GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Guarding Against Zero-day Threats

Michael Jensen
June 16, 2004

GIAC Security Essentials Certification (GSEC)
Practical Assignment: Version 1.4b, Option 1

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

While the number of discovered vulnerabilities has relatively stabilized over the past few years, the severity of those vulnerabilities has increased. More importantly, the time after a vulnerability announcement and the release of exploit code for that vulnerability has decreased over the years. Hackers are getting more creative and more efficient about identifying vulnerabilities and releasing exploits. In some cases, the exploits are released before the vendor is aware of the vulnerability. These types of threats are considered to be zero-day exploits and are quickly becoming the latest challenge to system administrators and security professionals.

The effects of zero-day exploits could create major consequences if steps are not taken to prevent the propagation of these threats. Defense in-depth is critical to mitigate the potential threats of zero-day exploits. It is imperative for IT organizations to adopt sound security policy and to have clear and concise procedures that adopt to the written policy in order to provide the fundamental foundation for protecting an organization from zero-day exploits. In addition to traditional layers of security, user awareness and implementation of security best practices will further lessen the effects of zero-day exploits. The IT community, including vendors, must be proactive and vigilant to effectively guard against zero-day exploits.

The Evolution of Vulnerabilities and Exploits

The relationship between vulnerabilities and exploits has evolved over many years and continues to be dynamic. In the past, IT security professionals, researchers and developers would publicly announce they found a vulnerability primarily to motivate the vendor to release a patch. This approach of vulnerability disclosure provided a window of opportunity for attackers to develop and circulate exploit code for the vulnerability announced. However, it would typically take months for an exploit created for that vulnerability to be publicly available and the vendor would often win the race to get the patch released before an exploit was disseminated. Additionally, the underlying nature of the file and macro virus exploits in the 1990s, which was primarily passive and slowly propagating, allowed ample time for security professionals and systems administrators to appropriately test and deploy the patch to vulnerable systems. With few exceptions, these conditions and ability to implement effective patch management procedures helped minimize the impact of exploits and kept compromised machines relatively isolated to their niche on the network.

The environment of modern information security is much more complex than just a few years ago. Attackers are becoming more efficient, creative and faster at creating exploits. By using reverse engineering techniques and tools available on the Internet, attackers are able to efficiently identify a vulnerability by simply analyzing the files in the patch released from the vendor. The average time to identify a vulnerability using reverse engineering techniques is only nine days from the time the patch is released. [1] Once the vulnerable files have been identified, an attacker can focus on generating and disseminating an exploit that attacks that vulnerability. These creative and

[1] Lang, “Microsoft Addresses Security.”

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

sophisticated techniques have contributed to significantly reducing the delay between vulnerability discovery and exploitation as depicted in Figure 1. [2,3] In 2001, Nimda surfaced 331 days after the patch for the vulnerability was released. This should have been ample time to test and deploy the appropriate patch to prevent infection. However, a one day reaction window for the Witty worm (Mar 2004) presents a tremendous challenge to implement an effective patch management program.

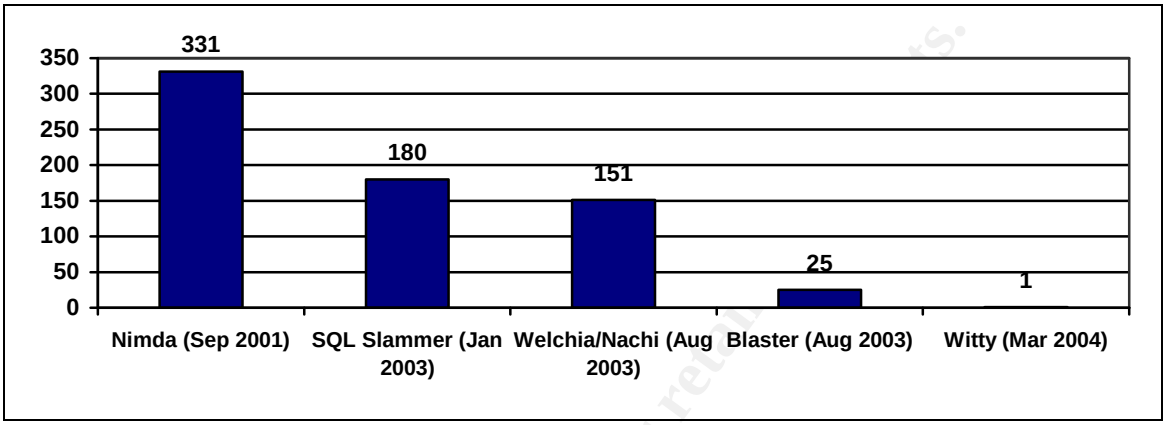


Figure 1: Days Between Patch Release and Exploitation

In some instances, an attacker may be the first to discover a security vulnerability. Rather than notifying the vendor of the vulnerability, the attacker will generate and release an exploit that attacks that vulnerability before the public, security community or vendor is aware of the vulnerability. These types of exploits are considered zero-day exploits and attack unknown and unpatched vulnerabilities. There have only been a few known zero-day exploits to date, but the threat of these exploits is increasing each day. Exploits that attack a known vulnerability for which there is not a patch or fix are considered zero-day vulnerabilities and are more common. Together, zero-day exploits and zero-day vulnerabilities constitute zero-day security threats. These types of threats, especially zero-day exploits, require security professionals to redefine their current security strategies.

In addition to generating exploits quicker and trying to achieve a zero-day exploit, attackers are designing exploits to maximize the number of systems compromised while increasing the rate of infection. In contrast to the earlier file and macro viruses, current exploits can be disseminated through active, self-propagating mass-mailing worms that could contain Trojan horses or hybrid threats and only take a few days or a few hours to spread. [4] The damage associated with the combination of developing exploits quickly and accelerating their propagation is significant. Figure 2 highlights some of the more interesting information about some of the recent worms and the financial damage that has resulted. [5,6,7]

[2] W2Knews, "The Patch Gap."
[3] Shannon, "The Spread of the Witty Worm."
[4] Joshi, "How to protect your company from 'zero-day' exploits."
[5] SANS, "Webcast: Security Strategies for Day-Zero Defense."

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Agent	Key Information	Financial Damage
Morris Worm (1988)	6,000 hosts or 10% of machines on the Internet	$98 million
Slammer (2003)	90% of all vulnerable systems hit within 10 minutes	$1.15 billion
MSBlaster (2003)	900,000 to 1,000,000 hosts infected	$525 million
SoBig.F (2003)	Peaked within 24hrs (1/17 emails infected)	$5.6 billion
Warhol Concept	Compromise 1,000,000 hosts in 15 minutes (in theory)	Est. >$100 billion
Flash Concept	All vulnerable hosts infected in tens of seconds (in theory)	Est. >$100 billion

Figure 2: Rate of Infection and Financial Damage Comparison

As illustrated, the Warhol and Flash concept worms could theoretically infect all vulnerable systems on the Internet in only a few minutes or less. Imagine a zero-day exploit that propagates with the Warhol or Flash rate of infection. The financial consequences globally would be staggering. Without proper security measures, it will only be a matter of time before that becomes a reality.

Understanding the most recent trends regarding vulnerability and malicious code is essential to identify and implement the most appropriate security solution for zero-day threats. In recent years the number of vulnerabilities being identified each year has only slightly increased. According to the latest Symantec Internet Security Threat Report, 2,636 vulnerabilities were documented in 2003, which is only an increase of less than two percent from the total number of vulnerabilities documented in 2002. The report also states the following more alarming findings: [8]

- The percentage of vulnerabilities for which exploit code was publicly available increased by 5% in 2003.
- The percentage of vulnerabilities that do not require specialized tools to exploit them increased by 6% in 2003.
- 70% of the vulnerabilities documented in 2003 were classified as easy to exploit.
- 594 new high-severity vulnerabilities were announced in the last half of 2003.
- 54% of the top ten submissions were blended threats.

These findings not only illustrate the evolution of the information security environment from a decade ago, but are indicators of the serious challenges security professionals encounter on a daily basis. An attacker can more easily and quickly compromise systems while not requiring a lot of knowledge about the exploit or vulnerability being used. The increase in publicly available exploit code, the ease of exploitation and the increase of high-severity vulnerabilities is a frightening combination. Add the reported

[6] Boettger, "The Morris Worm: How it Affected Computer Security and Lessons Learned by It."
[7] Staniford, "How to 0wn the Internet in Your Spare Time."
[8] Symantec, p.4.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

fact that more than half of the top ten submissions were blended threats, and there exists a potentially efficient, effective and dangerous delivery mechanism for zero-day threats.

Propagation of Zero-Day Threats

The earliest known zero-day exploit was discovered in March 2003 when the military realized one of their web servers had been compromised. The exploit involved an unchecked buffer overflow in the Windows 2000 dynamic link library, Ntdll.dll, used by the Web Distributed Authoring and Versioning (WebDAV) component of Microsoft IIS 5.0. A detailed description of the WebDAV protocol can be read in RFC 2518 (ftp://ftp.rfc-editor.org/in-notes/rfc2518.txt). The vulnerability could be exploited by simply sending a specially formed HTTP request to a system running IIS 5.0. This would either cause the system to fail, resulting in denial of service, or allow a remote attacker to execute arbitrary code in the LocalSystem security context. [9] This would give the attacker extensive privileges to local resources on the compromised system.

In October 2003, a zero-day exploit known as the Qhosts Trojan surfaced. The exploit attacked the Internet Explorer Object Data Remote Execution vulnerability (http://www.kb.cert.org/vuls/id/865940). The Trojan horse would automatically be downloaded and executed on an unsuspecting victim's system only when specific code embedded in a banner ad was accessed with Internet Explorer. The malware then would alter the Windows Registry and reconfigure the TCP/IP settings to use different DNS servers. This caused the network traffic from the compromised system to be redirected to other servers, effectively hijacking the browser's session. [10] With this passively propagating exploit, the attacker could execute arbitrary code in the security context of the current user.

The most recent zero-day exploit was discovered in June 2004. Techworld reported that a Dutch researcher discovered a sophisticated zero-day exploit that targets two newly discovered and unpatched Internet Explorer vulnerabilities: Local Resource Access and Cross-Zone Scripting. In conjunction with the old, unpatched Adodb.stream exploit from Aug 2003 (http://seclists.org/lists/fulldisclosure/2003/Aug/1703.html), this zero-day exploit is able to bypass Internet Explorer's security using malicious JavaScript code encrypted with the Windows Script Encoder. The following events would occur if a user clicks on a malicious link: [11]

> …the link uses an unknown vulnerability to open up a local Explorer help file -- ms-its:C:\WINDOWS\Help\iexplore.chm::/iegetsrt.htm. It delays executing anything immediately but instead uses another unknown vulnerability to run another file which in turn runs some script. This script is then used to run more script. And finally that script is used to run an exploit that Microsoft Corp. has been aware of since August 2003 but hasn't patched.

[9] CERT, "CERT Advisory CA-2003-09 Buffer Overflow in Core Microsoft Windows DLL."
[10] CERT, "CERT Incident Note IN-2003-04."
[11] McCarthy, "Internet Explorer carved up by zero-day hole."

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Essentially, the attacker could "leap frog" from vulnerability to vulnerability until an exploit could be used against an older, unpatched vulnerability. The complexity of this attack exemplifies the difficulties in guarding against zero-day exploits.

With the exception of the WebDAV exploit, the above examples of recent zero-day exploits propagated through web pages containing malicious code that were accessed by vulnerable Internet Explorer browsers. With browser-based attacks, the attacker relies on social engineering techniques to trick users in accessing the malicious web page. This is typically accomplished by sending a disguised URL to the victim in an email message. In some cases, it is possible that the URL or HTML code sent via email could automatically execute and download malware to a user's system by simply opening the message. This would occur without the user being aware. Most modern security measures, including perimeter firewalls, permit inbound and outbound network traffic on port 80. As a result, browser-based attacks are difficult to detect and block. Although these types of application layer attacks are increasing, other avenues for zero-day threat propagation exist.

The most dangerous and likely vector of propagation for zero-day threats is a blended threat. As described by Symantec, "blended threats combine the characteristics of viruses, worms, Trojan Horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack." Symantec further describes some of the more important characteristics of blended threats as: [12]

- Causes harm: Launches a Denial of Service (DoS) attack at a target IP address, defaces Web servers, or plants Trojan Horse programs for later execution.
- Propagates by multiple methods: Scans for vulnerabilities to compromise a system, such as embedding code in HTML files on a server, infecting visitors to a compromised Web site, or sending unauthorized email from compromised servers with a worm attachment.
- Attacks from multiple points: Injects malicious code into the .exe files on a system, raises the privilege level of the guest account, creates world read and writeable network shares, makes numerous registry changes, and adds script code into HTML files.
- Spreads without human intervention: Continuously scans the Internet for vulnerable servers to attack.
- Exploits vulnerabilities: Takes advantage of known vulnerabilities, such as buffer overflows, HTTP input validation vulnerabilities, and known default passwords to gain unauthorized administrative access.

Some of the more familiar blended threats include Blaster, Welchia, Sobig.F, Dumaru and BugBear. In April 2004, security firms discovered the "E" variant of Bugbear, which exploits an unpatched vulnerability in Internet Explorer. Viewing an attached MIME HTML file will download the Trojan to the victim's system. According to a TechWeb News article, "this zero-day exploit attempted to disable a wide range of in-memory programs, particularly personal firewall and antivirus software, including the BlackICE

[12] Symantec, "Definition of Blended Threat."

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

and ZoneAlarm firewalls, and F-Secure's and Symantec's anti-virus defenses." [13] It also installs a keylogger on the compromised system and sends the captured information to the attacker.

Continuously scanning for vulnerable servers allows a blended threat to propagate more efficiently. An attacker typically will leave a backdoor open on a compromised system. Once a blended threat scans and discovers an existing backdoor, it will try to compromise that system. This allows the attacker to install additional malicious code. Additionally, this creates another potential avenue for newer blended threats to use to propagate and infect the systems later.

Additional pathways that may contribute to the spread of zero-day threats include peer-to-peer (P2P) file sharing and instant messaging (IM). Unlike browser-based attacks, these avenues are easy to block at the network perimeter. If the appropriate ports are not closed at the perimeter, both of these create an avenue for blended threats to infect an organization's internal network. Mobile users that access the network remotely or bring laptops to connect to the network can also infect the network. Virtual private networks (VPN) provide a direct channel from remote systems to the internal network. If laptops and users' home systems are not properly secured, they can propagate zero-day threats directly to an organization's internal network.

Detecting a Zero-Day Compromise

The procedures used for detecting a zero-day compromise are not much different than those used to detect a typical compromise. One additional challenge of detecting a zero-day exploit is the fact that detailed information about the vulnerability exploited in a zero-day attack is not known until after the zero-day exploit has been discovered and analyzed. This requires security professionals and system administrators to possess current knowledge of the latest attack trends and the ability to apply this knowledge in an insightful manner. Through experience, security professionals and system administrators can recognize patterns that will lead to zero-day discoveries. The following events could be indicators that a zero-day threat exists on the network:

- Behavior-based systems (IDS and IPS) alerts
- Antivirus software alerts as a result of heuristic scanning
- Unusual events in the system log files (i.e. failed logons)
    - A central log server is highly recommended
- Poor system performance
- Unexplained system reboots
- Network traffic on unexpected ports, especially on ports known to be backdoor ports for known blended threats (i.e. MyDoom: TCP ports 3127 through 3198)
- Increased network traffic on a legitimate port
- Increased scanning activity
- Unusual SMTP traffic, especially originating from systems that should not be using SMTP

[13] TechWeb, "New Bugbear Worm Exploits Unpatched IE Vulnerability."

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Observing any of these events would require further investigation using the proper intrusion detection policies and procedures instituted by the organization.

Maintaining documentation of the baseline security configuration is essential to discover the signs of being compromised. File system integrity checkers, such as Tripwire, need to be part of the security strategy and will help detect any change made to a file on the system by an attacker.

Another technology that can be used to help identify and detect zero-day attacks is the honeypot. Honeypots can be an effective tool that can be used to assist in the detection of zero-day exploits. In addition to the ability to detect zero-day attacks, honeypots also can be used to identify the mechanism of the attack. After proper analysis, the zero-day attack can be reported to the vendor so appropriate mitigating solutions can be developed and deployed.

Limitations of the Typical Security Model

A typical security model will consist of a layered combination of perimeter firewalls, behavior-based systems and antivirus software. Each of these components, when used independently, is not sufficient to protect an enterprise from typical attacks. Furthermore, with the most recent browser-based attacks and circulating worms, it has become apparent that using only a combination of perimeter firewalls, behavior-based systems and antivirus solutions is inadequate to protect against zero-day threats. It is important to understand the limitations of each of the three main components that constitute the typical security model in order to implement the most appropriate mitigation strategy for zero-day threats.

Firewall Limitations

One of the most fundamental building blocks to an effective security strategy is a firewall. Firewalls operate at the networks perimeter and do not protect inside the local area network. Through policy, firewalls are configured to determine the nature of the traffic that's permitted to cross the network boundary. As seen with the recent browser-based zero-day exploit attacks, allowing inbound and outbound network traffic on port 80 (HTTP) also allows the malicious traffic in and out of the internal network. Attacks are taking advantage of this ubiquitous avenue and designing exploits that target the application layer rather than the network layer. Blended threats also pass through protocols that are typically allowed to pass through firewalls, making firewalls ineffective for these types of attacks.

Behavior-based Systems Limitations

Behavior-based systems include network-based intrusion detection systems (NIDS), host-based instruction detection systems (HIDS) and intrusion prevention systems (IPS). These systems are often used to augment firewalls and monitor network traffic for known attack patterns, monitor traffic that could indicate a compromise on the local machine, or provide deep packet inspection to prevent security threats from compromising the network. Attack patterns do not exist for zero-day exploits, making it

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

nearly impossible for IDS systems to detect one. As the name implies, intrusion detection systems do not provide protection, but merely notification that a potential security threat has bypassed the perimeter firewall. IDS and IPS also can generate a numerous amounts of false positive alerts that can lead to overlooking authentic warnings. To be effective and eliminate false positive alerts, IDS and IPS systems require considerable management and maintenance.

Antivirus Software Limitations

Antivirus software is a necessity for all machines but the effectiveness is dependent on the timely release of virus signature files. Virus signatures lag behind virus attacks, sometimes by several days because a virus must first be analyzed before a signature for it can be created, released and deployed. During this window of exposure, organizations are exposed to an attack and the resulting damages a zero-day threat may deliver. Making this problem even more challenging is the fact that blended threats are being designed to propagate faster and infect a larger number of systems.

Mitigating Zero-Day Threats

Effective protection from zero-day threats requires a comprehensive security solution that contains multiple layers of defense and response mechanisms. Despite the limiting factors to guard against zero-day threats, firewalls, behavior-based systems and antivirus solutions should still be the core technologies used in a modern security strategy. However, the unique nature of zero-day threats requires the overall solution to include additional layers of defense that complements the traditional layers of the typical security model. An organization can provide the foundation to guard against and minimize the impact of zero-day exploits by using sound security policy, border protection, system hardening, antivirus software, vulnerability management, application hardening, security best practices and end-user training.

Security policy is the most vital component of a multi-layer security approach and is the foundation for which all security measures should be implemented against. Without a sound security policy it is difficult to ensure the confidentiality, integrity and availability of data. A well designed and written security policy provides security professionals the guidelines to implement an effective protection plan. An organization's security policy should reflect the business needs as determined by a risk assessment and should clearly provide the layout for each component of the overall security strategy. Once the security policy has been created, an organization can proceed to implement the most appropriate measures to guard against zero-day threats.

Border protection

Border protection can be achieved from properly configured border routers, firewalls and behavior-based systems. Implemented firewall policies should enforce the business and application needs of the organization. A properly configured and secure network takes into consideration the physical layout of the network design. Network segmentation physically separates the network into zones. Putting firewalls on either side of a demilitarized zone (DMZ) helps to control the flow of traffic and protects the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

trusted internal resources from external attacks. This not only helps protect the trusted IT resources on the internal network, but would help prevent the spread of zero-day threats if the internal network was infected. Intrusion detection and prevention systems can by deployed inline to offer real-time protection. Constantly monitoring border traffic and examining the TCP/IP layers for patterns of abnormal activity is also necessary.

Wireless networks and virtual private networks have softened the security perimeter and can put protected networks at risk. If the remote system is not a secure end-point, it could potentially infect the internal network. Laptops and unmanaged systems present another challenge to maintain effective border protection. A user could infect the internal network if they connect an infected laptop or unmanaged system to the network. For instance, organizations that blocked UDP port 1434 at the perimeter were still affected by employees connecting laptops infected with the SQL Slammer worm to the internal network. This reinforces the need to prevent laptops and unmanaged systems from connecting to the internal network until it is confirmed the appropriate security patches have been installed and the latest antivirus signatures have been applied.

System Hardening

Misconfigured systems are commonly found on networks. In some cases, systems may still have the factory defaults set, such as default passwords and other insecure configurations. System administrators may not be aware of these insecure systems until they are compromised by an attacker. To minimize this from occurring, a system should be hardened before it is connected to the network. This involves applying the latest security patches to the operating system and applications installed, disabling and removing unneeded and insecure services, and implementing the appropriate user and file permissions.

All operating system patches and service packs should be applied before connecting a system to the network. Organizations should have a lab environment that allows for setting up and testing new machines. In this environment, machines can download the appropriate patches from a centralized patch server in private IP space and install them on the system without having to be connected to the Internet. Outside of this environment, the latest patches can be downloaded to an existing system on the Internet then burned onto a CD for distribution and installation on the systems in need of the patches. A patch management program should be used to maintain a secure patch level once the system has been connected to the network.

Most default installations for a variety of operating systems have many insecure and unneeded services enabled by default, such as telnet, FTP services and Web services. A system administrator or security professional should disable all services, especially server class services, before connecting a system to the network. The services needed for the organization to accomplish their business goals can then be activated and secured as the need arises. Leaving unneeded and insecure services enabled is not recommended because they tend to be forgotten. Consequently, the appropriate security patches for those services do not get installed, leaving the system vulnerable to attack. Disabling unnecessary services also reduces the number of patches that will need to be maintained on the system.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Most operating systems are shipped with the convenience of the user in mind rather than security. File and users permissions are typically escalated higher than necessary on most default installations. When setting up file and users permissions, it is always best to implement the least privilege model. If by chance an attacker happens to gain access to a system, the privileges available will be restrictive. As seen from the zero-day exploits mentioned earlier, the malicious code downloaded to the compromised machines was able to run in the security context of the user. If the user has minimal privileges, the impact would be minimized.

Additional hardening of systems can be accomplished through desktop lockdown tools. With Microsoft Windows, local security policies can be used to restrict the end-user's ability to change system settings that could result in a security misconfiguration. If the system is a member of a Microsoft Active Directory domain, group policies can be used to enforce access control, users rights and file system permissions as well as enforce strong password policies. Group policies empower system administrators to efficiently fine tune operating system settings and centrally manage systems in a secure fashion.

Antivirus Software

Having antivirus software installed on a machine is a vital component of the security strategy. It is important to force scheduled scans on a regular basis and update the virus definition files frequently. It is recommended that organizations use a centralized antivirus server to deploy virus signatures to workstations. Having workstations connect to a centralized server to download the latest antivirus definitions when connecting to the network will assist in preventing the spread zero-day threats. Heuristic virus scanning can further increase the chances of detecting zero-day threats.

Antivirus software should also be installed on email servers. If feasible, it is recommended that the antivirus software on the server is from a different vendor than that of the antivirus software installed on each desktop. This provides an additional layer of protection. Virus and worm variants are surfacing rapidly and the various antivirus corporations usually vary in the timely release of virus signatures for these variants. This layered approach provides fault tolerance against the potential problem of not being able to acquire the latest virus signatures from one of the vendors; virus signatures will still be available from the other vendor.

Patch Management

The first patches and service packs should be applied to new systems in the system hardening stage of the security model. Unless the system is demonstrating signs of compromise, it is impractical to remove a system from the network in order to apply the latest patches. An effective patch management program should be used to maintain a secure patch baseline on every system.

The rapid speed at which attackers are creating and disseminating exploits, the rapid pace of propagation and the increase frequency of major attacks pose a formidable challenge for an organization to deploy an effective and efficient patch management

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

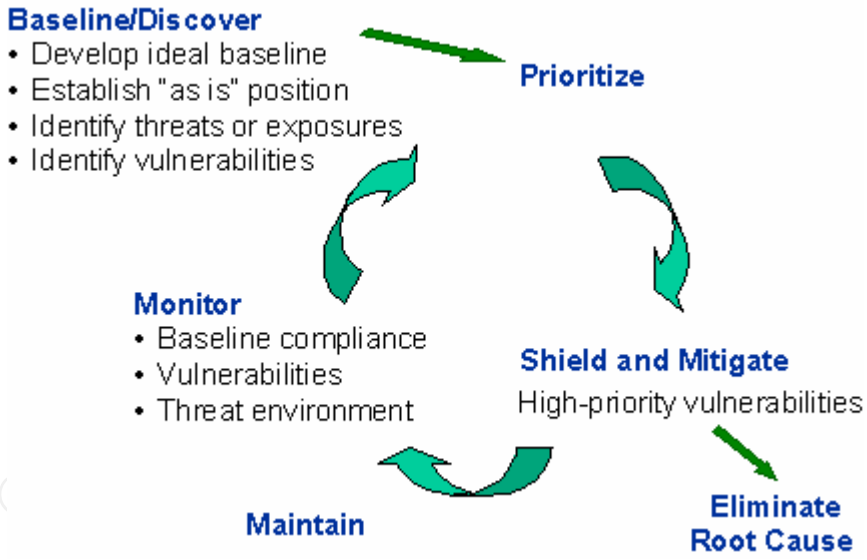
program. For instance, the time required to identify the means by which a zero-day exploit is propagating and the time for a vendor to create and release a patch for it may take longer than the time for the exploit to compromise all the vulnerable systems; remember the theorized rate of infection of the Warhol and Flash concept worms.

The heterogeneity of most networks, regardless of size, makes it nearly impossible to appropriately test a patch and deploy it before a zero-day threat is circulating. A patch management program needs to expedite the testing and deployment of patches without compromising the integrity of the system. Maintaining the latest security patch levels will assist in preventing the spread of zero-day threats. Centralized patch management and deployment is the most efficient and effective way to achieve this and should be used as a foundation for a patch management program. After a system is fully patched, it is important to perform regular vulnerability scans to ensure the new system configuration has not created a potential hole for an attacker to exploit.

Vulnerability Management

A proactive approach to protect against zero-day threats involves vulnerability management. The Gartner group defines vulnerability management as "a set of processes and technologies that are used to establish and maintain a security configuration baseline, discover, prioritize and mitigate vulnerabilities, establish security controls and eliminate root causes." [14]

Figure 3: Vulnerability Management Model



Source: Gartner Research (August 2003)

[14] Nicolett, "Vulnerability Management Defined."

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Gartner Research predicts, “Enterprises that implement a vulnerability management process will experience 90 percent fewer successful attacks than those that make an equal investment only in intrusion detection systems.” [15]

Configuration changes occur anytime you install patches, install new software or make changes to the system settings. A single change or a combination of change could introduce a new vulnerability. It is important to continually scan the local network for vulnerabilities after such activities. The goal is to find any potential vulnerability before an attacker does. If a vulnerability is found, it should be treated as a compromised machine. Frequent scanning and analyzing of port openings on a system and comparing the results to a known baseline will help indicate a new vulnerability. There are many port scanners available that will help accomplish this, but nmap and nessus are the more useful ones. In addition, file system integrity checking software should also be used to help identify changes.

Application Hardening

Attackers are creating zero-day exploits that attack the application layer, especially web applications. By targeting web applications, attackers are able to effectively bypass perimeter firewalls using port 80. Part of the application development process should involve vulnerability testing. Incorporating vulnerability testing into the development process will ensure that the first release of the application is secure.

Blocking Attachments

Relying on social engineering tactics, attackers take advantage of naïve end-users by using email messages to deliver malicious code and web links. Blocking email attachments to emails that may be harmful (.bat, .exe, .pif, .scr, .vbs) is a simple precaution for system administrators to implement. Regardless if the email server is blocking attachments, end-users need to be trained to scan attachments for viruses before opening them.

Honepots

Honeypots can be an important component of the security strategy. While honeypots act as intrusion detection systems, they also provide the ability to detect attacks that evade traditional detection systems, such as zero-day attacks. The more properly managed honeypots that are installed, the more chance zero-day attacks will be discovered before major consequences occur.

Even with the above measures, an organization’s IT infrastructure may still get infected with a zero-day exploit. Therefore, it is important for an organization to have incident handling procedures. Infected systems need to be removed from the network as quickly as possible to prevent the exploit from spreading. A thorough forensic analysis should be performed on the system in a manner that does not compromise the evidence. This is best left to IT staff who are trained to be incident handlers.

[15] Nicolett, “Predictions for IT Security Directors in 2004.”

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Education, Training and Communication

Implementing a multi-layer security strategy requires extensive knowledge to implement each component correctly. It is important to constantly be aware of the newly discovered vulnerabilities and attack methods that surface daily. This can be accomplished by reviewing information posted by incident advisory organizations. The following links provide a good starting point for staying current with the constantly evolving security environment:

- **BugTraq:** http://www.ntbugtraq.com/
- **Center for Internet Security:** http://www.cisecurity.org/
- **CERT:** http://www.cert.org/
- **Internet Storm Center:** http://isc.incidents.org/
- **Microsoft:** http://www.microsoft.com/technet/
- **SANS:** http://www.sans.com/
- **SearchSecurity.com** http://searchsecurity.techtarget.com/
- **SecurityFocus:** http://www.securityfocus.com/
- **Symantec:** http://www.symantec.com/avcenter/

Subscribing to security mailing lists is another good way to stay current with the latest security information.

Even after the internal network is effectively protected from external threats, it may not be protected from the end-user. Information security awareness needs to be extended to the end-user. Users need to be aware of and understand the potential risks associated with opening email attachments, connecting laptops and unmanaged systems to the internal network, and the potential consequences of having weak passwords. Training is essential to ensure the end-user demonstrates desktop security best practices everyday. This would include training the end-user to download an email attachment, scan it for viruses then open it from within the appropriate application. It would also include training them to use password protected screen savers when leaving the system for a specific length of time.

It is important for system administrators to communicate the latest threats to the end-user. Letting the end-user know about a new worm that is circulating by email with a specific attachment can mitigate the threat and prevent infection of the network. Without this warning, the end-user would be likely to open the attachment and infect the system and potentially, the network. Effective communication and information dissemination between the different groups responsible for maintaining the layers of the security strategy is also important. Having these communication channels will increase the effectiveness of the protection needed to mitigate the impact of zero-threats.

Conclusion

The information security environment is constantly evolving. Security threats are getting easier to exploit and attackers are using more sophisticated techniques to compromise

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

systems. Recent trends in vulnerabilities and malicious code indicate the chances of a serious zero-day attack are increasing. The impact a zero-day attack will have on an organization will be devastating and surpass the damage done by recent worms.

While it may currently be difficult to completely guard against zero-day exploits, organizations need to take a more comprehensive approach to security to reduce the effects of zero-day exploits. The typical reactive security model is not sufficient to guard against zero-day attacks. Attackers are designing exploits to circumvent the traditional IT security model as well as taking advantage of the delays in patch deployments. Organizations need to redefine the current security practices to include proactive measures. Implementing a multi-layer security model that incorporates reactive and, more importantly, proactive measures provides a solid foundation for an immediate solution. Each layer is dependent on the next for proper protection; therefore, the security model is only as strong as the weakest component. A comprehensive approach requires coordination with many different IT groups. It is important for each group to have the proper training and knowledge to effectively implement their component of the overall security model.

Zero-day threats are only in the beginning stages. If the history of vulnerabilities and exploits is any indicator, zero-day threats will progressively get worse and present the biggest challenge to guard against. New technologies that actively protect against zero-day threats need to be developed by vendors. Now is the time to develop technologies that can effectively protect an organization from the potentially devastating effects of a zero-day threat.

© SANS Institute 2004, Author retains full rights.

List of References

Boettger, Larry. “The Morris Worm: How it Affected Computer Security and Lessons Learned by It.” 24 December 2000.
URL: http://www.wbglinks.net/pages/reads/misc/morrisworm.html.

CERT. “CERT Advisory CA-2003-09 Buffer Overflow in Core Microsoft Windows DLL.” 25 April 2003. URL: http://www.cert.org/advisories/CA-2003-09.html.

CERT. “CERT Incident Note IN-2003-04.” 4 October 2003.
URL: http://www.cert.org/incident_notes/IN-2003-04.html.

Nicolett. M. “Vulnerability Management Defined.” Gartner. 3 September 2003.

Nicolett. M. “Predictions for IT Security Directors in 2004.” Gartner. 8 December 2003.

Joshi, Abhay. “How to protect your company from ‘zero-day’ exploits.” 01 March 2004.
URL: http://www.computerworld.com/securitytopics/security/virus/story/0,10801,90447,00.html.

Lang, Steven. “Microsoft Addresses Security.” 10 March 2004.
URL: http://www.varbusiness.com/showArticle.jhtml?articleId=18842152.

McCarthy, Kieren. “Internet Explorer carved up by zero-day hole.” 8 June 2004.
URL: http://www.techworld.com/opsys/news/index.cfm?NewsID=1689.

SANS Institute. “Webcast: Security Strategies for Day-Zero Defense.” 25 September 2003. URL: http://www.sans.org/webcasts/show.php?webcastid=90417.

Shannon, Colleen. Moore, David. “The Spread of the Witty Worm.” 27 April 2004.
URL: http://www.caida.org/analysis/security/witty/.

Staniford, Stuart. Paxson, Vern. Weaver, Nicholas. “How to 0wn the Internet in Your Spare Time.” 2002. URL: http://www.icir.org/vern/papers/cdc-usenix-sec02/.

Symantec. “Definition of Blended Threat.”
URL: http://securityresponse.symantec.com/avcenter/refa.html#b.

Symantec. “Symantec Internet Security Threat: Trends for July 1, 2003 – December 31, 2003.” Volume V (2004).

TechWeb News. “New Bugbear Worm Exploits Unpatched IE Vulnerability.” 6 April 2004. URL: http://www.techweb.com/wire/story/TWB20040406S0010.

W2Knews. “The Patch Gap.” 01 March 2004.
URL: http://www.w2knews.com/index.cfm?id=465.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.