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)

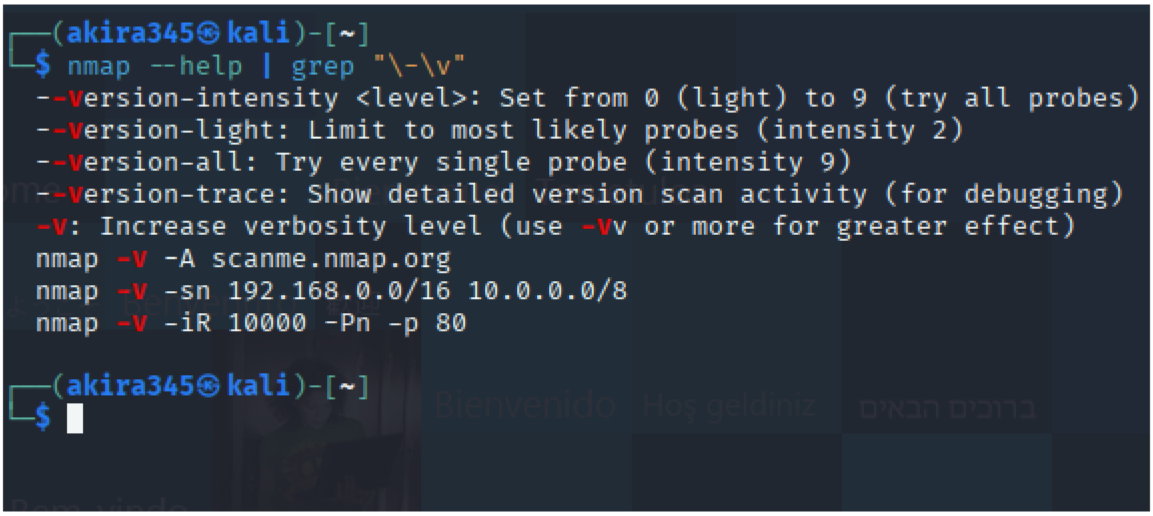
NSE scripts:

--script enables specific scripts;

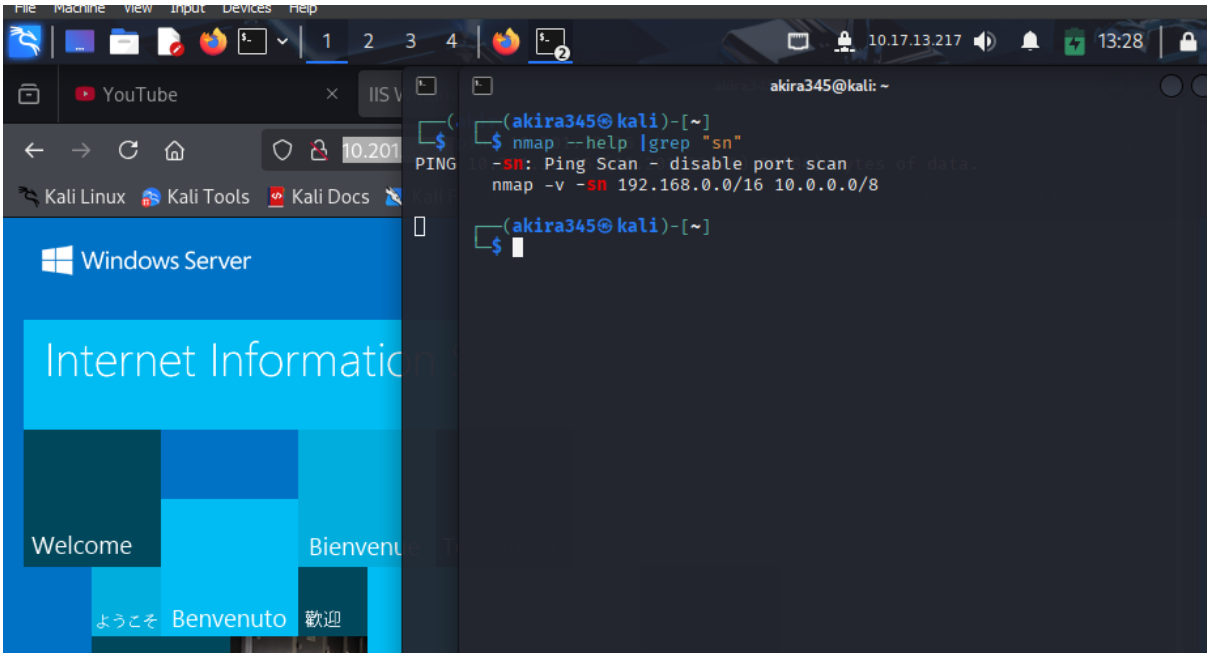
--script=vuln runs all vulnerability scripts

Overall a great room to practise and learn nmap commands.

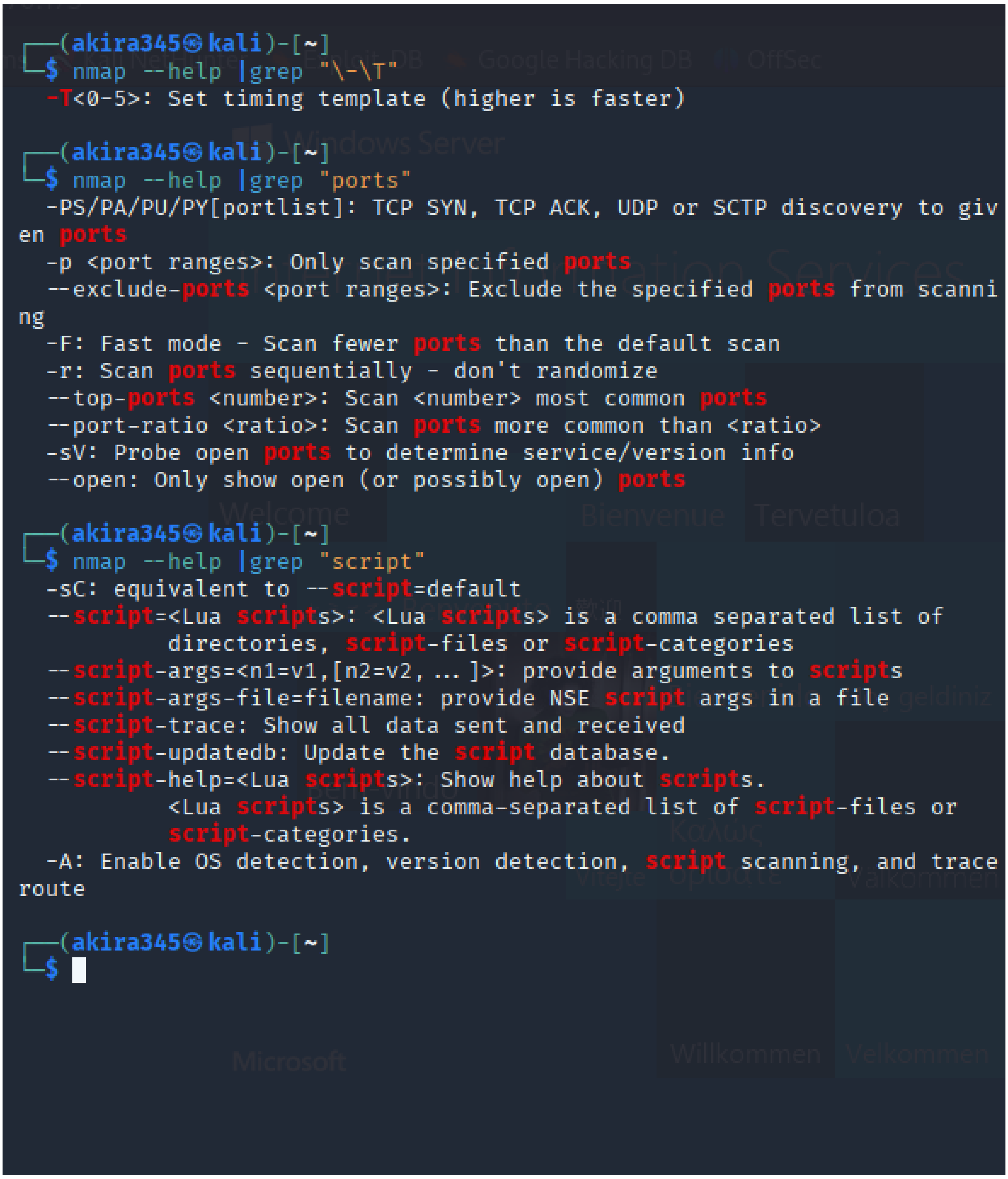
Screenshots



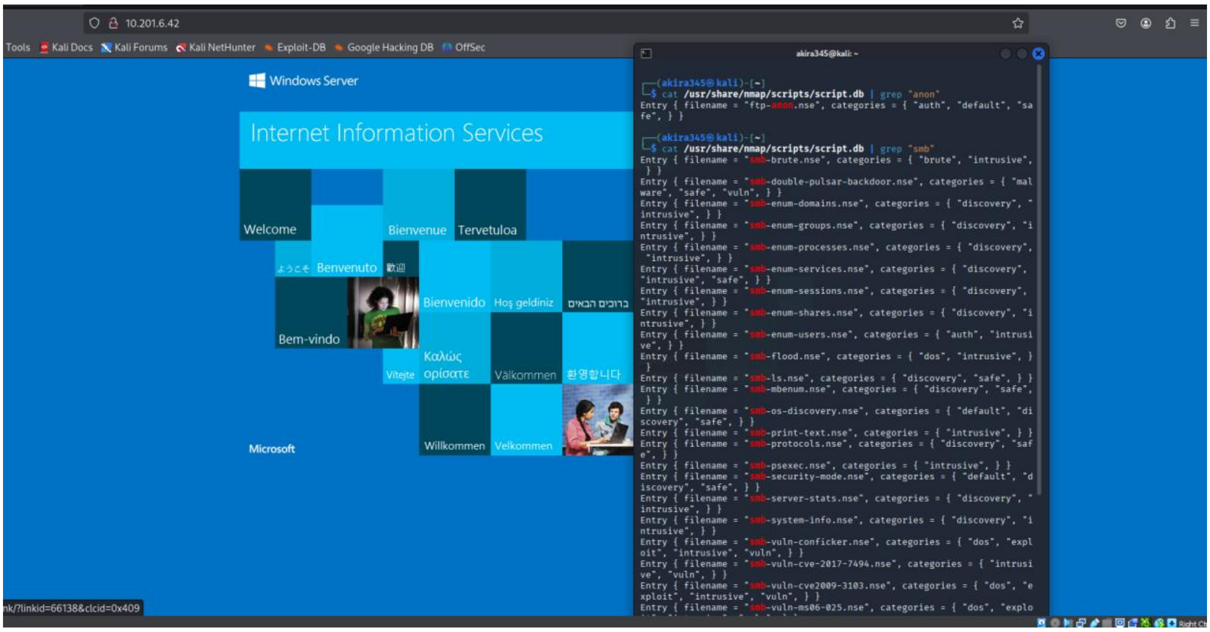
```
┌──(akira345㉿kali)-[~]
└─$ nmap --help | grep "\-\v"
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for 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)-[~]
└─$ 
```



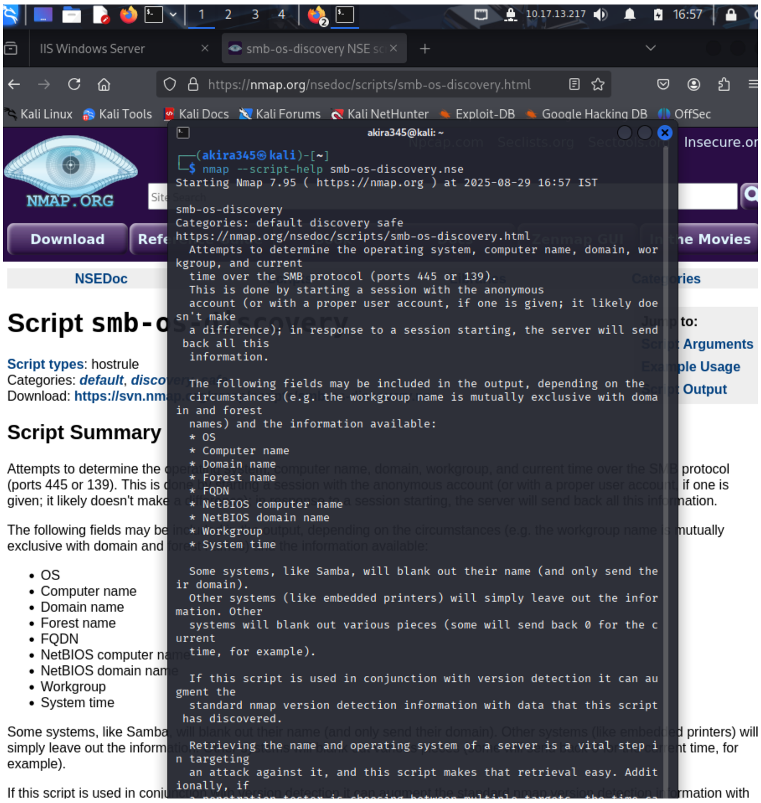
```
┌──(akira345㉿kali)-[~]
└─$ nmap --help |grep "sn"
  -sn: Ping Scan - disable port scan
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8

┌──(akira345㉿kali)-[~]
└─$ 
```



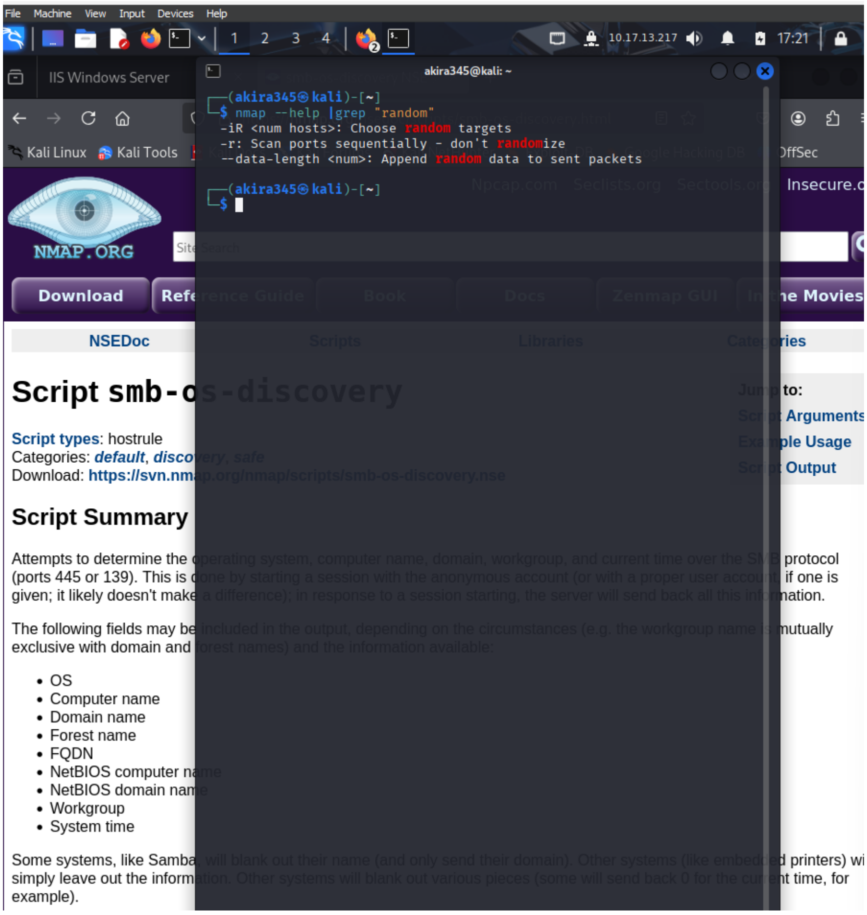
```
┌──(akira345㉿kali)-[~]
└─$ nmap --help |grep "\-\T"
  -T<0-5>: Set timing template (higher is faster)

┌──(akira345㉿kali)-[~]
└─$ nmap --help |grep "ports"
  -PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to giv
en ports
  -p <port ranges>: Only scan specified ports
  --exclude-ports <port ranges>: Exclude the specified ports from scanni
ng
  -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)-[~]
└─$ 
```



```
┌──(akira345㉿kali)-[~]
└─$ cat /usr/share/nmap/scripts/script.db | grep "anon"
Entry { filename = "ftp-anon.nse", categories = { "auth", "default", "sa
fe", } }

┌──(akira345㉿kali)-[~]
└─$ cat /usr/share/nmap/scripts/script.db | grep "smb"
Entry { filename = "smb-brute.nse", categories = { "brute", "intrusive",
 } }
Entry { filename = "smb-double-pulsar-backdoor.nse", categories = { "mal
ware", "safe", "vuln", } }
Entry { filename = "smb-enum-domains.nse", categories = { "discovery", "
intrusive", } }
Entry { filename = "smb-enum-groups.nse", categories = { "discovery", "i
ntrusive", } }
Entry { filename = "smb-enum-processes.nse", categories = { "discovery",
 "intrusive", } }
Entry { filename = "smb-enum-services.nse", categories = { "discovery",
"intrusive", "safe", } }
Entry { filename = "smb-enum-sessions.nse", categories = { "discovery",
"intrusive", } }
Entry { filename = "smb-enum-shares.nse", categories = { "discovery", "i
ntrusive", } }
Entry { filename = "smb-enum-users.nse", categories = { "auth", "intrusi
ve", } }
Entry { filename = "smb-flood.nse", categories = { "dos", "intrusive", }
 }
Entry { filename = "smb-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-mbenum.nse", categories = { "discovery", "safe",
 } }
Entry { filename = "smb-os-discovery.nse", categories = { "default", "di
scovery", "safe", } }
Entry { filename = "smb-print-text.nse", categories = { "intrusive", } }
Entry { filename = "smb-protocols.nse", categories = { "discovery", "saf
e", } }
Entry { filename = "smb-psexec.nse", categories = { "intrusive", } }
Entry { filename = "smb-security-mode.nse", categories = { "default", "d
iscovery", "safe", } }
Entry { filename = "smb-server-stats.nse", categories = { "discovery", "
intrusive", } }
Entry { filename = "smb-system-info.nse", categories = { "discovery", "i
ntrusive", } }
Entry { filename = "smb-vuln-conficker.nse", categories = { "dos", "expl
oit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-cve-2017-7494.nse", categories = { "intrusi
ve", "vuln", } }
Entry { filename = "smb-vuln-cve2009-3103.nse", categories = { "dos", "e
xploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms06-025.nse", categories = { "dos", "explo
```



```
┌──(akira345㉿kali)-[~]
└─$ nmap --script-help smb-os-discovery.nse
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 16:57 IST

smb-os-discovery
Categories: default discovery safe
https://nmap.org/nsedoc/scripts/smb-os-discovery.html
  Attempts to determine the operating system, computer name, domain, wor
kgroup, and current
  time over the SMB protocol (ports 445 or 139).
  This is done by starting a session with the anonymous
  account (or with a proper user account, if one is given; it likely doe
sn't make
  a difference); in response to a session starting, the server will send
 back all this
  information.

  The following fields may be included in the output, depending on the
  circumstances (e.g. the workgroup name is mutually exclusive with doma
in and forest
  names) and the information available:
  * OS
  * Computer name
  * Domain name
  * Forest name
  * FQDN
  * NetBIOS computer name
  * NetBIOS domain name
  * Workgroup
  * System time

  Some systems, like Samba, will blank out their name (and only send the
ir domain).
  Other systems (like embedded printers) will simply leave out the infor
mation. Other
  systems will blank out various pieces (some will send back 0 for the c
urrent
  time, for example).

  If this script is used in conjunction with version detection it can au
gment the
  standard nmap version detection information with data that this script
 has discovered.

  Retrieving the name and operating system of a server is a vital step i
n targeting
  an attack against it, and this script makes that retrieval easy. Addit
ionally, if
```



```
┌──(akira345㉿kali)-[~]
└─$ nmap --help |grep "random"
  -iR <num hosts>: Choose random targets
  -r: Scan ports sequentially - don't randomize
  --data-length <num>: Append random data to sent packets

┌──(akira345㉿kali)-[~]
└─$ ▌
```

Script smb-os-discovery

Script types: hostrule
Categories: *default*, *discovery*, *safe*
Download: https://svn.nmap.org/nmap/scripts/smb-os-discovery.nse

Jump to:
Script Arguments
Example Usage
Script Output

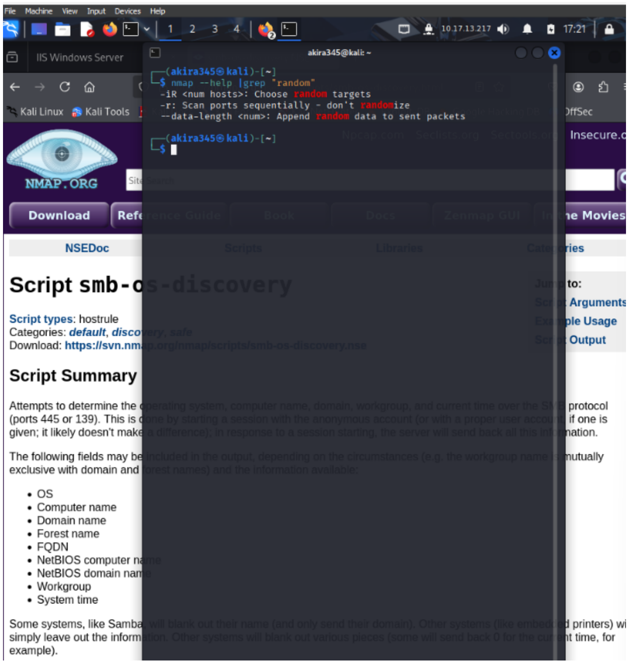
Script Summary

Attempts to determine the operating system, computer name, domain, workgroup, and current time over the SMB protocol (ports 445 or 139). This is done by starting a session with the anonymous account (or with a proper user account, if one is given; it likely doesn't make a difference); in response to a session starting, the server will send back all this information.

The following fields may be included in the output, depending on the circumstances (e.g. the workgroup name is mutually exclusive with domain and forest names) and the information available:

- OS
- Computer name
- Domain name
- Forest name
- FQDN
- NetBIOS computer name
- NetBIOS domain name
- Workgroup
- System time

Some systems, like Samba, will blank out their name (and only send their domain). Other systems (like embedded printers) wi simply leave out the information. Other systems will blank out various pieces (some will send back 0 for the current time, for example).



```
┌──(akira345㉿kali)-[~]
└─$ nmap --help |grep "random"
  -iR <num hosts>: Choose random targets
  -r: Scan ports sequentially - don't randomize
  --data-length <num>: Append random data to sent packets

┌──(akira345㉿kali)-[~]
└─$ ▌
```

Script smb-os-discovery

Script types: hostrule
Categories: default, discovery, safe
Download: https://svn.nmap.org/nmap/scripts/smb-os-discovery.nse

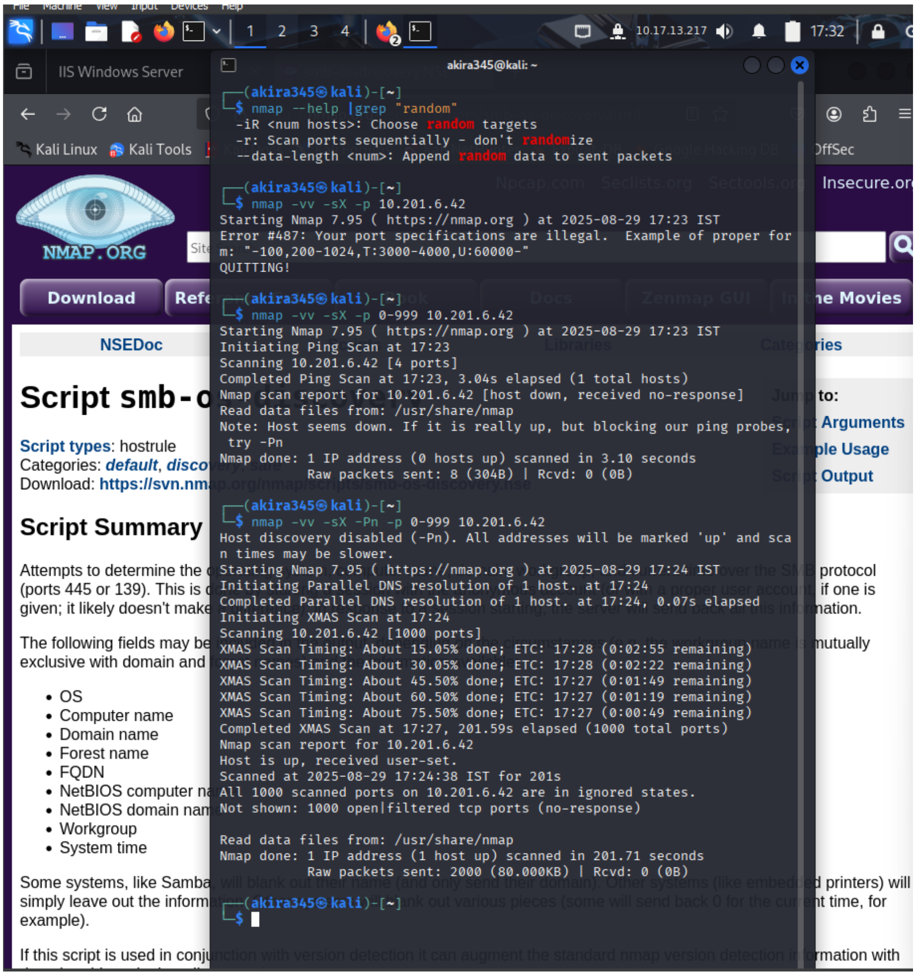
Script Summary

Attempts to determine the operating system, computer name, domain, workgroup, and current time over the SMB protocol (ports 445 or 139). This is done by starting a session with the anonymous account (or with a proper user account, if one is given; it likely doesn't make a difference); in response to a session starting, the server will send back all this information.

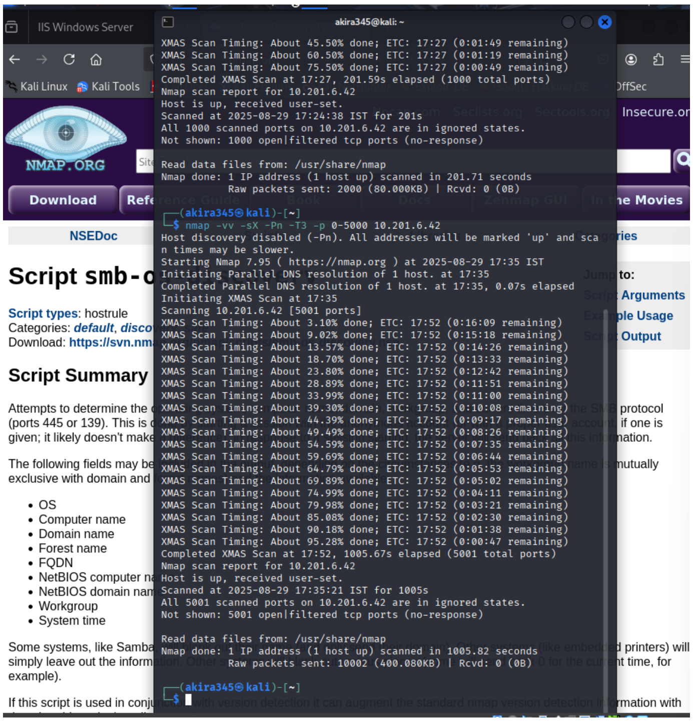
The following fields may be included in the output, depending on the circumstances (e.g. the workgroup name is mutually exclusive with domain and forest names) and the information available:

- OS
- Computer name
- Domain name
- Forest name
- FQDN
- NetBIOS computer name
- NetBIOS domain name
- Workgroup
- System time

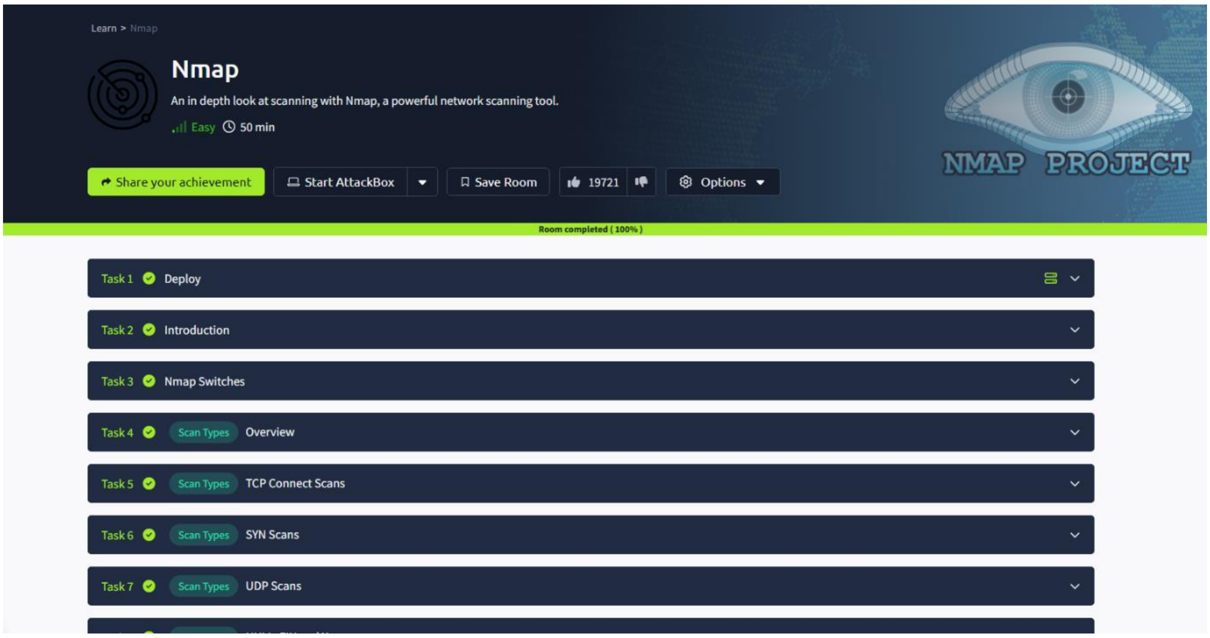
Some systems, like Samba, will blank out their name (and only send their domain). Other systems (like embedded printers) wi simply leave out the information. Other systems will blank out various pieces (some will send back 0 for the current time, for example).



```
┌──(akira345㉿kali)-[~]
└─$ nmap --help |grep "random"
  -iR <num hosts>: Choose random targets
  -r: Scan ports sequentially - don't randomize
  --data-length <num>: Append random data to sent packets

┌──(akira345㉿kali)-[~]
└─$ nmap -vv -sX -p 10.201.6.42
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 17:23 IST
Error #487: Your port specifications are illegal.  Example of proper for
m: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!

┌──(akira345㉿kali)-[~]
└─$ nmap -vv -sX -p 0-999 10.201.6.42
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 17:23 IST
Initiating Ping Scan at 17:23
Scanning 10.201.6.42 [4 ports]
Completed Ping Scan at 17:23, 3.04s elapsed (1 total hosts)
Nmap scan report for 10.201.6.42 [host down, received no-response]
Read data files from: /usr/share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes,
 try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds
           Raw packets sent: 8 (304B) | Rcvd: 0 (0B)

┌──(akira345㉿kali)-[~]
└─$ nmap -vv -sX -Pn -p 0-999 10.201.6.42
Host discovery disabled (-Pn). All addresses will be marked 'up' and sca
n times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 17:24 IST
Initiating Parallel DNS resolution of 1 host. at 17:24
Completed Parallel DNS resolution of 1 host. at 17:24, 0.07s elapsed
Initiating XMAS Scan at 17:24
Scanning 10.201.6.42 [1000 ports]
XMAS Scan Timing: About 15.05% done; ETC: 17:28 (0:02:55 remaining)
XMAS Scan Timing: About 30.05% done; ETC: 17:28 (0:02:22 remaining)
XMAS Scan Timing: About 45.50% done; ETC: 17:27 (0:01:49 remaining)
XMAS Scan Timing: About 60.50% done; ETC: 17:27 (0:01:19 remaining)
XMAS Scan Timing: About 75.50% done; ETC: 17:27 (0:00:49 remaining)
Completed XMAS Scan at 17:27, 201.59s elapsed (1000 total ports)
Nmap scan report for 10.201.6.42
Host is up, received user-set.
Scanned at 2025-08-29 17:24:38 IST for 201s
All 1000 scanned ports on 10.201.6.42 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 201.71 seconds
           Raw packets sent: 2000 (80.000KB) | Rcvd: 0 (0B)

┌──(akira345㉿kali)-[~]
└─$ 
```



```
XMAS Scan Timing: About 45.50% done; ETC: 17:27 (0:01:49 remaining)
XMAS Scan Timing: About 60.50% done; ETC: 17:27 (0:01:19 remaining)
XMAS Scan Timing: About 75.50% done; ETC: 17:27 (0:00:49 remaining)
Completed XMAS Scan at 17:27, 201.59s elapsed (1000 total ports)
Nmap scan report for 10.201.6.42
Host is up, received user-set.
Scanned at 2025-08-29 17:24:38 IST for 201s
All 1000 scanned ports on 10.201.6.42 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 201.71 seconds
           Raw packets sent: 2000 (80.000KB) | Rcvd: 0 (0B)

┌──(akira345㉿kali)-[~]
└─$ nmap -vv -sX -Pn -T3 -p 0-5000 10.201.6.42
Host discovery disabled (-Pn). All addresses will be marked 'up' and sca
n times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 17:35 IST
Initiating Parallel DNS resolution of 1 host. at 17:35
Completed Parallel DNS resolution of 1 host. at 17:35, 0.07s elapsed
Initiating XMAS Scan at 17:35
Scanning 10.201.6.42 [5001 ports]
XMAS Scan Timing: About 3.10% done; ETC: 17:52 (0:16:09 remaining)
XMAS Scan Timing: About 9.02% done; ETC: 17:52 (0:15:18 remaining)
XMAS Scan Timing: About 13.57% done; ETC: 17:52 (0:14:26 remaining)
XMAS Scan Timing: About 18.70% done; ETC: 17:52 (0:13:33 remaining)
XMAS Scan Timing: About 23.80% done; ETC: 17:52 (0:12:42 remaining)
XMAS Scan Timing: About 28.89% done; ETC: 17:52 (0:11:51 remaining)
XMAS Scan Timing: About 33.99% done; ETC: 17:52 (0:11:00 remaining)
XMAS Scan Timing: About 39.30% done; ETC: 17:52 (0:10:08 remaining)
XMAS Scan Timing: About 44.39% done; ETC: 17:52 (0:09:17 remaining)
XMAS Scan Timing: About 49.49% done; ETC: 17:52 (0:08:26 remaining)
XMAS Scan Timing: About 54.59% done; ETC: 17:52 (0:07:35 remaining)
XMAS Scan Timing: About 59.69% done; ETC: 17:52 (0:06:44 remaining)
XMAS Scan Timing: About 64.79% done; ETC: 17:52 (0:05:53 remaining)
XMAS Scan Timing: About 69.89% done; ETC: 17:52 (0:05:02 remaining)
XMAS Scan Timing: About 74.99% done; ETC: 17:52 (0:04:11 remaining)
XMAS Scan Timing: About 79.98% done; ETC: 17:52 (0:03:21 remaining)
XMAS Scan Timing: About 85.08% done; ETC: 17:52 (0:02:30 remaining)
XMAS Scan Timing: About 90.18% done; ETC: 17:52 (0:01:38 remaining)
XMAS Scan Timing: About 95.28% done; ETC: 17:52 (0:00:47 remaining)
Completed XMAS Scan at 17:52, 1005.67s elapsed (5001 total ports)
Nmap scan report for 10.201.6.42
Host is up, received user-set.
Scanned at 2025-08-29 17:35:21 IST for 1005s
All 5001 scanned ports on 10.201.6.42 are in ignored states.
Not shown: 5001 open|filtered tcp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1005.82 seconds
           Raw packets sent: 10002 (400.080KB) | Rcvd: 0 (0B)

┌──(akira345㉿kali)-[~]
└─$ 
```



Nmap

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

Easy 50 min

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