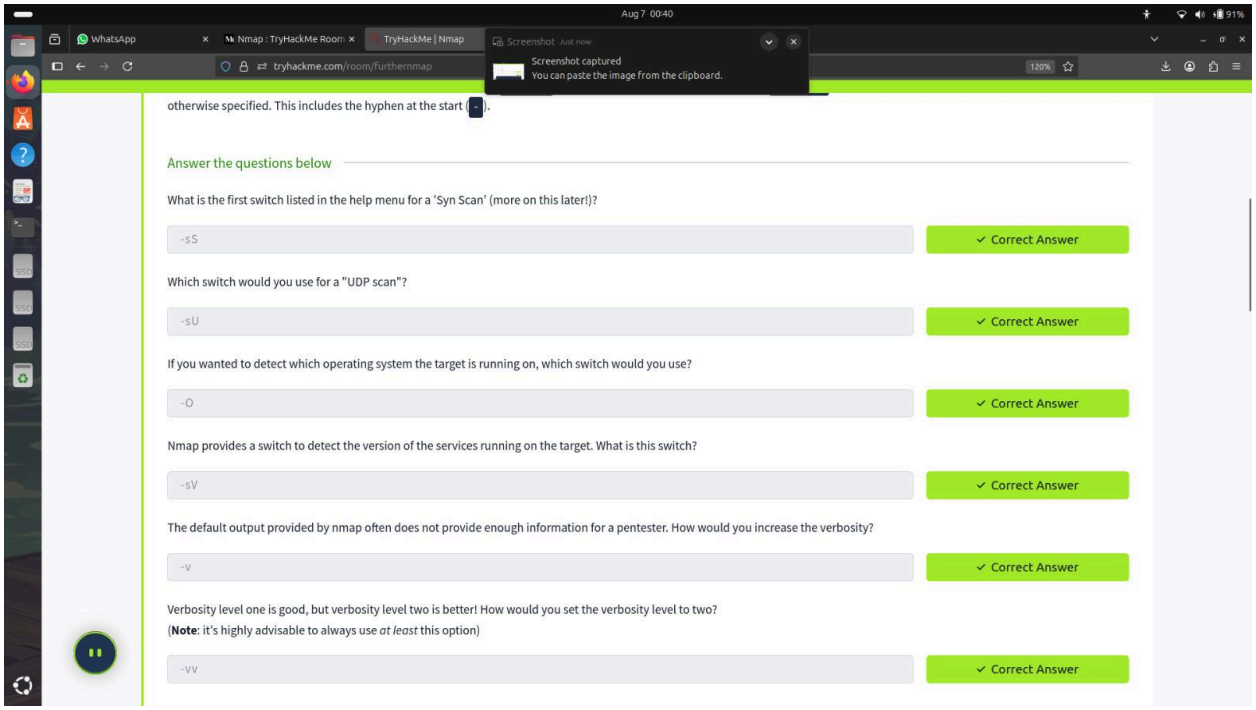
Report on "Further Nmap" Room - TryHackMe

This report summarizes the tasks and answers from the TryHackMe room "Further Nmap," based on the provided screenshots. The room covers advanced Nmap scanning techniques, including various scan types, firewall evasion, and the use of the Nmap Scripting Engine (NSE).

Task 3: Nmap Switches

This task introduces core Nmap command-line switches for customizing scans.

* Question: What is the first switch listed in the help menu for a "Syn Scan"?
  * Answer: -sS
* Question: Which switch would you use for a "UDP scan"?
  * Answer: -sU
* Question: If you wanted to detect which operating system the target is running on, which switch would you use?
  * Answer: -O
* Question: Nmap provides a switch to detect the version of the services running on the target. What is this switch?
  * Answer: -sV
* Question: How would you increase the verbosity?
  * Answer: -v
* Question: How would you set the verbosity level to two?
  * Answer: -vv
* Question: How would you save the Nmap results in three major formats?
  * Answer: -oA
* Question: How would you save the Nmap results in a "normal" format?
  * Answer: -oN
* Question: How would you save results in a "greppable" format?
  * Answer: -oG
* Question: How would you activate this setting? (Aggressive mode)
  * Answer: -A
* Question: How would you set the timing template to level 5?
  * Answer: -T5
* Question: How would you tell Nmap to only scan port 80?
  * Answer: -p 80
* Question: How would you tell Nmap to scan ports 1000-1500?
  * Answer: -p 1000-1500
* Question: How would you tell Nmap to scan all ports?
  * Answer: -p-
* Question: How would you activate a script from the Nmap scripting library?
  * Answer: --script
* Question: How would you activate all of the scripts in the "vuln" category?
  * Answer: --script=vuln



otherwise specified. This includes the hyphen at the start (-).

Answer the questions below

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

-sS ✓ Correct Answer

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

-sU ✓ Correct Answer

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

-O ✓ Correct Answer

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

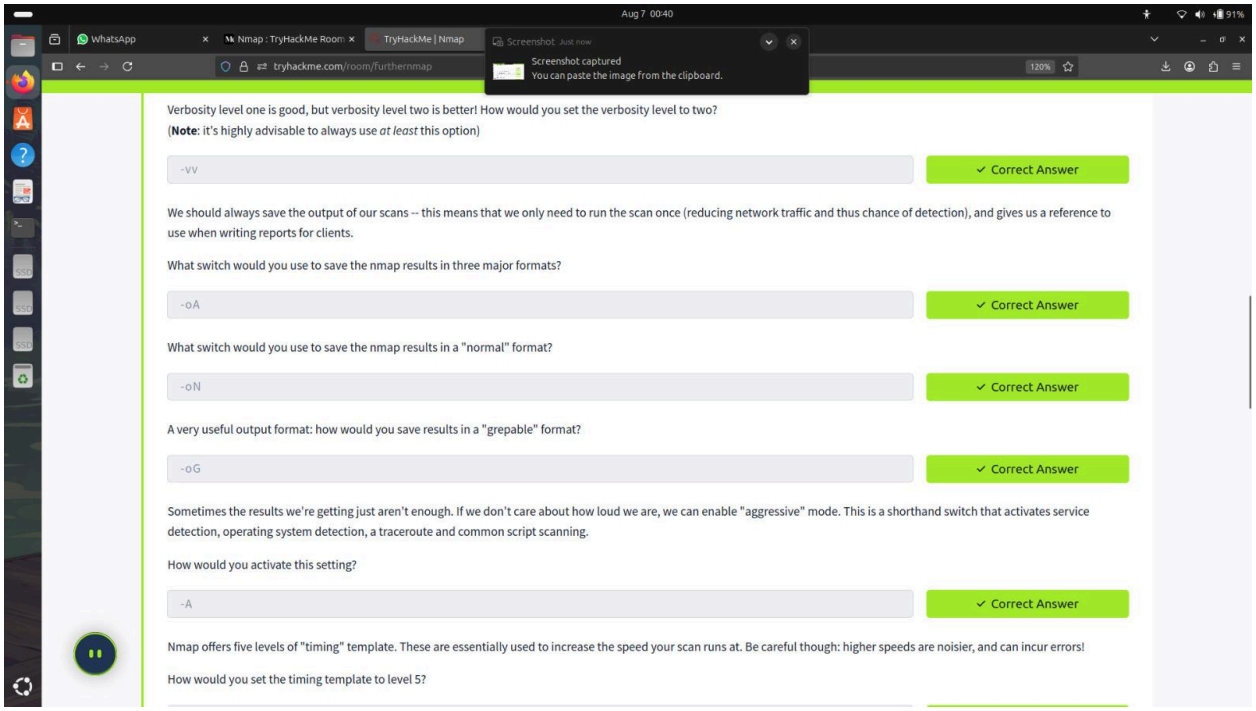
-sV ✓ Correct Answer

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

-v ✓ Correct Answer

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 ✓ Correct Answer



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 ✓ Correct Answer

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 ✓ Correct Answer

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

-oN ✓ Correct Answer

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

-oG ✓ Correct Answer

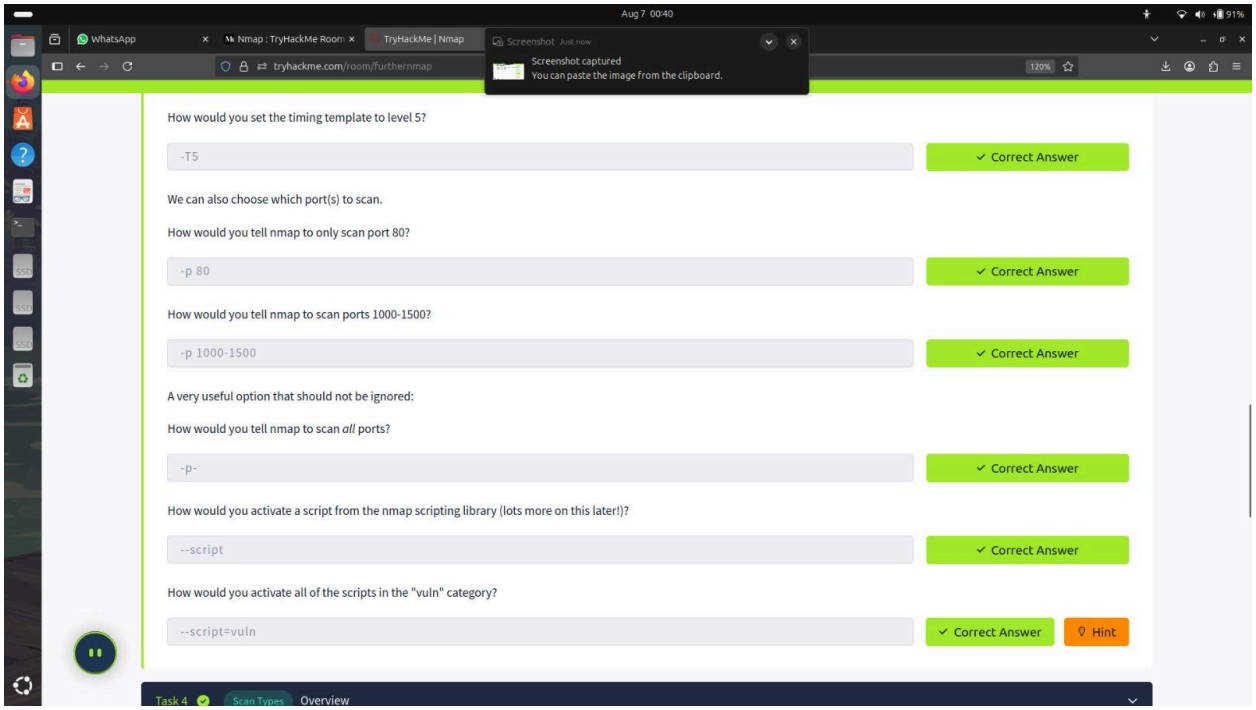
Sometimes the results we're getting just aren't enough. If we don't care about how loud we are, we can enable "aggressive" mode. This is a shorthand switch that activates service detection, operating system detection, a traceroute and common script scanning.

How would you activate this setting?

-A ✓ Correct Answer

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!

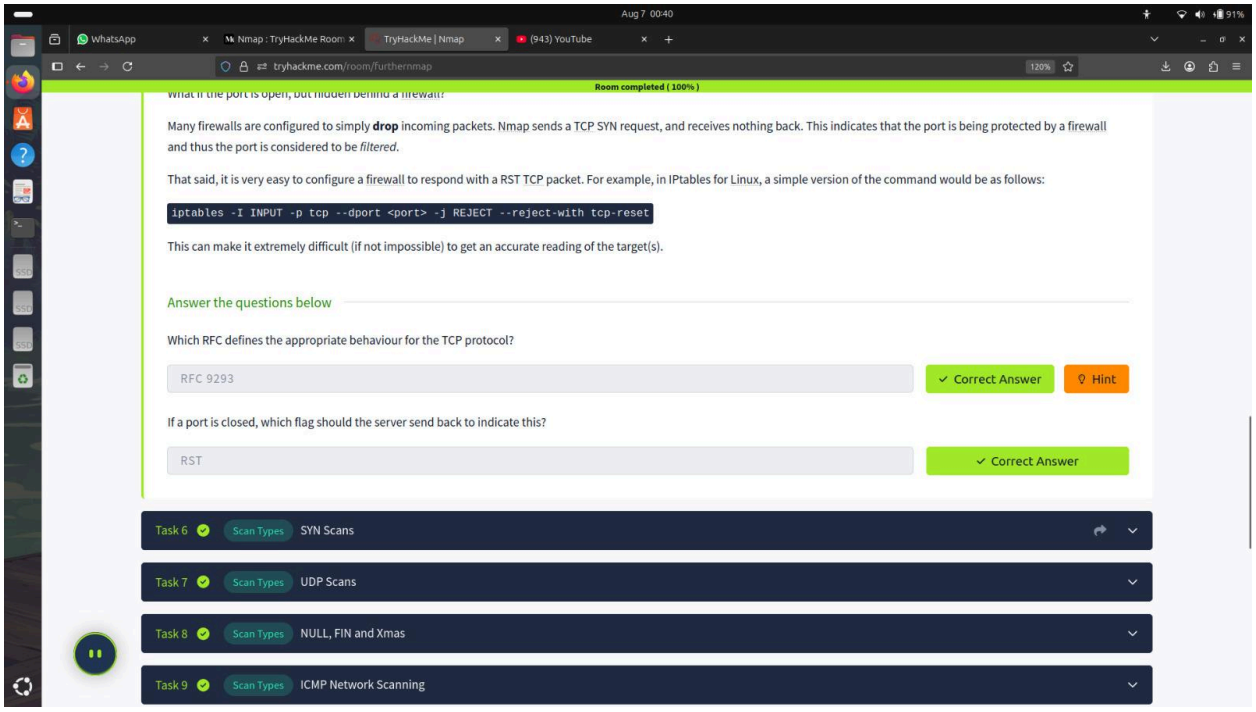
How would you set the timing template to level 5?



Task 4: Scan Types Overview

This task introduces the different types of Nmap scans.

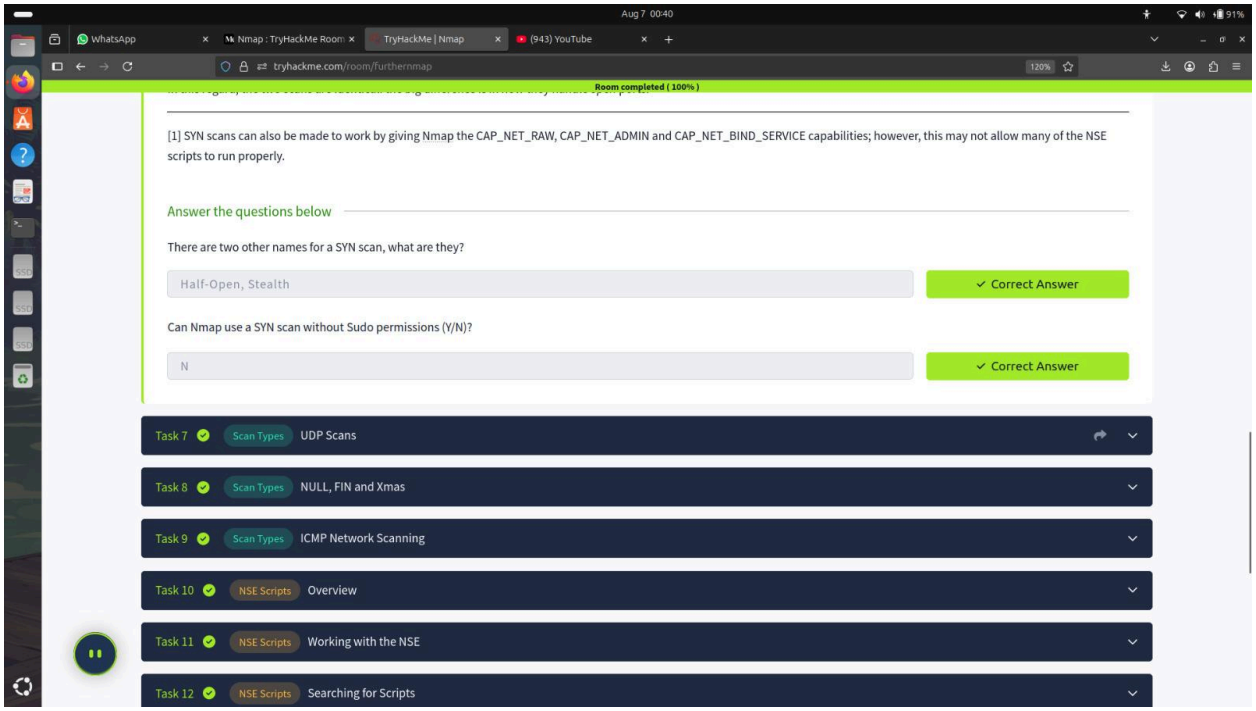
* Question: Read the Scan Types Introduction.
  * Answer: No answer needed.



Task 5: TCP Connect Scans

This task focuses on the fundamental TCP Connect scan.

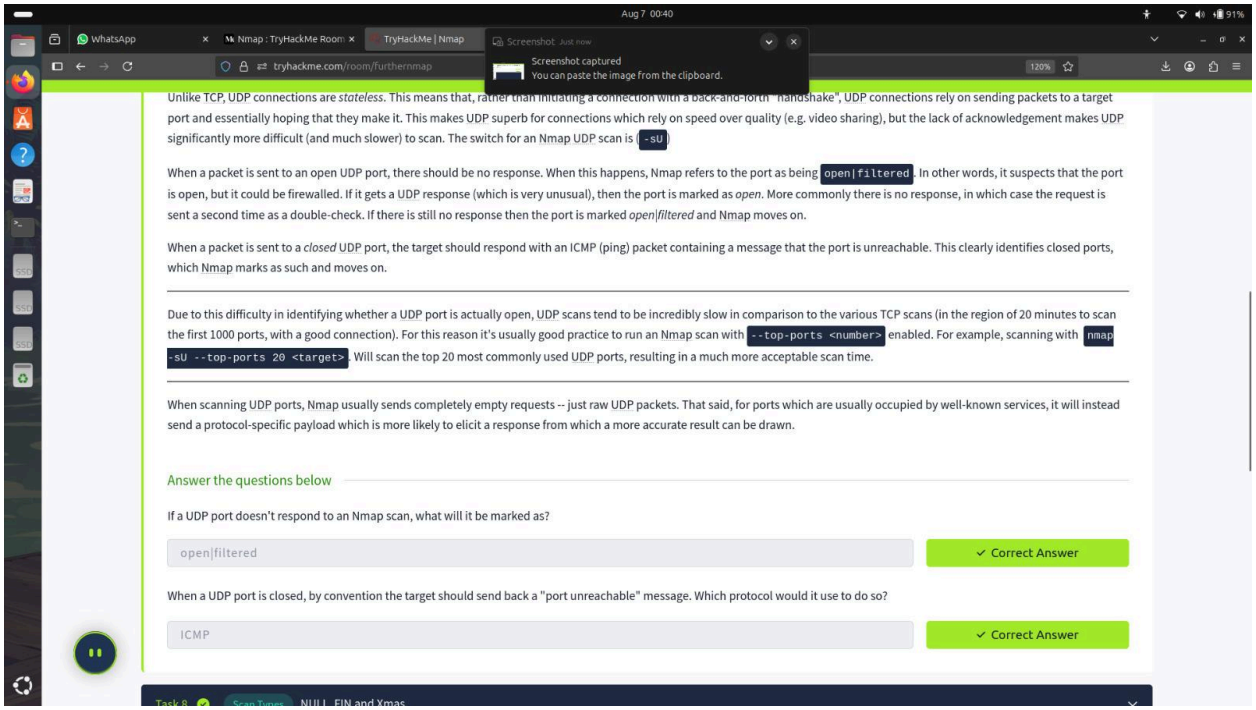
* Question: What networking constructs are used to direct traffic to the right application on a server?
  * Answer: Ports
* Question: How many of these are available on any network-enabled computer?
  * Answer: 65535
* Question: How many of these are considered "well-known"?
  * Answer: 1024
* Question: Which RFC defines the appropriate behavior for the TCP protocol?
  * Answer: RFC 9293
* Question: If a port is closed, which flag should the server send back to indicate this?
  * Answer: RST



Task 7: UDP Scans

This task covers scanning UDP ports, which behaves differently from TCP.

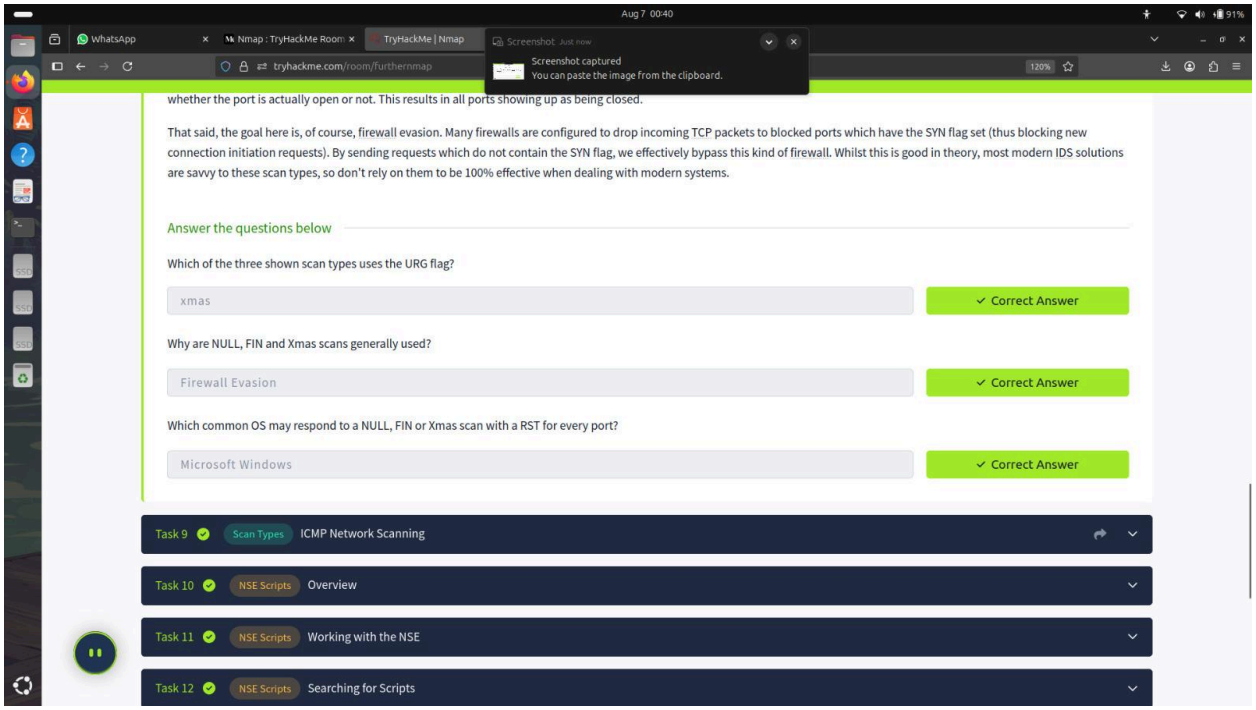
* Question: If a UDP port doesn't respond to an Nmap scan, what will it be marked as?
  * Answer: open|filtered
* Question: When a UDP port is closed, by convention the target should send back a "port unreachable" message. Which protocol would it use to do so?
  * Answer: ICMP



Task 8: NULL, FIN and Xmas Scans

This task explains stealthier scan types used for firewall evasion.

* Question: There are two other names for a SYN scan, what are they?
  * Answer: Half-Open, Stealth
* Question: Can Nmap use a SYN scan without Sudo permissions (Y/N)?
  * Answer: N
* Question: Which of the three shown scan types uses the URG flag?
  * Answer: xmas
* Question: Why are NULL, FIN and Xmas scans generally used?
  * Answer: Firewall Evasion
* Question: Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?
  * Answer: Microsoft Windows

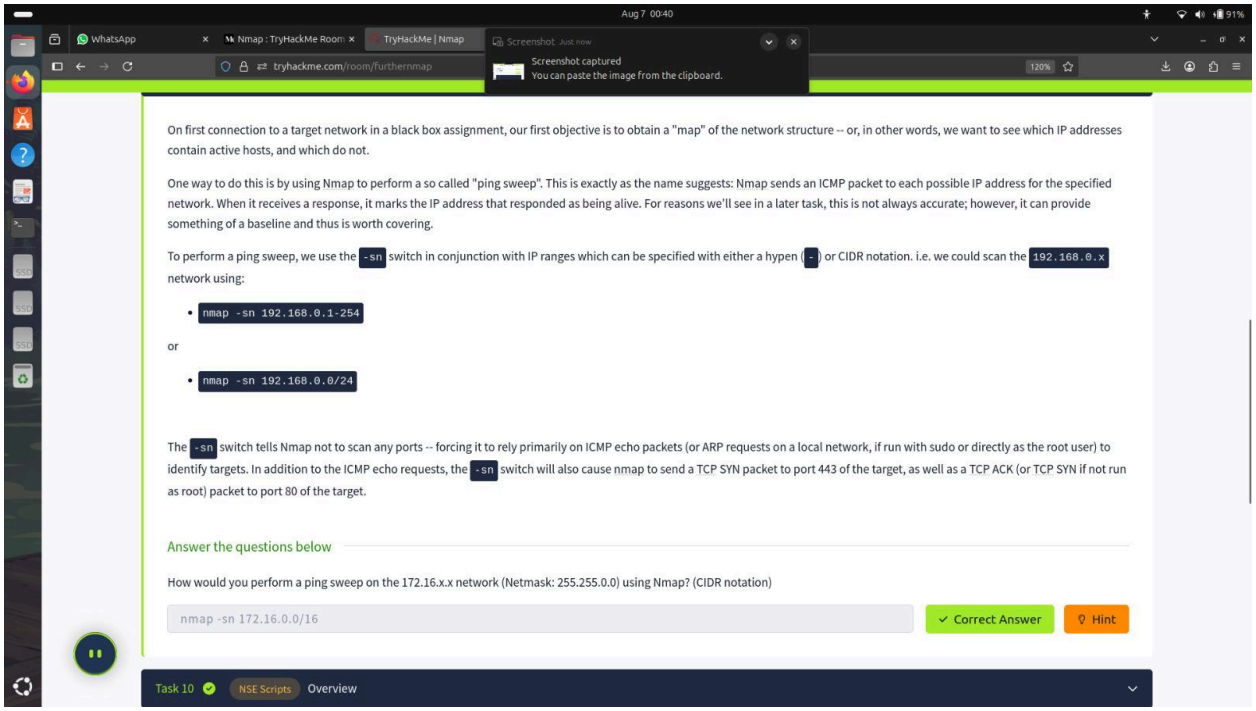


Task 9: ICMP Network Scanning

This task covers the "ping sweep" for identifying live hosts.

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

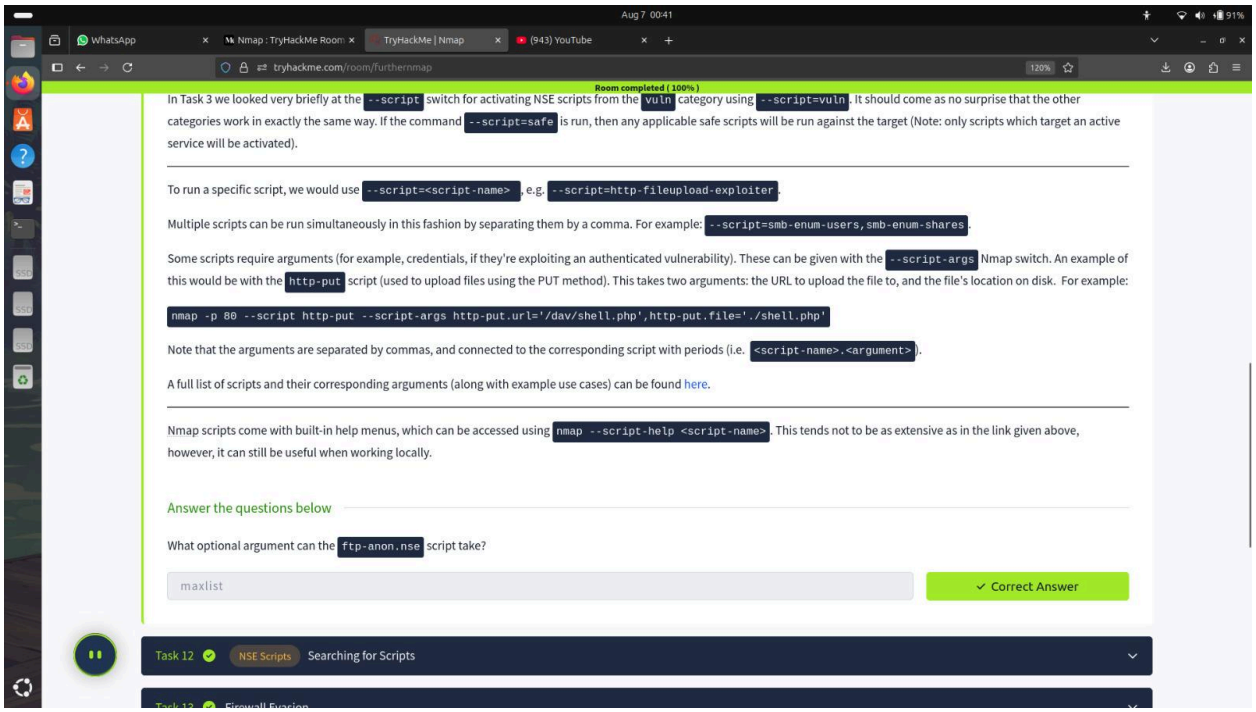
* Answer: nmap -sn 172.16.0.0/16



Task 10: NSE Scripts Overview

This task introduces the Nmap Scripting Engine.

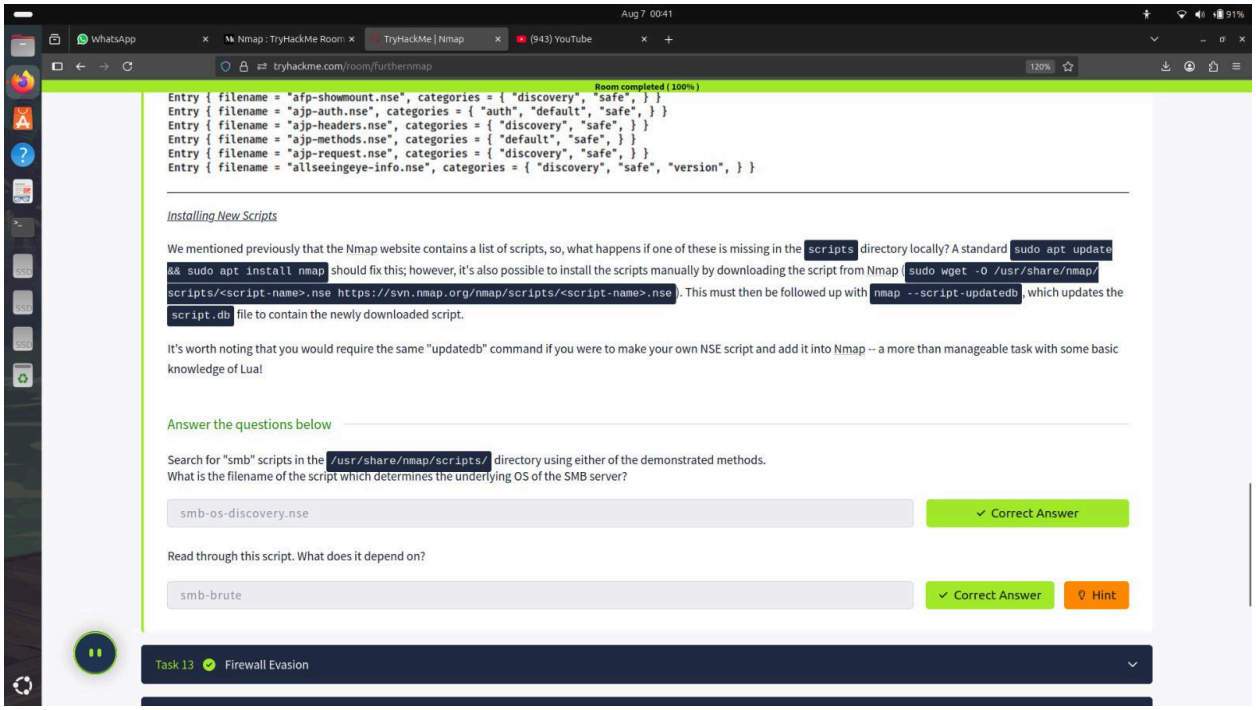
* Question: What language are NSE scripts written in?
  * Answer: Lua
* Question: Which category of scripts would be a very bad idea to run in a production environment?
  * Answer: intrusive



Task 12: Searching for Scripts

This task focuses on finding and using specific NSE scripts.

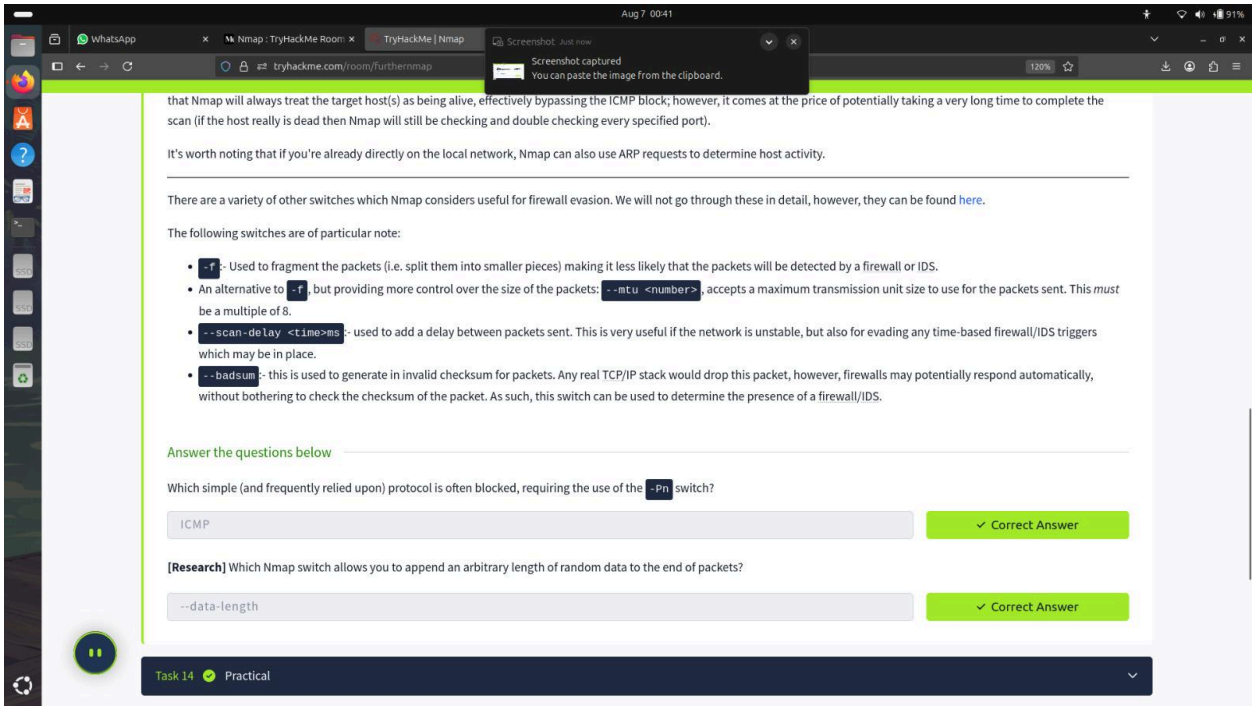
* Question: What optional argument can the ftp-anon.nse script take?
  * Answer: maxlist
* Question: What is the filename of the script which determines the underlying OS of the SMB server?
  * Answer: smb-os-discovery.nse
* Question: Read through this script. What does it depend on?
  * Answer: smb-brute



Task 13: Firewall Evasion

This task highlights additional switches for evading firewall detection.

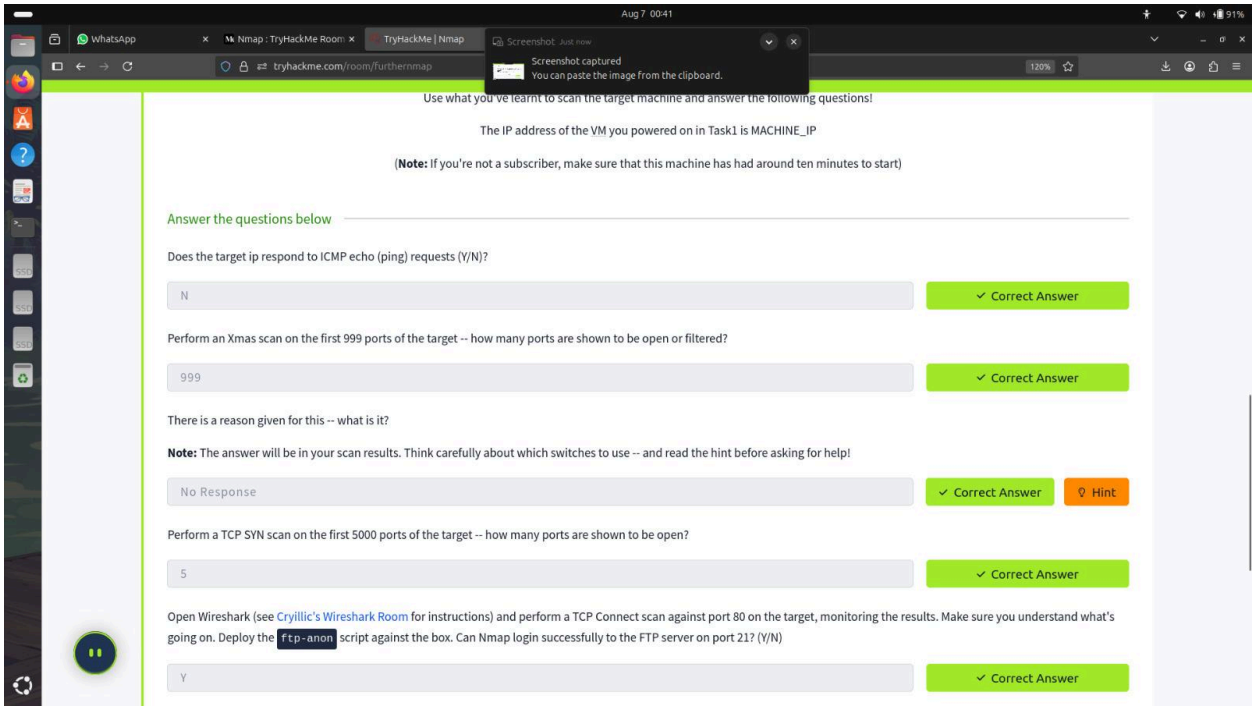
* Question: Which simple (and frequently relied upon) protocol is often being blocked, requiring the use of the -Pn switch?
  * Answer: ICMP
* Question: Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?
  * Answer: --data-length



Task 14: Practical

This task requires hands-on interaction with the target machine.

 * Question: Does the target IP respond to ICMP echo (ping) requests (Y/N)?
   * Answer: N
 * Question: Perform an Xmas scan on the first 999 ports of the target -- how many ports are shown to be open or filtered?
   * Answer: 999
 * Question: Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open?
   * Answer: 5
 * Question: Can Nmap login successfully to the FTP server on port 21? (Y/N)
   * Answer: Y



Task 15: Conclusion

This is the final task, concluding the room.

* Question: Read the conclusion.
  * Answer: No answer needed.