GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Reporting Incidents to an ISP with BlackICE / ClearICE Report Utility and the Importance of Submitting Firewall Logs to the Dshield.org Project

Victor Arnaud
GIAC Security Essentials Certification (GSEC)
Practical V1.4b Option 1
January 2004

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Abstract 2
Introduction 2
Events, In cidents and False Positives 3
BlackICE and ClearICE 5
BlackICE Intrusion Alert 6
Using ClearICE to Report the Incident 8
The Dshield.org Project and its Importance 12
Installing the Dshield.org Project Client and Submitting your Firewall Logs 13
Conclusion 17
Bibliography 19
Appendix A – Glossary 21
Appendix B – Using netstat 22

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

This practical has two objectives: guide users of BlackICE to report incidents to their ISPs (using ClearICE Report Utility) and show users the importance of submitting firewall logs to the dshield.org project. Since the installation of BlackICE does not require much work on a single workstation, I will assume that it's already installed and start from the incident itself, passing through the BlackICE's alert, blocking the intruder to avoid his activities and working with ClearICE to create an useful report to the attacker's ISP to help them track the malicious user.

Considering that all computers on the Internet are targets, you could help information security professionals and systems administrators. Submitting your firewall logs to the Dshield.org project, you help administrators and users all around the world to discover new trends in activities (anomalous and / or malicious) and to prepare better firewall rules. If more and more users and administrators submit their logs to dshield.org, their database will become bigger and the trends discovered easily. Also, firewall rules created based on their analysis will be more accurate.

Introduction

In the last few years, the number of computers and other devices connected to the internet have grown significantly [1]. New technologies, lower prices, softwares that are more user friendly and broadband connections are some of the factors responsible for this fast growth. With a huge number of devices connected to internet running vulnerable Operating Systems, the number of potential targets to malicious users has grown too.

One of the biggest problems for the information security professional is that a lot of users don't even know that they're targets and that their computers and / or devices could be used to attack other devices and networks if not properly configured and protected. Home and Small Office users have to install at least a Personal Firewall and Antivirus software on their computers to be protected against the most common threats on the Internet[2]. Intrusion Detection softwares and *Spyware uninstallers* [3] should also be considered.

After the installation, a great number of users forget about these softwares, because they rarely check their logs and alarming frequency. The firewall does its job and they are satisfied. This kind of behavior must change. Users have to be educated to report the most severe incidents that are detected by their Personal Firewalls to the attacker's ISP and to the local Incident Response Team too. There are excellent tools, such as ClearICE Report Utlity (works with BlackICE) that could help them on this task.

Their logs should be sent to projects such as Dshield.org (with client software covered later in this practical) to help the project to prevent script kiddies reckless actions, stop the spread of virus and worms, and even help track and prevent hacker break-ins.

According to CERT Coordination Center [4] (see Figure 1), the number of incidents reported are growing each year.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

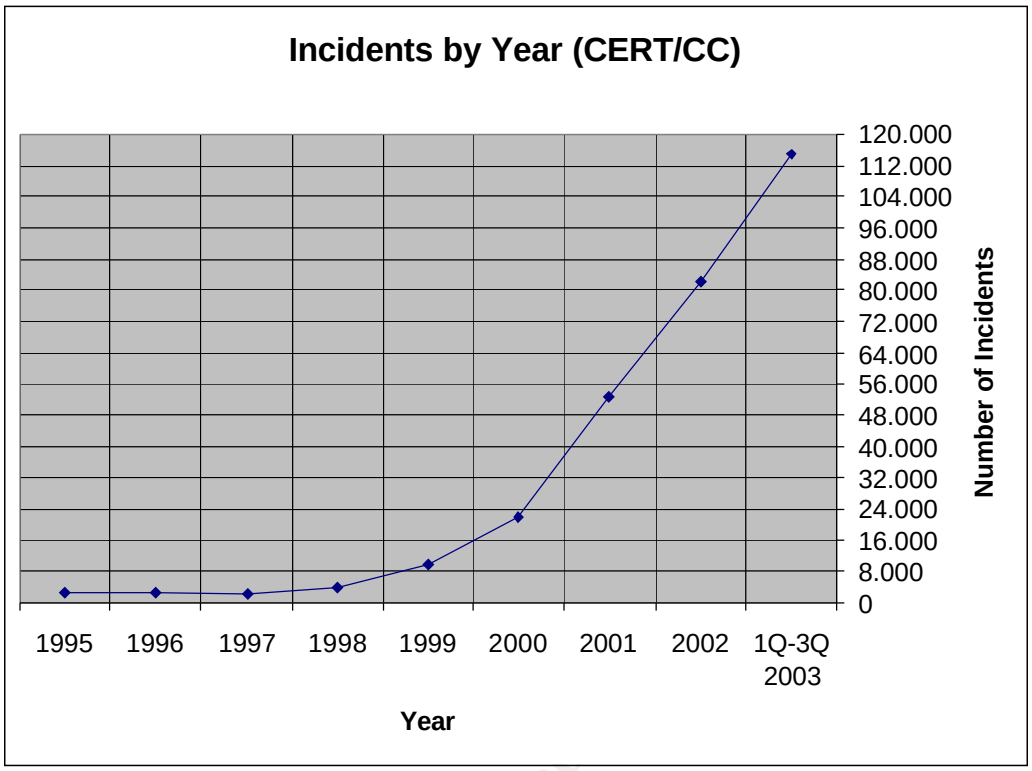

Figure 1 - Incidents by Year according to CERT / CC [4]

Events, Incidents and False Positives

According to SANS, an event is an observable occurrence in an information system or network that actually happened in some point in time (Examples: an e-mail, a phone call, a system crash, a system reboot.) and an incident is an adverse network event in an information system or network or the threat of the occurrence of such an event – it implies harm or the attempt to harm. Here is an example of both [14]:
Imagine a malicious code attack.

- An event: the user reporting that he might have been infected with a particular virus;
- A potential incident: his system exhibits behaviors typical for that particular virus;

False positives occur when a program interprets harmless activity as being an incident. Examples of this include:

- Remote computers which legitimately attempt to access a local computer, such as an Internet service providers who provide programs which monitor account usage;
- Programs installed on a computer which need to obtain information from the Internet, such as news or stock quotes, or "call home" to download updates.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

With these three definitions in mind, we should know start thinking of the log analysis of our Personal Fir ewall. We will probably have some false positives that don't have to be reported to the ISP, but sometimes it's very difficult to differentiate a false positive from a real incident. These logs sometimes could be very difficult to analyze and explain, so in the next few lines some real causes of false positives will be explained to better illustrate this topic:

Slow server responses : most firewalls block (and log) any inbound traffic for which there wasn't an associated and recent outbound request. This means that if you make a request, but the server responds too slowly (Example: five seconds), your firewall will consider that response as unsolicited and log it as a probe. The destination port of all server responses will be in the range of 1025 – 65535 (ephemera l ports). If you see in your firewall log "probes" against these ports and the source is a server you are communicating with, they are probably just slow server responses. To complicate matters, your attempt to surf to ONE web site, can actuall y result in communication with dozens of different hosts - often hosts that would appear to be unaffiliated with the site in question. If you see UDP probes in these port ranges AND the source is your DNS server then these are probably slow DNS responses.

Proximity probes: Larger web sites maintain mirrored content on many distributed web servers, often in multiple countries. When you first do a DNS lookup of a web site (e.g. www.windowsupdate.com) the site's load -balancing servers will send "proximity pr obes" fro m every location to your IP address. PC's that don't have a firewall will send back a reject packet (ICMP port unreachable) in response to these probes. In for mation in these packets allow the load balancers to deter mine which one is "closest" to the user, allowing it to provide the user the IP address of the nearest web server. Users running firewalls will log these proximity packets as probes (often on tcp/53) because they come from IP addresses that they did not make any outbound request to. This happens with one content hosting company that provides this capability as part of its hosting services (mirror -image.com, January 2004). When you surf to ANY website hosted by this company, you will be immediately "probed" by over 10 load -balancing se rvers in 6 countries.

Open proxy tests : If you are an IRC user you will likely be probed on several ports every time you attempt to connect to an IRC server. This to prevent anonymous IRC access through other user's PC's that are unknowing configured to al low "proxying".

Stale IP caches: If you have a dynamic IP address, you will often find that you receive a lot of unsolici ted probes when you first obtain a new IP addres s. This often because the previous user of that IP address was running some applicatio n which has cached their IP address somewhere and it's unaware that the owner of that IP has changed. Often the involved applications are Internet game servers, peer -to-peer file / music software (e.g. Gnutella, Napster , Kazaa, and Audio G alaxy.). Some o f these applications are poorly written to handle this situation and will incessantly pound an IP address thousands of times for many hours. As much as this may seem like a targeted

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

attack, it is really just a function of poorly written code that gives no consideration to how many firewall false positives it generates.

Search Engine Bots: Similarly, people often post web content with URLs that contain dynamic IP addresses (e.g. »123.123.123.123/blah/blah). Days, weeks, or months later web search bots may encounter this reference and then attempt to index that site. If you are the unfortunate person to have IP address 123.123.123.123 you now get a few dozen probes from abc.googlebot.com.

NetBIOS name lookup from IIS servers (Microsoft Web Servers): If an IIS server is also has NetBIOS over TCP/IP enabled, the server will often send NetBIOS name lookups directly at the users that surf to that site. This is due to IIS's attempt to associate a host name with every IP address that accesses it. Although this is technically not hostile, it's probably not advisable for webmasters to enable NetBIOS on their Internet facing network adapter. Unfortunately, this is a common scenario.

Source of probes is "Victim" of Spoofed DoS Attack : One or more attackers Syn-flood a victim web site, sending each TCP connect request with a different randomly spoofed IP address. The victim host sends a response (SYN/ACK) back to each of the spoofed IPs. If the DoS attack is running over a long period of time, potentially millions of spoofed IPs may be sent a response packet. Users running firewalls on any of these IPs will log this response packet as a probe.

Although some people can say that some of these real cases are more advanced false positives, the basic ones can be eliminated by knowing your system and your network, the applications that have access to the internet and which locations on the internet you are really visiting. A tool like netstat is perfect for this task (see Appendix B).

If after analyzing your logs, you still have doubts if it's a false positive or an incident, look for help from your ISP and your local Incident Response Team. They will help you to determine if it's a legitimate incident or harmless activity from the "attacker's" IP address and this will assure that you are not sending useless logs to the attacker's ISP and to the Dshield project.

BlackICE and ClearICE

The **BlackICE Protection 3.6** software consists of three components that can work together, according to its User Guide [5]: Intrusion Detection, Firewall and Application Protection .

The Intrusion Detection System (IDS) takes a copy of all incoming traffic and analyzes it for intrusions , as traffic enters your system. The "original" traffic continues up without being altered .

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Firewall component works as a Personal Firewall, with static rules, based on IP addresses and Ports, created by the user (or implicit) and works also in conjunction with the IDS engine. If the last one detects an event serious enough to pose an immediate threat to the system, it instructs the firewall to block all traffic from the intruder.

The Application Protection completes the software package. It gives this bundle one of the major characteristic of a Host Intrusion Detection System. Instead of analyzing only the network traffic, BlackICE can control which applications can run on the computer and which of them can connect to the network.

ClearICE Report Utility 5.1[6] is a software is used to analyze and report on the log events that are intercepted as a result of hackers and misbehaving software that is designed to steal user's information. ClearICE gives the user the ability to isolate the attack details and notify the attacker's ISP via email.

Since the installation of BlackICE does not require much work on a single workstation, I will assume that it's already installed - and configured in Paranoid mode - and I will start from the incident itself. The victim's machine is running a Windows XP Professional, so BlackICE and ClearICE are XP versions. Information on BlackICE installation can be found on its Users Guide[5].

BlackICE Intrusion Alert

To illustrate how BlackICE intrusion alert works, I created the following situation on a lab network:

Someone with the IP address 192.168.0.99, domain name uglyhacker.com is launching a massive Port Scan against the IP address 10.0.0.1 (victim) of a laptop. Port Scan is a technique used to discover what ports are available on the target computer. With that information it is possible to guess which Operating System the victim's machine is running.

The laptop is connected to the internet and suddenly the red icon from BlackICE is blinking on the taskbar (Figure 2).

Figure 2 - BlackICE Alert

Clicking twice on the red icon and the following window appears with the event highlighted (Figure 3):

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

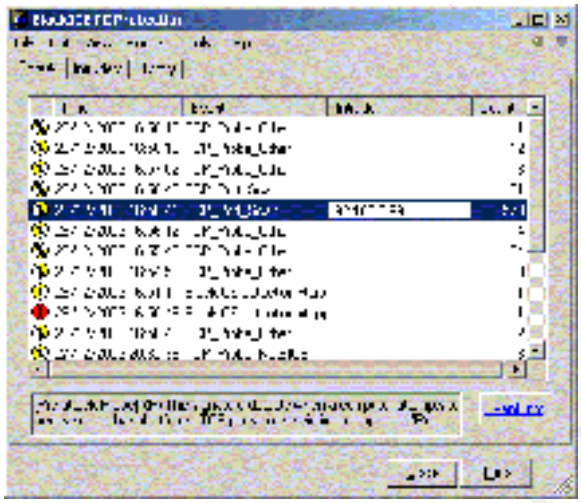

Figure 3 - Events

Reading the information from the **events tab**, we can say that someone from IP 192.168.0.99 launched a massive Port Scan against the laptop computer (573 attempts to connect to different ports). But we need more information.

So, clicking twice on the highlighted event, the **Intruders tab** will be shown. It gives me also the DNS uglyhacker.com that is pointing to the intruder's IP address (Figure 4).

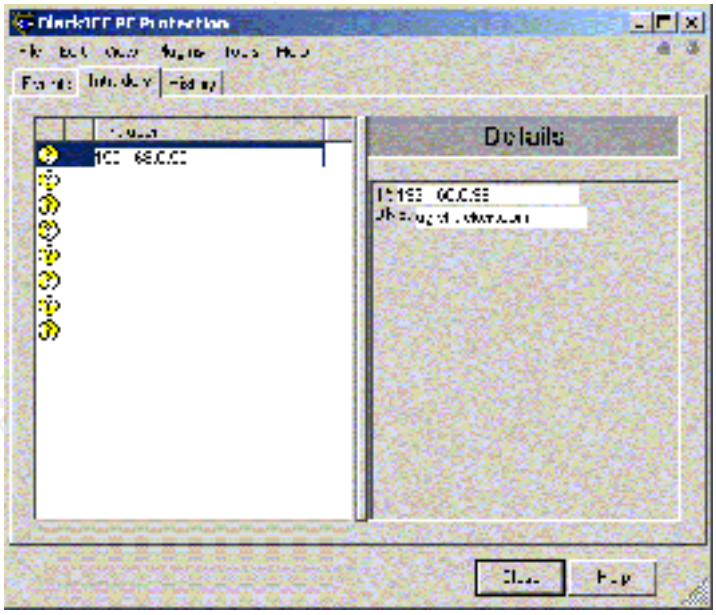

Figure 4 - Event Detail

Ok, now let's stop a little and see how much information we have gotten:

- Intruder's IP: **192.168.0.99**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- DNS Name: **uglyhacker.com**
- Type of attack: **massive TCP port scan**

That's not enough information to write a good report[7] to the attacker's ISP. We should also include information about ports from my computer that were scanned and the exact time that the incident happened (local and GMT - Greenwich Meridian Time that is measured from the Greenwich Meridian Line at the Royal Observatory in Greenwich, England.). Keep in mind that we still don't know to whom we will send this report. Usually, this kind of report is sent to the e-mail abuse@uglyhackerISP.com, where uglyhackerISP.com represents the domain name responsible for this IP address.

To facilitate this task (gathering additional information), the ClearICE Report Utility will be used in the next section of this practical. It gives us all the information necessary and also creates the report to be sent by email to the attacker's ISP.

Using ClearICE to Report the Incident

First of all, we have to download the ClearICE Report Utility. I went to google.com, searched for it and found a lot of sites that have this software for downloading (Example: http://www.getsomesoft.com/Internet/Security/2268_-ClearICE-Report-Utility.html).

Installation was very simple too. A typical Microsoft Windows software installation: "Next → Next → Finish" (it's covered on ClearICE Online Help Documentation[15].

With ClearICE downloaded and installed, clicking twice on its icon on the desktop the software window will be opened.

Now we have to import the event log from BlackICE to browse it with ClearICE. I click on **File** à **Import Event Log** (Figure 5).

Figure 5 - Importing the Event log from BlackICE

The logs were imported. We can browse the events clicking on **Browse** and then on the item **Browse Events** (Figure 6).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

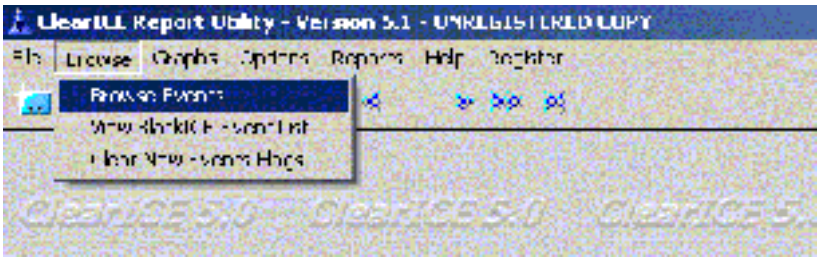

Figure 6 - Browsing Events

A lot of events appeared on ClearICE window. Search for the event that is under investigation (Intruder: 192.168.0.99 / Attack: TCP Port Scan / Victim IP: 10.0. 0.1) and highlight it (Figure 7).

The event is selected. After that, we click on the icon **Email event** that is circled with red on Figure 7 to email a report to the at tacker's ISP. By clicking on this icon, a copy of the report about the selected event is copied to the **clipboard**.

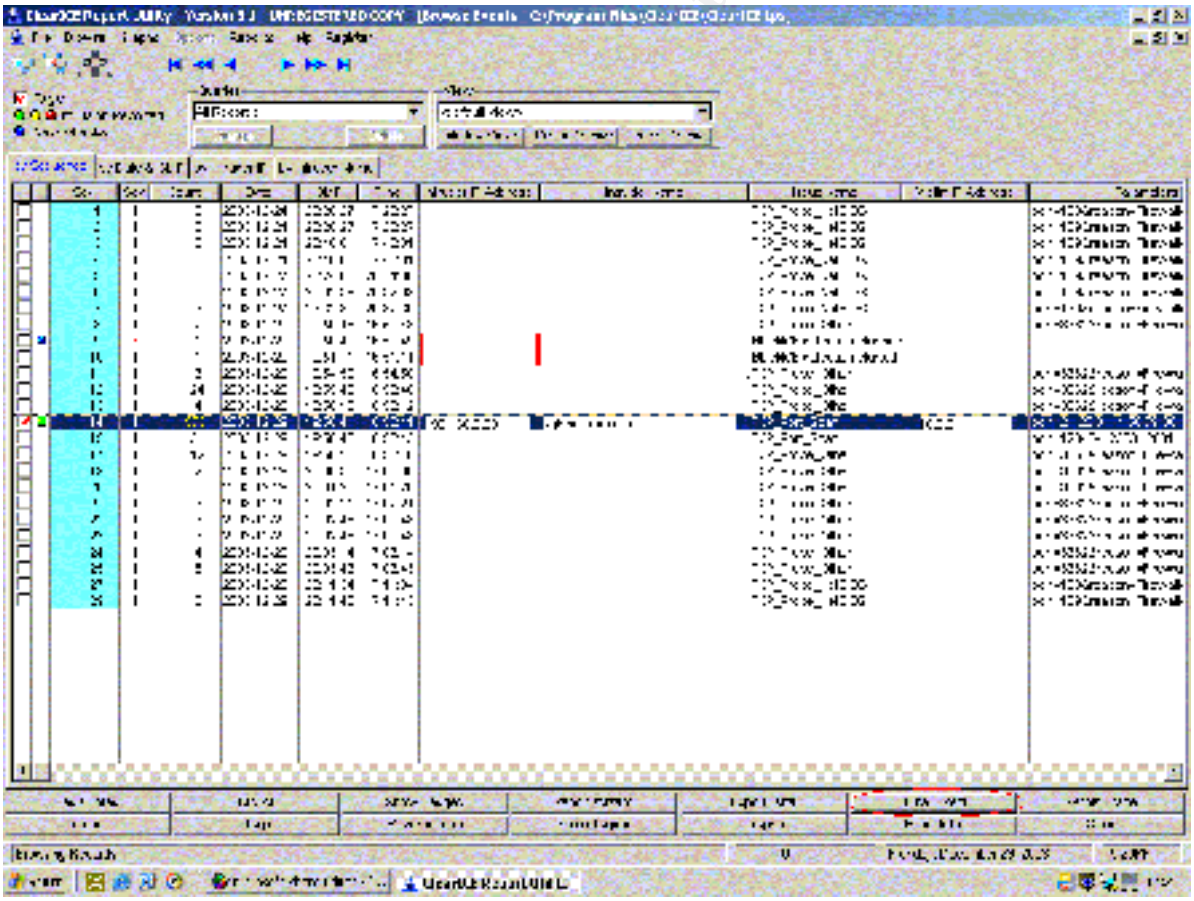

Figure 7 - Selecting the Event and Emailing it

It's interesting to read the warning that ClearICE pops up on the screen when I clicked on Email Event icon (Figure 8). When we do an online scan of

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

my computer (with Symantec Security Check for example), BlackICE firewall will consider that it is a n aggressive "movement" from an intruder. With that in mind, it's always wise to check if the event was not originated from an online security check.

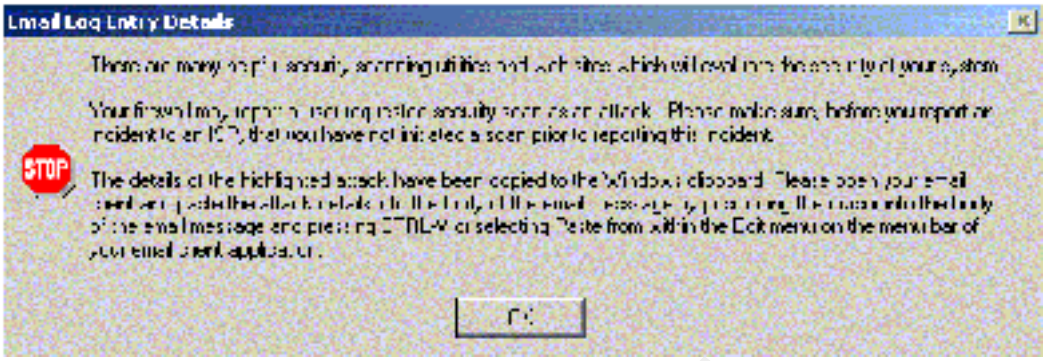

Figure 8 - Warning Message

After we read the warning message, open the E-mail client (Outlook XP) and create a new message. In the New Message Window , we click on the body of the message to paste the report that is on the clipboard (a simple Crtl-V will do the job). See Figure 9 and 10.

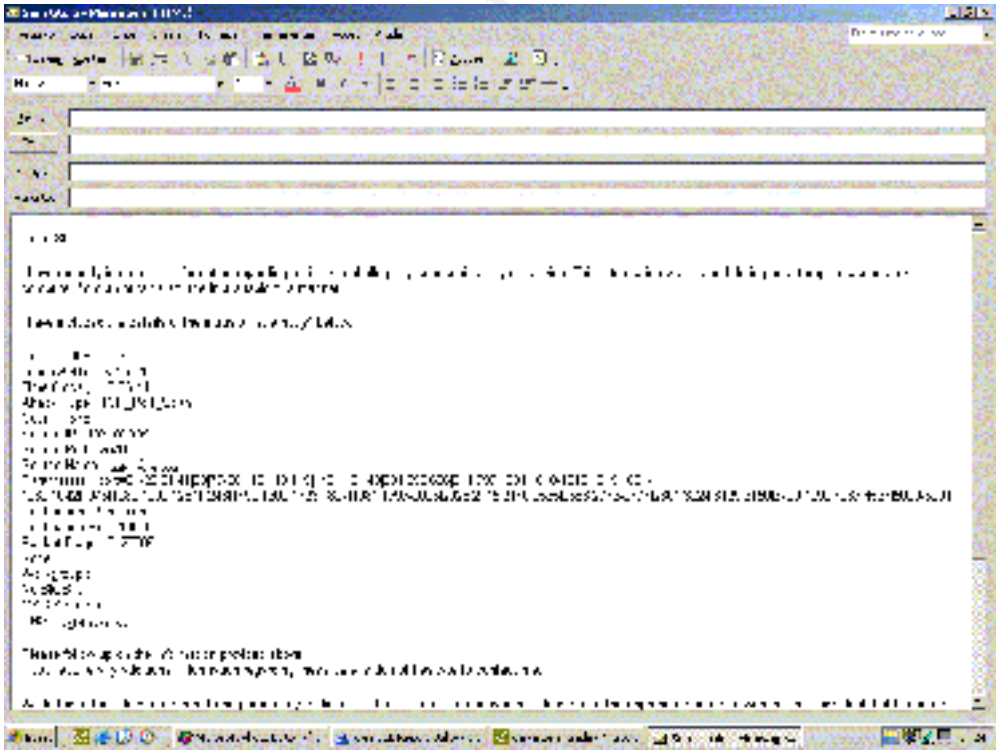

Figure 9 - Email message Part 1 of 2

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

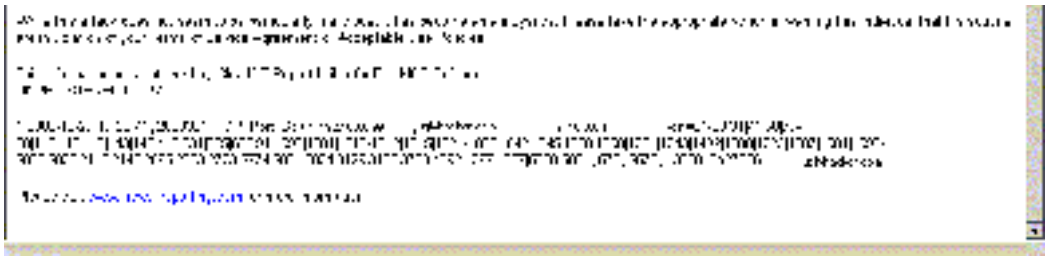

Figure 10 - Email Message Part 2 of 2

Our report is almost done. One last detail is pending: to whom will we send this email? ClearICE will make this task easier too. Going back to the ClearICE window, we click on the **WHOIS Trace** icon (next to **Email event** icon - figure 7) and the software will open an Internet browser with contact information from the attacker's ISP as we can see in figure 11.

Clicking on the **WHOIS Trace** icon will make ClearICE to access the site http://www.spamcop.net to perform a WHOIS of the attacker's IP address. This command will browse a database of records from various registrars to see if the requested address is there. If the address is found, the information is shown on the web browser.

With this contact information, we can send the report to the ISP from where the attack was originated.

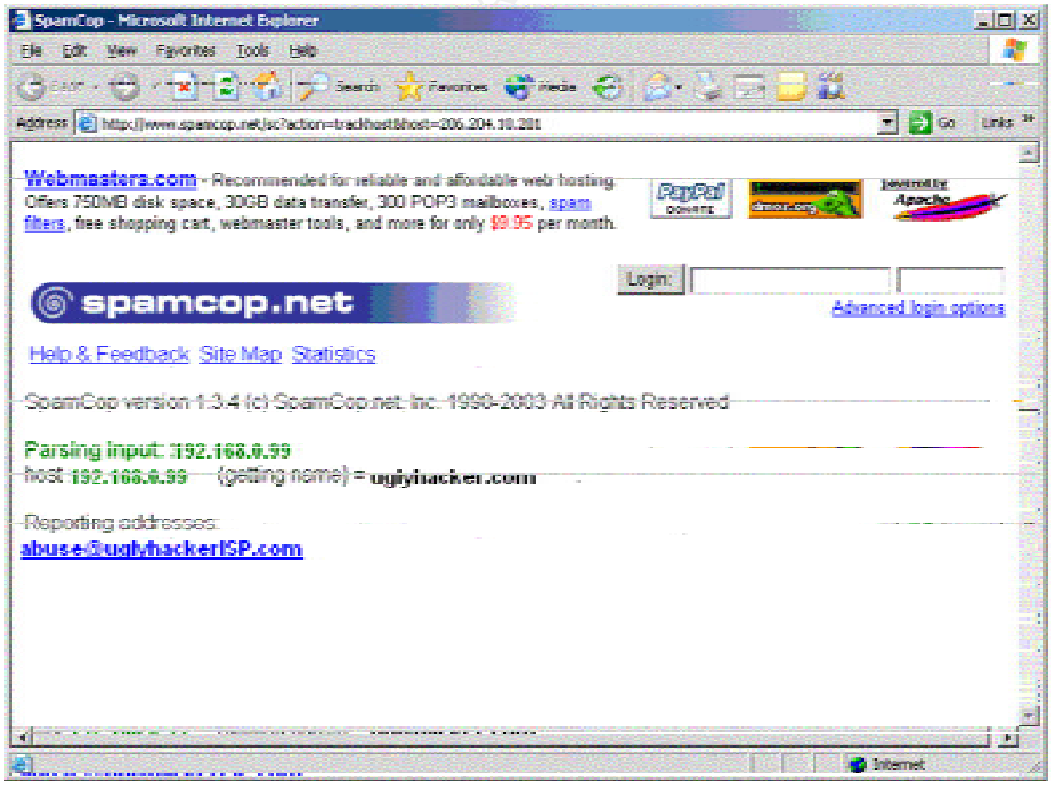

Figure 11 - Reporting Addresses (WHOIS)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Dshield.org Project and its Importance

The majority of home users are satisfied with the protection that personal firewalls afford them and don't bother to analyze the data these programs collect. Ports being probed and frequency of the Port Scan are rarely checked. The information stored in those unexamined log files could potentially prevent script kiddies rampages, stop the spread of virus and worms, and even help track and prevent hacker break-ins.

With that in mind, Dshield [8] was created by Johannes Ulrich as a location to centralize computer attack information. DShield is like a central agency for firewall log reports.

How does it work? Users and Administrators with firewalls or other intrusion detection systems download free DShield clients. Installation is done in less than five minutes. The client software doesn't interfere with the operation of the firewall.

Information from a single firewall often has little or no meaning by itself; when combined with many other firewall logs, however, it can highlight important trends and potential problems on the internet.

DShield.org is a project that has one objective: to collect data about malicious activity from all over the internet. This data is catalogued and summarized to be used to discover trends in activity and prepare better firewall rules. Nowadays, the project is prepared to handle data from simple packet filters logs. As firewall systems that produce this kind of logs are now available everywhere, this data can be submitted and used without much effort. In addition to its regular role, DShield also provides helpful data to the Internet Storm Center [9]. On this web site, data is interpreted and displayed as graphs and trends. It's possible to view data grouped by place of origin and it has other filter options too. Port-scanning activity often varies from place to place. This is especially true when viruses or worms propagate from a country of origin and spread outwards.

Using some functions from statistics [10], the researchers from Dshield.org are able to summarize all the data they receive, produce models and better understand the data (detect anomalies). I will try to illustrate how statistics can help with an example from **MARCHETTE [2002]** [11] with some modifications:

At your home network or company network, calculate the bandwidth used by all IP addresses (internal and external). With that value in hand, you can calculate the average of bandwidth consumption of a single IP address and the standard deviation. All the values that are outside the limits of the average (plus or minus two standard deviations) should be analyzed. With that analysis, you will probably be able to answer the following: Are they using an usual amount of bandwidth or is it a normal behavior of these IP addresses? Are they using an unusual amount compared to their past behavior (could be yesterday, last week, last month)??

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

How deep the analysis can go and how much information you can get will depend on your knowledge of statistics and on the data that you've collected. If you collect more data, your results will be more accurate , and if data is more detailed, the deeper your analysis can go.

At the Dshield.org project, they try to discover trends in activities over the internet and alert network administrators of potential dangers that can threat their networks. With that information network administrators can create more effective rules to reduce the risk of downtime (lack of availability) on their networks.

Installing the Dshield.org Project Client and Submitting your Firewall Logs

To send my logs to Dshield.org we have to install the client software [12] on the laptop computer. At www.dshield.org, we click on **Client Programs** (Figure 12) and choose **BlackICE Defender** (Figure 13).

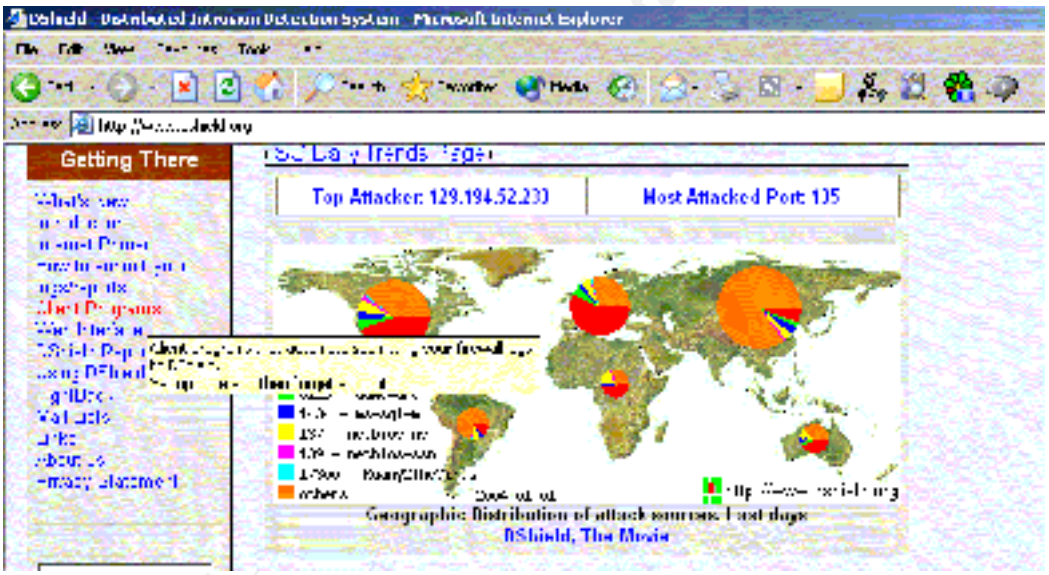

Figure 12 - Dshield.org -- Client Programs

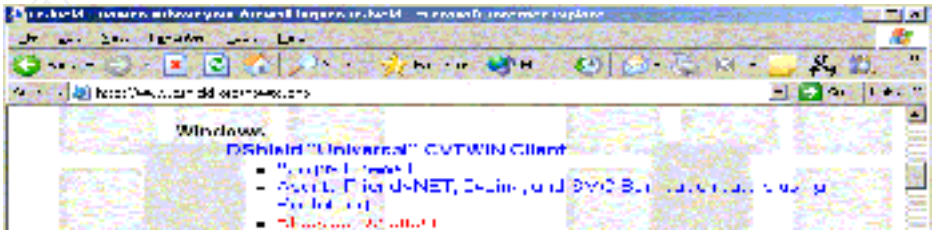

Figure 13 - Selecting BlackICE

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

At Windows Clients Download page we choose the complete install download and click on the respective link (Figure 14). Some configurations have to be done after the client installation, so we click on the link **How to configure specific firewalls/routers to work with CVTWIN** and take a look at these (configurations shown on figure 15) .

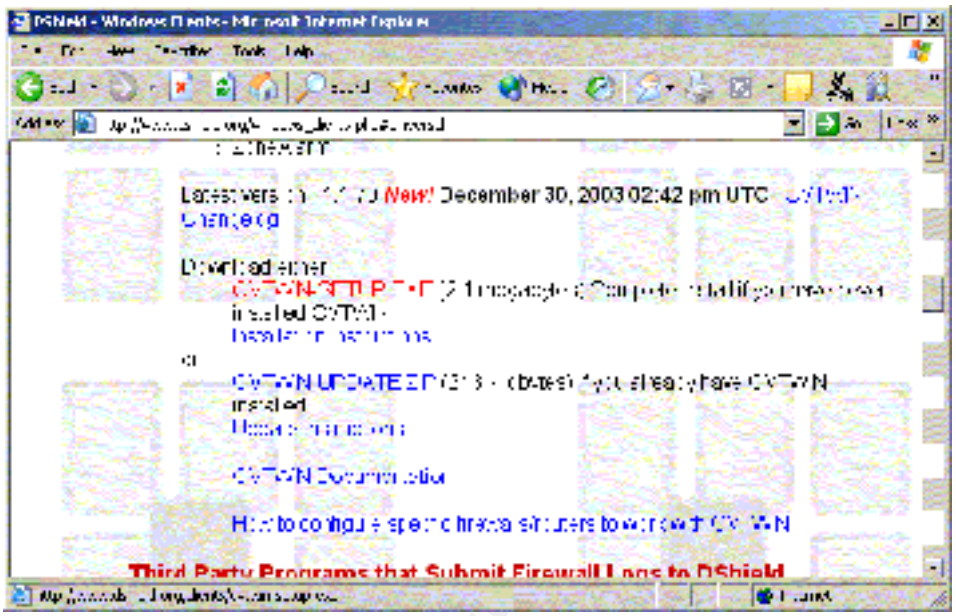

Figure 14 - Client Download and specific configurations of BlackICE

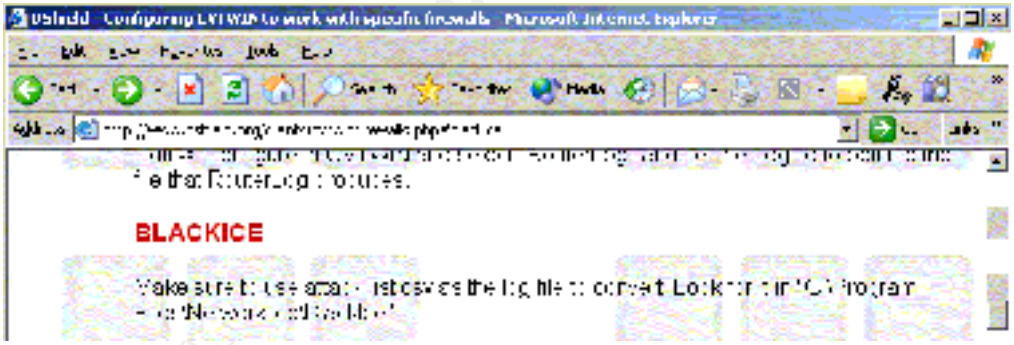

Figure 15 - Configuring BlackICE

After the file download, just click twice on its icon and install the client. It's a straight-through process with easy steps so I will jump directly to its configuration after installation.

The client is installed. Start it (**Programs** à **Dshield** à **Dshield** Client as shown on figure 16) and its window pops up on the screen.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

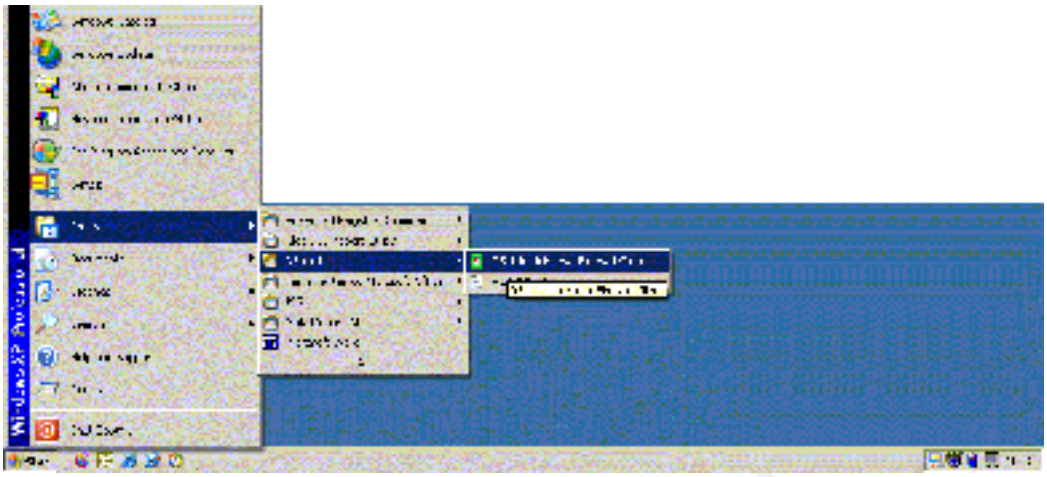

Figure 16 - Starting Dshield Client

With the client started , we can configure it, convert BlackICE logs, and send the converted logs to dshield.org.

To convert the logs, just click on **File** à **Convert BlackICE** (Figure 17). If the operation is done with no errors by the client, it will be possible to see on the screen the logs converted.

Figure 17 - Converting BlackICE logs

The logs were converted. Now we have to configure the client to send them to dshield.org. Clicking on Edit → Configure (Figure 18) the configuration window will appear (Figure 19).

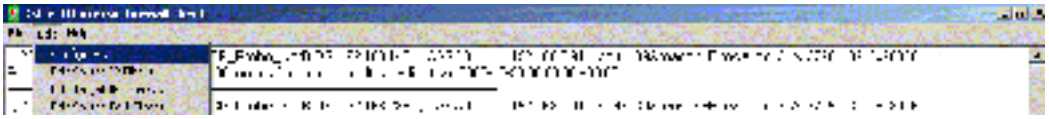

Figure 18 - Configuring Dshield Client

The fields **Email Address** and **SMTP Server Name** are required. Complete the first one with your e-mail address and the second one with your SMTP server address. Without them, we won't send the logs. Pay attention

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

to the field **Logfile** that is configured correctly according to instructions on Figure 15. After these configurations , I click on the **OK** icon to activate the changes. If you don't have a SMTP Server or don't remember yours, you can use **mail.dshield.org** to send your logs to them.

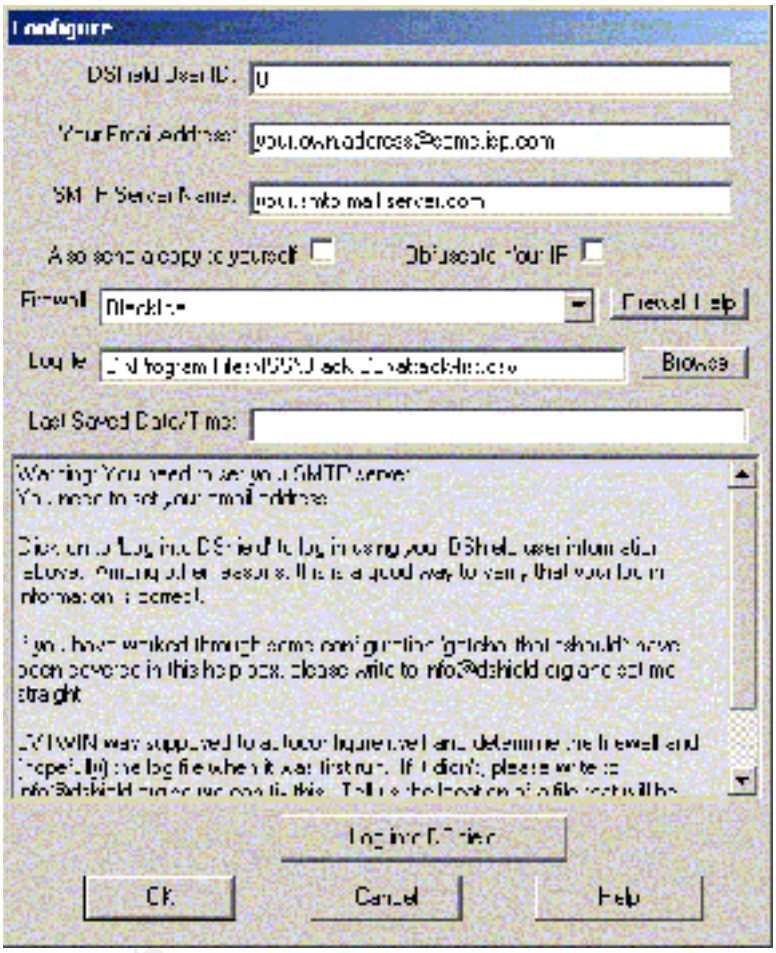

Figure 19 - Configuration window

Our last task is to send the converted logs. To accomplish that , we click on **File** à **Email to** report@dshiled.org and a few seconds later , we receive an **OK** message to confirm the success of the operation.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Figure 20 - Sending the logs

It's important to remember that users must send these logs periodically, not just once. They can automate log file submissions or they can choose to send in logs manually. There is a very simple how-to at http://www.dshield.org/clients/schedule_client.php that can help users to automate this task using Task Scheduler from Microsoft Windows.

Sometimes the firewall logs are full of false positives that can be eliminated. To eliminate them apply the Dshield filters based on the Source or destination IP address and ports (see figure 21) that generated the false positives. This you help Dshield Project to give us more accurate information, because these false positives could compromise their conclusions.

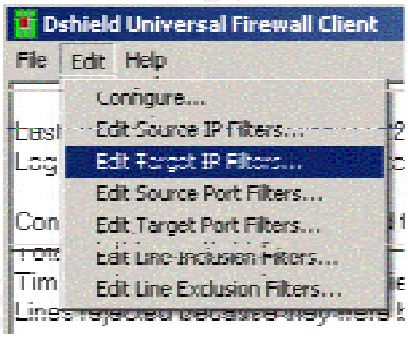

Figure 21 - Dshield Client Filters

Conclusion

Malicious activities are growing up on the Internet faster and faster. Everyone connected is at risk of being contaminated by a virus or worm or being hacked.

Home users have to do their part. Antivirus software and Personal Firewalls must be used on every computer to block these plagues. Every incident must be reported to the ISP that originated it to take the necessary precautions. If the attacker's ISP doesn't respond, report the incident to your local Incident Response Team.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Network administrators (and home users too) must contribute to projects like Dshield.org. This information sharing gives Dshield.org a capability of providing early warnings of major new security threats and the IP's that are originating it. With these information provided by Dshield.org, network administrators can prepare more accurate firewall rules.

Information Security is becoming more important every day. Unfortunately, it's becoming easier to create worms and virus or hack networks with the distribution of automated tools and broadband connections.

With this practical I expect to do a little more to spread the culture of incident reporting and the usage of tools like Dshield.org. These are important allies of the information security professionals.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Bibliography

[1]Allen Academy of E-learning - Drilling Down into Computer and Web Trends URL: http://www.allenacademy.com/elearning/about/page16.htm (January 2004)

[2] Home Network Security - Actions home users can take to protect their computer systems – CERT / CC URL: http://www.cert.org/tech_tips/home_networks.html (January 2004)

[3] **McCardle, Michael.** How Spyware fits into Defense in Depth (January 2003) – Sans Reading Room URL: http://www.sans.org/rr/papers/36/905.pdf (January 2004)

[4] CERT Coordination Center Incident Reporting Guidelines URL: http://www.cert.org/stats/cert_stats.html (January 2004)

[5] BlackICE PC Protection User Guide URL: http://documents.iss.net/literature/BlackICE/BIPCP_-UG_36.pdf (January 2004)

[6] ClearICE Report Utility URL: http://www.firewallreporting.com (January 2004).

[7] CERT Coordination Center Incident Reporting Guidelines URL: http://www.cert.org/tech_tips/incident_reporting.html (January 2004).

[8] Dshield Project URL: http://www.dshield.org (January 2004).

[9] Internet Storm Center URL: http://isc.incidents.org (January 2004).

[10] **Marchette, D.** Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint. Springer Verlag, July 2001.

[11] **Marchette, D.** Statistics and Computer Security – September 4 (2002). Sans Institute Webcast URL: http://www.sans.org/webcasts/archive.php.

[12] Dshield Client Software URL: http://www.dshield.org/howto.php (January 2004).

[13] **Cole, E.; Fossen, J.; Northcutt, S.; Pomeranz, H.** Sans Security Essentials with CISSP CBK Version 2.1 – Volume One. Sans Press.

[14] **Pham, Charles.** From events to incidents (November 2001) – Sans Reading Room URL: http://www.sans.org/rr/papers/27/646.pdf (January 2004)

[15] ClearICE Online Help Documentation URL: http://www.clariondeveloper.com/firewallreporting/clearice/clearicetutorial.htm (January 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Public Statistics URL: https://www.ecsirt.net/service/documents/wp4-links-of-public-statistics.html.

Ullrich, J.; Sachs, M. Internet Storm Center: Threat Update – November 19, 2003 and December 10, 2003. Sans Institute Webcast URL: http://www.sans.org/webcasts/archive.php

Girard, J. The Evolving Value of Personal Firewalls in the Enterprise (December 18, 2003). SearchSecurity.com Webcast URL: http://searchsecurity.stage.techtarget.com/webcastsTranscripts/0,289709,sid14,00.html?Offer=220library

Northcutt, S. et al. Inside Network Perimeter Security: The definitive Guide to Firewalls, VPNs, Routers, and Intrusion Detection Systems - Third Edition. USA, New Riders Publishing .

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix A – Glossary

All definitions from this glossary were taken from the Sans Security Essentials with CISSP CBK Version 2.1 Appendix F [13]:

Client: A system entity that requests and uses a service provided by another system entity, called a "server". In some cases, the server itself may be a client of some other server.

Domain Name: A domain name locates an organization or other entity on the Internet. For example, the domain name www.sans.org locates and Internet address for "sans.org" at Internet point 199.0.0.2 and a particular host server named "www". The "org" part of the domain name reflects the purpose of the organization or entity (in this example, "organization") and is called the top-level domain name. The "sans" part of the domain name defines the organization or entity and together with the top-level is called the second-level domain name.

Domain Name System (DNS): The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Event: An event is an observable occurrence in a system or network.

Firewall: A logical or physical discontinuity in a network to prevent unauthorized access to data or resources.

Incident: An incident is an adverse network event in an information system or network or the threat of the occurrence of such an event.

Internet Protocol (IP): The method or protocol by which data is sent from one computer to another on the Internet.

Intrusion Detection: A security management system for computers and networks. An IDS gathers and analyses information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

IP Address: A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.

Personal Firewalls: Personals Firewalls are those firewalls that are installed and run on individual PCs.

Port: A port is nothing more than an integer that uniquely identifies and endpoint of a communication stream. Only one process per machine can listen on the same port number.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Port Scan: A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, the computer provides. Port scanning, a favorite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.

Server: A system entity that provides a service in response to requests from other system entities clients.

Software: Computer programs (which are stored in and executed by hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.

User: A person, organization entity, or automated process that accesses a system, whether authorized to do so or not.

Virus: A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting – i.e. inserting a copy of itself into and becoming a part of – another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

WHOIS: An IP for finding information about resources on networks.

Worm: A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

Appendix B – Using netstat

This tutorial was taken from the URL:
http://netsecurity.about.com/cs/disasterrecovery/a/aa061603_2.htm

Netstat is a utility that will show you all open ports on your computer and your current connections. If your hacker is sloppy you may even be able to find his source IP address using netstat. To use netstat you need to open a command prompt window and type "netstat" followed by the parameters you want to use. The available parameters are:

- -a **displays all connections and listening ports**
- -e displays Ethernet statistics
- -n displays addresses and port numbers in numerical form
- -o **displays the owning process ID associated with each connection**
- -p proto shows connections for the protocol specified (TCP, UDP, etc.)
- -r displays the routing table
- -s displays statistics broken down by protocol
- interval redisplays selected statistics at the assigned interval

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Using netstat can yield a ton of valuable information. You may be able to find open ports, connections to IP addresses or connections opened by processes that you are not aware of.

For your evidence gathering purposes you will want to export the results to a text file that you can save and refer back to later. Typing "netstat –an >c:\log.txt" will run netstat using both the –a and the –n parameters and will save the results to a file called "log.txt" on your C drive. You can change the drive and file name to anything you choose.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Last Updated: April 26th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS