# Global Information Assurance Certification Paper

Timothy Glass
December 19, 2003
GSEC Practical Assignment Version 1.4b



# Tracking the Steps of the Attacker:

## "a *veil of protection from detection*"

## TABLE OF CONTENTS

*"The shaft of the arrow had been feathered with one of the eagle's own plumes. We often give our enemies the means of our own destruction." Aesop (620 BC - 560 BC)*

## 1 Abstract

We face an electronic battlefield everyday. While computers and the Internet offer to simplify our lives tremendously, the risk is still ever present. The balance between risk and security is an ongoing dilemma waged each and everyday. While the battlefield is not divided geographically by borders, neither is it motivated by a political power in some far away county. Nevertheless, the war rages onward at a staggering pace. The one common denominator is that security is neither one single product nor issue. Further, there is no silver bullet to secure information from the outside world. Rather it is an ongoing process and a layered structure of defense.

However, one thing seems to remain the same: after a computer has been compromised--whether it resides within the boundaries of a small home network, a home user or even the corporate enterprise-- the questions remain 'why' and 'how come this happened to me?' The motivation behind attacks perpetuated by the BlackHat community (the Attacker) is a study within itself. However, knowing the basic premise behind their actions and the steps they follow can be a great asset to understanding, giving us a firm foundation from which to construct a safer and more productive computer environment.

## 2 The Motives

One might think that financial gain would be at the forefront of most of the security headlines today. Granted, this incentive accounts for a large amount of the BlackHat community's motivations and activities. Often times, however, their motives draw from a combination of things.

*Storage and/or server* needs are a major motive for the Blackhat. There are many reasons behind this, from the type of content they need to store to distribution of their toolkits to other Blackhats. One advantage to storing and distributing their wares on your system is that, if discovered, they remain anonymous. For example, on August 4th 2003 hackers broke into a server on the network of the Kentucky Transportation Cabinet. The Blackhats had used the server to store pirated movies, music, electronic games and DVDs. [1]

*"Bragging rights"* can also factor into the equation, as the driving force behind some of these individuals and their actions.

[1] Ellen Messmer, NetworkWorldFusion, " Hackers Set Up Shop in State Agency's Server, " http://www.nwfusion.com/news/2003/0804kentuckyhackers.html

*IRC Channels* (Internet Relay Chat) are another motivating factor to Blackhats. This is desirable because the Blackhat needs to achieve administrative rights (sys ops) on the IRC channel. To accomplish this, a bot is usually used to maintain this presence for the Blackhat. Further, it should be noted that the IRC channels are the chosen means of communication for the Blackhat community. [2]

*Spammers* have clear motives. Nucleus Research says the average employee gets nearly 3,500 spam emails each year. [3] While spam in itself is bad enough, spammers are now sending out viruses that in turn convert a normal home PC or corporate desktop into a junk mail spamming machine which can be a very effective tool for the spammer. While this is, in fact, a new twist in an old game, it still works quite well. Anti-virus vendor Trend Micro estimated that the malware can enable the Spammer to send out at least 50,000 emails from each compromised machine. [4]

*Revenge* is another motive, whereby the Blackhat targets a server resulting in a denial-of-service attack. This lends itself to the next step.

Regardless of the motive behind the attack, concealment is of the utmost importance. Attackers must, at all times, conceal their identity from any of the above wrongdoing. Therefore, they utilize a compromised machine or machines to do their work. It is quite commonplace for an Attacker to have hundreds or even thousands of machines under his/her direct control, without the owner of the computer system's knowledge. Experienced Blackhats will take this last step via a method called *hopping,* wherein they go from one compromised machine to another. The final part of this equation is to sanitize the trail behind them, leaving no trace of their existence behind by scrubbing the logs.

### 3 The Myth

No matter how boring the data on your system may seem to you, one very important aspect to understand is that, most of the time, you or your company is just an IP address to an Attacker. It is the very link you use to connect to the outside world which creates the interest. That is all that is necessary for the BlackHat community to come knocking at your door.

Attackers do not seek out individuals personally. Their choice of victims has nothing to do with that, the exceptions being large corporate giants or desktops that hold the corporate jewels. For the most part, Attackers scan the vast wilds of the Internet seeking out vulnerabilities in operating systems and software programs to exploit and selecting their victims accordingly.

---

[2] The Honeynet Project, "Know Your Enemy"
[3] Ian Campbell and Rebecca Wettemann, "The Silent ROI Killer" http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,86145,00.html
[4] Linda Daily Paulson, "Spammers Begin Sending Viruses with their Junk Mail," IEEE Computer Volume 38 Number 8

## 4. Footprinting

"Footprinting," is a technique by which the Attacker gathers information to create a profile of his target, all the while learning the personal or corporate security posture before he or she makes their strike.

The basic premise of this act is "age old" as with its precursor, "non-digital crime", when a criminal cases or stalks his prey before he carries out the attack. With footprinting the Attacker can use standard network tools readily available to him or her, along with a host of tools that are being created on a daily basis in their very own underworld. However, footprinting is not limited to just tools, but also poorly configured systems, firewalls and even source code on the targeted web sites.

Any information the Attacker can glean becomes vital information that he or she needs to assemble this most exclusive footprint on you or your company. While doing research for this paper I viewed source code on one large corporation's web site that used what web designers call HTML comments, which is hidden code not displayed by web browsers but very viewable to someone with the knowledge to do so. Tucked neatly into the HTML document of their company's home page was vital company information for the company's remote employees to login and firewall settings as well. Example of web site code is shown on the following page.



**Sample HTML Code**

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>Any Company USA</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>
<body>
<img src="/XYZComapnyLogo..jpg" width="600" height="100" alt="Company Logo">
<!-- Sales Rep Logon Info make sure to login from the XXXXX server please use the
 username XXXXXX and password of XXXXXXX Remember our firewall settings need to be set
XXXXXXXX Mail server setting SMTP XXXX.XXXXX.net-->
</body>
</html>
```

Footprinting is not limited to settings and names of individuals, but valuable information such as to DNS severs, mail severs, live IP addresses and physical location of severs.

**5. Social Engineering**

Many times when we hear the words security breach we tend to focus on firewalls, routers, security settings and intrusion detection. However, frequently the weakest link is neither hardware nor software at all. Rather it is what is termed "social engineering."

Social engineering can prove to be one of the most effective methods any Attacker can use. Armed with persuasion and deception, the Blackhat makes use of the weakest link in the corporate or private security infrastructure, the human. The reasoning behind this simple yet successful method is largely due to the fact that as humans we just naturally want to be helpful.

A skilled Blackhat utilizes something as simple as communication as his or her means to glean useful information to mount an attack. This information harvest can be in the form of a phone conversation, printed material gained from dumpster diving such as memos, company newsletters, company phone books, manuals and even discarded code. It makes logical sense that media should not be disclosed or disposed of in such a way. Data can still fall into the unlawful hands of an Attacker when media is disposed of media incorrectly.

When data becomes unreadable to the human eye, this is only part of the equation. Many times all or part of the data remains behind and can be accessed by a knowledgeable person with the correct tools. Therefore Disk Sanitization should be a vital ingredient to securely remove any data before discarding any form of hardware or media that has housed data. For many, such as national laboratories, simply utilizing a disk Sanitization program is not enough and complete destruction is required when a hard drive needs to be disposed of.

Two students at the Massachusetts Institute of Technology, conducted a study. The yield from this study found that out of 158 used hard drives from a popular online auction the MIT students were able to recover 5,000 credit card numbers, medical, personal and financial records. Only 12 of the 158 had been properly cleansed. [5]

Still another issue that needs to be addressed is proper disposal of complete computer systems. A practice of many large corporations, businesses and government offices is to give or sell off surplus computer equipment after it is no longer needed. One such breach was that of a government department whereby 139 old computer systems were disposed of. Along with the computers went the data contained within them. Data found on them included 44

[5] Bruce Kaplan, Does your data go with it?
http://info-center.ccit.arizona.edu/~ccitinfo/newsletters/march2003/data_go_.html

government credit card numbers, patients' personal information and medical records. [6]

Many times Social Engineering can take a more passive form such as shoulder surfng. Today, we are a society on the go. From PDA's to laptops, our data and personal information is on the move traveling the friendly skies. Shoulder surfing is something that can be performed while sitting in an airport or any place where a computer screen may be viewed. However, it is not limited to just this method. Today caution should be taken while at the office and also with the placement of computer screens next to windows.

### 6. The Profile

While the Blackhat community is comprised of many faces with multiple avenues of expertise, Blackhats usually tend to exploit the vulnerabilities they know and are best at. Their toolbox allows them to access tools like the *autorooter,* which allows them to scan millions of computers in an automated fashion, requiring very little or no interaction on the part of the Attacker. Their ultimate goal is to find computer systems left vulnerable by things like un-patched operating systems or programs, as well as services left on by default installations, of which the user is unaware. Like an Easter egg hunt, the Attacker simply launches the scan and comes back days later to see what he has collected in this virtual Easter egg basket.

Many times, the Attacker's goal is to then create a type of database of information: the IP addresses scanned, what operating system is running on the system, what services are enabled and what applications are running on the computer. At this point, either the Attacker or the automated software he or she is running will expose whether or not the system is vulnerable and in what way. Today many Attackers simply cut a wide swath across the Internet, deploying their tools and then watching to see which ones work. This permits them to skip the database step in its entirety. While some Blackhats will target a network searching for a vulnerable computer, higher-end Blackhat toolkits enable them to not only scan and footprint the system for the version and applications that are running, but also to then launch the attack. This is accomplished all in one step.

### 7. It's a 24X7 Global Playground

The important thing to remember about the Blackhat community is that their automated scans of the Internet never rest. They work into the wee hours of the morning- in short 24 hours per day and seven days of the week. Thus, the Internet is a global playground for the Attacker. Furthermore, it is essential to understand that neither physical boundaries nor time zones affect the Blackhat, thus eliminating the assumption that any one time period is safer than the other for your network or computer system. Nor should one limit his or her attention to

[6] Judi Hasson, "VA toughens security after PC disposal blunders" http://www.fcw.com/fcw/articles/2002/0826/news-va-08-26-02.asp

certain time periods when reviewing the trail of data that resides within the log files of each and every computer.

### 8. The Secret to Their Success

When giving talks about Internet and computer security, I give several examples as to why I feel the Blackhats have such a great success rate. Perhaps most importantly is that they share well. We can all take an important lesson away from this. The Attacker's world is made up of a large global network of people that share the information they have learned, such as IP addresses they have already scanned and services that are left unattended and wide open. In short, the Attacker does not have to reinvent the wheel. A simple examination of the underground world's archive can quickly reveal what systems are out there, where the systems are and what exploit will conquer the computer. While the Attackers' toolkits are quite complicated in code, they are intuitive by nature, and user-friendly to the point that even a beginner is quite cable of launching an attack.

### 9. Tool Distribution and Education

The most common means for tool distribution, in addition to the education of less knowledgeable Blackhats, is via IRC Channels and web sites.[7]

Take for example a web site, whereby the BlackHat community sets up shop for a credit card bot. Calling themselves *carders,* this group of Blackhats can download and utilize the credit card bot. The bot is made up of IRC Client scripts, a few text files, a Visual Basic program and a Trojan Horse. The icing on the cake, per se, is the detailed instructions for use, along with a very intuitive user interface. However, the Blackhats do not stop there. They also include advice on how to commit credit card fraud. Again, the key element to their success is sharing both knowledge and tools. [8]

Some Attackers are what information security professionals call *script kiddies*, less experienced and usually younger Attackers. Once a script kiddy has compromised a computer, what usually transpires is that the more sophisticated Blackhat then creates a backdoor to allow easy access to the computer system where he or she can install Trojans, all the while eluding detection from system administers and end users.

One myth about protection from Blackhats involves changing system passwords or even accounts. This will not have any affect in locking out the remote Blackhat user from the system. With the system binaries now termed *trojaned,* the Attacker's activities are hidden, not even showing up in the computer log files. [9]

---

[7] Honeynet Project, "Automated Credit Card Fraud" http://www.honeynet.org/papers/profiles/cc-fraud.pdf

[8] Bill McCarty, "Automated Identity Theft," IEEE Volume 1 number 5

[9] The Honeynet Project, "Know Your Enemy"

In many cases, the Blackhat community will then probe and conquer its prey. Like an army taking a beachhead, it raises its flag in conquest by establishing a web site or server to distribute toolkits for the underground world of the Attacker. This only requires a compromised system to act as server, and this is usually done without anyone's knowledge. As stated above, this gives the Attacker a veil of protection from detection.

### 10. A Contributing Cause

There are several viable reasons behind why attacks are so easy to achieve. Throughout my research for this paper I found one of the worst problems to be that of the default installation.

I like to refer to this as, out of the box and into the hands of the Attacker, "the default installation." Many software vendors site ease of setup and use as their underlying reasoning behind this type of installation. The installation is not secure. For many users, they assume new and out of the box mean just that, a ready-to-go and a somewhat turn-key solution. This accounts for many new computers sold today, as well as operating systems and upgrades.

The default installation may lessen the amount of calls to the vendor's help desk, not to mention the vendor's time and resources to reissue software updates to the operating system. However, it will give the consumer a false sense of security assuming new really means "new." Users or system administers are then faced with the time consuming task of having to first do a "basic" securing of the system such as: turning off unnecessary services, renaming default accounts and passwords to enable them to connect to the Internet and be able to patch the operating system safely. [10]

### 11. Vulnerabilities

While vulnerabilities can be found in many forms from flawed software, un-patched systems, and unsecured services to misconfigured firewalls, the issue of trickery plays upon human nature and a predictable response. The latest trends seem to be utilizing just that.

Trickery allows the Blackhats to infiltrate with what seems to be a benign message. The message usually plays upon a request for information with a helpful link to click upon to provide the information that is being requested. Once clicked upon the user is redirected to a web site. While the web page looks official, many times with company logos and colors, it is a nothing more then a malicious web page and email that has been set up by an Attacker. The Attacker counts on a predictable response to achieve their goal along with misleading code embedded into the email. Coupled with the latest vulnerability in a popular web browser Microsoft internet Explorer this has all the vital ingredients the Attacker needs. Please see Example of code below:

[10] SANS Institute Internet Storm Center, Windows XP Surviving the First Day http://isc.sans.org

| Example of URL Obfuscation |
| --- |
| <a href="http://www.goodsite.org%01%00www.badguy.org<a/> |

When clicking on the link, one may think they are being directed to goodsite.org. However, the way the browser handles this is that they will be directed to badguy.org. This method allows the Blackhat to display an arbitrary fully qualified domain name (FQDN) which is much different than the one the user assumes they are going to. If fact, to add to users' confusion when looking at the lower part of the browser screen, the user will see www.goodguy.org. Furthermore, the address bar of IE will display www.goodguy.org. To see how this works, a test page has been set up at Secunia web site at the page below. http://www.secunia.com/internet_explorer_address_bar_spoofing_test/ [11]

Testing other browsers such as Mozilla 1.5, I noticed it did not truncate the URL in the address bar although it did when I moused over the link on the page.

### *12.* Conclusion

Over the last few years, we have seen the Blackhats' many creative ways of exploiting systems and means of defrauding users, from the trickery of cross scripting to utilizing exploits of vulnerable operating systems. One thing that will never change, in the worlds of both the Information Security Professional and the Blackhats, is that it will never be static. The driving forces behind both worlds are parallel in the sense that they are both dynamic and change is ever present and cannot be measured in years nor days but many times in seconds.

Often times users become their own worst enemy by predicable actions as well as becoming part of the security problem when failing to patch and update software. The corporate enterprise today performs a constant balancing act between time, testing and patch management.

The more sophisticated hardware and software become, computers and the Internet offer to simplify our lives. However, the trade off is risk. To help users better understand these risks and what to do about them, I created a weekly newsletter with security tips.

The conclusion I have arrived at is that neither the classroom nor text is the proving ground. Rather, the global reach of the world becomes the playing field. Information security professionals have learned to level this playing field by many means such as the Honeynet project and the lessons learned from this.[12]

---

[11] Secumia http://www.secunia.com/internet_explorer_address_bar_spoofing_test/

[12] Lance Spitzner, "Top Three Advances in Honeynet Technology" SANS Webcast http://www.sans.org/webcasts/show.php?webcastid=90433

## References

1.)Ellen Messmer, NetworkWorldFusion, " Hackers Set Up Shop in State Agency's Server, " http://www.nwfusion.com/news/2003/0804kentuckyhackers.html

2.)The Honeynet Project, "Know Your Enemy"

3.)Ian Campbell and Rebecca Wettemann, "The Silent ROI Killer" http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,86145,00.html

4.)Linda Daily Paulson, "Spammers Begin Sending Viruses with their Junk Mail," IEEE Computer Volume 38 Number 8

5.)Bruce Kaplan, Does your data go with it? http://info-center.ccit.arizona.edu/~ccitinfo/newsletters/march2003/data_go_.html

6.)Judi Hasson, "VA toughens security after PC disposal blunders" http://www.fcw.com/fcw/articles/2002/0826/news-va-08-26-02.asp

7.)Honeynet Project, "Automated Credit Card Fraud"
http://www.honeynet.org/papers/profiles/cc-fraud.pdf

8.)Bill McCarty, “Automated Identity Theft,” IEEE Volume 1 number 5

9.)The Honeynet Project, “Know Your Enemy”

10.)SANS Institute Internet Storm Center, Windows XP Surviving the First Day
http://isc.sans.org

11.)Secumia
http://www.secunia.com/internet_explorer_address_bar_spoofing_test/

12.) Lance Spitzner, “Top Three Advances in Honeynet Technology” SANS Webcast http://www.sans.org/webcasts/show.php?webcastid=90433