

Vulnerability assessment

Consegna S5:L4

Flavio Scognamiglio

Traccia



Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo). A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web. Gli obiettivi dell'esercizio sono:

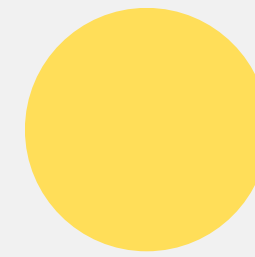
Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.

Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

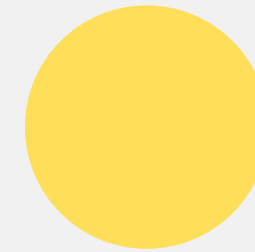
A cosa serve un vulnerability scanner

Un vulnerability scanner è un software automatizzato che esegue delle scansioni dei sistemi o di una rete alla ricerca di vulnerabilità conosciute. In questo caso stiamo utilizzando **Nessus** nella sua versione gratuita, ma esistono tanti altri tool simili.

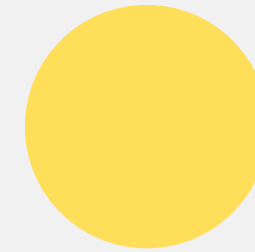
I vulnerability scanner si concentrano sulla rilevazione delle vulnerabilità note grazie all'ausilio di un database contenente le varie firme, e sulla scansione di dispositivi e porte.



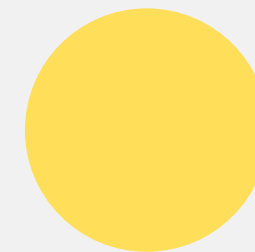
OpenVAS



Nuclei



Tsunami



Acunetix

Obiettivi VA

I principali obiettivi della fase di vulnerability assessment sono:



● — ○ **Identificare vulnerabilità note**

● — ○ **Valutarne il rischio**

● — ○ **Proporre soluzioni e mitigazioni**

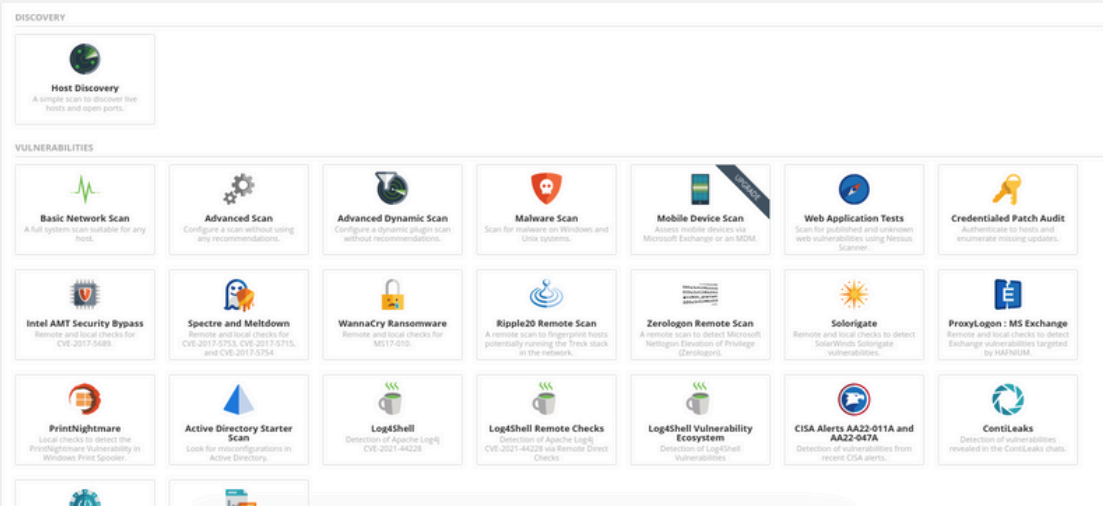
● — ○ **Scrivere il report finale**

Scansioni

Obiettivo: Metasploitable (192.168.1.101)

E' possibile scegliere diverse tipologie di scansione, inclusa una **scansione avanzata**. In questa modalità, si può configurare ogni singola impostazione per mirare specificamente l'obiettivo, evitando inutili scansioni lunghe e casuali.

Si possono anche disabilitare **plugin** non rilevanti per il bersaglio, ottimizzando così il processo di scansione. Questo dipende anche da come sono state effettuate le fasi precedenti, come l'information gathering, per ottenere una mappatura accurata del sistema da analizzare.



Settings					Credentials					Plugins				
STATUS					PLUGIN FAMILY ▲					LOCKED				
ENABLED					AIX Local Security Checks									
ENABLED					Alma Linux Local Security Checks									
ENABLED					Amazon Linux Local Security Checks									
ENABLED					Backdoors									
ENABLED					Brute force attacks									
ENABLED					CentOS Local Security Checks									
ENABLED					CGI abuses									
ENABLED					CGI abuses : XSS									
ENABLED					CISCO									
ENABLED					Databases									
ENABLED					Debian Local Security Checks									
ENABLED					Default Unix Accounts									
ENABLED					Denial of Service									
ENABLED					DNS									
ENABLED					F5 Networks Local Security Checks									
ENABLED					Fedora Local Security Checks									
ENABLED					Firewalls									

New Scan / Advanced Scan

[← Back to Scan Templates](#)

Settings

Credentials

Plugins

BASIC

• General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

metasploitable-advanced-scan

Description

Folder

My Scans

Targets

192.168.1.101

Upload Targets

Add File

Settings

Credentials

BASIC

DISCOVERY

ASSESSMENT

General

Brute Force

• Web Applications

Windows

Malware

Databases

REPORT

Save

Cancel

Settings

Credentials

Plugins

BASIC

DISCOVERY

Host Discovery

Port Scanning

Service Discovery

Identity

ASSESSMENT

REPORT

ADVANCED

General Settings

☒ Probe all ports to find services
When enabled, the scanner attempts to map each open port with the service that is running on that port, as defined by the Port scan range option. Caution: In

Search for SSL/TLS/DTLS services ☒

Controls how the scanner tests SSL-based services. Caution: Testing for SSL capability on all ports may be disruptive for the teste

Search for SSL/TLS on

All TCP ports

Search for DTLS on

None

Identify certificates expiring within x days

60

When enabled, the scanner identifies SSL and TLS certificates that are within the specified number of day

☒ Enumerate all SSL/TLS ciphers
When enabled, the scanner ignores the list of ciphers advertised by SSL/TLS services and enumerates them by attempting to establish connections using all

☐ Enable CRL checking (connects to the Internet)

Settings

Credentials

Plugins

BASIC

DISCOVERY

ASSESSMENT

General

Brute Force

Web Applications

Windows

Malware

Databases

REPORT

ADVANCED

Web Application Settings

Scan web applications

ON

Web Crawler

Start crawling from

/

The URL of the first page that is tested. If multiple pages are required, use a colon delimiter to separate them (e.g., /:php4:/b

Excluded pages (regex)

/server_privileges\.php|logout

Specifies portions of the web site to exclude from being crawled. For example, to exclude the /manual directory and all Perl C

Maximum pages to crawl

1000

The maximum number of pages to crawl.

Maximum depth to crawl

6

Limit the number of links Nessus follows for each start page.

☐ Follow dynamically generated pages

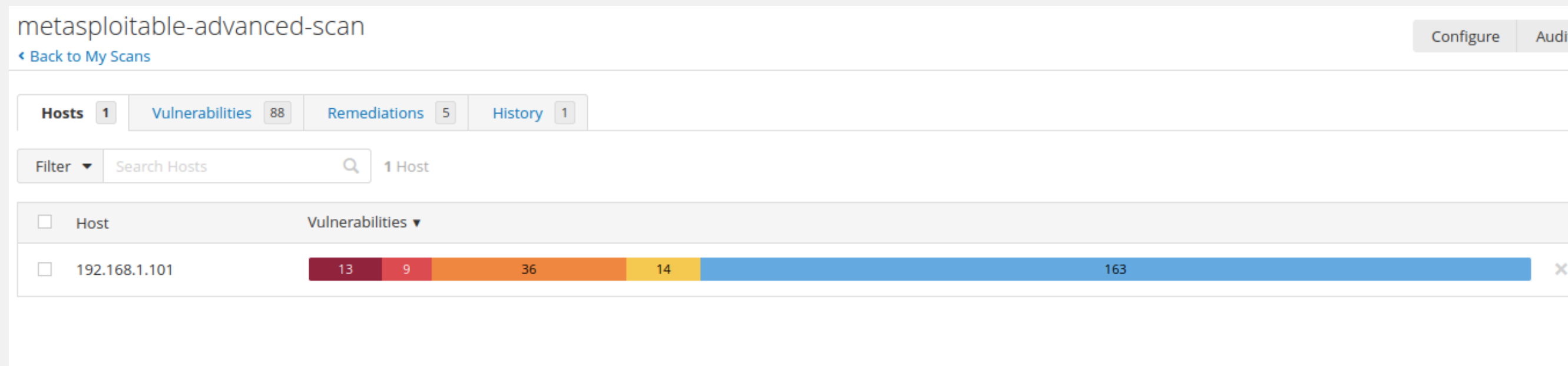
If selected, Nessus follows dynamic links and may exceed the parameters set above.

Application Test Settings

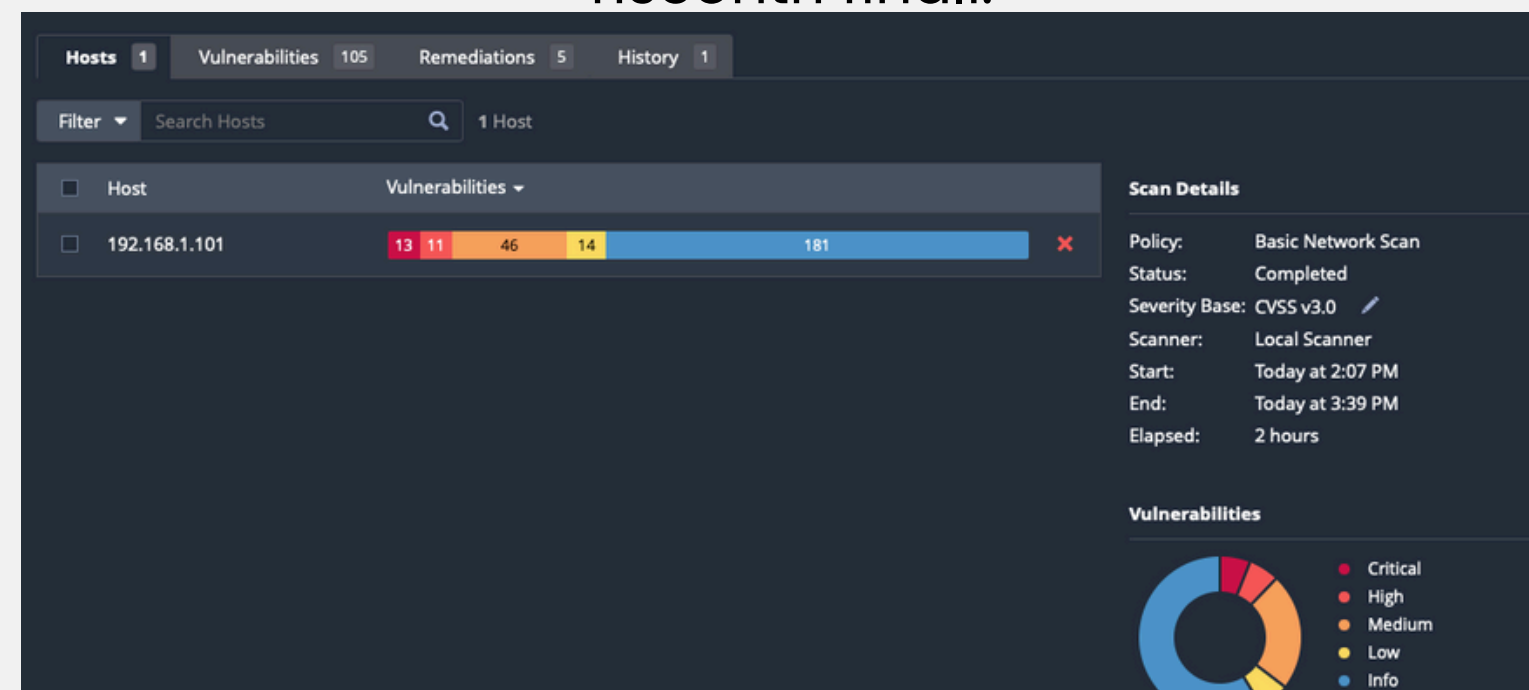
☐ Enable generic web application tests

Avvio scansione

Questa è una scansione più selettiva, abilitando ad esempio il port scanning solo per le porte conosciute, i servizi smb e le applicazioni web:



Una scansione volutamente più approfondita allungherebbe notevolmente le tempistiche, ma anche i riscontri finali:



<input type="checkbox"/> Sev ▾	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1		
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1		
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1		
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2		
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1		
<input type="checkbox"/> MIXED	4 Apache Tomcat (Multiple Issues)	Web Servers	4		
<input type="checkbox"/> MIXED	4 Phpmyadmin (Multiple Issues)	CGI abuses	4		
<input type="checkbox"/> CRITICAL	2 SSL (Multiple Issues)	Gain a shell remotely	3		
<input type="checkbox"/> MIXED	3 PHP (Multiple Issues)	CGI abuses	3		
<input type="checkbox"/> HIGH	7.5 *	5.9	rlogin Service Detection	Service detection	1		
<input type="checkbox"/> HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1		
<input type="checkbox"/> HIGH	7.5 *		CGI Generic Command Execution	CGI abuses	1		
<input type="checkbox"/> HIGH	7.5 *		CGI Generic Remote File Inclusion	CGI abuses	1		
<input type="checkbox"/> HIGH	7.5		NFS Shares World Readable	RPC	1		
<input type="checkbox"/> MIXED	15 SSL (Multiple Issues)	General	27		
<input type="checkbox"/> MIXED	5 ISC Bind (Multiple Issues)	DNS	5		
<input type="checkbox"/> MIXED	2 Twiki (Multiple Issues)	CGI abuses	2		
<input type="checkbox"/> MEDIUM	6.8 *		CGI Generic Local File Inclusion (2nd pass)	CGI abuses	1		

Eventuale scansione Windows 7 selettiva

Settings

Credentials

Plugins

STATUS

PLUGIN FAMILY

LOCKED

TOTAL

DISABLED	AIX Local Security Checks		11563
DISABLED	Alma Linux Local Security Checks		1342
DISABLED	Amazon Linux Local Security Checks		4640
ENABLED	Backdoors		123
ENABLED	Brute force attacks		25
DISABLED	CentOS Local Security Checks		4927
ENABLED	CGI abuses		6027
ENABLED	CGI abuses : XSS		705
DISABLED	CISCO		2425
DISABLED	Databases		993
DISABLED	Debian Local Security Checks		9423
DISABLED	Default Unix Accounts		172
ENABLED	Denial of Service		110
ENABLED	DNS		238
ENABLED	FS Networks Local Security Checks		1456
DISABLED	Fedora Local Security Checks		19034
ENABLED	Firewalls		467

STATUS

PLUGIN NAME

PLUGIN ID

DISABLED	AIX 5.1 : IV23847	22379
DISABLED	AIX 5.1 : IV24721	22380

Winzozz7 / Configuration

[← Back to Scan Report](#)

Settings

Credentials

Plugins

BASIC

DISCOVERY

ASSESSMENT

Host Discovery

Port Scanning

Service Discovery

Identity

Ports

Consider unscanned ports as closed

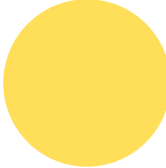
Port scan range: 139, 445, 3389

Report conclusivo

Dopo la scansione con Nessus bisognerebbe:



Analizzare il report per identificare le vulnerabilità.



Prioritizzare le vulnerabilità per gravità e impatto.



Pianificare le correzioni necessarie.



Implementare le soluzioni.



Verificare le correzioni con una nuova scansione.



Documentare e aggiorna il report di sicurezza.