Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# Why me? Minimizing your Internet Exposure

As the Internet community becomes more skilled in their use of attack tools, we are seeing an increase in the number and severity of Internet attacks. Internet neophytes and professionals alike are asking the same question "There are hundreds of thousands of computers on the Internet, why was my computer attacked?" This paper will be an overview analysis on some tactics you can use to reduce visibility as a cyber-target. The intended audience is not for the enterprise security professional but for the home user and sma...

Copyright SANS Institute
Author Retains Full Rights

AD

# Why Me?

# Minimizing your Internet Exposure

**Student: Kevin Wagner**

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b, Option 1
Global Information Assurance Certification (GIAC) Program

Date Submitted: April 30, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

# Table of Contents

**TABLE OF CONTENTS** ..... **2**
**ABSTRACT** ..... **3**
**THE ATTACKERS** ..... **7**
**ATTACK METHODOLOGY** ..... **9**
**THE MINIMIZATION OF YOUR PRESENCE** ..... **11**
*Social Engineering* ..... *11*
*User Habits* ..... *12*
*Visible Deterrents* ..... *12*
*Buying Time* ..... *15*
**PROTECTING YOUR VISIBILITY** ..... **17**
*Firewalls* ..... *17*
*Awareness Training* ..... *17*
*Anti-virus* ..... *18*
*Patching and Updating* ..... *19*
*Burglar Alarms/Honey Pots* ..... *19*
**CONCLUSION** ..... **20**
**LIST OF REFERENCES** ..... **21**

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

## Abstract

As the Internet community becomes more skilled in their use of attack tools, we are seeing an increase in the number and severity of Internet attacks. Internet neophytes and professionals alike are asking the same question "There are hundreds of thousands of computers on the Internet, why was my computer attacked?" This paper will be an overview analysis on some tactics you can use to reduce visibility as a cyber-target. The intended audience is not for the enterprise security professional but for the home user and small to mid sized businesses that do not have large dollars allocated for IT security.

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

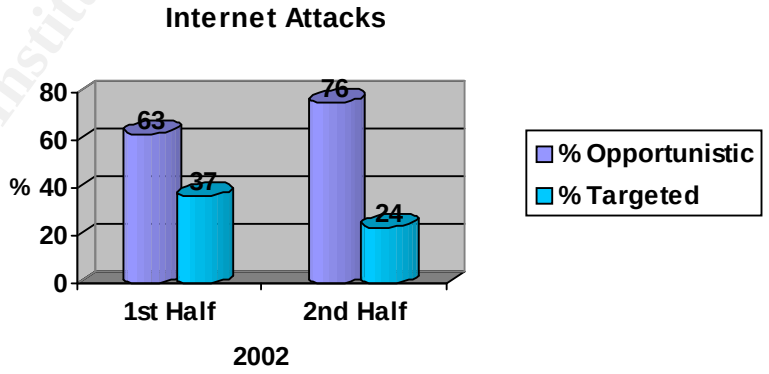
# Introduction

Nobody wants to be a victim of a cyber crime. The task of limiting your visibility to attackers may seem a daunting one at first so we need to take a look at some statistics on how targets are chosen and what can be done to minimize your visibility to these methods. This paper is intended to give home and small business users an awareness of methods to reduce their visibility to attack and prevent them from becoming an attacker's low hanging fruit.

When you own a car, you want to reduce its visibility to car thieves or at least make it appear more secure than others around it. One of the methods to do this is by using a steering wheel club. Car thieves are looking for a preferable model of car and one that can be quickly broken into without worry of being caught. This analogy compares well with Internet attackers looking to break into your systems. They, as well, are looking for a preferable model (Windows, UNIX, etc.) and one that can be quickly infiltrated without consequence (no patching, P2P file sharing, and failure to implement basic security). The attackers are looking for easy victims and will choose the less protected systems or the low hanging fruit.

During the first half of 2002, research conducted by Riptech[1] has shown that 63% of all attacks had the appearance of being opportunistic in nature while the remaining 37% were targeted attacks. Research conducted by Symantec[2] for the second half of 2002 shows us an increase in the opportunistic attacks to 76% leaving 24% of attacks as targeted (see Figure 1). Opportunistic attacks are explained to be attacks intended to exploit any vulnerable organization on the Internet. Targeted attacks are explained as attacks that are targeted at a pre-selected victim.

**Figure 1 Internet Attack Categories**




We can clearly see from this information that if a user or business wants to be made less visible as a target to attackers, they need to concentrate on reducing the effects of the more prevalent opportunistic attacks. This may seem like a tall order as we have

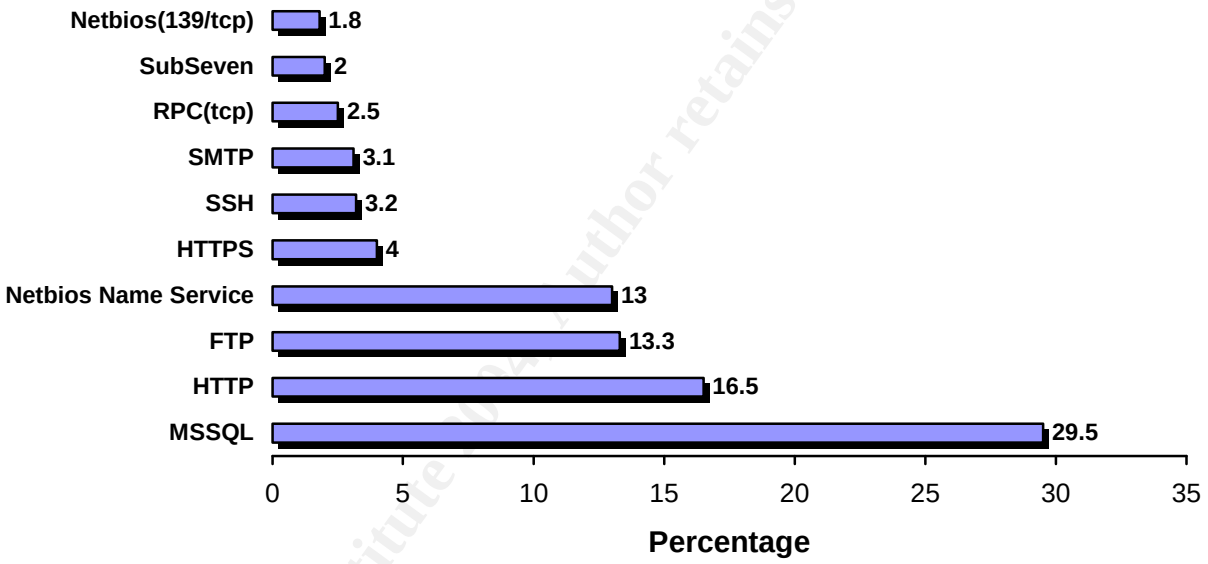
[1] Riptec, Incorporated, p. 6
[2] Symantec, p. 21


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

become attuned to using the Internet to conduct both business and personal affairs online. We want to have a noticeable Internet presence to increase our market visibility or to sell our product. Internet presence and attack visibility are two different things. Internet presence is awareness to all potential business partners while attack visibility is awareness to a select group of people that want to do you or your business harm.

The methods and means attackers use to infiltrate computers and/or networks has a direct effect on us on how we interact with the Internet. The previously mentioned studies show that 99.9% of all the scans used by attackers that were detected during the six-month period were focused on only 20 services. The top ten services are listed in Figure 2.

**Figure 2 Top Ten Scans by Service[3]**




The task of reducing visibility to attackers is more manageable now that we know how they choose their targets and how they infiltrate the ones that they do discover. We can use this data to elevate our company's security stance into a position that is superior to the average Internet user. In doing so, we move out of the realm of low hanging fruit into one that observes standard security practices. This will provide more of a challenge for an attacker than most systems on the Internet.

One caution we need to keep in mind is that it is virtually impossible to completely protect your PC or network from attack if you are being pursued by a talented and dedicated attacker. Even the best enterprise solutions have an Achilles heel an attacker can exploit. This thought process could be likened to our previous car analogy. Vehicles with the steering wheel club are moderately protected from car thieves but are not impervious to them.

[3] Symantec, p.22


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Using the concepts of risk analysis, a high risk with a low probability of success target will be viewed as unattractive to attackers. A low risk with a high probability of success target will be highly attractive and preferable for attackers. This is where the attackers prefer to go, an easy target with a low chance of discovery. Your goal should be to make your systems a higher risk than the other systems the attackers may look at.

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

# The Attackers

## Attacker Psychology

Before we talk about attackers and their Psychology, we need to understand the distinction between attackers and random worms. Attackers want into your system either through direct interaction or through an automated process. Internet worms are driven only by the intent to spread themselves and to cause either an annoyance or damage. Most of the items discussed here will help to protect you against worms but, since they are random and not considered a directed attack, we will concentrate the discussion on directed attacks.

Who would want to attack you? The Internet is a wide-open playing field that offers people anonymity and at the same time gives people a false sense of security in that anonymity. We will need to understand who these attackers are and what makes them want to view or destroy your data.

Studies have determined that there exists a common characteristic amongst all hackers and that is to minimize their actions and behavior as a service to the Internet community. This research has determined that the typical hacker may have a sense of inferiority and feel that the razing of a companies Internet presence gives them a sense of power they otherwise may not be able to attain. We need to reduce our appeal to these types to reduce our visibility and stay out of their radar.

Research conducted by Marc Rogers, a behavioral sciences researcher, and Jerrold Post, a psychiatrist, have indicated that not all hackers are criminals and have categorized them into four profiles.[4]

> **Old School Hackers:** These are the computer programmers from the early days of computing who are interested in lines of code and how they work with the system. Their actions are not typically criminal in nature but show a lack of concern for privacy due to the belief that the Internet is an open system by design.
>
> **Script Kiddies**: This group typically wants to be known as hackers and tend to brag online about their exploits. Script kiddies enjoy the thrill of downloading scripts to run exploits against companies to vandalize or disrupt their business.
>
> **Professional Criminals or Crackers:** This group makes their living by breaking into systems and then selling the information for profit. There is typically a link from this group to organized crime.
>
> **Coders and Virus writers:** This group typically has a background in programming but tend to only use their code in their own internal test networks. They depend on others, likely the Script Kiddies, to start the spread of the code on the Internet.

[4] Jeremy Quittner



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Each of these groups will profile a victim in a different manner. We need to take a look at how this is done and determine how we can minimize our attractiveness to them.

The old school hackers will typically not have an interest in opportunistic attacks. They will likely select a target based upon the information they know will exist there (typically academic institutions) and likely wouldn't do any damage to the data. This would be of greater concern if the information they accessed were confidential.

Script kiddies use attacks that will almost always be opportunistic in nature. They are quickly aware of the newest vulnerabilities and will employ a script once they can download it. Their intent is to do damage and to make it known they have done so. The best way to avoid this type of hacker is to minimize your exposure to opportunistic attacks.

The professional criminals or crackers will almost always use attacks that are targeted in nature. It is very difficult to protect yourself against this group because of the large amount of funds that are available to finance their efforts. Their attacks will typically be difficult to detect and will likely have some sort detrimental financial effect on you. Most home users and small businesses will not have to worry about the attention of this group.

The last group, coders and virus writers, will use opportunistic attacks to spread their code from machine to machine. Once again, the elimination of common vulnerabilities will reduce the affect this group has on you or your business. The damage from attacks will range from merely annoying to destructive.

We can see that the typical home user and small business generally need only be concerned with the script kiddies and the coders/virus writers. Both these groups employ attack methods that are opportunistic and depend upon a generic vulnerability in your defenses. This attack method is not targeted at you but will catch you if your defenses are not patched for the vulnerability they are scanning for.

When creating your security strategy, keep in mind the value of the data you are protecting. Putting a steering wheel club on an economy car will suffice whereas a club on a premium sports car will not suffice and will require additional security efforts. Also, thinking like an attacker will help you determine your vulnerability to attack. For example, an attacker may look favorably upon small to mid-sized companies because it implies a reasonable probability of a small and over-stretched IT team where there is likelihood that updates may be overlooked or delayed.

Now that we have an understanding of who the attackers are, what motivates them and the nature of their attacks, we will continue with some information on why and how some targets stand out more than others.


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

## Attack Methodology

To understand how you may have been profiled in the past or how you may be profiled in the future, there needs to be an understanding of the methodology of an attack. In this section we will be looking at the targeted attack directed at you or your organization. The methodology behind an opportunistic attack is slightly different due to the fact that the attackers are simply looking for the most targets vulnerable to a particular weakness. Once found, they will then target their victims using that exploit, limiting their results to the boundaries of the exploit.

In a targeted attack, Dr. Greg Miles describes a methodological process attackers use to gain as much information about a system and then proceed to exploiting or owning that system. It is as much a process about learning as it is in exploiting.[5] Miles goes on to describe the six stages of the methodology of an attack as originally written in the book Hacking Exposed: Network Security Secrets and Solutions by McClure, Scambray, and Kurtz.[6]

Stage1 – Target Acquisition
The choice of a target varies by hacker but from the previous discussion on attacker psychology, we have a general idea of where and how they attain their targets.

Stage 2 – Profiling
This stage is where the attackers gather information as it relates to the victims setup, business they are in, who they conduct business with and any other type of information that will give the hacker further insight into the business and how it operates. This is where your system needs to appear as an unattractive target to the attacker. From the information that has been gathered, the attacker will decide here whether to proceed with the attack or look for easier prey.

Stage 3 – Initial Access
After the profile is complete, the attacker can now proceed with their initial access through the use of the information they gathered in the profiling stage.

Stage 4 – Privilege Escalation
Once into a system, the attacker will proceed with privilege escalation to a higher authority user account. This will give the hacker access and control of any information on that system.

Stage 5 – Cover Tracks
Next thing an attacker will do is try to cover their tracks through the use of tools that can erase their activity so it cannot be traced back to them.

[5] Dr. Greg Miles, p.1
[6] McClure, Scambray and Kurtz, p.428


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Stage 6 – Backdoor
The last thing an attacker will do is setup a backdoor so they can access the system without having to be logged on with a power account.

Now that we understand the methodology of the attack, we need to know more about the methods that you can use to minimize your visibility. Having an understanding of both concepts will aid us in reducing the likelihood you will become a target to an attacker.

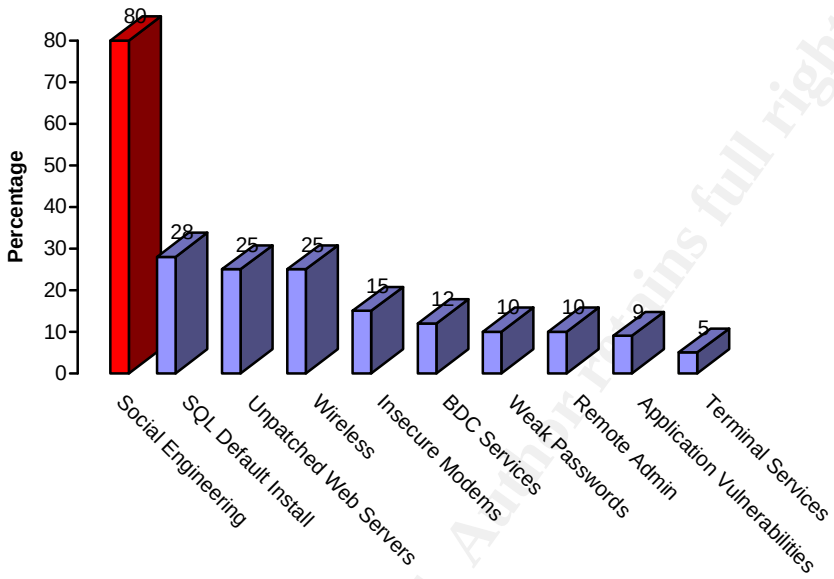
© SANS Institute 2004, Author retains full rights.


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

## The Minimization of your Presence

Paul Vlissidis from The NCC Group ran a two year study on the defenses of their customers and came up with some surprising statistics. Figure 3 represents his findings on how their penetration testing group was able to circumvent the defenses of some of the nations top security minded corporations.

**Figure 3 Attack Methods** [7]




**Note:** Percentages total more than 100% because some corporations were vulnerable to more than one type of attack.

Social engineering is clearly the most effective attack method. Next, we will discuss ways in which you can limit its effect and some other methods to minimize your visibility. This will help the attackers to look somewhere else.

### Social Engineering

We can see that a large percentage of the successful attacks were from an attacker using the technique called social engineering. In this case, social engineering is the process of gathering information about a person or company that will help an attacker get into your computer systems. Typically, this is in the form of a phone call or email claiming to be someone they aren't and requesting information on you or your company. One of the more blatant uses of social engineering is to simply phone someone in an office telling them you are from the IT department and are investigating the strength of user passwords to increase security. With minimal work, an attacker could have access to passwords, usernames, server names, OS version, workstation names, etc.

Social engineering is a difficult attack to defend against because it is used against something you have little control over – your users. One way to combat social engineering is to have drills and train your users to demonstrate a consistent awareness

[7] The NCC Group, p. 6


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

of security. If an attacker tries to extract information from a user and is properly questioned and then refused by them, the attacker will have a strong indication that your organization is security aware and will view you as an inhospitable target.

**User Habits**

Users are typically the weakest link into any organization. As we can see from the statistics in Figure 3, this is what attackers are depending on. Users tend to harbor a feeling that they are being controlled by the IT environment and they have a false sense of superiority when it comes to judging the impact of their own actions on the work environment.

With your users aware of what social engineering is and why security is a good thing, you now need to work on some of their other habits. They may not know that these habits help to contribute to the heightening of your visibility on the Internet.

On-line discussion or chat groups are another venue for your PC or organization to come to the attention of attackers. If instant messaging or the use of chatting is allowed at your organization, some rules should be implemented to limit your exposure. Simple things like not using your company name/location, not taunting a user, proper use of criticism if it needs to be used, not bragging about your security stature, etc.

These things seem like common sense but without the use of facial expressions, visual stature, or tone/inflection, a seemingly innocent statement may come across as an attack on the other person's credibility. For most people, they would take these things into consideration but there are some people that will take offense and, if it's the wrong person, they may attempt a targeted attack or may even post your information to a hackers chat list. This, at the very least, will project a non-professional image and will likely increase your visibility to just the people you are trying to avoid.

Users need to realize that the Internet could be a conduit to an attack and they should respect it as such. This will project an image that you are serious about your Internet presence. These factors along with basic security controls will lessen your visibility as a target to attackers profiling you or your company.

**Visible Deterrents**

We have discussed the attacker, the methods they employ and the most common type of attack. We haven't really talked about the ways you can project your image as a secure organization thereby reducing your attractiveness to attackers. Next, our discussion will move to some of the methods available to you to show you are in the security game and attackers should look elsewhere for an easier mark.

It is hard to believe that it still needs to be said that people should keep their software patched and up to date. The theory behind an Internet attack is to find a weakness or vulnerability in either the software, a default configuration or in the security stance taken. All three of these attack points are the responsibility of the owner of the data that is being advertised to the Internet for public visibility.


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Vulnerabilities in software (including operating systems and web browsers) are inevitable because it is next to impossible to think of all the potential possibilities for attack. Application vulnerabilities are a means to step around the built in security or finding a fault in the software to make it malfunction. We can use our analogy of a steering wheel club again. If there were a fault in the locking mechanism on the club allowing a car thief to bypass the security, such as striking the lock with a hammer, wouldn't the owner of the vehicle ensure that this was fixed or replaced immediately? This is the same for your computer. Vulnerabilities are known ways around the proper functionality of your software.

Just the simple act of keeping your system up to date will move you into a security stance more secure than most systems on the Internet. This will reduce your visibility to a multitude of attacks. This is exactly what we are trying to accomplish. If you don't have your system patched and up to date, you are inviting random or opportunistic attacks that can later lead to targeting by an attacker. Worms circulating on the Internet are not driven by an attacker in particular, they are looking for someone to activate them so they can propagate further. If you have a strong security stance in place, these annoyances will have minimal or no effect on you. This will leave you with more time and resources to deal with the real or targeted attacks.

Attackers that depend on opportunistic attacks generally have a focus on collecting the largest number of vulnerable systems. This is usually done through scripts created to harvest systems in a range of IP's that are susceptible to the most recent vulnerability. If you are patched for this, you have already reduced your visibility to these types of attacks.

**Search Engine Hacking**

Search engine hacking is one of the most interesting visibility factors that has come about recently. When users run into problems with their system, they usually post their error message to newsgroups requesting help for their situation. If you don't impose some form of discretion in your post, you may be giving an attacker a free pass into your system.

Attackers have realized the potential of using Google™ or other search engines to query for vulnerable computers to attack. Users are generally told to give as much information as possible so that others can use it to help solve their problem. Sometimes, users post error messages that contain within it their username and password in clear text. Simply put, the attacker enters into their favorite search engine a common error that will reveal some critical piece of information about you or your systems. This may easily give them the access they require to penetrate your system.

An example of a site dedicated to aid the attackers in their error searching can be viewed at http://johnny.ihackstuff.com/index.php?module=prodreviews (use the "googledorks!" menu item). When posting error messages to the Internet, be sure to remove any identifying or confidential information.


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

**Unresponsive Firewall**
A transparent firewall operates at layer 2 (Data Link layer) rather than the traditional Layer 3 (Network layer) by simply moving packets from one interface to the other without processing them further. [8]

Where is the advantage to visibility by doing this? The main benefit is that the transparent firewall is invisible to the Internet because it does not have an IP address. This will make it impervious to attacks.[9] If the transparent firewall is configured to drop packets (not respond to them like traditional firewalls) that do not conform to the configured rules, attackers will see this absence of response as a sign of enhanced security at your site. They will also know that you have taken steps to protect your network, making it more than trivial for an attacker to create a profile on you. The visibility of a strong security stance will make it easier for an attacker to move on to a less defended target.

**Banners**
An excellent way for an attacker to gain information on you is to view your banners that you are publishing freely to the Internet. Banners may reveal anything from software versions to the type of web server in place.

If you provide the attacker with easy access to the information he is seeking, they may not use techniques that you can detect while they are conducting information gathering. Simple examination of the HTTP headers or banners will reveal your web server unless you have taken steps to obscure it.[10] If there are no reconnaissance attempts, you may miss the attack until it's already upon you.

The removal or changing of banners that respond to external sources is an important step to reducing your visibility to attackers. Some say this is security through obscurity. I believe that projecting an image to the attacker that you are taking steps to minimize revealing information will make them think that an attack will require more effort than they would be willing to put forth.

**DNSSEC**
DNSSEC is short for DNS Security Extensions and is a method for securing the Domain Name System by implementing end-to-end authenticity and integrity.[11] DNSSEC uses digital signing to verify the identity of the requester with an authoritative server. There are a number of attacks that rely upon the unrestrictive nature of the DNS protocol that can lead an attacker to gaining more information about you or your company than you want them to have.

DNSSEC is still in its infancy stages but is gaining in popularity due to attacks that are using the trusting nature of the existing DNS protocol. If you implement DNSSEC, you

[8] Security Focus, p.2
[9] Security Focus, p.2
[10] Evolt.org, p.1
[11] DNSSEC.net, p.1


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

will be making a fairly bold statement that you embrace a strong security stance and are leading edge in the implementation of security configurations – a tough nut to crack.

**Security Practices**

Appearances do mean everything in security visibility. Implementing publicly visible and easy methods to contact your organization in the event of abuse or a related security issue will show that you are following publicly acceptable security practices.

Become involved and active in your local security community. Not only does this give you the visibility of a person/organization that embraces security but it also gives you a support group to fall back on in the event you do have a security incident. Following up on all suspicious activity with your ISP will likely not gain you a resolution but will gain you the reputation of being watchful.

All of these visible deterrents give an image to an attacker that you are security conscious and have likely implemented further security precautions that aren't readily visible to the attacker. Attackers will likely move on to any number of other targets that don't project themselves to be as 'prickly' as you.

**Buying Time**

One of the final visibility topics we will discuss is the ability to hamper the attacker from tailoring his attack by knowing what OS you are running. This topic is generally reserved for users more advanced than the typical home user but does have some merit as at least an insight into the steps attackers are willing to take.

The spoofing of your OS is by no means a guarantee of safety from attackers but may give you that small advantage over targets that do not employ such measures. If an attacker uses tools that have falsely detected your OS as a Linux variant and then notices packets coming from your PC/Network that are representative of some Windows-based applications, they can be reasonably sure that the OS is spoofed or you have Windows machines hidden behind your spoofing device.

What is OS Spoofing and what advantages are there to knowing what OS is in place? There is a good paper called the "Analysis of Remote Active Operating System Fingerprinting Tools" written by Ryan Spangler (University of Wisconsin)[12] that details three of the products (Nmap, RINGv2 and Xprobe2) used to fingerprint a remote OS. Spangler defines remote active operating system fingerprinting as the process of determining the identity of a remote host's operating system by actively sending packets to the remote host and viewing the responses. You might ask why this would be so valuable to an attacker. The value in knowing the OS is important to attackers because vulnerabilities are usually dependent on the OS version.

[12] Ryan Spangler, p.1,11,31


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

To protect yourself from these reconnaissance activities, you can employ a number of different options.

- The best defense is the use of a firewall that only allows needed ports to be open to the Internet with the remaining ports filtered. Nmap is more accurate when it finds at least one open TCP port and a closed TCP and UDP port.
- Another defense method is to change the characteristics of the TCP/IP stack through a packet mangler that can adjust the values on outgoing packets. This is usually reserved for more advanced users as the TCP/IP stack has built-in efficiencies and altering it may cause traffic issues.
- Implementing a Network Intrusion Detection System (NIDS) will allow for the detection of these tools across the network. This is generally reserved for larger corporations.
- Implementing a proxy or firewall to hide your machines. Once again, this is generally reserved for larger corporations.
- Block both incoming and outgoing ICMP traffic at the firewall. This will prevent attackers from probing your network.

Why is any of this of value to you? You have to keep in mind you are trying to reduce your visibility and to make an attacker think there are easier targets out there. If you go through the steps of spoofing your OS and the attacker finds out, they will know that you have a security mindset and will likely be taking additional precautions to secure yourself and to capture their activity.

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

## Protecting your Visibility

Now that you have seen some of the basic techniques you can use to limit your visibility to attackers, the discussion will turn to an overview of some products meant to aid in further protecting your visibility. Protection can come with a high price tag. Since this discussion is geared toward home and small business users, the overview will cover free or low cost products. These products function as well as the more costly versions that are available for corporate use. Keep in mind that protection implies lower visibility or attractiveness to an attacker thereby improving your security stance.

**Firewalls**

Firewalls are your best line of defense in decreasing your visibility to outside attackers. This can be one of the most important decisions you can make to protect your network from an outside attack. Different needs require different solutions. We will discuss only software firewalls as hardware firewalls are generally more expensive, require additional expertise and would be beyond the scope intended.

Henry Stephen Markus has produced a review of some of the best known personal firewalls available.[13] This paper is a must read for first-time firewall users as it contains some excellent background information on what a firewall is and how it works. The review can be found at www.firewallguide.com/software.htm.

Markus chose two products as the leaders in the race for the best personal firewall. These products are:

- Norton Personal Firewall by Symantec – 2002 version cost is minimal (renewal required) and includes features such as privacy features and cookie manager. Norton Internet Security (2004 version) has a firewall, anti-virus, privacy control, anti-spam and parental control.
- Zonealarm Free/Plus/Pro – There is a free version for personal use or advanced versions available for a minimal cost. Features include easy install and configuration, traffic blocking and email scans.

A properly configured firewall is essential to reducing your visibility to the Internet. They are meant to restrict unauthorized traffic in and out of your PC, thereby blocking the opportunistic traffic that is meant to find you.

**Awareness Training**

Everyone from the home user up to and including the top corporations in the country should have some form of security awareness training. User Training is often viewed as being unnecessary, costly and without a monetary return. In reality, it will save you in user downtime, help desk costs and other IT support costs.

Users will find value in training if you can show them some of the simple tricks attackers will use. This includes such things as lifting keyboards for passwords, an attempted

[13] Henry Stephen Markus, p.2


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

social engineering attack, a port scan simulation (and simultaneously how the scanners usage was detected by systems already in place) and other things that will pique their interest. Keep in mind that there is a fine line to giving enough information for awareness and to giving them the tools and the desire to try hacking out for themselves.

Training can be in the form of a defined training plan in the organizations large enough to support them or it can be in the form of users reading online material about the subject. The Carnegie Mellon CERT® Coordination Center has put out two guides called Home Computer Security[14] and Home Network Security.[15] Both guides are geared toward home users and are an excellent reference point for user security education.

How does awareness training help reduce visibility? If social engineering or user manipulation is removed from the attacker's bag of tricks, you have severely limited the most effective tools of an attacker. Why would an attacker stick around to try some of his less productive tools when he can go to another organization that is less prepared?

**Anti-virus**

Viruses can be both annoying and costly to you or your company. Most viruses can be prevented by using common-sense but that isn't always going to prevent an infection. Your best bet is to install an Anti-virus product set up correctly to detect and clean your virus infections. Viruses have a number of methods to gain access to your PC/network including e-mail, diskettes/CD-R, P2P file-sharing and downloads from the Internet. Viruses are meant to spread themselves to others whether it is at a basic level through e-mail or at a more advanced level by setting up its own SMTP server on an obscure port.

Some examples of free virus scanners are:

McAfee Virusscan (http://us.mcafee.com/root/package.asp?pkgid=100&cid=9901)
- A low cost defense against viruses (includes mail scan and auto-update)

Symantec Norton Antivirus (http://www.symantec.com/nav/nav_9xnt/)
- A low cost antivirus solution with similar features plus spyware and keystroke logger protection.

AVG (http://www.grisoft.com/us/us_dwnl_free.php)
- A free home user edition with standard features. A low cost professional edition is available.

Once you are infected, the virus will be making continual attempts to propagate itself to other machines. These attempts will be broadcasting to the Internet telling everyone that your system security is lacking. Preventing the infection and the subsequent actions performed by the virus will be a major step in reducing your visibility to attack.

[14] http://www.cert.org/homeusers/HomeComputerSecurity
[15] http://www.cert.org/tech_tips/home_networks.html


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

**Patching and Updating**

If you want to reduce your visibility, patching and updating your systems is one of those things that is mandatory (and free!). Almost all software companies offer patches and updates to their customers. The best way to keep up to date is to subscribe to mailing lists from your software vendor so that you can be alerted to any patches they have put into service.

Some of the better lists available that detail vulnerabilities include the following:

| | |
|---|---|
| Secunia | http://secunia.com/secunia_security_advisories/ |
| Scintelli | http://www.sintelli.com/ |
| NT Bugtrac | http://www.ntbugtraq.com/ (go to "subscribe" under Quick Links) |
| RedHat errata | http://www.redhat.com/security/ |
| MS Update | http://v4.windowsupdate.microsoft.com/en/default.asp |

Unpatched software is one of the first things an attacker looks for in opportunistic attacking. The benefits are obvious for keeping your patching up to date. You will have the best features of your software/OS, it will be secure and you will reduce your exposure and visibility to attackers.

**Burglar Alarms/Honey Pots**

Can you reduce your visibility by increasing your visibility? This sounds like an odd method to your goals but it does hold some merit. Burglar alarms and honey pots are systems that project to be something that they are not. Burglar alarm software notifies you when someone is attempting to access your system and keeps logs of the attackers IP and what operations they were attempting.[16] A honey pot does exactly what it sounds like – draws the attackers to a system and acts as a trap set to capture attackers or draw them away from your production systems.

How does a burglar alarm decrease my visibility? Well, it actually gives you a slight bit more visibility because it emulates software you may not have and responds to traffic as if the application were installed. The value is in how it works like a poor-mans honey pot providing an early warning system to an attack.

A honey pot requires more expertise to ensure that the system created as a honey pot doesn't act as a stepping stone for an attacker. Before implementing a honey pot, research needs to be done to ensure you are implementing a technology that suits your needs.

The benefit of a honey pot and/or a burglar alarm is mainly one of an early warning system. It may act as a tool to reduce the visibility of your critical systems by directing traffic away from them but if not properly implemented it may put your network at risk. We can see this is a slight twist to our topic. Instead of making your visibility lower and having someone else's system on the Internet appear more attractive, you are creating that attractive target within your own network.

[16] NFR Security, p.1


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

## Conclusion

Becoming invisible on the Internet is an impossible task due to the true nature of the Internet. Your presence there already means you are identifiable and visible. The goal of this paper is to show home and small business users the statistics behind how attacks are conducted and how can you make yourself an unattractive target to attackers.

Most attacks are opportunistic or random in nature. To decrease your visibility to these attacks you need to pay attention to some of the basic concepts in security like vulnerability patching and updates. To reduce your visibility to targeted attacks you need to project an image to the attacker that it won't be worth their while and they may even get caught if they attempt to infiltrate your defenses. You want them to think that there is an easier target just down the road.

Your security defenses can be likened to a minefield. Initially, when you make your first step into the Internet world you are faced with walking across a minefield where at any turn, you could trip a mine and make yourself known to the attackers. The intent of this paper is to turn the tables on the attackers. We want the minefield to be on your side. Instead of you, it will be the attacker that thinks he has to step through the minefield to get to your systems. Any false move and they will be caught.

Reducing your visibility to attackers should only be one of your defenses. Keep in mind that your security strategy should be a defense in depth strategy. Having multiple layers of defense will increase your chances of preventing an attack and also of detecting the attacker's presence.


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

# List of References

Blecher, Tim; Yoran, Elad. "Riptech Internet Security Threat Report." Volume 2, July 2002. URL: http://www.securitystats.com/reports/Riptech-Internet_Security_Threat_Report_vII.20020708.pdf (April 27, 2004)

Ahmad, David; Arnold, Cori Lynn; Dunphy, Brian; Prosser, Michael; Weafer, Vincent. "Symantec Internet Security Threat Report." Volume 3, February 2003. URL: http://www.securitystats.com/reports/Symantec-Internet_Security_Threat_Report_vIII.20030201.pdf (April 27, 2004)

Quittner, Jeremy. "Hacker Psych 101." March 14, 2004. URL: http://tlc.discovery.com/convergence/hackers/articles/psych.html (April 27, 2004)

Miles, Dr. Greg. "Yes Virginia, There is a Hacking Process" July 17, 2000. URL: http://www.securityhorizon.com/security_whitepapers/hacking_resolution/HackerProcess.html (April 27, 2004)

McClure, Stuart; Scambray, Joel; Kurtz, George. Hacking Exposed, Network Security Secrets and Solutions, Berkeley:Osborne/McGraw-Hill, 1999. 428-439

Vlissidis, Paul. "Hacker with wife and 3 kids to feed . . . give generously." URL: http://www.nccglobal.com/press_releases/IS%20Opportunities.pdf (April 27, 2004)

Tanase, Matthew. "Transparent, Bridging and In-line Firewall Devices." October 15, 2003. URL: http://www.securityfocus.com/infocus/1737 (April 27, 2004)

port80. "Mask your Web Server for Enhanced Security." 06/01/2003. URL: http://www.evolt.org/article/Mask_Your_Web_Server_for_Enhanced_Security/18/60160/ (April 27, 2004)

"DNSSEC – DNS Security Extensions, Securing the Domain Name System." URL: http://www.dnssec.net/ (April 27, 2004)

Spangler, Ryan. "Analysis of Remote Active Operating System Fingerprinting Tools." May 2003. URL: http://www.net-security.org/dl/articles/osdetection.pdf (April 27, 2004)

Markus, Henry Stephen. "Personal Firewall Reviews." March 25, 2004. URL: http://www.firewallguide.com/software.htm (April 27, 2004)

Rogers, Lawrence R. "Home Computer Security." 2002. URL: http://www.cert.org/homeusers/HomeComputerSecurity/ (April 27, 2004)



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Carnegie Mellon University. "Home Network Security." December 5, 2001. URL: http://www.cert.org/tech_tips/home_networks.html (April 27, 2004)

NFR Security. "Computer Burglar Alarm." June 26, 2002. URL: http://www.whitehatadvisory.com/articles/020626-nfr.html (April 27, 2004)

Granger, Sarah. "Social Engineering Fundamentals, Part1: Hacker Tactics." December 18, 2001. URL: http://www.securityfocus.com/infocus/1527 (April 27, 2004)

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 22nd, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **SANS Malaysia @ MCMC 2013** | **Cyberjaya, MY** | **Jun 03, 2013 - Jun 08, 2013** | **Live Event** |
| **SANS Pen Test Berlin 2013** | **Berlin, DE** | **Jun 03, 2013 - Jun 08, 2013** | **Live Event** |
| **Industial Control Systems Security Training - Houston** | **Houston, TXUS** | **Jun 10, 2013 - Jun 15, 2013** | **Live Event** |
| **Security Impact of IPv6 Summit 2013** | **Washington, DCUS** | **Jun 14, 2013 - Jun 16, 2013** | **Live Event** |
| **SANSFIRE 2013** | **Washington, DCUS** | **Jun 14, 2013 - Jun 22, 2013** | **Live Event** |
| **SANS Canberra 2013** | **Canberra, AU** | **Jul 01, 2013 - Jul 13, 2013** | **Live Event** |
| **Digital Forensics & Incident Response Summit 2013** | **Austin, TXUS** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS London Summer 2013** | **London, GB** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS Rocky Mountain 2013** | **Denver, COUS** | **Jul 14, 2013 - Jul 20, 2013** | **Live Event** |
| **SANS Mumbai 2013** | **Mumbai, IN** | **Jul 22, 2013 - Jul 27, 2013** | **Live Event** |
| **SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification** | **Washington, DCUS** | **Jul 22, 2013 - Jul 26, 2013** | **Live Event** |
| **SANS San Francisco 2013** | **San Francisco, CAUS** | **Jul 29, 2013 - Aug 03, 2013** | **Live Event** |
| **SANS SEC 560: Network Penetration Testing @ Bangalore 2013** | **Bangalore, IN** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **SANS Boston 2013** | **Boston, MAUS** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **Critical Security Controls Summit** | **Washington, DCUS** | **Aug 12, 2013 - Aug 18, 2013** | **Live Event** |
| **Industrial Control Systems Security Training - DC** | **Washington, DCUS** | **Aug 12, 2013 - Aug 16, 2013** | **Live Event** |
| **SANS Thailand 2013** | **Bangkok, TH** | **Aug 19, 2013 - Aug 31, 2013** | **Live Event** |
| **SANS Virginia Beach 2013** | **Virginia Beach, VAUS** | **Aug 19, 2013 - Aug 30, 2013** | **Live Event** |
| **Mobile Device Security Summit 2013** | **OnlineCAUS** | **May 30, 2013 - Jun 06, 2013** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |