Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Honeypot a jeho možnosti zvýšení zabezpečení serveru

Marek Šišák

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Šišák Marek

Informatika

Název práce

Honeypot a jeho možnosti zvýšení zabepečení serveru

Anglický název

Honeypot as security function on server

Cíle práce

Bakalářská práce je zaměřena na téma Honeypot a jeho možnosti zvýšení zabezpečení. Hlavním cílem práce je seznámení se a charakteristika Honeypotů. Dále se pak práce zaměří na analýzu možností zvýšení zabezpečení.

Metodika

Metodika bakalářské práce je založena na studiu a analýze odborných informačních zdrojů.

Harmonogram zpracování

1.Příprava a studium odborných informačních zdrojů, upřesnění cílů a volba postupu řešení 10/2013
2.Zpracování přehledu řešené problematiky 11 - 12/2013
3.Vypracování vlastního řešení, diskuze a zhodnocení výsledků 2/2014
4.Tvorba finálního dokumentu bakalářské práce 2 - 3/2014
5.Odevzdání bakalářské práce a teze 3/2014

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Honeypot a jeho možnosti zvýšení zabezpečení serveru" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 16.3.2015 _____

Poděkování

Rád bych touto cestou poděkoval Alexandru Vasilenkovi za užitečné rady, s jejichž pomocí mohla práce vzniknout a Tomáši Jaklovi za poskytnutí veřejné adresy, na kterou byl honeypot umístěn.

Honeypot a jeho možnosti zvýšení zabezpečení serveru

Honeypot as security function on server

Souhrn

Bakalářská práce se zaměřuje na problematiku honeypotů. Představuje tato zařízení, ukazuje jejich varianty a možnosti, kterak je dělit do skupin, či spojovat do sítě Honeynet. Dále se zabývá analýzou výsledků konkrétního honeypotu Kippo a popisuje možnost zvýšení zabezpečení serveru.

Summary

The bachelor thesis is focused on issues of honeypots. The thesis explains these tools and shows its variations. It also suggests options, how to divide them into groups or connect them to a network, called Honeynet. In addition it analysis results of a specific Honeypot Kippo and describes the possibility for server security improvement.

Klíčová slova: Honeypot, Kippo, Honeynet, Malware, SSH server, IP adresa

Keywords: Honeypot, Kippo, Honeynet, Malware, SSH server, IP adress

Obsah

1. Úvod

V dobách kolonizace nových vzdálených území se k přesouvání informací, věcí a financí využívaly lodě, které se plavily po oceánech a mořích. Samozřejmě se okamžitě našlo hodně osob, které se chtěly tohoto nákladu zmocnit. To ovšem nebylo v zájmu majitelů a ti začali svůj majetek chránit.

Od této doby uplynulo mnoho let. Přišla Průmyslová revoluce, která odstartovala technologický vzestup. Díky tomu se informace nebo peníze dostávaly přes velké vzdálenosti stále rychleji. Plachetnice nahradily parníky, parníky byly nahrazeny letadly a vznikl také zcela nový způsob přenosu informací a to s pomocí telekomunikačních zařízení.

Dnes přináší nejrychlejší možnosti přenosu, ať už údajů nebo financí, celosvětová síť Internet. Jejím používáním se lidem ulehčuje život a každým rokem se tudy přepraví stále vetší množství méně, či více důležitých informací. Uživatelé mají ve svých počítačích uloženy různé osobní údaje, které mohou být zneužity a proto je nutné, je chránit. Stejně jako dřív dochází i dnes k útokům pirátů, kteří se mohou k cizímu majetku dostat novou cestou prostřednictvím počítačových sítí. Každým rokem jsou jejich techniky vyspělejší a částka vydávána na protipirátskou ochranu se celosvětově zvyšuje. Počítače jsou nyní již nedílnou součástí lidských životů a zneužití některých informací může vést k fatálním následkům.

Počítačoví piráti jsou vždy o krok napřed. Aby mohla být vytvořena ochrana proti postupům a technikám, jež používají, musí být nejdříve jejich praktiky odhaleny. Podobně, jako kouzelník neprozradí svůj trik, tak ani hacker nemá zájem na odhalení svých tajemství. Jak ale přinutit člověka s nekalými úmysly, aby prozradil jaké postupy používá? Nejjednodušší možností je sledování zmíněných nežádoucích kroků. Sledování je ale možné pouze v případě, že už je pachatel znám. Nejlepším způsobem je tedy vytvoření pasti, do které je útočník nalákán. Ve světě informačních technologií představují tuto past honeypoty.

Správná past musí mít návnadu a způsob, kterým svůj cíl zachytí. Jako návnada je použito něco, po čem útočník touží, v IT tedy například přístup na nějaký server, webová aplikace nebo síťová služba. Návnada se tváří, jako běžná služba, kterou představuje. Ve chvíli, kdy na ni pachatel narazí, je důležité získat jeho zájem a zároveň nevzbudit podezření, pak už stačí, aby na návnadu skočil. V tom okamžiku je možné začít studovat pachatelovo chování.

Získané informace poté budou sloužit k pochopení postupů a vytváření nejrůznějších obranných zařízení, bojujících v nekonečné bitvě proti zlým úmyslům.

2. Cíl a metodika

Práce se zabývá nežádoucí aktivitou směrovanou z internetu na server či lokální počítač. Hlavním cílem práce je seznámení se s honeypoty, otestování jednoho konkrétního, konečná analýza získaných výsledků a možnosti dalšího postupu pro zvýšení bezpečnosti.

V první části je analyzována problematika nežádoucí aktivity v systému, protože pokud má být popisováno zařízení vytvořené na shromažďování údajů o nežádoucích aktivitách, je nutné si nastínit jejich varianty. Po definování výrazu Malware a popsání jeho některých příkladů, následují kapitoly věnované honeypotům samotným. V nich je vymezeno, co přesně jsou a jaký účel mají, je nahlédnuto do jejich historie, kterak se z jednoduchých malých programů vyvíjely v plnohodnotná zařízení, obsahují možnosti jejich rozdělení podle nejrůznějších kritérií a závěrem jsou představeny příklady konkrétních řešení. V poslední části kapitoly teoretických východisek jsou ještě zmíněny architektury honeynetů a požadavky, které na ně jsou kladeny.

Praktická část popisuje vytvoření podmínek pro umístění honeypotu Kippo na SSH server, jeho následnou instalaci, spuštění a konečné zhodnocení nasbíraných výsledků v číselné i grafické podobě. Dále nabízí řešení vysledovaného problému.

Metodika je založena na studiu odborné literatury zejména z internetových zdrojů uvedených v seznamu literatury. Většina teoretických poznatků je čerpána ze starších zdrojů, protože jejich struktura se nezměnila.

3. Teoretická východiska

Pro pochopení smyslu počítačové ochrany je dobré seznámit se s nežádoucími prvky, před kterými je nutné systém bránit. Uživatel může svůj počítač nebo informace v sítích vystavit nepříjemnostem zejména vinou neopatrnosti. Pokud své PC nechrání aktuálními antivirovými programy, nemůže se pak divit, že si z internetu odnáší nejrůznější typy škodlivého softwaru. Stejně tak, jako když je moc důvěřivý a nedá si pozor na to, komu dává své citlivé informace. Veškerý škodlivý software je sjednocen ve výrazu malware, naopak techniky, jež mají za cíl vylákávat z lidí informace psychologickými metodami, shrnuje pojem sociální inženýrství.

S vývojem metod škodlivých se ruku v ruce vyvíjí i metody obranné. Proti virům a škodlivému softwaru má každý svědomitý uživatel ve svém počítači antivirový program. Ty jsou nyní již na takové úrovni, že si jejich práce osoba pracující na PC ani nevšimne. Aby se na tuto úroveň dostaly, musela se ujít dlouhá cesta, spočívající ve sledování aktivit ohrožujících počítačové systémy.

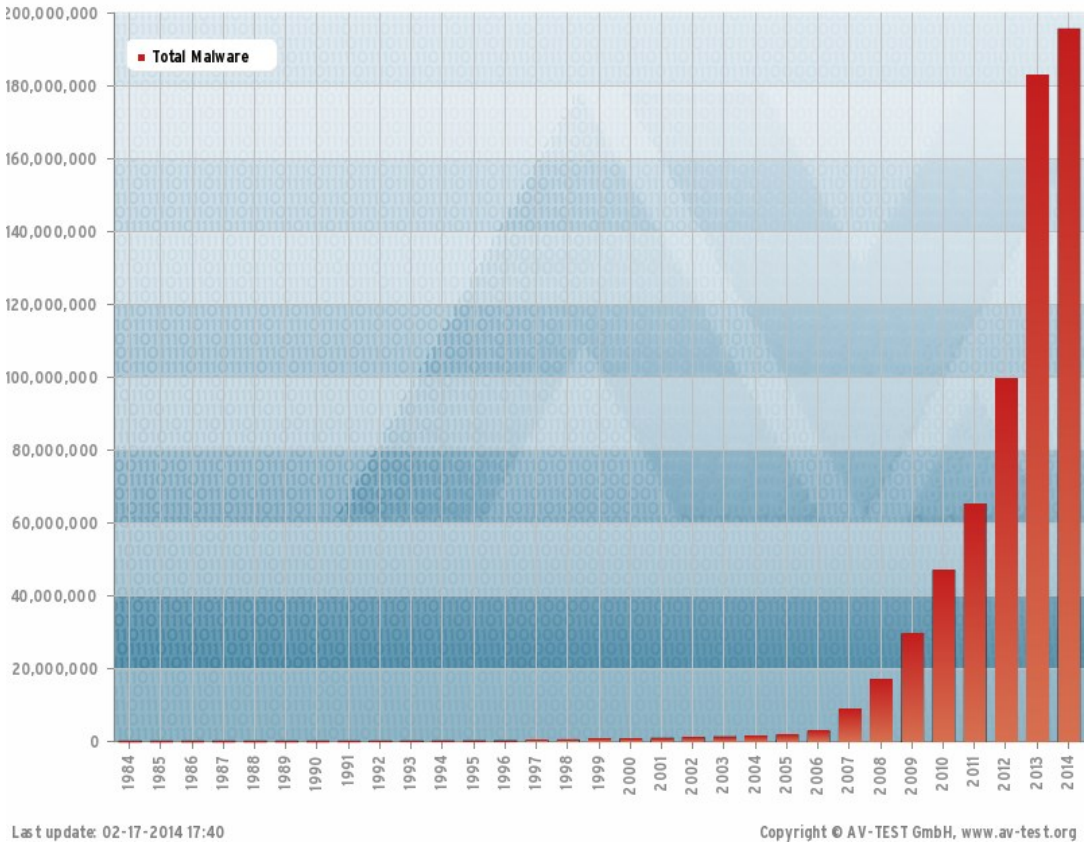
Honeypoty byly a jsou dobrým pomocníkem pro sběr těchto informací. Největší užitek z nich mají právě antivirové společnosti, které jejich prostřednictvím objevují nové druhy útoků, malwaru nebo trendů mezi komunitou útočníků. Z dob 90. let, kdy sledování útoku bylo něco až tajemného a první záznam dal dokonce vznik detektivnímu románu popisujícímu hon na kyberzločince, se honeypoty dostaly do fáze, ve které si je může vyzkoušet každý. Musí si ovšem dobře uvědomovat rizika, která s sebou sledování něčeho nebezpečného přináší.

3.1 Malware

Výraz malware v sobě skrývá kombinaci dvou anglických slov malicious software (zákeřný software). Sjednocuje všechny počítačové programy, které mají za úkol infiltrovat se do počítače uživatele a následně v něm provádět nevyžadovanou činnost bez uživatelova vědomí.

Vznik malwaru je velice nevinný. V raných dobách informačních technologií se někteří programátoři rozhodli otestovat svoje dosavadní schopnosti a zároveň také poškádlit své kolegy. Ze zvědavosti nebo pro zábavu, tak vytvářeli první programy s negativními procesy. Malware zpočátku neměl velký význam, programy ve většině případů nebyly distribuovány a zanikaly. Postupem času si lidé se špatnými úmysly začali uvědomovat možnosti, jak využít nežádoucí software ke svým nekalým účelům. Zjistili, že jeho prostřednictvím lze získat cenné informace z počítačů obětí nebo poškozovat data nic netušících uživatelů. [7]

Dnes se tento zákeřný software nejčastěji využívá ke krádežím osobních informací, jako jsou ověřovací údaje pro online bankovní transakce, čísla kreditních karet, sociálního pojištění nebo hesla. [7] Množství malweru stoupá exponenciální řadou (viz. Obr. 1) a v roce 2014 překonalo hodnotu 200 milionů aplikací.



Obr. 1: Rozšíření malware aplikací (1984-2014)[8]

Viry

Počítačové viry fungují stejně, jako viry biologické. Jedná se o parazitický program, který modifikuje zdrojový kód napadeného programu a vkládá do něj kopie sebe sama. Fakticky virus ovšem není plnohodnotný program, protože ke svému fungování potřebuje hostitele. Jakmile je hostitelský program spuštěn, virus se tváří, jako jeho součást a začne vykonávat svou činnost. Bez antivirových prostředků je identifikace viru velmi těžká, může se projevit například zabráním místa v paměti a to je ta nejmenší škoda, kterou může napáchat. V horším případě může ničit data, shromažďovat údaje infikovaného uživatele anebo jeho prostřednictvím rozesílat nežádoucí e-maily/spamy. Viry lze dělit podle typu hostitelů, činnosti nebo způsobu šíření. Rezidentní viry se šíří v okamžiku spuštění hostitele, kdežto nerezidentní čekají na svou příležitost v operační paměti a infikují soubory, se kterými uživatel až do vypnutí počítače pracuje. [9]

Červi

Počítačový červi se podobají počítačových virům, stejně jako oni se replikují a jejich cíle jsou stejné. Oproti virům mají tu výhodu, že ke svému působení nepotřebují žádný hostitelský program. Sítí se šíří pomocí paketů, jakmile infikují daný systém, snaží se z něj infiltrovat do dalších systémů, to může mít za následek přehlcení přenosové sítě. Název červi dostali podle toho, že pro svou činnost využívají bezpečnostní mezery (chyby) v systému. [10]

Trojští koně

Na rozdíl od červů a virů trojští koně neovládají schopnosti replikace. Technika jejich působnosti se vyznačuje tím, že se tváří, jako žádoucí programy, které mohou mít pro uživatele přínos. Když dojde k situaci, že oběť program spustí, trojský kůň začne páchat svou nežádoucí činnost. Trojští koně nemohou infikovat ostatní programy, ale mohou být nositeli virů, či červů, kteří to dokážou. Tyto programy se nejčastěji snaží svým obětem poškodit data, vylákat z nich citlivé informace (čísla kreditních karet, bankovní údaje, hesla), šířit jejich prostřednictvím spamy a v poslední řadě také k sledování jejich

činnosti. [10] O to mají zájem reklamní agentury, které poté ze získaných informací zjistí, jaký produkt můžou danému člověku nabídnout.

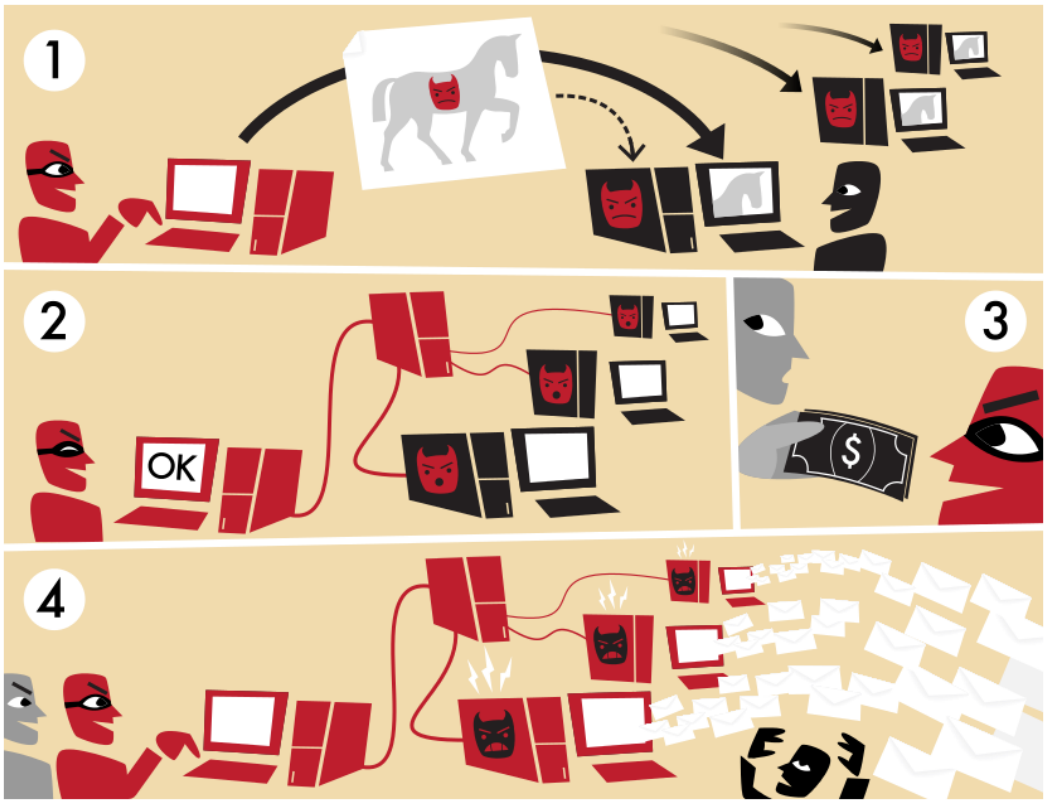
Boti

Boti, odvozeni od robotů, vykonávají v napadeném systému automatizovanou činnost, která má za následek, že jejich majitel může převzít kontrolu nad infikovaným počítačem. Sjednocují se do sítí dalších napadených PC nazývané Botnet, která může čítat až několik tisíc počítačů. [10]

Jedním z prvních botů byl GM (game manager), ten vzniknul vcelku zajímavou cestou. Skupina finských programátorů, stojící za vznikem jednoho z nejstarších komunikačních serverů v reálném čase: Internet Relay Chat (IRC), hledala způsob, jak si zahrát logickou textovou hru Hunt the Wumpus, bez nutnosti hledání živého hráče. Správce serveru Greg Lindahl tedy naprogramoval bota, který poskytoval své herní služby na diskusním kanále IRC. [32]

Správce vytvoří botnet skrze (C&C) servery napojené na příhodný komunikační kanál. Pomocí příloh e-mailů nebo závadných webových stránek nakazí vzdálené počítače a tím de facto jeho práce pro danou chvíli končí. Botnet funguje, jako služba k pronájmu, takže další činnost nastartuje až v momentně, kdy si tuto síť k rozesílání spamu nebo DDoS útoků[1] objedná někdo, kdo stojí o podobné záležitosti. Všechnu černou práci odvádějí napadené počítače nic netušících uživatelů. Nejúspěšnější botnety mají na svědomí desítky milionů nakažených PC. Jako představa o schopnostech botnetů poslouží BredoLab, ten v době svého rozkvětu dokázal za pouhý den rozeslat kolem 3,5 miliardy e-mailů. [32]

[1] DDoS útok spočívá ve vytvoření velkého množství požadavků na webovou službu či stránku, čímž dochází k jejímu přehlcení a následné nefunkčnosti.



Obr. 2: Formování botnetu a jeho následné využití k rozesílání spamu [31]

Konkrétní příklady dnešního malwaru

Z několika set tisíců druhů nového malwaru, který každodenně vzniká, byly na 22. ročníku konference SECURITY označeny za ty nejdominantnější dva: Cryptoloker (WIN32/Filecoder) a Hesperbot (WIN32/Hesperbot).

Cryptoloker se snaží vydělávat vlastníkům obdobně. Šifruje obsah pevného disku a podvodníci poté nabízejí za nemalý finanční obnos dešifrovací zařízení.

Druhý zmíněný úspěšný malware Hespebot se specializuje na internetové bankovnictví. Obsahuje skrytý VNC server, to znamená, že útočník může sledovat a případně nenápadně ovládat inkriminovaný počítač.

Dalším trikem infiltrace počítače bývají stránky s údajnými zajímavými videi. Na stránce může být několik odkazů, pod většinou z nich se dokonce video zobrazí, ale pak náhle některé z dalších videí nelze spustit, uživatel se dozví, že k jeho přehrání si musí stáhnout potřebný přehrávač, který je samozřejmě nabídnut. Nejedná se ovšem o nic jiného, než jeden z malwarů. [13]

3.2 Sociální inženýrství

Pojem sociální inženýrství označuje akce, které mají za cíl vylákat od svých obětí důležité informace prostřednictvím různých psychologických a sociálních metod. Je daleko jednodušší získat data přímo od dané osoby, než je shromažďovat s pomocí malwaru. Sociální inženýrství využívá faktu, že největší nebezpečí pro ochranu systému má na svědomí lidský faktor. Vlastnosti, jako neznalost nebo důvěřivost jsou hnacími motory této zákeřné techniky. Pokud člověk nabyde pocitu, že mu nehrozí nebezpečí a rozhodne se pomyslné dveře do svého bytu otevřít, nepomůže mu před útočníkem, kolik zámků má na dveřích. Neexistuje tudíž žádný softwarový prostředek, který by mohl systém před tímto typem nežádoucí aktivity bránit. Jediným prostředkem ochrany je tedy znalost uživatelů. [14]

Na firemní úrovni má zaškolení zaměstnanců obrovský význam, každá chyba, jevící se bezvýznamně, může pro vedení znamenat velké nepříjemnosti a finanční ztrátu. Každý zaměstnanec tedy musí pochopit vážnost celé situace a dodržoval všechna bezpečností opatření a směrnice.

3.3 Charakteristika honeypotů

Honeypot je bezpečností prostředek počítače, který na rozdíl třeba od firewallu[2] nemá za úkol problém řešit, ale snažit se porozumět chování útočníka a výslednou analýzu poté použít k vylepšení obrany systému. Název honeypot (medový hrnek) metaforicky vystihuje, že by se mělo jednat o něco pro potencionálního útočníka lákavého, ten by se pak měl pokusit do systému proniknout a honeypot zdokumentuje jeho kroky. Jedná se vlastně o takovou infiltraci do technik hackerů. Lance Spitzner vidí honeypoty, jako prostředek, jehož hodnota spočívá v jeho nezákonném a neoprávněném používání. Zároveň je označuje za velmi dynamické nástroje, s jejichž pomocí lze dosáhnout mnoho nejrůznějších cílů. [6]

Historie

Popis jednoho z prvních zmapování neoprávněného přístupu do počítače se nachází v knize Clifforda Stolla Kukaččí vejce. Za autorova působení v počítačovém centru Lawrenceových laboratořích v Berkeley na konci devadesátých let došlo k vniknutí do počítačů. Clifford Stoll ovšem namísto zablokování útočníkova účtu, začal sledovat jeho činnost, postupně zjišťoval útočníkův záměr (prodej vojenských informací třetí straně) a ve svém díle zdokumentoval jeho postup. Na základě toho byl německý hacker, který se dokázal nabourat do tří desítek vojenských počítačů dopaden. [1] Tento případ měl za následek zvýšený zájem o sledování technik síťových útočníků a prevenci proti nim.

Autorem další práce je Bill Cheswick. Ten do své honeypotové pasti dokázal nalákat holandského hackera a zdokumentoval jeho činnost v díle An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied. [3]

Jedna z prvních volně šiřitelných implementací honeypotu byla Deception Toolkit Freda Cohena. Lze jí aplikovat na operační systémy Unixového typu. Jedná se o kombinaci jazyků Perl a C. Slouží jako prostředek popsání útočníkovi aktivity,

[2] Firewall je zařízení oddělující komunikaci mezi sítěmi

v okamžiku zachycení nežádoucího průniku, začne zaznamenávat jeho postup, chování a činnost do souborů. [2]

Pro operační systémy firmy Microsoft Windows NT vzniknul CyberCop Sting, který umožňoval tiché sledování potencionálních problémů na firemních počítačových sítích. Na serverech s monitorovací technologií vytvořil fiktivní podnikové systémy s mírnou dávkou zabezpečení. Návnada – virtuální síť TPC/IP umístěná na jediném serveru nebo pracovní stanici, mohla simulovat několik různých typů síťových zařízení, včetně routerů nebo Unixových serverů. Každé virtuální zařízení má svojí vlastní reálnou IP adresu, ze které může odesílat nebo přijímat originálně vypadající pakety do a z daného síťového prostředí. [4]

V roce 1999 se začala formovat skupina Honeynet Project. Jedná se o neziskovou výzkumnou organizaci pro bezpečnost, která se zabývá studií nástrojů, taktik a motivů vedoucím k síťovým útokům, analyzování výsledků a jejich prezentaci celosvětové veřejnosti. Má tři základní pilíře:

- VÝZKUM
- POVĚDOMÍ
- NÁSTROJE

Dnes shrnuje veškeré poznatky o honeypotech a vytváří stále nové bezpečností aplikace. [5]

3.4 Dělení honeypotů

Honeypoty se dají dělit podle různých vlastností. Jejich rozdělení nemusí být vždy definitivní a jednotlivé skupiny se navzájem prolínají. V této části budou popsány možná třídění podle následujících faktorů: realizace, účel, míra a směr interakce.

- Dle míry interakce

Míra interakce obecně znamená, co je honeypot ochotný útočníkovi dovolit. Logicky platí, že čím více dovoluje, tím více může ze strany útočníka získat, zároveň se ale vystavuje vyššímu bezpečnostnímu riziku zneužití.

- Dle směru interakce

Tímto způsobem lze rozdělit na serverové (3.3.3) a klientské honeypoty (3.3.4).

- Dle realizace

Jestli jsou realizovány, jako skutečná zařízení v síti (3.3.5) nebo se jedná o simulace až několika honeypotů na jednom stroji (3.3.6).

- Dle účelu

Dělením, jehož autorem je vývojář Marty Roesch, vznikají dvě skupiny podle toho, zdali se využívají k lepšímu zabezpečení sítě organizace (3.3.7) či k výzkumným účelům (3.3.8). Tento druh rozdělení není definitivní a jeden honeypot může být jednou zařazen v první skupině a jindy v té druhé. Určujícím faktorem je aktuální využití daného zařízení. [6]

3.4.1 Honeypoty s nízkou mírou interakce

Honeypoty s nízkou mírou interakce simulují pouze drobnou množinu funkcí určité služby, procesu a dalších běžných aktivit operačního systému. Tyto aktivity nemohou být zneužity k získání plného přístupu k honeypotu. [15]

Využívají se ke sledování již známých útoků a hrozeb. Jejich největší výhodou je lehká instalace, realizace, ovládání a nízká hrozba pro síť, dokonce nemusí být ani instalovány v operačním systému, jehož služby simulují. [16] Z tohoto důvodu se těší větší uživatelské oblibě. Kvůli omezenému poli působnosti slouží zejména k monitorování automatických útoků, ke sledování šíření známých červů a dalšímu sběru dat.

Výstupními hodnotami této skupiny jsou časy útoků, cílové IP adresy a adresy, ze kterých k vniknutí dochází. [6]

3.4.2 Honeypoty s vysokou mírou interakce

Oproti předchozí skupině honeypoty s vysokou mírou interakce nesázejí na jednoduchost, nízkou míru rizika a časovou nenáročnost. Neemulují žádné služby, ale nabízejí útočníkovi rovnou všechny aspekty operačního systému, z čehož vyplývá mnohonásobně vyšší riziko zneužití. [15] Tyto honeypoty jsou komplexnější a dají se útočníkem plně ovládnout, to může mít za následek, napadení dalších systémů jejich prostřednictvím. Vyšší nároky na implementaci, čas a správu jsou vykoupeny velkým množstvím informací, které o vniknutí poskytují. S jejich pomocí lze pozorovat útočníkovi postupy, nástroje, se kterými pracuje, slabiny systému a zároveň umožňují detekovat i malware využívající nové způsoby napadení. [6, 16]

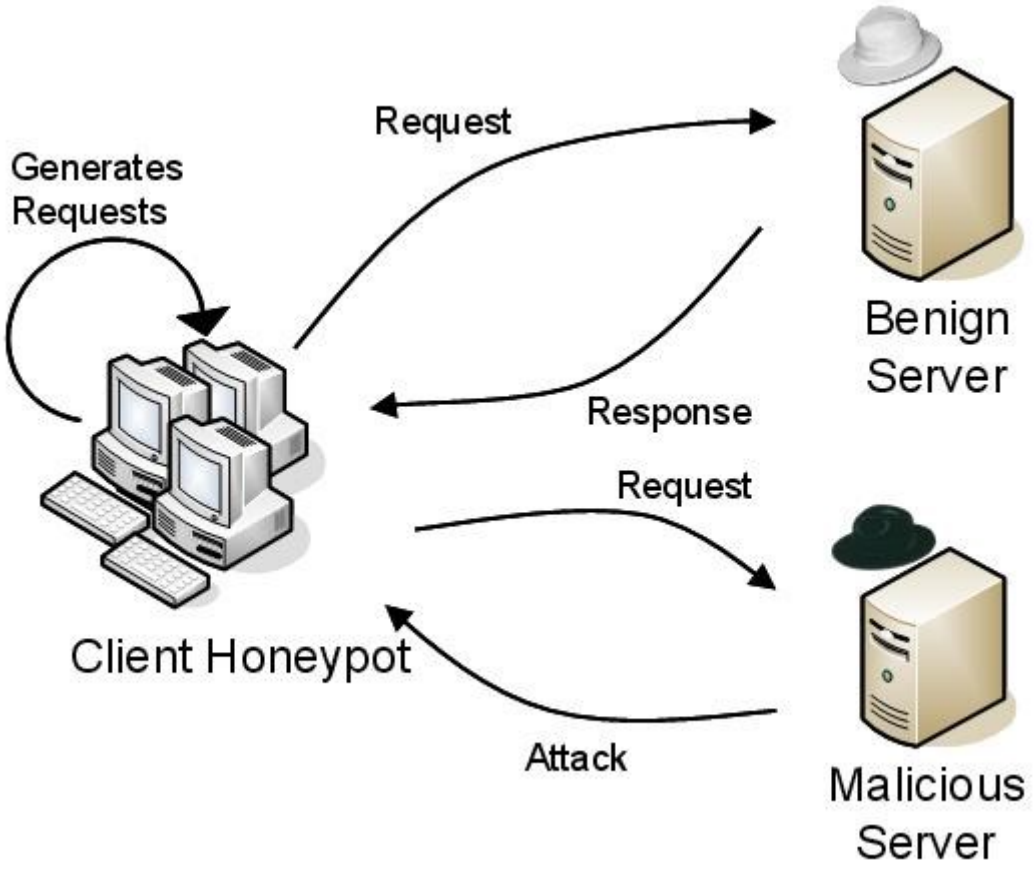
3.4.3 Serverové honeypoty

Mezi historicky nejrozšířenější skupinu patří honeypoty serverové, které se drží tradičního pasivního pojetí. Chovají se jako servery, vystavující nějaké zranitelné služby a vyčkávají na to, až budou napadeny. V okamžiku, kdy zachytí nějaký kontakt, navážou interakci a snaží se monitorovat zejména nové útočné techniky. Umisťují se na klíčové síťové uzly, kde dokáží detekovat červy a zpracovávat velké množství požadavků. [5, 16]

3.4.4 Klientské honeypoty

Klientské honeypoty napodobují chování běžného uživatele systému. Aktivně procházejí webové stránky a snaží se vyhledat pochybné servery. Na rozdíl od předešlé skupiny musejí rozeznávat mezi běžnými a škodlivými servery (Obr. 3). Mezi techniky k získávání svého cíle využívají například statistickou analýzu vzorků známého škodlivého softwaru a jeho následné porovnávání se softwarem, na který narazí. Jinou technikou jsou schopny zachytit zcela nové vzorky malwaru. Při ní používají

specializovaný operační systém, řízený zranitelným klientem, komunikujícím s potencionálním škodlivým serverem. Po každé interakci, zkontroluje systém, zda nedošlo k neoprávněným změnám a pokud ano, označí server za škodlivý. Z tohoto serveru je pak honeypot schopen odhalit neznámé útoky. [5, 16]



Obr. 3: Schéma komunikace klientského honeypotu s běžným (bílý klobouk) a škodlivým (černý klobouk) serverem [5]

3.4.5 Fyzické honeypoty

Fyzické honeypoty jsou reálná zařízení v síti s vlastní IP adresou. Jejich přístup je vysoko-interaktivní a tudíž představují větší riziko provozu. Hlavní nevýhodou fyzických honeypotů jsou vysoké náklady instalace a údržby. Pro velké adresové prostory je jejich nasazení nepraktické až nemožné, v takových situacích přicházejí na řadu honeypoty virtuální. [17]

3.4.6 Virtuální honeypoty

Virtuální honeypoty jsou oblíbené zejména díky jednoduché správě, přístupnosti pro téměř každého uživatele a nízkým nákladům jejich nasazení, protože na jednom stroji může být za pomoci virtualizace nasezeno stovky honeypotů. Kvůli těmto aspektům se dají využívat častěji, než předešlá fyzická skupina.

V praxi fungují tak, že jeden fyzický počítač hostí několik virtuálních strojů, které se tváří, jako reálné stroje lákající svou kořist. Pro tento postup se obvykle k nastavení honeypotů využívají nástroje, jako VirtualBox nebo User-mode Linux. Tyto nástroje umožňují běh více operačních systémů a jejich aplikací současně na jednou fyzickém PC, což zajišťuje jednodušší shromažďování nasbíraných dat. [17]

3.4.7 Produkční honeypoty

Produkční honeypoty zabezpečují sítě konkrétní organizace a pomáhají zmírňovat bezpečnostní rizika. Název produkční je odvozen od toho, že je komerční společnosti umisťují do prostředí k produkčním systémům. Jsou na ně kladeny nižší požadavky, než na honeypoty určené na výzkum. Z toho důvodu je jejich implementace jednodušší a obvykle je riziko jejich zneužití nižší, protože jsou moc jednoduché na to, aby mohly být zneužity k napadení a poškození systému.

Nejvíce přispívají v rámci odhalování útoků. Využívají schopnosti přesnosti v detekci a efektivního sběru dat, na jejichž základě je společnost schopna zjistit, jaké konkrétní hrozby se v jejích sítích pohybují. Další službou, kterou prokazují je prevence. Útočníka může nasazení honeypotu zmást, zaměří se na dotyčný systém s tím, že skrývá něco důležitého a odvádí svou pozornost od méně zabezpečených systémů. Dále ho může odradit možnost odhalení jeho metod. Funkce honeypotů v oblasti prevence je však spíše podpůrná, hlavní slovo mají Firewally. [6]

3.4.8 Výzkumné honeypoty

Honeypoty určené na výzkum jsou navrženy tak, aby dávaly svým majitelům informace o hackerské komunitě. Jakmile se útočník dostane do systému, je mu ponechána volnost. Během záškodnické činnosti získává honeypot údaje o útočníkovi, jeho krocích, komunikaci, technikách a o nástrojích, co používá. Získání těchto důležitých informací je vykoupeno vyšším rizikem, časovou náročnosti a zvýšeným úsilím při údržbě. Pomocí výzkumných honeypotů vzniká v antivirových společnostech software, který brání systémy a uživatele před útoky, jež byly jejich prostřednictvím zachyceny. Tato zařízení jsou velmi důležitá v oblasti bezpečnosti, z toho důvodu se o ně zajímají i vládní organizace či armáda. [6]

3.5 Přehled konkrétních honeypotů

Předešlá kapitola ukázala, že honeypoty mohou mít velké množství vlastností a různých účelů. Řadí se mezi ně jednoduché programy i celé falešné operační systémy. HIHAT nachytává útočníky na webové služby, HoneyD simuluje IP adresy a Sebek sleduje klávesy stisknuté útočníkem, v následujících řádcích budou tyto a další honeypoty podrobněji popsány.

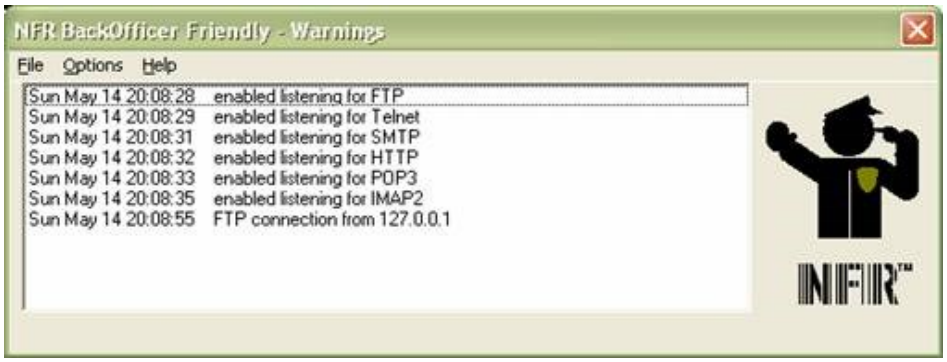
3.5.1 Agros

Agros je chráněný emulační systém vycházející z prostředí Quemu, jehož vlastnosti rozšiřuje za účelem detekce nežádoucí činnosti. K detekci útoků využívá dynamickou analýzu Taint (skvrna). Ta označí všechny příchozí data a zaznamenává každou snahu o jejich využití nelegální cestou. Agros je virtuální systém a lze ho aplikovat na více operačních systémů (Windows, Unix, Linux). [18]

3.5.2 BackOfficer Friendly

BackOfficer Friendly (BOF) je velmi jednoduchý honeypot od dnes již neexistující NFR Security, která přešla pod správu Check Point Software Technologies. Původně byl vytvořen k odhalení nástroje pro vzdálenou správu Back Orifice, ten umožňuje

ovládnout počítač pomocí jednoduché konzole [20]. BOF se postupně vyvíjel a začal nabízet novou možnost rozpoznávání pokusů o připojení k službám FTP, SMTP, POP3 nebo Telnet. Jakmile přijde na spojení s některou ze zmíněných služeb, upozorní uživatele a současně vytváří falešné odpovědi, čímž marní útočníkův čas, který získává majitel honeypotu k zastavení nežádoucí činnosti. O útočníkovi poskytuje jen málo informací. [19]



Obr. 4: Back Officer Friendly [28]

3.5.3 Dioneda

Dioneda je nástupcem honeypotu Nepenthes, který byl sestrojen za účelem sběru známého samostatně šiřitelného malwaru. [19] Dioneda pokračuje v jeho stopách a shromažďuje kopie červů nebo botů nalákaných na zranitelné síťové služby. Je napsaná v jazyce Python a s pomocí knihovny Libemu je schopna emulovat a detekovat Shellcode[3]. Nabízí protokoly SMB, HTTP na portu 80, FTP na portu 21 a na portu 69 TFTP [24].

3.5.4 GHH

Google Hack Honeypot je zaměřený na útočníky, kteří k vniknutí do systému využívají vyhledávače, jejichž prostřednictvím lze ze špatných webových serverů získat citlivé údaje. Simuluje zranitelnou webovou aplikaci a povolí vyhledávačům svoje indexování. Běžným uživatelům je zmíněná aplikace skryta, protože na její odkaz nelze narazit obyčejným "brouzdáním" po internetu, ale jen s pomocí vyhledávače. Tento odkaz je

[3] Shellcode – kód s jehož pomocí je možné ovládat služby na jiných počítačích

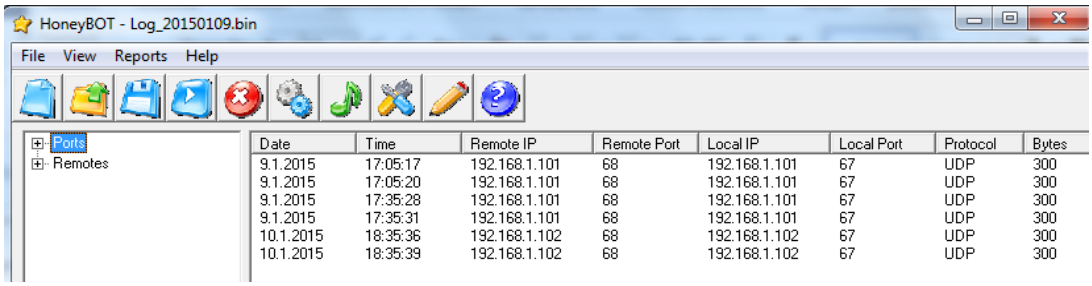
veden na již existující webovou stránku. Útočníka pak monitoruje na základě jeho dotazů na aplikaci ve vyhledávači. [23]

3.5.5 HIHAT

The High Interaction Honeypot Analyses Toolkit dokáže z libovolné PHP aplikace vytvořit honeypot webového charakteru. Útočník má tedy dojem, že komunikuje s běžnými aplikacemi typu PHPNuke či PHPMyAdmin a ty díky své transformaci monitorují jeho činnost a ukládají kopie škodlivého malweru k pozdější analýze. Dále mohou prostřednictvím získaných IP adres vytvářet mapy, zobrazující odkud útoky přicházejí a z nasbíraných hodnot vytvářet grafy. [22]

3.5.6 HoneyBOT

HoneyBOT nabízí uživateli honeypot, běžící v operačním systému Windows, se střední mírou interakce. Jeho práce spočívá ve vytvoření falešných zařízení tvářících se, jako zranitelné služby. Zatímco si útočník myslí, že komunikuje s běžným serverem, HoneyBOT tuto komunikaci zaznamenává a ukládá k budoucí analýze. Stejně, tak jsou shromažďovány trojské koně a další malware, který útočník na server umístí. [21]



Obr. 5: HoneyBot

3.5.7 HoneyD

HoneyD je jednoduchý honeypot vytvářející v síti virtuální zařízení. Jeden takový honeypot se dá použít pro simulaci velkého množství IP adres, služeb či portů a to jak v prostředí operačního systému Linux, tak i Windows. Může být také využit k vytvoření

honeynetu monitorujícího síť. Podporuje možnost vytvoření virtuální síťové topologie obsahující příslušné trasy a routery. Routerům může být nastavena ztrátovost paketů nebo jiná typická vlastnost sloužící k účelu zvýšení uvěřitelnosti této topologii. [15]

3.5.8 Kippo

Kippo je zařízení se střední mírou interakce napsané v jazyce Python. Tváří se, jako běžná SSH služba a zabývá se útoky na servery. Postupně si vytváří soubory kippo.log, do kterých ukládá nasbírané informace o útocích. Mezi tyto informace patří IP adresy, časy útoku nebo hesla a uživatelská jména použitá k pokusu o přihlášení se.

```
2015-02-20 13:13:51+0100 [kippo.core.honeypot.HoneyPotSSHFactory] New connection: 103.41.124.42:41499 (80.243.106.4:22) [session: 2594]
2015-02-20 13:13:52+0100 [HoneyPotTransport,2594,103.41.124.42] Remote SSH version: SSH-2.0-PUTTY
2015-02-20 13:13:52+0100 [HoneyPotTransport,2594,103.41.124.42] kex alg, key alg: diffie-hellman-group1-sha1 ssh-rsa
2015-02-20 13:13:52+0100 [HoneyPotTransport,2594,103.41.124.42] outgoing: aes128-ctr hmac-sha1 none
2015-02-20 13:13:52+0100 [HoneyPotTransport,2594,103.41.124.42] incoming: aes128-ctr hmac-sha1 none
2015-02-20 13:13:52+0100 [HoneyPotTransport,2594,103.41.124.42] NEW KEYS
2015-02-20 13:13:52+0100 [HoneyPotTransport,2594,103.41.124.42] starting service ssh-userauth
2015-02-20 13:13:52+0100 [SSHService ssh-userauth on HoneyPotTransport,2594,103.41.124.42] root trying auth none
2015-02-20 13:13:53+0100 [SSHService ssh-userauth on HoneyPotTransport,2594,103.41.124.42] root trying auth password
2015-02-20 13:13:53+0100 [SSHService ssh-userauth on HoneyPotTransport,2594,103.41.124.42] login attempt [root/monk123] failed
2015-02-20 13:13:54+0100 [-] root failed auth password
2015-02-20 13:13:54+0100 [-] unauthorized login:
2015-02-20 13:13:54+0100 [SSHService ssh-userauth on HoneyPotTransport,2594,103.41.124.42] root trying auth password
2015-02-20 13:13:54+0100 [SSHService ssh-userauth on HoneyPotTransport,2594,103.41.124.42] login attempt [root/b747400] failed
2015-02-20 13:13:55+0100 [-] root failed auth password
2015-02-20 13:13:55+0100 [-] unauthorized login:
2015-02-20 13:13:55+0100 [SSHService ssh-userauth on HoneyPotTransport,2594,103.41.124.42] root trying auth password
2015-02-20 13:13:55+0100 [SSHService ssh-userauth on HoneyPotTransport,2594,103.41.124.42] login attempt [root/kramer1] failed
2015-02-20 13:13:56+0100 [-] root failed auth password
2015-02-20 13:13:56+0100 [-] unauthorized login:
2015-02-20 13:13:56+0100 [HoneyPotTransport,2594,103.41.124.42] Got remote error, code 11
        reason:
2015-02-20 13:13:56+0100 [HoneyPotTransport,2594,103.41.124.42] connection lost
```

Obr. 6: Útok zaznamenaný Kippem

3.5.9 Potemkin

Potemkin je hybridní systém, který si klade za cíl, poskytnou vysoko-interaktivní honeypoty velkému množství adresovacích prostorů. K tomu používá jen pár fyzických serverů. Ty v případě detekce útočné aktivity vytvoří pro všechna spojení virtuální stroje tzv. Honeyfarm, které budou posléze útočníkem napadeny. O plánování provozu mezi servery se stará brána, s její pomocí lze přesměrovávat tok informací na další honepoty. [17]

3.5.10 Sebek

Sebek je honeypot navržen pro Linux, sbírající data o nebezpečných aktivitách. První verze sloužila k zaznamenávání útočníkova stisku kláves. Je složen ze dvou komponent. První je klient, jehož úkolem je zachycení útočníkových akcí, jako jsou zmíněné stisky kláves, nahrávání dat nebo zadávání hesla. Akce klienta jsou maskovány, běžný útočník by tedy na ně neměl narazit. Klient poté získaná data skrytě posílá druhé komponentě server, který je shromažďuje. [19]

3.6 Honeynety

Spojením několika vysoko-interaktivních honeypotů do sítě vzniká honeynet. Tato síť je obsáhlý druh architektury a veškerý provoz na ní je monitorován a zaznamenáván. Jedná se o síť určenou k napadení případnými útočníky, jejímž hlavním cílem je shlukování nabytých informací. Může představovat jakýkoliv typ systému, či služby od databáze po Cisco routery. Právě flexibilita dává honeynetům jejich pravou sílu. [5]

3.6.1 Honeywall

Hlavní komponentou ke správnému nastavení architektury honeynetu je honeywall. Jedná se o bránu, která odděluje síť honeypotů od ostatních sítí. Veškerý síťový provoz musí projít touto branou, pokud se chce dostat dovnitř nebo ven. Pokud je pojato podezření, je možné výměnu informací s neznámým uživatelem zastavit. [5]

3.6.2 Požadavky na honeynet

Existuje několik požadavků, které musí honeynet realizovat:

- **Kontrola dat:** Vždy se může stát, že se škodlivému kódu nebo útočníkovi podaří prolomit honeynet a následně ho zneužít k napadení či poškození jiného systému na síti. Vhodná kontrola dat toto riziko minimalizuje. Nejlepším způsobem je nezůstat pouze u jedné vrstvy ochrany, ale zkombinovat jich několik. Nastavit potencionálnímu útočníkovy vhodný stupeň volnosti,

neprovádět kontrolu pouze automaticky, ale i manuálně nebo nastavit více upozornění na útok.

- **Sběr dat:** Úkolem je posbírat, co nejvíc dat tak, aby nedošlo k odhalení. Platí stejné pravidlo, jako u kontroly dat a to, že by se mělo zajistit více zdrojů, určených pro sbírání informací. Také je nutné přizpůsobit sběrná zařízení tomu, že velká porce škodlivé aktivity prochází skrze zašifrované kanály. Dále je důležité vyvarovat se modifikacím honeypotů, protože každá změna zvyšuje riziko odhalení. Data uložená na honeypotech mohou být upravena nebo smazána, proto by se měla ukládat mimo ně na oddělených chráněných systémech.
- **Analýza dat:** Honeynet by nebyl užitečný, kdyby nedokázal přijatá data analyzovat a převést je na konkrétní, srozumitelné údaje.
- **Kolekce dat:** Vztahuje se pouze na organizace, jež vlastní více honeynetů v distribuovaném prostředí. Všechna nasbíraná data musí být centrálně shromažďována na jednom místě, tak mohou být dále kombinována a jejich hodnota půjde nahoru. [5]

4. Vlastní práce

Pro účely praktické části práce byl zvolen honeypot Kippo (3.4.8), běžící na linuxové distribuci Ubuntu. Jeho spuštění v prostředí domácí sítě by nepřineslo žádný efekt. Proto bylo nutné získat veřejnou IP adresu, která umožní kontakt honeypotu s okolním světem. Jednou z možností je vyhledání společnosti pronajímající virtuální servery (VPS) a u ní si společně s dalšími službami adresu koupit. Na vytvoření této práce se finance hostingovým společnostem poskytovat nemusely, protože byla využívána dynamická veřejné IP adresa autorova známého.

Před samotnou instalací honeypotu musel být nainstalován OpenSSH server. Jedná se o volně dostupný komunikační protokol Secure Shell, který umožňuje spojení mezi vzdálenými počítači. K instalaci klientské a serverové aplikace stačí zadat do příkazové řádky dva jednoduché příkazy: *sudo apt-get install openssh-client a sudo apt-get install openssh-server*. Open SSH server má předdefinován port 22, na kterém je aktivita hackerů logicky nejvyšší, pohybuje se na něm velké množství botů a z důvodu bezpečnosti byl před instalací Kippa změněn na port 8925. [25]

Posledním krokem příprav byla instalace vybraných Python balíčků a knihoven: *apt-get install python-dev openssl python-openssl python-pyasn1 python-twisted* a dále programu subversion: *:-$ apt-get install subversion*. [26]

```
The following extra packages will be installed:
  libexpat1-dev libpython-dev libpython2.7-dev python-twisted-conch
  python-twisted-lore python-twisted-mail python-twisted-names
  python-twisted-news python-twisted-runner python-twisted-words python2.7-dev
Suggested packages:
  python-twisted-runner-dbg
The following NEW packages will be installed:
  libexpat1-dev libpython-dev libpython2.7-dev python-dev python-pyasn1
  python-twisted python-twisted-conch python-twisted-lore python-twisted-mail
  python-twisted-names python-twisted-news python-twisted-runner
  python-twisted-words python2.7-dev
The following packages will be upgraded:
  openssl
1 upgraded, 14 newly installed, 0 to remove and 264 not upgraded.
Need to get 23,7 MB of archives.
After this operation, 40,2 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Obr. 7: Instalace Python balíčků

4.1 Instalace a konfigurace

Prvním bodem instalace bylo vytvoření uživatele kippo a nastavení domovského adresáře home/kippo. Uživatel kippo byl vzápětí použit na stažení Kippa samotného.

Kippo běží standardně na portu 2222. Jak už bylo uvedeno v předešlé kapitole, největší aktivita útočníků se vyskytuje na portu 22. Z toho důvodu byl změněn port z 2222 na 22. Porty nižší než 1024 může běžně používat jen uživatel root. Proto byl nainstalován balíček AuthBind, umožňující používání nižších portů i ostatním uživatelům bez nutnosti změn aplikace. Po spuštění startovacího skriptu byla jeho část editována vložením příkazu *authbind –deep* před stávající příkaz *twistd -y kippo.tac -l log/kippo.log --pidfile kippo.pid*. Tím se dostal Authbind do běhu. Nyní je možné spustit skript příkazem *start.sh*. [26]

4.2 Spuštění a první záznamy

První akcí testující funkčnost honeypotu bylo vyzkoušení přihlášení se, jako uživatel marek s heslem acs. Kippo vypsalo následující řádky a uložilo je do souboru kippo.log:

[SSHService ssh-userauth on HoneyPotTransport,2,193.84.36.110] marek trying auth none

[SSHService ssh-userauth on HoneyPotTransport,2,193.84.36.110] marek trying auth keyboard-interactive

[SSHService ssh-userauth on HoneyPotTransport,2,193.84.36.110] login attempt [marek/acs] failed

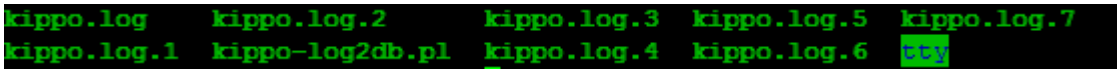
Aby byl přístup k honeypotu možný bezproblémově i z jiného počítače, byl vytvořen uživatel marek příkazem: *sudo useradd – d /home/marek -s /bin/bash -m marek*.
Teď, když bylo Kippo v běhu, stačilo už jen čekat na první útoky a ty přišly 38 minut po otestování hesla acs v 15:44. Z IP adresy 218.87.111.118 bylo vyzkoušeno heslo wubao a jiamima pod uživatelem root. Za 21 vteřin od prvního útoku, už byla z adresy lokalizované v Číně zkoušena tradiční hesla: admin, root, 1234, 12345, password.

```
2015-02-19 15:44:56+0100 [SSHService ssh-userauth on HoneyPotTransport,8,218.87.111.118] root trying auth password
2015-02-19 15:44:56+0100 [SSHService ssh-userauth on HoneyPotTransport,8,218.87.111.118] login attempt [root/12345] failed
2015-02-19 15:44:57+0100 [-] root failed auth password
2015-02-19 15:44:57+0100 [-] unauthorized login:
2015-02-19 15:44:57+0100 [SSHService ssh-userauth on HoneyPotTransport,8,218.87.111.118] root trying auth password
2015-02-19 15:44:57+0100 [SSHService ssh-userauth on HoneyPotTransport,8,218.87.111.118] login attempt [root/1234] failed
2015-02-19 15:44:58+0100 [-] root failed auth password
```

Obr. 8: Záznam použití hesel 12345 a 1234

Poté se honeypot na několik hodin odmlčel. Druhá interakce přišla až další den 20. 2. 2015 ve 4:56. Adresy 103.41.124.21 a 103.41.124.45 se zkoušely připojit ke službě SSH nepřetržitě do 5:12.

S přibývajícími útoky si Kippo začalo vytvářet nové soubory, do kterých si ukládalo nashromážděné informace. Pro zobrazení informací tu jsou dva příkazy. První *ls kippo* vypíše soubory v adresáři a pro otevření konkrétního souboru stačí zadat *less ./kippo/kippo.konkrétní log, který chce uživatel otevřít.*



Obr. 9: Výpis adresáře kippo

4.3 Kippo-Graph

Z nasbíraných výsledků by se dělaly závěry jen velmi obtížně, naštěstí byl vyvinut plně funkční skript k vizualizaci statistických hodnot z použitého SSH honeypotu, nazývá se Kippo-Graph.

Pro potřeby grafu se nainstaloval databázový server MySQL, v němž byla vytvořena databáze kippo. Následně byl nahrán Kippo-Graph, jemuž byla nastavena přístupová cesta do databáze. Tento skript vytvoří různé grafy z hodnot získaných Kippem, ty jsou poté dostupné z adresy: http://použitýserver/kippo-graph. Poněvadž jsem používal dynamickou adresu, nelze uvést konkrétní adresu, na které jsou výsledky k dispozici. [27]

4.4 Údaje za první den činnosti

Za sledované období od 15:44 19. 2. 2015 do 18:01 20. 2. 2015 bylo zachyceno celkem 6 651 odlišných hesel, vyzkoušených k proniknutí na SSH server. Jednalo se, jak o hesla typicky nebezpečná (54321, admin, root), tak o středně bezpečné, kombinující alespoň písmena s číslicemi (merlin5, biliboi00, viking12), dále o hesla zajímavá (safranek, dontbestupid, fucking, ======) a také byla použita silnější hesla (!Q@Q#Q, massymo.008, 0-ds9fihgjhgdsa).

Nejvyšší četnost měla hesla: wilkins, napporn, Pa$$w0rd!, Nu-E-BuN, Imir@Ninie, !@#$%qwert a w8bchat. Ve sledovaném časovém úseku se objevily celkem v šesti případech.

Výpis IP adres nabízí Obr. 10. Z adresy 80.243.106.7 byly provedeny zkušební pokusy.

IP address	Geolocation	Sessions count
103.41.124.112	Central District, Hong Kong	209
103.41.124.21	Central District, Hong Kong	417
103.41.124.22	Central District, Hong Kong	208
103.41.124.26	Central District, Hong Kong	569
103.41.124.27	Central District, Hong Kong	209
103.41.124.32	Central District, Hong Kong	209
103.41.124.34	Central District, Hong Kong	210
103.41.124.40	Central District, Hong Kong	209
103.41.124.42	Central District, Hong Kong	210
103.41.124.45	Central District, Hong Kong	416
103.41.124.51	Central District, Hong Kong	209
103.41.124.63	Central District, Hong Kong	691
103.41.124.64	Central District, Hong Kong	635
175.126.82.235	Republic of Korea	6
177.99.169.130	Brasília, Brazil	2
193.84.36.110	Prague, Czech Republic	1
204.10.23.198	El Segundo, United States	1
206.71.221.105	Augusta, United States	1
212.129.17.146	France	151
218.87.111.118	Nanchang, China	8
23.228.196.60	Walnut, United States	1
31.169.80.205	Sanayi, Turkey	1
42.123.87.96	China	73
60.250.188.9	Taiwan	1
80.243.106.7	Czech Republic	6
89.184.9.133	Kazan', Russia	2
96.88.195.228	United States	1

Obr. 10: Celkový přehled (1. sloupec – IP adresa, 2. sloupec – lokalita adresy, 3. sloupec -počet připojení)

Adresa 103.41.124.63, která byla se 691 pokusy za první den pozorování nejaktivnější. Je lokalizovaná v Hong Kongu a stejně, jako další adresy 103.41.124.xxx ukazuje při bližším sledování údajů na Kings Collage Old Boys Association Primary School. Je

tedy možné, že server nebo počítače této školy byly napadeny a nyní slouží, jako prostředek k útokům.

4.5 Analýza výsledků

Za 105 hodin provozu bylo zaznamenáno celkem **65 525 pokusů** o přihlášení na SSH server v **15 482 relacích**, z toho vyplývá průměr 10,4 pokusu za minutu, k tomu bylo použito **26 827 jedinečných hesel** z **94 IP adres**.

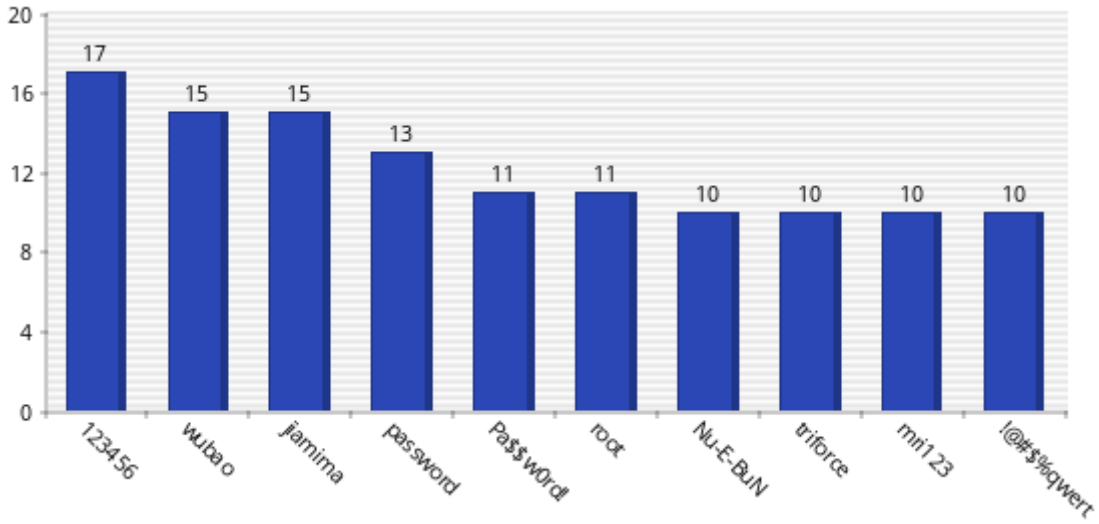
Adresy byly lokalizované celkově ze 17 států, vyjma Afriky a samozřejmě Antarktidy z každého kontinentu. K útokům bylo použito **30 uživatelských jmen**. Nejčastější jméno root bylo zaznamenáno v drtivé většině případů, konkrétně v 65 367. Druhý admin s hodnotou 38 výrazně zaostával. 6 pokusů měla na svědomí jména adm a test, 4 zapsalo ubnt.

Nejnižší aktivitu zaznamenal Honeypot první den svého provozu 19. 2. 2015, kdy v čase od 15:44 do 23:59 získal údaje pouze o 46 pokusech. Naopak největší aktivita přišla v sobotu 21. 2. 2015, kdy došlo ke 23 933 pokusům.

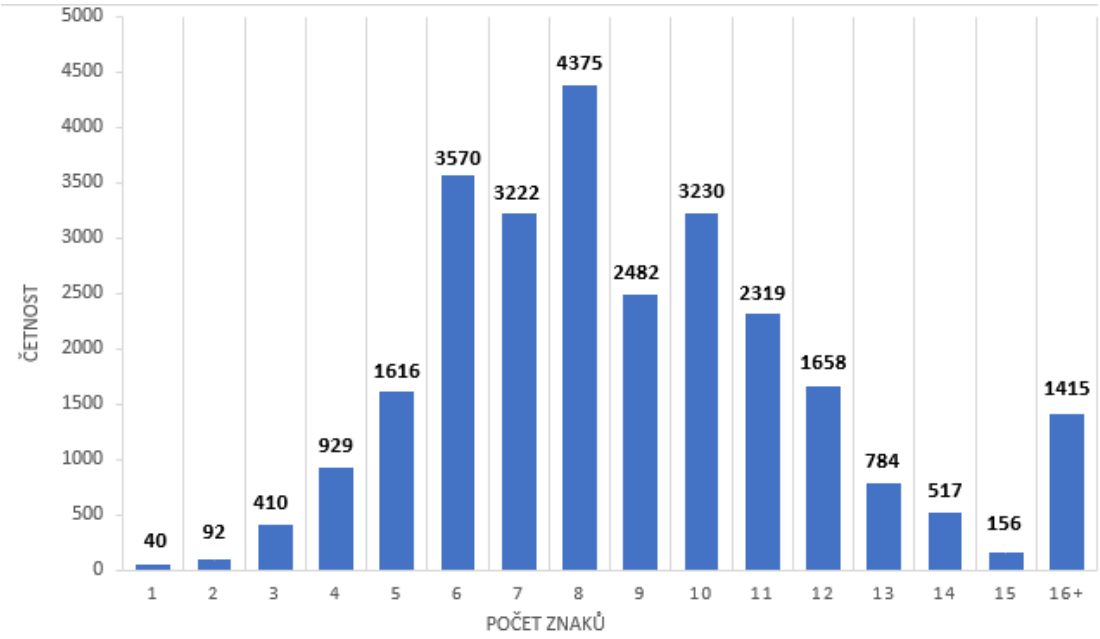
Dominantní SSH klient SSH-2.0-PUTTY byl použit v 15 452 případech, o to že nemá 100% zásluhu na útocích, se postaraly SSH-2.0-libssh2_1.4.3 a SSH-2.0-Erlang s 1 záznamem.

Analýza použitých hesel

Z 26 827 shromážděných jedinečných hesel mělo největší četnost heslo 123456 s hodnotou 17 pokusů (Obr. 11). Nejčastějšími kombinacemi uživatelského jména a hesla byly v 15 případech root/1234, root/wubao a root/jiamina. **Nejdelší heslo mělo 100 znaků**, nejkratší 1, nejčetnější byla hesla s 8 znaky (Obr. 12).



Obr. 11: Přehled a četnost 10 nejpoužívanějších hesel

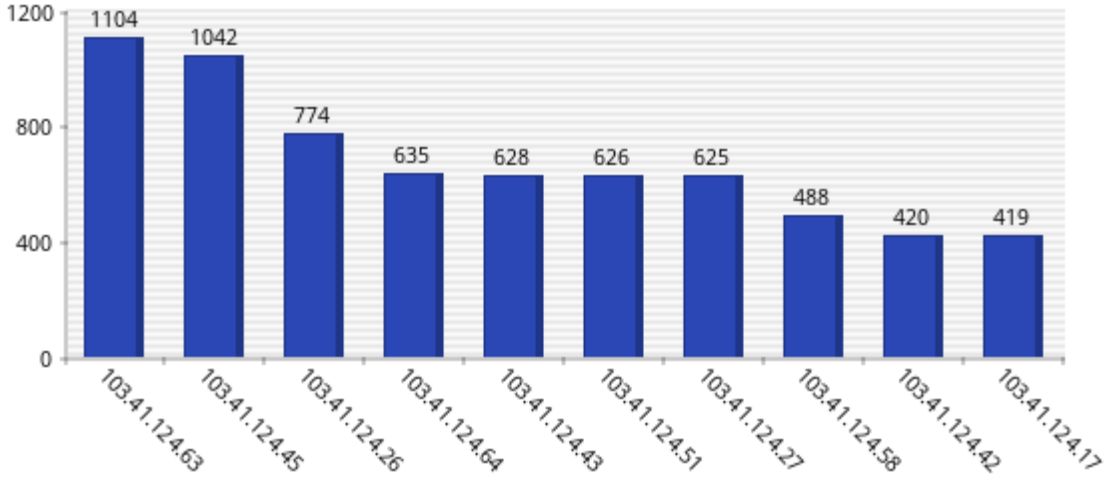


Obr. 12: Délka vyzkoušených hesel a počet výskytu

Při některých útocích byla zkoušena hesla náhodná bez větší souvislosti. Některé útoky, ale byly vedeny systematicky. 22. 2. 2015 ve 4:08 začal útok z adresy 42.123.87.96, uživatel root se snažil připojit s pomocí potencionálních příjmení začínajících heslem cadbury a vracel se dále abecedou přes nejrůznější jména typu bowton či bladecki až po hesla bigard a biermeier, u kterých byl v čase 4:17 ukončen.

Analýza identifikovaných adres

Z 94 IP adres, se kterými přišlo během provozu Kippo do kontaktu, byla nejaktivnější adresa **103.41.124.63 s 1104 relacemi**, další výsledky nabízí Obr. 13. Tab. 1 zase ukazuje země, ze kterých útoky přicházely a počet relací z daného státu. Z tabulky lze vyčíst, že zdaleka nejvyšší aktivita proudila z asijských zemí. Zajímavostí je fakt, že zachycená česká adresa patří České zemědělské univerzitě. Závěrečný Obr. 14 ukazuje detail útoku z brazilské půdy.



Obr. 13: Přehled nejaktivnějších IP adres

Hong Kong	14343	Portugalsko	95	Brazílie	2	Taiwan	1
Francie	286	Jižní Korea	91	Rusko	2	Turecko	1
Čína	268	Malajsie	73	Ukrajina	2		
Indie	170	Itálie	14	ČR	1		
USA	123	Seychelly	9	Švédsko	1		

Tab. 1: Počet zachycených relací na stát

Total connection attempts from 177.99.169.130: 6					
Timestamp	IP	Session	Username	Password	Success
2015-02-20 17:55:37	177.99.169.130	21	root	dindinger	0
2015-02-20 17:55:38	177.99.169.130	21	root	dinarte	0
2015-02-20 17:55:39	177.99.169.130	21	root	dimura	0
2015-02-20 17:55:58	177.99.169.130	22	root	ditchella	0
2015-02-20 17:56:00	177.99.169.130	22	root	disoza	0
2015-02-20 17:56:04	177.99.169.130	22	root	disiena	0

Obr. 14: Detail brazilského útoku

4.6 Kroky útočníků po vniknutí

Pokud se útočníkovi podaří odhalit heslo a jeho prostřednictvím se přihlásí, většinou se jen hned odhlásí. Častým krokem je změna odhaleného slabého hesla na heslo silnější, aby byly nalezené informaci pouze pro potřebu konkrétního útočníka. Útočníci se dále snaží získat přístup k uživateli root, stahují IRC boty pro škodlivou činnost, nebo jiná velká data za účelem zjištění rychlosti stahování serveru. Záznam stahování většina hackerů následně maže. [29, 30]

4.7 Zvýšení zabezpečení serveru

Základem bezpečného serveru je jeho zodpovědná správa, spojená se stahováním aktualizačních balíčků a nastavením silného hesla.

Tato práce využívala služby komunikačního protokolu SSH. Pro bezpečnostní účely je velmi užitečné zakázat přihlašování pomocí hesla a povolit pouze přihlášení prostřednictvím klíčů. Klient si vygeneruje privátní a veřejný klíč. Veřejný klíč nahraje na všechny své servery a soukromý si ponechá. Pro přihlášení použije elektronický podpis zašifrovaný soukromým klíčem, server podpis ověří dříve nahraným veřejným klíčem, a pokud je vše v pořádku, vpustí uživatele dál. [33]

Nasazení honeypotu odhalilo tisíce útoků spočívajících v hádání hesel. Činnost botů, kteří zkoušejí stále dokola nějaká hesla, způsobuje zátěž pro server. Zařízení řešící tento problém se nazývá Fail2ban.

Fail2ban pročítá autentizační log a hledá v něm neúspěšné pokusy o přihlášení. Skrze nástroj k nastavování pravidel firewallu IPtables, znemožňuje na určitou dobu přístup nežádoucím IP adresám. Uvnitř programu si uživatel zvolí, po kolikátém neplatném přihlášení zablokuje jeho adresu a tím výrazně sníží pravděpodobnost odhalení hesla. Doporučuje se nastavit si adresy, které nemohou být zablokovány, aby nedocházelo k uzavření si přístupu, vinou omylem napsaného hesla. Démon[4] Fail2ban se nezaměřuje jenom na SSH, ale je aplikovatelný i pro PHP, Apache, Courier a další služby. [33]

4.8 Diskuze

Práce měla za cíl nejdříve seznámit čtenáře libovolného zaměření s pojmem honeypot. Z rozhovorů vedených o tématu práce bylo zjištěno, že ani jedna osoba z autorova okolí nevěděla, co je honeypot a nikdo si ho nedokázal alespoň přibližně zařadit.

Kapitola teoretická východiska nabídla všem čtenářům přehlednou charakteristiku a popis tohoto sledovacího zařízení. Díky tomu každý může získat přehled o této problematice a o hrozbách v počítačových sítích. Bude vědět, že otevření přílohy v e-mailu z neznámé adresy může znamenat nakažení počítače. Dokáže si představit reálné fungování honeypotů i cestu, kterou musely projít, aby se vyvinuly do současné podoby. Čtenář by měl být schopen porozumět principu rozdělení honeypotů do skupin dle logických kritérií, na konkrétních příkladech zjistit různé možnosti sledování útočníků a v neposlední řadě získat povědomí o variantě propojení několika zařízení do sítě, nazývající se honeynet.

Z výsledků práce vyplývá, že aktivita útočníků je opravdu obrovská a proudí z celého světa. První rada, se kterou se uživatel PC v oblasti bezpečnosti setkává, se týká kvalitně nastaveného hesla. Častokrát nejsou uživatelé neznalí možností zneužití počítačů řádně informováni o hrozbách, které na ně číhají a díky slabému heslu přicházejí o cenné informace. Každý bezpečnostní technik nabádá uživatele k vytvoření hesla kombinujícího písmena různých velikostí s číselnými hodnotami a speciálními znaky. Z práce je jasně vidět, že pokud správce serveru nastaví častého uživatele typu

[4] Démon je v informatice označení pro dlouhodobě spuštěný program, který pracuje na pozadí.

root se slabým heslem, má zaručeno, že se mu na server dostane třetí strana, o kterou nestojí.

Většina útoků byla vedena s pomocí botů, kteří se v intervalech několika minut snažily uhodnout heslo. Tyto boty lze eliminovat s pomocí zařízení Fail2ban, čímž se zajistí zvýšení bezpečnosti serveru.

Pomocí uvedených informací a konkrétních výsledků této práce by si měl každý, bez ohledu na úroveň svých znalostí informačních technologií, udělat představu o možných hrozbách a jejich objemu v počítačových sítích.

Závěr

V současnosti žije na naší planetě přes 7 miliard lidí a bohužel ne každý žije svůj život s dobrými úmysly. Vývoj je dynamický, nezastavuje se před morálními hodnotami. Vedle metod přispívajících k rozvoji a prospěchu společnosti, se bohužel stále zdokonalují i způsoby vedoucí k destrukci, sabotáži či zneužití. Vědeckofantastické romány dávají každému jedinci příklady, jak může náš svět vypadat, pokud přestaneme chránit naše soukromí a střežit svoje zájmy. Pro přehnanou důvěřivost není dnes již místo a v informačních technologiích to platí obzvlášť. Takřka každý týden některá z velkých bank informuje o pokusech získat od uživatelů citlivé informace nebo dokonce čerpat jejich finance, servery firem jsou přehlcovány DDoS útoky a běžný uživatel se mnohdy bez svého vědomí dělí o čas procesoru s malwarem.

Nezbývá než se proti těmto způsobům obrnit, seznamovat se s novými poznatky v oblasti bezpečnosti, sledovat zprávy o novinkách ve vývoji škodlivého softwaru a být na něj připraven. Jedině tak má člověk šanci nebýt zneužit.

Seznam použitých zdrojů

[1] STOLL, Cliff. Kukaččí vejce [online]. [New York] : [Doubleday], [1989] [cit. 2013-12-02]. Dostupné z: http://www.root.cz/knihy/kukacci-vejce/

[2] Deception Toolkit. [online]. [cit. 2013-12-02]. Dostupné z: http://www.all.net/dtk/

[3] In Which a Cracker is Lured, Endured, and Studied. CHESWICK, Bill. AT&T BELL LABORATORIES. [online]. [cit. 2013-12-03]. Dostupné z: http://web.cheswick.com/ches/papers/berferd.pdf

[4] Network Associates Ships CyberCop Sting. [online]. [cit. 2013-12-02]. Dostupné z: http://www.serverwatch.com/news/article.php/1399041/Network-Associates-Ships-CyberCop-Sting.htm

[5] *The Honeynet Project* [online]. [cit. 2013-12-02]. Dostupné z: https://www.honeynet.org/

[6] LANCE, Spitzner. *Honeypots: Tracking hackers*. Boston: Addison-Wesley, 2003. ISBN 03-211-0895-7.

[7] Who creates malware and why?. [online]. [cit. 2014-03-03]. Dostupné z: http://www.securelist.com/en/threats/detect?chapter=72

[8] Antivirové programy. PC-SECURITY. [online]. [cit. 2014-03-04]. Dostupné z: http://pc-security.cz/zabezpeceni-pocitace/antivirove-programy/

[9] Viruses, Worms and Trojans. [online]. [cit. 2014-03-04]. Dostupné z: http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/Viruses/

[10] What Is the Difference: Viruses, Worms, Trojans, and Bots?. CISCO. [online]. [cit. 2014-03-04]. Dostupné z: http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html

[11] Microsoft Windows. MICROSOFT. [online]. [cit. 2014-03-05]. Dostupné z: http://windows.microsoft.com/cs-cz/windows/home

[12] What is Adware and Spyware?. SYMANTEC. *PC Tools* [online]. [cit. 2014-03-05]. Dostupné z: http://www.pctools.com/security-news/what-is-adware-and-spyware/

[13] Ohlédnutí za SECURITY 2014 - I. HOAX.CZ. [online]. [cit. 2014-03-05]. Dostupné z: http://www.hoax.cz/malware/aktuality/ohlednuti-za--security-2014---i---prednaska-lepe-uz-bylo_413

[14] What is Social Engineering?. WEBROOT INC. [online]. [cit. 2014-03-06]. Dostupné z: http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering

[15] Honeypot Background. [online]. [cit. 2015-01-13]. Dostupné z: http://www.honeyd.org/background.php

[16] Honeypoty - nebezpečí na klientské straně. [online]. [cit. 2015-01-13]. Dostupné z: http://computerworld.cz/securityworld/honeypoty-nebezpeci-na-klientske-strane-47635

[17] Index.html. [online]. [cit. 2015-02-13]. Dostupné z: http://books.gigatux.nl/mirror/honeypot/final/

[18] Argos - An emulator for capturing zero-day attacks. [online]. [cit. 2015-02-21]. Dostupné z: http://www.few.vu.nl/argos/?page=1

[19] honeypot utilities. [online]. [cit. 2015-02-21]. Dostupné z: http://securitytools.wikidot.com/honeypot-utilities

[20] Back Orifice Windows Remote Administration Tool. [online]. [cit. 2015-02-21]. Dostupné z: http://www.cultdeadcow.com/tools/bo.html

[21] HoneyBOT - the windows honeypot. [online]. [cit. 2015-02-22]. Dostupné z: http://www.atomicsoftwaresolutions.com/about.php

[22] HIHAT - High Interaction Honeypot Analysis Tool. [online]. [cit. 2015-02-22]. Dostupné z: http://hihat.sourceforge.net/index.html

[23] GHH - The "Google Hack" Honeypot. [online]. [cit. 2015-02-26]. Dostupné z: http://ghh.sourceforge.net/

[24] Dioneda - catches bugs. [online]. [cit. 2015-03-01]. Dostupné z: http://dionaea.carnivore.it/

[25] OpenSSH Server. [online]. [cit. 2015-03-02]. Dostupné z: https://help.ubuntu.com/lts/serverguide/openssh-server.html

[26] How To Install Kippo, an SSH Honeypot, on an Ubuntu Cloud Server. [online]. [cit. 2015-03-02]. Dostupné z: https://www.digitalocean.com/community/tutorials/how-to-install-kippo-an-ssh-honeypot-on-an-ubuntu-cloud-server

[27] Kippo-Graph - BruteForce Labs Blog. [online]. [cit. 2015-03-03]. Dostupné z: http://bruteforce.gr/kippo-graph

[28] Технология Honeypot. Часть 3: Обзор существующих Honeypot. [online]. [cit. 2015-03-04]. Dostupné z: http://www.securitylab.ru/contest/283103.php

[29] SSH Brute Force – The 10 Year Old Attack That Still Persists. [online]. [cit. 2015-03-6]. Dostupné z: http://blog.sucuri.net/2013/07/ssh-brute-force-the-10-year-old-attack-that-still-persists.html

[30] Running A SSH Honeypot With Kippo: Let's Catch Some Script Kiddies. [online]. [cit. 2015-03-9]. Dostupné z: http://blog.macuyiko.com/post/2011/running-a-ssh-honeypot-with-kippo-lets-catch-some-script-kiddies.html

[31] Botnet – Wikipedie. [online]. [cit. 2015-03-14]. Dostupné z: http://cs.wikipedia.org/wiki/Botnet

[32] Seriál Příchod hackerů - Root.cz. [online]. [cit. 2015-03-13]. Dostupné z: http://www.root.cz/serialy/prichod-hackeru/#ic=serial-box&icc=title

[33] Bezpečnost - Root.cz. [online]. [cit. 2015-03-15]. Dostupné z: http://www.root.cz/bezpecnost/