

Nessus

Learn how to set up and use Nessus, a popular vulnerability scanner.

- Nessus is a vulnerability scanner to find and report vulnerabilities.

Task 2: Installation

- Register an account to get an activation code: [here](#)
- download the **Nessus-#.##.#-debian6_amd64.deb** file
- go to the folder you have the file downloaded (most likely your download folder): `cd Download/`
- install the package using: `sudo dpkg -i <filename>`
- start Nessus service using: `sudo /bin/systemctl start nessusd.service`
- Open up Firefox and go to the following URL: <https://localhost:8834/>
- Set up the scanner by selecting the option **Nessus Essentials**
- Input the activation code and set your username and password
- The plugins will take some time to download, then you have successfully installed Nessus

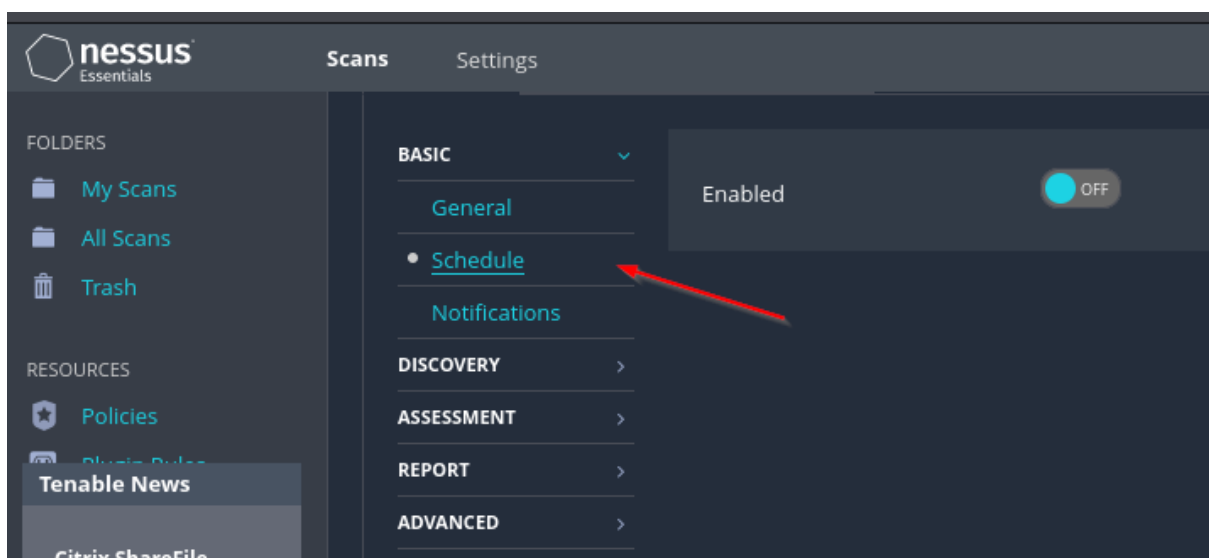
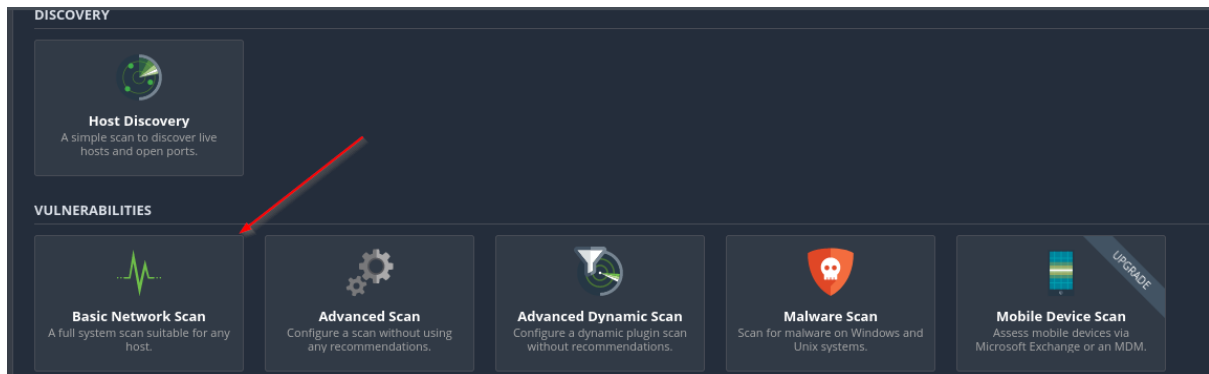
Task 3: Navigation and Scans

- The answers to the questions for this task can be located within the Nessus application.

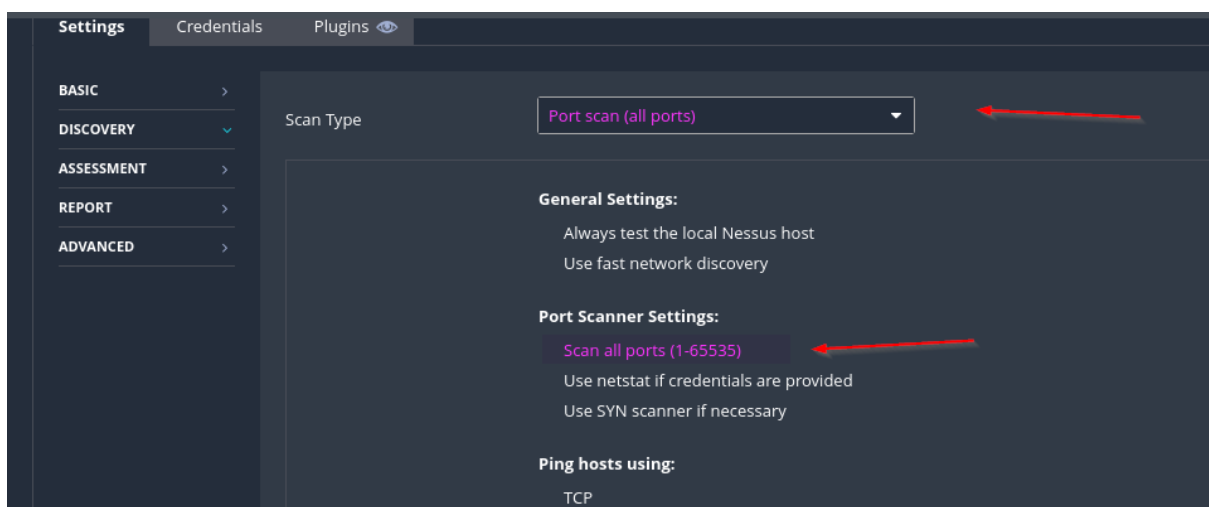
Question	Answers
What is the name of the button which is used to launch a scan?	New Scan
What side menu option allows us to create custom templates ?	Policies
What menu allows us to change plugin properties such as hiding them or changing their severity?	Plugin Rules
In the ' Scan Templates ' section after clicking on ' New Scan ', what scan allows us to see simply what hosts are alive?	Host Discovery
One of the most useful scan types, which is considered to be ' suitable for any host '?	Basic Network Scan
What scan allows you to ' Authenticate to hosts and enumerate missing updates '?	Credentialed Patch Audit
What scan is specifically used for scanning Web Applications ?	Web Application Tests

Task 4: Scanning!

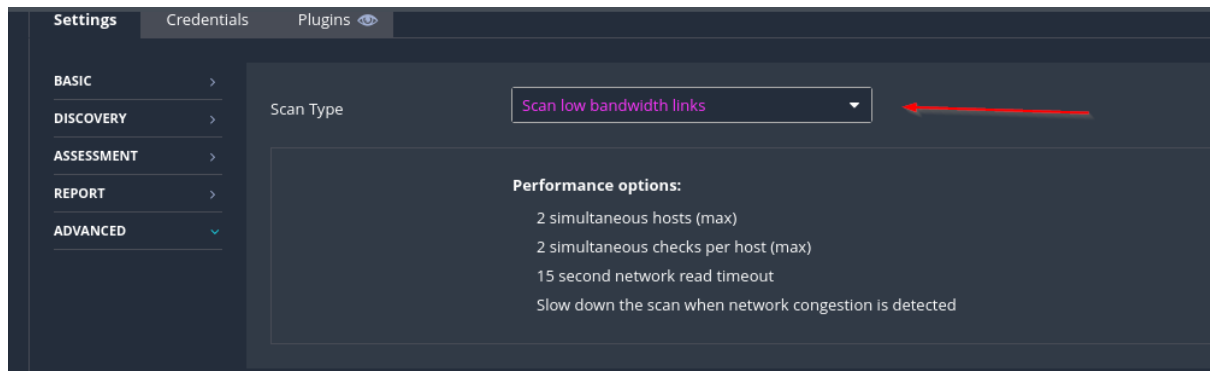
- Create a basic network scan



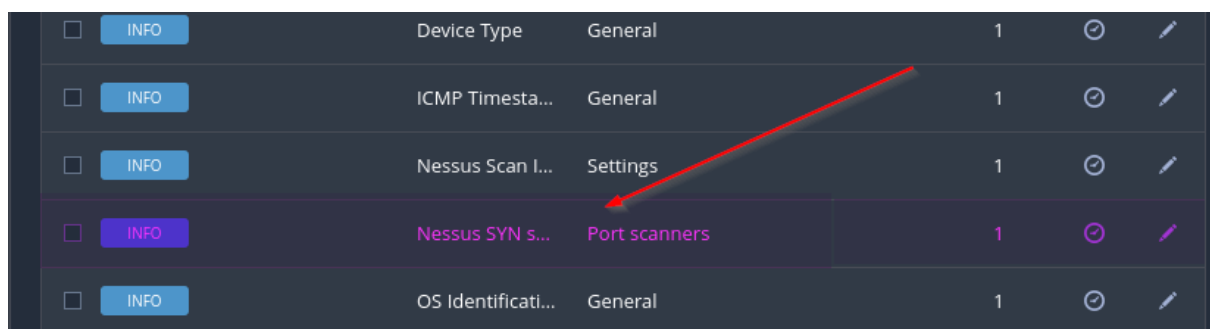
- Under 'DISCOVERY' (on the left) set the 'Scan Type' to cover ports 1-65535. What is this type called?



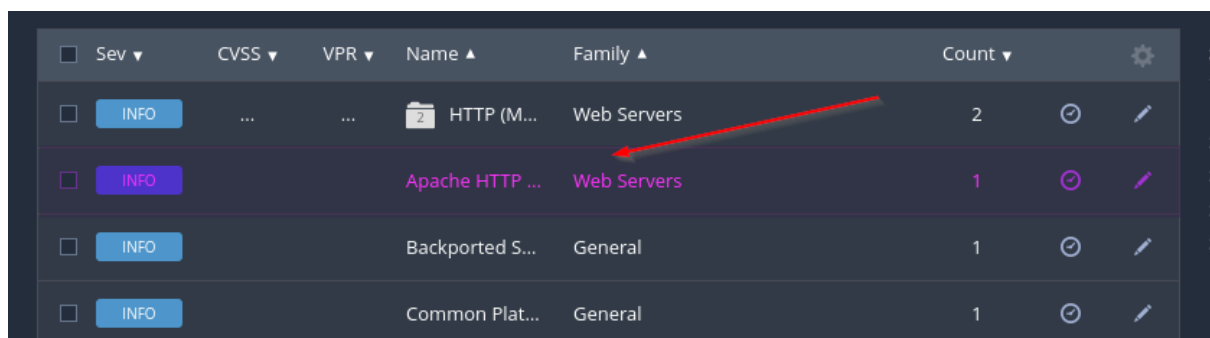
- What '**Scan Type**' can we change to under '**ADVANCED**' for lower bandwidth connection?



- which '**Vulnerability**' in the '**Port scanners**' family can we view the details of to see the open ports on this host?



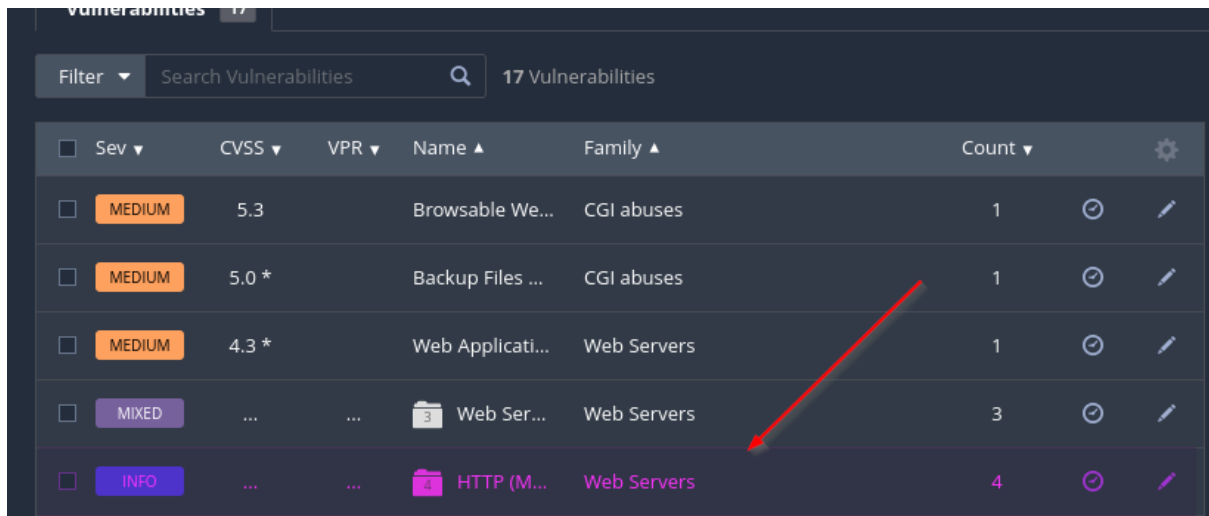
- **Apache HTTP Server Version** reported by Nessus?



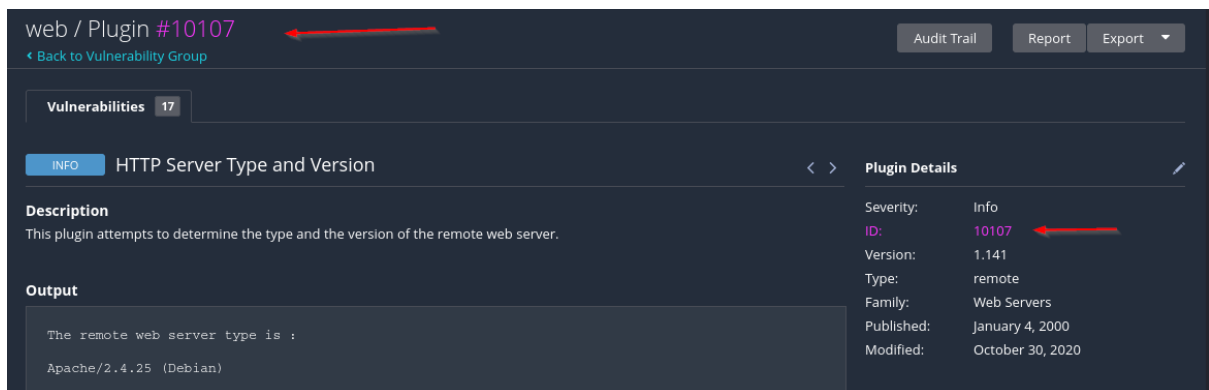
Question	Answers
Create a new ' Basic Network Scan ' targeting the deployed VM. What option can we set under ' BASIC ' (on the left) to set a time for this scan to run? This can be very useful when network congestion is an issue	Schedule
Under ' DISCOVERY ' (on the left) set the ' Scan Type ' to cover ports 1-65535. What is this type called?	Port scan (all ports)
What ' Scan Type ' can we change to under ' ADVANCED ' for lower bandwidth connection?	Scan low bandwidth links
After the scan completes, which ' Vulnerability ' in the ' Port scanners ' family can we view the details of to see the open ports on this host?	Nessus SYN scanner
What Apache HTTP Server Version is reported by Nessus?	2.4.99

Task 5: Scanning a Web Application!

- Go to the web application scan type and scan your target



Sev	CVSS	VPR	Name	Family	Count	
MEDIUM	5.3		Browsable We...	CGI abuses	1	
MEDIUM	5.0 *		Backup Files ...	CGI abuses	1	
MEDIUM	4.3 *		Web Applicati...	Web Servers	1	
MIXED	Web Ser...	Web Servers	3	
INFO	HTTP (M...	Web Servers	4	



web / Plugin #10107		Audit Trail	Report	Export
<div>Vulnerabilities 17</div> <div>INFO HTTP Server Type and Version</div>				
Description This plugin attempts to determine the type and the version of the remote web server.		Plugin Details		
Output The remote web server type is : Apache/2.4.25 (Debian)		Severity: Info ID: 10107 Version: 1.141 Type: remote Family: Web Servers Published: January 4, 2000 Modified: October 30, 2020		

- authentication page discovered by the scanner that transmits credentials in cleartext

web / 10.10.111.9

[Back to Hosts](#)

Vulnerabilities 17

Filter Search Vulnerabilities 17 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	
<input type="checkbox"/>	MEDIUM	5.3		Browsable We...	CGI abuses	1	
<input type="checkbox"/>	MEDIUM	5.0 *		Backup Files ...	CGI abuses	1	
<input type="checkbox"/>	MEDIUM	4.3 *		Web Applicati...	Web Servers	1	
<input type="checkbox"/>	MIXED	3 Web Ser...	Web Servers	3	

web / 10.10.111.9 / Web Server (Multiple Issues)

[Back to Vulnerabilities](#)

Vulnerabilities 17

Search Vulnerabilities 3 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	
<input type="checkbox"/>	LOW	2.6 *		Web Server Tr...	Web Servers	1	
<input type="checkbox"/>	INFO			Web Server Di...	Web Servers	1	
<input type="checkbox"/>	INFO			Web Server ro...	Web Servers	1	

LOW Web Server Transmits Cleartext Credentials >

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Output

```
Page : /login.php
Destination Page: /login.php
```

- What is the file extension of the config backup?

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼		
<input type="checkbox"/>	MEDIUM	5.3		Browsable We...	CGI abuses	1	🔄	✎
<input type="checkbox"/>	MEDIUM	5.0 *		Backup Files ...	CGI abuses	1	🔄	✎
<input type="checkbox"/>	MEDIUM	4.3 *		Web Applicati...	Web Servers	1	🔄	✎

Solution

Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

See Also

<http://www.nessus.org/u?8f3302c6>

Output

```
It is possible to read the following backup file :  
  
- File : /config/config.inc.php.bak  
  URL  : http://10.10.111.9/config/config.inc.php.bak
```

To see debug logs, please visit individual host.

- Which directory contains example documents? (This will be in a php directory)

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼		
<input type="checkbox"/>	MEDIUM	5.3		Browsable We...	CGI abuses	1	🔄	✎
<input type="checkbox"/>	MEDIUM	5.0 *		Backup Files ...	CGI abuses	1	🔄	✎
<input type="checkbox"/>	MEDIUM	4.3 *		Web Applicati...	Web Servers	1	🔄	✎

```
The following directories are browsable :  
  
http://10.10.111.9/config/  
http://10.10.111.9/docs/  
http://10.10.111.9/dvwa/  
http://10.10.111.9/dvwa/css/  
http://10.10.111.9/dvwa/images/  
http://10.10.111.9/dvwa/includes/  
http://10.10.111.9/dvwa/includes/DBMS/  
http://10.10.111.9/dvwa/js/  
http://10.10.111.9/external/  
http://10.10.111.9/external/phpids/  
http://10.10.111.9/external/phpids/0.6/  
http://10.10.111.9/external/phpids/0.6/docs/  
http://10.10.111.9/external/phpids/0.6/docs/examples/  
http://10.10.111.9/external/phpids/0.6/lib/  
http://10.10.111.9/external/phpids/0.6/lib/IDS/  
http://10.10.111.9/external/phpids/0.6/tests/  
http://10.10.111.9/external/phpids/0.6/tests/IDS/  
http://10.10.111.9/external/recaptcha/
```

- What vulnerability is this application susceptible to that is associated with X-Frame-Options?

web / 10.10.111.9
[Back to Hosts](#)

Vulnerabilities 17

Filter Search Vulnerabilities 17 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	
<input type="checkbox"/>	MEDIUM	5.3		Browsable We...	CGI abuses	1	
<input type="checkbox"/>	MEDIUM	5.0 *		Backup Files ...	CGI abuses	1	
<input type="checkbox"/>	MEDIUM	4.3 *		Web Applicati...	Web Servers	1	

web / Plugin #85582
[Back to Vulnerabilities](#)

Vulnerabilities 17

MEDIUM Web Application Potentially Vulnerable to Clickjacking

Description
 The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Question	Answers
What is the plugin id of the plugin that determines the HTTP server type and version?	10107
What authentication page is discovered by the scanner that transmits credentials in cleartext?	login.php
What is the file extension of the config backup?	.bak
Which directory contains example documents? (This will be in a php directory)	/external/phpids/0.6/docs/examples/
What vulnerability is this application susceptible to that is associated with X-Frame-Options?	Clickjacking

END.