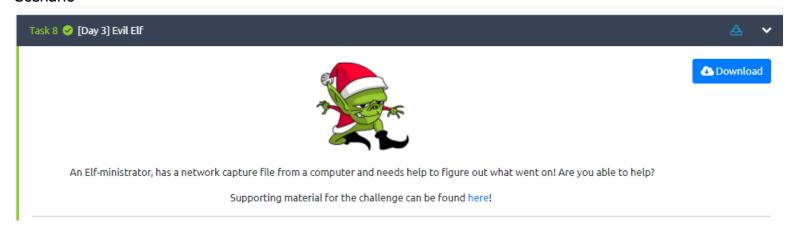
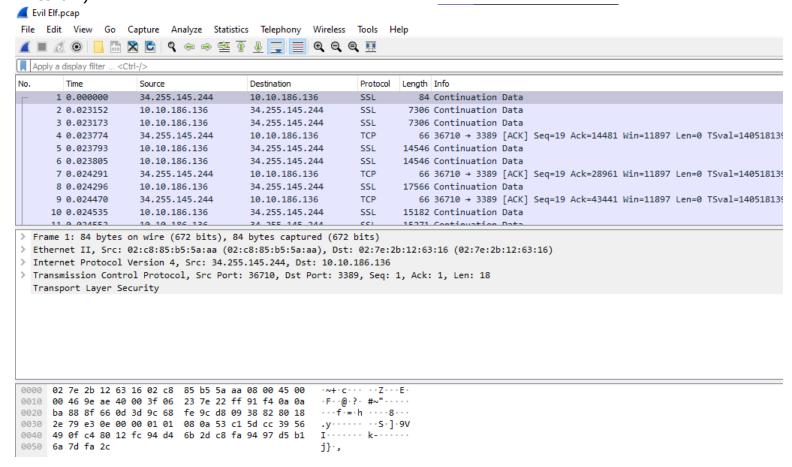
Day 3 - Evil Elf

Scenario



so here we need to analyze the network capture file Evil Elf.pcap (let's download it and launch our wireshark)



now let's find out what happened in this captured network file

here we found the tcp session connections of $34.255.145.244:36710 \rightarrow 10.10.186.136:3389$ which will be the RDP port

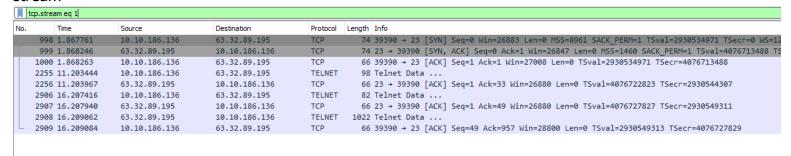
//nothing interesting here since the tcp stream was encrypted by SSL

985 1.748794	34.255.145.244	10.10.186.136	TCP	66 36710 → 3389 [ACK] Seq=901 Ack=6319639 Win=11897 Len=0 TSval=1405181826 TSecr=961957958
986 1.748854	34.255.145.244	10.10.186.136	TCP	66 36710 → 3389 [ACK] Seq=901 Ack=6328449 Win=11897 Len=0 TSval=1405181826 TSecr=961957958
007 1 740310	10 10 100 130	24 255 445 244	CCI	10050 Continuation Date

if we notice that, there's a tcp 3-way handshake session established with the ip 10.10.186.136:39390 ->

63.32.89.195:23 (Telnet port)

//telnet data will be transfered in plaintext form, so let's check out what happen here by following the tcp stream



Question: Whats the destination IP on packet number 998? -63.32.89.195

oh my aren't that the /etc/shadow file content? & the threat actor just write 'ps4' into the christmas_list.txt

```
■ Wireshark · Follow TCP Stream (tcp.stream eq 1) · Evil Elf.pcap.

                                                                                                                          ×
echo 'ps4' > christmas_list.txt
cat /etc/shadow
root:*:18171:0:99999:7:::
daemon:*:18171:0:99999:7:::
bin:*:18171:0:99999:7:::
sys:*:18171:0:99999:7:::
sync:*:18171:0:99999:7:::
games:*:18171:0:99999:7:::
man:*:18171:0:99999:7:::
lp:*:18171:0:99999:7:::
mail:*:18171:0:99999:7:::
news:*:18171:0:99999:7:::
uucp:*:18171:0:99999:7:::
proxy:*:18171:0:99999:7:::
www-data:*:18171:0:99999:7:::
backup:*:18171:0:99999:7:::
list:*:18171:0:99999:7:::
irc:*:18171:0:99999:7:::
gnats:*:18171:0:99999:7:::
nobody:*:18171:0:99999:7:::
systemd-network:*:18171:0:99999:7:::
systemd-resolve:*:18171:0:99999:7:::
syslog:*:18171:0:99999:7:::
messagebus:*:18171:0:99999:7:::
 apt:*:18171:0:99999:7:::
lxd:*:18171:0:99999:7:::
uuidd:*:18171:0:99999:7:::
dnsmasq:*:18171:0:99999:7:::
landscape: *: 18171:0:99999:7:::
sshd:*:18171:0:99999:7:::
pollinate:*:18171:0:99999:7:::
ubuntu:!:18232:0:99999:7:::
buddy:$6$3GvJsNPG$ZrSFprHS13divBhlaKg1rYrYLJ7m1xsYRKxlLh0A1sUc/6SUd7UvekBOtSnSyBwk3vCDqBhrgxQpkdsNN6aYP1:18233:0:99999:7:::
```

Question: What item is on the Christmas list? -ps4

now let's crack buddy account hash using john the ripper & we've found the credential

Question: Crack buddy's password!

-rainbow