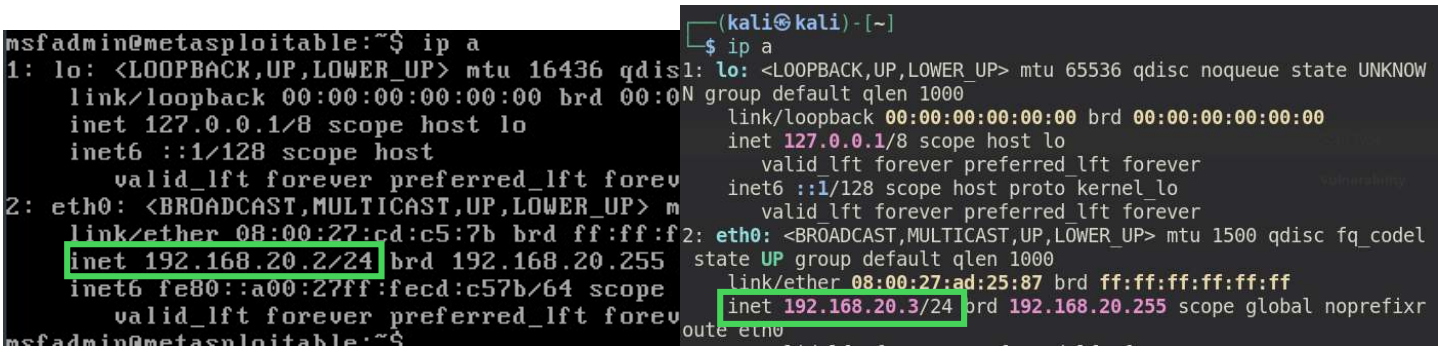
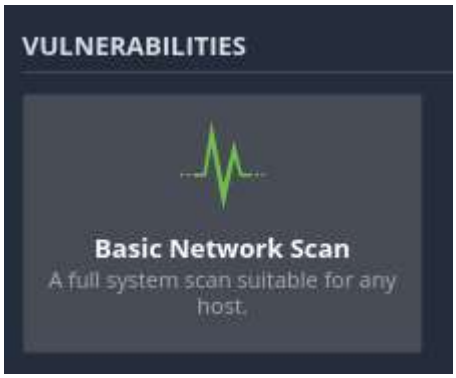
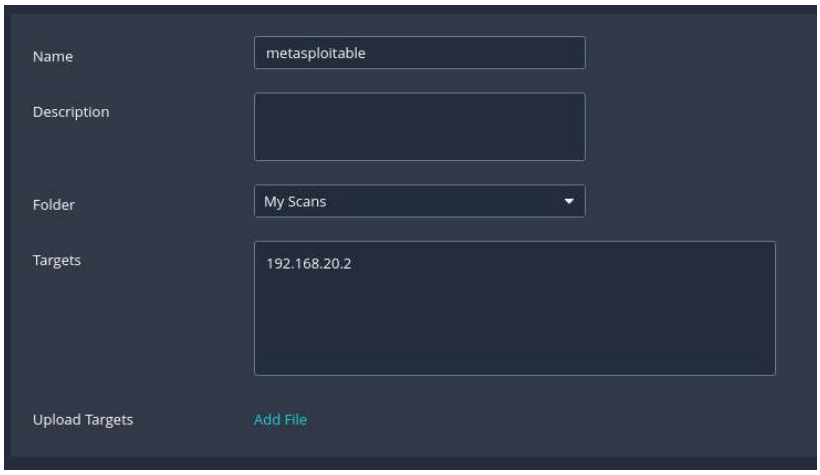
Come primo passo, sono andato a impostare gli indirizzii IP e i settaggi delle macchine in maniera tale che siano entrambe sotto la stessa rete interna:

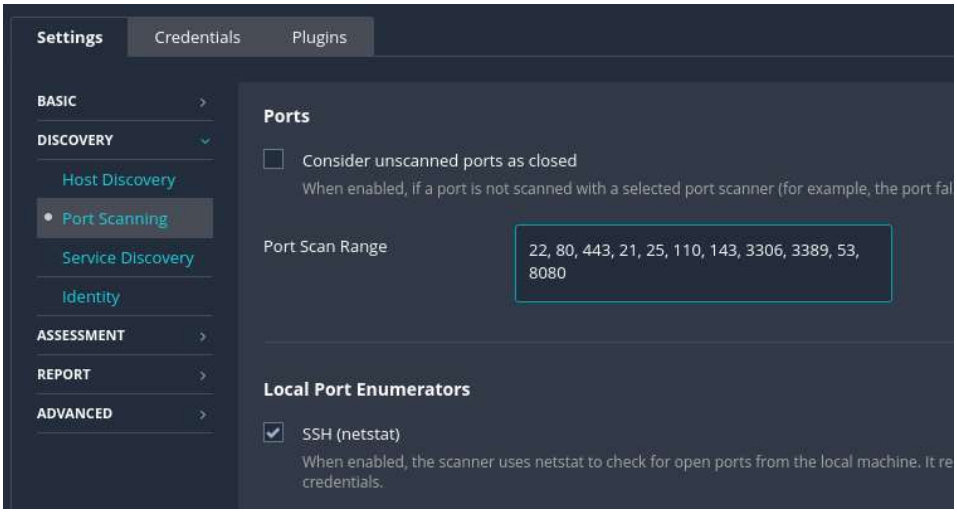


Adesso vado a fare la configurazione di nessus sul browser andando al link https://kali:8834 e andando a creare una nuova scansione cliccando Basic Network Scan poi inserisco il nome della scansione e l'indirizzo IP da scansionare.

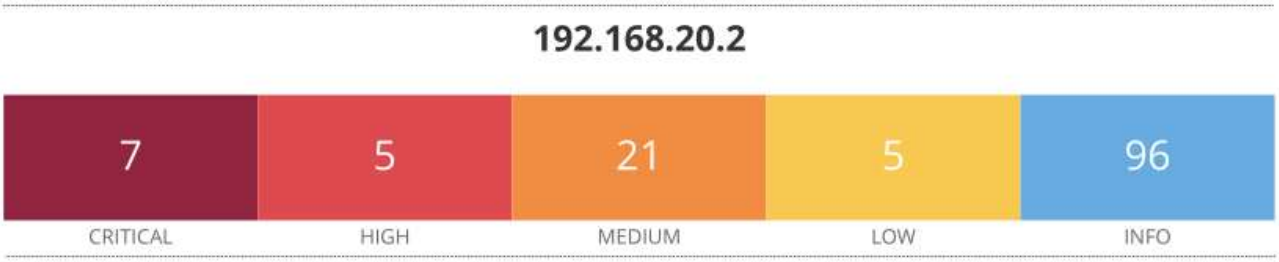




Per andare a impostare delle determinate porte per la scansione, nel menu a sinistra è presente una sezione "Discovery"con a sua volta una sezione "Port Scanning" dove sono andato ad impostare le specifiche porte da analizzare:



Successivamente è possibile far partire la scansione e analizzare il report che nessus darà in output.



Adesso vado ad analizzare le vulnerabilità critiche che nessus ha trovato all'interno della macchina metasploitable dato che le vulnerabilità più hanno un livello di criticità più è alta la priorità nel risolverle.

La prima vulnerabilità trovata parla di un file di lettura/inclusione che è stato trovato nel connettore AJP il quale, un utente remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni web.

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

There is a vulnerable AJP connector listening on the remote host.

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

La soluzione consigliata data è quella di aggiornare la configurazione AJP per richiedere l'autorizzazione o in alternativa aggiornare il server.

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

Risk Factor

High

la seconda vulnerabilità parla della chiave remota SSH generata su Debian o Ubuntu contiene un bug nel generatore di numeri casuali della libreria OpenSSL. Viene detto che tale problema è dovuto dal packager di Debian che rimuove tutte le risorse di entropia nelle versioni remote di OpenSSL.

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key 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 set up decipher the remote session or set up a man in the middle attack.

La soluzione consigliata è quella di considerare tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutto il materiale chiave SSH, SSL e OpenVPN dovrebbe essere rigenerato

Solution

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

Risk Factor

Critical

.

La terza vulnerabilità parla del servizio di crittografia tramite SSL 2.0 o SSL 3.0 che sono considerati affetti da difetti crittografici.

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

La soluzione consigliata è quella di disabilitare il sistema di crittografia SSL 2.0 o SSL 3.0

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

La quarta vulnerabilità parla del server VNC che è in esecuzione sull'host remoto è protetto da una password debole dato che nessus è riuscito ad accedervi con la password "password"

61708 - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

La soluzione consigliata è quella di inserire una password forte nel server VNC

Solution

Secure the VNC service with a strong password.