PENETRATION TESTING AS ACTIVE SECURITY CHECK ON

Radek BERAN

Abstract: In this paper I focus my attention on the issue of penetration testing, their advantages, disadvantages and possibilities to use them in the teaching process in computer science, information and communication technology. The results of the experimental penetration tests can help teachers make students acquainted with the possibility usage of active safety.

Key words: penetration testing, computer security

PENETRAČNÍ TESTOVÁNÍ JAKO AKTIVNÍ OVĚŘENÍ BEZPEČNOSTI

Resumé: V příspěvku se zaměřuji na problematiku penetračního testování, výhody, nevýhody a možnosti jejich použití při učebním procesu v oblasti Informatika a informační a komunikační technologie. Výsledky provedených experimentálních penetračních testů mohou učiteli pomoci seznámit studenty s možností využití aktivní počítačové bezpečnosti.

Klíčová slova: penetrační testování, počítačová bezpečnost

1 Úvod

V současnosti jsou studenti v rámci rozpracovaného rámcového vzdělávacího programu, ve vzdělávací oblasti "Informatika a informační a komunikační technologie", seznamováni s učivem zahrnující i témata údržba a ochrana dat. Nabývají znalosti v oborech antivirová ochrana, firewall, zálohování dat a dalších sférách počítačové bezpečnosti. Očekává se, že výslednými znalostmi bude znalý student, který účelně organizuje data a chrání je proti zneužití a poškození.

To je ovšem role pouze pasivní. Na druhou stranu penetrační testy jsou cestou aktivní, která otevře studentům povědomí o možnostech účinného cíleného prověření počítačové bezpečnosti.

2 Co je penetrační test?

Stručně a velmi obecně řečeno je to plánované a řízené použití současných útočných technik a taktik používaných pro průniky do bezpečnosti počítačových systémů nebo síťové infrastruktury, jejichž účelem je zjištění slabin v zabezpečení těchto systémů nebo infrastruktury. Penetrační testy bývají nazývány etickým hackingem. Vyžadují totiž stejné znalosti a schopnosti, jako používají hackeři, avšak s tím rozdílem, že nejde o následné zneužití chyby pro vlastní prospěch, ale o poučení se z ní a její nápravy.

Využívají a zjišťují se konfigurační chyby a další bezpečnostní mezery v ochraně. Výsledek penetračního testu udává aktuální informaci o stavu systémů a nabízí reálné ověření nastavené bezpečnostní politiky.

První penetrační testy se začaly provádět na počátku 90. let minulého století. Kvůli působení jednoho z prvních počítačových červů si obrovské množství uživatelů uvědomilo stávající křehkost počítačových systémů, jejich hodnotu i cenu dat v nich uložených, nedostatky i význam zabezpečení. Pro prověření systémového nastavení se začaly objevovat jednoduché nástroje, většinou se jednalo o množství různorodých skriptů, které prověřovaly lokální konfigurace systémů. V dnešní době je takovýchto nástrojů velké množství a jejich šíře záběru odpovídá vzrůstajícím potenciálním hrozbám.

3 Dělení provádění penetračních testů

Dále uvedené dělení penetračních testů není specifikované žádnou normou a vychází z nejčastěji používaného způsobu členění. Základní rozdělení útoků provedeme dle lokality, ze které útok přichází.

Vnější útoky jsou prováděny z prostředí internetu a jejich cílem je prověření bezpečnosti veřejně dostupných systémů. Například testování internetových aplikací, nejčastěji elektronických obchodů, elektronického bankovnictví, zkoušky odepření služby (DoS), mail servery a další.

Vnitřní testy jsou realizovány z prostředí uvnitř společnosti. Na kvalitní zabezpečení veřejně dostupných zdrojů z internetu bývá většinou myšleno a je mu věnována náležitá pozornost. Naproti tomu bezpečnost interních

systémů bývá ponechána na schopnostech a znalostech zaměstnanců firmy. Technická a bezpečnostní opatření organizací bývají v tomto ohledu příliš optimistická a nepředpokládají útok z vnitřní sítě. Důsledkem toho jsou neaktuální verze bezpečnostních záplat na produkčních serverech apod. Cílem útoku z vnitřní sítě je většinou snaha získat citlivá data za účelem profitu z těchto informací.

Pokud se v případě kvalitně prováděného vnějšího testu nezjistí žádné zásadní bezpečnostní riziko, bývá přistoupeno k využití sociálního inženýrství. Často se využívá neznalosti uživatelů, například podvodný e-mail nebo telefonát s cílem získat informace potřebné k provedení jiného typu útoku. Například požadavek na změnu hesla z důvodu testování systému, zaměstnancem „náhodně" nalezená USB paměť s automaticky spouštěným trojským koněm apod. Cílem interních testů může být také prověření chování zaměstnanců, ať administrativních, tak pracovníků IT oddělení.

Vnitřní i vnější testy mohou být prováděny ze dvou odlišných úrovní znalostí o testovaných systémech. Jedná-li se o tzv. white box test, má provádějící tester detailní znalosti o testované infrastruktuře, často zahrnující síťové diagramy, zdrojové kódy a IP adresy. Nezřídka je mu poskytnut i běžný uživatelský účet. Naproti tomu tzv. black box test simuluje útok testera, který o vnitřní infrastruktuře neví naprosto nic. Všechny potřebné informace musí zjistit sám.

4 Způsoby provádění penetračních testů

Podle toho, zda je cílem fyzické ověření možnosti penetrace do cílového systému či nikoliv, můžeme dělit metody testování do dvou velkých skupin:

- neprůnikové testy nebo analýzy zranitelností, jejichž cílem je identifikace přítomných zranitelností a posouzení jejich závažnosti, tj. možnosti zneužít dané zranitelnosti k útoku,
- průnikové nebo penetrační testy, kdy je nad rámec analýzy zranitelností provedeno fyzické ověření možnosti zneužít identifikované zranitelnosti k útoku vůči systému a identifikaci dalších slabin (např. přechod k dalšímu systému).

Při průnikových testech existuje podstatně vyšší riziko nežádoucích efektů – zastavení testované služby nebo restart serveru při přetížení. Náprava způsobených škod může být bez důkladných příprav mnohem nákladnější, než samotný penetrační test.

Naproti tomu provádění neprůnikových testů přináší zejména v interním prostředí jeden z nejefektivnějších postupů pro analýzu zranitelností. Počet nejrůznějších zařízení připojených do LAN je již u středních firem tak velký, že ověření všech identifikovaných zranitelností průnikovým testem bývá pro provozovatele příliš drahé nebo časově náročné. Využití automatizovaných nástrojů identifikujících pouze zranitelnosti je v takovém případě opodstatněné a skýtá vhodný přehled o úrovni zabezpečení prostředí. Tento typ testů je i vysoce účinnou formou sběru údajů pro ověření dodržování některých bezpečnostních pravidel (např. zda jsou do sítě připojena výhradně autorizovaná zařízení, provozovány jen autorizované služby, instalují se vyžadované bezpečnostní záplaty apod.). Pro ověření identifikovaných kritických hrozeb je následně možné využít provedení doplňkových penetračních testů.

5 Oblasti testování

Z hlediska penetračního testování, na které se zaměřuje především pozornost, definujeme tři následující oblasti:

- internetové technologie
- komunikační technologie
- bezdrátové technologie

Oblast testování internetové technologie představuje to, co většina lidí chápe pod pojmem penetrační testy. Do této oblasti patří například testování internetových aplikací, zkoušky odepření služeb (DoS) a systémová identifikace. Oblast prověrek komunikačních technologií zahrnuje kontrolu modemových připojení, ústředen a služeb VoIP. Bezdrátová technologie je zahrnuta jako součást obecné metodiky, do které je zahrnuta kontrola sítí 802.11, detekce bezdrátových systémů a technologie RFID.

6 Jak a čím testovat

Struktura a postupy použité při testování jsou často utajovanou záležitostí, většinou z důvodů ochrany dlouhodobě nabývaného firemního know-how. Z tohoto pohledu je zajímavá veřejně dostupná metodika The Open Source Security Testing Methodology Manual (OSSTMM), která systematickým způsobem mapuje oblast bezpečnostních testů. Primárním cílem metodiky OSSTMM je vytvoření pravidel pro rozhodování o tom, co se bude testovat, jak a kdy.

Nezávisle na použité metodice jsou základní kroky penetračních testů jednoduché:

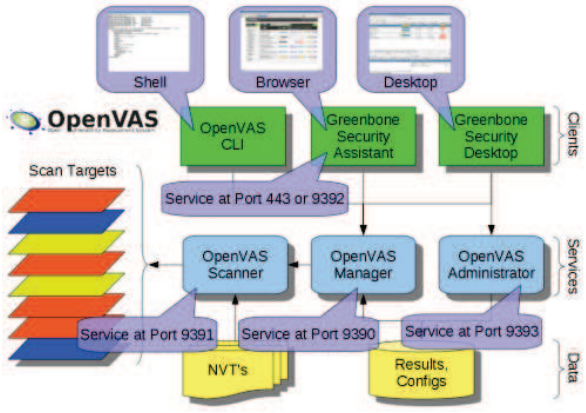
automatické skenování a následný manuální postup, specifický pro každého testera.

Automatické skenování patří mezi úvodní operace testování a někdy bývá mylně zaměňováno za vlastní penetrační testy. Primárním cílem tohoto kroku je vyloučení chyby lidského faktoru, konkrétně pak přehlédnutí již známých systémových nedostatků.

Poměrně jednoduše definovaný cíl přináší celou řadu úskalí. Obecné automatické bezpečnostní skenery musí pokrývat více operačních systémů, což prakticky znamená udržovat aktuální databázi bezpečnostních problémů. Dalším problémem je „inteligence" testů. Automatické bezpečnostní skenery by na náhodně objevené chyby měly reagovat podobně jako skutečný útočník. To je nesnadný úkol, ale někteří výrobci se s ním vypořádali velmi chytrým způsobem.

Například produkt Retina CS Management firmy eEye Digital Security (http://www.eeye.com/products/retina) je implementován pomocí technologie CHAM, která by umožnila nalezení i doposud neznámých chyb. Jedním z výstupů ISS X-Force je stále se aktualizující znalostní databáze bezpečnostních problémů, využívaná skenerem a dalšími produkty.

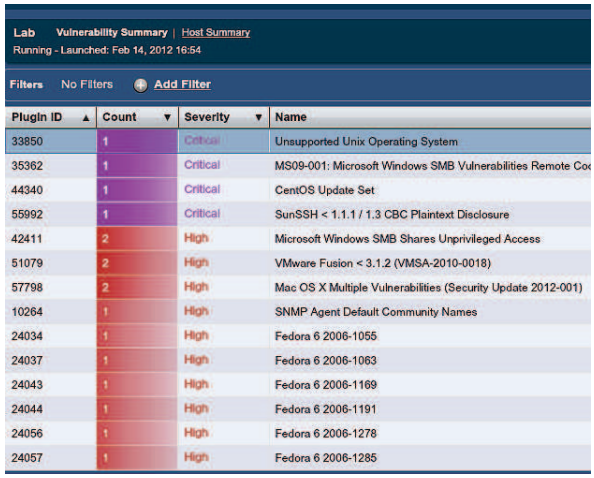
Z kategorie „open" softwaru je asi nejznámější program Open Vulnerability Assesment System (OpenVAS) (http://www.openvas.org). Jedná se o síťový bezpečnostní skener s příjemným uživatelským rozhraním v současnosti dostupný ve verzi 5 (květen 2012) pod GNU GPL licencí. Jde o soustavu několika služeb a nástrojů, které nabízejí komplexní a výkonný test zranitelnosti a řešení pro správu zranitelností. Počet využívaných modulů je více než 25 000 (květen 2012). Aktuálnost bezpečnostního skeneru je podpořena denními aktualizacemi z databáze



*(**Obr 1:** Schéma činnosti OpenVAS)*

Network Vulnerability Tests (NVT).

Program Nessus ve verzi 5 (květen 2012) (http://www.tenable.com/products/nessus), původně vyvíjený pod GPL, nyní zpoplatněný, je založen na architektuře „zásuvných modulů" (plugins), umožňující snadné rozšiřování prováděných kontrol. Vlastní skripty pro ověření bezpečnostní chyby lze programovat pomocí jazyka Nessus Attack Scripting Language (NASL) anebo jazyka C. V současné době je k dispozici cca 48 742 modulů (květen 2012). Všechny tyto moduly a pokročilé funkce skenování jsou placené. Pro domácí použití je ovšem k dispozici verze Nessus for Home s omezením na 16 IP adres, což je většinou pro domácí síť dostačující.



*(**Obr 2:** Přehled zjištěných zranitelností programem Nessus)*

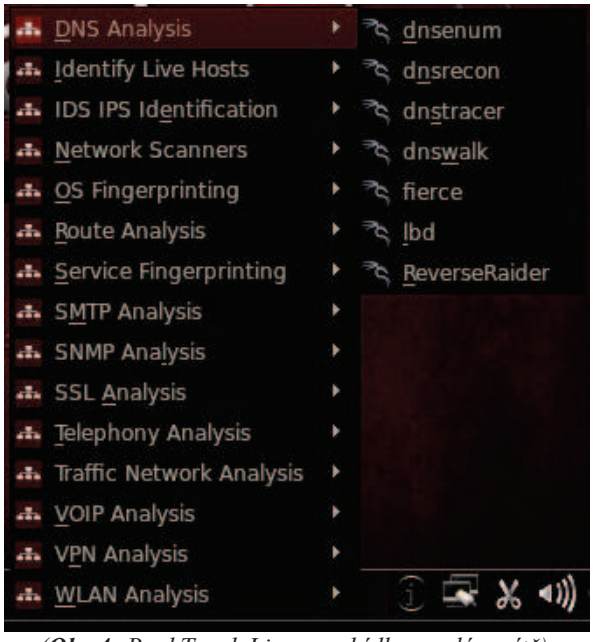
Řešení všechno v jednom firmy GFI s názvem GFI LANguard (http://www.gfi.cz/lannetscan) slouží pro skenování a audit sítě, detekce otevřených portů, vyhodnocení a nápravě bezpečnostních zranitelností, management bezpečnostních záplat operačních systémů i aplikací třetích stran a pro řešení několika dalších oblastí, které pro nás však v tuto chvíli nejsou klíčové.

V průběhu bezpečnostního auditu se oproti skenovaným IP provádí přes 15 000 bezpečnostních testů. GFI LANguard nabízí možnost provádět multiplatformní audit (Windows, Mac OS, Unix, Linux) napříč celým prostředím včetně virtuálních strojů. Umožňuje ověřit bezpečnostní nastavení a stav sítě.

Pro vytváření vlastních testů zranitelnosti nabízí systém průvodců i pro velmi komplexní testy. Skriptovací stroj je kompatibilní s jazyky Python a VBScript. GFI LANguard obsahuje i potřebné nástroje pro vývoj skriptů – Script editor a debugger.

Doposud představené produkty jsou určeny převážně pro provádění automatizovaných analýz zranitelností. Pro poslední fázi penetračního testování, pro skutečné ověření identifikovaných

*(**Obr 3:** BackTrack Linux, základní nabídka)*



*(**Obr 4:** BackTrack Linux, nabídka analýzy sítě)*

kritických hrozeb je velmi vhodná volně dostupná distribuce BackTrack Linux (http://www.backtrack-linux.org). Obsahuje velké množství skriptů a jednoúčelových programů na úrovni hackingu. Rozhodně není vhodný pro použití začátečníkem, protože spuštění skriptu může způsobit neočekávané chování kteréhokoliv z dotčených systémů. V rukou znalého testera však představuje neocenitelnou pomůcku při prověřování vytipovaných bezpečnostních problémů.

Distribuci je možné po stažení vypálit na CD, vytvořit bootovatelný flash disk nebo instalovat na notebook v režimu možnosti startu původního operačního systému (Microsoft Windows 7) nebo BackTrack Linuxu. Do těchto instalací je možné doplnit i některé výše zmíněné systémy, např. Nessus nebo OpenVAS.

7 Výhody a nevýhody penetračních testů

Výhody:

- při pečlivém a důsledném provedení poskytuje velmi přesné informace o skutečném stavu zabezpečení
- ukazuje slabá místa v systému a s tím spojená rizika
- kategorizace rizik umožňuje určit, které riziko je nejvyšší a je nutné jej řešit jako první
- jde o účinný způsob jak zajistit, aby byly minimalizovány úspěšné útoky na klíčové zaměstnance
- poskytuje nezávislý pohled na účinnost stávajících bezpečnostních procesů, zajišťující, aby instalace bezpečnostních záplat a správa konfigurace byly řádně prováděny

Nevýhody:

- není jednoznačným a stoprocentním důkazem o bezpečnosti nebo děravosti systému. Dnes provedený test nezohledňuje zranitelnosti odhalené zítra. Ne všechny zranitelnosti nebo způsoby jejich zneužití jsou veřejně známy.
- i přes důkladnou přípravu a velké nasazení odpovědného IT oddělení trvá zotavení systému po úspěšném provedení penetračního tetování určitou dobu
- není ekvivalentem postupu útočníka. Testující a útočník používají obdobné nástroje, jejich postupy a cíle jsou však podstatně odlišné. Útočník chce proniknout do systému teoreticky jakoukoliv cestou a postačí mu identifikovat jedinou zranitelnou cestu. Úlohou testujícího specialisty je komplexně a systematicky vyhodnotit všechny slabiny systému. Testující pracuje v rozsahu, čase a podmínkách stanovených v zadání a pravidlech. Útočník je v otázce přístupu k útoku a směru útoku absolutně neomezený.

8 Závěr

Vzrůstající počet nejrůznějších mobilních a jiných zařízení do stávajících systémů a zvyšující se informovanost jejich uživatelů by měla být alarmem pro správce a provozovatele. Ve veřejných zdrojích internetu jsou dnes pro hloubavé zájemce dostupné nejrůznější nástroje

a postupy. A nejsou úplně nezávadné. Neexistuje systém, který by nebyl něčím pro někoho zajímavý a je jen otázkou času a prostředků, kdy bude využit nebo zneužit. Penetrační testy nabízejí cestu, jak aktivně ověřit stav jejich zabezpečení.

9 Literatura

[1] MALINA, Richard, *Tajemství penetračních testů*. [online]. c2004 [cit. 2004-08-22]. <http://www.nextsoft.cz/~malina/cs/articles/pentesty/tajemstvi_pentestu.htm>.
[2] Wikipedia.org, *Penetration test* [online]. last revision 20th of April [cit. 2012-05-10]. <http://en.wikipedia.org/wiki/Penetration_test>.
[3] ADAMEC, Pavol; SALLER, Erik. Používat penetrační testy?. *DSM – data security management*, 2005, roč. 2005, č. 2, s. 10–13. Praha: TATE International, s.r.o., 2005- . ISSN 1211-8737.
[4] Wikipedia.cz. *BackTrack Linux* [online]. c2012, [cit. 2012-05-10]. <http://cs.wikipedia.org/wiki/BackTrack>
[5] WILHELM, Thomas. *Professional penetration testing: creating and operating a formal hacking lab.* Amsterdam: Elsevier, Syngress, 2010. ISBN 978-1-59749-425-0.
[6] HERZOG, Pete. *OSSTMM 3: The Open Source Security Testing Methodology Manual 3.0* [online]. 14. 2. 2010 [cit. 2012-05-10]. <http://www.isecom.org/mirror/OSSTMM.3.pdf>.
[7] GFI.CZ - GFI Česká republika & Slovensko. *GFI LANguard :: bezpečnostní skener, skener zranitelnosti, port scanner a patch management* [online]. c2011 [cit. 2012-05-10]. <http://www.gfi.cz/ lannetscan/>
[8] ISVS.CZ - Informační Systémy Veřejné Správy. *ISVS.CZ - Informační Systémy Veřejné - Penetrační testy - jak se provádějí a k čemu jsou? (1. díl)* [online]. 19. 11. 2007 [cit. 2012-05-10]. <http://www.isvs.cz/bezpecnost/penetracni-testy-jak-se-provadeji-a-k-cemu-jsou-1-dil.html>.
[9] ISVS.CZ - Informační Systémy Veřejné Správy. *ISVS.CZ - Informační Systémy Veřejné - Penetrační testy - jaké jsou jejich varianty a výsledky? (2.díl)* [online]. 20. 11. 2007 [cit. 2012-05-10]. <http://www.isvs.cz/bezpecnost/penetracni-testy-jake-jsou-jejich-varianty-a-vysledky-2-dil.html>.
[10] MIKO, Karel. *Co přinese a nepřinese za užitečné informace penetrační test* [online]. 2001 [cit. 2012-05-10]. <http://www.dcit.cz/cs/system/files/AFOI_2001_Miko.pdf>.
[11] GOLOMBEK, Kamil. Aplikační bezpečnost v plenkách. *DSM – data security management*, 2005, roč. 2005, č. 3, s. 14–17. Praha: TATE International, s.r.o., 2005- . ISSN 1211-8737.

Ing. Radek Beran
34. základna komunikačních a informačních systémů
Armáda České republiky
Dobrovského č. 6
771 11, Olomouc, ČR
Tel: +420 973 402 310
E-mail: radek.beran@seznam.cz, beranr@army.cz