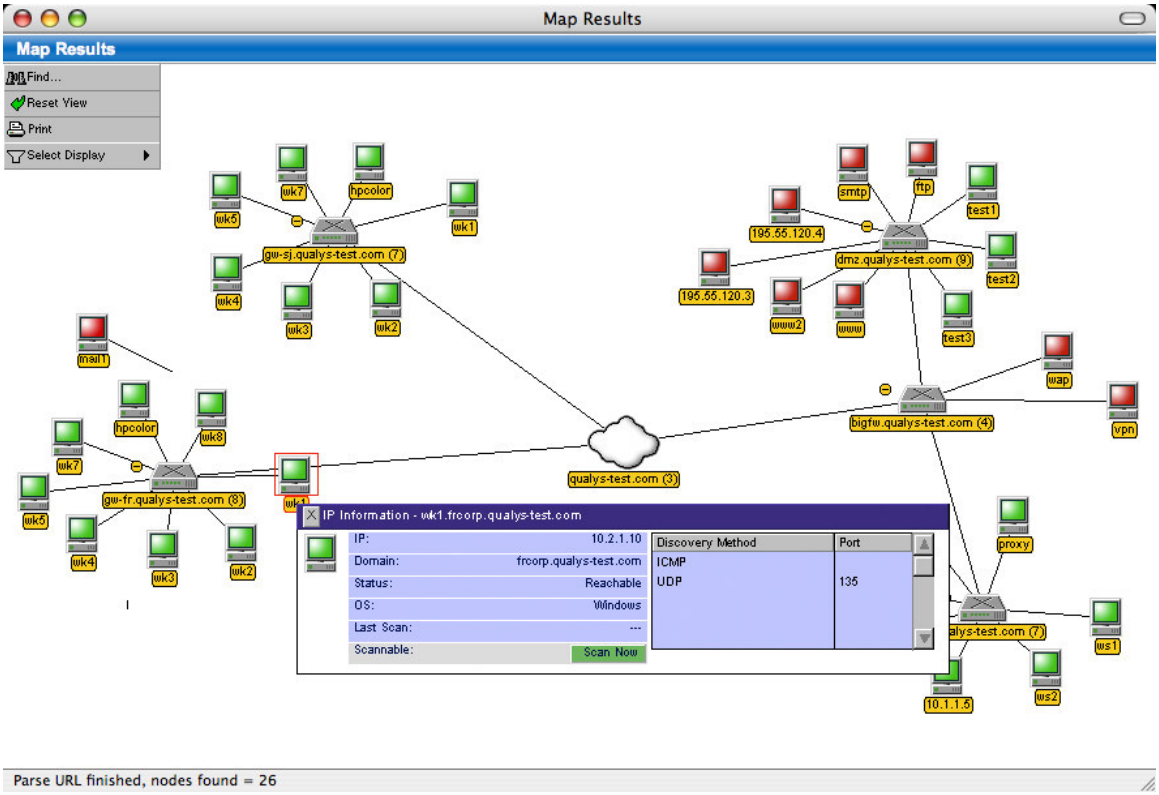
Perimeter Mapping (The First Step):

With the QualysGuard appliance which we will install inside the corporate network, the QualysGuard mapping feature produces a map of all visible devices on your internal network. The scope of the network discovery includes the devices found for a domain through the internal DNS in your network, plus any additional unregistered hosts discovered on the network. Mapping identifies all network devices including PCs, servers, network printers, firewalls, etc. and reports comprehensive information about them. The map report provides a topology of network devices in graphical and text formats. QualysGuard Mapping can detect rogue devices including virtual hosts that may have been maliciously placed on your network. It also finds weaknesses due to DNS server and firewall misconfigurations. Using the extensive Qualys vulnerability database, we will detect any network penetration weaknesses at your network perimeter as well as inside the network.



Identify Network Security Vulnerabilities:

Driven by the largest and most up-to-date KnowledgeBase of vulnerability checks in the industry, QualysGuard's external and internal scanners safely and accurately detect security vulnerabilities and penetration weaknesses across the entire network. QualysGuard's extremely accurate scans eliminate the time drain of chasing false positives, false negatives and host crashes.

Scan Results

File ▾ View ▾ Help ▾

QUALYSGUARD® ENTERPRISE

ON DEMAND SECURITY

September 19, 2007

Scan Results

Chief Information Security Officer
quays_hd
Manager

Qualys, Inc.
1600 Bridge Parkway
RWC, California 94065
United States of America

Created:09/19/2007 at 13:57:00 (GMT-0700)

Report Summary

Date:	05/28/2007 at 20:00:08 (GMT-0700)
Active Hosts:	1
Total Hosts:	3
Type:	Scheduled
Status:	Finished
Reference:	scan/1180407607.8431
Scanner Appliance:	167.216.252.38 (Scanner 4.4.56-1,Web 5.0.193-8,Vulnsigs 1.17.60-3)
Duration:	00:04:11
Title:	Daily Webservers
Asset Groups:	Extranet
IPs:	64.41.134.59-64.41.134.61
Option Profile:	Daily Webserver

Summary of Vulnerabilities

Total: 84 Security Risk (Avg): 5.0

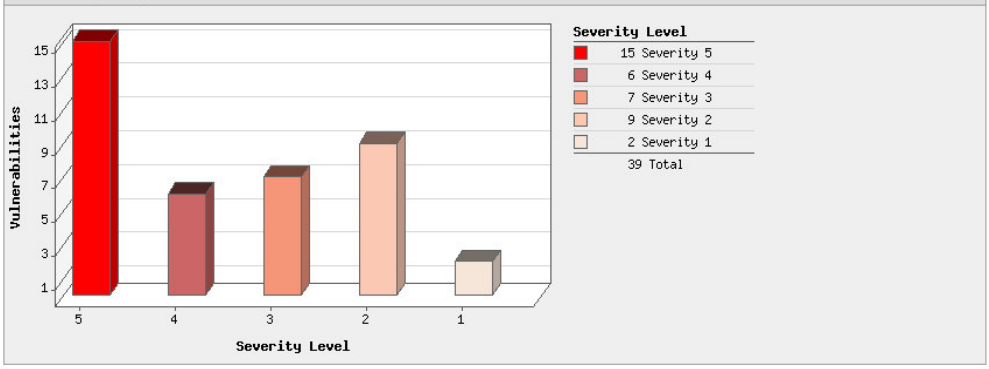
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	15	3	0	18
4	6	6	0	12
3	7	6	1	14
2	9	1	5	15
1	2	0	23	25
Total	**39**	**16**	**29**	**84**

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Web server	10	9	3	22
Database	12	4	2	18
CGI	7	2	3	12
TCP/IP	3	0	8	11
Information gathering	0	0	9	9
Total	**32**	**15**	**25**	**72**

Vulnerabilities by Severity



Analyze Threats with Powerful Reporting:

Intuitive and easy-to-read reports provide both executive-level summaries and detailed technical analysis. QualysGuard Qualys reports provide a detailed description of each vulnerability which includes: (1) the security threat, (2) the consequences should the vulnerability be exploited, and (3) the recommended solution to remediate the vulnerability, including links to the appropriate patches. QualysGuard provides powerful reporting options including a detailed analysis of each discovered vulnerability as in the report displayed below.

Vulnerabilities (37)

5 Microsoft IIS Chunked Encoding Heap Overflow Variant Vulnerability port 80/tcp **New**

First Detected: 12/23/2006 at 10:22:11 (GMT-0800) **Last Detected:** 12/23/2006 at 10:22:11 (GMT-0800)

Times Detected: 1

QID:	10571
Categroy:	CGI
CVE ID:	CVE-2002-0147
Vendor Reference	-
Bugtraq ID:	4490
Last Update:	11/30/2005

THREAT:

A heap overflow condition in the 'chunked encoding transfer mechanism' related to Active Server Pages has been reported in Microsoft Internet Information Server (IIS).

Web clients can send data to ASP (Active Server Pages) scripts in variable sized chunks. This is part of the HTTP protocol specification and is known as a chunked encoding transfer. The chunked encoding transfer mechanism must allocate a buffer in order to handle the transfer. There is a lack of sufficient bounds checking on this buffer, which is dynamically allocated by the ISAPI extension that handles ASP scripting. The result is a remotely exploitable heap overflow.

This vulnerability is a variant of the vulnerability discussed in BID 4485 "Microsoft IIS Chunked Encoding Transfer Heap Overflow Vulnerability".

IMPACT:

If this vulnerability is successfully exploited, a malicious user could cause a denial of service condition or execute arbitrary instructions on the vulnerable host.

SOLUTION:

Microsoft released an IIS cumulative patch to address several vulnerabilities, including this one. For more information regarding these IIS vulnerabilities and for patch download locations and instructions, read Microsoft Security Bulletin MS02-018.