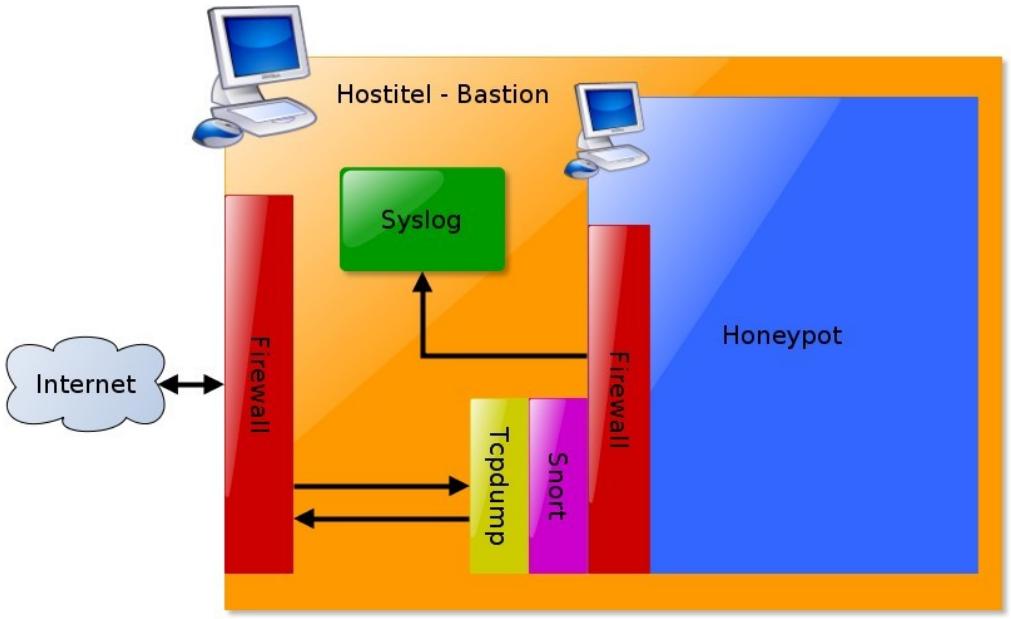
Honeypot na bázi linuxu

Softwarový projekt "Honeypot na bázi linuxu" je implementací vysoce interaktivního honeypotu. Jde o virtualizační prostředí, ve kterém je spuštěno několik virtuálních honeypotů čekajících na akce útočníků (především různých útoků směřujících na autentizaci). Tyto akce jsou důkladně zaznamenávány. Po detekci kompromitace virtuálního stroje je tento následně zastaven, uložen jeho obraz a na jeho místě spuštěna nová instance.



Navrhovaný honeypot je vysoce interaktivní a virtuální. jde o upravenou linuxovou distribuci, která je provozována ve virtualizovaném prostřední některého z volně dostupných virtualizačních nástrojů.

Pro využití v honeypotu je vhodná malá a rozšířená distribuce ve starší verzi (Debian 4.9 Etch v čisté instalaci zabíral 246 MB). Rozšířenost a starší verze zvětší šanci, že k této distribuci jsou známy bezpečnostní chyby a je pro útočníky lákavým cílem. Malá velikost je výhodná pro případné následné kontroly integrity souborů na systémovém disku.

Druhým krokem je výběr vhodných služeb, tak aby byly pro útočníka zajímavé a přitáhly jeho pozornost. Pro nasazení v honeypotu byly uvažovány čtyři základní služby a to webový server, ftp server a servery pro vzdálený přístup ssh a telnet. Tyto služby byly uvažovány zejména kvůli své rozšířenosti, kdy jednu či více takovýchto služeb provozuje téměř každý server a proto se tyto služby stávají velice často cílem útoků jak automatizovaných nástrojů, tak reálných útočníků.

Třetím krokem je upravení programů, služeb a konfigurace systému takovým způsobem, aby mohly být všechny aktivity v systému monitorovány a zaznamenávány. Při této modifikaci prvků operačního systému, je záměrně ponecháno několik bezpečnostních nedostatků tak, aby byla větší šance na přilákání útočníka a úspěšnou kompromitaci systému. Jako nejlepší způsob, jak výrazně oslabit autentizaci se ukázala možnost modifikace systému PAM. PAM je systém, který zajišťuje autentizační mechanizmy pro různé aplikace v systémů. Kompilace vlastního jádra je nezbytná kvůli nasazení

jaderného patche Grsecurity a jeho rozšířených možností pro audit systému.

Důležitou částí návrhu je volba nejvýhodnější virtualizační technologie. Pro možné nasazení honeypotu byly vybrány a otestovány tři řešení: QEMU + KVM, VMware Player a VirtualBox OSE.

Hostitel honeypotu obsahuje firewall. Tento firewall zaručí, že kompromitovaný systém honeypotu není pro okolí nebezpečný. Schéma navrženého systému je na obrázku. Klíčovým prvkem pro monitorování honeypotu je služba syslog. Všechny údaje ze sledování aktivit uvnitř v systému honeypotu jsou předávány do systémového syslogu. Ten je nakonfigurovaný tak, aby vše přeposílal na vzdálený syslog server spuštěný na počítači, který honeypot hostuje. Všechny zprávy tak jsou ukládány mimo honeypot a tím pádem mimo dosah útočníka.

Pro monitorování uvnitř honeypotu byly zvoleny nástroje Auditd a Grsecurity. Auditd i Grsecurity umožňují odesílat nasbíraná data do syslogu a jsou tedy pro nasazení optimální. Pro monitorování síťového provozu z vnějšku byl zvolen Tcpdump, spolu s nástrojem pro detekci síťových útoků Snort. Firewall přímo v honeypotu, který je také vidět na schématu, nemá mít žádné omezující pravidla a slouží pouze pro detekci skenování portů na honeypotu.

Literatura

Tomáš Mlčoch: Zachycení síťových útoků pomocí Honeypotů, bakalářská práce, Brno, FIT VUT v Brně, 2011

Popis konfigurace systému Honeypotu

```
#
# Pristupove udaje do systemu:
# root:hp123
# tomas:tomas123
#
# Pristupove udaje do redakcniho systemu Drupal: admin:administrator

#
# Instalace nezbytnych balicku
#

# Pokud by se pri instalaci objevil problem s chybejicim balickem,
# pridejte do souboru: /etc/apt/sources.list nasledujici dva radky:
# deb http://archive.debian.org/debian/ etch main non-free contrib
# deb-src http://archive.debian.org/debian/ etch main contrib
# Radky pridejte bez uvodniho znaku "#"
# A provedte update databaze prikazem:
apt-get update

apt-get install ssh
apt-get install telnet
apt-get install syslog-ng
apt-get install python
apt-get install apache2 libapache2-mod-php5 php5-common php5-sqlite

# Nyni nainstalujte dodane balicky:
# Napr pomoci prikazu: dpkg -i balicek.deb
#
# auditd_1.7.4-1_i386.deb
# bash_4.2-1_i386.deb
# libaudit0_1.7.4-1_i386.deb
# linux-headers-2.6.19.1-grsec_2.6.19.1-grsec-10.00.Custom_i386_minimal.deb
# linux-image-2.6.19.1-grsec_2.6.19.1-grsec-10.00.Custom_i386_minimal.deb
# openssh-server_4.3p2-9etch3_i386.deb
# pampython.deb
# proftpd_1.3.3c_i386.deb

#
# Nyni nakopirujte konfiguracni soubory na honeypot.
#

#
# Vytvorte na honeypotu nekolik falesnych uctu:
#

useradd salesman -c "Account for remote FTP access." --create-home --password
uldjfb1sA.kiA --uid 1005  # pass: 10ftpsales
useradd customer -c "Account for customer FTP access." --create-home --password
aNXysuveAPDzM --uid 1006  # pass: customer123
useradd admin -c "Account for FTP administration." --create-home --password
uX4iVNrmuD1UU --uid 1007  # pass: offspring-blink182
useradd boos -c "CEO" --create-home --password .suOjTQP1e1GA --uid 1010  # pass:
iamtheboos
useradd mpetr -c "1. Supervisor." --create-home --password 4KPOammLGXyDE --uid
```

```
1008  # pass: petr&p3tr
useradd knovak -c "2. Supervisor." --create-home --password 4KOQ7erIMZ2sHQ --uid
1009  # pass: 1975leden11
useradd pkalandra -c "3. Supervisor." --create-home --password 9wwuyqafp8HAI --uid
1012  # pass: kr1st1na
useradd accountancy -c "..." --create-home --password rRxJKs8mytH0. --uid 1011  #
pass: iK9aqE.d

#
# Zkopirujte na honeypot falesna data
#

# Zmente vlastniky falesnych dat v domovskych slozkach na odpovidajici uzivatele
# (Pokud jste data kopirovaly pod superuzivatelem, byl by vlastnik techo dat
# root a toto nechceme.)
chown -R salesman:salesman /home/salesman/*
chown -R customer:customer /home/customer/*
chown -R admin:admin /home/admin/*
chown -R boos:boos /home/boos/*
chown -R mpetr:mpetr /home/mpetr/*
chown -R knovak:knovak /home/knovak/*
chown -R pkalandra:pkalandra /home/pkalandra/*
chown -R accountancy:accountancy /home/accountancy/*

# Zmente vlastnika a skupinu pro webove stranky
chown -R www-data:www-data /var/www/*

#
# Restart pocitace
# Pri novem startu by se melo nastartovat nove jadro s grsecurity.
#

# Odstraneni stareho jadra
aptitude purge linux-image-2.6.18-6-686 linux-image-2.6-686

# Odstraneni nepotrebnych balicku
aptitude purge netcat usbutils manpages man-db logrotate libc6-i686 tasksel
tasksel-data laptop-detect installation-report eject ed dselect dmidecode acpid
acpi info groff-base

# Smazani nepouzitych locale souboru
apt-get install localepurge
localepurge
aptitude purge localepurge

# Odstranit osirele balicky
apt-get install deborphan
deborphan | xargs apt-get -y remove --purge
aptitude purge deborphan

# Uklizeni balickovaci cache
apt-get clean
aptitude clean
rm /var/cache/apt/pkgcache.bin
rm /var/cache/apt/srcpkgcache.bin

# NastavenÃ syslog.conf jako nezmÄ›nitelnÃ½ a nesmazatelnÃ½
chattr +iu /etc/syslog.conf
```

```
# Nastavit init skripty, aby se spoustely po startu systemu
chmod 755 /etc/init.d/aptitude-log
update-rc.d aptitude-log defaults

chmod 755 /etc/init.d/dpkg-log
update-rc.d dpkg-log defaults

chmod 755 /etc/init.d/auditd-rules
update-rc.d auditd-rules defaults

chmod 755 /etc/init.d/firewall
update-rc.d firewall defaults

#
# V poslednich krocich byly pridany inicializacni skripty, ktere se
# spusti po startu systemu. Proto system restartujte.
#

# Nastaveni spravne casove zony
# Pouze v pripade, ze jste nastavili spatnou casovou zonu behem instalace a
# vadi vam posunuty cas v zaznamech syslogu.
# tzconfig
```

OPEN SOURCE LICENCE VUT V BRNĚ
Verze 1.

INSTALACÍ, KOPÍROVÁNÍM NEBO JINÝM POUŽITÍM SOFTWARE POTVRZUJETE, ŽE SOUHLASÍTE S PODMÍNKAMI TÉTO LICENČNÍ SMLOUVY. POKUD S TĚMITO PODMÍNKAMI NESOUHLASÍTE, SOFTWARE NEINSTALUJTE, NEKOPÍ-RUJTE ANI NEPOUŽÍVEJTE. JESTLIŽE NEMÁTE PLATNOU LICENCI NA SOFTWARE, NEJSTE OPRÁVNĚNI SOFTWARE INSTALOVAT, KOPÍROVAT ANI JINAK POUŽÍVAT.

Definice:

Software se pro účely této smlouvy rozumí počítačový program (skupina počítačových programů tvořící jeden funkční celek) schopný autorskoprávní ochrany a s ním související dokumentace.

Dílem založeným na Software se pro účely této smlouvy rozumí dílo, které obsahuje zcela nebo jen zčásti Software nebo jakoukoli jeho část, popřípadě je ze Software nebo jeho části odvozeno. Na části díla schopného samostatné-ho užití, které neobsahují žádnou část Software ani nejsou ze Software odvozeny, se tato definice nevztahuje, pokud jsou šířeny samostatně.

Zdrojovým kódem se pro účely této licence rozumí veškerý zdrojový kód pro všechny moduly, které Software nebo dílo na něm založené obsahuje, plus jakékoli další soubory pro definici rozhraní, plus dávkové soubory potřebné pro kompilaci a instalaci spustitelného programu. Zvláštní výjimkou jsou však ty programové komponenty, které jsou normálně šířeny (buď ve zdrojové, nebo binární formě) s hlavními součástmi operačního systému, na němž spustitelný program běží (tj. s překladačem, jádrem apod.).

Každý, kdo použije Software, stává se **Uživatelem**. Uživatel se zavazuje dodržovat tyto licenční podmínky.

VUT V BRNĚ UDĚLUJE UŽIVATELI LICENCI K UŽÍVÁNÍ SOFTWARE ZA NÁSLEDUJÍCÍCH PODMÍNEK:

1. Uživatel smí užívat Software zdarma pro vlastní potřebu k jakýmkoli účelům.

2. Uživatel smí kopírovat a šířit doslovné kopie spustitelného Software a zdrojového kódu Software tak, jak jej obdržel, na libovolném médiu, za předpokladu, že na každé kopii viditelně a náležitě zveřejní zmínku o autorských právech a absenci záruky, ponechá nedotčené všechny zmínky vztahující se k této licenci a k absenci záruky a dá každému příjemci spolu se Software kopii této licenční smlouvy. Za fyzický akt přenesení kopie může Uživatel žádat poplatek a podle vlastního uvážení může nabídnout za poplatek záruční ochranu.

3. Uživatel může modifikovat svoji kopii či kopie Software anebo kterékoliv jeho části, a tak vytvořit dílo založené na Software, a kopírovat a rozšiřovat takové modifikace či dílo, pokud jasně uvede, že se jedná o modifikované dílo. Tyto modifikace či dílo lze licencovat pouze za podmínek čl. 2 těchto licenčních podmínek, bez ohledu na to, zda jsou šířeny samostatně nebo ve spojení s jiným dílem.
Ustanovení předchozí věty se však nepoužije na díla, která jsou pouhým spojením jiného díla, jež není na Software založeno, se Software nebo dílem založeným na Software na paměťovém nebo distribučním médiu.

4. Kopie Software nebo díla na něm založeného v objektové anebo spustitelné podobě musí Uživatel:
a) doprovodit zdrojovým kódem ve strojově čitelné formě. Zdrojový kód musí být rozšiřován podle ustanovení čl. 2, a to na médiu běžně používaném pro výměnu programového vybavení; nebo
b) doprovodit písemnou nabídkou nejméně na tři roky, podle níž poskytne Uživatel jakékoli třetí straně, za poplatek nepřevyšující výdaje skutečně vynaložené na fyzickou výrobu zdrojové distribuce, kompletní strojově čitelnou kopii odpovídající zdrojovému kódu, jenž musí být šířen podle ustanovení čl. 2 na médiu běžně používaném pro výměnu programového vybavení; nebo

c) doprovodit informacemi, které dostal ohledně nabídky na poskytnutí zdrojového kódu. (Tato alternativa je povolena jen pro nekomerční šíření a jenom tehdy, pokud Uživatel obdržel program v objektovém nebo spustitelném tvaru spolu s takovou nabídkou, v souladu s písmenem b výše.)

5. Uživatel nesmí kopírovat, modifikovat, poskytovat sublicence anebo šířit Software jiným způsobem než výslovně uvedeným v této licenci. Jakýkoli jiný pokus o kopírování, modifikování, poskytnutí sublicence anebo šíření Software je neplatný a automaticky ukončí práva daná touto licencí. Třetí osoby, které od Uživatele obdržely kopie anebo práva v souladu s touto licencí, však nemají své sublicence ukončeny, dokud je jejich chování v souladu s těmito licenčními podmínkami.

6. Pokud nemůže Uživatel šířit Software tak, aby vyhověl zároveň svým závazkům vyplývajícím z této smlouvy a jiným platným závazkům, nesmí jej v důsledku toho šířit vůbec.

7. Uživatel není odpovědný za vymáhání dodržování podmínek této licence třetími stranami.

8. VZHLEDEM K BEZPLATNÉMU POSKYTNUTÍ LICENCE K SOFTWARE SE NA SOFTWARE NEVZTAHUJE ŽÁDNÁ ZÁRUKA, A TO V MÍŘE POVOLENÉ ZÁKONEM. POKUD NENÍ PÍSEMNĚ STANOVENO JINAK, POSKYTUJE VUT V BRNĚ SOFTWARE "TAK, JAK JE", BEZ ZÁRUKY JAKÉHOKOLIV DRUHU, AŤ VÝSLOVNÉ NEBO KONKLUDENTNÍ, VČETNĚ, ALE NEJENOM, ZÁRUK ZA KVALITU A VÝKONNOST SOFTWARE, ZA PRODEJNOST A VHODNOSTI PRO URČITÝ ÚČEL.
VUT V BRNĚ V ŽÁDNÉM PŘÍPADĚ NEODPOVÍDÁ ZA ŠKODY, VČETNĚ VŠECH OBECNÝCH, SPECIÁLNÍCH, SKUTEČNÝCH NEBO UŠLÉHO ZISKU VYPLÝVAJÍCÍCH Z UŽÍVÁNÍ ANEBO NESCHOPNOSTI UŽÍVAT SOFTWARE (VČETNĚ ALE NIKOLI JEN, ZTRÁTY NEBO ZKRESLENÍ DAT, NEBO TRVALÝCH ŠKOD ZPŮSOBENÝCH VÁM NEBO TŘETÍM STRANÁM, SELHÁNÍ FUNKCE SOFTWARE V SOUČINNOSTI S JINÝMI SOFTWARE, NEBO V PŘÍPADĚ, ŽE PROGRAM PORUŠUJE PRÁVA TŘETÍCH OSOB), A TO I V PŘÍPADĚ, ŽE VUT V BRNĚ VĚDĚLO O MOŽNOSTI TAKOVÝCH ŠKOD, TO VŠE V NEJŠIRŠÍ MOŽNÉ MÍŘE POVOLENÉ ZÁKONEM.

Závěrečná ustanovení:

Nevynutitelnost anebo neplatnost anebo neúčinnost kteréhokoli ujednání této smlouvy neovlivní vynutitelnost anebo platnost anebo účinnost jejích ostatních ustanovení.

Tyto licenční podmínky poskytují stejný rozsah licenčních oprávnění jako licenční podmínky GNU GPL licencí a Software splňuje podmínky pro označení Open Source Software.

Otázky touto smlouvou neupravené včetně otázek jejího vzniku a zániku se řídí českým právem.

V případě soudního sporu budou příslušné české obecné soudy.

Instalací, kopírováním nebo jiným použitím Software Uživatel prohlašuje, že se s obsahem této smlouvy důkladně seznámil, že je souhlas s touto smlouvou projevem jeho skutečné, vážné, svobodné a určité vůle prosté omylu a že není uzavřena v tísni za nápadně nevýhodných podmínek.

tel.: 54114 1144, fax: 54114 1270 E-mail: info@fit.vutbr.cz, Web: http://www.fit.vutbr.cz/