The SANS Institute’s *Top Twenty Most Critical Internet Security Vulnerabilities*

Introduction

The SANS Institute maintains an online list of the *Top Twenty Most Critical Internet Security Vulnerabilities* to computer systems. The list categorizes these vulnerabilities: Windows, Unix, and General. The full text of *the SANS Top Twenty* list can be found at http://www.sans.org/top20.htm**.**

This document demonstrates StormWatch’s effectiveness in protecting against the vulnerabilities in this top twenty list.

Top Vulnerabilities In Windows Systems (W)

W1 - Unicode Vulnerability (Web Server Folder Traversal)

StormWatch prevents attackers from obtaining a command shell from a vulnerable web server. StormWatch also prevents the web server from accessing folders outside the web directory.

W2 - ISAPI Extension Buffer Overflows

StormWatch’s buffer overflow protection defends against ISAPI extension attacks as well as new, unknown attacks. This generic buffer overflow protection protects other services as well, such as Microsoft SQLServer.

W3 - IIS RDS exploit (Microsoft Remote Data Services)

StormWatch prevents this attack. StormWatch protection is in fact broader than this as it can protect against attackers accessing ***any*** sensitive COM components on the system.

W4 - NETBIOS - unprotected Windows networking shares

StormWatch can control access to local shares and other resources from remote applications, independent of operating system configuration.

W5 - Information leakage via null session connections

StormWatch can restrict access to NETBIOS services to specified network devices, preventing information gathering attacks from arbitrary sources. StormWatch can be configured to protect the HKLM/System/CurrentControlSet/Control/LSA/RestrictAnonymous registry key, which prevents null session connections to the system. It would be able to prevent a privileged user from disabling RestrictAnonymous functionality.

W6 - Weak hashing in SAM (LM hash)

StormWatch prevents any user from reading the SAM file where the weak hashes are stored. Furthermore, StormWatch can be configured to protect the key HKLM\System\CurrentControlSet\Control\LSA\ LMCompatibilityLevel, which controls whether LAN Manager Authentication will be accepted. It could prevent even a privileged user from enabling LM Authentication. StormWatch will also log failed attempts to the central console. These are centrally correlated to detect when password-guessing attacks are attempted in a distributed mode.

Top Vulnerabilities In Unix Systems (U)

U1 - Buffer Overflows in RPC Services
U2 - Sendmail Vulnerabilities
U3 - Bind Weaknesses
U5 - LPD (remote print protocol daemon)
U6 – sadmind and mountd

The above vulnerabilities (U1, U2, U3, U5 and U6) all have buffer overflows as their root cause and will be prevented in the StormWatch Solaris agent by similar mechanisms that are already provided in the StormWatch Windows agents

U4 - R Commands

StormWatch file access controls will protect the rhosts configuration files from being altered by rogue/malicious applications. In addition, StormWatch can control which network applications are allowed to act as servers on particular ports. StormWatch is able to block R Command execution and operation, even if a privileged user enables the services, and control the environment of the rcommand service to prevent it from accessing unauthorized portions of the system.

U7 - Default SNMP Strings

StormWatch has application control mechanisms to regulate SNMP access. It can prevent SNMP from running, or control which network devices are able to access the service.

StormWatch also controls snmpd so any application level vulnerabilities cannot affect the system.

Top Vulnerabilities That Affect All Systems (General)

G1 - Default installs of operating systems and applications

StormWatch provides mechanisms that allow the administrator to detect and enforce application and shared library versions. For example, StormWatch can detect which systems are vulnerable to exploits such as W2 and W3 and prevent loading of the vulnerable DLLs until they are upgraded. Moreover, StormWatch addresses another issue raised in G1 – default installations that install and automatically start vulnerable services that are not used by a majority of systems and for those that are enabled, controls their execution environment. StormWatch provides centrally managed control of what applications can run on a server irrespective of how it was installed.

G2 - Accounts with No Passwords or Weak Passwords

StormWatch does not do system auditing. However, StormWatch can control which applications and services are allowed to accept interactive logins across the network. In addition, StormWatch can control which network devices are allowed to connect to these services.

G3 - Non-existent or Incomplete Backups

StormWatch provides rules that protect the integrity of the system files, independent of user privilege levels. Modification to files can be tracked and either prevented or simply logged.

G4 - Large number of open ports

StormWatch has strong, configurable network control mechanisms that can regulate both incoming and outgoing connections on a per-application basis. Network access control can also be based on behavior of applications. StormWatch also detects attempts to discover open ports including distributed port scans.

G5 – Not filtering packets for correct incoming and outgoing addresses

StormWatch has strong, configurable network control mechanisms that can filter both incoming and outgoing connections. StormWatch includes functions such as detection of unauthorized packet sniffers, checks for malformed packets and DOS attacks, prevention of covert ICMP channels, and other network level validation. As always, the system administrator is notified of any abnormalities.

G6 - Non-existent or incomplete logging

StormWatch provides monitoring capabilities that log access to any file or registry entries, can distinguish between read and write attempts to the file, and can allow or prevent the action. This is in addition to any system logging that may or may not be enabled. System log entries can be sent to the central management console where they can be automatically correlated across multiple systems (global event correlation).

G7 - Vulnerable CGI Programs

StormWatch allows programs to operate securely within their bounds. Furthermore StormWatch's configurable rule system allows system administrators to write custom policies for any particular program they may run. These policies enforce the program's behavior and prevent vulnerable programs from being exploited maliciously. For example you can control access from CGI scripts to sensitive resources such as network file servers, customer databases etc.

Conclusion

StormWatch is an extensible and configurable security product that addresses all of the vulnerabilities cited in the SANS Institute's *Top Twenty Critical Internet Security Vulnerabilities* report. Its combination of file, registry, memory, and network protection defends against the most dangerous attacks today and will tomorrow as *different* applications become subject to critical vulnerabilities. Furthermore the security provided by StormWatch applies to desktops and servers.