

Class Six

Topics:

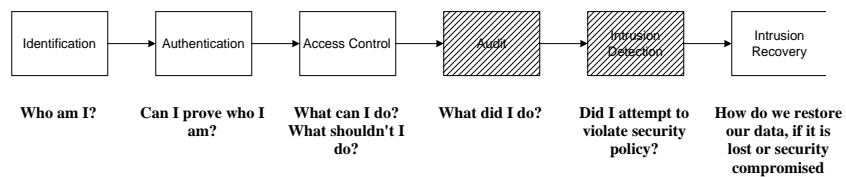
- **Event Auditing**
 - Host auditing in different systems
 - Log analysis
 - Intrusion Detection
 - Honeypots
- **Processor Hardware & Operating System Security**
 - OS & Processor Security Features
 - Reference Monitors & Security Kernels
 - The Trusted Computing Base
 - Hardware Protections
- **Extra: Installing the snort Intrusion Detection System on Windows XP**

8/24/2007

Class 6

1

The Security Transaction Lifecycle and Audit



8/24/2007

Class 6

2

Audit of User Actions and System Changes

- Who did what?
- Emphasis on **accountability** for system command execution (use of operating system services)
- Areas of concern:
 - Valid access attempts, and invalid attempts (password not valid)
 - Valid function performed, for specific sensitive functions (e.g. accesses to classified data, etc.)
 - Functions attempted but denied due to improper authority
 - All commands executed by powerful users (security administrators)
- Evidence of these activities is written to a protected data store, called an audit log

8/24/2007

Class 6

3

Log analysis/reduction

- Audit logs usually end up with very large numbers of events
- Audit logs must be searched for events of interest and summarized to view trends.
- Log analysis and reduction tools can assist:
 - Databases
 - Network event monitoring tools (MRTG, Cricket, etc.)
 - Scripts
 - Commercial products (Sawmill, etc.)
- See <http://www.loganalysis.org> for more information

8/24/2007

Class 6

4

Centralized Log Management

- Audit logs may be maintained on the device itself or may be sent to a central log server
- Syslog is the service usually used for sending log data to a server
- Ideally, the log server will provide intrusion forensics that can stand up in court
 - Server is secured and tamper-resistant
 - Consistent time stamps throughout the network (NTP)
- Can correlate logs from different servers, trace potential intrusions (and other anomalies) throughout the network:
 - Firewall logs
 - Web server logs
 - Router logs
 - DNS, mail, etc.
- Beware of what systems DON'T log! This may not be documented!

8/24/2007

Class 6

5

Intrusion Detection - Advanced Audit of Security Relevant Events

- Attempt to detect patterns in system use, to distinguish “normal” use from “malicious” use
- May look for:
 - Anomalies, any deviation from “normal” use
 - Misuse, patterns specific to “hacking” attempts
- Anomaly detection:
 - May use statistical or neural network methods of analysis
 - Requires determining a baseline of “normal” behavior
- Misuse detection:
 - Requires a database of “attack signatures”
 - Must be able to detect minor variations on a known signature
 - Success is correlated to completeness and currency of signature database

8/24/2007

Class 6

6

Intrusion Detection - Advanced Audit of Security Relevant Events

- Network vs. Host-based Intrusion Detection
 - Network – a “tap” observes network traffic on a subnet, independent of any system on the network
 - Host-based – Collect host audit records and forward them to an analytic engine
- All products require skilled analyst and the ability to distinguish false from real results
- See <http://www.acm.org/crossroads/xrds2-4/intrus.html> for an introduction
- Stephen Northcutt’s book **Network Intrusion Detection: An Analyst’s Handbook** is excellent reading.

8/24/2007

Class 6

7

Honeypots

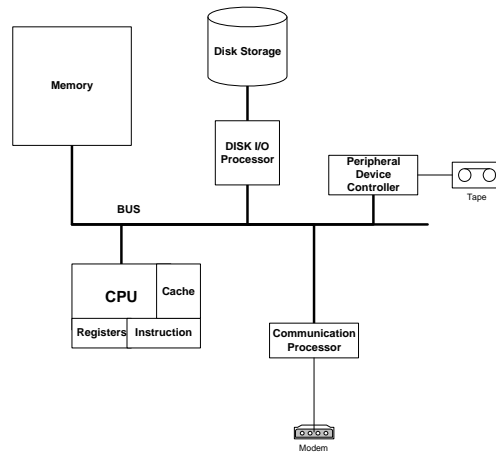
- “A host or network with known vulnerabilities deliberately exposed to a public network. Honeypots are useful in studying attackers' behavior and also in drawing attention away from other potential targets”
from: <http://www.nwfusion.com/techinsider/2002/0624security2.html>
- May run a simulated server environment, giving reasonable-looking responses without providing any real services
- May exist on unadvertised IP address, hence any access is by definition not authorized
- Used for:
 - Research, trends, finding new unpublicized exploits
 - Gathering evidence
 - Slowing down intruders (works for spam emailers). See “La Brea” at <http://lrp.steinkuehler.net/Packages/LaBrea.htm>

8/24/2007

Class 6

8

Computer Hardware Overview



8/24/2007

Class 6

9

What Does an Operating System Do?

- Provides a command interface (a "shell") to the user
- Manages hardware resources:
 - Processor
 - Memory
 - Disk
 - Other devices
- Manages processes, tasks, and users
- Provides program interfaces (APIs) to permit application software to use hardware resources

8/24/2007

Class 6

10

Features of Modern Operating Systems

- Multiuser, multiprogramming
 - More than one process at a time
 - More than one user at a time
- Memory management, sharing, and protection
 - Assign specific processes and users to their own memory addresses
- Preemptive multitasking
 - CPU switches rapidly between various processes and tasks
 - The Operating System and not the process or task determines when the switching will occur
- Access controls
 - Define and enforce rules permitting or prohibiting access to resources by different tasks, processes, or users

8/24/2007

Class 6

11

How should an Operating System Protect Security

- By protecting its own executable code from illicit modification
- By preventing modification or viewing of its own private memory areas
- By protecting users' private memory areas from other users
- By enforcing system security rules, and preventing the unauthorized bypassing of these rules

Application software should use and not hinder operating system and hardware security features

8/24/2007

Class 6

12

Command Interpreter Security Issues

- Illicit shell meta-characters
 - Get a script that invokes a shell to execute something of your choosing
 - Example: entering the following may cause a poorly coded cgi to display a password file:

```
http://your.host/cgi-bin/cgiipgm?%0Acat%20/etc/passwd
```

Where %0A is a newline character and %20 is a blank space
- Directory traversal
 - “Walking” a Web application out of its root directory so as to access unauthorized files.
 - Example: entering the following to a poorly coded Web application:

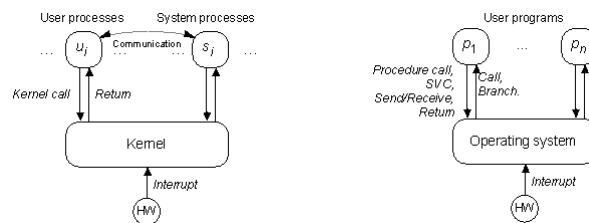
```
../../../../../../../../../../../../etc/passwd
```

8/24/2007

Class 6

13

Kernel vs. Monolithic Operating Systems



8/24/2007

Class 6

14

How the Operating System Works - Memory Management

- Virtual Memory
 - Treats disk space as addressable main memory
 - Pages or segments stored in virtual memory may "really" be on disk or in real memory
 - A process requesting a page or segment not in real memory generates a **page fault**, a processor interrupt which reads the page/segment from disk and moves it into real memory
 - Some function in the hardware or operating system handles converting virtual addresses to real hardware addresses

8/24/2007

Class 6

15

Memory Management Security Issues

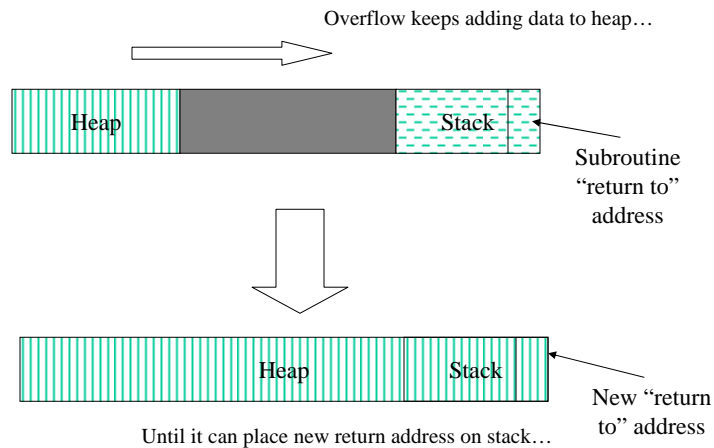
- Real Memory Protection
 - Mechanisms to prevent a process from accessing memory not belonging to it (either operating system memory or another user's process)
- Page File Protection
 - Sensitive information may be stored on disk as part of virtual memory management.
 - Entire processes (including their memory space) may be swapped out to disk, if they are inactive (waiting for input/output)
 - Page files and swap files may be reviewed after the fact for passwords, cryptographic keys, and other sensitive information
 - ISSUE: Object Reuse (different process uses same memory object)
- Buffer overflows
 - "Stuffing" more information into buffer storage areas may cause it to overrun into other areas of storage (including areas containing executable code)
 - "Heap" overflows "Stack". "Stack" contains program counter (address of next executable instruction)
 - A carefully crafted buffer overflow can cause systems to execute arbitrary code

8/24/2007

Class 6

16

Buffer Overflow Illustrated



8/24/2007

Class 6

17

Process Timing

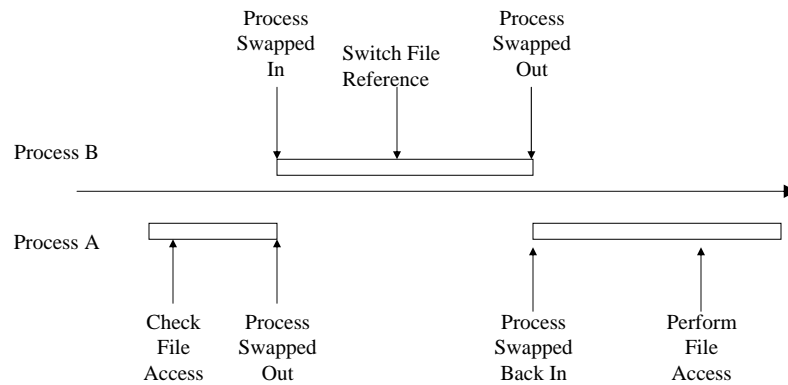
- In a multiprogramming, multiuser environment, instruction execution timing is unpredictable
 - A process may be interrupted at any time
 - Between any two steps in a process, some other process may "cut in line" for an unknown amount of time
 - If this other process can tamper with security-relevant values or settings, security can be compromised this way.
 - These attacks are a game of odds. You need to get the timing just right. Computers are very patient and will keep trying until they succeed
- Security Concerns
 - TOCTTOU
 - Race Conditions

8/24/2007

Class 6

18

Timing Exploits Illustrated



8/24/2007

Class 6

19

Security Kernels

- A design concept for secure operating systems
- Definition
 - Mediates all subject/object access
 - Central point which manages all security
 - Enforces capabilities and reference validation
 - An implementation of the Security Kernel Concept
- Characteristics
 - Tamper proof
 - Bypass proof
 - Assurance of correct functioning
 - Fault tolerant
 - Interface with and fullest use of hardware protections
 - Simplicity

8/24/2007

Class 6

20

Security Kernels

- Advantages
 - Separates security functions from others
 - Keeps security-relevant functions together
 - Facilitates security verification and testing
- Issues
 - System Performance
 - Security kernel may become large, hence harder to manage

8/24/2007

Class 6

21

Hardware Protections

- “Built into” the silicon
- Part of chip’s instruction set
- Helps operating system reliably implement security protections
 - Process Privilege
 - Timing
 - Memory protection

8/24/2007

Class 6

22

Execution Domains - Controlling access to privileged machine instructions

- Simplest case - 2 domains
 - User
 - System or kernel
- Multi-domain architectures are called "ring" architectures
 - Inside ring (ring 0) is most privileged, can execute all machine instructions and can access all memory and device addresses
 - Each ring has full rights to the resources of the rings outside of it
 - A ring can only access the ring inside of it in a highly controlled fashion, through "gates"
 - Rings define scope of control, inner rings have broader scope of control than outer rings
 - Bits associated with a process determine its ring
 - Bits associated with a resource determine the least privileged ring which can access it

8/24/2007

Class 6

23

Memory Protection - Controlling access to real memory

- Protect processes from each other
- Protect security critical code
- How?
 - Bounds registers
 - Tag bits
 - Access keys (associated with pages in real memory)
 - Descriptor-based address translation (associated with process are the access rights to a physical address)

8/24/2007

Class 6

24

Timing Protections

- Preventing a security-critical operation from being interrupted:
 - Uninterruptible instructions
 - Ability to turn on or turn off external interrupts
- Interrupting or blocking normal process swapping can be very expensive – hence the best timing protection is to not write software vulnerable to these attacks.

8/24/2007

Class 6

25

Hardware Architecture - Intel Pentium

- Intel-based x386 processors have a 4 ring architecture. Procedures calls between rings are protected.
 - Calls to another ring can only be done in protected mode, not real or 8086 mode
 - Call must be made through a call gate descriptor (can't call to an arbitrary location in a more privileged process)
 - Process executing the call must have proper access rights, else a hardware exception results

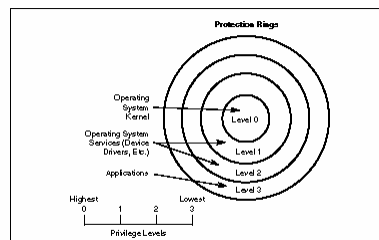


Figure 4-3. Protection Rings

8/24/2007

Class 6

26

Operating System Architecture - Windows NT

- Uses a kernel and user mode
- Only the NT Executive runs in kernel mode
- Environment Subsystems and all user applications run in user mode
- User mode applications can only access addresses in their own 32-bit space For example, user applications can't communicate directly with the Hardware Abstraction Layer, all such communication must be mediated through the NT Executive
- Kernel functions (part of the NT Executive) include:
 - Process dispatch and scheduling
 - Handling interrupts for physical devices
 - Handling processor exceptions (such as divide by zero)
 - Handling power failure recovery

8/24/2007

Class 6

27

Operating System Architecture - Windows NT

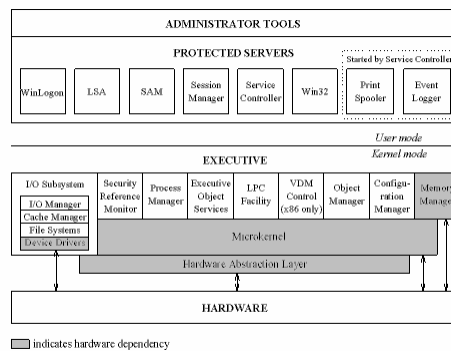


Figure 2-1. Windows NT System Overview

8/24/2007

Class 6

28

Operating System and Hardware Security Features

- Least privilege (for processes)
- Fail safe- access based on permission rather than exclusion
- Simplicity or economy of mechanism
- Continuous protection
- Extensibility and modularity
- Layering, abstraction, data hiding (downward dependence - reveal to upper layers only what they need to know)
- TCB minimization (minimize security-critical code size)
- Operating System and Hardware Security Implementation
 - Memory Protection
 - System and User States
 - Rings (scope of control)
 - Process isolation
 - Object reuse controls

8/24/2007

Class 6

29

Security flaws can exist in hardware

- Hardware flaws that affect security protections would be serious
- They might be mitigated at the operating system or firmware (BIOS) level
- The OpenBSD project believes they have found flaws in Intel processors that present serious security flaws
- See <http://marc.info/?l=openbsd-misc&m=118296441702631> and <http://hardware.slashdot.org/hardware/07/06/28/1124256.shtml>
- Alternatively, an adversary could deliberately introduce security flaws into hardware for late use

8/24/2007

Class 6

30

Extra Material: Installing snort on a Windows XP system



8/24/2007

Class 6

31

Download snort

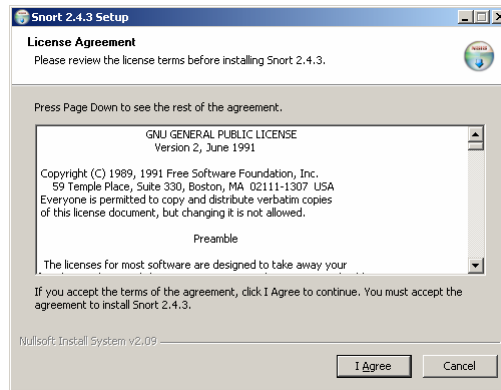
- <http://www.snort.org/dl/binaries/win32/> Contains the Windows binaries
- Download the installer, the MD5 hash, and the SIG

8/24/2007

Class 6

32

Install snort

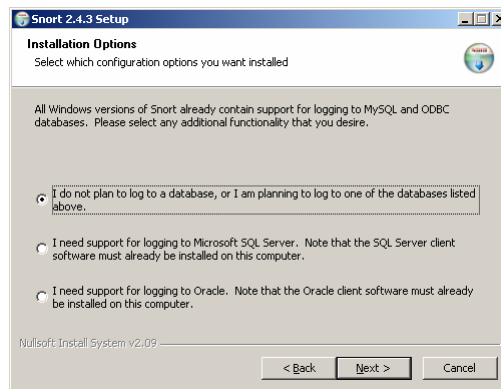


8/24/2007

Class 6

33

Install snort

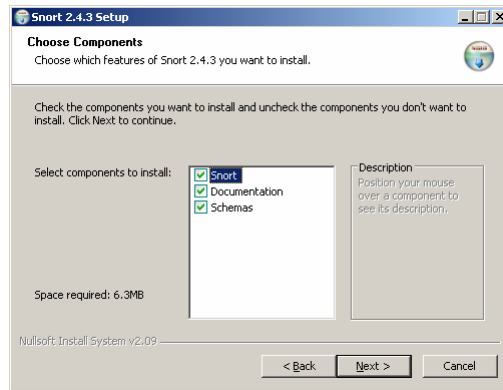


8/24/2007

Class 6

34

Install snort

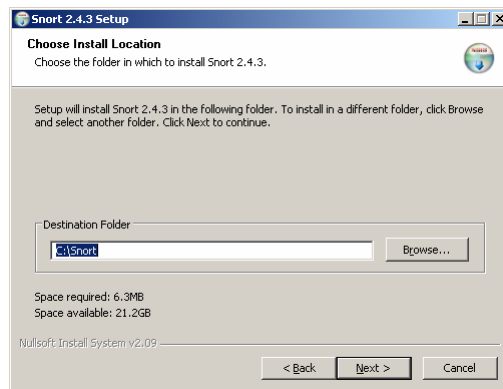


8/24/2007

Class 6

35

Install snort

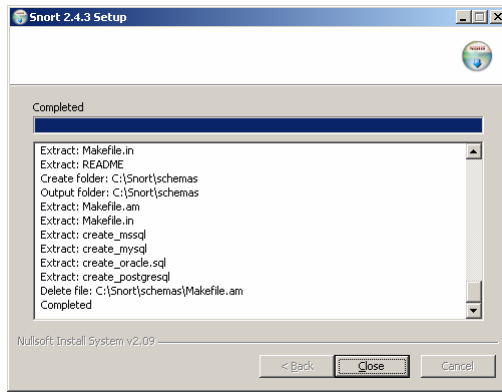


8/24/2007

Class 6

36

Done!

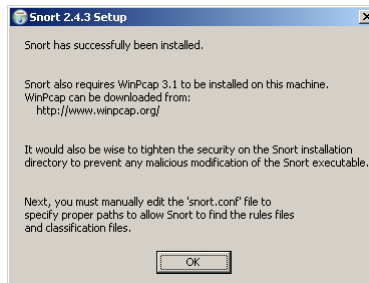


8/24/2007

Class 6

37

Well, almost done

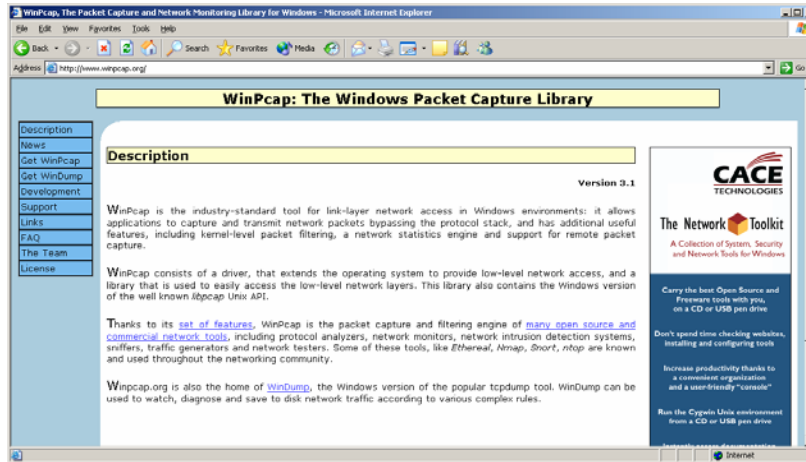


8/24/2007

Class 6

38

Installing winpcap



8/24/2007

Class 6

39

Installing winpcap

- Download the auto-installer (WinPcap_3_1.exe)
- Start the install:



8/24/2007

Class 6

40

Installing winpcap

- If you have a previous version of winpcap, it will prompt you to automatically uninstall it
- A reboot is required when installation is complete

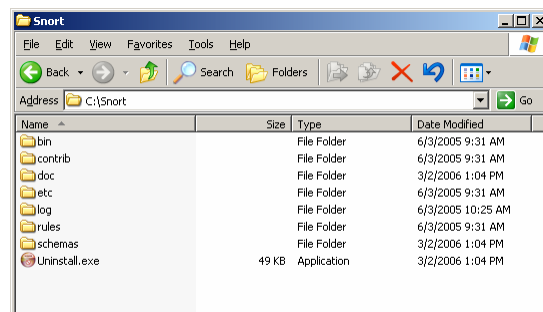
8/24/2007

Class 6

41

Configuring snort

- Everything “snort” will be in C:\Snort (snort will **not** be in your program menu):



8/24/2007

Class 6

42

Configuring snort

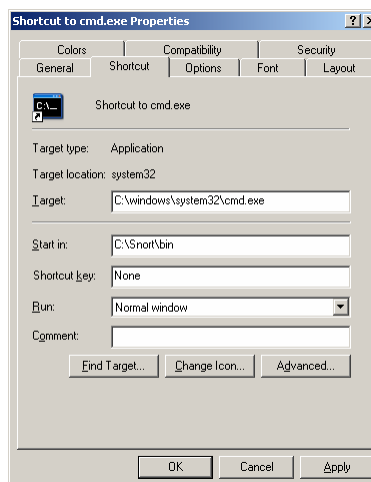
- The snort executable is in the C:\Snort\bin directory
- It must be run from a command prompt
- Create a shortcut to cmb.exe in C:\Snort\bin
- Right click on it and change Shortcut Properties so that it starts in C:\Snort\bin

8/24/2007

Class 6

43

Configuring snort



8/24/2007

Class 6

44

Configuring snort

- `snort -v` will give you a packet dump
- Be sure to specify the right network interface:
 - Mine defaulted to generic dialup
 - I had to type the following to get snort to use my Ethernet card:

```
snort -v -i \Device\NPF_{CD7C5043-1ED7-4860-BABC-711528990BEC}
```

8/24/2007

Class 6

45

Configuring snort: Finding the Interface to use with snort

```
C:\Snort\bin>snort.exe -W
```

```
.._  -*> Snort! <*-
o"  )~  Version 2.4.3-ODBC-MySQL-FlexRESP-WIN32 (Build 26)
""   By Martin Roesch & The Snort Team: http://www.snort.org/team.html
      (C) Copyright 1998-2005 Sourcefire Inc., et al.
NOTE: Snort's default output has changed in version 2.4.1!
      The default logging mode is now PCAP, use "-K ascii" to activate
      the old default logging mode.
Interface  Device      Description
-----
1 \Device\NPF_GenericDialupAdapter (Generic dialup adapter)
2 \Device\NPF_{E7C1012D-B5C6-4432-8B7C-20BA02C1ECE6} (VMware Virtual Ethernet Adapter)
3 \Device\NPF_{496EA415-546F-4870-AF6D-7147730A7CF0} (VMware Virtual Ethernet Adapter)
4 \Device\NPF_{03433976-1F6E-4DB8-BA72-96114AB2F15A} (Dell Wireless WLAN 1450 Dual Band WLAN Mini-PCI Card (Microsoft's Packet Scheduler) )
5 \Device\NPF_{CD7C5043-1ED7-4860-BABC-711528990BEC} (Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler) )
C:\Snort\bin>
```

In this case, you would specify the 5th one (\Device\NPF_{CD7C5043-1ED7-4860-BABC-711528990BEC}) unless you wanted to monitor traffic from the wireless card.

8/24/2007

Class 6

46

Configuring snort

- To start logging intrusions:

```
snort -l C:\Snort\Log -c C:\Snort\etc\snort.conf -A  
console -i \Device\NPF_{CD7C5043-1ED7-4860-BABC-  
711528990BEC}
```

- What this does:

-l C:\Snort\Log – Where intrusion information is logged

-c C:\Snort\etc\snort.conf – What file determines the snort configuration

-A console – Send alerts to console window

-i \Device\NPF_{CD7C5043-1ED7-4860-BABC-711528990BEC} –
Which interface to read traffic from

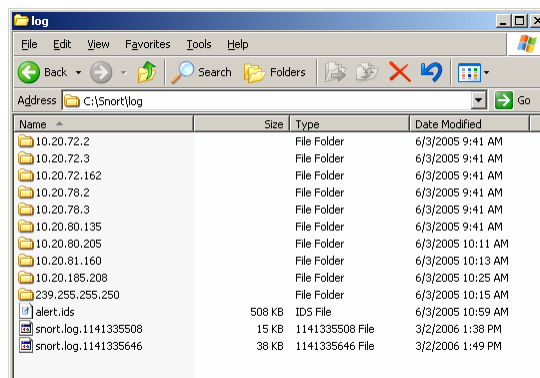
8/24/2007

Class 6

47

Reviewing snort logs

- Log files are located in C:\Snort\log



8/24/2007

Class 6

48

Configuring snort (from the documentation)

The first thing we need to configure is our local network. We need to distinguish internal from external traffic. Open up C:\Snort\etc\snort.conf with Notepad and find the line var HOME_NET any and replace "any" with the IP range and subnet mask. i.e. 192.168.0.1/24 If you have more than one internal subnet you can specify them all by putting them in brackets and separate them with a comma. Now we need to define the external network, find the line var EXTERNAL_NET any. You can replace any with the IP address(es) of the external networks, or you can leave "any" to set all networks not defined as HOME_NET as external.

Next we have to define the services on our network. Find the following lines and replace \$HOME_NET with the IP address(es) of the server(s) running the services.

```
var DNS_SERVERS $HOME_NET
var SMTP_SERVERS $HOME_NET
var HTTP_SERVERS $HOME_NET
var SQL_SERVERS $HOME_NET
```

These are the most popular ones, there are others in the snort.conf file. If you do not need to monitor the service you can remove them from monitoring by commenting the line out with a # at the start of the line. Last thing we need to configure is the rules to monitor. SNORT includes over 1500 rules and we probably don't need them all. Scroll to the bottom of the snort.conf until you find the rules section, the first rule is:

```
include $RULE_PATH/local.rules
```

Here you will find a whole assortment of rules. To stop SNORT from monitoring a rule you can comment it out with a # at the start of the line.

```
# include $RULE_PATH/local.rules
```

Lastly we need to setup Snort to log to the Event Logs and to run as a service. This can be done easily by running the following from a command prompt:

```
snort /SERVICE /INSTALL -I C:\Snort\Log -c C:\Snort\etc\snort.conf -E
```

8/24/2007

Class 6

49

Resources

- <http://thelazyadmin.com/index.php/archives/121-Running-SNORT-IDS-on-Windows-2003.html>
- <http://www.snort.org/>
- <http://www.winpcap.org/>
- <http://www.sans.org/resources/tdfaq/snort.php>

8/24/2007

Class 6

50