

IT Security Incident Reporting Form

Instructions: For you to re-coop some of your compromised points, please submit this per incident.

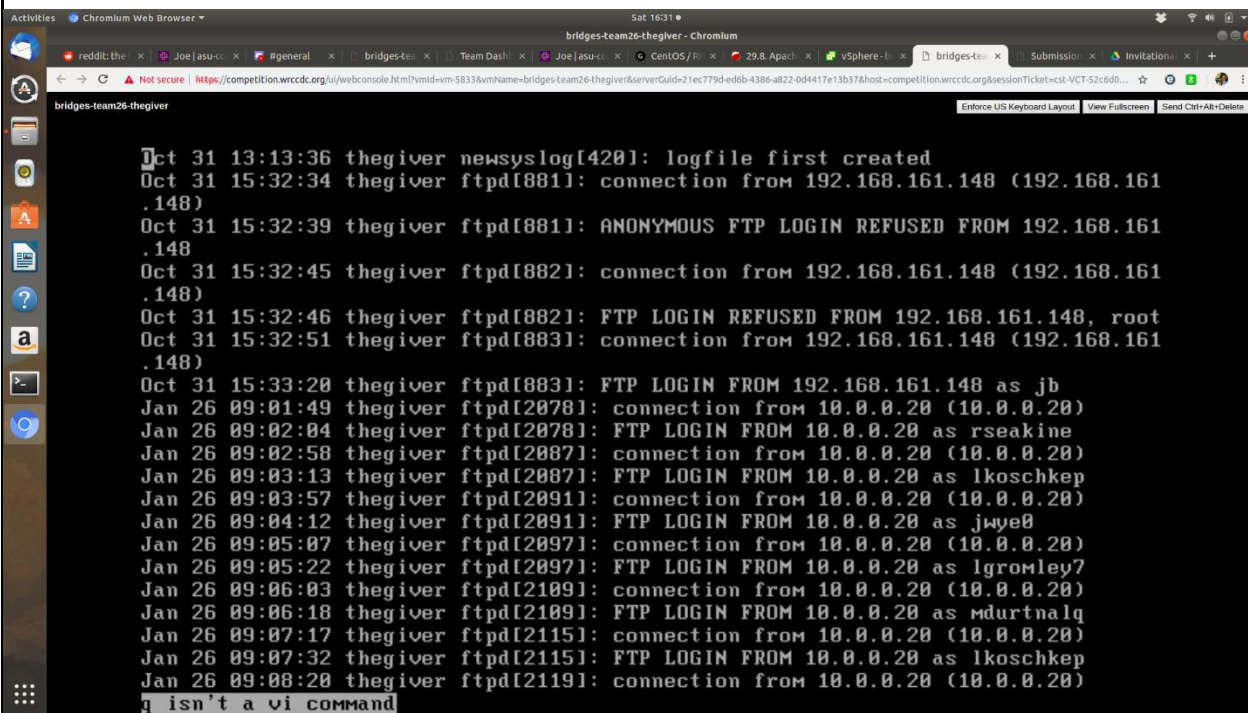
1. Contact Information for this Incident

TEAM #: 26

2. Incident Description.

Provide a brief description of the Incident:

Anonymous ftp login blocked



The screenshot shows a terminal window titled 'bridges-team26-thegiver - Chromium'. The terminal displays a series of system logs and FTP connection attempts. The logs show that an anonymous FTP login was refused from IP 192.168.161.148. Subsequent logs show successful FTP logins from IP 10.0.0.20 as various users, including 'jb', 'rseakine', 'lkschkep', 'jwye0', 'lgromley7', 'mdurtnalq', and 'lkschkep'. The terminal also shows a prompt 'q isn't a vi command'.

```
Oct 31 13:13:36 thegiver newsyslog[420]: logfile first created
Oct 31 15:32:34 thegiver ftpd[881]: connection from 192.168.161.148 (192.168.161.148)
Oct 31 15:32:39 thegiver ftpd[881]: ANONYMOUS FTP LOGIN REFUSED FROM 192.168.161.148
Oct 31 15:32:45 thegiver ftpd[882]: connection from 192.168.161.148 (192.168.161.148)
Oct 31 15:32:46 thegiver ftpd[882]: FTP LOGIN REFUSED FROM 192.168.161.148, root
Oct 31 15:32:51 thegiver ftpd[883]: connection from 192.168.161.148 (192.168.161.148)
Oct 31 15:33:20 thegiver ftpd[883]: FTP LOGIN FROM 192.168.161.148 as jb
Jan 26 09:01:49 thegiver ftpd[2078]: connection from 10.0.0.20 (10.0.0.20)
Jan 26 09:02:04 thegiver ftpd[2078]: FTP LOGIN FROM 10.0.0.20 as rseakine
Jan 26 09:02:58 thegiver ftpd[2087]: connection from 10.0.0.20 (10.0.0.20)
Jan 26 09:03:13 thegiver ftpd[2087]: FTP LOGIN FROM 10.0.0.20 as lkschkep
Jan 26 09:03:57 thegiver ftpd[2091]: connection from 10.0.0.20 (10.0.0.20)
Jan 26 09:04:12 thegiver ftpd[2091]: FTP LOGIN FROM 10.0.0.20 as jwye0
Jan 26 09:05:07 thegiver ftpd[2097]: connection from 10.0.0.20 (10.0.0.20)
Jan 26 09:05:22 thegiver ftpd[2097]: FTP LOGIN FROM 10.0.0.20 as lgromley7
Jan 26 09:06:03 thegiver ftpd[2109]: connection from 10.0.0.20 (10.0.0.20)
Jan 26 09:06:18 thegiver ftpd[2109]: FTP LOGIN FROM 10.0.0.20 as mdurtnalq
Jan 26 09:07:17 thegiver ftpd[2115]: connection from 10.0.0.20 (10.0.0.20)
Jan 26 09:07:32 thegiver ftpd[2115]: FTP LOGIN FROM 10.0.0.20 as lkschkep
Jan 26 09:08:20 thegiver ftpd[2119]: connection from 10.0.0.20 (10.0.0.20)
q isn't a vi command
```

3. Information: Check & Fill In all of the following that apply to this incident.

c Loss / Compromise of Data:____None_____
c Damage to Systems: ____None_____
c System or Service Affected:____FTP_____
c IP Address:____198.168.220.40_____
c System Name:_Thegiver_____

Provide a brief description:

Unauthorized user attempted to enter machine through FTP.

6. What Steps Have Been Taken So Far? Check all of the following that apply to this incident.

c No action taken	c Restored backup from tape
c System Disconnected from network	c Log files examined (saved & secured)
c Updated virus definitions & scanned system	c Other – please describe:

Provide a brief description:

We disabled unauthorized login.

Please submit this completed form to: whiteteam@wrccdc.org