

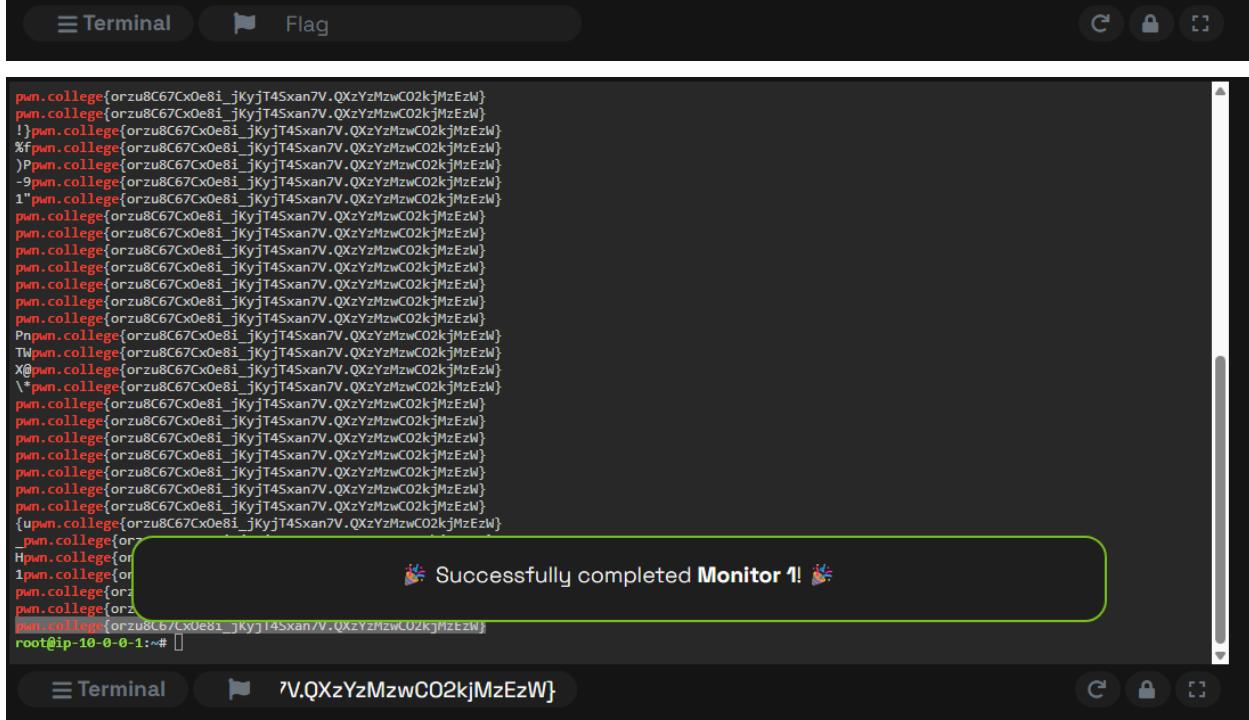
Jaleel Williamson

jayw-713

CSCI 400 Lab 12

10/15/25

- Monitor 1

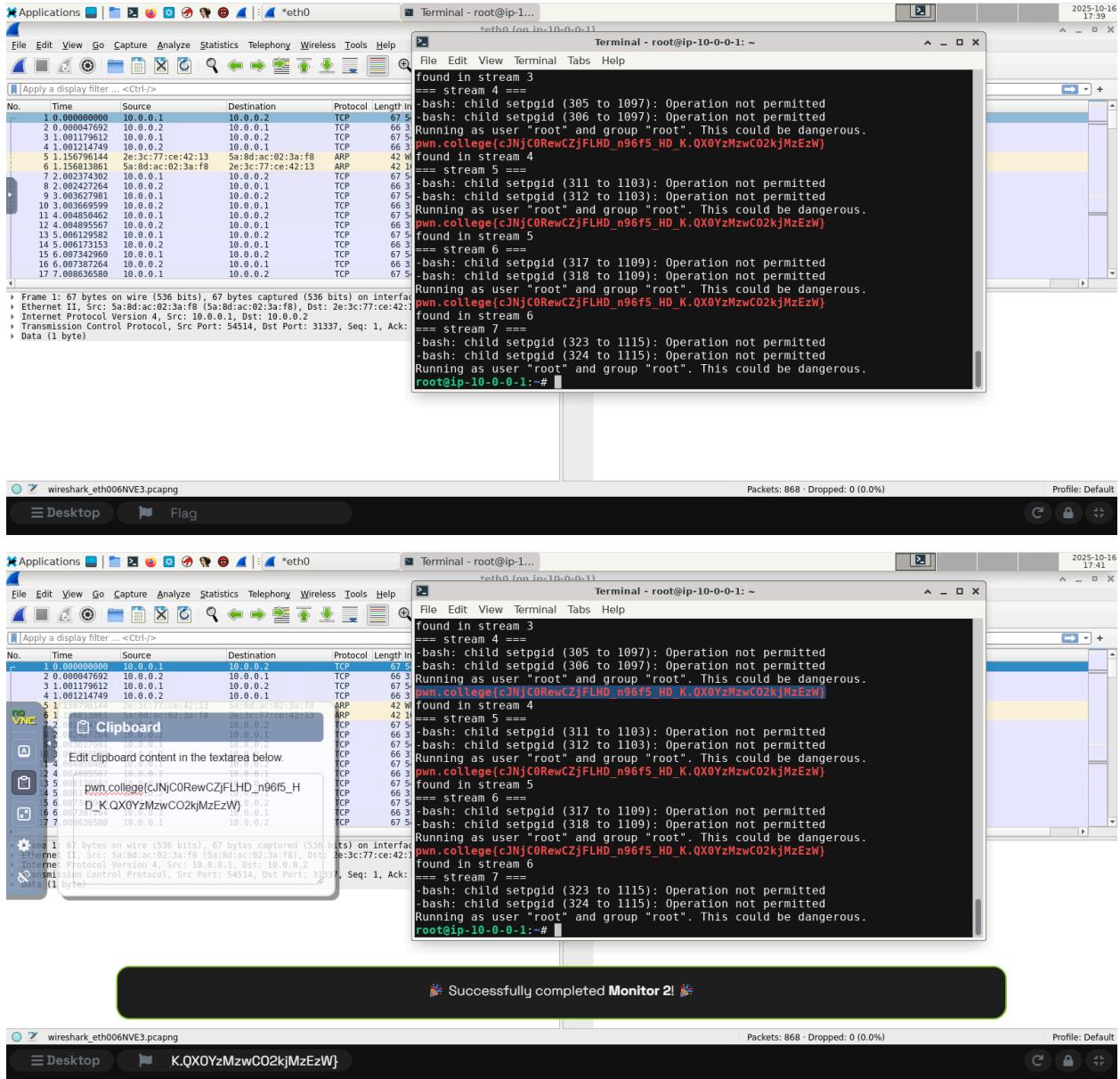


● Monitor 2

The screenshot shows two windows side-by-side. The left window is Wireshark displaying network traffic on interface eth0. A display filter is applied: `[tcp.port == 31337]`. The list of captured frames shows multiple TCP connections between 10.0.0.1 and 10.0.0.2. Frame 1 is selected, showing its details and bytes panes. The details pane shows a PSH ACK segment with sequence number 1 and acknowledgement number 2. The bytes pane shows the raw hex and ASCII data, including the string "z 9". The right window is a terminal window titled "Terminal - root@ip-10-0-0-1" running the command `*eth0 (tcp port 31337) (on ip-10-0-0-1)`. A search bar at the top contains the string "pwn{". The terminal output shows several captured frames, with frame 1 selected. The details pane shows a PSH ACK segment with sequence number 1 and acknowledgement number 2. The bytes pane shows the raw hex and ASCII data, including the string "z 9".

I couldn't retrieve the flag.

2nd Attempt



Successful capture of monitor 2

- Firewall 1

```
hacker@intercepting-communication-firewall-1:~$ /challenge/run
root@ip-10-0-0-1:~# iptables -I INPUT -p tcp --dport 31337 -j DROP
iptables -I INPUT -p udp --dport 31337 -j DROP
root@ip-10-0-0-1:~# pwn.college{QpNvLtvQ40CP5u100fnC8B0R6Cd.0F00A{jNxwCO2kjMzEzW}}
```

The terminal window shows the command `/challenge/run` being executed, followed by the configuration of iptables rules to drop traffic on ports 31337 for both TCP and UDP. The final command `pwn.college{QpNvLtvQ40CP5u100fnC8B0R6Cd.0F00A{jNxwCO2kjMzEzW}}` is run to complete the challenge.

```
hacker@intercepting-communication-firewall-1:~$ /challenge/run
root@ip-10-0-0-1:~# iptables -I INPUT -p tcp --dport 31337 -j DROP
iptables -I INPUT -p udp --dport 31337 -j DROP
root@ip-10-0-0-1:~# pwn.college{QpNvLtvQ40CP5u100fnC8B0R6Cd.0F00A{jNxwCO2kjMzEzW}}
```

The terminal window shows the same sequence of commands as the previous screenshot. A green rounded rectangle highlights a message at the bottom: "Successfully completed Firewall 1! 🎉".

- Firewall 2

```
hacker@intercepting-communication:firewall-2:~$ /challenge/run
root@ip-10-0-0-1:~# iptables -I INPUT 1 -p tcp -s 10.0.0.2 --dport 31337 -j ACCEPT
iptables -I INPUT 2 -p tcp -s 10.0.0.3 --dport 31337 -j DROP
root@ip-10-0-0-1:~# pwn.college{o_DVZOL6lb8xWAXzeAD6UhBzg3J.0VO0AjNzwC02kjMzEzW}
```

```
hacker@intercepting-communication:firewall-2:~$ /challenge/run
root@ip-10-0-0-1:~# iptables -I INPUT 1 -p tcp -s 10.0.0.2 --dport 31337 -j ACCEPT
iptables -I INPUT 2 -p tcp -s 10.0.0.3 --dport 31337 -j DROP
root@ip-10-0-0-1:~# pwn.college{o_DVZOL6lb8xWAXzeAD6UhBzg3J.0VO0AjNzwC02kjMzEzW}
```

🎉 Successfully completed Firewall 2! 🎉

- Firewall 3

```
hacker@intercepting-communication~firewall-3:~$ /challenge/run
root@ip-10-0-0-1:~# iptables -I OUTPUT 1 -p tcp -d 10.0.0.2 --dport 31337 -j ACCEPT iptables -L OUTPUT -n --line-numbers | grep 31337 || iptables
-S | grep 31337
-bash: child setpgid (11 to 169): Operation not permitted
Bad argument 'iptables'
Try 'iptables -h' or 'iptables --help' for more information.
-bash: child setpgid (13 to 171): Operation not permitted
-A OUTPUT -p tcp -m tcp --dport 31337 -j DROP
root@ip-10-0-0-1:~# iptables -I OUTPUT 1 -p tcp -d 10.0.0.2 --dport 31337 -j ACCEPT
iptables -L OUTPUT -n --line-numbers | grep 31337 || iptables -S | grep 31337
-bash: child setpgid (16 to 174): Operation not permitted
1   ACCEPT    tcp  --  0.0.0.0/0          10.0.0.2        tcp dpt:31337
2   DROP      tcp  --  0.0.0.0/0          0.0.0.0/0        tcp dpt:31337
root@ip-10-0-0-1:~# iptables -L OUTPUT -n --line-numbers
Chain OUTPUT (policy ACCEPT)
num  target     prot opt source          destination
1    ACCEPT    tcp  --  0.0.0.0/0          10.0.0.2        tcp dpt:31337
2    DROP      tcp  --  0.0.0.0/0          0.0.0.0/0        tcp dpt:31337
root@ip-10-0-0-1:~# nc -v 10.0.0.2 31337
Connection to 10.0.0.2 31337 port [tcp/*] succeeded!
pwn.college{8nrS2l04QyAuHT4Cm3VwAeqyzF.0FM1AjNzwCO2kjMzEzW}
```

Terminal

Flag



```
hacker@intercepting-communication~firewall-3:~$ /challenge/run
root@ip-10-0-0-1:~# iptables -I OUTPUT 1 -p tcp -d 10.0.0.2 --dport 31337 -j ACCEPT iptables -L OUTPUT -n --line-numbers | grep 31337 || iptables
-S | grep 31337
-bash: child setpgid (11 to 169): Operation not permitted
Bad argument 'iptables'
Try 'iptables -h' or 'iptables --help' for more information.
-bash: child setpgid (13 to 171): Operation not permitted
-A OUTPUT -p tcp -m tcp --dport 31337 -j DROP
root@ip-10-0-0-1:~# iptables -I OUTPUT 1 -p tcp -d 10.0.0.2 --dport 31337 -j ACCEPT
iptables -L OUTPUT -n --line-numbers | grep 31337 || iptables -S | grep 31337
-bash: child setpgid (16 to 174): Operation not permitted
1   ACCEPT    tcp  --  0.0.0.0/0          10.0.0.2        tcp dpt:31337
2   DROP      tcp  --  0.0.0.0/0          0.0.0.0/0        tcp dpt:31337
root@ip-10-0-0-1:~# iptables -L OUTPUT -n --line-numbers
Chain OUTPUT (policy ACCEPT)
num  target     prot opt source          destination
1    ACCEPT    tcp  --  0.0.0.0/0          10.0.0.2        tcp dpt:31337
2    DROP      tcp  --  0.0.0.0/0          0.0.0.0/0        tcp dpt:31337
root@ip-10-0-0-1:~# nc -v 10.0.0.2 31337
Connection to 10.0.0.2 31337 port [tcp/*] succeeded!
pwn.college{8nrS2l04QyAuHT4Cm3VwAeqyzF.0FM1AjNzwCO2kjMzEzW}
```

🎉 Successfully completed Firewall 3! 🎉

Terminal

F.0FM1AjNzwCO2kjMzEzW]

