Service Scanning

We're ready to take it a step further and start exploring a machine! The first thing we need to do is identify the operating system and any available services that might be running. A service is an application running on a computer that performs some useful function for other users or computers. We call these specialized machines that host these useful services "servers" instead of workstations, allowing users to interact with and consume these various services. What we're interested in are services that have either been misconfigured or have a vulnerability. Instead of performing the actions expected as part of the service, we are interested to see if we can coerce the service into performing some unintended action that supports our objectives, such as executing a command of our choosing.

Computers are assigned an IP address, which allows them to be uniquely identified and accessible on a network. The services running on these computers may be assigned a port number to make the service accessible. As discussed prior, port numbers range from 1 to 65,535, with the range of well-known ports 1 to 1,023 being reserved for privileged services. Port 0 is a reserved port in TCP/IP networking and is not used in TCP or UDP messages. If anything attempts to bind to port 0 (such as a service), it will bind to the next available port above port 1,024 because port 0 is treated as a "wild card" port.

To access a service remotely, we need to connect using the correct IP address and port number and use a language that the service understands. Manually examining all of the 65,535 ports for any available services would be laborious, and so tools have been created to automate this process and scan the range of ports for us. One of the most commonly used scanning tools is Nmap(Network Mapper).

Nmap

Let us start with the most basic scan. Suppose that we want to perform a basic scan against a target residing at 10.129.42.253. To do this we should type `nmap 10.129.42.253` and hit return. We see that the `Nmap` scan was completed very quickly. This is because if we don't specify any additional options, Nmap will only scan the 1,000 most common ports by default. The scan output reveals that ports 21, 22, 80, 139, and 445 are available.

```
MichaelLuka@htb[/htb]$ nmap 10.129.42.253

Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-25 16:07 EST
Nmap scan report for 10.129.42.253
Host is up (0.11s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 2.19 seconds
```

Under the `PORT` heading, it also tells us that these are TCP ports. By default, `Nmap` will conduct a TCP scan unless specifically requested to perform a UDP scan.

The `STATE` heading confirms that these ports are open. Sometimes we will see other ports listed that have a different state, such as `filtered`. This can happen if a firewall is only allowing access to the ports from specific addresses.

The `SERVICE` heading tells us the service's name is typically mapped to the specific port number. However, the default scan will not tell us what is listening on that port. Until we instruct `Nmap` to interact with the service and attempt to tease out identifying information, it could be another service altogether.

As we gain familiarity, we will notice that several ports are commonly associated with Windows or Linux. For example, port 3389 is the default port for Remote Desktop Services and is an excellent indication that the target is a Windows machine. In our current scenario, port 22 (SSH) being available indicates that the target is running Linux/Unix, but this service can also be configured on Windows. Let us run a more advanced `Nmap` scan and gather more information about the target device.

We can use the `-sC` parameter to specify that `Nmap` scripts should be used to try and obtain more detailed information. The `-sV` parameter instructs `Nmap` to perform a version scan. In this scan, Nmap will fingerprint services on the target system and identify the service protocol, application name, and version. The version scan is underpinned by a comprehensive database of over 1,000 service signatures. Finally, `-p-` tells Nmap that we want to scan all 65,535 TCP ports.

```
MichaelLuka@htb[/htb]$ nmap -sV -sC -p- 10.129.42.253

Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-25 16:18 EST
Nmap scan report for 10.129.42.253
Host is up (0.11s latency).
Not shown: 65530 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 ftp      ftp          4096 Feb 25 19:25 pub
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.2
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: PHP 7.4.3 - phpinfo()
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: GS-SVCSCAN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-02-25T21:21:51
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 233.68 seconds
```

This returns a lot more information. We see that it took a lot longer to scan 65,535 ports than 1,000 ports. The `-sC` and `-sV` options also increase the duration of a scan, as instead of performing a simple TCP handshake, they perform a lot more checks. We notice that this time there is a VERSION heading, which reports the service version and the operating system if this is possible to identify.

So far, we know that the operating system is Ubuntu Linux. Application versions can also help reveal the target OS version. Take OpenSSH, for example. We see the reported version is `OpenSSH 8.2p1 Ubuntu 4ubuntu0.1`. From inspection of other Ubuntu SSH package changelogs, we see the release version takes the format `1:7.3p1-1ubuntu0.1`. Updating our version to fit this format, we get `1:8.2p1-4ubuntu0.1`. A quick search for this version online reveals that it is included in Ubuntu Linux Focal Fossa 20.04.

1:8.2p1-4ubuntu0.1 release

All | Shopping | Images | News | Maps | More | Settings | Tools

About 4,650 results (0.36 seconds)

launchpad.net › ubuntu › +source › 1:8.2p1-4ubuntu0.1

1:8.2p1-4ubuntu0.1 : openssh package : Ubuntu

8 Jun 2020 — openssh (**1:8.2p1-4ubuntu0.1**) focal; urgency=medium * d/p/lp-1876320-*: avoid applying defaults for every include statement (LP: #1876320) ...

launchpad.net › ubuntu › focal › +package › openssh-ser...

openssh-server : Focal (20.04) : Ubuntu - Launchpad.net

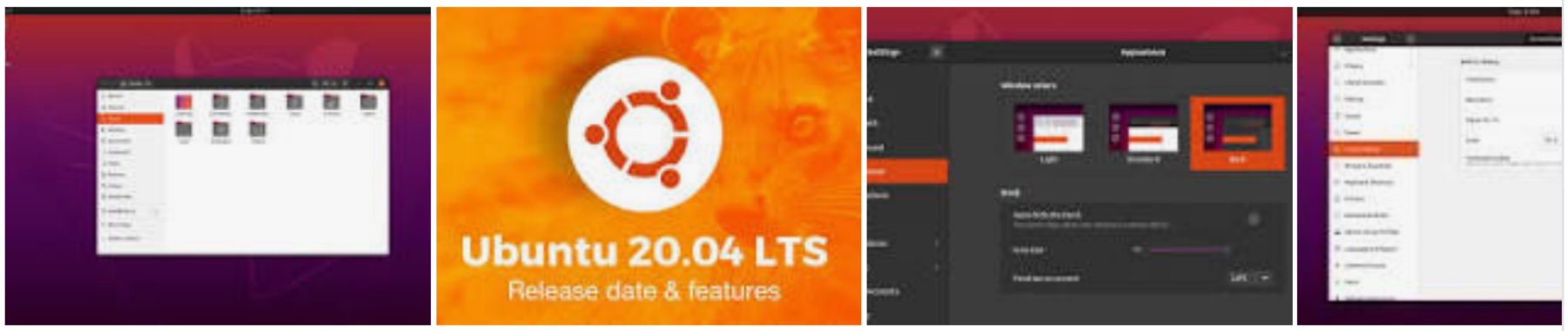
openssh **1:8.2p1-4ubuntu0.1** source package in Ubuntu. Published versions. openssh-server 1:8.0p1-6build1 in amd64 (**Release**) · openssh-server 1:8.2p1-4 in ...

Another quick search reveals that the release date of this OS is April 23rd, 2020.

ubuntu focal 20.04 release date

All | News | Shopping | Images | Videos | More | Settings | Tools

About 1,320,000 results (0.50 seconds)



April 23, 2020

Ubuntu 20.04 was released on Thursday **April 23, 2020**. 14 May 2020

www.omgubuntu.co.uk › News

Ubuntu 20.04 Download Link & Top Features (Updated ...

About featured snippets | Feedback

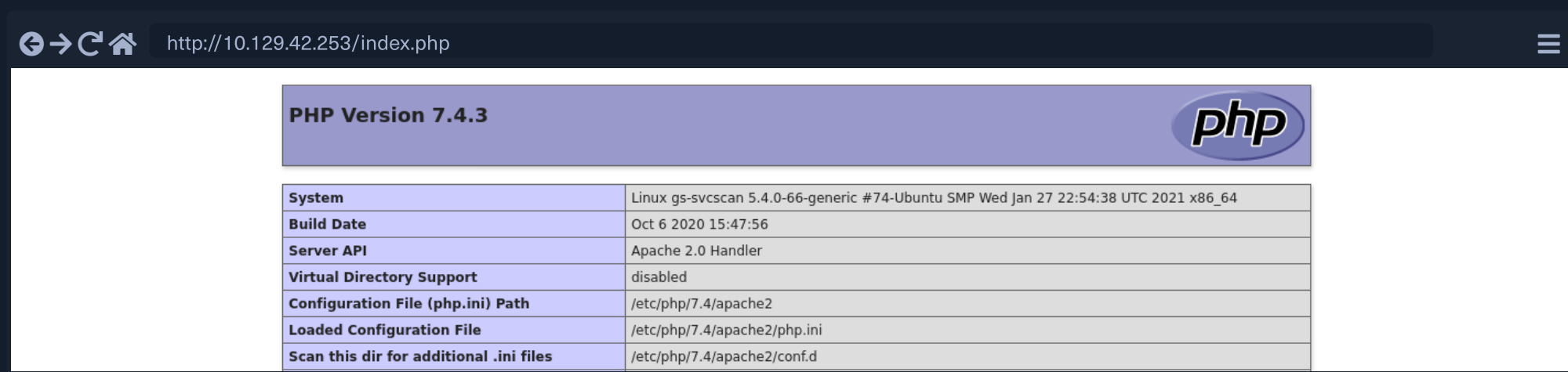
wiki.ubuntu.com › FocalFossa › ReleaseNotes

release notes for Ubuntu 20.04 LTS (Focal Fossa) - Ubuntu Wiki

Linux Kernel. **Ubuntu 20.04** LTS is based on the long-term supported **Linux release** series 5.4. Notable features and enhancements in 5.4 since 5.3 ...

FocalFossa/ReleaseNotes ... · Kubuntu · UbuntuStudio · FoundationsTeam ...

However, it is worth noting that this cross-referencing technique is not entirely reliable, as it is possible to install more recent application packages on an older OS version. The script scan `-sC` flag causes `Nmap` to report the server headers `http-server-header` page and the page title `http-title` for any web page hosted on the webserver. The web page title `PHP 7.4.3 - phpinfo()` indicates that this is a PHPInfo file, which is often manually created to confirm that PHP has been successfully installed. The title (and PHPInfo page) also reveals the PHP version, which is worth noting if it is vulnerable.



Nmap Scripts

Specifying `-sC` will run many useful default scripts against a target, but there are cases when running a specific script is required. For example, in an assessment scope, we may be asked to audit a large Citrix installation. We could use this `Nmap` script to audit for the severe Citrix NetScaler vulnerability (CVE-2019–19781), while `Nmap` also has other scripts to audit a Citrix installation.

Nmap Scripts

```
MichaelLuka@htb[/htb]$ locate scripts/citrix

/usr/share/nmap/scripts/citrix-brute-xml.nse
/usr/share/nmap/scripts/citrix-enum-apps-xml.nse
/usr/share/nmap/scripts/citrix-enum-apps.nse
/usr/share/nmap/scripts/citrix-enum-servers-xml.nse
/usr/share/nmap/scripts/citrix-enum-servers.nse
```

The syntax for running an Nmap script is `nmap --script <script name> -p<port> <host>`. `Nmap` scripts are a great way to enhance our scans' functionality, and inspection of the available options will pay dividends. Check out the Network Enumeration with Nmap module for a more detailed study of the `Nmap` tool.

Attacking Network Services

Banner Grabbing

As previously discussed, banner grabbing is a useful technique to fingerprint a service quickly. Often a service will look to identify itself by displaying a banner once a connection is initiated. Nmap will attempt to grab the banners if the syntax `nmap -sV --script=banner <target>` is specified. We can also attempt this manually using `Netcat`. Let us take another example, using the `nc` version of `Netcat`:

Banner Grabbing

```
MichaelLuka@htb[/htb]$ nc -nv 10.129.42.253 21

(UNKNOWN) [10.129.42.253] 21 (ftp) open
220 (vsFTPd 3.0.3)
```

This reveals that the version of `vsFTPd` on the server is `3.0.3`. We can also automate this process using `Nmap's` powerful scripting engine: `nmap -sV --script=banner -p21 10.10.10.0/24`.

FTP

It is worth gaining familiarity with FTP, as it is a standard protocol, and this service can often contain interesting data. A `Nmap` scan of the default port for FTP (21) reveals the vsftpd 3.0.3 installation that we identified previously. Further, it also reports that anonymous authentication is enabled and that a `pub` directory is available.

FTP

```
MichaelLuka@htb[/htb]$ nmap -sC -sV -p21 10.129.42.253

Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-20 00:54 GMT
Nmap scan report for 10.129.42.253
Host is up (0.081s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 ftp      ftp          4096 Dec 19 23:50 pub
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.2
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
```

Let us connect to the service using the `ftp` command-line utility.

FTP

```
MichaelLuka@htb[/htb]$ ftp -p 10.129.42.253

Connected to 10.129.42.253.
220 (vsFTPd 3.0.3)
Name (10.129.42.253:user): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.

ftp> ls
227 Entering Passive Mode (10,129,42,253,158,60).
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Feb 25 19:25 pub
226 Directory send OK.

ftp> cd pub
250 Directory successfully changed.

ftp> ls
227 Entering Passive Mode (10,129,42,253,182,129).
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            18 Feb 25 19:25 login.txt
226 Directory send OK.

ftp> get login.txt
local: login.txt remote: login.txt
227 Entering Passive Mode (10,129,42,253,181,53).
150 Opening BINARY mode data connection for login.txt (18 bytes).
226 Transfer complete.
18 bytes received in 0.00 secs (165.8314 kB/s)

ftp> exit
221 Goodbye.
```

In the above shell, we see that FTP supports common commands such as `cd` and `ls` and allows us to download files using the `get` command. Inspection of the downloaded `login.txt` reveals credentials that we could use to further our access to the system.

FTP

```
MichaelLuka@htb[/htb]$ cat login.txt

admin:ftp@dmin123
```

SMB

SMB (Server Message Block) is a prevalent protocol on Windows machines that provides many vectors for vertical and lateral movement. Sensitive data, including credentials, can be in network file shares, and some SMB versions may be vulnerable to RCE exploits such as EternalBlue. It is crucial to enumerate this sizeable potential attack surface carefully. `Nmap` has many scripts for enumerating SMB, such as smb-os-discovery.nse, which will interact with the SMB service to extract the reported operating system version.

SMB

```
MichaelLuka@htb[/htb]$ nmap --script smb-os-discovery.nse -p445 10.10.10.40

Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 00:59 GMT
Nmap scan report for doctors.htb (10.10.10.40)
Host is up (0.022s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: CEO-PC
|   NetBIOS computer name: CEO-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2020-12-27T00:59:46+00:00

Nmap done: 1 IP address (1 host up) scanned in 2.71 seconds
```

In this case, the host runs a legacy Windows 7 OS, and we could conduct further enumeration to confirm if it is vulnerable to EternalBlue.

The Metasploit Framework has several modules for EternalBlue that can be used to validate the vulnerability and exploit it, as we will see in a coming section. We can run a scan against our target for this module section to gather information from the SMB service. We can ascertain that the host runs a Linux kernel, Samba version 4.6.2, and the hostname is GS-SVCSCAN.

SMB

```
MichaelLuka@htb[/htb]$ nmap -A -p445 10.129.42.253

Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-25 16:29 EST
Nmap scan report for 10.129.42.253
Host is up (0.11s latency).

PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn Samba smbd 4.6.2
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.32 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

Host script results:
|_nbstat: NetBIOS name: GS-SVCSCAN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-02-25T21:30:06
|_  start_date: N/A

TRACEROUTE (using port 445/tcp)
HOP RTT       ADDRESS
1   111.62 ms 10.10.14.1
2   111.89 ms 10.129.42.253

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.72 seconds
```

Shares

SMB allows users and administrators to share folders and make them accessible remotely by other users. Often these shares have files in them that contain sensitive information such as passwords. A tool that can enumerate and interact with SMB shares is smbclient. The `-L` flag specifies that we want to retrieve a list of available shares on the remote host, while `-N` suppresses the password prompt.

Shares

```
MichaelLuka@htb[/htb]$ smbclient -N -L \\\\10.129.42.253

    Sharename       Type      Comment
    ---------       ----      -------
    print$          Disk      Printer Drivers
    users           Disk
    IPC$            IPC       IPC Service (gs-svcscan server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
```

This reveals the non-default share `users`. Let us attempt to connect as the guest user.

Shares

```
MichaelLuka@htb[/htb]$ smbclient \\\\10.129.42.253\\users

Enter WORKGROUP\users's password:
Try "help" to get a list of possible commands.

smb: \> ls
NT_STATUS_ACCESS_DENIED listing \*

smb: \> exit
```

The `ls` command resulted in an access denied message, indicating that guest access is not permitted. Let us try again using credentials for the user bob (`bob:Welcome1`).

Shares

```
MichaelLuka@htb[/htb]$ smbclient -U bob \\\\10.129.42.253\\users

Enter WORKGROUP\bob's password:
Try "help" to get a list of possible commands.

smb: \> ls
  .                                   D        0  Thu Feb 25 16:42:23 2021
  ..                                  D        0  Thu Feb 25 15:05:31 2021
  bob                                 D        0  Thu Feb 25 16:42:23 2021

        4062912 blocks of size 1024. 1332480 blocks available

smb: \> cd bob

smb: \bob\> ls
  .                                   D        0  Thu Feb 25 16:42:23 2021
  ..                                  D        0  Thu Feb 25 16:42:23 2021
  passwords.txt                       N      156  Thu Feb 25 16:42:23 2021

        4062912 blocks of size 1024. 1332480 blocks available

smb: \bob\> get passwords.txt
getting file \bob\passwords.txt of size 156 as passwords.txt (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
```

We successfully gained access to the `users` share using credentials and gained access to the interesting file `passwords.txt`, which can be downloaded with the `get` command.

SNMP

SNMP Community strings provide information and statistics about a router or device, helping us gain access to it. The manufacturer default community strings of `public` and `private` are often unchanged. In SNMP versions 1 and 2c, access is controlled using a plaintext community string, and if we know the name, we can gain access to it. Encryption and authentication were only added in SNMP version 3.

Much information can be gained from SNMP. Examination of process parameters might reveal credentials passed on the command line, which might be possible to reuse for other externally accessible services given the prevalence of password reuse in enterprise environments. Routing information, services bound to additional interfaces, and the version of installed software can also be revealed.

SNMP

```
MichaelLuka@htb[/htb]$ snmpwalk -v 2c -c public 10.129.42.253 1.3.6.1.2.1.1.5.0

iso.3.6.1.2.1.1.5.0 = STRING: "gs-svcscan"
```

SNMP

```
MichaelLuka@htb[/htb]$ snmpwalk -v 2c -c private  10.129.42.253

Timeout: No Response from 10.129.42.253
```

A tool such as onesixtyone can be used to brute force the community string names using a dictionary file of common community strings such as the `dict.txt` file included in the GitHub repo for the tool.

SNMP

```
MichaelLuka@htb[/htb]$ onesixtyone -c dict.txt 10.129.42.254

Scanning 1 hosts, 51 communities
10.129.42.254 [public] Linux gs-svcscan 5.4.0-66-generic #74-Ubuntu SMP Wed Jan 27 22:54:38 UTC 2021 x86_64
```

Conclusion

Service scanning and enumeration is a vast subject that we will learn more about as we go along. The aspects we have covered here apply to many networks, including HTB machines.

Start Instance

1 / 1 spawns left

Waiting to start...

Questions

Answer the question(s) below to complete this Section and earn cubes!

Cheat Sheet

Get VPN Key

Target: Click here to spawn the target system!

+ 1 Perform an Nmap scan of the target. What is the version of the service that is running on port 8080?

Submit your answer here...

Submit

Hint

+ 0 Perform an Nmap scan of the target and identify the non-default port that the telnet service running on.

Submit your answer here...

Submit

Hint

+ 1 List the SMB shares available on the target host. Connect to the available share as the bob user. Once connected, access the folder called 'flag' and submit the contents of the flag.txt file.

Submit your answer here...

Submit

Hint

Previous Next

Cheat Sheet

Go to Questions

Table of Contents

Introduction

Infosec Overview

Setup

Getting Started with a Pentest Distro

Staying Organized

Connecting Using VPN

Pentesting Basics

Common Terms
Basic Tools
Service Scanning
Web Enumeration
Public Exploits
Types of Shells
Privilege Escalation
Transferring Files

Getting Started with Hack The Box (HTB)

Starting Out
Navigating HTB

Attacking Your First Box

Nibbles - Enumeration
Nibbles - Web Footprinting
Nibbles - Initial Foothold
Nibbles - Privilege Escalation
Nibbles - Alternate User Method - Metasploit

Problem Solving

Common Pitfalls
Getting Help

What's Next?

Next Steps
Knowledge Check

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left