THE NORTHCAP UNIVERSITY

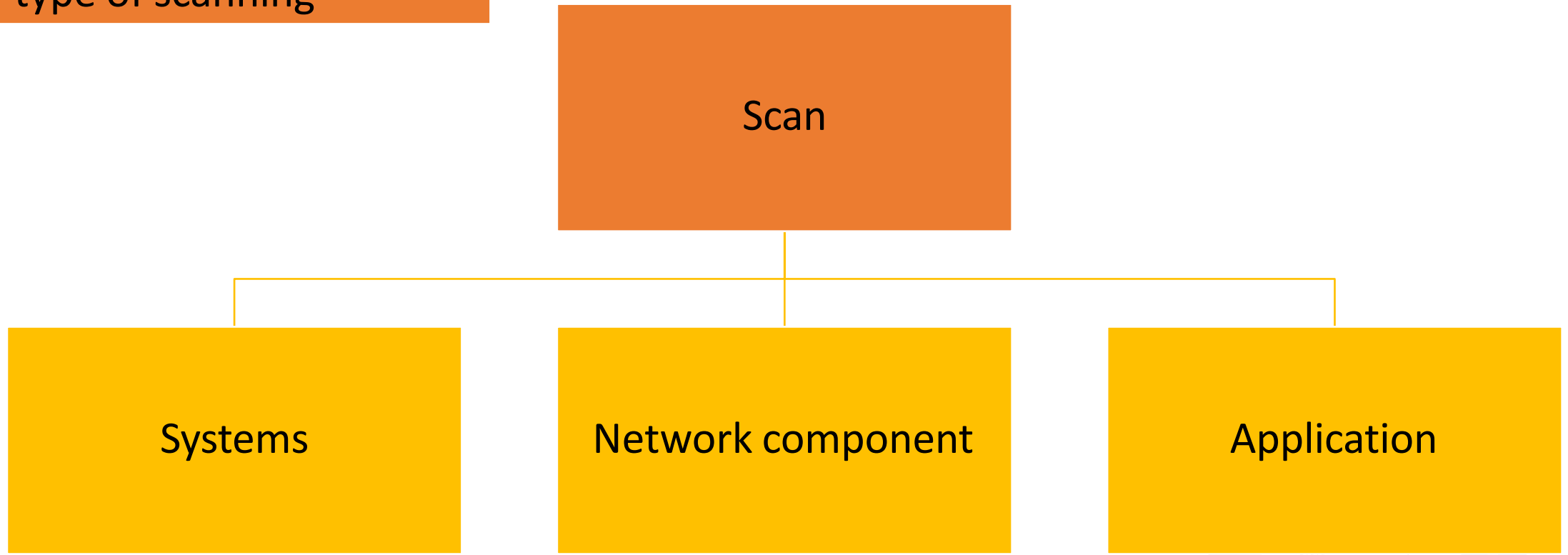
Vulnerability Scanning

30 YEARS OF EXCELLENCE

NAAC Accredited

Vulnerability scanning

Vulnerability scanning is another type of scanning



Vulnerability scanning

THE NORTHCAP UNIVERSITY

It includes a **database of vulnerabilities** based on which it **performs the check** on the remote host.

Database **contains** (service, port, packet type, a potential path to exploit, etc.) to **check the security issue**.

They can scan the network and websites **against thousands of vulnerabilities**, provide the list of issues and **suggest the remediation as well**.

Features of Popular scanners

THE NORTHCAP UNIVERSITY

Maintain an **updated** database for **latest vulnerabilitie s**.

Detect vulnerabilities with **less false positive.**

Scan multiple targets simultaneously.

Provide a **detailed report** with vulnerabilities

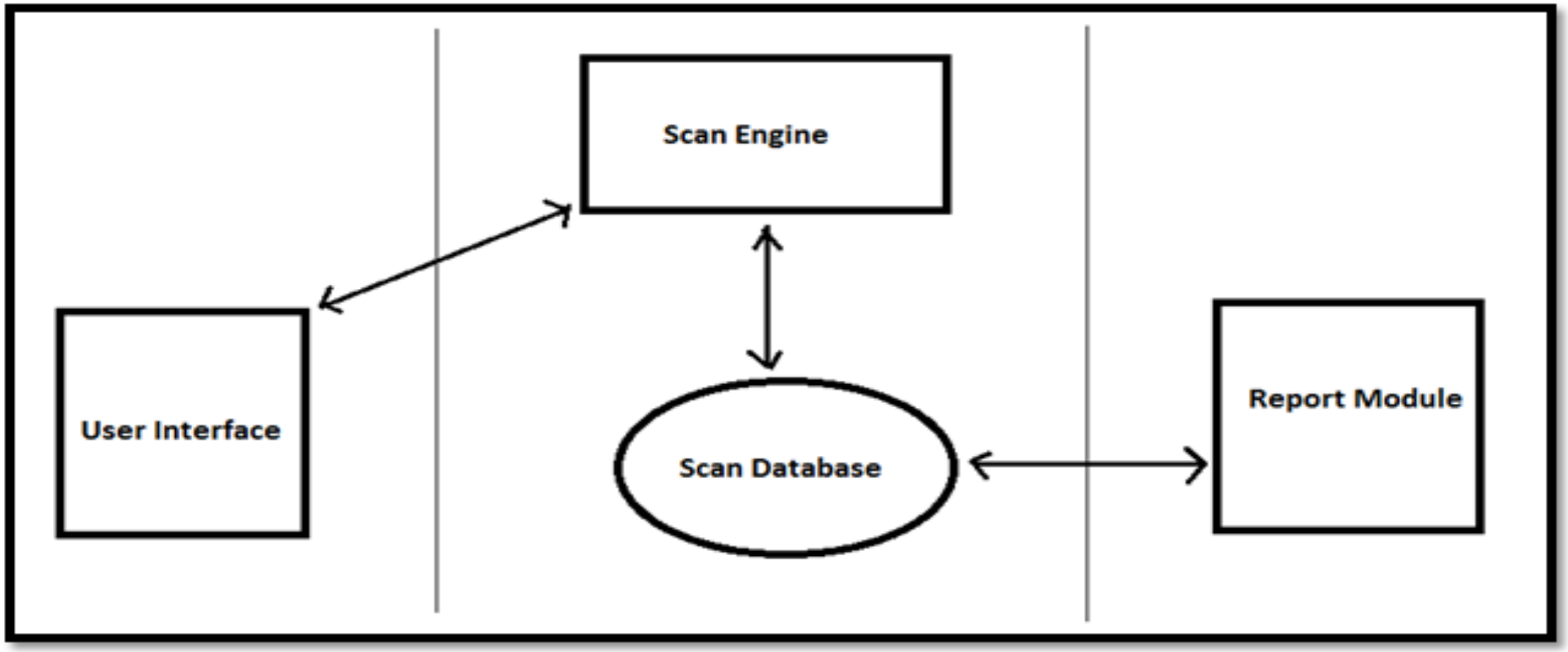
Recommenda tion to fix the vulnerabilities .

Fast and can save you time

30 YEARS OF EXCELLENCE

NAAC Accredited

Scanner Architecture



Components of Scanner

THE NORTHCAP UNIVERSITY

1. User Interface

Interface with which **user interacts to run or configure** a scan.

Can be a GUI or CLI

2. Scan Engine

Execute the scan based on the **installed and configured plug-ins.**

3. Scan Database:

Stores the data required by the scanner

1) contain **vulnerability information**,

2)steps to mitigate the vulnerability,

3)CVE- ID mapping (Common Vulnerability and Exposures)

4) scan results, etc.

4. Report Module:

Provides the options to **generate** the different type of **reports** like

1) Detailed report,

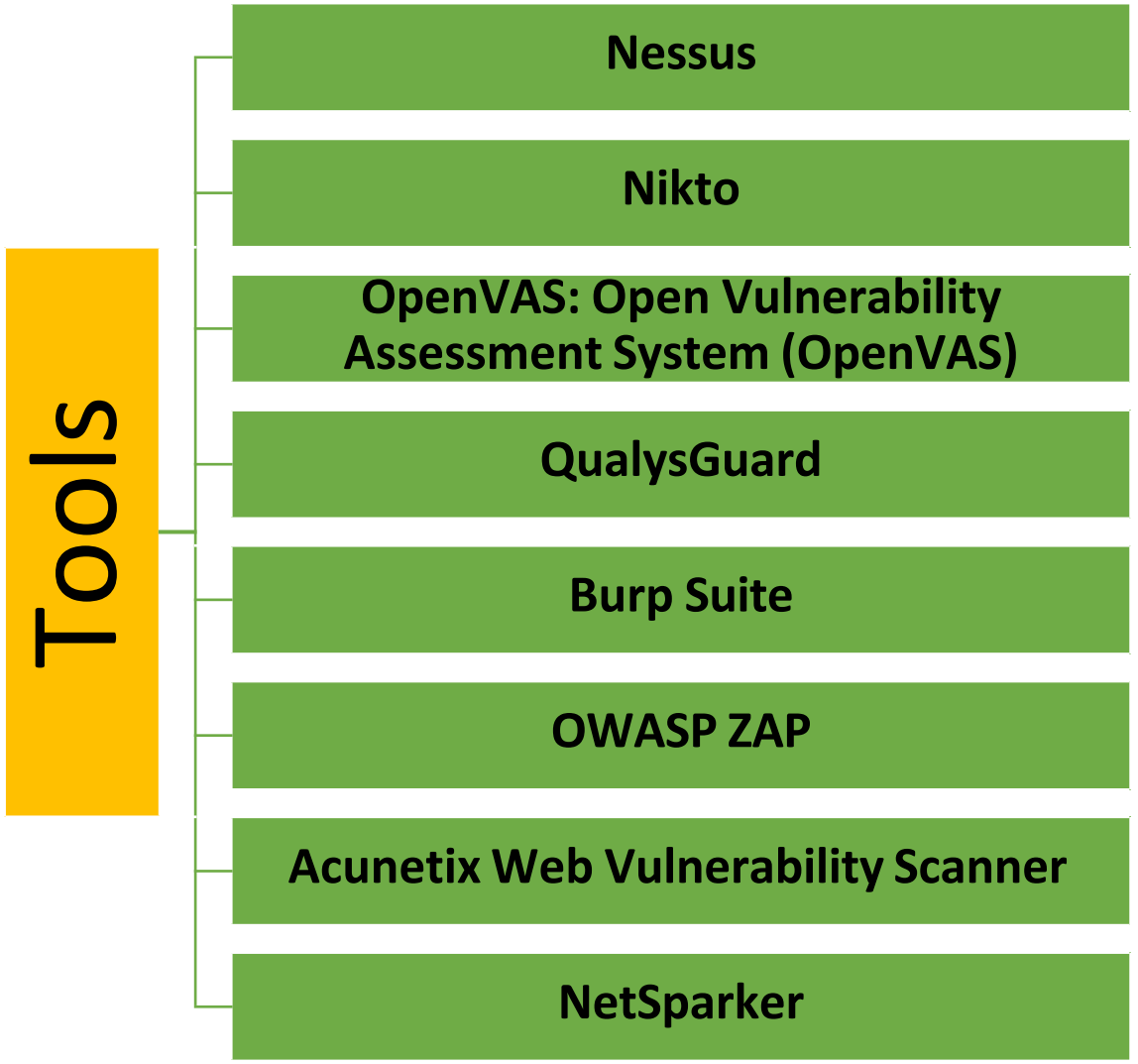
2) Vulnerabilities List

3) Graphical report, etc.

30 YEARS OF EXCELLENCE

NAAC Accredited

Top Vulnerability scanner tools



Tool 1: Nikto

Nikto

Nikto

- **Scan webservers for**
  - Vulnerabilities
  - **Dangerous files**,
  - **Outdated server software**
  - Other problems.

Advantages

- **Easy to use** without much instructions
- Performs **generic and server type specific checks**.
- Captures any **cookies received**.

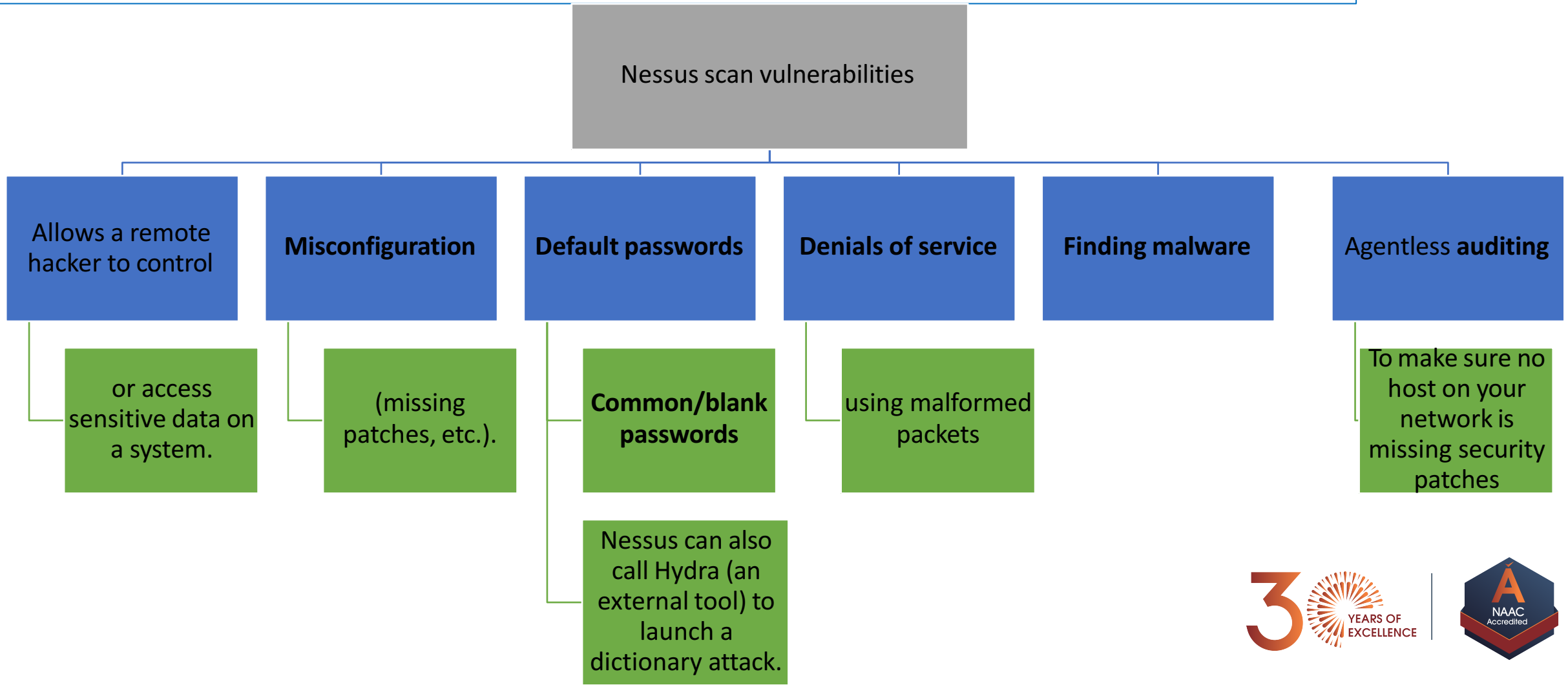
Tool 2: Nessus

Introduction to NESSUS

Nessus

- Nessus developed by **Tenable Network Security**
  It is **free of charge for personal use** in a non-enterprise environment For **enterprise,**
- **1500$/year**.
- Used by over **75,000 organizations worldwide.**
- Begins by **port scan** with one of its four internal port scanners (or can optionally use Nmap)
- To determine which ports are open on the target and then tries various exploits on them
- **New vulnerability checks** (**called plugins**) on a daily basis.

NESSUS: Applications



NESSUS

THE NORTHCAP UNIVERSITY

- The **user manual** can be downloaded From http://static.tenable.com/documentation/nessus_6.4_user_guide.pdf

- The **Nessus scanner** can be downloaded from http://www.tenable.com/products/nessus/select-your-operating-system

Nessus

THE NORTHCAP UNIVERSITY

What is a Plugin?

- Every audit in the Tenable Nessus® vulnerability scanner is **coded as a plugin**: a simple program which **checks for a given flaw**.
- Nessus uses more than **60,000+ different plugins**, covering local and remote flaws.

Staying Up-to-Date?

- New vulnerabilities are discovered and published **every day**.
- As a result, staying up-to-date is a must if you want to perform a security scan. Every week, several dozens of plugins are added in the Tenable Nessus plugin feeds.

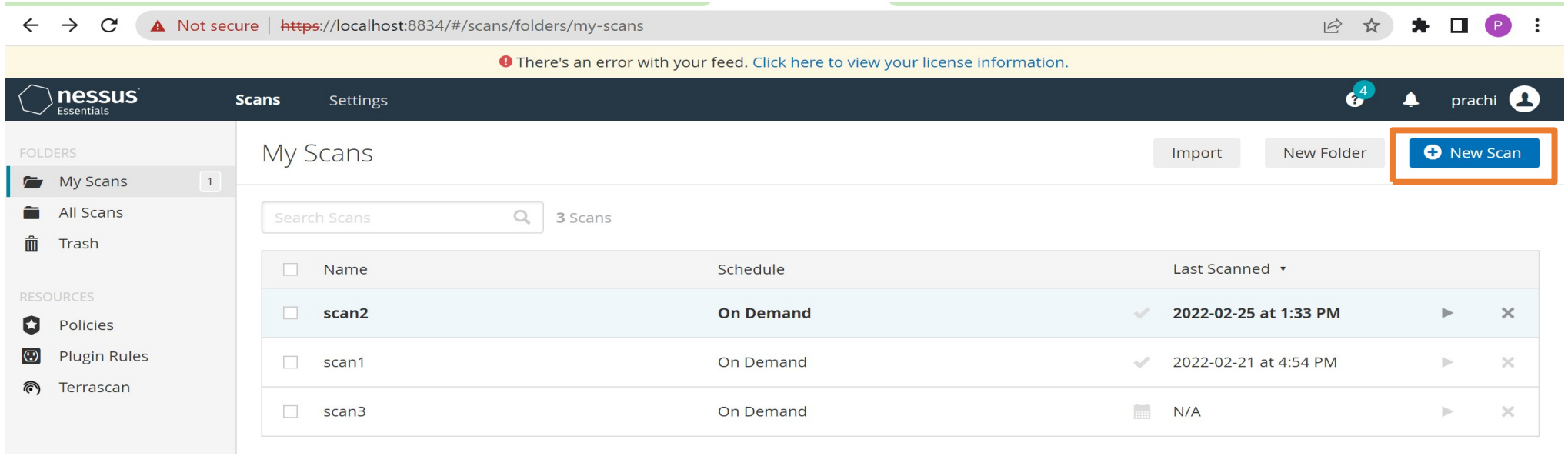
30 YEARS OF EXCELLENCE

NAAC Accredited

Nessus Steps

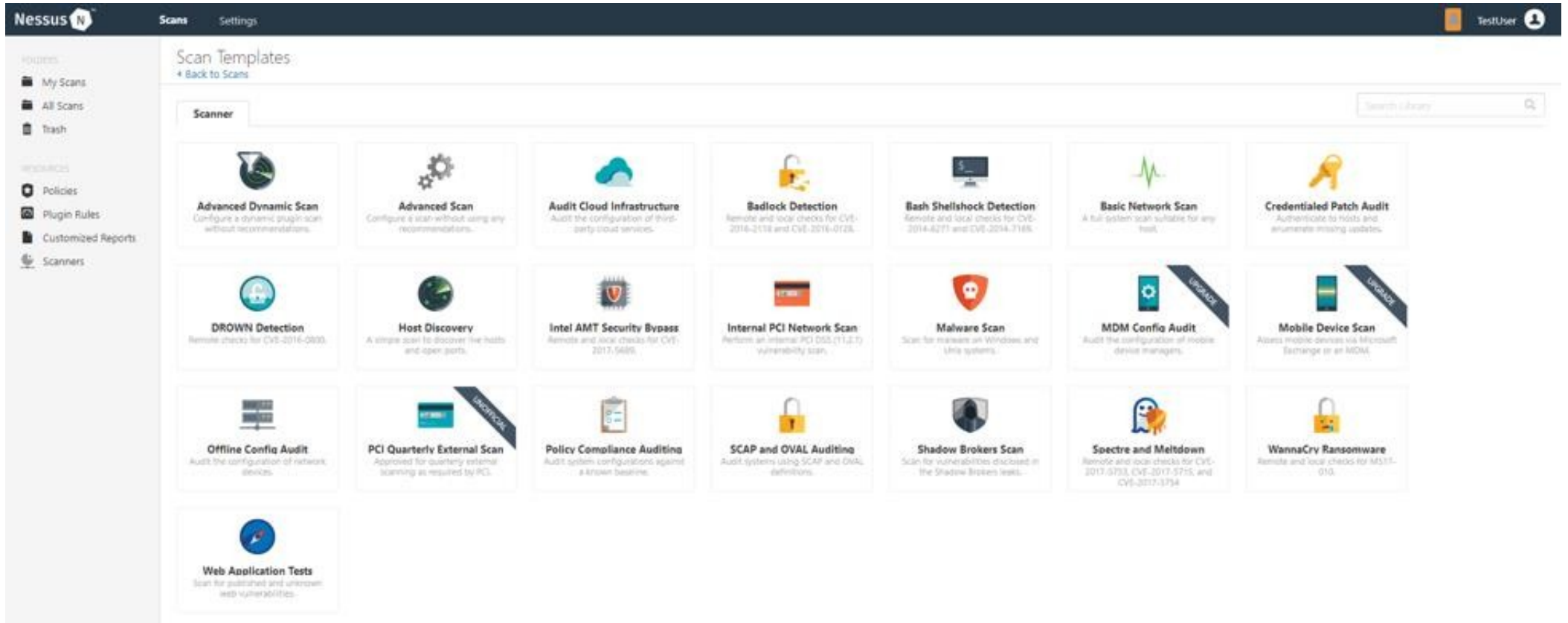
Step 1: Creating a Scan

- To create your scan:
  - In the upper-right corner of the My Scans page, click the New Scan button.



Nessus Steps

- Step 2: Choose a Scan Template

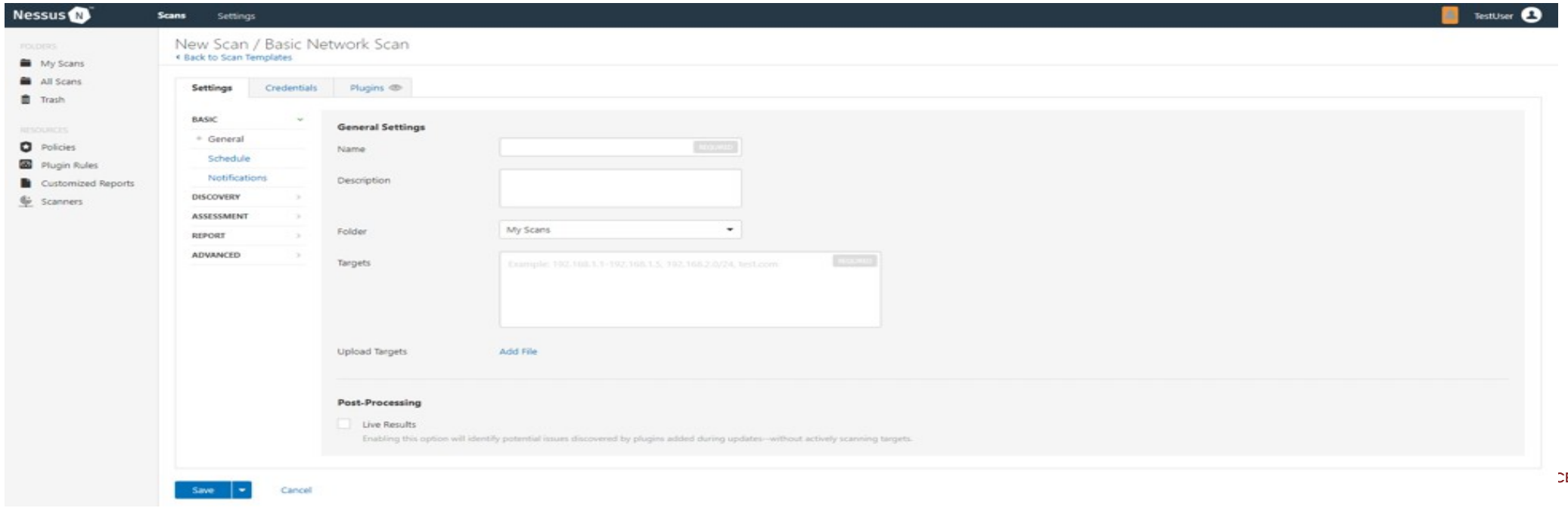


- refer to Scan and Policy Settings in the Nessus User Guide.

Nessus Steps

Step 3: Configure Scan Settings

- Prepare your scan by configuring the settings available for your chosen template.
  - The Basic Network Scan template has several default settings preconfigured, which allows you to quickly perform your first scan and view results without a lot of effort.



Nessus Steps

THE NORTHCAP UNIVERSITY

Step 3: Con figure Scan Settings

1. Configu re the settings in the Bas ic Settings section

The follo wing are Basic settings:

Setting	Description
Name	Specifies the name of the scan or policy. This value is displayed on the Nessus interface.
Description	(Optional) Specifies a description of the scan or policy.
Folder	Specifies the folder where the scan appears after being saved.
Targets	Specifies one or more targets to be scanned. If you select a target group or upload a targets file, you are not required to specify additional targets.

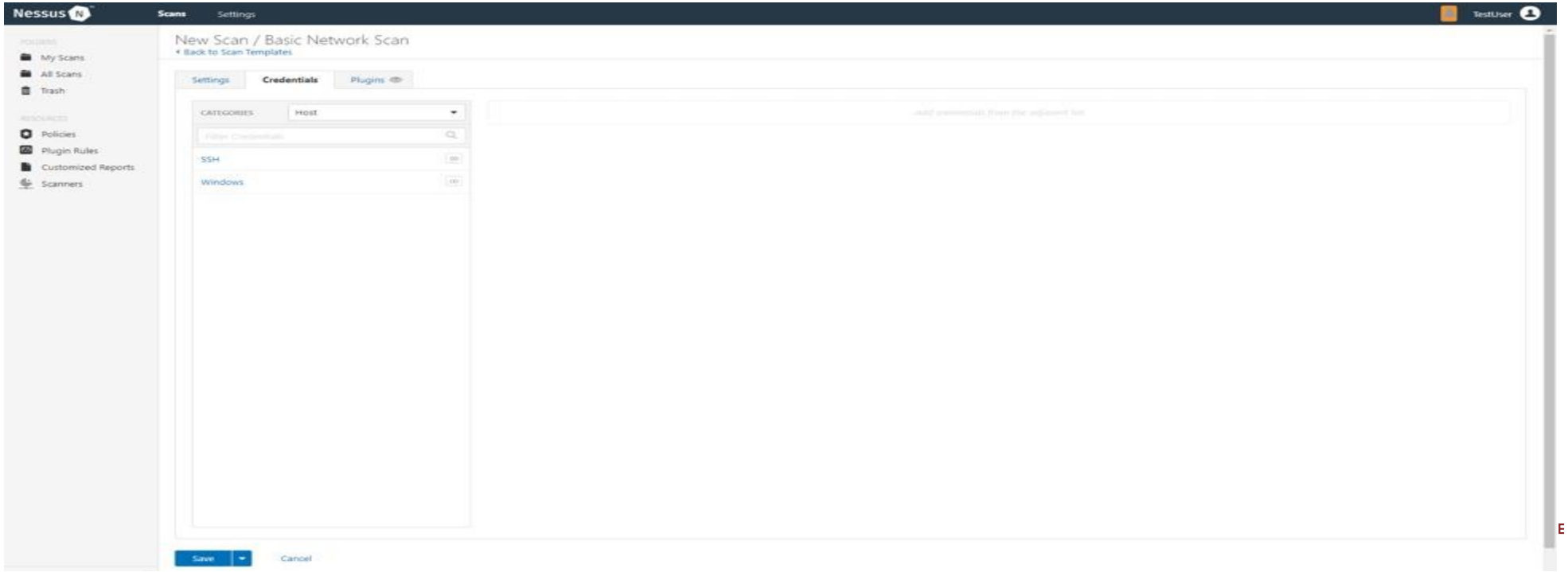
NAAC Accredited

Nessus Steps

Step 3: Configure Scan Settings

3. Configure Credentials

- Optionally, you can configure Credentials for a scan. This allows credentialed scans to run, which can provide much more complete results and a more thorough evaluation of the vulnerabilities in your environment.



Nessus Steps

THE NORTHCAP UNIVERSITY

Step 4: Launch Scan

- After you have configured all your settings, you can click the Save button.
- Click launch to launch the scan immediately
- The time it takes to complete a scan involves many factors, such as network speed and congestion, so the scan may take some time to run.

30 YEARS OF EXCELLENCE | NAAC Accredited

Nessus Steps

THE NORTHCAP UNIVERSITY

Step 5: Viewing Your Results

To view vulnerabilities:

1. In the top navigation bar, click Scans.
2. Click the scan for which you want to view results.
3. Do one of the following:
    1. Click a specific host to view vulnerabilities found on that host.
    2. Click the Vulnerabilities tab to view all vulnerabilities.
4. (Optional) To sort the vulnerabilities, click an attribute in the table header row to sort by that attribute.
5. Clicking on the vulnerability row will open the vulnerability details page, displaying plugin information and output for each instance on a host.

30 YEARS OF EXCELLENCE

NAAC Accredited

Nessus Steps

THE NORTHCAP UNIVERSITY

Step 5: Vie wing Your Results

- Viewin g scan results can help y ou understand your organization's security posture an d vulner abilities.

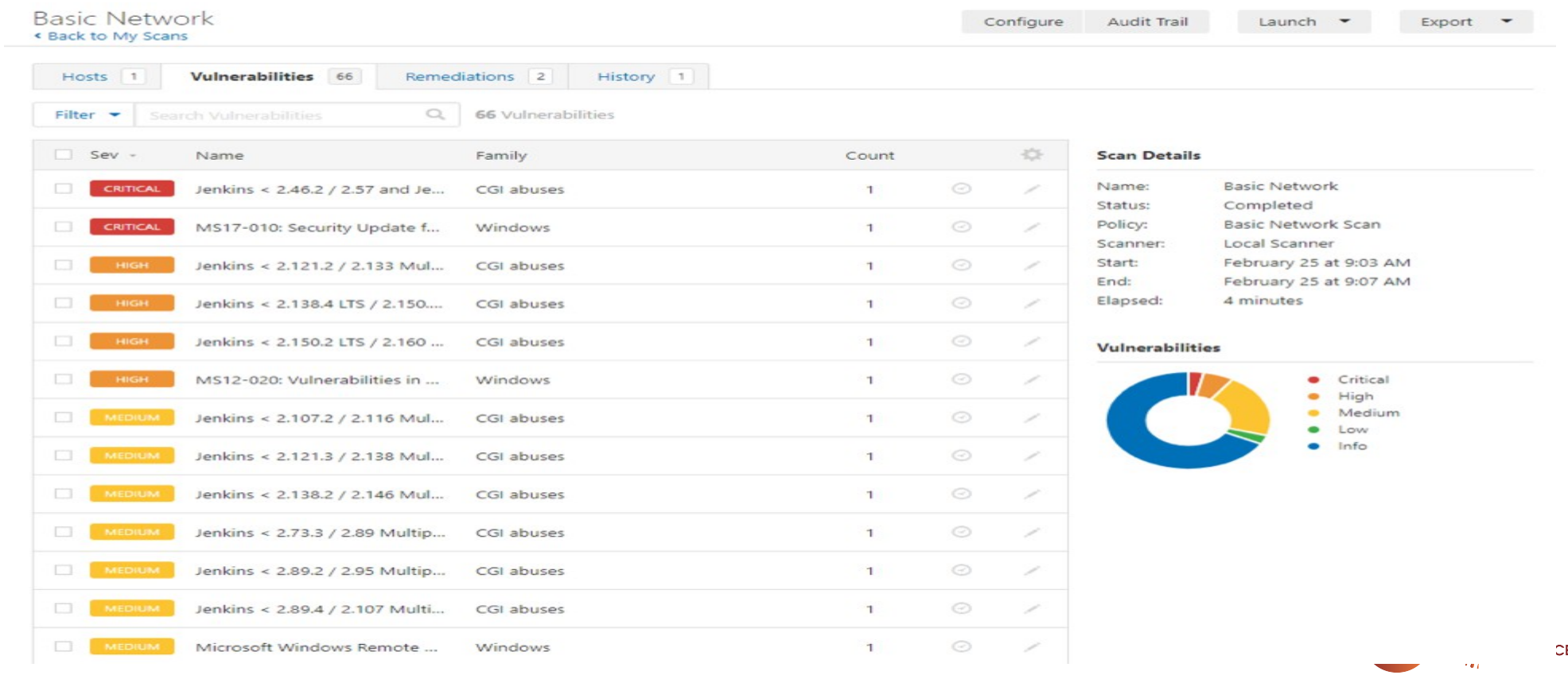
age	Description
Hosts	Displays all scanned targets.
Vulnerabilities	List of identified vulnerabilities, sorted by severity.
Remediations	If the scan's results include remediation information, this list displays all remediation details, sorted by the number of vulnerabilities.
Notes	Displays additional information about the scan and the scan's results.
History	Displays a list of scans: Start Time, End Time, and the Scan Statuses.

NAAC Accredited

Nessus Steps

Step 5: Viewing Your Results

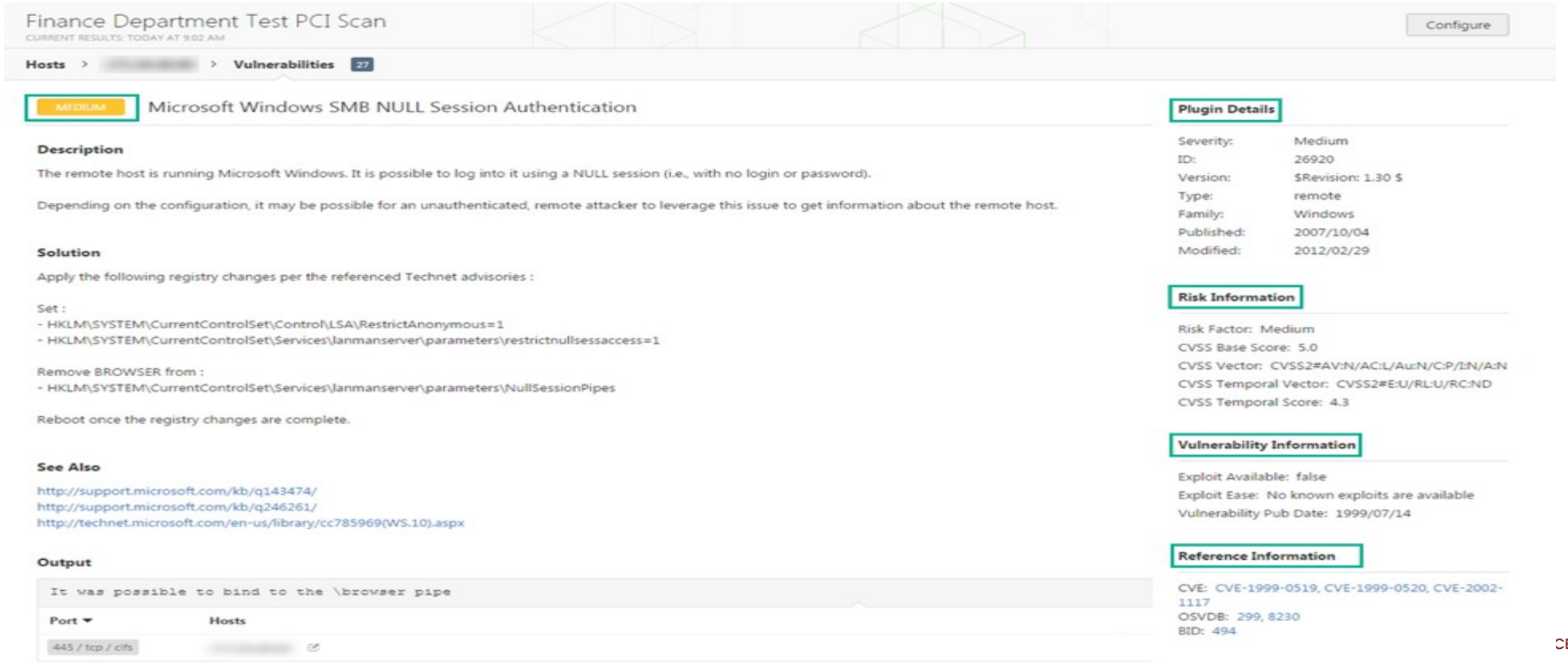
- Viewing scan results by vulnerabilities gives you a view into potential risks on your assets.



Nessus Steps

Step 5: Viewing Your Results

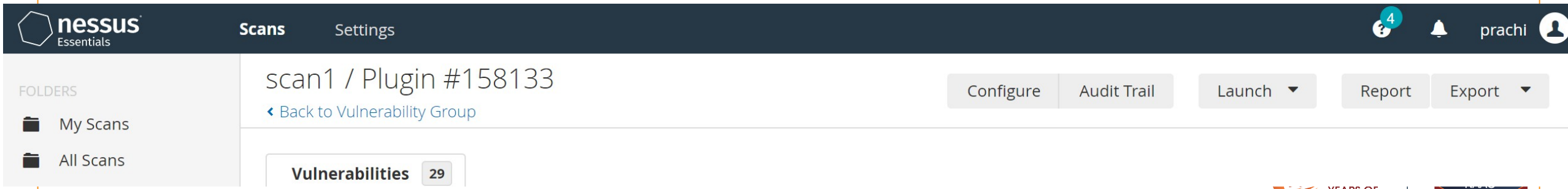
To view vulnerabilities:



Nessus Steps

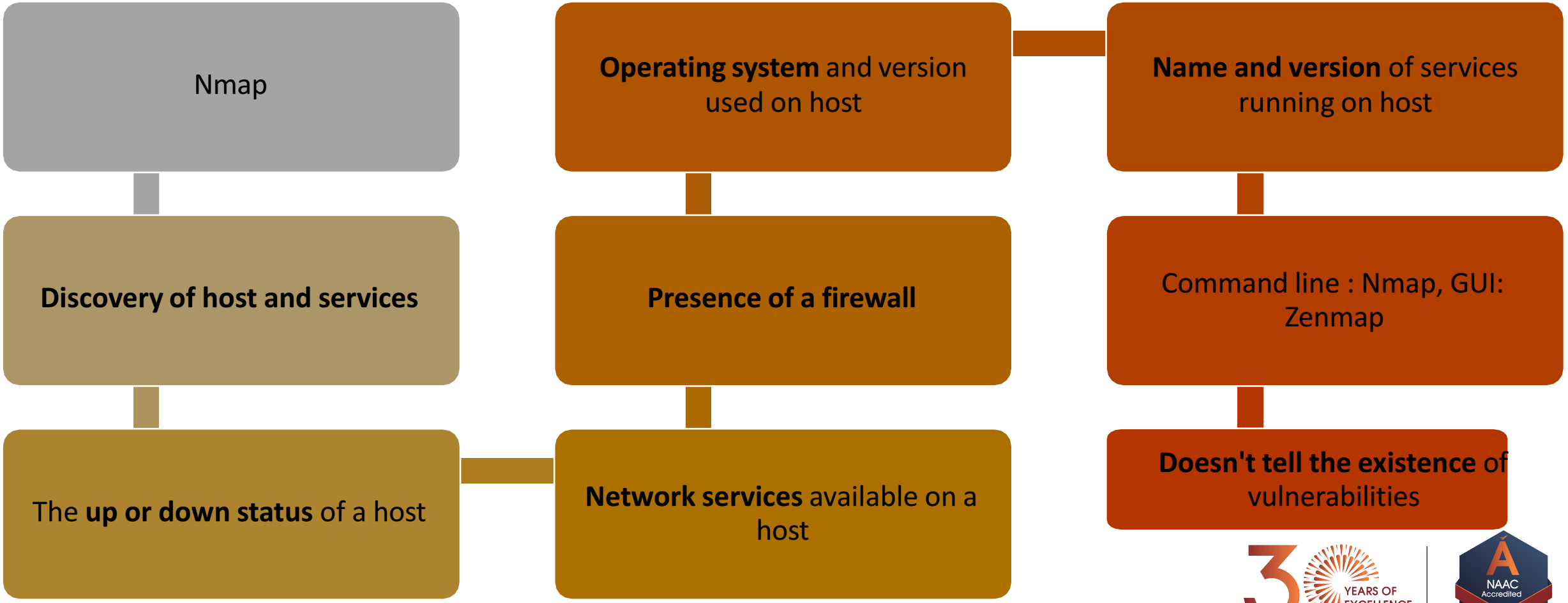
- Step 6: Reporting Your Results
  - Now you need to report your findings to your team.
  - Scan results can be exported in several file formats.

- To Export a Scan Report:
  - Start from a scan's results page
  - In the upper-right corner, click Export.



Nessus vs Nmap

Nmap (port scanning tool)



Nessus

THE NORTHCAP UNIVERSITY

Nessus is

vulnerability scanner, Although it scans ports just like NMAP

Checks for open ports and its potential vulnerabilities

Policies set *what* will be scanned along with *how* it'll be scanned (external or internal)

Administrators set up policies, scans and view reports.

Over **60,000 plugins** look for vulnerabilities in **Operating Systems (Unix, Linux, Windows) to specific application categories**

In Class Exercise

THE NORTHCAP UNIVERSITY

Implement Nessus on website and generate report

Write steps and attach screenshot of each step

30 YEARS OF EXCELLENCE

NAAC Accredited

Home Exercise