USING NETCAT AND NMAP

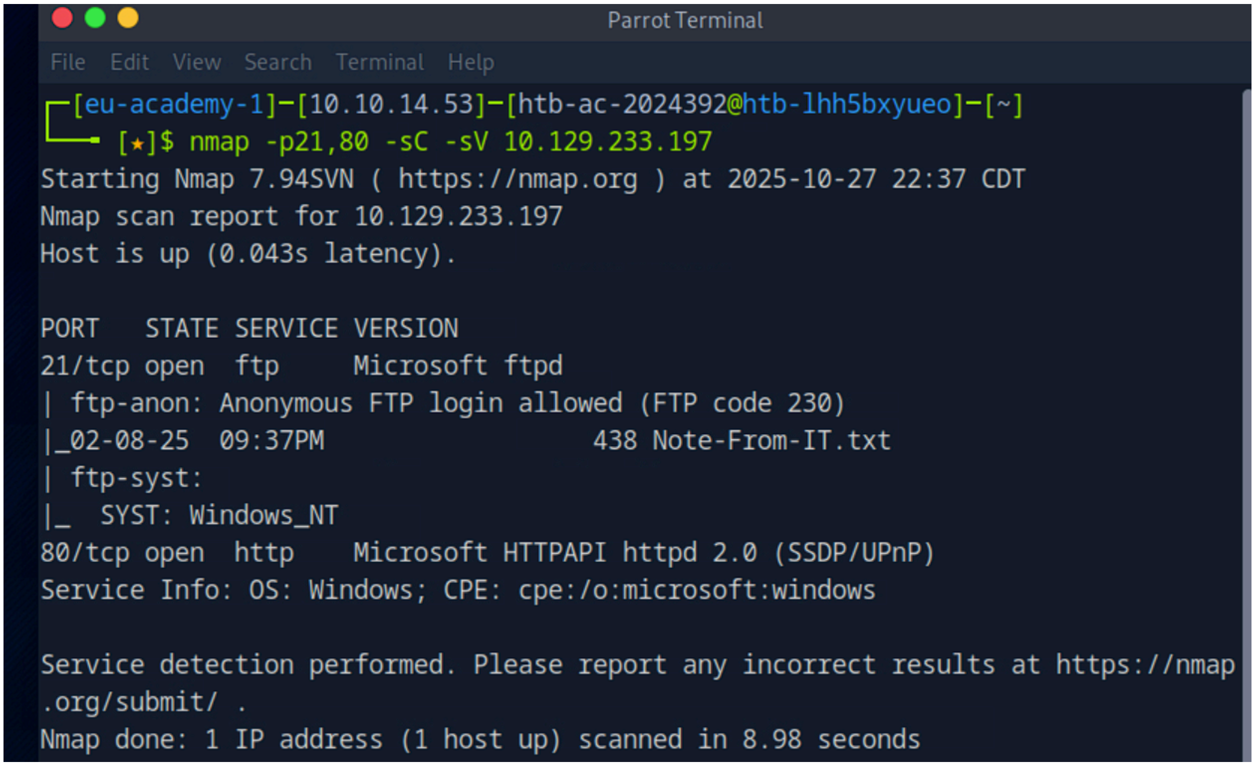
The goal is to target the machine with ip “10.129.233.197”:
I aimed to scan the open ports using “namp” followed by options:

- sV : after nmap discover what ports are open sv option will send “probes” to that port to try and “speak” with the service and by analyzing the response nmap can determine :

1. Name of the service
2. Version of the service
3. Additional info “like what kind of os the service is running on

- sC: is short for “scripts = default - -” nmap has strong script engine “SNE:Nmap Scripting Engine” has hundreds of scripts doing advance tasks and its design in a way to not break the target system , some of the scripts tasks:
    1. Uncover additional information.
    2. Looking for common vulnerabilities.
    3. Collect information about settings.

So after very long introduction here what the command should look like : **nmap -p21,80 -sC -sV 10.129.23.197**



```
┌─[eu-academy-1]─[10.10.14.53]─[htb-ac-2024392@htb-lhh5bxyueo]─[~]
└──╼ [★]$ nmap -p21,80 -sC -sV 10.129.233.197
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-27 22:37 CDT
Nmap scan report for 10.129.233.197
Host is up (0.043s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_02-08-25  09:37PM                  438 Note-From-IT.txt
| ftp-syst:
|_  SYST: Windows_NT
80/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.98 seconds
```

So after the scan we notice that .. hmm port 80   and port 21 and thanks to “sc . sv guys” we see additional information and .. wow anonymous log in is on .. means we can log in easily log in using (User anonymous and pass word anything) as shown in the next screenshot.. but we notice that port 80 doesn't return enough information ?.. what i understand is that some request filtering is applied

The second step is to connect to the ftp using netcat :
nc 10.129.233.197 21

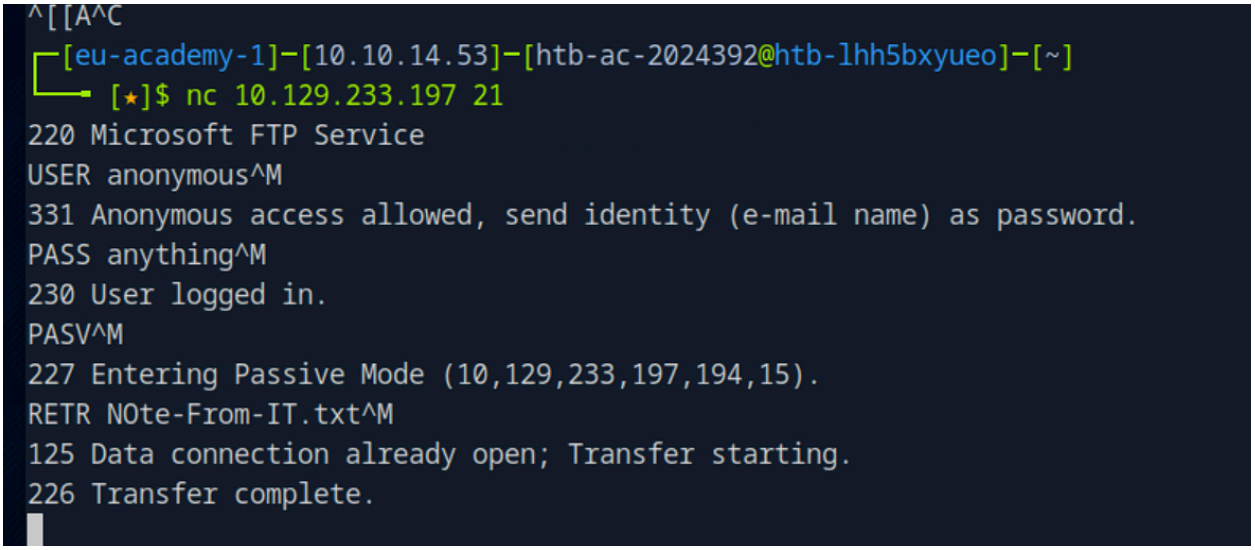
- Notice : during the connection and my attempt to sing in using the anonymous credentials after making a mistake entering the correct credentials could return wrong password even if you enter the right password , after a long search i found that when using netcat to interact with the ftp server netcat does not inherently understand ftp protocol it simply sends raw commands without managing the session state , ftp relies on a strict sequence of commands and respons so when entering incorrect login credentials changes the server session state this means the server may expect a different command or reject the next attempt due to the broken sequence

As a result the correct password might be rejected if its valid because the session has lost protocol synchronization,the proper solution is to terminate the session and reconnect the server in order to reset the command sequence correctly.

The command to the FTB server are:

```
USER anonymous [ctrl v]  [ctrl v] [enter]
PASS anything [ctrl v]  [ctrl v] [enter]
```

When interacting with the FTP server via Netcat commands must be manually formatted . FTP requires eatch command to be terminated with CRLF instead of just LF . USING [ctrl v] [ctrl v] [enter] before pressing enter inserts the required carriage return so the server correctly interprets the command . since netcat does not automatically append CRLF like a real FTP client

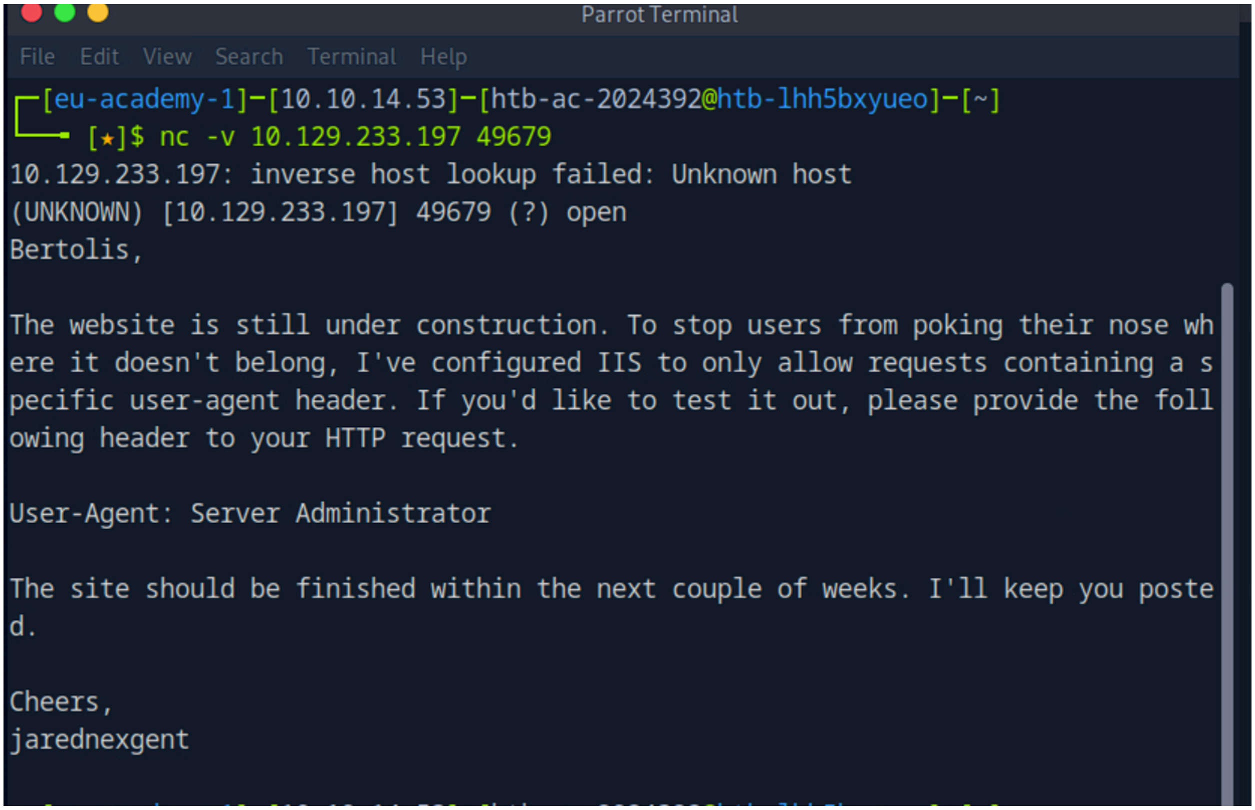


```
^[[A^C
┌─[eu-academy-1]─[10.10.14.53]─[htb-ac-2024392@htb-lhh5bxyueo]─[~]
└──╼ [★]$ nc 10.129.233.197 21
220 Microsoft FTP Service
USER anonymous^M
331 Anonymous access allowed, send identity (e-mail name) as password.
PASS anything^M
230 User logged in.
PASV^M
227 Entering Passive Mode (10,129,233,197,194,15).
RETR NOte-From-IT.txt^M
125 Data connection already open; Transfer starting.
226 Transfer complete.
```

FTP has two channels for its operation :

1. Control channel : to receive commands on port 21
2. Data channel : to sends data work on dynamic ports depending on the mode passive or active

I choose passive mode and made a connection to the data channel using the port control channel sends “last two numbers in the address on the screen shot above” “194,15” due to the limitation of FTP protocol it cannot sends the port number in direct massage because its 16 bit , so FTP returns the port number in two bits each (0-256) and you can calculate the port number (P1*256+P2).
In anew terminal connect to the dynamic port given and restore the file using RETR command :
nc -v 10.129.233.197 dynamic port
RETR Note-From-IT.txt



```
┌─[eu-academy-1]─[10.10.14.53]─[htb-ac-2024392@htb-lhh5bxyueo]─[~]
└──╼ [★]$ nc -v 10.129.233.197 49679
10.129.233.197: inverse host lookup failed: Unknown host
(UNKNOWN) [10.129.233.197] 49679 (?) open
Bertolis,

The website is still under construction. To stop users from poking their nose wh
ere it doesn't belong, I've configured IIS to only allow requests containing a s
pecific user-agent header. If you'd like to test it out, please provide the foll
owing header to your HTTP request.

User-Agent: Server Administrator

The site should be finished within the next couple of weeks. I'll keep you poste
d.

Cheers,
jarednexgent
```

After receiving the file we will be greeted with a massage and it seams if we want to access the page we have to send a HTTP request and on its header : User-Agent=Server administrator

So we go back and use necat to staples a port 80 connection : **nc-v 10.129.233.197 80**

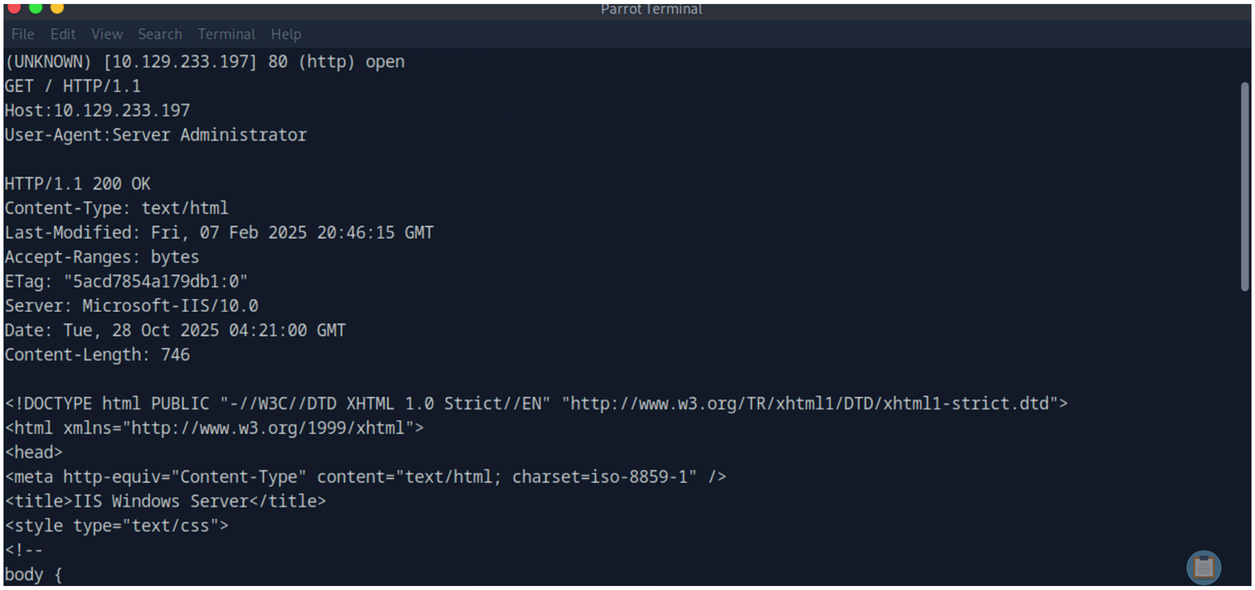
And enter the commands :

Get /HTTP/1.1

Host:10.129.233.197

User-Agent: Server administrator

And the flag will be in the end of the html response



```
(UNKNOWN) [10.129.233.197] 80 (http) open
GET / HTTP/1.1
Host:10.129.233.197
User-Agent:Server Administrator

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Fri, 07 Feb 2025 20:46:15 GMT
Accept-Ranges: bytes
ETag: "5acd7854a179db1:0"
Server: Microsoft-IIS/10.0
Date: Tue, 28 Oct 2025 04:21:00 GMT
Content-Length: 746

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
```