PCAP Command-Line Madness!

Hal Pomeranz / hal@sans.org / @hal_pomeranz

tcpdump

You can use it to capture some packets

```
tcpdump -n -i ens0 -w full-packets.pcap
```

Or maybe just the packet headers

```
tcpdump -n -i ens0 -s 160 -w headers-only.pcap
```

But did you know?

You can capture a collection of PCAP files

```
tcpdump -n -i ens0 -w mypcap -C 1000 -W 7
tcpdump -n -i ens0 -w mypcap-%j -G 86400 -W 14
```

You can filter large PCAPs into smaller chunks

```
tcpdump -n -r large.pcap -w dns.pcap 'port 53'
tcpdump -n -r large.pcap -w smb.pcap
    'tcp and port 445'
```

tshark

All the filtering power of Wireshark

Only output the fields you want

It's like AWK for packets!

```
tshark -n -r example.pcap -Y http.request
   -T fields -e frame.time -e ip.src
   -e http.request.method -e http.host
   -e http.request.uri -e http.user_agent
   -e http.referer
```

Ugh! That timestamp!

Default timestamp format is ugly

Sneaky conversion trick: -e frame.time_epoch + AWK

```
tshark -n -r example.pcap -Y http.request
   -T fields -e frame.time_epoch … |
   awk '{$1=strftime("%F %T", $1); print}'
```

Because I **`sed`** So

tshark and shell commands go great together!

Let's look at Google search activity in a PCAP

```
tshark -n -r example.pcap
   -Y 'http.host contains google.com and
   http.request.uri contains "/search?"'
   -T fields -e http.request.uri |
      sed 's/.*q=//' | sed 's/&.*//'
```

The Command-Line Histogram

Find the most visited web sites

```
tshark -n -r example.pcap -Y 'http.request'
   -T fields -e http.host |
   sort | uniq -c | sort -n
```

Noise Reduction

Only track sites with Google analytics cookies

Gives you top web sites visited, no advertising domains

```
tshark -n -r example.pcap
    -Y 'http.cookie contains "_utm"'
    -T fields -e http.host |
        sort | uniq -c | sort -n
```

Other Useful PCAP Tools

`capinfos` – Show basic PCAP stats

`editcap` – Split PCAPs by date and time

`ngrep` – String searching in packet content

`tcpflow` – Write TCP streams to files

`nfpcapd` – Create Netflow data from PCAP

Snort and Bro can also read from PCAPs!

Thanks For Listening!

Any final questions?

Hal Pomeranz
hal@sans.org
@hal_pomeranz

Slides! – http://deer-run.com/~hal/