Global Information Assurance Certification Paper

Techniques for Identifying the Threat to your Systems from Researching the Apparent Source of an Attack

David Lemmon

July 9, 2000

I. Introduction

The purpose of this paper is to introduce the reader to a **process** that will enable a system administrator or information security analyst to determine the threat against their systems and networks. If you have ever wanted to know more about who might have attacked or probed your system than just the IP address that appeared in the var/log/messages of your machine, then this paper may help you. Although it is rare, some of these simple techniques may actually help you identify the perpetrator of an attack on your system. While most system administrators are rightly concerned first with securing their hosts and networks from attack, part of doing that job correctly also demands that you have an understanding of the threat against those systems and networks as well. *The risk any system connected to the net faces is a product of vulnerability **and** threat*. The techniques covered in this paper will help you in determining possible actors and possible motivations of the attacker. If you can understand your attacker, than you can better defend and respond to attacks against your network. Of course, it is important to understand that hackers will loop through several systems during the attack phase. So why bother researching the apparent source of an attack? What if your system is the first system of many that the hacker will use in his attack against other systems? Could you be held liable for damage done by the attacker to someone elses' systems downstream? What if he or she is operating from within a country that has no laws against hacking and can thus operate with impunity? Or, what if the hacker is just unskilled and has left clues behind that a skilled researcher could use to identify him? All of these reasons justify taking a small amount of time to research the apparent source of a serious attack or intrusion. Of course all of these techniques should be used AFTER you have secured your system and/or consulted with law enforcement personnel. This should be done if the level and seriousness of the attack justify such an action. Next we will review the tools that are used in the threat identification process.

II. The Tools

The tools listed below outline a *step by step process* that will help you to enumerate the attacking host and possible actors that may have used that host to attack your system. This section is **not** intended to be a tutorial for how to use each tool on its own. There are many sources of information that cover each tool by itself in more detail. Many of you are certainly familiar with or have used many of the tools listed below at one time or another. Keep in mind that here we are talking about the overall process of characterizing the threat from a domain. The first steps in the threat identification process are simply to know who owns the IP used in the attack. For detailed switchology on the use of each tool, consult the man pages or other sources for each tool listed. An excellent source for detailed use of these tools can be found in *Unix in a Nutshell*.[1] Their basic use and operations are listed below. Note: it is advisable to find a web proxy or gateway website for conducting any type of intelligence collection operation against the attacking host itself. In this way, you do not run the risk of further antagonizing or scaring off a potential intruder who might be watching the connection logs from his victimized host. A good

all around site that contains most all the tools listed below is www.samspade.org. [2] This site also contains a brief description of each tool and its use. For instance, to learn more about "dig" command simply hit the more information radio button listed beside the tool. Another useful site is http://network-tools.com/5/.

a. Dig –x /nslookup: The first step in the process is to reverse the offending IP address. The "dig –x ip" command will perform a reverse lookup on an IP address from its domain name server. The "-x" option will ensure that you receive all records possible about your host from the DNS table. This might include nameservers, email servers, as well as the host' resolved name. The nslookup command, "nslookup ip", will also perform a reverse lookup of the host IP address, but will only return the resolved name.
b. Whois: The next step in the process is to perform a whois lookup on the IP address to see who owns or at least who the offending IP is registered to. This can be somewhat of a tricky operation. Use the resolved name above to try to determine what country or region the IP address might be based in, and then be sure to use the proper whois gateway for that region of the world. The main gateways are ARIN – the American Registry, APNIC – the Asian Pacific Registry, and RIPE – the European Registry. There are dozens of others, but most addresses should be registered in one of the above online centralized databases. If your whois data does not match your resolved name, for example the resolved name www.cnn.com and whois database ARIN indicates the registered owner is CNN network (a match), then you may have to do some more digging. Whois databases can contain outdated information. You may want to then research your IP with the country specific whois database to determine the correct registered owner. A good collection of country specific whois databases can be found at http://www.allwhois.com. For more information on conducting detailed whois queries check out http://www.sans.org/y2k/, by Donald McLachlan.[3]
c. Ping : Conduct the "ping ip" command to determine if your attacking IP is currently on-line. Note that many administrators block ICMP traffic, so this is not conclusive evidence either way.
d. Traceroute: The next step in the process is to conduct a "traceroute ip" to determine possible paths from your proxy site to the target system. Traceroute may help you in two ways. If your IP does not resolve it may give you a clue as to its parentage. Look at the resolved host just **before** your target, this host' name may be the upstream provider for the attacking host, and thus a point of contact, or they may in fact have the same domain as your attacking host, although that is not always true. Also, a traceroute might give you an important clue as to the physical location of the attacking box. Carefully look at the path the packets traveled. Do they tell you what city they are in? Often times they will. If you can determine what city the attack came from, you have just narrowed down considerably the possible pool of candidates of who the attacker might be.
e. Finger : Conduct a "finger @ip" command to determine who is currently logged onto the system that attacked you. Now, to be frank, this command will rarely work, since most administrators wisely turn this service off. However, it does not hurt to try. Keep in mind that many systems that are compromised and used as lily pads to attack other hosts are poorly configured (that is why they were compromised in the first place!!) and may have the finger service running. If it is running, finger root@ip to see the last time root was logged on and more importantly, from where root was logged on from. You might be surprised to see root logged on from a third system in yet another country. Keep following the trail as long as

your commands are not refused. I have been able to trace back hackers through several countries using this simple, often overlooked technique. Look for strange login names and for users logged into the system remotely. This may indicate from were the host was compromised from and is the next clue on where to focus your research.

f. Anonymous Surfing: Surfing anonymously to the domain from were your attacking IP is hosted is the next step in the threat identification process. You will know this domain name by looking at the resolved name of the host and the Whois data. One technique that is very useful is to use a search engine such as www.altavista.com with the specialized advanced search option of "+host:domain name and hack*." This query will return the web links of possible hackers that operate from the domain name you queried. You can substitute warez or mp3, etc, to focus in on terms of interest specific to warez or mp3 dealers. The number of webpages returned by the query, as well as the details on those pages, gives you an indication of what level of threat to assess to a certain domain. For example, if you were investigating a host registered to demon.co.uk (Demon Internet) you would type +host:demon.co.uk and hack* in the altavista query box. You may be surprised to see a return of some 22,000 plus hacking related pages hosted on this domain. As a threat analyst, I can conclude that Demon Internet seems to harbor many hackers and as a domain, represents a viable threat to my organization. As a standard practice you might want to block certain domains at your firewall, if you are not already blocking ALL:ALL. Another possibility to widen the search is to use "+link:domain name" in the altavista search.[4] This will show all webpages that have a link to the domain in question listed on their webpage. In other words, the ever popular "here is list of my hacker friends and their c001 hacker sites" pages will appear via this search. You will also want to keep in mind the **target** of the attack. What were the hackers going after? Can you tell? Conduct searches for the resources targeted and combine these terms with Boolean operators like "and espionage." Check newswires or other competitive intelligence sources to determine if possible who might be going after your companies' resources. A good site to use to conduct your searches anonymously is www.anonymizer.com..

g. USENET: The last step in the process of threat identification is to conduct a USENET traffic search on your domain. Sites such as www.deja.com are excellent for this. Search on the attacking IP address in quotes to see if other people are reporting activity from this IP in any security newsgroups. Search on the domain name or hacker aliases that you might have collected from your anonymous surfing above, or from the returns of your finger queries. You can expand the headers of the postings by clicking on "view original posting." This may show you the actual server that posted the message, even if the hacker attempted to spoof his mailing address in the visible header. This method can reveal the **true** location of your hacker. Clicking on author profile can also give you valuable information. Look at the newgroups your hacker post to and look at the number and sophistication of those postings. Pay attention to off subject postings. A hacker will often let down is guard when talking about his favorite band or hobby, for example. You can also search on sites such as www.icq.com if you have a hacker alias from a defaced webpage or from your altavista search narrowed by the domain +hacker criteria noted above.

III. Putting it All Together

Once you have completed the process outlined above and gathered all the information from these tools, you should be able to reach an educated guess about the threat level from the domain that you are analyzing. Hopefully, you were able to collect information about the numbers and

sophistication levels of the hackers that operate from the attacking domain, possible candidates for the attack (through finger or specialized altavista searches), and what other CERTs may be seeing from that domain (via newsgroups or newswire searches). An excellent site to check for archived postings of recently seen attacks is both http://www.sans.org and http://www.securityfocus.com. Ask yourself "were there thousands of hacker pages hosted on the domain that you were investigating?" Likewise, did you find thousands of postings on USENET from this domain concerning hacking? Did you run a search on your organization's name plus hack* ? Were there postings from other administrators detailing attacks from this domain? Were the attacks they mentioned similar to yours or different? Now you might be able to determine if that FTP probe, for example, was just a random probe that targeted several other companies as well as yours or targeted your company specifically. Could you tell from the logs that the attacker was attempting to find a vulnerable FTP server to set up a warez or mp3 site perhaps? Being able to provide an educated guess as to the motivation of your hacker is important. Knowing whether your company has been singled out for an attack as opposed to being just randomly selected, will change the level of concern you have with regard to assessing the threat. The process listed above can be used to narrow down possible candidates or characterize the threat level from responsible domains. And as a byproduct it will also provide you with all the necessary names, phone numbers, and points of contact that may be useful when it comes time to notify the pertinent parties involved.

IV. Conclusion

Always keep in mind that the IP you are investigating is only the apparent source of the activity you see on your logs. As mentioned earlier, this does not mean that you should ignore the IP address, only be cognizant of it's limitations for determining the possible attribution of the event you are investigating. While this process will educate the administrator on how to characterize the threat to his company from analyzing IP addresses that appear in the logs, a complete determination of the threat your organization faces is a more involved process. What you can be sure of is that many threat entities will probe and attempt to intrude upon your systems over time. These may range from Class I (privacy), II (industrial espionage), or Class III (terrorism) attacks as defined by Winn Schwartau's Infowar.com site.[5] Attackers may range from the script kiddie aimlessly probing the networks, to a dedicated industrial espionage hacker looking for your company's secrets. Depending on your company's resources and the value of those resources, you should also investigate the possibility of staffing a professional competitive intelligence cell in your company or in sponsoring an assessment of the threat to your company's systems from a group of intelligence and information security specialists. As one such company states "The serious threat to your IT infrastructure is not a teenage hacker defacing your web site. The true dangers are information and monetary theft, business disruption and critical infrastructure failure. Perpetrators are likely to be professional criminals, hacktivists, competitors or even foreign intelligence agencies. The most costly intrusions are likely to be those that you fail to detect."[6] The bottom line, you need to know the threat against your systems as well as its vulnerabilities.

Endnotes:

[1]McLachlan, Donald. "Contacting Host Owners ver 2.0." 8 Apr 2000. URL: http://www.sans.org/y2k/contacting.htm (12 July 2000).

[2]Gilly Daniel. Unix in a Nutshell. O'Reilly & Associates, Inc. 1994.

[3] Atkins, Steve. Sam Spade Organization. 7 July 2000. URL: http://www.samspade.org (7 July 2000).

[4] George Kurtz, Stuart McClure, and Joel Scambray. Hacking Exposed. Osborne/McGraw-Hill, 1999., p10-11.

[5]Schwartau, Winn. InfoWar.Com Ltd. 8 July 2000. URL: http://www.infowar.com (8 July 2000).

[6] IDefense, iDefense. 8 July 2000. URL: http://www.idefense.com (9 July 2000).