

Elevate Labs - Task 3

By Harshith Gangisetty

Here i am Using Nessus vulnerability scanner

Before we approach to the target, I am scanning my network using nmap

```
(kali㉿kali)-[~]  
$ sudo nmap -sn 10.0.2.0/24  
[sudo] password for kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-03 16:29 EDT  
Nmap scan report for 10.0.2.1
```

I wanted to scan the target 10.0.2.5

Settings

Credentials

Plugins

BASIC

• General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Description

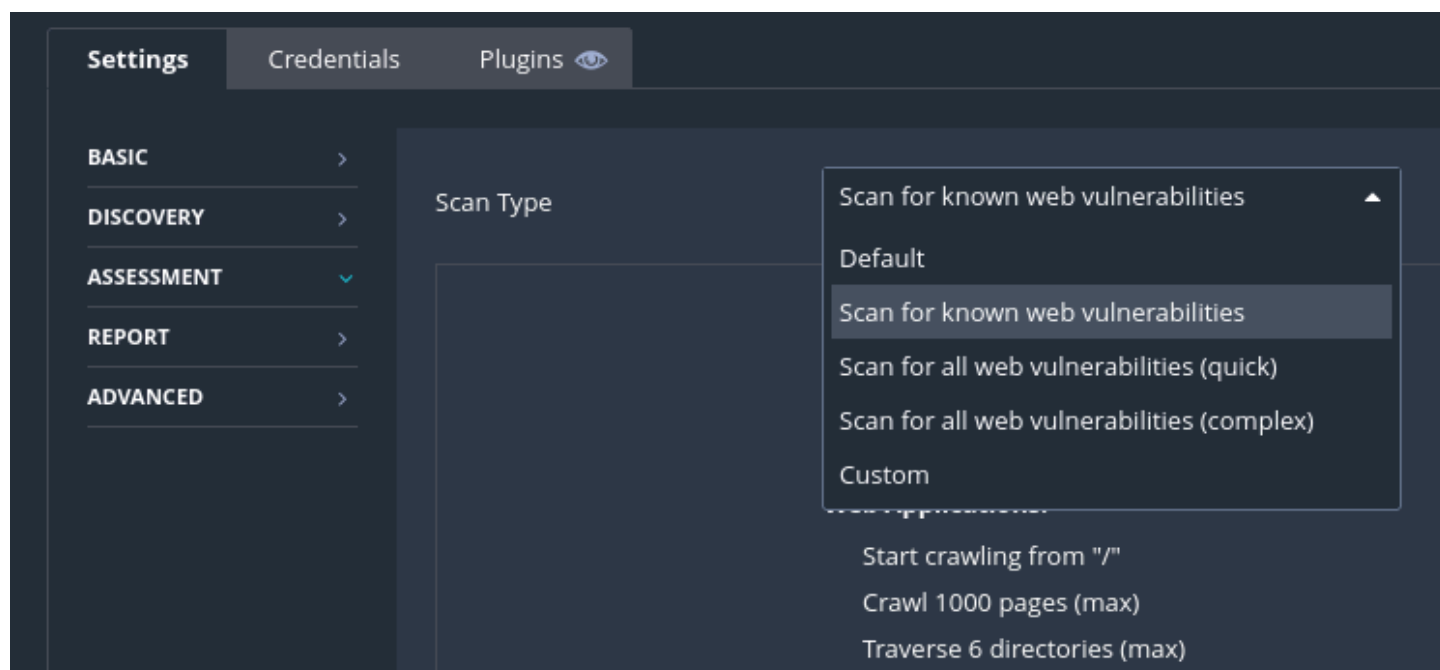
Folder

Targets

First_scan

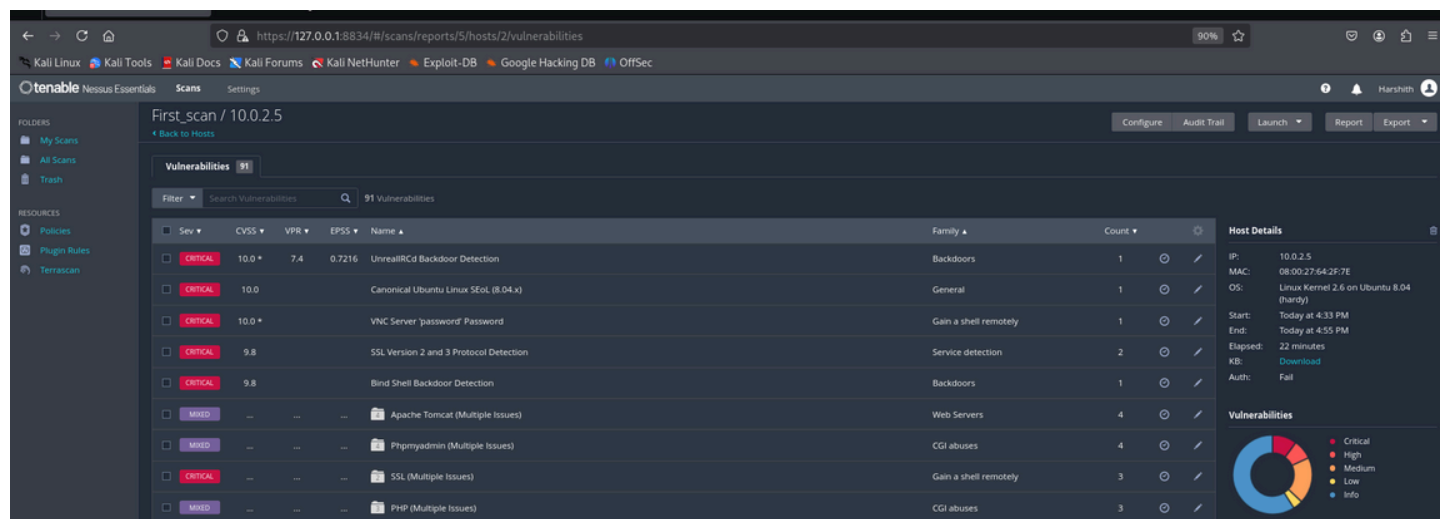
My Scans

10.0.2.5



I am scanning for known web vulnerabilities for a better report

After configuring the scan these are the results:



The metasploitable has many known vulnerabilities put inside which is being shown

A few critical are listed below :

1)**Back door execution** : The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.
One of the mitigations are , Having a network scan more regularly , detect untrusted software

2) **Weak Password** :The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution: Secure the VNC service with a strong password.