NMap, Wireshark, and SNORT

Outline

- Security Concepts
- Security Categories
- Security Roles
- Host Security
- Vulnerability Scanning
- Intrusion Detection
- NMAP
- Wireshark
- SNORT

Security Concepts

- "Defense In Depth" -- security at multiple layers: at the application, at the host, in the network level
- "Least Privilege" -- only provide as much access as is necessary to complete a task, no more than that
- "End-to-End Security" -- security at the application layer tends to be more valuable than network security
- "Secure By Design" -- design new systems with security in mind, not after the system is deployed
- "No Silver Bullet" -- there is no perfect security; it is a process that requires vigilance

Security Categories

- These are well defined in ISO-17799
- Risk Analysis
- Vulnerability Assessment
- Host Security
- Network Security
- Intrusion Detection
- Incident Handling
- Education and Training
- Policy Development
- Enforcement

Security Roles

- Chief Security Officer (Policy Development)
- Acceptable Use Policy Officer (Policy Enforcement)
- Accounts Manager (Identity Management)
- Network Engineer (Firewalls, VPNs, IDS)
- Incident Response Team
- Training Specialist
- System Manager
- Auditor

Host Security

- If you do good Host Security, everything else is easier!
- **Anti-Virus Software**
- **OS Patches are Up-to-date**
- **Application Patches are Up-to-date**
- Disable Unused Services
- Access Control Lists

- Account Management
- User Training: phishing e-mails
- User Training: selecting good passwords
- User Training: downloading software
- Physical Access

Vulnerability Assessment

- This is an iterative and repetitive process
  - Discover the network
  - Enumeration the devices on the network
  - Enumerate the services on the network
  - Find vulnerabilities in those services
  - Report and Repair the affected systems
  - REPEAT

Vulnerability Assessment
(standard practices)

- Perform scans at regular intervals, i.e. weekly or monthly
- Perform scans when new critical exploits are announced
- Provide PGP-signed e-mail to notify customers about upcoming scans
- Conduct scans from a well known source
- Maintain a list of Admin Contacts

Vulnerability Scanners (open source products)

- **NMap**
  - **http://nmap.org**
- Nikto - Web Vulnerabilities
  - http://www.cirt.net/nikto2
- Microsoft Baseline Security Analyzer
  - http://technet.microsoft.com/en-us/security/cc184923
- Sara (end-of-life)
  - http://www-arc.com/sara/

Vulnerability Scanners (commercial products)

- NESSUS (free version for home-use)
  - http://www.nessus.org/
- Rapid7 Nexpose (free version for 32 hosts)
  - http://www.rapid7.com/products/vulnerability-management.jsp
- Qualys QualysGuard
  - http://www.qualys.com

Intrusion Detection

- Exactly what it sounds like: sniffing network traffic to look for attacks
- Two common approaches:
  - “**anomaly detection**”, looking for unusual behavior on the network
  - “**signature matching**”, compare packets against a database of know attack signatures
- Passive monitors are called “IDS”-- In-line monitors can block traffic and are “IPS”, intrusion prevention

Intrusion Detection (issues)

- What exactly is “good” traffic and “bad” traffic? And with all the protocols there are, is it even possible to imagine being successful at detecting new attacks or variations on old ones???
- Network traffic doesn’t tell you as much as the Host can
- Can get a lot of alarms that are “false positives”
- If you have limited resources, there are more important tools: Host Security, Firewalls, Anti-Virus, Vulnerability Scans...
- IDS systems can be extremely resource intensive
- IDS systems can create their own security problems

IDS -- Open Source

- **SNORT**
  - **http://www.snort.org/**
  - http://www.bleedingsnort.com/
- BRO
  - http://www.bro-ids.org/

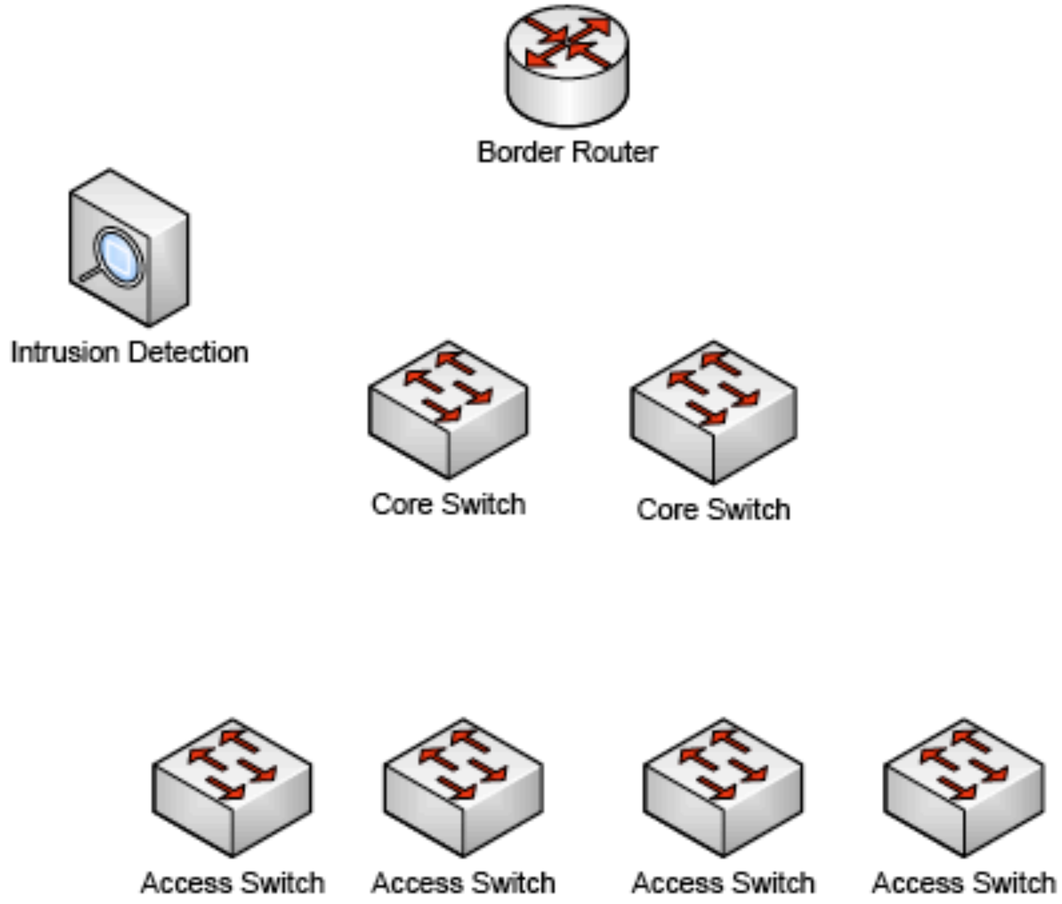
IDS - commercial

- Juniper IDS, Cisco IDS, ...
- SourceFire IPS (the commercial arm of SNORT)
- HP/3COM Tipping Point IPS

IDS - Enterprise Deployment Considerations

- Determine the appropriate place(s) within the network to deploy the monitor
- Enable "MONITOR" ports on HP Switches
- Enable "SPAN" ports on CISCO Switches
- Trunk VLANs to a single monitor port
- Make sure the machine is isolated/secure

Enterprise IDS
(where do you position the IDS?)



*WARNING *

- Your enterprise or law enforcement may have a strict policies or laws forbidding you from sniffing network traffic

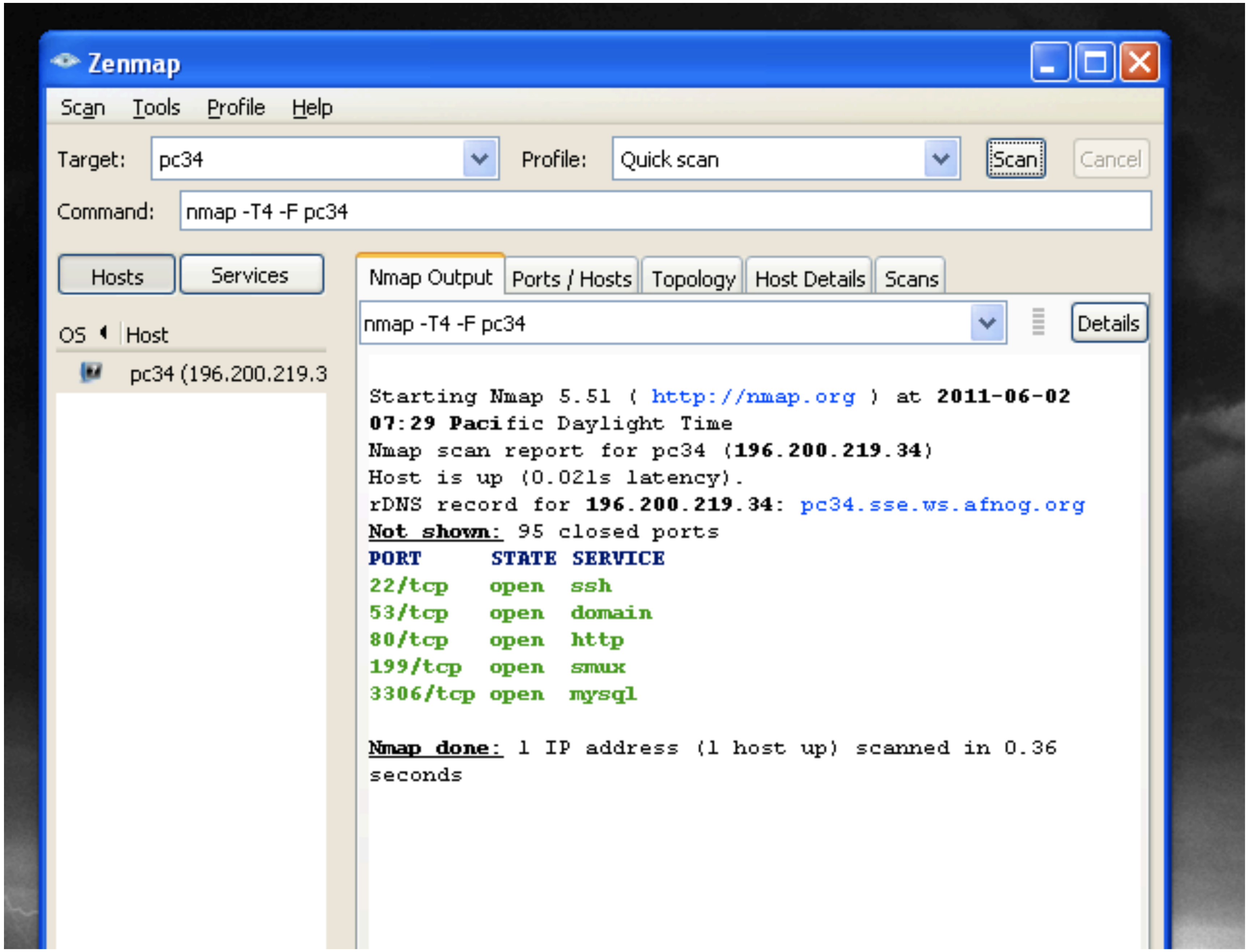
- Your enterprise or law enforcement may have a strict policies or laws forbidding you from scanning the network

- Make absolutely sure you have the authority to conduct these activities **BEFORE** you do them.

NMap

- One of the most popular scanning tools
- More than just a port scanner-- can also determine OS versions, Application versions, and run vulnerability scripts
- Available on all OS's
- A GUI front-end is available: ZenMap

ZenMap



```
Starting Nmap 5.51 ( http://nmap.org ) at 2011-06-02
07:29 Pacific Daylight Time
Nmap scan report for pc34 (196.200.219.34)
Host is up (0.021s latency).
rDNS record for 196.200.219.34: pc34.sse.ws.afnog.org
Not shown: 95 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
199/tcp  open  smux
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.36
seconds
```

NMap: simple scans

- TCP SYN Scan -- nmap sends SYN, but does not complete the connection, "TCP Half-Open"
- TCP CONNECT Scan -- nmap, TCP full connection
- TCP Bad Flags Scan -- nmap uses odd or illegal TCP flag combinations to produce error responses
- TCP ACK Scan -- nmap sends ACK to produce error response
- UDP Scan -- nmap sends a UDP packet

NMap: syntax

- nmap <SCANTYPE> <PORTS> <HOSTS>
- nmap -sT -p80 pcXX # TCP Port 80
- nmap -sS -p U:53,137,T:21-25,80 pcXX # Multiple Ports
- nmap -sT -p80 196.200.216.0/24 # A Whole Subnet
- nmap -A -T4 pcXX # OS FingerPrint
- nmap -v -sn 192.168.0.0/16 10.0.0.0/8 # Ping Subnets

NMap Scripting Engine

- NMap Scripting Engine (NSE)
- Can run complex tests agains services
- Ex. nmap -sC pcXX
- Ex. nmap --script smb-os-discovery somepc

NMap Scripting Engine

- nmap --script smb-check-vulns.nse -p445 <host>
- sudo nmap -sU -sS --script smb-check-vulns.nse -p U:137,T:139 <host>

Script Output

```
Host script results:
| smb-check-vulns:
|   MS08-067: NOT VULNERABLE
|   Conficker: Likely CLEAN
|   regsvc DoS: regsvc DoS: NOT VULNERABLE
|   SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
|   MS06-025: NO SERVICE (the Ras RPC service is inactive)
|_  MS07-029: NO SERVICE (the Dns Server RPC service is
inactive)
```

NMap Exercises

*WARNING *

- Your enterprise or law enforcement may have a strict policies or laws forbidding you from sniffing network traffic

- Your enterprise or law enforcement may have a strict policies or laws forbidding you from scanning the network

- Make absolutely sure you have the authority to conduct these activities **BEFORE** you do them.

WireShark

- Wireshark is both a packet sniffer **AND** a protocol decoder
- Wireshark is extremely popular for trouble-shooting network issues
- Available on most OS's, however the GUI on Linux/ Gnome or Windows is actually nicest
- Available in a GUI version and a CLI version--the CLI version is called "**tshark**"
- Free/Open Source Software

WireShark:

what is protocol decoding?

- protocol decoding: reading the packets off of the interface, and interpreting them based on the type of protocol in the packet
- protocol decoding: requires a library of "decoders" templates that have all of the network protocol definitions
- these come with the package, but others can be added-- there are tens of 100's of protocols
- some example: IP, TCP, UDP, ICMP, ARP, IPV6, ND, DHCP, DNS, SMTP, HTTP, ...

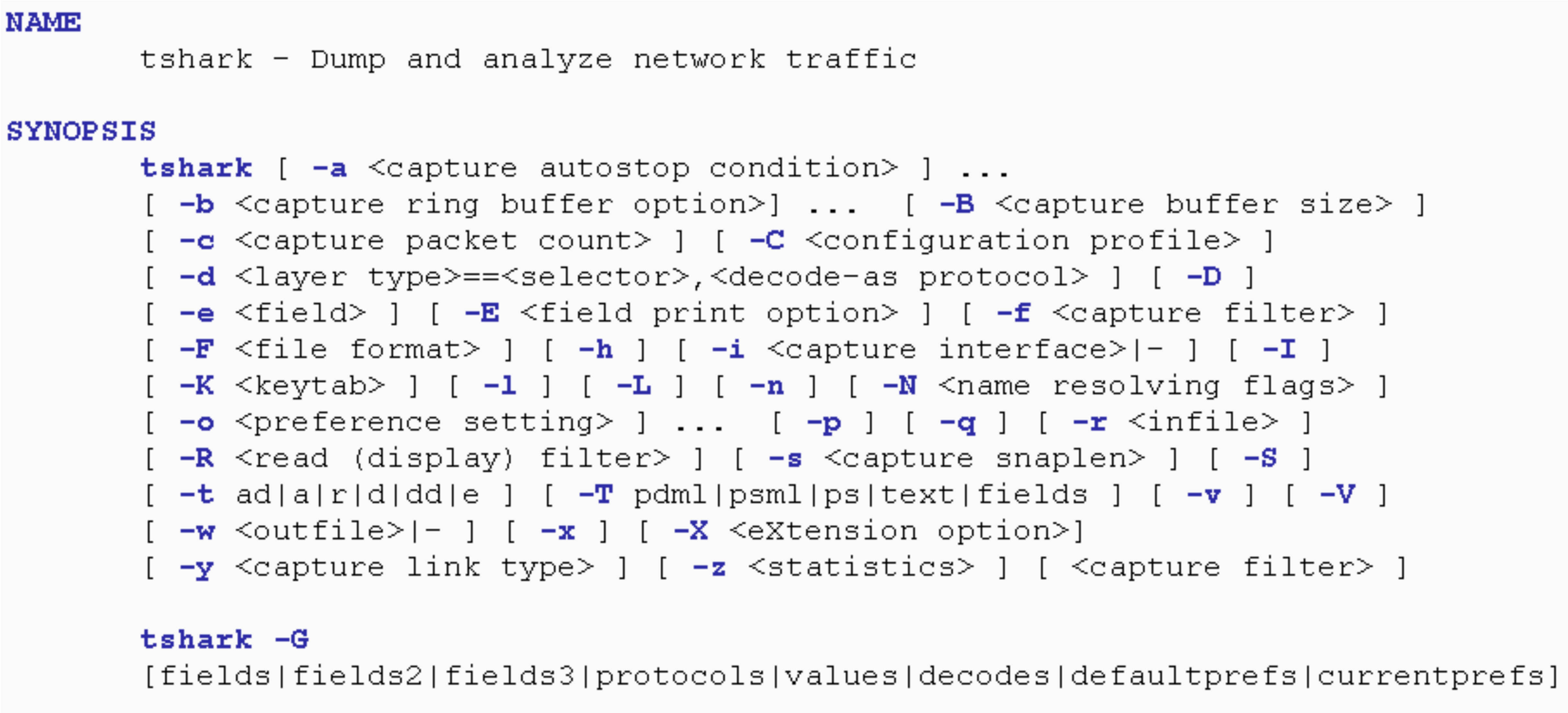
A few words about tcpdump

- tcpdump is the grandfather of all the sniffers
- you will find tcpdump will be installed by default on most systems
- tcpdump depends on “LibPcap”, the packet capture library
- this is “old school”, and doesn’t have the level of decoding capability of the newer programs, like tshark
- tcpdump example (note: syn is 0x2, syn/ack is 0x12): sudo tcpdump -n -i em0 -s 64 -w /tmp/packets ‘tcp [13]&0xFF==0x12’

A few words about sniffing

- **Promiscuous Mode**: in order to see traffic other than the traffic sent directly to and from your machine, the interface must be in this mode--you must have root access
- **Interface Issue**s: different media types have different drivers, and may behave differently. ethernet interfaces usually work.-- other types may or may not work depending on your platform/os/drivers
- **VLAN Issues**: whether your interface strips VLAN tags or leaves them on, and whether the interface can monitor a VLAN trunk or not. This is especially important when you are monitoring multiple subnets.

WireShark (tshark): the CLI interface

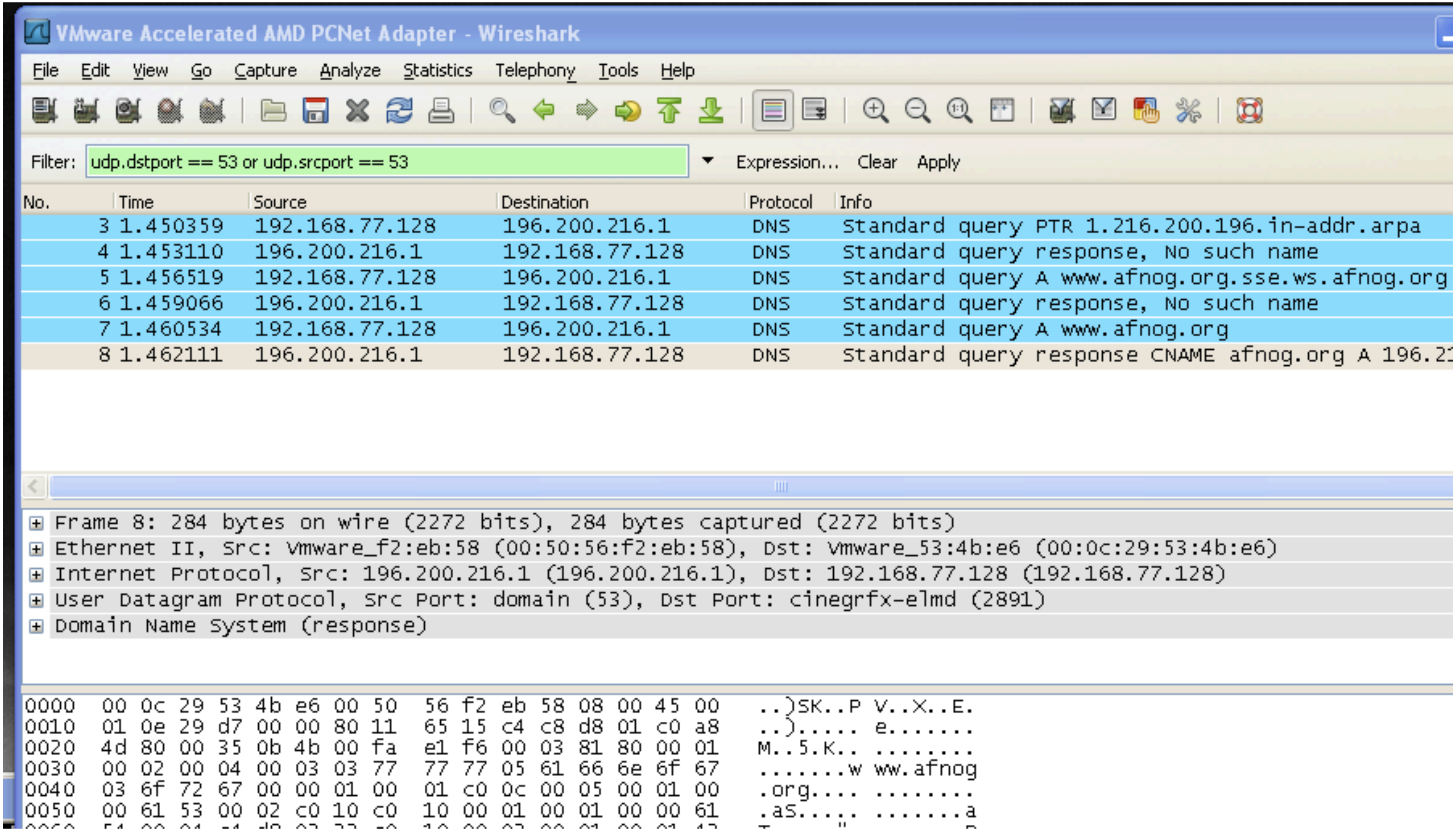


```
NAME
       tshark - Dump and analyze network traffic

SYNOPSIS
       tshark [ -a <capture autostop condition> ] ...
       [ -b <capture ring buffer option>] ...  [ -B <capture buffer size> ]
       [ -c <capture packet count> ] [ -C <configuration profile> ]
       [ -d <layer type>==<selector>,<decode-as protocol> ] [ -D ]
       [ -e <field> ] [ -E <field print option> ] [ -f <capture filter> ]
       [ -F <file format> ] [ -h ] [ -i <capture interface>|- ] [ -I ]
       [ -K <keytab> ] [ -l ] [ -L ] [ -n ] [ -N <name resolving flags> ]
       [ -o <preference setting> ] ...  [ -p ] [ -q ] [ -r <infile> ]
       [ -R <read (display) filter> ] [ -s <capture snaplen> ] [ -S ]
       [ -t ad|a|r|d|dd|e ] [ -T pdml|psml|ps|text|fields ] [ -v ] [ -V ]
       [ -w <outfile>|- ] [ -x ] [ -X <eXtension option>]
       [ -y <capture link type> ] [ -z <statistics> ] [ <capture filter> ]

       tshark -G
       [fields|fields2|fields3|protocols|values|decodes|defaultprefs|currentprefs]
```

Wireshark: the GUI interface


VMware Accelerated AMD PCNet Adapter - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

Filter: udp.dstport == 53 or udp.srcport == 53

```
No.   Time      Source          Destination     Protocol Info
    3 1.450359  192.168.77.128  196.200.216.1   DNS      Standard query PTR 1.216.200.196.in-addr.arpa
    4 1.453110  196.200.216.1   192.168.77.128  DNS      Standard query response, No such name
    5 1.456519  192.168.77.128  196.200.216.1   DNS      Standard query A www.afnog.org.sse.ws.afnog.org
    6 1.459066  196.200.216.1   192.168.77.128  DNS      Standard query response, No such name
    7 1.460534  192.168.77.128  196.200.216.1   DNS      Standard query A www.afnog.org
    8 1.462111  196.200.216.1   192.168.77.128  DNS      Standard query response CNAME afnog.org A 196.2
```

```
⊞ Frame 8: 284 bytes on wire (2272 bits), 284 bytes captured (2272 bits)
⊞ Ethernet II, Src: Vmware_f2:eb:58 (00:50:56:f2:eb:58), Dst: Vmware_53:4b:e6 (00:0c:29:53:4b:e6)
⊞ Internet Protocol, Src: 196.200.216.1 (196.200.216.1), Dst: 192.168.77.128 (192.168.77.128)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: cinegrfx-elmd (2891)
⊞ Domain Name System (response)
```

```
0000  00 0c 29 53 4b e6 00 50  56 f2 eb 58 08 00 45 00   ..)SK..P V..X..E.
0010  01 0e 29 d7 00 00 80 11  65 15 c4 c8 d8 01 c0 a8   ..)..... e.......
0020  4d 80 00 35 0b 4b 00 fa  e1 f6 00 03 81 80 00 01   M..5.K.. ........
0030  00 02 00 04 00 03 03 77  77 77 05 61 66 6e 6f 67   .......w ww.afnog
0040  03 6f 72 67 00 00 01 00  01 c0 0c 00 05 00 01 00   .org.... ........
0050  00 61 53 00 02 c0 10 c0  10 00 01 00 01 00 00 61   .aS..... .......a
```

tshark: examples

- # tshark -D   # show available interfaces
- # tshark -i em0 port 53   # sniff DNS traffic on iface em0
- # tshark -V port 25   # sniff and decode SMTP traffic

WARNING

- Your enterprise or law enforcement may have a strict policies or laws forbidding you from sniffing network traffic
- Your enterprise or law enforcement may have a strict policies or laws forbidding you from scanning the network
- Make absolutely sure you have the authority to conduct these activities **BEFORE** you do them.

tshark exercises

SNORT

- Designed by Marty Roesch in 1998 as a replacement for tcpdump. (He wanted prettier output.)
- It grew into an exception protocol decoding tool, and then a packet matching tool
- Now it's a complete Free/Open Source Intrusion Detection Platform, with a commercial company known as "SourceFire"
- http://www.snort.org/
- http://www.sourcefire.com/

SNORT

- signature-based IDS, therefore you have all the issues about managing signatures that you would with any of these
- there is a large user community that develops new rules for matching new attacks (emergingthreats.net for free, from SourceFire for money)
- there are automated tools for downloading new signature files (oinkmaster, pulledpork)

SNORT

- can be run on the command-line as a packet sniffer, just like **tcpdump** or **tshark**
  - example: snort -dve -i eth1 ...
- the other mode is as an IDS, running as a daemon in the background
- the 2nd mode is also known as "packet logging mode"
  - example: snort -D -b -l /logdir

SNORT
what kind of attacks does it detect?

- match any of the standard IP packet fields: src, dst, src port, dst port
- match contents within the packets
- detect fragmentation attacks
- detect port scanning
- detect chunked HTTP attacks (yes, it can assemble TCP streams)
- and 1000's more...

SNORT: daemon options

```
snort -D -e -i eth1 -c /etc/snort/snort.conf -K ascii -l
/etc/snort/logs -A full -s
```

-D	daemon mode
-e	display link layer / MACs
-i eth1	capture from iface eth1
-c /etc/snort/snort.conf	config file
-K ascii	output ascii files by ip address
-A full	fully decode packet headers
-s	also output to syslog

SNORT configuration

- With so much power, there is a lot of complexity in the configuration
- “snort.conf” contains the directives
- define local network services for reference
- use include statements bring in the rules from the rules directory
- pre-processor section is used to configure that advanced matching pre-processor

SNORT configuration approaches

- if you just plug it in and turn it on, you will get a **HUGE** number of matches and false positive alerts
- the easy way to configure is to reduce the RuleSet down to almost nothing, and then add rules sections one at a time

SNORT
what do I do when I detect an attack?

- it can launch a custom script (or)
- it can begin archiving packets of the attack to disk (or)
- it can notify you via e-mail (or)
- it can even generate responses to the attack

Security Take-Aways

- Good Host Security is hugely beneficial
- OS Updates are critical
- Application Updates are critical as well
- A Vulnerability Scanning regimen is worthwhile
- An Anti-Virus regimen is worthwhile
- Traffic Analysis can be helpful for resolving problems
- The Tools to do this are freely available
- There is no such thing as "perfect" security; be prepared to deal with successful attacks if they happen.