

# QualysGuard Sales Training for Partners & Resellers

*QualysGuard is a highly effective, simple-to-use, online service that instantly identifies and maps all of the IP devices on your Internet connection, analyzes the devices for potential security vulnerabilities, prepares reports on potential security risks, and helps you determine the most appropriate corrective measures. The service requires no installation, setup, hardware purchases, software development, security expertise or special training to use.*

# Agenda

- Overview
- QualysGuard Demo
- Qualys Sales Academy
- Q & A



# Overview

“  
*The Internet is like a vault with a screen door on the back. I don't need jackhammers or atom bombs to get in when I can walk through the door.*”

- anonymous

# Overview

- The “Penetrable” Network
- An Industry View
- The Challenge of Vulnerability Management
- The QualysGuard Solution



# *The Penetrable Network*

- They're getting in...
  - Grabbing confidential data
  - Disrupting or clogging servers (denial of service)
  - Defacing websites



# *It's a Serious Problem*

- **Most sites are compromised**
  - It's a moving target
  - New attacks are evident every day
- **E-Commerce opens new doors to hackers**
  - 70% have experienced a serious attack according to FBI survey
  - 42% have taken a direct financial loss



# *A Lucrative Vulnerability Market*

## ■ Losses need to be reduced

- ▶ Fortune 1000 companies sustained losses of more than \$45 billion in 1999 from the theft of proprietary information
- ▶ The average Fortune 1000 company reported 2.45 incidents with an estimated loss per incident in excess of \$500,000 -- 44 of 97 said they had more than 1,000 separate incidents



# *Solution Requires Ongoing Process*

- No cure -- only management
- Requires a continual process of testing and retesting
  - Constantly monitor points of access
  - Constantly monitor potential vulnerabilities
  - Constantly test for problems
  - Constantly worry





# *The QualysGuard Solution*

- **A Subscription Service that provides**
  - **Visual monitoring of access points**
  - **Gathering vulnerability data**
  - **Random or scheduled scanning for vulnerabilities**
  - **Secure reporting of problems with recommended fixes**



# Let's Take a Look...

## ■ Detailed demo in “Sales Academy”

The screenshot displays the QualysGuard web interface. At the top, there are navigation links for Home, Help, and Log Out, along with a COLT logo. The main content area is divided into three sections:

- Prioritized Vulnerability List:** A table with columns for IP, Vulnerability, and Severity.
- My Account:** A summary of account details including subscriber name, service option, contact information, and subscription status.
- Vulnerability News:** A list of recent security news items with dates and titles.

IP	Vulnerability	Severity
195.68.109.131	Girlfriend backdoor Brute Force Attack Remote SQL queries with MSADC	5
195.68.109.131	Remote Windows user list can be stolen Your system MAY BE Backdoored	4

<b>Subscriber:</b>	Heuristics, Inc.
<b>Service Option:</b>	Qualysguard Unlimited
<b>Your Contact:</b>	Kim MARTY (408) 747 6022
<b>IP in Subscription:</b>	4
<b>Add more IPs</b>	
<b>Previous Scan :</b>	August 18, 2000 at: 2:30 pm

**Vulnerability News** [More]

- August 18, 2000 - Sun Java Web Server Vulnerability
- August 17, 2000 - BB4 Technologies Big Brother Directory Traversal Vulnerability
- August 17, 2000 - Microsoft SQL Server Enterprise Manager Password Disclosure Vulnerability
- August 16, 2000 - Blackboard CourseInfo 4.0 Plaintext Administrator Password Vulnerability
- August 15, 2000 - Webmin Multiple SSL Session Requests Denial of Service Vulnerability
- August 14, 2000 - Microsoft SQL Server Enterprise Manager Password Disclosure Vulnerability

very  
simple  
interface

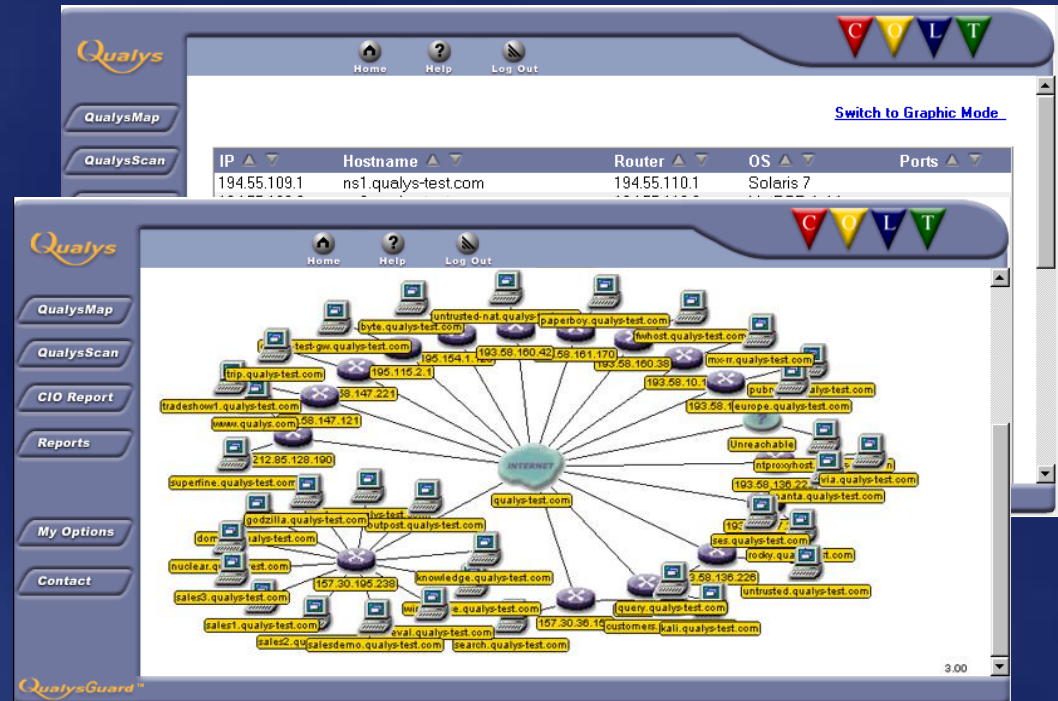
very  
clear  
answers



# Information Discovery: Topology

## ■ QualysMap network topology

- Text or Graphic
- Shows access points
- Rescan on a regular basis to identify security holes



# Vulnerability Scanning

## ■ Premier network diagnostic tool for administrators

- ▶ Severity levels
- ▶ Brief description
  - ◆ Drill-down for details

The image shows two overlapping screenshots of the Qualys web interface. The top screenshot displays the 'QualysScan' configuration page, which includes a navigation menu with 'QualysMap', 'QualysScan', and 'CIO Report'. The main content area contains a 'QualysScan' header, a description of IP address entry methods, and a form labeled 'Enter a range of IP addresses'. The bottom screenshot shows a 'Vulnerability Scan Report' page with a 'Delete' button and a 'Summary' table.

Summary	
Activity	Manual vulnerability analysis on 195.68.109.131
Date	08/15/2000 at 00:57:35
Duration	4 minutes 10 seconds
Customer ID	quaysn_pb
Company	qualys, inc.
Target Hosts	195.68.109.131
Active Hosts	1
Total Hosts	1
Reference	quaysn_pb/katana/2000.08.15.00:57:35
Scanner	195.68.109.142



# Drilling Down...

## ■ Specifics of the scan

- Diagnosis
- Consequences
- Solutions
- Results

The screenshot displays the QualysGuard interface. At the top, there are navigation links for Home, Help, and Log Out, along with a COLT logo. The main content area is titled 'VULNERABILITY REPORT' and shows the IP address '10.0.2.124'. A vulnerability is listed under the category 'netbios' with a severity of 4, indicated by four red bars. The vulnerability title is 'Remote Windows user list can be stolen'. The report includes a 'Diagnosis' section explaining that NetBIOS MS RPC access can be used to steal user lists, a 'Consequences' section describing potential attacks like brute force password cracking, and a 'Solutions' section suggesting to disable the GUEST account or restrict hosts. The 'Results' section lists the following user accounts: Administrateur, PSYCHOVIKING\$, and IUSR PSYCHOVIKING.

QualysGuard™



# Scanning Performance

- **Highly concurrent scanning**
  - ▶ Over 50,000 scans per hour
  - ▶ Typically 2½ minutes per IP
- **Runs tests specific to vulnerable resources**
- **Uses efficient vulnerability knowledge base**
- **Uses <30% of available bandwidth**



# Highly Confidential Reporting

- Targeted reports
  - Mapping & Scanning
  - CIO Report
  - Scan results delivered exclusively to the subscriber

