Interpretace výsledků penetračních testů

Mgr. Karel Miko, CISA
miko@dcit.cz
DCIT, a.s., http://www.dcit.cz

ČIMIB

AGENDA

- K ČEMU BY (NE)MĚLY SLOUŽIT PENETRAČNÍ TESTY
- (NE)SPRÁVNÉ ZADÁNÍ PRO PENETRAČNÍ TEST
- VYPOVÍDACÍ HODNOTA PENTESTU -KDY (NE)PANIKAŘIT!
- PRÁCE S NÁLEZY
- BEZPEČNOST KONTRA FUKČNOST

ČIMIB

K ČEMU BY (NE)MĚLY SLOUŽIT PENETRAČNÍ TESTY?

- **K čemu rozhodně ANO**

- Především: Ověření reálné odolnosti systému
- Lze zhodnotit efektivitu procesů dohledu/monitoringu (ve variantě „přepadovka“)
- Může obsahovat netradiční metody (DoS útoky, trojské koně, sociální inženýrství, …)
- Lze najít chyby v „custom“ kódu (ty nejsou v globálních DB zranitelností)

- **K čemu rozhodně NE**

- Zkoumá jen to, co je zjistitelné po síti (nezhodnotí nastavení řady věcí „uvnitř“ systému)
- Nedává ucelený obraz o bezpečnosti systému
- Není vhodný pro testování izolovaných komponent
- Nenahrazuje code review
- Black-box varianta negarantuje prověření 100% systému (zejména u aplikací)

Co je penetrační test

- Vymezení pojmu penetrační test (pro jistotu)
  - Penetrační test je **posouzení úrovně bezpečnosti metodou pokusu o průnik** do testovaného systému / databáze / sítě / …
  - Zcela jednoznačně se jedná o **technickou formu posouzení** (auditu) bezpečnosti
  - Metodami i použitými nástroji **blízký reálnému útoku** (nejedná se o pouhé spuštění nástroje/scanneru)
  - Penetrační test má **mnoho variant** (interní, externí, aplikační, wifi, dialup, bluetooth, …)
- Občas bývá za penetrační test chybně považován Vulnerabity Assessment
  - Jedná o čistě mechanickou/strojovou záležitost (false-positives)
  - Neobnáší demonstraci nalezených slabin (stačí méně knowhow)

ČIMIB

(NE)SPRÁVNÉ ZADÁNÍ PRO PENETRAČNÍ TEST (1)

- Co je možné podrobit penetračnímu testu?
  - Testovat lze prakticky cokoli u čeho existuje riziko „nabourání“
  - Což často vede k megalomanským zadáním
  - Nutno balancovat šířku a hloubku testů (musí zadavatel)
  - Čím širší a/nebo hlubší tím dražší
- Prověřit penetračním testem veškerá zařízení?
  - U externího testu (z Internetu) – ANO
  - U interního: firma 60+ zaměstnanců – neefektivní
  - U interního: firma 200+ zaměstnanců – téměř nereálné
  - Nestačí zadat „naše interní síť = 100 serverů + 1000 stanic“
  - Je možné (a běžné) kombinovat penetrační test (detailní) s vulnerability assessmentem (pouze strojový)

ČIMIB

(NE)SPRÁVNÉ ZADÁNÍ PRO PENETRAČNÍ TEST (2)

- „Obyčejný“ pentest vs. pentest WWW aplikací
  - Dnes v podstatě samostatné disciplíny
  - V zadání penetračního testu je vhodné explicitně zmínit, zda je požadování důkladné prověření WWW aplikací
  - Zadání testu WWW aplikací je složitější (testovací účty, …)
  - WWW aplikace má smysl testovat jak z Internetu tak zevnitř
- Výsledky penetračních testů velmi rychle zastarávají
  - Pokud nezpracujete výsledky do cca 6 měsíců, významně ztratí na vypovídací hodnotě
  - Raději rozdělte test v čase do několika samostatných etap
- Zcela nesrozumitelné zadání
  - „Nabídněte cenu testu 1 IP adresy“ (my si to vynásobíme sami)

(NE)SPRÁVNÉ ZADÁNÍ PRO PENETRAČNÍ TEST (3)

- Rozsah testů lze omezit i časem
  - „Poptáváme specialistu na 3 dny on-site testů“ (ať se ukáže, kam se dostane)
  - Lze, ale musíme vědět, co chceme zjistit
  - Používá se zejména u obtížně ohraničitelných testů (např. test odolnosti velkých MS Windows prostředí)
- „Custom“ aplikace testovat při dodávce (před releasem)
  - Speciálně u WWW aplikací je penetrační test vhodné akceptační kritérium před spuštěním do provozu
  - Pozor: i menší upgrade může vnést do aplikace zásadní slabiny
- Testování „krabicových aplikací“
  - Poměrně běžně obsahují celkem závažné slabiny
  - Uvědomte si, že děláte práci (platíte) za výrobce SW

ČIMIB

VYPOVÍDACÍ HODNOTA PENTESTU
KDY (NE)PANIKAŘIT! (1)

- Penetrační test nemá z principu ambici dát úplnou informaci o stavu bezpečnosti
  - Nestačí mít 99% systému v pořádku, tester se snaží najít to 1% (v případě průniku je jedno, jestli bylo špatně 1% nebo 50%)
  - Tester postupuje cestou „nejmenšího odporu“ – pokouší se proniknout přes nejslabší místa (zbytek není až tak zajímavý)
  - V případě průniku obvykle test „končí“ (nelze vyloučit, že může existovat i další možnost napadení)
- Penetrační test není žádné teoretizování
  - Demonstrovaný průnik je obvykle tvrdá realita a lze jej jen velmi obtížně zpochybnit
  - Pokud se do systému naboural specialista (v řádu jednotek dní) může totéž dosáhnout např. technicky zdatný zaměstnanec

VYPOVÍDACÍ HODNOTA PENTESTU
KDY (NE)PANIKAŘIT! (2)

- Když test nic nenajde – buďte na pozoru
  - Buď je testovaný systém dobře zabezpečen nebo testy nebyly dostatečně důkladné
  - Např. tlak na cenu → omezení kapacit → menší detail testu
  - Obtížně zhodnotit, neboť obvykle není test s čím srovnat (paralelní test od různých dodavatelů není obvyklý)
  - Kvalita testera se srovnává obtížně
- Není nález jako nález
  - Pentest by neměl obsahovat „false-positives“nálezy
  - Vyžadujte ke každému nálezu doporučení (byť by mělo být částečně obecné)
  - Neděste se: někdy i na první pohled závažné nálezy lze akceptovat

PRÁCE S NÁLEZY(1)

- Nálezy je nutné kategorizovat
  - Základní ohodnocení nálezů podle závažnosti provede dodavatel (např. high, medium, low) – je to pouze jeho názor
  - Rozdělte si nálezy podle vlastních priorit, ty nemusí být identické s pohledem dodavatele
  - Zohledněte, které opatření budete implementovat vlastními silami (zohledněte své kapacity) a které přenesete na externisty
- Získejte maximum doplňujících informací
  - Prodiskutujte s dodavatelem praktickou zneužitelnost odhalených zranitelností, tester má často k dispozici pouze jeden úhel pohledu
  - Využijte specialistů (na konzultace/diskuze) dokud projekt běží, po podpisu akceptačního protokolu to bude obtížnější

PRÁCE S NÁLEZY(2)

- Ověřovací (nikoli opakované) testy
  - Pokud se s dodavatelem dohodnete předem, obvykle je schopen provést po opravách velmi rychlé ověření (1-2 člověkodny)
  - Obvykle nepotřebujete zopakovat celý test (pokud, tak s delším časovým odstupem)
- Nálezy a jejich opravy v aplikacích
  - Bývají nejnáročnější – nejedná se o úpravu nastavení nýbrž o změny v kódu (J2EE, .NET, …)
  - Ve většině případů nejste schopni vyřešit vlastními silami
  - Optimální je mít s dodavatelem smluvně podchyceno, že závažné bezpečnostní chyby odstraní jako reklamaci (koneckonců jste mu za své peníze našli defekty v jeho díle)

BEZPEČNOST KONTRA FUKČNOST

- Penetrační test si kupujete, aby chyby hledal (ne řešil)
  - Tester objektivně nemusí být schopen navrhnout správné řešení (nezná celý kontext, jeho specializace je chyby hledat)
- Najít slabinu je často jednodušší než ji napravit
  - Některá doporučení mají povahu „hraběcí rady“ (diskutujte je)
  - Ne každá nebezpečná věc se dá vypnout
  - Občas apriori odpor: „když to funguje, tak to nebudeme měnit“
- Všechny nálezy pentestu pravděpodobně nevyřešíte
  - U interního testu je téměř pravidlem
  - U starších aplikací bývají jakékoli změny obtížné
- Tradiční protipóly – funkčnost vs. bezpečnost
  - Business požadavky často proti bezpečnosti např. „neobtěžovat“ heslem, zavirovaný klient taky klient, …

Děkuji za pozornost

- Kontakt:
  - Karel Miko
  - DCIT, a.s.
  - miko@dcit.cz

- V případě zájmu:
  - Podrobnější informace a vzory výstupních zpráv interních i externích penetračních testů na požádání e-mailem