

TASK 3

Tryhackme Room: Nmap

Writer: Mark Alexander Varghese

Date:29-08-2025

I completed the Nmap room on TryHackMe this week, admittedly three weeks past my planned schedule due to some unexpected delays and technical issue.

I got hands-on with several powerful Nmap flags—each useful in different reconnaissance scenarios:

- sS: SYN scan (stealthy, half-open)

- sU: UDP scan

- O: OS detection; -sV: service version detection

- Verbosity flags: -v and -vv to control output detail

Output options:

- oA (all formats)

- Aggressive scanning: -A combines OS detection, version detection, traceroute, and common NSE script scanning

- Timing template: -T5 for the fastest scans

- Port selection: -p 80, -p 1000-1500, or -p- (all ports)

NSE scripts:

- script enables specific scripts;

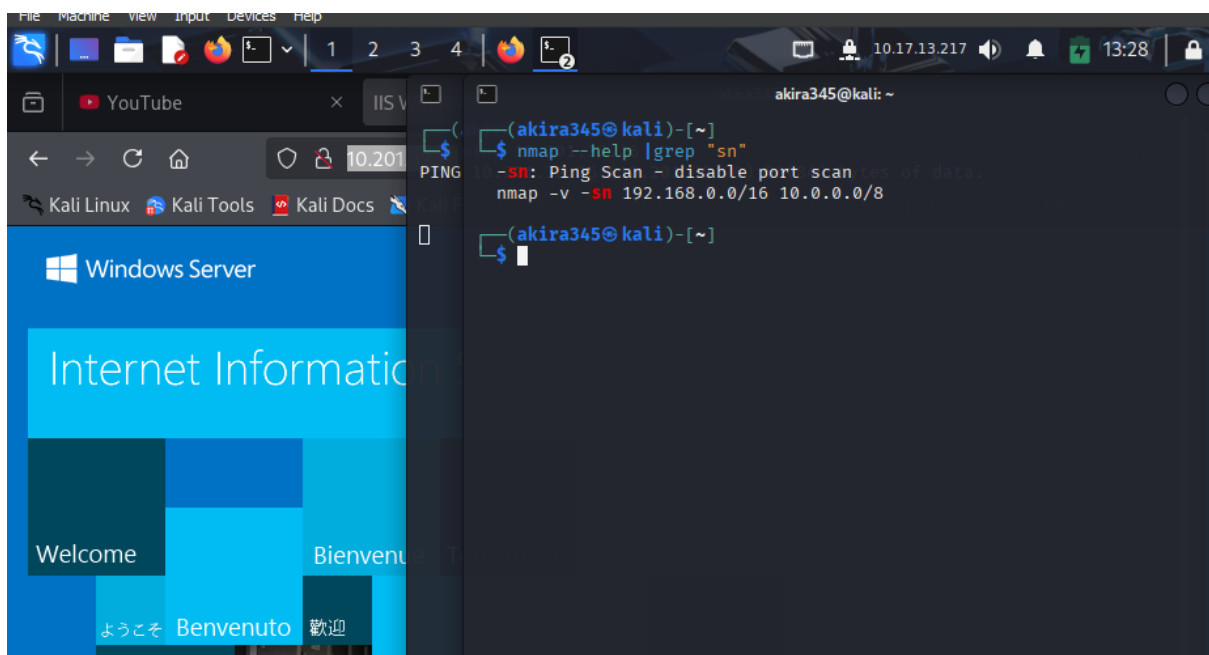
- script=vuln runs all vulnerability scripts

Overall a great room to practise and learn nmap commands.

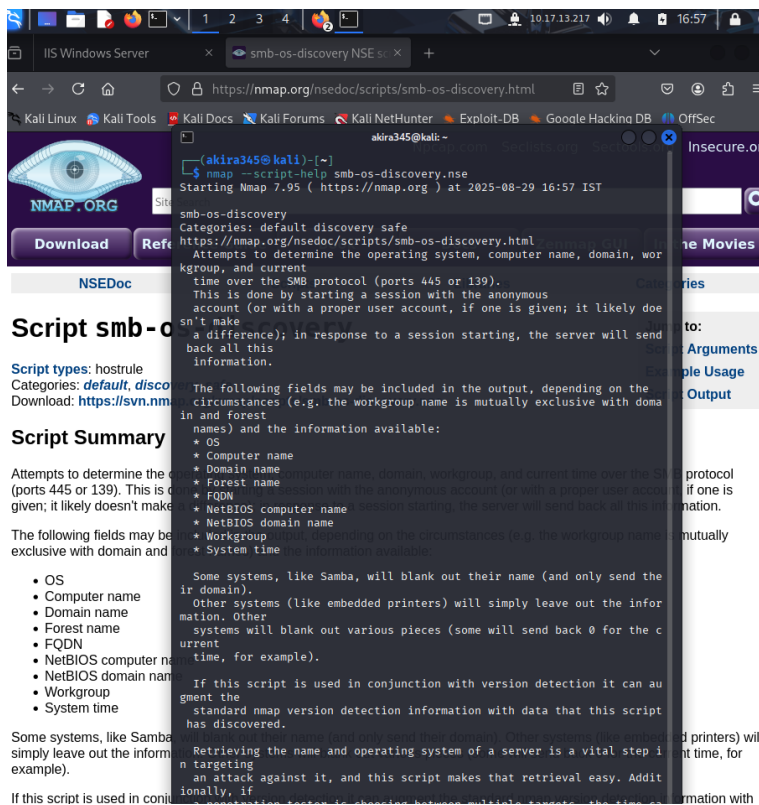
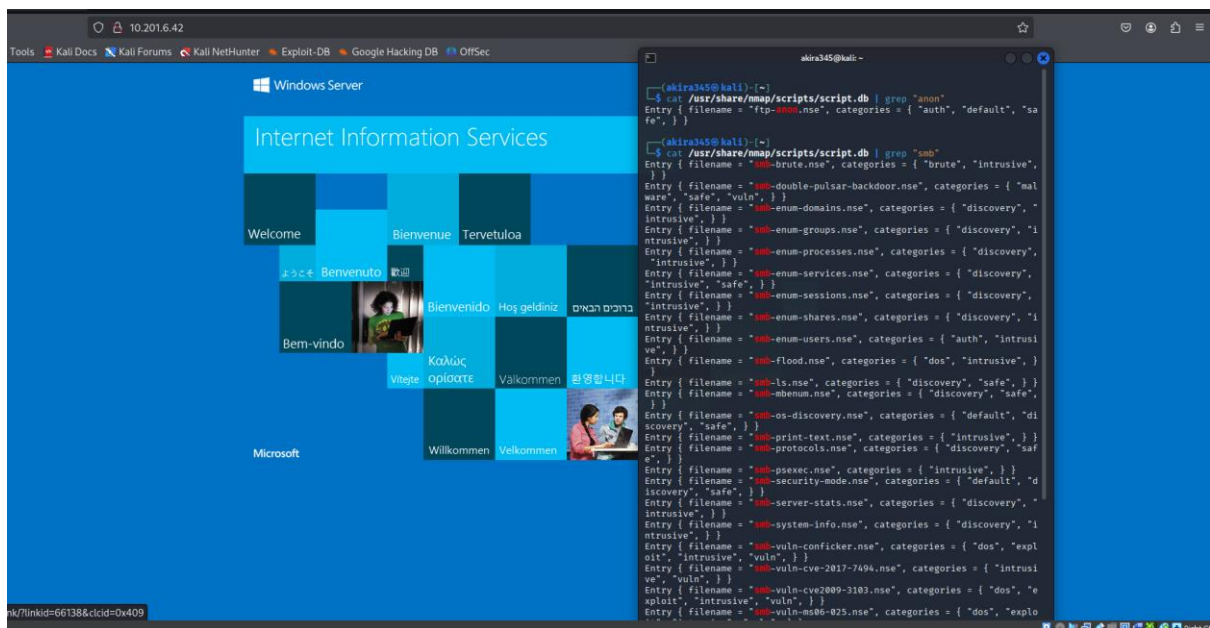
Screenshots

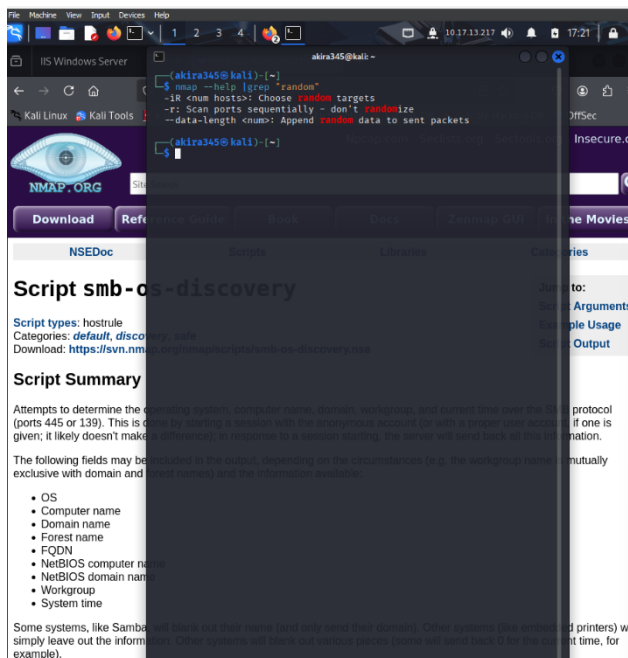
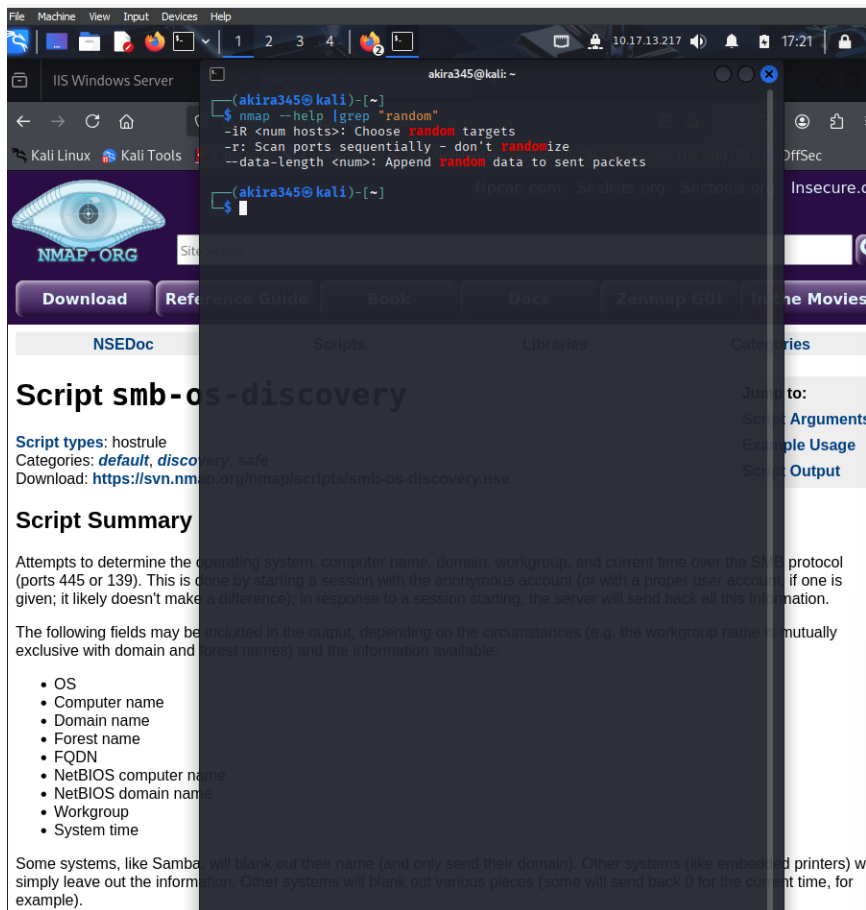
```
(akira345@kali)-[~]
$ nmap --help | grep "\-v"
--version-intensity <level>: Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)
-v: Increase verbosity level (use -vv or more for greater effect)
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80

(akira345@kali)-[~]
$
```



```
(akira345@kali)-[~]  
$ nmap --help |grep "\-T"  
-T<0-5>: Set timing template (higher is faster)  
  
(akira345@kali)-[~]  
$ nmap --help |grep "ports"  
-PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports  
-p <port ranges>: Only scan specified ports  
--exclude-ports <port ranges>: Exclude the specified ports from scanning  
-F: Fast mode - Scan fewer ports than the default scan  
-r: Scan ports sequentially - don't randomize  
--top-ports <number>: Scan <number> most common ports  
--port-ratio <ratio>: Scan ports more common than <ratio>  
-sV: Probe open ports to determine service/version info  
--open: Only show open (or possibly open) ports  
  
(akira345@kali)-[~]  
$ nmap --help |grep "script"  
-sC: equivalent to --script=default  
--script=<Lua scripts>: <Lua scripts> is a comma separated list of directories, script-files or script-categories  
--script-args=<n1=v1,[n2=v2, ...]>: provide arguments to scripts  
--script-args-file=filename: provide NSE script args in a file  
--script-trace: Show all data sent and received  
--script-updatedb: Update the script database.  
--script-help=<Lua scripts>: Show help about scripts.  
    <Lua scripts> is a comma-separated list of script-files or script-categories.  
-A: Enable OS detection, version detection, script scanning, and trace route  
  
(akira345@kali)-[~]  
$
```





[illegible]

Learn > Nmap



Nmap

An in depth look at scanning with Nmap, a powerful network scanning tool.

Easy 50 min



Share your achievement

Start AttackBox

Save Room

19721



Options

Room completed (100%)

Task 1 Deploy



Task 2 Introduction



Task 3 Nmap Switches



Task 4 Scan Types Overview



Task 5 Scan Types TCP Connect Scans



Task 6 Scan Types SYN Scans



Task 7 Scan Types UDP Scans

