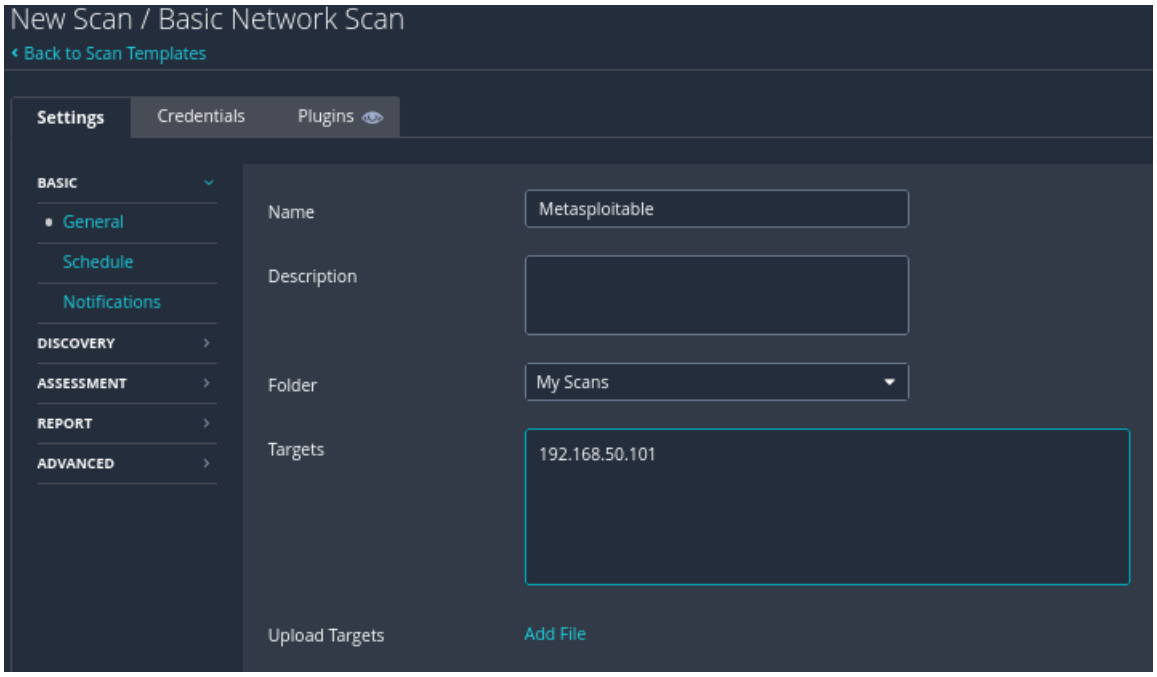
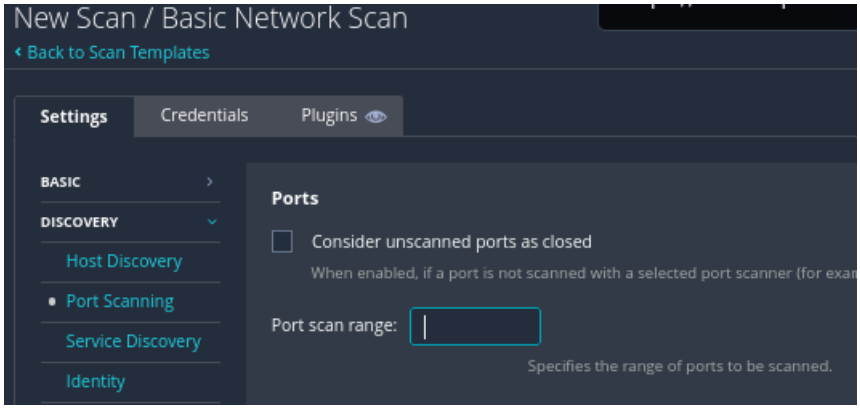
L'esercizio consiste nell'eseguire un Vulnerability Scanning sulla macchina Metasploit, focalizzandosi sulle porte comuni quali 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389.

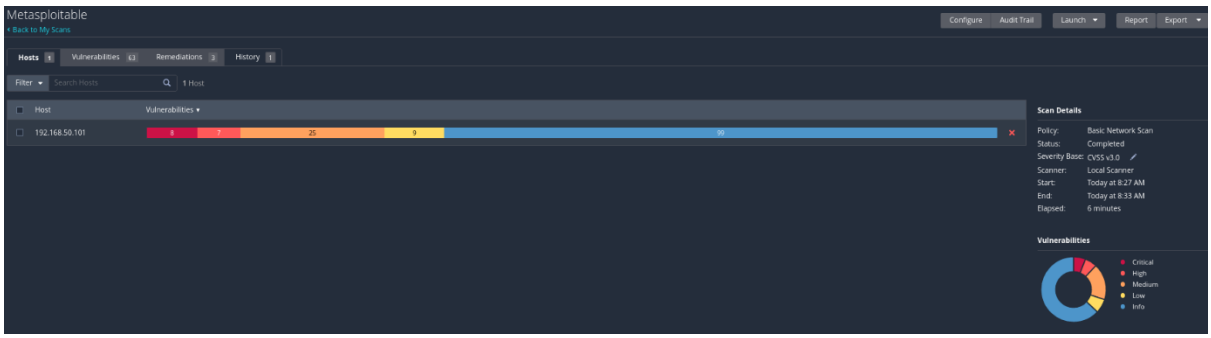
Per prima cosa servirà configurare i dettagli della scansione, scegliendo il tipo di scansione e aggiungendo nome e target da scansionare.



Le eventuali porte da scansionare vengono inserite durante la configurazione della scansione, scegliendo dal menù della sezione DISCOVERY l'opzione 'Custom' alla voce 'Scan Type'. Questo aprirà la possibilità di selezionare un range di porte dalla sottosezione 'Port Scanning'.



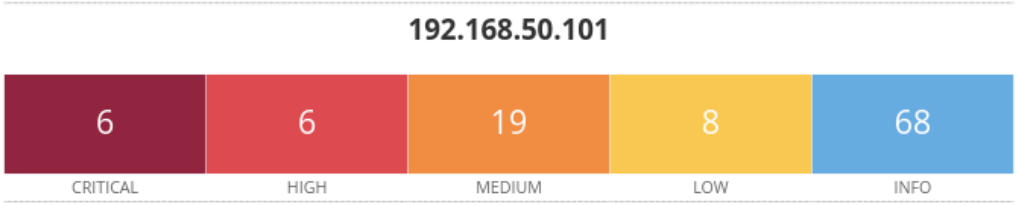
Una volta salvate le impostazioni è possibile iniziare lo scan, il quale restituirà i risultati dopo alcuni minuti.



Cliccando sulla scansione è possibile avere un'anteprima delle vulnerabilità trovate, con relativa criticità, punteggio CVSS, nome e altri dati.

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.6495	UnrealIRCd Bac...	Backdoors	1
CRITICAL	10.0 *			VNC Server 'pas...	Gain a shell remotely	1
CRITICAL	9.8	9.0	0.9728	Apache Tomcat ...	Web Servers	1
CRITICAL	9.8			SSL Version 2 a...	Service detection	2
CRITICAL	...	...	...	SSL (Multi...	Gain a shell remotely	3
HIGH	7.5	5.9	0.0358	Samba Badlock ...	General	1
HIGH	7.5 *	5.9	0.015	rlogin Service D...	Service detection	1
HIGH	7.5 *	5.9	0.015	rsh Service Det...	Service detection	1
HIGH	7.5			NFS Shares Wor...	RPC	1

A questo punto è possibile generare un report completo dei risultati dello scan che contiene una lista dettagliata di tutte le vulnerabilità trovate, insieme a link e risorse aggiuntive per effettuare analisi più approfondite.



Vulnerabilities Total: 107

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9728	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0*	5.1	0.0967	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.0967	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	7.4	0.6495	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0234	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0358	90509	Samba Badlock Vulnerability

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Language: English

CRITICAL Nessus Plugin ID 134862

Information | Dependencies | Dependents | Changelog

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).

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.

See Also

http://www.nessus.org/u?8ebe6246

Plugin Details

Severity: Critical

ID: 134862

File Name: ajp_lfi_ghostcat.nbin

Version: 1.46

Type: remote

Family: Web Servers

Published: 3/24/2020

Updated: 7/17/2024

Configuration: Enable thorough checks

Supported Sensors: Nessus