IDC IT Security Roadshow Central and Eastern Europe

Penetrační test & bezpečnostní audit: Co mají společného? V čem se liší?

Karel Miko, CISA (miko@dcit.cz)

DCIT, s.r.o (www.dcit.cz)

DCIT

Penetrační test i bezpečnostní audit hodnotí bezpečnost předmětu šetření, který z nich si ale vybrat?

Obsah příspěvku:

- Co je penetrační test?
- Co je bezpečnostní audit?
- Průběh testu/auditu a použité metody
- Výstupy testu/auditu a jejich přínosy pro zákazníka
- Nejčastější nálezy a zjištění

DCIT

Penetrační test je zhodnocení bezpečnosti pokusem o průnik

- metodami i použitými nástroji blízký reálnému útoku (zvláště varianta „bez znalosti“) - Ethical Hacking
- je prováděn vzdáleně - po síti (z internetu - „externí“, z vnitřní sítě - „interní“)
- ve „skryté“ variantě prověří také monitorovací a reakční mechanizmy (dohled nad systémem)
- předmětem jednotlivá zařízení případně část sítě (speciálně např. WWW aplikace, Wi-Fi sítě aj.)
- jedním z hl. přínosů je využití kombinačních schopností odborníků - v tzv. „aktivní variantě“

Základní kroky penetračního testu

- rekognoskace - sběr informací o testovaném prostředí (registrované IP adresy, DNS domény, ...)
- zmapování prostředí na síťové úrovni - portscany, analýza filtrovacích mechanizmů, odhad topologie
- automatizované testy bezpečnostních slabin
- speciální testy zjištěných služeb (WWW, SMTP, …)
- manuální testy na základě výsledků aut. testů
- identifikace zranitelností - známé slabiny (CVE, CERT, BUGTRAQ) i nepublikované slabiny
- příp. praktická demonstrace zneužití slabin

DCIT

Výsledek penetračního testu Vám poskytne obrázek o tom, čeho by při současné úrovni znalostí mohl dosáhnout útočník při reálném útoku

- výstupem je nejen nález, ale i doporučení
- ani negativní výsledek testu nedává „jistotu“
- reálný útočník disponuje „neomezeným“ časem
- nástroje a metody jsou stále agresivnější
- znalost bezpečnostních slabin se neustále vyvíjí, řada existujících slabin nebyla doposud odhalena / zveřejněna (význam opakování)

DCIT

Nejčastější nálezy a jiné poznatky z praxe

- častá otázka: „Je to legální?“
- penetrační testy / hacking není mechanická záležitost
- zranitelný systém neochrání IDS ani správce u konzole
- bezp. slabiny nevznikají, existují již léta jen se o nich neví (v horším případě je znají jen někteří - „black-hat“)
- dobrá rada: systémy přístupné z Internetu by měly počítat s tím, že budou (resp. mohou být) napadeny
- obvyklé příčiny úspěšných průniků
  - defaultní nastavení, chybějící patche (rostoucí hrozba červů)
  - chyby v implementaci vlastních WWW aplikací
  - triviální hesla do systémů a aplikací
  - „security by obscurity“ u některých SW produktů

Bezp. audit je zhodnocení stavu bezpečnosti vůči vybranému etalonu

- s penetračním testem nelze srovnávat audit managementu inf. bezpečnosti (např. podle ISO17799)
- srovnáváme audit na technologické úrovni: servery, firewally, síťové prvky apod. (problém: volba etalonu)
- audit je prováděn fyzicky přímo na zkoumaném zařízení (např. serveru), nikoli po síti
- audit vyžaduje plný přístup ke zkoumaným zařízením, je prováděn za asistence administrátora
- audit je neinvazivní, časově relativně nenáročné šetření

DCIT

Základní scénář bezp. auditu (serveru)

- úvodní sběr informací o účelu zkoumaného zařízení (zpravidla interview s administrátorem)
- provedení technického šetření na místě
  - je prováděno přímo na serveru za asistence správce
  - je požadován plný přístup ke zkoumanému systému (tj. přístup pod privilegovaným uživatelem - root apod.)
  - 1. krok - automatizovaný sběr informací SW nástrojem (konfiguraci OS, WWW serveru, pošt. serveru, DB, …)
  - 2. krok - doplňkový manuální sběr informací
  - sběr informací je „pasivní“ - nedochází k modifikaci systému, není zkoumán obsah dat

Výsledkem bezpečnostního auditu je detailní zhodnocení konfigurace posuzovaného zařízení (server, firewall aj.).

- výstupem je nejen nález, ale i doporučení
- otázka volby etalonu - doporučení výrobců, nezávislých organizaci (NSA, CERT), zkušenosti z praxe
- audit do jisté míry spoléhá na bezchybnost systému opatřeného aktuálními updaty
- přestože při současné složitosti systémů je strojové zpracování nutné, není výrok auditu mechanickou záležitostí

DCIT

Nejčastější nálezy a jiné poznatky z praxe

- audit poskytuje vysokou míru detailu - obvykle nejsou podrobně zkoumána kompletně všechna zařízení
- zabezpečení dodávaných systémů není ani u renomovaných dodavatelů samozřejmostí (ti navíc často garantují funkčnost jen na „své“ konfiguraci)
- vhodná doba bývá překvapivě před spuštěním systému
- nejčastější identifikované problémy:
  - chybná nastavení plynoucí ze standardní konfigurace
  - zejména u interních systémů absence patchů (1 rok i více)
  - „pochybné“ požadavky některých SW na široká oprávnění
  - neodborné zásahy administrátora
  - důraz na funkčnost nikoli bezpečnost systému

Penetrační test vs. bezpečnostní audit

Názory se různí:

- 1. Extrém - negativní výsledek penetračního testu je nejvyšší možný stupeň jistoty zabezpečení zkoumaného systému
- 2. Extrém - penetrace (black-box) je nesystematický přístup, který v případě negativního výsledku vytváří pouze „iluzi“ o úrovni bezpečnosti

Pravda je někde uprostřed:

- ani audit ani penetr. test neposkytuje absolutní jistotu, oba se však mohou vhodně doplňovat
- lze nalézt příklady slabin, které audit odhalí a penetrační test nikoli (a naopak)

DCIT

Penetrační test vs. bezpečnostní audit

	penetrační test	bezpečnostní audit
metoda	pokus o průnik (po síti)	šetření na místě za asistence správce
cíl	zjistit míru zranitelnosti	komplexní analýza a zhodnocení
provedení	obvykle back-box testing	k dispozici plná informace o systému
rizika	možné omezení provozu	minimální (pouze pasivní šetření)
hl. přínosy	řekne: „jaký by byl zhruba výsledek reálného útoku“	návrhy zcela konkrétních změn nastavení jednotlivých parametrů
výhoda	ověření reakčních procesů	ideální podklad pro revizi nastavení
nevýhoda	zůstávají skryté problémy (průnikem test „končí“)	neodhalí implementační chyby (akt. verzi považuje za bezchybnou)
výstupy	členění dle zařízení a zjištěných slabin (1 závěrečná zpráva)	komplexní analýza „parametr-aktuální hodnota-doporučená hodnota“ (1 zpráva o každém zařízení)

Otázky

kontakt: Karel Miko, miko@dcit.cz

DCIT