Global Information Assurance Certification Paper

Are You Being Scanned?

Jack Stinson
November 13, 2000

Overview

This paper examines the data captured in the log file of the ZoneAlarm Personal Firewall on a PC connected to a cable modem over a 129 day period [13]. There is nothing special about this computer. It is a family computer and has no business sensitive information. The computer and cable modem were frequently turned-off during this period so the data is not for 24x7 coverage.

Introduction

The Internet was created in an open and trusting environment, designed to facilitate the free exchange of technical collaborative information. This open and trusting model no longer applies and it is necessary for PC users to re-examine the trust relationship that exists between a user's computer and the Internet [12]. In the past, a home user felt immune from Internet attacks because their connection was only temporary. This has changed with the growing use of cable modem and DSL circuits [1, 2, 9] [1]. The home computer must be protected against attacks and compromise just as office computers must be protected. The first step in protecting a computer is with the computer itself [3, 11, 12]. Only necessary features/services should be allowed. Common holes in protection include unintentional file shares, ftp servers, web servers, etc. The next step is to protect the computer from the network. This can be accomplished with "personal firewall" software products. Some of these products are ZoneAlarm, BlackICE Defender, Norton Personal Firewall, etc. Reviews of several products can be found in these references [4, 5, 14].

ZoneAlarm

Since ZoneAlarm is free to individuals, I installed it on my PC. The new release was installed when it became available and included a logging feature. The material for this analysis was obtained from the log file. To help analyze the data, the ZoneAlarm log file was imported into a spreadsheet. This allowed sorting on different headings to be performed so that patterns can be detected.

ZoneAlarm can be configured with different levels of security. It also allows the user to allow or deny any program access to the network. ZoneAlarm has had no noticeable impact on data transfer rates and is transparent to applications that are allowed network access. One of the nice features is that network traffic outbound from the PC is checked

[1] Dial-up systems can also be probed since a PPP connection provides a tunnel for TCP, UDP and ICMP traffic. The difference is that the PC's IP address is generally not fixed and the speed of the connection.

and can be allowed or denied. As a check of the capabilities of ZoneAlarm, Gibson's ShieldsUP! and Port Scan were run against the PC with ZoneAlarm in the "high" protection mode [3]. Each port tested was declared to be in "stealth mode" meaning no response was received from the PC. This means that from the network's perspective the ports were not open or closed they did not even exist. If all the ports are "stealth," then it cannot be determined by probing if the PC is on the network or not.

Scan Data and Analysis

During the 129 day period, ZoneAlarm blocked 1,942 probes. These are listed in Table 1. Of these probes, 1,246 were pings from numerous sites and 320 were NNTP probes from the service provider. The remaining 376 probes were against multiple ports and from multiple sites. The common service names or attack names were determined from references [6, 8].

Table 1: Summary of ZoneAlarm Log Files

Port	Transport	Service or Trojan Name	Number of Attacks
0	ICMP	Ping	1246
53	N/A	DNS	1
27015	N/A		13
27016	N/A		3
21	TCP	FTP	26
23	TCP	TELNET	10
25	TCP	SMTP	1
53	TCP	DNS - Zone	7
80	TCP	HTTP	2
88	TCP	Kerberos	61
98	TCP	TAC News	4
109	TCP	POP2	2
110	TCP	POP3	1
111	TCP	SunRPC	18
119	TCP	NNTP	320
143	TCP	IMAP	1
445	TCP	Microsoft - DS	2
1010	TCP	Doly Trojan v1.35	2
1028	TCP		1
1070	TCP		1
1107	TCP		1
1138	TCP		1
1151	TCP		2
1243	TCP	Subseven	14
1295	TCP		1
1307	TCP		1
1317	TCP		1

1568	TCP		1
1732	TCP	Proxim	1
1735	TCP	Privatchat	1
1738	TCP	GameGen1	1
1739	TCP	Webaccess	1
1791	TCP	EA1	1
2057	TCP		1
2384	TCP		1
2484	TCP		1
3128	TCP	Squid Proxy	1
3367	TCP		1
4899	TCP		1
6667	TCP	Schedule Agent	2
6688	TCP		8
6699	TCP		62
8080	TCP	Wingate sniffers/Proxy	1
9704	TCP		1
12345	TCP	NetBus 1.x Port	5
20136	TCP		1
27374	TCP	SubSeven 2.1	69
40466	TCP		1
47624	TCP		1
0	UDP		1
22	UDP	SSH	6
161	UDP		1
407	UDP		1
1025	UDP		1
1419	UDP		1
3283	UDP		1
6112	UDP	Dtspcd	12
6970	UDP		4
10085	UDP		1
31337	UDP	Back Oriffice	4
31789	UDP	Hack'a 'Tack	2
47624	UDP		1

Ports probed included common services[2] and Trojans[3] for both Unix and Windows systems. Hackers are looking to exploit Trojans and holes in the operating system or programs. In one instance when a hole was announced in the POP2 email program, I was probed twice on that port within in days of the announcement. One of the nice features of ZoneAlarm is that it can be setup to deny all access and only open ports for the

[2] FTP, TELNET, HTTP, SMTP, etc are called services. These ports provide access to/from the computer for these applications.

[3] A Trojan is a program that is hidden from normal operations and provides information or access that would not normally be granted.

applications that you approve. This feature provides more protection than just denying well-known Trojan ports. This is seen the large number of probes blocked on port 6699, but this port was not listed as being assigned or as being used by a Trojan. A good idea is to keep-up with recent information on attacks, vulnerabilities, viruses, Trojans and scanning activity by checking the SANS Global Incident Analysis Center and reading the National Infrastructure Protection Center (NIPC) CyberNotes newsletter [7, 10]. This way you can check unusual log file entries against new vulnerability exploits.

Summary

Protecting your PC is not a single action. It must be layers of protection so that if unintentional trust is granted to a system at one level, it can be blocked at another. If your PC is has file shares or is running servers, you are granting others trust to your system. Protecting your PC with a firewall is good, but don't rely only on the firewall.
Closing thoughts: Active protection is your responsibility, otherwise you are relying on luck. With this in mind remember that without protection: The attacker has to be lucky only once to compromise your system, but you have to be lucky all the time not to have your system compromised.

References

1. Ashland, Joanne. "DSL and Computer Security Issues." 07 September 2000. URL: http://www.sans.org/infosecFAQ/DSL.htm
2. Brandt, Andrew. "Unsafe at High Speed" PC World. 06 January 2000. URL: http://www.pcworld.com/hereshow/article.asp?aid=14624&pg=1
3. Gibson, Steve. Shields UP!. Gibson Research Corporation. URL: https://grc.com/x/ne.dll?bh0bkyd2
4. Johnson, Mark. "DSL (Defending Someone's Lair) in the 'Always-On' World of High-Speed Internet from Home." 11 October 2000. URL: http://www.sans.org/infosecFAQ/DSL_home.htm
5. Lake, Matt. "Instant Internet Security." PC World. 13 July 2000. URL: http://www.pcworld.com/hereshow/article.asp?aid=17587
6. Miller, Toby, et al, "Commonly Probed Ports." URL: http://www.sans.org/y2k/ports.htm
7. National Infrastructure Protection Center (NIPC). "CyberNotes." URL: http://www.nipc.gov/
8. Naval Surface Warfare Center. "Port Numbers." URL: http://www.nswc.navy.mil/ISSEC/Docs/portnum.txt
9. Pardo, Ed. "Cable Modems and Corporate Security." 21 March 2000. URL: http://www.sans.org/infosecFAQ/cable.htm
10. SANS Institute Global Incident Analysis Center. URL: http://www.sans.org/giac.htm
11. Sengstack, Jeff, "Make Your PC Hacker-Proof." PC World. September 2000. URL: http://www.pcworld.com/hereshow/article.asp?aid=17759&pg=1

12. Stinson, Jack, et al, "Trust Model: Defining and Applying Generic Trust Relationships in a Networked Computing Environment." May 2000. URL: http://ips.aticorp.org/DHIAP/
13. Zone Labs Inc. ZoneAlarm ™. URL: http://www.zonealarm.com/default.htm
14. Zych, Tina, "Personal Firewalls: What are they, how do they work.", 22 August 2000. URL: http://www.sans.org/infosecFAQ/personal_fw.htm