PENETRAČNÍ TESTOVÁNÍ

KDYŽ MÁTE HOTOVO, HACKRŮM ZAČÍNÁ NOVÁ SMĚNA...

Penetrační testování simuluje reálné útoky a prověřuje funkčnost bezpečnostních mechanizmů 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.

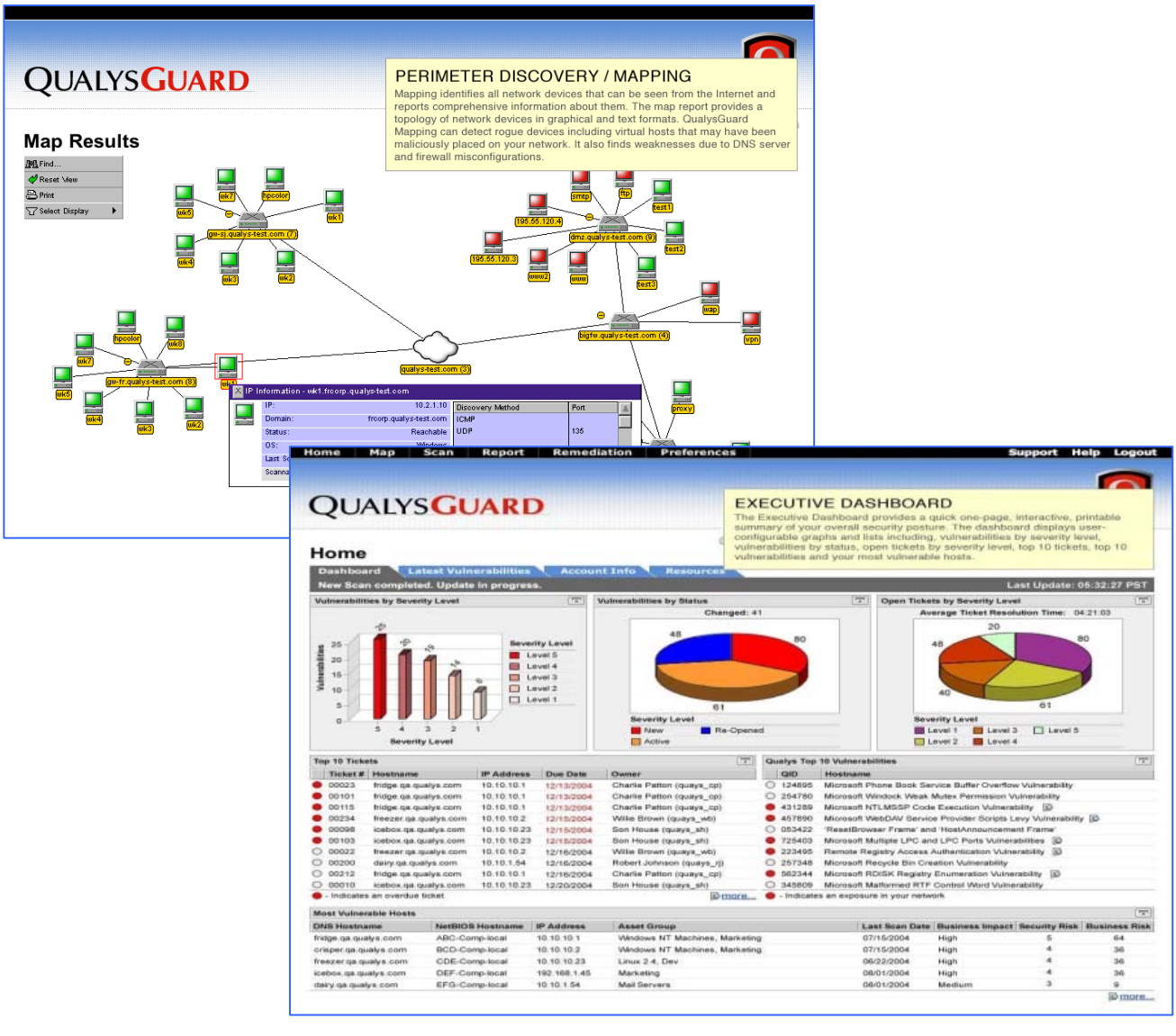
Přednost penetračního testování RAC spočívá ve vysoce profesionálním přístupu a odborném zázemí specializované a renomované firmy, výběru a nasazení nezávislých a vysoce specializovaných testovacích nástrojů a technik. Pro vlastní testování je použita především technologie ***QualysGuard®*** s největší 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®.***



NABÍZÍME BEZPEČNOST VAŠIM SYSTÉMŮM…

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 zranitelností

- 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 slabin 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 mechanizmů 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

V100521