

Security Service Offerings

Network Vulnerability Assessment

Don't let the Hackers win. See what's happening on your network's doorstep right now.

We are now offering Network Vulnerability Assessments as part of our continuing mission to end network intrusions, one network at a time. Networks are vulnerable for two reasons: First, network owners simply do not understand how vulnerable they are. Second, if they do understand the risks, they believe it is too expensive to remediate their vulnerabilities. Our remote network vulnerability assessment gives network owners and their IT managers a quick and easy way to gauge their network's vulnerability. And since there are no hardware requirements, the procedure is quick, unobtrusive, and transparent. After the test, our team helps you sift through the information and make sense of it all.

What is it?

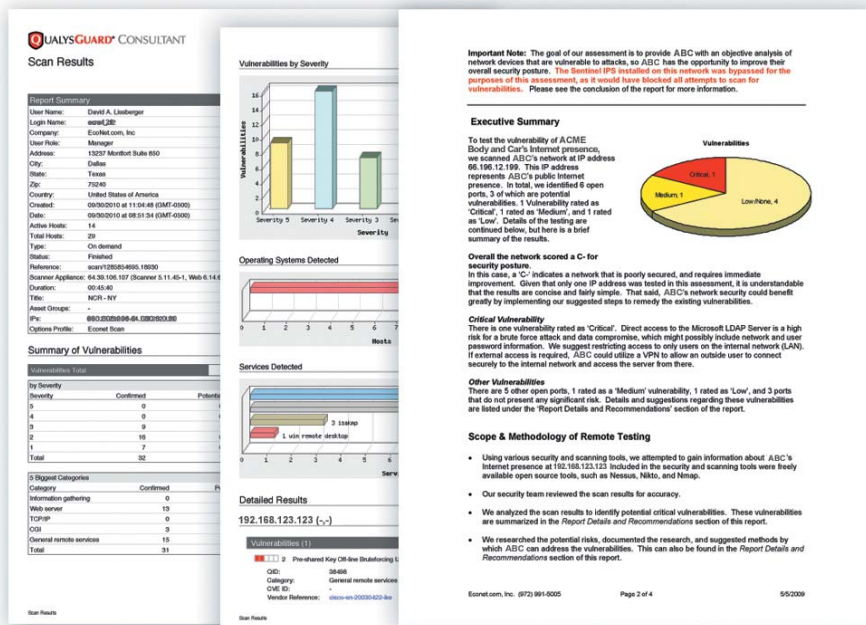
Simply put, our **Network Vulnerability Assessment** finds holes in your network, and our staff helps you determine the best way to plug them. It may be an open port on your firewall; or perhaps a service on one of your servers that hackers can easily exploit. Whatever the issue may be, our assessment can identify it, and determine how critical it is. Then, it's up to you to plug that hole, and we can help you with that, too.

Who needs it?

The obvious answer is 'everyone'. In reality, there are two types of companies for which this assessment is designed: Companies that want to know how vulnerable they are, and companies that are required by law to document their network and its vulnerabilities. In these situations, our assessment and the report that comes with it are perfect.

What are my options?

We offer this assessment as a one-time consultation, or as an annual subscription of either four quarterly or 12 monthly assessments. We also offer additional security consulting, if necessary. Please contact us directly for pricing.



UALYS GUARD CONSULTANT
Scan Results

Report Summary

User Name: David A. Lindberger
Login Name: david@abc.com
Company: Econet.com, Inc.
User Role: Manager
Address: 13237 Montfort Blvd 850
City: Dallas
State: Texas
Zip: 75240
Country: United States of America
Created: 09/30/2010 at 11:04:49 (GMT-0500)
Date: 09/30/2010 at 08:33:34 (GMT-0500)
Active Hosts: 14
Total Hosts: 29
Type: On-demand
Status: Finished
Reference: scan12020909010000
Scanner Appliance: 64.30.108.102 (Banner: 5.11.45-1, Web: 1.4.4)
Duration: 00:45:40
Title: NCR-NT
Need Group: -
IP: 89.233.248.86 (89.233.248.86)
Options Profile: Econet Scan

Summary of Vulnerabilities

Vulnerability Total		
By Severity	Confirmed	Potential
Critical	0	0
High	0	0
Medium	3	3
Low	18	18
Unrated	7	7
Total	32	32

By Severity Categories

Category	Confirmed	Potential
Information gathering	0	0
Web server	19	19
Exchange	0	0
CGI	3	3
Current remote services	18	18
Total	31	31

Vulnerabilities by Severity

Bar chart showing counts for Severity 5, Severity 4, Severity 3, and Severity 2.

Operating Systems Detected

Bar chart showing counts for various operating systems.

Services Detected

Bar chart showing counts for various services.

Detailed Results

192.168.123.123 (-)

Vulnerabilities (1)

Pre-owned Key Off-line (Unauthorized)

CVE: CVE-2009-3555
Category: General remote services
Weakness Reference: http://www.cve.org/CVE-2009-3555

Important Note: The goal of our assessment is to provide ABC with an objective analysis of network devices that are vulnerable to attacks, so ABC has the opportunity to improve their overall security posture. The SentinelIPS installed on this network was configured for the purposes of this assessment, as it would have blocked all attempts to scan for vulnerabilities. Please see the conclusion of the report for more information.

Executive Summary

To test the vulnerability of ABCME Body and Car's Internet presence, we scanned ABC's network at IP address 66.166.12.159. This IP address represents ABC's public Internet presence. In total, we identified 8 open ports, 3 of which are potential vulnerabilities. 1 vulnerability rated as 'Critical', 1 rated as 'Medium', and 1 rated as 'Low'. Details of the testing are continued below, but here is a brief summary of the results.

Overall the network scored a C- for security posture. In this case, a 'C-' indicates a network that is poorly secured, and requires immediate improvement. Given that only one IP address was tested in this assessment, it is understandable that the results are concise and fairly simple. That said, ABC's network security could benefit greatly by implementing our suggested steps to remedy the existing vulnerabilities.

Critical Vulnerability

There is one vulnerability rated as 'Critical'. Direct access to the Microsoft LDAP Server is a high risk for a brute force attack and data compromise, which might possibly include network and user password information. We suggest restricting access to only users on the internal network (LAN). If external access is required, ABC could utilize a VPN to allow an outside user to connect securely to the internal network and access the server from there.

Other Vulnerabilities

There are 5 other open ports, 1 rated as a 'Medium' vulnerability, 1 rated as 'Low', and 3 ports that do not present any significant risk. Details and suggestions regarding these vulnerabilities are listed under the 'Report Details and Recommendations' section of the report.

Scope & Methodology of Remote Testing

- Using various security and scanning tools, we attempted to gain information about ABC's Internet presence at 192.168.123.123. Included in the security and scanning tools were freely available open source tools, such as Nessus, Nmap, and Nmap.
- Our security team reviewed the scan results for accuracy.
- We analyzed the scan results to identify potential critical vulnerabilities. These vulnerabilities are summarized in the Report Details and Recommendations section of this report.
- We researched the potential risks, documented the research, and suggested methods by which ABC can address the vulnerabilities. This can also be found in the Report Details and Recommendations section of this report.

Econet.com, Inc. (972) 991-5005 Page 2 of 4 5/5/2009

What do I get?

We use the latest scanning tools to identify security vulnerabilities, track remediation and ensure regulatory compliance. Driven by the most comprehensive knowledge base in the industry.

Automates all steps of vulnerability assessment, management and policy compliance

Trusted, unbiased third-party security auditing and compliance reporting meets industry and regulatory compliance requirements.

Discover all assets across the entire network

Accurate and always up-to-date vulnerability audits

Easy-to-use, comprehensive reporting

Cost efficient with no hidden costs
Measurable TCO: 35% less than software solutions

Secure, with complete end-to-end data encryption