Global Information Assurance Certification Paper

Name: Mike Adams
Version Number: GIAC Security Essentials Certification (GSEC) Practical
Assignment: Version 1.4b (amended August 29, 2002), Option 1
Title: Analysis of Intrusions Detected on a Windows 98 PC with a Dialup Connection and with a Cable Modem Connection

Abstract

A previous version of this paper was written (and passed) for KickStart. It examined an actual case log of intrusions detected by BlackICE Defender (a personal firewall and intrusion detection system) on a typical family computer running Windows 98 with a 56K dialup Internet connection and fairly typical family Internet usage. I examined how many intrusions occurred, what type of intrusions they were, and what hackers may have been attempting to achieve by the various intrusions. After KickStart was eliminated and merged into GSEC, those who were previously enrolled in KickStart but switched to GSEC (like myself) were given the opportunity to expand on their previous KickStart papers for GSEC.

This paper does that, expanding on the original paper by comparing and contrasting the results from the dialup connection with the results from a high-speed cable modem connection for the same computer and operating system. Intrusions detected in both cases were researched on the Internet to try to determine the intent of the intrusions. In addition, the data was examined to determine any differences in the types of attacks, frequency of attacks, sophistication of attacks, etc. Additionally, the purpose of this paper is also to show how even casual Internet users are regularly attacked by hackers probing their systems, and why a personal firewall is important when accessing the Internet from home - regardless of whether that connection is a dialup or always-on connection. Without personal firewall protection, little stands between ordinary Internet users and often-hostile attackers.

Glossary

BIND: The Berkeley Internet Name Daemon, the most popular DNS server software.
BlackICE Defender: Personal firewall and intrusion detection software for PCs.
DHCP: Dynamic Host Configuration Protocol, a way of dynamically assigning IP addresses.
DNS: Domain Name Server, a server that translates domain names to IP addresses.
Dynamic IP address: An IP address assigned to a system for the current session only, and then reassigned to another system.
IRC: Internet Relay Chat.

ISP: Internet Service Provider.
NetBus: A Remote Access/Control Trojan Horse.
PCAnywhere: Remote access software from Symantec.
POP3: Post Office Protocol 3, used to receive email.
Shields Up!: A free service that tests systems for open ports and intrusion exposure.
SMTP: Simple Mail Transfer Protocol, used to send email.
SNMP: Simple Network Management Protocol.
SOCKS: A protocol that a proxy server can use to accept requests and forward them across the Internet.
SQL: Structured Query Language, a language for database programming.
Static IP address: A single IP address assigned to a system semi-permanently (i.e., not just for the current session).
SubSeven: A Remote Access/Control Trojan Horse.
TFTP: Trivial File Transfer Protocol.
Trojan Horse: A malicious program pretending to be something it is not, as in the ancient story of the Trojan Horse.

Introduction

In this paper, I will examine actual case logs of intrusions detected by BlackICE Defender on a typical home PC running Windows 98 – first with a typical 56K dialup internet connection, then with a high-speed cable modem connection. This is a family computer, with fairly typical family Internet usage. I will examine how many intrusions occurred for each type of internet connection, what type of intrusions they were, and what hackers may have been attempting to achieve by the various intrusions. I also will compare and contrast the results from the dialup connection with the results from the high-speed cable modem connection.

The purpose of this paper, in addition to analyzing the data from two types of Internet connections, is then to also examine any differences in the types of attacks, frequency of attacks, sophistication of attacks, etc. For example, were attackers able to attempt more sophisticated follow-up attacks because of the always-on connection versus the dynamic IP address of a dialup connection? Or did BlackICE Defender protect the PC sufficiently so that the only difference was the number of attempted attacks?

Most computer users are oblivious to intrusions that occur regularly on their systems. Even people who are aware of some risks may assume that those risks apply mostly to companies, or at least to individuals with always-on Internet connections (i.e., DSL or cable modems). Articles in the media (sometimes by security "experts!") have even been guilty of propagating this myth. While always-on Internet connections often provide a static IP address (or at least a dynamic IP that changes very infrequently), most dialup access providers assign dynamic IP addresses that are only assigned for the duration of the user's

session, and then are reassigned to new connections. This makes it more difficult for hackers, since intrusions frequently follow a staged approach over multiple sessions. The IP address at next login to a dialup ISP is not likely to be the same as for the previous session. Still, this doesn't stop hackers from trying….

Intrusions on the Dialup Connection

BlackICE Defender was installed on my home PC in mid-December 1999. It provides a very friendly user interface, and both visual and audible alarms when an intrusion is detected.

Within the first week, intrusions were already being detected and prevented by BlackICE Defender. Over a 78-week period from December 17, 1999 to June 15, 2001, 275 intrusion attempts were detected. This represents an average of approximately 3.5 intrusions per week, or one intrusion every other day on average! So much for the myth of such attacks pertaining mostly to high-speed, always-on connections!

The 275 intrusions are broken down by type in Table 1 below. As can be readily seen, the vast majority, about 70%, were various port probes. These port probes are further broken down by type of port probe in Table 2 below.

Table 1: Types of Intrusions (Most frequent to least frequent) on Dialup Connection

Type of Intrusion	Number of Intrusions	Percent of Intrusions
Port probes	192	69.82%
PCAnywhere pings	50	18.18%
DNS Spoofs	10	3.64%
TCP OS fingerprint	8	2.91%
HTTP URL contains "~"	4	1.45%
Suspicious URL	2	0.73%
Port scans	2	0.73%
DNS BIND version request	1	0.36%
Back Orifice pings	1	0.36%
HTTP GET data very long	1	0.36%
POP3 login failed	1	0.36%
SMTP uucp-style recipient	1	0.36%
Scan by sscan program	1	0.36%
UDP Trojan Horse probe	1	0.36%

Table 2: Types of Port Probes (Most frequent to least frequent) on Dialup Connection

Type of Port Probe	Number of Intrusions	Percent of Intrusions
TCP port probe	80	29.09%
UDP port probe	28	10.18%
FTP port probe	22	8.00%
SubSeven port probe	14	5.09%
Proxy port probe	9	3.27%
SOCKS port probe	8	2.91%
DNS port probe	6	2.18%
DNS TCP port probe	6	2.18%
DNS UDP port probe	5	1.81%
RPC port probe	4	1.45%
RPC TCP port probe	3	1.09%
IRC port probe	2	0.73%
SNMP port probe	2	0.73%
TCP port scan	2	0.73%
Telnet port probe	1	0.36%

Intrusions on the Cable Modem Connection

On April 19, 2002, a high-speed, always-on cable modem was installed on the same PC. Over only the next 9-week period from April 19, 2002 to June 21, 2002, 755 intrusion attempts were detected! This represents an average of approximately 83.9 intrusions per week, or about 12 intrusions every day on average – about 24 times as many as with a dialup connection!

The 755 intrusions are broken down by type in Table 3 below. As can be readily seen, the vast majority, about 87%, were various port probes. These port probes are further broken down by type of port probe in Table 4 below.

Table 3: Types of Intrusions (Most frequent to least frequent) on Always-On Cable Modem Connection

Type of Intrusion	Number of Intrusions	Percent of Intrusions
Port probes	659	87.28%
Duplicate IP Address	95	12.58%
ISS Ping Scan	1	0.13%

Table 4: Types of Port Probes (Most frequent to least frequent) on Always-On Cable Modem Connection

Type of Port Probe	Number of Intrusions	Percent of Intrusions
SQL port probe	441	58.41%
SubSeven port probe	68	9.01%
FTP port probe	67	8.87%
TCP port probe	59	7.81%
RPC TCP port probe	7	0.93%
NetBus port probe	5	0.66%
Proxy port probe	4	0.53%
DNS TCP port probe	4	0.53%
SNMP port probe	2	0.26%
Telnet port probe	1	0.13%
TFTP port probe	1	0.13%

Protection

Fortunately, BlackICE Defender did an excellent job of detecting and preventing the intrusions. To further test BlackICE Defender, I used the free *Shields Up!* service from Gibson Research Corporation [<https://grc.com/x/ne.dll?bh0bkyd2>] to analyze the relative effectiveness of BlackICE Defender on both the dialup connection and the always-on cable modem connection. In both cases, it indicated that my PC was in "stealth mode." To *Shields Up!*, my PC was not visible at the IP address it was connected to. The PC did not respond to any of the port probes and did not appear to exist or to be in service.

Summarized Descriptions of Intrusions

Now let's briefly examine the various intrusions which BlackICE Defender detected [as listed above in Tables 1 through 4].

Port probes: About 70% of the intrusions were port probes with a dialup connection. With the always-on cable modem connection, about 87% were port probes. These essentially represent reconnaissance by hackers or malicious programs. Hackers could be gathering information about a system to determine what sort of attacks can be mounted based on what services are running or in a LISTENING state. Large scale scans of many ports and IP addresses are often run, frequently by script-kiddies, so these normally don't represent personal attacks; however, if weaknesses are found, an attacker (or a malicious program) may attack any vulnerable machines. With a dialup dynamic IP address there is generally less risk from port probes, since it is unlikely that the user will still have the same IP address by the time a human checks logs of port probe results from a scripted attack. In an attack like this, there is much more of a risk with an

always-on connection that keeps the same IP address. This difference is becoming less true with malicious programs like the SQL Snake, however, which seeks out machines to attack and tries to gain administrative control, all without human intervention. Tables 2 and 4 break down the port probes by type. Basically Tables 2 and 4 show that the port probes tend to fall into two categories: probes of miscellaneous TCP/UDP ports or more targeted probes looking for specific services. Examples of more targeted probes include FTP port probes, probes for the SubSeven Trojan Horse, proxy port probes, SOCKS port probes, IRC port probes, SNMP port probes, telnet port probes, and SQL port probes, each of which will be discussed individually below.

The following intrusion discussions are in alphabetical order by intrusion name.

Back Orifice Ping: Someone pinged the PC looking for the infamous Back Orifice Trojan. If this Trojan had been detected, the hacker could have taken remote control of the PC with disastrous results (editing the Registry, viewing cached passwords, sending and receiving files, etc.) The hacker appears to have been running a wide sweep of addresses, because the xid parameter was set to 0x0, so they were not targeting this particular PC. The password was set to the default Back Orifice password (0x7A69), but the default port was changed from the default port to 0x04D5, indicating that it may have been a more serious attacker, and not just a script-kiddie. This analysis was based on the data from BlackICE and on information from Internet Security Systems' BlackICE Defender web page on this exploit at:
[<http://www.iss.net/security_center/advice/Intrusions/2001506/>]

DNS BIND version request: Someone is looking for DNS servers running versions of the BIND DNS server with known security holes. This doesn't apply to my PC.

DNS spoof successful: Although a DNS spoof can potentially allow an attacker to redirect from a friendly web site to a hostile web site, these particular cases seem to be false positives caused by my ISP redirecting through a caching server.

Duplicate IP Address: I believe that this is probably a false positive (not actually an attack), however I'm still trying to figure this one out. I believe my cable company uses DHCP to allocate IP addresses, and I suspect it has something to do with this DHCP configuration; but I'm still not sure of that, because the IP address has not changed.

FTP port probes: These are typically mass port scans which can represent either attempts to locate FTP servers to break into or attempts to find FTP servers which can be used for storage and retrieval of files between hackers, a kind of a hijacking of an FTP server for their own ends.

HTTP GET data very long: A URL with a length of 16098 characters was received. This appears to have been an attempt to execute a buffer overflow.

HTTP URL contains ~: An attempt to access a file with the DOS naming convention and using a "~" was intercepted. Each of these appears to have occurred while working with FrontPage, and these occurrences do not appear to have been attacks, though there is a vulnerability in unpatched versions of IIS and PWS.

IRC port probes: Attempts to see if the IRC service is running and could possibly be exploited.

ISS Ping Scan: An attacker is using the Internet Scanner from ISS to check my system for any common system vulnerabilities. Interestingly, ISS also now owns BlackICE Defender. Detailed information about this exploit can be found in the following CERT advisory:
<http://www.cert.org/advisories/CA-1993-14.html>

NetBus port probes: These attackers are scanning systems to find ones that have been infected with the NetBus Trojan Horse program. NetBus is one of a group of Trojans that are classified as Remote Access/Control Trojans which give a hacker great control over a system that has previously been compromised with the Trojan. Detailed information about NetBus can be found at the following web site: < http://www.nwinternet.com/~pchelp/nb/netbus.htm>.

PCAnywhere pings: These can be broken down into two categories: definitely hostile or possibly hostile/possibly accidental. Those that originated from outside my ISP's address range (7 out of 50, or 14%) are definite attempts to find a system running PCAnywhere with poor security. Those that originated from inside my ISP's address range may be attempts to find a system running PCAnywhere with poor security or they may be accidental pings resulting from someone within the ISP's address range (and with poorly configured PCAnywhere software) scanning the network for PCAnywhere agents.

POP3 login failed: This appears to have been generated by myself, upon unsuccessful logins to my email account.

Proxy port probes: These are attempts to find proxy servers. Hackers can exploit these as jumping off points to go on to access other systems with anonymity.

Scan by sscan program: sscan is a hacker tool that scans systems for vulnerabilities. It usually precedes more concerted attacks, and can even be configured to automatically run scripts of malicious commands. CERT Incident

Note IN-99-01 [<http://www.cert.org/incident_notes/IN-99-01.html>] describes this tool and associated exploits in great detail.

SMTP uucp-style recipient: This appears to have been triggered by a poorly formatted link in an email from Web Monkey that contained variables defined with percent signs.

SNMP port probes: Attempts to find systems running SNMP, a networking protocol that can easily be hacked to allow great access to the system and to the network to which it may be attached.

SOCKS port probes: Attackers are looking for systems running improperly configured SOCKS, which they could then use to bounce attacks to other systems while concealing their identity.

SQL Snake: I first saw an SQL port probe on May 12, 2002. Then, beginning on May 20, 2002, I began experiencing a large number of SQL port probes. This was the first sign of the now-infamous SQL Snake. This worm looks for Microsoft SQL servers with no admin password. If it succeeds in getting in, it gains administrative control, infects the system, tries to spread further to other systems, and tries to email critical system configuration and password files to an attacker's email address. It spreads across the Internet without the need for any human action, and is still quite active. Much of the above description is summarized from the detailed information in this CERT Incident Note: <http://www.cert.org/incident_notes/IN-2002-04.html>.

SubSeven port probes: These attackers are scanning systems to find ones that have been infected with the Trojan Horse program SubSeven. SubSeven is one of a group of Trojans that are classified as Remote Access/Control Trojans which give a hacker great control over a system that has previously been compromised with the Trojan. Detailed information about SubSeven can be found at: <http://www.commodon.com/threat/threat-sub7.htm>.

Suspicious URL: This can indicate that someone has constructed a data packet to attempt to execute malicious code on my PC; however, in this case it appears to have been a false positive generated by myself. This analysis was based on the data from BlackICE and on information from Internet Security Systems' BlackICE Defender web page on this exploit at: <http://www.iss.net/security_center/advice/Intrusions/2002500/?>

TCP OS fingerprint: These were generated by attackers sending TCP messages to gauge the response from my system and determine what OS my PC was running. These would normally precede more specific attacks targeted at my system's specific holes once the OS was identified. These are more of a threat with an always-on, static IP address connection than with a dialup connection,

since they represent reconnaissance that a hacker can try to take advantage of later.

Telnet port probe: These are from attackers looking for servers running the telnet service, which would potentially allow them to log on to the machine.

TFTP port probe: This was an attempt by an attacker to see if the TFTP service was running. If it had been, there are several different exploits that could have been used. These are described at: <http://www.iss.net/security_center/advice/Services/TFTP/Intrusions/default.htm>

UDP Trojan Horse probe: This was a hacker scanning UDP port 2140, most likely to see if my system had been infected with the Trojan Horse program Deep Throat, which runs on that port. Deep Throat is one of a group of Trojans that are classified as Remote Access/Control Trojans. Detailed information about Deep Throat can be found at <http://www.commodon.com/threat/threat-dt.htm>.

Comparisons and Conclusions

Comparing and contrasting the types of attacks, frequency of attacks, sophistication of attacks, etc. between the two connections, the following is easily seen:

- There was a huge increase in the number of attempted attacks with the always-on connection – about 24 times as many as with the dialup connection!

- There were no PC Anywhere pings during the initial 9 weeks with the always-on connection. This is likely due to the fact that I was one of the very first cable modem customers when my cable company put internet access in. There were few other customers to even run PC Anywhere! A couple months after the 9-week period examined in this paper I did begin getting a few PC Anywhere pings originating from other customers on the cable company's network.

- In both cases, the majority of attacks were port probes, looking for services and open ports of entry.

- There was no apparent evidence of any sophisticated follow-up attacks with the always-on connection. I believe that BlackICE Defender sufficiently shielded the ports and covered evidence of any PC being on at my IP address. This was very reassuring, since I was concerned about the safety of an always-on connection. Without a personal firewall, I believe that there would have been a high probability of more serious followup attacks.

- The most noted difference, the tremendous number of SQL port probes, was not due to the type of connection at all – it was simply a matter of timing. The SQL snake was first reported in the wild on May 20, 2002, the day that BlackICE started beeping like a storm with SQL port probes. More than 58% of all attacks against the always-on connection were SQL snake port probes. And, according to my current logs, it shows little signs of abating.

So perhaps, ultimately, the primary difference that was seen (other than simple frequency of attacks, due to the always-on connection) is the stark and obvious truth that the sophistication of automated attacks continues to grow. The SQL snake is out there growing independent of human interaction now. Just as many home users don't maintain their antivirus software and signatures, users and administrators, whether at home or at work, are also not very good about consistently patching systems against new exploits.

As can be readily seen, even a normal home PC with 56K modem dialup access and dynamic IP address gets hammered on pretty frequently and severely. Now millions have always-on connections…and web servers and business servers are up 24x7. Every day there are new, more sophisticated exploits, viruses, and worms. The greatest need in security over the next few years may well be to educate system administrators and the masses.

For Further Information

Lists of common Trojan Horses, with detailed info:
<http://www.commodon.com/threat/>

A very long list of Trojan Horses (and the ports they normally listen on) can be found at: <http://www.simovits.com/nyheter9902.html>

Additional info about BlackICE Defender (now called BlackICE PC Protection):
< http://blackice.iss.net/product_pc_protection.php>

References/Citations

Anonymous. "NetBus: BO's Older Cousin." 25 November 1998. <http://www.nwinternet.com/~pchelp/nb/netbus.htm> (last visited 6 January, 2003).

CERT Coordination Center, Carnegie Mellon University Software Engineering Institute. "CERT Advisory CA-1993-14 Internet Security Scanner (ISS)." Last revision 19 Sept, 1997.

<http://www.cert.org/advisories/CA-1993-14.html> (last visited 6 January, 2003).

CERT Coordination Center, Carnegie Mellon University Software Engineering Institute. "CERT Incident Note IN-99-01: " "sscan" Scanning Tool." 28 January, 1999.
<http://www.cert.org/incident_notes/IN-99-01.html> (last visited 8 January, 2003).

CERT Coordination Center, Carnegie Mellon University Software Engineering Institute. "CERT Incident Note IN-2002-04: " Exploitation of Vulnerabilities in Microsoft SQL Server." Last updated 23 May, 2002.
< http://www.cert.org/incident_notes/IN-2002-04.html> (last visited 8 January, 2003).

Fratto, Mike. "SQL Snake is your Problem." Network Computing. 24 June, 2002.
<http://www.networkcomputing.com/1313/1313buzz2.html> (last visited 6 January, 2003).

Gibson, Steve. "Shields Up! Internet Connection Security for Windows Users." 2001.
http://grc.com/x/ne.dll?rh1bi2l2=rqfsevl3 (last visited 6 January, 2003).

Kelloway, Don. "The Basics of SubSeven (aka Sub7 or Backdoor_G)." Threats to your Security on the Internet.
http://www.commodon.com/threat/threat-sub7.htm (last visited 6 January, 2003)

Kelloway, Don. "The Basics of Deep Throat." Threats to your Security on the Internet.
http://www.commodon.com/threat/threat-dt.htm (last visited 6 January, 2003)

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

Network ICE. BlackICE Defender (software), version 2.5. Network ICE, 1999-2001. [Note: BlackICE is now owned by Internet Security Systems (ISS) and the newest version of the product is now called BlackICE PC Protection.]

Network ICE and Internet Security Systems. "Database of Intrusions Detected by Network ICE."
<http://www.iss.net/security_center/advice/Intrusions/> (last visited 6 January, 2003)

Network ICE and Internet Security Systems. "Back Orifice Ping." Database of Intrusions Detected by Network ICE.
<http://www.iss.net/security_center/advice/Intrusions/2001506/> (last visited 6 January, 2003)

Network ICE and Internet Security Systems. "Suspicious URL." Database of Intrusions Detected by Network ICE. <http://www.iss.net/security_center/advice/Intrusions/2002500/> (last visited 6 January, 2003)

Network ICE and Internet Security Systems. "TFTP/Intrusions." <http://www.iss.net/security_center/advice/Services/TFTP/Intrusions/default.htm> (last visited 6 January, 2003)

Northcutt, Stephen. KickStart Day 3 Intrusion Detection: The Big Picture. SANS GIAC, 2000-2001.

Walker, Robin. "Cable Modem Troubleshooting Tips." 1 September 2002. <http://homepage.ntlworld.com/robin.d.h.walker/cmtips/dhcp.html> (last visited 6 January, 2003).