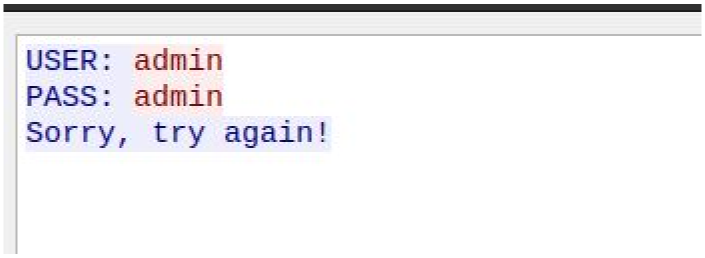
MarketDump [by butrintkomoni]

Points: 30 Points
Description: We have got informed that a hacker managed to get into our internal network after pivoiting through the web platform that runs in public internet. He managed to bypass our small product stocks logging platform and then he got our costumer database file. We believe that only one of our costumers was targeted. Can you find out who the customer was?
Link: https://www.hackthebox.eu/home/challenges/Forensics
Download Link: https://www.hackthebox.eu/home/challenges/download/66
Zip Password: hackthebox
sha256:d0ed5b6cc06bcb191fc0d83195542f7c1276835b1d8e2c5508e907ba740b64f6

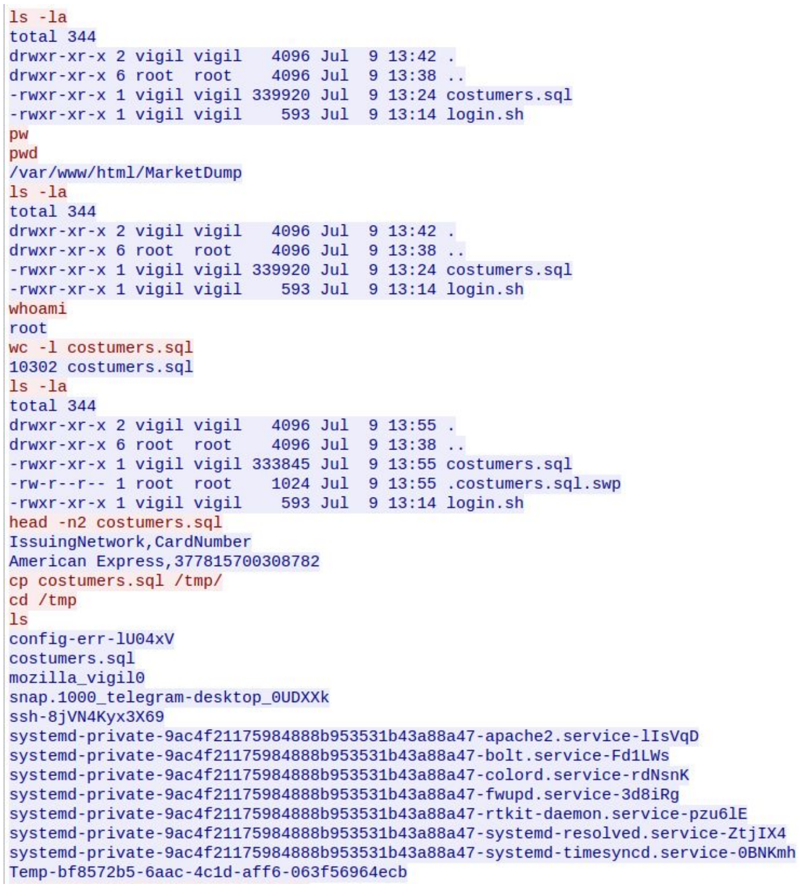
Wireshark

In the challenge description it states that we will be working with a web platform so I will filter the traffic to HTTP.



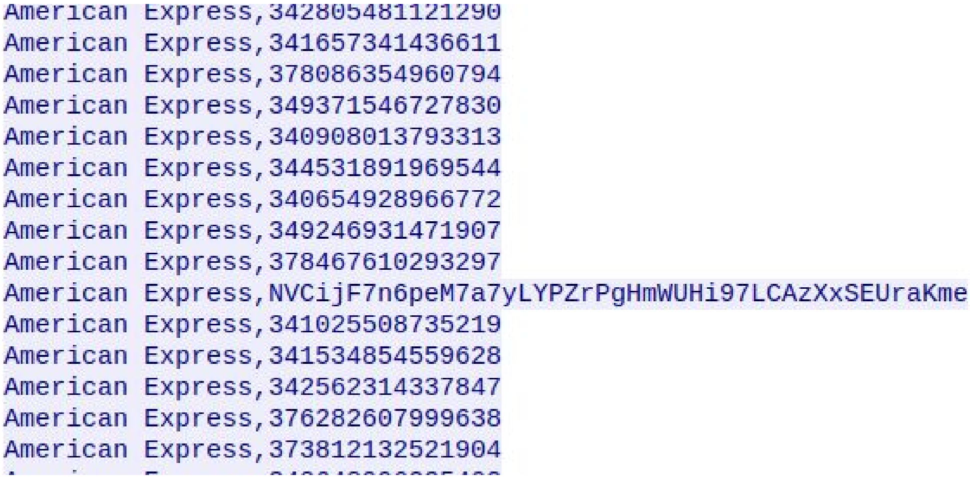
```
USER: admin
PASS: admin
Sorry, try again!
```

At stream 1051 someone tries a set of common credentials on a telnet server.



```
ls -la
total 344
drwxr-xr-x 2 vigil vigil   4096 Jul  9 13:42 .
drwxr-xr-x 6 root  root    4096 Jul  9 13:38 ..
-rwxr-xr-x 1 vigil vigil 339920 Jul  9 13:24 costumers.sql
-rwxr-xr-x 1 vigil vigil    593 Jul  9 13:14 login.sh
pw
pwd
/var/www/html/MarketDump
ls -la
total 344
drwxr-xr-x 2 vigil vigil   4096 Jul  9 13:42 .
drwxr-xr-x 6 root  root    4096 Jul  9 13:38 ..
-rwxr-xr-x 1 vigil vigil 339920 Jul  9 13:24 costumers.sql
-rwxr-xr-x 1 vigil vigil    593 Jul  9 13:14 login.sh
whoami
root
wc -l costumers.sql
10302 costumers.sql
ls -la
total 344
drwxr-xr-x 2 vigil vigil   4096 Jul  9 13:55 .
drwxr-xr-x 6 root  root    4096 Jul  9 13:38 ..
-rwxr-xr-x 1 vigil vigil 333845 Jul  9 13:55 costumers.sql
-rw-r--r-- 1 root  root    1024 Jul  9 13:55 .costumers.sql.swp
-rwxr-xr-x 1 vigil vigil    593 Jul  9 13:14 login.sh
head -n2 costumers.sql
IssuingNetwork,CardNumber
American Express,377815700308782
cp costumers.sql /tmp/
cd /tmp
ls
config-err-lU04xV
costumers.sql
mozilla_vigil0
snap.1000_telegram-desktop_0UDXXk
ssh-8jVN4Kyx3X69
systemd-private-9ac4f21175984888b953531b43a88a47-apache2.service-lIsVqD
systemd-private-9ac4f21175984888b953531b43a88a47-bolt.service-Fd1LWs
systemd-private-9ac4f21175984888b953531b43a88a47-colord.service-rdNsnK
systemd-private-9ac4f21175984888b953531b43a88a47-fwupd.service-3d8iRg
systemd-private-9ac4f21175984888b953531b43a88a47-rtkit-daemon.service-pzu6lE
systemd-private-9ac4f21175984888b953531b43a88a47-systemd-resolved.service-ZtjIX4
systemd-private-9ac4f21175984888b953531b43a88a47-systemd-timesyncd.service-0BNKmh
Temp-bf8572b5-6aac-4c1d-aff6-063f56964ecb
```

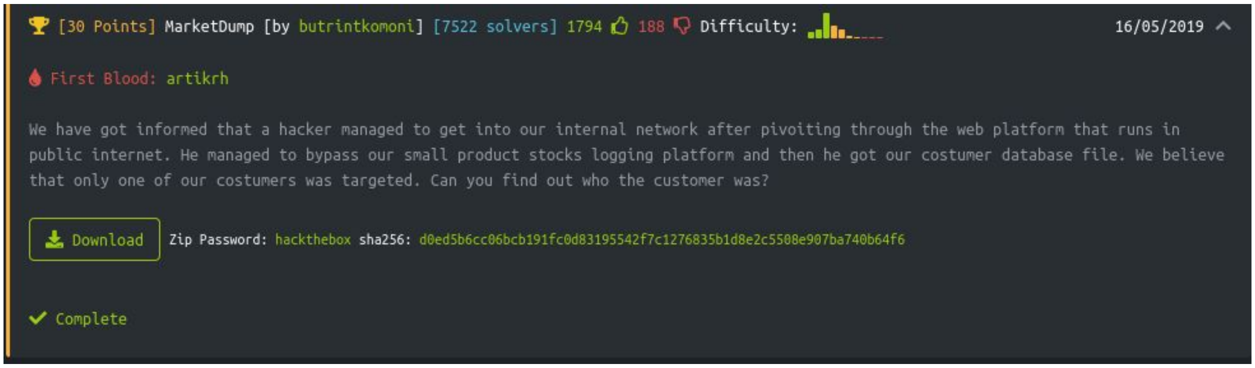
At stream 1056 the attack has gained access to the linux machine as root. The attacker uses the command “cat costumers.sql”. To display Card numbers.



```
American Express,342805481121290
American Express,341657341436611
American Express,378086354960794
American Express,349371546727830
American Express,340908013793313
American Express,344531891969544
American Express,340654928966772
American Express,349246931471907
American Express,378467610293297
American Express,NVCijF7n6peM7a7yLYPZrPgHmWUHi97LCAzXxSEUraKme
American Express,341025508735219
American Express,341534854559628
American Express,342562314337847
American Express,376282607999638
American Express,373812132521904
```

NVCijF7n6peM7a7yLYPZrPgHmWUHi97LCAzXxSEUraKme looks encrypted.

When decrypted it displays: HTB{DonTRuNAsRoOt!MESsEdUpMarket}



[30 Points] MarketDump [by butrintkomoni] [7522 solvers] 1794 188 Difficulty: 16/05/2019

First Blood: artikrh

We have got informed that a hacker managed to get into our internal network after pivoiting through the web platform that runs in public internet. He managed to bypass our small product stocks logging platform and then he got our costumer database file. We believe that only one of our costumers was targeted. Can you find out who the customer was?

Zip Password: hackthebox sha256: d0ed5b6cc06bcb191fc0d83195542f7c1276835b1d8e2c5508e907ba740b64f6

✓ Complete