NEW YORK INSTITUTE
OF TECHNOLOGY

INCS-615: Advanced Network and Internet Security
Lab – Nessus Vulnerability Scanning Platform

Overview:

This lab is focused on letting you gain hands-on experience of a vulnerability scanning platform that is used in the real-world by many of the enterprises. Also, you will need to research about 5 vulnerabilities that are related to Network Scanning and provide information about them.

Download Nessus here:
https://www.tenable.com/downloads/nessus?loginAttempted=true

Tool Tutorial: https://youtu.be/lT6Px9zJM3s

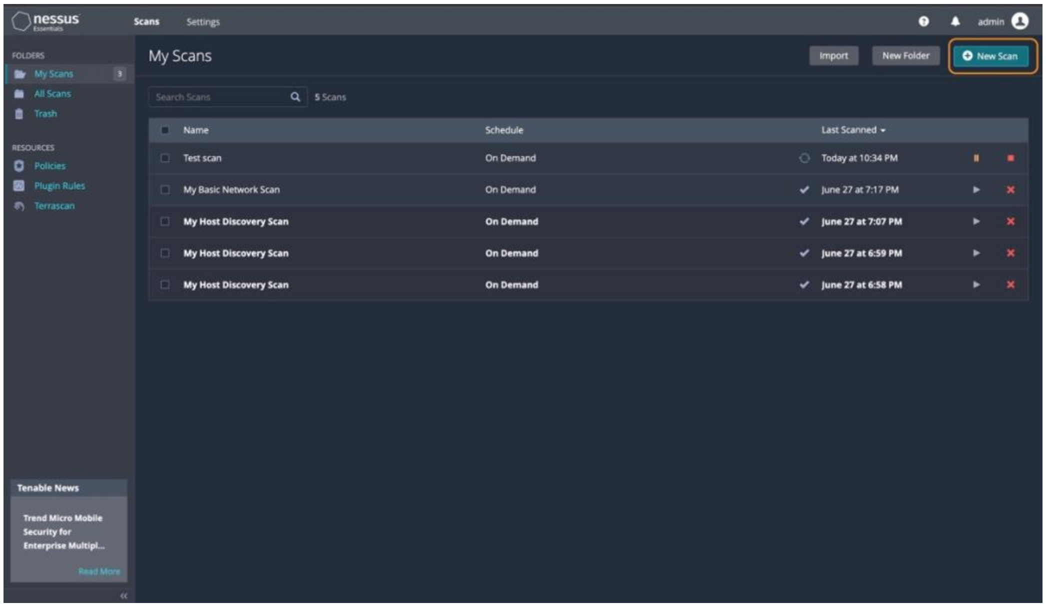
1. Start from 2:50 for the downloading and installation of Nessus. VMWare is not required.
2. Start from 12:00 for knowing about the scanning by the tool.

Default Nessus port is 8834: https://localhost:8834/

NEW YORK INSTITUTE
OF TECHNOLOGY

Steps after downloading and running the Nessus:

Step 1: Select New Scan



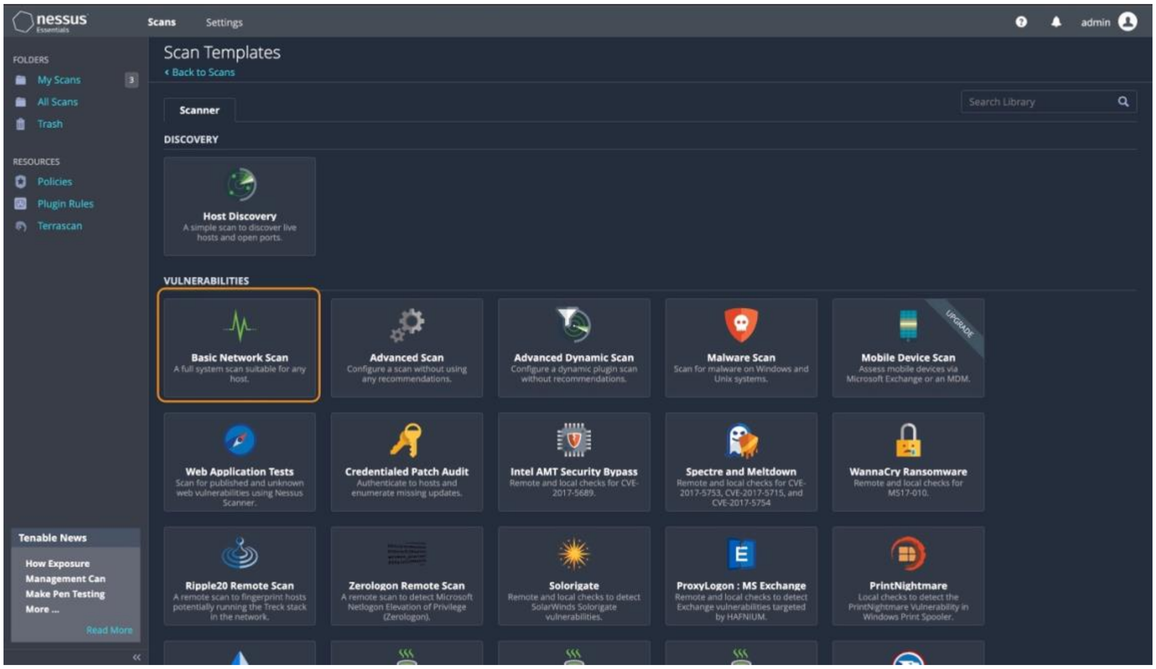
My Scans

5 Scans

Name	Schedule	Last Scanned
Test scan	On Demand	Today at 10:34 PM
My Basic Network Scan	On Demand	June 27 at 7:17 PM
My Host Discovery Scan	On Demand	June 27 at 7:07 PM
My Host Discovery Scan	On Demand	June 27 at 6:59 PM
My Host Discovery Scan	On Demand	June 27 at 6:58 PM

Trend Micro Mobile Security for Enterprise Multipl...

Step 2: Select Basic Network Scan



Scan Templates

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware
Remote and local checks for MS17-010.

Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

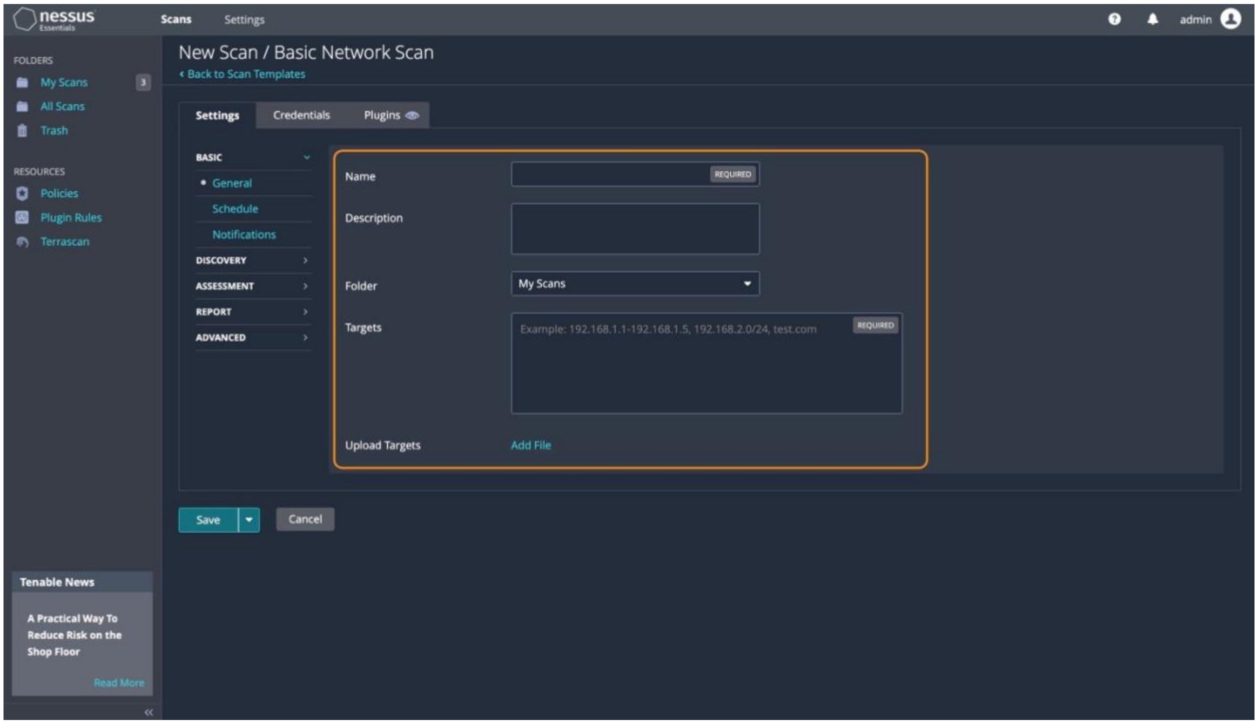
Solorigate
Remote and local checks to detect SolarWinds Solorigate vulnerabilities.

ProxyLogon : MS Exchange
Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

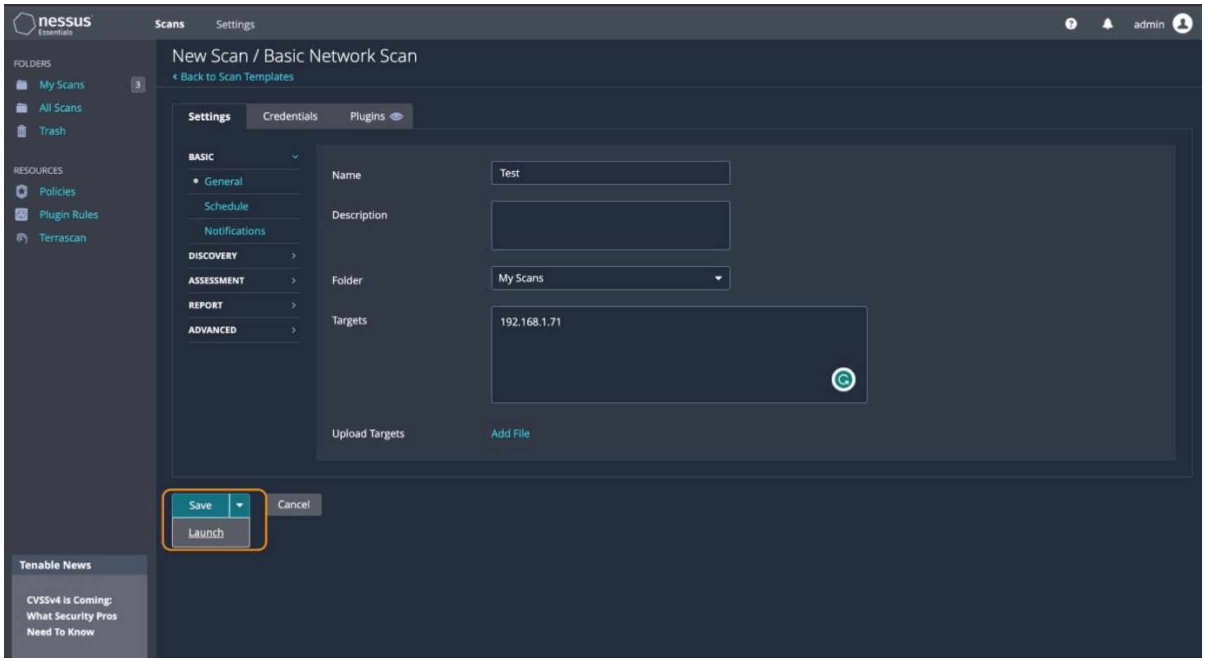
PrintNightmare
Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.

How Exposure Management Can Make Pen Testing More ...

Step 3: Fill the details. Ensure you enter your IP Address



Step 4: Launch Scan from the dropdown


Name: Test

Description:

Folder: My Scans

Targets: 192.168.1.71

Task 1: Network Scanning and finding vulnerabilities.

Find out vulnerabilities in the report on your IP address. Provide information about any of the 2 vulnerabilities from the report and ways to mitigate them. Screenshots of the results required.

Task 2: Generic Network Scanning Vulnerability Research.

1. Research about Network Scanning Vulnerabilities and provide description.
2. Find out 5 network scanning vulnerabilities in general and provide description about those and the mitigation techniques.

Note: If the Network Scanning did not generate at least 2 vulnerabilities other than 'Info' category, research about 2 vulnerabilities and provide description and mitigation techniques. A report screenshot is required showing the results do not contain at least 2 vulnerabilities other than Info category.