Retina CHAM™ (Common Hacking Attack Methods)

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

Normal Scanner Function

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

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

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 to an 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 them 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 left wide open to a hacker.

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 overflows, format string attacks, path attacks, munged byte attacks, among others. This is how a hacker would likely attack your network!

CHAM Vulnerability Procedure

If CHAM finds a vulnerability:

- Retina will display, in the Audits window, the service in which it found a vulnerability.
- Retina will also inform you of what attack CHAM performed to find the vulnerability.
- Retina will provide you with contact information with which you can 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 we have a reply from the vendor, we will forward the information to the person or organization that initially reported the vulnerability.

Note that eEye reserves the right to choose an appropriate response to CHAM vulnerability reports. If you custom build a piece of software that generates a large amount of CHAM vulnerabilities, we may just send you an email advising you to hire new software engineers!

When Should You Use CHAM

CHAM should be used 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. With this, CHAM has the potential of succeeding in these attacks and bringing down your machine.

CHAM provides a level of network security expertise that you will not find in most companies and products. It is a valuable tool that allows you to dramatically improve the security level of mission-critical network servers and workstations. We recommend making CHAM an integral part of your applications development process, we certainly did!