Fireside Fridays

Packet Crafting

Thanks to our sponsors!

ACTIVE | COUNTERMEASURES

BLACK HILLS
Information Security
• 2008 •

WILD WEST
HACKIN' FEST

Antisyphon Training

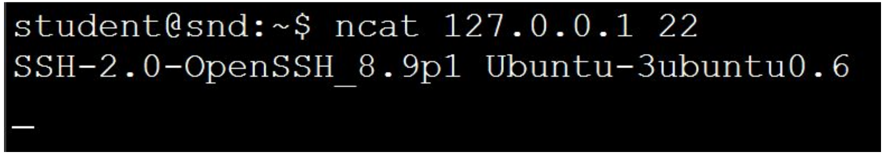
Tools for the labs

- Ncat
  - Or possibly other Netcat variations
- Hping3

Netcat, nc, ncat

- Raw socket tool
- Can connect to remote services
- Can open local listening ports
- Listening can create reverse shell (mini C2)
- Great for transfers when no protos in common
- Some minor packet crafting capability
- Each tool is similar but slightly different options

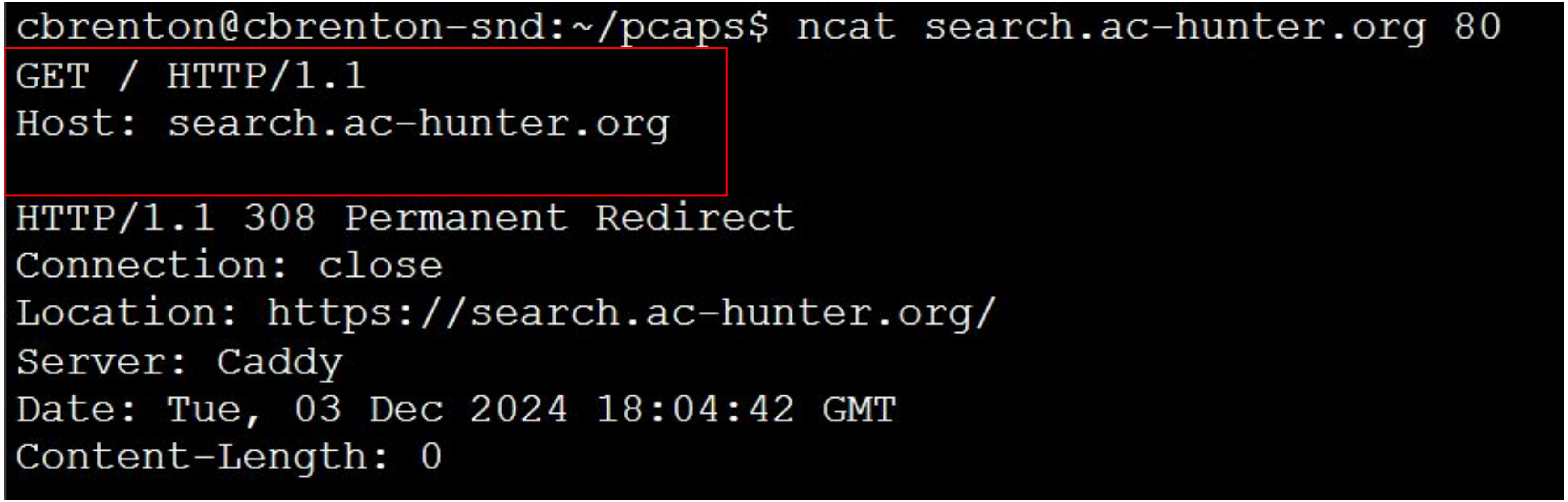
Simple banner grabbing



```
student@snd:~$ ncat 127.0.0.1 22
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6

_
```

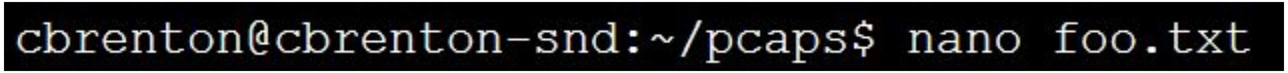
Connect to remote port 22
Print any data that is returned
CTRL-C to exit

Interacting with services

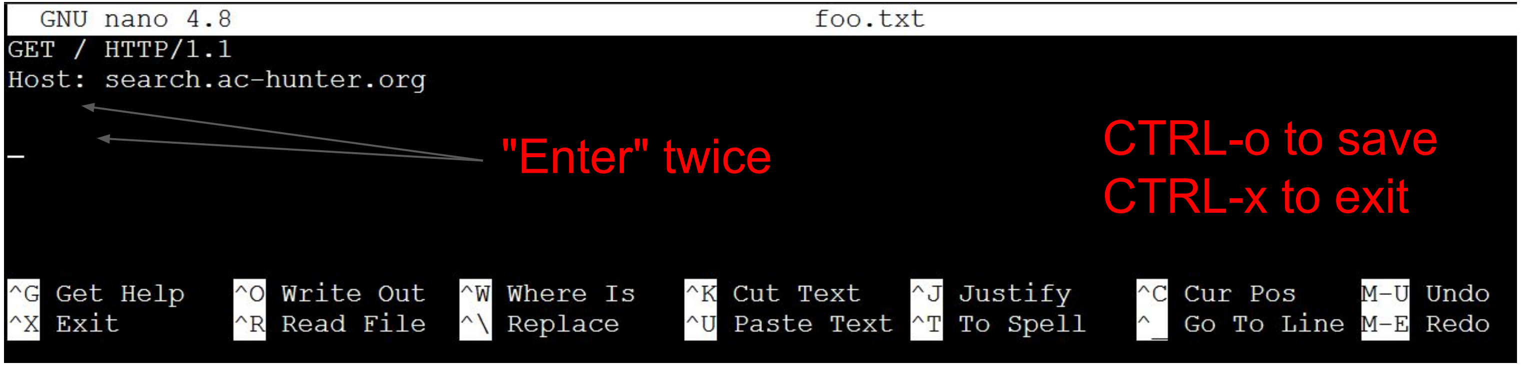


```
cbrenton@cbrenton-snd:~/pcaps$ ncat search.ac-hunter.org 80
GET / HTTP/1.1
Host: search.ac-hunter.org

HTTP/1.1 308 Permanent Redirect
Connection: close
Location: https://search.ac-hunter.org/
Server: Caddy
Date: Tue, 03 Dec 2024 18:04:42 GMT
Content-Length: 0
```

Sending data



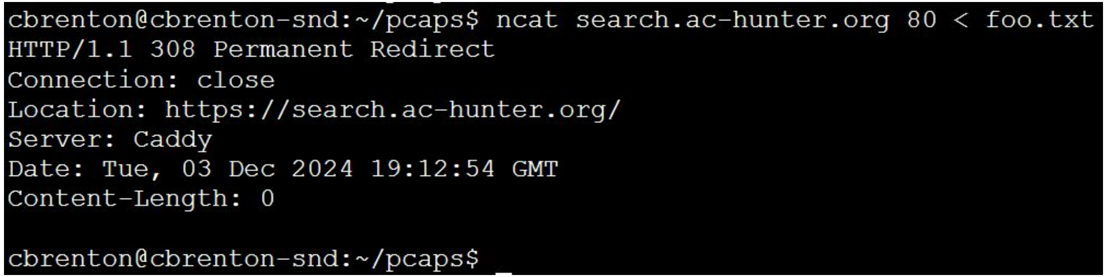
```
cbrenton@cbrenton-snd:~/pcaps$ nano foo.txt
```



```
  GNU nano 4.8                                                foo.txt
GET / HTTP/1.1
Host: search.ac-hunter.org


```

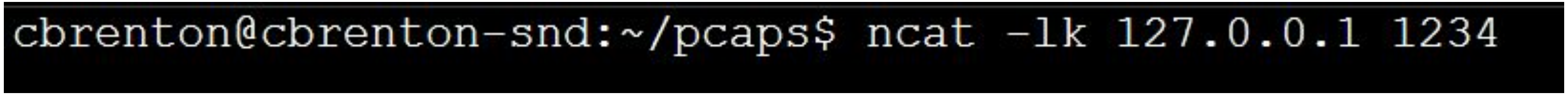
"Enter" twice

CTRL-o to save
CTRL-x to exit



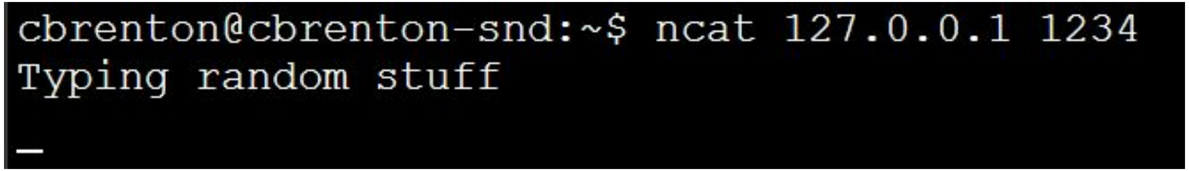
```
cbrenton@cbrenton-snd:~/pcaps$ ncat search.ac-hunter.org 80 < foo.txt
HTTP/1.1 308 Permanent Redirect
Connection: close
Location: https://search.ac-hunter.org/
Server: Caddy
Date: Tue, 03 Dec 2024 19:12:54 GMT
Content-Length: 0

cbrenton@cbrenton-snd:~/pcaps$ _
```

Local listening port



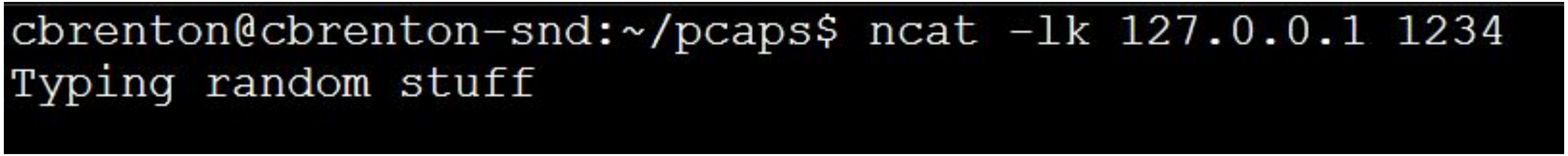
```
cbrenton@cbrenton-snd:~/pcaps$ ncat -lk 127.0.0.1 1234
```

2nd terminal



```
cbrenton@cbrenton-snd:~$ ncat 127.0.0.1 1234
Typing random stuff

_
```

Back in the first terminal

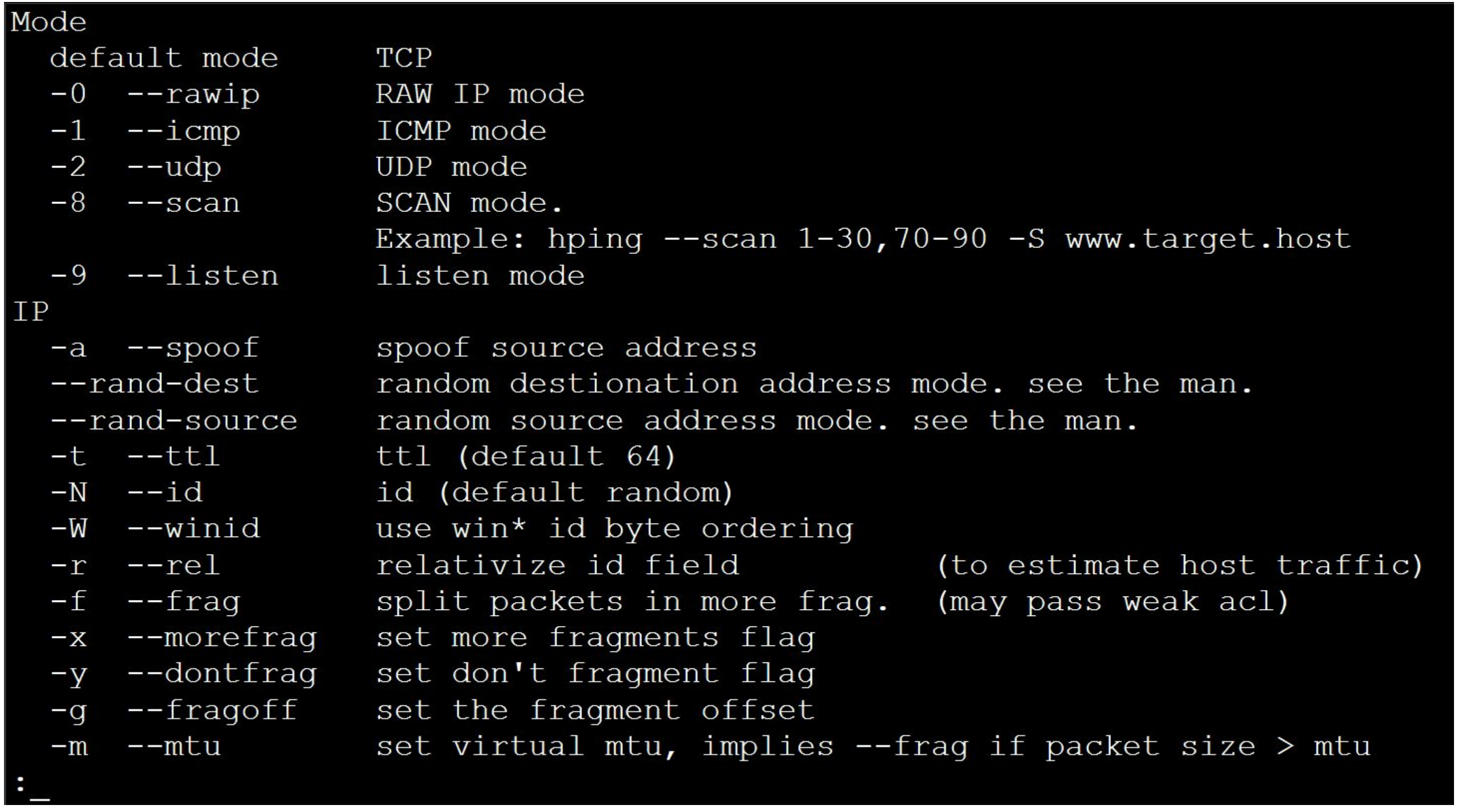


```
cbrenton@cbrenton-snd:~/pcaps$ ncat -lk 127.0.0.1 1234
Typing random stuff
```

hping3

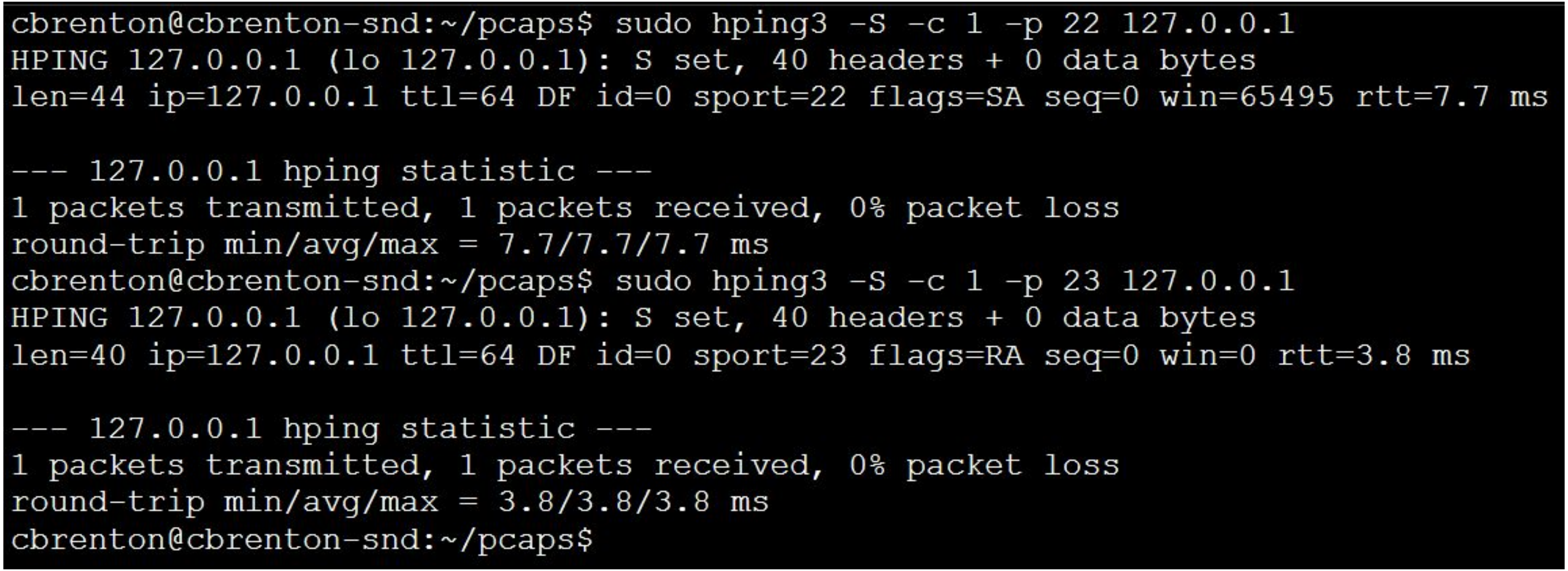
- Let's you create custom IP packets
- Change IP/TCP/UDP/ICMP fields as you desire
- Great way to see how firewall responds to various types of packets
- Scans can be scripted
- Scapy is more feature rich, but more to learn

Some hping3 options



```
Mode
  default mode     TCP
  -0  --rawip      RAW IP mode
  -1  --icmp       ICMP mode
  -2  --udp        UDP mode
  -8  --scan       SCAN mode.
                   Example: hping --scan 1-30,70-90 -S www.target.host
  -9  --listen     listen mode
IP
  -a  --spoof      spoof source address
  --rand-dest      random destionation address mode. see the man.
  --rand-source    random source address mode. see the man.
  -t  --ttl        ttl (default 64)
  -N  --id         id (default random)
  -W  --winid      use win* id byte ordering
  -r  --rel        relativize id field          (to estimate host traffic)
  -f  --frag       split packets in more frag.  (may pass weak acl)
  -x  --morefrag   set more fragments flag
  -y  --dontfrag   set don't fragment flag
  -g  --fragoff    set the fragment offset
  -m  --mtu        set virtual mtu, implies --frag if packet size > mtu
:_
```

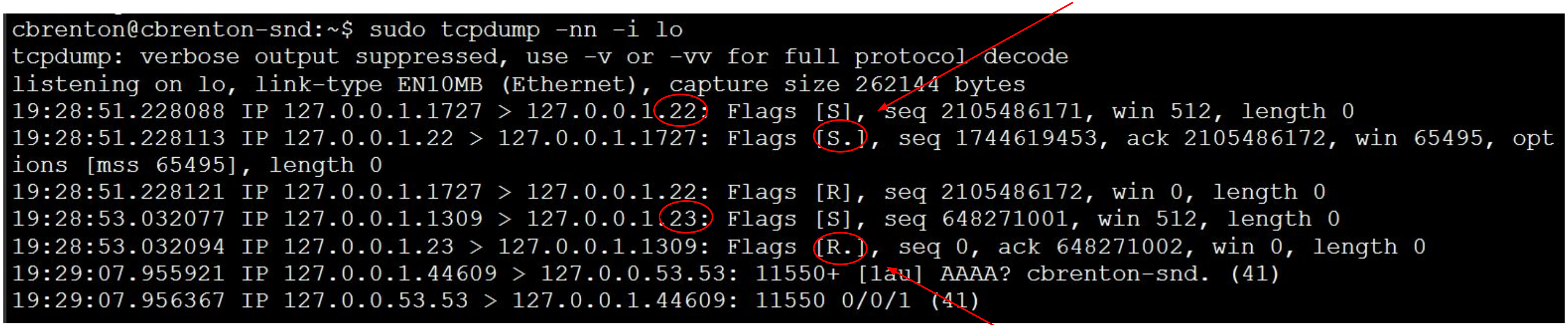
Scanning open/closed ports



```
cbrenton@cbrenton-snd:~/pcaps$ sudo hping3 -S -c 1 -p 22 127.0.0.1
HPING 127.0.0.1 (lo 127.0.0.1): S set, 40 headers + 0 data bytes
len=44 ip=127.0.0.1 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=65495 rtt=7.7 ms

--- 127.0.0.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.7/7.7/7.7 ms
cbrenton@cbrenton-snd:~/pcaps$ sudo hping3 -S -c 1 -p 23 127.0.0.1
HPING 127.0.0.1 (lo 127.0.0.1): S set, 40 headers + 0 data bytes
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=23 flags=RA seq=0 win=0 rtt=3.8 ms

--- 127.0.0.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.8/3.8/3.8 ms
cbrenton@cbrenton-snd:~/pcaps$
```

What tcpdump sees

Port is open



```
cbrenton@cbrenton-snd:~$ sudo tcpdump -nn -i lo
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
19:28:51.228088 IP 127.0.0.1.1727 > 127.0.0.1.22: Flags [S], seq 2105486171, win 512, length 0
19:28:51.228113 IP 127.0.0.1.22 > 127.0.0.1.1727: Flags [S.], seq 1744619453, ack 2105486172, win 65495, opt
ions [mss 65495], length 0
19:28:51.228121 IP 127.0.0.1.1727 > 127.0.0.1.22: Flags [R], seq 2105486172, win 0, length 0
19:28:53.032077 IP 127.0.0.1.1309 > 127.0.0.1.23: Flags [S], seq 648271001, win 512, length 0
19:28:53.032094 IP 127.0.0.1.23 > 127.0.0.1.1309: Flags [R.], seq 0, ack 648271002, win 0, length 0
19:29:07.955921 IP 127.0.0.1.44609 > 127.0.0.53.53: 11550+ [1au] AAAA? cbrenton-snd. (41)
19:29:07.956367 IP 127.0.0.53.53 > 127.0.0.1.44609: 11550 0/0/1 (41)
```

Port is closed

Wrap up

- Thank you for attending!
- Certs usually go out in 24 hours
- Video should be posted within 24 hours
- If you have any lingering questions, drop me an email at chris@activecountermeasures.com