DEFENSIVE WALL 1: Proactive Software Assurance

Summary: The application layer is now the leading point of attack. The most important aspect of proactive software assurance is application security in its infancy and development groups are not yet integrating security into application design and programming. If we want to turn the tide against the attackers, our highest priority must be to help programmers design applications and develop code with fewer security flaws.

6.1 Source Code and Binary Code Analysis Tools
6.2 Application Security Scanners (White Box Tools)
6.3 Application Security Scanners (Black Box Tools)
6.4 Application Source Code Monitoring and Analysis Tools
6.5 Source Code and Binary Code Analysis Tools (White Box Scanners)
6.6 Application Source Code Monitoring and Analysis Tools
6.7 Application Source Code Monitoring and Analysis Tools (Black Box Scanners)
6.8 Application Source Code Monitoring and Analysis Tools (White Box Scanners)
6.9 Application Source Code Monitoring and Analysis Tools (Black Box Scanners)

DEFENSIVE WALL 2: Blocking Attacks: Network Based

Summary: Although many of the most damaging attacks will come from external, malicious traffic from the outside makes up the vast majority of all recorded attacks – and those attacks that do come from anyone, anywhere in the world. Effective cyber defense starts with a perimeter that makes it very hard for those external attacks to get in.

5.1 Intrusion Prevention (IPS/IDS) Detection and PC and host IPS/IDS systems, as well as cloud-based IPS/IDS systems.
5.2 Network Intrusion Prevention (NIPS) Systems
5.3 Network Intrusion Prevention (NIPS) Systems (Web Application Firewalls)
5.4 Network Intrusion Prevention (NIPS) Systems (Web Application Firewalls) (Web Application Firewalls)

DEFENSIVE WALL 3: Blocking Attacks: Host Based

Summary: If an attack gets through the network defenses, the PPI, the user is the final line of defense. And even if the user is poorly protected or not at all, the damage can be minimized. The individual protection devices are deployed to stop the attack as early as possible. These devices are designed to provide a broad spectrum of protection against malicious content and management threats to enable organizations to provide stronger protection with reduced acquisition and operation costs.

5.1 Endpoint Security
5.2 Network Access Control (NAC)
5.3 System Integrity Checking Tools
5.4 Application Security Scanners (White Box Tools)
5.5 Application Security Scanners (Black Box Tools)

DEFENSIVE WALL 4: Eliminating Security Vulnerabilities

Summary: Vulnerabilities are the root cause of many of today’s attacks. As the number of applications, both internal and external, grows, the number of attack surfaces that need to be monitored and defended increases. Companies need to find new and efficient ways to identify and mitigate these vulnerabilities.

3.1 Network Discovery Tools
3.2 Application Security Scanners (White Box Tools)
3.3 Security Auditors and Security Auditing Tools
3.4 Vulnerability Management Tools
3.5 Vulnerability Management Tools (Network Security Auditors)
3.6 Application Security Scanners (White Box Tools)

DEFENSIVE WALL 5: Safely Supporting Authorized Users

Summary: This area is where we ensure that authorized users are not unduly restricted by security requirements while unauthorized individuals are blocked.

5.1 Identity and Access Management
5.2 Mobile Data Protection and Storage Encryption
5.3 Storage and Backup Encryption
5.4 Fixing Configuration Flaws
5.5 Mobile Device Management

DEFENSIVE WALL 6: Tools to Manage Security and Maximize Effectiveness

Summary: This area is where we ensure that security is not just an afterthought but that it is an integral part of the design process.

6.1 Log Management and Security Information and Event Management (SIEM)
6.2 Media Sanitization and Recovery
6.3 Security Skills Development
6.4 Security Awareness Training
6.5 Forensics Tools
6.6 Governance, Risk, and Compliance Management Tools

SANS is the world leader in computer security training for professionals. Our mission is to help security professionals worldwide strengthen their skills and knowledge, helping them protect organizations and societies from the world’s most experienced cyber attackers. SANS offers a comprehensive range of programs that provide hands-on, relevant training in today’s most critical areas. The SANS curriculum is available in both classroom and virtual formats. For more information, visit www.sans.org.
The SANS Cyber Attack Threat Map illuminates the key elements present in nearly every attack and offers a means to map the steps in successful attacks so that the best defensive approaches can be identified. Each attack can be examined using a specific path through the map. As examples, we show how the SQL Injection attack to steal credit card numbers (in blue) and the Tibetan/Falun Gong attacks (in red) were carried out.

### Top 8 Most Dangerous Attack Vectors

1. **Web site attacks** to plant browser exploits
   - Attackers are exploiting trusted, high-profile websites and loading packages of browser exploits such as Mipack that commemorate any user that surfs to a website hosting an attacker's content, scripts created by the attacker
   - Devices and connect them to their computers, the infection spread, loading packages of browser exploits

2. **Targeted phishing attacks** / **spying phishing**
   - This powerful and common attack vector, users are duped by a site that appears to come from trusted sources, exporting them to a site on links or sites that compromise their systems

3. **Malware in embedded devices**
   - Attackers have manipulated the IT supply chain, altering USM-enabled consumer electronics devices, such as electronic picture frames and thumb drives.
   - When unsuspecting consumers purchase the infected devices and connect them to their computers, the infection spread, loading packages of browser exploits

4. **Browser scripting attacks** that turn a browser into a communications channel
   - With this ill-timed technique, if a computer user inside an enterprise simply surfs to a website hosting an attacker's content, scripts created by the attacker can then be known through communication endpoints, giving the attacker full VLAN-style access inside the enterprise firewall via the victim's browser

5. **The latest Metasploit releases**
   - The most recent release of this premier exploitation framework includes high-quality packages for over two hundred vulnerabilities, on a variety of platforms including Windows, Linux, and the Apple iPhone.

6. **Pass-the-hash tools widely available**
   - This is a fast and easy way for hackers to gain access to a system without needing to brute force the password, and it's how attackers are doing it now.

7. **Fast-flux bot-net servers**
   - To protect their bot-nets of hundreds of thousands or millions of compromised machines, attackers are employing obfuscation and redirection techniques known as fast-flux, confounding investigators and authors who try to shut down their criminal enterprise.

8. **Cold Boot Attacks**
   - Because the contents of RAM remain in place for several minutes without power, an attacker with physical access to a desktop or laptop computer can quickly reboot the system from a USB thumb drive or hard drive and copy the machine's memory to the drive. In just a few minutes, all of the secrets locked inside memory such as passwords, encryption keys, and sensitive data, can be retrieved, often without the victim even knowing that the attack occurred.

---

### SANS Top 20 Vulnerabilities

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-Site Scripting</td>
<td>Cross-site scripting is a technique that allows an attacker to inject malicious JavaScript into a web page and execute it in the context of the victim’s site.</td>
</tr>
<tr>
<td>Clickjacking</td>
<td>Clickjacking is a technique that overlays an image of a button or link on a web page, which can be clicked on by the user, leading to a different URL.</td>
</tr>
<tr>
<td>Same-Origin Policy Bypass</td>
<td>Same-Origin Policy Bypass is a vulnerability in web browsers that allows an attacker to access sensitive data, such as cookies, from a different origin.</td>
</tr>
</tbody>
</table>

---

### SQL Injection Attack To Steal Credit Card Numbers

- **Threat vector:** SQL Injection
- **Vulnerability:** SQL injection attacks allow an attacker to execute arbitrary SQL statements on a server.
- **Impact:** The attacker can steal sensitive data, such as credit card numbers, from the database.
- **Prevention:** Use parameterized queries and input validation to prevent SQL injection attacks.

---

### What types of protection could have stopped them?

- **Database Firewalls:** Protect against unauthorized access to the database by monitoring and controlling database access.
- **Log Management and Security Information and Event Management:** Monitor and analyze security events to detect and respond to attacks.
- **Virtual Private Networks:** Provide an encrypted communication channel between the client and server.
- **Storage and Backup Encryption:** Protect data at rest and in transit.
- **Identity and Access Management:** Control access to resources based on user identity.
- **Application Security Scanners (White Box Tools):** Identify vulnerabilities in web applications.
- **Source Code and Binary Code Testing Tools and Services (White Box Scanners):** Analyze code for security defects.

---

### To get your free vendor-sponsored whitepapers, visit

www.sans.org/tools.php