CNF Tools Practicum

Gabe Kaptchuk

Test Wednesday

- I don’t know what’s on the test
- I don’t know what you can bring to the test
- If you have questions, post to Piazza
- If you have questions about Networks, feel free to ask me!

Goals

- Gain an understanding of a few practical networking tools used regularly
- Tools used to troubleshoot real deployed networks
  - We are not limited to the scope of material already covered
- We are going to be going quickly, so this presentation may be helpful as reference material

Class Overview

Practical Tools Used by Network Administrators

- ifconfig / netstat
- /etc/host
- ping / traceroute
- nslookup / dig
- netcat (nc)
- wget / curl
- nmap
- ssh
- scp / sftp
- Charles Proxy
- Chrome Developer Tools

Fun Stuff Used by Developers

- bettercap (evercap)
- scapy

About Using Tools

- We focus on UNIX tools
  - Most of these tools have been ported to Windows
- Network tools can be dangerous
  - Please don't use bettercap on the Hopkins network
    - (If you are going to ignore this advice, you've never heard of us.)
- Theory is nice but reality is messy
- Not sure how to use a tool?
  - `$man <toolname>`
  - `http://lmgtfy.com/?q=<toolname>`

Class Overview

Practical Tools Used by Network Administrators

- ifconfig / netstat
- /etc/host
- ping / traceroute
- nslookup / dig
- netcat (nc)
- wget / curl
- nmap
- ssh
- scp / sftp
- Charles Proxy
- Chrome Developer Tools

Fun Stuff Used by Developers

- bettercap (evercap)
- scapy

ifconfig/netstat

- Useful for understanding what is going on with your own system

```
$ ifconfig -a
```

- How are you connected to the network?

- Reset your internet interface

```
$ sudo ifconfig <interface> down
$ sudo ifconfig <interface> up
```

- What ports on your machine are open?

```
$ netstat –a
```

ifconfig/netstat

- Setup internet connection from the command line

```
$ ifconfig eth0 192.168.2.2
$ ifconfig eth0 netmask 255.255.255.0
```

- MAC soofing/change you MAC

```
$ ifconfig en0 ether dd:bb:aa:cc:ee:ff
```

Class Overview

Practical Tools Used by Network Administrators

- ifconfig / netstat
- /etc/host
- ping / traceroute
- nslookup / dig
- netcat (nc)
- wget / curl
- nmap
- ssh
- scp / sftp
- Charles Proxy
- Chrome Developer Tools

Fun Stuff Used by Developers

- bettercap (evercap)
- scapy

/etc/host

- Static table lookup for hostnames on Unix
- Associates IP addresses to hostnames
- DNS supersedes /etc/hosts but useful for:
  - Bootstrapping when DNS is running
  - Host specific services
  - Local network configuration
- Trivia: used to be the only way to resolve hostnames before DNS!

/etc/host

```
##
# Host Database
##
127.0.0.1          localhost
255.255.255.255    broadcasthost
::1                localhost

hostname.com       128.220.13.76
```

Class Overview

Practical Tools Used by Network Administrators

- ifconfig / netstat
- /etc/host
- ping / traceroute
- nslookup / dig
- netcat (nc)
- wget / curl
- nmap
- ssh
- scp / sftp
- Charles Proxy
- Chrome Developer Tools

Fun Stuff Used by Developers

- bettercap (evercap)
- scapy

ping

- Useful for making sure you are connected to the internet
- Specific protocol that sends out an echo request to another host.
- Most hosts can configured to respond to `ping` requests
  - Some hosts will be specifically configured to not respond for security reasons

```
$ ping <hostname or ip-address>
$ ping 8.8.8.8     (Google DNS servers)
```

ping of death

- Correctly formatted ping packet is typically 80ish bytes
- Can we create malformed packets?
- Yes. Ping of death: 65,535 byte ping.

No.	Time	Source	Destination	Protocol	Length	Info
1	0…	127.0.0.1	127.0.0.1	ICMP	88	Echo (ping) request id=0xc08e, seq=0/0, ttl=64 (no res…
2	1…	127.0.0.1	127.0.0.1	ICMP	88	Echo (ping) request id=0xc08e, seq=1/256, ttl=64 (no r…

```
▶ Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
▶ Null/Loopback
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xaf2e [correct]
    Identifier (BE): 49294 (0xc08e)
    Identifier (LE): 36544 (0x8ec0)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
  ▶ [No response seen]
    Timestamp from icmp data: Feb 22, 2016 09:34:06.272914000 EST
    [Timestamp from icmp data (relative): 0.000025000 seconds]
  ▼ Data (48 bytes)
      Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...
      [Length: 48]
```

traceroute

- Provides information about the path a packet takes
  - Sends packet to a destination
  - At each router asks for a reply when it passes on the packet

micharu123@charon: ~ — 90×13

```
traceroute: Warning: google.com has multiple addresses; using 65.199.32.25
traceroute to google.com (65.199.32.25), 64 hops max, 52 byte packets
 1  fios_quantum_gateway (192.168.1.1)  1.993 ms  1.180 ms  1.117 ms
 2  lo0-100.bltmmd-vfttp-308.verizon-gni.net (71.179.161.1)  46.967 ms  11.245 ms  9.141 m
s
 3  t0-9-0-1.bltmmd-lcr-21.verizon-gni.net (100.41.129.136)  11.521 ms
    t0-9-0-1.bltmmd-lcr-22.verizon-gni.net (100.41.129.138)  12.620 ms  9.514 ms
 4  * * *
 5  0.ae6.gw12.phl6.alter.net (140.222.230.33)  15.170 ms  13.739 ms
    0.ae10.gw12.phl6.alter.net (140.222.230.41)  12.081 ms
 6  google-gw.customer.alter.net (152.179.249.30)  11.770 ms  12.735 ms  13.034 ms
 7  * * *
```

`Finger` (Yes Really)

- Legacy
- Displays information about users on a remote machine
- No longer a default binary
- Service on linux was called `fingerd`

```
build@ubuntu: ~ — 90×25
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up finger (0.17-15) ...
build@ubuntu:~$ finger
Login     Name       Tty      Idle  Login Time   Office     Office Phone
build     Build     *:0             Feb 17 15:36 (:0)
build     Build      pts/9      4d  Feb 17 15:37 (:0)
build     Build      pts/0      3d  Feb 17 15:38 (:0)
build     Build      pts/23     3d  Feb 17 15:41 (:0)
build     Build      pts/24         Feb 21 16:01 (pool-68-134-188-174.bltmmd.fios.verizon.
net)
build@ubuntu:~$ finger build
Login: build                            Name: Build
Directory: /home/build                  Shell: /bin/bash
On since Wed Feb 17 15:36 (PST) on :0 from :0 (messages off)
On since Wed Feb 17 15:37 (PST) on pts/9 from :0
    4 days idle
On since Wed Feb 17 15:38 (PST) on pts/0 from :0
    3 days 21 hours idle
On since Wed Feb 17 15:41 (PST) on pts/23 from :0
   3 days 21 hours idle
On since Sun Feb 21 16:01 (PST) on pts/24 from pool-68-134-188-174.bltmmd.fios.verizon.net
   3 seconds idle
No mail.
No Plan.
build@ubuntu:~$
```

Morris Worm

- Berkley Network Programs
  - sendmail
  - *finger*
  - rexec
- Bug in finger server that downloads code in replace of finger request and executes it
- Berkley finger server:
  - Reads a request from the originating host
  - Executes *finger* program with the request as an argument
  - Returns output
- Finger server reads the remote request with *gets()*
  - 512 byte request buffer
  - Provide 536 bytes of data (24 extra bytes)
- *Server's stack frame is overwriten and program counter points to worm code*

whois

- Looks up the registration record of a domain

```
Domain Name: JHU.EDU

Registrant:
   Johns Hopkins University
   5801 Smith Avenue
   Suite 3110B
   Baltimore, MD 21209
   UNITED STATES

Administrative Contact:
   Alan V Shackelford
   Manager, Enterprise Web Services
   Johns Hopkins University
   5801 Smith Avenue
   Davis Building, Suite 3110B
   Baltimore, MD 21209
   UNITED STATES
   (667) 208-6120
   hostmaster@jhmi.edu

Technical Contact:

   Enterprise Services Group
   Johns Hopkins University
   5801 Smith Avenue
   Davis Building, Suite 3110B
   Baltimore, MD 21209
   UNITED STATES
   (667) 208-6120
   hostmaster@jhmi.edu

Name Servers:
   ENS1.JHMI.EDU
   ENS1.JHU.EDU       128.220.1.75, 2606:2b00:0:405::10

Domain record activated:    19-Mar-1987
Domain record last updated: 01-Apr-2015
Domain expires:             31-Jul-2016
```

Class Overview

Practical Tools Used by Network Administrators

- ifconfig / netstat
- /etc/host
- ping / traceroute
- nslookup / dig
- netcat (nc)
- wget / curl
- nmap
- ssh
- scp / sftp
- Charles Proxy
- Chrome Developer Tools

Fun Stuff Used by Developers

- bettercap (evercap)
- scapy

nslookup/dig

- Command line DNS tools
- The two tools are slightly different, but usually give you the same answer
- Both perform a full DNS lookup and you can direct them to specific DNS servers

```
$nslookup <hostname>
$dig <hostname>
```

dig (Domain Information Groper)

```
; <<>> DiG 9.8.3-P1 <<>> cs.jhu.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26703
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;cs.jhu.edu.                    IN      A

;; ANSWER SECTION:
cs.jhu.edu.             155059  IN      A       128.220.13.76

;; Query time: 24 msec
;; SERVER: 192.168.200.1#53(192.168.200.1)
;; WHEN: Mon Feb 22 15:21:54 2016
;; MSG SIZE  rcvd: 44
```

nslookup

```
Server:         192.168.200.1
Address:        192.168.200.1#53

Non-authoritative answer:
Name:   cs.jhu.edu
Address: 128.220.13.76
```

Class Overview

Practical Tools Used by Network Administrators

- ifconfig / netstat
- /etc/host
- ping / traceroute
- nslookup / dig
- netcat (nc)
- wget / curl
- nmap
- ssh
- scp / sftp
- Charles Proxy
- Chrome Developer Tools

Fun Stuff Used by Developers

- bettercap (evercap)
- scapy

netcat (nc)

- Testing basic UDP/TCP connections
- Allows the users on the two ends to exchange text
- Has both a listening component

```
nc –l <port-num>
```

- And a connection component

```
nc <ip-addr> <port-num>
```

Class Overview

Practical Tools Used by Network Administrators

- ifconfig / netstat
- /etc/host
- ping / traceroute
- nslookup / dig
- netcat (nc)
- wget / curl
- nmap
- ssh
- scp / sftp
- Charles Proxy
- Chrome Developer Tools

Fun Stuff Used by Developers

- bettercap (evercap)
- scapy

wget

- `curl` is an alternative to `wget` that has slightly different parameters
- Command line interface for making HTTP(S) requests
- `$ curl -H "Host: cs.jhu.edu" -H "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8" -H "Upgrade-Insecure-Requests: 1" -H "User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.109 Safari/537.36" -H "Accept-Language: en-US,en;q=0.8" -H "Cookie:`
`__utma=39856377.132711982.1452690273.1455721900.1455721900.1; __utmc=39856377; __utmz=39856377.1455721900.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided); __qca=P0-1507557502-1455721900041; _ga=GA1.2.132711982.1452690273;`
`r12smSESSION=AUXyVlvl3rNb6TYo/Zi5DvCVHDe1G4ciN8hVgOK31dXgrL4LDDLJweiqWw2qOPpcoEZVzw03OwJnjODjTk2WaVGJtEH1WVHy6M3OBzbNowtXqDT8l+k1qUz1FbXirFjwDj0J39o5neTwrBJ/CtynIrKvBkWJlL0AdPFtZ4Kic3Z/AVYPOTxxux/zAGByPV28ysuk2I5HLIm0/mT0khFktPjkhIEYAnAfqNXq5KPMnO2/lB/LbbTwWNyr5Aoeph4+LjJ/m0dXkT3j/qRgK5OaS2EDAnQ65huszWYQgtBylq/s9RnAitXLMdV5KmLJxrWnXQe9W3NJ5WsThkw1xPK/fhibCOP5Yc1tMYuevMUSSVdOqhE/j5GSG2hzVDkJngAeTd99f00h3KeM09/VeFPAxMMfSMeHPxxx+Dl9UhKkagfCmLfAtOpks6k0iBtHxFPV4fEkvXAwRfoXVnrIp56pTkx60Q79GWWeA6x801S3HesBq2BWr9soICskeudJwsjUPnKGjQkmsHeFtemwlvc6bSZmUD4qFOZE5wDmnwYqFMpsgj5+lnesuXemuOU/rn4Wxuoczw08wufac2z2mihkLwU6Ig3Z28T1+iW3Rgg202EQh4yYYSG0wcB1jEkyY2dUasWREsrNPQoFN5vr+D4+0ujWHEwvRXXoJIl9fcaj5ailIElxZvHD4s4IcdFVifSfkCkfheIGno4q7jthbLplatf3zMEoJtmfKLP1eDAC/e2l/Bbz7yPQithgTYhXE1wgZO+UY1/1IVn/EK3FSCnz49/zNMv9wqmrZ+8q7cBWiFY29aZiTPz7MDfrVBFU/MwefHuiaMLzXFoOfXqXnOnK5RntthgIyrpnUwW+i6WikSk1YMX4fm/bCNCgdPSt/Ntv3PtR0k0qX/NbH8rJ3sIQPdURtD2Ov6I1N4jvj0HVN9w6sg+0w0NatGvT0pDUdRihPbHrM4yPblKPR+6M0yoqC/qTerF1yrn5s7dbTLqPI6s4aas/gleaMeSKWn0OFlm/vS5hlbIPgaolTYUxNLBqtozZRWQWIqbpYmhQFbb/ONU9rRJ/Pb7lwMENyDQLMnsijRnDKidGP9SS8itj8Lf3pfjCn8F0S8n6GNVefUzh7PX6oheLeUCG1MCOFUOy+hYdfrKXVfNlv+xhIvaXDnuDR7OxNgbBDW8b"`
`--compressed http://cs.jhu.edu/`
- `$ curl cs.jhu.edu`

Class Overview

Practical Tools Used by Network Administrators

- ifconfig / netstat
- /etc/host
- ping / traceroute
- nslookup / dig
- netcat (nc)
- wget / curl
- nmap
- ssh
- scp / sftp
- Charles Proxy
- Chrome Developer Tools

Fun Stuff Used by Developers

- bettercap (evercap)
- scapy

nmap

- Helpful for figuring out what hosts are on your network
- Extremely powerful network tool. These are only some of the applications
- OS fingerprinting, host scan, Port scan
- We will go over some of the uses of nmap now, but there are always more

zmap

- Research tool from University of Michigan
- Capable of performing a complete scan of the IPv4 address space in under 5 minutes
  - 3,706,452,992 public addresses

```
$ zmap --bandwidth=10M --target-port=80 --max-targets=10000 --output-file=results.csv
```

Class Overview

Practical Tools Used by Network Administrators

- ifconfig / netstat
- /etc/host
- ping / traceroute
- nslookup / dig
- netcat (nc)
- wget / curl
- nmap
- ssh
- scp / sftp
- Charles Proxy
- Chrome Developer Tools

Fun Stuff Used by Developers

- bettercap (evercap)
- scapy

ssh (Secure Shell)

- Access a shell on a remote machine (port 22)
- Communication channel is encrypted
- Can be used to generally secure a communication channel using port forwarding
  - There are better solutions for this, but it's a quick and dirty solution
- Two flavors of authentication
  - Password Based
  - Key Based

Class Overview

Practical Tools Used by Network Administrators

- ifconfig / netstat
- /etc/host
- ping / traceroute
- nslookup / dig
- netcat (nc)
- wget / curl
- nmap
- ssh
- scp / sftp
- Charles Proxy
- Chrome Developer Tools

Fun Stuff Used by Developers

- bettercap (evercap)
- scapy

scp/sftp(Secure Copy)

- Copy a file (usually across the network) in a secure way

```
$ scp gkaptchuk@porcini.isi.jhu.edu:~/Desktop/test.txt .
```

```
$ scp ~/Desktop/test.txt
gkaptchuk@porcini.isi.jhu.edu:~/Desktop/test2.txt
```

- Security Side Note: difference between FTP and SFTP

Class Overview

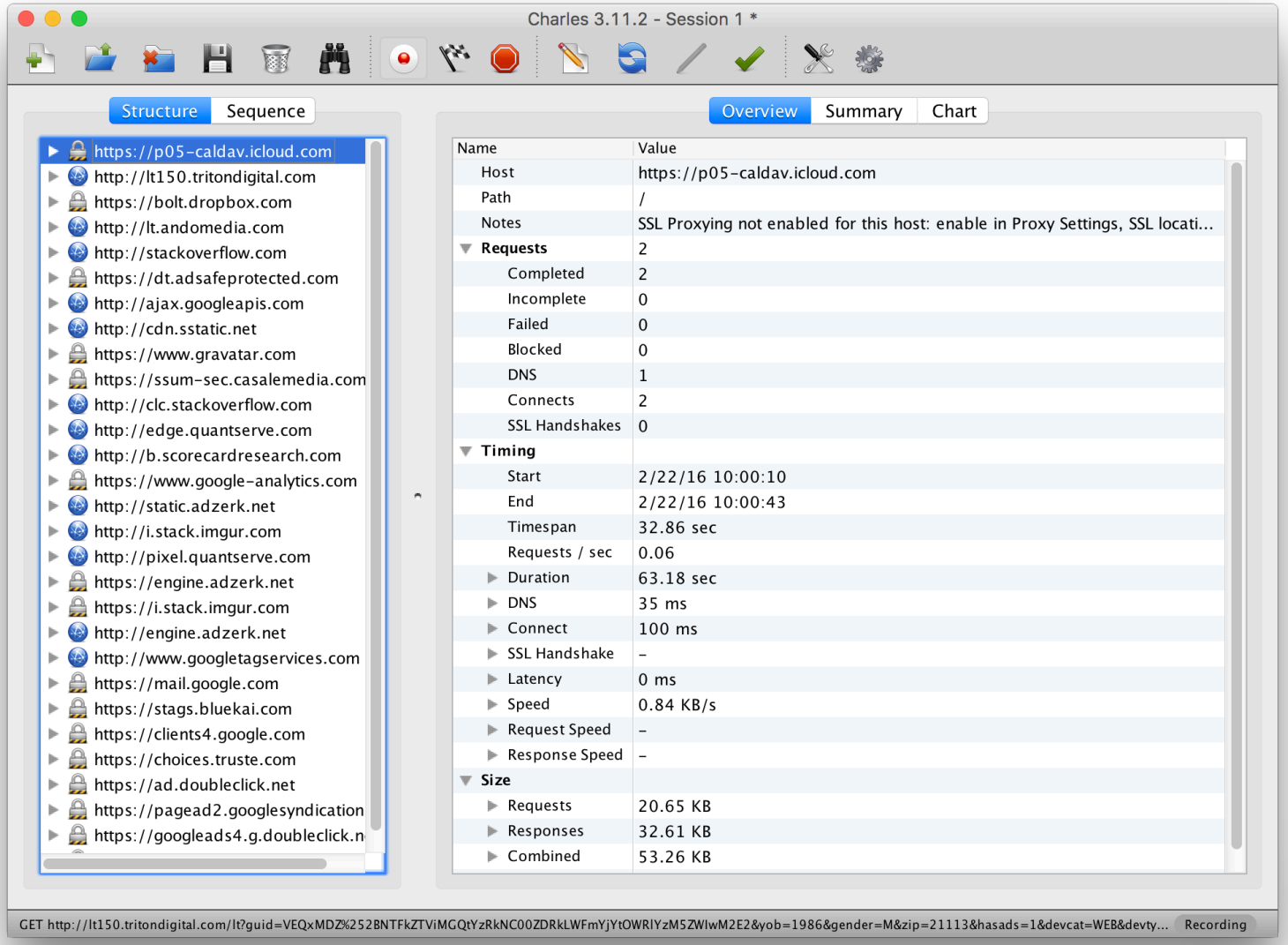
Practical Tools Used by Network Administrators

- ifconfig / netstat
- /etc/host
- ping / traceroute
- nslookup / dig
- netcat (nc)
- wget / curl
- nmap
- ssh
- scp / sftp
- Charles Proxy
- Chrome Developer Tools

Fun Stuff Used by Developers

- bettercap (evercap)
- scapy

charles (proxy)



Class Overview

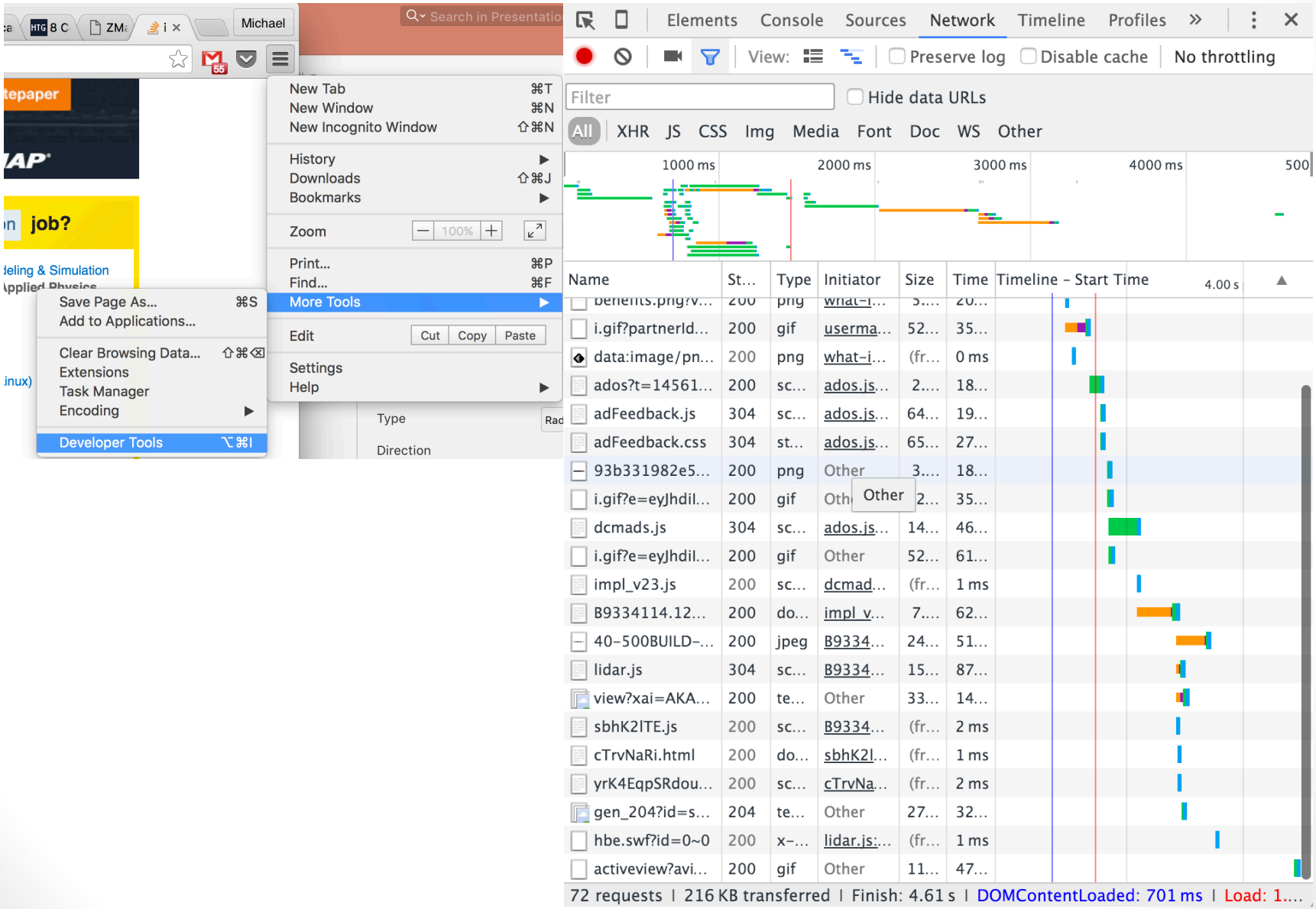
Practical Tools Used by Network Administrators

- ifconfig / netstat
- /etc/host
- ping / traceroute
- nslookup / dig
- netcat (nc)
- wget / curl
- nmap
- ssh
- scp / sftp
- Charles Proxy
- Chrome Developer Tools

Fun Stuff Used by Developers

- bettercap (evercap)
- scapy

chrome dev tools



Class Overview

Practical Tools Used by Network Administrators

- ifconfig / netstat
- /etc/host
- ping / traceroute
- nslookup / dig
- netcat (nc)
- wget / curl
- nmap
- ssh
- scp / sftp
- Charles Proxy
- Chrome Developer Tools

Fun Stuff Used by Developers

- bettercap (evercap)
- scapy

bettercap

DISCLAIMER

Please do not use bettercap on the Hopkins network or on any other network that you do not the administrator. It should be used to examine your own traffic only and should not be used with any malicious intent. Do not try to compromise the security or privacy of others. Hopkins sys-admins are scary people.

bettercap

- Written in ruby (just in this presentation because this is the only good piece of ruby ever created)
- Proxies all traffic through the machine by manipulating the ARP table on the local network

```
$gem install bettercap
$bettcap –sniffer
```

Class Overview

Practical Tools Used by Network Administrators

- ifconfig / netstat
- /etc/host
- ping / traceroute
- nslookup / dig
- netcat (nc)
- wget / curl
- nmap
- ssh
- scp / sftp
- Charles Proxy
- Chrome Developer Tools

Fun Stuff Used by Developers

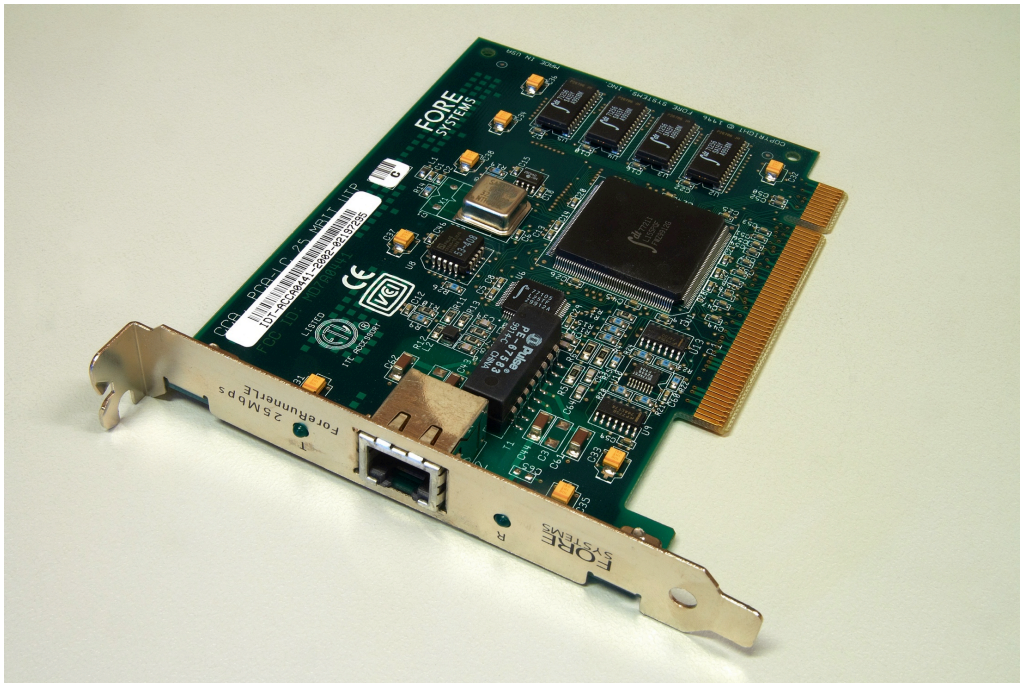
- bettercap (evercap)
- scapy

scapy

- We are going to be using scapy for our class exercise, so this is the part where you should pay attention
- Scapy is a python library used to generate, manipulate, and monitor network traffic
  - If you don’t know python, then the projects in this class have probably been impossible and you should probably learn it before next class period
- Scapy designed with a security slant
  - When tools do weird things on the network, they are usually designed for nefarious purposes

DETOUR: NIC

- Network Interface Controller



- Usually off board mechanism for network connections. Comes in both WiFi and Ethernet flavors

Image from Wikipedia

DETOUR: Snooping

- Usually NIC's drop all messages whose IP's do not match their own
  - Traffic never makes it to CPU
- Unlike wired networks, pretty much all wifi traffic can be seen as broadcast
  - If you are listening, you can hear everyone's traffic

scapy

- Created precisely because there are too many tools! For example, there exists numerous tools for the following:
  - Packet forging: modifies packets and sends them
  - Sniffing: capture and dissect packets
  - Testing: does unitary tests
  - Scanning: the above with additional parameters
  - Fingerprinting: uses a protocol for the advantage of learning something about a remote computer
- Tools have a nasty habit of only showing information *they* think would interest you