```
Target: FAWN box
```

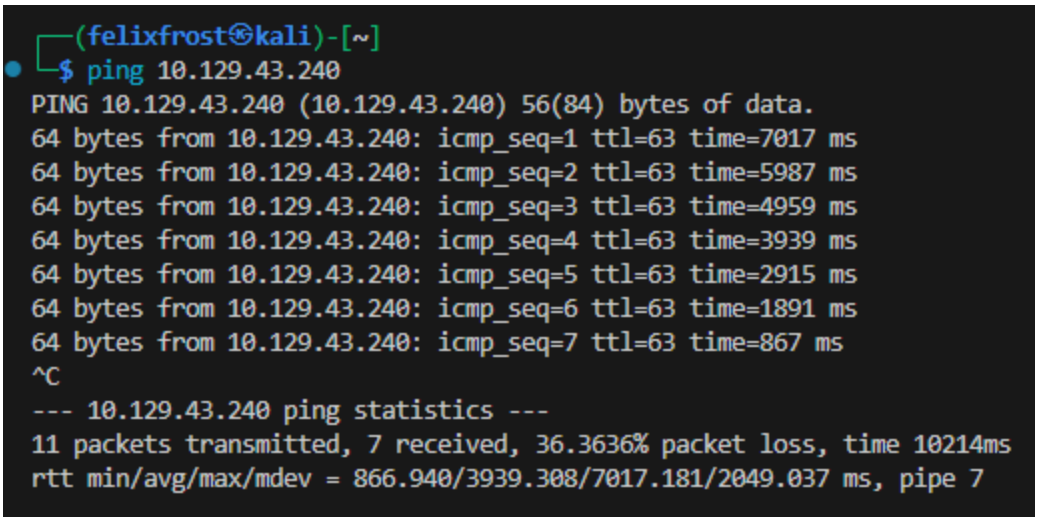
IP: 10.129.43.240
OS: Linux

1. Executive summary

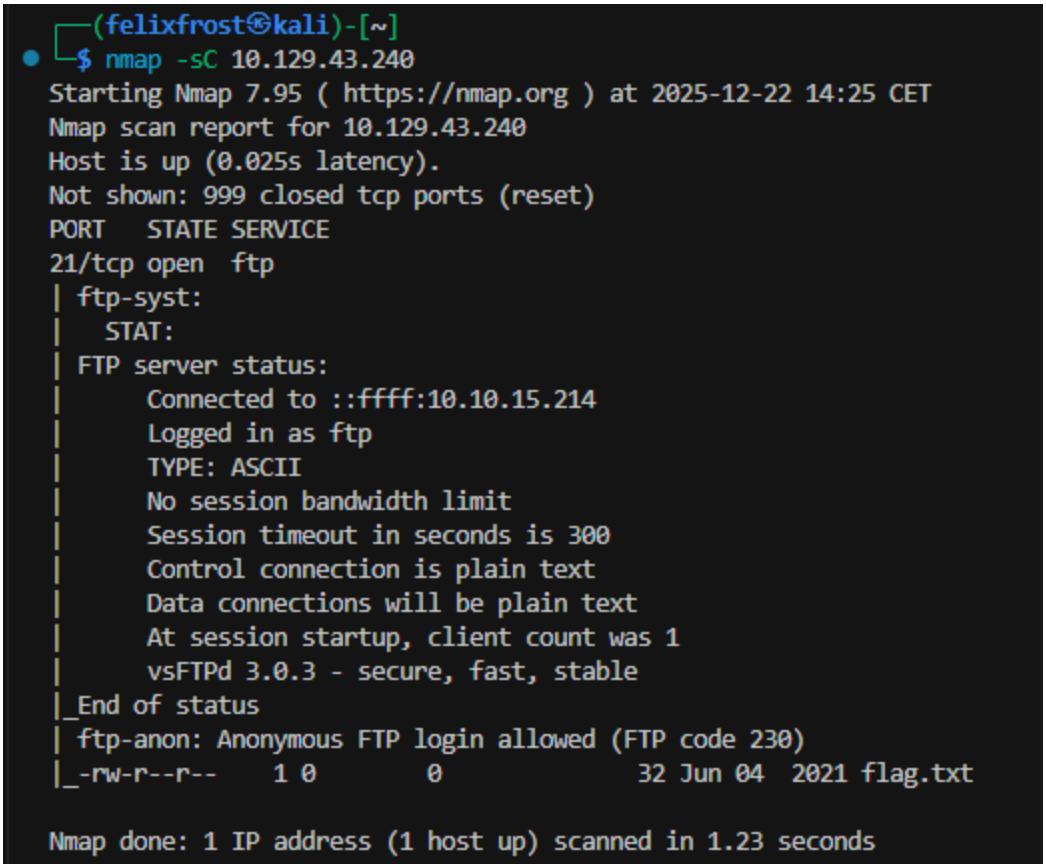
A misconfiguration was identified in the target infrastructure related to a file sharing service. The system is misconfigured to accept connections as the anonymous user which lacks authentication. This allows any attacker on the local network to gain access to files on the server without having to authenticate.

1. Enumeration

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



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

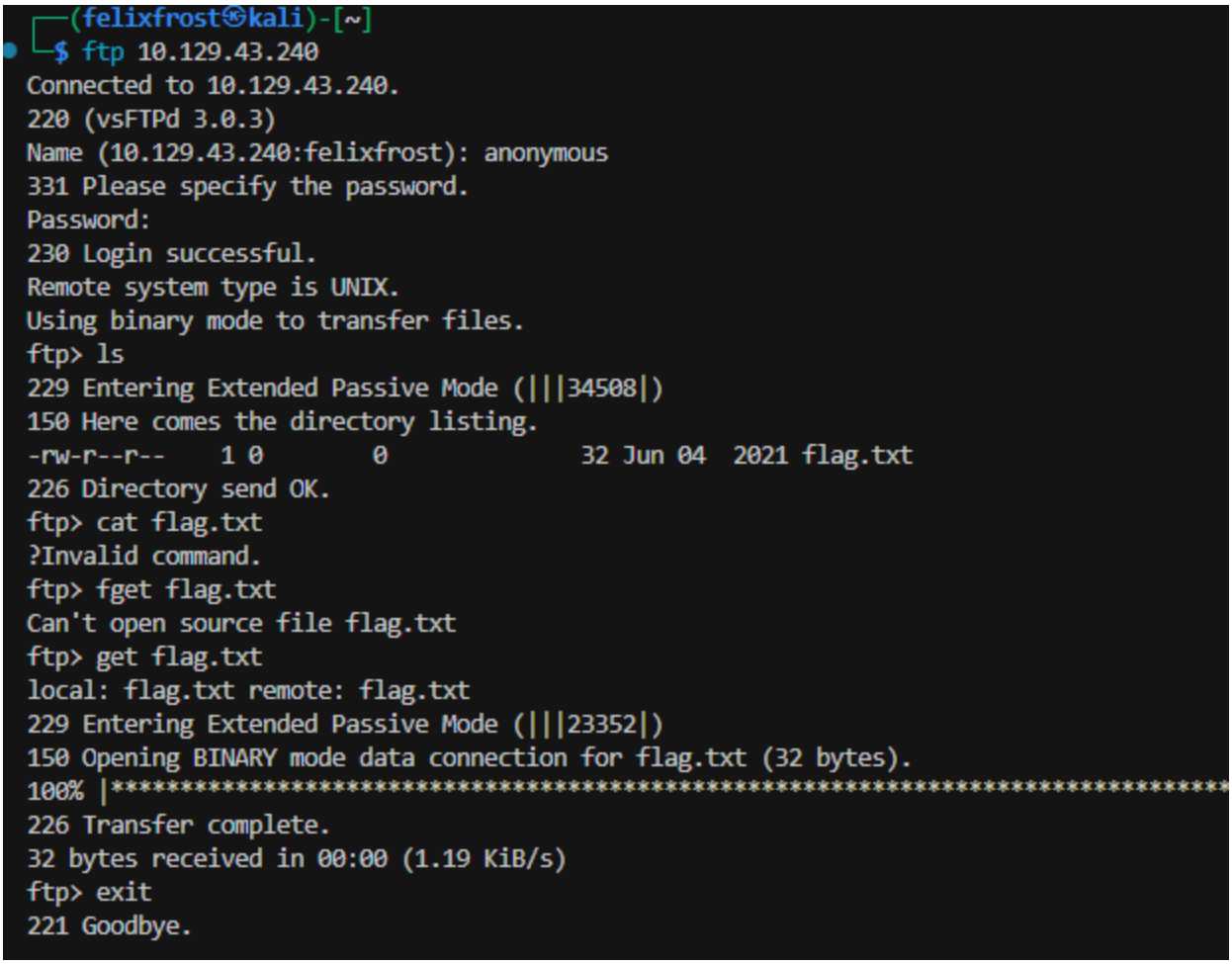


2. Exploitation

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.



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