

# Report Scan Porte con Nessus

## S5-L3

### Introduzione

In questa esercitazione scansioneremo porte comuni usando Nessus su Kali Linux con target Metasploitable su VirtualBox.

**Port scan:** Common ports.

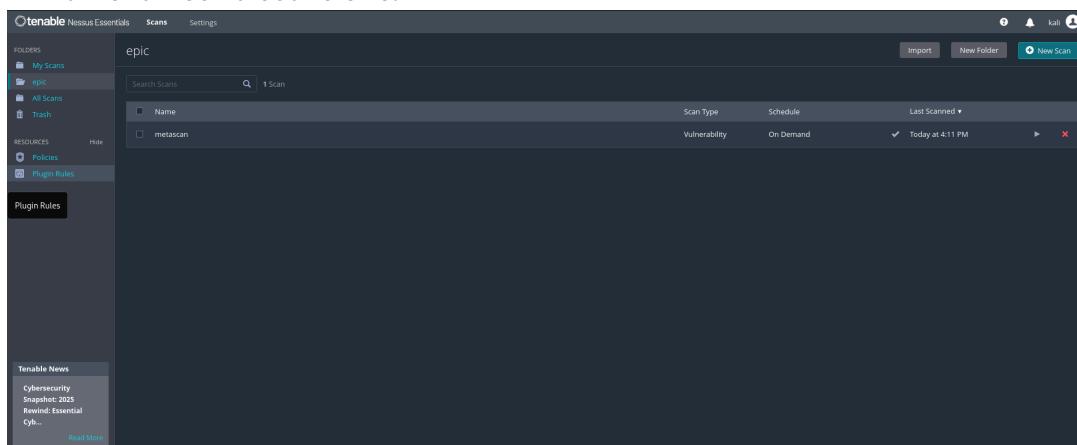
### Passo 1: Configurare Scansione Nessus

Accedi all'interfaccia di Nessus:

1. **Accedi a "My Scans"** - Visualizza tutte le scansioni eseguite e pianificate
2. **Clicca "New Scan"** - Avvia una nuova scansione
3. **Scegli "Basic Network Scan"** - Per scansione completa del sistema

Nella schermata di configurazione, inseriamo :

- **Nome:** descrittivo per la scansione
- **Descrizione:** facoltativa
- **Cartella di destinazione:** organizza le scansioni
- **Target:** indirizzo IP (192.168.10.11)
- **Avviamo la nostra scansione:**



### Passo 2: Analizzare Risultati Scansione

Una volta completata la scansione, visualizzerai:

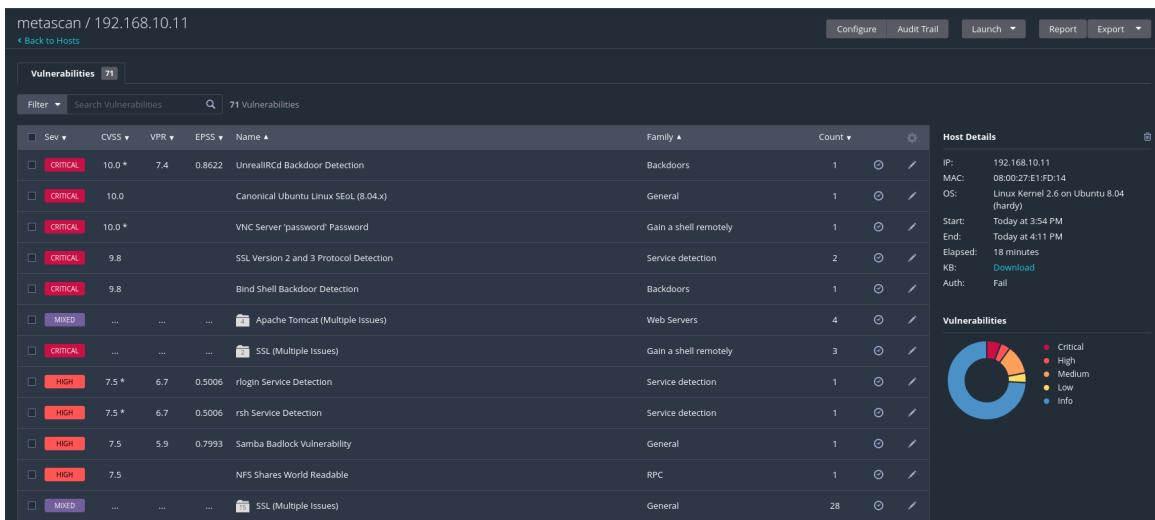
### Dettagli Principali:

- **Indirizzo IP target:** 192.168.10.11
- **Vulnerabilità rilevate:** lista classificata per severità
- **Diagramma a torta:** distribuzione vulnerabilità per criticità

## Classificazione Vulnerabilità

Le vulnerabilità vengono ordinate da più a meno critica:

Severità	Count
CRITICAL	11
HIGH	7
MEDIUM	23
LOW	7
INFO	137



## Dettagli Vulnerabilità Esempio

### UnrealIRCd Backdoor Detection (CRITICAL):

- **Plugin ID:** 46882
- **Type:** remote
- **Family:** Backdoors
- **Port:** 6667/tcp
- **Description:** The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.
- **Soluzione:** Riscarica software, verifica MD5/SHA1, reinstalla
- **CVSSv3.0 Impact Score:** 5.9

Per ogni vulnerabilità, Nessus fornisce:

- Description dettagliata
- Solution consigliata
- See Also (link utili per approfondimento)
- Output della scansione
- Plugin Details e Risk Information

The screenshot shows the metascan / Plugin #46882 interface. At the top, there are buttons for 'Configure' and 'Audit Trail'. Below that, a navigation bar has 'Vulnerabilities' selected, showing a count of 71. A red 'CRITICAL' button is next to the title 'UnrealIRCd Backdoor Detection'. The main content area starts with a 'Description' section: 'The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.' Below it is a 'Solution' section: 'Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.' There is also a 'See Also' section with links to security lists and an advisory document. The 'Output' section contains a terminal-like window showing the command 'netstat -an | grep :6667' and its output, which includes 'uid=0(root) gid=0(root)'. At the bottom, a table shows port information: 'Port ▲' and 'Hosts' columns, with one entry for '6667 / tcp / irc' and '192.168.10.11'.

## Conclusioni

L'utilizzo di Nessus è fondamentale per la cybersecurity professionale:

- **Enumerazione servizi** - Identifica servizi attivi e versioni
- **Analisi porte aperte** - Scopre configurazioni non sicure
- **Valutazione rischio** - Classifica vulnerabilità per criticità
- **Prioritizzazione fix** - Guida basata su CVSS e VPR (Common Vulnerability Scoring System e Vulnerability Priority Rating).