Úvodní znalosti o hackingu a crackingu

Antonín Neumann

11. května 2013

Kapitola 1

Základní pojmy

Hacker

Hacker je počítačový specialista nebo programátor, který má detailní znalosti systému. Tento dokáže dokonale používat a dokonce si ho umí přizpůsobil podle svých potřeb. Často se tento termín zaměňuje s pojmem cracker, to ale není správné označení. Jako další možné označení hackerů je možné považovat „white hacker“ či lépe „white hat hacker“.

Cracker

Cracker je člověk, který své počítačové znalosti používá k průnikům do systémů za účelem škodit nebo ke svému vlastnímu prospěchu. Takový člověk má obsáhlé znalosti o bezpečnosti, fungování počítačů, kryptografii a podobně. Rovněž se můžeme setkat s označením „black hacker“ nebo přesněji „black hat hacker“.

Hacking versus cracking

Hacking se zabývá zkoumáním fungování systémů a procesů, které s tím souvisí. Hackerům jde především o získávání informací. Je pravda, že občas proniknou někam, kde nemají co pohledávat (například do systémů FBI apod.), ale vždy je to za účelem získání nějakých informací, které většinou dávají ve prospěch veřejnosti. Hacker má totiž často velmi odlišné chápání o proprietárního softwaru a utajování informací než většina světových zákonů. Často jsou také hackeři najímáni různými společnosti, aby odhalili a pomohli opravit bezpečností chyby v jejich softwaru nebo vnitrofiremních systémech.

Naproti tomu stojí cracking neboli prolamování, jak by mohl znít český překlad, který se zabývá především průnikem do systémů za účelem osobního prospěchu nebo získání větší moci. Může jít například o crackování her, aby šli hrát bez zakoupení originálního média, nebo o prolamování programů ke kterým je nutné si koupit licenci. Dalším druhem crackingu je ten odehrávající se online na síti, zde jde útočníkovi většinou o získání přístupových údajů k nějakým Vašim účtům, nejčastěji těm bankovním. Pro získání Vašich citlivých údajů cracker využívá mnoho technik jako například phishing, sociální inženýrství, XSS nebo Injection. Některé si dále podrobněji představíme.

Kapitola 2

Techniky průniků do systémů

Malware

Malware je souhrné označení pro skupinu programů, které slouží ke vniknutí, nakažení nebo poškození počítačového systému. Tento výraz je složeninou anglických slov pro zákeřný software (malicious software). Do této skupiny patří zejména trojské koně, počítačové viry a červy a různé druhy spyware a adware programů.

Trojský kůň

Jedná se o skrytou část programu (aplikace), s jejíž existencí a funkčností by povětšinou uživatel nesouhlasil. Název pro tento typ malware pochází z řecké mytologie o dobytí města Trója řeckou armádou.

Trojský kůň může být šířen jako samostatný program, například spořič obrazovky nebo jiný jednoduchý nástroj, a nebo může být přidán do již existující aplikace, například nelegální kopie nějakého software šířeného pomocí internetových fór nebo peer-to-peer sítí. Z tohoto důvodu velká část softwarových společností poskytuje ke svým produktům tzv MD5 hash, který ověřuje pravou identitu toho daného programu nebo aplikace.

Funkce trojských koní může být velmi různorodá, nejznámější jsou keyloggery, backdoor (zadní vrátka), spam server atd.

Trojské koně s funkcí zadních vrátek slouží ke zpřístupnění Vašeho počítače útočníkovi, ten na tom posléze může vydělat peníze tím, že z Vašeho počítače bude rozesílat nevyžádané obchodní e-maily nebo Váš počítač zapojí do nějakého botnetu za účelem pronajmutí k DDoS útoku. Trojský kůň se na rozdíl od počítačového viru nedokáže sám replikovat a dostat na další počítače nebo do jiných programů.

Počítačový virus

Počítačový virus je program, který se dokáže replikovat, tj. vytvářet kopie sebe sama tzv. potomky a ke své existenci potřebuje nějaký jiný soubor nebo program tzv. hostitele. Některé viry, respektive jejich potomci mohou být tzv. polymorfní, to znamená, že každá generace viru je trochu odlišná od té předchozí (potomek se liší od svého rodiče), čímž se může zhoršit jejich odhalitelnost různými antivirovými programy.

Virus může na infikovaném počítači vykonávat různé druhy úkonů, například mazat nějaké důležité soubory na disku, měnit jejich obsah atp. Ovšem moderní operační systémy dnes poskytují celkem dobrou ochranu v podobě administrátorských účtů a řízení uživatelský účtu tzv. ACL (Access Control List), kdy ke změně nějaké důležité části systému potřebujete administrátorská práva. Z tohoto důvodu se také doporučuje používat při běžné práci počítač jen s omezenými právy (toto se týká hlavně OS Windows, jelikož u Linuxu tento systém funguje již řadu let).

Virus se na rozdíl od počítačového červa, nedokáže sám šířit mezi počítači, tuto činnost musí vykonat, většinou nevědomky, sám uživatel a to zkopírováním nakaženého souboru nebo programu z jednoho počítače na druhý.

Počítačový červ

Je program, který je schopen automatického rozesílání svým kopií na jiné počítače. Po napadení systému převezme kontrolu nad síťovou komunikací a začne ji využívat ke svému šíření. Sekundární funkcí červa je většinou nést nějaký „náklad" (anglicky payload), který vykoná v napadeném počítači nějakou další činnost. Nejčastěji jsou jako náklad nošeny viry nebo trojské koně.

První počítačový červ, vytřený J. F. Schochem a J. A. Huppem, byl určený k monitorování vytížení procesorů počítačů připojených k síti a v případě nečinnosti jim zadat nějakou úlohu. Některé další červy odstraňovali jiný malware nalezený v počítači a stahovali bezpečností aktualizace opravující chyby v softwaru. Takže původním účelem červů nebylo škodit, ale spíše pomáhat.

Spyware a keylogger

Spyware je program sloužící k odesílání různých dat z počítače útočníkovy bez vědomí uživatele.

Keylogger je software (existují ale i hardwarové keyloggery), který snímá stisknutí jednotlivých kláves a ukládá je. Softwarový keylogger je většinou považován za druh spyware, jelikož bez odeslání stisknutých kláves, které zaznamenal, je téměř k ničemu. Existují ovšem i keyloggery, které uživatelé používají vědomě za účelem zjištění činností prováděných s počítačem během jejich nepřítomnosti.

Phishing

Phishing je typ útoku tzv. sociálního inženýrství, slovo pochází z anglického slova „fishing" neboli rybaření, protože nahodíte udičku (rozešlete zprávu) a čekáte kolik rybek se chytne (kolik uživatelů zadá své údaje).

Princip útoku spočívá v hromadném rozeslání zpráv, například e-mailem, ve kterých se účastník vydává nejčastěji za nějakou bankovní instituci nebo administrátora populární služba a informuje uživatele o nutnosti zadat nebo změnit jeho heslo u dané služby, případně cokoliv jiného, co uživatele přiměje k zadání svých přístupových údajů.

Ve zprávě je také uveden odkaz na stránky, které vytvořil sám útočník a má je pod svojí plnou kontrolou. Tato stránka je velmi často na první pohled k nerozeznání od oficiální stránky služby, které se útok týká.

Uživatel, domnívajíce se že je na oficiálních stránkách služby, zadá do formuláře svoje přihlašovací údaje, po odeslání formuláře útočník často přesměruje uživatele tentokráte na skutečné stránky služby, přičemž uživateli se zdá jako by se nic nestalo a zadá-li své přihlašovací údaje podruhé, normálně se ke službě přihlásí. Tím je pro něj záhada vyřešena a víc se tím většinou nezabývá. Zadáním přístupových údajů ještě na útočníkových stránkách ovšem dojde k jejich odeslání přímo do rukou útočníka, který s nimi poté může libovolně naložit.

Naštěstí tyto útoky pocházejí nejčastěji od zahraničních útočníků a překládají se za pomoci strojových překladů, které hlavně pro češtinu nejsou ještě stoprocentní a tak většina lidí při přijetí takové zprávy zpozorní a své citlivé údaje nikam nezadá.

XSS (Cross-site scripting)

XSS je metoda narušení webové stránky podstrčení vlastního JavaScriptového kódu za pomocí využití bezpečnostních chyb ve skriptech, především neošetření vstupních dat zadávaných uživateli. Ten typ útok můžeme rozdělit na dva typy, lokální nebo také nestálý (non-persistent) a stálý (persistent, stored).

Lokální typ útoku je založený na modifikaci URL adresy a zobrazuje se pouze na počítači, který vstoupil na stránku pomocí takto změněné URL adresy.

Perzistentní typ útoku změní data pro všechny uživatele, kteří si stránku otevřou. Činí tak nejčastěji ve spojení s databází, do které je útočníkům škodlivý kód neošetřený uložen a zobrazuje se tak při každém načtení stránky.

Zatímco první typ útoku většinou není nijak nebezpečný a používá se spíše k pobavení nebo zmatení uživatele, nejčastěji někoho známého. U druhého typu je to horší a v konečném důsledku může dojít k narušení bezpečnosti celé služby nebo ke ztrátě nějakých citlivých dat.

Zamezení těmto útokům není nijak složité, stačí jen důsledné ošetřovat všechny vstupy do aplikace tzv. escapováním. V PHP je k tomuto účelu funkce htmlspecialchars.

SQL Injection

SQL injection je podobně jako XSS útok, založena na podsunutí vlastního kódu (v tomto případě SQL dotazu) skrze neošetřený vstup. V tomto typu útoku může útočník použít a jakýkoli SQL dotaz, který databáze umožňuje.

Ukládá-li aplikace například komentáře od uživatelů do databáze a nemá ošetřený vstup proti SQL injection, může útočník místo svého vzkazu vložit do formuláře svůj SQL dotaz. Tento dotaz poté může z celé databáze zobrazit jakékoli informace, například veškeré informace o uživatelích, včetně jejich hesel, rodných čísel nebo jiných citlivých údajů a zobrazit je útočníkovi.

Ochrana před tímto typem útoku je opět velmi jednoduchá a to pomocí již zmíněného escapování. V PHP je k tomuto účelu připravená funkce mysql_real_escape_string.

DoS a DDoS útoky

DoS útok (anglicky Denial of service attack, česky odmítnutí služby) je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a pádu, nefunkčnosti nebo nedostupnosti služby pro ostatní uživatele.

DDoS (Distubuovaný DoS) útok je charakterizován zapojením většího množství počítačů najednou. Většinou je takový útok vedený z počítačů, které byli předtím nakaženy nějaký malwarem, takže uživatelé těchto počítačů vůbec netuší, že se takového útoku účastní.

Dnes asi nejčastějším typem DoS útoku je tzv. SYN flood. Tento typ zasílá na server mnoho TCP/SYN packetů (ty slouží pro zahájení komunikace mezi serverem a klientem) s padělanou hlavičkou odesílatele. Takovýto packet je serverem přijat jako běžná žádost o navázání připojení a server na něj odpoví TCP/SYN-ACK packetem a poté čeká na potvrzující TCP/ACK packet. Ovšem potvrzující TCP/ACK packet nikdy nedorazí, jelikož hlavička odesílatele byla falešná, žádost ovšem nějakou dobu blokuje ostatní legitimní žádosti o připojení. No a je-li takovýchto žádostí několik tisíc za sekundu vede to velmi rychle k přehlcení a pádu serveru načež se stává webová služba pro uživatele nedostupnou.

Existují také jiné typy DoS útoků jako například Nukes, Teardrop nebo Ping-flood.

Kapitola 3

Hackerský manifest

Předmluva

Esej Svědomí hackera (anglicky The Conscience of a Hacker) byla napsána 8. ledna 1986 Loydem Blankeshipem známým jak The Mentor. V současnosti je tato esej přeložena do mnoho ze světových jazyků a je zkopírována na bezpočtu internetových stránkách. Esej slouží jako náhled do filozofie hackerů ze 80. let, v současnosti hlavně jako průvodce začínajících hackerů. Text obhajuje myšlenky, že by technologie měly být využívány k rozšiřování našich obzorů a svět by měl zůstat svobodný.

Úvod

Hackerem se člověk nestane, narodí se jím.

Využíváme existujících služeb bez placení, mohly by být skoro zadarmo, kdyby nepatřily smelinářským hltounům, a vy nás nazýváte zločinci. My objevujeme... a vy nás nazýváte zločinci. Dychtíme po vědomostech... a vy nás nazýváte zločinci. Existujeme bez barvy pleti, bez národnosti, bez náboženských předsudků a vy nás nazýváte zločinci. Vy stavíte atomové bomby, vy vedete války, vy vraždíte, podvádíte a lžete nám a chcete, abysme (sic) věřili tomu, že je to pro naše vlastní dobro, přesto jsme my zločinci. Následující text byl napsán krátce po mém zatčení...

Mentor

Svědomí hackera

Dneska chytli dalšího. Jsou toho plný noviny. "Mladík odsouzen za Skandální Počítačový Zločin", "Hacker zatčen za průnik do banky"...

Zasraný děti. Všechny jsou stejný.

Ale zkusili jste se někdy s tou svou trojitou psychologií a technomozkem padesátejch let podívat očima hackera? Položili jste si někdy otázku, jaká síla ho zformovala, co vytvářelo jeho osobnost?

Jsem Hacker. Vstup do mého světa...

Můj život začíná školou... Jsem chytřejší něž většina ostatních děcek, ty kecy co nám vykládají mě nudí...

Zasranej flákač. Všichni jsou stejný.

Jsem na gymplu nebo na střední. Učitelka už po patnáctý vysvětluje, jak se krátí zlomek. Chápu to. "Ne, slečno Smithová, nepsal jsem postup. Udělal jsem to z hlavy..."

Zasraný děcko. Nejspíš to někde opsal. Všichni jsou stejný.

Dneska jsem udělal objev. Objevil jsem počítač. Počkej chvíli, to je skvělý. Dělá to, co chci. A když to udělá chybu, tak je to kvůli tomu, že jsem něco zvoral. A ne jenom proto, že mě nemá rád...

...nebo se cítí být mnou ohrožený...

...nebo si myslí, že jsem vychcanej parchant...

...nebo že nemám rád učení a neměl bych tu bejt...

Zasraný děcko. Furt jenom hraje samý hry. Všechny jsou stejný.

A pak se to stalo... otevřely se dveře do světa... elektronický signál se řítí telefonní linkou jako heroin žilou narkomana, nachází úkryt před ubíjející každodenností... nachází board.

"To je to místo... sem patřím..."

Každýho tu znám. I když jsem je v životě neviděl, nikdy jsem s nima nemluvil, a možná že už o nich nikdy neuslyším... Znám vás všechny...

Zatracený děti. Furt jenom obsazujou linku. Všechny jsou stejný...

Vsaď prdel, že jsme všichni stejný!

Ve škole jste nás krmili po lžičkách dětským jídlem a my chtěli steak... kusy masa, který k nám proklouzly byly předžvýkaný a bez chuti. Ovládali nás sadisti a ignorovali tupci. Bylo pár těch co nás mělo učit a našlo v nás ochotné žáky, ale těch bylo jako kapek vody v poušti.

"Toto je teď náš svět... Svět elektronů a spínačů, krása baudu. Využíváme existujících služeb bez placení, mohly by být skoro zadarmo, kdyby nepatřily smelinářským hltounům, a vy nás nazýváte zločinci. My objevujeme... a vy nás nazýváte zločinci. Dychtíme po vědomostech... a vy nás nazýváte zločinci. Existujeme bez barvy pleti, bez národnosti, bez náboženských předsudků a vy nás nazýváte zločinci. Vy stavíte atomové bomby, vy vedete války, vy vraždíte, podvádíte a lžete nám a chcete, abysme věřili tomu, že je to pro naše vlastní dobro, přesto jsme my zločinci.

Ano, jsem zločinec. Mým zločinem je zvědavost. Mým zločinem je posuzování lidí podle toho co říkají a co si myslí a ne podle toho, jak vypadají. Můj zločin je to, že jsem chytřejší než ty, což je věc, kterou mi nikdy neodpustíš. Jsem Hacker a toto je můj manifest. Můžete zastavit jednotlivce, ale nemůžete nás zastavit všechny... konec konců, všichni jsme stejní.

+++The Mentor+++[7]

Literatura

[1] http://phpfashion.com/escapovani-definitivni-prirucka

[2] http://php.vrana.cz/cross-site-scripting.php

[3] http://php.vrana.cz/obrana-proti-sql-injection.php

[4] http://www.panickov.esitex.com/clanky/hacking.html

[5] http://www.linuxexpres.cz/blog/hacker-vs-cracker

[6] http://www.techrepublic.com/blog/security/hacker-vs-cracker/1400

[7] http://blisty.cz/art/14662.html

[8] http://www.soom.cz/

[9] http://www.viry.cz/

[10] http://vtm.e15.cz/nejznamejsi-hackeri-sveta-zacali-utocit-jiz-v-detskem-veku

[11] http://www.fi.muni.cz/usr/jkucera/pv109/2003/xcerveny.htm

[12] http://www.security-portal.cz/clanky/kdo-je-hacker

[13] http://windows.microsoft.com/cs-CZ/windows7/Viruses-frequently-asked-questions