

# PENETRAČNÍ TESTOVÁNÍ



## KDYŽ MÁTE HOTOVO, HACKRŮM ZAČÍNÁ NOVÁ SMĚNA...

**Penetrační testování** simuluje reálné útoky a prověřuje funkčnost bezpečnostních mechanismů za provozu. Útoky mohou být vedeny skrytě nebo otevřeně, z vnitřní infrastruktury nebo z vnějšího okolí IS, zaměřené na konkrétní objekt nebo všechny dostupné systémy a služby z daného prostředí, za předem definovaných podmínek.

**Přednost penetračního testování RAC** spočívá ve vysoce profesionálním přístupu a odborném zázemí specializované a renomované firmy, výběru a nasazení nezávislých a vysoce specializovaných testovacích nástrojů a technik. Pro vlastní testování je použita především technologie **QualysGuard®** s největší dostupnou databází zranitelností na trhu a každodenní aktualizací. RAC vždy přísně dbá systémového přístupu k řešení a kompatibility s mezinárodně uznávanými standardy pro ISMS a QMS.

### Konkurenční výhody RAC

**RAC ISSEC:** metodika praktického, bezpečnostního zkoumání, ve všech fázích životního cyklu ISMS.

**RAC CISS:** služba periodického a proaktivního testování a zabezpečení přístupu na Internet.

**RAC QGVM:** služba návrhu, implementace a podpory procesu správy zranitelností ICT technologií realizovaná pomocí 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**

IP Information - wk1.frcorp.qualys-test.com

IP:	10.2.1.10
Domain:	frcorp.qualys-test.com
Status:	Reachable
OS:	Windows
Last Scan:	
Scanner:	

**QUALYS GUARD**

**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 tickets, 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	Vulnerabilities
Level 5	5
Level 4	4
Level 3	3
Level 2	2
Level 1	1

**Vulnerabilities by Status**

Severity Level	Count
New	48
Re-Opened	61
Active	80

**Open Tickets by Severity Level**

Severity Level	Count
Level 1	48
Level 2	20
Level 3	61
Level 4	80
Level 5	5

**Top 10 Tickets**

Ticket #	Hostname	IP Address	Due Date	Owner
00023	fridge.qa.qualys.com	10.10.10.1	12/15/2004	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	Wilde 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	12/15/2004	Wilde 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
124895	Microsoft Phone Book Service Buffer Overflow Vulnerability
254780	Microsoft Worddoc Weak Mutex Permission Vulnerability
431289	Microsoft NTLMSSP Code Execution Vulnerability
457890	Microsoft WebDAV Service Provider Scripts Levy Vulnerability
953422	'RealBrowser Frame' and 'HostAnnouncement Frame'
725403	Microsoft Multiple LPC and LPC Ports Vulnerabilities
323495	Remote Registry Access Authentication Vulnerability
257348	Microsoft Recycle Bin Creation Vulnerability
562344	Microsoft RDS/K Registry Enumeration Vulnerability
345806	Microsoft Malformed RTF Control Word Vulnerability

**Most Vulnerable Hosts**

QID	Hostname	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
	crisper.qa.qualys.com	BCD-Comp-local	10.10.10.2	Windows NT Machines, Marketing	07/15/2004	High	4	36
	freezer.qa.qualys.com	CDE-Comp-local	10.10.10.23	Linux 2.4, Dev	06/22/2004	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

## Základní nabídka penetračních testů

Společnost RAC je připravena realizovat testování dle individuálních potřeb zákazníků, s využitím těchto základních typů penetračních testů:

### Testování z vnějšího prostředí

- ▶ průzkum daného rozsahu IP adres
- ▶ klasické penetrační testování
- ▶ skryté penetrační testování

### Testování z vnitřního prostředí

- ▶ testování uvnitř LAN/WAN/DMZ
  - systémy nedostupné z Internetu
  - prověření intranetových serverů
- ▶ host-based testování
  - lokální zranitelnosti systémů
  - testování politik domény

### Testování wireless Wi-Fi sítí

- ▶ monitoring dostupných Wi-Fi sítí
- ▶ analýza Wi-Fi provozu
- ▶ penetrační testování AP
- ▶ penetrační testování VPN přístupových bodů

### Pravidelné penetrační testování

- ▶ služba RAC CISS

### Proces periodické správy zranitelnosti

- ▶ služba RAC QGVM

## Primární využití penetračních testů

- ▶ Průzkum a inventarizace přiděleného rozsahu internetových IP adres a získání všech dostupných informací o přiděleném rozsahu
- ▶ Detailní testování všech existujících slabín a zranitelností internetových serverů a dalších aktivních zařízení (routery a firewally)
- ▶ Návrh opatření k nalezeným hrozbám a zranitelnostem

## Skryté penetrační testování

- ▶ Je vedeno bez informování administrátorů IT nebo externí firmy spravující počítačovou síť
- ▶ Cílem je prověřit připravenost a funkčnost reakčních mechanismů na útok

## Testování z vnitřního prostředí

- ▶ Detailní testování systémů nepřístupných z Internetu (DMZ, LAN) nebo prověření bezpečnosti intranetových serverů a zařízení pomocí externího penetračního zařízení
- ▶ Volitelně i testování lokálních (host-based) zranitelností a nastavení politiky domény (pouze některé typy OS systémů)

## Testování wireless Wi-Fi sítí

- ▶ Monitoring Wi-Fi segmentu a identifikace všech dostupných Wi-Fi zařízení
- ▶ Dostupnost Wi-Fi sítě vně perimetru organizace
- ▶ Detailní a komplexní testování všech existujících potencionálních zranitelností detekovaných AP / VPN přístupových bodů



Risk Analysis Consultants, s. r. o.  
Španělská 2  
120 00 Praha 2  
Česká republika  
+420 221 628 400  
rac@rac.cz  
www.rac.cz

Risk Analysis Consultants je nezávislá poradenská společnost poskytující služby a řešení ve všech oblastech bezpečnosti informací v souladu s mezinárodními normami, související národní legislativou a respektováním individuálních podmínek klientů. Od roku 1995 pomáhá zajišťovat bezpečnost informací v informačních systémech organizací státní správy, bank, finančních institucí, telekomunikačních společností a průmyslových podniků v České republice i v zahraničí.



QR kód RAC