Know Your Enemy – Trend Analysis

Trend: Life expectancy increasing for unpatched or vulnerable Linux deployments.

Assessment Date: 17 December, 2004

EDITORS NOTE: *When this paper was first released, some readers confused this paper as a comparison between Windows and Linux. That is not the case. The purpose of this paper is to make you ask the question "Why is no one hacking Linux anymore?".*

EXECUTIVE SUMMARY

Increasing life expectancy

The past 12-24 months has seen a significant downward shift in successful random attacks against Linux-based systems. Recent data from our honeynet sensor grid reveals that the average life expectancy to compromise for an unpatched Linux system has increased from 72 hours to 3 months. This means that a unpatched Linux system with commonly used configurations (such as server builds of RedHat 9.0 or Suse 6.2) have an online mean life expectancy of 3 months before being successfully compromised.

Meanwhile, the time to live for unpatched Win32 systems appears to continues to decrease. Such observations have been reported by various organizations, including Symantec [1], Internet Storm Center[2] and even USAToday[3]. The few Win32 honeypots we have deployed support this. However, Win32 compromises appear to be based primarily on worm activity.

THE DATA

Background

Our data is based on 12 honeynets deployed in eight different countries (US, India, UK, Pakistan, Greece, Portugal, Brazil and Germany). Data was collected from the calendar year of 2004, with most of the data collected in the past six months. Each honeynet deployed a variety of different Linux systems accessible from anywhere on the Internet. In addition, several Win32 based honeypots were deployed, but these were limited in number and could not be used to identify widespread trends.

A total of 24 unpatched Unix honeypots were deployed, of which 19 were Linux, primarily Red Hat. These unpatched honeypots were primarily default server installations with additional services enabled (such as SSH, HTTPS, FTP, SMB, etc). In addition, on several systems insecure or easily guessed passwords were used. In most cases, host based firewalls had to be modified to allow inbound connections to these services.

These systems were targets of little perceived value, often on small home or business networks. They were not registered in DNS or any search engines, so the systems were found by primarily random or automated means. Most were default Red Hat installations. Specifically one was RH 7.2, five RH 7.3, one RH 8.0, eight RH 9.0, and two Fedora Core1 deployments. In addition, there were one Suse 7.2, one Suse 6.3 Linux distributions, two Solaris Sparc 8, two Solaris Sparc 9, and one Free-BSD 4.4 system.

Of these, only four Linux honeypots (three RH 7.3 and one RH 9.0) and three Solaris honeypots were compromised. Two of the Linux systems were compromised by brute password guessing and not a specific vulnerability. Keep in mind, our data sets are not based on targets of high value, or targets that are well known. Linux systems that are of high value (such as company webservers, CVS repositories or research networks) potentially have a shorter life expectancy.

THE FINDINGS

Life expectancy dramatically increasing

There has been extensive documentation and publications on the tremendous increase in criminal and attacking activity on the Internet.[4] What is surprising is that even though threats and activity are reported as increasing, we see the life expectancy of Linux increasing against random attacks.

By random attacks, we mean threats that don't care which systems they compromised, often scanning large network blocks to find and compromise systems. These tools can be fully autonomous (such as worms) or launched and managed by humans (such as autorooters or massrooters).

By combining the data from all of the Linux systems deployed, we see a mean life expectancy of 3.0 months for systems that were compromised. For systems still uncompromised, we see a mean of 4.46 months. Finally, for the entire population of machines, we see a mean time of survival, including those still uncompromised: 4.1 months. The longest surviving Linux honeypot was an unpatched Red Hat 7.3 system that was online (and never compromised) for over 9 months. This is a dramatic increase from the life expectancy for default Linux systems of 72 hours seen in 2001/2002.

This life expectancy is all the more surprising when compared to vulnerable Win32 systems. Data from the Symantec Deepsight Threat Management System indicates a vulnerable Win32 system has life expectancy not measured in months, but merely hours. The limited number of Win32 honeypots we have deployed support this, several being compromised in mere minutes. However, we did have two Win32 honeypots in Brazil online for several months before being compromised by worms.

In addition, we identified several other interesting trends. First, we have identified that the older the Linux distribution, the more likely it was to be compromised if left unpatched. Based on how default installations are becoming more secure, this is to be expected. Of the 5 RH 7.3 honeypots deployed for two months or longer, three were successfully compromised. Of the 8 RH 9.0 honeypots deployed for two months or longer, only one was compromised. Of the 2 Fedora Core 1 honeypots deployed for two months or longer, neither was compromised. The most common successful attacks were password guessing and exploits against HTTPS.

Also, once a system was compromised, it was more likely to be compromised again. For example, once compromised, a Red Hat Linux honeypot based in the UK was then repeatedly compromised 18 more times in a single month.

Another surprise was in relation to the Solaris based honeypots (all default installs of Solaris 8 or 9 on Sparc). Of the four Solaris honeypots deployed two months or more, three were compromised in less then three weeks. The fourth has been online for over six months without a compromise. There is not enough data here to attempt any conclusions. One note, default installations of Solaris8 and Solaris9 have more services enabled by default than most current Linux distributions and lack a simple, host based firewall.

Of the seven systems compromised in the past six months, six of them were used for IRC bouncing, bots, and/or phishing scams. The seventh compromise was terminated before motives could be established. On at least one of the systems attackers attempted to setup a forged bank for the purpose of harvesting bank information and credit cards.

REASONS

There are several possible explanations for this large increase in life expectancy in Linux systems. Any of the following (or combination thereof) could potentially explain the reason for this change. Keep in mind, we have not verified all of these possibilities.

1. Default installations of Linux distributions are becoming harder to compromise. New versions are more secure by default, with fewer services automatically enabled, privileged separation in services such as OpenSSH, host based firewalls filtering inbound connections, stack protection for common threats, and other security mechanisms. This was demonstrated by the fact that in most of our Linux honeypot deployments, modifications had to be made to the default configuration to enable services and/or allow inbound connections.

Also, older versions have been around longer, giving attackers more time to identify vulnerabilities and release attack tools. For example, searching SecurityFocus.com for advisories results in 584 advisories for Red Hat 7.3, 285 for Red Hat 9.0, and 127 for Fedora Core 1.

2. The primary threat is changing from machine-focused to human-focused. There is an growing trend towards social engineering, attacking the people using computers. In some cases, it is no longer the computer that is valuable, but the individual's information that resides on it. Also, its often becoming easier to attack the user as opposed to the system, as newer installations are more secure by default. As a result, considerably more effort is being expended in strategies such as phishing[5] to extract valuable information from targets, or malicious websites and mobile code that compromise client systems.

3. Based purely on economies of scale, attackers are targeting Win32 based systems and their users, as this demographic represents the largest percentage of install base.

4. Windows, through piracy and low-cost distributions in developing countries (such as China), has increased market penetration. As a result, it should be expected that a greater threat could exist to W32 than Linux.

APPENDIX

Additional references

[1] Symantec Internet Security Threat Report, January 1 – June 30, 2004

[2] Internet Storm Center - http://isc.sans.org/survivalhistory.php

[3] USAToday – "Unprotected PCs can be hijacked in minutes"
http://www.usatoday.com/money/industries/technology/2004-11-29-honeypot_x.htm

[4] CERT Incidents - http://www.cert.org/stats/cert_stats.html & http://www.cert.org/about/ecrime.html

[5] MessageLabs – "Phishing attacks skyrocket in 2004"
http://news.com.com/Phishing+attacks+skyrocket+in+2004/2100-7349_3-5479145.html?tag=nefd.top