# Global Information Assurance Certification Paper

Laurie Zirkle
SANS Security Essentials
GSEC Practical Assignment
Version 1.2f (amended August 13, 2001)

# An Informal Analysis of One Site's Attempts to Contact Host Owners

## Introduction

To contact? Or not to contact? It seems to be a question that periodically rises and creates a myriad of opinions. How do I find a contact for a site? Should I send a copy to the parent domain? What information should my e-mail contain? Should I call? How long should I go before I block the site? How many times should I see scans or probes from a particular site before attempting to contact someone? Why should I bother? Does anybody really care? What good might it do?

The Incidents mailing list hosted by SecurityFocus has had postings and (sometimes heated) discussions regarding whether or not host owners should be contacted. Some people hold the opinion that a port scan is nothing to be concerned about; others are very thankful that port scans from their site were reported.

This paper will look at one system administrator's attempts to contact host owners of machines that scan or probe her network[1]. After a brief discussion of various ways to identify possible contacts, this person's data will be used to show how different sites may respond and how probes have multiplied over a definitive period of time. The paper concludes by mentioning two projects that might help the overburdened system/network/security administrator to simplify the whole process of contacting a host owner.

## How to Identify Site Contacts

With the advent of the World Wide Web, resources for identifying site contacts have increased dramatically. There are many more registries in 2001 that can be used to correlate a host IP number or domain name with the owner of the address space. The three Regional Internet Registries (RIRs) are the American Registry for Internet Numbers (ARIN), Réseaux IP Européens Network Coordination Centre (RIPE NCC) and Asia Pacific Network Information Centre (APNIC). Each has a WHOIS service which, when queried, will (hopefully) return information relevant to the identifier used in the query.

There are also many Local Internet Registries that provide a more localized WHOIS service. These local registries are subsets of the regional registries. The

[1] For the purpose of this document, *scans*, *probes* and *exploit attempts* will be collectively referred to as simply **probes**.

regional registry sometimes returns the owner of the whole address block and references the appropriate local registry for more specific information about the host in question.

WHOIS proxy sites now exist which eliminates the need for the user to make recursive queries through multiple sites; the proxy server does all or most of the work. Some ISPs that own and re-allocate address blocks utilize a software package called rwhois (Referral Whois), which will provide information on the IP or domain under their control. And if, for whatever reason, a browser is not available and UNIX is the operating system of the machine being used, the whois command is still available.

Donald McLachlan and the SANS GIAC Community put together a short tutorial called "*Contacting Host Owners*" which describes some of the methods GIAC analysts use.[2] In addition, each of the RIRs have a Frequently Asked Question (FAQ)[3] link from their homepage, which gives pointers and explanations about how to try to contact host owners and suggestions for further information.

## One Site's Basic Setup

Informal data has been collected since March 2000. The public-domain software packages in use over time include portsentry, Snort, and xinetd. Output from various UNIX and third-party daemons, along with FreeBSD's LOG_IN_VAIN sysctl option (where appropriate), is also utilized. Initially, the various software programs sent data to local UNIX syslog files on each machine. The log files would be checked periodically during the day; when probes were detected, a message would be sent to the WHOIS contact for that machine. A file with fields for *date of e-mail*, *IP address* and (starting February 2001) *Owner* are created for each month; any responses are also recorded in this file. The notification e-mail is set up as a template[4] that is filled in with the appropriate data and log entries. Sometimes the structure of the template is slightly changed to reflect the nature of the probes or to show this is a repeated occurrence.

As time progressed and probes became more frequent,

[2]McLachlan, Donald and the GIAC Community. "Contacting Host Owners". Version 0.2. March 31, 2001. URL: http://www.incidents.org/react/contacting.php (17 Nov 01).

[3]ARIN: http://www.arin.net/cgi-bin/whois.pl (enter a question mark in the search box);
RIPE: http://www.ripe.net/ripencc/faq/hackin.html ;
APNIC: http://www.apnic.net/info/faq/abuse/using_whois.html .

[4]A sample template is included as *Appendix A*.

the amount of machines to be watched also increased. To simplify this manual log checking procedure, some UNIX PC's were scrounged together to serve as syslog servers. All syslog data was dumped both locally and to the servers and logcheck was installed on all machines to monitor the log files and send appropriate alerts.

The criterion for sending a "probe message" is not set in stone. It will vary over time, workload, noise level, recent alarms and/or other types of notifications (i.e., CERT, NIPC, SANS), stealth of probe, targeted machine and general crabbiness of the system administrator. Second and third notifications will get sent out when an IP is seen for more than just one occurrence; log entries for the most recent occurrence and for the previous occurrences are included. When all attempts to contact a host owner by e-mail have gone unanswered and probe attempts are still occurring, the host will be blocked for an unspecified period of time.

If too much time has passed between the date of the probe and the current date, no notification will be sent. Exceptions to this are actual exploit attempts, extremely noisy/huge probes and multiple attempts from the same IP number[5]. For the record, all local probes are forwarded upon receipt to the liaison for the internal domain.

## The Data

From the beginning of March 2000 to the end of October 2001, a total of 4276 notification messages were sent. Out of 4276 messages, 239 of them were repeat (or multiple) messages to a site that had already been contacted. Of all the responses received, 1639 were actual responses and 1379 were automated responses[6]. There were 22 phone responses, most of which were received the same day that the probe e-mail was sent. And out of 4276 sent e-mails, some of which had multiple recipients, only 558 were returned as either bounced or undeliverable.

Some sites would respond with an automated response upon receipt of the e-mail, followed by an actual response (or responses). Some sites sent more than one automated

[5]With the advent of Code Red, Nimda and the various incarnations, it has become too time consuming to try to manually contact the host owner for each and every probe. For information on other options, see the section titled "**There Must Be A Better Way**".

[6]Some responses originally categorized as "actual" moved to "automated" over time as the message was always in the same template. The message may not have been an auto-responder per se, just a person sending a pre-written message to save time.

response; one to acknowledge the e-mail and one to report the problem resolved. Actual responses ranged from asking for more information to disparaging remarks and instruction about notification of "harmless" port scanning to reports of the problem being resolved. A fair amount of actual responses included some sort of appreciation for bringing their attention to this matter.

A rough breakdown by month gives the following figures:

| *MONTH* | *# E-MAILS SENT* | *MULTIPLE NOTIFICATIONS* | *AUTOMATED RESPONSES* | *ACTUAL RESPONSES* | *NO RESPONSE* |
|---|---|---|---|---|---|
| March 2000 | 59 | 2 | 12 | 34 | 20 |
| April | 86 | 2 | 18 | 42 | 34 |
| May | 93 | 2 | 19 | 58 | 34 |
| June | 102 | 4 | 12 | 40 | 60 |
| July | 60 | 4 | 7 | 26 | 33 |
| August | 92 | 4 | 23 | 46 | 33 |
| September | 88 | 2 | 21 | 27 | 40 |
| October | 115 | 1 | 30 | 40 | 49 |
| November | 111 | 4 | 29 | 62 | 29 |
| December | 92 | 2 | 37 | 27 | 24 |
| January 2001 | 161 | 6 | 66 | 76 | 48 |
| February | 189 | 2 | 77 | 97 | 50 |
| March | 173 | 2 | 59 | 88 | 45 |
| April | 282 | 12 | 94 | 102 | 102 |
| May | 309 | 13 | 87 | 124 | 115 |
| June | 307 | 6 | 83 | 143 | 111 |
| July | 283 | 12 | 79 | 118 | 97 |
| August | 447 | 48 | 171 | 142 | 167 |
| September | 515 | 80 | 166 | 169 | 198 |
| October | 727 | 31 | 289 | 178 | 289 |
| **TOTALS** | 4291 | 239 | 1379 | 1639 | 1578 |

It's easy to see that what started out as less than 100 electronic mail messages per month in March 2000 have increased to over 700 messages in October 2001. It should be obvious this means that the total number of actual probes is much more than the amount of e-mail that has been sent out.

Taking an informal look at where these notifications were sent is interesting. Out of the 4276 messages that were sent out, less than 10% were sent to .EDU contacts (414 messages). Messages to some of the US Internet Service Providers broke down something like this: 221 included security@uu.net, 69 went to abuse@rr.com, 98 went

to @Home, 76 went to Pacific Bell, 33 went to Concentric, 24 went to Exodus, 125 included Verio, 29 went to Southwestern Bell, 35 went to abuse@psi.com, 38 were addressed to AOL; this totals to at least 748 messages to ISPs here in this country alone.

For countries outside the USA, the total counts were along these lines: 132 messages were sent to German sites, 108 messages to Italian sites, 82 to Brazilian sites, 57 to French sites, 54 messages to Polish sites, 29 messages to Russian sites, 538 to Korean sites, 83 to Japanese sites, 266 messages to Chinese sites, at least 102 to Taiwanese sites, 22 to Hong Kong, at least 209 messages to Canadian sites and 58 messages to Mexican sites. That's at least 1740 messages to sites outside the USA, with Korea accounting for almost one-third (1/3) of them.

As stated earlier, responses covered a wide range, from automated to foreign language. It is absurd to think that the ISPs or other high-volume provider can answer every piece of e-mail manually, so the automated responder makes perfect sense. Even though repeated automated responses may get frustrating after a time, they are better than no response at all. Some examples of automated responses are included in *Appendix B*. Actual responses were interesting, to say the least. At least 118 respondents actually admitted that the machine in question had been compromised[7]. Another 66 answers included the information that the problem had been taken care of. 48 individuals responded that the computer was infected with the most recent virus. At least 9 responses were from sites using some sort of load balancing (like 3DNS boxes from F5). Some of the responses have been known to cause the author to come very close to spraying her computer with her beverage of the moment. A sampling of actual responses is included in *Appendix C* for the reader's enjoyment.

## There Must Be A Better Way

On March 15, 1999 the Computer Security Institute released the results of their fourth "Computer Crime and Security Survey", Cyber attacks rise from inside and outside organizations. The conclusion they drew was that for the third straight year, everything from system penetration to unauthorized access to theft of proprietary

[7]These respondents actually used **compromise** in their message.

information rose in numbers.[8]

On July 26, 2000 congressman Stephen Horn (R-CA) made this comment in his opening statement at the hearing on Computer Security: A War Without Borders: "From the 'ILOVEYOU' virus to attempts to enter the space shuttle's communications system, cyber attacks are on the rise."[9]

On October 15, 2001 Newsbytes published the article "*CERT: Cyber Attacks Set To Double in 2001*". The amount of attacks reported to CERT from January 2001 to October 2001 is 60% more than the amount of attacks reported for the whole year of 2000.[10]

Using the data from this particular site, electronic mail notifications of probes rose from 59 in March 2000 to 727 in October 2001. In 2000, the **highest** amount of notifications sent was 115. In 2001, the **lowest** amount was 161. One conclusion that can be drawn from this is that this process must be automated as much as possible. If not, a system administrator will suffer the same fate as the FBI and CIA recently have: too much data and not enough manpower to assimilate it.

Thankfully, there are two entities that have worked long and hard to help manage the collection of data and notification of host owners: the Attack Registry & Intelligence Service (ARIS) from the folks at SecurityFocus and the Distributed Intrusion Detection System of Dshield.org. Both of these are free services that only require member signup.

ARIS provides an open-source extractor and an ARIS analyzer product. With these, a system/network/security administrator has the ability to submit incident log output anonymously and to access a secure web-based Incident Console to help with the tracking of incidents, creation of incident reports and generating attacker notification messages.[11] ARIS extractor can accept logs from Snort (both Unix and Windows versions), ISS Real Secure, Cisco Secure (formerly Net Ranger) and Network ICE (Black ICE Defender and ICE-pac Security Suite). While the ARIS analyzer will help show if other sites have seen the same attacker, it is primarily intended to help the individual manage intrusion

[8]Rapalus, Patrice. "Cyber attacks rise from outside and inside corporations". 1999 Computer Crime and Security Survey. March 5, 1999. URL: http://www.gocsi.com/prelea990301.htm (17 Nov 01).

[9]Horn, Stephen. "Opening Statement". Congressional hearing on "Computer Security: A War Without Borders". July 26, 2000. URL: http://www.house.gov/reform/gmit/hearings/2000hearings/000726cybersecurity/000726sh.htm (17 Nov 01).

[10]McWilliams, Brian. "CERT: Cyber Attacks Set To Double in 2001". Newsbytes, The Washington Post. October 15, 2001. URL: http://www.securityfocus.com/news/266 (17 Nov 01).

[11]SecurityFocus. "ARIS analyzer Data Sheet". Attack Registry and Intelligence Service. Copyright SecurityFocus, 2001. URL: http://aris.securityfocus.com/AboutAris.asp (23 Nov 01).

detection notifications.[12]

On the other hand, Dshield.org does attempt to categorize and summarize attack trends based on the data received from individuals.[13] There are 9 Windows clients and 12 Unix clients provided by Dshield.org, in addition to their own native format. Registered users can also enable the FIGHTBACK option, which will forward selected submissions to the implicated ISP in response to an attack. Dshield.org also provides daily reports and database summaries from the data received by them.

## Conclusion

With the rise in scans, probes and intrusions, a system administrator can easily become swamped by information from intrusion detection systems. As the site used in this paper shows probes went from an average of 89 per month in 2000 to 339 per month in 2001. There are ISPs, companies and individual administrators that do care if their machines are compromised; not all port scans are innocent. If we ever wish to have a relatively secure Internet, we must persist in any way possible to keep notifying and if necessary blocking sites that are involved in scans, probes and intrusions.



[12] SecurityFocus. "ARIS analyzer FAQ". Attack Registry and Intelligence Service. Copyright SecurityFocus, 2001. URL: http://aris.securityfocus.com/FAQ.asp (23 Nov 01).

[13] Dshield.org. "Dshield Introduction". Dshield - Introduction. 10/10/01. URL: http://www.dshield.org/intro.html (23 Nov 01).

## Appendix A

*Template Probe Notification*

Subject: Probes from 111.222.333.444

Hello, our logs show the following machine has been probing machine on our net here at LOCATION.
     111.222.333.444

Your system may be compromised.  Please let me know if you need more information.  If you are doing these probes, please let us know why we shouldn't block your site from the aaa.bbb network.

Thanks.

---
Here are some entries from our log files (all times are Eastern Standard Time [EST]/GMT –0500):

[Insert log file entries here]

--
Jane Doe  E-mail: jane@aaa.bbb  Pager: (123) 987-6540
Title  Voice: (123) 456-7890  Fax: (123) 456-1234
Company, City State Zip

## Appendix B

*Sample of automated responses*

**EXAMPLE**
This is to acknowledge that we have received your email on abuse and we are now investigating this case.
Please include the Full Header of the Abuser Mail and Anti Hacking Software Log Report to expedite your complaint and speed up the investigations. If you have enclosed the complete information, kindly disregard this message.
We will inform you of the findings when the investigation has completed. If you did not get any feedback from us within 14 days, your case is considered untraceable due to incomplete information. Any dissatisfaction please do not hesitate to email us back.

**EXAMPLE**
Thank you for informing us of possible abuse on Epoch Internet's network. We apologize for any inconvenience this may have caused you while accessing the Internet.
Epoch Internet takes these reports seriously. All of our customers must adhere to our Acceptable Use Policy (AUP), which can be found at http://www.epoch.net/corpinfo/aup.html. It is designed to protect our service, our customers, and the Internet community from irresponsible or illegal activities.
Violators of Epoch Internet's AUP may risk immediate termination of service. Epoch Internet will also report to law enforcement authorities any actions which may be considered illegal.
We appreciate your concern and assure you that we will investigate this matter immediately.

**EXAMPLE**
This is a follow-up message from the UUNET Internet Abuse Investigations Department to let you know the security incident referenced in the subject line above was researched and handled according to UUNET's Service Agreement with its customers.
If you wish to pursue legal action against this user, please have the authorities contact us for information on where to send a subpoena.
If you incur additional security incidents that you believe originate from a UUNET customer, please report them as separate incidents to the appropriate email address below.
Unless you wish to pursue further action, we will close this incident, but it can be re-opened at any time by replying to this email or referring to the ticket# above when calling UUNET Security Support.
This message is intended only for the use of the intended recipient.
If you have received this communication in error, please destroy all copies of this message and its attachments and notify us immediately.

**EXAMPLE**
Hello, The user will be detected and we'll give him a warning.

**EXAMPLE**
----- The following is an automated response to your message
----- generated on behalf of abuse@inwind.it
---------- English message follows ----------
--

Grazie della segnalazione.
Ci attiveremo immediatamente per I necessary controlli e le eventuali azioni.
Inwind condanna qualunque attivita di spam e la violazione della “netiquette”, considerando obiettivo prioritario garantire un uso corretto del servizio da parte dei propri clienti.
Le invitiamo a segnalare ulteriori comportamenti non corretti da parte di utenti InWind ad abuse@inwind.it indicando, se possibile, l’indirizzo di posta elettronica InWind utilizzato, l’indirizzo IP dell’utente e la data e ora in cui e stata effettuata l’operazione.
Cordiali saluti.
InWind Staff

---

Thanks for writing.
InWind makes any effort to guarantee appropriate use of the service by its customers, and will take action against spammers and users that violate “netiquette”.
Feel free to send us further messages regarding violations made by InWind customers. Include in your message, at best, the following information regarding our user:

- InWind e-mail account
- Originating IP address
- Date and time of the operation

Regards.
InWind Staff

**EXAMPLE**
This mailbox is now closed. Your message has been forwarded to the appropriate party.

**EXAMPLE**
This auto-response message is to let you know that we received your e-mail, and though we may not be able to reply to your message, we take all abuse concerns seriously, and will look into the problem, and take proper action against it.

**EXAMPLE**
This is an automatically generated reply to your message. Please do not respond to this message.
Thank you for your message. This response is to acknowledge receipt of mail sent to either abuse@xtra.co.nz or security@xtra.co.nz with your email address as the sender.
Xtra has automated the procedures for reporting allegations of abuse and security breaches involving our network or customers. From 14 August 2001, we no longer accept complaints via email. Please complete the appropriate web forms at http://xtra.co.nz/help/0,,4128-647432,00.html

## Appendix C

*Samples of actual responses*

**EXAMPLE**
The logs don't show a scan.  Port 137 is Microsoft Netbios traffic.

**EXAMPLE** (in response to ftp attempts)
Hi, We have no idea whois doing it or how to stop it.  Very sorry !
Let me know if I can be of any help my cell no. is 999/888-7777.
Thanks.

**EXAMPLE** (in response to a port 111 scan)
We had a test in mail relaying with 211.53.56.212 The result is following..
This ip was rejected  So.. we guess this is not doing spam-relay any more

**EXAMPLE**
You are welcome!
Unfortunately, my original conviction that this was harmless may not bear out.  We have investigated, and the owner of the machine in question thinks he may have been the victim of a Trojan horse imported with a recent Red Hat Linux kernel update.  He thinks his box may have been intruded into, in which case the port scan you saw could have been intentional and more sinister!  Our guy then wiped his machine, and our security folks are now hopping mad at him for destroying the evidence...
It all makes for an interesting life.  In any case, thank you again for your vigilance.  Unless all the Guys (and Gals) With White Hats co-operate, we won't be able to beat those bastards!

**EXAMPLE**
> Gack.  I kinda guessed it was Linux (most of the compromises are nowadays).
And Linux is so easy to set up straight from the box!  Why, any idiot can do it!  And now I can prove it.

**EXAMPLE**
Thanks letting us know that our system could have been compromised.
One of our Linux machines (for testing purposes only) was somehow not included in our Red Hat up to date service and did not receive the latest security patches.  It was hacked on the 11th of this month.  We immediately switched off the machine and are re-installing at this moment.

**EXAMPLE** (two months after notification)
Thanks for your advice.  We found the person that was scanning you.
Steps appropriate have been taken.

**EXAMPLE**
Those are harmless.  Port 137 is netbios-sn – this is a dialup windows machine that has Wins enabled.  More than likely the dialup user was connecting to a web server at your site and his brain-dead windows software was trying to get some kind of windows name resolution (I know next to nothing about windows so I really don't know exactly why it is

doing this.) We see this all the time, both incoming and outgoing. We take a very strong stance against net abuse, but this is honestly nothing to worry about at all.

**EXAMPLE**
Thanks for the info. Sheesh, machine's been up for 12 hours and it gets hit with code red. Bloody hell. We're fixing as I write this. Our apologies for the inconvenience.

**EXAMPLE**
It is a compromised customer. Thank you for informing us.

**EXAMPLE**
We did have a machine compromised over the weekend. We have located it and shut it down. Sorry for the inconvenience.

**EXAMPLE**
Port 79 is "finger", a common internet service offered by many servers. I don't think from what's below that there's any reason to believe anything interesting was going on, just looks like someone ran "finger @yourhost" to see if you ran the service. Try it on our servers and you'll get an actual response (in fact, I wrote the original finger daemon for unix back in the early 80's so I know something about what it is).

**EXAMPLE**
It's a NetBIOS port. There's a virus running around right now that port probes. The customer in question is a DSL customer (novice) and wouldn't know how to hack.
I'll pass the word along to the person responsible for that computer.

**EXAMPLE**
Sorry, for problem cause, we will stop this immed. Mny Tks.

**EXAMPLE**
Thank you for notifying us of this situation.
I have forwarded your complaint to our abuse department. We have a strict policy against port scanning and attempts to gain unauthorized access to other systems. We will terminate service for any customer who repeatedly performs such infractions. In the future, please send any logs of suspicious activity to abuse@speakeasy.net, and appropriate action will be taken.

**EXAMPLE** (in response to logs showing port 515 scan)
What were they probing?

**EXAMPLE**
I have contacted the customer and informed him of what had happened. He has since found out that he has been locked out of the box in question. He has disconnected it from the network, wiped the drive and is reinstalling his OS. I also suggested that he do a thorough security check of his entire network so this does not occur again.

## References


SecurityFocus. Incidents Mailing List Archive. URL: http://www.securityfocus.org/intrusions (17 Nov 01).

American Registry for Internet Numbers. "About Arin". URL: http://www.arin.net/arinintro.htm (17 Nov 01).

Reseaux IP Eurpoeens. "About RIPE". URL: http://www.ripe.net/ripencc/about.html (17 Nov 01).

Asia Pacific Network Information Centre. "APNIC Information and FAQ's". URL: http://www.apnic.net/info/index.html (17 Nov 01).

Network Solutions, Inc. "About RWhois". URL: http://www.rwhois.net/rwhois/about.html (17 Nov 01).

McLachlan, Donald and The SANS GIAC Community. "Contacting Host Owners". Version 0.2, March 31, 2001. URL: http://www.incidents.org/react/contacting.php (17 Nov 01).

Rapalus, Patrice. 1999 Computer Crime and Security Survey. March 5, 1999. URL: http://www.gocsi.com/prelea990301.htm (17 Nov 01).

Horn, Stephen. Congressional Hearing on "Computer Security: A War Without Borders". July 26, 2000. URL: http://www.house.gov.reform/gmit/hearings/2000hearings/000726cybersecurity/000726sh.htm (17 Nov 01).

McWilliams, Brian. "CERT: Cyber Attacks Set To Double in 2001". Newsbytes, The Washington Post. October 15, 2001. URL: http://www.securityfocus.com/news/266 (17 Nov 01).

SecurityFocus. Attack Registry and Intelligence Service. Copyright SecurityFocus, 2001. URL: http://aris.securityfocus.com (23 Nov 01).

Euclidian Consulting. Distributed Intrusion Detection System. URL: http://www.dshield.org (23 Nov 01).