



## NETWORK VULNERABILITY ASSESSMENT

To compete in today's changing landscape, you look for more efficient and productive ways to bring products and services to market. Information technology can afford you these benefits; taking advantage of the new and exciting features IT offers can be paramount to your company's growth. However prior to taking on added resources, it's important to have an IT infrastructure that can readily respond to market forces. Your infrastructure needs to offer efficient management, ease of use, and adequate support for the latest advances in networking and server hardware while maintaining its integrity and security.

### Vulnerability Scan and Control Assessment

Accudata Systems can help you assess the security of your network infrastructure by performing a complete vulnerability scan and assessment at each network point of entry, including servers, infrastructure, and application components used for the exchange of information between employees, customers, and business partners. The assessment searches for both documented and undocumented points of entry; it reviews, documents, and tests them for accessibility, unauthorized access, and level of security.

We customize each vulnerability assessment to your specific IT environment and needs, but cover critical areas such as:

- Primary point of entry segments, such as external and internal segments, DMZs, and partner networks
- Remote site assessments
- Servers from primary datacenters
- Physical system access and social engineering
- Optional wireless security assessment
- Dial-up systems assessment
- Documentation of findings and recommendations
- Presentation of findings to increase management awareness

You get a holistic view of the current state of your network security and its vulnerabilities.

### Data Collection Tools and Methods

Accudata Systems uses a variety of state-of-the-art tools and methodologies for data collection during each vulnerability assessment. Along with hardware and software inventorying tools, firsthand data collection and a variety of automated tools and manual processes are used to document network systems. Additionally, we use custom scripts and procedures to assess your systems and networks.

### Optional Assessments

In addition to a comprehensive vulnerability assessment, Accudata Systems offers a number of optional assessments depending on your environment and your specific needs. These include:

- Internal & External Penetration Testing
- Denial of Service Testing
- Wireless Security Assessment
- Dial-up Systems Discovery and Review
- Enterprise Technical Security Controls & Tools Review
- Phone Switch and Unified Messaging Systems Vulnerability Review

### Recurring Assessments

Performing regular assessments, semi-annually or quarterly, can be extremely important to the security of your environment because it documents the state of your network against new systems or discovered vulnerabilities over a defined period of time. All processes, results, and recommendations – including prioritization metrics – are compiled in a formal document, stored, and compared to previous assessments to uncover persistent problems or new issues.

### Reporting and Documentation

Accudata Systems documents the results of the assessment and presents you with a full report of its findings. The report prioritizes your network vulnerabilities based on multiple risk and resolution levels, so you know immediately which systems are most vulnerable, the potential impact, and how difficult it will be to correct the problem. Additionally, the report recommends changes and best practices based on standards such as ISO 17799 and the SANS/ FBI Top 20 list, for achieving and maintaining a highly secure infrastructure.

**Sample Discovered Vulnerabilities Report**

RPT REF	VULNERABILITY NAME	RISK LEVELS			OVERALL RISK FACTOR	RESOLUTION LEVELS			RESOLUTION DIFFICULTY FACTOR	RISK : RES JUSTIFICATION FACTOR
		Business Impact Level	Probability Level	Threat Simplicity Level		Cost Level	Complexity level	Time Level		
G-3-1	Windows RPC Vulnerability	7	5	11	120	1	1	1	16	104
G-3-2	Windows NT Unauthenticated Sessions Discovered	5	4	10	95	2	4	6	57	38
G-3-3	Default SNMP Management Discovered	4	5	11	95	2	5	2	49	46
G-3-4	Web Cross Site Scripting Vulnerabilities	5	7	3	87	3	4	5	62	25
G-3-5	pcAnywhere Discovered	0	0	0	0	0	0	0	0	0
Category Average		5	5	9	99	2	4	4	46	53

**Assessment Category**  
The assessed area that contains the listed vulnerabilities.

**Vulnerability Name**  
The name or identification of each vulnerability that is discovered.

**Overall Risk Factor**  
An Accudata Systems generated metric that derives a single Overall Risk Factor from the three risk criteria of business impact, data sensitivity and threat simplicity.

**Resolution Difficulty Factor**  
An Accudata Systems generated metric that derives a single Resolution Difficulty Factor from the three resolution criteria of cost, complexity and time.

**Program Management**  
An Accudata Systems generated metric that helps prioritize which vulnerabilities to eliminate first by comparing Overall Risk Factor to Resolution Difficulty Factor.

**Category Average**  
The average values for the discovered vulnerabilities in this category.

**Risk Levels**  
Based on experience and client input, Accudata Systems rates each vulnerability according to these 3 risk criteria.

**Resolution Levels**  
Based on experience and client input, Accudata Systems rates each vulnerability according to these 3 resolution criteria.

**Sample Detailed Report**

Aspect Examined / Vulnerability Discovered

SECTION G-3-1 - Windows RPC Vulnerability

Overall Risk			Resolution Difficulty			Program Justification		
LEVEL	V	SCALE	LEVEL	V	SCALE	FACTOR	V	SCALE
Business Impact	7	Major	Cost	1	Normal	Overall Risk	120	High Risk
Probability	5	Corp. Std.	Complexity	1	Routine	Resolution Difficulty	16	Easy
Threat Simplicity	11	Simple	Time	1	Nominal	RISK:RES Justification	104	Considerable Upside

What is the overall risk of this vulnerability?

What is the overall difficulty involved in resolving this vulnerability?

What is the potential business impact if an event occurs?

What is the level of probability an event will occur?

What is the level of simplicity to create this event?

How expensive is it to resolve this vulnerability?

How complex is it to resolve this vulnerability?

How much time will it take to resolve this vulnerability?

What is the Risk to Resolution ratio? Is the vulnerability worth mitigating?