UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

Intrusion Detection Systems

Darren R. Davis
Student Computing Labs

Overview

- Intrusion Detection
  - What is it?
  - Why do I need it?
  - How do I do it?
- Intrusion Detection Software
  - Network based
  - Host based
- Intrusion Prevention

Disclaimer

- Please review your organizations policy on monitoring network traffic!
- Please review any security policies.
- In a public organization such as the University of Utah, there are potential issues if you monitor users activity.
- Possible Privacy Issues!

U of U Network Monitoring

- The U of U has an IT Policy
  - http://www.it.utah.edu/network_monitoring_policy_15Nov01.html
- Colleges and Departments may establish additional policies
- NIDS constitutes network monitoring
- Make sure you have both administrative and network management approval (Policy)

Definitions and Terms

- False Positive
  - A false positive is when your IDS indicates and event occurred when in fact it didn’t.
  - “The boy that cried wolf!”
- False Negative
  - Is when your IDS does not detect attacking activity.
  - “The wolf shows up and the boy is asleep.”

What is Intrusion Detection?

- An Intrusion Detection System (IDS) looks for specific events that indicate a potential attack on a system or network.
- An attack or intrusion is generally associated with events outside the organization.
- Misuse is associated with events within the organization.

IDS Approaches and Types

- There are several approaches
  - Pattern Matching Detection
  - Statistical Anomaly Detection
- There are several types
  - Host Based
  - Network Based

Pattern Matching Detection

- Looks for specific events
  - Like did my host log file record an attempt to log in as root?
  - Did my network IDS see mapping attempts occur?
  - If you match the pattern or sets of events, then indicate an attack.
  - Problem is there can be false positives.

UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

Statistical Anomaly Detection

- Applies heuristics to the problem
  - Basically the system tries to determine “normal” activity and if something out of ordinary occurs then indicate an attack.
  - This is an attempt to minimize false positives.
  - This type still has issues like determining what is normal or not normal activity.

Host Based IDS

- Examine System Logs
  - syslog
- Examine Filesystem
  - File integrity or “Finger Printing”
- Examine System Process Execution
  - Watch Networking Stack
  - TCPWrappers
  - Process Accounting

Network Based IDS or NIDS

- Examine Network Traffic
  - Network “sniffing”
  - Pattern match network packets
  - Watch network flows

Do I Need Intrusion Detection?

- The simple answer is yes!
  - You will need to determine to what degree
- Threats will exist in any organization. Vulnerabilities will always exist and you need a way to determine if someone is examining your systems for potential weaknesses.
- Ignorance is not bliss

How Do I Detect Intrusions?

- What is effective?
  - Collection of Host and Network based
- Various collection of software packages both commercial and open source.

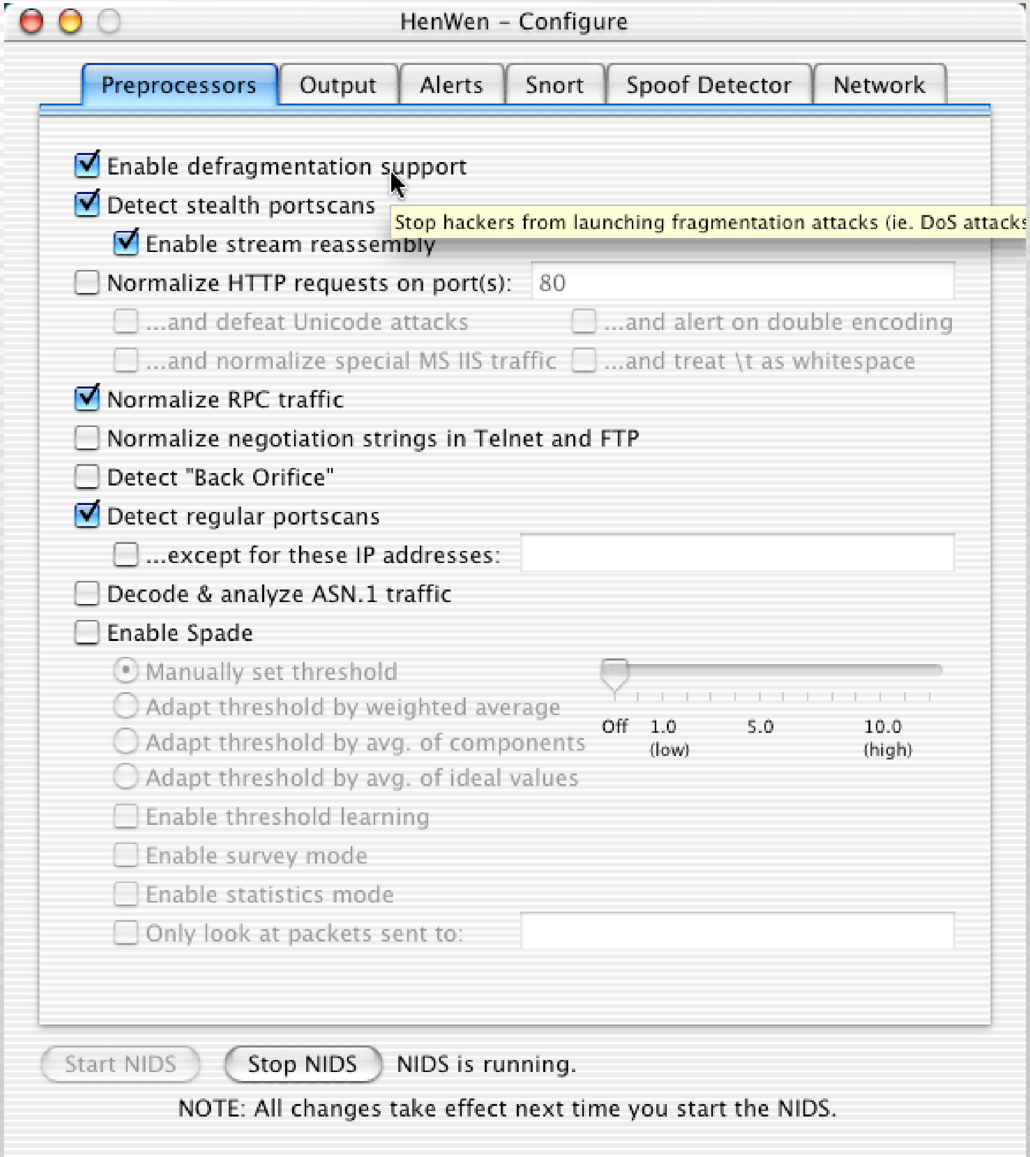
Host Based

- Will be covered in future meetings
  - File Integrity or “Finger Printing”
    - Tripwire
    - Radmind
  - Log file scanning
  - Network Port Watching
    - TCPWrappers
  - Other approaches

Network Based

- This meeting will focus on Snort using HenWen.
- HenWen is a Mac OS X GUI front end for Snort.
- Snort works on a pattern matching approach.

HenWen



☑ Enable defragmentation support

Stop hackers from launching fragmentation attacks (ie. DoS attacks

☑ Detect stealth portscans

☑ Enable stream reassembly

☐ Normalize HTTP requests on port(s): 80

☐ ...and defeat Unicode attacks ☐ ...and alert on double encoding

☐ ...and normalize special MS IIS traffic ☐ ...and treat \t as whitespace

☑ Normalize RPC traffic

☐ Normalize negotiation strings in Telnet and FTP

☐ Detect "Back Orifice"

☑ Detect regular portscans

☐ ...except for these IP addresses:

☐ Decode & analyze ASN.1 traffic

☐ Enable Spade

● Manually set threshold

○ Adapt threshold by weighted average

○ Adapt threshold by avg. of components

○ Adapt threshold by avg. of ideal values

☐ Enable threshold learning

☐ Enable survey mode

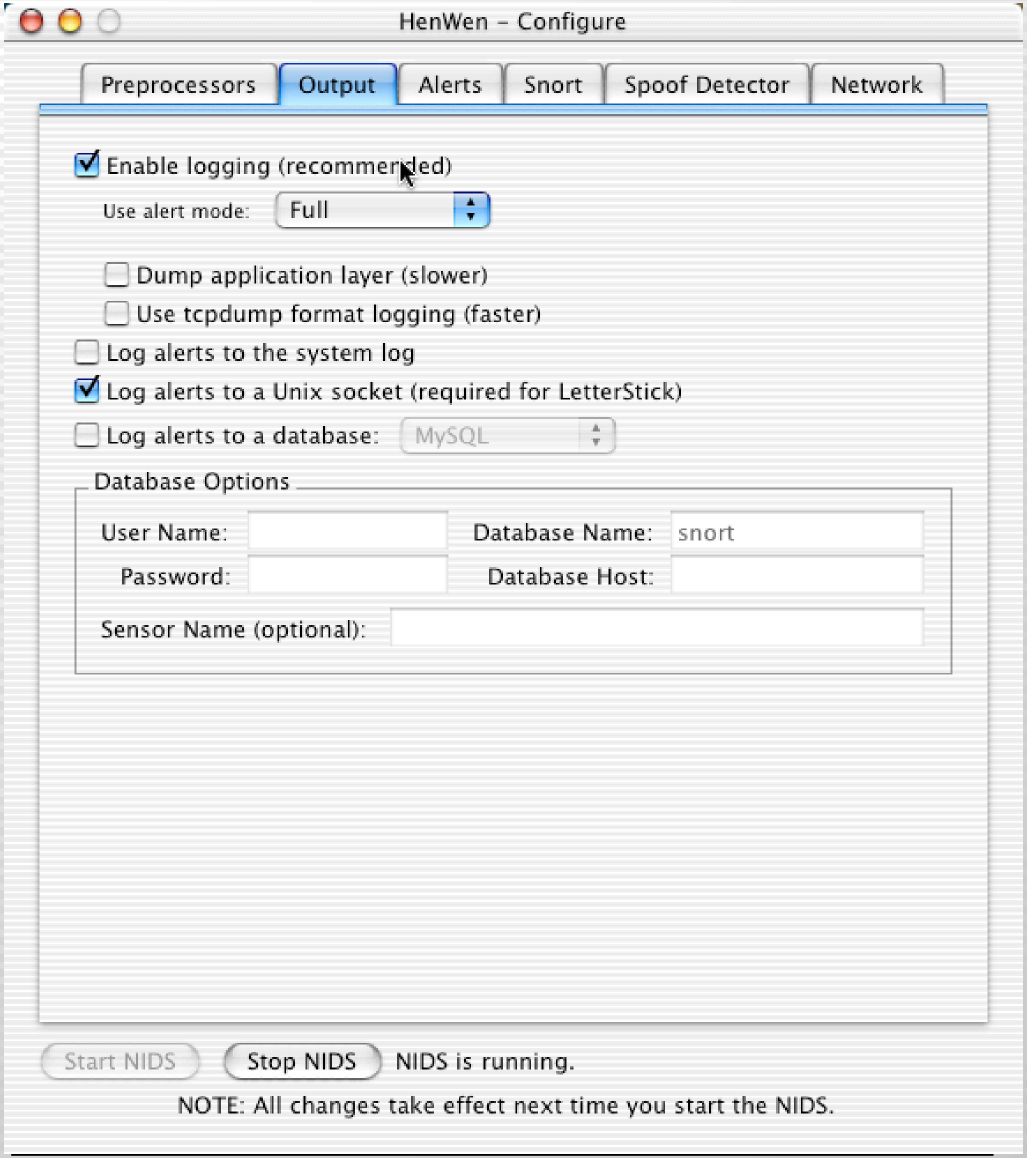
☐ Enable statistics mode

☐ Only look at packets sent to:

NIDS is running.

NOTE: All changes take effect next time you start the NIDS.

HenWen



☑ Enable logging (recommended)

Use alert mode: Full

□ Dump application layer (slower)

□ Use tcpdump format logging (faster)

□ Log alerts to the system log

☑ Log alerts to a Unix socket (required for LetterStick)

□ Log alerts to a database: MySQL

Database Options

User Name:

Database Name: snort

Password:

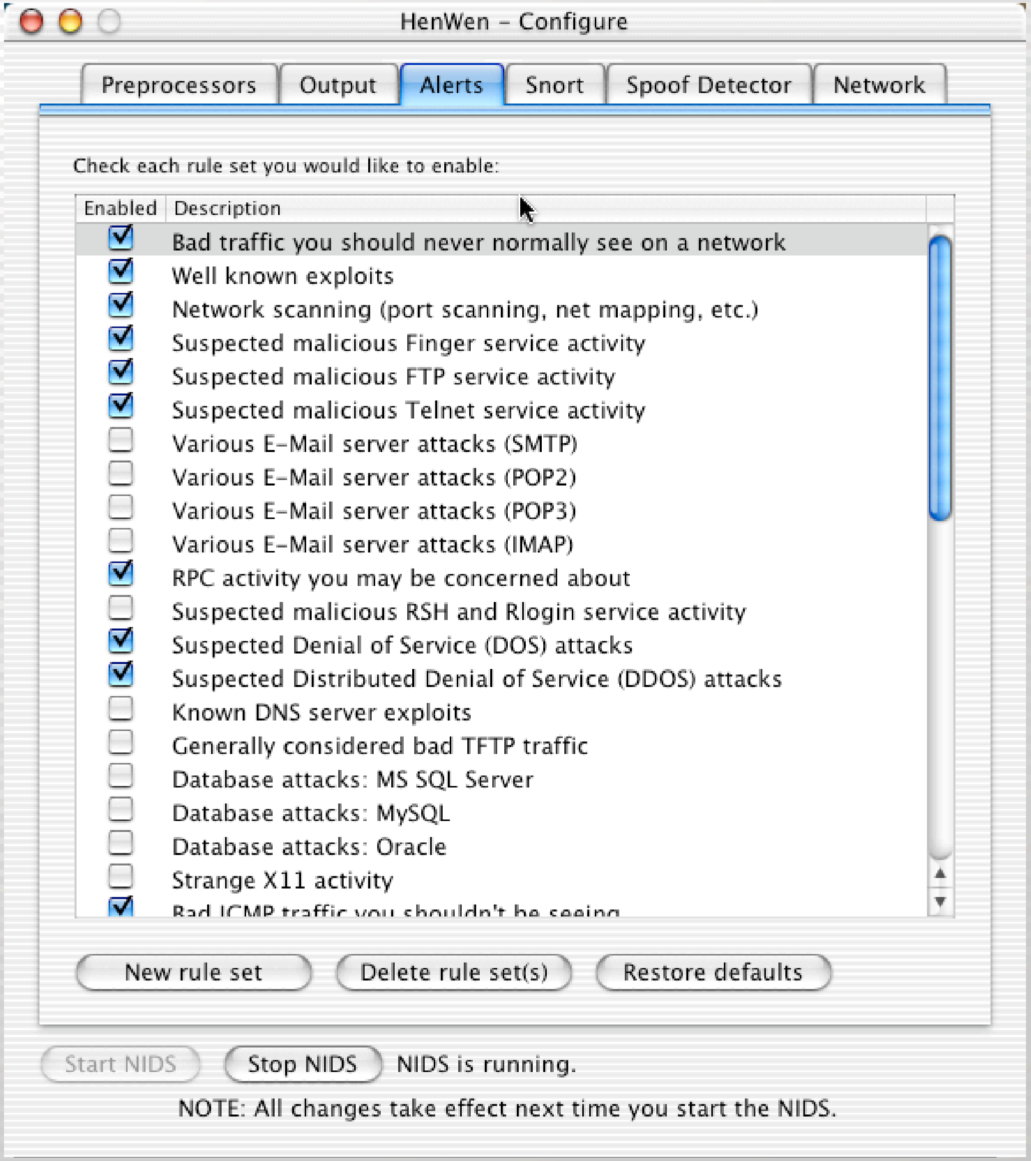
Database Host:

Sensor Name (optional):

NIDS is running.

NOTE: All changes take effect next time you start the NIDS.

HenWen



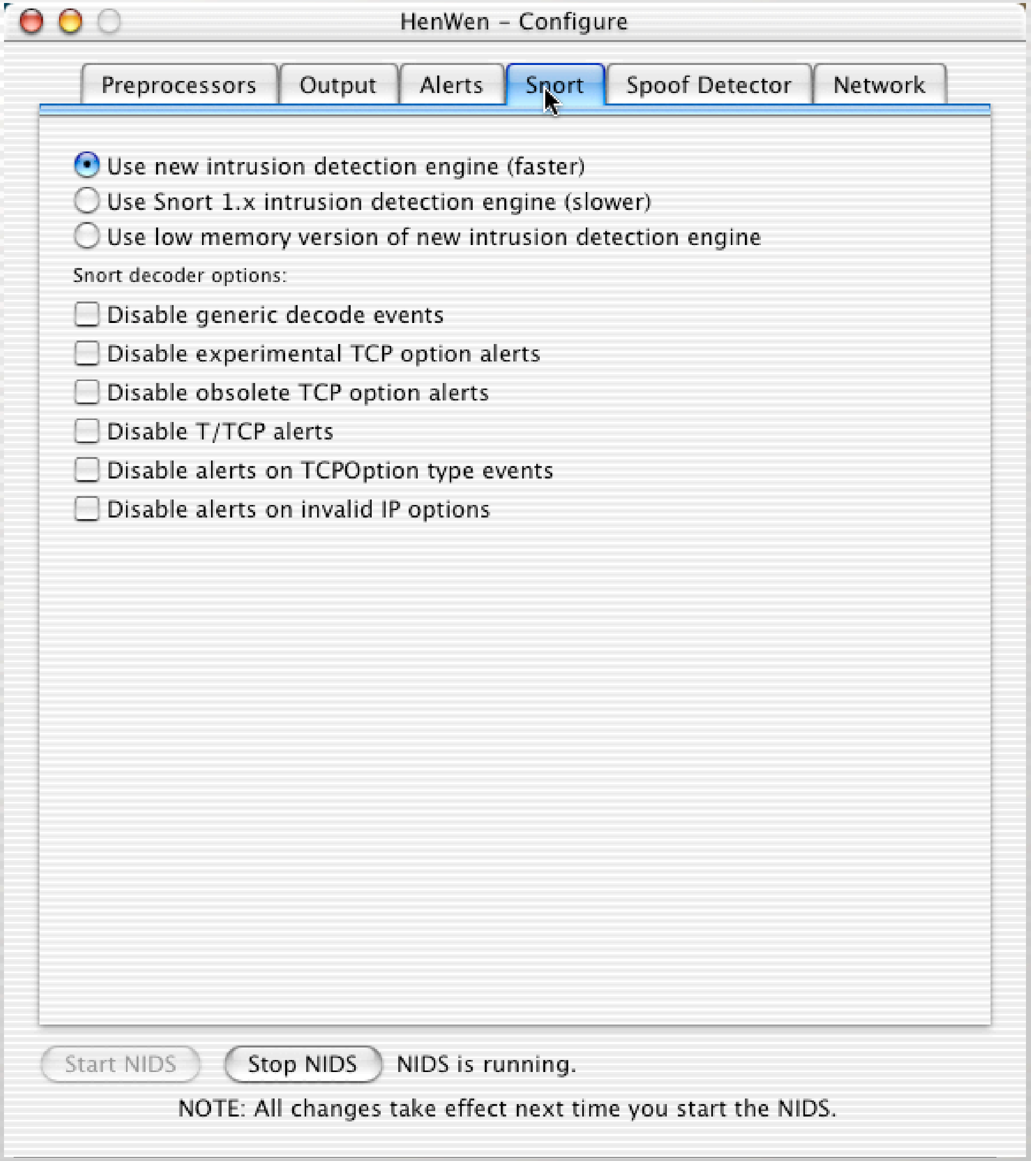
Check each rule set you would like to enable:

Enabled	Description
☑	Bad traffic you should never normally see on a network
☑	Well known exploits
☑	Network scanning (port scanning, net mapping, etc.)
☑	Suspected malicious Finger service activity
☑	Suspected malicious FTP service activity
☑	Suspected malicious Telnet service activity
☐	Various E-Mail server attacks (SMTP)
☐	Various E-Mail server attacks (POP2)
☐	Various E-Mail server attacks (POP3)
☐	Various E-Mail server attacks (IMAP)
☑	RPC activity you may be concerned about
☐	Suspected malicious RSH and Rlogin service activity
☑	Suspected Denial of Service (DOS) attacks
☑	Suspected Distributed Denial of Service (DDOS) attacks
☐	Known DNS server exploits
☐	Generally considered bad TFTP traffic
☐	Database attacks: MS SQL Server
☐	Database attacks: MySQL
☐	Database attacks: Oracle
☐	Strange X11 activity
☑	Bad ICMP traffic you shouldn't be seeing

NIDS is running.

NOTE: All changes take effect next time you start the NIDS.

HenWen



● Use new intrusion detection engine (faster)
○ Use Snort 1.x intrusion detection engine (slower)
○ Use low memory version of new intrusion detection engine

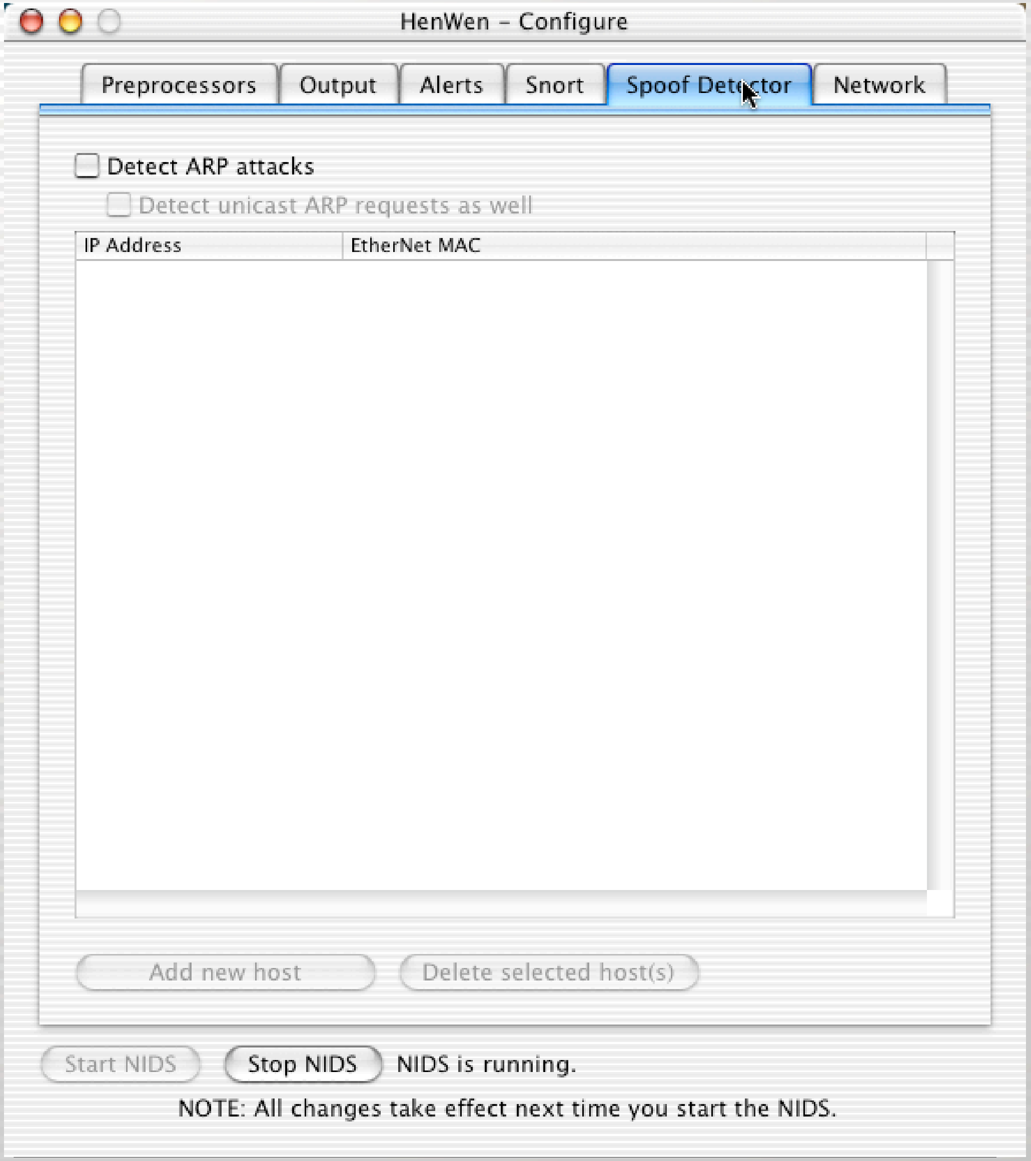
Snort decoder options:

- □ Disable generic decode events
- □ Disable experimental TCP option alerts
- □ Disable obsolete TCP option alerts
- □ Disable T/TCP alerts
- □ Disable alerts on TCPOption type events
- □ Disable alerts on invalid IP options

NIDS is running.

NOTE: All changes take effect next time you start the NIDS.

HenWen



HenWen – Configure

□ Detect ARP attacks

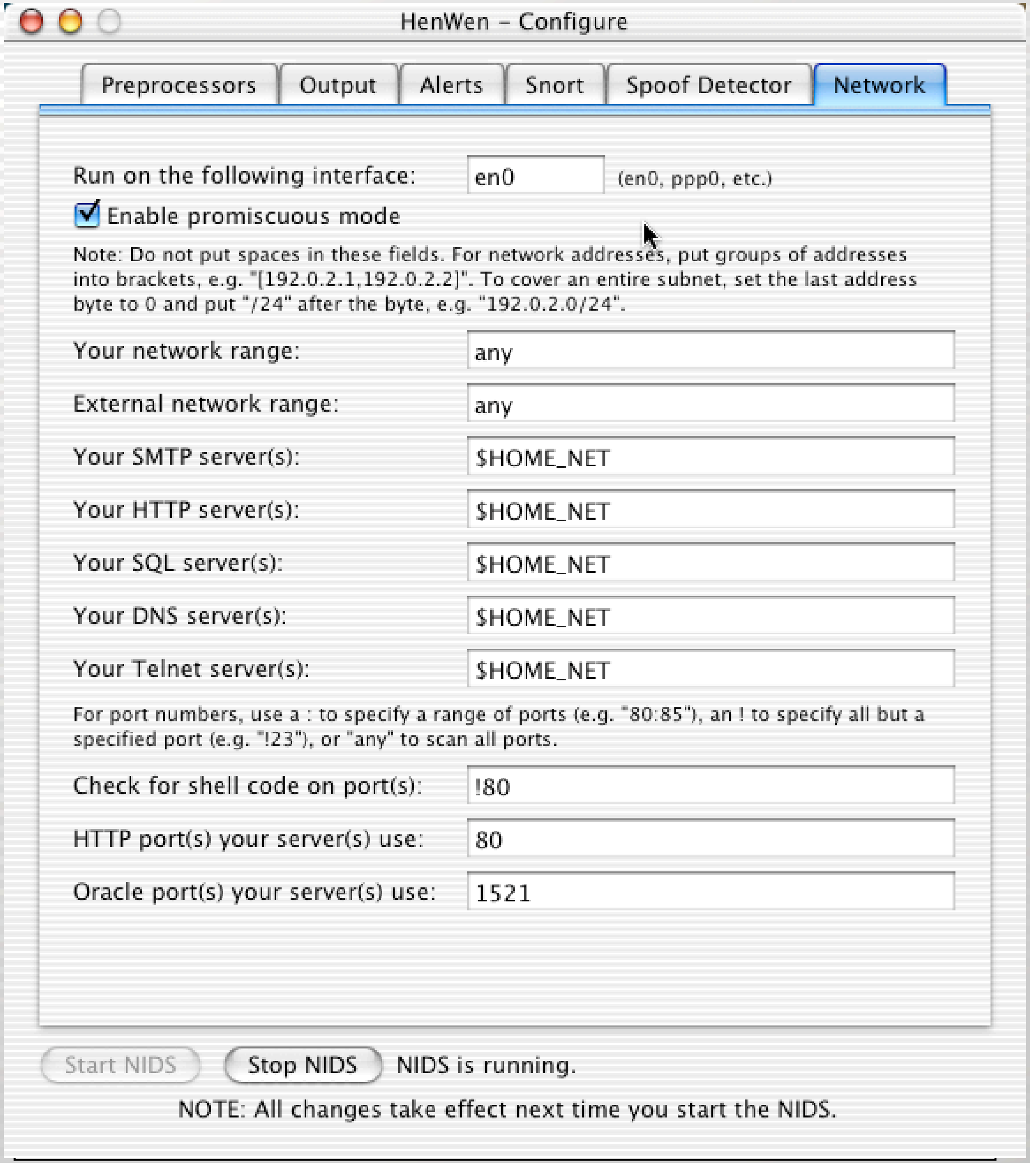
□ Detect unicast ARP requests as well

IP Address	EtherNet MAC

NIDS is running.

NOTE: All changes take effect next time you start the NIDS.

HenWen



Run on the following interface: en0 (en0, ppp0, etc.)

☑ Enable promiscuous mode

Note: Do not put spaces in these fields. For network addresses, put groups of addresses into brackets, e.g. "[192.0.2.1,192.0.2.2]". To cover an entire subnet, set the last address byte to 0 and put "/24" after the byte, e.g. "192.0.2.0/24".

Your network range: any

External network range: any

Your SMTP server(s): $HOME_NET

Your HTTP server(s): $HOME_NET

Your SQL server(s): $HOME_NET

Your DNS server(s): $HOME_NET

Your Telnet server(s): $HOME_NET

For port numbers, use a : to specify a range of ports (e.g. "80:85"), an ! to specify all but a specified port (e.g. "!23"), or "any" to scan all ports.

Check for shell code on port(s): !80

HTTP port(s) your server(s) use: 80

Oracle port(s) your server(s) use: 1521

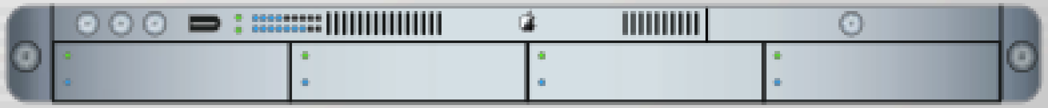
NIDS is running.

NOTE: All changes take effect next time you start the NIDS.

/var/log/snort/alert

```
[**] [100:2:1] spp_portscan: portscan status from 218.73.229.61: 7 connections across 7 hosts: TCP(7), UDP(0) [**]
05/24-05:17:31.219371

[**] [100:3:1] spp_portscan: End of portscan from 218.73.229.61: TOTAL time(1s) hosts(7) TCP(7) UDP(0) [**]
05/24-06:03:36.543659

[**] [100:1:1] spp_portscan: PORTSCAN DETECTED from 172.198.99.217 (THRESHOLD 4 connections exceeded in 2 seconds) [**]
05/24-14:19:05.212321

[**] [100:2:1] spp_portscan: portscan status from 172.198.99.217: 6 connections across 6 hosts: TCP(6), UDP(0) [**]
05/24-14:35:48.829367

[**] [100:3:1] spp_portscan: End of portscan from 172.198.99.217: TOTAL time(2s) hosts(6) TCP(6) UDP(0) [**]
05/24-14:43:58.893324

[**] [100:1:1] spp_portscan: PORTSCAN DETECTED from 193.252.170.79 (THRESHOLD 4 connections exceeded in 2 seconds) [**]
05/26-12:07:43.622195

[**] [100:2:1] spp_portscan: portscan status from 193.252.170.79: 7 connections across 7 hosts: TCP(7), UDP(0) [**]
05/26-12:07:47.623947

[**] [100:2:1] spp_portscan: portscan status from 193.252.170.79: 1 connections across 1 hosts: TCP(1), UDP(0) [**]
05/26-12:54:20.594093

[**] [100:3:1] spp_portscan: End of portscan from 193.252.170.79: TOTAL time(6s) hosts(7) TCP(8) UDP(0) [**]
05/26-15:23:23.095528
```

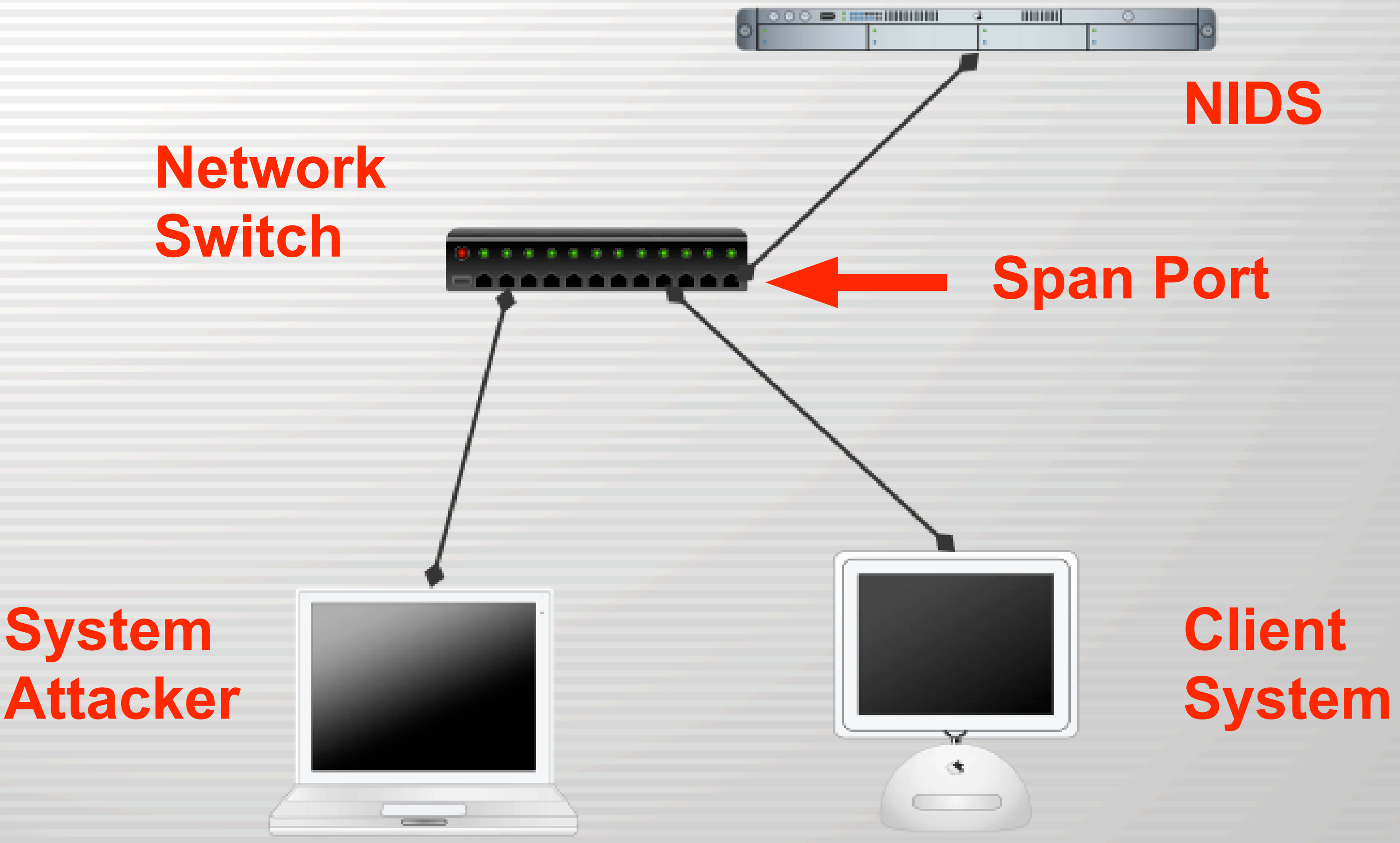
Demonstration



NIDS in a Switched Network

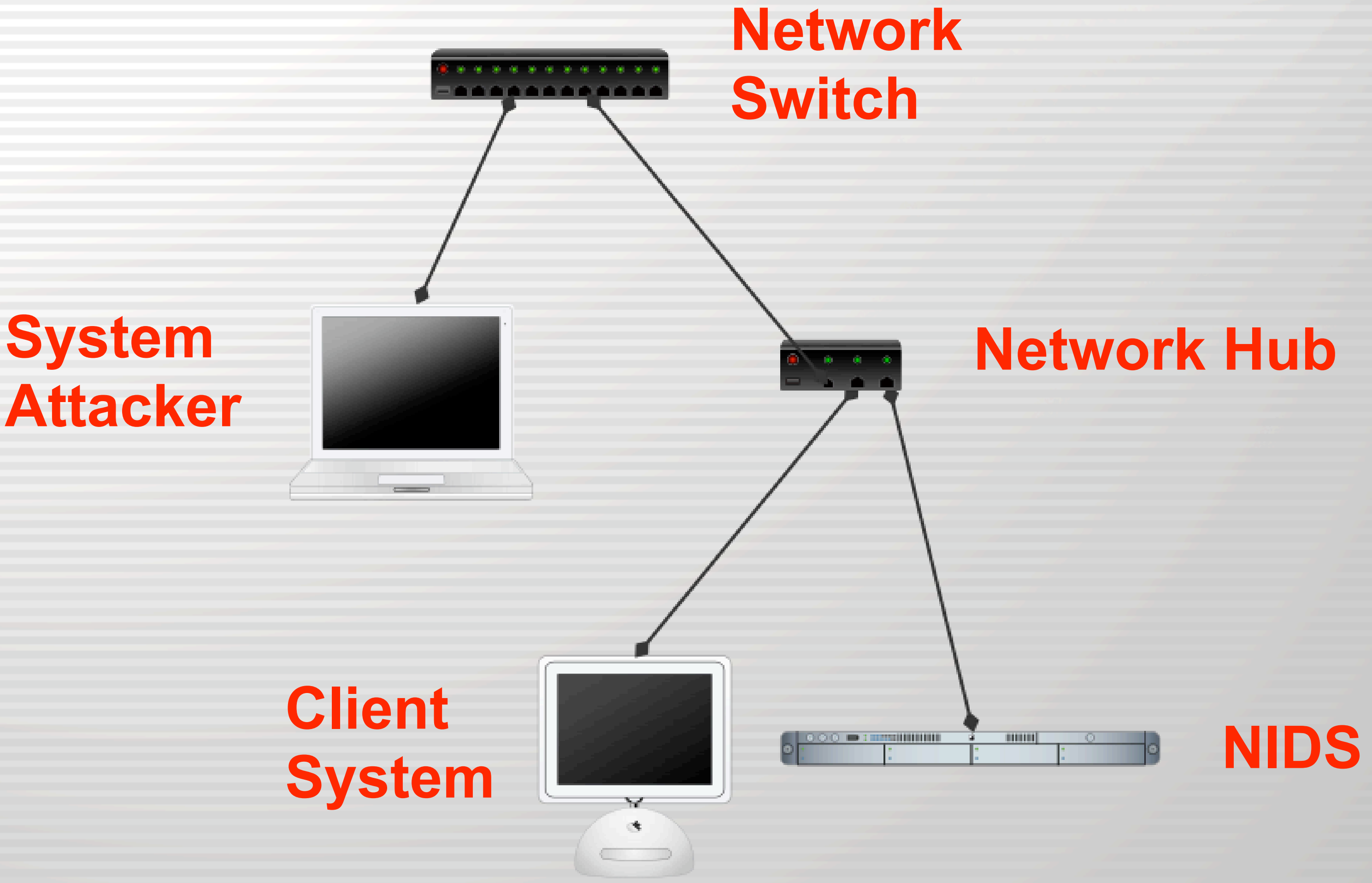
- A Switched Network poses some technical hurdles that you must overcome.
- You need to put the NIDS in a location on your network where it can monitor the traffic you are concerned about.

Span Port



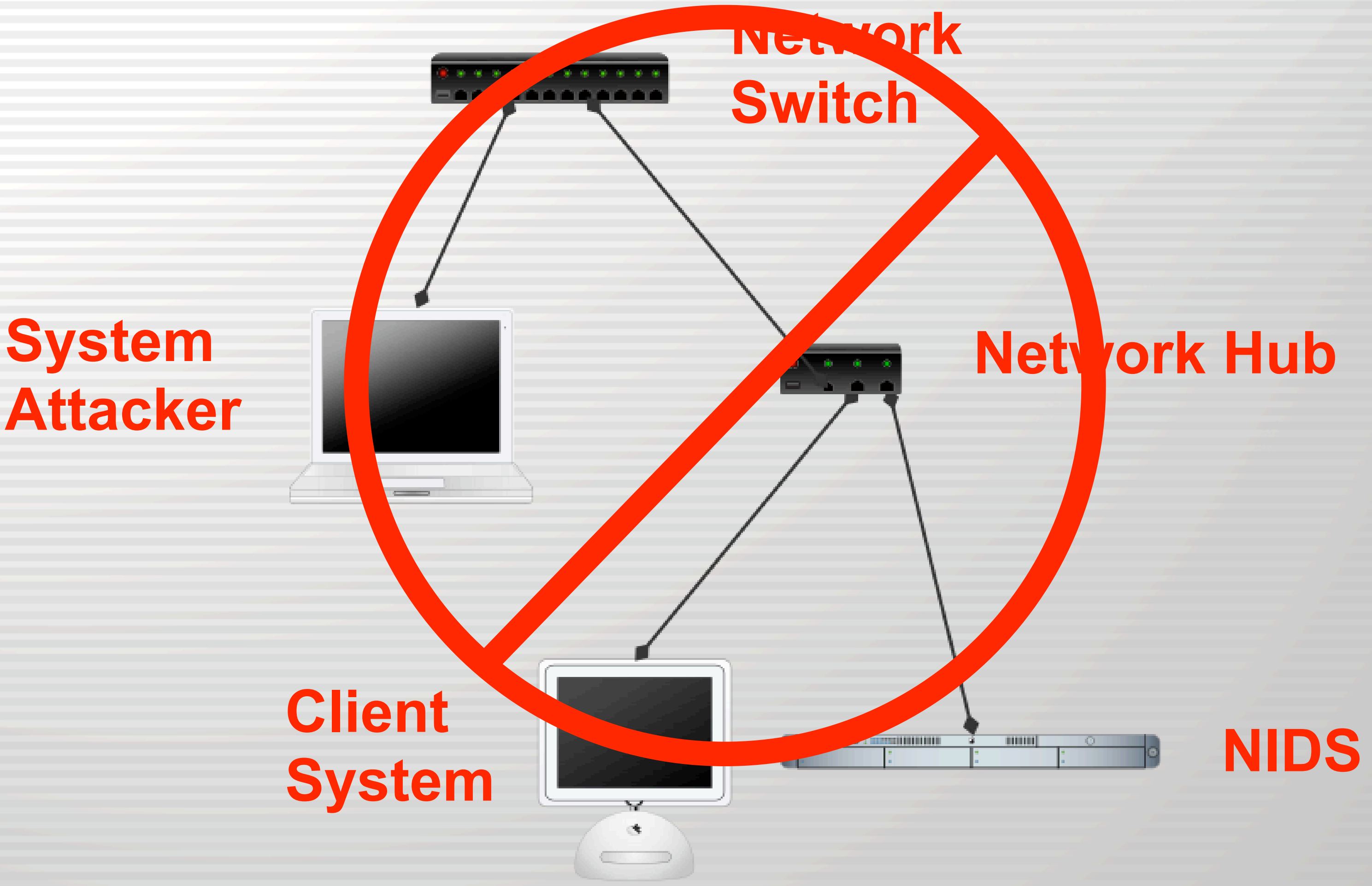
UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

Using a Hub



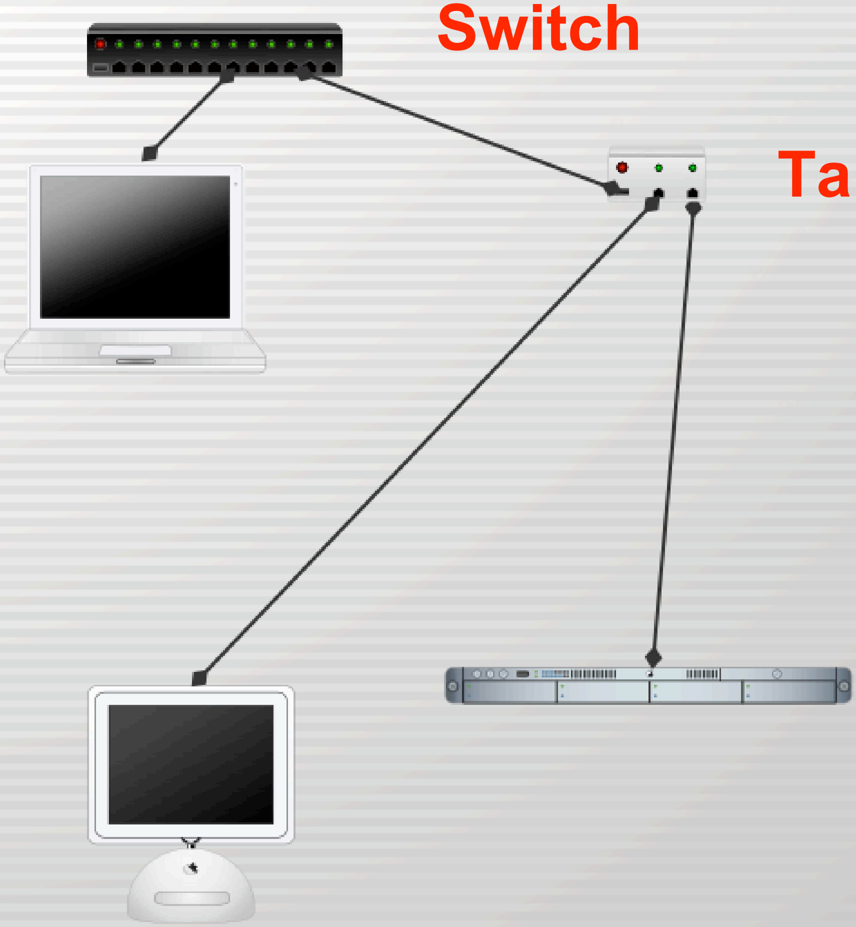
UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

Using a Hub



UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

Network Taps



Network Switch

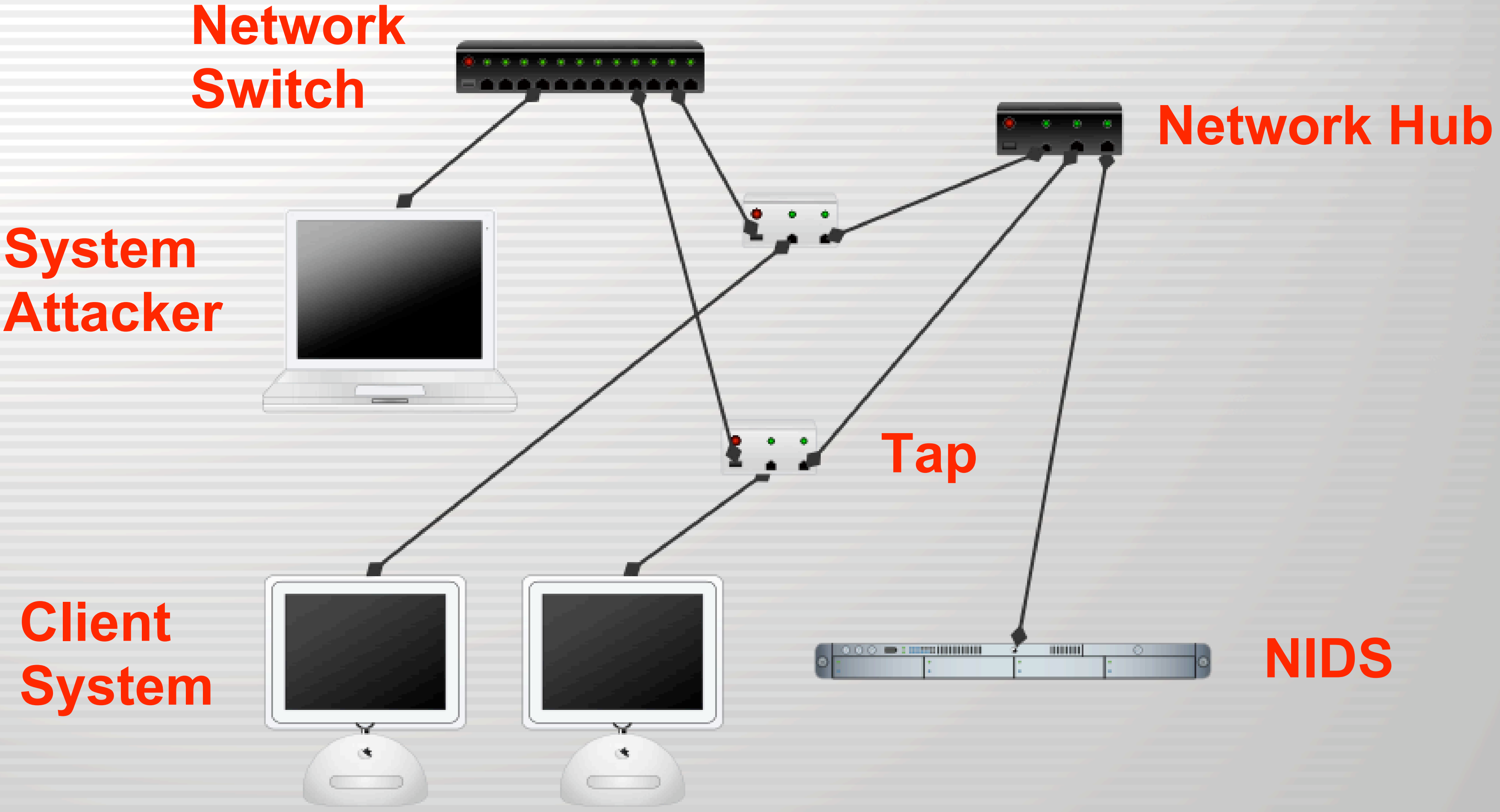
System Attacker

Tap

NIDS

Client System

Multiple Network Taps



Network Switch

Network Hub

System Attacker

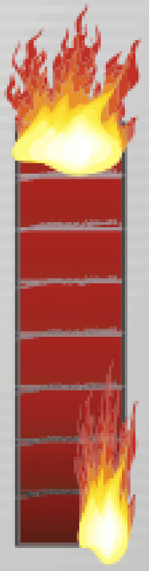
Tap

Client System

NIDS

Intrusion Prevention

- Intrusion detection is generally separated from intrusion prevention.
- Intrusion Prevention includes
  - Firewalls
  - Network port security
  - Systrace (process jail)
  - Basically keeping attackers out



Honeypots

- Honeypots are systems that are made to look like real systems or network services but used to monitor attacker activity.
- Can be used as an advanced warning while you gather intelligence about the attacker to ward off an attack.

Common Questions

- Hopefully this will answer some of the common questions asked.

?

I have a firewall, why do I care?

- Just by keeping people out (Intrusion Prevention) does not mean you are not at risk.
- The attackers may already be inside.
- If you don’t know that attacks are being attempted, what do you do the day a new exploit is available and they compromise your machines?

Aren’t MAC addresses unique?

- What about using MAC address to trace an attacker?
  - MAC addresses get replaced by gateways, so you can only trace back to the gateway
  - Some gateways have extensive logging
  - Some systems like Linux allow administrators to change MAC addresses

Aren’t switched networks secure?

- More secure than non-switched networks, but still vulnerable.
  - ARP Spoofing
  - MAC Flooding
  - MAC Duplicating
- See SANS report on why your switched network isn’t secure

OK, my IDS gives me an alert!

- Now what?
  - Security policy and incident handling
    - SANS a good source of information
  - Record and retain log information
  - University of Utah
    - Contact Institutional Security Office (ISO)
    - http://iso.utah.edu/

Do I worry about mapping?

- When you install a NIDS you may see port scanning activity (mapping), do you worry about it?
- Well, if you saw someone walking through your neighborhood checking to see if doors are locked do you worry?

Can my NIDS keep up?

- In some networking environments you may have more network traffic (packets) than your NIDS can sort through.
- May need multiple NIDS to monitor groups of machines.

Things to Remember

- Attackers will most likely try and gain information about your network (mapping and reconnaissance)
- Your NIDS could be targeted or used to gather intelligence by attackers
  - Encrypt data whenever possible like between agent and monitor or if you remote syslog (use secure syslog).

More Things to Remember

- There are limitations to your IDS or NIDS, know them!
- Keep software current. Both for the systems you are trying to protect as well as your monitoring and server infrastructure.

Resources

- SANS Institute
  - http://www.sans.org/resources/idfaq
- Snort or HenWen
  - http://www.snort.org/
  - http://home.attbi.com/~dreamless/
- Top 75 Security Tools
  - http://www.insecure.org/tools.html

Resources

- Systrace
  - http://www.citi.umich.edu/u/provos/systrace

Questions and Answers

?