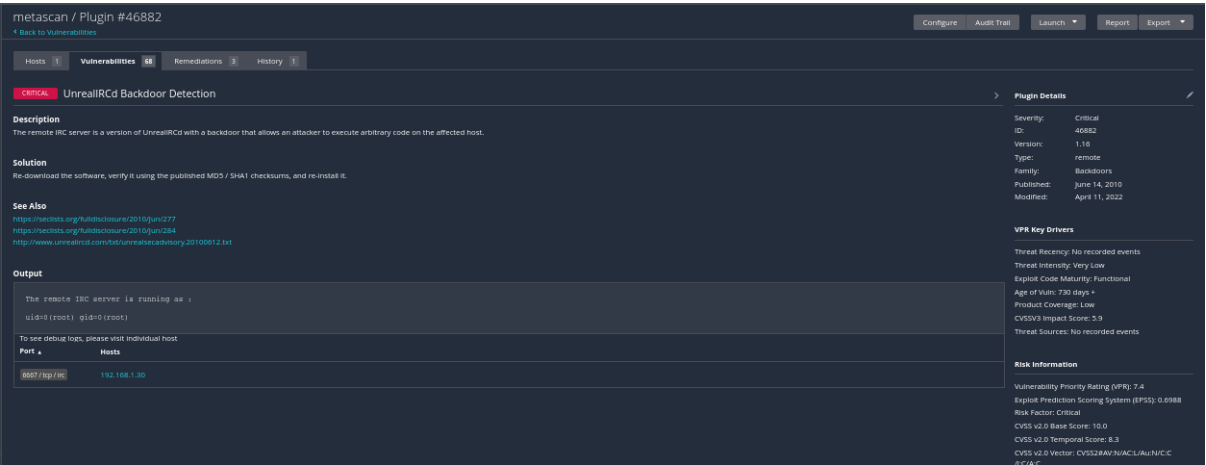
I livelli di vulnerabilità sono 5:

1. CRITICAL: come dice gia la parola è quella più pericolosa
2. HIGH: meno pericolosa della critical ma comunque ancora troppo alto il rischio
3. MEDIUM: rischio medio
4. LOW: basso rischio
5. INFO: questa vulnerabilità è abbastanza sicura anche se ovviamente non al 100%

Una volta finita la scansione possiamo scaricare in pdf un report, dove vengono elencate e spiegate tutte le vulnerabilità.

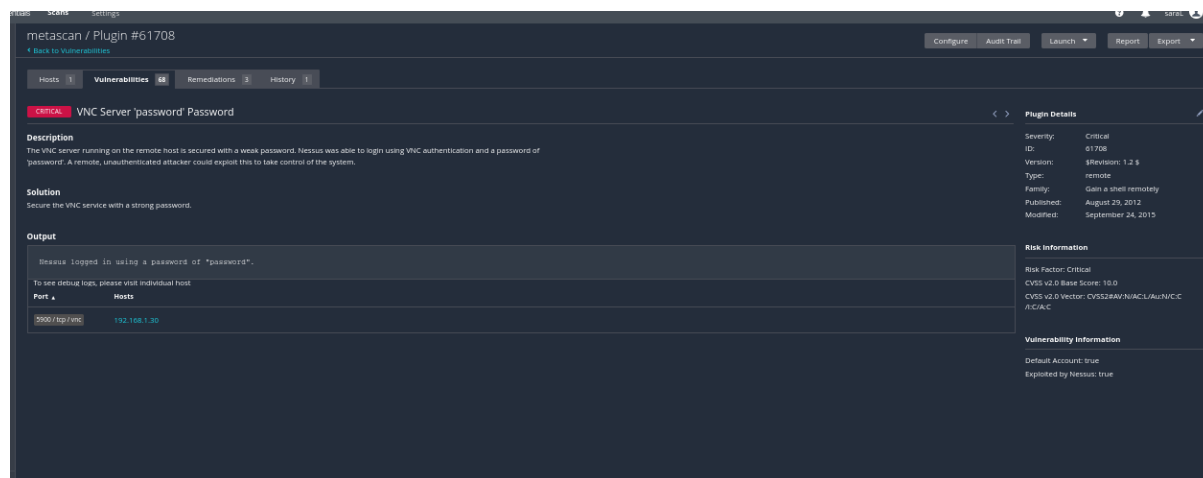
Fatto questo, oggi ne analizzeremo 5.

VULNERABILITA' 1: UnrealIRCd Backdoor Detection CRITICAL



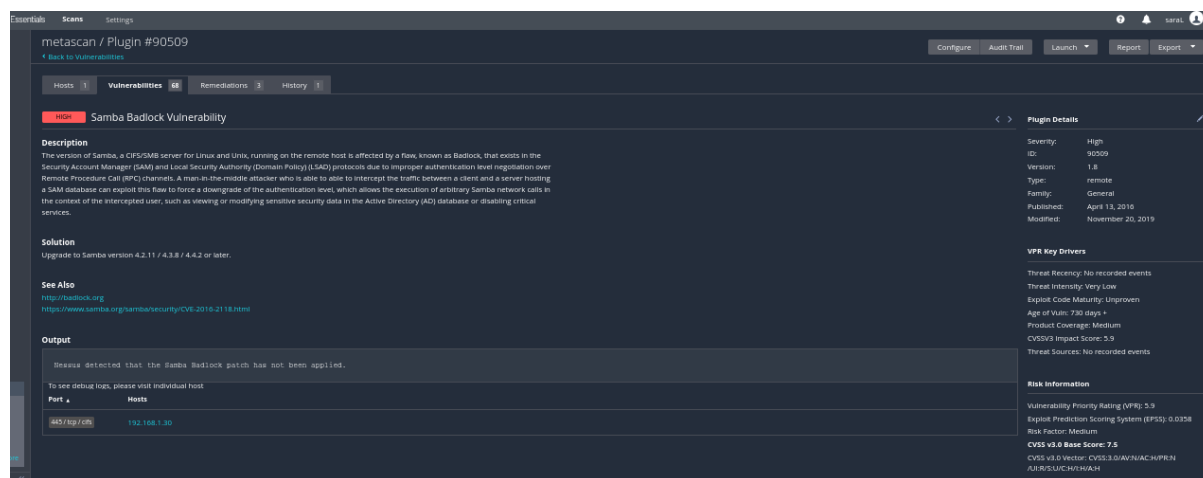
Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un utente malintenzionato di eseguire codice arbitrario sull'host interessato. Scaricare nuovamente il software, verificarlo utilizzando i checksum MD5/SHA1 pubblicati e reinstallarlo.

VULNERABILITA' 2: VNC Server 'password' Password **CRITICAL**



Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema. Proteggi il servizio VNC con una password complessa.

VULNERABILITA' 3: Samba Badlock Vulnerability **HIGH**



La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, presente nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione sui canali RPC (Remote Procedure Call). Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come visualizzare o modificare dati sensibili di sicurezza nel database di Active Directory (AD) o disabilitare servizi critici. Aggiorna alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.

VULNERABILITA' 4: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) **CRITICAL**

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 al fatto che un pacchettizzatore Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un aggressore può facilmente ottenere la parte privata della

chiave remota e usarla per decifrare la sessione remota o impostare un attacco man in the middle.Considerare tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

Hosts1Vulnerabilities46Remediations3History1

CriticalDebian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

>Plugin Details

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL, and OpenVPN key material should be re-generated.

See Also

<http://www.nessus.org/VT107956dc>
<http://www.nessus.org/VT144224>

Output

No output recorded.

To see debug logs, please visit individual host

Port	Hosts
5432/tcp/postgresql	192.168.1.30
25/tcp/smtp	192.168.1.30

Severity: Critical

ID: 22321

Version: 1.27

Type: remote

Family: Gain a shell remotely

Published: May 15, 2008

Modified: November 16, 2020

VPR Key Drivers

Threat Recency: 120 to 305 days

Threat Intensity: Very Low

Exploit Code Maturity: Functional

Age of Vm: 730 days

Product Coverage: Medium

CVSSv3 Impact Score: 3.6

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.1

Exploit Prediction Scoring System (EPSS): 0.1173

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Temporal Score: 8.3

CVSS v2.0 Vector: CVSS2:AV:N/AC:L/Au:N/C:C/RGAC

CVSS v2.0 Temporal Vector: CVSS2:AV:N/AC:L/Au:N/C:C

VULNERABILITA’ 5: Apache Tomcat SEoL (<= 5.5.x) **CRITICAL**

metascan / Plugin #171340

Back to Vulnerability Group

ConfigureAudit TrailLaunchReportExport

Hosts1Vulnerabilities46Remediations3History1

CriticalApache Tomcat SEoL (<= 5.5.x)

>Plugin Details

Description

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of Apache Tomcat that is currently supported.

See Also

<https://tomcat.apache.org/tomcat-5.5-eol.html>

Output

URL: http://Host: 003.homelnet.telecomitalia.it:8180/
Installed version: 5.5
Security End of Life: September 30, 2012
Time since Security End of Life (Est.): ~ 12 years

To see debug logs, please visit individual host

Port	Hosts
8180/tcp/www	192.168.1.30

Severity: Critical

ID: 171340

Version: 1.5

Type: combined

Family: Web Servers

Published: February 10, 2023

Modified: May 6, 2024

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score: 10.0

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PRN:A/SN:SC/HR:MAH

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2:AV:N/AC:L/Au:N/C:C/RGAC

Vulnerability Information

CPE: cpe:/a:apache:tomcat:5

Unsupported by vendor: true

In base alla sua versione, Apache Tomcat è inferiore o uguale a 5.5.x. Pertanto, non è più mantenuto dal suo fornitore o provider. La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, potrebbe contenere vulnerabilità di sicurezza. Esegui l'aggiornamento a una versione di Apache Tomcat attualmente supportata.