Nmap

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

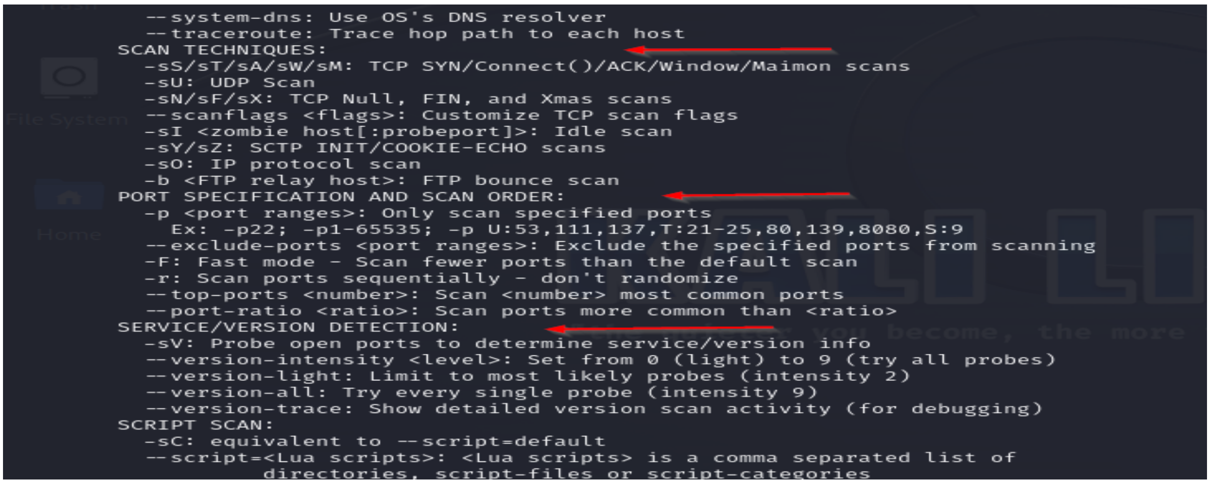
Task 2: Introduction

Nmap is used for active reconnaissance and enumeration. Enumeration involves extracting information from a target system or network and comes after reconnaissance.

Question	Answer
What networking constructs are used to direct traffic to the right application on a server?	ports
How many of these are available on any network-enabled computer?	65535
[Research] How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)	1024

Task 3: Nmap Switches

- To find answers to the questions in this task, refer to the Nmap manual page by using the command "**man nmap."**



```
    --system-dns: Use OS's DNS resolver
    --traceroute: Trace hop path to each host
  SCAN TECHNIQUES:
    -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
    -sU: UDP Scan
    -sN/sF/sX: TCP Null, FIN, and Xmas scans
    --scanflags <flags>: Customize TCP scan flags
    -sI <zombie host[:probeport]>: Idle scan
    -sY/sZ: SCTP INIT/COOKIE-ECHO scans
    -sO: IP protocol scan
    -b <FTP relay host>: FTP bounce scan
  PORT SPECIFICATION AND SCAN ORDER:
    -p <port ranges>: Only scan specified ports
      Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
    --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>
  SERVICE/VERSION DETECTION:
    -sV: Probe open ports to determine service/version info
    --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)
  SCRIPT SCAN:
    -sC: equivalent to --script=default
    --script=<Lua scripts>: <Lua scripts> is a comma separated list of
             directories, script-files or script-categories
```

Question	Answer
What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?	-sS
Which switch would you use for a "UDP scan"?	-sU
If you wanted to detect which operating system the target is running on, which switch would you use?	-O
Nmap provides a switch to detect the version of the services running on the target. What is this switch?	-sV

The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?	-V
Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two? (**Note**: it's highly advisable to always use *at least* this option)	-VV
We should always save the output of our scans -- this means that we only need to run the scan once (reducing network traffic and thus chance of detection), and gives us a reference to use when writing reports for clients.What switch would you use to save the nmap results in three major formats?	-oA
What switch would you use to save the nmap results in a "normal" format?	-oN
A very useful output format: how would you save results in a "grepable" format?	-oG
Sometimes the results we're getting just aren't enough. If we don't care about how loud we are, we can enable "aggressive" mode. This is a shorthand switch that activates service detection, operating system detection, a traceroute and common script scanning. How would you activate this setting?	-A
Nmap offers five levels of "timing" template. These are essentially used to increase the speed your scan runs at. Be careful though: higher speeds are noisier, and can incur errors! How would you set the timing template to level 5?	-T5
We can also choose which port(s) to scan. How would you tell nmap to only scan port 80?	
How would you tell nmap to scan ports 1000-1500?	-P 1000-1500
A very useful option that should not be ignored: How would you tell nmap to scan *all* ports?	-p-
How would you activate a script from the nmap scripting library (lots more on this later!)?	--script
How would you activate all of the scripts in the "vuln" category?	--script=vuln

Task 5: Scan Types TCP Connect Scans

- The syntax is: **nmap -sT [target]**
- TCP Connect scan involves a three-way handshake with each target port to determine if a service is open or closed.
- An "open" port has the "SYN/ACK" flag set in the response, indicating it is accepting connections.

- A "closed" port has the "RST" (reset) flag set in the response, while a "filtered" port doesn't yield any response and is often due to firewall blocking.

Question	Answer
Which RFC defines the appropriate behaviour for the TCP protocol?	RFC 9293
If a port is closed, which flag should the server send back to indicate this?	RST

Task 6: Scan Types SYN Scans

- SYN scan (-sS) syntax is "**nmap -sS <target>**" and aims to scan TCP ports. It takes longer time to show result
- Unlike full three-way handshake TCP scans, SYN scans send an RST TCP packet after receiving a SYN/ACK from the server.

Question	Answer
There are two other names for a SYN scan, what are they?	half-open, stealth
Can Nmap use a SYN scan without Sudo permissions (Y/N)?	N

Task 7: Scan Types UDP Scans

- The Syntax is **nmap -sU [target]** and this scan takes a longer time to show the results
- An open UDP port is indicated when Nmap receives a response from the port
- A closed UDP port is identified when Nmap receives an ICMP "Port Unreachable" message in response to its probe.
- If Nmap doesn't receive any response, including an ICMP "Port Unreachable" message, it typically categorizes the UDP port as filtered. This suggests the presence of a firewall or network filtering that obstructs Nmap from determining the port's state.

Question	Answer
If a UDP port doesn't respond to an Nmap scan, what will it be marked as?	open|filtered
When a UDP port is closed, by convention the target should send back a "port unreachable" message. Which protocol would it use to do so?	ICMP

Task 8: Scan Types NULL, FIN, and Xmas

- Null: -sN, FIN: -sF, Xmas: -sX

Question	Answer
Which of the three shown scan types uses the URG flag?	Xmas
Why are NULL, FIN and Xmas scans generally used?	firewall evasions
Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?	Microsoft windows

Task 9: Scan Types ICMP Network Scanning(-sn)

- To map a network structure, first conduct a "ping sweep" using Nmap, where Nmap sends ICMP packets to all possible IP addresses in the network. IP addresses that respond to the ICMP request are marked as active hosts.

Question	Answer
How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)	nmap -sn 172.16.0.0/16

Task 10: NSE Scripts Overview

- The **N**map **S**cripting **E**ngine (NSE) is used to extend Nmap's functionality
- An extensive list of the categories can be found on Nmap's official website: here

Question	Answer
What language are NSE scripts written in?	Lua
Which category of scripts would be a *very* bad idea to run in a production environment?	Intrusive

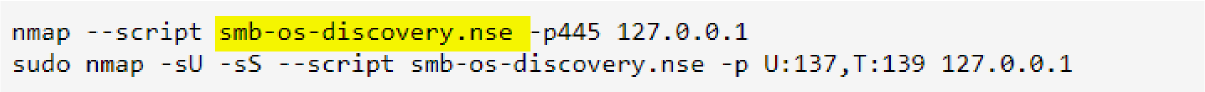
Task 11: NSE Scripts Working with the NSE

- Syntax to run a specific script is **--script=<script-name>**
- Multiple scripts can be run simultaneously e.g **nmap --script=vuln,exploit,auth <target>**
- Some scripts require arguments using **--script-args** Nmap switch
- An extensive list of the scripts and their arguments can be found here, this will help to answer the question in the task

Question	Answer
What optional argument can the ftp-anon.nse script take?	maxlist

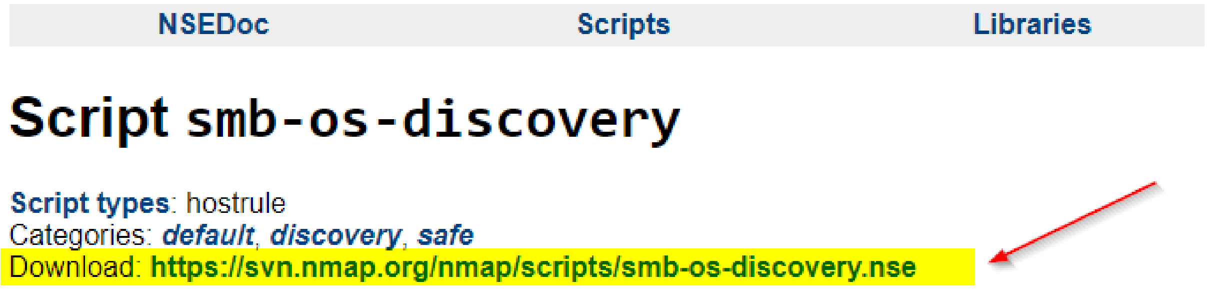
Task 12: NSE Scripts Searching for Scripts

- To *find* these scripts, you either go to the Nmap website or go to your Linux at /usr/share/nmap/scripts.
- To answer the question in the task, you can use either of the two methods, the screenshot will show the first method, which is making use of the official website



```
nmap --script smb-os-discovery.nse -p445 127.0.0.1
sudo nmap -sU -sS --script smb-os-discovery.nse -p U:137,T:139 127.0.0.1
```

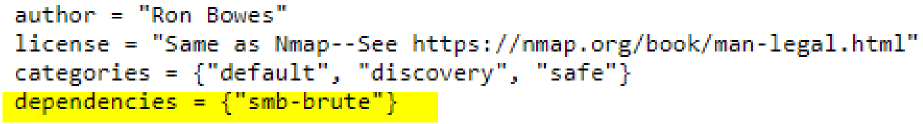
- The get the second question, go to the link in the download section, this will take you directly to the script



Script smb-os-discovery

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

- Then find the dependencies



```
author = "Ron Bowes"
license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
categories = {"default", "discovery", "safe"}
dependencies = {"smb-brute"}
```

Question	Answer
Search for "smb" scripts in the /usr/share/nmap/scripts/ directory using either of the demonstrated methods. What is the filename of the script which determines the underlying OS of the SMB server?	smb-os-discovery.nse
Read through this script. What does it depend on	smb-brute

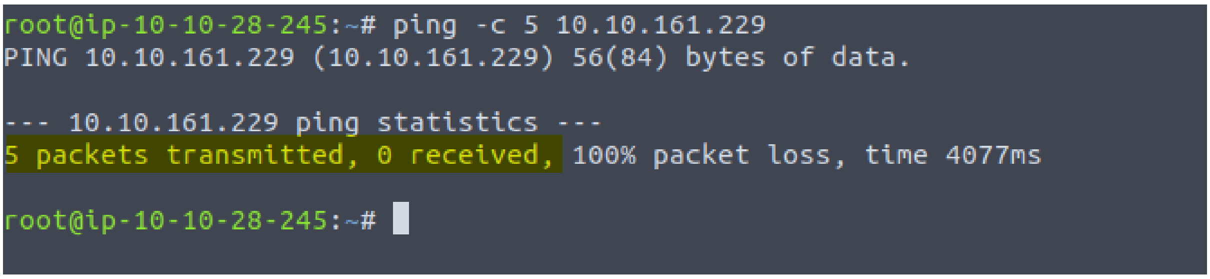
Task 13: Firewall Evasion

- Windows hosts with default firewalls often block ICMP packets, causing Nmap to register them as inactive.
- To bypass this issue, Nmap offers the -Pn option, which skips pinging the host before scanning, treating it as alive

Question	**Answer**
Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the `-Pn` switch?	ICMP
[Research] Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?	--data-length

Task 14: Practical

- To answer the first question, the command is **ping -c 5 <target>**, you can use any number of the count, it doesn't have to be 5, since 0 packets were received, it means the target did not respond to the ICMP request

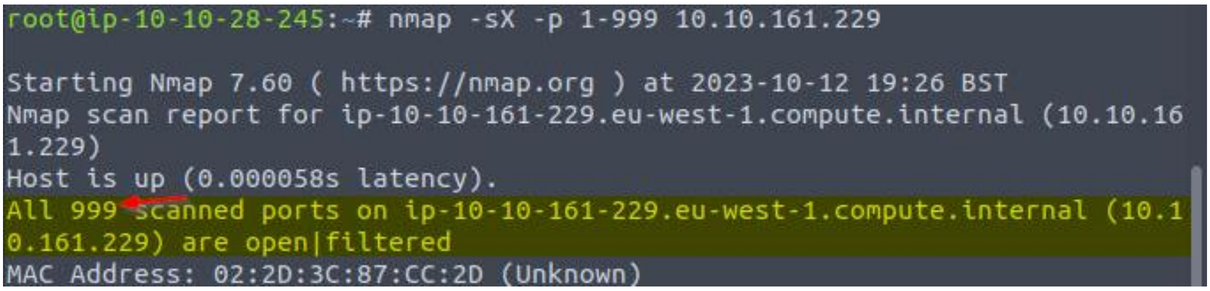


```
root@ip-10-10-28-245:~# ping -c 5 10.10.161.229
PING 10.10.161.229 (10.10.161.229) 56(84) bytes of data.

--- 10.10.161.229 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4077ms

root@ip-10-10-28-245:~#
```

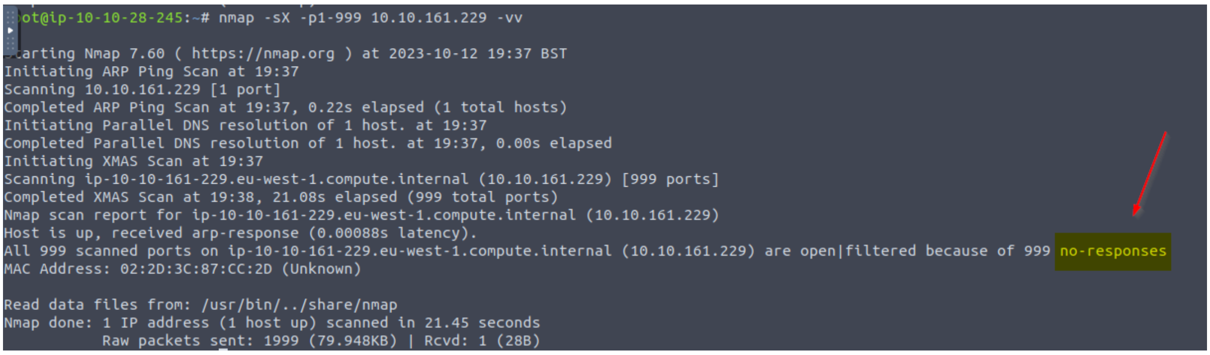
- To answer the second question, use the command **nmap -Sx -P 1-999 <target>**



```
root@ip-10-10-28-245:~# nmap -sX -p 1-999 10.10.161.229

Starting Nmap 7.60 ( https://nmap.org ) at 2023-10-12 19:26 BST
Nmap scan report for ip-10-10-161-229.eu-west-1.compute.internal (10.10.16
1.229)
Host is up (0.000058s latency).
All 999 scanned ports on ip-10-10-161-229.eu-west-1.compute.internal (10.1
0.161.229) are open|filtered
MAC Address: 02:2D:3C:87:CC:2D (Unknown)
```

- Add -vv to increase verbosity of the scan, you will see the reason

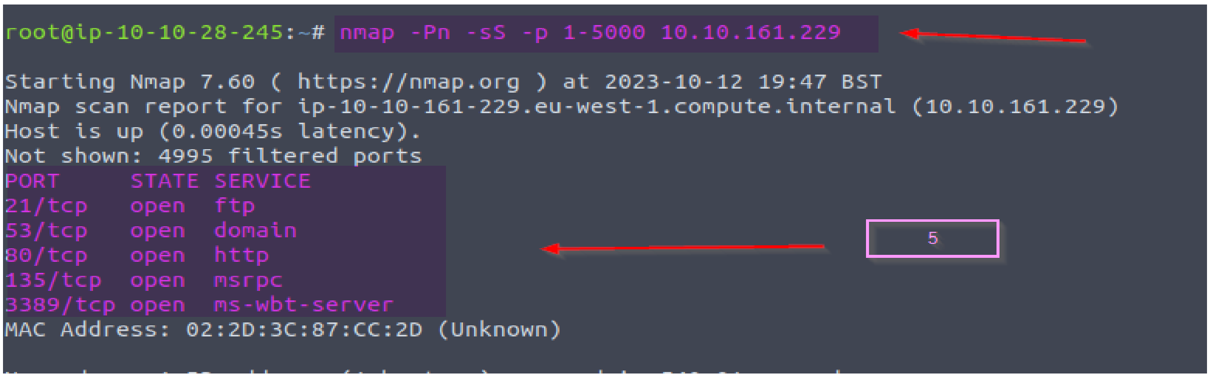


```
ot@ip-10-10-28-245:~# nmap -sX -p1-999 10.10.161.229 -vv

arting Nmap 7.60 ( https://nmap.org ) at 2023-10-12 19:37 BST
Initiating ARP Ping Scan at 19:37
Scanning 10.10.161.229 [1 port]
Completed ARP Ping Scan at 19:37, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:37
Completed Parallel DNS resolution of 1 host. at 19:37, 0.00s elapsed
Initiating XMAS Scan at 19:37
Scanning ip-10-10-161-229.eu-west-1.compute.internal (10.10.161.229) [999 ports]
Completed XMAS Scan at 19:38, 21.08s elapsed (999 total ports)
Nmap scan report for ip-10-10-161-229.eu-west-1.compute.internal (10.10.161.229)
Host is up, received arp-response (0.00088s latency).
All 999 scanned ports on ip-10-10-161-229.eu-west-1.compute.internal (10.10.161.229) are open|filtered because of 999 no-responses
MAC Address: 02:2D:3C:87:CC:2D (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.45 seconds
           Raw packets sent: 1999 (79.948KB) | Rcvd: 1 (28B)
```

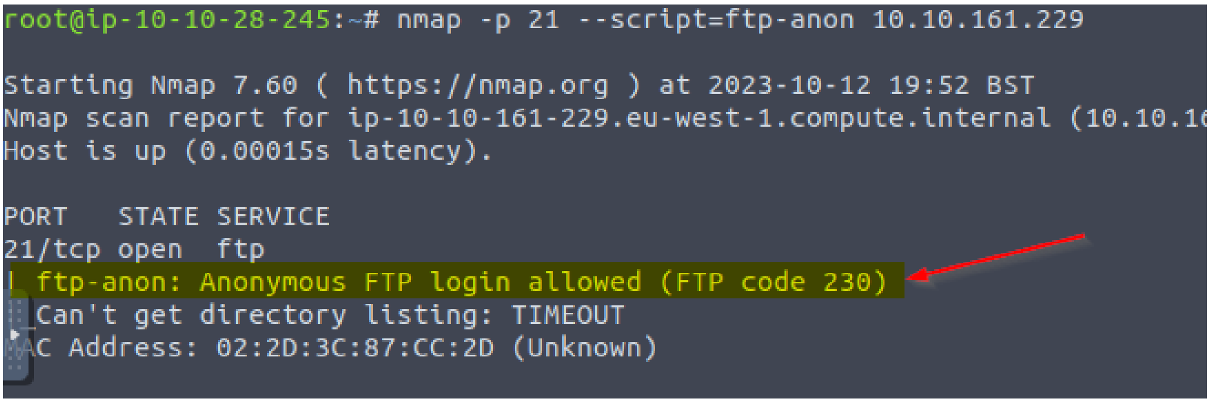
- Use the command **nmap -Pn -sS -p 1-5000 <target>**



```
root@ip-10-10-28-245:~# nmap -Pn -sS -p 1-5000 10.10.161.229

Starting Nmap 7.60 ( https://nmap.org ) at 2023-10-12 19:47 BST
Nmap scan report for ip-10-10-161-229.eu-west-1.compute.internal (10.10.161.229)
Host is up (0.00045s latency).
Not shown: 4995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server
MAC Address: 02:2D:3C:87:CC:2D (Unknown)
```

- Syntax to answer the last question**: nmap -p 21 –script=ftp-anon <target>**

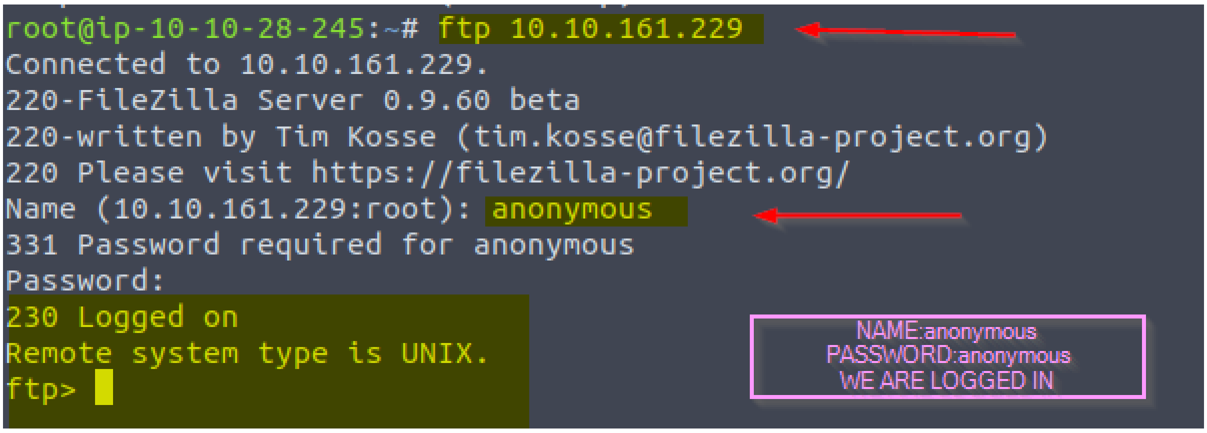


```
root@ip-10-10-28-245:~# nmap -p 21 --script=ftp-anon 10.10.161.229

Starting Nmap 7.60 ( https://nmap.org ) at 2023-10-12 19:52 BST
Nmap scan report for ip-10-10-161-229.eu-west-1.compute.internal (10.10.16
Host is up (0.00015s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
MAC Address: 02:2D:3C:87:CC:2D (Unknown)
```

- **OPTIONAL:** let's test to see if we can log in successfully



```
root@ip-10-10-28-245:~# ftp 10.10.161.229
Connected to 10.10.161.229.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
Name (10.10.161.229:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp>
```

NAME:anonymous
PASSWORD:anonymous
WE ARE LOGGED IN

END.