



nSENSE

nSense WebScan & SystemScan



February 2005

Abstract

On-line applications are rapidly increasing in number and complexity and as result, so are security vulnerabilities. nSense provides a comprehensive automated solution for auditing the security situation of your Web-facing platform, the services running on it, and importantly, the applications that stakeholders use to interact with your organization. The solution is comprised of two products: an application scanning tool (WebScan) and a system scanning tool (SystemScan).

This purpose of this document is to give you an overview of the technologies behind nSense WebScan & SystemScan and to help you discover why using these security auditing tools is imperative for your company.

1. Introduction

Application security is one of the most challenging aspects of Internet security. The increase of damaging malicious-code attacks, data theft, and on-line fraud, along with upcoming legal requirements, will soon force all organizations with Web-facing applications to take a more aggressive approach to security. Gartner reported in 2004 that 70% of all vulnerabilities are discovered in the application layer. Traditional defenses and solutions such as nessus scans and firewalls only reveal and prevent 30% of newly discovered vulnerabilities.

Put simply, application level security ensures that Internet applications interact with end users only in ways that were intended by the application's developers. Application level security is focused on preventing the unauthorized use of eBusiness resources and customer information by hackers attempting to gain access to the network directly through the application. Application level hacks typically exploit weaknesses in HTML coding, Common Gateway Interfaces (CGIs), or third-party products such as Web servers or scripts (e.g. php asp jsp).

"Securing Web applications needs to be a key element of every company's overall IT security plan".

John Pescatore
Vice President of Research, Information Security at Gartner Group.

2. nSense WebScan

nSense WebScan is *the* next generation security scanning tool that provides automated vulnerability discovery in Web applications. nSense WebScan was developed to address the challenge of managing security in a dynamic, increasingly complex Web-enabled environment.

nSense WebScan works beyond Intrusion Detection Systems (IDS) and firewalls by using allowed ports and protocols to identify vulnerabilities in the on-line applications, thus ensuring the security of your entire Web presence. Firewalls and other traditional intrusion prevention mechanisms do not detect attacks against the Web application and are insufficient when it comes to preventing attacks on the application layer. Many IT employees have a false sense of security regarding their companies' Web-facing applications. They believe that the security level is high based on an assumption that firewalls and traditional scans like nessus can detect all vulnerabilities and prevent intrusions. Vulnerabilities in Web applications are located in the code written by the developer and often are not corrected with standard patching. Closing these security holes means examining and revising the code directly.

nSense WebScan systematically detects and communicates Web application vulnerabilities and intrusions for any on-line business in real time on an ongoing basis, and provides intelligent methodological approaches for resolution of the vulnerabilities it discovers.

WebScan has three main phases:

1. Information gathering and analysis;
2. Attack; and
3. Compile and report.

Through the use of intelligence technology not available in any other automated Web application assessment tool, nSense WebScan is capable of making astute text and structure analyses in Phase One. With this information, in Phase Two WebScan creates a unique array of attacks based on a complex internal methodology, and then systematically executes these attacks against the application. In Phase Three, WebScan compiles the vulnerabilities discovered into two reports: one concise, clearly written summary for non-technical decision makers; and a second, detailed report with problem descriptions, the vulnerable code that was identified, and methods and recommendations for eliminating the security holes.



nSense WebScan tests for a number of different vulnerabilities including:

- Cross Site Scripting
- SQL Injection
- Cookie Poisoning
- Parameter Tampering
- Dynamic Forceful browsing
- WebDav Vulnerabilities
- Forceful Browsing based on textual analysis
- Textual Analysis - Suspicious Content
- Authentication Bypassing
- Simple Object Access Protocol Vulnerabilities
- File Disclosure
- Stealth Commanding
- 2-phase Cross Site Scripting Discovery

nSense WebScans are run over the Internet as an ASP service provided by nSense. Reports can be delivered in several ways.

These report types include:

- Rich Text Format Report (print)
- Auditor Report (html)
- On-line Report
- XML Report
- Expert Review Report (Service)
- Executive Summary Report (Service)

Feature Listing:

- http/https application recording
- Custom exception fingerprinting
- Hidden SQL Injection discovery (resetting statements)
- User defined forceful browsing lists
- User defined XSS/SQL Injection attacks & fingerprints
- Custom suspicious content fingerprinting
- Scheduled Scans (limit on hours)
- Application Exploring

For sample nSense WebScan reports please visit:

<http://karhu.nsense.net>

Username: demo

Password: demo

For sample expert review & executive summary reports please contact Antamis on +32 (0)2 211 34 39 or info@antamis.com.

3. nSense SystemScan

Sense SystemScan is an Internet security scanning tool that provides automated vulnerability discovery in platforms and the services they provide.

nSense SystemScan uses a unique combination of different security products that are individually regarded as standards in the IT security industry, which are complemented with software specifically developed by nSense for nSense to further increase scan effectiveness. Products incorporated include: nessus, nikto, nmap, hping2, Dominohunter, and NBScan.

As new vulnerabilities appear frequently, nSense SystemScan is being continuously developed in order to stay one step ahead of hackers. nSense SystemScan is suitable for scanning any of the following units your company might be hosting:

- Web servers
- firewalls
- routers and switches
- mail servers
- dns servers
- and more...

When a scan is complete, SystemScan compiles the vulnerabilities into a summary and audit report. The summary is concise, clearly written, and easy for non-technical decision makers to understand. The detailed audit report has thorough problem descriptions and recommendations for eliminating the vulnerabilities.

nSense SystemScans are run over the Internet as an ASP service provided by nSense. Reports can be delivered in several ways.

These report types include:

- Scan Report Rich Text Format
- On-line Report
- Expert Review Report (Service)
- Executive Summary Report (Service)

For sample nSense SystemScan reports please visit:

<http://karhu.nsense.net>

Username: demo

Password: demo

For sample expert review & executive summary reports please contact Antamis on +32 (0)2 211 34 39 or info@antamis.com.

4. Conclusion

WebScan and SystemScan combined enable nSense to provide a unique solution covering the platform and network levels, along with the extremely important application layer of the on-line services.

To set up a sales presentation or to learn more about nSense products, call Antamis on +32 (0)2 211 34 39, or write to info@antamis.com.

