


Day 3 - Evil Elf

Scenario

Task 8 [Day 3] Evil Elf



[Download](#)


An Elf-ministrator, has a network capture file from a computer and needs help to figure out what went on! Are you able to help?

Supporting material for the challenge can be found [here!](#)

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

Evil Elf.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	34.255.145.244	10.10.186.136	SSL	84	Continuation Data
2	0.023152	10.10.186.136	34.255.145.244	SSL	7306	Continuation Data
3	0.023173	10.10.186.136	34.255.145.244	SSL	7306	Continuation Data
4	0.023774	34.255.145.244	10.10.186.136	TCP	66	36710 → 3389 [ACK] Seq=19 Ack=14481 Win=11897 Len=0 TSval=140518139
5	0.023793	10.10.186.136	34.255.145.244	SSL	14546	Continuation Data
6	0.023805	10.10.186.136	34.255.145.244	SSL	14546	Continuation Data
7	0.024291	34.255.145.244	10.10.186.136	TCP	66	36710 → 3389 [ACK] Seq=19 Ack=28961 Win=11897 Len=0 TSval=140518139
8	0.024296	10.10.186.136	34.255.145.244	SSL	17566	Continuation Data
9	0.024470	34.255.145.244	10.10.186.136	TCP	66	36710 → 3389 [ACK] Seq=19 Ack=43441 Win=11897 Len=0 TSval=140518139
10	0.024535	10.10.186.136	34.255.145.244	SSL	15182	Continuation Data
11	0.024553	10.10.186.136	34.255.145.244	SSL	15271	Continuation Data

> Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)

> Ethernet II, Src: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa), Dst: 02:7e:2b:12:63:16 (02:7e:2b:12:63:16)

> Internet Protocol Version 4, Src: 34.255.145.244, Dst: 10.10.186.136

> Transmission Control Protocol, Src Port: 36710, Dst Port: 3389, Seq: 1, Ack: 1, Len: 18

Transport Layer Security

0000 02 7e 2b 12 63 16 02 c8 85 b5 5a aa 08 00 45 00 ..+..c... ..Z...E.

0010 00 46 9e ae 40 00 3f 06 23 7e 22 ff 91 f4 0a 0a .F...@...?..#~".....

0020 ba 88 8f 66 0d 3d 9c 68 fe 9c d8 09 38 82 80 18 ...f...=h8...

0030 2e 79 e3 0e 00 00 01 01 08 0a 53 c1 5d cc 39 56 .y..... ..S...9V

0040 49 0f c4 80 12 fc 94 d4 6b 2d c8 fa 94 97 d5 b1 I..... k.....

0050 6a 7d fa 2c j}}.,

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 -> 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

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

1/3

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

tcp.stream eq 1						
No.	Time	Source	Destination	Protocol	Length	Info
998	1.867761	10.10.186.136	63.32.89.195	TCP	74	39390 → 23 [SYN] Seq=0 Win=26883 Len=0 MSS=8961 SACK_PERM=1 TSval=2930534971 TSecr=0 WS=12
999	1.868246	63.32.89.195	10.10.186.136	TCP	74	23 → 39390 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=4076713488 TS
1000	1.868263	10.10.186.136	63.32.89.195	TCP	66	39390 → 23 [ACK] Seq=1 Ack=1 Win=27008 Len=0 TSval=2930534971 TSecr=4076713488
2255	11.203444	10.10.186.136	63.32.89.195	TELNET	98	Telnet Data ...
2256	11.203967	63.32.89.195	10.10.186.136	TCP	66	23 → 39390 [ACK] Seq=1 Ack=33 Win=26880 Len=0 TSval=4076722823 TSecr=2930544307
2906	16.207416	10.10.186.136	63.32.89.195	TELNET	82	Telnet Data ...
2907	16.207940	63.32.89.195	10.10.186.136	TCP	66	23 → 39390 [ACK] Seq=1 Ack=49 Win=26880 Len=0 TSval=4076727827 TSecr=2930549311
2908	16.209062	63.32.89.195	10.10.186.136	TELNET	1022	Telnet Data ...
2909	16.209084	10.10.186.136	63.32.89.195	TCP	66	39390 → 23 [ACK] Seq=49 Ack=957 Win=28800 Len=0 TSval=2930549313 TSecr=4076727829

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:::
uidd*: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$3GvJsNPG$ZrSFprHS13divBhlaKg1rYrYLJ7m1xsYRKx1Lh0A1sUc/6Sud7UvekB0tSnSyBwk3vCDqBhrgxQpkdsNN6aYP1:18233:0:99999:7:::
```

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

```
(nobodyatall@0xDEADBEEF)-[~/Desktop/research]
$ john --wordlist=/usr/share/wordlists/rockyou.txt buddyHash
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
rainbow          (buddy)
1g 0:00:00:00 DONE (2020-11-28 09:03) 3.333g/s 853.3p/s 853.3c/s 853.3C/s 123456..freedom
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Question: Crack buddy's password!

-rainbow