Global Information Assurance Certification Paper

Personal Firewall - BlackICE PC Protection 3.5
SANS Security Essentials, GSEC Practical Assignment
Version 2.0, Option 1
Chai Heng, Tan
August 25, 2002

Abstract

It is not an overstatement I believe to say that the Internet is the most successful sort of a big scale open-access implementation. Started as a closed network of researchers who exchanged scientific information, today its availability to the public has enabled phenomenal number of users, including some unethical users, to gain access to Internet. Widespread implementation of information protection and access control has thus become a significant issue in today's fast-paced, Internet-driven world. And with so many users, network security weaknesses are quite easily exposed; making Internet sites risk inevitable break-ins and resultant damage. The need to protect these sites, servers, workstations etc. is unavoidable; it is both crucial and essential. This is where firewalls come into play.

Introduction

In this document, I will describe the implementation of a personal firewall, BlackICE PC Protection (prior to version 3.5, the software is known as BlackICE Defender), from Internet Security Systems (ISS) as a personal firewall. It ensures that all communications attempting to access the local computer or originating from it meet individuals' security policy needs. Its simplicity and effectiveness render it very helpful for beginners. It works on dial-up, LAN, cable modem, DSL router and even Wireless connections. Related concepts pertaining to BlackICE such as firewalls and intrusion detection system will also be presented here.

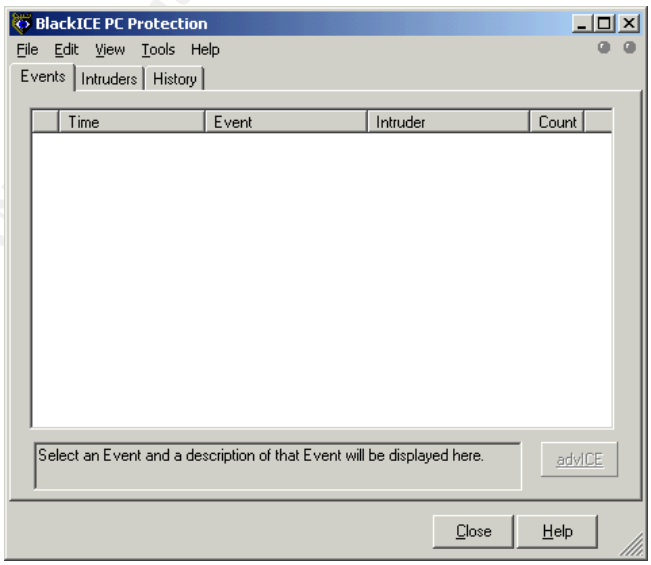

Figure 1

Firewall Overview

A firewall can be software or hardware-based device that acts as a protector in between 2 or more networks, separating and safeguarding traffic from each other. Usually firewalls work by examining the network packets traversing through it, and based on the pre-defined rule sets (source and destination IP address, source and destination ports, combination of these, etc.) and making decision on either accepting or rejecting the packets. There are a number of types of firewalls available nowadays, and more advanced discoveries and innovations will create more in the future.

1. Router firewall – The most traditional form of firewall. Some may argue that a router is not a firewall in true sense, as it lacks the level of flexibility and features that a full-security enterprise firewall. Also, it can only make limited decisions on packets traveling through it. Most routers on the Internet make use of access-lists to provide speed and functionality and this more or less is done with the expense of routed packets' security. This is why enterprise and personal firewalls are implemented; to assist in filtering and securing the internal networks and workstations from outside threats by complementing the routers.

2. Packet filters – operating at network layer (Layer 3 of the OSI model*), this type of firewalls are fast and software-based, although not as fast as hardware based firewalls (MAC layer* firewalls). MAC (Media Access Control) Layer is one of the 2 components that make up Layer 2 (DataLink Layer) of the OSI model. It is fast because the packets traversing through the firewall need not be inspected by another upper layer before routing decisions are made. As its name implies, a packet filter works by inspecting every packet that passes through the firewall. Checking each whole individual packet will render the firewall useless, as it will be bogged down by the inspection overheads. As such, only the content of individual packet headers are checked. Like routers, decisions are made based on the source and destination address as well as ports in IP packets since rulesets are defined based on these parameters too.

   *Further information regarding OSI and MAC layers can be found at http://webopedia.internet.com/quick_ref/OSI_Layers.asp

3. Proxy systems - packet filters firewalls allow a direct connections between 2 end systems once the initial connect-request has been approved, more or less like an open tunnel through the firewall.

Figure 2

As Figure 2 shows, a connection initiated by a user will terminate at the firewall and a new connection will be established to the target host and vice versa. Thus any further connection attempted to the same host will need to pass the firewall and subject to inspection by it. The security overhead in this type of filter tends to cause more delay.

4. Stateful packet inspection – firewall technology goes a step further by improving on proxy systems technology; by having "memory" of previously established connections (called dynamic states table). The term "stateful" here implies that the firewall will not only filter the packets, and not only check it based on IP addresses and ports, but also verify each arrived packets to see if they belong to prior sessions or is attempting to establish a new one. If it belongs to an established connection, it will be passed without consuming as much processing power as if it's a new connection. This can be seen as having the best of both worlds. BlackICE PC Protection can be considered as an enhanced type of stateful packet inspection firewall.

Intrusion Detection System (IDS) Overview

In addition to using firewalls to block attacks intrusion detection systems can be utilized to detect and react to them. Attacks in progress and compromised machines behind the firewall that are sending out bogus data etc.can be detected by monitoring the content of the traversing data. A single firewall (conventional method of protection) placed as a security buffer between networks is not sufficient anymore nowadays as no matter how the firewall is set up, some data needs to be passed through it, else it defeats the purpose of having network connections at the first place. Thus a system, which can pro-actively monitor all activities traveling through the firewall, is necessary.

BlackICE – its background

IIS (Internet Security Systems, http://www.iss.net), the maker of BlackICE PC Protection, is a software security company founded in 1994. Prior to version 3.5, BlackICE PC Protection is known as BlackICE Defender(version 2.9). It is a stateful firewall, containing two independent modules as outlined earlier (firewall and IDS). An evaluation copy of the firewall can be downloaded at http://www.iss.net/products/networkice/eval/register.php.

In essence, BlackICE PC Protection encompasses the following features :

- **Firewall capabilities** – blocks all unauthorized activities, including both inbound and outbound traffic traversing the protected computer.
- **Intrusions detection** – probably the mandatory of all personal firewalls, comprises of the ability of capturing all suspicious and illicit activities alike. The captured information can act as the evidence of intrusion attempts should it be needed later on.
- **Applications Control** – proves 2 levels of applications security; preventing unauthorized application from communicating with the internet, as well as safeguarding from local applications from being

started that might launch other programs. This is especially critical in a world where email and files are being transferred in such massive traffic, where Trojans and worms are being delivered effortlessly. Should the computer be infected with these, BlackICE will be able to preventing them from launching or/and communicating information to the outside world from the computer.

All these features are exclusive of each other and can be customized, or enabled/disabled separately.

Installation

Minimum requirement

Operating system	: Windows98, Windows ME, Windows NT(Service Pack 5 or later), Windows 2000, Windows XP Home or Professional
Processor	: Pentium or equivalent
Memory	: 16MB minimum
Hard Disk Space	: 10MB

Installation Procedure

Before installing BlackICE, it is very vital to ensure that the computer is free from viruses. This is because during installation BlackICE will perform baselining, which will create an MD5 checksum for all executables on the machine. This checksum will change dramatically, even though the file has been modified very slightly. This allows BlackICE to safely launch authorized programs after verifying their originality. If there are viruses still lurking in the local machine, they might be included in the baselined programs, making them appear as credible applications.

Usually, most anti-virus programs include real-time scanning feature that monitors malicious virus activities on the local machine continuously. This should be disabled before installing BlackICE. One suggestion will be disconnecting the machine from any network (standalone) before disabling it. This way, virus threat from the network can be eliminated. Once the program has been launched, the real-time scanning feature can be re-activated. Also, most recent updates of BlackICE should be obtained from the Internet.
There are basically three places where BlackICE's configuration can be defined. With these settings tweaked to the user's preference, granular control can be provided.

1. BlackICE Settings – control panel of BlackICE
2. Advanced Firewall Settings – defining rule set to allow/block traffic
3. Advanced Application Protection Settings – protecting outbound traffic originating from the local computer and preventing bogus programs from being launched.

1. BlackICE Settings

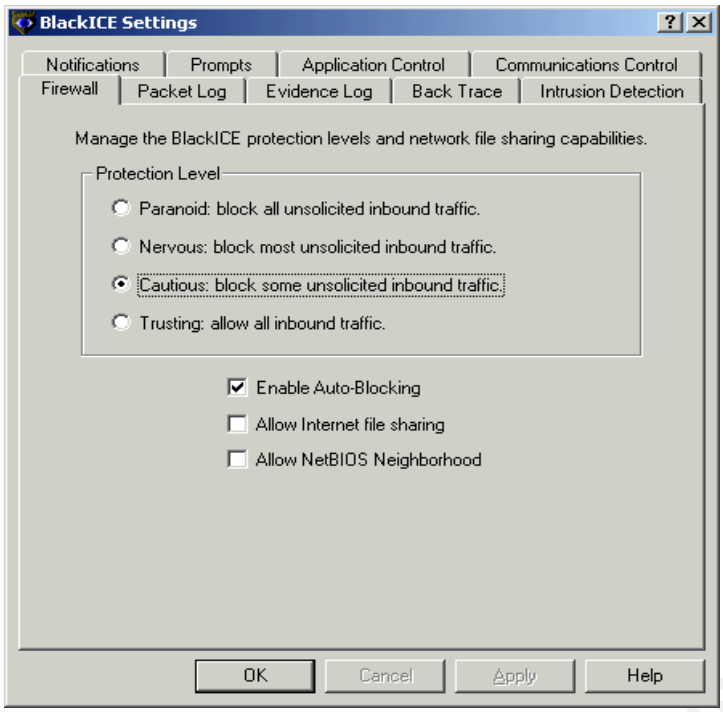

Figure 3

Firewall :
provides 4 levels of protection, from letting in all inbound traffic to blocking all unsolicited inbound traffic.

> **Trusting** mode - means no ports will be blocked; traffic attempting to connect to any ports will be allowed. This is not advisable as it defeats the purpose of putting a firewall. This is only recommended if this mode is enabled for a specific period of time and the network the local computer is on is made sure to be clean of hackers (local LAN with limited number of PCs)
> **Cautious** mode - will block all well-known TCP and UDP ports (i.e. ports 0-1023)..
> **Nervous** mode - As known, TCP will establish a stateful session with the target computer; exchanging information on dedicated connections If this is not desirable, this mode can be selected.
> **Paranoid** mode - will block all TCP and UDP ports, blocking all uncalled-for connections from outside.

The firewall feature also allows **Auto-Blocking**; when enabled, will block the IP address(es) or port(s) for 24 hours if inbound traffic conform to the rules set in "**Advanced Firewall Settings**". "Allow Internet file sharing" and "Allow NetBIOS Neighborhood" work together with the levels of protection mentioned above to determine the "furtiveness level" of the computer. Should they need to be checked, for example if the computer was part of a domain prior to installation, and the level of protection is "**Trusting**", attackers will be

able to see the services running on it and will try to break into it. Here, the IDS with its **Auto-Blocking** feature will kick in to block or shut them off completely if they perform certain critical attacks. Thus, proper rule sets should be configured before this setting is activated. If the two features are not checked, and the level of protection is checked at "**Paranoid**", the attackers will only be able to see the IP address of the machine, nothing more. This is the stealthiest mode. Of course this will disable them to continue exchanging domain information.

Packet Log

As the name implies, it enables logging of all network traffic, not only suspicious ones. As the amount of data might be humongous, especially on the Internet, it is advisable to set the log file size and the number of log files. The data will be saved in a round robin manner, retaining only the latest information captured. When viewed, it may not make sense to the general population, but experts can extract a lot of information from it, usually needed when an intrusion is reported. Normal text file viewer can't be used to view this file; usually they are decoded by using standard protocol analyzers such as Ethereal (http://www.ethereal.com/) or DICE (http://www.ngthomas.co.uk/dice.htm). Figure 4 shows a screenshot from DICE packet log analyzer. The file is by default in the format of **logxxx.enc**.

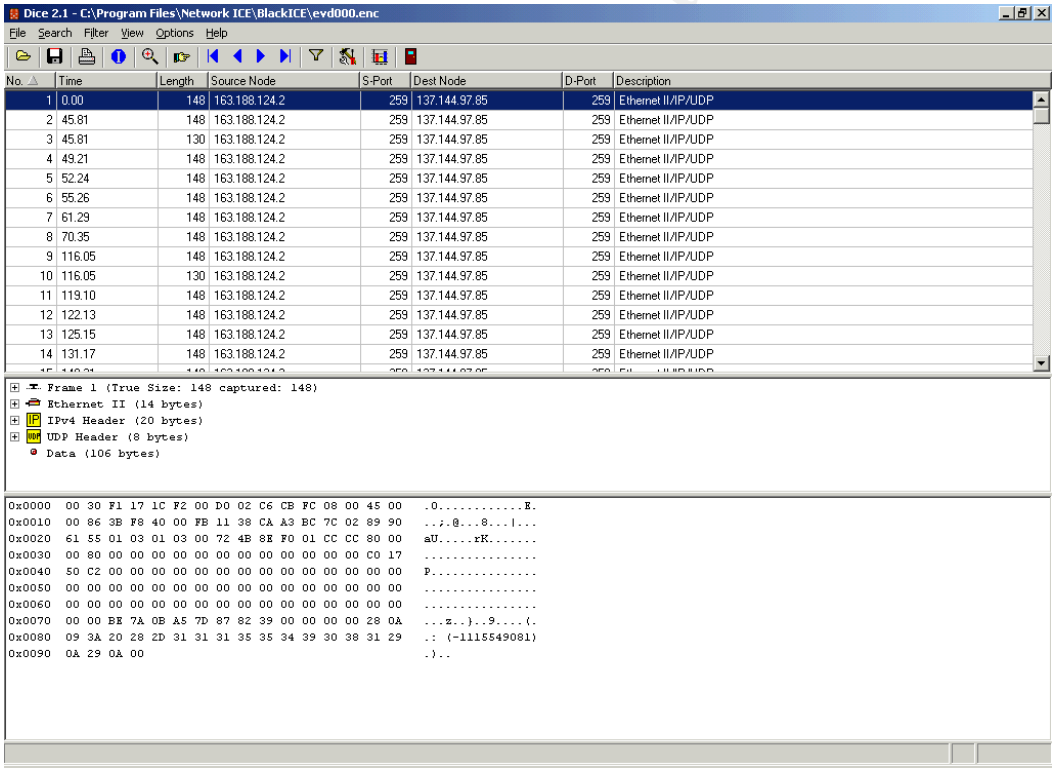

Figure 4

Evidence Log

This is the subset of Packet Log and by default **evdxxx.enc** format. As opposed to packet logging that records every thing on the wire, evidence-logging records only detected attacks. An event is categorized as an attack if

the detected packet is targeted towards the computer, as opposed to network wide sweep. For example, an attacker performs a port scanning sweep throughout the network; this will be logged in the Packet Log file. The attacker then zooms in to a particular machine he/she is interested in, and starting to break into it; this event will be logged/written in both the Packet Log and Evidence Log file.

Back Trace

Back Trace will enable the attacked computer to trace back the attack to the originating machine, resolving to its IP address and NetBIOS/DNS names. The Indirect Trace and Direct Trace can be configured to define the severity level of trace. **An indirect trace** does not make contact with the intruder's system but collect information indirectly from other sources, thus it acquires less information. Indirect tracing is best used to trace lower-severity events.
A **direct trace** on the other hand traces an event all the way back to the intruder's system to collect information, thus it can acquire more information. It is best used to trace higher-severity events, however, if the intruder has firewall installed, he/she intruders can in turn detect and block a direct trace. Direct trace also records the MAC address of the attacker; sometimes the detected IP address may be spoofed. A great concern nowadays is that using wireless connections, one can even spoof the MAC address, making it almost impossible to trace the origin of attacks. There are ways to overcome this, but that is out of the scope of discussion here.

Intrusion Detection

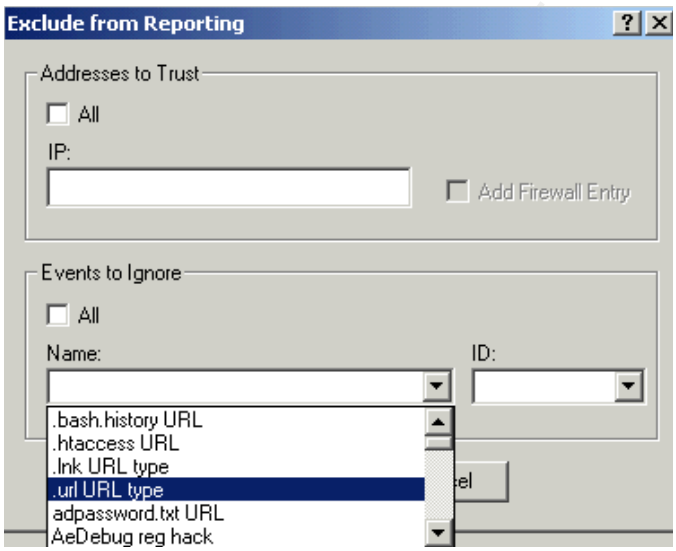

Figure 5

Here BlackICE can be configured to handle IP addresses or/and signatures (events) that triggers an attack alarm. For example, a hacker may attempt an "**AeDebug reg hack**", which writes to the registry, triggering the launch of unintended program(s) when system crashes. The attacker might place a program on the target machine and by performing this hack, the program will

be launched when the system crashes, and it is not hard to crash a machine (intensive port scanning will usually do the job).

Communications Control

Essentially, it controls **outbound** traffic as opposed to inbound traffic that the firewall feature provides. It filters and manages the allowable applications from accessing the network. If an application is trying to access outside resources, the user by default will have a choice of whether to block or allow it; this will be used as the action basis for BlackICE in the future should the same event happens. When I installed a VPN suite and it tried to connect to the authentication server, BlackICE prompted me with the pop-up window as in Figure 6. The "**Install Mode Options**" allows application that is being installed to be treated as just that, rather than as an application being launched.

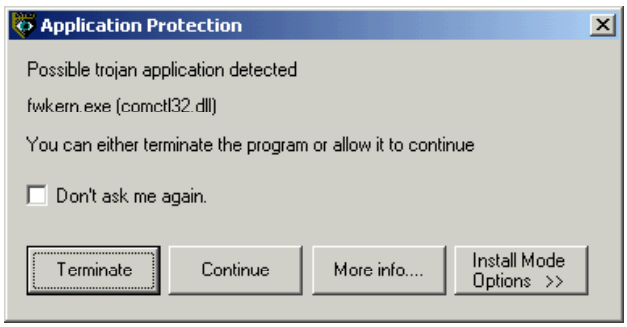

Figure 6

Application Control

This setting determines which application is allowed to be launch from the local machine (Web browser, spreadsheet etc.). Baselining performed during the installation will register all existing applications installed with an MD5 checksum. If the executables are found to be different (modified) or if it's a new application (unknown application), BlackICE will alert the user on the next course of action.

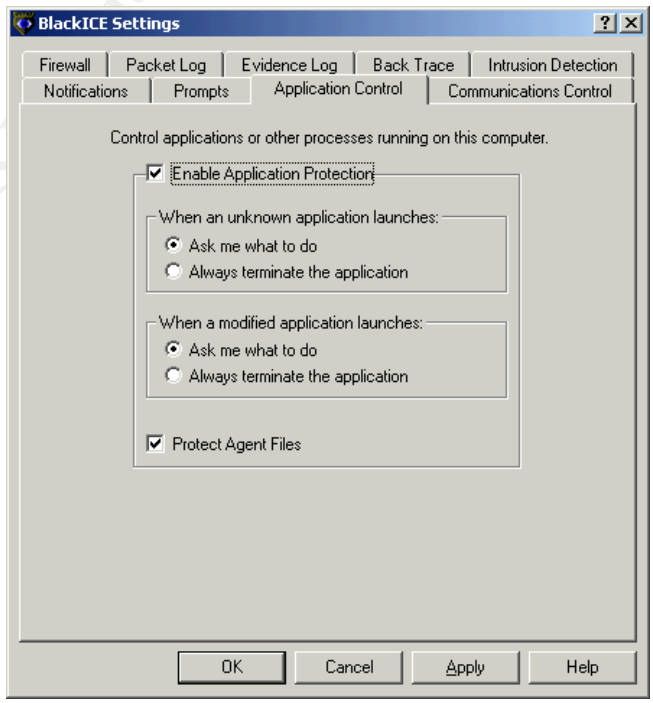

Figure 7

Prompts and Notifications

These are typically the user preference on how desired it is to be notified by the application (confirmation dialog, audible alerts etc.). The default setting is recommended as it prompts on changes made and events are notified with visible indicator enabled and audio indicator disabled.

2. Advanced Firewall Settings

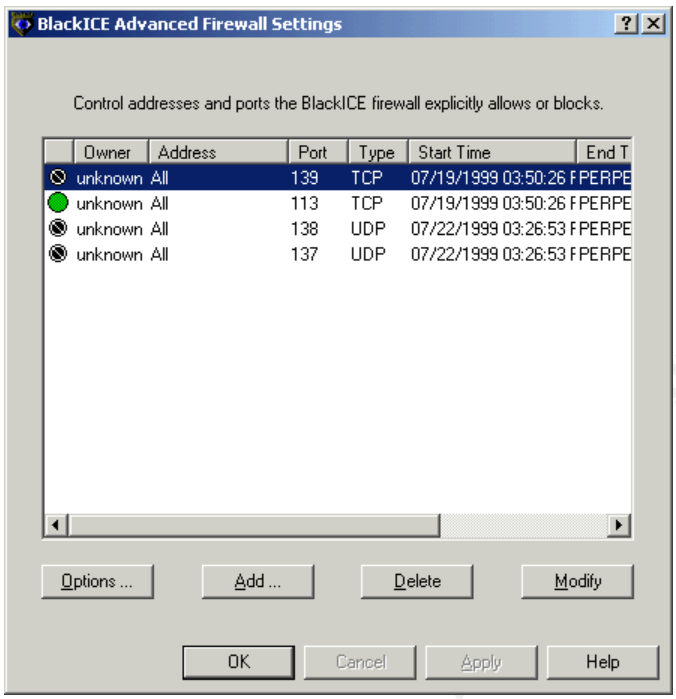

Figure 8

This is the actual firewall configuration location. It allows for granular control of incoming traffic, which can be filtered based on IP address(es) or port(s). Also, the type of connection protocol can be defined and controlled as well, be it connection-oriented (TCP, connectionless(UDP) or IP (e.g. ICMP). One feature to be noted here is BlackICE provide the functionality to allow/block a specific port from all addresses or all ports from a single host. To specify an IP address range, a dash can be placed between each distinct IP address example: 1.1.1.1-1.1.1.28. This is a very useful feature as it's straightforward to identify particular attacker(IP address) or dangerous ports, e.g. Telnet (ports). Telnet is dangerous as everyone can sniff the logins and passwords data that passes between the telnet client and the telnet server. As the rules specified can be applied to be in effect for a defined duration of time (or forever), a user can set the machine to be accessible by a certain host or opening a certain port for a period of time (secured period) without actually compromising the machine's security. Also, warnings can be configured to prompt the user before a block is expired.

3. Advanced Application Protection settings

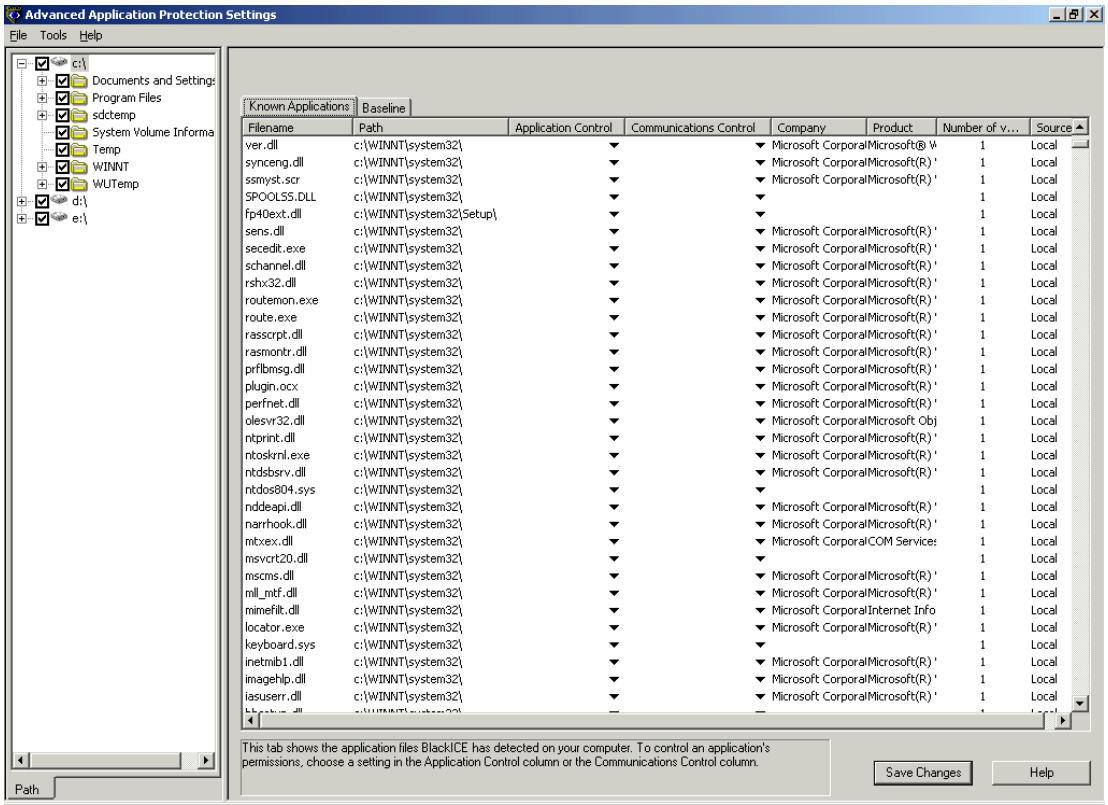

Figure 9

When BlackICE is installed, a list of currently installed applications on the computer is created. Whenever the computer launches an application, BlackICE will compare the application with the one listed during installation, if for any reason the program has changed, the user will be given an option to stop the program from running or allowing it to run. By clicking on the "**Baseline**" tab, and checking the desired checkbox on the left (drives on the hard drive), a user can determine the executables found on the hard drive. Clicking on "Save Changes" can perform re-baselining. Listed in the "**Known Applications**" tab are the applications detected during installation. From here, the user can also perform application and communication control. I would prefer to go through this list the first time right after BlackICE is installed to fine-tune the applications security level. Here, applications and communications control can be defined for each of the discovered programs. It is worth mentioning that other than .exe, file with other extensions are also baselined, for example .dll, .ocx., .drv etc..

I'm being attacked- what's next?

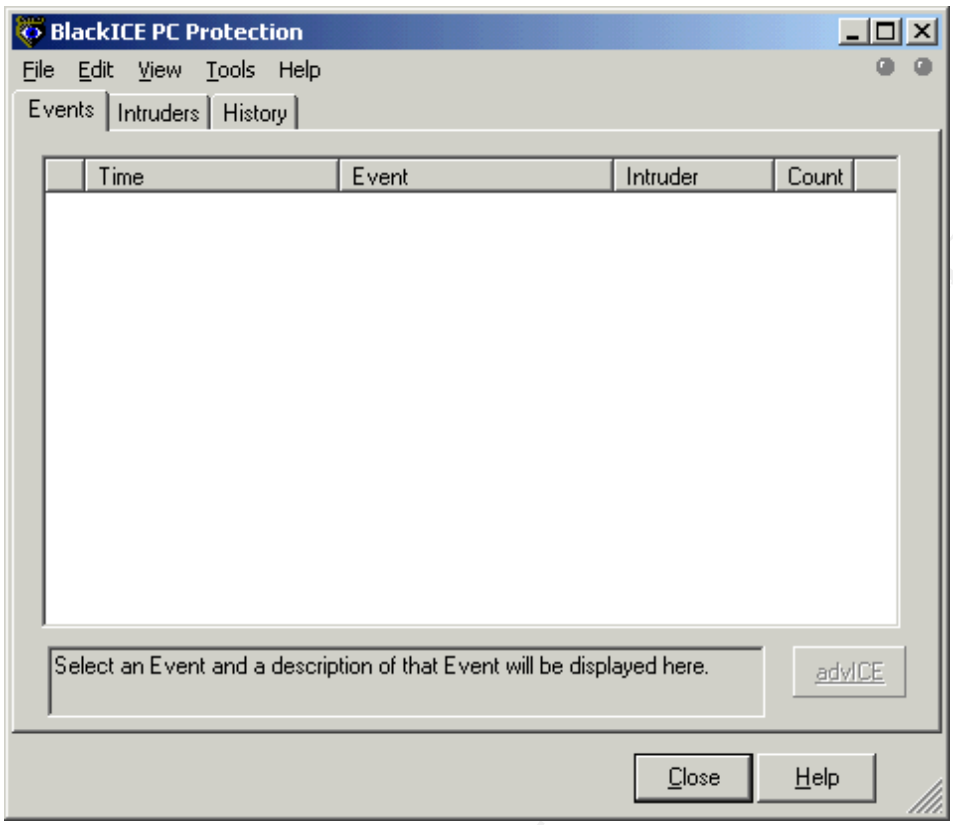

Figure 10

The "Events" tab list all the occurrences of possible hacking/intrusion activities. A user might get a lot of them, but they may no necessarily be indications that the local machine in particular is being attacked. Simply because the machine is detecting probes does not mean that a hacker has penetrated the system. Likewise, it doesn't mean that the hacker is after that particular user; in all probability the local machine can always be one of thousands of machines the hacker is scanning. The 'attacker' may be performing a network wide scan, using tools such as nessus (http://www.nessus.org) or nmap (http://www.insecure.org), trying to find random machines that are not protected to feed on. This is analogous to a burglar walking down a road of cars parked by the side, looking for unlocked ones to steal. Often, the most common threats are the attackers looking for sensitive information such as banking information, passwords, credit card information by performing a network wide scan looking for open ports, be them TCP or UDP. This is common especially with cable modems and DSL routers users for various reasons:

1. IP addresses are retained for a period of time.
2. The connections are always "on"
3. The connections are fast

The rule of thumb of defining "real" attacks from system wide scanning is to look at the events logged in the main window. If there is only a single attack from someone, that most probably means he or she is doing a network san (like the burglar), while if a lot of attacks are detected coming from a particular user, it may be an indication that he or she is conducting an active penetration attempt.

When suspicious activities have been identified, the next step is to gather more information and proof about the attacker. There are 3 common files that can be used as evidence and to look for more information; Attack-list.csv, Packet log and Evidence log. Of all these files, Attack-list.csv provides a record of all activities listed in the main BlackICE window plus a few more fields. It is in comma separated spreadsheet format and can be easily read and interpreted by most users. As this file is being written to in real-time, a copy of it should be made and sent, not the file itself. The can then be sent to the attacker's ISP and usually proper course of action is defined by the ISP. It has to be noted that only the attacker's ISP can take measures against the attacker, not the attacked user's ISP. What they will require usually is more than just the csv file; if further information is needed, both the packet log and evidence log file can also be sent to them. As mentioned earlier, these 2 files can only be read by using specific program, such as sniffer programs.

Improvement Suggestions

Of course, no product can claim to be perfect. The same goes with BlackICE. There are a few areas that the users need to be aware of. First of all, the user interface is not as user-friendly. One will need to play around with it before he/she can get accustomed to the various settings available. When I started using BlackICE, its Application Control features will sometimes pop-up to ask whether or not to allow certain executables to run, even if I've checked "**Don't ask me again**". This to me is analogous to a double-edged sword as there are some applications that I would like to always run and some I would prefer to be asked before being executed. It would be beneficial if there were an extra feature offering this customized setting. Also, the main window (when clicking on the icon on the taskbar) is quite an annoyance when it is recording an attack (blinking), even though it's just a UDP port sweep probe, and although I've closed certain ports (Telnet for example), BlackICE still shows that that port is being probed. To the general population, making a rule set in the firewall will also need some practice before being put to use. This is critical especially when VPN (Virtual private Network) connection in involved; blocking or allowing the wrong IP address or port will cause a blizzard of problems later on.

Conclusion

All in all, BlackICE PC Protection provides a decent firewall system for average home users. Coupled with its Intrusion Detection System and Application Control feature, in my opinion it offers great protection in

safeguarding personal computers. Proper attention however should be taken into configuring it as mention above before placing it on the network. I look forward to the future release of BlackICE and hopefully pleasing improvements will be made.

References:

Internet Security System : BlackICE Product FAQ
http://documents.iss.net/literature/BlackICE/BI35FAQ.pdf (Aug 16, 2002)

Internet Security System : Oh my gosh, I'm being HACKED!!! What do I do now? Version : 1.8.6.4. Document Date: Oct 1, 1999
http://www.iss.net/security_center/advice/Support/KB/q000040/default.htm (Aug 17, 2002)

Internet Security System : What can I use as evidence?
Version: 1.8.5.5. Document Date: Jan 17, 2001
http://www.iss.net/security_center/advice/Support/KB/q000016/default.htm (Aug 17, 2002)

API Technology : Common Firewall Types
Document Date: Aug 17, 2001
http://www.apitechnology.com/firewalls.htm (Aug 18, 2002)

Twiggs, Will
ComTest Technologies, Inc : **Network Security : Firewalls**
Document Date: Jan 15, 2000
http://www.comtest.com/tutorials/firewalls.html#how (Aug 16, 2002)

Kessler, Gary
Information security Magazine – Securing Cable Modems
July 2000
http://www.infosecuritymag.com/articles/july00/features3.shtml (Aug, 15, 2002)

Finnie, Scott
Review: BlackICE PC Protection 3.5.cdf
Version : Vol. 2, Issue No. 30. Document Date: Aug 15, 2001
http://www.scotsnewsletter.com/30.htm#review1 (Aug 12, 2002)

Signatures Reference Guide
Version : 3.
http://documents.iss.net/literature/BlackICE/SignatureRefGuide30.pdf (Aug 16, 2002)

Boran, Seán
Personal Firewalls/Intrusion Detection systems
Document Date : Apr 16, 2002
http://www.boran.com/security/sp/pf/pf_main20001023.html (Aug 15, 2002)

Internet Security System : Once BlackICE detects a hacker on a port, how does it stop the attack?
Version: 1.9.6. Document Date : Mar 10, 2000
http://www.iss.net/security_center/advice/Support/KB/q000158/default.htm
(Aug 25, 2002)

Microsoft Windows AEDEBUG Registry Key Vulnerability
http://online.securityfocus.com/bid/1044/discussion/

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor