netVigilance

ScoutNews Team **05 March 2004**

Issue #10

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Dueling Worms - the Sand Worms in Frank Herbert's novel 'Dune' come to mind, only inside your network. The **Harkonnens** vs. **Atreides**. We have seen variation after variation after variation on a virus this week flooding networks and emails worldwide. You will notice SecureScout now has Registry Checks for the **Bagle.c,d,e,h&i worms as well as the Netsky.c,d & e worms**. To finish up the week in news – Adrian Lamo, white hat hacker turned student and writer tells how to profile a network to make breaking in a bit easier. See if you can spot your network in his story. There is an easy visualization exercise you can download, that helps you demonstrate wireless vulnerabilities. While it may not be an office party trick, it is effective tool to educate.

New Feature Alert:

- The powerful Command Line Interface [**CLI**] previously only available in NX is now in **SecureScout SP** V.1.9.120, available just this week.
- From the CLI there you can use the **NEW** RangeScan feature. RangeScan a new scan type in addition to "IpSweep, HostID, VulnScan"
- RangeScan now allow for the scanning of Large Ranges Class-B and Class-A networks. One huge benefit: it will find and start scanning in one step. **No waiting**.
- At some future date, we'd like to incorporate the CLI functions into Adminclinet and Webclient. For now, incorporate this new scan type in your next scan. Larger scans now start faster.

Top Security News Stories this Week

❖ **Bagle, MyDoom and NetSky Virus Authors at War**

Top news story this week - anti-virus researchers have uncovered bit of a bitter battle between virus authors. It seems that some of the programming code found inside the recent Bagle viruses reveals a verbal onslaught, aimed at the author(s) of the Netsky worm. Since last Friday, more than 10 variants of the Netsky, Bagle and MyDoom worms have been discovered. Mutants spreading in the past 24 hours have contained messages that indicate the authors of MyDoom and Bagle have teamed up against Netsky's author, antivirus experts

said. Virii warriors are vying for attention and pole position and talk trash about each other. Oh my. Make no mistake, the pranks and spitting contests among the virus writers are becoming increasingly more malicious. This weeks SecureScout update has checks for most of these worms. Keep on your toes out there.

http://itvibe.com/default.aspx?NewsID=2372
http://zdnet.com.com/2100-1105_2-5168983.html
By Rich Kavanagh – ITVibe / ZdNet

- **RSC Report: The 'Hot Stuff' in Security Today**

The recent RSA Conference is the technology industry's premier security event. As cyber security has become an ever larger concern, the data security industry has also mushroomed. Although the lingo has changed from the pre-spam days, you could divide the technology on display from the nearly 250 companies into one of two categories: "hot stuff" and "perennial stuff." First, the hot stuff: *Appliances; Software appliances; Intrusion prevention; Antispam; Wireless; SSL VPNs; Identity management; and of course Proactive vs. reactive*. Proactive software is the good stuff, which anticipates security problems. Reactive software is the bad kind, which reacts to the problem you've just encountered. And the best software combines proactive and reactive solutions. That way, when the proactive software doesn't work, the reactive software can tell you what just happened to you. Proactive and preemptive describes SecureScout's approach to network security. Check out Tim's take on what is hot and what are the perennial foundations of any good security effort.

http://zdnet.com.com/2100-1105_2-5169242.html
By Tim Clark – ZDNET

- **Increasing Security Awareness: Visualizing WEP Insecurity To The Masses**

There is nothing like the old "show and tell" to get your point across. This article [and downloadable .PDF] describes how one can setup and perform a small wireless demonstration that is quick and easy to perform with a good visual result to trigger the attention of the people you work with. The goal of the setup is to demonstrate a well-known WEP vulnerability. In order to demonstrate the WEP vulnerability, we will use the OpenBSD operating system. You don't need any prior OpenBSD knowledge, all the information you need is in here. Check the link below for more info on how to set this up. Note: for this demonstration, you do not need hours of traffic capturing. It can all be done within 30 minutes (maximum).

http://www.net-security.org/dl/articles/sthuy_article_wep_cracking.pdf
By Stijn Huyghe - Telindus High-Tech Institute

- **Profiling Network Administrators – Hacker Tells All**

Read the insightful Network World Fusion story by Adrian Lamo, the white hat hacker who pled guilty to accessing The New York Times computers without permission. It seems the young lad has agreed to share what he knows about some of the common IT security slips network administrators make. The belief that attacks will inherently come from the outside sets networks up to fall. Security is not always a linear process. If you're going to profile intruders, profile defenders too - be they good examples, or terrible warnings. This is an interesting story worth taking the time to read. Forewarned is forearmed.

http://www.nwfusion.com/research/2004/0301hackerslamo.html
By Adrian Lamo - Network World Fusion

- **Network Protocol Stack & TCP Hacking - Linux**

As any network administrator will tell you, network devices form the bottom layer of the protocol stack. They use a link layer protocol (usually Ethernet) to communicate with other devices to send and receive traffic. The interface put up by the network device driver copy packets from a physical medium; perform some error checks, then puts up the packet to the network layer. Output interfaces receive packets from the network layer, perform some error checks, and then send them out over the physical medium. One most important lesson we get from the sample TPC hack program in this article is that it is not always necessary to change the kernel source when we are doing any protocol related modification. It is the object oriented implementation of Linux kernel which allows us to play with data objects inside the kernel. If you are on a Linux box, you might take a moment and browse through this article.

http://www.linuxgazette.com/node/view/8781
http://rootprompt.org/article.php3?article=6240
By Shyamjithe - LinuxGazette

New Vulnerabilities Tested in SecureScout

Ten new vulnerability Test Cases have been incorporated into the SecureScout database this week including Registry Check for the Bagle c, d, e, h & i worms and the Netsky c, d and e worms! Of course, these weekly updates essential in keeping your network scanning tool one step in front of the hackers, inside or outside the organization.

- **14410 W32/Bagle.c & W32/Bagle.d Worms (Registry Check)**

W32/Bagle.d has minor code changes but the behavior is identical to the W32/Bagle.c version. This is a mass-mailing worm with the following characteristics:
- Contains its own SMTP engine to construct outgoing messages.
- Harvests email addresses from the victim machine
- The From: address of messages is spoofed
- Contains a remote access component (notification is sent to hacker)

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

CVE Link: No CVE link available
McAfee: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101059
SecureScout Test Case: http://descriptions.securescout.com/tc/14410

- **14411 W32/Bagle.e Worm (Registry Check)**

This is a mass-mailing worm with the following characteristics:
- Contains its own SMTP engine to construct outgoing messages.
- Harvests email addresses from the victim machine
- The From: address of messages is spoofed
- Contains a remote access component (notification is sent to hacker)

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

CVE Links: No CVE link available
McAfee: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101061
SecureScout Test Case: http://descriptions.securescout.com/tc/14411

- **14412 W32/Bagle.h Worm (Registry Check)**

This is part escalating mass-mailing worm. Like its predecessors, this worm checks the system date. If it is the 25th March 2005 or later, the worm simply exits and does not propagate. Of course, it:
- Contains its own SMTP engine to construct outgoing messages.
- Harvests email addresses from the victim machine
- The From: address of messages is spoofed
- Contains a remote access component (notification is sent to hacker)
- Peer To Peer Propagation.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

CVE Link: No CVE link available
McAfee: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101068
SecureScout Test Case: http://descriptions.securescout.com/tc/14412

- **14414 W32/Netsky.c & W32/Netsky.d & W32/Netsky.e Worms (Registry Check)**

The description applies to W32/Netsky.c, W32/Netsky.d and W32/Netsky.e versions of the W32/Netsky worm. The only exception is that W32/Netsky.d and W32/Netsky.e do not use network or peer-to-peer replication.

This virus spreads via email and mapped drives. It sends itself to addresses found on the victim's machine and by copying itself to folders on drives C: & Z:
The virus also attempts to deactivate the W32/Mydoom.a and W32/Mydoom.b viruses.

The virus sends itself via SMTP - constructing messages using its own SMTP engine. It queries the DNS server for the MX record and connects directly to the MTA of the targeted domain and sends the message.

The worm copies itself to directories containing the string share on the local system and on mapped network drives. This will result in propagation via KaZaa, Bearshare, Limewire, and other P2P application.

Filenames are carried within the worm, for example:
1000 Sex and more.rtf.exe
3D Studio Max 3dsmax.exe
Adobe Photoshop 9 full.exe
Adobe Premiere 9.exe
Ahead Nero 7.exe
Best Matrix Screensaver.scr
Clone DVD 5.exe Magix Video Deluxe 4.exe

Cracks & Warez Archive.exe … and a whole lot of other enticing names.

Test Case Impact: **Attack** Vulnerability Impact: **Attack** Risk: **High**

CVE Link: No CVE link available
McAfee: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101048
http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101064
http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101067
SecureScout Test Case: http://descriptions.securescout.com/tc/14414

- **14415 W32/Bagle.i Worm (Registry Check)**

Yes, this is yet another variant on that evil mass-mailing worm. Besides spoofing an address and carrying a mean payload, check out what the subject and body text says. Now anyone who opens a message with these subjects and body text and THEN opens the attachment is already in a world of trouble. Well, they better be running this Test Case daily, if not more. The messages are constructed as follows:

From : (address is spoofed)

Body : Hey, dude, it's me ^_^ :P
Argh, i don't like the plaintext :)
I don't bite, weah!
Looking forward for a response :P
Subject : Weah, hello! :-)
Hokki =)
Weeeeee! ;)))
Hi! :-)
^_^ meay-meay!
^_^ mew-mew (-:

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

CVE Link: No CVE link available
McAfee: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101068
SecureScout Test Case: http://descriptions.securescout.com/tc/14415

- **19007 Hijack Adultlinks.Quickbar**

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

CVE Link: No CVE link available
PestPatrol: http://www.pestpatrol.com/PestInfo/a/adultlinks_quickbar.asp

http://www.pestpatrol.com/Support/HowTo/How_To_Clear_a_Hijack.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19007

- **19008 Hijack Americlicks**

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

CVE Link: No CVE link available
PestParol: http://www.pestpatrol.com/PestInfo/a/americlicks.asp
http://www.pestpatrol.com/Support/HowTo/How_To_Clear_a_Hijack.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19008

- **19009 Hijack Hijack AutoSearch**

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

CVE Link: No CVE link available
PestPatrol: http://www.pestpatrol.com/PestInfo/a/autosearch.asp
http://www.pestpatrol.com/Support/HowTo/How_To_Clear_a_Hijack.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19009

- **19010 Hijack BrowserPal**

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found. Resets your browser's settings to point to other sites. Slows down your browser.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

CVE Link: No CVE link available
PestPatrol: http://www.pestpatrol.com/PestInfo/b/browserpal.asp
http://www.pestpatrol.com/Support/HowTo/How_To_Clear_a_Hijack.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19010

- **19011 Hijack ClearSearch**

  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found. Resets your browser's settings to point to other sites. Slows down your browser.

  Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

  CVE Link: No CVE link available
  PestPatrol: http://www.pestpatrol.com/PestInfo/c/clearsearch.asp
  http://www.pestpatrol.com/Support/HowTo/How_To_Clear_a_Hijack.asp
  SecureScout Test Case: http://descriptions.securescout.com/tc/19011

New Vulnerabilities this Week

Microsoft Windows Window Message Subsystem Design Error Vulnerability
A serious design error in the Win32 API has been reported. The issue is related to the inter-window message passing system. This vulnerability is wide-ranging and likely affects almost every Win32 window-based application. Attackers with local access may exploit this vulnerability to elevate privileges if a window belonging to another process with higher privileges is present. One example of such a process is antivirus software, which often must run with LocalSystem privileges.

A paper, entitled "Win32 Message Vulnerabilities Redux" has been published by iDEFENSE that describes another Windows message that may be abused in a similar manner to WM_TIMER. Microsoft has not released patches to address problems with this message. There are likely other messages which can be exploited in the same manner.
For more information, see http://www.securityfocus.com/bid/5408/discussion/
Source: SecurityFocus

Buffer Overflow in WinZip
A buffer overflow vulnerability in WinZip can result in the arbitrary execution of code on the vulnerable system. This vulnerability is a result of a flaw in the parameter parsing routine. WinZip will crash when it provides long strings to certain parameters of MIME archives (.mim, .uue, .uu, .b64, .bhx, .hqx, and .xxe extensions). WinZip has made available version 9.0, which doesn't have the buffer overflow vulnerability.
For more information, see
http://www.winnetmag.com/WindowsSecurity/Article/ArticleID/41916/WindowsSecurity_41916.html
Source: Windows and NT Magazine

GWeb '../' Input Validation Flaw Discloses Files to Remote Users
A vulnerability has been reported in theJava-based GWeb server. A remote user can view files

located anywhere on the target server. It is reported that the web server does not filter the '../' directory traversal characters from user-supplied GET requests. A remote user can submit a specially crafted URL to traverse the directory and view files on the target system with the privileges of the web service.
For more information, see http://www.securitytracker.com/alerts/2004/Mar/1009305.html
Source: Security Tracker

FreeBSD-SA-04:04.tcp - Many Out-of-Sequence TCP Packets - Denial-of-Service
The Transmission Control Protocol (TCP) of the TCP/IP protocol suite provides a connection-oriented, reliable, sequence-preserving data stream service. When network packets making up a TCP stream (``TCP segments'') are received out-of-sequence, they are maintained in a reassembly queue by the destination system until they can be re-ordered and re-assembled.

The problem is that FreeBSD does not limit the number of TCP segments that may be held in a reassembly queue. As a result, a remote attacker may conduct a low-bandwidth denial-of-service attack against a machine providing services based on TCP (there are many such services, including HTTP, SMTP, and FTP). By sending many out-of-sequence TCP segments, the attacker can cause the target machine to consume all available memory buffers (``mbufs''), likely leading to a system crash.

It may be possible to mitigate some denial-of-service attacks by implementing timeouts at the application level. Either upgrade your system to 4-STABLE, or to the RELENG_5_2, RELENG_4_9, or RELENG_4_8 or patch your present system.
For more information, see http://www.zone-h.com/advisories/read/id=4088
Source: Zone - h

Adobe Acrobat Reader Buffer Overflow in Parsing XML Forms Lets Remote Users Execute Arbitrary Code
A buffer overflow vulnerability was reported in Adobe Acrobat Reader in the processing of XML Forms. A remote user can execute arbitrary code on a target user's system.

NGSSoftware reported that a remote user can create a specially crafted XML Forms Data Format (XFDF) file that, when loaded by a target user, will trigger a stack overflow and execute arbitrary code. XFDF files typically have a file extension of '.xfdf' and a MIME type of 'application/vnd.adobe.xfdf'.

It is reported that the XFDF parser makes an unsafe sprintf() call in the OutputDebugString() function (regardless of whether debugging is performed or not).

The bottom line: a remote user can cause arbitrary code to be executed when a target user opens a specially crafted file. The report indicates that, according to the vendor, the current version of Adobe Acrobat Reader (6.0) is not vulnerable.
For more information, see http://www.ngssoftware.com/advisories/adobexfdf.txt
http://www.infosyssec.com/cgi-bin/flink.cgi?target=www.infosyssec.com/infosyssec/aaa33.htm
Source: Security Tracker

Vulnerability Resource
Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the ‘security portal for information system security professionals’ is well founded. http://www.infosyssec.org/infosyssec/

Thank You

Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com.