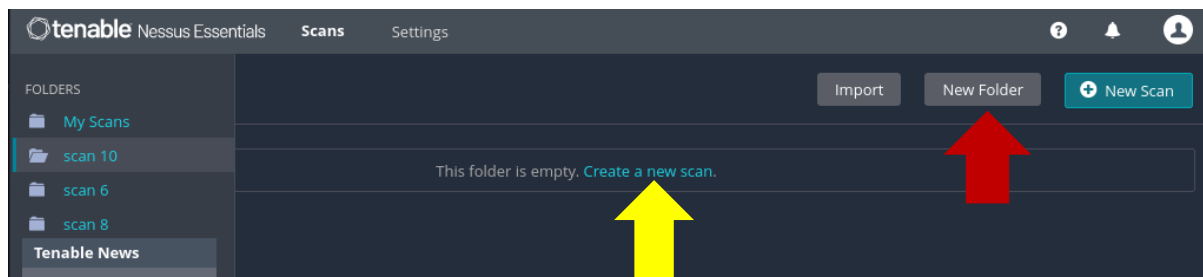


PRATICA S5/L4

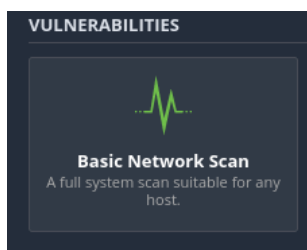
Obiettivo: Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable, poi analizzare attentamente il report per ognuna delle vulnerabilità riportate

1) Scansione di Metasploitable con Nessus.

Per la scansione di Metasploitable2, abbiamo aperto il software Nessus, siamo andati sulla cartella "New Folder" dove abbiamo creato una nuova cartella, come indicato con la freccia rossa qui sotto.



Dopo la creazione della cartella, abbiamo cliccato su "create new scan" come indicato sopra con la freccia gialla. È uscita una nuova schermata e abbiamo cliccato su "Basic Network Scan".



Cliccando su Basic Network Scan abbiamo ottenuto la schermata qua sotto, che permette di inserire le informazioni per la scansione. e abbiamo inserito le informazioni richiesti come si può vedere su l'immagine sotto. Dopo di che abbiamo salvato tutto cliccando su save(

PRATICA S5/L4

Indicato con una freccia rossa).

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Georges

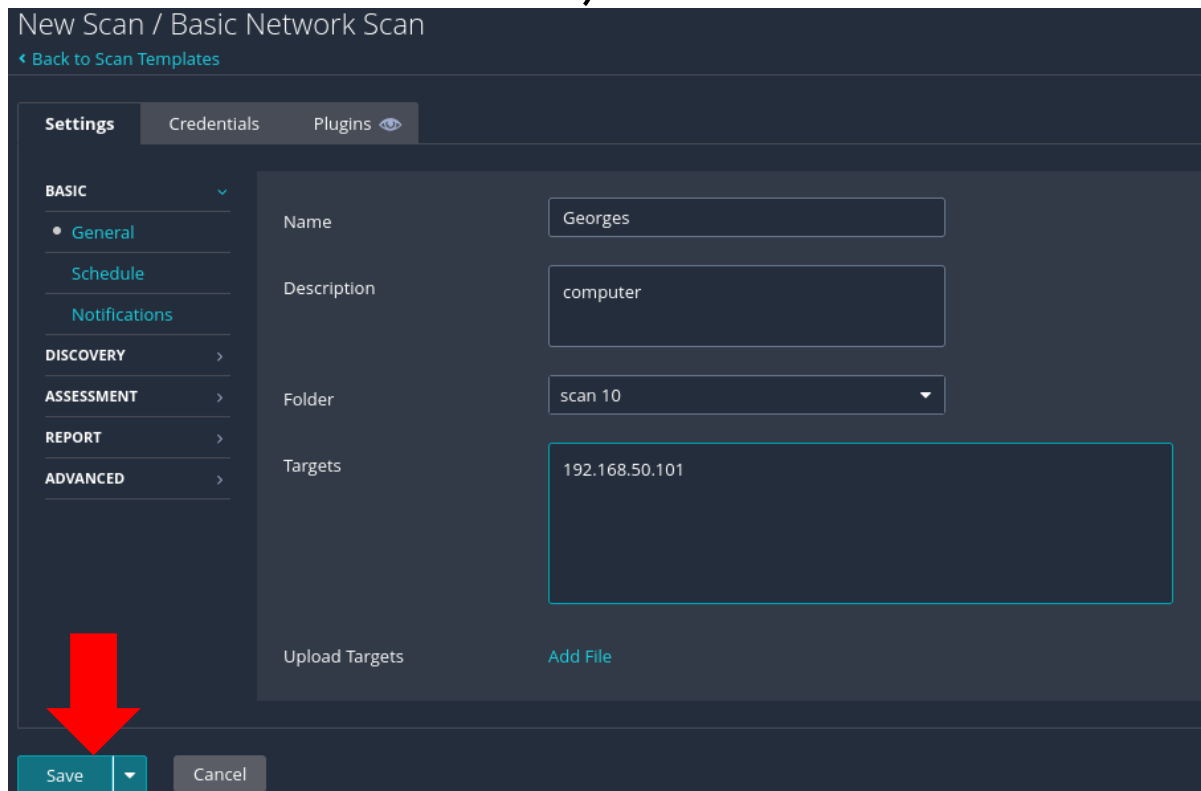
Description: computer

Folder: scan 10

Targets: 192.168.50.101

Upload Targets Add File

Save Cancel



Dopo di che abbiamo iniziato la scansione cliccando su Launch, come indica la freccia rossa su l'immagine che segue.

tenable Nessus Essentials Scans Settings

FOLDERS

- My Scans
- scan 10
- scan 6
- scan 8
- Tenable News
- EduLog Parent Portal

Import New Folder New Scan

Schedule	Last Scanned	Launch
On Demand	Today at 11:13 AM	

Dopo la scansione abbiamo ottenuto un report con i diversi livelli di vulnerabilità andando dal più critico al più basso, come possiamo vedere sulle immagini seguenti.



PRATICA S5/L4

Georges / 192.168.50.101 [Configure](#)

[Back to Hosts](#)

Vulnerabilities 65

Filter Search Vulnerabilities 65 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *		NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Versi...	General	1
CRITICAL	10.0 *		UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	DNS (Multiple Issues)	DNS	5
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5 *		rlogin Service Detection	Service detection	1

Host Details

IP: 192.168.50.101
OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Start: Today at 3:56 PM

Vulnerabilities

Legend: Critical, High, Medium, Low, Info

MIXED	15	SSL (Multiple Issues)	General	28
MIXED	5	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9			SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9			SSL DROWN Attack Vulnerability (Decrypti...	Misc.	1
MEDIUM	5.3			HTTP TRACE / TRACK Methods Allowed	Web Servers	1
MIXED	6	SSH (Multiple Issues)	Misc.	6
MIXED	2	SMB (Multiple Issues)	Misc.	2
MIXED	2	TLS (Multiple Issues)	Misc.	2
MIXED	2	TLS (Multiple Issues)	SMTP problems	2
LOW	3.7			SSL/TLS Diffie-Hellman Modulus <= 1024 B...	Misc.	1
LOW	2.6 *			X Server Detection	Service detection	1
INFO	6	SMB (Multiple Issues)	Windows	7
INFO	2	HTTP (Multiple Issues)	Web Servers	4

Possiamo notare che i livelli di vulnerabilità sono classificati in ordine decrescente, i livelli critical e high sono livelli da risolvere subito perché sono miniere d'oro per i black hat.

PRATICA S5/L4

Cliccando su una vulnerabilità possiamo vedere che Nessus ci fa la descrizione del problema e ci propone delle soluzioni per risolvere il problema.

The screenshot displays the Nessus user interface for a specific vulnerability. The top navigation bar includes the Tenable logo, 'Nessus Essentials', and tabs for 'Scans' and 'Settings'. The user's name, 'GEORGES FOTSING', is visible in the top right corner. On the left sidebar, there are sections for 'FOLDERS' (listing various scan folders like 'My Scans', 'scan 10', etc.) and 'RESOURCES' (including 'Tenable News' with links to CVE-2023-46805 and CVE-2024-21887).

The main content area is titled 'Georges / Plugin #46882' and includes buttons for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. Below this, a 'Vulnerabilities' section shows a count of 73. The selected vulnerability is 'UnrealIRCd Backdoor Detection', marked as 'CRITICAL'. The 'Description' states: 'The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.' The 'Solution' advises: 'Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.' The 'See Also' section provides links to security advisories. The 'Output' section shows a log entry: 'The remote IRC server is running as : uid=0 (root) gid=0 (root)'. Below this, a table lists the 'Port' (6667 / tcp / irc) and 'Hosts' (192.168.50.101).

On the right side, the 'Plugin Details' section lists attributes: Severity (Critical), ID (46882), Version (1.16), Type (remote), Family (Backdoors), Published (June 14, 2010), and Modified (April 11, 2022). The 'VPR Key Drivers' section lists threat metrics: Threat Recency (No recorded events), Threat Intensity (Very Low), Exploit Code Maturity (Functional), Age of Vuln (730 days +), Product Coverage (Low), CVSSV3 Impact Score (5.9), and Threat Sources (No recorded events). The 'Risk Information' section shows a 'Vulnerability Priority Rating (VPR): 7.4'.