The People's Government of Pangea

Department of Information Technology

Cyber Operations Team

Intrusion Report

Looking at the Snort logs, Red Team has been attacking our web (10.0.150.70) and mail (10.0.150.60) servers mostly. They tried uploading a script to our web server and running it (script.txt):

```
root@www:/IT# ls
descript.ion  script.txt  test.txt
root@www:/IT# cat script.txt
test fileroot@www:/IT# ls Oal
ls: cannot access Oal: No such file or directory
root@www:/IT# ls -al
total 16
drwxrwsr-x  2 root     www-data 4096 Apr  1 09:38 .
drwxr-xr-x 24 root     root     4096 Mar 31 17:39 ..
-rw-r--r--  1 www-data www-data   48 Apr  1 09:38 descript.ion
-rw-r--r--  1 www-data www-data    9 Apr  1 09:38 script.txt
-rw-r--r--  1 www-data www-data    0 Apr  1 09:17 test.txt
root@www:/IT# rm test.txt
root@www:/IT# rm script.txt
root@www:/IT# ls
descript.ion
root@www:/IT# cd
root@www:~#
```

The attackers are coming from the 10.10.20.0/24 subnet.