AVANTGARDE

TIME TO LIVE ON THE NETWORK

Executive Summary

This experiment tests to see how well commonly used computer platforms withstand Internet attacks in the wild. The experiment quantifies the amount of time it takes for a computer to be attacked and compromised when placed on a live network for the very first time and qualifies the type of attack method used to successfully compromise a computer over a two week period. Six different platforms were used in the experiment to simulate the possible computer environments used by the average home computer user – Windows Small Business Server 2003, Windows XP Service Pack 1, Windows XP Service Pack 1 with ZoneAlarm, Windows XP Service Pack 2, Macintosh OS X 10.3.5 and Linspire (Linux).

Results showed that all of the computers faced some form of Internet attack during the experiment, with a combined total of 305,955 attacks recorded; the largest number of those attacks targeted the regular Windows SP1 machine. The computers were successfully compromised a total of ten times over the fourteen-day experiment period with the very first compromise occurring on the regular Windows XP SP1 machine in less than 4 minutes immediately after placing the computer live on the Internet. Three specific attack methods successfully compromised certain computers in this experiment – weak password, DCOM (Distributed Component Object Model) and LSASS (Local Security Authority Subsystem Service) – with the majority (9) of the compromises falling on the regular Windows XP SP1 machine and one successful compromise on the Windows SBS 2003 machine. DCOM and LSASS are commonly used hacker exploits that can go un-noticed by the end-user until the computer has already been compromised.

Four out of the six computers used in this experiment were not successfully compromised by an Internet attack: Linspire (Linux), Macintosh OS X 10.3.5, Windows XP SP1 with ZoneAlarm, and Windows XP SP2. The Linspire (Linux), Windows XP SP1 with ZoneAlarm and Windows XP SP2 systems placed first, second and third respectively, when measuring systems with the fewest number of Internet attacks. These systems provided the best protection against attempts to compromise the computer during the two week period with each receiving less than 0.50% of the total 305,955 attacks.

Overview

Working together on the Time to Live on the Network (TTLN) project, Kevin Mitnick and Marcus V. Colombano investigated the ability of computers using different platforms to survive on a live network similar to real-life conditions. The project, through empirical evidence, attempted to answer the following questions:

- How long will it take each platform to become infected by a malicious virus or broken into by a hacker?

AVANTGARDE
Marketing & Design

665 Third Street
Nº 329
San Francisco
California
94107 · USA

T +1.415.281.9196
F +1.415.281.9197
avantgarde.com

- What happens to each machine as their systems become corrupted by these invasions? At what point does the system die or does it become a danger to the other members on the "net"?
- Which systems survive and why?
- Do third party applications add value to the operating systems?

Environment

The TTLN project tested the following stock environments on an open Internet connection using SBC Yahoo DSL:

- Windows SBS (Small Business Server) 2003
- Windows XP SP (Service Pack) 1
- Windows XP SP (Service Pack) 1 with ZoneAlarm
- Windows XP SP (Service Pack) 2
- Macintosh OS X 10.3.5
- Linspire (Linux)

Time Frame

Two weeks from September 9 to September 23, 2004

Overall Quantitative Results

Total # of Attacks:	305955

Total Attacks by Machine	**Attacks**	**% Total Attacks**
Windows SBS 2003	25222	8.24%
Windows XP SP1	139024	45.44%
Windows XP SP1 with ZoneAlarm 5.1 (Free)	848	0.28%
Windows XP SP2	1386	0.45%
Mac OS X 10.3.5	138647	45.32%
LinSpire (Linux)	795	0.26%

Total Compromises by Machine	**Compromises**	**Compromise Times**
SBS 2003	1	Less than 8 hours
XP SP1	9	Less than 4mins
XP SP1 with ZoneAlarm 5.1 Free	0	0

XP SP2	0	0
Mac OS X 10.3.5	0	0
LinSpire	0	0

Intruders

Based on our analysis of the incoming attacks, we determined they were likely automated based on the behavior of the attacking agent. More specifically, after each compromise in this exercise, the attacking agent attempted to download additional malicious code and attack other victims by replicating itself to other systems. This is typical behavior of a worm — to replicate itself to as many targets as possible. The attacks we've examined appear to be several variants of malicious code-like worms and auto-rooters which are automated programs that scan network address spaces looking for more victims to infect. The victims in this case are the "low hanging fruit"; namely, systems that are vulnerable because a firewall is not blocking incoming or controlling outgoing connections.

Time to Live

As we suspected, the time to live on the Internet is quite short, unless precautions are taken. The system running the regular Windows XP with Service Pack 1 was compromised in less than 4 minutes. This system was installed right out of the box with the default settings configured by Microsoft.

Methods of Attack

We identified three different attack methods used to compromise two separate systems on our honeynet.

- **Weak Password** – the default configuration (NetBIOS enabled) exposed both the XP SP 1 and the Windows SBS 2003 by exposing hidden shares such as C$, ADMIN$, etc. The attacking agent simply had to guess any account's password that had administrator rights. The administrator account was configured with a simple, easy-to-guess password—"password."
  - Both, the Windows SBS 2003 and the regular Windows XP Home Edition with SP1 systems were compromised using this method by correctly guessing a weak password.
- **DCOM** – There have been several vulnerabilities reported within the Distributed Component Object Model. Among the many vulnerabilities, the exploit code of one of them has been circulating in the wild for several months. The patch to fix this vulnerability was not released until after Service Pack 1 was deployed in this experiment.
  - This vulnerability was exploited 4 times to compromise the Windows XP SP1 system, which did not have a firewall between the computer system and the Internet.
- **LSASS** – A buffer overflow vulnerability in the Windows Operating system was published in April, 2004. The exploit code has been released on many web sites

throughout the world. The patch to this vulnerability was released after Service Pack 1.

- This vulnerability was exploited 5 times to compromise the Windows XP SP1 system, which did not have a firewall in between the computer system and the Internet.

The Three Best Performing Platforms

These three platforms performed the best in protecting against attempts to compromise the computer:

- Linspire (Linux) – This system was installed using the default settings out of the box. After conducting our own security test, we discovered that the only open port was 7741, which did not appear to connect to any service or application. Because this system responded to ICMP ping requests, there was a low number of attempts to compromise the system—795 attacks. This was the system which experienced the fewest attacks in the experiment. No attacks were successful because there were no exposed ports (services) to exploit.
- Windows XP SP1 with ZoneAlarm 5.1 – This system was essentially a clone of the regular Microsoft Windows XP SP1 system. The only difference was that a free personal firewall product available to the general public was installed on the system. By default, ZoneAlarm blocks all incoming ports so there are no exposed services that a hacker can exploit. ZoneAlarm also blocked ICMP pings that are used to determine if a system is up or "alive." As such, the system survived all attempts to compromise it. Because the system was blocking probes such as pings, the number of attempts was statistically closer to the Linspire machine. This system came in second place in preventing attacks while connected to the Internet.
- Windows XP SP2 – This system was also configured the same as the system running the regular Microsoft Windows XP SP1, except that it had Window's latest Service Pack 2. The Windows XP SP2 firewall is turned on by default, which effectively blocks all incoming traffic unless the user specifically configures it not to. As such, the system survived all attempts to compromise it. This system came in third place in preventing attacks while connected to the Internet.

Findings

- The majority of attackers were automated bots/worms
- The attacks were indiscriminate in the host they tried to attack i.e. it did not matter if the attacked machine was Windows XP, Linux, or Mac OS X. The attacks were mostly the same, attacks focused on Windows vulnerabilities.
- The attack scenario was the same for all attacks:

1. System was scanned for availability and open ports
2. The attacker(s) tried to exploit known vulnerabilities on each system for each open port
3. If an attacker's exploit was successful the attacker attempted to:
    - Download a copy of the malicious code on to the victim's machine

    - Perform a malicious act such as contacting its home base to set itself up for a denial of service attack or to store illicit information.
    - Spread the malicious code to other machines.
- The attacks on the non-Windows-based machines were unsuccessful due to the fact the attackers were trying Windows-based exploits. The fact that the Mac did not get compromised was due to the fact that its operating system was not a target for the attackers. It tied in first place as the machine experiencing the most attacks in this experiment, meaning that it would have been very vulnerable had code been written to compromise its system.
- The Windows XP machines equipped with either Service Pack 2 or protected by the ZoneAlarm third party firewall product were virtually invisible on the network and therefore received relatively few attempted attacks.
- The Windows XP SP1 machine equipped with the third party ZoneAlarm firewall product received the fewest number of attacks of all the Windows-based machines (848 attacks).
- The computers were successfully compromised a total of ten times over the fourteen day experiment period, with the very first compromise occurring on the Windows XP SP1 machine in less than 4 minutes after placing the computer live on the Internet.
- Three specific attack methods successfully compromised certain computers in this experiment – weak password, DCOM (Distributed Component Object Model) and LSASS (Local Security Authority Subsystem Service) – with the majority (9) of the compromises falling on the regular Windows XP SP1 machine and one successful compromise on the Windows SBS 2003 machine. DCOM and LSASS are commonly used hacker exploits that can go un-noticed by the end-user until the computer has already been compromised.
- Four out of the six computers used in this experiment were not successfully compromised by an attack: Linspire (Linux), Macintosh OS X 10.3.5, Windows XP SP1 with ZoneAlarm, and Windows XP SP2.
- The Linspire (Linux), Windows XP SP1 with ZoneAlarm and Windows XP SP2 systems placed first, second and third respectively, when measuring systems with the fewest number of Internet attacks. These systems provided the best protection against attempts to compromise the computer during the two week period with each receiving less than 0.50% of the total 305,955 attacks.

Conclusions and Recommendations

The results of this experiment reveal that Linux-based machines and Windows-based machines using an application firewall are the best at preventing attacks to a computer. Linspire (Linux), Windows XP1 with ZoneAlarm and Windows XP SP2 placed first, second and third respectively, when measuring systems with the fewest number of Internet attacks or attempts to compromise the computer.

The regular Windows XP SP1 does not include an integrated firewall application and was the most vulnerable to attacks and compromises while connected to the Internet. Although a vulnerability was related to choosing a weak password, the other successful

compromises resulted from exploiting known vulnerabilities existing within the exposed services.

The system running Windows XP SP1 equipped with the ZoneAlarm third-party firewall product provided the best protection against attacks during the two week period and was virtually invisible from hackers while running live on the network. As a result, it received the fewest number of attacks (848) compared to the regular Windows XP SP1 (139,024) and Windows XP SP2 (1,386) machines.

While the firewall applications in the Windows XP SP1 with ZoneAlarm and Windows XP SP2 machines both proved to be effective in preventing actual compromises in this experiment, we recommend further study based on a real-world scenario that includes user interactions such as Internet browsing, e-mail usage and the opening of e-mail attachments. With evolving viruses, worms, spyware and Trojans being ever more prevalent on the Internet and able to infiltrate systems through avenues such as Web surfing, e-mail, peer-to-peer programs and instant messaging programs, we believe inbound blocking alone does not provide enough protection. Today's state-of-the-art personal firewalls also contain outbound blocking capabilities which prevent spyware and Trojans from 'calling home' to either steal personal information or turn the compromised PC into a "bot." This is a clear case of 3rd party applications adding value to the operating system.

Conclusions

- No machine is immune from attack. Attackers are indiscriminate and if a security hole exists an attacker will find it. It is only a matter of time.
- Security breaches can happen in as little time as it takes you to turn on and log into your machine.
- OS patches are not enough. Each patch only fixes a known set of vulnerabilities.
- Every machine on the Internet should have adequate security to protect itself and the network from incoming and outgoing attacks. This includes the use of a firewall and virus protection to close security holes and shield vulnerable resources.
- As members of the Internet community, everyone is responsible to help protect the network. That means that a users' responsibility does not stop at protecting their own machines from attack but only starts there. Users are also responsible for keeping attacks from leaving their system and infecting others.
- Third party applications add value to the operating system and are an important part of the entire security community.