

# PENETRATION TESTING



WHEN YOU FINISH YOUR WORK,  
HACKERS JUST START THEIR NEW SHIFT...

**Penetration testing** simulates real attacks and verifies functionality of protection mechanisms under the working condition. Attacks can be led hidden or disclosed, within infrastructure or from the external environment of the IS, is focused on the particular object or all available systems as well as services from the existing environment, under predetermined conditions.

**Advantage of RAC penetration testing** is based on a highly professional attitude as well as expert background of the specialized and prestigious company, selection and loading of independent and highly specialized testing equipment as well as techniques. For proper testing is used primarily **QualysGuard®** technology with the largest available database of vulnerabilities and daily updates on the market. RAC always has a strict systematic approach to the solutions and compatibility with internationally established standards for ISMS and QMS.

## Competitive advantages of RAC

**RAC ISSEC:** methodology of practical and secure investigation in all phases of ISMS life-cycle.

**RAC CISS:** service of periodical and proactive testing as well as internet access protection.

**RAC QGVM:** service of design, implementation and support of ICT technologies' vulnerabilities administration process performed by QualysGuard®.

**QUALYS GUARD**

**PERIMETER DISCOVERY / MAPPING**  
Mapping identifies all network devices that can be seen from the Internet 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.

**Map Results**

**EXECUTIVE DASHBOARD**  
The Executive Dashboard provides a quick one-page, interactive, printable summary of your overall security posture. The dashboard displays user-configurable graphs and lists including: vulnerabilities by severity level, vulnerabilities by status, open tickets by severity level, top 10 vulnerabilities and your most vulnerable hosts.

**Home**

Dashboard Latest Vulnerabilities Account Info Resources

New Scan completed. Update in progress. Last Update: 05:32:27 PST

**Vulnerabilities by Severity Level**

Severity Level	Count
Level 5	35
Level 4	25
Level 3	15
Level 2	10
Level 1	5

**Vulnerabilities by Status**

Severity Level	Count
Level 5	48
Level 4	61
Level 3	80

**Open Tickets by Severity Level**

Severity Level	Count
Level 5	48
Level 4	20
Level 3	61
Level 2	80

**Top 10 Tickets**

Ticket #	Hostname	IP Address	Due Date	Owner
00023	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (qa_ys_cp)
00101	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (qa_ys_cp)
00115	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (qa_ys_cp)
00234	freezer.qa.qualys.com	10.10.10.2	12/15/2004	Willie Brown (qa_ys_wb)
00098	icebox.qa.qualys.com	10.10.10.23	12/15/2004	Son House (qa_ys_sh)
00103	icebox.qa.qualys.com	10.10.10.23	12/15/2004	Son House (qa_ys_sh)
00022	freezer.qa.qualys.com	10.10.10.2	12/16/2004	Willie Brown (qa_ys_wb)
00200	dairy.qa.qualys.com	10.10.1.54	12/16/2004	Robert Johnson (qa_ys_rj)
00212	fridge.qa.qualys.com	10.10.10.1	12/16/2004	Charlie Patton (qa_ys_cp)
00010	icebox.qa.qualys.com	10.10.10.23	12/20/2004	Son House (qa_ys_sh)

**Qualys Top 10 Vulnerabilities**

QID	Hostname
124655	Microsoft Phone Book Service Buffer Overflow Vulnerability
254780	Microsoft Windows Weak Mutex Permission Vulnerability
431289	Microsoft NTLMSSP Code Execution Vulnerability
457890	Microsoft WebDAV Service Provider Scripts Levy Vulnerability
053422	"ResetBrowser Frame" and "HostAnnouncement Frame"
725403	Microsoft Multiple LPC and LPC Ports Vulnerabilities
223495	Remote Registry Access Authentication Vulnerability
291348	Microsoft Reynolds Bin Creation Vulnerability
562344	Microsoft RDISK Registry Enumeration Vulnerability
345809	Microsoft Malformed RTSP Control Ward Vulnerability

**Most Vulnerable Hosts**

DNS Hostname	NetBIOS Hostname	IP Address	Asset Group	Last Scan Date	Business Impact	Security Risk	Business Risk
fridge.qa.qualys.com	ABC-Comp-local	10.10.10.1	Windows NT Machines, Marketing	07/15/2004	High	5	64
criper.qa.qualys.com	BCD-Comp-local	10.10.10.3	Windows NT Machines, Marketing	07/15/2004	High	4	38
freezer.qa.qualys.com	CDE-Comp-local	10.10.10.23	Linux 2.4, Dev	09/22/2004	High	4	36
icebox.qa.qualys.com	DEF-Comp-local	192.168.1.45	Marketing	08/01/2004	High	4	36
dairy.qa.qualys.com	EFG-Comp-local	10.10.1.54	Mail Servers	08/01/2004	Medium	3	9

# WE OFFER SECURITY TO YOUR SYSTEMS...

## Basic offer of penetration tests

RAC Company is prepared to perform testing according to the customer's individual needs by utilization of the basics of penetration testing:

### External environmental testing

- Investigation of a specified scope of the IP addresses
- Standard penetration testing
- Hidden penetration testing

### Internal environmental testing

- Testing within LAN/WAN/DMZ
  - Systems inaccessible from the internet
  - Verification of internet servers
- host-based testing
  - Local vulnerability of systems
  - Domain policy testing

### Wireless Wi-Fi networks testing

- monitoring of available Wi-Fi networks
- analysis of Wi-Fi functioning
- penetration testing of AP
- penetration testing of VPN entry points

### Regular penetration testing

- service RAC CISS

### Process of periodical administration of vulnerabilities

- service RAC QGVM

## Primary utilization of penetration tests

- Investigation and inventory control of a specified scope of the Internet IP addresses and acquirement of all available information about the specified scope.
- Detailed testing of all existing weaknesses and vulnerabilities of internet servers as well as other active facilities (routers and firewalls)
- Design of arrangements to recovery threats and vulnerabilities.

## Hidden penetration testing

- Is led without keeping network IT administrators nor an external company administering computer informed
- The purpose is to verify the preparedness and functionality of the reaction mechanism to an attack

## Internal environment testing

- Detailed testing of systems inaccessible from the Internet (DMZ, LAN) or a verification of a security of intranet servers and facilities by external penetration equipment
- Testing of local (host-based) vulnerabilities and domain policy setting (only some types of OS systems) are also elective

## Wireless Wi-Fi networks testing

- Wi-Fi segment monitoring and identification of all available Wi-Fi facilities
- Availability of Wi-Fi network within perimeter of an organization
- Detailed and complex testing of all existing prospective vulnerabilities detectable AP / VPN entry points



Risk Analysis Consultants, s. r.o.  
Španělská 2  
120 00 Prague 2  
Czech Republic  
+420 221 628 400  
rac@rac.cz  
www.rac.cz

Risk Analysis Consultants is a Czech based professional provider of information security services and solutions. We have assisted organizations from government and commercial sectors in protecting their information since 1995. We are the only firm exclusively specialized in the information security field in the Czech market, and one of the few in Europe and as well as the world.



QR code RAC