

S5L3

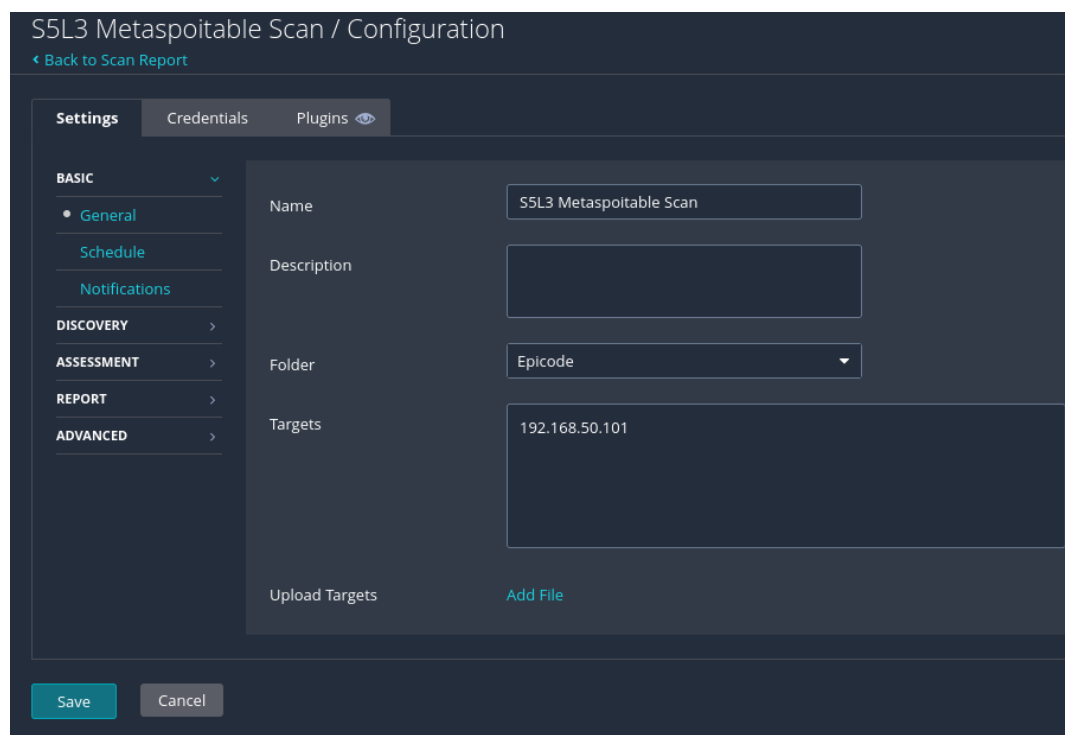
Obiettivo:

Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

Target: Metasploitable2. Porte scansionate: 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389. Tipo di scansione scelta: Basic Network Scan.

**(Nessus è uno strumento di vulnerabilità utilizzato per eseguire scansioni di sicurezza su sistemi e reti. Aiuta a identificare potenziali vulnerabilità, configurazioni errate e difetti di sicurezza, come porte aperte o software obsoleti. È uno dei più utilizzati scanner di vulnerabilità in ambito IT, grazie alla sua facilità d'uso e alle numerose opzioni di personalizzazione.)*

Per svolgere l'esercizio di oggi, abbiamo creato una scansione "custom" (personalizzata) tramite **Nessus***, questo tipo di scansione personalizzata ci permetterà di realizzare una scansione su misura per le nostre necessità. Nella prima parte di configurazione, troveremo una tab chiamata "Basic" che ci chiede delle informazioni iniziali, che ho compilato in questo modo:



The screenshot shows the 'S5L3 Metasploitable Scan / Configuration' window in Nessus. The 'Settings' tab is active, and the 'BASIC' section is expanded. The 'General' sub-tab is selected, showing the following fields:

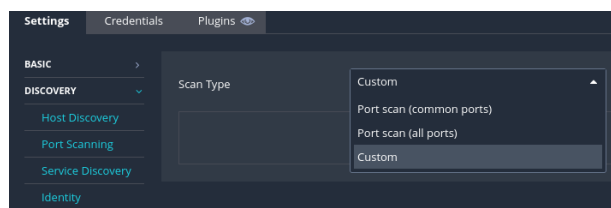
- Name:** S5L3 Metasploitable Scan
- Description:** (empty text box)
- Folder:** Epicode (selected from a dropdown menu)
- Targets:** 192.168.50.101 (entered in a text box)

At the bottom of the configuration window, there are 'Save' and 'Cancel' buttons. Below the 'Targets' field, there is an 'Upload Targets' button and a link to 'Add File'.

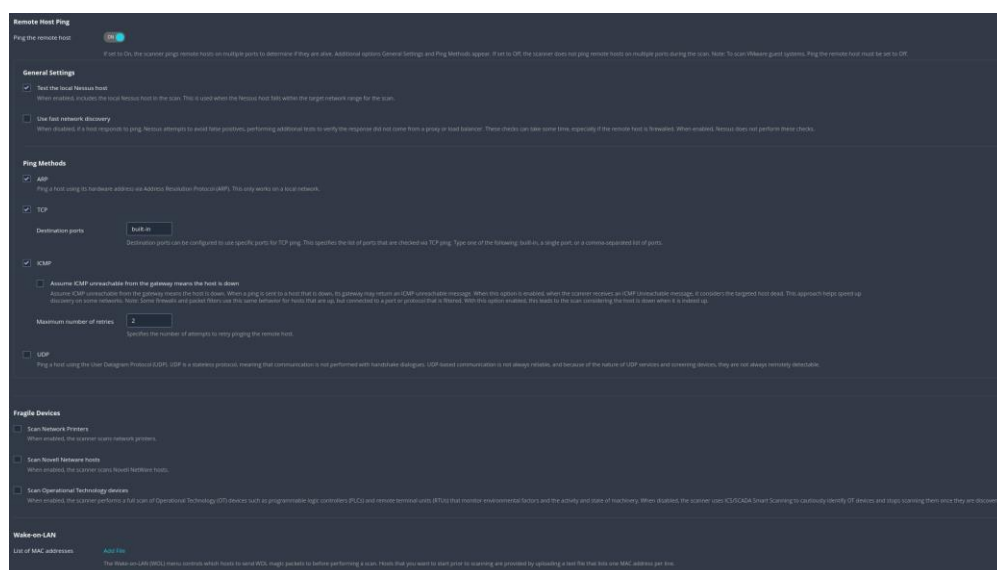
La tab "Schedule" permette di pianificare la scansione ad un orario preciso o giorno.

La tab "Notification" ci permette di ricevere una notifica tramite mail, ma per farlo bisogna configurare un SMTP Server.

Una volta configurata la tab **Basic** possiamo passare al **Discovery**, questa ci permette di scegliere il tipo di Scan che vogliamo effettuare e nel nostro caso scegliamo “Custom” perché vogliamo dare delle porte specifiche da controllare.



La **Host Discovery** di Nessus serve a identificare quali dispositivi (host) sono attivi e raggiungibili nella rete target. Prima di eseguire una scansione completa, Nessus utilizza questa fase per individuare gli indirizzi IP attivi, determinare quali host sono online e quindi determinare quali potrebbero essere vulnerabili a specifiche minacce. (Questa tab l’ho lasciata di default)



La **Port Scanning** in Nessus serve a identificare le porte aperte su un host o una rete, determinando quali servizi sono in ascolto su di esse. Durante questa fase, Nessus invia pacchetti a diverse porte e analizza le risposte per capire se una porta è aperta, chiusa o filtrata.

Questo processo è fondamentale per capire quali applicazioni o servizi sono attivi su un dispositivo, e per identificare eventuali porte vulnerabili che potrebbero essere sfruttate in un attacco. Nel nostro caso ho configurato il Port range, indicando le porte interessate.



Per questo esercizio mi sono soffermato a questa parte della configurazione e una volta date queste direttive a Nessus ho avviato la scansione; una volta completata la scansione, il programma genererà un elenco di vulnerabilità riscontrate con un tag che indica il livello di pericolo per la sicurezza, accompagnato da un colore identificativo.

Sev	CVE	VPO	EPSS	Name	Family	Count
CRITICAL	10.0			Canonical Ubuntu Linux Ssh, (B-D-4)	General	1
CRITICAL	10.0			VNC-Server Password Password	Gain a shell remotely	1
CRITICAL	9.8	8.9	0.9447	Apache Tomcat AJP Connector Request Injection (Gh0stcat)	Web Servers	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	—	—	—	SSL (Multiple Issues)	Gain a shell remotely	3
CRITICAL	7.5	5.9	0.8111	Samba Bedrock Vulnerability	General	1
CRITICAL	7.5			NFS Shares World Readable	RPC	1
CRITICAL	—	—	—	SSL (Multiple Issues)	General	28
CRITICAL	—	—	—	ISC Bind (Multiple Issues)	DNS	5
CRITICAL	6.9			TLS Version 1.0 Protocol Detection	Service detection	2
CRITICAL	5.9	4.4	0.827	SSL Anonymous Cipher Suites Supported	Service detection	1
CRITICAL	5.9	3.6	0.9635	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened ecryptons)	Misc.	1
CRITICAL	—	—	—	SSH (Multiple Issues)	Misc.	6
CRITICAL	—	—	—	DNS (Multiple Issues)	DNS	4
CRITICAL	—	—	—	HTTP (Multiple Issues)	Web Servers	3
CRITICAL	—	—	—	SMB (Multiple Issues)	Misc.	2
CRITICAL	—	—	—	TLS (Multiple Issues)	Misc.	2
CRITICAL	—	—	—	TLS (Multiple Issues)	SMTP problems	2
CRITICAL	2.0			X Server Detection	Service detection	1
CRITICAL	2.1	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1

Da questo elenco possiamo analizzare singolarmente ogni vulnerabilità, ma il programma ci offre anche un servizio di report autogenerato che analizza ogni vulnerabilità, fornendo link utili per la risoluzione e per la comprensione della vulnerabilità stessa.

Generate Report - 1 Host Selected

Report Format: HTML PDF CSV

Select a Report Template:

INTERNAL

Complete List of Vulnerabilities by Host

Detailed Vulnerabilities By Host

Detailed Vulnerabilities By Plugin

Vulnerability Operations

Template Description:

This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:

None

Formatting Options:

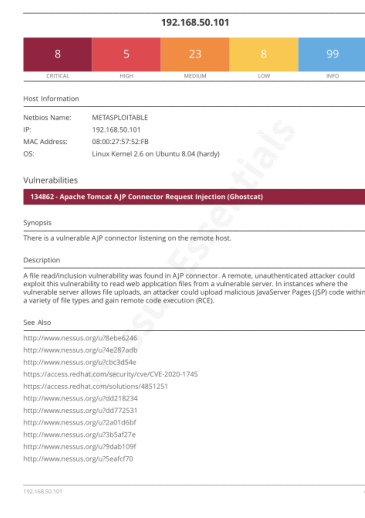
Of course, you can customize the report.

Generate Report

Cancel

Save as default

Una volta generato il report avremo una struttura ben organizzata dalla vulnerabilità più critica a quella meno critica, analizzeremo insieme qualche vulnerabilità critica.



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

In questa vulnerabilità (*Apache Tomcat AJP*) il report ci avvisa di aver trovato una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un attaccante remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni web da un server vulnerabile. Nei casi in cui il server vulnerabile consenta il caricamento di file, un attaccante potrebbe caricare pagine JavaServer (JSP) dannose e ottenere l'esecuzione di codice remoto (RCE).

E ci propone anche una soluzione, che non sempre può risultare assoluta, spesso le soluzioni proposte possono non essere sufficienti per la soluzione della vulnerabilità.

201352 - Canonical Ubuntu Linux SEoL (8.04.x)
Synopsis
An unsupported version of Canonical Ubuntu Linux is installed on the remote host.
Description
According to its version, Canonical Ubuntu Linux is 8.04.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.
See Also
http://www.nessus.org/u?3bdb2d2e
Solution
Upgrade to a version of Canonical Ubuntu Linux that is currently supported.
Risk Factor
Critical

In questa vulnerabilità (Canonical Ubuntu Linux SEoL) il report ci avvisa di aver trovato una vulnerabilità a livello di versione, ci avvisa che abbiamo una versione obsoleta e che non è più mantenuto dal suo fornitore o provider. La mancanza di supporto implica che non verranno rilasciate nuove patch di sicurezza per il prodotto. Di conseguenza, potrebbe contenere vulnerabilità di sicurezza.

Allo stesso tempo propone la soluzione di aggiornare alla versione corrente e ottenere le nuove patch di sicurezza.

Durante questo esercizio, ho avuto l'opportunità di esplorare e apprendere numerose funzionalità di Nessus, un tool che si è rivelato fondamentale per il controllo delle vulnerabilità e la sicurezza informatica. Grazie alle sue potenti capacità di scansione e alla vasta gamma di opzioni di configurazione, Nessus permette di identificare e correggere facilmente le debolezze nei sistemi, risultando uno strumento altamente efficace per la protezione delle infrastrutture.

Nonostante l'ampio numero di funzionalità offerte, l'interfaccia di Nessus risulta estremamente intuitiva e user-friendly, facilitando l'approccio anche per chi si avvicina per la prima volta alla gestione delle vulnerabilità. Questo mi ha permesso di concentrarmi più facilmente sulle analisi e sugli interventi necessari, senza la necessità di una curva di apprendimento complessa. Nessus, quindi, si conferma come uno strumento essenziale per chiunque voglia migliorare la sicurezza dei propri sistemi.