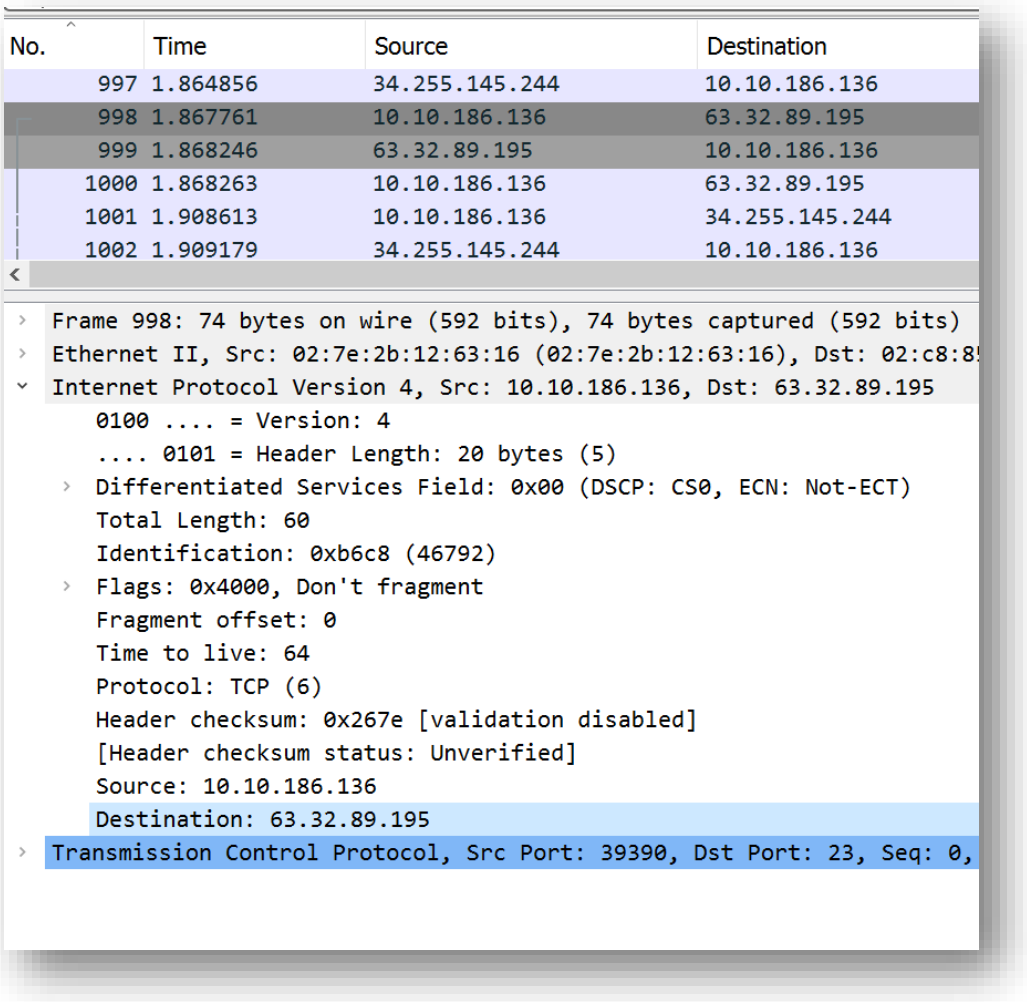
https://docs.google.com/document/d/1ZVsOtW7mM-4neZZ4QtYCEp__exiMrvlUCXTxhB-zyxk/edit

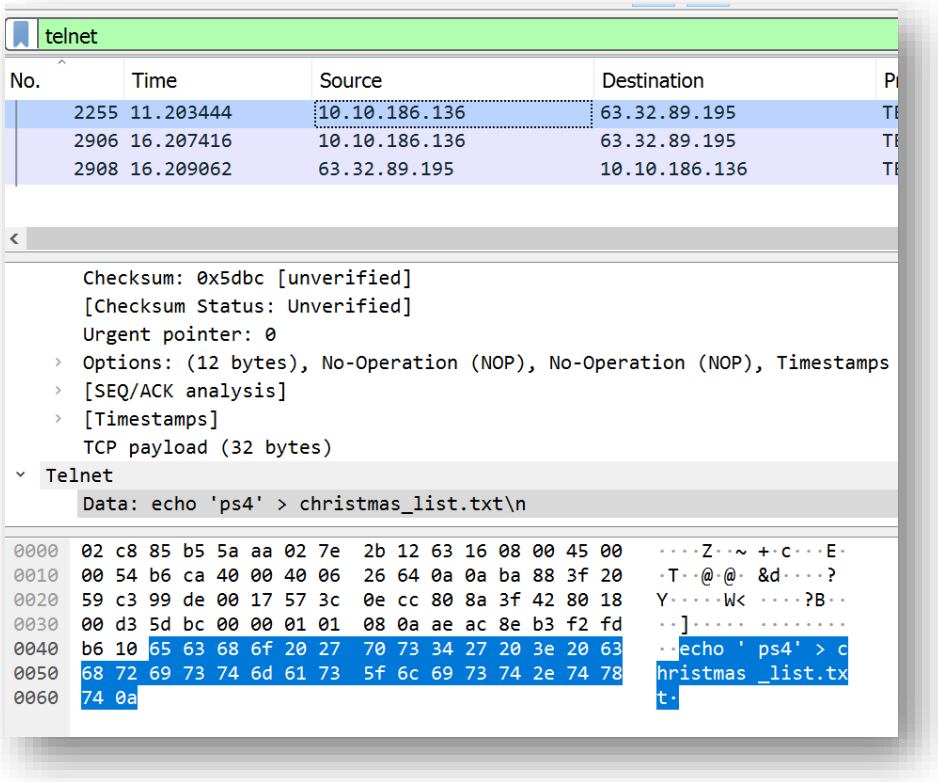
[Day 3] Evil Elf

1. **Whats the destination IP on packet number 998?**



- Destination IP is 63.32.89.195

2. **What item is on the Christmas list?**
   - From the tutorial document, it tells us to filter the .cap file by searching for telnet



- Telnet has three packets; the first one has data: echo 'ps4' > christmas_list.txt
- So, ps4 is on Christmas list

3. Crack buddy's password!

- The third telnet packet, #2908 has a bunch of data

- This is the result of cat-ting out the shadow file on a linux machine:
- buddy:$6$3GvJsNPG$ZrSFprHS13divBhlaKg1rYrYLJ7m1xsYRKxlLh0A1sUc/6SUd7UvekBOtSnSyBwk3vCDqBhrgxQpkdsNN6aYP1:18233:0:99999:7:::
- buddy is the username and the red part is the password hash
- Need to hash a dictionary and compare if any results match this hash; if they do, then they are the same password
- $6 denotes the hashing algorithm used
    - Sha512crypt 6
    - Hash-Mode is 1800
    - Download a password list file
    - https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt
- Use hashcat:
    - Hashcat -m 1800 <file with hash> <password file>
    - The result:

```
chetboii@gamingDesktop:~$ hashcat -m 1800 /mnt/d/GitHub\ Stuff/Advent\ of\ Cyber\ CTF/task8_hash.txt  /mnt/d/GitHub\
Stuff/Advent\ of\ Cyber\ CTF/rockyou.txt
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-AMD Ryzen 5 2600 Six-Core Processor, 4096/14285 MB allocatable, 12MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
* Zero-Byte
* Single-Hash
* Single-Salt
* Uses-64-Bit

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

* Device #1: build_opts '-cl-std=CL1.2 -I OpenCL -I /usr/share/hashcat/OpenCL -D LOCAL_MEM_TYPE=2 -D VENDOR_ID=64 -D
CUDA_ARCH=0 -D AMD_ROCM=0 -D VECT_SIZE=4 -D DEVICE_TYPE=2 -D DGST_R0=0 -D DGST_R1=1 -D DGST_R2=2 -D DGST_R3=3 -D DGST
_ELEM=16 -D KERN_TYPE=1800 -D _unroll'
* Device #1: Kernel m01800-pure.ba606752.kernel not found in cache! Building may take a while...
* Device #1: Kernel amp_a0.a8af4c69.kernel not found in cache! Building may take a while...
Dictionary cache built:
* Filename..: /mnt/d/GitHub Stuff/Advent of Cyber CTF/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

$6$3GvJsNPG$ZrSFprHS13divBhlaKg1rYrYLJ7m1xsYRKxlLh0A1sUc/6SUd7UvekBOtSnSyBwk3vCDqBhrgxQpkdsNN6aYP1:rainbow

Session..........: hashcat
Status...........: Cracked
Hash.Type........: sha512crypt $6$, SHA512 (Unix)
Hash.Target......: $6$3GvJsNPG$ZrSFprHS13divBhlaKg1rYrYLJ7m1xsYRKxlLh0...N6aYP1
Time.Started.....: Wed Mar 18 21:21:54 2020 (2 secs)
Time.Estimated...: Wed Mar 18 21:21:56 2020 (0 secs)
Guess.Base.......: File (/mnt/d/GitHub Stuff/Advent of Cyber CTF/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      834 H/s (8.67ms) @ Accel:128 Loops:32 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 1536/14344384 (0.01%)
Rejected.........: 0/1536 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidates.#1....: 123456 -> mexico1

Started: Wed Mar 18 21:21:37 2020
Stopped: Wed Mar 18 21:21:57 2020
chetboii@gamingDesktop:~$
```

- Password is appended to the end of the hash
- Password is: rainbow