

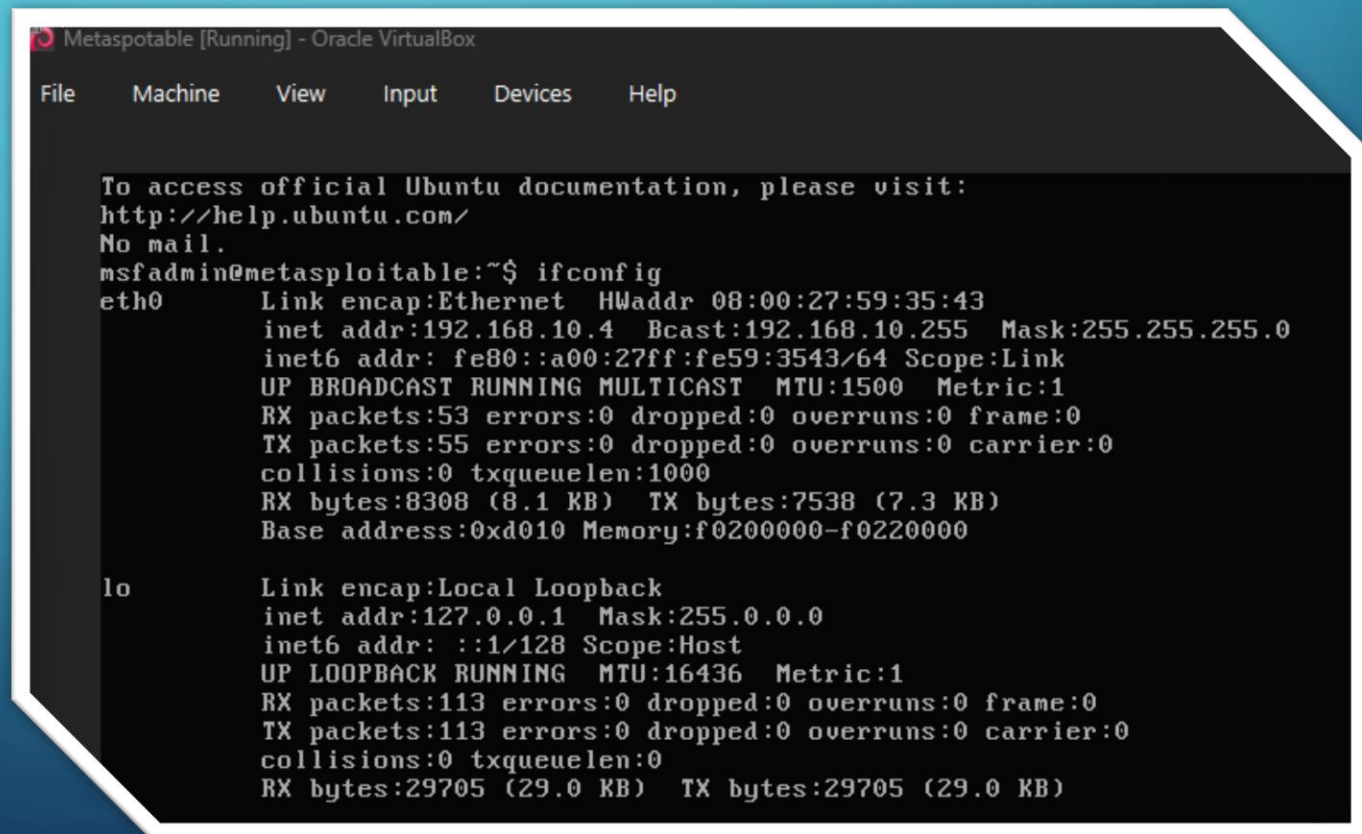


# VULNERABILITY SCANNING

- TARGET: METASPLOITABLE.
- PORTE: SOLO LE PORTE COMUNI (ES. 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389).
- TIPO DI SCANSIONE: BASIC NETWORK SCAN: CONFIGURAZIONE PREDEFINITA PER UNA SCANSIONE DI RETE.

# METASPLOITABLE

- Il Target si tratta di Metasploitable, una macchina virtuale (VM) appositamente progettata per essere insicura, piena di vulnerabilità volontarie, usata come ambiente di apprendimento e pratica per professionisti della sicurezza informatic

A screenshot of a terminal window titled "Metasploitable [Running] - Oracle VirtualBox". The window has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The terminal text shows a user prompt "msfadmin@metasploitable:~\$" followed by the command "ifconfig". The output displays network configuration for "eth0" and "lo".

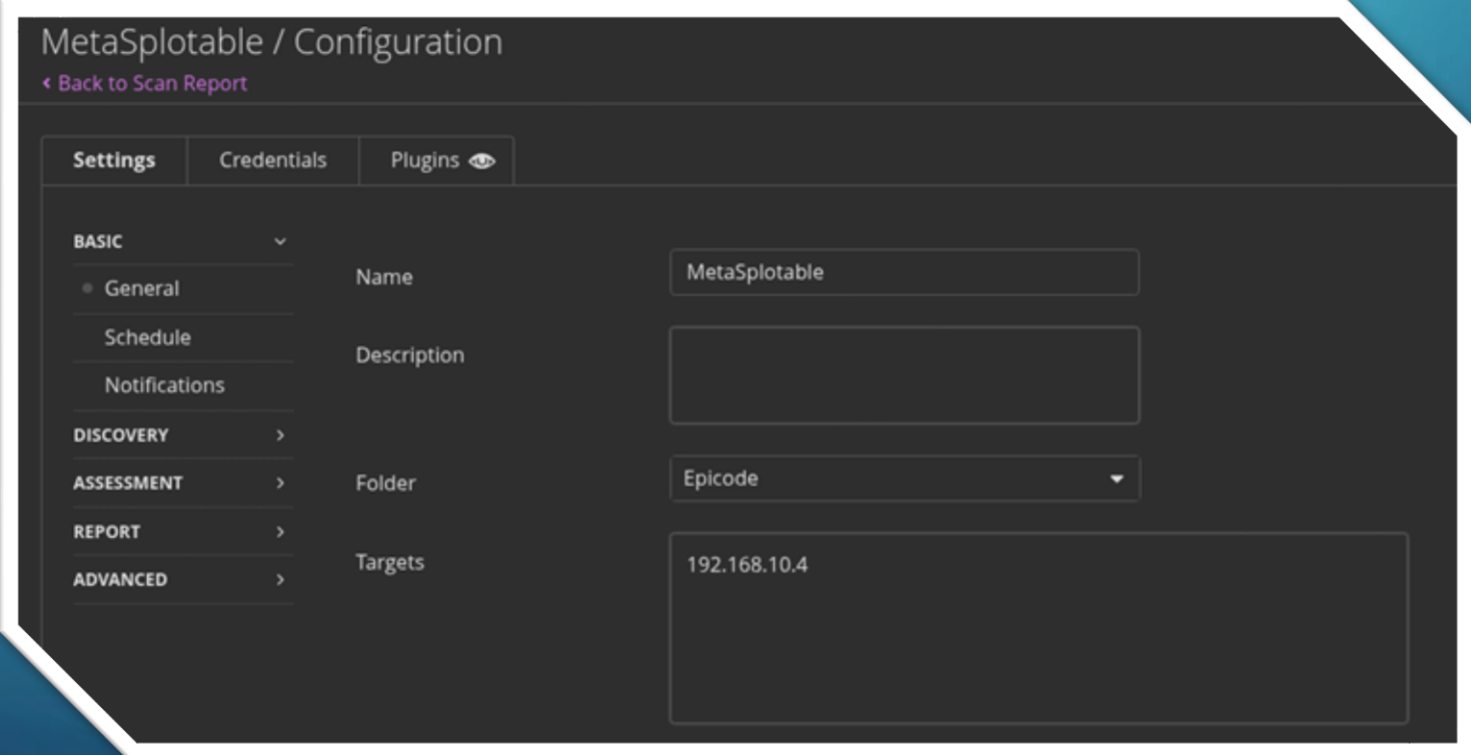
```
Metasploitable [Running] - Oracle VirtualBox
File Machine View Input Devices Help

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:59:35:43
          inet addr:192.168.10.4  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe59:3543/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:53 errors:0 dropped:0 overruns:0 frame:0
          TX packets:55 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8308 (8.1 KB)  TX bytes:7538 (7.3 KB)
          Base address:0xd010 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29705 (29.0 KB)  TX bytes:29705 (29.0 KB)
```


# INIZIO CONFIGURAZIONE

- Basic: in questa sezione si inseriscono informazioni di carattere generale sulla scansione come nome, descrizione, sistemi target (MetaSploable:192.168.10.4)



MetaSploable / Configuration

[← Back to Scan Report](#)

Settings Credentials Plugins 

**BASIC** ▾

- General
- Schedule
- Notifications

**DISCOVERY** >

**ASSESSMENT** >

**REPORT** >

**ADVANCED** >

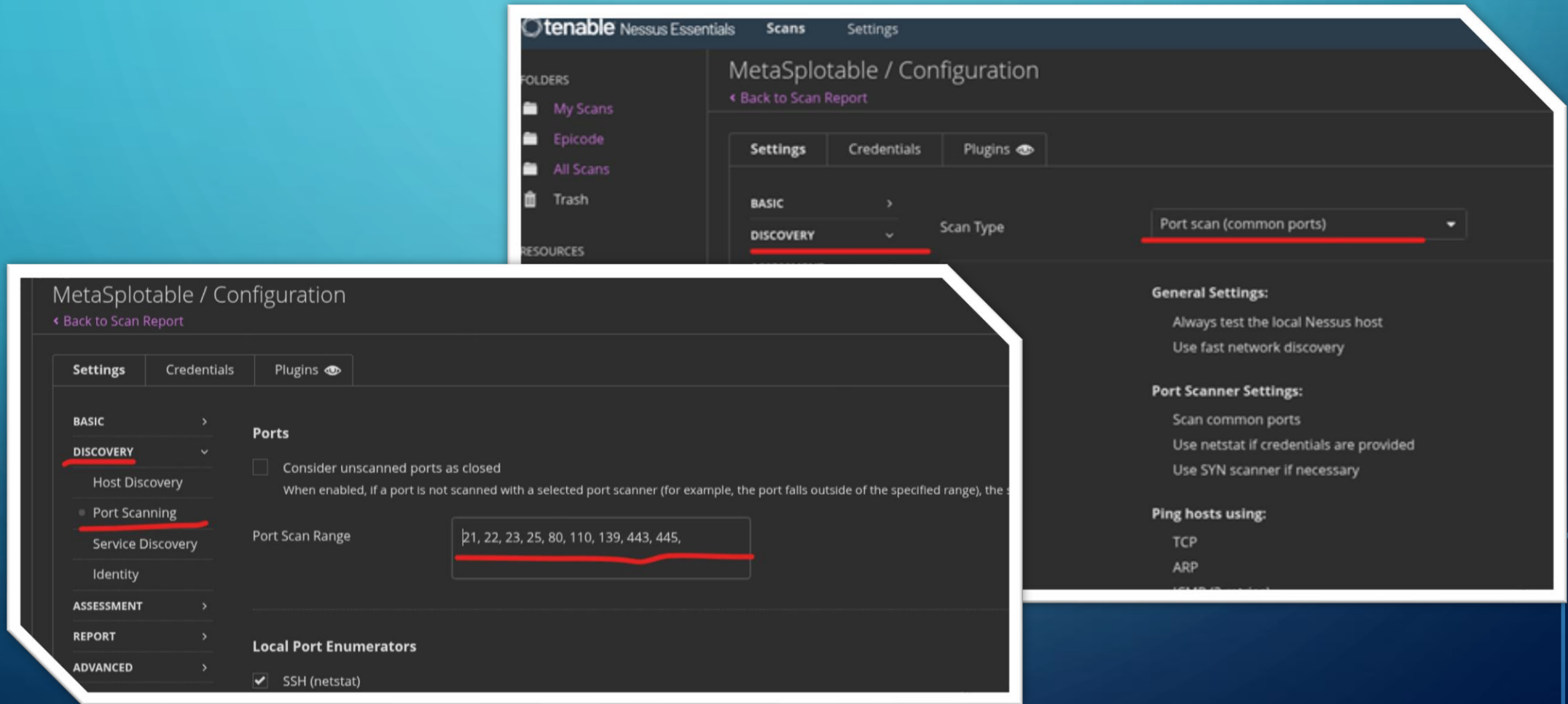
Name: MetaSploable

Description:

Folder: Epicode ▾

Targets: 192.168.10.4

- Discovery: in questa sezione si inseriscono le modalità per effettuare l'host discovery ed il port scanner. Sono state selezionate solo le porte comuni (es. 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389)
- Si può selezionare nella tendina common ports facendo eseguire a Nessus le porte comuni, o si possono personalizzare solo le comuni interessanti nel nostro caso attuale abbiamo usato il default.



# ANALISI REPORT

- Dashboard delle Vulnerabilita trovate

