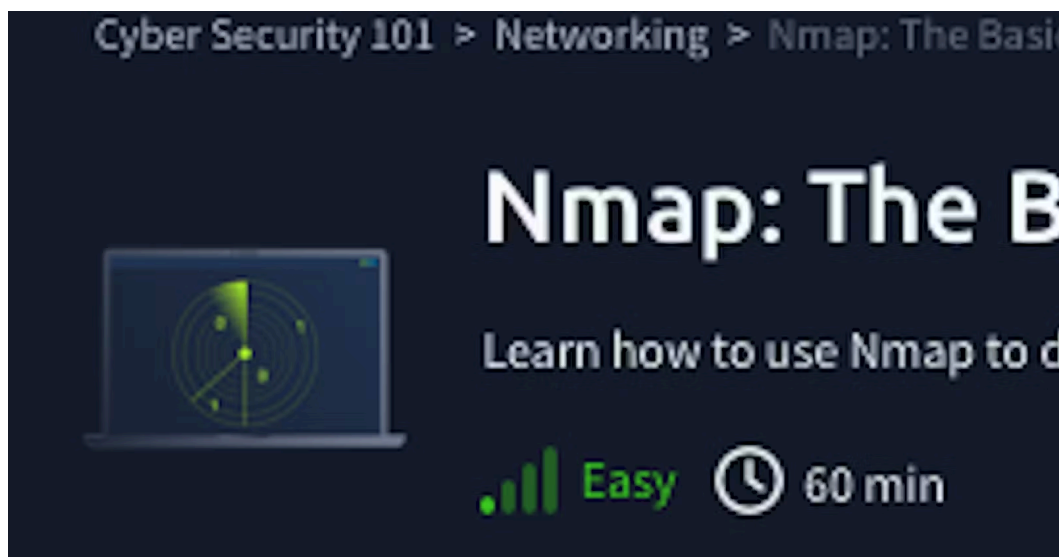


 Follow

Networking: Nmap: The Basics (TryHackMe)



J3bitok

Oct 27, 2024 ·  2 min read

In this article, I will write a write-up for Nmap: The Basics that covers Host Discovery: Who is Online, Port Scanning: Who is Listening, Version Detection: Extract More Information, Timing: How Fast is Fast, and Output: Controlling What You See.

1. What is the last IP address that will be scanned when your scan target is 192.168.0.1/27 ? 192.168.0.31



```

root@ip-10-10-5-216:~# nmap -sL 192.168.0.1/27

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-26 21:10 BST
Nmap scan report for ip-192-168-0-0.eu-west-1.compute.internal (192.168.0.0)
Nmap scan report for ip-192-168-0-1.eu-west-1.compute.internal (192.168.0.1)
Nmap scan report for ip-192-168-0-2.eu-west-1.compute.internal (192.168.0.2)
Nmap scan report for ip-192-168-0-3.eu-west-1.compute.internal (192.168.0.3)
Nmap scan report for ip-192-168-0-4.eu-west-1.compute.internal (192.168.0.4)
Nmap scan report for ip-192-168-0-5.eu-west-1.compute.internal (192.168.0.5)
Nmap scan report for ip-192-168-0-6.eu-west-1.compute.internal (192.168.0.6)
Nmap scan report for ip-192-168-0-7.eu-west-1.compute.internal (192.168.0.7)
Nmap scan report for ip-192-168-0-8.eu-west-1.compute.internal (192.168.0.8)
Nmap scan report for ip-192-168-0-9.eu-west-1.compute.internal (192.168.0.9)
Nmap scan report for ip-192-168-0-10.eu-west-1.compute.internal (192.168.0.10)
Nmap scan report for ip-192-168-0-11.eu-west-1.compute.internal (192.168.0.11)
Nmap scan report for ip-192-168-0-12.eu-west-1.compute.internal (192.168.0.12)
Nmap scan report for ip-192-168-0-13.eu-west-1.compute.internal (192.168.0.13)
Nmap scan report for ip-192-168-0-14.eu-west-1.compute.internal (192.168.0.14)
Nmap scan report for ip-192-168-0-15.eu-west-1.compute.internal (192.168.0.15)
Nmap scan report for ip-192-168-0-16.eu-west-1.compute.internal (192.168.0.16)
Nmap scan report for ip-192-168-0-17.eu-west-1.compute.internal (192.168.0.17)
Nmap scan report for ip-192-168-0-18.eu-west-1.compute.internal (192.168.0.18)
Nmap scan report for ip-192-168-0-19.eu-west-1.compute.internal (192.168.0.19)
Nmap scan report for ip-192-168-0-20.eu-west-1.compute.internal (192.168.0.20)
Nmap scan report for ip-192-168-0-21.eu-west-1.compute.internal (192.168.0.21)
Nmap scan report for ip-192-168-0-22.eu-west-1.compute.internal (192.168.0.22)
Nmap scan report for ip-192-168-0-23.eu-west-1.compute.internal (192.168.0.23)
Nmap scan report for ip-192-168-0-24.eu-west-1.compute.internal (192.168.0.24)
Nmap scan report for ip-192-168-0-25.eu-west-1.compute.internal (192.168.0.25)
Nmap scan report for ip-192-168-0-26.eu-west-1.compute.internal (192.168.0.26)
Nmap scan report for ip-192-168-0-27.eu-west-1.compute.internal (192.168.0.27)
Nmap scan report for ip-192-168-0-28.eu-west-1.compute.internal (192.168.0.28)
Nmap scan report for ip-192-168-0-29.eu-west-1.compute.internal (192.168.0.29)
Nmap scan report for ip-192-168-0-30.eu-west-1.compute.internal (192.168.0.30)
Nmap scan report for ip-192-168-0-31.eu-west-1.compute.internal (192.168.0.31)
Nmap done: 32 IP addresses (0 hosts up) scanned in 0.01 seconds
root@ip-10-10-5-216:~#

```

2. How many TCP ports are open on the target system at 10.10.235.198 ? 6

```

root@ip-10-10-5-216:~# nmap -sT 10.10.235.198

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-26 21:15 BST
Nmap scan report for ip-10-10-235-198.eu-west-1.compute.internal (10.10.235.198)
Host is up (0.00032s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
8008/tcp   open  http
MAC Address: 02:30:2C:9B:FC:9F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
root@ip-10-10-5-216:~#

```

3. Find the listening web server on 10.10.235.198 and access it with your browser. What is the flag that appears on its main page?

THM{SECRET_PAGE_38B9P6}

to start there's a hint on the question that you should access via

`http://ip_address:port_number`. Remember the computer has 65535 ports so I tried to use common ports like 80, 8080, etc, and the browser didn't open. I ran a command `nmap -sV -A 10.10.235.198` that gave us a comprehensive overview of our target machine IP which included open ports, 8008 showed

`8008/tcp open http lighttpd/1.4.74`. On opening the browser

`http://ip_address:8008` I got the flag



```

root@ip-10-10-5-216:~# nmap -sV -A 10.10.235.198
Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-26 21:23 BST
Nmap scan report for ip-10-10-235-198.eu-west-1.compute.internal (10.10.235.198)
Host is up (0.00035s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE VERSION
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
|_ fingerprint-strings:
|_   DNSStatusRequest, DNSVersionBindReq, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, JavaRMI, Kerberos, LANDesk-RC,
|_   BindReq, LDAPSearchReq, LPDString, NCP, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq,
|_   lServer, WMSRequest, X11Probe, afp, gloop, oracle-tns:
|_   Sat Oct 26 20:23:51 UTC 2024
17/tcp    open  qotd?
|_ fingerprint-strings:
|_   DNSStatusRequest:
|_     You will pioneer the first Martian colony.
|_   DNSVersionBindReq:
|_     Ships are safe in harbor, but they were never meant to stay there.
|_   GenericLines:
|_     Never commit yourself! Let someone else commit you.
|_   GetRequest:
|_     ... A solemn, unsmiling, sanctimonious old iceberg who looked like he
|_     waiting for a vacancy in the Trinity.
|_   Mark Twain
|_   HTTPOptions:
|_     You will gain money by an illegal action.
|_   Help:
|_     You are so boring that when I see you my feet go to sleep.
|_   Kerberos:
|_     Try to value useful qualities in one who loves you: THM AttackBox
|_   NULL:
|_     The countdown had stalled at 'T' minus 69 seconds when DesTree, the first
|_     female ape to go up in space, winked at me slyly and pouted her thick,
|_     rubbery lips unmistakably -- the first of many such advances during what
|_     would prove to be the longest, and most memorable, space voyage of my
|_     career.
|_     Winning sentence, 1985 Bulwer-Lytton bad fiction contest.
|_   RPCCheck:
|_     Your life would be very empty if you had nothing to regret.
|_   RTSPRequest:
|_     Better hope the life-inspector doesn't come around while you have your
|_     life in such a mess.
|_   SMBProgNeg:
|_     Learn to pause -- or nothing worthwhile can catch up to you.
|_   SSLSessionReq:
|_     You're being followed. Cut out the hanky-panky for a few days.
|_   TLSSessionReq:
|_     You will be married within a year.
|_   X11Probe:
|_     You are wise, witty, and wonderful, but you spend too much time reading
|_     this sort of trash.
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
8008/tcp  open  http      lighttpd 1.4.74
|_ http-server-header: lighttpd/1.4.74
|_ http-title: Types and Styles of Coffee
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://
g/cgl-bin/submit.cgi?new-service:
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port13-TCP-V=7.60I=78D=10/26Time=671d4fD8NP=x86_64-pc-linux-gnuKr(NULL
SF:L_ID,"Sat\x20Oct\x2026\x2020:23:51\x20UTC\x202024\n")Kr(GenericLines,1D
SF:,"Sat\x20Oct\x2026\x2020:23:51\x20UTC\x202024\n")Kr(GetRequest,1D,"Sat\
SF:x20Oct\x2026\x2020:23:51\x20UTC\x202024\n")Kr(HTTPOptions,1D,"Sat\x20Oc
SF:tl\x2026\x2020:23:51\x20UTC\x202024\n")Kr(RTSPRequest,1D,"Sat\x20Oct\x20

```

Types and Styles of Coffee — Mozilla Firefox

TryHackMe | Cyber Secur... Types and Styles of Coffee x +

10.10.235.198:8008

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator

Flag

THM{SECRET_PAGE_38B9P6}

Types and Styles of Coffee

Coffee is enjoyed worldwide in various forms. Here's an overview of popular coffee types and styles:

Espresso-Based Drinks

1. Espresso

A concentrated shot of coffee brewed by forcing hot water through finely-ground coffee beans.

g/cgl-bin/submit.cgi?new-service:

```

SMBProgNeg:
  Learn to pause -- or nothing worthwhile can catch up to you.
SSLSessionReq:
  You're being followed. Cut out the hanky-panky for a few days.
TLSSessionReq:
  You will be married within a year.
X11Probe:
  You are wise, witty, and wonderful, but you spend too much time reading
  this sort of trash.
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
8008/tcp  open  http      lighttpd 1.4.74
|_ http-server-header: lighttpd/1.4.74
|_ http-title: Types and Styles of Coffee
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgl-bin/submit.cgi?new-service:
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port13-TCP-V=7.60I=78D=10/26Time=671d4fD8NP=x86_64-pc-linux-gnuKr(NULL
SF:L_ID,"Sat\x20Oct\x2026\x2020:23:51\x20UTC\x202024\n")Kr(GenericLines,1D
SF:,"Sat\x20Oct\x2026\x2020:23:51\x20UTC\x202024\n")Kr(GetRequest,1D,"Sat\
SF:x20Oct\x2026\x2020:23:51\x20UTC\x202024\n")Kr(HTTPOptions,1D,"Sat\x20Oc
SF:tl\x2026\x2020:23:51\x20UTC\x202024\n")Kr(RTSPRequest,1D,"Sat\x20Oct\x20
SF:tl\x2026\x2020:23:51\x20UTC\x202024\n")Kr(RPCCheck,1D,"Sat\x20Oct\x2026\x2020
SF:23:51\x20UTC\x202024\n")Kr(DNSVersionBindReq,1D,"Sat\x20Oct\x2026\x2020
SF:0:23:51\x20UTC\x202024\n")Kr(DNSStatusRequest,1D,"Sat\x20Oct\x2026\x2020
SF:0:23:51\x20UTC\x202024\n")Kr(Help,1D,"Sat\x20Oct\x2026\x2020:23:51\x20U
SF:TC\x202024\n")Kr(SSLSessionReq,1D,"Sat\x20Oct\x2026\x2020:23:51\x20UTC
SF:x202024\n")Kr(TLSSessionReq,1D,"Sat\x20Oct\x2026\x2020:23:51\x20UTC\x20
SF:2024\n")Kr(Kerberos,1D,"Sat\x20Oct\x2026\x2020:23:51\x20UTC\x202024\n")
SF:Kr(SMBProgNeg,1D,"Sat\x20Oct\x2026\x2020:23:51\x20UTC\x202024\n")Kr(X11

```

Your streak has increased. You're 27

4. What is the name and detected version of the web server running on 10.10.235.198 ?

running `nmap -A ip_address` brings it up notice that our attack machine uses `lighttpd` and not the web servers like `nginx` so that a hint too

```
root@kali-10-10-5-216:~# nmap -A 10.10.235.198
Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-26 22:28 BST
Stats: 0:01:48 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 22:30 (0:00:21 remaining)
Nmap scan report for 10.10-10-235-198.eu-west-1.compute.internal (10.10.235.198)
Host is up (0.00030s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime?
|_ fingerprint-strings:
|_   DNSStatusRequest, DNSVersionBindReq, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, JavaRMI, Kerber
BindReq, LDAPSearchReq, LPDString, NCP, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TL
Server, WMSRequest, X11Probe, afp, glsp, oracle-tns:
|_   Sat Oct 26 21:28:50 UTC 2024
17/tcp    open  qotd?
|_ fingerprint-strings:
|_   DNSStatusRequest:
|_     There is no character, howsoever good and fine, but it can be destroyed by
|_     ridicule, howsoever poor and witless. Observe the ass, for instance: his
|_     character is about perfect, he is the choicest spirit among all the humbler
|_     animals, yet see what ridicule has brought him to. Instead of feeling
|_     complimented when we are called an ass, we are left in doubt.
|_     Mark Twain, "Pudd'nhead Wilson's Calendar"
|_   DNSVersionBindReq:
|_     Someone whom you reject today, will reject you tomorrow.
|_   GenericLines:
|_     Your society will be sought by people of taste and refinement.
|_   GetRequest:
|_     The first thing we do, let's kill all the lawyers.
|_     Shakespeare, "Henry VI", Part IV
|_   HTTPOptions:
|_     There is no distinctly native American criminal class except Congress.
|_     Mark Twain
|_   Help:
|_     Your present plans will be successful.
|_   NULL:
|_     Good day to deal with people in high places; particularly lonely stewardesses.
|_   RPCCheck:
|_     You never have to change anything you got up in the middle of the night
|_     write.
|_     Saul Bellow
|_   RTSPRequest:
|_     Hell is empty and all the devils are here.
|_     Shakespeare, "The Tempest" THM AttackBox
|_   SSLSessionReq:
|_     Its name is Public Opinion. It is held in reverence. It settles everything.
|_     Some think it is the voice of God.
|_     Mark Twain
|_   TLSSessionReq:
|_     Q: "What is the burning question on the mind of every dyslexic
|_     existentialist?"
|_     there a dog?"
22/tcp    open  ssh          OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
8008/tcp  open  http         lighttpd/1.4.74
|_ http-server-header: lighttpd/1.4.74
|_ http-title: Types and Styles of Coffee
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
s/cgi-bin/submit.cgi?new-service:
```

5. What is the non-numeric equivalent of `-T4`? `-T` aggressive
6. What option must you add to your `nmap` command to enable debugging? `-d`
7. What kind of scan will Nmap use if you run `nmap MACHINE_IP` with local user privileges? Connect Scan

Thank you for reading my article. Please leave any questions or comments on improving my learning journey and the THM challenges. We can also connect more on [LinkedIn](#) or [X](#).

Subscribe to our newsletter

Read articles from **Sharon Jebitok** directly inside your inbox. Subscribe to the newsletter, and don't miss out.

Enter your email address

SUBSCRIBE

Did you find this article valuable?

Support **Sharon Jebitok** by becoming a sponsor. Any amount is appreciated!



Sponsor

[Learn more about Hashnode Sponsors](#)

nmap

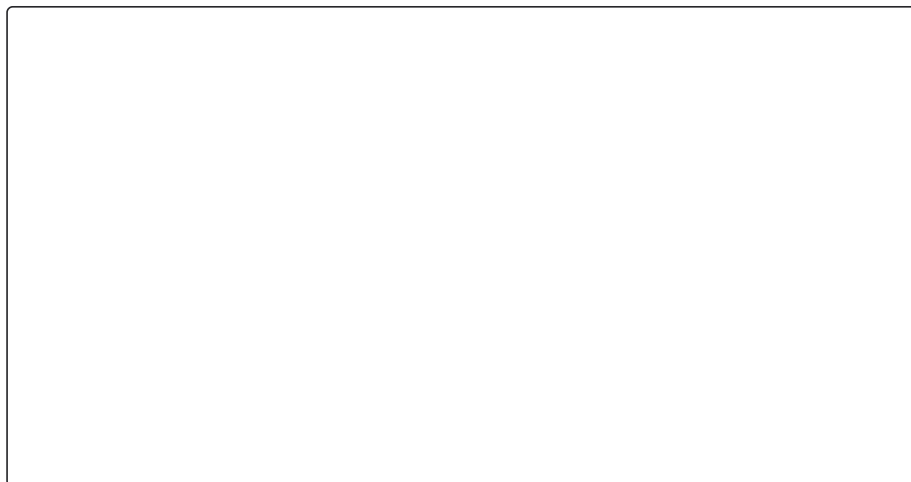
networking

Write Up

tryhackme

MORE ARTICLES

J3bitok

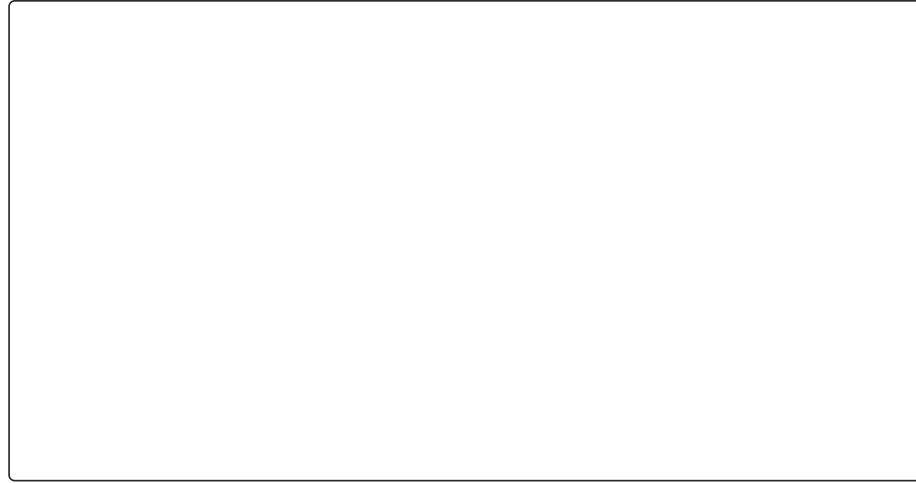


The Advent of Cyber: Day 16: Azure - Wareville's Key Vault grew three sizes that day. (TryHackMe)

In this article, we'll cover Azure - Wareville's Key Vault, which grew three sizes that day. The wri...

J3bitok





The Advent of Cyber: Day 10: Phishing - He had a brain full of macros, and had shells in his soul. (...)

In this article, we'll cover Phishing - He had a brain full of macros and had shells in his soul wri...



The Advent of Cyber: Day 12: Web timing attacks: If I can't steal their money, I'll steal their joy!...

In this article, we'll cover Web Timing Attacks Attacks—If you'd like to WPA, press the star key! wr...

©2025 Sharon Jebitok

[Archive](#) • [Privacy policy](#) • [Terms](#)





Powered by Hashnode - Build your developer hub.

[Start your blog](#)

[Create docs](#)

