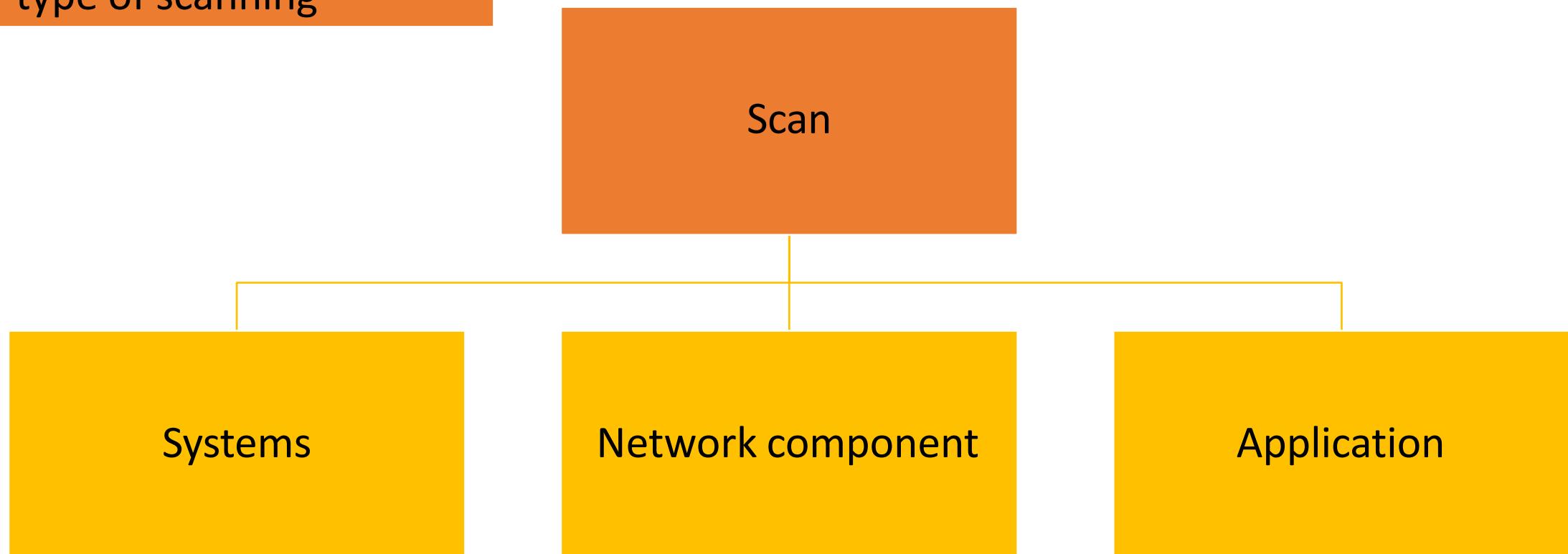


Vulnerability Scanning



Vulnerability scanning

Vulnerability scanning is another type of scanning



Vulnerability scanning

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

Maintain an **updated** database for **latest vulnerabilities**.

Detect vulnerabilities with **less false positive.**

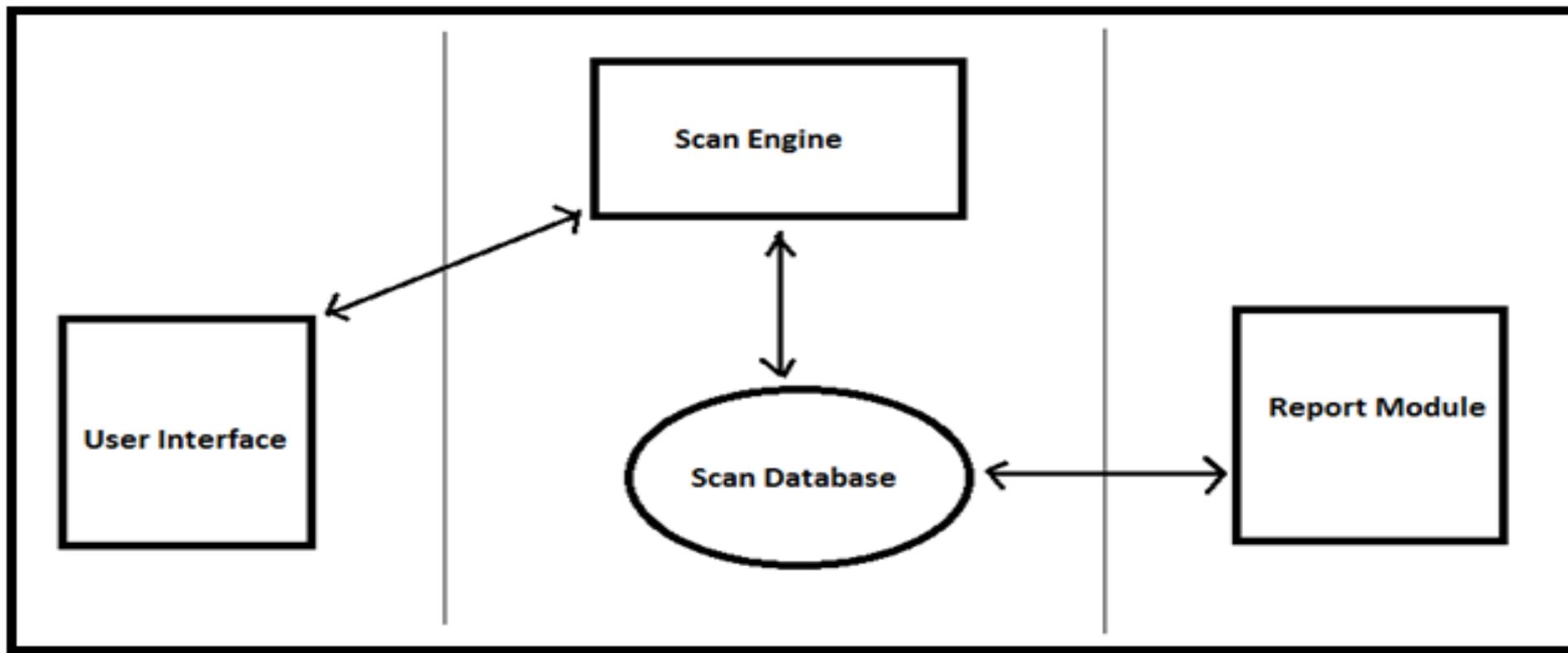
Scan multiple targets simultaneously.

Provide a **detailed report** with vulnerabilities

Recommendation to fix the vulnerabilities .

Fast and can save you time

Scanner Architecture



Components of Scanner

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

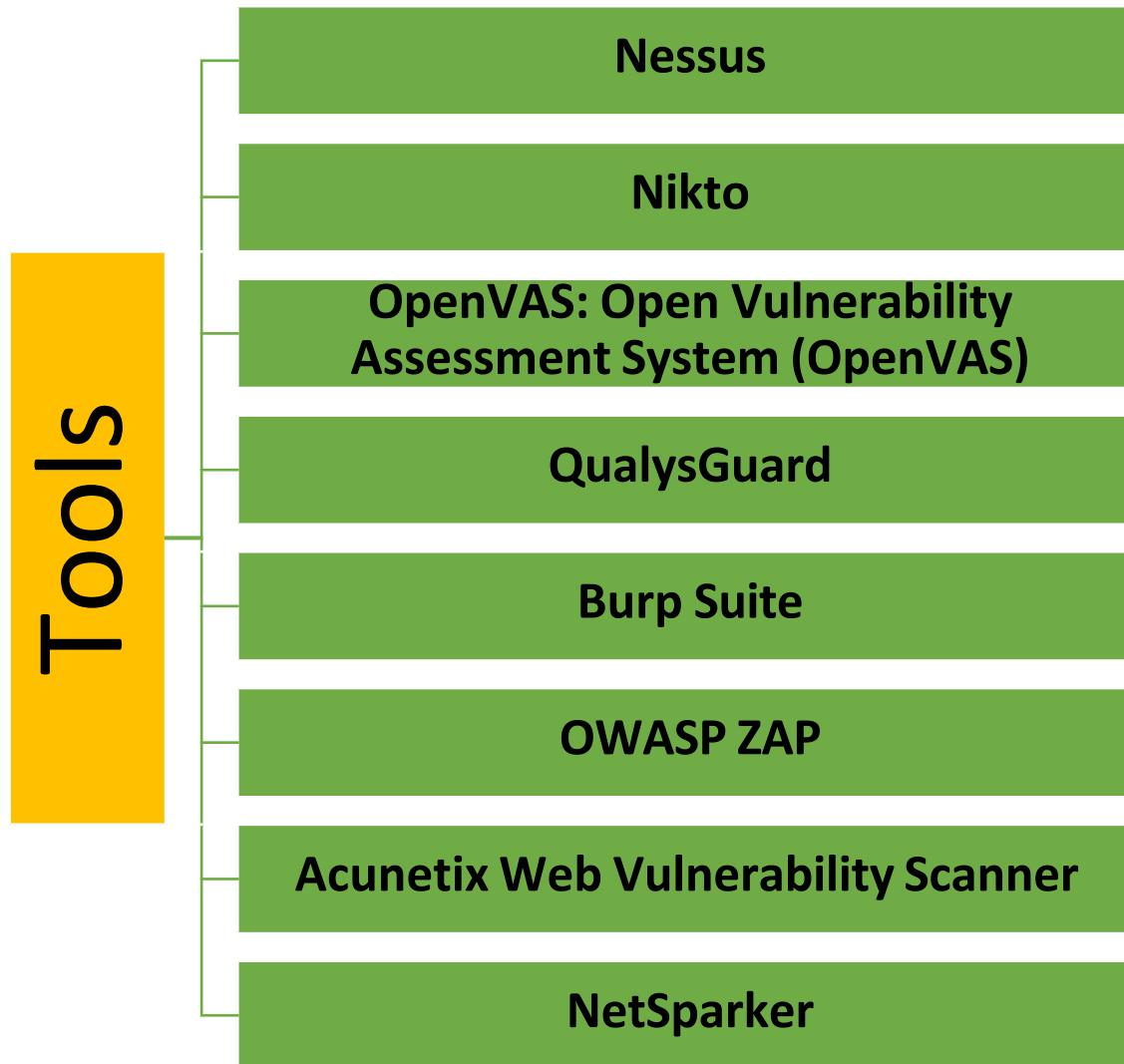
1) Detailed report,

2) Vulnerabilities List

3) Graphical report, etc.



Top Vulnerability scanner tools



Tool 1: 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 - Outdated server software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.

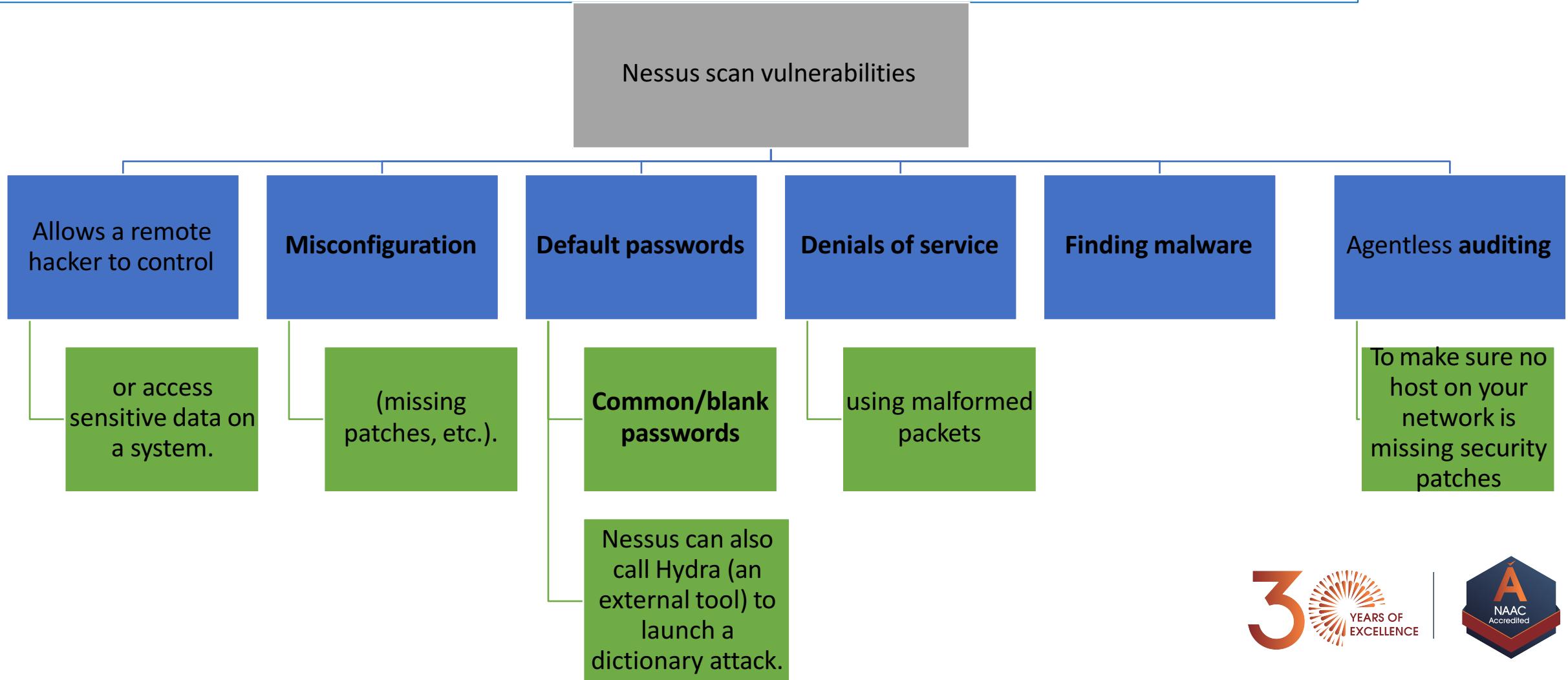
Tool 2: Nessus

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



- 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>

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.

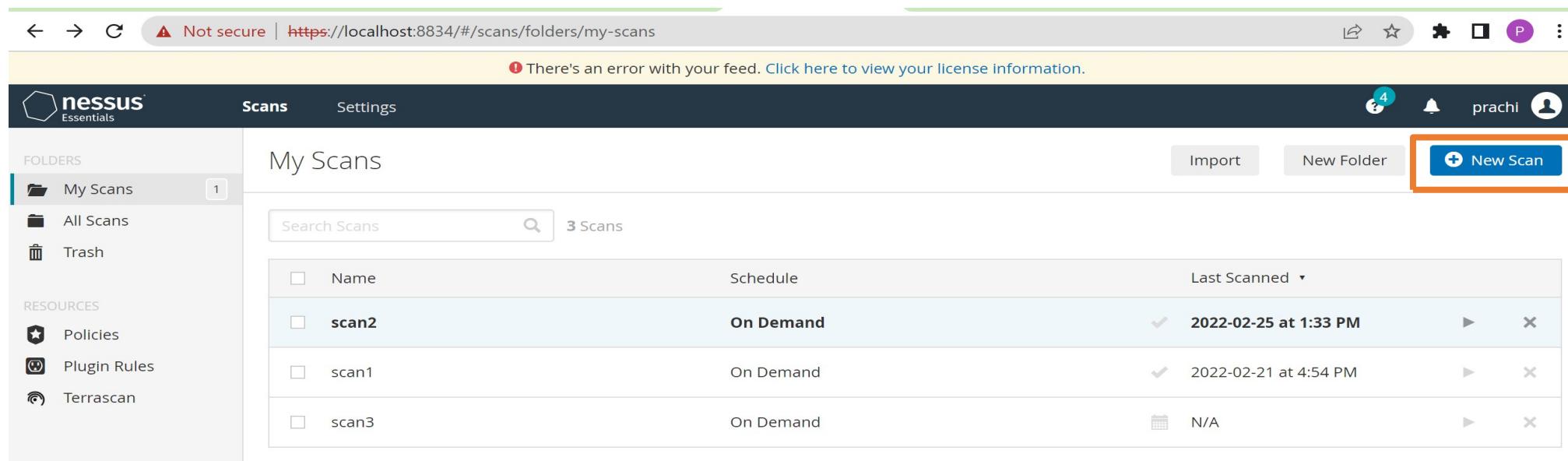
Staying Up-to-Date?

- 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.

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.



The screenshot shows the Nessus Essentials interface. The top navigation bar includes links for 'Scans' and 'Settings'. A message at the top right says, 'There's an error with your feed. Click here to view your license information.' On the far right, there are notifications (4), a bell icon, and a user profile for 'prachi'. Below the navigation is a sidebar with 'FOLDERS' containing 'My Scans' (1), 'All Scans', and 'Trash'. Under 'RESOURCES' are 'Policies', 'Plugin Rules', and 'Terrascan'. The main area is titled 'My Scans' and shows a table with three rows of scan details:

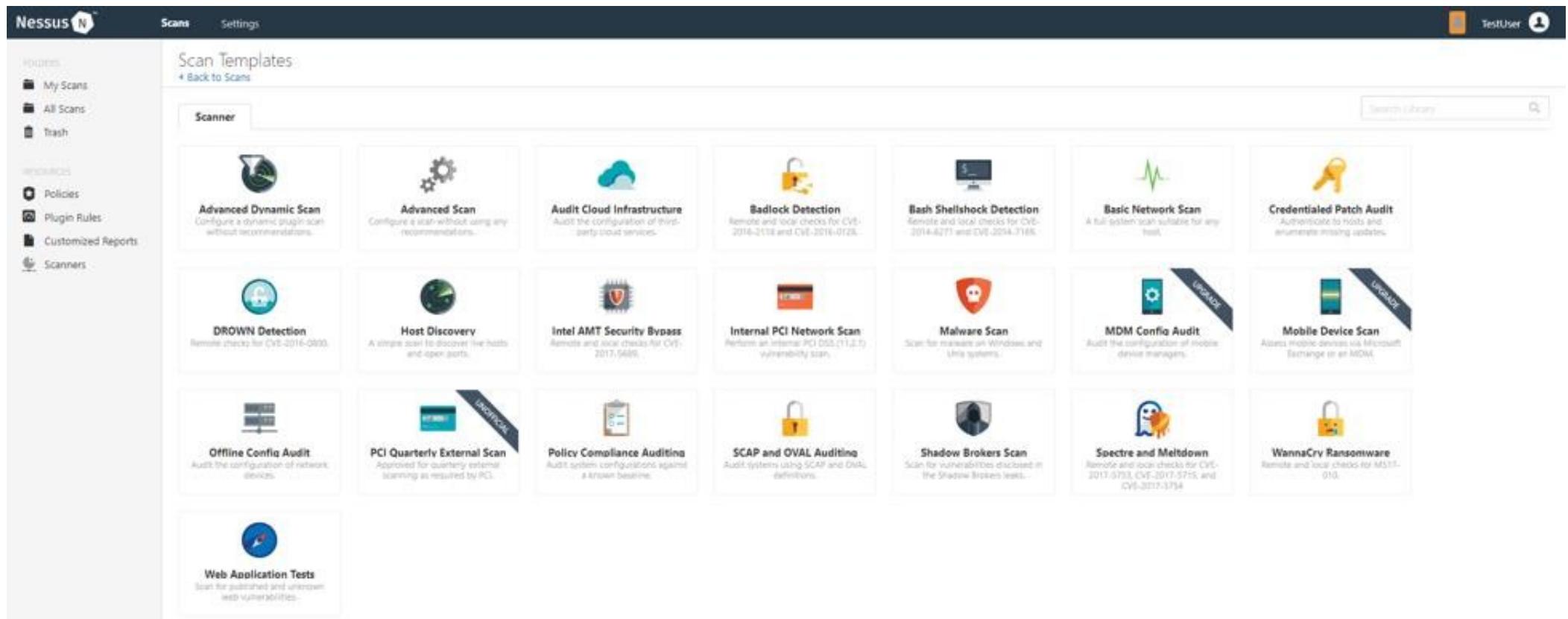
Name	Schedule	Last Scanned
scan2	On Demand	2022-02-25 at 1:33 PM
scan1	On Demand	2022-02-21 at 4:54 PM
scan3	On Demand	N/A

At the top right of this section are buttons for 'Import', 'New Folder', and a prominent blue 'New Scan' button, which is highlighted with an orange box.



Nessus Steps

- Step 2: Choose a Scan Template

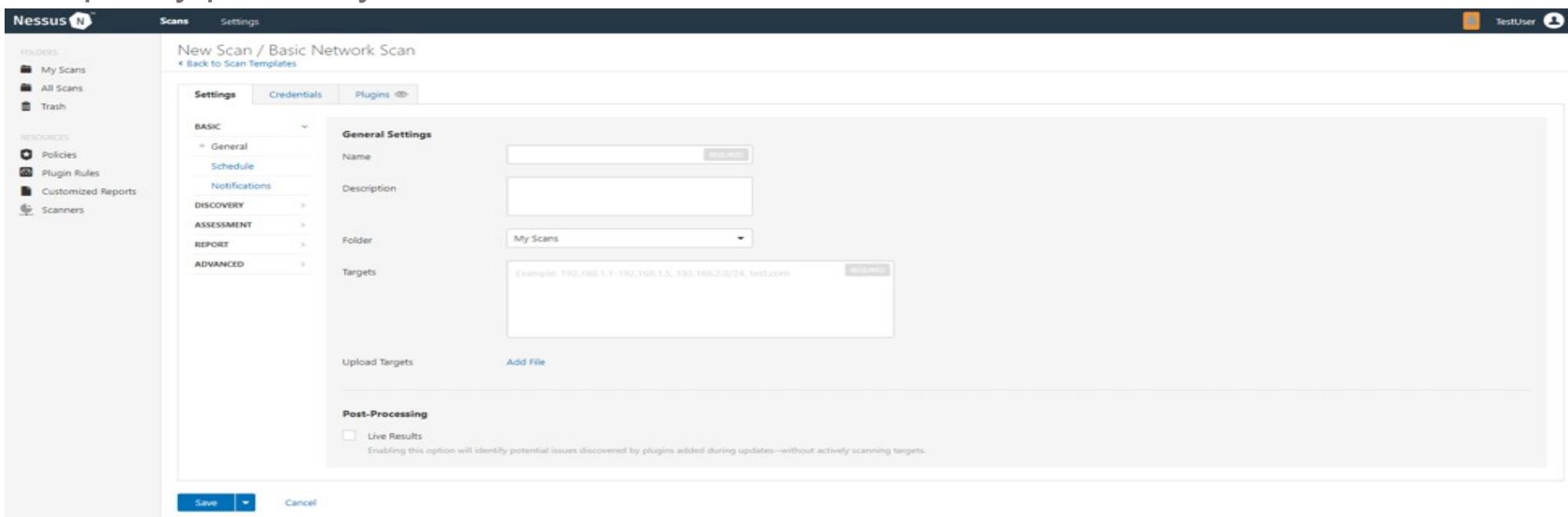


- refer to [Scan and Policy Settings](#) in the Nessus User Guide.

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

Step 3: Configure Scan Settings

1. Configure the settings in the Basic Settings section

The following 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.

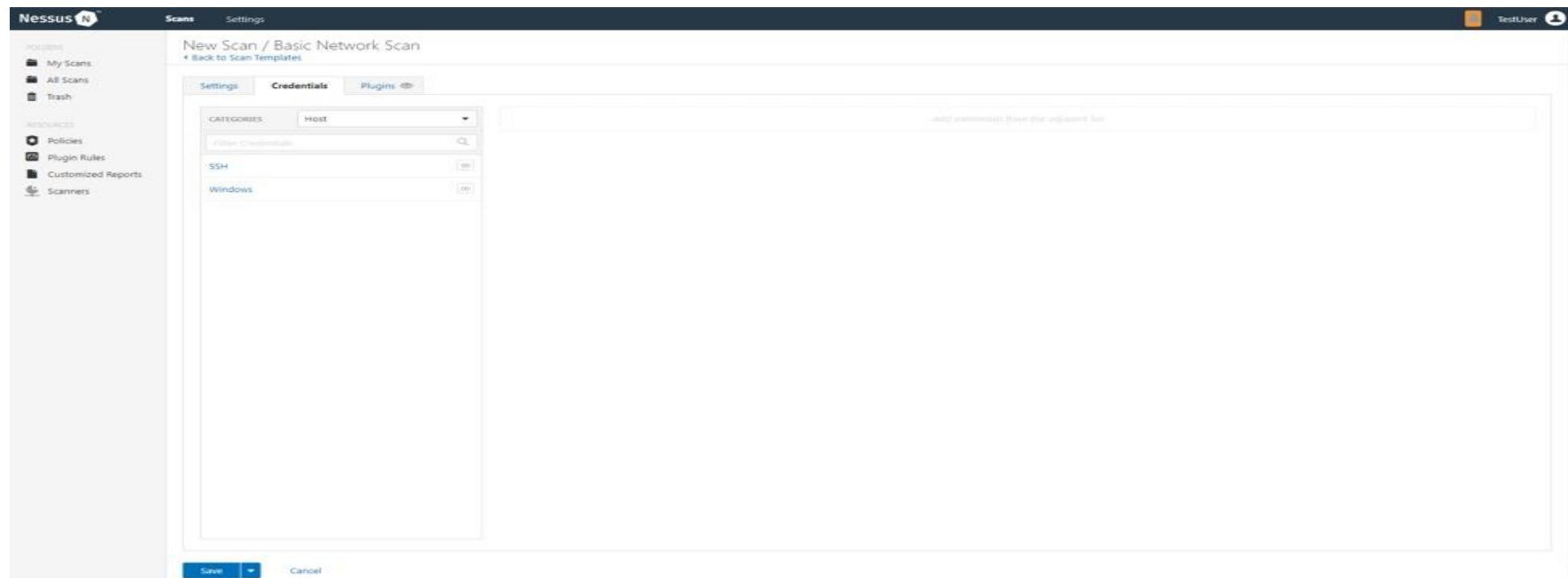


Nessus Steps

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

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.

Nessus Steps

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.



Nessus Steps

Step 5: Viewing Your Results

- Viewing scan results can help you understand your organization's security posture and vulnerabilities.

Page	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.



Nessus Steps

Step 5: Viewing Your Results

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

Basic Network
[Back to My Scans](#)

Configure Audit Trail Launch Export

Hosts	1	Vulnerabilities	66	Remediations	2	History	1
Filter	Search Vulnerabilities	66 Vulnerabilities					
Sev	Name	Family	Count				
Critical	Jenkins < 2.46.2 / 2.57 and Je...	CGI abuses	1				
Critical	MS17-010: Security Update f...	Windows	1				
High	Jenkins < 2.121.2 / 2.133 Mul...	CGI abuses	1				
High	Jenkins < 2.138.4 LTS / 2.150....	CGI abuses	1				
High	Jenkins < 2.150.2 LTS / 2.160 ...	CGI abuses	1				
High	MS12-020: Vulnerabilities in ...	Windows	1				
Medium	Jenkins < 2.107.2 / 2.116 Mul...	CGI abuses	1				
Medium	Jenkins < 2.121.3 / 2.138 Mul...	CGI abuses	1				
Medium	Jenkins < 2.138.2 / 2.146 Mul...	CGI abuses	1				
Medium	Jenkins < 2.73.3 / 2.89 Multip...	CGI abuses	1				
Medium	Jenkins < 2.89.2 / 2.95 Multip...	CGI abuses	1				
Medium	Jenkins < 2.89.4 / 2.107 Multi...	CGI abuses	1				
Medium	Microsoft Windows Remote ...	Windows	1				

Scan Details

Name:	Basic Network
Status:	Completed
Policy:	Basic Network Scan
Scanner:	Local Scanner
Start:	February 25 at 9:03 AM
End:	February 25 at 9:07 AM
Elapsed:	4 minutes

Vulnerabilities



● Critical
● High
● Medium
● Low
● Info

CE



Nessus Steps

Step 5: Viewing Your Results

To view vulnerabilities:

Finance Department Test PCI Scan
CURRENT RESULTS: TODAY AT 9:02 AM

Hosts > [REDACTED] > Vulnerabilities 27

MEDIUM Microsoft Windows SMB NULL Session Authentication

Description
The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password). Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

Solution
Apply the following registry changes per the referenced Technet advisories :

Set :
- HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1

Remove BROWSER from :
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes

Reboot once the registry changes are complete.

See Also
<http://support.microsoft.com/kb/q143474/>
<http://support.microsoft.com/kb/q246261/>
[http://technet.microsoft.com/en-us/library/cc785969\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx)

Output
It was possible to bind to the \browser pipe

Port	Hosts
445 / tcp / cifs	[REDACTED]

Plugin Details

Severity: Medium
ID: 26920
Version: \$Revision: 1.30 \$
Type: remote
Family: Windows
Published: 2007/10/04
Modified: 2012/02/29

Risk Information

Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/E:N/A:N
CVSS Temporal Vector: CVSS2#E:U/RL:U/RC:ND
CVSS Temporal Score: 4.3

Vulnerability Information

Exploit Available: false
Exploit Ease: No known exploits are available
Vulnerability Pub Date: 1999/07/14

Reference Information

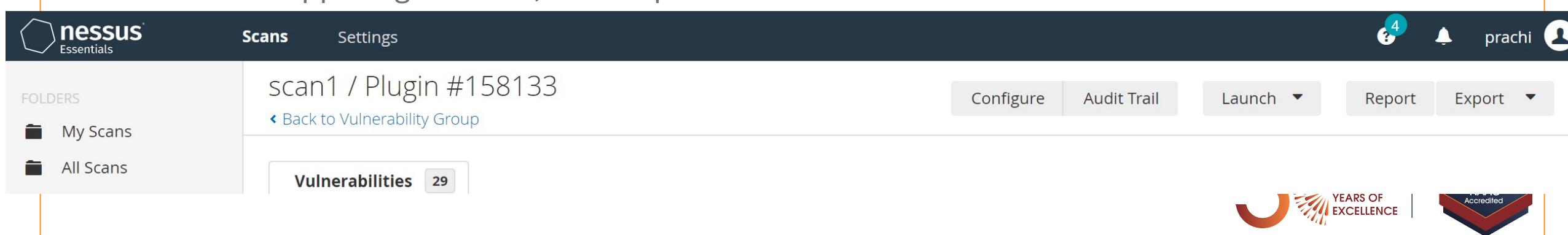
CVE: CVE-1999-0519, CVE-1999-0520, CVE-2002-1117
OSVDB: 299, 8230
BID: 494

CE



Nessus Steps

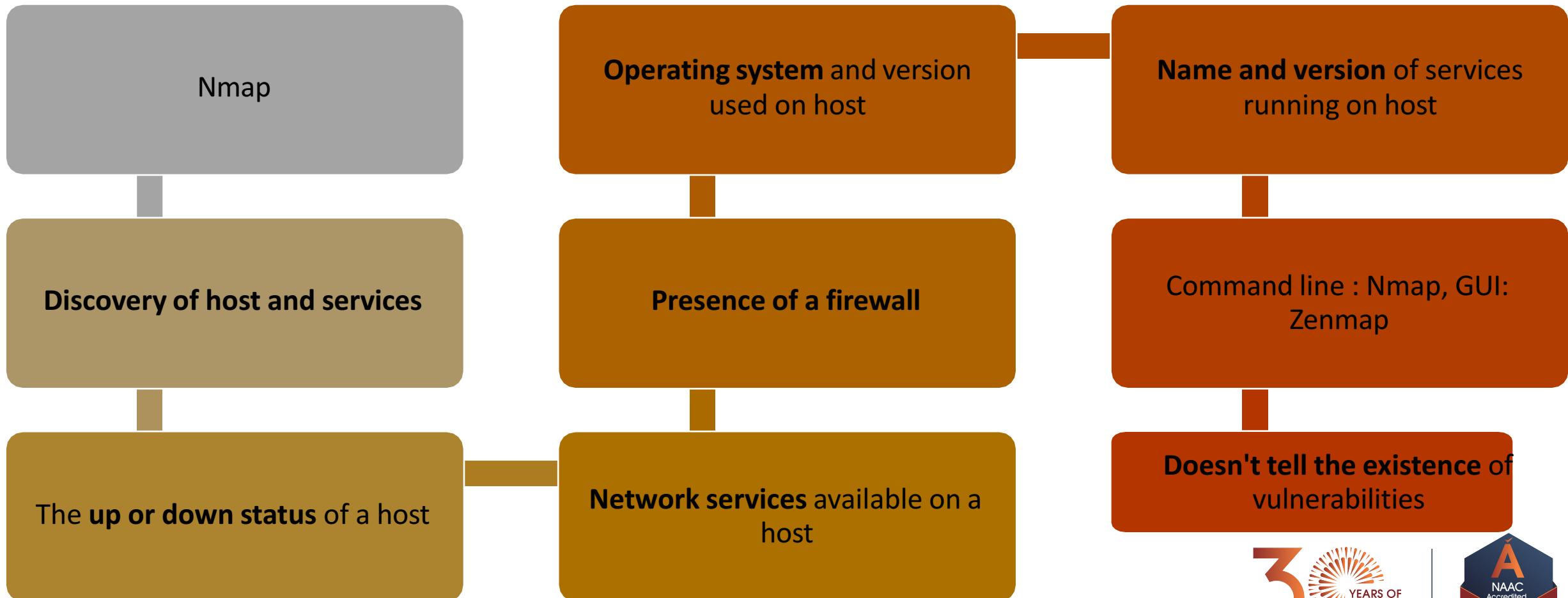
- Step 6: Reporting Your Results
 - Now you need to report your findings to your team.
 - Scan results can be exported in several file formats.
- To Export a Scan Report:
 - Start from a scan's results page
 - In the upper-right corner, click Export.

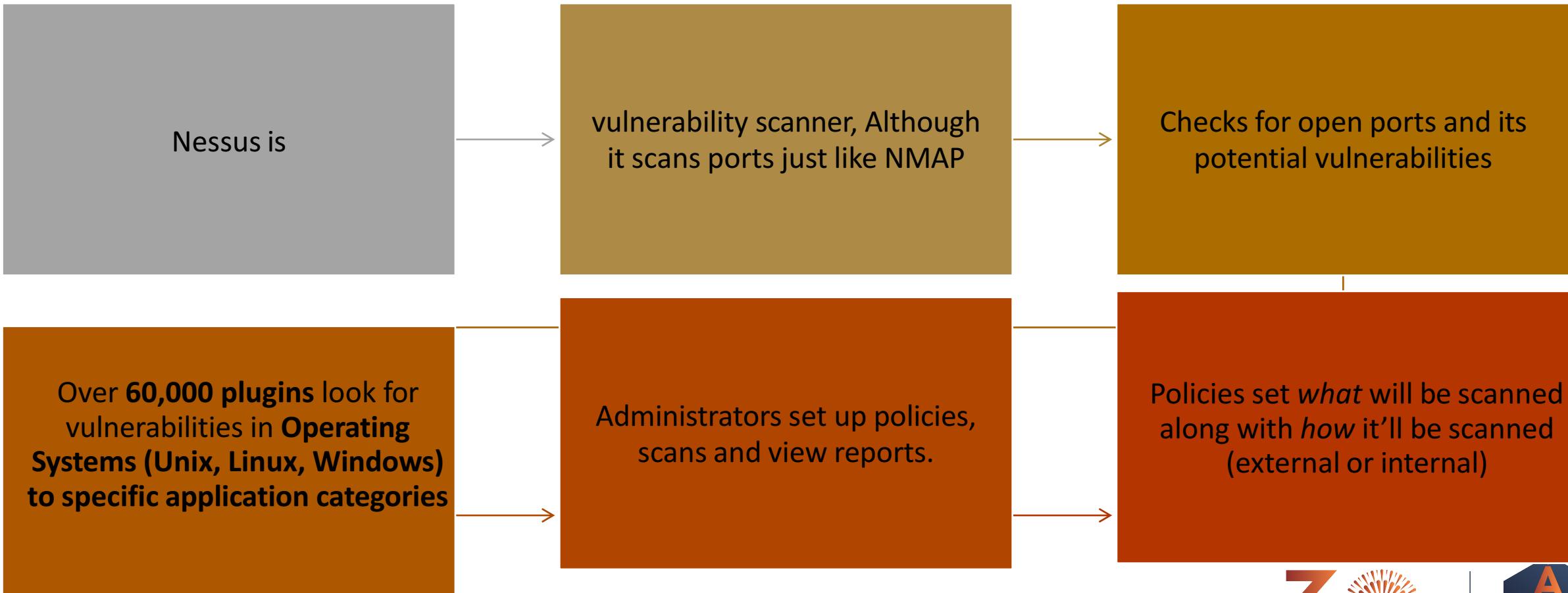


The screenshot shows the Nessus Essentials web interface. At the top, there is a navigation bar with tabs for 'Scans' and 'Settings'. On the far right of the top bar, there are icons for notifications (4), a user profile ('prachi'), and a help icon. Below the top bar, the main content area has a sidebar on the left labeled 'FOLDERS' with options 'My Scans' and 'All Scans'. The main content area displays a scan titled 'scan1 / Plugin #158133'. It includes a back button 'Back to Vulnerability Group', a 'Configure' button, an 'Audit Trail' button, a 'Launch' dropdown menu, a 'Report' button, and an 'Export' dropdown menu. At the bottom of the content area, there is a 'Vulnerabilities' section with a count of '29'. The bottom right corner features two accreditation logos: 'Years of Excellence' and 'Accredited'.

Nessus vs Nmap

Nmap (port scanning tool)





In Class Exercise

Implement Nessus
on website and
generate report

Write steps and
attach screenshot
of each step

Home Exercise

Go through
Nessus (Ref
document)



Inbuilt tool
of Kali