

- Monitor 1

[illegible]

- Monitor 2

The top screenshot shows a Wireshark capture of a TCP connection from 10.0.0.1 to 10.0.0.2 on port 31337. The packet list shows a sequence of packets, including a SYN packet (Seq=1, Win=502) and several ACK packets. The packet details pane shows the selected packet (Seq=1, Win=502) and its raw data in hexadecimal and ASCII.

The bottom screenshot shows the same capture with a display filter applied: `pwn()`. The packet list shows a sequence of packets, including a SYN packet (Seq=1, Win=502) and several ACK packets. The packet details pane shows the selected packet (Seq=1, Win=502) and its raw data in hexadecimal and ASCII. The search results pane at the bottom indicates that no packets contained the string in their converted data.

I couldn't retrieve the flag.

2nd Attempt

The screenshot displays a Wireshark network capture and a terminal window. The terminal window shows a series of commands and their outputs, indicating a successful exploit attempt. The Wireshark capture shows the network traffic corresponding to the terminal session.

Terminal Window Output:

```
root@ip-10-0-0-1: ~  
found in stream 3  
=== stream 4 ===  
-bash: child setpgid (305 to 1097): Operation not permitted  
-bash: child setpgid (306 to 1097): Operation not permitted  
Running as user "root" and group "root". This could be dangerous.  
pwn.college(cJNjC0RwCZjFLHD_n96f5_HD_K.QX0YzMzwC02kMzEzW)  
found in stream 4  
=== stream 5 ===  
-bash: child setpgid (311 to 1103): Operation not permitted  
-bash: child setpgid (312 to 1103): Operation not permitted  
Running as user "root" and group "root". This could be dangerous.  
pwn.college(cJNjC0RwCZjFLHD_n96f5_HD_K.QX0YzMzwC02kMzEzW)  
found in stream 5  
=== stream 6 ===  
-bash: child setpgid (317 to 1109): Operation not permitted  
-bash: child setpgid (318 to 1109): Operation not permitted  
Running as user "root" and group "root". This could be dangerous.  
pwn.college(cJNjC0RwCZjFLHD_n96f5_HD_K.QX0YzMzwC02kMzEzW)  
found in stream 6  
=== stream 7 ===  
-bash: child setpgid (323 to 1115): Operation not permitted  
-bash: child setpgid (324 to 1115): Operation not permitted  
Running as user "root" and group "root". This could be dangerous.  
root@ip-10-0-0-1:~#
```

Wireshark Capture:

The Wireshark capture shows the network traffic corresponding to the terminal session. The capture is filtered for the interface `eth0`. The packet list shows several packets, including ARP requests and TCP connections. The packet details pane shows the selected packet (No. 1) and its details.

Clipboard:

The clipboard content is displayed in the terminal window, showing the command used to capture the traffic:

```
pwn.college(cJNjC0RwCZjFLHD_n96f5_HD_K.QX0YzMzwC02kMzEzW)
```

Success Message:

A green banner at the bottom of the terminal window indicates the successful completion of the exploit:

```
Successfully completed Monitor 2!
```

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.0F00AjNbwCO2kjMzEzW}
```

```
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.0F00AjNbwCO2kjMzEzW}
```

🎉 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_DVZOL61b8xWAXzeAD6Uh8zg3J.0V00AjNxwC02k}MzEzW}
```

```
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_DVZOL61b8xWAXzeAD6Uh8zg3J.0V00AjNxwC02k}MzEzW}
```

🎉 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{8nrS2l04QyAuHT4Cm3VwAeaqzF.0FM1AjNxoCO2k-jMzEzW}
```

```
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{8nrS2l04QyAuHT4Cm3VwAeaqzF.0FM1AjNxoCO2k-jMzEzW}
```

🎉 Successfully completed Firewall 3! 🎉