



Retina CHAM™ (Common Hacking Attack Methods)

eEye Digital Security incorporates its proprietary CHAM technology into most of its products. In this paper we focus on the use of CHAM in Retina, the Network Security Scanner. For many clients, CHAM provides a level of value-add unmatched by any security product in the market.

Normal Scanner Function

Retina audits your network for known vulnerabilities and provides the fixes through Auto Fix-It and appropriate links to vendors and security sites. The vulnerabilities Retina audits are continuously updated. Retina users can update their vulnerability database through the Auto Update functionality within Retina.

These vulnerabilities typically relate to various operating systems and widely distributed software. Security software R&D houses such as eEye Digital Security, and thousands of black and white hat hackers around the world discover them.

Problem Definition

Are you using custom developed software on your network like most large companies? Are you using an old version of a commercial software product? Are you using specialized software products? If the answer to any of these questions is yes, then your network may still be at high risk from external attack, even if you use a traditional scanner.

These custom and uncommon software products have not typically gone through the scrutiny of thousands of hackers probing and testing them like most operating systems and common software products. Vulnerabilities associated with these products have not been discovered, posted and updated on the Retina database (nor competitor scanners of course). These custom and uncommon software products may be a door wide open on your network to any hacker who finds them.

CHAM Thinks Like A Hacker

When you turn on the CHAM functionality, Retina takes on two functions. First, it performs a normal scan identifying known vulnerabilities as it normally does. Second, it becomes your own personal, 100% confidential, internal hacker-consultant.

Retina learns as much information as possible about your network from the scan and then uses that information to discover unknown vulnerabilities in your network. This is the artificial intelligence aspect of the software. Based on the gathered information, Retina CHAM then performs various hacking attacks on several protocols that you may pre-select in the Policies menu (FTP, POP3, SMTP, HTTP). The attacks include buffer overflows, format string attacks, path attacks, munged byte attacks, and others. This is how a hacker would most likely attack your network!



CHAM Vulnerability Procedure

If CHAM finds a vulnerability:

- Retina will display, in the Audits window, in what service it found the vulnerability.
- Retina will also inform you of what attack CHAM performed to find the vulnerability.
- Retina will provide you with contact information with which to send a screen shot of the Audit window to eEye.
- eEye will then typically contact the software vendor in which the vulnerability was found and alert them to the vulnerability. eEye may also suggest the fix.
- Once eEye has a reply from a vendor they will forward the information to the person or organization that reported the vulnerability.

Note that eEye reserves the right on how to respond to CHAM vulnerability reports. If you custom build a piece of software that generates a lot of CHAM vulnerabilities, eEye may just send you an email advising to hire new software engineers!

When Should You Use CHAM

You should use CHAM for those servers and machines that require a very high level of security and scrutiny. By using CHAM you have essentially hired a high-end penetration-testing expert who is probing your specific network for vulnerabilities. The only way to discover unknown vulnerabilities in your system is to simulate intelligent hacker attacks. CHAM is able to simulate this thought process and has the potential of succeeding in these attacks, thus bringing down your machine.

CHAM provides a level of network security expertise that you do not find in most software products. It is a valuable tool that allows you to dramatically improve the security level of mission-critical network servers and workstations.