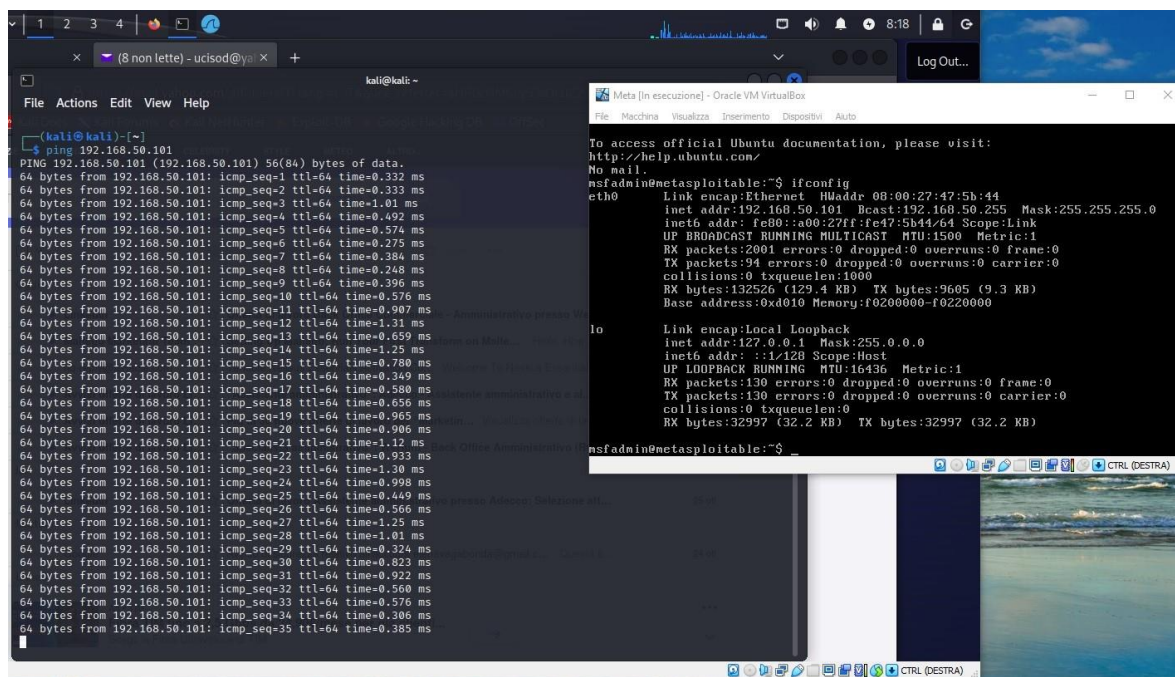


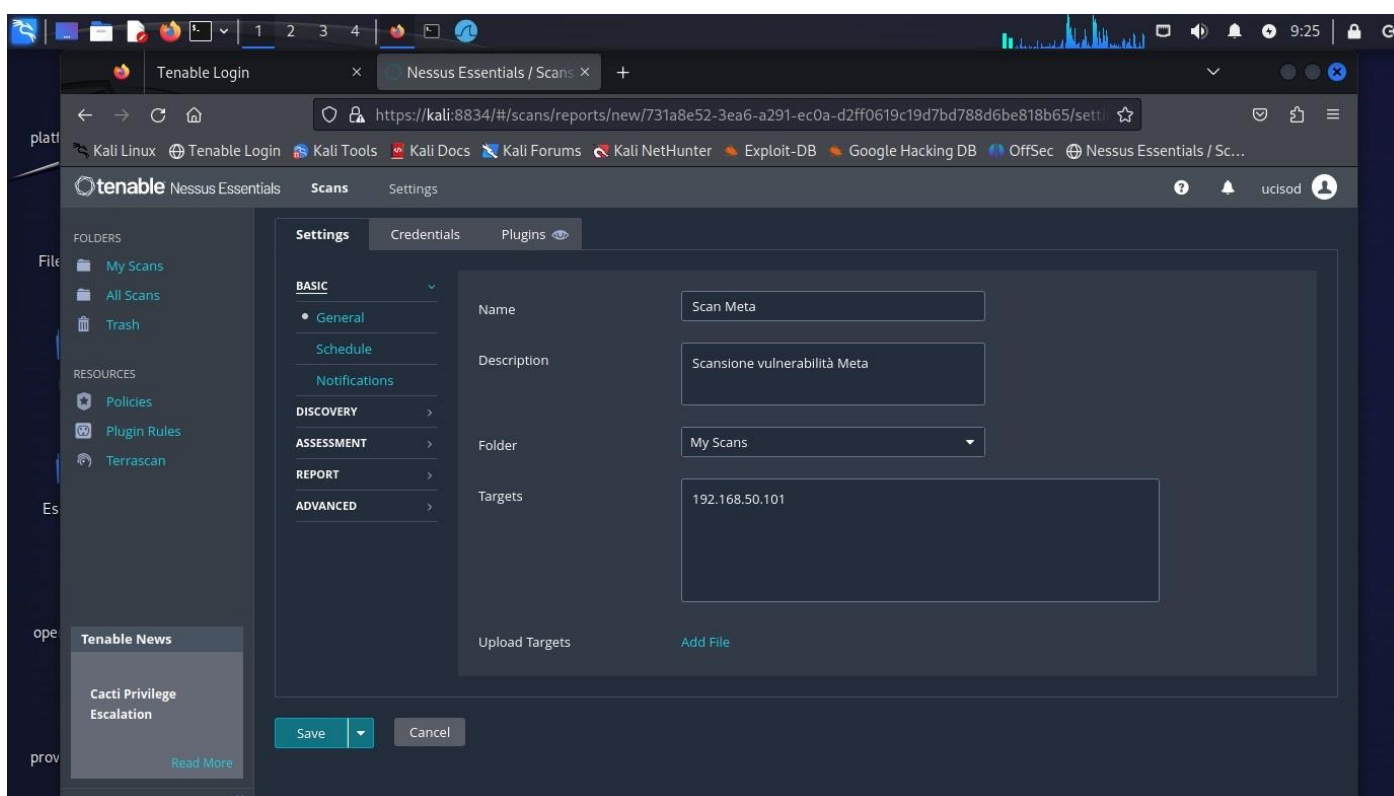
Esercitazione 26/10/2023

Nell'esercizio odierno ci viene richiesta una scansione delle vulnerabilità del programma Metasploitable attraverso l'uso di Nessus e di commentare le prime criticità

Prima di tutto controllo che le macchine riescano a pingare tra loro



Fatto ciò avvio la scansione (tipo di scansione port scan "common ports") con il comando "Launch"



A questo punto il sistema ci ha trovato un totale di 70 vulnerabilità tra cui:

- 5 Critical
- 10 Mixed
- 4 High
- 3 Medium
- 2 Low

The screenshot shows the Nessus Essentials interface. The left sidebar contains navigation options like 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'Terrascan'. The main content area is titled 'Scan Meta' and shows a summary of a scan on host 192.168.50.101. The summary includes a bar chart showing the distribution of vulnerabilities by severity: 12 Critical, 7 High, 25 Medium, 8 Low, and 136 Info. The scan details on the right indicate the policy is 'Basic Network Scan', the status is 'Completed', the scanner is 'Local Scanner', and the scan took 19 minutes.

Host	Vulnerabilities
192.168.50.101	12 Critical, 7 High, 25 Medium, 8 Low, 136 Info

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 9:26 AM
- End: Today at 9:45 AM
- Elapsed: 19 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

The screenshot shows the Nessus Essentials interface with the 'Vulnerabilities' page selected. The left sidebar is the same as the previous screenshot. The main content area displays a list of 70 vulnerabilities. The table shows columns for Severity, CVSS, VPR, Name, Family, and Count. The vulnerabilities are sorted by severity, with Critical at the top. The right sidebar shows 'Host Details' for 192.168.50.101, including IP, MAC, OS, and scan details. A 'Vulnerabilities' donut chart is also present on the right.

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Sha...	RPC	1
CRITICAL	10.0		Unix Operating S...	General	1
CRITICAL	10.0 *		VNC Server 'pass...	Gain a shell remotely	1
CRITICAL	9.8		Bind Shell Backdo...	Backdoors	1
MIXED	DNS (Multipl...	DNS	5
MIXED	Apache Tom...	Web Servers	4
CRITICAL	SSL (Multiple...	Gain a shell remotely	3
MIXED	SSL (Multiple...	Service detection	3
HIGH	7.5		NFS Shares World...	RPC	1
HIGH	7.5 *	6.7	rlogin Service Det...	Service detection	1
HIGH	7.5 *	6.7	rsh Service Detec...	Service detection	1
HIGH	7.5	6.7	Samba Badlock V...	General	1
MIXED	SSL (Multiple...	General	28
MIXED	ISC Bind (Mu...	DNS	5
MEDIUM	6.5		TLS Version 1.0 P...	Service detection	2

Host Details

- IP: 192.168.50.101
- MAC: 08:00:27:47:5B:44
- OS: Linux kernel 2.6 on Ubuntu 8.04 (hardy)
- Start: Today at 9:26 AM
- End: Today at 9:45 AM
- Elapsed: 19 minutes
- KB: Download

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

1 vulnerabilità livello critico:

Nome: **NFS Exported Share Information Disclosure**

Descrizione: la descrizione ci riporta che almeno un file NFS (Network File System), cioè un file o directory che sono presenti su un server NFS che li rende accessibili ai soli client che hanno i permessi per accedervi, non è sufficientemente protetto, pertanto un utente malintenzionato potrebbe avere accesso a questa condivisione e sfruttarla per accedere al file sull'host remoto, leggendolo o modificandolo.

Soluzione: Come possibile soluzione ci riporta quella di configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni

Osservazioni: Il programma ci riporta alcune informazioni utili quali, oltre a quelle già citate, i dettagli del plugin informazioni sui rischi

2 vulnerabilità livello critico:

Nome: **Unix Operating System Unsupported Version Detection**

Descrizione: Secondo il numero di versione riportato il programma ci avvisa che il sistema operativo Unix in esecuzione sull'host remoto non è più supportato e questa mancanza implica che il fornitore non rilascerà alcuna patch di sicurezza (correzione o aggiornamento software progettato proprio per risolvere le vulnerabilità).

Soluzione: Il programma ci consiglia di eseguire l'upgrade ad una versione sistema operativo Unix che sia supportata

3 vulnerabilità livello critico:

Nome: **VNC Server 'password' Password**

Descrizione: La terza criticità si riferisce al fatto che il server VNC (Virtual Network Computing) in esecuzione sull'host remoto non è sufficientemente protetto poiché ha una password debole e ci avvisa del fatto che Nessus è riuscito ad accedervi utilizzando una password standard "password". Un utente malintenzionato non autenticato, dunque, potrebbe sfruttare questa situazione per assumere il controllo del sistema

Soluzione: Nessus ci consiglia di proteggere il servizio VNC con una password complessa

4 vulnerabilità livello critico:

Nome: **Bind Shell Backdoor Detection**

Descrizione: Una shell (una componente software tramite la quale è possibile impartire comandi e richiedere l'avvio di programmi) è in esecuzione senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

Soluzione: Il programma ci indica di verificare se l'host remoto è stato compromesso e, se necessario, di reinstallare il sistema