



**eEye Digital Security®**

## **eEye Digital Security White Paper**

Retina® Network Security Scanner

Understanding CHAM – Common Hacking Attack Methods

For more information about Retina® Network Security Scanner  
[www.eeye.com](http://www.eeye.com)

---



**© 2004 eEye Digital Security.  
All Rights Reserved.**

This document contains information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of eEye Digital Security.

For the latest updates to this document, please visit:

**<http://www.eeye.com>**

#### **Warranty**

This document is supplied on an "as is" basis with no warranty and no support.

#### **Limitations of Liability**

In no event shall eEye Digital Security be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained in this document is subject to change without notice.

No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this white paper.

#### **Disclaimer**

All brand names and product names used in this document are trademarks, registered trademarks, or trade names of their respective holders. eEye Digital Security is not associated with any other vendors or products mentioned in this document.

## **Understanding CHAM – Common Hacking Attack Methods**

eEye Digital Security incorporated its proprietary CHAM technology into Retina Network Security Scanner as a way to offer advanced vulnerability detection to those seeking to substantially challenge their network infrastructure. While Retina is the industry's fastest and most comprehensive non-intrusive scanner, utilizing the CHAM feature is strictly for advanced users as it subjects the network to intrusive penetration testing.

This paper outlines normal scanner functionality as it compares to CHAM and how/when CHAM should be utilized.

### **The Retina Foundation**

eEye's Retina Network Security Scanner is recognized as the best vulnerability assessment and remediation product on the market – setting the standard in terms of speed, ease of use, reporting, non-intrusiveness and advanced scanning capabilities using AI technology.

Retina's speed is unmatched, as it can scan every machine on a network including a variety of operating systems, networked devices and third party or custom applications, all in record time. Retina can scan an average Class C network in under 15 minutes – up to 15 times faster than the competition – and was the only scanner capable of reliably scanning an entire Class B network in under 2 hours. As a result, Retina won the 2002 Network World Blue Ribbon Award over the leading competitors and was rated as the best vulnerability scanner on the market.

After scanning, Retina delivers a comprehensive report that details all vulnerabilities on the systems tested and suggests appropriate fixes such as downloading related patches or using Retina's automatic repair capabilities to correct improper configurations. The vulnerabilities Retina audits are continuously updated and users can even create custom audits via Retina's open architecture and easy to use interface.

For distributed enterprise environments, Retina can be deployed in conjunction with REM™ Remote Enterprise Management to create a robust enterprise vulnerability assessment and remediation management system. Enterprise customers often prefer this Retina/REM centralized vulnerability assessment management and remediation structure. More information on REM and the enterprise solution is available online via the eEye Website.

## **The Need for CHAM**

With the robust capabilities of the non-intrusive Retina, why would an organization want to utilize the CHAM feature and subject their network to intensive penetration testing?

Quite simply, traditional scanning products are unable to detect hidden vulnerabilities within custom developed software, specialized applications and outdated software products. Many companies use some form of custom applications, which can often be overlooked by scanners, but may still be exposed and unknowingly vulnerable to attack.

Custom and uncommon software products have not typically gone through the scrutiny of thousands of hackers probing and testing them on a daily basis like most COTS operating systems and software applications. Therefore, there may be vulnerabilities associated with these products that have simply remained undiscovered. These custom and uncommon applications may be the weak link in a network and enable a hacker to gain access to critical data.

## **CHAM Thinks Like A Hacker**

CHAM was developed to operate like a hacker and scour any customized applications for weaknesses. When CHAM functionality is enabled, Retina takes on two roles. First, it performs a normal, non-intrusive scan to identify all known vulnerabilities. Next, Retina switches into CHAM mode and becomes a confidential “hacking-consultant” by testing for network weaknesses in unusual applications or customized programs.

When Retina examines a network, it culls information about the network devices and learns how they communicate on the network. Information on these points of communication can be utilized by CHAM in performing numerous hacking attempts on selected protocols. These attacks utilize a proprietary 'decision tree modeling' structured engine which intelligently seeks to compromise target machines. CHAM currently targets HTTP, FTP, SMTP and POP3 protocols (the most heavily used protocols on the Internet and in intranets today). This allows it to behave in a non-scripted fashion reacting to data it finds and tuning its behavior based on environment-specific data.

Retina's CHAM feature will audit the target service for buffer overflows. During this audit, Retina will attempt to discover buffer overflows by sending malformed data to the server. Malformed data is defined as unexpected, too much, too little or abnormal data content. Under CHAM, Retina will attempt 'format string attacks' which are a class of attack also known as 'channeling' attacks. Under this mode of attack, attempts are made to merge two or more data streams into a single data stream. Special sequences may be found that would allow an attacker using the same sequences to gain control of the process or service hosting the targeted data streams.

It may be possible for CHAM to disrupt the service or to find a point in the oversized data where malicious payload could be attached by an attacker — which could enable them to inject data into the process or to transplant malicious code onto the host itself. In some instances CHAM will also attempt to attack path variables as well, which can lead to service compromise or privilege escalation. Additionally, CHAM will look for deviances from published RFCs for each service audited.

These types of attacks used by CHAM will simulate the methods a cracker would likely use when trying to compromise a machine.

### **CHAM Vulnerability Procedure**

If Retina's CHAM finds a vulnerability it will do several things, namely:

- Display the service in which the vulnerability was found in the Audits window of Retina.
- Inform the user of what attack CHAM performed to find the vulnerability.
- Provide contact information with which a screen shot of the Audit window can be sent to eEye's vulnerability research team for further evaluation – if so desired. Upon receipt of a new vulnerability, eEye will work with the customer to verify the issue and then contact the software vendor in which the vulnerability was found to alert them of the vulnerability. eEye does not create software fixes or patches for vendors, but may suggest fixes as deemed appropriate. Once a reply is received from the vendor, eEye will forward the information to the person or organization that initially reported the vulnerability.

Please note, eEye reserves the right to choose an appropriate response to CHAM vulnerability reports. If custom developed software yields a large amount of reported CHAM vulnerabilities, eEye will not debug code and is not responsible for any corrective action. The offer to look at vulnerabilities is on a time-permitting basis and done as a favor to our valued customers.

### **When to Utilize CHAM**

CHAM should be used only for those servers and machines that are not part of a production or mission critical network. By using CHAM, administrators will initiate high-end penetration testing that probes for uncommon network vulnerabilities. The only way to discover unknown vulnerabilities in specific applications and customized software is to subject these systems to simulated, intelligent hacker attacks.

By initiating CHAM, administrators realize and acknowledge the potential of CHAM success in these attacks and bringing down the system tested.

CHAM provides a level of network security expertise that is unavailable in any other network security scanner. It is a valuable tool that allows organizations to dramatically improve the security level of their custom or homegrown applications.

For more information on Retina, REM, and other eEye Digital Security offerings, please visit the eEye Website at: [www.eEye.com](http://www.eEye.com).