Ethical Hacking and Countermeasures

Version 6

Module XXIII

Evading IDS, Firewalls, and Honeypots

Scenario

eGlobal Bank had expanded its web presence to include a large number of Internet services. In addition to regular banking services, the Bank was now offering bill payment and other transactional services online. They were becoming concerned at the increasing number of web-hacking attacks that were being directed at the Banking Sector.

The Bank had basic experience in security and had a firewall installed by a third party supplier few months ago. Few days later, bank officials were taken aback by the news that their servers were hacked and sensitive information of thousands of customers was stolen. The stolen information consisted of the details about the customers' bank account numbers, credit card numbers, and their passwords.

Something had gone wrong with the Web server.

How could the web server be targeted even though the firewall was installed?

darkREADING
RISKY BUSINESS

Attackers Use New 'Call-Home' Method to Infiltrate Home Networks

Honeynet Project researchers witness stealthy new method of botnet communication

JANUARY 17, 2008 | 5:45 PM

By Kelly Jackson Higgins
Senior Editor, *Dark Reading*

Now the bad guys have discovered a way to set up a stealthy, continuous connection between the machines they infect and their own command and control servers.

Researchers with the Honeynet Project have been studying a new method being used by botnet operators and other cyber criminals that sets up what's called a "reverse tunnel proxy" connection -- a connection through the victim's Network Address Translation (NAT)-based filtering device such as a home router or other router or firewall.

What makes this approach different from traditional botnet relationships is that the command and control machine doesn't rely on the bot to "check in" and get its latest instructions, so it's more of a continuous connection, says Ralph Logan, a member of the board for the Honeypot Project and its chief public relations officer.

"The bot and the C&C don't need to maintain a connection for reconfiguration, 're-tooling,' or retasking," says Logan, who is also principal with The Logan Group. "They've created a new way to bypass any kind of routing device that gives you private IP addresses behind it."

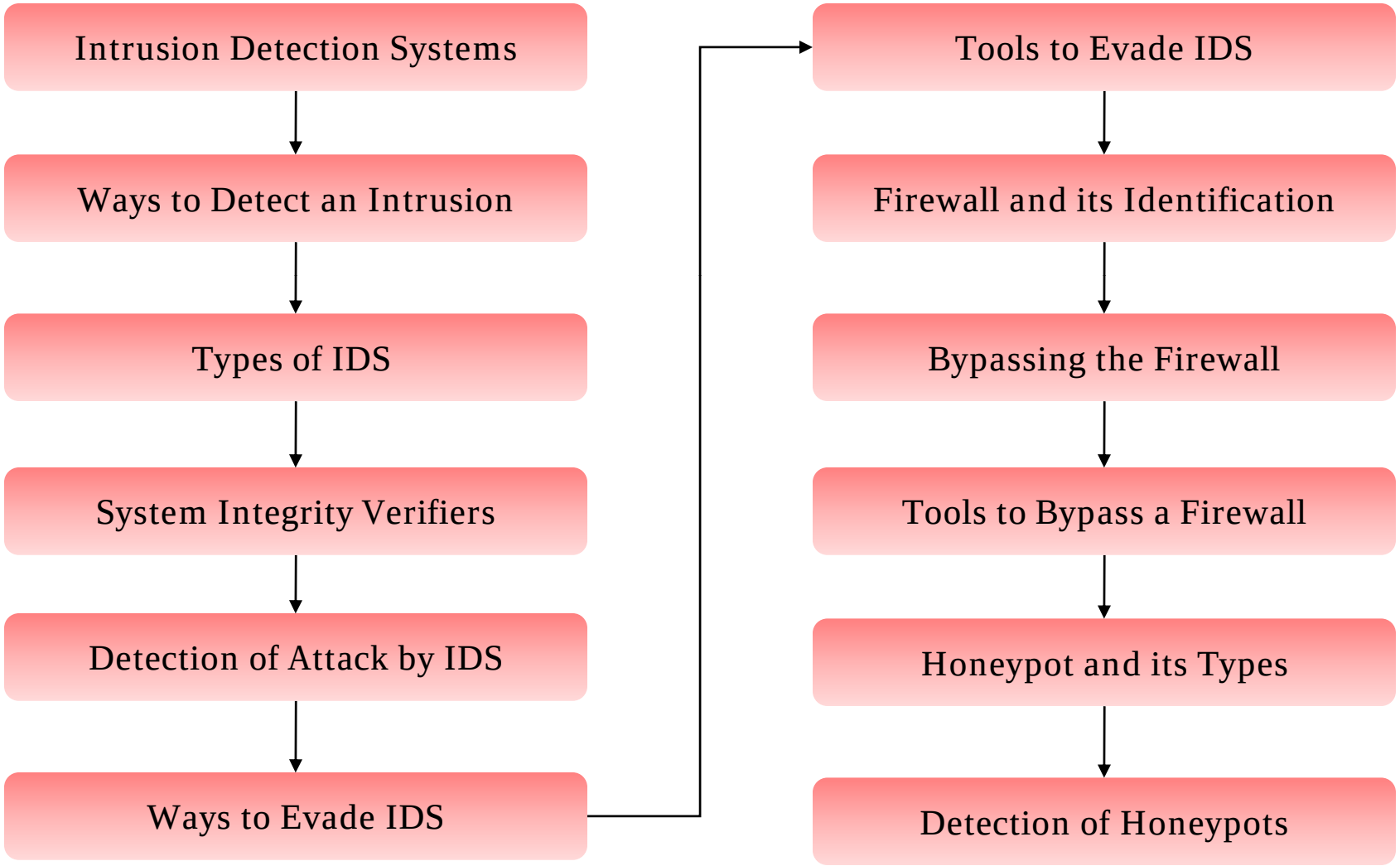
Source: *http://www.darkreading.com/*

Module Objective

This module will familiarize you with :

- Intrusion Detection Systems
- Ways to Detect an Intrusion
- Types of IDS
- System Integrity Verifiers
- Detection of Attack by IDS
- Ways to Evade IDS
- Tools to Evade IDS
- Firewall and its Identification
- Bypassing the Firewall
- Tools to Bypass a Firewall
- Honeypot and its Types
- Detection of Honeypots

Module Flow



Introduction to Intrusion Detection Systems

Attackers/hackers are always looking to compromise networks

Customizing the settings will help prevent easy access for hackers

IDS, Firewalls, and Honeypots are important technologies which can deter an attacker from compromising the network

Terminologies

Intrusion Detection System (IDS)

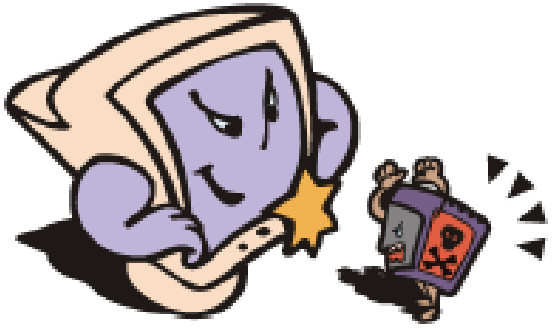
- An IDS inspects all of the inbound and outbound network activity, and identifies suspicious patterns that indicate an attack that might compromise a system

Firewall

- A firewall is a program or hardware device that protects the resources of a private network from users of other networks

Honeypot

- A honeypot is a device intended to be compromised. The goal of a honeypot is to have the system probed, attacked, and potentially exploited



Intrusion Detection System

Intrusion Detection Systems (IDS)

An intrusion detection system (IDS) gathers and analyzes information from within a computer or a network, to identify possible violations of security policy, including unauthorized access, as well as misuse

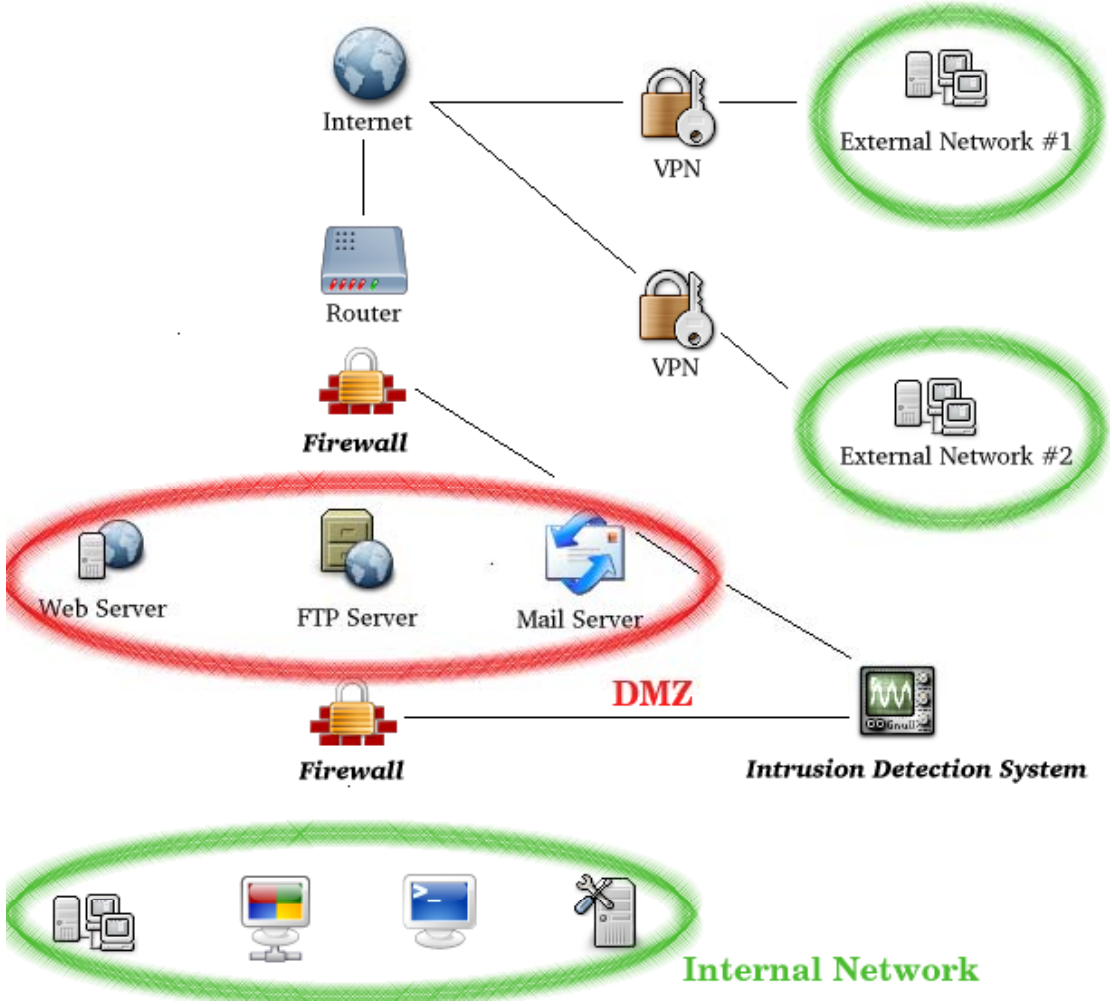
An IDS is also referred to as a “packet-sniffer,” which intercepts packets that are traveling along various communication mediums and protocols, usually TCP/IP

The packets are then analyzed after they are captured

An IDS evaluates a suspected intrusion once it has taken place, and signals an alarm

Intrusion Detection System

IDS Placement



Ways to Detect an Intrusion

There are three ways to detect an intrusion:

Signature recognition

- It is also known as misuse detection. Signature recognition tries to identify events that misuse a system

Anomaly detection

- Anomaly detection is different from signature recognition in the subject of the model

Protocol Anomaly detection

- In this type of detection, models are built on TCP/IP protocols using their specifications

Types of Intrusion Detection Systems

Network-based Intrusion Detection

- These mechanisms typically consist of a black box that is placed on the network in promiscuous mode, listening for patterns indicative of an intrusion

Host-based Intrusion Detection

- These mechanisms usually include auditing for events that occur on a specific host. These are not as common, due to the overhead they incur by having to monitor each system event

Log File Monitoring

- These mechanisms are typically programs that parse log files after an event has already occurred, such as failed log in attempts

File Integrity Checking

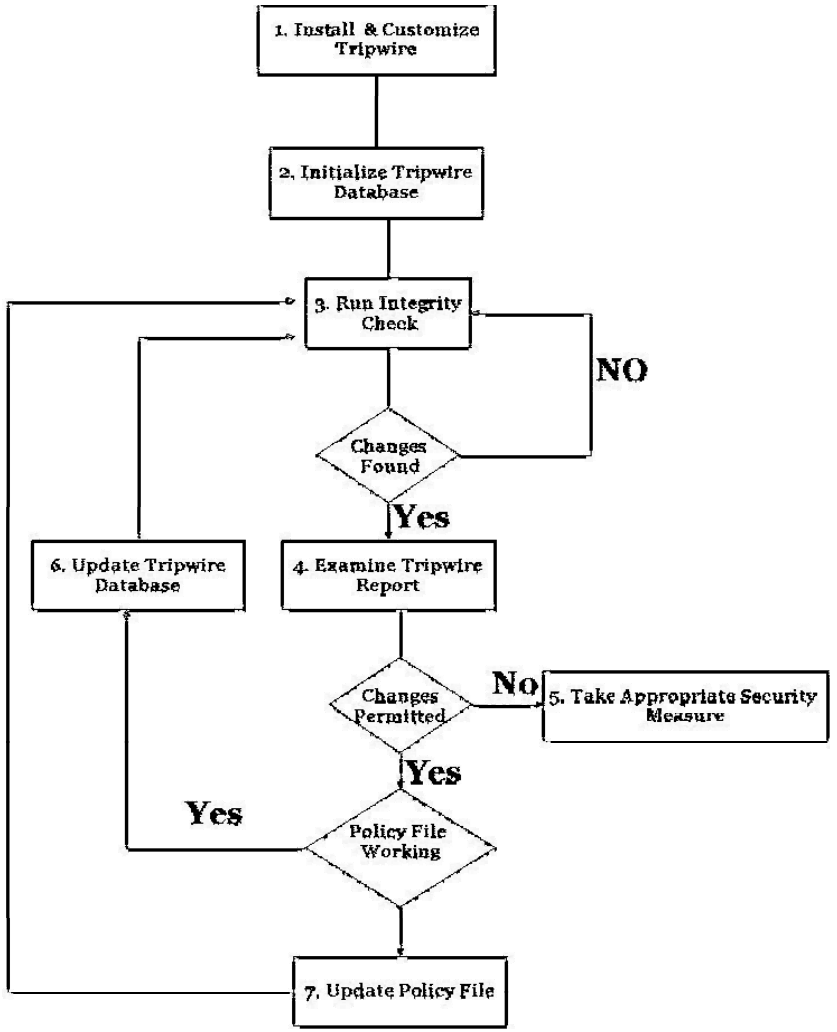
- These mechanisms check for Trojan horses, or files that have otherwise been modified, indicating an intruder has already been there, for example, Tripwire

System Integrity Verifiers (SIV)

System Integrity Verifiers (SIV) monitor system files detect changes by an intruder

Tripwire is one of the popular SIVs

SIVs may watch other components, such as the Windows registry, as well as chron configuration, to find known signatures



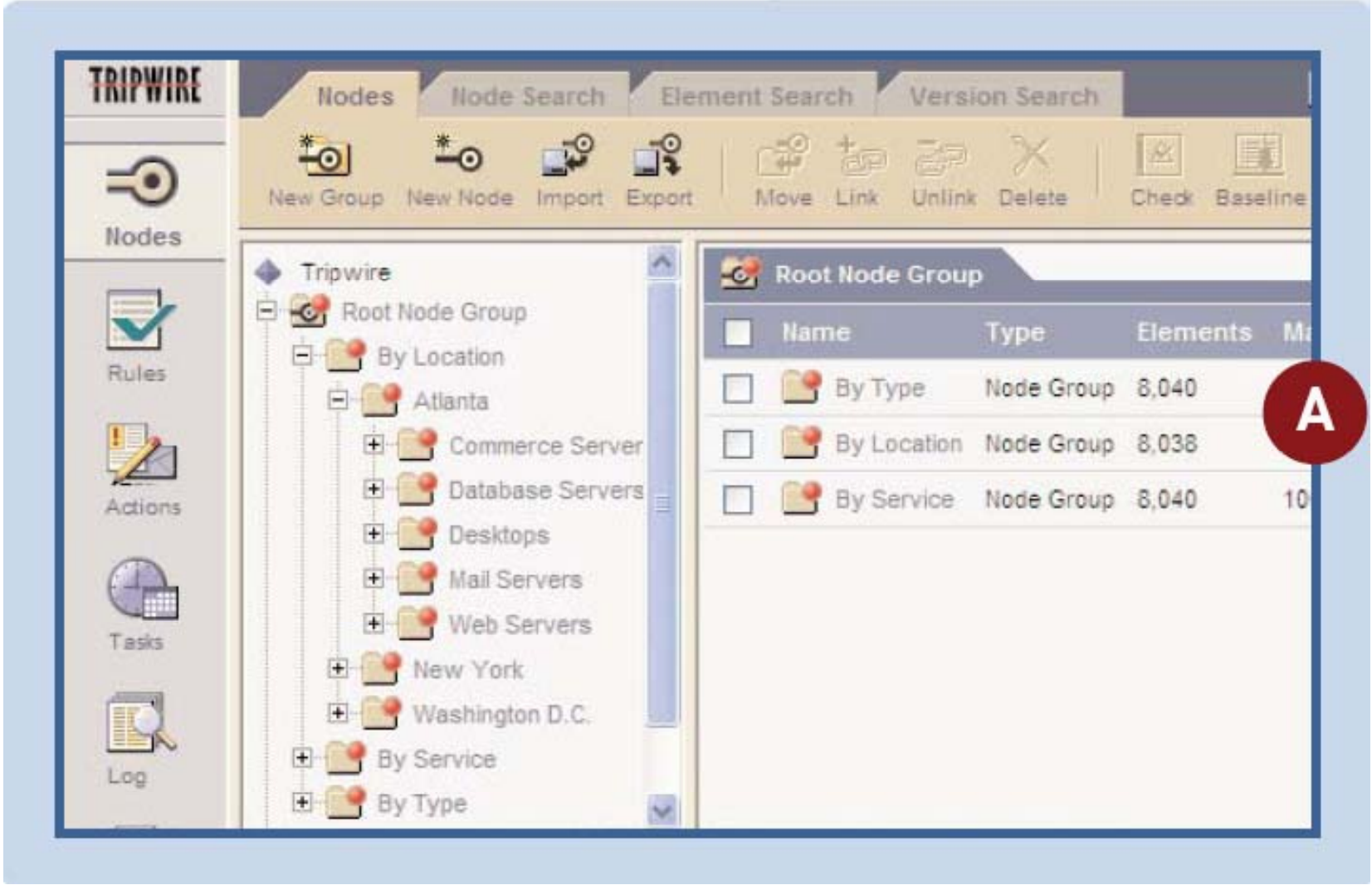
Tripwire (www.tripwire.com)

Tripwire is an SIV monitor

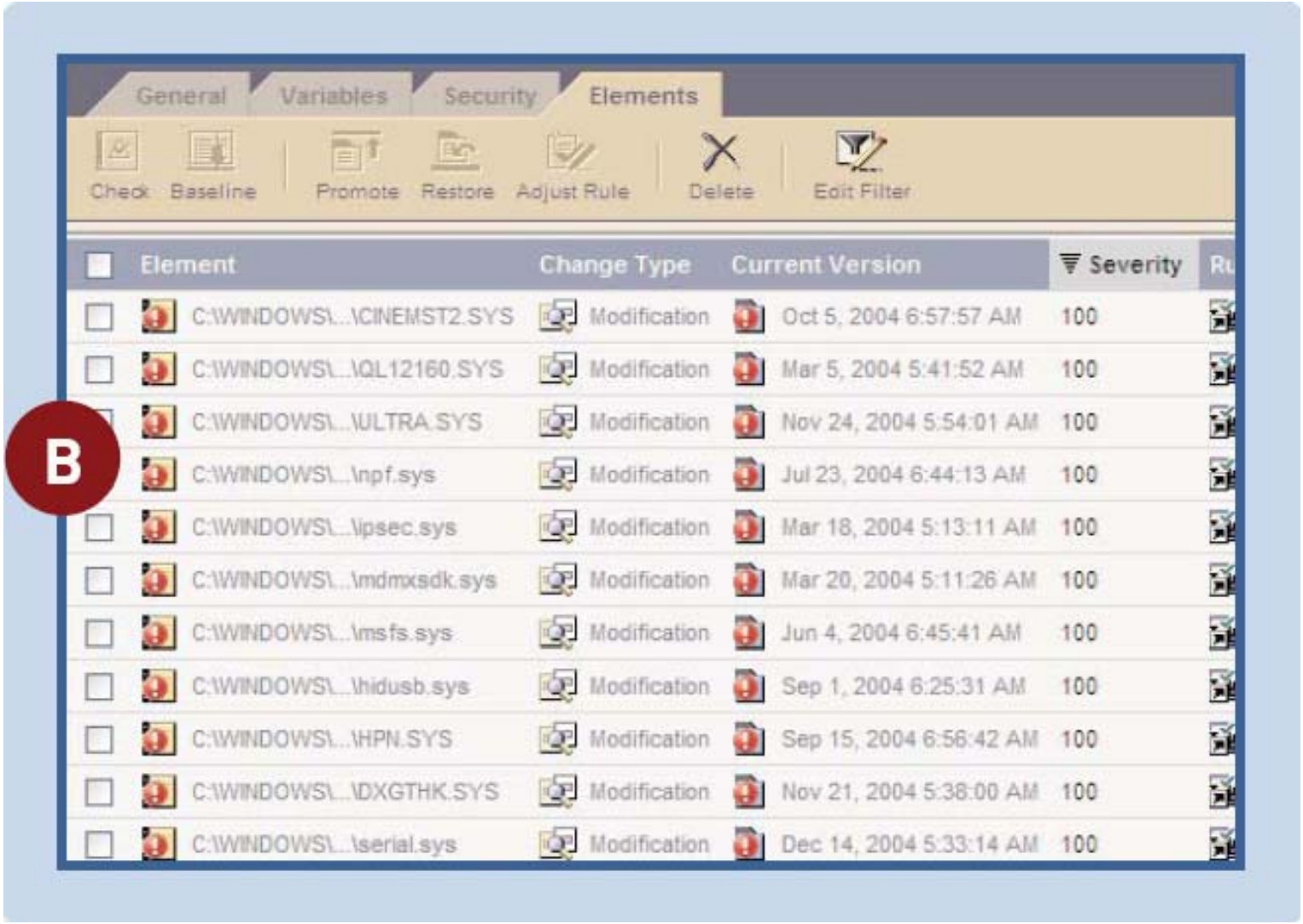
It works with a database that maintains information about the byte count of files

If the byte count has changed, it will be identified with the system security manager

Tripwire: Screenshot 1



Tripwire: Screenshot 2



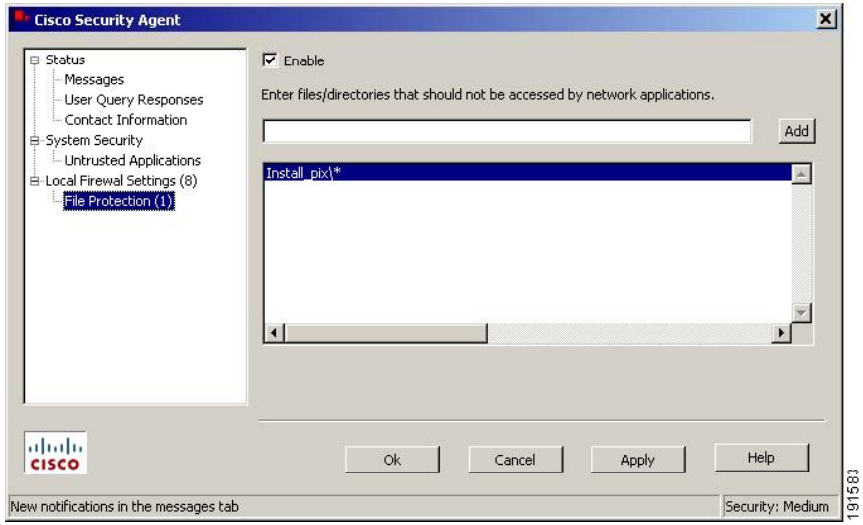
Cisco Security Agent (CSA)

Cisco (CSA) is a host-based IDS system

CSA software protects the server and desktop computing systems by identifying threats and preventing malicious behavior

It mitigates new and evolving threats without requiring reconfigurations or emergency patch updates, while providing robust protection with a reduced operational cost

CSA does not rely on signature matching



True/False, Positive/Negative

	True	False
Positive	An alarm was generated and a present condition should be alarmed	An alarm was generated and there is no condition present to warrant one
Negative	An alarm was **NOT** generated and there is no condition present to warrant one	An alarm was **NOT** generated and a present condition should be alarmed

Source: The Practical Intrusion Detection Handbook by Paul E. Proctor

Signature Analysis

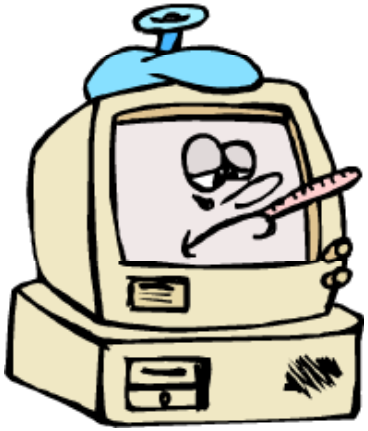
Signature analysis refers to an IDS that is programmed to interpret a series of packets, or a piece of data contained in those packets, as an attack

For example, an IDS that watches web servers might be programmed to look for the string “phf” as an indicator of a CGI program attack

Most IDSes are based on Signature Analysis

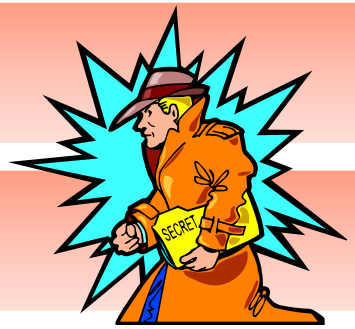
General Indications of Intrusion System Indications

- Modifications to system software and configuration files
- Gaps in the system accounting
- Unusually slow system performance
- System crashes or reboots
- Short or incomplete logs
- Logs containing strange timestamps
- Logs with incorrect permissions or ownership
- Missing logs
- Abnormal system performance
- Unfamiliar processes
- Unusual graphic displays or text messages



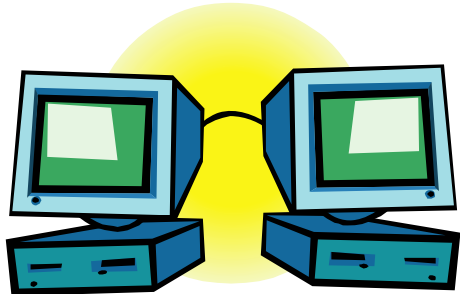
General Indications of Intrusion File System Indications

- The presence of new, unfamiliar files, or programs
- Changes in file permissions
- Unexplained changes in file size
- Rogue files on the system that do not correspond to your master list of signed files
- Unfamiliar file names in directories
- Missing files



General Indications of Intrusion Network Indications

- Repeated probes of the available services on your machines
- Connections from unusual locations
- Repeated log in attempts from the remote hosts
- Arbitrary data in log files, indicating an attempt at creating either a Denial of Service, or a crash service



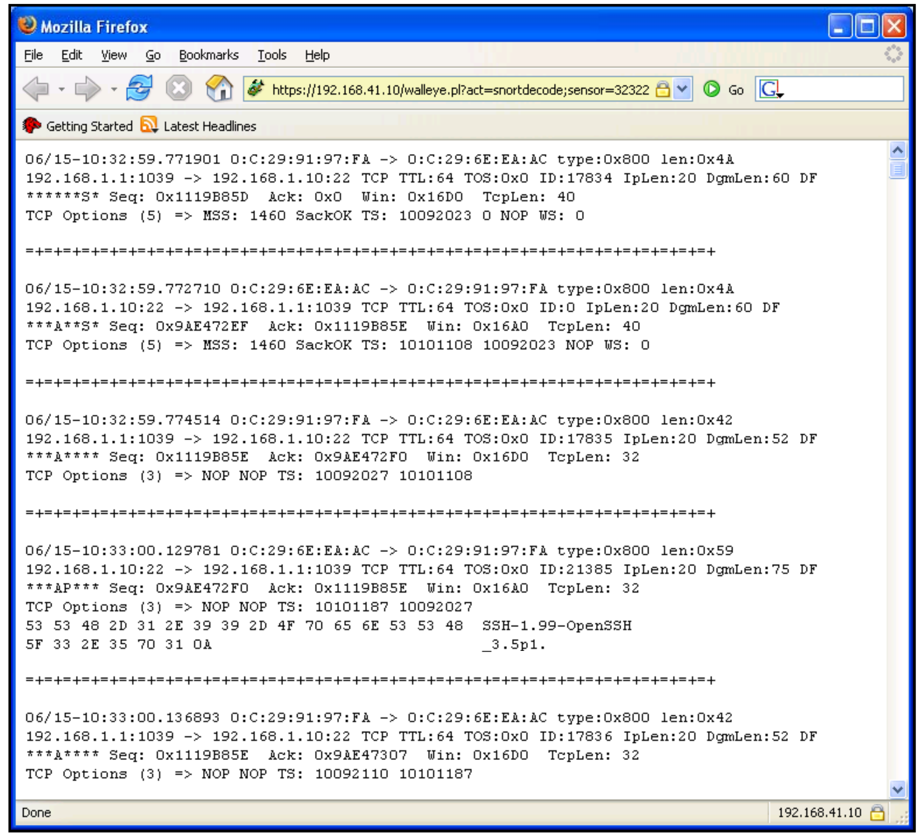
Intrusion Detection Tools

- Snort 2.x (www.snort.org)
- BlackICE Defender (NetworkICE)
- Check Point RealSecure (Check Point Software Technologies)
- Cisco Secure IDS (Cicso Systems)
- Dragon Sensor (Network Security Wizards)
- eTrust Internet Defense (Computer Associates)
- HP Openview Node Sentry (Hewlett-Packard)
- Lucent RealSecure (Lucent Technologies)
- Network Flight Recorder (Network Flight Recorder)
- RealSecure (ISS)
- SilentRunner (SilentRunner)
- Vanguard Enforcer (Vanguard Integrity Professionals)

Snort

Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks

It can perform protocol analysis and content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts

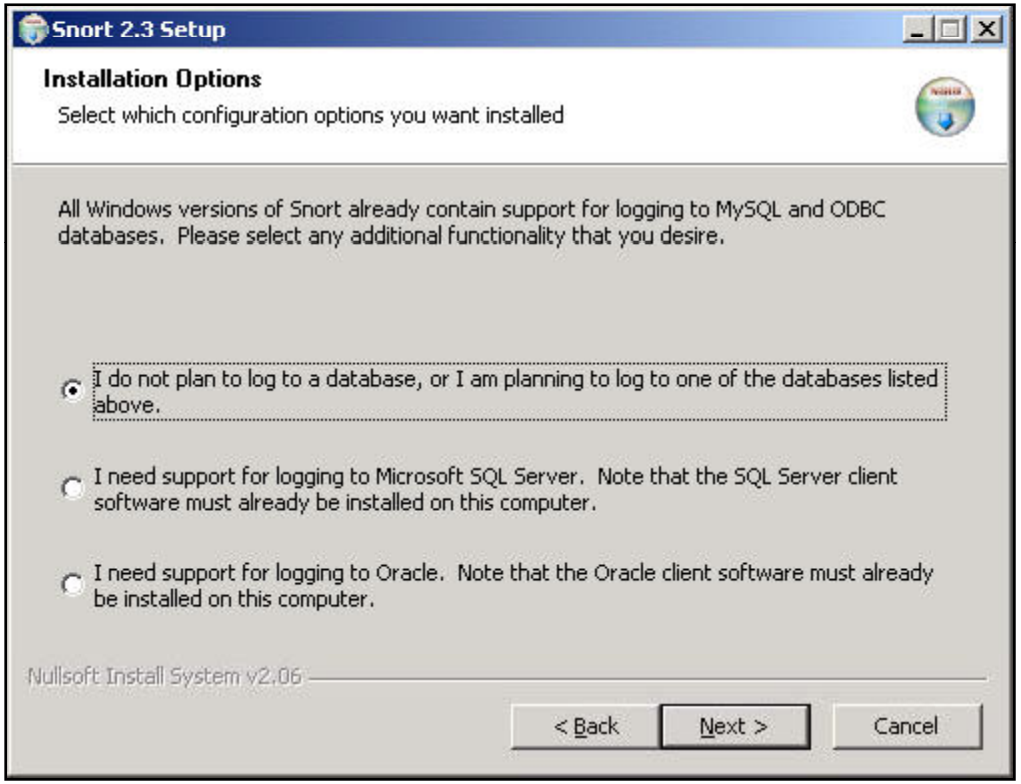


Running Snort on Windows 2003

Install Snort and the rules database (You can download from (http://www.snort.org)

Change to c:\snort\bin directory and run this command

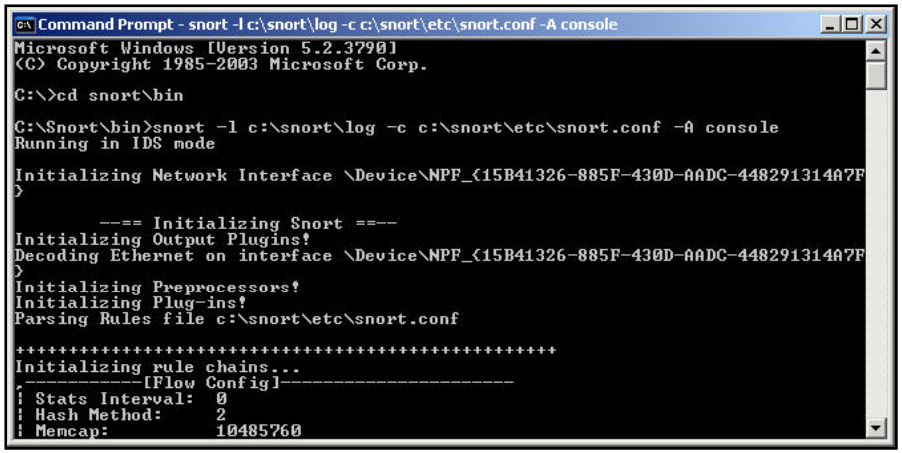
snort -l C:\Snort\Log -c C:\Snort\etc\snort.conf -A console

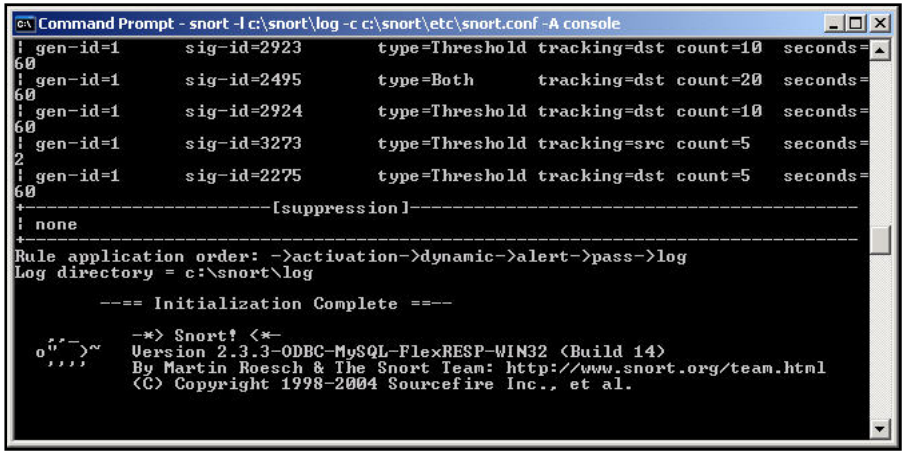


Snort Console

```
snort -l C:\Snort\Log -c C:\Snort\etc\snort.conf -A console
```

This command will configure SNORT to write its log files to C:\Snort\Log and also points out the location of the snort.conf file. The -A console switch sends SNORT output alerts to the console window

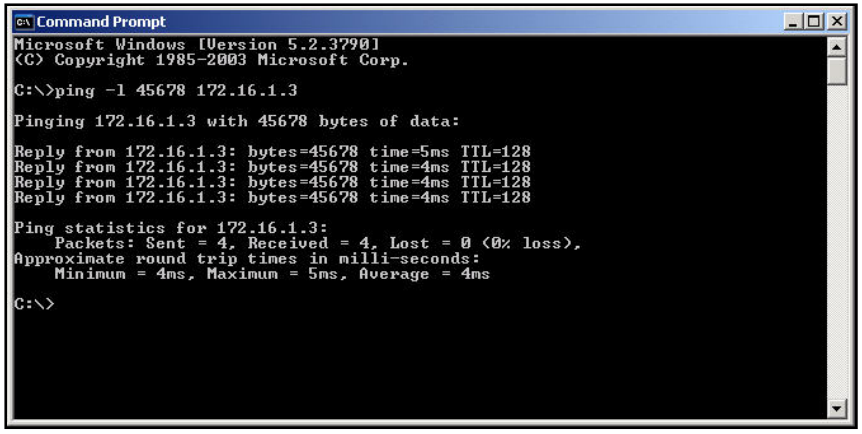


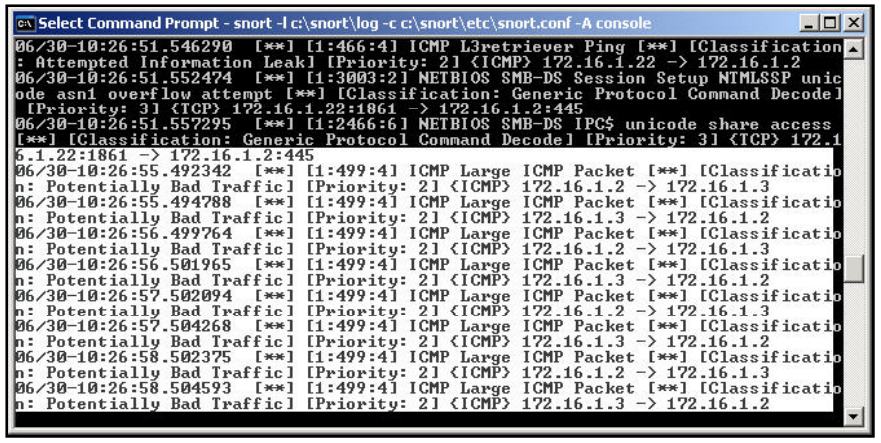


Testing Snort

With SNORT running, you can test it by opening a command prompt and run:

- `ping -l 45678 xxx.xxx.xxx.xxx`





Configuring Snort (snort.conf)

The first thing to do after installation is to configure the local network

Distinguish the 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. 10.0.0.0/24

If you have more than one internal subnet you can specify them all by putting them in brackets and separating them with a comma

Next, define the external network, by finding the line var EXTERNAL_NET any

Replace “any” with the IP address(es) of the external networks, or you can leave "any" to set all the networks not defined as HOME_NET as external. Next, 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 service

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

Snort Rules

SNORT includes over 2500 rules, which may or may not be needed

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 an assortment of rules

To stop SNORT from monitoring a particular rule, you can comment it out with a # at the start of the line

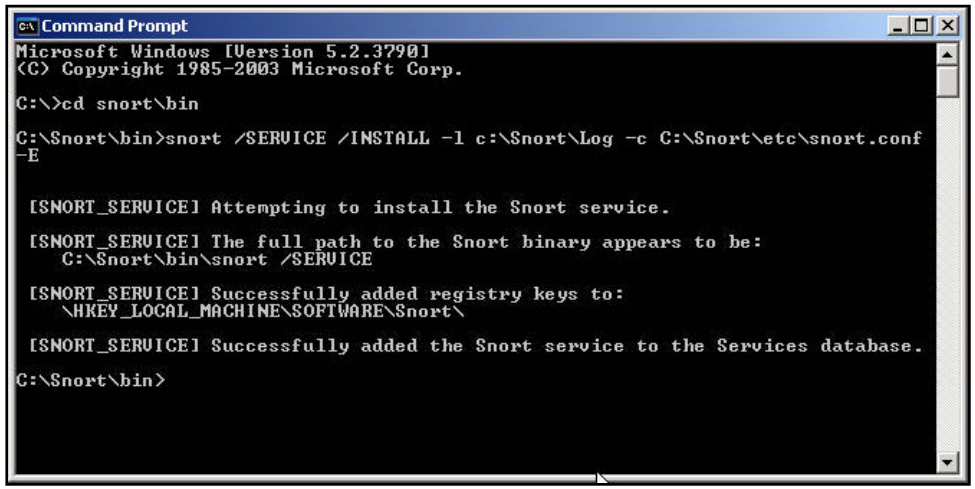
```
# include $RULE_PATH/local.rules
```

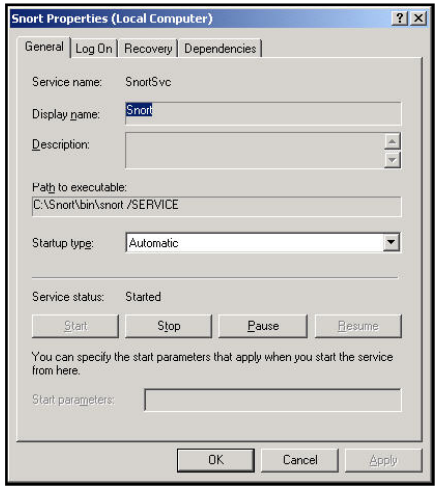
Set up Snort to Log to the Event Logs and to Run as a Service

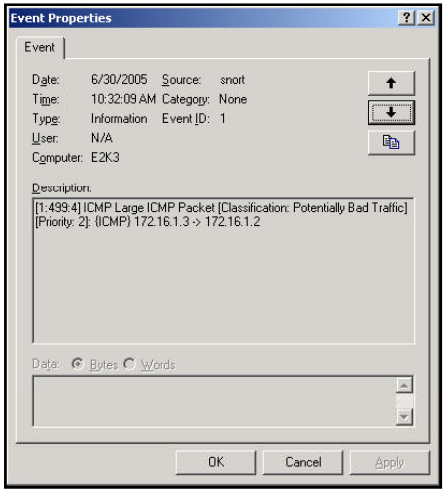
This can be done easily by running the following from a command prompt:

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

This will install SNORT as a service, launch it when the server starts up, and logs alerts to the Event Logs







Using EventTriggers.exe for Eventlog Notifications

Eventtriggers.exe is included in Windows XP and 2003 and allows you to configure notifications based on events written to the logs

For example, if you have set up SNORT, and want to be notified when an event is written to the log, you can do so with eventtriggers.exe

You can create event triggers for any event written to the event logs

From a command prompt run:

```
eventtriggers.exe /create /eid /tr /ru /rp /tk
```

`/create` - is used to create an event trigger, /delete can be used to delete the trigger
`/eid` - is the event id number you wish to track
`/tr` - is the name you would like to give to the event trigger
`/ru` - is the user name to run under user\domain or user@domain.com are both acceptable
`/rp` - is the user password
`/tk` - is the action you would like performed when triggered

If SNORT were to write an event to the logs with event ID of 2006, the command would be:

```
eventtriggers.exe /create /eid 2006 /tr SNORT_Detection /ru x@xsecurity.com
/ru passwerd|) /tk "net send 192.168.1.34 SNORT has detected an attack!!!"
```

SnortSam

SnortSam is a plugin for Snort, an open-source light-weight Intrusion Detection System (IDS)

The plugin allows for an automated blocking of IP addresses on the following firewalls:

- Checkpoint Firewall-1
- Cisco PIX firewalls
- Cisco Routers (using ACL's or Null-Routes)
- Former Netscreen, now Juniper firewalls
- IP Filter (ipf), available for various Unix-like OS'es such as FreeBSD
- FreeBSD's ipfw2 (in 5.x)
- OpenBSD's Packet Filter (pf)
- Linux IPchains
- Linux IPtables
- Linux EBtables
- WatchGuard Firebox firewalls
- 8signs firewalls for Windows
- MS ISA Server firewall/proxy for Windows
- CHX packet filter
- Ali Basel's Tracker SNMP through the SNMP-Interface-down plugin

Steps to Perform After an IDS Detects an Attack

- Configure a firewall to filter out the IP address of the intruder
- Alert the user/administrator (sound/e-mail/page)
- Write an entry in the event log. Send an SNMP Trap datagram to a management console like Tivoli
- Save the attack information (timestamp, intruder IP address, victim IP address/port, protocol information)
- Save a tracefile of the raw packets for later analysis
- Launch a separate program to handle the event
- Terminate the TCP session - Forge a TCP FIN or RST packet to forcibly terminate the connection

Evading IDS Systems

Many simple network intrusion detection systems rely on **"pattern matching"**

Attack scripts have well-known patterns, so compiling a database of the output of known attack scripts provides good detection, but can be easily evaded by simply changing the script

IDS evasion focuses on the foiling signature matching by altering an the attacker's appearance

- For example, some POP3 servers are vulnerable to a buffer overflow when a long password is entered

You can evade it by changing the attack script

Ways to Evade IDS

- Insertion
- Evasion
- Denial-of-service
- Complex Attacks
- Obfuscation
- Desynchronization - Post Connection SYN
- Desynchronization-Pre Connection
- Fragmentation
- Session Splicing

Tools to Evade IDS

- SideStep
- ADMutate
- Mendax v.0.7.1
- Stick
- Fragrouter
- Anzen NIDSbench

IDS Evading Tool: ADMutate

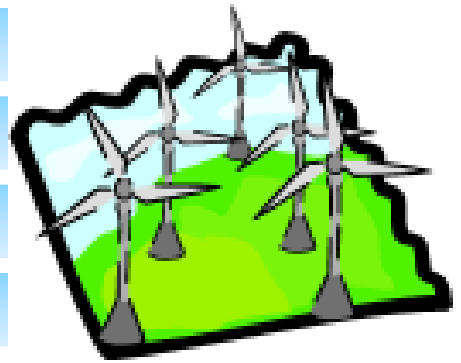
http://www.ktwo.ca/security.html

ADMutate accepts a buffer overflow exploit as input, and randomly creates a functionally equivalent version which bypasses IDS

Once a new attack is known, it usually takes the IDS vendors hours or days to develop a signature. But in the case of ADMutate, it has taken months for signature-based IDS vendors to add a way to detect a polymorphic buffer overflow

Packet Generators

- Aicmpsend 1.10 (http://www.elxsi.de/)
- Blast v2.0 (http://www.foundstone.com/rdlabs/blastbeta.html)
- CyberCop Scanner's CASL (http://www.nai.com)
- Ettercap 0.1.0 (http://ettercap.sourceforge.net/)
- Hping2 beta 54 (http://www.kyuzz.org/antirez/hping/)
- ICMPush 2.2 (http://hispachack.ccc.de/)
- IPsend (http://www.coombs.anu.edu.au/^avalon)
- Libnet (http://www.packetfactory.net/libnet)
- MGEN Toolset 3.2 (http://manimac.itd.nrl.navy.mil/MGEN/)
- Net::RawIP (http://www.quake.skif.net/RawIP)
- SING 1.1 (http://sourceforge.net/projects/sing)



Firewall

What is a Firewall

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from other network users

A firewall is placed at the junction point, or gateway between the two networks, which is usually a private network and a public network such as the Internet

Firewalls protect against hackers and malicious intruders

What does a Firewall do

- A firewall examines all the traffic routed between the two networks to see if it meets certain criteria
- It routes packets between the networks
- It filters both inbound and outbound traffic
- It manages public access to the private network resources such as host applications
- It logs all attempts to enter the private network and triggers alarms when hostile or unauthorized entries are attempted

Packet Filtering

Address Filtering

- Firewalls can filter packets based on their source and destination addresses and port numbers

Network Filtering

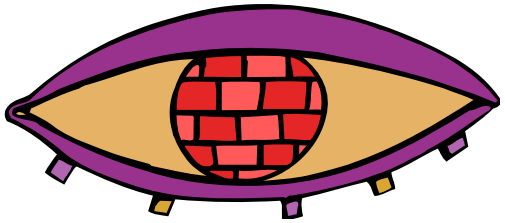
- Firewalls can also filter specific types of network traffic
- The decision to forward or reject traffic depends upon the protocol used, for example: HTTP, ftp, or telnet
- Firewalls can also filter traffic by packet attribute or state

What can't a Firewall do

A firewall cannot prevent individual users with modems from dialing into or out of the network, bypassing the firewall altogether

Employee's misconduct or carelessness cannot be controlled by firewalls

Policies involving the use and misuse of passwords and user accounts must be strictly enforced



How does a Firewall Work

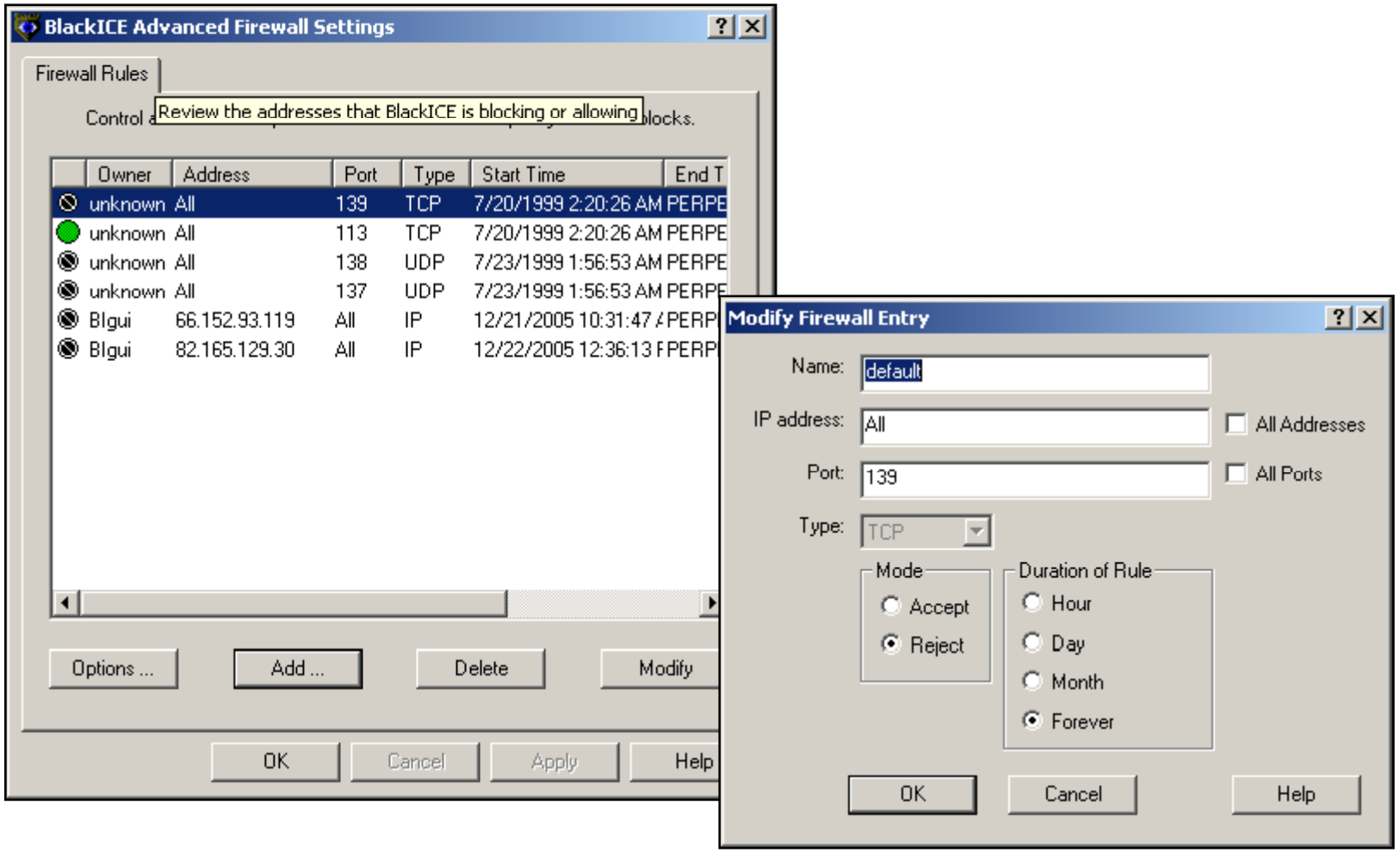
A firewall may allow all traffic unless it meets a certain criteria, or it may deny all traffic

The type of criteria used to determine whether or not traffic should be allowed through varies from one type of firewall to another

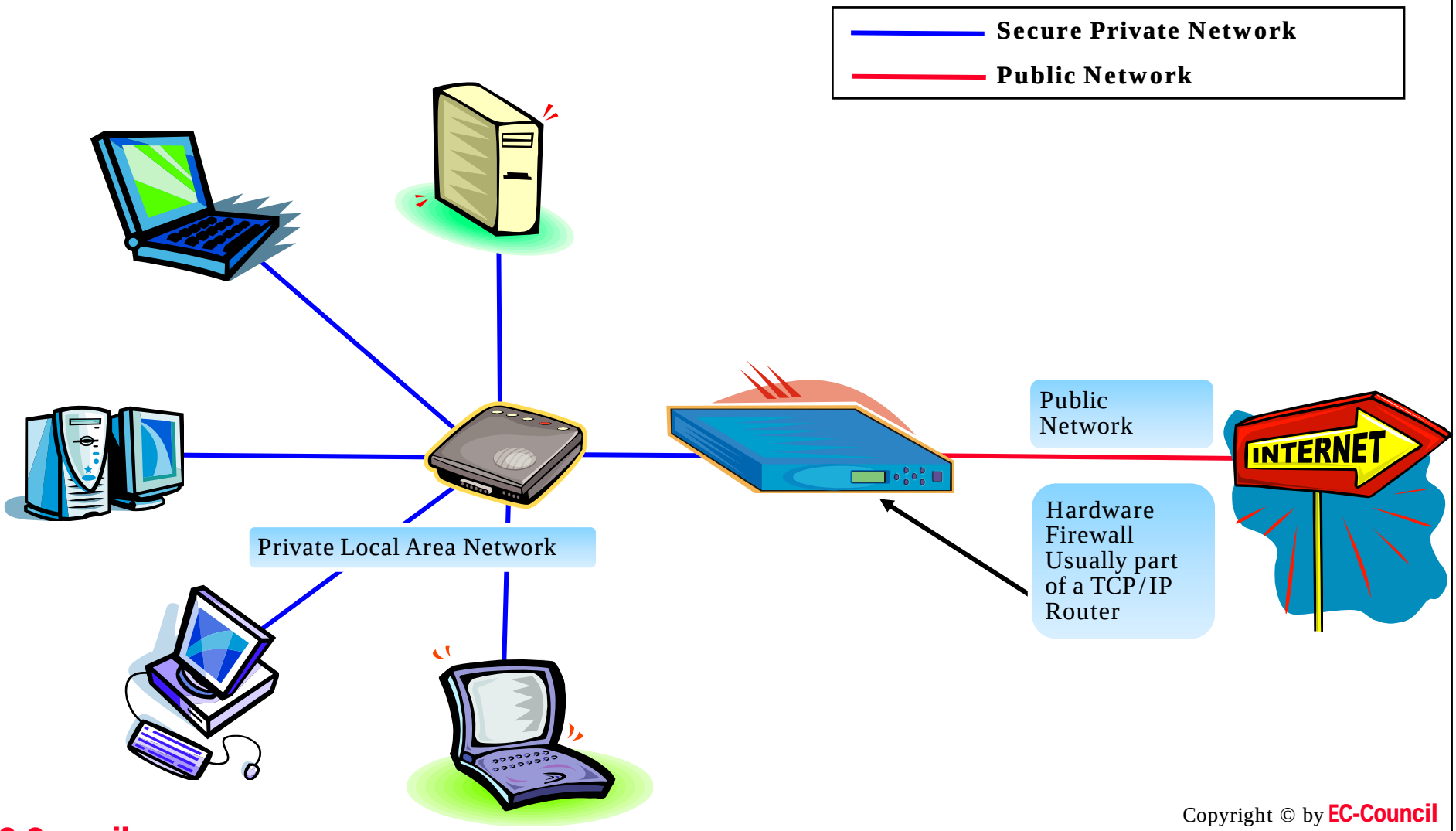
Firewalls may be concerned with the type of traffic, or with the source or destination addresses and ports

They may also use complex rule bases that analyze the application data to determine if the traffic should be allowed through

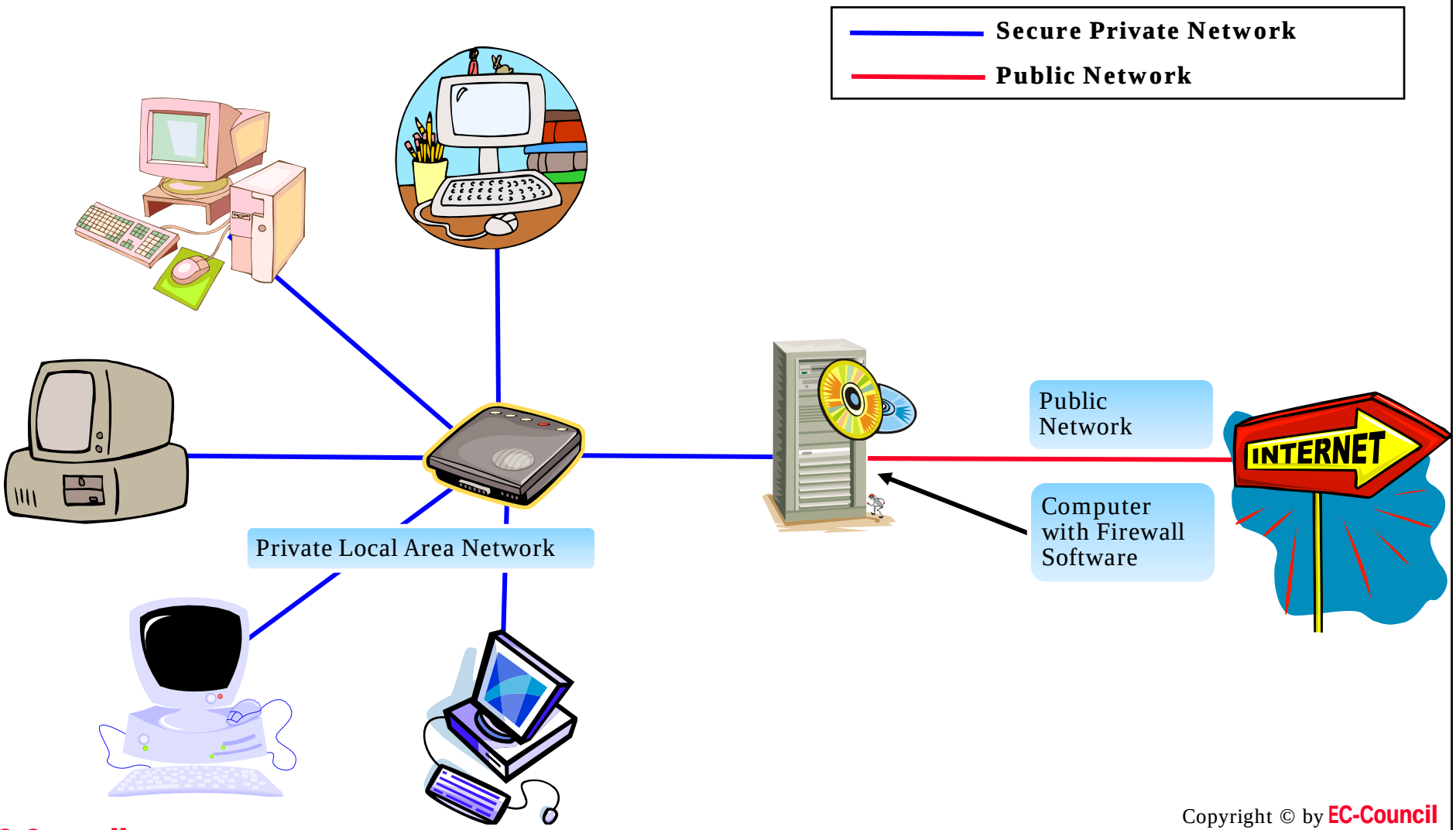
Firewall Operations



Hardware Firewall



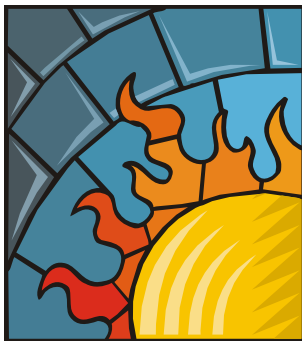
Software Firewall



Types of Firewalls

Firewalls fall into four categories:

- Packet filters
- Circuit level gateways
- Application level gateways
- Stateful multilayer inspection firewalls

Packet Filtering Firewall

Packet filtering firewalls work at the network level of the OSI model (or the IP layer of TCP/IP)

They are usually part of a router

In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded

Depending on the packet and the criteria, the firewall can:

- Drop the packet
- Forward it, or send a message to the originator

Rules can include the source and destination IP address, the source and the destination port number, and the protocol used

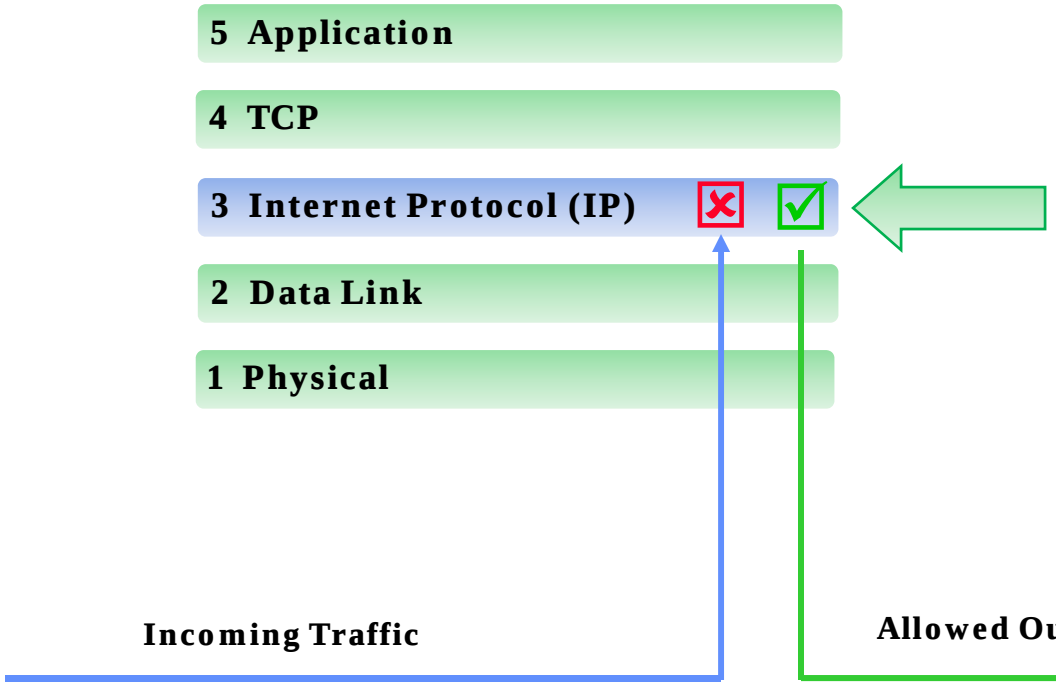
The advantage of packet filtering firewalls is their low cost and low impact on the network's performance

Most routers support packet filtering

IP Packet Filtering Firewall

☒ = Disallowed

☑ = Allowed



Traffic is filtered based on specified rules, including the source and the destination IP address, packet type, and port number

Unknown traffic is only allowed up to level 3 of the Network Stack

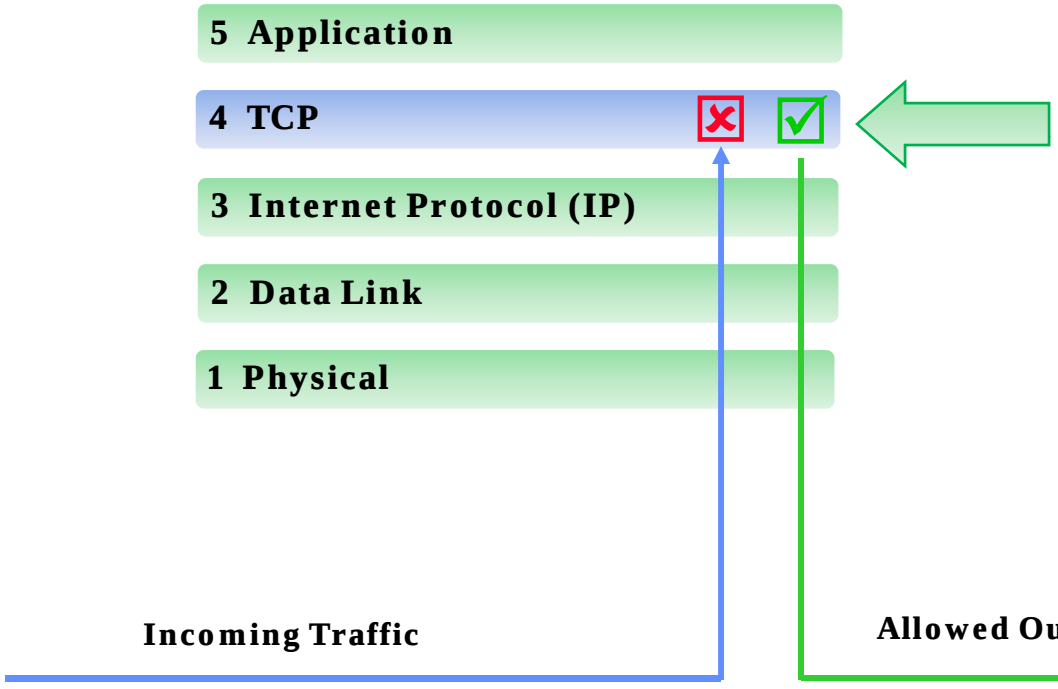
Circuit-Level Gateway

- Circuit-level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP
- They monitor TCP handshaking between packets to determine whether a requested session is legitimate
- Information passed to a remote computer through a circuit-level gateway appears to have originated from the gateway
- Circuit-level gateways are relatively inexpensive
- They hide information about the private network they protect
- Circuit-level gateways do not filter individual packets

TCP Packet Filtering Firewall

☒ = Disallowed

☑ = Allowed



Traffic is filtered based on specified session rules, such as when a session is initiated by a recognized computer

Unknown traffic is only allowed up to level 4 of the Network Stack

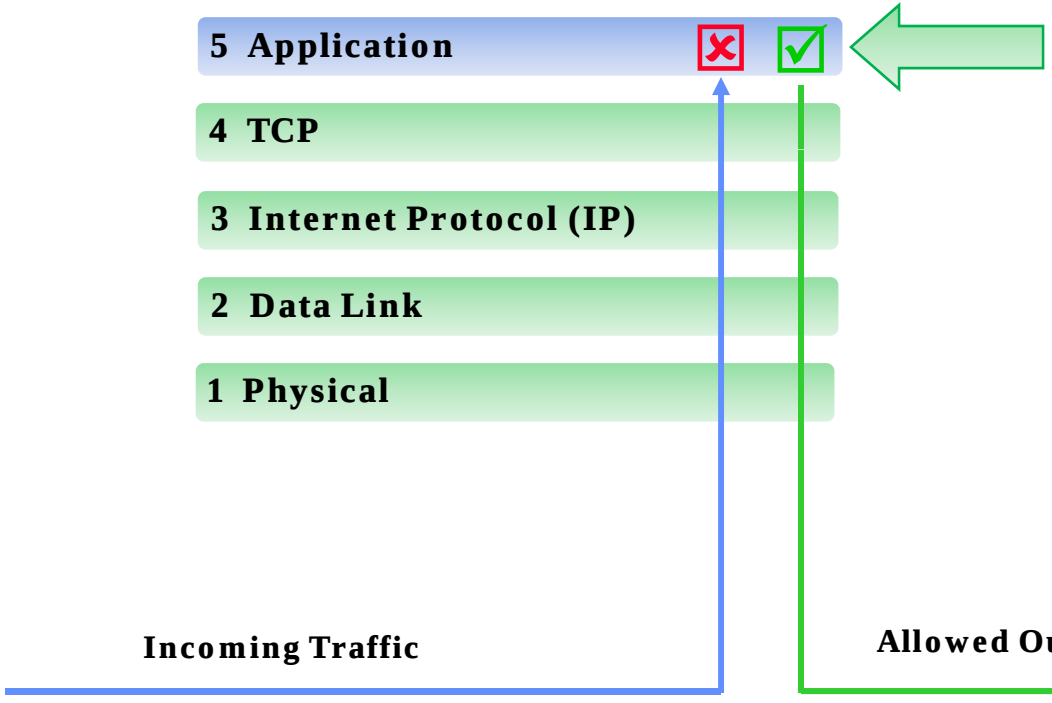
Application-Level Firewall

- Application-level gateways are also called proxies
- They can filter packets at the application layer of the OSI model
- Incoming or outgoing packets cannot access services for which there is no proxy
- An application-level gateway that is configured to be a web proxy will not allow any FTP, gopher, telnet or other traffic through
- Because they examine packets at an application layer, they can filter an application specific commands such as http:post and get

Application Packet Filtering Firewall

☒ = Disallowed

☑ = Allowed



Traffic is filtered based on specified application rules, such as specified applications (such as a browser) or a protocol, such as FTP, or combinations

Unknown traffic is only allowed up to the top of Network Stack

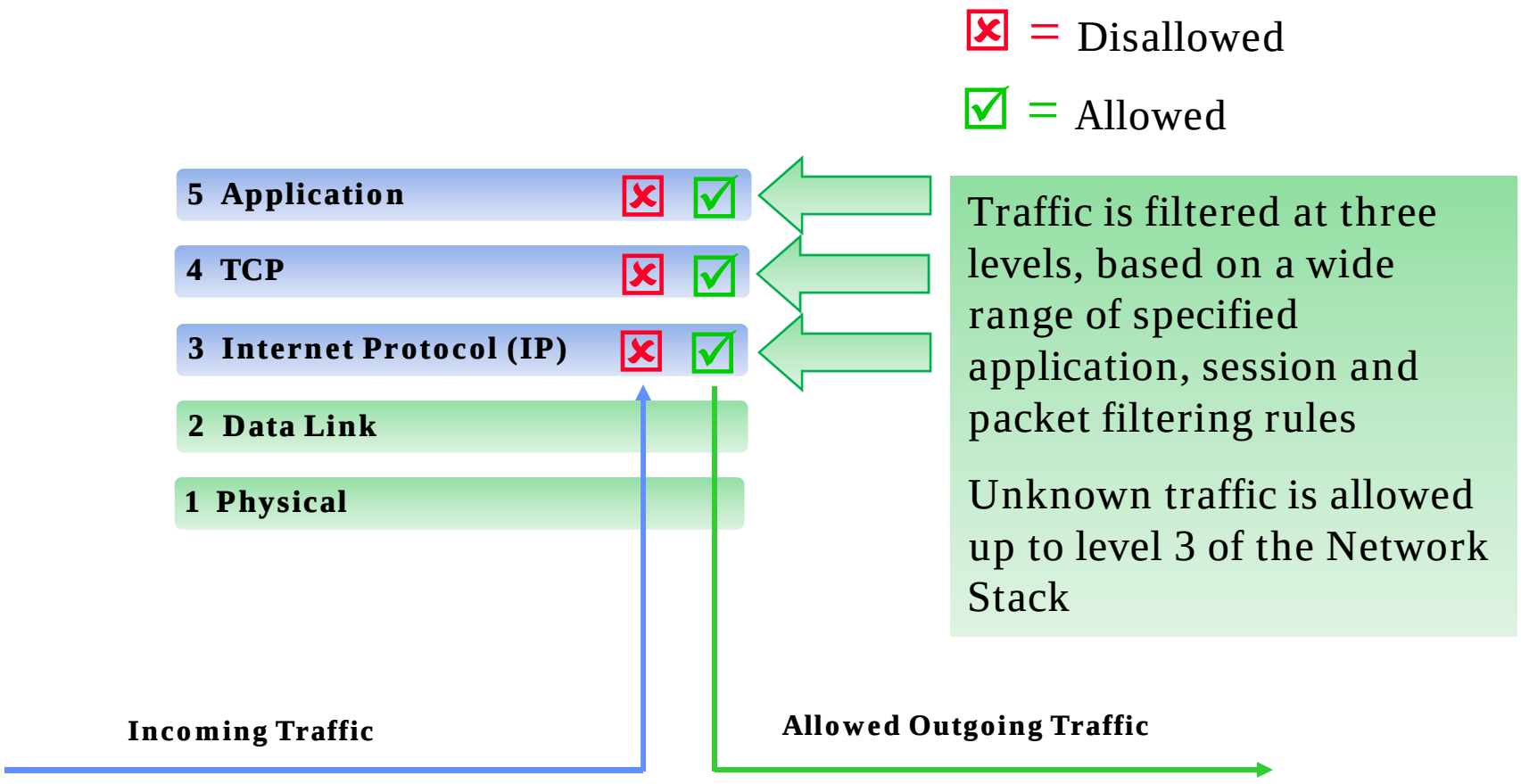
Stateful Multilayer Inspection Firewall

Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls

They filter packets at the network layer, to determine whether session packets are legitimate, and they evaluate the contents of packets at the application layer

They are expensive and require competent personnel to administer the device

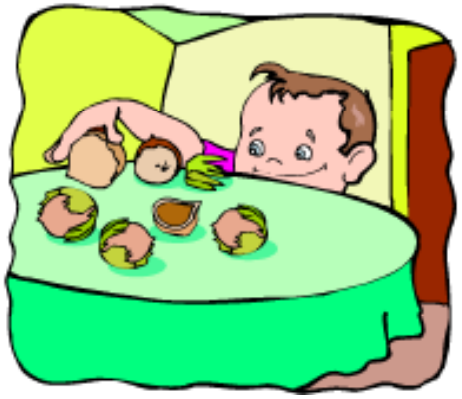
Packet Filtering Firewall



Firewall Identification

Listed below are a few techniques that can be used to effectively determine the type, version, and rules of almost every firewall on a network

- Port Scanning
- Firewalking
- Banner Grabbing



Firewalking

Firewalking is a method to collect information from remote networks that are behind firewalls

It probes ACLs on packet filtering routers/firewalls

Firewalking requires three hosts:

- Firewalking Host
- Gateway Host
- Destination Host

Banner Grabbing

Banners are messages sent out by network services while connecting to the service

They announce which service is running on the system

Banner grabbing is a simple method of OS detection

Banner grabbing also helps in detecting services run by firewalls

The three main services which send out banners are FTP, telnet, and web servers

An example of SMTP banner grabbing is:

- telnet mail.targetcompany.org 25

Breaching Firewalls

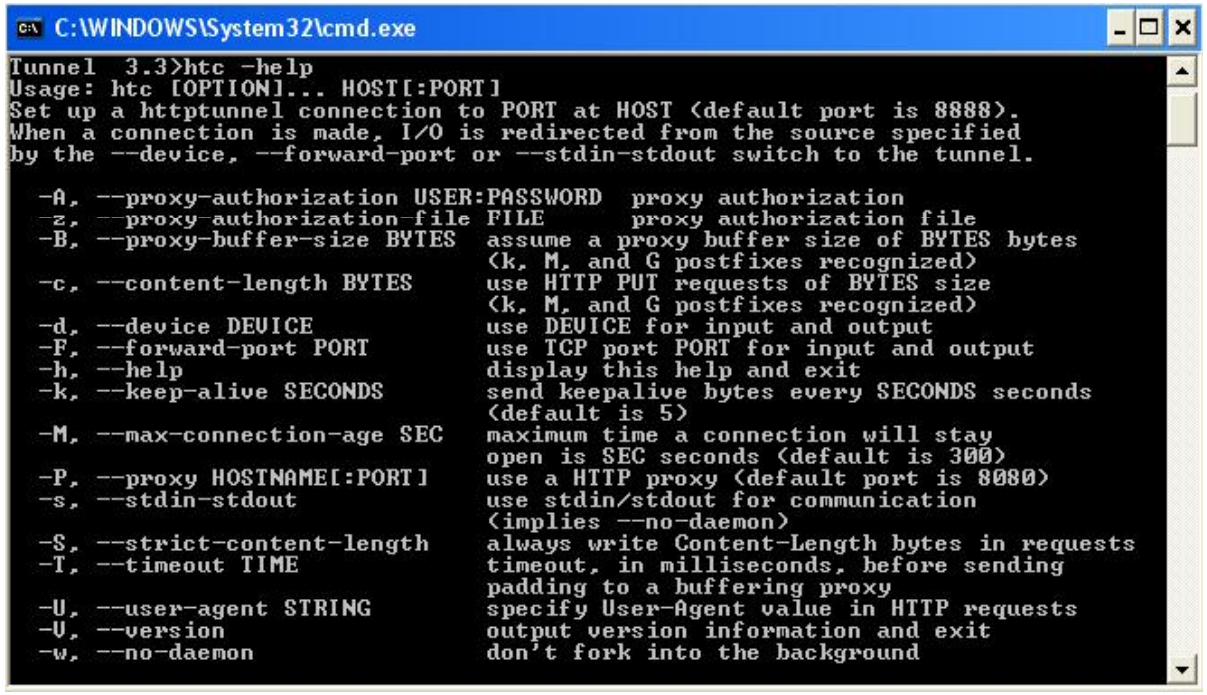
One of the easiest and most common ways for an attacker to slip by a firewall is by installing network software on an internal system, which communicates by using a port address permitted by the firewall's configuration

A popular port is TCP port 80, which is normally used by the web server

Many firewalls permit traffic by using port 80 by default

Bypassing a Firewall Using HTTP Tunnel

Httptunnel creates a bi-directional virtual data path tunneled in HTTP requests. The requests can be sent via an HTTP proxy, if desired



Placing Backdoors Through Firewalls

The Reverse WWW Shell

This backdoor should work through any firewall that allows users to surf the WWW. A program is run on the internal host that produces a child everyday at a special time

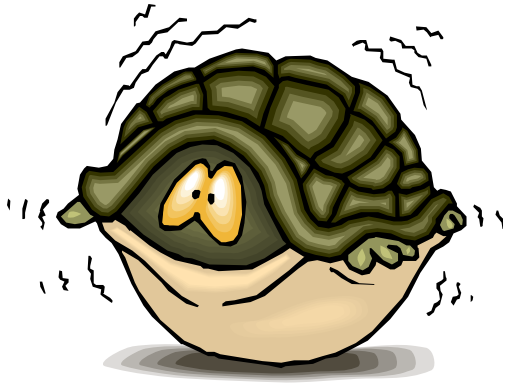
For the firewall, this child acts like a user; using the browser client to surf the Internet. In reality, this child executes a local shell, and connects to the WWW server operated by the hacker via a legitimate-looking http request, and sends a stand-by signal

The legitimate-looking answer of the WWW server operated by the hacker is, in reality, the command the child will execute on its machine in the local shell

Hiding behind a Covert Channel: LOKI

LOKI is an information tunneling program. It uses Internet Control Message Protocol (ICMP) echo response packets to carry its payload. ICMP echo response packets are normally received by the Ping program, and many firewalls permit the responses to pass

Simple shell commands are used to tunnel inside ICMP_ECHO/ICMP_ECHOREPLY and DNS name lookup query/reply traffic. To the network protocol analyzer, this traffic seems like ordinary packets of the corresponding protocol. However, to the correct listener (the LOKI2 daemon), the packets are recognized for what they really are



Tool: NCovert

NCovert allows to hide users network file transfers across the Internet

It hides your file transfer by cloaking it in seemingly harmless data using packet forgery

Advanced features allow to hide the user's true IP address

With careful planning, the user can hide the target's true IP address

ACK Tunneling

Trojans normally use ordinary TCP or UDP communication between their client and server parts

Any firewall between the attacker and the victim that blocks incoming traffic will usually stop all Trojans from working. ICMP tunneling has existed for quite some time now, and blocking ICMP in the firewall is considered safe

ACK Tunneling works through firewalls that do not apply their rule sets on TCP ACK segments (ordinary packet filters that belong to this class of firewalls)

Tools to Breach Firewalls

007 Shell

- 007 Shell is a covert shell ICMP tunneling program. It works similar to LOKI
- It works by putting data streams in the ICMP message past the usual 4-bytes (8-bit type, 8-bit code, and 16-bit checksum)

ICMP Shell

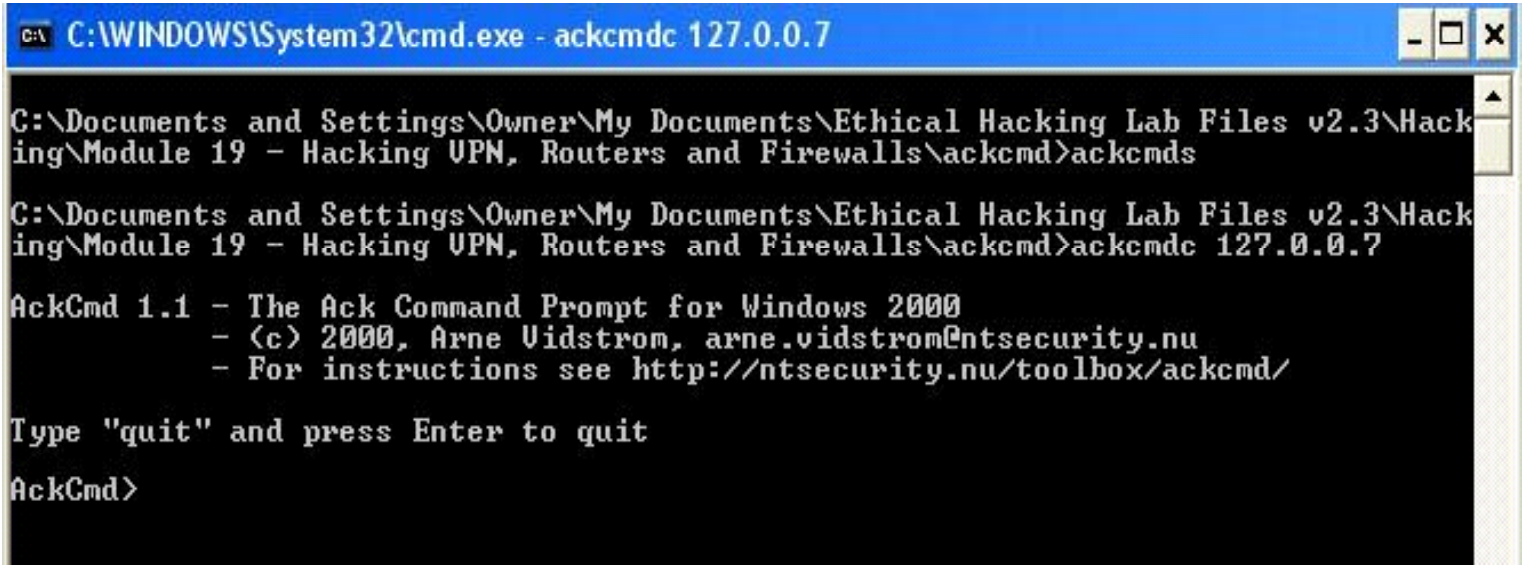
- ICMP Shell (ISH) is a telnet-like protocol. It provides the capability of connecting a remote host to an open shell, using only ICMP for input and output
- The ISH server runs as a daemon on the server side. When the server receives a request from the client, it will strip the header and look at the ID field. If it matches the server's ID, then it will pipe the data to "/bin/sh."
- It will then read the results from the pipe and send them back to the client, where the client then prints the data to stdout

Tools to Breach Firewalls (cont'd)

AckCmd

AckCmd is a client/server combination for Windows 2000 that opens a remote command prompt to another system (running the server part of AckCmd)

It communicates using only TCP ACK segments. This way the client component is able to directly contact the server component through the firewall



Tools to Breach Firewalls (cont'd)

Covert_TCP 1.0

- Covert_TCP 1.0 manipulates the TCP/IP header to transfer a file, one byte at a time, to a destination host
- Data can be transmitted by concealing it in the IP header
- This technique helps in breaching a firewall from the inside, as well as exporting data with innocent-looking packets that contain insufficient data for sniffers or firewalls to analyze

Common Tool for Testing Firewall and IDS

Firewall Tester

- Written by **Andrea Barisani** , who is a system administrator and security consultant
- Firewall Tester is a tool designed for testing firewalls and Intrusion Detection Systems
- It is based on a client/server architecture for generating real TCP/IP connections
- The client is a packet generator tool (ftest), while the server (ftestd) is an intelligent network listener capable of processing and replying to ftest-generated packets. All packets generated by ftest have a special signature encoded in the payload that permits identification

IDS Testing Tool - IDS Informer

BLADE Software's **IDS Informer** application safely tests the effectiveness of any intrusion detection system (IDS), or intrusion prevention (IPS) system, in a lab or production environment

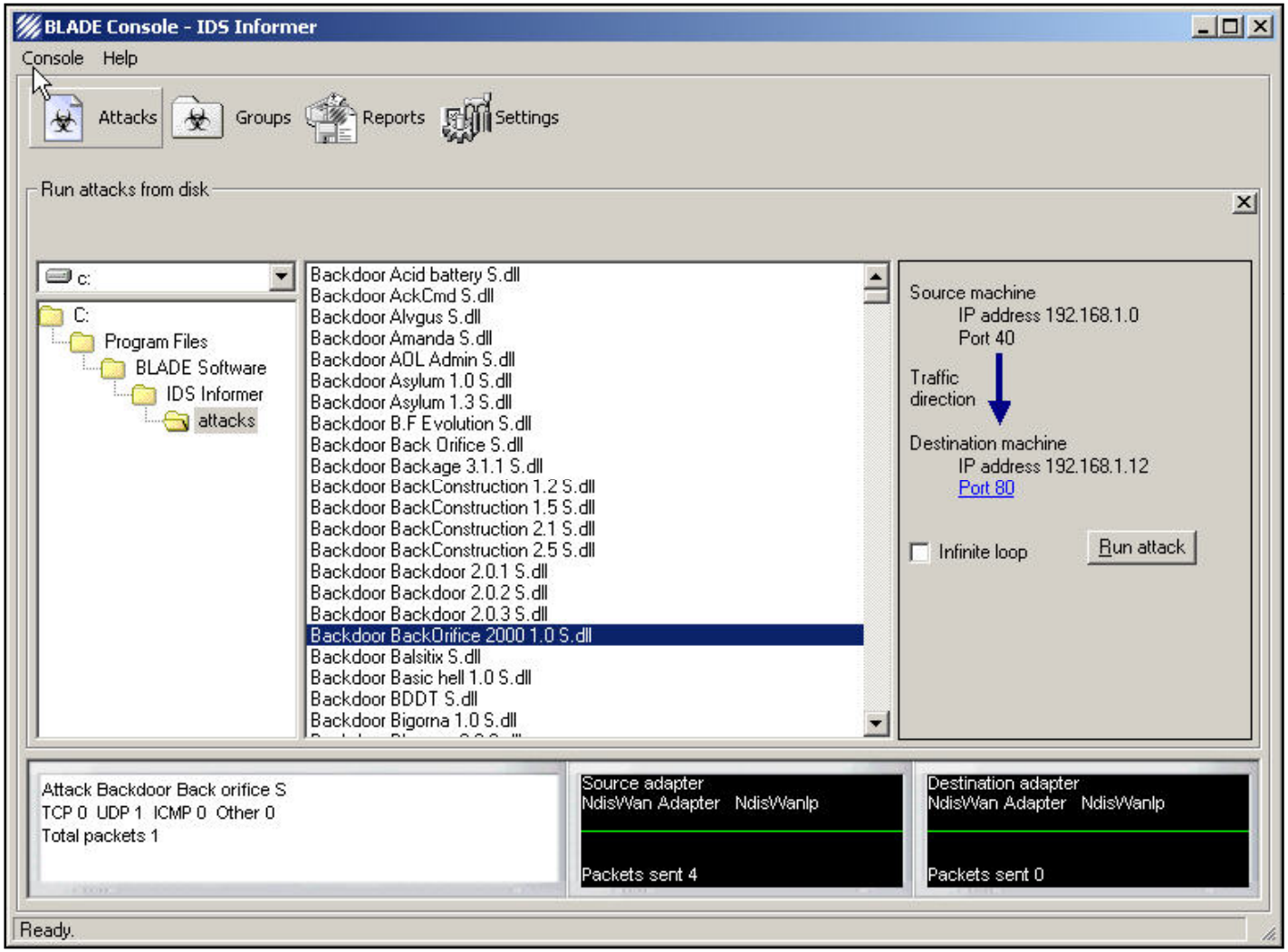
It takes only a few seconds to create and run tests in IDS Informer, and each test can contain any number of simulated attacks

http://www.bladesoftware.net/

IDS Testing Tool - IDS Informer (cont'd)

- Replay pre-defined network traffic to validate policy compliance without putting production systems at risk
- Customize testing via rate of transmission (per attack and per packet), packet time-out, and expiration values
- Retransmit stateful attacks between two unique hosts from a single PC
- Spoof any source or destination IP address and port combination
- Spoof any source or destination MAC address
- Guarantee packet delivery
- Control packet expiration, timeout, and retries

IDS Informer: Screenshot



IDS Testing Tool - Evasion Gateway

Evasion Gateway applies known evasion techniques to circumvent firewalls, routers, and intrusion detection systems (IDS)

Evasion Gateway searches for a wide-range of host-based vulnerabilities, and validates network requirements such as, the minimum acceptable pack fragmentation size

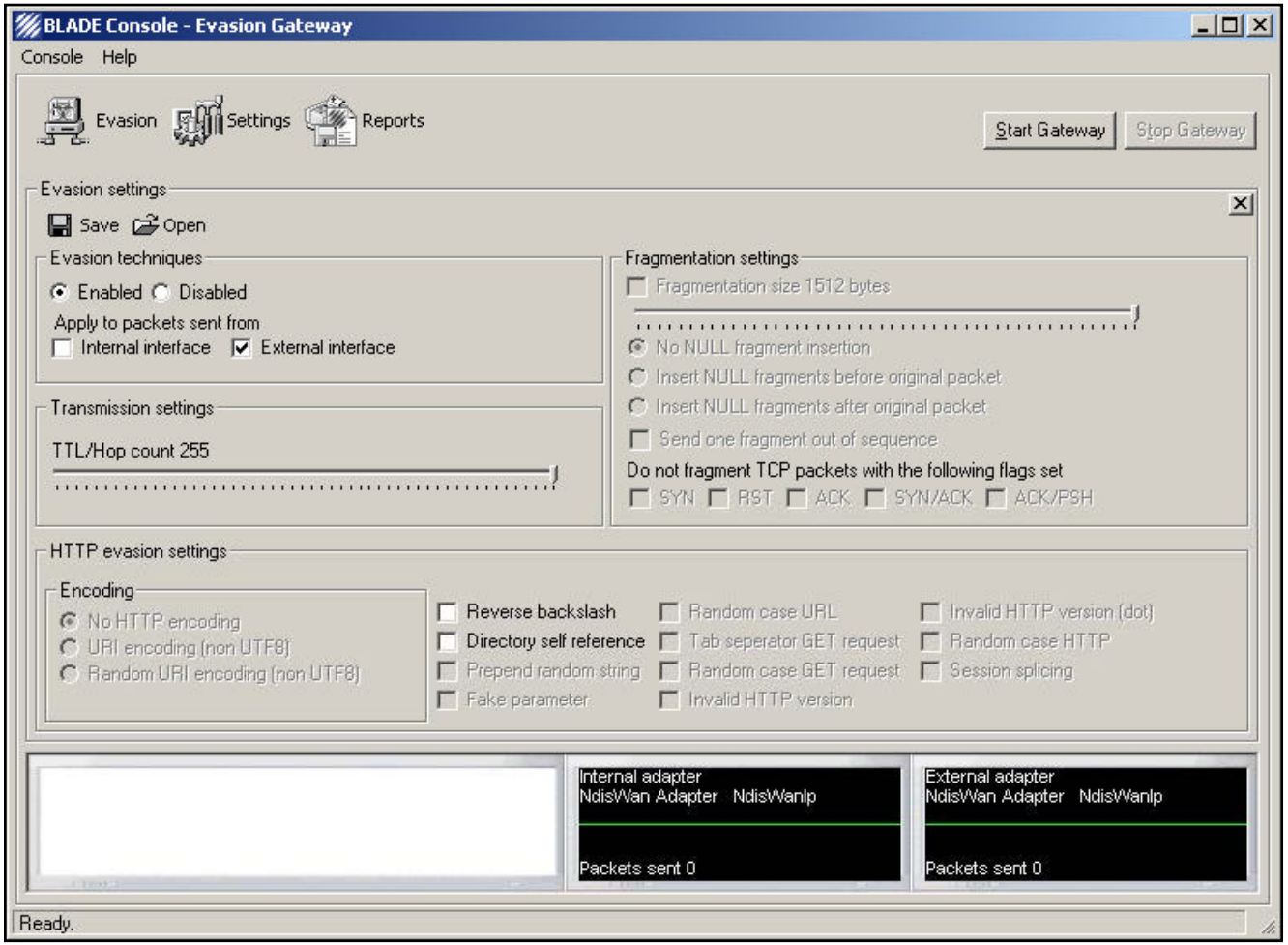
Clear, concise, results from these tests help administrators to identify hidden and unexpected weaknesses, and improve the overall security posture

IDS Testing Tool - Evasion Gateway (cont'd)

Features:

- Bi-directional network based evasion
- Fragmentation
- HTTP Evasion
- URI Encoding
- Random URI encoding (non UTF8, random hex encoding)

Evasion Gateway: Screenshot



IDS Tool: Event Monitoring Enabling Responses to Anomalous Live Disturbances (Emerald)

The EMERALD environment is a distributed scalable tool suite for tracking malicious activity through and across large networks

Features:

- Presents a structure to associate the results of the tool's distributed analysis
- Enables world-wide exposure and reaction ability towards synchronized attacks
- Monitors set of units that analyze, operate, and respond in the network

IDS Tool: BlackICE

BlackICE consists of an intrusion detection system that warns about attacks and resists threats against the Systems

It has PC and Server protection for Windows-based systems

Features:

- Blocks illegitimate communications
- Warns the user of threat
- Reports the details of threats
- Consists of integrated Firewall and Intrusion detection system

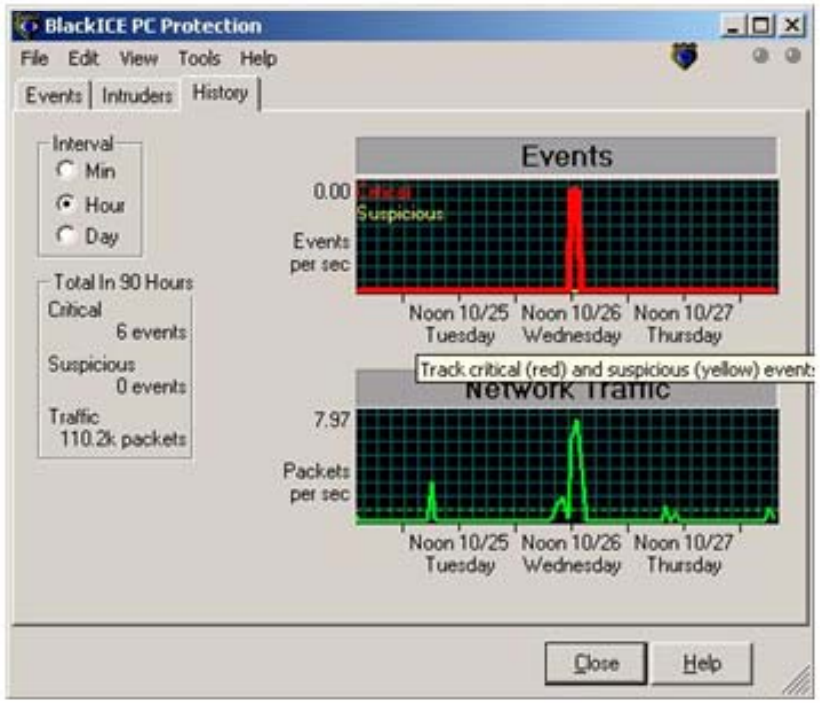


Fig: BlackICE

IDS Tool: Next-Generation Intrusion Detection Expert System (NIDES)

NIDES performs real-time check of user action on several target systems linked via Ethernet

It uses C, Perl languages to write 'agen' process for both Sun and non-Sun platforms

Features:

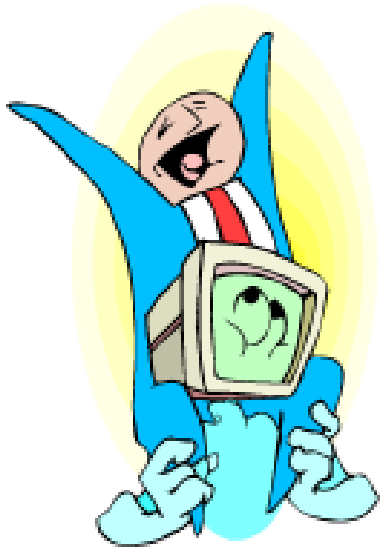
- Has optimized storage structures
- Reports the status of System and target host
- Increases the number of rules generating alert information

IDS Tool: SecureHost

SecureHost avoids attacks by immediately halting the suspected applications

Features:

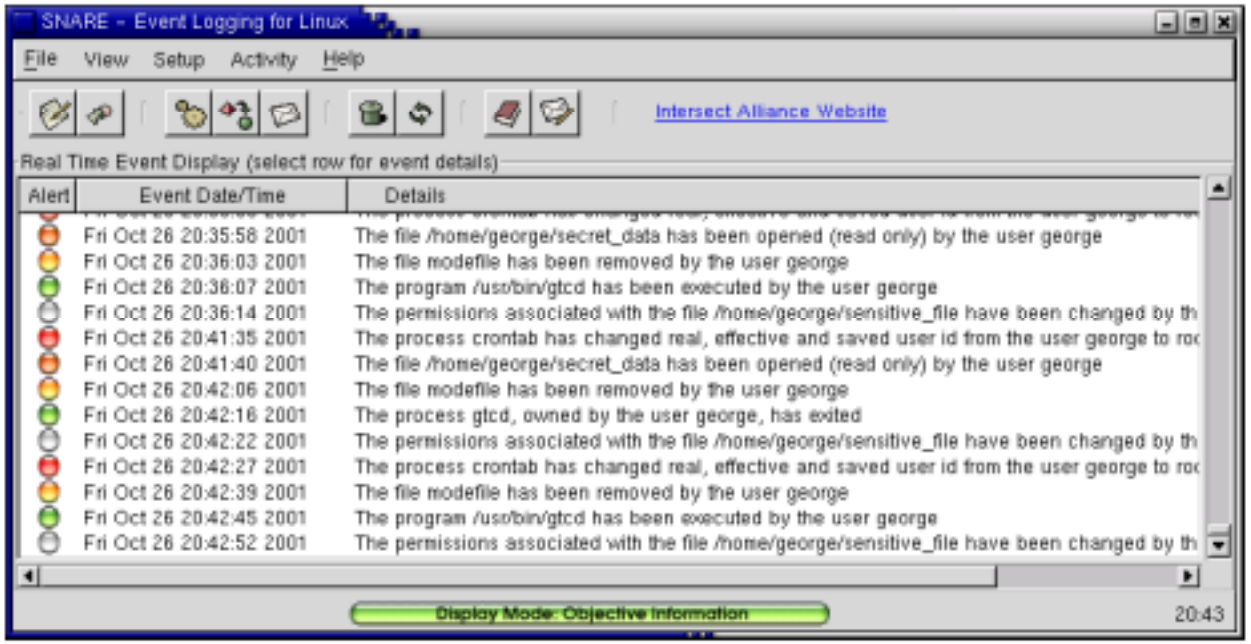
- Supervises the Enterprise network for application performance
- Integrates with other SecureNet intrusion detection products, thus maximizing security
- Monitors file integrity in real time
- Reduces downtime of network components



IDS Tool: Snare

Snare stands for System iNtrusion Analysis and Report Environment

SNARE is an open source host based Intrusion Detection tool designed for Linux OS



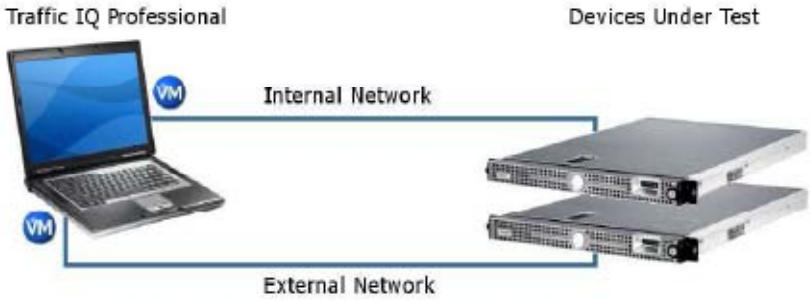
IDS Testing Tool: Traffic IQ Professional

Traffic IQ Professional enables security professionals to quickly and easily audit and validate the behavior of security devices by generating standard application traffic or attack traffic between two virtual machines

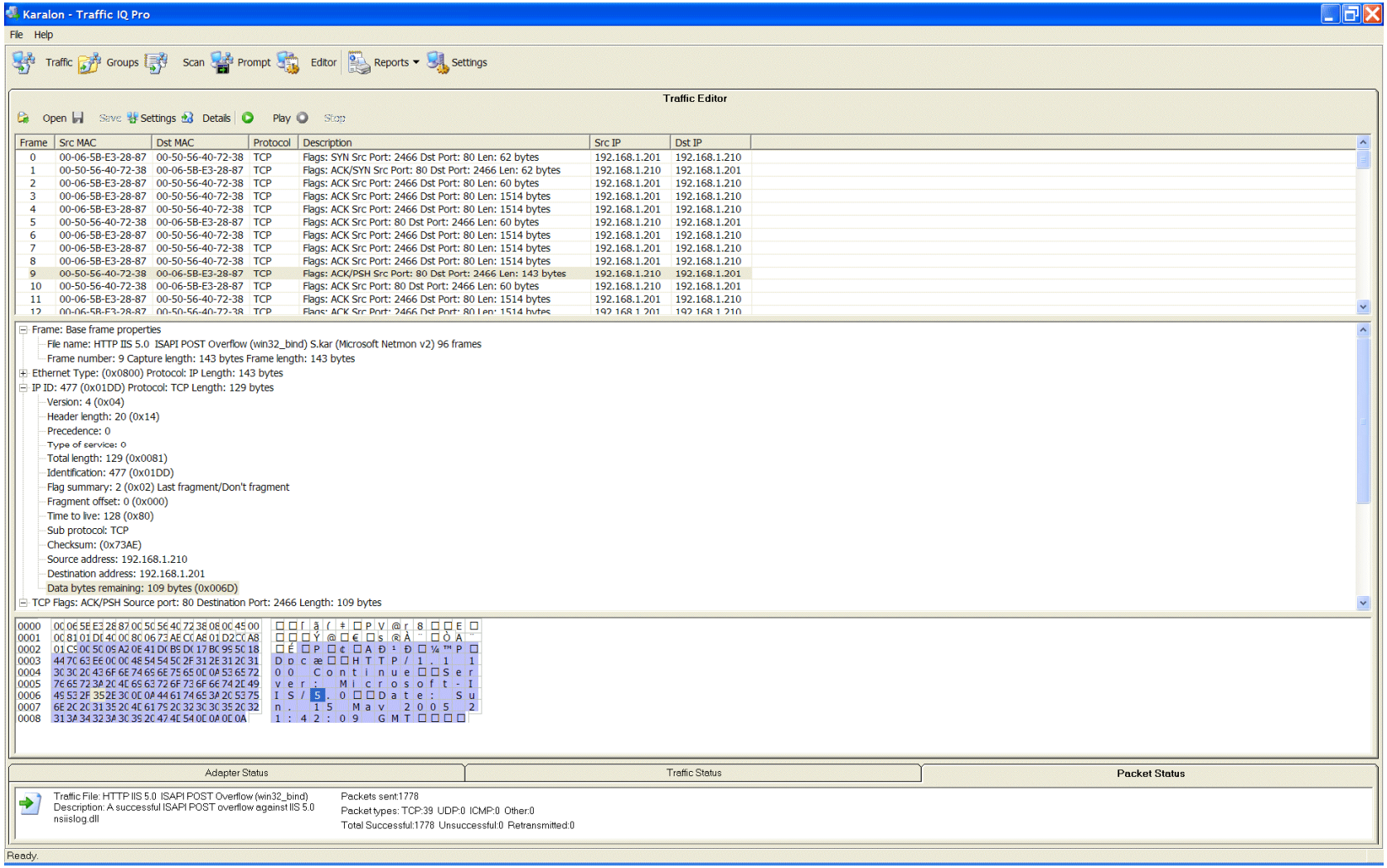
The unique features and packet transmission capabilities of Traffic IQ Professional make the tasks of reliably auditing, validating, and proving security compliance , easy and quick to complete

Traffic IQ Professional can be used to assess, audit, and test the behavioral characteristics of any non-proxy packet-filtering device including:

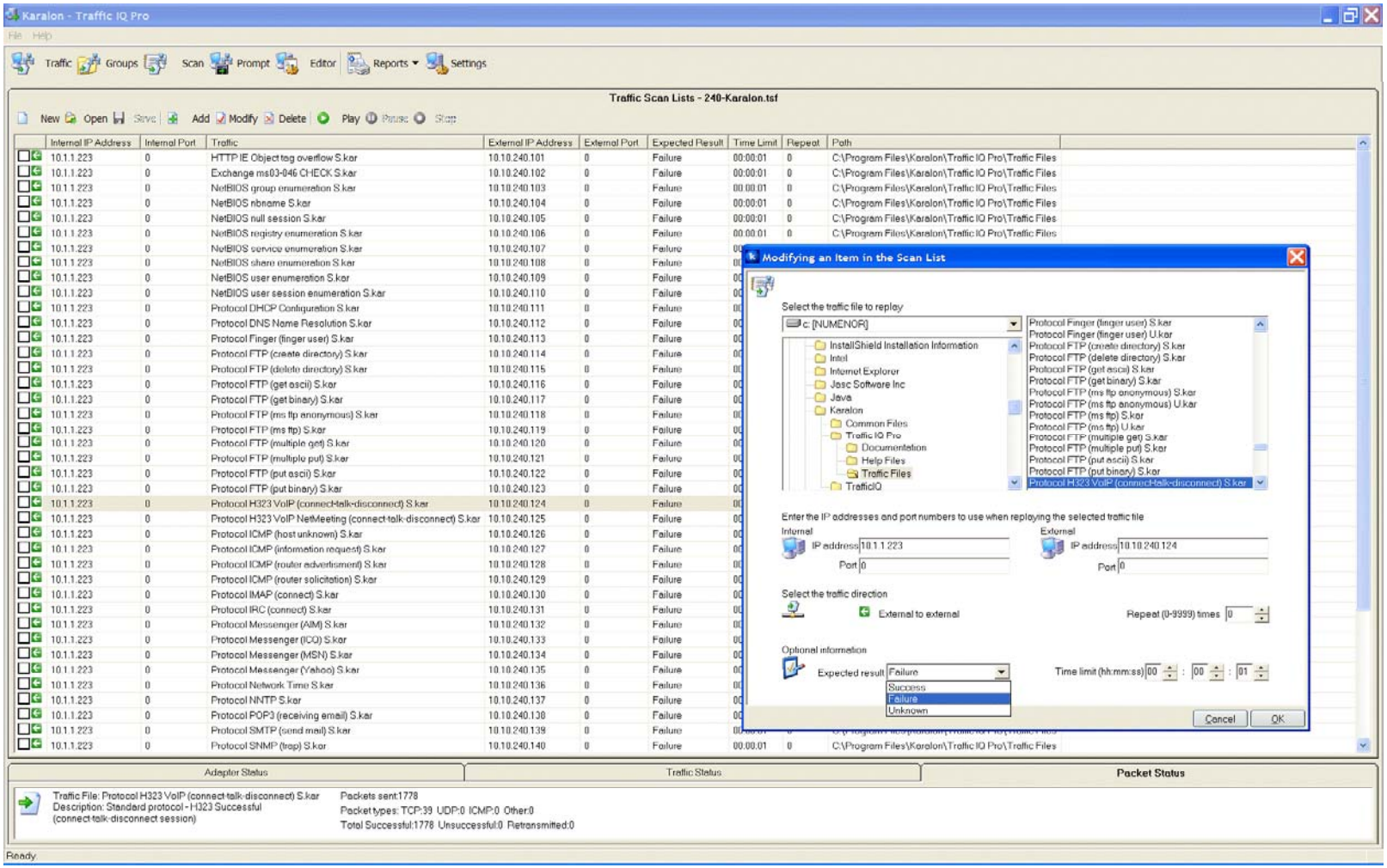
- Application layer firewalls
- Intrusion detection systems
- Intrusion prevention systems
- Routers and switches



Traffic IQ Professional: Screenshot 1



Traffic IQ Professional: Screenshot 2



IDS Testing Tool: TCPOpera

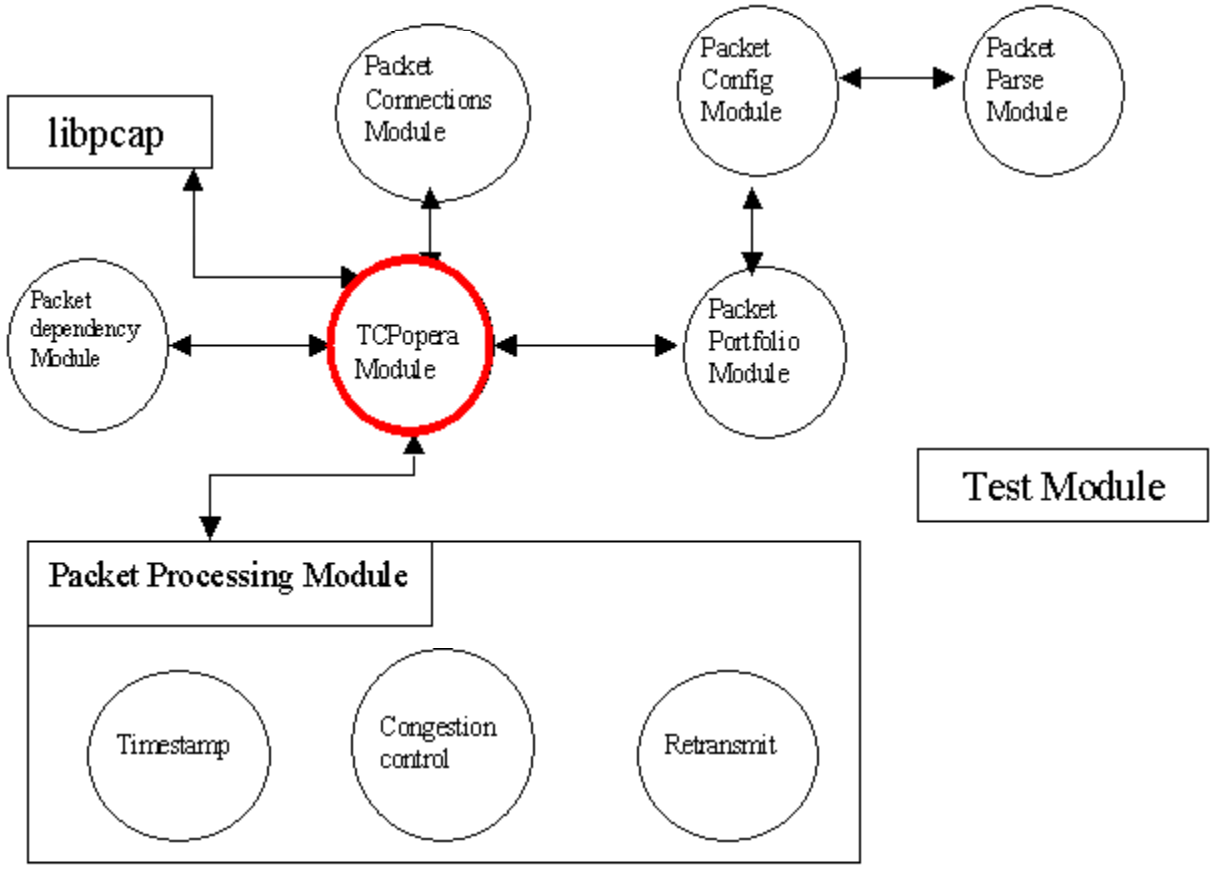
TCPopera is a tool that extends TCPreplay by allowing users to define network conditions and play out traffic in a realistic environment where packets may be delayed or lost

How would TCPopera aid in IDS testing?

- Does the IDS track TCP connection state?
- How well does the IDS perform under different network conditions (false positives!)?
- How does the IDS handle retransmitted packets?

TCPopera has the potential to provide IDS testing environments with traffic that exhibits TCP behavior quickly

TCPOpera (cont'd)



IDS Testing Tool - Firewall Informer

The Firewall Informer application actively tests the configuration and performance of any firewall or other packet-filtering device, including, routers, switches, and gateways

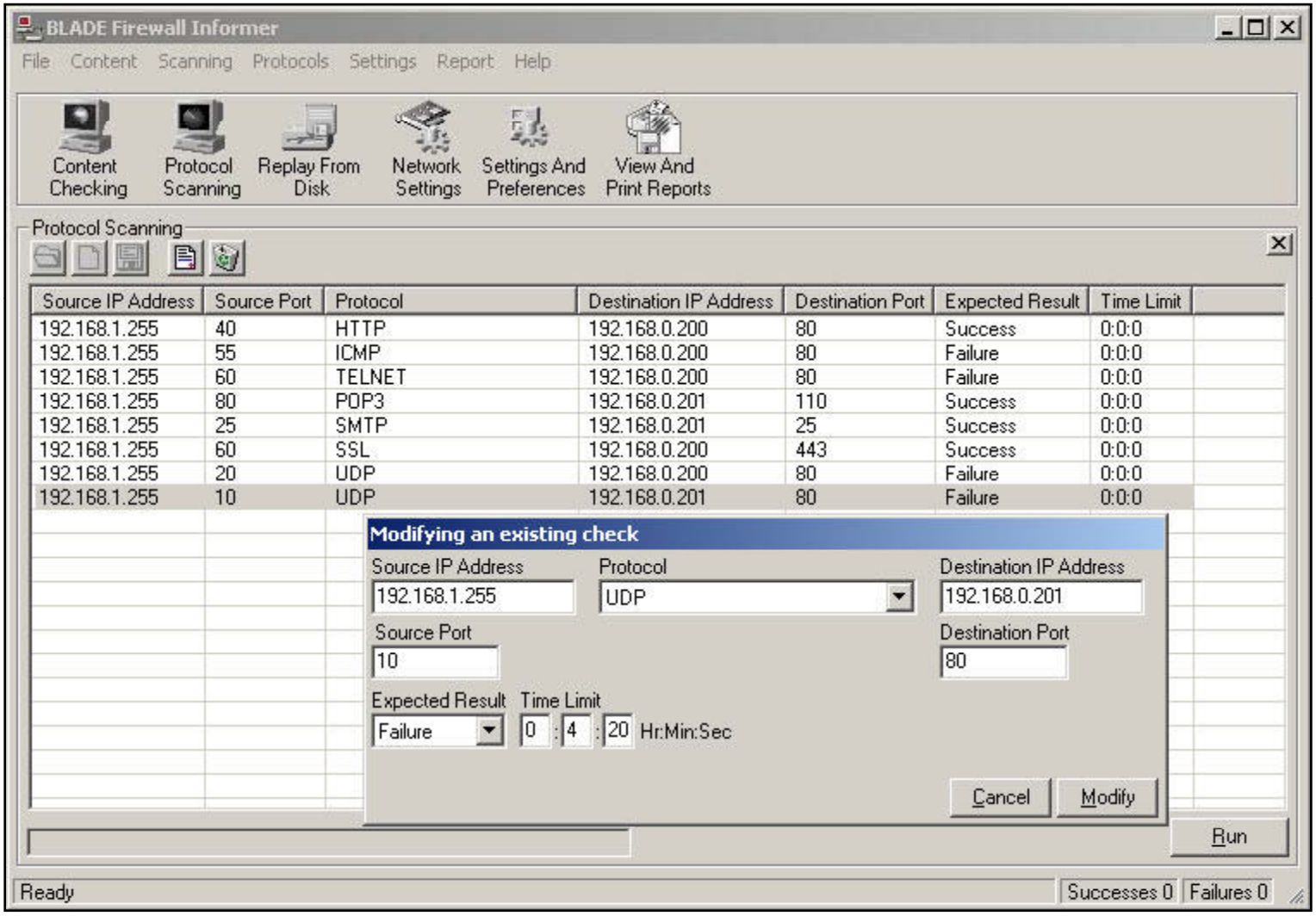
Unlike the passive approach of vulnerability assessment products, Firewall Informer uses BLADE Software's patent-pending **S.A.F.E.** (**S**imulated **A**ttack **F**or **E**valuation) technology, to actively and safely test security infrastructures with real-world exploits to determine if devices are working according to security policies

IDS Testing Tool - Firewall Informer (cont'd)

Features:

- Firewall Informer sends and receives packets without the need for protocols to be bound to the cards
- It customizes testing via rate of transmission (per attack or per packet), packet time-out, and expiration values
- It retransmits stateful attacks between two unique hosts from one PC
- It spoofs any source or destination IP address and port combination
- It spoofs any source or destination MAC address
- It guarantees packet delivery
- It controls packet expirations, timeouts, and retries

Firewall Informer: Screenshot



Atelier Web Firewall Tester

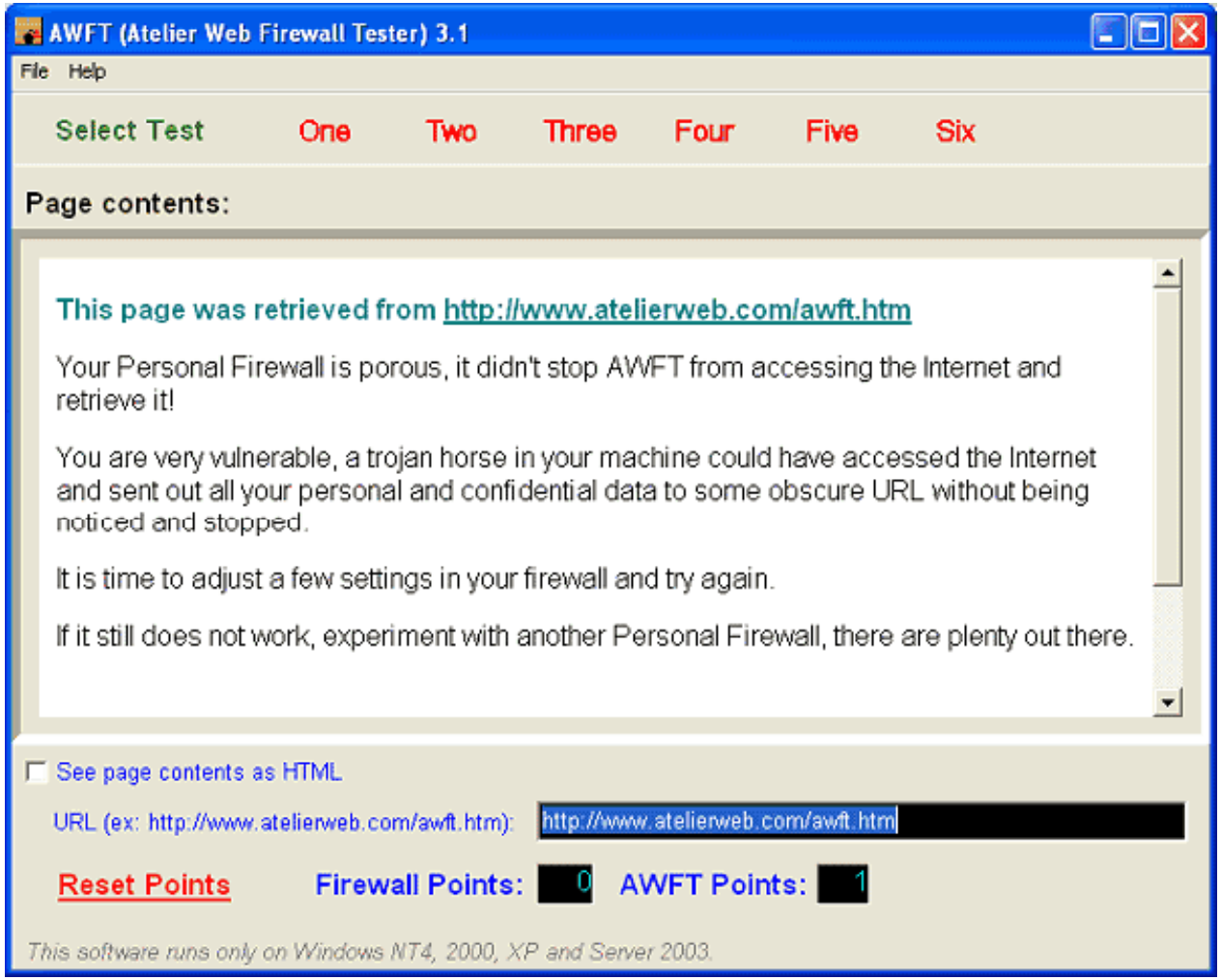
www.atelierweb.com

Atelier web firewall tester is a tool for probing personal firewall software strengths against outbound connection attempts from unauthorized programs

It is intended to help you tweak your existing personal firewall software for improved protection or make a rational choice of a PF within the available alternatives in the market-place

It offers 6 different tests; each of them establishes a HTTP connection and attempts to download a web page

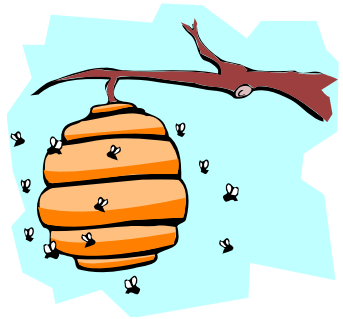
Atelier Web Firewall Tester: Screenshot



Honeypot

What is a Honeypot

A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource



It has no production value; anything going to, or from a honeypot, is likely a probe, attack, or compromise

A honeypot can be used to log access attempts to those ports including the attacker's keystrokes. This could send early warnings of a more concerted attack

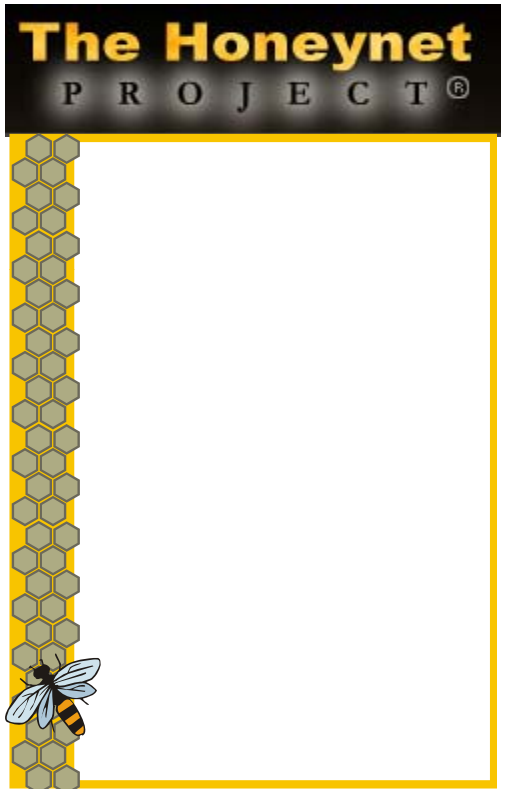
The Honeynet Project

Founded in April 1999, “The Honeynet Project” is a non-profit research organization of security professionals, dedicated to information security

All the work of the organization is open source and shared with the security community

The project intends on providing additional information on hackers, such as the motives behind their attacks, how they communicate, when they attack systems, and their actions after compromising a system

The Honeynet Project is a four-phased project
http://www.honeynet.org/



Types of Honeypots

Honeypots are classified into three basic categories:

- Low-interaction honeypot
  - Eg: Specter, Honeyd, and KFSensor
- Medium-interaction honeypot
- High-interaction honeypot
  - Eg: Honeynets

Advantages and Disadvantages of a Honeypot

Advantages:

- Honeypot collects small data sets of high value
- It reduces false positives
- It catches new attacks and reduces false negatives
- It works in encrypted or IPv6 environments
- It is a simple concept requiring minimal resources

Disadvantages:

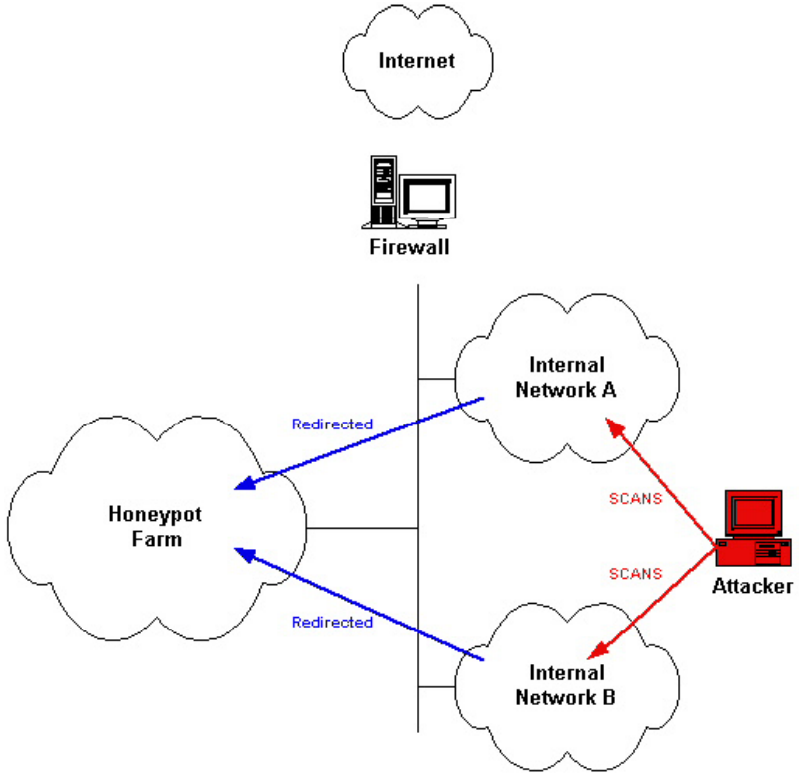
- It has a limited field of view (microscope)
- It involves risk (mainly high-interaction honeypots)

Where to Place a Honeypot

A honeypot should be placed in front of the firewall on the DMZ

Check for the following while placing honeypots:

- Router-addressable
- Static address
- It is not subjected to a fixed location for a long time



Honeypots

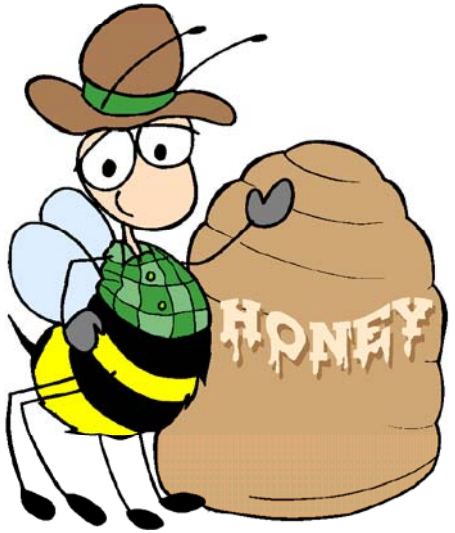
There are both commercial and open source Honeypots available on the Internet

Commercial Honeypots

- KFSensor
- NetBait
- ManTrap
- Specter

Open Source Honeypots

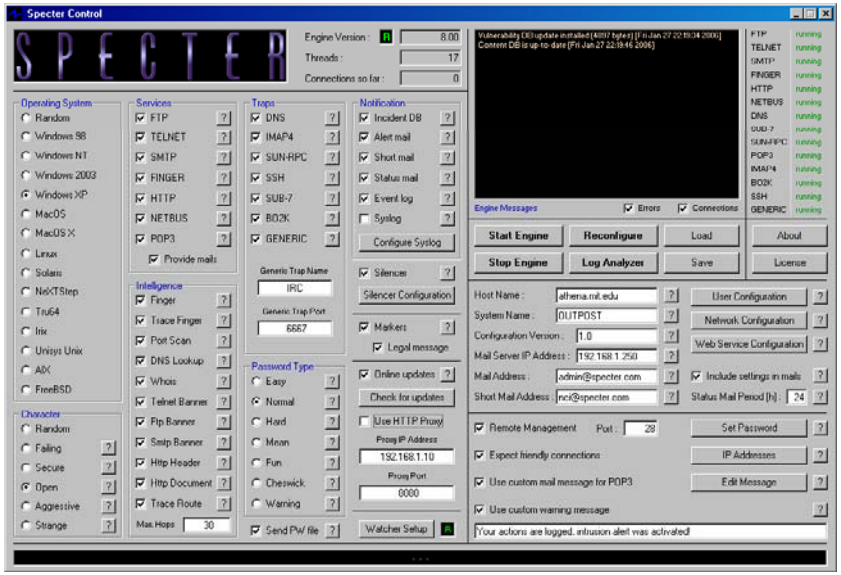
- Bubblegum Proxypot
- Jackpot
- BackOfficer Friendly
- Bait-n-Switch
- Bigeye
- HoneyWeb
- Deception Toolkit
- LaBrea Tarpit
- Honeyd
- Honeynets
- Sendmail SPAM Trap
- Tiny Honeypot



Honeypot-SPECTER

SPECTER is a smart honeypot or deception system

SPECTER automatically investigates the attackers while they are still trying to break in

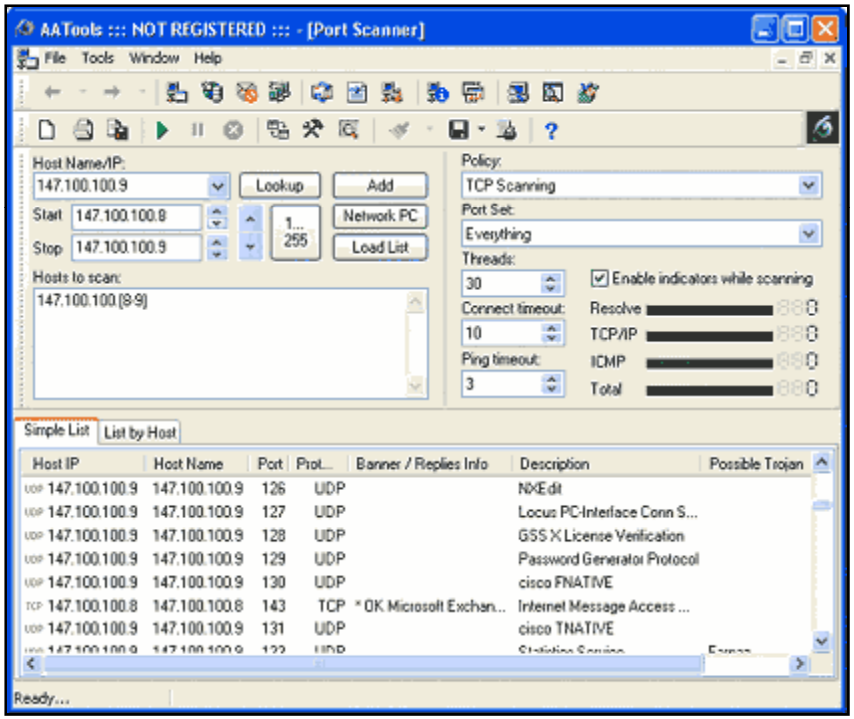


Honeypot - honeyd

Honeyd is maintained and developed by Niels Provos, a software engineer at Google

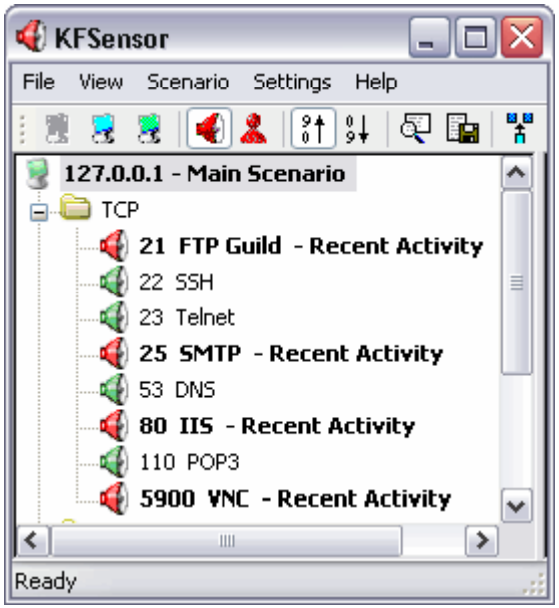
It is a small daemon that creates virtual hosts on a network

It is an open source software released under the GNU General Public License



Honeypot - KFSensor

KFSensor is a host-based Intrusion Detection System (IDS) that acts as a honeypot, to attract and log potential hackers and port scanner-kiddies, by simulating vulnerable system services and Trojans

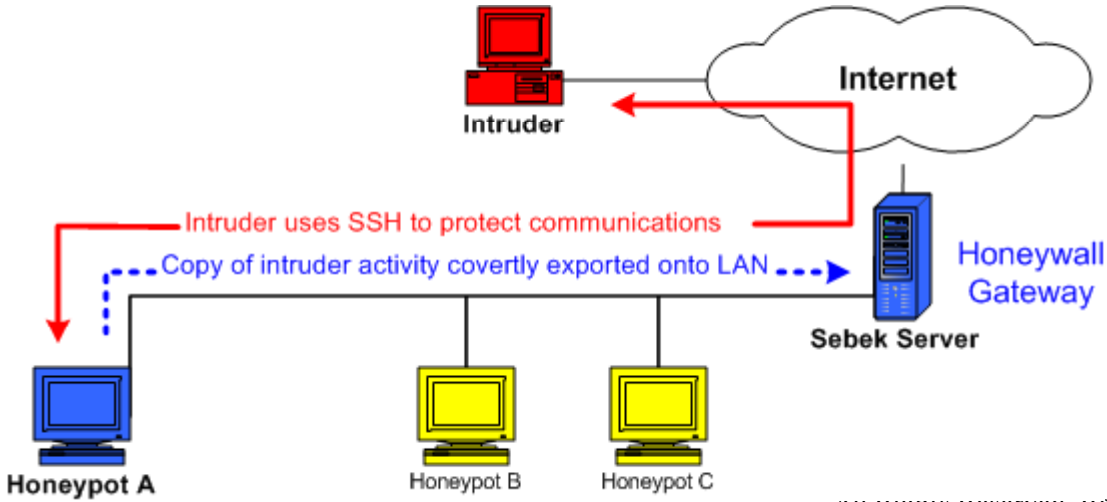


Sebek

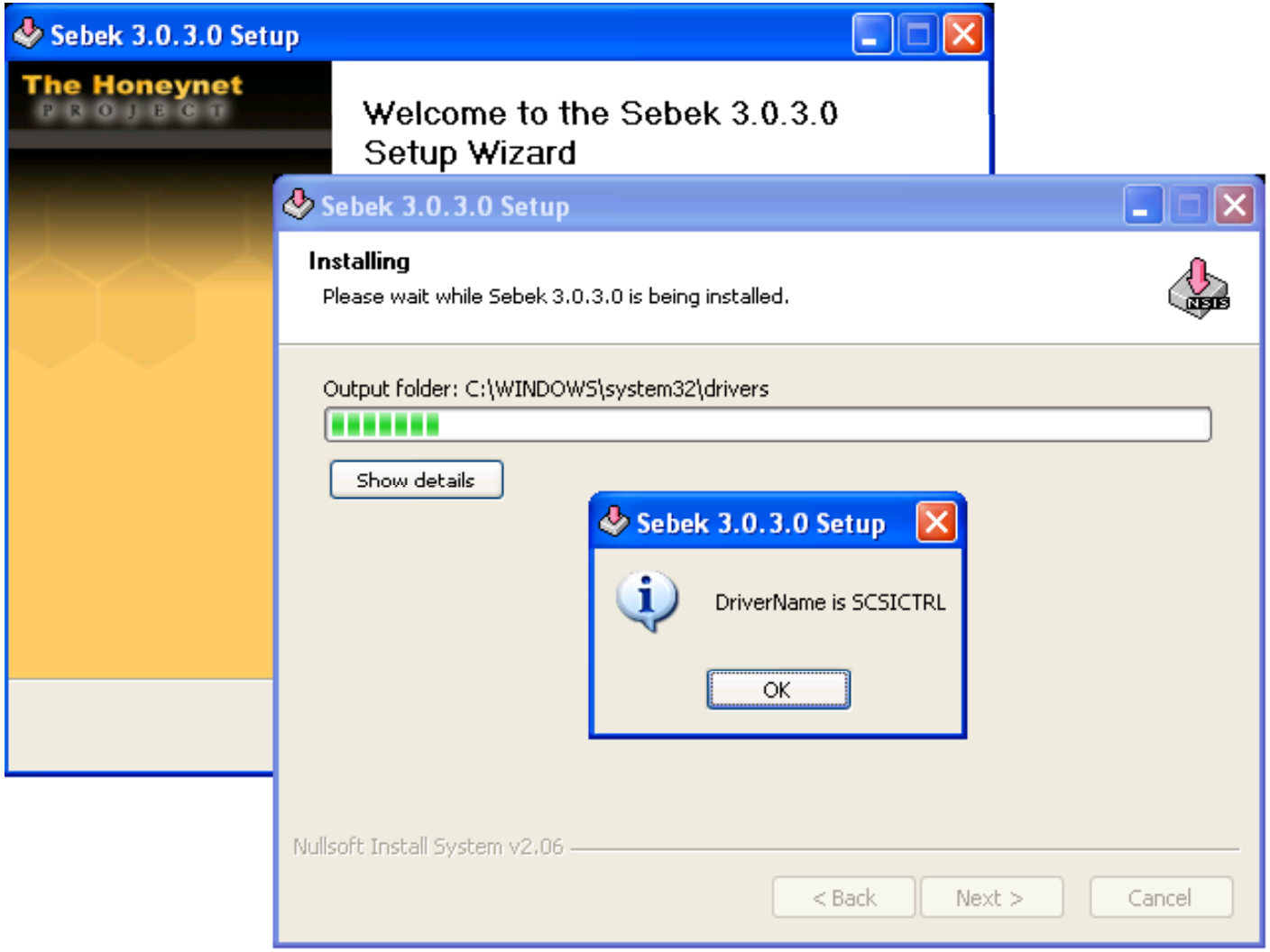
Sebek is a data capture tool

The first versions of Sebek were designed to collect keystroke data from within the kernel

Sebek also provides the ability to monitor the internal workings of the honeypot in a glass-box manner, as compared to the previous black-box techniques



Sebek: Screenshot



Physical and Virtual Honeypots

Physical Honeypots	Virtual Honeypots
A physical honeypot is a real machine on the network with its own IP address	A virtual honeypot is simulated by another machine that responds to network traffic sent to the virtual honeypot
Physical honeypots are often high-interaction, allowing the system to be completely compromised. They are expensive to install and maintain	For large address spaces, it is impractical or impossible to deploy a physical honeypot for each IP address. In that case, virtual honeypots can be deployed

Tools to Detect Honeypots

Send-Safe Honeypot Hunter

- Send-Safe Honeypot Hunter is a tool designed for checking lists of HTTPS and SOCKS proxies for so-called "honeypots"

Nessus Security Scanner

- The Nessus Security Scanner includes NASL (Nessus Attack Scripting Language); a language designed to write security tests easily and quickly
- Nessus has the ability to test SSLized services such as https, smtps, imaps, and more. Nessus can be provided with a certificate so that it can be integrated into a PKI-fied environment

What to do When Hacked

Incident response team:

- Set up an "incident response team." Identify those people who should be called whenever a suspected intrusion is in progress

Response procedure:

- Priorities between network uptime and intrusion should be decided
- Whether or not to pull the network plug on suspected intrusion should be decided
- Should continued intrusion be allowed in order to gather evidence against the intruder?

Lines of communication:

- Mode of propagating the information through corporate hierarchies, from the immediate supervisor up to the CEO
- Decision to inform the FBI or police, and notifying the partners (vendors/customers)

What Happened Next

eGlobal bank contacted Pentes, an external security auditing agency for auditing their system security and finding the cause of attack on their servers. Jason, an expert penetration tester with the company was sent on the site for investigation of the attack.

The initial audit and forensics from the investigation and first test revealed that the attack had resulted largely from mis-configuration of the firewall and poor communication of security rules throughout the Bank's system. Without a documented security policy and with an ineffective firewall, the Bank was unknowingly permitting the transfer of undesirable traffic across the network.

Summary

- Intrusion Detection Systems (IDS) monitor packets on the network wire and attempt to discover if a hacker is trying to break into a system
- System Integrity Verifiers (SIV) monitor system files to find when an intruder changes. Tripwire is one of the popular SIVs
- Intrusion Detection happens either by Anomaly detection or Signature recognition
- An IDS consists of a special TCP/IP stack that reassembles IP datagrams and TCP streams
- Honeypots are programs that simulate one or more network services that are designated on a computer's ports
- A simple Protocol verification system can flag invalid packets. This can include valid, but suspicious, behavior such as several fragmented IP packets
- In order to effectively detect intrusions that use invalid protocol behavior, IDS must re-implement a wide variety of application-layer protocols to detect suspicious or invalid behavior
- One of the easiest and most common ways for an attacker to slip by a firewall is by installing network software on an internal system, that uses a port address permitted by the firewall's configuration

"The toaster pastry fits right into the floppy drive! This allows you to transfer data from your computer to your mouth. The information is stored in your fat cells, thus transforming your pot belly into a high-capacity hard drive!"

"Yesterday I changed everyone's password to 'password'. I sent it to everyone in a memo, put it on a big sign on the wall and printed it on all of the coffee cups. Guess how many people called me this morning because they forgot the password."