

https://docs.google.com/document/d/1ZVsOtW7mM-4neZZ4QtYCEp_exiMrvlUCXTxhB-zyxk/edit

[Day 3] Evil Elf

1. What's the destination IP on packet number 998?

No.	Time	Source	Destination
997	1.864856	34.255.145.244	10.10.186.136
998	1.867761	10.10.186.136	63.32.89.195
999	1.868246	63.32.89.195	10.10.186.136
1000	1.868263	10.10.186.136	63.32.89.195
1001	1.908613	10.10.186.136	34.255.145.244
1002	1.909179	34.255.145.244	10.10.186.136

> Frame 998: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

> Ethernet II, Src: 02:7e:2b:12:63:16 (02:7e:2b:12:63:16), Dst: 02:c8:89:19:50:00 (02:c8:89:19:50:00)

> Internet Protocol Version 4, Src: 10.10.186.136, Dst: 63.32.89.195

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0xb6c8 (46792)

> Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 64

Protocol: TCP (6)

Header checksum: 0x267e [validation disabled]

[Header checksum status: Unverified]

Source: 10.10.186.136

Destination: 63.32.89.195

> Transmission Control Protocol, Src Port: 39390, Dst Port: 23, Seq: 0, Len: 0

- 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				
No.	Time	Source	Destination	P
2255	11.203444	10.10.186.136	63.32.89.195	TE
2906	16.207416	10.10.186.136	63.32.89.195	TE
2908	16.209062	63.32.89.195	10.10.186.136	TE

Checksum: 0x5dbc [unverified]				
[Checksum Status: Unverified]				
Urgent pointer: 0				
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps				
> [SEQ/ACK analysis]				
> [Timestamps]				
TCP payload (32 bytes)				

Telnet				
Data: echo 'ps4' > christmas_list.txt\n				

0000	02 c8 85 b5 5a aa 02 7e 2b 12 63 16 08 00 45 00	...	Z...	~ + . c ... E.
0010	00 54 b6 ca 40 00 40 06 26 64 0a 0a ba 88 3f 20	...	T...	@. & d ... ?
0020	59 c3 99 de 00 17 57 3c 0e cc 80 8a 3f 42 80 18	...	Y...	W< ... ? B..
0030	00 d3 5d bc 00 00 01 01 08 0a ae ac 8e b3 f2 fd	...]	...
0040	b6 10 65 63 68 6f 20 27 70 73 34 27 20 3e 20 63	...	echo ' ps4' > c	
0050	68 72 69 73 74 6d 61 73 5f 6c 69 73 74 2e 74 78	...	hristmas _list.tx	
0060	74 0a	...	t.	

- 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

```

TCP payload (950 bytes)
Telnet
Data: root*:18171:0:99999:7:::\n
Data: daemon*:18171:0:99999:7:::\n
Data: bin*:18171:0:99999:7:::\n
Data: sys*:18171:0:99999:7:::\n
Data: sync*:18171:0:99999:7:::\n
Data: games*:18171:0:99999:7:::\n
Data: man*:18171:0:99999:7:::\n
Data: lp*:18171:0:99999:7:::\n
Data: mail*:18171:0:99999:7:::\n
Data: news*:18171:0:99999:7:::\n
Data: uucp*:18171:0:99999:7:::\n
Data: proxy*:18171:0:99999:7:::\n
Data: www-data*:18171:0:99999:7:::\n
Data: backup*:18171:0:99999:7:::\n
Data: list*:18171:0:99999:7:::\n
Data: irc*:18171:0:99999:7:::\n
Data: gnats*:18171:0:99999:7:::\n
Data: nobody*:18171:0:99999:7:::\n
Data: systemd-network*:18171:0:99999:7:::\n
Data: systemd-resolve*:18171:0:99999:7:::\n
Data: syslog*:18171:0:99999:7:::\n
Data: messagebus*:18171:0:99999:7:::\n
Data: _apt*:18171:0:99999:7:::\n
Data: lxd*:18171:0:99999:7:::\n
Data: uidd*:18171:0:99999:7:::\n
Data: dnsmasq*:18171:0:99999:7:::\n
Data: landscape*:18171:0:99999:7:::\n
Data: sshd*:18171:0:99999:7:::\n
Data: pollinate*:18171:0:99999:7:::\n
Data: ubuntu:1:18232:0:99999:7:::\n
Data: buddy:$6$3GvJsnPG$Zr5FprHS13divBh1akg1rYrYL37m1xsYRKx1Lh0A1sUc/6Sud7UvekBOTs5SyBwk3vCDqBhrgxQpkdsNN6aYP1:18233:0:99999:7:::\n
00c0 3a 3a 3a 0a 67 61 6d 65 73 3a 2a 3a 31 38 31 37 ...:game s*:1817

```

- This is the result of cat-ting out the shadow file on a linux machine:
- buddy:\$6\$3GvJsNPG\$ZrSFprHS13divBhlaKg1rYrYLJ7m1xsYRKxlLh0A1sUc/6Sud7UvekB0tSnSyBwk3vCDqBhrgxQpkdsNN6aYP1:18233:0:99999:7:::
- 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/6Sud7UvekB0tSnSyBwk3vCDqBhrgxQpkdsNN6aYP1: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