Chapter 7

THREATS AND VULNERABILITIES

INTRODUCTION

Six years ago, the SANS Institute [1] and the National Infrastructure Protection Center (NIPC) at the FBI released a document summarizing the Ten Most Critical Internet Security Vulnerabilities, with regards to securing the Web client. Thousands of enterprises used that list, and the expanded Top-20 lists that followed one, two, and three years later, to prioritize their efforts so they could close the most dangerous holes first. The vulnerable services and the threats that they posed, led to worms like Blaster, Slammer, Code Red and many others, that have been on these lists [1].

This chapter presents an overview of these vulnerabilities and threats, and is a marked deviation from the previous Top-20 lists. In addition to Windows and UNIX categories, SANS and NIPC have also included cross-platform applications and networking products. The change reflects the dynamic nature of the evolving threat landscape and the vulnerabilities that attackers target. Unlike the previous Top-20 lists, this list is not cumulative in nature. SANS and NIPC have only listed critical vulnerabilities and threats from 2005 and 2006. If you have not patched your systems for a length of time, it is highly recommended that you first patch the vulnerabilities listed in the Top-20 2005 list [1].

SANS and NIPC have made a best effort to make this list meaningful for most enterprises. Hence, the Top-20 is a consensus list of vulnerabilities and threats that require immediate remediation. It is the result of a process that brought together dozens of leading security experts. They come from the most security-conscious government agencies in the UK, US, and Singapore; the leading security software vendors and consulting firms; the top university-based security programs; many other user enterprises; and the SANS Institute [1].

The SANS Top-20 is a living list. It includes step-by-step instructions and pointers to additional information useful for correcting the security flaws. SANS and NIPC will update the list and the instructions as more critical vulnerabilities and more current or convenient methods of protection are identified, and they welcome your input along the way. This is

a community consensus list – your experience in fighting attackers and in eliminating the vulnerabilities and threats, can help others who come after you [1].

TOP THREATS AND VULNERABILITIES IN WINDOWS SYSTEMS

The family of Windows Operating systems supports a wide variety of services, networking methods and technologies. Many of these components are implemented as Service Control Programs (SCP) under the control of Service Control Manager (SCM), which runs as Services.exe. Vulnerabilities in these services that implement these Operating System functionalities are one of the most common avenues for exploitation [1].

Windows Services

Remotely exploitable buffer overflow vulnerabilities continue to be the number one issue that affects Windows services. Several of the core system services provide remote interfaces to client components through Remote Procedure Calls (RPC). They are mostly exposed through named pipe endpoints accessible through the Common Internet File System (CIFS) protocol, well known TCP/UDP ports and in certain cases ephemeral TCP/UDP ports. Windows also contains several services which implement network interfaces based on a variety of other protocols, including several Internet standards such as SMTP, NNTP etc. Many of these services can be exploited via anonymous sessions (sessions with null username and password) to execute arbitrary code with SYSTEM privileges [1].

Description

Earlier versions of the operating system, especially Windows NT and Windows 2000, enabled many of these services by default for better out of the box experience. These non essential services increase the exploit surface significantly. The critical vulnerabilities were reported in the following Windows Services in 2005 and 2006:

- MSDTC and COM+ Service
- Print Spooler Service
- Plug and Play Service
- Server Message Block Service
- Exchange SMTP Service
- Message Queuing Service
- License Logging Service
- WINS Service
- NNTP Service
- NetDDE Service
- Task Scheduler [1]

Exploit code is available for most of these vulnerabilities and has been seen in the wild. Zotob worm and its variants exploited the buffer overflow in Plug and Play service [1].