Vulnerability Assessment

Target: Metasploitable Machine

A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed. The security scanning process consists of four steps: testing, analysis, assessment and remediation.

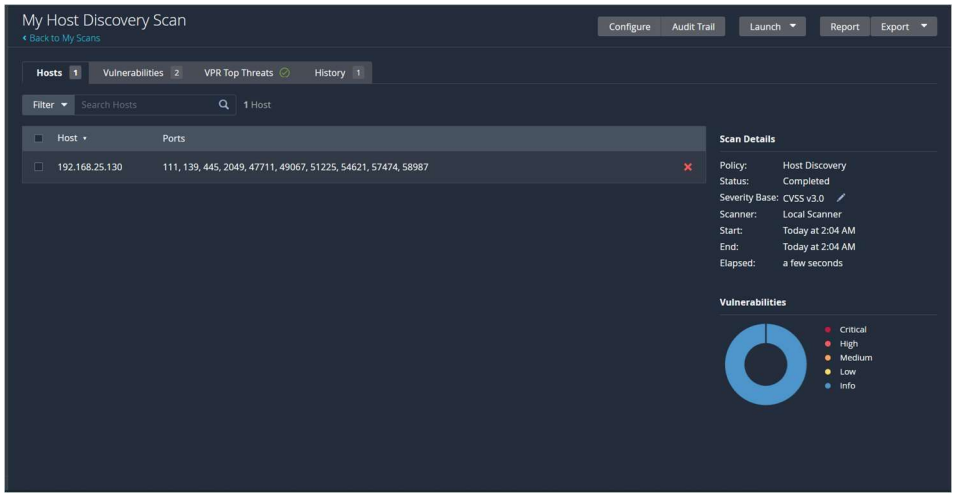
Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. Nessus employs the Nessus Attack Scripting Language (NASL), a language that describes individual threats and potential attacks.

Nessus has a modular architecture consisting of centralized servers that conduct scanning, and remote clients that allow for administrator interaction. Administrators can include NASL descriptions of all suspected vulnerabilities to develop customized scans.

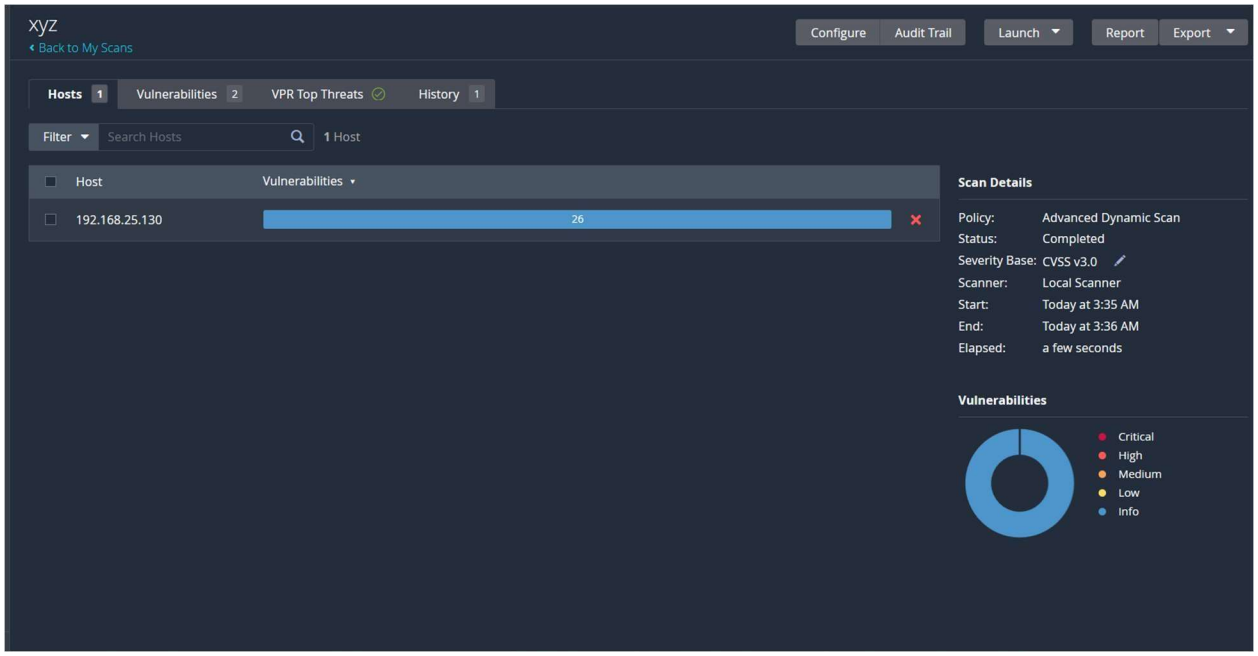
Download Nessus

```
┌──(root㉿kali)-[~]
└─# cd /home/kali/Downloads/

┌──(root㉿kali)-[/home/kali/Downloads]
└─# ls
Nessus-10.3.0-debian9_amd64.deb

┌──(root㉿kali)-[/home/kali/Downloads]
└─# dpkg -i Nessus-10.3.0-debian9_amd64.deb
(Reading database ... 347466 files and directories currently installed.)
Preparing to unpack Nessus-10.3.0-debian9_amd64.deb ...
Unpacking nessus (10.3.0) over (10.3.0) ...
Setting up nessus (10.3.0) ...
Unpacking Nessus Scanner Core Components ...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner
```

Host discovery scan



Dynamic CVE scan



Ransomware: