Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Ing. Tomáš Výmola

Metody detekce on-line hrozeb ve virtuálním prostředí

On-line Threats Detection Techniques in a Virtual Environment

Disertační práce

Studijní program:	Inženýrská informatika
Studijní obor:	Inženýrská informatika
Školitel:	doc. Mgr. Roman Jašek, Ph.D.

Zlín, prosinec 2013

ABSTRAKT

Cílem disertační práce je zmenšení nebezpečí a omezení vybraných rizik, které hrozí počítačovým systémům ve virtuálním prostředí, a navržení vhodného řešení této problematiky. Hlavní část této práce je zaměřena na využití systémů detekce k vyhledávání aktuálních hrozeb. Používané systémy detekce již spolehlivě detekují většinu incidentů, ale jsou většinou neúčinné proti cíleným útokům na konkrétní počítačové systémy.

V úvodní, teoretické části, se zabývám komplexním rozdělením bezpečnostních řešení. Jsou zde popsány hlavní způsoby a přístupy k detekci hrozeb a její výhody a nevýhody. Dále se zabývám detekcí incidentů za využití systému honeypotů. Jsou zde uvedeny slabé i silné stránky tohoto způsobu detekce a možnosti rozšíření tohoto systému. V závěrečné sekci teoretické části se zabývám metodikou incidentů. Zaměřuje se na Advanced Persistent Threat, rozebírá jednotlivé části incidentu a určuji slabá místa těchto typů útoků.

V praktické části je navržena metodika systému detekce pomocí honeypotů. Vychází se ze standartních vlastností honeypotů, rozšířených o nově navržené a vytvořené prvky, které zvyšují efektivnost detekce incidentů.

V další části je dle metodiky a návrhu, vytvořena laboratoř, která na aktuálních hrozbách porovnává účinnost jednotlivých způsobů detekce. Byly stanoveny hypotézy, které jsou zde statisticky vyhodnoceny.

Klíčová slova:

Bezpečnost počítačových systémů, Honeypot, útok, detekce, Advanced Persistent Threat

ABSTRACT

The aim of the Doctoral thesis is to decrease danger and reduce certain risks that can threaten computer systems in a virtual environment, and to propose a suitable solution to this problem. The main part of the thesis focuses on using detection systems to search for current threats. The already used detection systems have reliably detected most of the incidents; however, they are usually ineffective against targeted attacks on specific computer systems.

The introduction - theoretical background - deals with a complex division of security solutions. There are described the main methods of and approaches to threat detection and its advantages and disadvantages. Furthermore, the thesis also addresses incident detection using honeypots. There are presented the strengths and weaknesses of this detection method and options for expanding the system. The final section of the theoretical background is aimed at the methodology of incidents. It focuses mainly on the Advanced Persistent Threat, analyzes the different parts of the incident, and determines the weaknesses of these types of attacks.

The practical application comprises a draft of detection system methodology using honeypots. It is based on the standard characteristics of honeypots, expanded by newly designed and created features that enhance the effectiveness of incident detection.

According to the methodology and draft, the next section describes a creation of a laboratory which on the latest security threats compares the efficiency of individual detection methods. There were determined hypotheses that are statistically evaluated in this section.

Keywords:

Computer Security, Honeypot, Attack, Detect, Advanced Persistent Threat

Děkuji tímto vedoucímu mé disertační práce doc. Mgr. Romanu Jaškovi Ph.D., za přátelský přístup, za odborné vedení, rady a připomínky, které mi poskytl během zpracování mé práce a během celého studia.

Chtěl bych také poděkovat své ženě a dětem za trpělivost při zpracování disertační práce.

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory
APT	Advanced Persistent Threats
C2	Command and Control Server
CMD	Shell v operačním systému Microsoft Windows
D-IDS	Distribuovaný systém detekce narušení
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Systém
FTP	File Transfer Protocol
HIDS	Host-based Intrusion Detection Systém
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Systém detekce narušení IDS (Intrusion Detection Dystem)
IPS	Systém prevence narušení IPS (Intrusion Prevention System)
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IS	Informační systémy
LAN	Lokální síť
MAC	Media Access Control Address
NIDS	Network-based Intrusion Detection System
OPSEC	Operations Security
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtuální privátní síť
WWW	World Wide Web
XINETD	Extended Internet Daemon

ÚVOD

V současné době roste jak na internetu, tak i v lokálních sítích počet bezpečnostních incidentů. Organizace jsou stále více nuceny pro svoji ochranu zavádět různé systémy, které monitorují IT narušení bezpečnosti.

Již od 60. a 70. let minulého století se objevují útoky na sálové počítače. Nejčastěji se objevovaly dva typy incidentů: narušení bezpečnosti ze strany uživatelů anebo pomocí počítačových programů (malware). [35]

Jak ale hodnota informací obsažených v IS roste, roste i zájem o zcizení těchto dat. Moderní metody bezpečnostních incidentů jsou již mnohem více sofistikované a dopady útoků způsobují velké škody. Při útoku přímo na infrastrukturu se mohou objevit i ztráty na životech. Změnili se i útočníci. Nejprve to byli jedinci, kteří víceméně poukazovali na zranitelnosti systémů a tyto hrozby byly míněny jako žert. Dnešní útočníci se seskupují pod hlavičkou organizovaného zločinu za vidinou finančního zisku, nebo pod ochranou některých vlád, za záminkou ochrany národní bezpečnosti. To poukazuje na vysokou hodnotu dat a informací, které se vyskytují v IS. [34]

Bohužel stávající stav zabezpečení a ochrany je velmi tristní. Dle společnosti ESET se vyskytuje přes 100 000 nových hrozeb denně. Některé útoky jsou cíleny jen na malou skupinu uživatelů a zařízení. Jsou tak velmi těžce detekovány standartními technologiemi. [17] V poslední době jsou to útoky typu Advanced Persistent Threats (APTs), které jsou vícefázové a trvající delší časový úsek. Než je takový typ útoku zjištěn a neutralizován, trvá to někdy týdny nebo měsíce. Tyto typy útoků jdou momentálně odhalit jen vysoce vyspělými nástroji na vstupních bodech sítí [1]. Informace o APTs útocích nejsou moc časté, ale pokud se jedná již o způsobení velké škody, nezbývá organizacím než je zveřejnit. [57]

Společnost Kaspersky Lab provedla mezi svými klienty v roce 2013 průzkum a výsledky jsou alarmující. Datové úniky byly vyčísleny na £1,4 mil. přímo ze ztrát konkrétních incidentů, přerušení podnikání a výdajů za služby sanačních specializovaných firem. Pro malé a střední podniky v průměru 100 až 200 zaměstnanců byly vyčíslena průměrná ztráta ve výši 60 000 liber za incident. Téměř čtvrtina firem uvedla, že jejich síťové infrastruktury byly napadeny. Tyto incidenty přišli na £1,1 mil. pro velké podniky a 48.000 liber pro malé a střední podniky za incident. Vzhledem k široké škále různých útoků Kaspersky Lab uvedl, že není možno se pouze spoléhat na zabezpečení pomocí antivirových systémů, ale je potřeba komplexnější přístup. [26]

Nyní se standardní zabezpečení sítí opírá o firewally, bezpečností politiky systémů, a antivirové programy. Většina systémů není připravena k certifikaci dle norem ISO/IEC 27001 a ISO/IEC 270002 – ISMS.

Některé IT oddělení provádějí analýzu logů systémů, kontroly přenosu dat a mění průběžně nastavení dle zveřejněných hrozeb. Vše ale závisí na množství znalostí lidí a investovaných financí do bezpečnosti.

Podceňování hrozeb se ale nevyplácí. V poslední době se povedlo velké množství úspěšných útoků na mezinárodní korporace. V důsledku těchto útoků společnosti ztratily důvěru klientů a škody se vyšplhaly do vysokých nákladů.

Základním kamenem ochrany systémů je včasná detekce nebezpečí. Většina organizací řeší bezpečnostní incidenty, až se objeví a nepředchází těmto událostem. To má pak za následek nákladné opravy systémů a zhoršení pověsti. Některé organizace mají zakoupeny komplexní řešení na detekci od velkých firem, které nejsou přesně customizovány. A tak kvůli různorodosti jejich infrastruktury musí používat i více překrývajících se systémů detekce. To je pak důsledkem velkého množství falešných poplachů, kterým následně správci nevěnují důslednou pozornost. Tím se úroveň zabezpečení rapidně snižuje. Pro zvýšení zabezpečení a předcházení útoků je potřeba používat efektivní metody detekce, což je tématem mé disertační práce.

1.1 Důvody volby tématu disertační práce

Prvotním důvodem pro volbu tohoto tématu je jeho aktuálnost a velmi rychlý vývoj v dané oblasti. Informační bezpečnost je problematika současná, které je nutno v dnešní době věnovat velkou pozornost.

Dalším z důvodů byla praktická zkušenost v oblasti bezpečnosti IS. Již od roku 1999, jako správce informačních systémů a následně jako správce sítě na Fakultě managementu a ekonomiky, jsem byl nucen řešit nespočet bezpečnostních incidentů. Tato oblast mě zajímá, a nadále se jí věnuji v rámci doktorského studia na Fakultě aplikované a informatiky.

Všechny tyto skutečnosti ovlivnily zaměření mé disertační práce a doufám, že naplním stanovené cíle a práce bude přínosem jak po stránce teoretického poznání, tak po stránce praktického využití.

Detekce hrozeb je nyní trvalý trend a zároveň nutnou součástí každého informačního systému. Proto jsem si také vybral tuto problematiku k řešení.

2 CÍLE DISERTAČNÍ PRÁCE

Hlavním cílem je výzkum v oblasti detekce online hrozeb s aplikovaným výstupem výzkumu v návrhu inovativních, efektivních a přínosných metod detekcí ve virtuálním prostředí respektující současný vývoj jak v hrozbách, tak v bezpečnosti IT zaměřených na rozsáhlé korporátní - podnikové sítě. K naplnění hlavního cíle je nutné uskutečnit následující dílčí cíle:

- Vymezení pojmů z informační bezpečnosti a detekce útoků.
- Přístupy a koncepty detekce hrozeb, včetně jejich silných a slabých stránek.
- Definování postupů a způsobů detekce, kterými lze efektivně zvýšit zabezpečení těchto systémů.
- Identifikovat klíčové faktory ovlivňující bezpečnost ve virtuálním prostředí.
- Možnosti inovace a rozšíření na již realizovaných systémech detekce
- Realizace zpracování detekce online hrozeb za účelem nalezení vhodných postupů a nástrojů využitelných v oblasti zabezpečení informačních systémů
- Analyzovat možnosti aplikace navrženého systému a vyhodnocení experimentů na vybraných systémech v laboratorních podmínkách na aktuálních hrozbách.

3 ZVOLENÉ METODY ZPRACOVÁNÍ

Úspěšná realizace základního cíle a dílčích cílů práce vyžaduje využití vhodných metod zpracování. Metody vědecké práce se většinou vzájemně kombinují a doplňují.

K dosažení stanovených cílů jsou použity následující metody:

- Rešerše

Rešerše dostupných informačních zdrojů se zaměření na systémy detekce a popisy incidentů, ohrožující informační systémy.

Cílem rešerše bylo zjistit:

- Jaké jsou základní typy bezpečnostních řešení?
- Jaké je rozdělení dle přístupu k detekci anomálií?
- Jaké jsou výhody a nevýhody stávajících řešení?
- Jakých metod lze použít k zvýšení účinnosti detekce on-line hrozeb ve virtuálním prostředí?
- Jaké jsou hrozby, které ohrožují informační systémy?
- Jaké mají silné a slabé stránky?

K vzhledem nedostatku české literatury, na zadané téma, které se dynamicky vyvíjí, byly analyzovány především zahraniční zdroje.

Při řešení disertační práce jsou využity i další metody vědecké práce:

- Analýza a syntéza

Metody analýzy je využito pro vyhodnocení poznatků týkající se vyhodnocení stávajících systémů detekce a aktuální hrozeb. Naopak s využitím syntézy jsou propojeny poznatky získané literární rešerší, konzultacemi s odborníky s cílem identifikovat klíčové faktory, které ovlivňují zabezpečení systémů a jsou podstatné pro detekci incidentů.

4 ZÁKLADNÍ TYPY BEZPEČNOSTNÍCH ŘEŠENÍ

Následující kapitola se zabývá možnostmi detekcí hrozeb ve virtuálním prostředí. To zahrnuje základní přehled klasifikace systémů detekce narušení bezpečnosti, a popisuje některé základními pojmy z metodologie: detekci anomálií a základní mechanismy detekce anomálií.

4.1 Host a network-based systémy

Systémy detekce a prevence narušení se dělí na systémy detekce narušení IDS (intrusion detection system) a systémy prevence narušení IPS (intrusion prevention system). Dále lze systémy detekce a prevence narušení dělit na host-based (host based IDS, tj. HIDS) a network-based (NIDS). Pro obě kategorie je společné kontinuální sledování systému, schopnost upozornit administrátora na odhalený útok a záznam průběhu útoku. HIDS systémy se nasazují přímo na jednotlivé servery nebo uživatelské stanice. Jedná se o softwarové produkty, z čehož vyplývá, že možnost jejich nasazení je limitována podporou pro používané operační systémy na sledovaných počítačích. Monitorují systémová volání, logy, chybová hlášení a podobně. Chrání před útoky na operační systém a aplikace provozované na počítači. Dokáže vyhodnotit úspěšnost případného útoku.
A komplexnější NIDS, které využívají informace získané z celého segmentu lokální sítě.[39]

4.2 Systém detekce narušení

Systém detekce narušení IDS slouží k odhalování pokusů o narušení integrity, utajení a dostupnosti dat v chráněné síti. Jedná se o soubor nástrojů, metod a zdrojů, které nám pomáhají identifikovat, zpřístupnit a hlásit neautorizované a neschválené aktivity. Jedná se o pasivní systém, který pouze upozorňuje a sám nečiní aktivní protiopatření. Prostřednictvím upozornění a statistik poskytuje obsluze informace o zaznamenaných útocích. Jde jen o jednu část ochrany celkového ochranného systému. Detekuje také aktivity provozu, které nemusejí nutně znamenat ohrožení systému.

Některé klasické IDS umí také aktivně reagovat na detekovaný útok. V tomto případě se většinou jedná o spolupráci s firewallem, který dynamicky mění části své politiky tak, aby zamezil komunikaci vyhodnocené jako útok. Takto kooperují například systémy podporující standard OPSEC . [22]

Funkcionalita tohoto řešení však plně nenahrazuje systém prevence narušení – IPS je schopen zastavit spojení ještě před jeho navázáním, protože nemusí navazovat spojení s firewallem a ten nezpracovává požadavek IDS. [45]

V případě šifrovaných přenosů navíc paradoxně klesá účinnost detekčních nástrojů, které jsou schopny přímo na firewallu odhalit některé pokusy o průnik,

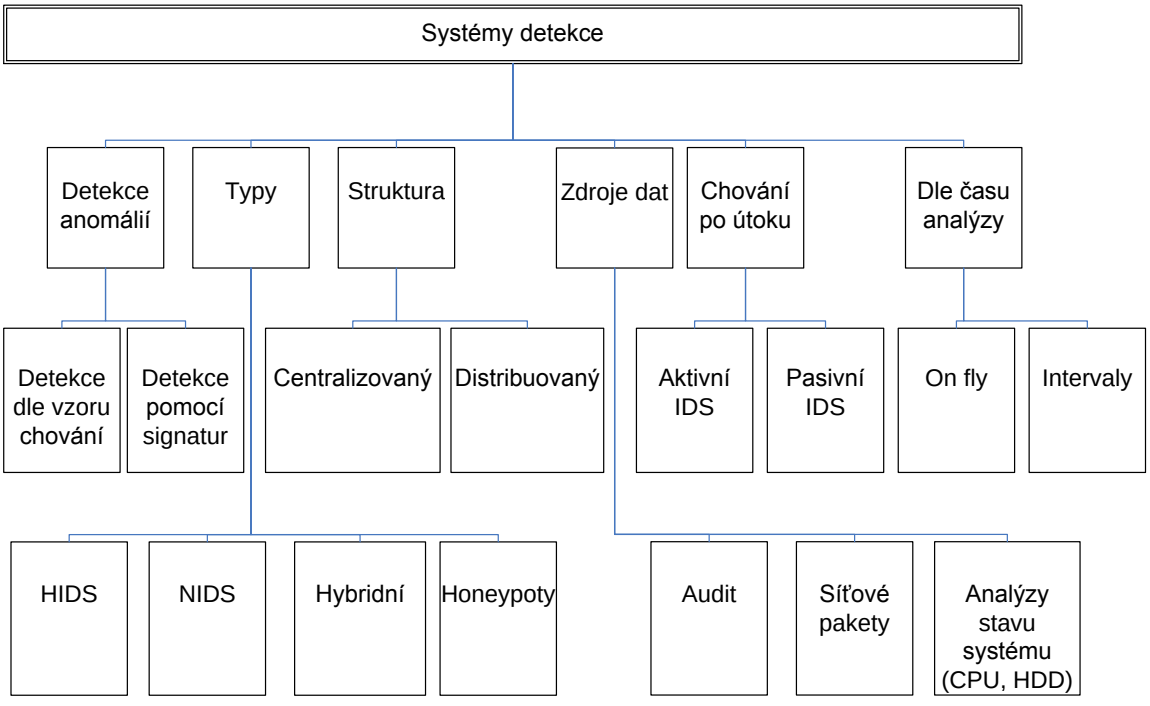
konkrétně mám na mysli IDS, které fungující na principu vyhledávání „škodlivých vzorků“ přímo v komunikačních kanálech. Tyto metody mohou v případě WWW serverů velmi dobře fungovat s protokolem HTTP, nikoliv však s protokolem HTTPS. V této oblasti samozřejmě existují řešení, která pamatují i na HTTPS variantu – šifrované spojení může uživatel navázat nikoli přímo s WWW serverem, ale s firewallem, který se stane „prostředníkem“ v komunikaci, řešením může také být nasazení patřičného detekčního systému přímo na WWW server.

4.3 Klasifikace systémů detekce

Systémy detekce používají jednu ze dvou hlavních detekčních technik. První z nich, detekce anomálií, zkoumá otázky spojené s detekcí odchylek od normálního systému nebo chování uživatele. Druhá, detekce vzorů, využívá popisy vzorů a známých signatur útoků. Obě metody mají své nesporné výhody a nevýhody, stejně jako využití ve vhodných oblastech.

Při třídění oblastí rozdělujeme systémy detekce narušení bezpečnosti (IDS) dle zdrojů dat. K dispozici je řada nástrojů IDS, které využívají informace získané z jednoho hostitele (systému) – to jsou (host based IDS, tj. HIDS) a ty, IDS, které využívají informace získané z celého segmentu lokální sítě (network based IDS, tj. NIDS).

Níže zobrazené schéma ukazuje komplexní rozdělení systémů detekce dle různých přístupů k této problematice. [27]



Obr. 4.1: Klasifikace systémů detekce narušení bezpečnosti

5 DETEKCE ANOMÁLIÍ

Systémy detekce narušení musí být schopny rozlišovat mezi normální (nekritickou bezpečnou) a abnormální činností uživatele, a musí detekovat škodlivé pokusy včas. Nicméně rozpoznávání chování uživatele v souladu s bezpečnostními pravidly není tak jednoduché, mnohé typy chování jsou nepředvídatelné a nejasné. Aby bylo možné klasifikovat tyto akce, systémy detekce průniku využívají detekce anomálních přístupů, někdy označované jako chování založené na rozpoznání signatur, tj. podle známých typů normálního chování, nebo také založené na znalostech.

5.1 Detekce dle vzoru chování

Vzory chování jsou vhodné při hodnocení jak uživatele, tak i chování systému. Detektory anomálií jsou postavené na profilech, které představují běžné použití. Systém funguje na porovnání dříve vytvořeného profilu chování a dle aktuálního profilu chování. Porovnání těchto profilů odhalí možné nesoulady a může detekovat pokusy o útok. Nejprve musíme nastavit počáteční profily systému s ohledem na chování uživatele.

To je problém spojený s profilováním: nejprve systému dovolíme, aby "se učil" na jeho vlastních, zkušených uživatelích a cvičíme systém do bodu, kde se dříve dotěrné chování systému stává normálním chováním. Porovnání s aktuálními generovanými profily bude schopen detekovat všechny možné rušivé činnosti. Dále je zde zřejmá potřeba profily aktualizovat a aplikovat systém vzdělávání, což je obtížný a časově náročný úkol.

Všechny aktuální profily chování, které neodpovídají sadám normálních profilů chování, lze považovat za podezřelé akce. Proto se tyto systémy vyznačují velmi vysokou účinností detekce a jsou schopni rozeznat mnoho útoků, které jsou nové pro systém. Nevýhoda je jejich náchylnost k vytváření falešných poplachů, což je obecný problém. [21]

5.1.1 Výhody této metody detekce anomálií

Možnost detekce nových útoků, menší závislost na IDS, na operačním prostředí (ve srovnání se systémy detekcí útoků dle signatur), schopnost odhalovat zneužívání uživatelských oprávnění.

5.1.2 Největší nevýhody této metody

Je podstatný počet falešných poplachů. Zneužití systému nelze vysledovat v průběhu tvorby profilu, protože všechny uživatelské aktivity během těchto fází jsou legitimní.

Uživatel chování může měnit s časem, což vyžaduje neustálou aktualizaci databáze profilu normálních chování (to může znamenat, že je třeba čas od času

uzamknout systém, který je spojen s větším množstvím falešných poplachů). Pak je nutnost přepravit testovací systém pro testování se škodlivými typy chování, pro ověření správnosti systému.[25]

Obr. 5.1: Chování uživatelů v systému [25]

5.2 Detekce dle rozpoznávání nebezpečných signatur

Systémy mají uložené informace o abnormální, rizikovém chování systému. Jsou často používány v real-time systémech detekce průniku (z důvodu jejich nízké výpočetní složitosti).

Signatury se dělí do dvou kategorií:

- Signatury útoku - popisují vzory akcí, které mohou představovat bezpečnostní hrozbu. Typicky jsou prezentovány jako časově závislý vztah řady činností, které mohou být prokládané neutrálními prvky.
- Pomocí detekce vybraných textových řetězců, které vypadají na podezřelé akce (například - /etc/passwd).

Jakákoliv akce, která není považována za jednoznačně zakázanou, je dovolena. Jejich přesnost je velmi vysoká (nízký počet falešných poplachů). Ale ani tyto typy nedosahují stoprocentní detekci a nejsou imunní vůči novým útokům.

Jsou dva hlavní přístupy spojené s rozpoznáním nebezpečných signatur:

- Detekce na úrovni rozpoznání paketů zneužívající chyby v IP, TCP, UDP nebo ICMP paketech. Velmi jednoduše lze ověřit, zda paket je legitimní nebo ne. Obtíže se mohou vyskytnout s možností fragmentaci paketů a nutností jejich sestavením. Je dobře známo, že hackeři používají fragmentaci paketů, aby se vyhnuli mnoha IDS nástrojům.
- Ověřování protokolů na úrovni aplikační vrstvy - mnoho typů útoků využívá programové nedostatky. Aby bylo možné účinně detekovat takové útoky, musí IDS kontrolovat více aplikačních vrstev. [39]

5.2.1 Metody detekce dle signatur mají následující výhody

- velmi nízký počet falešných poplachů
- jednoduché algoritmy
- snadné vytváření databází útoku podpisu

- snadné implementace
- typicky minimální využití systémových zdrojů.

5.2.2 Některé nevýhody

- Obtíže při aktualizaci informací o nových typech útoků (nutná neustálá aktualizace)
- Nemožnost detekovat nové typy útoků
- Nutnost propojení na IDS s analýzou a systémem záplatování bezpečnostních děr, což je časově náročný proces
- Detekuje pouze útoky závislé na operačním systému (verze, platforma, používané aplikace atd.)
- Mají problémy s vnitřními útoky. Typické zneužití oprávnění uživatele není detekováno jako nebezpečná činnost (z důvodu nedostatku informací o uživatelském oprávnění)

Komerčně nabízené produkty IDS často používají metodu detekcí signatur ze dvou důvodů. Za prvé, je to jednodušší danou signaturu spojit se známým útokem a přiřadit jméno k útoku, např. Ping of Death, která se používá na celém světě.

Zadruhé, musí být databáze popisů útoků pravidelně aktualizována (přidáním popisu nově objevených útoků a zneužití), které mohou vytvářet docela dobrý zdroj příjmů pro dodavatele nástrojů IDS. Aktualizace databáze je zároveň méně náročný úkol, než je spojená se změnou chování uživatelů typových programů. [39]

5.3 Vlastní detekce dle vzorů chování

Třetí metoda detekce narušení bezpečnosti je podrobnější než dvě dříve zmíněné. Je to z důvodů skutečnosti, že správce systému monitoruje různé atributy systému a sítě (ne nutně určených k zabezpečení, např. vytížení procesoru). Platí zde pravidlo, že informace získané tímto způsobem jsou konstantní na specifické prostředí. Tato metoda shromažďuje informace z každodenního sledování provozních zkušeností správců jako základ pro detekci anomálií. To lze považovat za zvláštní případ metody Normální detekce chování. Rozdíl spočívá v tom, že profil je zde součástí lidského poznání.

Jedná se o velmi silnou techniku, protože umožňuje detekci na neznámý typ útoků. Provozovatel systému může odhalit jemné změny, které nejsou zřejmé ostatním systémům. Jeho vlastní nevýhoda je spojena s tím, že lidé musí pochopit komplexní proces, a proto se může stát, že některé typy útoků mohou projít nepozorovaně. [27]

6 HONEYPOTY

Honeypot můžeme považovat za systém detekce incidentů, v tom smyslu, že honeypot láká útočníky (jako včely na med) a pak zaznamenává všechnu jejich činnost, kterou útočník vyvíjí proti pasti. Myšlenka honeypotů, tedy medových hrníčků, není otázkou posledních měsíců. Tato myšlenka je založena na tom, že vytvoříme systémy, které nemají řádné zabezpečení a pozorně sledujeme dění na těchto systémech. Již v této fázi je nutné udělat první koncepční rozhodnutí. Pokud je útoků na naši síť velké množství a chceme monitorovat pouze reálné útoky, průzkumy či nové viry, vytvoříme "produkční" honeypot.

Tento typ honeypotů se vyznačuje tím, že není uveden v DNS, nevedou na něj žádné linky ani jiné odkazy. Jeho hlavní výhodou je naprosto nulové množství falešných poplachů. Pokud totiž vyjdeme z myšlenky, že systém, který neposkytuje žádné služby a nemá žádnou produkční hodnotu a nemá existovat, dojdeme logicky k závěru, že každou komunikaci s "produkčním" honeypotem lze chápat jako útok. [48]

Pokud však chceme studovat nové metody útočníků, virů atd., pak zvolíme "studijní" honeypot. Tento typ je v některých oblastech přesným protikladem produkčního honeypotu. U tohoto typu honeypotu volíme "lákavé´" DNS jméno např. fw.firma.cz, firewall.firma.cz, mail.firma.cz apod. Ve vnitřní síti se pak použijí jména typu mzdy, personální atd. Takto zvoleným jménem si zajistíme dostatek materiálu pro další studium potenciálního nepřítele.

Honeypot servery jsou dedikované servery, pracovní stanice a celé sítě shromažďující informace o útočnících a vetřelcích, kteří napadají počítačové systémy. Je důležité mít na paměti, že honeypot nenahrazuje tradiční bezpečnostní systémy, ale pouze je doplňuje. Honeypot funguje jako vábnička a může vám prozradit například tzv. backdoor útoky, kdy útočník přebere kontrolu nad nějakým serverem ve vnitřní síti (např. díky červu využívajícímu bezpečnostní díry v programech) a interaktivně pak stáhne důvěrná data. Z pohledu sítě se jedná o běžný provoz, z pohledu firewallu se může jednat o spojení iniciované zevnitř sítě, takže tento typ útoků je velmi těžké odhalit. Pak honeypot simuluje útočníkům různé služby sítě, a jeho sledováním se můžeme o útoku a jeho rozsahu dozvědět více. Umožní nám detekovat i šifrované útoky, které klasické IDS nejsou schopny registrovat.

Honeypoty dělíme do základních skupin. Jsou to tzv. low-interaction, medium-interaction a high-interaction. Rozdíly mezi těmito skupinami jsou zřejmé již z názvu. [48]

Zatímco low-interaction poskytují často pouze přihlašovací prompt, který se jen tváří jako nějaká služba a neumožňují sledovat chování útočníka po proniknutí do systému, high-interaction dávají útočníkovi k dispozici nejen

službu či její část, ale celý stroj včetně operačního systému. Nevýhodou low-interaction honeypotu je skutečnost, že se dozvíme výrazně méně informací než u high-interaction, neboť tam je možné sledovat i to, co útočník dělá, jak se snaží za sebou "zametat stopy" atd. Low-interaction honeypots mají podstatnou výhodu ve zpracování nasbíraných údajů, neboť to je obvykle podstatně jednodušší. [42]

Low-interaction honeypoty jsou jednoduší na instalaci, konfiguraci a implementací, díky své jednoduché konstrukci a pouze základním funkcím. Tyto typy pouze napodobují celou řadu služeb. Útočník je omezen pouze na vybrané služby. Například nastavíme honeypot na emulaci standartního unixového serveru s několika vybranými službami, jako je SSH a FTP. Útočník skenováním pouze zjistí, o jaký systém se jedná a které služby na něm běží. Pak může pomocí útoku hrubou silou se pokusit o přihlášení. Honeypot zachytí tyto pokusy, ale nedovolí útočníkovi se přihlásit, protože tam žádný skutečný systém není. Útočníkova iterace je tak pouze omezena na pokusech o přihlášení.

Dalším podobným příkladem je napodobit FTP, kde je povoleno anonymní přihlášení na honeypot. Útočník se přihlásí a může si stáhnout kopii souborů s hesly. Tento soubor je ovšem neplatný. Interakce je tady omezena jen na pokus o přihlášení anonymní přístup a možnost stáhnout si soubor s hesly.

Kombinace skupin low-interaction a high-interaction je medium-interaction honeypot. Není to pouze jednoduchá emulace služeb. Taky ale služby nejsou tak dokonale simulovány jako u high-interaction honeypotu. Tento fiktivní systém poskytuje pouze vlastní emulované prostředí s omezeným přístupem do systému. Útočník se po napadení domnívá, že se jedná o reálný systém. To dává dostatek času odhalit tuto akci pomocí IDS.

Celkově je honeypot systém svým nastavením snadnější kořistí pro vetřelce než ostré produkční systémy, ale je upraven menšími systémovými modifikacemi tak, aby jejich aktivita byla zaznamenávána pro pozdější vysledování útoku. Hlavní myšlenka je, že vetřelec pronikne do systému a umožní mu opakovat své návštěvy. Během těchto následujících návštěv jsou informace shromážděny a zaznamenávány. Bezpečnost honeypotu musí být neustále sledována a ošetřena proti zneužití, které by se mohlo vymknout kontrole. Pokud je dobře nastaven a monitorován, tak je pramalým rizikem pro zbytek sítě.[48],[16]

Dalším využitím high-honeypotů je detekce, sledování a lokalizace botů. Bot je malware, který je bez vědomí uživatele nainstalován na uživatelském zařízení. Obsahuje komunikační a řídící modul a umožňuje neautorizovanému uživateli vzdáleně tento počítač ovládat a využít pro plnění různých příkazů. Jelikož komunikace mezi boty je šifrována a neustále dynamicky mění řídící servery, i přesto se dá pomocí honeypotů určit řídící centrum, a následně omezit jeho činnost v naší síti. [5]

6.1 Výhody a nevýhody honeypotů

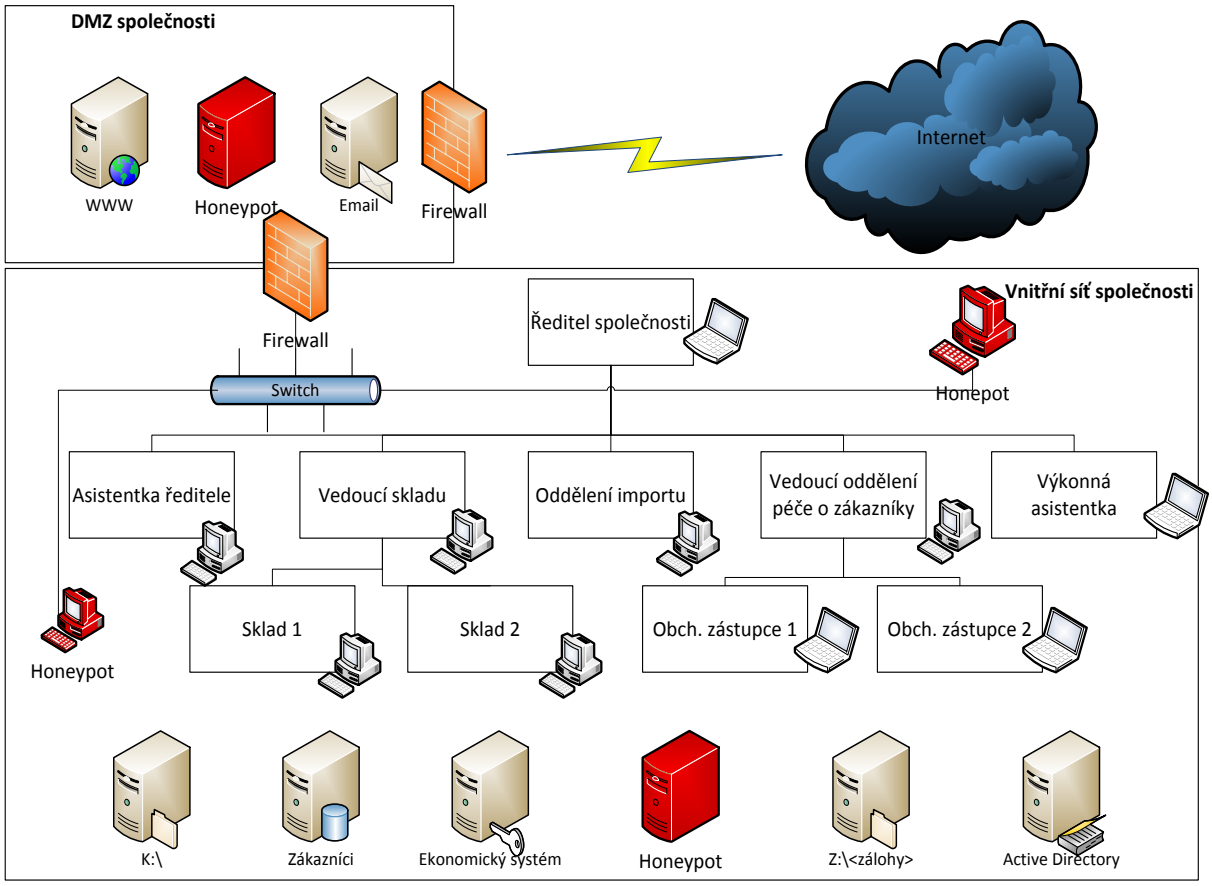
Honeypoty nám nabízejí mnoho výhod a nevýhod. Výhody spojené s honeypot technologiemi jsou: [42][49]

- Hodnota dat: Honeypoty produkují relativně málo údajů, ale velmi cenné ve srovnání s firewally, systémovými logy a IDS. Tyto aplikace produkují velké množství dat, která se pak těžce vyhodnocují. V honeypotu jsou získané údaje potenciálním upozorněním na skenování prostředí nebo útok.
- Zdroje: Honeypoty jsou pasivní prvky v síti. Tyto systémy čekají na činnost útočníků. Naopak systémy firewallů a IDS generují mnoho informací a ty mohou zahltit administrátory.
- Jednoduchost: Honeypoty, především low-interaction honeypoty, stačí pouze nainstalovat a spustit.
- Někde v síti organizace vyčkávají na aktivitu útočníků. Tato vlastnost zabraňuje chybné konfiguraci. Je to další výhoda oproti komplexním systémům.
- Návratnost investice: Honeypoty umí prokázat svou hodnotu. Pokud nasadíte honeypot a honeypot upozorní na útok, pak můžeme okamžitě vidět jeho přínos k bezpečnosti. Ostatní systémy, které má organizace na zajištění bezpečnosti, například firewally, nemají tuto charakteristiku a administrátor si není jistý, zda tento firewall je dobrý nebo není.

Bohužel však tato technologie přináší některé podstatné nevýhody, které jsou následně popsány:

- Úzké zorné pole: Největší nevýhodou honeypoty je, že mají úzký zorné pole. Honeypoty detekují pouze aktivity proti nim, ale žádné jiné aktivity ve zbytku sítě. To je hlavní důvod pro použití honeypotů spolu s dalšími prvky pro ochranu síťe (firewally, IDS, …).
- Fingerprinting

  Fingerprinting – slouží k zjišťování parametrů operačního systému Toto je další nevýhodou honeypotů, zejména komerčních verzí. Pokud útočník identifikuje honeypot může tuto identifikaci použít v budoucnu. Pak se snáze bude vyhýbat honeypotů a ty nebudou schopny útok detekovat. Pak to není užitečným prvkem. [32]
- Riziko: Honeypoty představují riziko pro organizaci. Když honeypot není správně nastaven a udržován, je pravděpodobné, že může být zneužit k útoku, infiltrovat a poškodit jiné systémy. Riziko se liší v závislosti na velikosti úrovně interakce, tj. zvyšuje s úrovní interakce nasazenými honeypoty.



Obr. 6.1: Tradiční rozmístění honeypotů v síti společnosti

6.2 Rozšíření honeypotů

V následujících kapitolách jsou uvedeny speciální verze implementací honeypotů které jsou modifikace výše uvedených základních typů.

6.2.1 Honeynet

Další pojem související s honeypoty je honeynet. Honeynet je jako honeypot, ale místo toho aby to byla jedna past, tak je to síť rozmístěných pastí, které upozorňují nebo shromažďují informace o útocích. Honeynets může být použito v sítích LAN, ale i WAN. Honeypoty shromažďují více údajů, než jednoduchý honeypot. Poskytují lepší a komplexnější údaje k pochopení útoku. [60]

6.2.2 Virtuální Honeynet

Klasické řešení honeypotu znamená, jeden počítač jeden honeypot. Virtuální řešení nabízí možnost honeynetu (skupina honeypotů) na jednom počítači. Pojem virtuální, v tomto případě znamená, že na jednom fyzickém stroji běží několik nezávislých počítačů, s možností různých operačních systémů. V praxi to znamená, že na hardware naistalujeme speciální operační systém (hypervisor), který umí vytvořit virtuální počítače a propojit je pomocí virtuální sítě.

Toto řešení má ale některé výhody a nevýhody oproti tradičnímu řešení honeypotů. [18],[58]

Výhody:

- Snížení nákladů na implementaci a provoz
- Jednoduchý management
- Jednoduchý způsob klonování virtuálních strojů
- Jednoduchá správa síťových připojení
- Flexibilita nasazení

Nevýhody:

- Existuje možnost kompromitace hypervisoru, a tím můžeme ovládnout nainstalované virtuální počítače (hosty). [6]
- Existuje možnost detekce, že počítač běží ve virtuálním režimu. Dřív to znamenalo, že se jedná na 100% o honeypot. V dnešní době ale běží 90% serverů ve virtuálním prostředí, a provozujeme zde i nezanedbatelné množství pracovních stanic. [43],[19]

6.2.3 Honeypoty na produkčních systémech

Je speciální verze honeypotu, implantována v produkčním systému. Pokud uživatel nemá přístup k produkčním systémům, povolíme mu na produkčním systému se přihlásit. Po ověření ale není vpuštěn do produktivní verze, ale do sandboxu, s imaginárními daty. Útočník má pocit, že operuje uvnitř napadnutého systému, ale nalézá se pouze v sandboxu, který je monitorován. Všechny informace o aktivitách útočníka předává řídicímu systému. Závisí na systému administrátora, jestli bude o tomto honeypotu informovat uživatele. Může posloužit i jako možnost zachycení neautorizovaných přístupů do autorizovaných systémů.

6.2.4 Honeyfarm

Dva a více honeypotů tvoří honeynet. Obvykle se používá pro sledování větší nebo rozmanitější sítě, ve které několik kusů honeypotů nemusí být dostačující. Honeynets a honeypot jsou obvykle implementovány jako součást větších síťových systémů pro detekci narušení. Honeyfarm je centralizovaný sběr honeypotů a systém analytických nástrojů. [59]

6.2.5 Honeypot agent

Další doplňkem výše uvedeného řešení je honeypot agent. Původní řešení systému honeypots mělo jedno velké omezení. Honeypots vyčkávali na útočníka a jeho role byla pasivní. V návrhu tohoto řešení se stávalo, že útočník si honeypots nevšiml a prováděl svou činnost, aniž by byl detekován tímto systémem. Proto jsme toto řešení rozšířili o agenta, který nasměřuje útočníka na systém honeypots.

Jelikož tyto typy útoků simulují chování uživatelů, musí agend podstrčit útočníkovi i uživateli malou past. Podstata pasti spočívá v rozdílu chování mezi stálým uživatelem a botem. V uživatelském systému jsou pomocí agenta nastaveny pasti. Běžnému uživateli jsou na první pohled skryty, nebo nejsou zajímavé pro jeho práci. Například si běžný uživatel nevšímá systémových souborů, různých TMP adresářů, a podobně. Bot se snaží naopak provést sběr informací o napadnutém systému, a proto prohledává všechna zákoutí systémů. To je fáze, kde přicházejí na scénu Honeypot systémy, které nabízejí zajímavé informace pro boty. V následující kapitole představíme všechny kroky, jak systém funguje.

6.3 Aktuální stav

Koncept honeypotu se poprvé objev v roce 1990 v knize Cliffa Stolle „The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage“ [50] a v roce 1991 v článku Billa Cheswicka [23]. V roce 1997 Fred Cohen zařadil honepoty do systému Deception Toolkit, což je sada bezpečnostních nástrojů určených na ochranu informačních systémů.[9] V roce 1997 vznikl projekt The Honeynet Project. Práce této organizace přispěly ke zvýšení informovanosti a ukázaly hodnotu technologie honeypot. Jsou vydávány série prací pod společným názvem “Know your enemy”, a shromažďuje informace o této technologii. [41]

V dnešní době se koncept honeypotů se používá v aktuálních významných projektech:

- Projektu Honey Pot, kde honeypoty používají v rámci distribuovaného systému pro identifikaci spammerů. [56]
- Projekt Nepenthes se používají honeypoty k zachycení a studovaní nových typů útoků. [61]
- Glastopf Project shromažďuje data z útoků na webové aplikace. [44]http://glastopf.org/
- Projekt Honeyd - Jedná se o systém low-interaktion honeypotů použitých pro zachycení aktivit útočníků. [42]
- Projekt HoneySink – Tento projekt se zaměřuje na monitorování systémů botů a jejich eliminaci. [2]
- Projekty v rámci Nic.cz [33] a Cesnet.cz [8] na monitorování aktivit útočníků v rámci těchto sítí.

6.4 Právní otázky

Další bod, který je třeba zmínit, jsou právní problémy spojeny s honeypoty. Základní aspekty jsou:

- odpovědnost
- soukromí

Musíme právně ošetřit odpovědnost pro organizaci nebo osobu, které systém honeypotů implementovala. Musíme vzít v úvahu tu možnost, že pokud útočník infiltruje honeypoty, můžou být zneužity k ohrožení jiných systémů a to může mít právní následky. [49]

Další složité téma je soukromí. Úroveň ochrany osobních údajů závisí na úrovni interakce a nasazení honeypotů. V sítích high-interaction honeypotů je ztráta soukromí uživatelů akutní zejména proto, že honeypoty jsou vysoké interakční systémy rozmístěné v síti a sbírají informace o útočnících a uživatelích. Například na high-interaction honeypotech jsme schopni zachytit konverzaci útočníků pomocí IRC kanálů. Proto je důležité stanovit, jaké informace mohou být zachyceny. [49]

7 AKTUÁLNÍ SITUACE HROZEB

Pro úspěšnou instalaci a činnost IDS musíme velmi dobře pochopit chování útočníků. Klasickým trendovým útokům zabráníme komerčním řešení, které zachytí 90% incidentů. Většinou tyto incidenty sledují okamžitý zisk a výnos, a po průniku do systému po určité době sami zaniknou. Tyto hrozby jsou nasazeny masově za účelem získání přístupu k velkému množství dat a zdrojů. V návaznosti na ně se v krátké době objeví řešení na jejich detekci a odstranění. Běžným případem jsou bankovní trojské koně, které se snaží infiltrovat velké množství počítačů a snaží se získat přístup k finančním účtům obětí. Tyto hrozby jsou velmi obecně zaměřeny na rozsáhlé cílové skupiny. Pokud narazí na cíl s vyšší ochranou, nevynakládají větší úsilí na jeho infiltraci a raději se zaměří na systémy s minimálním zabezpečením. I pokud se jedná o částečně cílený útok, například na klienty jednoho bankovního domu, útočníci vždy hledají slabší oběti.

Jinou kapitolou jsou ovšem útoky typu APT. Tyto typy útoků jsou přesně cílené a přesně vědí, co potřebují. Váš systém již není obecný cíl, ale již byl vybrán pro konkrétní důvod. To znamená, že útočníci se přizpůsobí konkrétním situacím a snaží do té doby, pokud není splněn cíl útoku nebo náklady na útok přerostou nad hodnotou získané kořisti.

7.1 APT útoky

Hrozby typu APT jsou sofistikované, vícenásobné útoky na konkrétní organizaci. APT (Advanced Persistent Threat - Přetrvávající pokročilé hrozby) patří do kategorie kybernetických útoků, jejich cílem nejčastěji bývají jak komerční subjekty, politické a státní instituce, tak i jednotlivci. Tyto typy hrozeb vyžadují dlouhodobé vysoké utajení. Jsou prováděny skupinou útočníků, kteří jsou výborně zasvěceni do problematiky. Používají více typů zranitelností k prolomení klíčových bezpečnostních systémů. V počáteční fázi APT se zaměřují na získání informací o konfiguraci sítě a serverových operačních systémů. Později se zaměří na instalaci rootkitů a jiného malware k získání ovládání a na komunikaci s Command & Control Server útočníků. Napadené objekty jsou dlouhodobě kompromitovány za účelem krádeže duševního vlastnictví, kopírování důvěrných a citlivých dat, nebo finančního zisku. Jednotlivé systémy jsou často dlouhodobě infikovány, a po dosažení cílů útočníka někdy vyřazeny z provozu.

7.1.1 Co je to APT

Přesná definice APT neexistuje, ale můžeme vysvětlení shrnout do následujících vlastností: [10],[12]

Advanced - Pokročilé je především proto, že útočník je schopen použít celé spektrum pokročilých technik k tomu, aby pronikl do systému. Ty mohou zahrnovat technologie k infikování systémů, různé zpravodajské techniky a sociální inženýrství. Zatímco jednotlivé komponenty útoku nemusejí být klasifikovány

jako pokročilé (např. malware vyrobený z běžně dostupných komponent nebo nakoupené exploidy), může být subjektivní sestava těchto komponent hodnocena velmi nebezpečně vzhledem k individuálnímu přístupu a vyhlédnutému cíli. K dosažení cíle je potřeba strávit nějaký čas hledáním zranitelnosti a slabých míst v daném systému, a poté sestavit funkční exploit. Začlenit ho například do polymorfního malwaru, vytipovat si konkrétní osobu v dané organizaci a za použití technik sociálního inženýrství dosáhnout toho, aby daná osoba tento malware spustila. Např. tak, že jí zašle mail s přílohou, která bude tento škodlivý kód obsahovat. Dále se může jednat o falešný wifi access point či úmyslně pohozený přenosný disk v prostorách společnosti nebo zaslaný poštou konkrétní osobě, kompromitaci partnera, který je důvěryhodný a má přístup do systému. Těchto možností je spousta.

Persistent – Přetrvávající jsou především proto, že útočníci si potřebují zajistit trvalý přístup do napadené organizace. Snaží se trvale unikat detekci konvenčních systémů zabezpečení, přetrvávat v systému po dlouhou dobu a neoprávněně získávat podnikové informace. Útočnici ale neví, kde přesně se informace nacházejí a snaží se vyvíjet jen malou aktivitu k následnému šíření z důvodu odhalení útoku. Ve skutečnosti tato pomalá aktivita šíření je úspěšná a špatně detekovatelná. Pro případ odhalení, se snaží si vytvořit ještě další přístup do systému. A pokud společnost pojme podezření, že je kompromitována, obvykle nenalezne všechny přístupové body. A útočníci mohou dále vyvíjet svoji činnost.

Threat – APTs jsou hrozbou, protože mají schopnost a záměr. Tyto útoky jsou prováděny koordinovaně pomocí lidského ovládání, než bezduché a automatizované kódy. Útočníci mají konkrétní cíl a jsou dobře vybaveni, motivováni, organizováni a financováni.

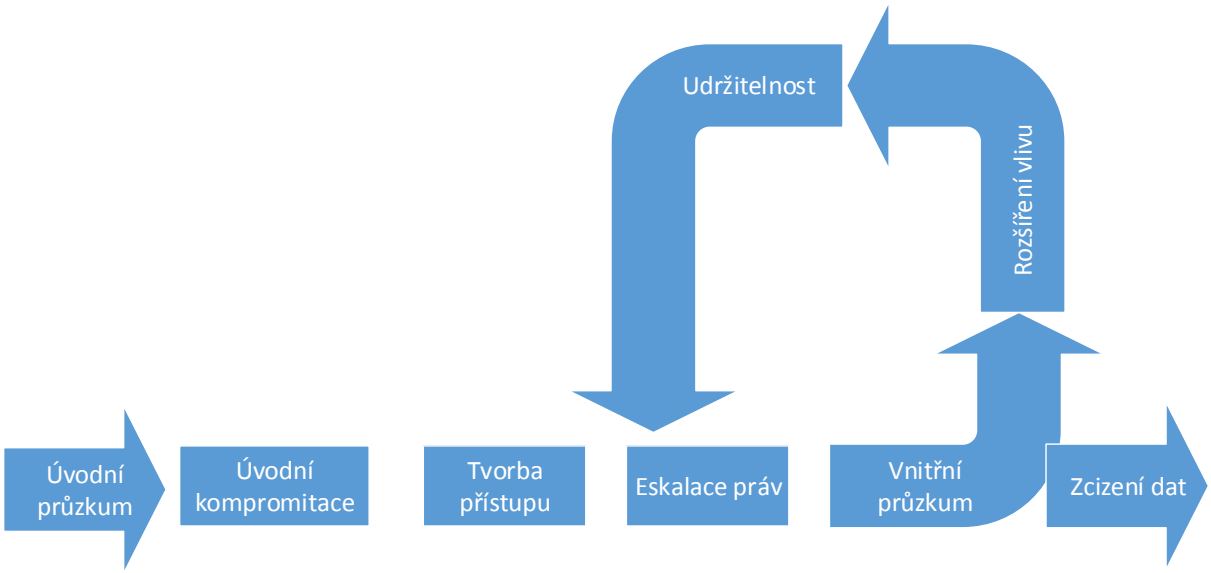
Konvenční útočník nemá zájem o konkrétní cíl. Potřebuje tisíce čísel kreditních karet, proniknout do bankovních účtů, změnit počítače na zombie, nebo cokoliv, co přinese rychlý finanční zisk. Čím větší a aktuální zabezpečení, tím menší riziko útoku. Proti tomu ale APT útočník je jiný, a pokud má konkrétní důvod zaútočit, najde slabé místo v zabezpečení. Zabezpečen proti tomuto druhu útoku je relativní. Jsou trpělivější a pravděpodobně vyzkouší více různých druhů útoků. A tím mají větší šanci na úspěch. [46]

7.1.2 Cyklus APT

APT má již pevně definovanou metodiku, která byla ověřena v posledních letech. Začíná phishing a sociálním inženýrstvím a končí exportem velkých objemů ukradených dat na servery útočníků. Používají techniky a metody, které neustále vyvíjejí a mají velkou schopnost se efektivně přizpůsobit. Udržují své nástroje o krok napřed, než jsou aktuální stavy napadených systémů. [24]

Útočníci mohou mít více paralelně běžících kampaní. Každá se skládá z jedné anebo více operací. Tyto operace jsou většinou rozděleny do více fází. Například

v úvodní fázi je cílem útočníka zajistit počáteční vstupní bod do cílového systému. Následující fáze jsou pak většinou paralelizovány a rozděleny mezi jednotlivé buňky kvůli lepší efektivnosti útoků. Následný odstavec popisuje základní provozní fáze v rámci jednoho APT útoku. V následujících sekcích jsou popsány detaily těchto fází a jejich možná detekce. [34],[13],[14]



Obr 7.1: Cyklus APT útoku

Zvolení cíle

Útočnici si zvolí cíl dle odhadu velikosti a důležitosti budoucího zisku informací, nebo dostanou zadání cíle od zadavatele. V poslední době jsou zadavateli, jak firmy, kteří potřebují konkurenční informace, tak vlády států. Tyto útoky jsou velmi nákladné na potřebné vybavení, tak i na tým lidí, kteří jsou specialisté na konkrétní fáze útoku.

Úvodní průzkum

Provedou úvodní průzkum klasickými technikami softwarového průzkumu anebo například metodami sociálního inženýrství. Zjistí stav zabezpečení, typy systémů, návyky uživatelů. Tento bod je velmi důležitý pro budoucí úspěch kompromitace. Objekt nesmí nabýt dojmu, že bude cílem útoku.[34]

Příprava infrastruktury

APT útoky obvykle zahraňují vysoký stupeň přípravy. Je nutno připravit infrastrukturu na ovládání útoku. Například registrovat potřebné domény u dynamických poskytovatelů.

Dále vytvořit servery pro:

- Ovládání útoku – Command and Control (C2 server) [11]
- Servery pro sběr dat, nejčastěji FTP server
- Webové servery na umístění falešných webových stránek, určených pro phishing.

Pro tyto činnosti je nejlépe využít napadených serverů. Útočníci si hodně často tyto zdroje pronajímají. Dokonce lze zneužít jako C2 server i veřejné služby např. Google code, Google Aps a různé blogovací služby. Komunikace pak s těmito službami nevzbuzuje v napadeném systému podezření a probíhá na protokolu HTTPS. Nikdo nezablokuje například komunikaci s google. A pokud jsou odhaleny, tak velké firmy na toto upozornění nereagují a C2 server může běžet dál. [30]

První kompromitace

Představuje způsoby, kterými se útočníci snaží vniknout do cílové organizace. Nejčastějším způsobem je phishing. Po úvodním průzkumu známe chování cíle, jeho operační systém, systém zabezpečení a verze jeho software. [34],[13]

Phishing je email obsahující buď škodlivou přílohu, nebo hypertextový odkaz na nebezpečný soubor. Předmět a text emailu jsou většinou pro příjemce důležité. Email vypadá, že je odeslán důvěryhodným odesilatelem, a text emailu je důležitý pro příjemce. Může to být kolega, jednatel společnosti, IT oddělení nebo obchodní partner. Je vytvořen v jazyce příjemce.

Doručeno: 25. Září 2013

Od: Josef Novák <josef.novak@firma.cz>

Předmět: Zápis z porady

Vážení kolegové,

v příloze najdete záznam z jednání, které se uskutečnilo dne 13. 9. 2013, včetně přílohy.

Záznam posílám rovněž dalším přítomným účastníkům.

S pozdravem Alois Dvořák, kancelář ředitele

Příloha:

zapis_z_jednani20130901.pdf

Obr.7.2: Ukázka phishingu

Útočník pro tyto emaily nejčastěji vytvoří speciální emailovou schránku na podobné doméně.

Např. pro firma.cz si zaregistruje firma.eu. Tato adresa je ovšem skryta v hlavičce emailu pro odpověď a na první pohled email vypadá, že pochází z domény firma.cz.

V příloze emailu se může nacházet škodlivý software, v našem případě zapis_z_jednani20130901.pdf. To není pravý PDF soubor, ale je to spustitelný soubor exe s ikonou od Adobe.

Obr.7.3: Kompletní název infikovaného souboru

Většinou uživatelé odklepnou informační varování, že se jedná o spustitelný soubor a spustí je. Adresát může na tento email odpovědět, že příloha je poškozena a útočník pod hlavičkou, v našem případě kanceláře ředitele, odpoví na pravým souborem PDF. Adresát tak nabyde dojmu, že vše je v pořádku.

Dalším častým způsobem phishingu je verze, že vás email odkáže na infikované webové stránky. Na těchto stránkách zpustíte kód, který zjistí verzi operačního systému, webového přihlížeče a doplňků v něm. Dle této informace podstrčí exploit, určený pro tuto kombinaci.

Exploit je speciální program, který využívá programátorskou chybu, která způsobí nezamýšlenou činnost software (prohlížeče nebo některého doplňku) a umožní jej ovládnout ve svůj prospěch. V našem případě se jedná o nežádoucí instalaci backdooru na uživatelův počítač.

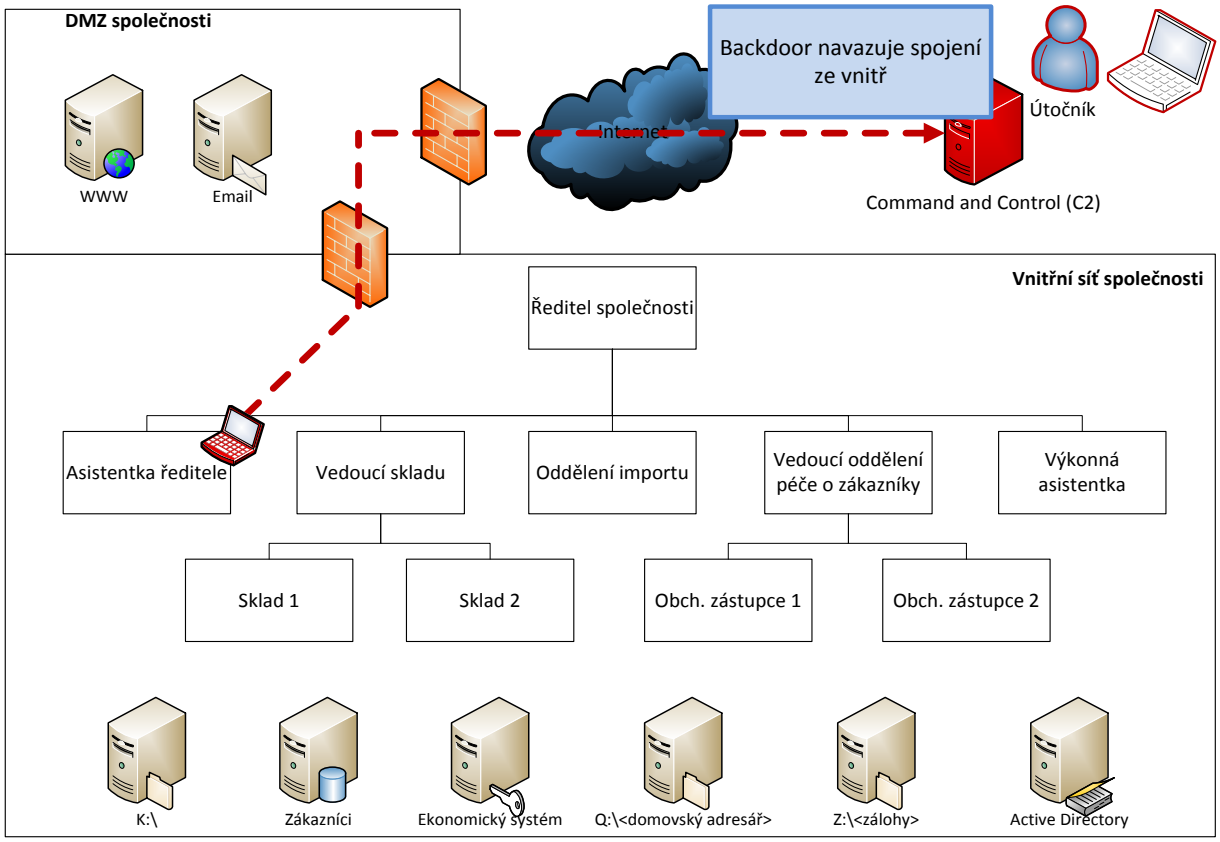
Tento typ útoků rozpoznává i zdroje přístupu. Když přistoupí uživatel, na nějž je útok zaměřen, spustí kód. Pokud přistoupí uživatel, na kterého není útok zaměřen, zobrazí se mu jen bezpečná stránka. Například software prověřující nebezpečné odkazy. Toho můžou docílit například pomocí IP adresy, verzí operačního systému, času přístupu a podobných vhodných kombinací.

Méně častým jevem je kompromitace oběti pomocí sociálních sítí a instant messaging. Instant messaging je internetová služba, která umožňuje svým uživatelům zasílat zprávy provádět hlasové a video hovory, sledovat zda jsou přítomni, přeposílat soubory a jinak komunikovat. Oproti emailu spočívá v přenosu zpráv v reálném čase. Tato forma komunikace je více osobní. Pomocí těchto kanálů útočník odešle oběti hypertextový odkaz směřující na infikovaný web.

Tvorba přístupů

Tato fáze zahrnuje opatření, které zajistí kontrolu cílové sítě v systémech mimo síť. V našem případě při spuštění přílohy z emailu, příjemce spustí nebezpeční exe soubor, z kterého následovně nainstaluje do svého systému backdoor.

Backdoor (zadní vrátka) je software, který umožní útočníkovi projít bezpečnostními mechanismy a posílat příkazy vzdáleně do systému. V každém případě backdoor zahájí komunikaci s venkovním serverem Command and Control (C2). Použitá taktika komunikace z vnitřní sítě ven je těžce kontrolovatelná síťovými firewally. Většinou nerozpoznají, zda se jedná o incident anebo o chování uživatele. Tyto jsou nastaveny na kontrolu komunikace z vně sítě dovnitř. Backdoor se může chovat jako prohlížeč a tímto způsobem je těžce detekovatelný. Komunikační metody mezi těmito systémy jsou od prostého textu s jednoduchým kódováním až po šifrovaný kanál. Na ovládání backodorů používá útočník buď textové příkazy anebo grafické uživatelské rozhraní.



Obr.7.4: Komunikace z infikovaného systému na server řízený útočníkem (C2)

Standartní backdoor typicky komunikuje pomocí http protokolu, který jednoduše splyne s legitimním provozem. Existují i verze, které komunikují pomocí

vlastního protokolu, který si autoři sami navrhnou. Backdoor obsahuje dlouhý seznam funkcí, kterými útočníci mohou ovládat napadený počítač. Mezi hlavní funkce patří:

- Vytvořit/měnit/mazat/spouštět programy
- Nahrát a stáhnout soubory
- Vytvářet a mazat adresáře
- Výpis/zastavení/start procesů
- Editace registrů
- Zachytávání obrazovek uživatelského rozhraní
- Zachytávání kláves
- Zachytávání pohybu myši
- Spuštění příkazové řádku
- Vytvoření grafického vzdáleného přístupu
- Sběr hesel
- Seznam uživatelů
- Výpis informací o okolní síti
- Výpis o okolních počítačích
- Možnost se uspat na určitou dobu
- Odhlásit přihlášeného uživatele
- Vypnout/restartovat systém

Eskalace práv

Tato fáze se zabývá získáváním práv na napadeném systému. Nejčastěji se jedná o jména a hesla, která jím posléze dovolí kompromitovat další systémy. Útočníci používají většinou veřejně dostupných nástroje, k získání legimity uživatele. Jedná se o utility sloužící např. získání hesel uložených v hash registrech Windows. Hesla o rozsahu méně než osm znaků se dají prolomit na rychlých systémech v krátké době. Ale ne všechny systémy používají jednotné přihlašování. Některé systémy mají své separátní přístupové údaje. Například přístupy na k externí databázi, hostovanou u poskytovatele webhostingu. Proto útočník nasazuje nástroj typu keylogger. Keylogger zaznamenává stisky kláves do souboru a později tyto záznamy odesílá útočníkovy na další zpracování. [34],[13]

Další nástroj na získání přístupových údajů je utilita typu form grabbers. Sbírá údaje, které jsou odesílány pomocí webových formulářů v internetových prohlížečích. Funguje bez ohledu na to, zda aplikace odesílá data pomoci protokolu HTTP nebo protokolu HTTPS (Secure Hypertext Transfer Protocol).

Vnitřní průzkum

V této fázi průzkumu sbírá útočník informace o prostředí oběti. Většinou používá primárně vestavěných příkazů, aby prozkoumal systém a síťové prostředí. Jedná se o jednoduché příkazy, které jsou v každém operačním systému. Ale pokud se umí využít tak jsou mocnými nástroji. Tyto úkony nejsou detekovány prozatím žádným komerčními systémy. Pro zrychlení operace, používají dávkové soubory typu .bat a nebo .cmd . [31]

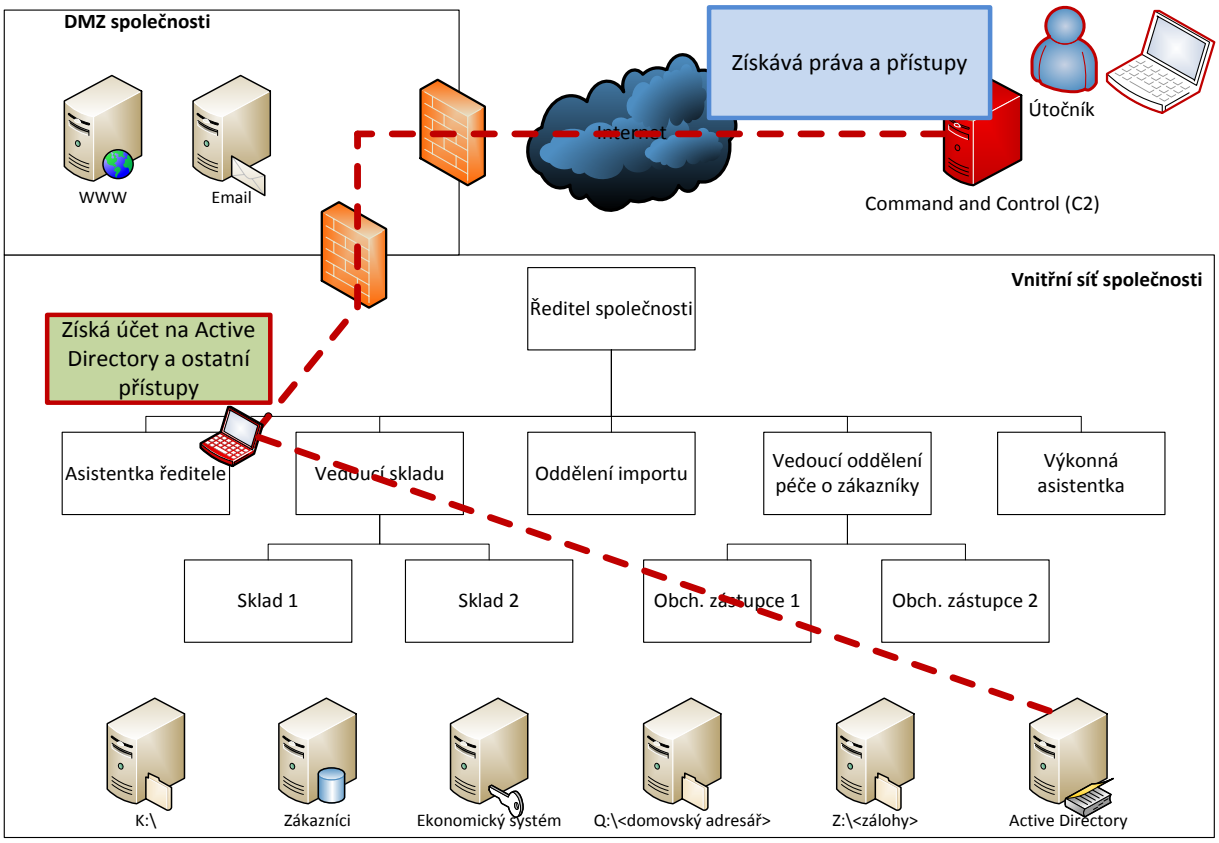
```
ipconfig /all>>”C:\Windows\temp\26.txt”
net start>>” C:\Windows\temp\26.txt”
tasklist /v>>” C:\Windows\temp\26.txt”
net user >>” C:\Windows\temp\26.txt”
net localgroup administrators>>” C:\Windows\temp\26.txt”
netstat -ano>>” C:\Windows\temp\26.txt”
net use>>” C:\Windows\temp\26.txt”
net share>>” C:\Windows\temp\26.txt”
net session>>” C:\Windows\temp\26.txt”
net view>>” C:\Windows\temp\26.txt”
net view /domain >>” C:\Windows\temp\26.txt”
net group /domain>>” C:\Windows\temp\26.txt”
net group “domain users” /domain>>” C:\Windows\temp\26.txt”
net group “domain admins” /domain>>” C:\Windows\temp\26.txt”
net group “domain controllers” /domain>>” C:\Windows\temp\26.txt”
net group “exchange domain servers” /domain>>” C:\Windows\temp\26txt”
net group “exchange servers” /domain>>” C:\Windows\temp\26.txt”
net group “domain computers” /domain>>” C:\Windows\temp\26.txt”
```

Obr. 7.5: Ukázka skriptu použitého v fázi Vnitřní průzkum

Předchozí skript získá následující údaje:

- Výpis nastavení sítě infikovaného počítače, podrobnosti o síťových rozhraních, IP adresy, MAC adresy a zda má statickou IP adresu nebo přidělenou dynamicky pomocí DHCP serveru
- Seznam služeb spuštěných na napadeném systému
- Seznam spuštěných procesů

- Seznam lokálních účtů v systému
- Seznam lokálních administrátorů
- Seznam síťových připojení
- Seznam připojení a sdílených souborů na napadeném systému
- Seznam mapovaných diskových jednotek
- Seznam sdílených disků a prostředků
- Informace o doméně nebo pracovní skupině
- Informace o doméně “domain admins”, ”domain controllers”,“exchange domain servers”,“exchange servers”, domain computers”



Obr. 7.6: Útočník získá legitimní práva z infikovaného počítače

Rozšíření vlivu

Jakmile útočník získá legitimní účty uživatelů a přehled o síti, může se v ní nepozorovaně pohybovat.

- Může se připojit k síťovým prostředkům
- Může vzdáleně spouštět příkazy na jiných systémech

- Může se přihlásit do produkčních systémů pomocí legitimních přihlašovacích údajů

Všechny tyto akce dělá jako legitimní uživatel nebo správce systému, pro správu sítě. Tyto operace jsou velmi obtížné zjistit. [13]

Udržitelnost

V této fázi útočník podniká opatřen pro trvalé zajištění a dlouhodobou kontrolu nad klíčovými systémy v síti z vnějšího prostředí. Existuje více možností:

- Použít legitimní VPN přístup

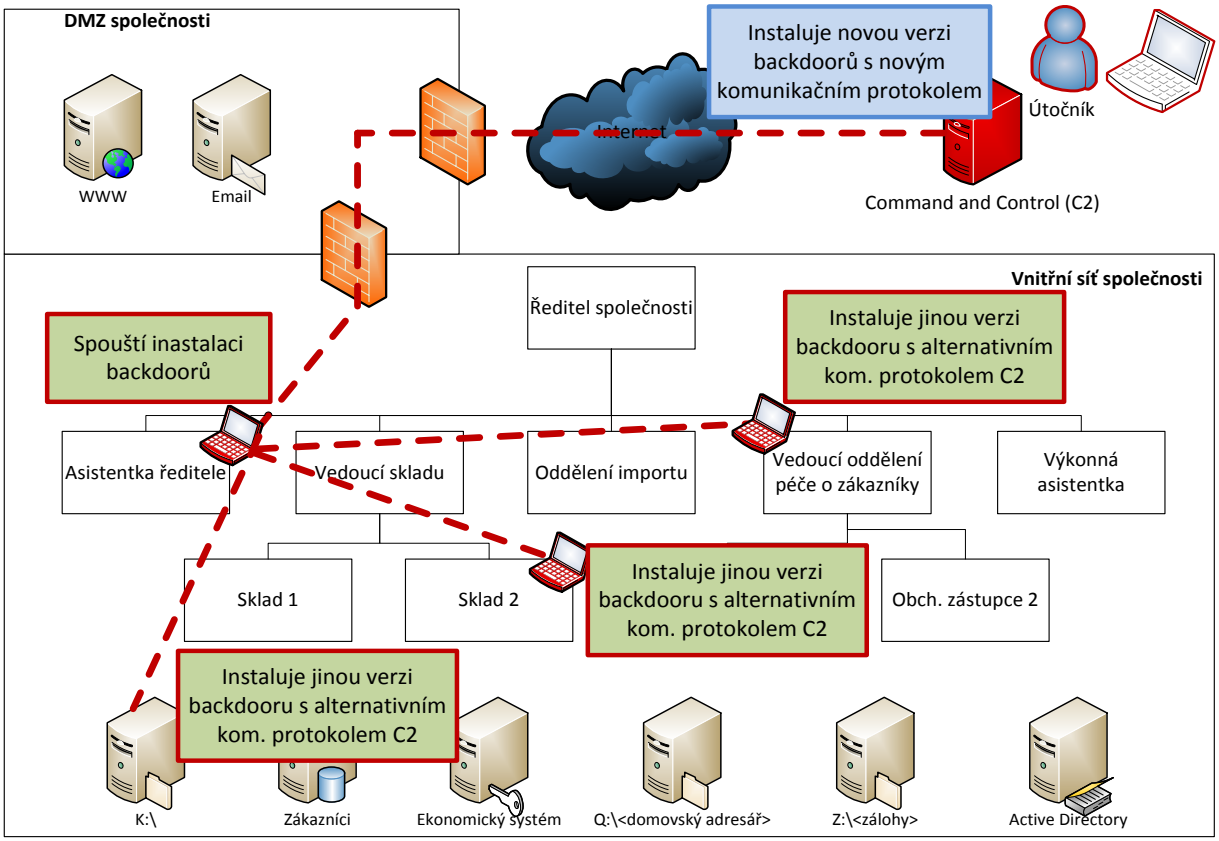
  Útočníci obecně hledají legitimní přístup do napadené sítě. Pomocí jména a hesla do VPN se můžou legitimně propojit do sítě bez podezření bezpečnostních mechanismů. Pokud získají účet s vysokým oprávněním, jsou schopni se pohybovat po celé síti.

- Instalace nových backdoorů na okolní systémy v síti

  Během svého pobytu v síti, útočníci instalují nové backdoory na okolní systémy. Pokud je backdoor objeven a odstraněn mají další možnost se do systému opět dostat. Obvykle je nasazeno a různě roztroušeno více typů a verzí backdoorů.

- Přihlašovaní na webové portály

  Pomocí ukradených identit se útočníci mohou hlásit do webových služeb a portálů ze uvnitř sítě i na systémy vně napadené sítě. Například přístup na webmail. [13]



Obr. 7.7: Útočník instaluje nové verze backdorů na okolní systémy

Útočník je obeznámen s bezpečnostním řešením v cílové síti. Upravuje verze backdoorů a ostatních nástrojů, aby nebyli detekovatelné používaným antivirovým řešením. Nejprve si toto řešení otestuje a posléze nasadí do infiltrované sítě. Pak musí své programy neustále testovat na nové aktualizace antivirů.

Zcizení dat

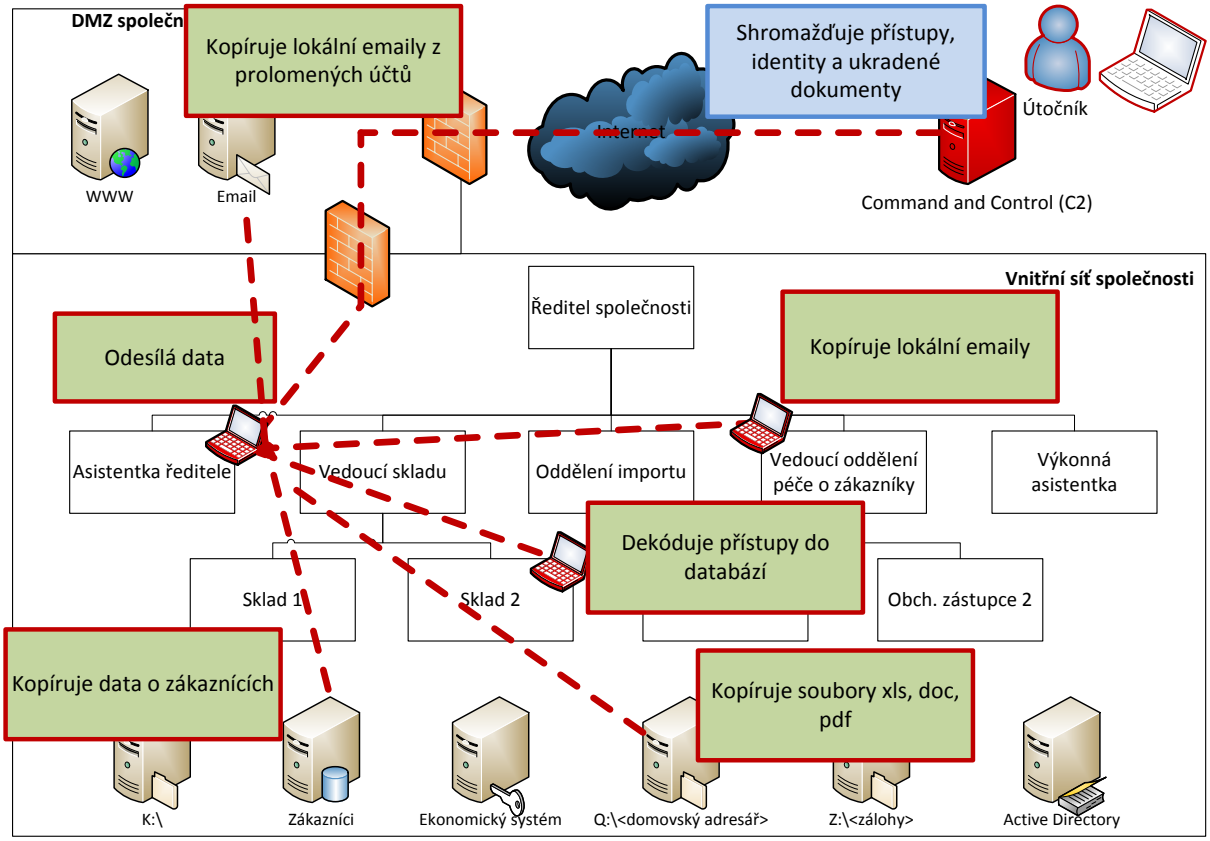
Konečným cílem útoku je zpravidla dat nebo dokumenty s údaji, které mají pro vetřelce hodnotu. Jakmile útočníci najdou zajímavé soubory dat, zabalí je do archivních souborů. K tomuto používají nejčastěji archivační nástroje ZIP a RAR. Tyto soubory si pro jistotu chrání hesly. A následné pomocí dávkového souboru legitimní cestou odešlou na svůj server. [34]

```
@echo off
cd /d c:\windows\tasks
rar.exe a archiv.rar –v50m “C:\Documents and Settings\User\Dokumenty\Slozka” –heslo123
ftp -s:upload_files.txt
del %0
```

Obr. 7.8: Ukázka cmd skriptu uploadu dat na C2 server pomocí příkazů systému

Po vytvoření komprimovaného souboru útočníci zahájí přenos nejčastěji pomocí FTP, který je v systému nebo použijí některý ze svých backdoorů. Ukradená data rozdělí na menší soubory, aby nevzbudili pozornost při zatížení linky.

Dalším cílem je monitoring komunikace uvnitř organizace. Útočníky zajímají uložené emaily, jako jsou například soubory PST (osobní složky) určené pro Microsoft Outlook. Pokud útočník získá přístup k administrativnímu účtu centrálního poštovního serveru, může sledovat všechny emaily v rámci organizace.



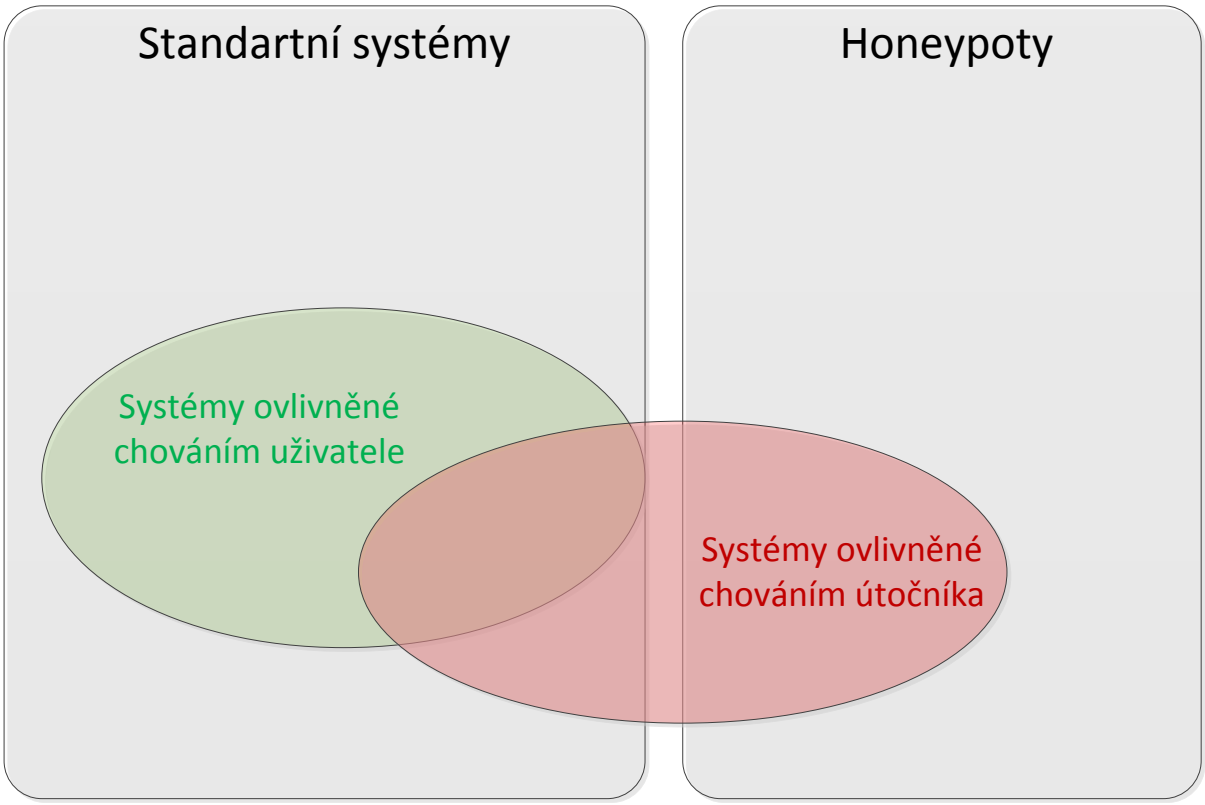
Obr. 7.9: Útočník shromažďuje odcizené informace na centrální počítač

Dále se v disertační práci podrobně zaměříme na fázi Rozšíření vlivu. Předchozí fáze je možné detekovat kvalitními standartními nástroji. Ale pokud se útočník dostane až do fáze Rozšíření vlivu, znamená to, že standartní bezpečnostní techniky selhaly. Tato fáze je standartními technikami zabezpečení skoro neodhalitelná. Útočník se chová jako běžný uživatel a využívá běžné nástroje. Jedna z metod, jak detekovat útočníka, je pomocí systému honeypotů.

Tento systém si můžeme představit následovně:

Definujeme dvě množiny: Množinu standartních systémů a množinu honeypotů. Tyto dvě množiny jsou disjunktní. Dále existují další dvě množiny dle ovlivněných systémů: systémy ovlivněné běžným chováním uživatele a systémy ovlivněné chováním útočníka. Tyto dvě množiny budou mít průnik. Čím bude útok

přesnější, tím více se budou překrývat. Množina uživatele, by neměla mít při správném nastavení systémů, průnik s množinou honeypotů. Pokud to nastane, je vyvolán falešný poplach a rozsah množin se musí upravit. Na následujícím grafu je tento systém znázorněn graficky.



Obr. 7.10: Chování uživatelů v rámci systémů

8 EXPERIMENTÁLNÍ ČÁST

V rámci experimentální části je vytvořen systém na detekci on-line hrozeb. Tento systém je vytvořen dle informací z praxe a rozborem aktuálních rizik. Hlavním cílem tohoto systému je detekovat incidenty, které se nepodařilo zachytit klasickými bezpečnostními mechanismy.

Pro tento typ systému jsem zvolil řešení na principu honeypotů. Základní část tvoří systém senzorů - honeypotů, v různých modifikacích a rozšíření o různé funkce. Tyto senzory předávají informace o incidentech centru administrace, kde jsou vyhodnoceny a dle závažnosti se vykonají bezpečnostní opatření.

8.1 Slovník základních pojmů

Zde jsou uvedeny základní pojmy související z následujícím řešení.

8.1.1 Bezpečnostní incident

Událost, která je zaznamenána na senzorech systému. Většinou bez významných následků, ale může ovlivnit bezpečnost. Tato událost by mohla být závažná a je nutné ji brát na vědomí. Je to možná bezpečnostní hrozba. Incident se může skládat v určitém časovém intervalu z více útoků.

Incident je popsán následujícími údaji:

SRC	zdroj incidentu, nejčastěji IP adresa
CAS	čas incidentu, začátek útoku
PROTOKOL	služba nebo protokol, na který byl incident cílen. Např. TCP, HTTP, ICMP
ZAVAZNOST	Ohodnocení incidentu 1-3

8.1.2 Senzor

Zdroj informací pro řídicí systém, který umí přenášet informace z určité části sítě na honeypot.

8.1.3 Centrum administrace

Centrum, kde se setkávají informace z honeypotů. Tyto informace dále vyhodnocuje a zpracovává. Při zadaném pravidle provede adekvátní činnost. Spravuje a řídí systémy senzorů. Zpřístupňuje data administrátorovi pomocí webového rozhraní.

8.2 Popis řešení

V počítačové praxi se setkáváme s různými bezpečnostními jevy. Standartní bezpečnostní mechanismy odhalí velké množství průniků, ale ne všechny. Stává se že, některý systém má zvláštní chování a po důkladném rozboru nalezneme

bezpečnostní incident. Většinou ale nenalezneme zdroj původu. Pomocí detekcí různých hodnot na systému honeypotů můžeme vysledovat dle chování jednotlivých systémů zdroj nákazy, a následně tento zdroj můžeme eliminovat.

Navrhovaným systémem nelze nahradit všechny tradiční formy zabezpečení a detekce, ale je to jejich vhodný doplněk. Je to také silný nástroj na bezpečnost ve virtuálním prostředí a vynikající pomůcka k podrobnějšímu studiu bezpečnostních incidentů

Toto řešení můžeme rozdělit do tří základních bloků:

Blok Honeypotů - Systém senzorů

- Detekují bezpečnostní incidenty v sítích na senzorech a informace odesílá do Centra administrace

Blok Agend

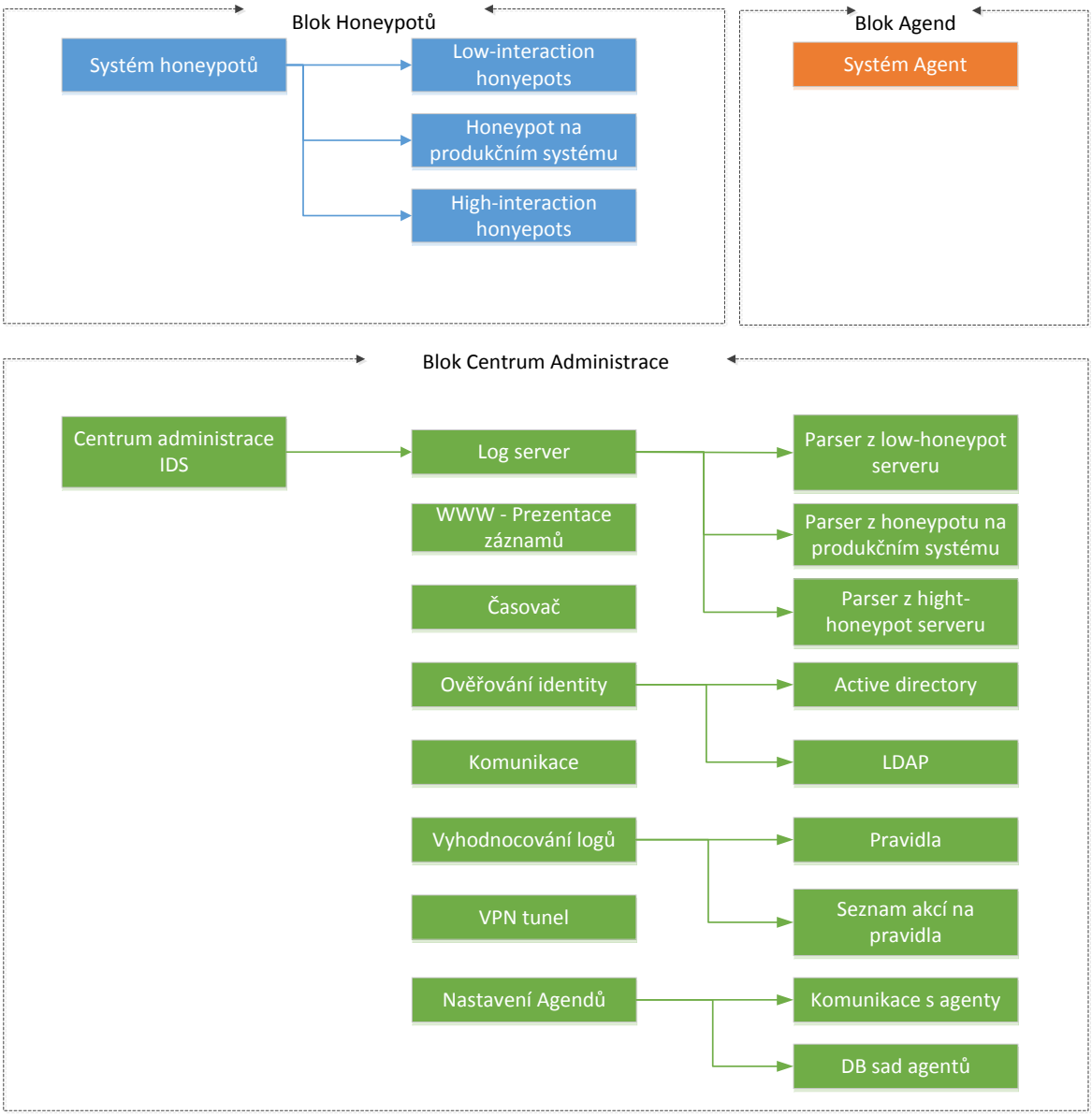
- Nasměřuje útočníka na systém honeypotů

Blok Centrum Administrace

- Sbírá informace ze senzorů
- Ukládá informace pro pozdější použití
- Vyhodnocuje informace
- Prezentuje výsledky pro administrátory
- Spouští na určitý typ incidentu upozornění pro administrátory
- Komunikuje s jinými bezpečnostními prvky
- Zabezpečuje komunikaci se senzory
- Vytváří a zabezpečuje komunikaci s agenty

Systém honeypotů zachytí bezpečnostní incident. Tuto informaci neprodleně předá Centru administrace. Informace se vyhodnotí, podle pravidel vytvoří akci a prezentuje výsledek administrátorům.

Využitím tohoto systému oprávněnými pracovníky povede především je zvýšen bezpečnosti počítačových systémů. Nasazením například ve firmách můžeme minimalizovat kompromitace jejich obchodních informací a předcházet špionáži. Další možnost je nasazení ve společnostech, které mají striktní bezpečnostní standarty, a potřebuje identifikovat zdroj incidentu.



Obr. 8.1: Blokový diagram komponent systému detekce

8.3 Seznam a činnosti hlavních aktérů systému

Administrátor

Správce systému – spravuje celkový chod systému, zodpovídá za bezpečnost a provádí akce proti činnosti útočníků.

Hlavní funkce administrátora jsou:

- Instaluje honeypoty
- Nastavuje systém Agend
- Řeší incidenty
- Řeší falešné incidenty

Uživatel

Osoba, která používá systém k běžným činnostem a nenarušuje bezpečnost systému. Pokud se mu ale podaří vyvolat incident, tento je po ověření v centru Administrace administrátor označen jako falešný.

Útočník

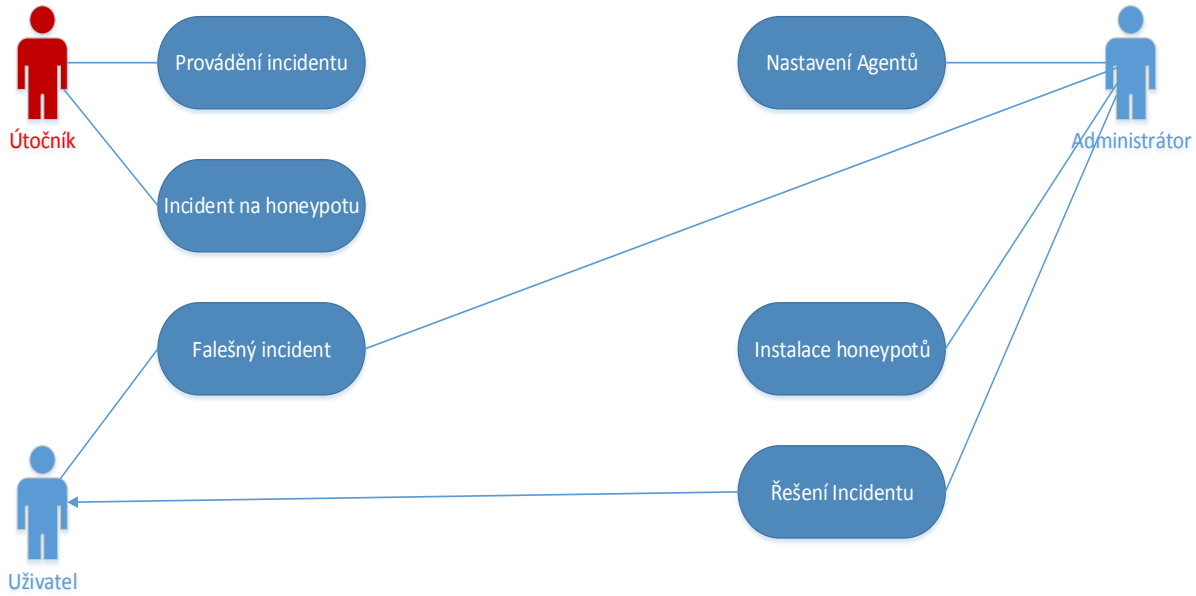
Objekt, osoba, software anebo systém, snažící se kompromitovat náš systém. Provádí incidenty a může být zachycen systémem honeypotů

Adresářová služba

Objekt, který ověří pravost a identitu uživatele v systému pomocí jména a hesla.

8.4 Činnosti hlavních aktérů systému

Na následujícím digramu jsou uvedeny činnosti hlavních aktérů systému a vazbami mezi nimi.



Obr. 8.2: Činnosti hlavních aktérů systému

Dále budeme činnosti jednotlivých aktérů probírat podrobněji v návaznosti na základní komponenty systému.

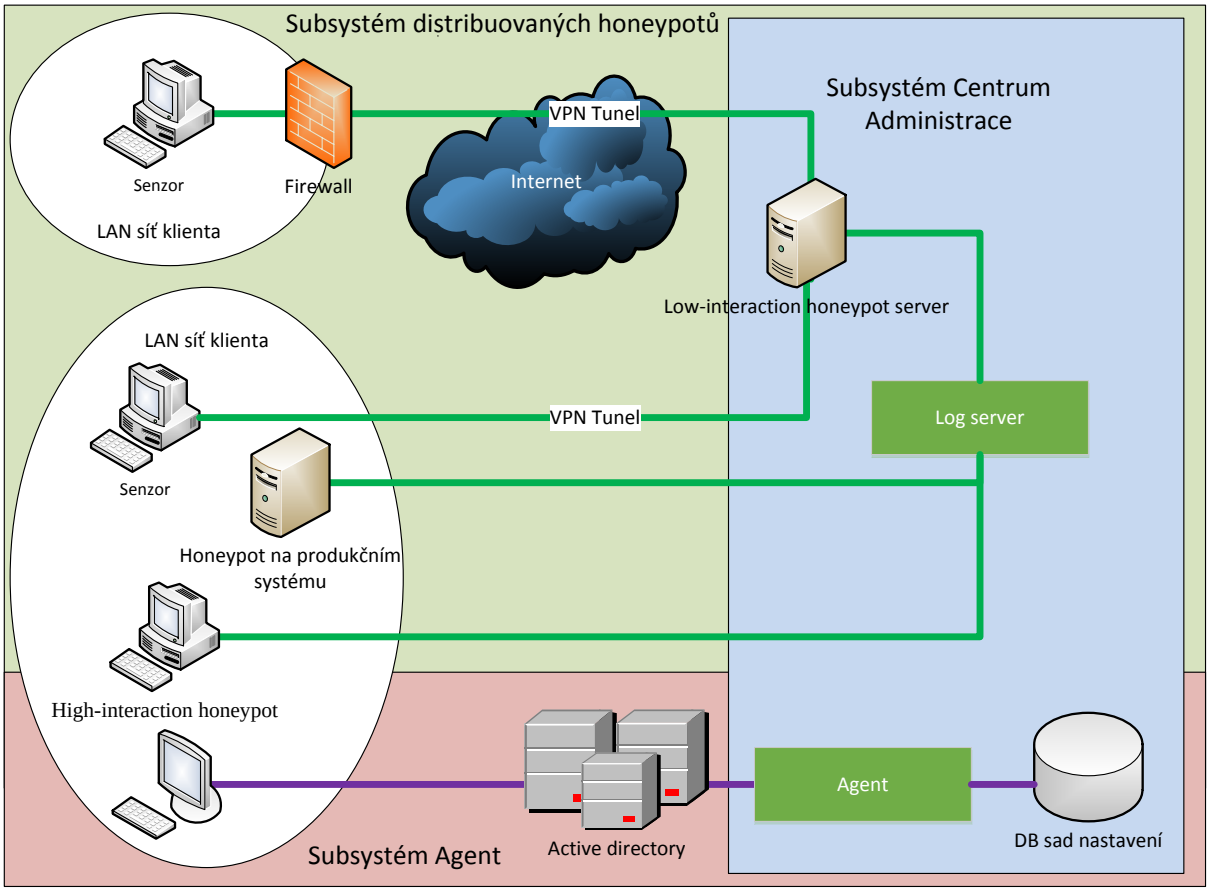
9 NÁVRH ŘEŠENÍ

Tento systém se skládá z mnoha částí, které po určitých úpravách do sebe zapadají. Ještě před pár lety nebylo možno tento systém v tomto rozsahu postavit, nebyly k dispozici spolehlivé a potřebné technologie a rozsahy výpočetních kapacit.

9.1 Architektura systému

Navržený systém vychází z teoretických poznatků popsaných v úvodních kapitolách. Celkový systém navrhovaného IDS lze rozdělit do několika základních subsystémů:

- Systém distribuovaných honeypotů
- Systém Agent
- Subsystém Centrum Administrace



Obr. 9.1: Logické schéma základních subsystémů

Následně bude o jednotlivých součástech psáno podrobněji a bude prezentována funkcionalita každé z nich.

9.1.1 Subsystém distribuovaných honeypotů

Původní základ systémů mojí disertační práce tvoří systém D-IDS SURFcert IDS (*SURFcert,* 2012). Tento systém jsem zvolil po letité zkušenosti s různými druhy D-IDS systémů. Projekt SURFcert IDS je distribuován pod GPL licencí. Využil jsem jádro tohoto systému a následně rozšířil o další funkce.

9.1.2 Subsystém low-interaction honeypotů

Low-interaction poskytují pouze přihlašovací prompt, který se jen tváří jako nějaká služba a neumožňují sledovat chování útočníka po proniknutí do systému.

Výhody tohoto systému jsou:

- Jednoduchá instalace.
- Jednoduchá konfigurace.
- Jednoduché zpracování zachycených údajů.
- Možnost nasadit jako outsourcing do spravované společnosti.
- Možnost použít dynamicky velké množství senzorů.

Nevýhody systému jsou:

- Máme méně informací o útoku, než na ostatních typech honeypotů.
- Je vhodné znát cílovou síť, pro efektivní nasazení.

Požadavky na ideální systém D-IDS k implementaci low-interaction honeypotů

V současné době je většina D-IDS založena nejčastěji na systémech typu Snort [47] nebo jiných komerčních řešení. Tradiční koncepty jsou popsány v úvodu disertační práce.

Současné D-IDS více méně trpí některou z následujících nevýhod:

- Sensory nejsou rozšiřitelné pro rozšíření o nové typy honeypotů a nebo popisy signatur.
- Sensory využívané jako honeypoty nebo k analýze incidentů mohou být ohroženy.
- D-IDS generuje falešné poplachy.
- Instalace senzorů není uživatelsky přívětivá.

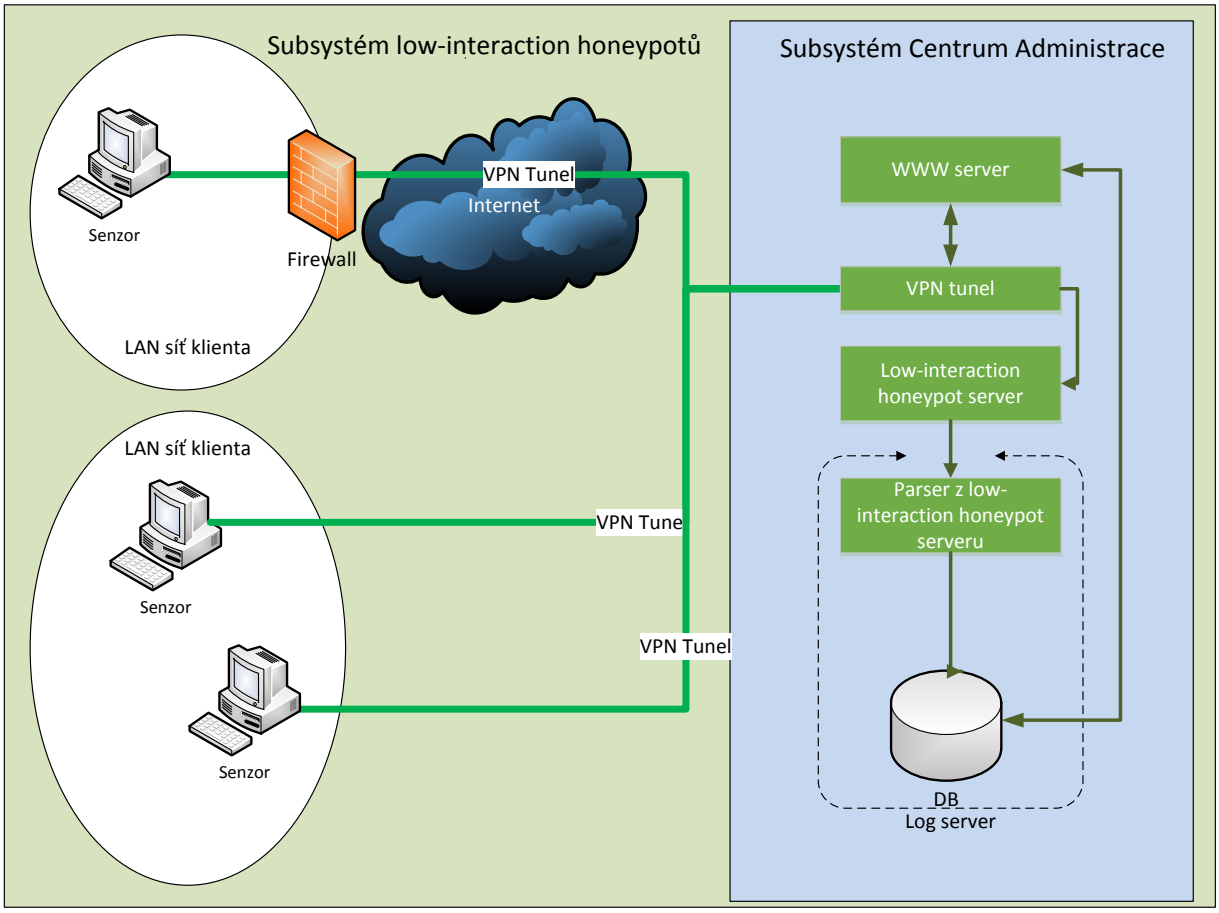
Základní požadavky pro D-IDS systém jsou:

- Senzor by měl běžet fyzicky mimo centrálních serverů, které tvoří jádro D-IDS.

- Senzor by měl být zcela pasivní.
- Senzor by měl být bezúdržbový.
- D-IDS by neměl způsobovat falešné pozitivní výstrahy.
- Sensor by měl být schopen běžet na standartní síti LAN.
- Senzor by měl být připojitelný z celé sítě internet.
- Senzor by měl bezpečně komunikovat s centrálními servery.

Původní základ systémů tohoto subsystému tvoří systém D-IDS SURFcert IDS. Tento systém jsem zvolil po zkušenosti s různými druhy D-IDS systémů a splnění výše uvedených požadavků. Projekt SURFcert IDS je distribuován pod GPL licencí. Využil jsem jádro tohoto systému a následně rozšířil o další funkce.

Primární využití systému je zachycení aktivit na vybraných portech, dle aktuálních hrozeb. Sekundární využití je možnost sběru vzorků malware a tím zjistit, kde mají naše bezpečnostní systémy slabiny.



Obr. 9.2: Grafické schéma subsystému low-interaction honeypotů

V předcházejícím schématu lze vidět, že senzory nejsou implementovány na centrálních serverech. Senzory jsou umístěny mimo toto centrum a jsou připojeny pomocí sítě. Použití distribuované řešení není omezeno jen jednou sítí, ale

senzory můžou být umístěny ve více sledovaných sítí po celém internetu. Tento předpoklad je řešen pomocí VPN tunelů. Senzor je fyzicky přítomen ve sledované síti, ale pomocí virtuálního rozhraní je propojen s centrálním serverem. Centrální server zajišťuje sběr informací z honeypotů, zpracovává tyto výsledky a následně zobrazuje přes webové rozhraní.

Tento subsystém se dělí na části:

- VPN Tunel
- Low-interaction honeypot server
- Senzor
- Log server
- Webový server

VPN Tunel

Senzory požádá o propojení tunelem centrální server. Na centrálním serveru je spuštěn xinetd, který po detekci spojení pro každé připojení vytvoří OpenVpn tunel [40]. Na centrálním serveru vytvoří TAP rozhraní. Je to virtuální rozhraní, které přenáší provoz z tunelu na server. TAP obdrží také klientovu IP adresu. To umožní, aby byl server prakticky přítomen v klientské síti, kde je umístěn senzor. Tento proces se dá shrnout do následujících kroků:

- Senzor se spustí.
- Senzor zkontroluje, zda má certifikát.
- Pokud senzor nemá certifikát, požádá o jeden ze serveru.
- Senzor spustí připojení k serveru.
- Xinetd na serveru detekuje příchozí připojen.
- Server vytvoří virtuální TAP rozhraní.
- TAP rozhraní dostane IP adresu ze sítě klienta.
- Tunel je aktivní, honeypot může detekovat všechna příchozí spojení a analyzovat je.

Použitý software:

- OS Debian
- OpenVPN 2.2
- Xinetd

Low-interaction honeypot server

Aby bylo možné analyzovat provoz, který přichází skrz tunel, používáme honeypot Dionaea s kombinací s honeypotem Amun. Informace z honeypotu jsou ukládány v databázi PostgreSQL, která je spuštěna na logovacím serveru. Výhodou použití honeypotu pro tuto analýzu je fakt, že můžeme garantovat 0 falešných poplachů. Informace lze považovat na 100% spolehlivé. To poskytuje výhodu nad technikami, jako je síťová analýza a nebo logování toků na firewallu.

Použitý software:

Dionaea

Pro tento typ honeypotu jsem zvolil systém Dionaea(http://dionaea.carnivore.it/). Jedná se o honeypot který primárně slouží ke sběru malware. Emuluje, známe zranitelnosti služeb. Zachycený škodlivý kód je primárně uložen disku, ale není nikde spuštěn. Následně jsou vzorky útoků odeslány k analýze. Tento software je nástupce dřívějšího systému Nepenthes. Tento systém byl vytvořen v PERLu, ale jeho největší nevýhoda je nemožnost podpory IPv6 a TLS. [15]

Dionaea používá základní skriptovací jazyk Python. Podporuje modulární řešení senzorů, IPv6 a TLS (self-signed certicate). Základní protokoly implementované Dionaeou jsou:

- SMB

  Hlavní protokol o řešení Dionaea je SMB (port 445). SMB má slušnou historii vzdálených využitelných chyb a je velmi populární cíl pro červy. Podporuje nahrávání souborů.

- HTTP

  Podporuje http na portu 80 ale i HTTPS na portu 443. Pro protokol HTTPS je po spuštění vytvořen self-signed SSL certifikát.

- FTP

  Povoluje základní FTP server na portu 21, kde se můžou vytvářet adresáře, nahrávat a stahovat soubory.

- TFTP

  Povoluje připojení na protokolu UDP portu 64, kde se můžou vytvářet adresáře, nahrávat a stahovat soubory. Na tuto službu jsem prozatím nezaznamenal žádný útok.

- MSSQL

  Tento modul implementuje Rabular Data Stream protocol, který se používá pro Microsoft SQL Server. Ten naslouchá na portu TCP/1433 a umožňuje

klientům se přihlásit. Je možné dekódovat spuštění dotazů na databázi, ale Dionaea nemůže odpovědět, nejsou zde žádné databáze.

- MySQL

  Tento modul implementuje MySQL Wire Stream protocol.

- SIP (VoIP)

  Jedná se o modul VoIP pro honeypot Dionaea.VoIP používá protokol SIP, protože to je de facto dnešní standardem pro VoIP. Na rozdíl od některých jiných VoIP lákadel, tento modul není připojení k externímu VoIP registračnímu serveru. Jen prostě čeká na příchozí zprávy SIP (např. OPTIONS nebo INVITE).

Amun

Je honeypot, který může být použit jako další v systému SURFcert IDS. Pomocí AMUNu jsem nastavil protokoly, které nejsou obsaženy v Dionaele. [4]Jedná se o služby POP3 (port 110) a IMAP (port 143).

Další moduly použité na honeypot serveru:

P0f

Pasivní fingerprint. Program P0f sleduje komunikaci mezi honeypotem a útočníkem. Dle této komunikace dokáže určit, o jaký operační systém na straně útočníka se jedná. Je naprosto nezachytitelný a komunikaci nijak neomezuje. [62] Tyto informace se ukládají na logovací server.

Senzor

Jediným účelem senzoru je vytvoření mostu mezi klientskou sítí a centrálním serverem. Senzor řídí vytvoření a zánik tunelu, který se používá k připojení centrálnímu serveru. Hlavní funkce senzoru jsou čtyři:

- Tvorba a zánik tunelu mezi senzorem a centrálním serverem.
- Správa senzorem používaných OpenVPN certifikátů.
- Vzdálená aktualizace senzoru.
- Aktualizace informací o stavu serveru.

Certifikáty na snímači se používají k tvorbě a zajištění tunelu a identifikaci snímače na centrálním serveru. Při prvním spuštění senzoru bude senzor požadovat nastavení certifikátu a jména senzoru. Od této doby se pak bude identifikovat na základě těchto parametrů. Senzor také obsahuje několik skriptů pro aktualizaci na novou verzi. Tyto skripty senzor aktualizují, pokud jsou k dispozici nové verze. Tento způsob aktualizace zajišťuje, že není potřeba ručně aktualizovat nasazené senzory. Vzdáleně můžeme sledovat stav senzoru a provádět určité akce, např. restart snímače, vypnutí snímače atd.

Základní systém senzoru: Debian-Live OS

Minimální požadavky na senzor jsou:

- 1GB místa na disku.
- Minimálně jedna síťová karta.
- Firewall s povolenými odchozenými spojeními z portu 1194 a 4443 (nebo 443).

Port 1194 se používá pro nastavení OpenVPN, port 4443 se používá pro vzdálené aktualizace a výměnu informací mezi snímačem a serverem. Připojení vždy zahajuje símač, proto je povoleno pouze spojení směrem k serveru na zvolených portech.

Tento senzor se dá samostatně spustit z USB disku anebo virtuálně pomocí VmWare ESX serveru.

Log server

Na tomto serveru běží databáze, kam se ukládají k analýze informace z honeypot serveru.

Použitý software: PostgreSQL.

Doporučení pro nasazení

- Vhodné pro všechny velikosti sítí.
- Vyšší efektivita s kombinací rozšíření Agent.
- Hlavní cíl je detekce zdroje incidentu.

9.1.3 Subsystém honeypotů na produkčních systémech

Speciální verze honeypotu, implementována v produkčním systému. Povolíme útočníkovi se přihlásit na produkční systém ke služby nespojenou s produkčním systémem. Např. databázový server MySQL, který bude mít povolenou službu SSH na portu 22. Na ní bude zavěšen systém Kippo, na detekci přihlášení ke službě SSH. Reálná služba na správu serveru SSH bude přesměrována na port 2222 a bude omezen jen na konkrétní IP adresy. Útočník bude mystifikován a pokoušet se přihlásit na standartní port 22, který bude logován systémem Kippo a informace odesílány do Centra Administrace. Na tento typ subsystému je vhodné použít implementaci medium-honeypotů.

Výhody:

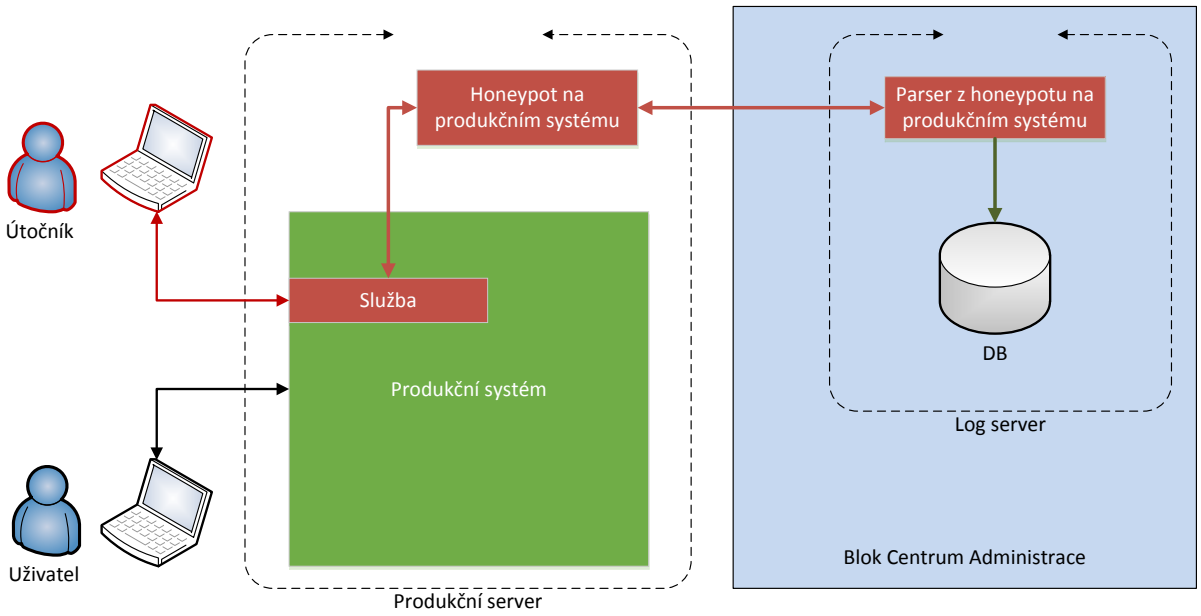
- Zvyšuje efektivitu detekce APT útoků

Nevýhody:

- Musíme mít přístup na produkční systém

- Složité nastavení a ovládání
- Potřebujeme velmi dobré znalosti o honeypotech a produkčním systému

Pokud máme přístup na produkční server, můžeme zajistit přenos neúspěšných přihlašovacích údajů do centra administrace k analýze. Při zpětné analýze, můžeme zjistit, o které účty byl zájem.



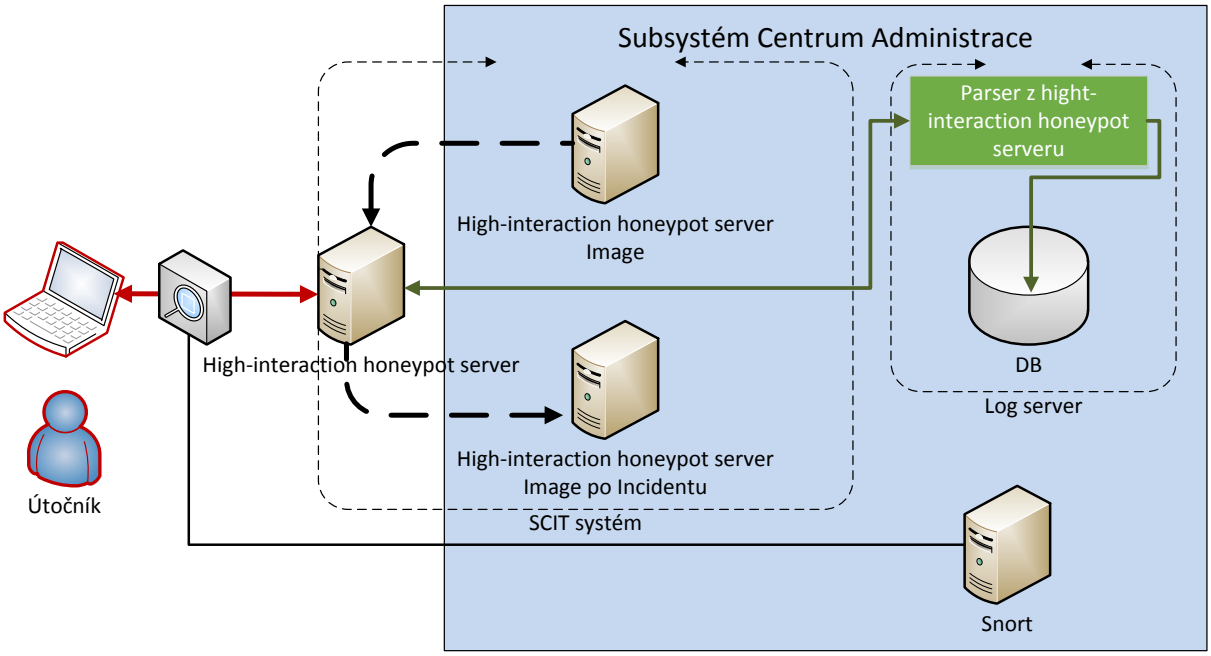
Obr. 9.3: Grafické schéma subsystému honeypotů na produkčních systémech

Doporučení pro nasazení

- Střední a velké organizace
- Vyšší efektivita s kombinací rozšíření Agent
- Kde máme pod správou produkční systémy

9.1.4 Subsystém high-interaction honeypotů

Tento systém honeypotů v konceptu této disertační práce se nesnaží zkoumat např. účinek exploidů na systém a hledat nové softwarové zranitelnosti. Hlavním cílem je vytvořit honeypot, který se bude podobat již používaným systémům v síti. Jeho hlavní úkolem není výzkum, jakým způsobem útočník provede útok, ale zjistit jaké informace má a získal o našem systému. Pak můžeme účinně eliminovat útok. Dnešní době si nemůžeme dovolit vyřadit z provozu celé systémy, musíme jen přesně identifikovat napadené místo a to opravit. Proto tento typ honeypotu je zabezpečen standartním logováním nainstalovaných služeb, nastavených na vhodnou úroveň citlivosti.



Obr. 9.4: Grafické schéma subsystému high-interaction honeypotů

Výhody:

- Můžeme zjistit, které účty útočník kompromitoval.
- Můžeme zjistit, kam se ztrácejí naše data.

Nevýhody:

- Náročná implementace nutnost výborná znalost implementované služby.
- Může být ovládnut útočníkem.

Zabezpečení high-interaction honeypotů

- SNORT – monitorujeme datové toky z/do honeypotu.
- SCIT obnovení – Po napadení systému provedeme rotaci serverů na původní stav. Ze zálohy vezmeme nekomprimovaný server a nahradíme napadený. Napadený server přesuneme na bezpečné místo mimo síť a ponecháme určitý časový okamžik, pro případ forenzní analýzy útoku.

Použité systémy

- Modifikovaný webmail

  Zaznamenává všechny operace provedené před a po přihlášení. Odeslané emaily jdou přes modifikovaný SMTP server. Odesílá ověřovací údaje do Centra Administrace k dalšímu ověření.

- Modifikované FTP

  Zaznamenává všechny operace provedené před a po přihlášení. Uložené soubory jsou odeslány do Centra Administrace do archívu incidentu. Odesílá ověřovací údaje do Centra Administrace k dalšímu ověření.

- SSH server

  Je použito systému Kippo (http://code.google.com/p/kippo/). Loguje všechnu činnost na SSH serveru. Odesílá ověřovací údaje do Centra Administrace k dalšímu ověření.

- Modifikovaný SMTP server

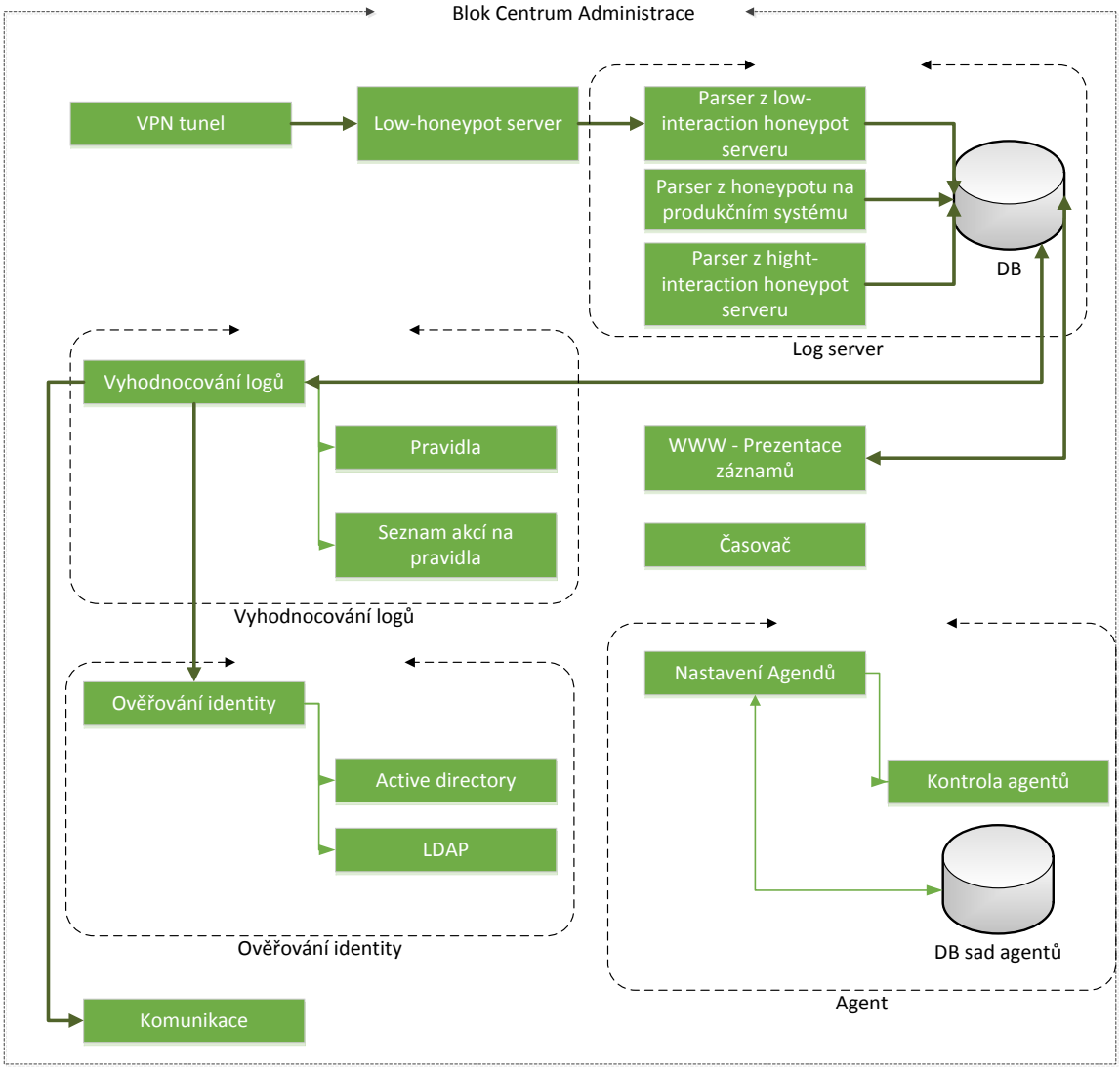
  Zachytává poštu skrz něj poslanou, ale neodesílá ji. Pouze ji zaznamenává do souborů a zasílá informace na centrální log server.

Doporučení pro nasazení

- Střední a velké organizace
- Vyšší efektivita s kombinací rozšíření Agent
- Kde máme pod správou produkční systémy
- Vhodná kooperace se správci sítě
- Administrátor musí znát dobře nasazené systémy
- Potřebujeme vědět komplexní informace o útoku
- Nutnost krizových postupů

9.1.5 Centrum Administrace IDS

Je základní částí systému honeypotů. Následuje grafické schéma s jednotlivými bloky Centra Administrace a vyznačenými vazbami.



Obr. 9.5: Grafické schéma Centra Administrace

Hlavní část systému IDS je Centrum administrace, které má základní funkce:

- Shromažďuje informace ze senzorů
- Parsuje data ze honeypotů
- Ukládá informace pro pozdější použití
- Vyhodnocuje informace
- Prezentuje výsledky pro administrátory
- Spouští na určitý typ incidentu upozornění pro administrátory
- Komunikuje s jinými bezpečnostními prvky
- Zabezpečuje komunikaci se senzory
- Vytváří a zabezpečuje komunikaci s agenty

Jednotlivé základní bloky jsou:

VPN tunel

Obstarává komunikaci mezi senzory a honeypoty pomocí open source software OpenVPN.

Log Server

Shromažďuje informace z honeypotů, které přijímá přes VPN Tunel a ukládá je do databáze. Dělí se na části dle použité technologie. První část shromažďuje všechny události ze low-interaction honeypotů. Základ je tvořena systémem SURFcert IDS. Druhá část sbírá události z produkčních honeypotů a high-interaction honeypot systémů. Tato část je tvořena převážně PERL skripty. Parsuje logy z honeypotů a ukládá je do databáze.

Časovač

Pomocí linuxového démona Cron spouští v určitých časových intervalech automatické PERL skripty a zálohování.

Centrum komunikace

Obsahuje skripty pro komunikaci s administrátory. Umožnuje upozornění na incident pomocí emailu a sms.

Ověřován identity

Kontroluje z databáze uživatelské data sesbíraná na honeypotech: přihlašovací jméno a heslo. Tyto informace ověřuje vůči LDAP nebo AD. Realizováno pomocí PHP. Výsledky předává do bloku Vyhodnocování logů

Vyhodnocení logů

Základní část Centra Administrace, vyhodnocuje data z honeypotů. Dle zadaných pravidel kontroluje databázi, a pokud nalezne shodu, spustí adekvátní akci - poplach. Realizováno pomocí SQL triggerů.

WWW server

Tento server slouží k prezentaci dat z databáze pro administrátory. Webové rozhraní slouží jako přehled o stavu, ale také o stavu senzorů. Je dostupné pomocí protokolu http na portu 8080. Postaveno na systému SURFcert IDS. Seznam některých funkcí webového rozhraní:

- Informace o útocích
- Reporty
- Dálkové ovládání pro senzory a jejich stav

- Rozšíření vyhledávání
- Ověření uživatele
- Nastavení systému
- Editace a vytvořen pravidel a upozornění
- Zobrazení statistik

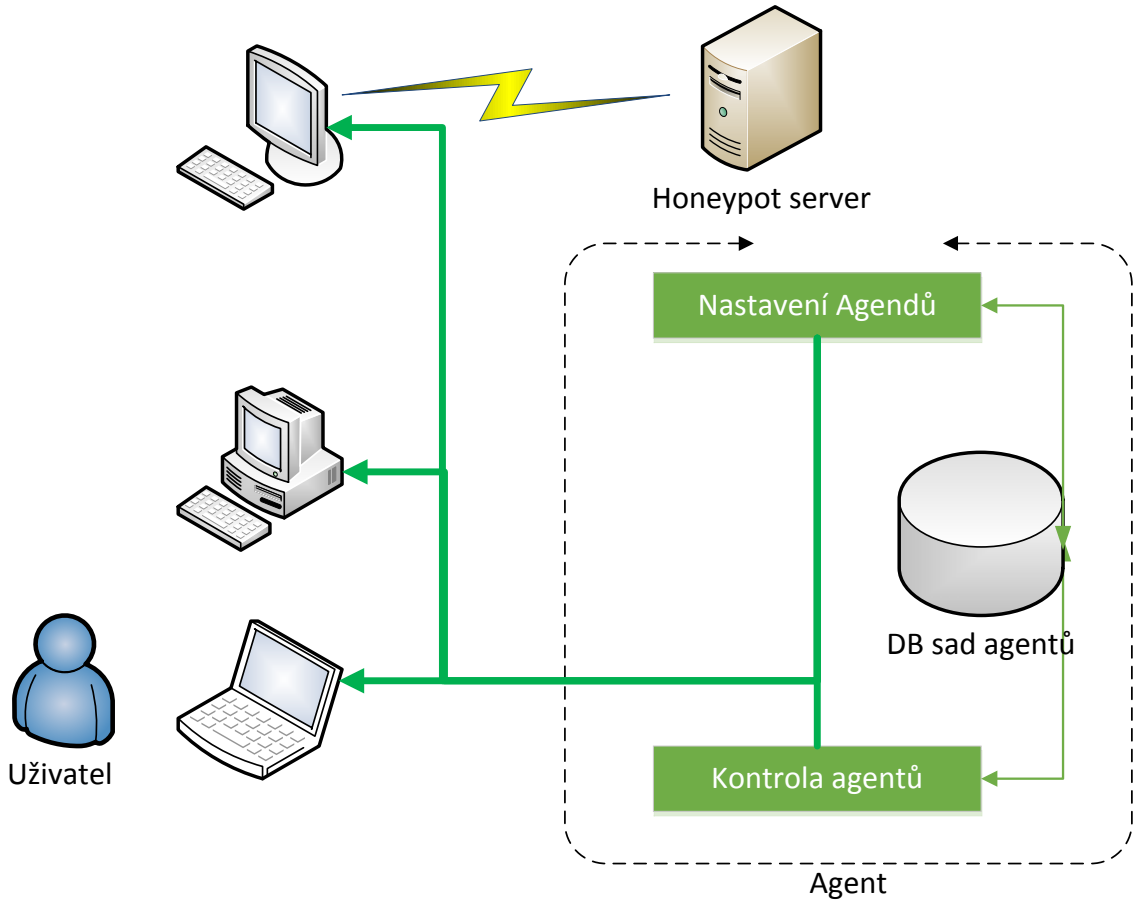
Použitý software:

Perl, PHP, Apache, RRDTool.

9.1.6 Subsystém AGENT

Tato část systému se implementuje do sledované sítě na námi vybrané hostitelské systémy. Vloží do produkčního systému nějakou nadbytečnou informaci, která není podstatná pro uživatele toho zařízení. Předpokládáme, že uživatel svým chováním nikdy na tuto podstrčenou informaci nepřijde a pokud ano, nebude jí věnovat pozornost. Ale pokud bude systém kompromitován, tak útočník nemůže tuto informaci vyhodnotit, zda je či není důležitá. Následně tuto informaci použije. Při dalším kroku incidentu s vysokou pravděpodobností kontaktuje odpovídající honeypot.

Možný způsob řešení je například pomocí pravidel Active Directory Police. Nastavíme do hostitelského systému možnost připojení na FTP server s uživatelským jménem a heslem. Běžný uživatel si tohoto nastavení nepovšimne anebo mu nebude věnovat pozornost. Útočníkovo chování je ale odlišné. Útočník shromažďuje informace o napadeném systému, a tyto informace použije pro své další kroky. V tomto případě se bude snažit přihlásit na FTP server – honeypot se zadaným uživatelským jménem a heslem.



Obr. 9.6: Grafické schéma subsystému AGENT

Pro implementaci Agenda do uživatelského systému musíme mít k tomu systému adekvátní přístup a oprávnění.

Možnosti nasazení Agenta do uživatelského systému:

- Manuálně

  Nastavíme vybrané parametry manuálně.

- Dávkovým souborem

  Pomocí skriptu v dávkovém souboru nastavíme falešné informace.

- Active Directory

  V rámci domény můžeme implementovat pravidla na zvolený systém pomocí doménové politiky.

Možné pluginy

- FTP

  Implementujeme do Totaclmd (http://www.ghisler.com/), nebo jiného používaného klienta, odkazy na honeypoty. Minimální úroveň přístupu: jako běžný uživatel s právy pro nastavení programu Totalcmd.

- Sdílené disky

  Implementujeme do systému odkazy na pevné disky s přihlašovacími údaji.

- POP3

  Implementujeme do systému falešné emailové účty, které odkazují na adekvátní honeypot.

- HTTP

  Nechává v systému odkazy na různé webové služby, např. na webmail, s uloženými přihlašovacími údaji.

Slabé a silné stránky

Výhody:

- Zvyšuje účinnost systému honeypotů (ověřeno v experimentu).
- Honeypot se tváří více jako reálný systém.
- Detekce APT útoků.
- Detekce kompromitovaných účtů.
- Nemusíme nasazovat tak velké množství honeypotů.

Nevýhody:

- Možnost spuštění falešného poplachu.
- Nutnost oprávnění a přístupu k systému, kde budeme Agenda implementovat.

Doporučení pro nasazení

- Vhodné pro střední a velké sítě s podporou Active Directory / LPAD.
- Nasadit v systémech a u uživatelů, o kterých máme informace o jejich návycích a chování. Nejlépe pro běžné uživatele, kteří neexperimentují se systémem.
- Vhodné pro implementace na počítače, které necestují a zůstávají větší část své doby ve firemní síti.
- Není nutné implementovat všechny možnosti. Zvolte možnosti odpovídající dle chování uživatele.
- Nenasazovat do konfigurace Agenta více možností na falešné systémy, než je reálný počet produkčních systémů v síti. Při velkém množství falešných odkazů útočník pojme podezření na honeypot.

  Počet produkčních systémů > Počet odkazů na honeypoty nasazených Agentem na jeden systém.

9.2 Vybrané případy užití

V této kapitole se zaměříme na případy užití, nejprve z pohledu útočníka, postupem detekce útoku na honeypotu a následně z pohledu administrátora a uživatele.

9.2.1 Útočník APT

Následují vybrané případy užití z pohledu útočníka. Pro správné nasazení IDS je potřeba znát tyto případy užití. Základní cyklus APT útoku se nachází na obrázku 5.1. Pro systémy honeypotů jsou důležité fáze v následujícím pořadí:

- Eskalace práv
- Vnitřní průzkum
- Rozšíření vlivu

Následují konkrétní jednotlivých fází.

Eskalace práv

Tato fáze se zabývá získáváním práv na napadeném systému. Nejčastěji se jedná o přihlašovací údaje, které posléze útočníkovi dovolí kompromitovat další systémy. Útočníci používají většinou software z veřejně dostupných zdrojů. Pokud je na systému použitý Agent, útočník získá i podstrčené údaje, a další kroky budou detekovány systémem honeypotů.

Tabulka 9-1 Incident na honeypotu - Eskalace práv

Případ užití: Incident na honeypotu - Eskalace práv
Stručný popis:
Útočník získává informace z napadeného systému pomocí odposlechu a odchytání informací z napadeného systému.
Primární aktéři:
Útočník
Vedlejší aktéři:
C2 server Uživatel
Vstupní podmínky:
Útočník má přístup k napadenému systému. Útočníku může komunikovat s řídícím serverem C2.
Hlavní scénáře:

1. Útočník stáhne potřebné nástroje, vhodné pro zvolený systém 2. Útočník aktivuje nástroj k zisku přístupových informací - získá údaje z agenta 3. Získané údaje uloží 4. Získané údaje odešle na C2
Výstupní podmínky:
Žádné.
Alternativní scénáře:
Žádné.

Vnitřní průzkum

V této fázi průzkumu sbírá útočník informace o prostředí oběti. Většinou používá primárně vestavěných příkazů, aby prozkoumal systém a sítové prostředí. Jedná se o jednoduché příkazy, které jsou dostupné v každém operačním systému. Ale pokud je útočník umí využít tak jsou mocnými nástroji. Pro zrychlení operace, používají dávkové soubory typu bat nebo cmd. Tyto skripty nejsou detekovatelné žádnými komerčními systémy. Pokud byl na systému nasazen Agent, získá útočník i informace také o okolních systémech, což budou honeypoty.

Tabulka 9-2 Incident na honeypotu - fáze Vnitřní průzkum

Případ užití: Incident na honeypotu - fáze Vnitřní průzkum
Stručný popis:
Útočník získává informace o okolních systémech z napadeného systému pomocí průzkumu systému standartními nástroji.
Primární aktéři:
Útočník
Vedlejší aktéři:
C2 server
Vstupní podmínky:
Útočník má přístup k napadenému systému Útočníku může komunikovat s řídícím C2 serverem
Hlavní scénáře:

1. Útočník stáhne potřebné skripty z C2 serveru 2. Útočník nasadí skripty pro získání informací 3. Získané údaje uloží 4. Získané údaje odešle na C2 serverem
Výstupní podmínky:
Žádné.
Alternativní scénáře:
Žádné.

Rozšíření vlivu

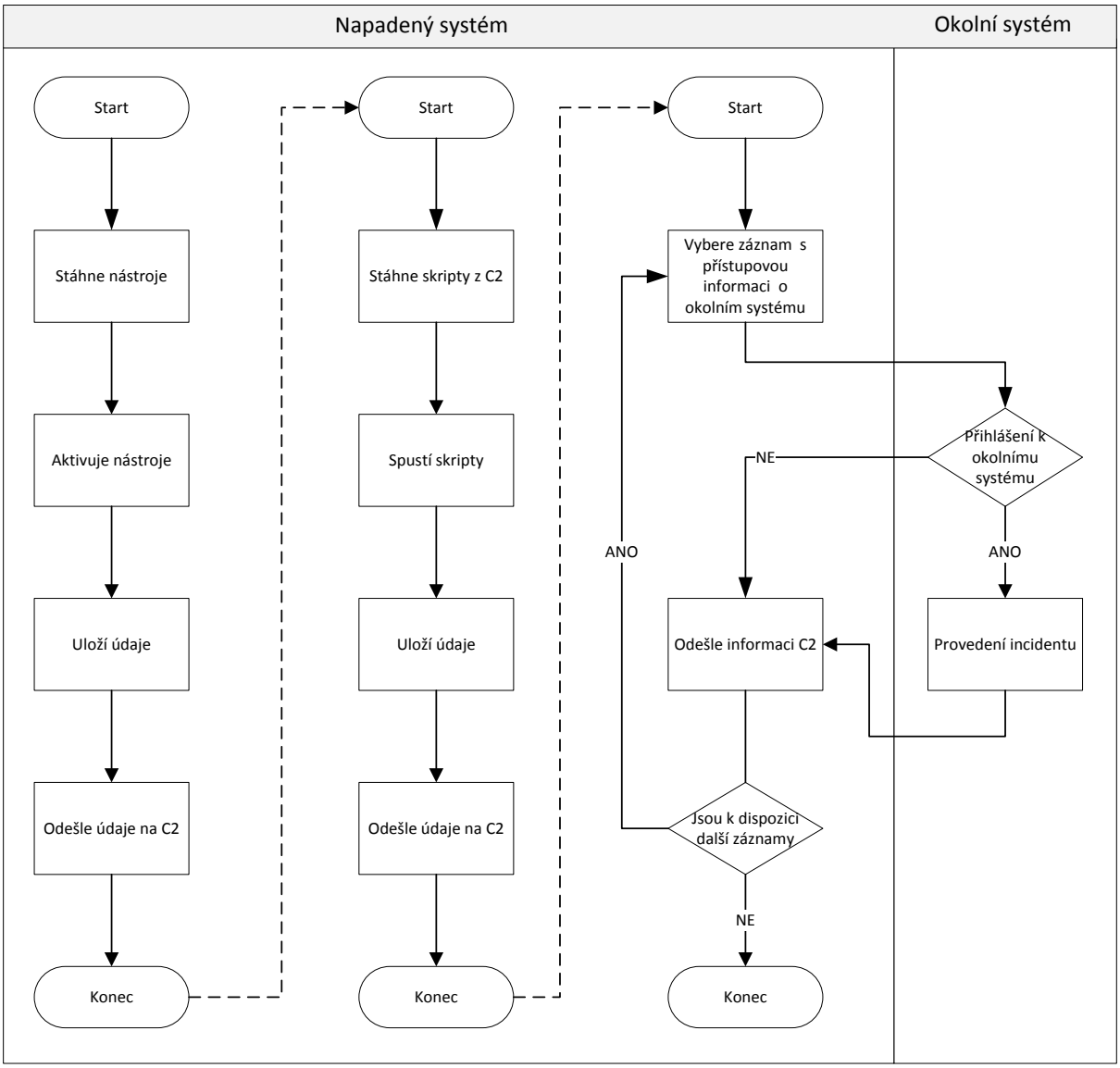
Jakmile útočník získá legitimní účty uživatelů a přehled o síti, může se v ní nepozorovaně pohybovat. V tomto kroku je vysoká pravděpodobnost, že pokud útočník použije informace z předcházejících kroků, bude detekován pomocí honeypotu.

Tabulka 9-3 Incident na honeypotu - fáze Rozšíření vlivu

Případ užití: Incident na honeypotu - fáze Rozšíření vlivu
Stručný popis:
Útočník se snaží rozšířit svůj vliv na jiné systémy.
Primární aktéři:
Útočník
Vedlejší aktéři:
C2 server
Vstupní podmínky:
Útočník má přístup k napadenému systému. Útočník má přístupové údaje získané předcházejících kroků. Útočníku může komunikovat s řídícím serverem C2.
Hlavní scénáře:
1. Útočník zvolí informace k napadení okolních systémů ze získaných údajů 2. Útočník se připojí k cíli pomocí získaných údajů - může to být honeypot 3. Když je přihlášení úspěšné 3.1. Provede incident dle systému

4. Odešle zprávu o incidentu na C2 server 5. Když má k dispozici další údaje 5.1.Pokračuj bodem 1. Případ užití končí
Výstupní podmínky:
Žádné.
Alternativní scénáře:
Žádné.

Na následujícím diagramu jsou kombinace všech tří předchozích scénářů.



Obr. 9.7: Diagram Incidentu na honeypotu - Eskalace práv, Vnitřní průzkum a Rozšíření vlivu

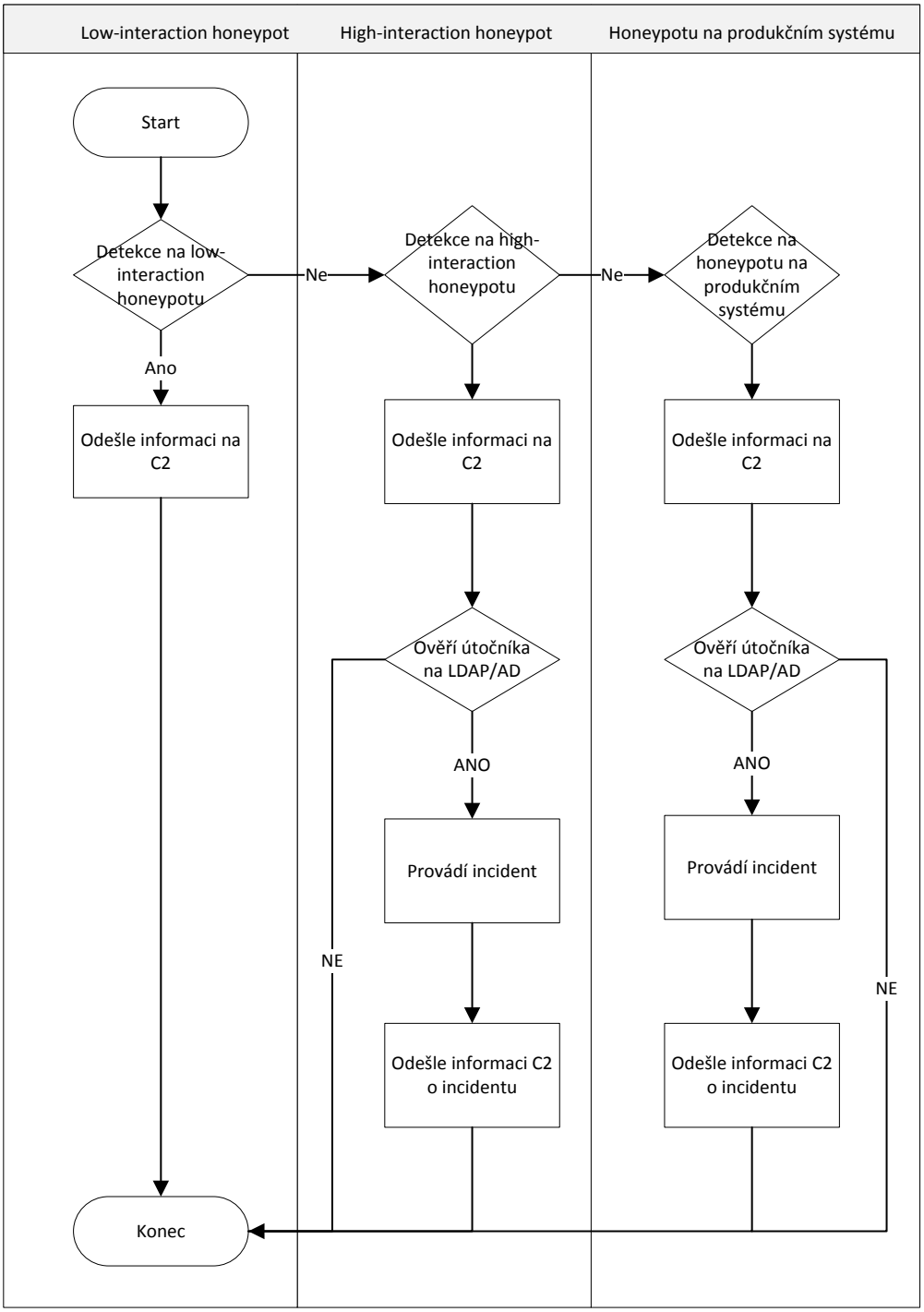
9.2.2 Honeypot

V následujícím scénáři je popis zaznamenání incidentu útočníka na honeypotu. Útočník ve fázi Rozšíření vlivu se zkouší připojit na honeypot. Ten připojení detekuje a provádí níže uvedené kroky.

Tabulka 9-4 Případ užití: Detekce incidentu na honeypotu

Případ užití: Detekce incidentu na honeypotu
Stručný popis:
Honeypot zaznamená incident na některém typu
Primární aktéři:
Vedlejší aktéři:
Útočník
Vstupní podmínky:
Hlavní scénáře:
• Když je incident identifikován na low-interaction honeypotu • Low-interaction honeypot odešle informaci o incidentu Centru Administrace • Případ užití končí • Když je incident identifikován na honeypotu na produkčním systému nebo na high-interaction honeypotu • Honeypot odešle informace o incidentu Centru Administrace • Když ověří útočníka na LDAP/AD serveru • Provádí incident • Když se ověření útočníka nezdaří • Případ užití končí • Honeypot odešle informace o incidentu Centru Administrace • Případ užití končí
Výstupní podmínky:
Žádné.
Alternativní scénáře:
Žádné.

Na dalším diagramu je zobrazen postup na systému honeypotů, pokud se útočník pokusí o incident na některý honeypot.



Obr. 9.8: Diagram Detekce incidentu na Honeypotu

9.2.3 Vyhodnocení incidentu

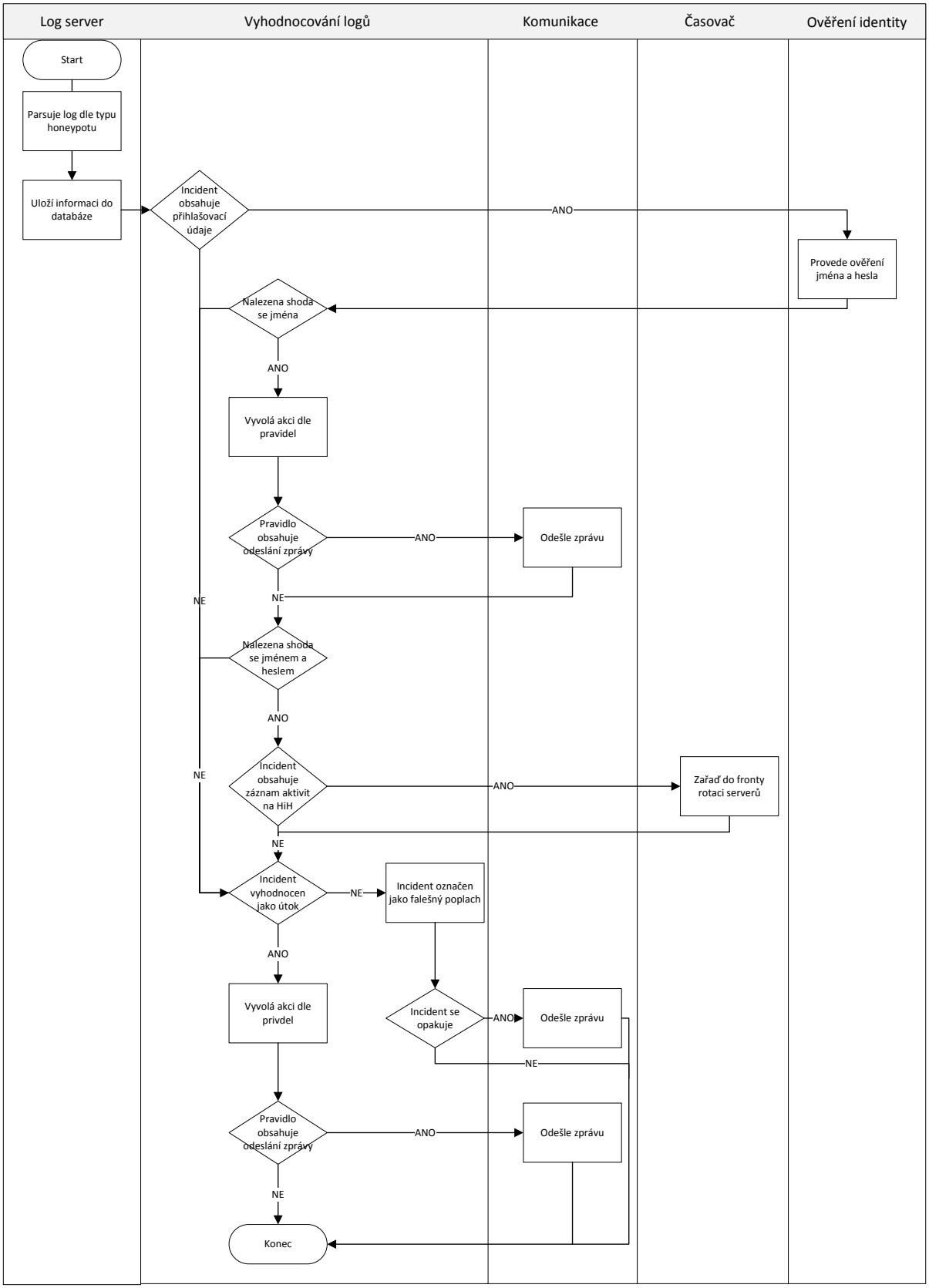
Pokud se projeví incident, Centrum administrace přijme informaci o incidentu a provede jeho následné vyhodnocení. Při závažném incidentu neprodleně kontaktuje administrátora, ohledně řešení eliminace útoku.

Tabulka 9-5 Incident

Případ užití: Incident
Stručný popis:
Centrum administrace detekuje incident na honeypotu, vyhodnotí jej a informuje administrátora o události.
Primární aktéři:
Administrátor
Vedlejší aktéři:
Vstupní podmínky:
Centrum administrace přijme informaci o incidentu na honeypotu.
Hlavní scénáře:
1. Sekce Log server parsuje log dle typu honeypotu 2. Uloží informaci do databáze 3. Sekce Vyhodnocování logů parsuje informaci o incidentu 4. Když je v incidentu obsaženo přihlašovací jméno nebo heslo 4.1. Provede ověření jména a hesla přes Ověřování identity 4.2. Když je nalezena shoda se jménem 4.2.1. Vyvolá akci dle pravidel 4.2.2. Když pravidlo obsahuje odeslání zprávy 4.2.2.1. Sekce Komunikace odešle vhodnou zprávu administrátory 4.2.3. Když je nalezena shoda se jménem a heslem 4.2.3.1. Když incident obsahuje záznam aktivit útočníka po ověření na high-interaction honeypotu 4.2.3.1.1. Zařaď do fronty Časovače rotaci serverů na dotyčném honeypotu 5. Když je incident vyhodnocen jako útok 5.1. Vyvolá akci dle pravidel 5.2. Když pravidlo obsahuje odeslání zprávy 5.2.1. Sekce Komunikace odešle vhodnou zprávu administrátory

6. Když není incident vyhodnocen jako útok 6.1. Incident je označen jako falešný poplach 6.2. Když se tento incident opakuje 6.2.1. Sekce Komunikace odešle vhodnou zprávu administrátory 7. Případ užití končí
Výstupní podmínky:
Žádné.
Alternativní scénáře:
Žádné.

Na digramu jsou podrobně zobrazeny postupy a rozděleny dle subsystémů Centra administrace. Při vyhodnocení incidentu jsou aktivovány subsystémy Log server, Vyhodnocování Logů, Komunikace, Časovač a subsystém Ověření identity na adresářové službě.



Obr. 9.9: Diagram – Detekce incidentu na honeypotu

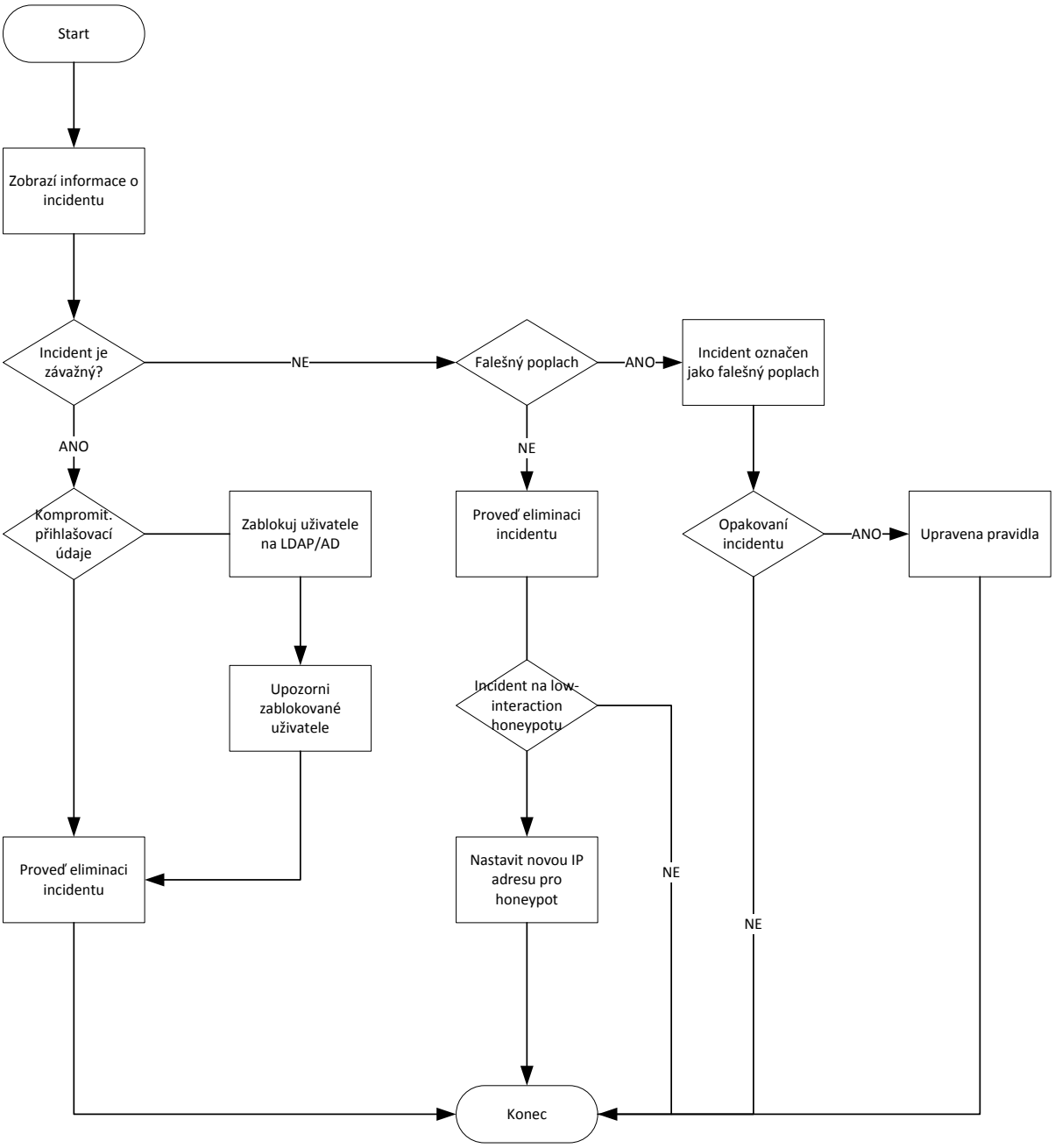
9.2.4 Administrátor

Scénář z pohledu Administrátora. Centrum administrace upozornilo administrátora na možný incident. Administrátor se přihlásí do systému, pro podrobnější informace, a pokud se jedná o útok, zahájí jeho řešení.

Tabulka 9-6 Administrátor - Incident

Případ užití: Administrátor - Incident
Stručný popis:
Administrátor vyhodnotí incident a provede adekvátní kroky.
Primární aktéři:
Administrátor
Vedlejší aktéři:
Uživatel
Vstupní podmínky:
Centrum administrace přijme incident Centrum administrace odešle oznámení administrátorovi o incidentu
Hlavní scénáře:
1. Administrátor se přihlásí do systému 2. Centrum administrace zobrazí informace o incidentu 3. Administrátor zkontroluje závažnost incidentu 4. Když je incident vyhodnocen jako závažný 4.1. Když jsou kompromitovány přihlašovací údaje 4.1.1. Zablokuje uživatele na AD/LDAP 4.1.2. Upozorní zablokovaného uživatele 4.2. Provede odpovídající úkony na eliminaci incidentu 5. Když není incident závažný 5.1. Když administrátor rozhodne, že nejde o falešný poplach 5.1.1. Provede odpovídající úkony na eliminaci incidentu 5.1.2. Když je incident na low-interaction honeypotu 5.1.2.1. Administrátor může změnit IP adresu low-interaction honeypotu 5.2. Když administrátor rozhodne, že jde o falešný poplach

5.2.1. Incident označen jako falešný poplach 5.2.2. Když se tento typ incidentu opakuje 5.2.2.1. Jsou upravena pravidla 6. Případ užití končí
Výstupní podmínky:
Žádné.
Alternativní scénáře:
Žádné.



Obr. 9.10: Diagram Vyhodnocení incidentu administrátorem

9.2.5 Agent

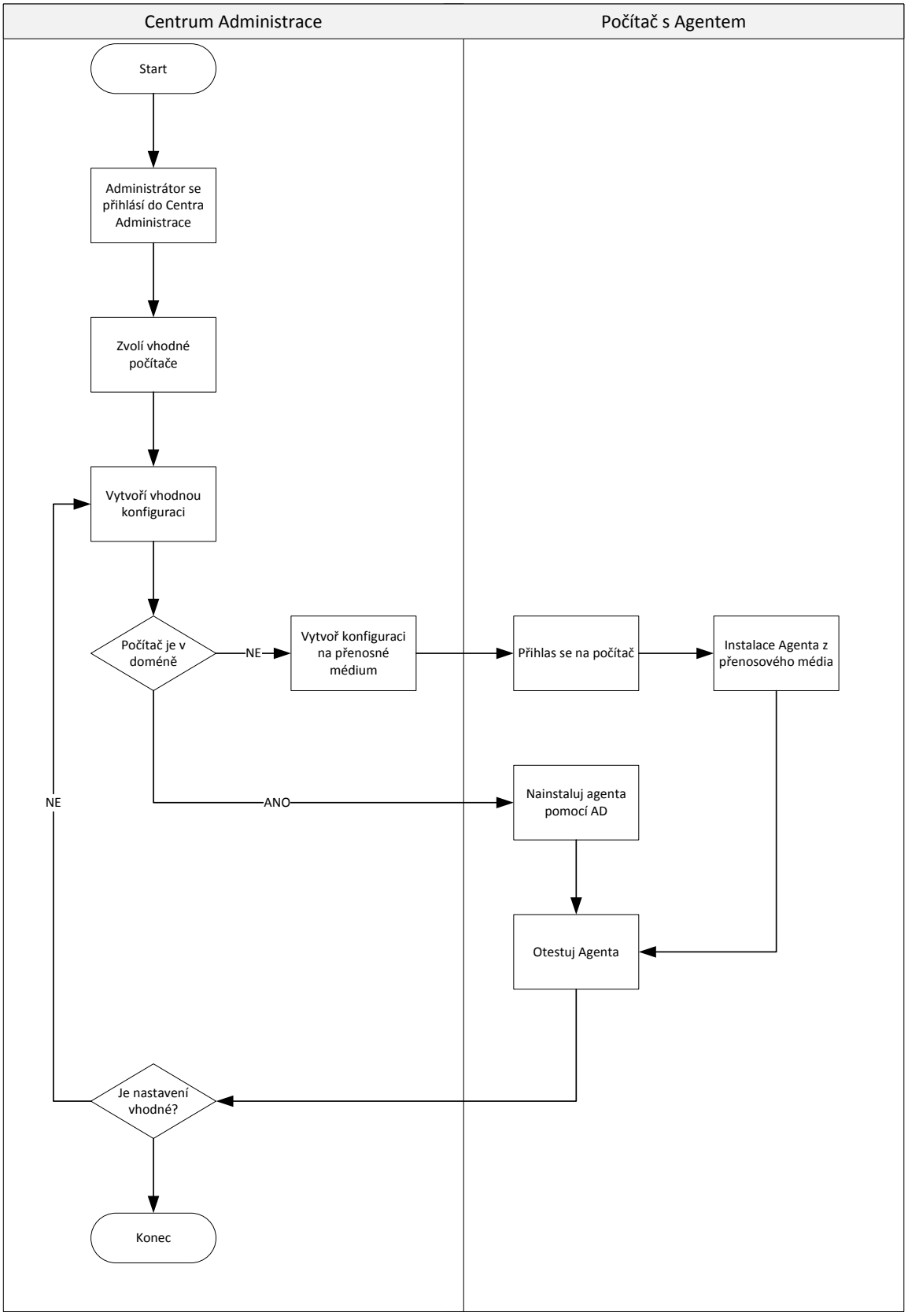
Agent implementuje do sledované sítě na námi vybrané hostitelské systémy. Nadbytečnou informaci, která není podstatná pro uživatele tohoto zařízení.

Implementace tohoto řešení je pomocí politik AD/LDAP nebo manuálně pomocí administrátora.

Tabulka 9-7 Nastavení Agenta

Případ užití: Nastavení Agenta

Stručný popis:
Administrátor instaluje a provozuje Agenta
Primární aktéři:
Administrátor
Vedlejší aktéři:
Vstupní podmínky:
Hlavní scénáře:
1. Administrátor se přihlásí do Centra Administrace 2. Zvolí vhodné honeypoty, na které zaměří Agenta 3. Zvolí vhodné počítače 4. Vytvoří vhodnou konfiguraci 5. Když je uživatelský počítač v doméně 5.1. Nainstaluj Agenta pomocí AD 5.2. Otestuj Agenta 6. Když není zvolený počítač v doméně 6.1. Vytvoř vhodnou konfiguraci na přenosné médium 6.2. Přihlas se na zvolený počítač jako administrátor 6.3. Nainstaluj Agenta z přenosového média 6.4. Otestuj Agenta 7. Když není Administrátor spokojen s nastavením 8. Pokračuj bodem 4 9. Případ užití končí
Výstupní podmínky:
Žádné.
Alternativní scénáře:
Žádné.



Obr. 9.11: Diagram - Implementace Agenta

9.2.6 Uživatel

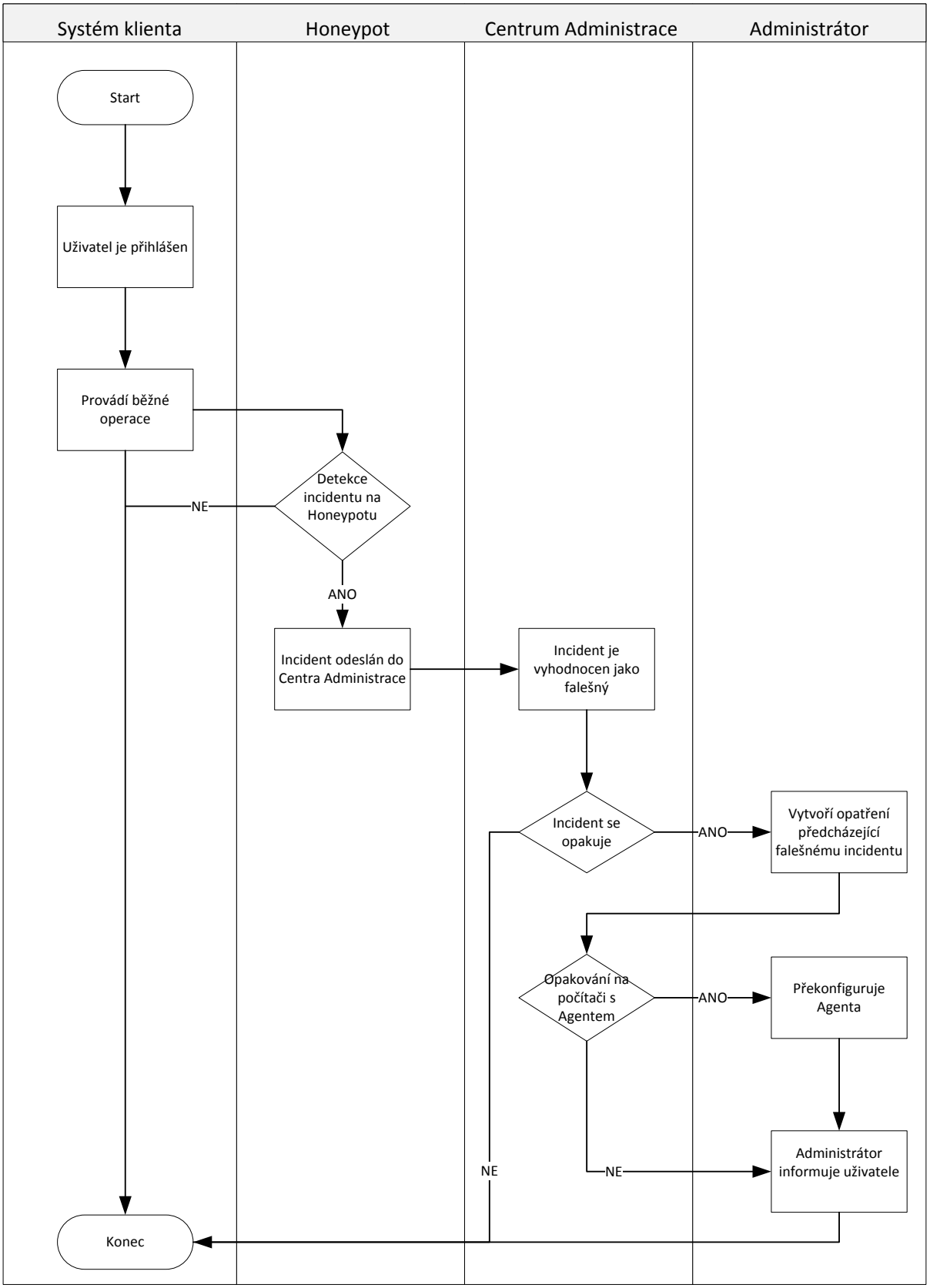
Dalším podstatným aktérem tohoto systému je uživatel. Uživatel by neměl mít tušení, že je nasazen systém honeypotů. Dle všeho by měl v systému vykonávat svoji obvyklou činnost. Pokud bude zachycen na některém z honeypotů mělo by se jednat o omyl. Když se incident od uživatele opakuje, a administrátor prověří informaci, zda se nejedná o útok, musí administrátor pozměnit pravidla na detekci incidentů. Pokud je instalován na systému uživatele Agent měla by být administrátorem pozměněna jeho konfigurace.

Tabulka 9-8 Falešný incident

Případ užití: Falešný incident
Stručný popis:
Uživatel provede incident na honeypotu jednou nebo opakovaně
Primární aktéři:
Uživatel
Vedlejší aktéři:
Administrátor
Vstupní podmínky:
Uživatel je přihlášen v systému
Hlavní scénáře:
1. Uživatel je přihlášen ve vlastním systému 2. Uživatel provádí běžné operace 3. Když je incident detekován na honeypotu 3.1. Incident je předán Centru Administrace 3.2. Incident je vyhodnocen jako falešný 3.3. Když se incident opakuje 3.3.1. Administrátor vytvoří opatření, předcházejícímu opakovanému incidentu 3.3.2. Když se incident opakuje z počítače s Agentem 3.3.2.1. Administrátor překonfiguruje Agenta 3.3.3. Administrátor kontaktuje uživatele 4. Případ užití končí
Výstupní podmínky:

Žádné.
Alternativní scénáře:
Žádné.

V následujícím digramu je zobrazen postup na řešení falešného incidentu v závislostech na jednotlivých součástech systému IDS.



Obr. 9.12: Diagram – Falešný incident

10 REALIZACE EXPERIMENTU

Byly stanoveny následující cíle:

- Analyzovat možnosti aplikace navrženého systému a vyhodnocení experimentů na vybraných systémech v laboratorních podmínkách na aktuálních hrozbách.
- Verifikovat navržený systém na skutečných hrozbách.
- Porovnat úspěšnost detekce incidentů na klasických honeypotech a na honeypotech, které jsou podpořeny systémem agentem.
- Detekovat kompromitované uživatelské účty.

Hlavní cílem experimentu bylo porovnat úspěšnost detekce incidentů na klasických honeypotech a na honeypotech, které jsou mapovány agentem.

10.1 Experimentální laboratoř

Byla vytvořena virtuální experimentální síť simulující reálnou instituci. Byla realizována pomocí virtualizačních serverů a několik fyzických pracovních stanic. Rozsah sítě simuloval střední firmu za firewalem při použití NATování. Byla nastavena vnitřní síť v rozsahu IP adres 10.2.1.1 - 10.2.6.255. Tato síť byla oddělena firewallem se striktními pravidly. Datové toky byly kontrolovány IDS SNORT a v případě podezření na nebezpečnou situaci anebo při pokusu zneužití laboratoře byl pokus pozastaven. Do sítě bylo vždy vloženo 5 kompromitovaných strojů a byly sledovány v délce 7 dní. Síť byla rozdělena na 5 virtuálních VLAN [7]. Pomocí VLAN se infikované stroje nemohli v průběhu celého experimentu ovlivňovat a byla zaručena jejich disjunktnost.

Následující kapitola popisuje stavbu laboratoře a použité vybavení

10.1.1 Použité HW zařízení a operační systémy

Na tvorbu hlavního jádra laboratoře byly použity následující hardwarové a operační systémy:

VMware ESXi, 5.1.0.

- SUPERMICRO 1U, 2x AMD Opteron Six Core 4226, 24GB RAM, 2x1 TB HDD
- DELL 1U, 1x Intel® Xeon® CPU X3360@ 2,86GHz, 4 Core, 4GB RAM, 2x500GB HDD

VMware ESXi, 4.1.0.

- Gigabyte X58A-UD3R, 1x Intel® Core™ i7 CPU 950 @ 3,07GHz, 4 Core, 12GB RAM 2x1, 2x2,5 TB HDD

- MSI MS-7250, AMD Athlon™ 64 X2 Dual Core Processor 5200+, 4GB RAM, 2x250GB
- MSI MS-7250, AMD Athlon™ 64 X2 Dual Core Processor 5200+, 6GB RAM, 2x500GB

Windows Server 2008R2 – Hyper-V

- Gigabyte X58A-UD3R, 1x Intel® Core™ i7 CPU 950 @ 3,07GHz, 4 Core, 12GB RAM 2x1, 2x1,5 TB HDD

NAS

- Synology DSM 4.2, 4x2,5 TB HDD

1 x PC ATX – AMD 2 GB RAM, HDD 160GB

10.1.2 Platforma pro laboratoř

Laboratoř byla vybudována většinou na systému VMware ESXi. Použití toho software jsem zvolil pro jednoduchost tvorby virtuálních serverů a jejich univerzální přenositelnost na jiný hardware. Vybudování sítě pomocí VMware ESXi není tak nákladné, jako kdybychom potřebovali pro každý systém vlastní dedikovaný hardware. Pomocí VMware ESXi můžeme podle potřeby rozložit zatížení systémů a můžeme libovolně měnit jejich hardwarové nároky. Laboratoř můžeme rozdělit na 6 systémů.

- Systém sad
- Systém standartních honeypotů
- Systém honeypotů mapovaných agentem
- Systém produkčních honeypotů
- Systém administrace
- Systém zabezpečení laboratoře
- Systém záloh

Následně rozebereme jednotlivé systémy podrobněji.

10.1.3 Použité systémy pro podporu laboratoře

Doménový řadič AD: Windows Server 2008R2 – Hyper-V

IDS Snort - SNORT

SMTP server pro laboratorní síť

DHCP – CISCO

Databázové servery: PostgreSQL

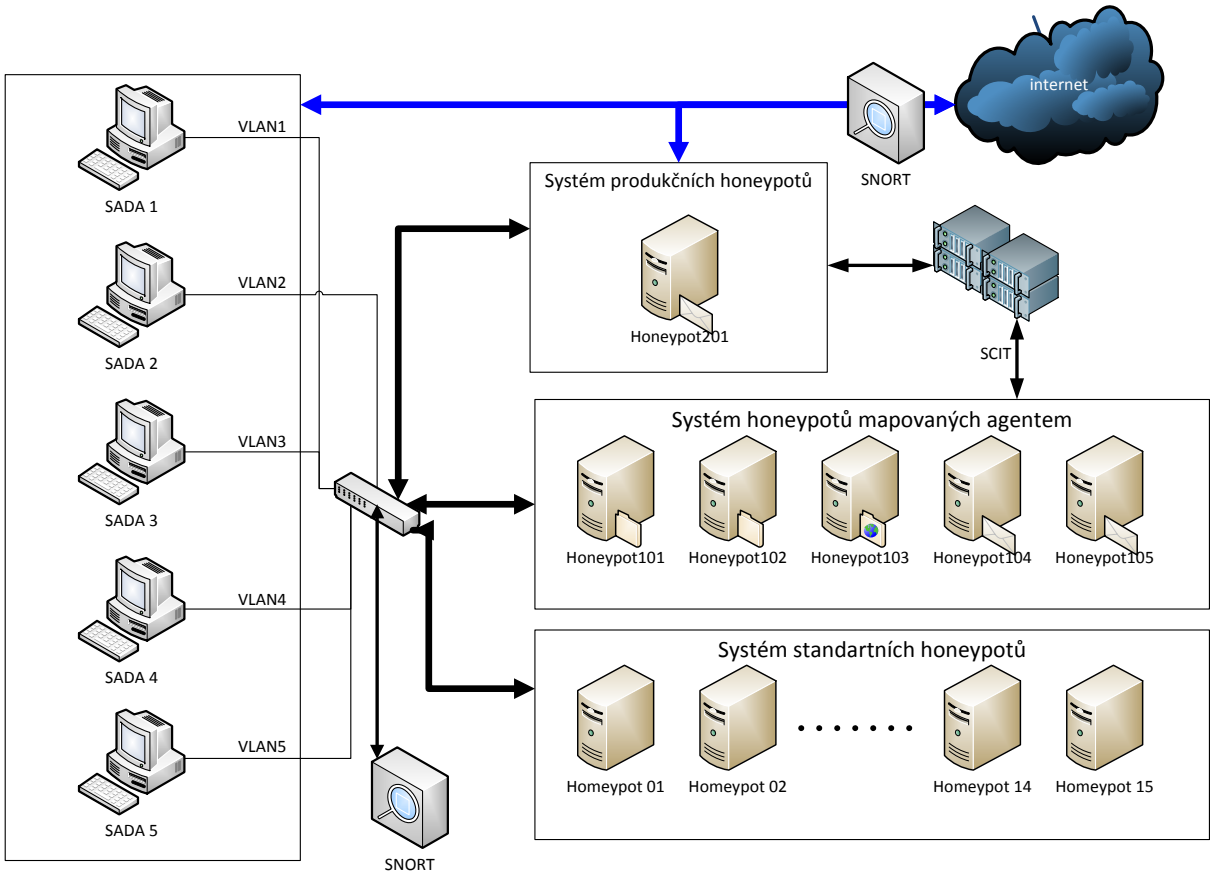
SCIT systém

CLONEZILLA

VMware vCenter Converter Standalone Client

10.1.4 Blokové schéma zapojení

Hlavní část experimentu je znázorněna na níže uvedeném grafu.



Obr. 10.1: Schéma zapojení systémů honeypotů a testovacích sad

Systém sad

Tento systém obsahuje zdroje nákaz a je vstupní branou pro útočníky. Navazuje na fázi Eskalace práv dle schématu útoku. Zdroje pro nákazy pro tyto sady byly vybírány z následujících zdrojů:

Z reálného prostředí byly částečně virtualizovány infikované stroje z posluchá-ren anebo od uživatelů, kteří udělili souhlas s touto operaci. Byla odstraněna nej-prve citlivá soukromá data a změněny přihlašovací údaje. Laboratorní sít co nej-více připomínala strukturou zdrojovou síť, ze které pochází napadené stroje. Dále na tyto stroje byli nasazeni agenti. Pokud to typ infekce povolil, byli stroje virtu-alizovány a provozovány ve virtuálním prostředí. Pokud ne, některé typy infekcí testovali, zda se nejedná o virtuální stroj, bylo použito jejich klonů na podobný fyzický stroj a ten následně připojen do laboratorní sítě.

Dále byly testovány zdroje nákaz z internetu. Z internetových zdrojů a fór byly staženy reálné nákazy a implementovány na čistý systém s odpovídajícím softwarovým vybavením. Dále tento stroj byl provozován jako fyzický stroj anebo byl virtualizován, dle druhu nákazy.

Dalším typem sad byly virtuální stroje, které byly dány k dispozici na ověření schopností reálného člověka, který se snažil získat co nejvíc informací o laboratorní síti.

Sady reprezentovaly následující operační systémy:

- Microsoft Windows XP Professional Service Pack 2
- Microsoft Windows XP Professional Service Pack 3
- Microsoft Windows Server 2003
- Microsoft Windows 7 Professional
- Microsoft Windows 7 Home
- Fedora Core 6 s kompromitovaným účtem root

Tyto sady byly provozovány v laboratorním systému a umístěny tak, aby každá sada byla spuštěna v jedné VLANě. Což znamenalo, že mohla přistupovat neomezeně ke všem částem sítě, ale nebyla schopna přistupovat k paralelně běžící sadě. SADA1 připojena k VLANě1, SADA2 připojena k VLANě2 atd.

Po skončení každé sady experimentu byl fyzický stroj přeinstalován a virtuální smazán.

Následně na těchto strojích se prováděli náhodně během pracovní doby manuální činnosti, jako připojování k síťovým diskům, prohlíženi internetu, spouštění programů, čtení pošty přes Microsoft Outlook a webmail a samozřejmě různé druhy přístupu na produkčních honeypot. Na tyto systémy se uživatel snažil přihlašovat určitými přihlašovacími údaji, zadanými v AD.

Systém honeypotů

Tyto segmenty byly navzájem propojeny, aby simulovali reálnou síť. Nebyly zde implementovány ostatní reálné zařízení jako tiskárny a reálné pracovní stanice a servery. Bylo to z důvodů výzkumu, abychom ověřili, zda infikované zařízení se budou snažit šířit na ostatní zdroje. Všechny honeypoty měli propojení do VLANY1-5, tedy se nacházeli vždy ve stejné VLANě jako vybraná SADA.

Systém standartních honeypotů

Anebo dále označovány jako honeypoty které nebyly mapovány Agentem.

Tato část systému byla realizována pomocí senzorů low-interaction honeypotů projektu SURFcert IDS. Tento senzor byl virtualizován a připojen do všech 5 VLAN. Honeypoty neměli na infikovaných počítačích žádný záznam o činnosti a

průběžně měnili svou IP adresu pomocí DHCP. Byli zjistitelné z pozice útočníka pouze skenováním a procházením sítě. V experimentu se jedná o honeypoty01 - 15.

Tyto honeypoty byly nastaveny pro účely experimentu na následující služby:

Tabulka 10-1 Služby na systému standartních honeypotů

Název	Služba	Protokol	Port
Dosažitelnost cíle	ICMP	ICMP4	
FTP server	FTP	TCP	21
Webový server	HTTP	TCP	80
Poštovní server	POP3	TCP	110
Sdílení souborů	Microsoft-DS, SMB	TCP	445

Systém honeypotů mapovaných agentem

Tato část byla realizována pomoci high-interaction honeypotů a připojena do všech 5 VLAN. Na rozdíl od standartního systému honeypotů byly tyto honeypoty určitým způsobem mapovány na infikovaných počítačích pomocí agenta. Jedná se o střední typ honeypotů, na které je povoleno přihlášení a následná činnost je mapována. V experimentu se jedná o honeypoty101 - 105. Dále je popis konkrétních honeypotů a jejich mapování z agenta na jednotlivé služby a porty TCP, na které se pak při vyhodnoceni experimentu zaměříme. Všechny tyto honeypoty samozřejmě registrují i na další služby jako segment low-interaction honeypotů.

Pro každou sadu experimentu, byly vygenerovány jedinečné přihlašovací údaje a zaneseny do AD. Tyto údaje, pokud byly kompromitovány, dále sloužili k identifikaci sady, ze které útok pocházel, jak z vnitřní sítě, tak z internetu po skončení životnosti sady.

Honeypoty 101-105 jsou high-interaction honeypoty, na kterých je povolena jen prioritní služba při přístupu z laboratorní sítě. Každý honeypot obsahoval 6 síťových adaptérů Každý honeypoty byl připojen do jiné VLANy1 až 5. Ovládání honeypotu probíhalo na administrativní VLANě, pomocí připojení na dalším síťovém adaptéru. Adaptéry 1-5, připojené do laboratorní sítě měly nastaveny firewall na povolení prioritní služby a dalších služeb jako systém standartních honeypotů.

Následuje podrobný seznam honeypotů101-105 na mapovaných agentem a jejich zaměření.

Honeypot101

Agent mapován z napadeného počítače na prioritní službu: Microsoft-DS - permanentně

Port: 445

Systém honeypotu: Windows Server 2008 R2

Na infikovaném stroji je mapován disk S, který se nachází na honeypotu101. Obsahuje systém adresářů, které nejsou zajímavé pro běžné uživatele. Jeho struktura adresářů byla následující adresáři SYS. Tento adresář se mapuje permanentně po přihlášení uživatele do systému. Aktivita a přístupy do mapovaného adresáře, prohlížení a manipulace a přístupy k souborům jsou odesílány na logovací server.

Honeypot102

Agent mapován na prioritní službu: Microsoft-DS – příležitostně

Port: 445

Systém honeypotu: Windows Server 2008 R2

Na infikovaný stroj se mapuje disk P se strukturou adresářů a souborů nezajímavých pro uživatele. Tento disk ale není připojen permanentně po přihlášení uživatele, ale připojuje se jen na určitý časový úsek, dle zadání v Plánovači úloh. Následně se po určité době opět odpojí. Ve skriptu jsou zadány přihlašovací údaje, které mají svůj ekvivalent v AD, pro pozdější ověření, zda údaje byly dále zneužity.

Honeypot103

Agent mapován na prioritní službu: FTP

Port: 21

Systém honeypotu: Fedora Core 6, použito modifikovaného ProFTPD Serveru jako medium-interaction honeypotu.

Na infikovaných strojích jsou údaje pro připojení na FTP. Jsou zadány přihlašovací údaje v programu Totalcmd a v dávce zabudovaného klienta FTP.Tyto útoky na Totalcmd byly populární ve Q2-Q4 roku 2012.

Na infikovaný počítač se administrátor v průběhu pracovní doby přihlašoval a připojoval se na FTP server. Tyto logy následně byly odeslány na logovací server a tam označeny jako normální provoz.

Honeypot104

Agent mapován na prioritní službu: POP3

Port: 110

Systém honeypotu: Fedora Core 6

Infikovaný stroj měl v registrech vytvořen záznam aplikace Outlook Express, Outlook a Mozzila ThunderBird o připojení k poštovnímu serveru pomocí služby POP3 na honeypotu104. Tyto údaje byli ověřitelné ve služby AD. Administrátor stroje spouštěl v pracovní době některé emailové klienty a tyto se připojovali na zadaný poštovní server. Záznamy z honeypotu104, které způsobil administrátor,

byly posléze označeny na logovacím serveru jako falešné incidenty. Údaje o jménu a heslu při použití Outlook Expresu jsou uloženy v registrech, v jednoduše dekódovatelné formě. Tyto údaje byly shodné s údaji v AD.

Honeypot105

Agent mapován na prioritní službu: HTTP

Port: 80

Systém honeypotu: Fedora Core 6

Infikovaný stroj měl v položkách IE, Firefoxu nebo Google chrome odkaz na přístup na poštu pomocí webového rozhraní. Adresa pošty byla http://webmail.vymola.info. Přihlašovací údaje byly zapamatovány ve výše uvedených systémech. Útočník nemusel pro přihlášení na webmail zadávat jméno a heslo, vše bylo předvyplněné. Údaje byly opět shodné s údaji v AD.

Systém produkční honeypot

Tento honeypot201 je realizován jako high-interaction honeypot. Základ tvoří virtuální stroj s operačním systém CentOS Linux 5.3 s těmito službami:

Kippo

Kippo je medium-interaction SSH honeypot navržený pro zaznamenání útoků hrubou silou na přihlášení, a po úspěšném přihlášení, systém provádí interakce s útočníkem. Vše se zaznamenává.

Základní vlastnosti jsou.

- Falešný systém s možností přidat / odebrat soubory. Plně falešný souborový systém podobný Debianu 5.0.
- Možnost přidání falešného obsahu, takže útočník může k "falešným" souborům, například / etc / passwd.
- Session záznamy jsou uložené v kompatibilním formátu UML pro snadné přehrávání s časovými záznamy odesílány na logovací server.
- Kippo ukládá soubory stažené pomocí wget pro pozdější kontrolu

FTP

Použito modifikovaného ProFTPD serveru [53] jako medium-interaction honeypotu. Zaznamenává všechny pokusy o přihlášení a po úspěšném přihlášení a ověření přihlašovacích údajů, je útočník vpuštěn do systému.

Vlastnosti tohoto honeypotu:

- Falešný systém s možností přidat / odebrat soubory. Plně falešný souborový systém podobný Debianu 5.0.

- Možnost přidání falešného obsahu. Útočník se může dostat k souborům, které nejsou ale přístupné přes http protokol.
- Záznamy o aktivitách jsou odeslány na logovací server.
- Uložené soubory jsou kopírovány a archivovány pro pozdější kontrolu.

Webmail

Bylo použito upravené řešení SquirrelMail [54]. Byl přidán skript na monitorování přihlášení. Při zadání přihlašovacích údajů, byly tyto údaje ověřeny přes AD a následně odeslány na logovací server. Útočníkovi bylo dovoleno pří úspěšném přihlášení se pohybovat v emailovém účtu. Tento účet obsahoval náhodnou korespondenci. Útočník mohl odeslat email, ale ten byl přesměrován do souboru /tmp/webmail. Po analýze tento soubor pak posloužil k identifikaci závažnosti útoku.

Tento honeypot byl na rozdíl od ostatních připojen jak do interní sítě, tak i do internetu. Byl přísně sledován a pomocí technologie SCIT byl rotován a neustále obnovován. Případný incident, tak nebyl schopen napáchat větší škody v okolních sítích a internetu.

Systém administrace

Vyhodnocení a zpráva experimentu probíhalo v Centru Administrace.

Systém zabezpečení laboratoře

Monitoring

V průběhu experimentu hrozilo zneužití laboratoře k dalším útokům mimo vyhrazenou oblast, a proto byla všechna komunikace v laboratoři kontrolováno pomocí IDS Snort (http://www.snort.org/).

SNORT je IDS program sloužící k detekci útoků a odposlechu v síti, kde hledá vzorky známých útoků a v případě nalezení je schopen provádět různé akce. Obsahuje velkou databázi vzorků, které se průběžně aktualizuj, a udržují. Není to firewall, což znamená, že detekuje již vzniklé problémy, ale nijak jim nezabraňuje. Snort běžel v módu Network intrustion detection system mode. V módu Snort odchytává síťová data a analyzuje je v kontextu s uživatelem definovanými pravidly a provádí předefinované akce. Snort byl připojen ke všem přístupovým kanálům pomocí TAP. To znamená, že komunikace např. mezi infikovaným zařízením a portem switche je kompletně duplikována na port Snortu, aniž by byla tato komunikace nějak modifikována.

Dále Snort podporuje více konfigurací na základě VLAN ID nebo IP podsítě v rámci jedné instance Snortu. To umožnilo v rámci jedné instalace SNORTu vytvořit vlastní konfigurační soubor pro každou virtuální sít 1-5 lépe než pro každou

VLANu použít samostatnou instalaci SNORTu. Každá tato konfigurace tak mohla mít jiné nastavení preprocesoru a jiná pravidla detekce.

Pokud IDS Snort detekoval porušení integrity experimentu, byl tento incident vyhodnocen administrátorem a byly podniknuty kroky, které se snažily udržet experiment v chodu a zároveň zabránit ohrožení systémů, mimo laboratoř.

Kontrola SMTP komunikace - SMTP server pro laboratorní síť

Simple Mail Transfer Protocol (zkratka SMTP) je internetový protokol určený pro přenos zpráv elektronické pošty (e-mailů) mezi přepravci elektronické pošty (MTA). Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem.

Pro kontrolu a zachycení odeslaných emailů z kompromitovaných systémů byl do laboratoře přidán SMTP server který zachytával SMTP komunikaci pro celou laboratoř.

Bylo použito modifikovaného systému Sendmail, který zachytával odeslané emaily a ukládal je pro pozdější zpracování. Tyto zprávy byly následně blokovány a nikdy nedošli k zadanému adresátovi.

Systém záloh a zdroje honeypotů

Jelikož honeypoty101-105, zvláště honeypot201 mohli být v rámci experimentu zneužity, byla nasazena technologie SCIT pro jejich bezpečný chod.

SCIT

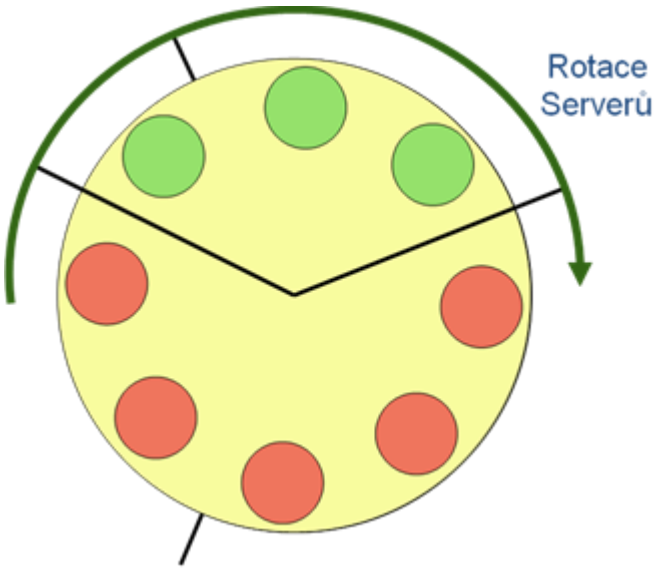
tolerantní přístup k obraně před hrozbami počítačových útoků. Je to jiný pohled na bezpečnost systémů než tradiční IDS a IPS.

SCIT namísto spouštění bezpečnostních mechanismů, které brání vniknutí do systému, zabrání pouze k selhání systému, ale útok neodstraňuje. Zaměřuje se na kritickou část infrastruktury serverů. Typicky lze přístup použít na zlepšení dostupnosti služeb a spolehlivosti systémů. Základní parametry lze popsat v následujících bodech:

- Akceptujeme narušení systému, nezjištěný útok může být i úspěšný, ale nesmí omezit funkčnost systému v určitém časovém intervalu.
- Využít náhradních, záložních serverů pro dostupnost a obnovu služeb.
- Základní stavební kameny tohoto řešení jsou konstantní rotace serverů a systém obnovy celého serveru, bez ohledu na to, zda je zjištěno narušení systému nebo ne.

Tento přístup využívá virtualizačních technologií ke snížení nákladů. Pozitivní je snížení doby expozice, po kterou systém vystavujeme nebezpečí, a zvyšuje dobu, po kterou můžeme pohodlně řešit bezpečnostní incident a následně mu zabránit. [36],[37]

V následujícím příkladu je ukázkové schéma s 8 servery. Použijeme 5 serverů červené barvy, které jsou exponovány a zabezpečují činnost. 3 servery zelené barvy jsou odpojeny a probíhá jejich obnova. Obnovovány jsou i v případě, že neexistuje podezření o jejich napadení. Je to rychlejší, než jejich kontrola, zda byly kompromitovány. Interval rotace je konstantní časový okamžik, a v ukázkovém případě platí: čas obnovení jednoho serveru < 3 * interval rotace

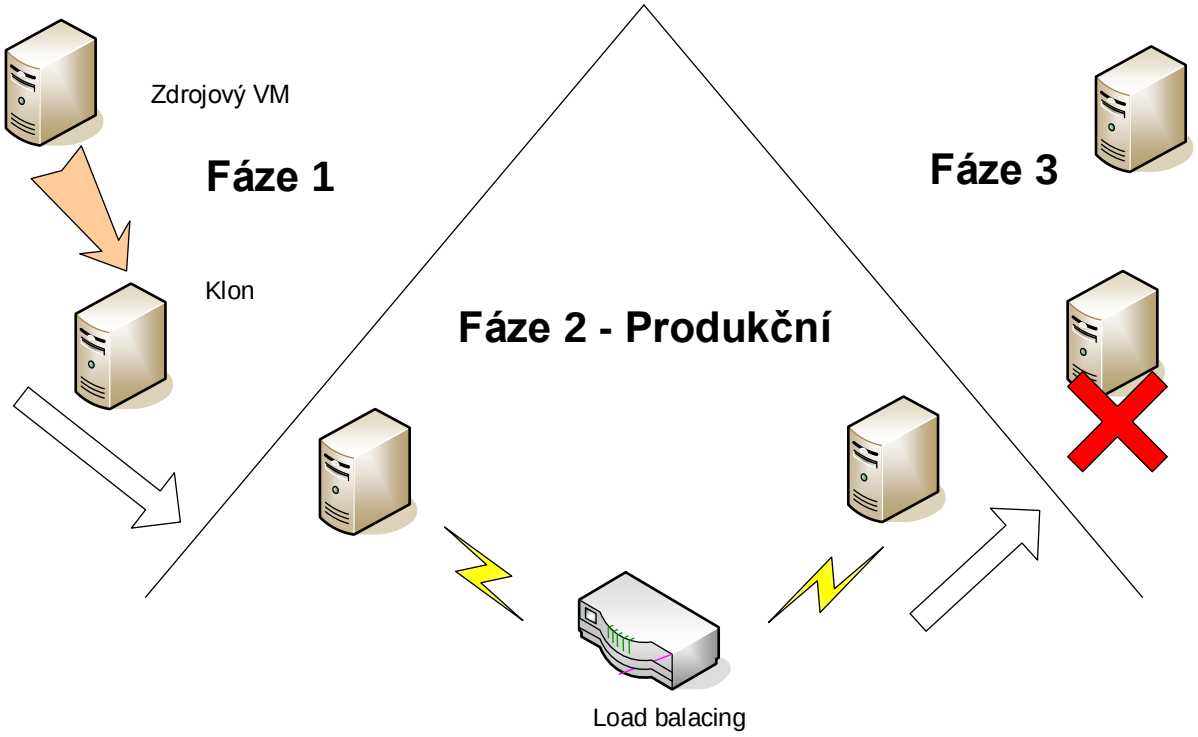


Obr. 10.2: Ukázka rotace serverů: 5 online a 3 offline servery

Při realizaci laboratoře byla tato myšlenka mírně modifikována pro potřeby experimentu.

Realizace tohoto systému v rámci experimentu bylo založen na VMvare ESXi serveru. Pro tuto možnost bylo zvoleno prostředí VMware VIMA. VIMA je virtuální stroj, který obsahuje sadu softwaru. Zde je možné využít VIMA na spouštění skriptů a agentů pro správu ESXi systémů. VIMA zahrnuje části jako VI Perl Toolkit a VMware Infrastructure remote CLI pro správu ESXi serverů. Zde je také spuštěn skript SCITclone.sh, který provádí samostatné klonování dle zadaných parametrů.

SCITclone.sh generuje plnohodnotné stroje z původního originálu VM (které zahrnují všechny VMDK soubory s ním spojené). Každý klonovaný virtuální stroj zdědí všechny atributy vztahující se ke zdrojovému VM, kromě UUID a jména, které bude unikátní v rámci všech vytvořených klonů. Musí se jen brát na zřetel volné místo na datovém úložišti. To zahrnuje samotnou velikost virtuálního stroje, ale také závisí na velikosti odkládacího souboru a prostoru pro případné snímky.



Obr. 10.3: Blokové schéma zapojení SCIT

Popis fází na blokovém schématu

1. Vytvoří klon VM z originálního VM' pomocí skriptu SCITclone.sh
2. VM' je v produkční fázi
3. Po určeném intervalu je spuštěna opět fáze 1, a následně VM' je odpojen, na určitý časový úsek archivován, a pokud se nepoužil k další analýze, tak smazán.

10.1.5 Vlastní realizace experimentu

Experiment probíhal v intervalu od 8.1.2013 do 6.8.2013 tj. 30 týdnů. V rámci experimentu probíhalo testování 5 sad na samostatných VLANech v každém týdnu v délce 7 dní. To znamená, že každá sada viděla pouze systém honeypotů a nemohla ovlivnit paralelně běžící sadu. Výsledky byly zaznamenány v administračním systému a následně zpracovány. Každé přihlašovací údaje, zadané v jednotlivých sadách byly jedinečné a byly speciálně vygenerovány pro každou sadu. Tyto údaje měli ekvivalent v AD, které bylo speciálně použito pro tento experiment. Jména uživatelů odpovídaly reálným jménům, hesla byly čerpány z databáze slovníkových útoků na honeypoty. Všechny honeypoty se nacházeli ve stejné VLANě. Pouze Honeypot201 byl přístupný ze dvou VLAN. První VLAN z laboratorní sítě, druhá z vnější sítě. Každý honeypot v laboratorní síti měl náhodně přidělenou IP adresu v délce trvání jedné sady, tj. 7 dní.

Při dalším běhu sad honeypoty změnili svou IP adresu. Výjimku tvořilo rozhraní honeypot201 přístupné z vnější sítě, adresa se neměnila po dobu celého experimentu.

10.1.6 Důsledek

Při experimentu nebyly ohroženy žádné organizace, osoby a systémy. Experiment byl proveden se souhlasem zodpovědné osoby a nebyly porušeny pravidla komunikace v sítích.

11 VÝSLEDKY EXPERIMENTU

11.1Zdroje útoků v rámci experimentu

V rámci experimentu probíhalo testování 5 sad na samostatných VLANech v každém týdnu v délce 7 dní. Celkem bylo použito celkem 150 sad.

Infekce sad pocházely z následujících zdrojů:

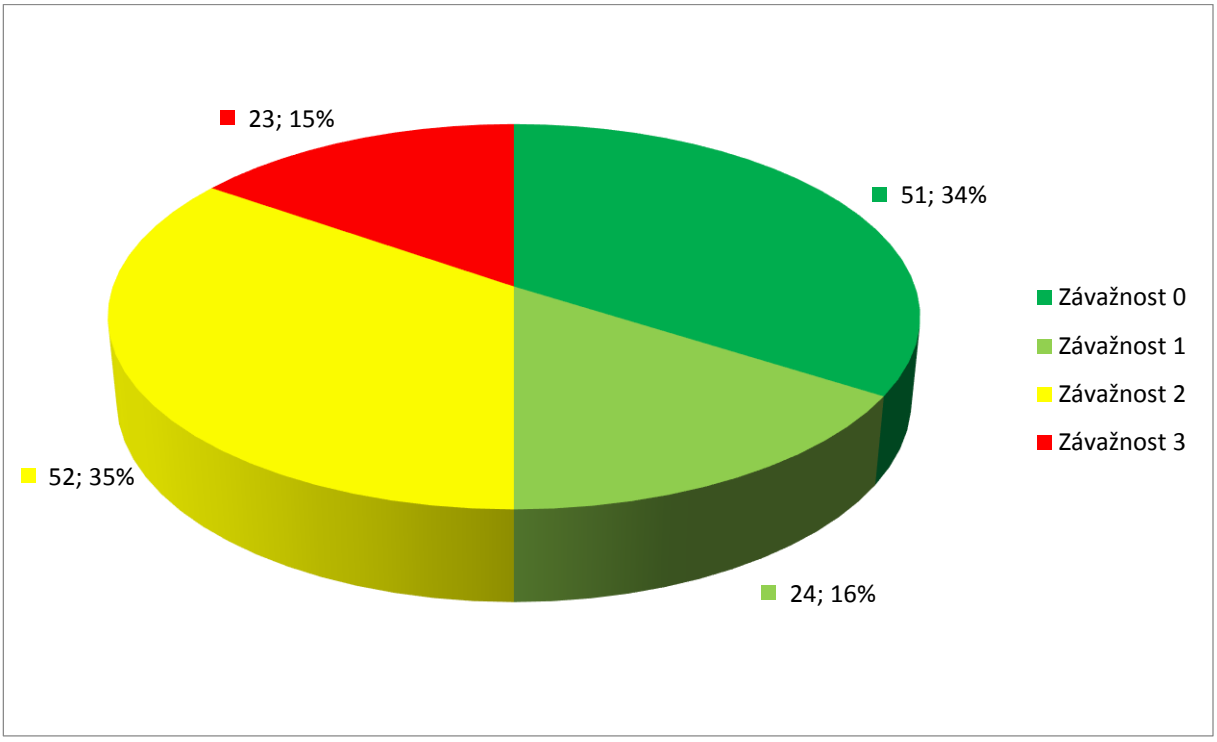
- Virtualizované infikované systémy z reálného prostředí
- Klonované infikované systémy z reálného prostředí
- Reálný útočník
- Systém s implementovanou infekcí pomocí administrátora
- Systémy s implementovanou infekcí pomocí uživatele
- Některé sady byly kombinace výše uvedených možností

11.2Detekované nebezpečí incidentu dle závažnosti

Každá sada byla zapojena v laboratoři 7 dní. Po dobu své životnost vyvíjela nějakou aktivitu, která byla detekována na systémech honeypotů. Závažnost aktivity byla ohodnocena čtyřstupňovou stupnicí 0-3 dle níže uvedené tabulky.

Tabulka 11-1 Stupnice závažnosti incidentů

Nebezpečnost incidentu	Popis a vysvětlení
Závažnost 0	Není detekován žádný incident.
Závažnost 1	Pouze detekce incidentu na honeypotech, bez pokusu o kompromitaci účtu.
Závažnost 2	Detekce incidentu na honeypotech101-105,201, pokus o kompromitaci uživatelského účtu na honeypotu z napadeného stroje.
Závažnost 3	Kompromitován uživatelský účet. Bylo evidováno úspěšné přihlášení na některém ze systému honeypotů.



Obr. 11.1: Graf: Ohodnocení nebezpečnosti incidentů během pokusu

Dle výsledků 45% sad nebylo zaznamenáno na žádném honeypotu. Tyto sady po přesunu do laboratoře nevyvíjely žádnou aktivitu, aby se z infikovaného systému šířili dále nebo jej žádný honeypot nezaznamenal.

Útočníci na 56% sadách se snažily infikovat nebo prozkoumávat okolí napadené sady a tyto aktivity byly zaznamenány minimálně na jednom z honeypotů.

Útočníkům z 50% sad se pokusilo kompromitovat jeden ze dvou údajů: uživatelské jméno nebo heslo

Z 15% sad se podařilo infiltrovaly high-interaction honeypoty s kompromitovanými údaji a úspěšně se útočník přihlásit. Dále mohl vyvíjet nelegální činnost.

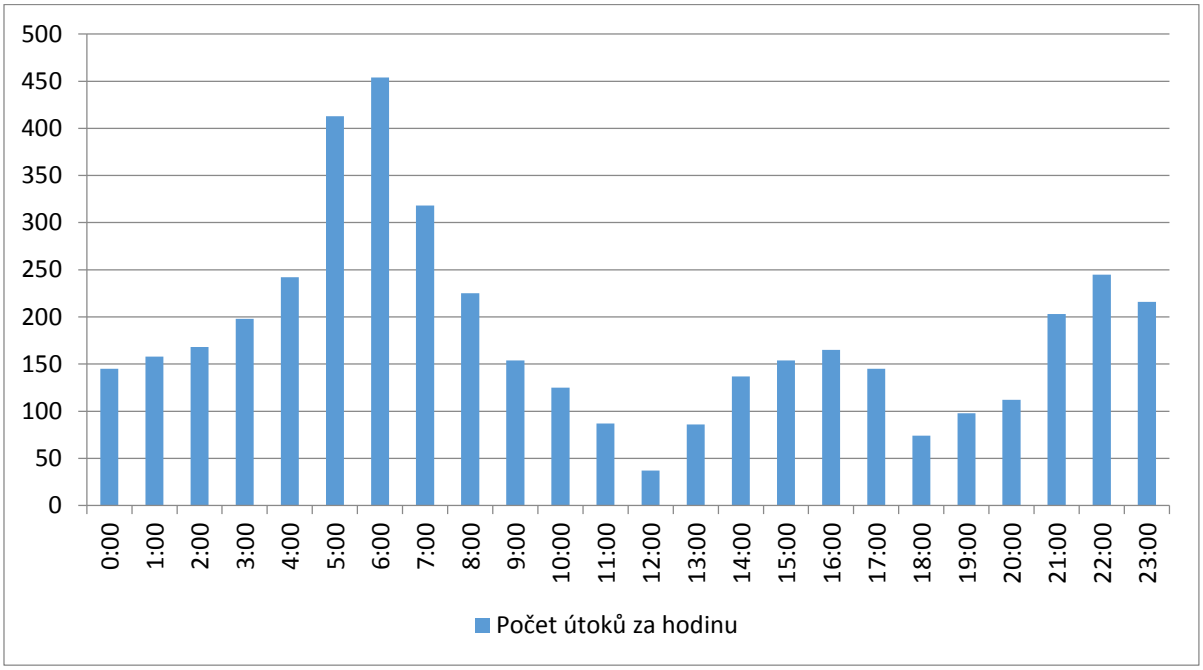
V následující tabulce zobrazujeme přehledně časový interval, délku jednotlivých sad a úroveň aktivity jednotlivých sad.

Tabulka 11-2 Celkový přehled experimentu včetně závažnost incidentů

Datum od	do	SADA1	SADA2	SADA3	SADA4	SADA5
8.1.2013	15.1.2013	2	3	3	3	3
15.1.2013	22.1.2013	1	3	3	2	3
22.1.2013	29.1.2013	3	1	2	2	2
29.1.2013	5.2.2013	3	3	3	1	2
5.2.2013	12.2.2013	2	2	2	2	0
12.2.2013	19.2.2013	3	0	0	0	2
19.2.2013	26.2.2013	0	3	3	1	2
26.2.2013	5.3.2013	2	2	0	1	0
5.3.2013	12.3.2013	0	2	1	1	1
12.3.2013	19.3.2013	2	1	0	0	2
19.3.2013	26.3.2013	0	1	0	2	1
26.3.2013	2.4.2013	0	2	0	0	0
2.4.2013	9.4.2013	0	2	2	0	1
9.4.2013	16.4.2013	0	3	0	1	1
16.4.2013	23.4.2013	2	1	3	0	1
23.4.2013	30.4.2013	0	0	3	0	2
30.4.2013	7.5.2013	2	2	2	2	2
7.5.2013	14.5.2013	3	0	0	0	0
14.5.2013	21.5.2013	2	0	0	0	0
21.5.2013	28.5.2013	2	1	0	0	1
28.5.2013	4.6.2013	0	2	3	2	1
4.6.2013	11.6.2013	1	2	0	1	2
11.6.2013	18.6.2013	0	0	2	0	2
18.6.2013	25.6.2013	2	2	2	2	0
25.6.2013	2.7.2013	2	0	2	0	0
2.7.2013	9.7.2013	3	0	2	0	0
9.7.2013	16.7.2013	2	0	2	2	0
16.7.2013	23.7.2013	3	0	1	3	2
23.7.2013	30.7.2013	2	2	0	3	1
30.7.2013	6.8.2013	0	1	2	2	2

11.3 Aktivita sad dle denní doby

V rámci experimentu bylo zaznamenáno 4359 incidentů na všech systémech honeypotů pocházející z laboratoře nebo z vnější sítě. Incidenty byly pro přehlednost seskupovány v rámci časového intervalu 1 hodina.

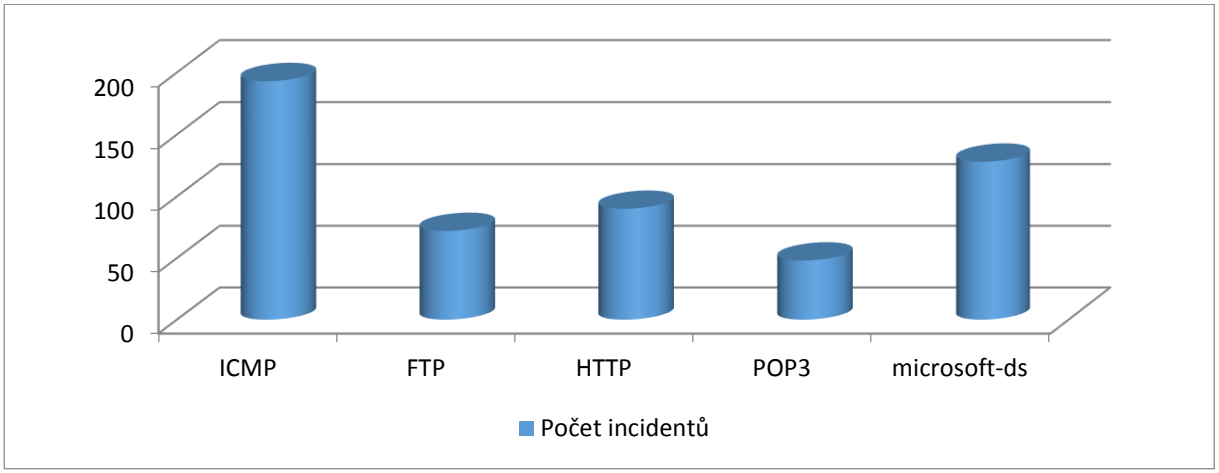


Obr. 11.2: Graf: Aktivita sad v závislosti na denní době na všech sledovaných službách

Z výše uvedeného grafu lze odvodit, že útočníci nebo boty jsou nejvíce aktivní v brzkých ranních hodinách. Využívají skutečnosti, že v tuto dobu není většinou přítomna lidská obsluha, a útoky jsou řízeny z východních časových pásem. Aktivita některých útoků byla konstantní i více hodin.

11.4Počet incidentů na jednotlivých službách

Na honeypotech01-15 a 101-105 byly vyhodnoceny počty incidentů v době trvání experimentu. Incident se skládá z jednoho nebo více útoků zaměřených na konkrétní službu. Sledovali jsme služby ICMP, FTP, http, POP3 a Microsoft-DS.



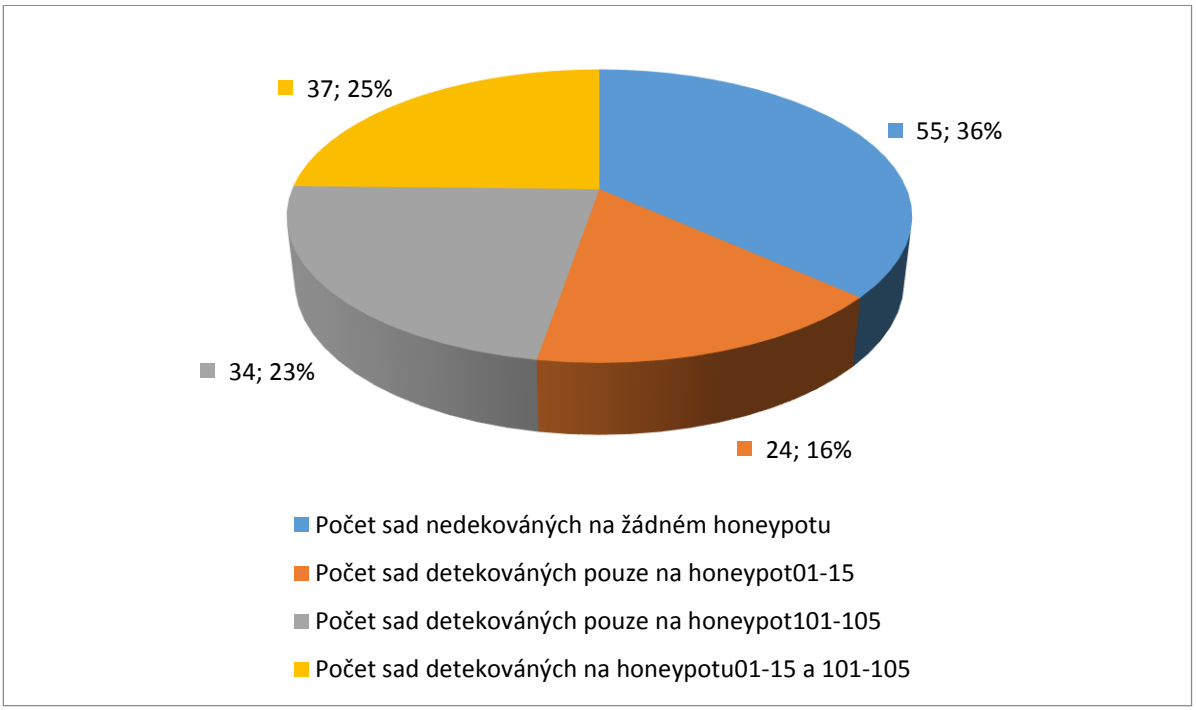
Obr. 11.3: Graf: Počet incidentů na jednotlivých službách na honeypotech1-15 a 101-105

Graf potvrzuje trend posledních let. Útočníci se nejvíce zajímají o služby FTP a Microsoft-DS. Služba FTP je jednoduše zranitelná a velmi oblíbená při přístupu

na webové servery. Microsoft-DS při slabém zabezpečení nabízí útočníkovy většinou hodnotné data.

11.5Srovnání úspěšnosti detekce incidentů na standartních honeypotech a na honeypotech, které jsou mapovány agentem

Vztah mezi počtem detekovaných incidentů na systémech standartních honeypotů, a na systémech honeypotů mapovaných agentem, je vidět na následujícím grafu.



Obr. 11.4: Graf: Počet sad detekovaných na určitých typech honeypotů

Na grafu lze vidět vyšší úspěšnost detekce honeypotů, které jsou ovlivněny agentem. Následně rozebereme důvody. Z experimentu vyplynulo že honeypoty, které jsou mapované v infikovaném systému pomocí agenta, mají úspěšnost 55%

Honeypoty01-05, které útočník detekuje pouze skenováním a procházením sítě, byly zjištěny útočníky v 38% případů.

42% infikovaných sad nebylo detekováno na žádném honeypotu.

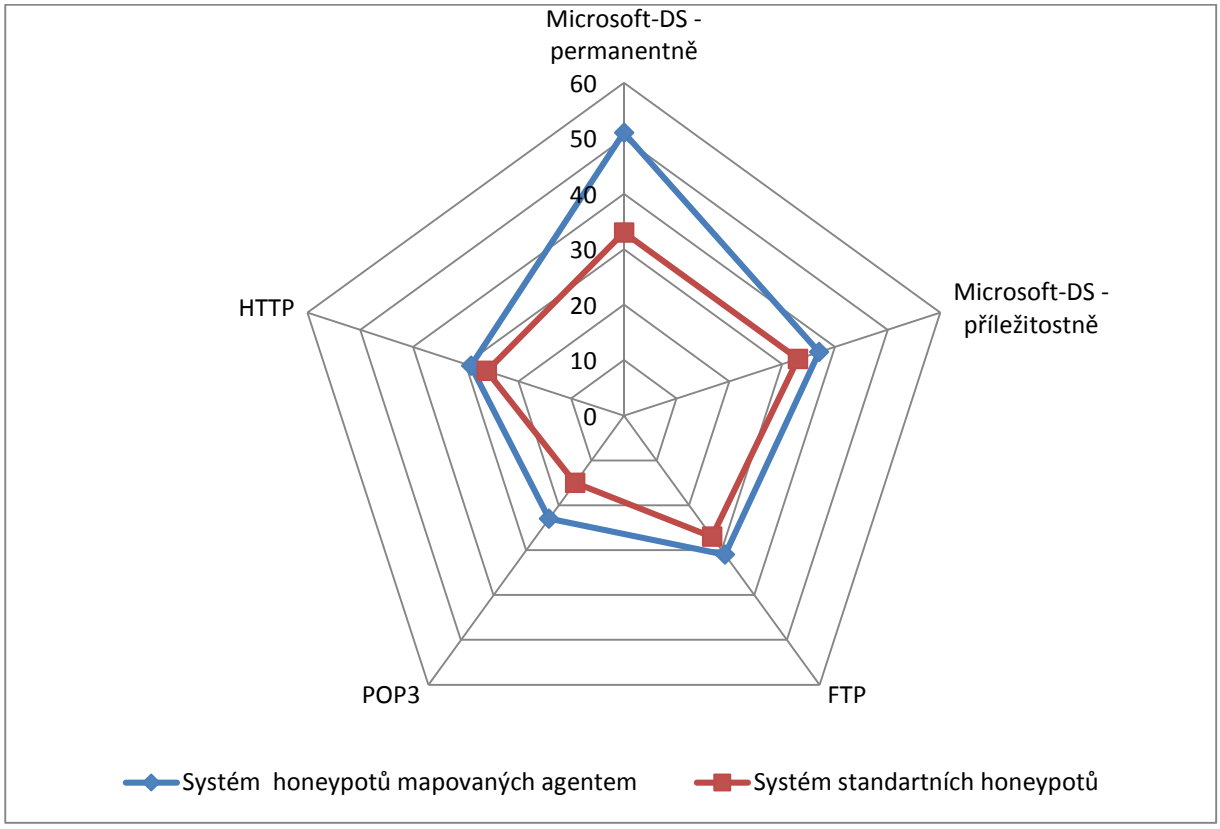
Dále jsem se v experimentu zaměřil na vybrané služby, které jsou nejvíce útočníky zneužívány. Následovně byly sledovány a vyhodnoceny níže uvedené údaje.

Tabulka 11-3 Seznam honeypotů mapovaných agentem a jejich popis

Název	Hlavní zaměření	Služba	Port

honeypot101	Mapováno agentem	Microsoft-DS - permanentně	445
honeypot102	Mapováno Agentem příležitostně bez hesla, jen pomocí uživatelského jména. Disk se připojuje a odpojuje jen v určitých časových úsecích.	Microsoft-DS - příležitostně	445
honeypot103	FTP	FTP	21
honeypot104	POP3	POP3	110
honeypot105	http://lokalni webmail	HTTP	80

Dle následujícího paprskového grafu je zřejmé, že systém honeypotů mapovaných agentem je efektivnější než systém standartních honeypotů.



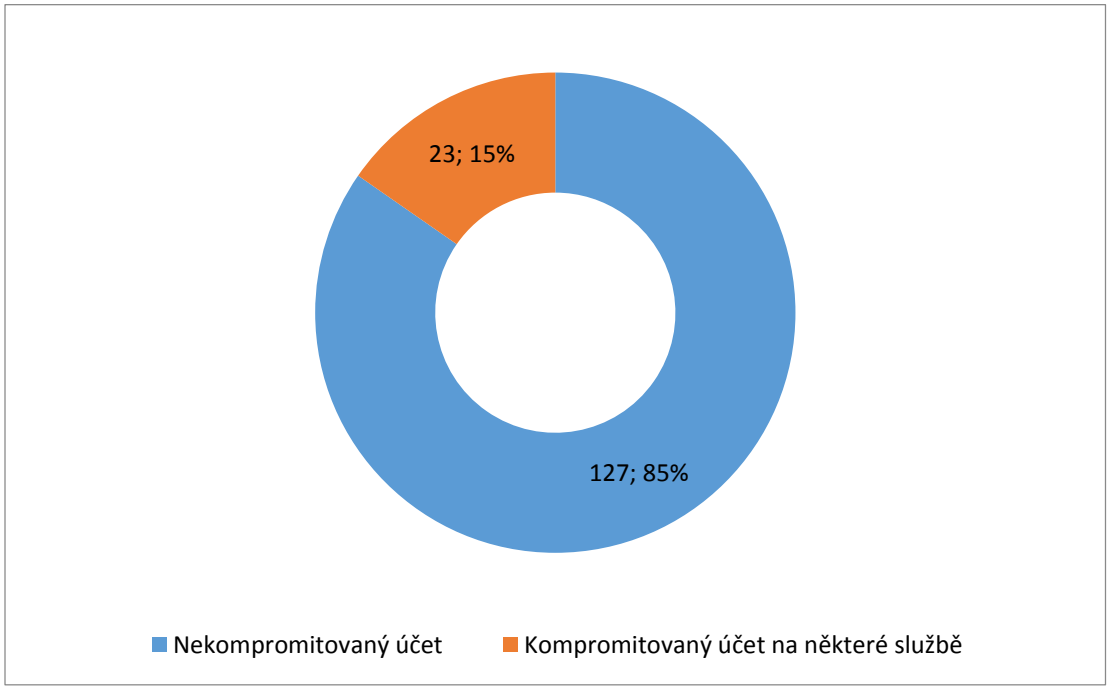
Obr. 11.5: Graf: Srovnání aktivit na vybraných portech mezi systémem standartních honeypotů a systémem honeypotů s agentem

Z grafu vyplývá, že největší zájem útočníků byl službu Microsoft-DS na portu 445. Je to nejvíce používaná služba pro připojení síťových disků v rámci organizace. Celková vyšší úspěšnost detekce honeypotů, kteří jsou mapovány agentem je dána systémem, jak útočníci vyhledávají další cíle. Pokud je útok zachycen na obou typech honeypotů pravděpodobně to znamená, že útočník použil nějaký síťový skener a prohledával komplexně celý segment sítě.

Vyšší počet záznamů na honeypotech mapovaných agentem je dána vyspělostí útoku. Útočník neskenuje celý segment sítě, ale čerpá informace o budoucích cílech z infikovaného systému. Následně tyto informace použije a zkouší se připojit na konkrétní zadané adresy.

11.6 Kompromitované uživatelské účty

Při experimentu bylo vytvořeno 150 sad. Pro každou sadu byl vygenerován jedinečný uživatelský účet. Tyto účty byly implementované pomocí agenta do infikovaného systému.



Obr. 11.6: Graf: Poměr kompromitovaných a nekompromitovaných účtů

Dle grafu se v 15% případů podařilo útočníkům zjistit uživatelské údaje z infikovaného systému a je úspěšně použít na některém z cílových honeypotů. Kompromitovaný uživatelský účet v reálném prostředí je vysoká hrozba pro systém, a v dnešní době většinou standartními bezpečnostními nástroji detekovatelný.

11.7 Kompromitované uživatelské účty na vybraných službách dle zdroje útoku

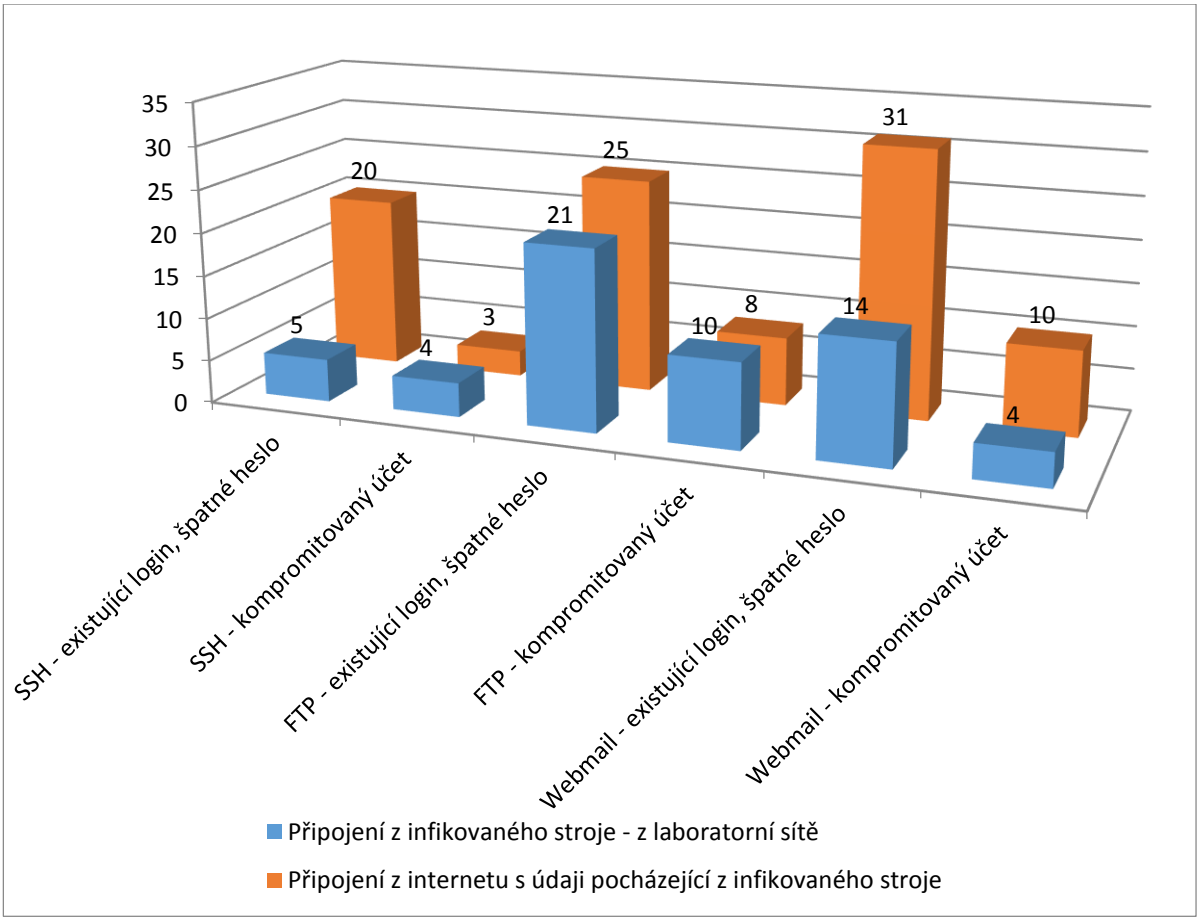
V experimentu se útočníkům podařilo kompromitovat uživatelské účty. Následně porovnáme nebezpečí kompromitovaných účtů vybrané služby. Tyto útoky jsem rozdělil do dvou skupin:

- útok na existující, kompromitované přihlašovací jméno (Login) a chybné heslo. Honeypot vrací informaci

  Login Failed for user – Bad Password

- útok na existující přihlašovací jméno (Login) a heslo (Password), které jsou po ověření vyhodnoceny správné. Honeypot vrací informaci:

  User logged in successfully



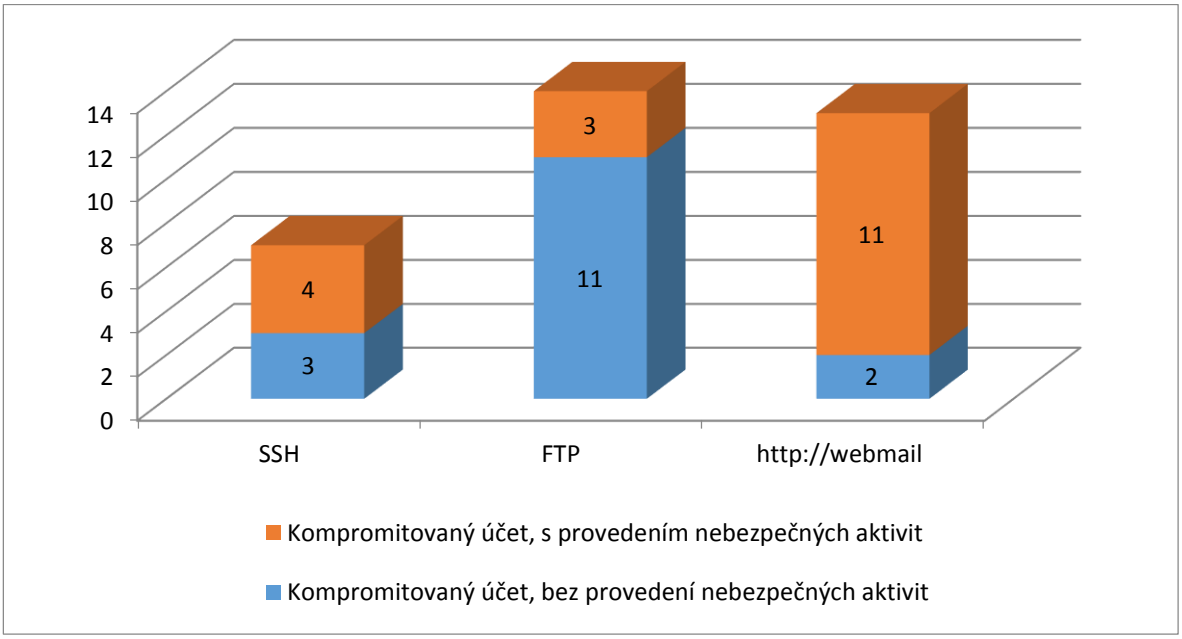
Obr. 11.7: Graf: Počet incidentů na vybrané služby dle počtu kompromitovaných uživatelských účtů a zdroje útoku.

Z grafu vyplývá, že útočníci detekovali z napadených systémů názvy uživatelských účtů, ale dekódování správného hesla je již těžší.

V některých případech bylo zaznamenáno přihlášení na konkrétní služby jak z vnitřní sítě, tak i z venkovní. Útočník nejprve otestoval účet z vnitřní sítě a dále získané data odeslal na svůj řídící server. Po určité době byly tyto informace použity pro přístup na honeypot z vnější sítě.

11.8Zneužití kompromitovaných účtů

Po kompromitování uživatelských přístupových údajů, po úspěšném přihlášení na honeypotu, útočnici začali provádět v některých případech nebezpečnou aktivitu.



Obr. 11.8: Graf: Počet zneužitých kompromitovaných účtů v rámci experimentu

11.8.1 Kompromitace účtů na SSH

Ze 7 kompromitovaných účtů, u 4 účtů byly zaznamenány a vyhodnoceny nebezpečné aktivity.

Útočník se snažili získat hesla systému, stáhnout malware a připravit jeho spuštění

11.8.2 Kompromitace účtů na FTP

Oblíbený cíl útočníků. FTP servery se nejčastěji používají k přenosu souborů na webové servery. I když je tato technologie již dávno zastaralá, pořád se používá pro svou rychlost, efektivitu a podpory různých platforem a systémů. Bohužel kompromitace tohoto protokolu je velmi jednoduchá. Ale v tomto případě pohodlnost a efektivnost, vítězí na zabezpečením.

Útočníci se při kompromitaci FTP účty nejprve snažili stáhnout data, pak nahrát své skripty, na které by v reálném provozu přistoupili pomocí protokolu http. Byly to sady skriptů na rozesílání spamu, ovládání botů a instalace bota pro tvorbu DDOS útoku.

11.8.3 Kompromitace účtů na http://webmail

Tento způsob kompromitace byl vytvořen uživatelem, který se přihlašoval na honeypotu a klikl na podvodný email, který uživatele přesměroval na podvodnou stránku a zadal uživatelské jméno a heslo.

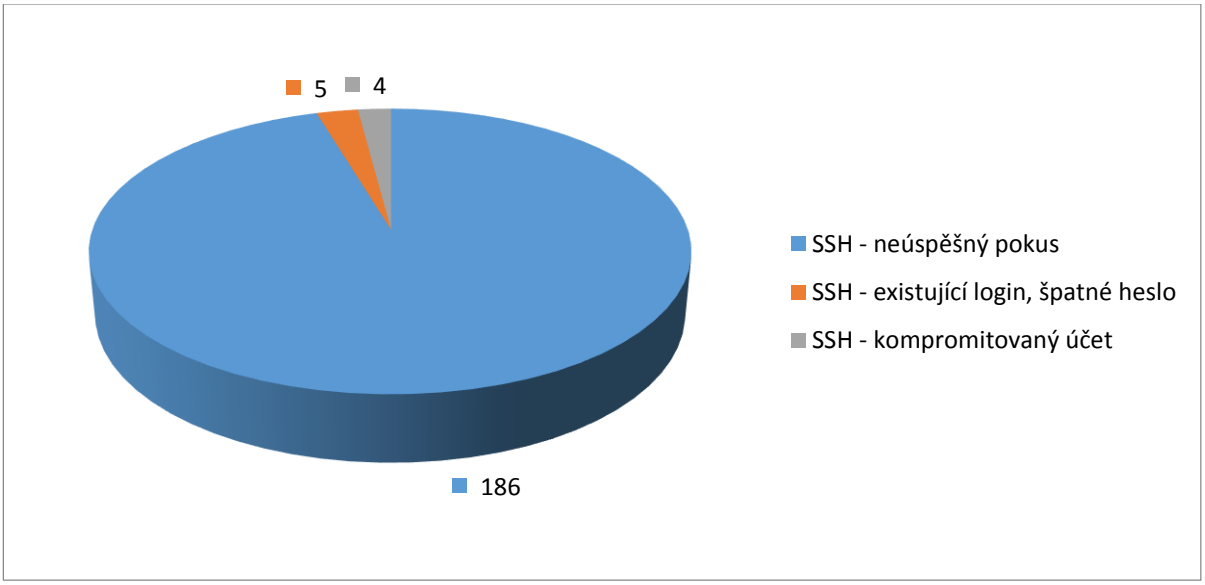
Tento účet byl ve velmi krátké době zneužit na rozesílání spamu V laboratoři byl ovšem odchycen. Tento typ útoku je velmi nebezpečný pro organizaci. Organizace se může objevit na některém systému blacklistů, a emailová komunikace je pak blokována, pro podezření rozšiřování spamu.

Útočníci se připojovali na kompromitovaný účet z vnější sítě, změnili ve webovém rozhraní emailového systému hlavičku odesílatele. Následně v určitých časových intervalech začali rozesílat kolekce spamů. V roce 2012 se tento útok dařilo jednoduše detekovat i na velkých poštovních serverech, jelikož útočníci posílali v jednom intervalu velkou dávku. V roce 2013 se postup změnil, a systém odesílání je po menších dávkách, nejčastěji v ranních hodinách a pracovní době organizace.

11.9 Pokusy o kompromitaci vybraných služeb z vnitřní sítě

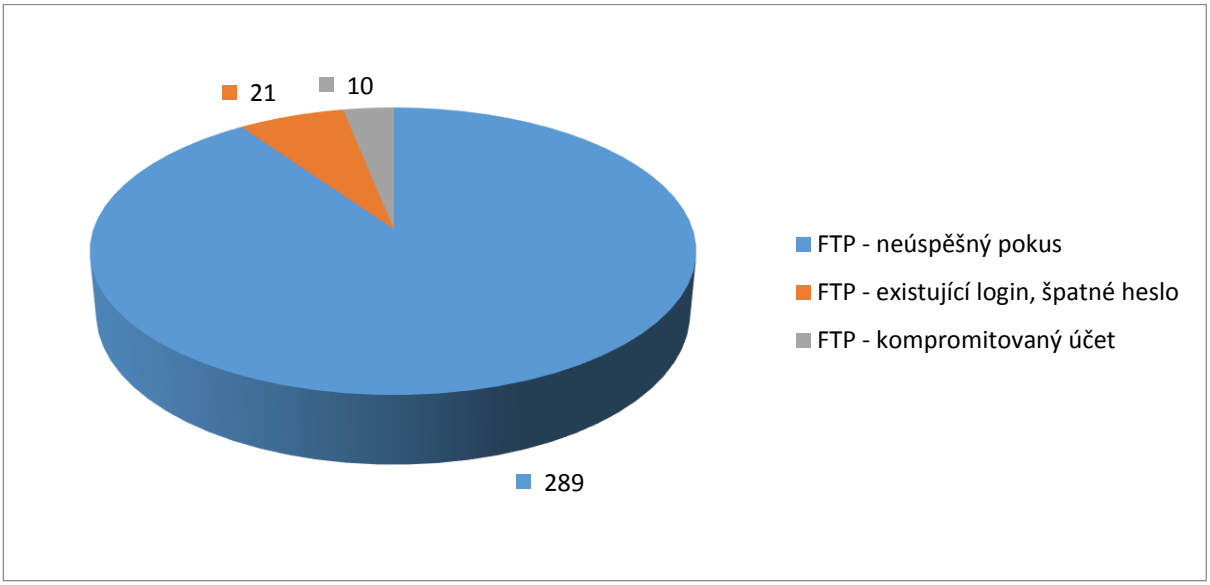
V následující kapitole představíme útoky dle rozdělení na jednotlivé služby a dle zdroje. Jedná se o nejtěžší incidenty, velmi nebezpečné pro každou organizaci.

Na uvedených grafech jsem se zaměřil na služby SSH, FTP a http://webmail přístupných z laboratorní sítě.



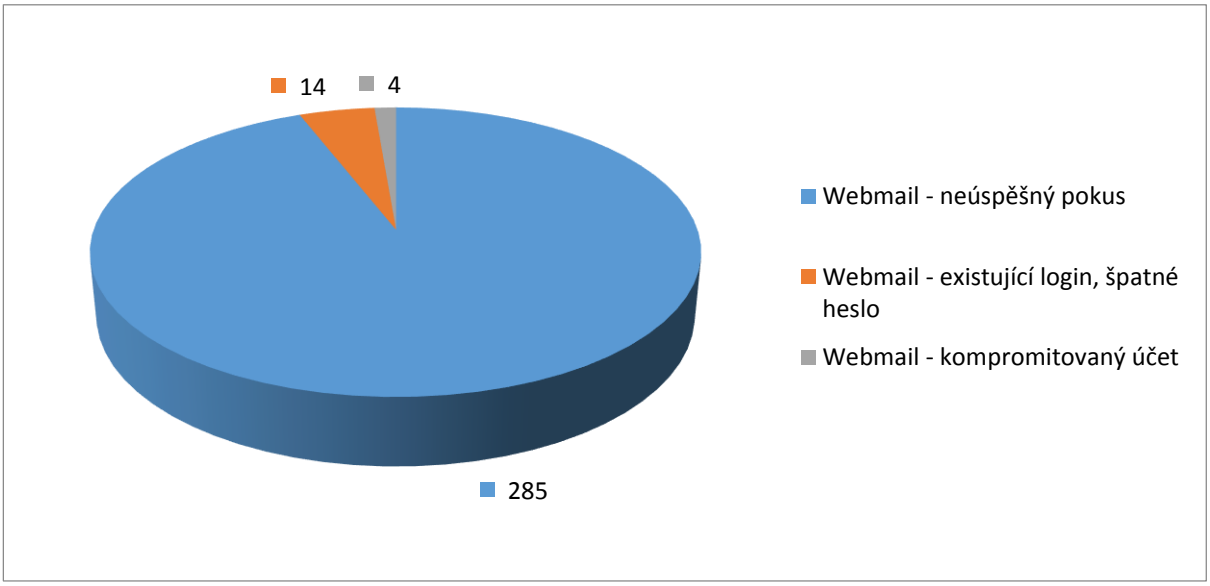
Obr. 11.9: Graf: Útoky z laboratorní sítě na službu SSH

Pokud je ovládnuta služba SSH, ve většině případů se jedná o účet, který je používán správcem systému. Standartní postup je přihlásit se na účet SSH jako normální uživatel, bez zvláštních práv, a následně se z přihlášeného systému přihlásit jako root.



Obr. 11.10: Graf: Útoky z laboratorní sítě na službu FTP

Většina FTP účtů bývá spojována se službami HTTP. Přes FTP účet nahráváme skripty a data do webového uložiště, přístupného dle nastavení webového serveru. Pokud útočníci kompromitují FTP účet, modifikují v datové uložišti nejčastěji soubory typu .php, např. index.php. Do skriptu vloží řádek, který návštěvníka webu přesměruje na infikovanou útočníkovu stránku. Tento řádek bývá zakódován, pro složitější detekci pomocí antivirů.



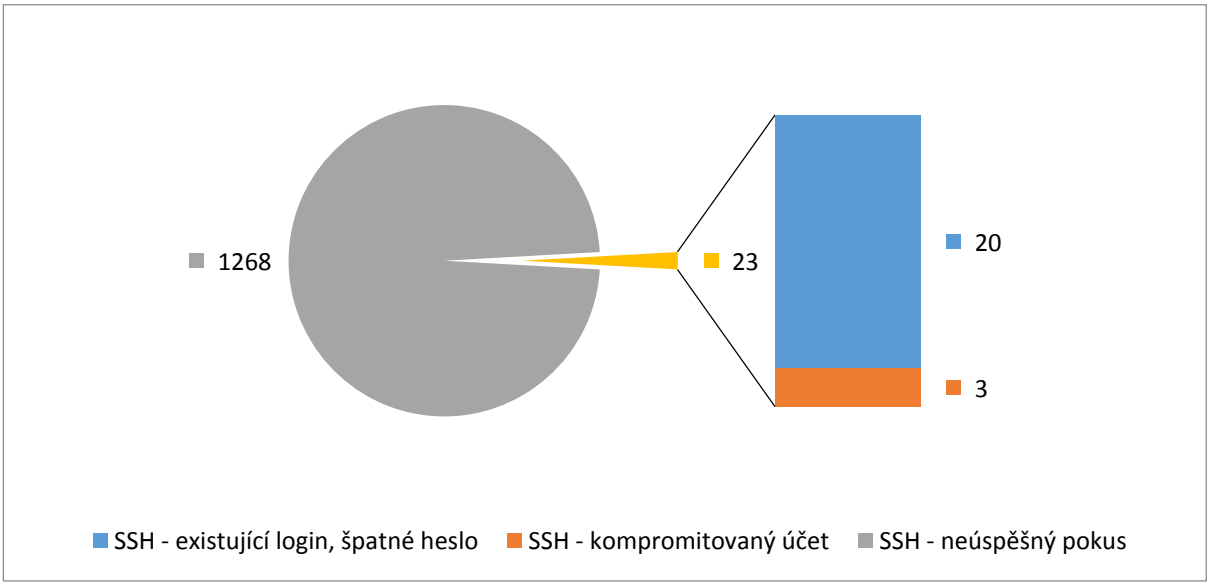
Obr. 11.11: Graf: Útoky z laboratorní sítě na službu Webmail

Služba Webmail slouží k přístupu k poště uživatele z webového rozhraní. Pokud útočník kompromituje uživatelský účet, po přihlášení může z jeho účtu odesílat spamy a zneužít kontakty v adresáři. V první řadě, pokud je to ve Webmailu povoleno, nastaví jiné jméno odesílatele. Detekce je obtížnější, útočníci odesílají spamy po malých skupinách, v náhodnou dobu.

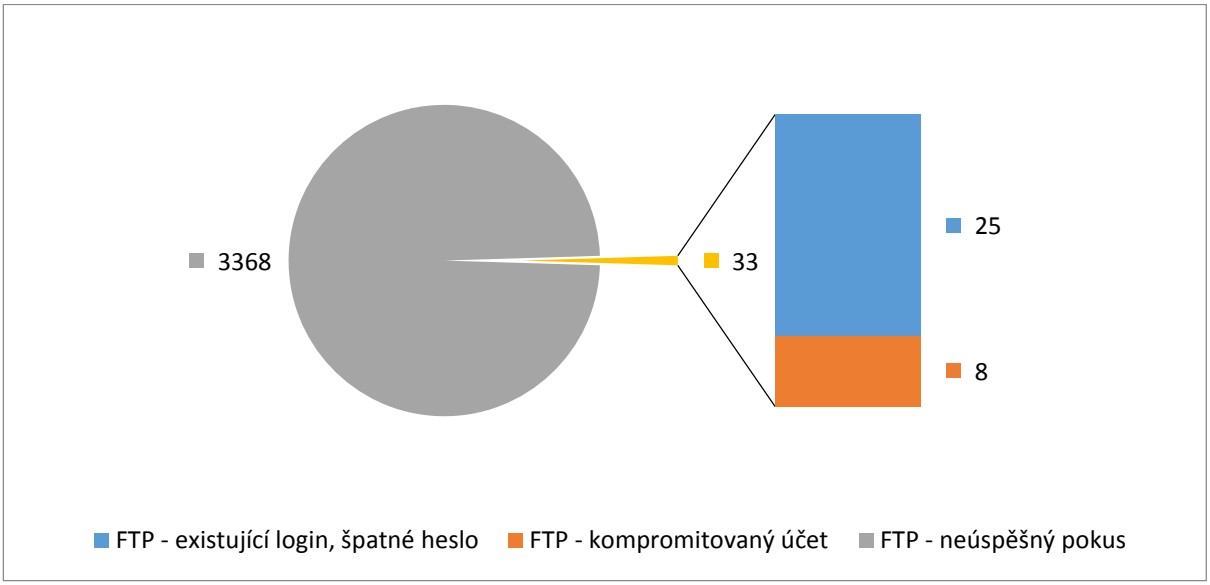
11.10 Pokusy o kompromitaci vybraných služeb z vnější sítě

Na níže uvedených grafech jsou zobrazeny úspěšné a neúspěšné pokusy v rámci experimentu na služby SSH, FTP a ttp://webmail

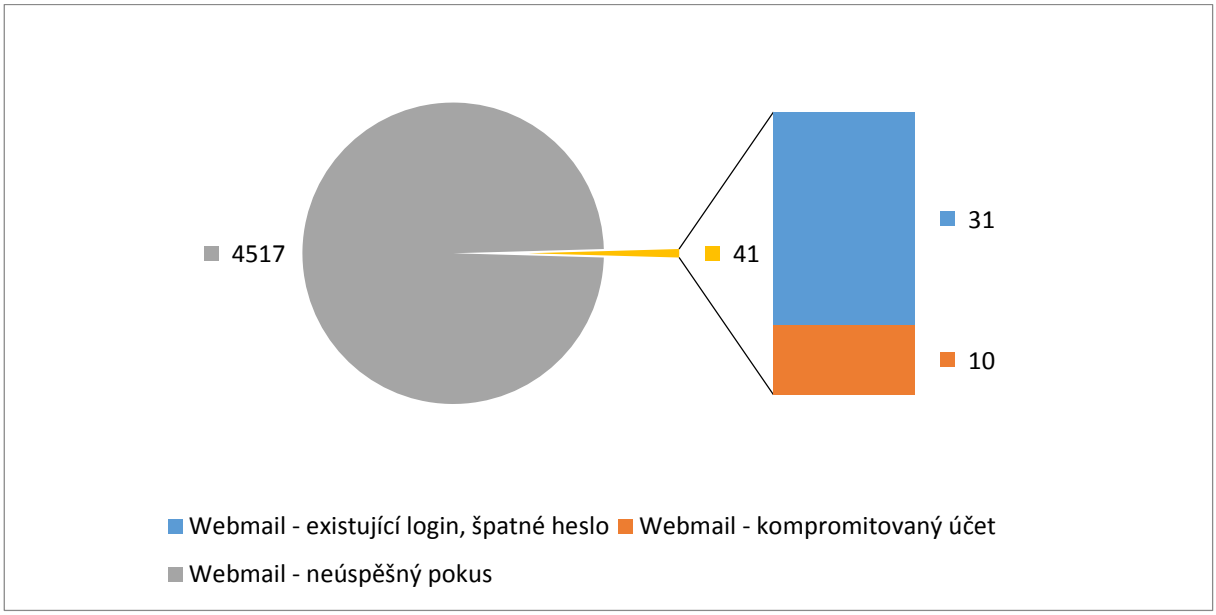
Vysoký počet neúspěšných pokus je způsobený útoky hrubou silou pomocí slovníku. Jelikož jsou tyto typy útoků snadno zjistitelné, útočníci tento postup z vnitřní sítě používají výjimečně.



Obr. 11.12: Graf: Útoky z vnější sítě na službu SSH



Obr. 11.13: Graf: Útoky z vnější sítě na službu FTP



Obr. 11.14: Graf: Útoky z vnější sítě na službu http://webmail

Incidenty označené kompromitovaný účet, nejsou důsledkem prolomení účtu hrubou silou z venkovní sítě, ale zjištěním přihlašovacích údajů na napadených systémech ve vnitřní síti. Tyto útočník shromáždí a odešla na řídící server, který jej pak ve vhodnou dobu zneužije k dalším možnostem útoku.

Tabulka 11-4 Incidenty na vybraných službách vedené z vnější sítě

Incident na službu z vnější sítě	**Neúspěšný pokus**	**Existující login, špatné heslo**	**Kompromitovaný účet**
SSH	1268	20	3
FTP	3368	25	8
Webmail	4517	31	10

Tabulka 11-5 Incidenty na vybraných službách vedené z vnitřní sítě

Incident na službu z laboratorní sítě	**Neúspěšný pokus**	**Existující login, špatné heslo**	**Kompromitovaný účet**
SSH	186	5	4
FTP	289	21	10
Webmail	285	14	4

Při porovnání incidentů v položce neúspěšné pokusy ze zdrojové laboratorní a vnější sítě, lze pozorovat vysoký nárůst neúspěšných pokusů z vnější sítě. Tento rozdíl je způsobený jednodušším vedením útoku z vnější sítě než z vnitřní. Zdroj ve vnitřní síti můžeme snáze detekovat. Zdroj z vnější sítě můžeme zablokovat na firewalech, ale pokud pochází z nějakého segmentu adres, velkého providera, kterého si nemůžeme dovolit blokovat, je pro správce tento postup zbytečný. Můžeme nahlásit zdroj útoku, ale většinou bez efektu.

11.11 Analýza závislostí v kombinační tabulce úspěšnosti detekce

V této části porovnáváme úspěšnost detekce incidentů na systému standartních honeypotů a na honeypotech, které jsou mapovány agentem.

11.12 Test χ^2 kontingenční tabulce

Tento neparametrický test používáme při vyšetřování možné závislosti dvou nominálních proměnných. Výsledky pozorování zapisujeme pro přehlednost do tzv. kontingenční tabulky.

Kontingenční tabulka vznikne, třídíme-li soubor podle variant 2 kvalitativních znaků A a B, kdy A má r variant a B má s variant.

Tabulka 11-6 Schéma kontingenční tabulky

A\B	B_1	B_2	…..	B_s	$\sum_j$
A_1	n_{11}	n_{12}	…..	n_{1s}	$n_{1.}$
A_2	n_{21}	n_{22}	…..	N_{2s}	$n_{2.}$
…..	…..	…..	…..	…..	…..
A_r	n_{2r1}	n_{r2}	…..	n_{rs}	$n_{r.}$
$\sum_i$	$n_{.1}$	$n_{.2}$	…..	$n_{.s}$	n

Nulová hypotéza: A a B jsou nezávislé.

Testové kritérium má tvar:

$$\chi^2 = \sum_{i=1}^{r}\sum_{j=1}^{s}\frac{\left(n_{ij} - n_{ij}^*\right)^2}{n_{ij}^*};$$

(11.1)

kde $n_{ij}^{*} = \frac{n_i - n_j}{n}$ jsou teoretické četnosti.

Kritický obor je vymezen $\chi^2 \geq \chi^2_{1-\alpha}\big((r-1)(s-1)\big)$.

Je-li r=s=2 potom kontingenční tabulka přechází v tzv. čtyřpolní tabulku. [28]

Čtyřpolní tabulka je speciálním případem kontingenční tabulky, kdy měřená data mohou nabývat právě jedné ze dvou kategorií, např. ano/ne.

V případě čtyřpolní tabulky lze, však výpočet χ^2 lze však výpočet zjednodušit použitím vztahu

$$\chi^2 = n.\frac{(ad-bc)^2}{(a+b).(a+c).(b+d).(c+d)} \tag{11.2}$$

Význam písmen ve vzorci je patrný ze schématu čtyřpolní tabulky. Čtyřpolní tabulka má 1 stupeň volnosti, vypočítanou hodnotu χ^2 proto srovnáme s kritickou hodnotou pro 1 stupeň volnosti a zvolenou hladinu významnosti (0,05). [20]

Tabulka 11-7 Schéma čtyřpolní tabulky [20]

	α	non α	
β	a	b	a+b
non β	c	d	c+d
	a+c	b+d	n

11.13 Výpočet pomocí čtyřpolní tabulky

Pro experiment jsme si stanovili hypotézy:

H_0: Úspěšnost systém standartních honeypotů je nezávislá na úspěšnosti systému honeypotů mapovaných agentem.

H_1: Úspěšnost systému honeypotů mapovaných agentem je vyšší.

11.13.1 Vstupní data

Systém standartních honeypotů: 15 honeypotů

Systém honeypotů mapovaných agentem: 5 honeypotů

Bylo testováno 150 sad na systémech standartních honeypotů a na systémech honeypotů mapovaných agentem

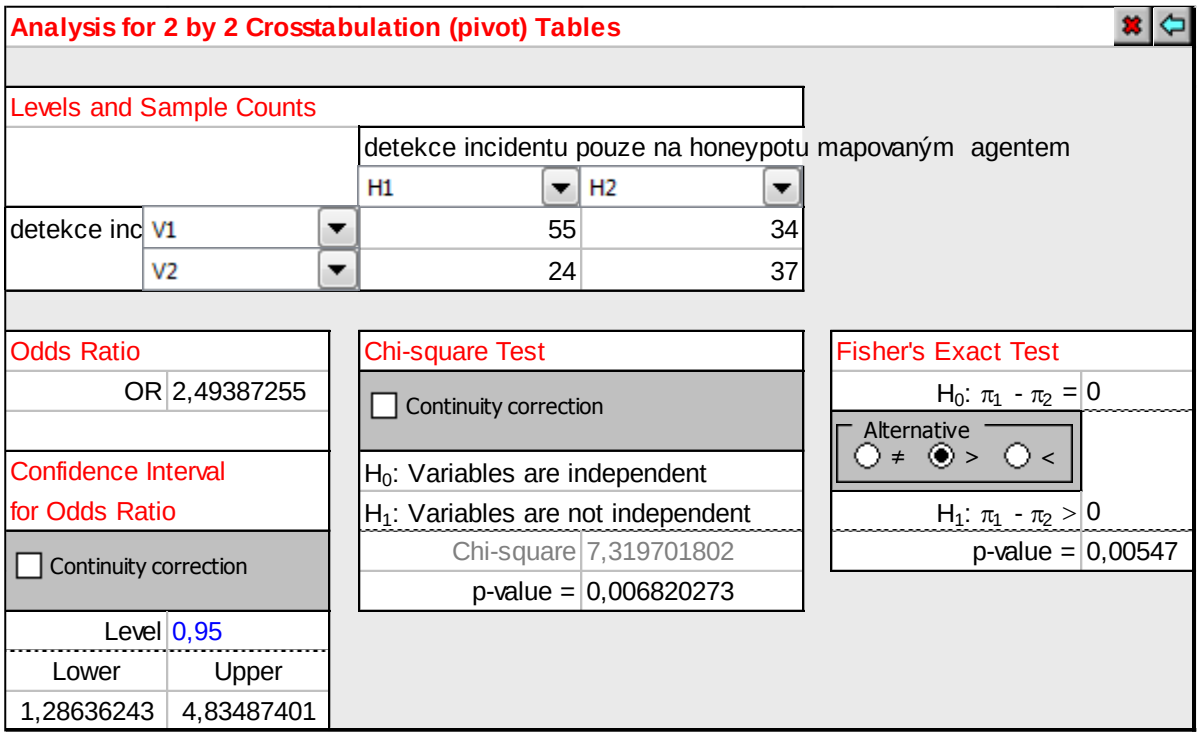
Tabulka 11-8 Tabulka popisu četností a počtu incidentů

Označení četnosti	Popis	Počet incidentů
Četnost 0	nebyl detekován incident ani na jednom typu honeypotu	55
Četnost 1	detekce incidentu pouze na standartním honeypotu	24
Četnost 2	detekce incidentu pouze na honeypotu mapovaným agentem	34
Četnost 3	detekce incidentu na obou tvou typech honeypotů	37

Počet incidentů: Je hodnota kolik honeypotů příslušné skupiny registrovalo nějaký incident.

Tabulka 11-9 Kontingenční tabulka

detekce incidentu pouze na standartním honeypotu	detekce incidentu pouze na honeypotu mapovaným agentem: **Ne**	**Ano**	
Ne	55	34	89
Ano	24	37	61
	79	71	150



Obr. 11.15: Výpočet pomocí programu XLStatistics

11.13.2Výsledek

$\chi^2_{0,05}(0,05) = 7,3197$ – Odmítáme nulovou hypotézu na hladině významnosti 0,05

Platí

H_1: Úspěšnost systému honeypotů mapovaných agentem je vyšší.

Systému honeypotů mapovaných agentem je výrazně vyšší než úspěšnost systém standartních honeypotů.

12 HLAVNÍ VÝSLEDEK PRÁCE

Hlavním cílem disertační práce bylo navrhnout inovativní, efektivní a přínosné metody detekce on-line hrozeb ve virtuálním prostředí respektující současný vývoj jak v hrozbách, tak v bezpečnosti IT zaměřených na podnikové sítě.

K naplnění hlavního cíle bylo nutné uskutečnit následující dílčí cíle:

- Vymezení pojmů z informační bezpečnosti a detekce útoků.

Uvedeno v teoretické části disertační práce. Zaměřil jsem se na základní pojmy z oblasti bezpečnostních řešení a základní pojmy z oblasti bezpečnostních incidentů.

- Přístupy a koncepty detekce hrozeb, včetně jejich silných a slabých stránek.

V úvodních kapitolách Základní typy bezpečnostních řešení a Detekce anomálií je uveden základní přehled klasifikace systémů detekce narušení bezpečnosti. Jsou zde popsány základními pojmy z metodologie: detekci anomálií a základní mechanismy detekce anomálií. Dále jsou zde vyjmenovány jejich silné a slabé stránky

- Definování postupů a způsobů detekce, kterými lze efektivně zvýšit zabezpečení těchto systémů.

Bylo zvoleno řešení na systému detekce pomocí honeypotů. V teoretické části jsou uvedeny základní parametry a možnosti rozšíření. V experimentální části je uveden popis řešení a realizace provedena v kapitole Realizace experimentu.

- Identifikovat klíčové faktory ovlivňující bezpečnost ve virtuálním prostředí.

Teoretické části jsou uvedeny hlavní faktory ohrožující počítačové systémy. Je zde popsána metodika incidentů a určeny její slabé místa, kde je možné incident detekovat. Hlavním klíčovým faktorem jsou přístupové údaje do systémů.

- Možnosti inovace a rozšíření na již realizovaných systémech detekce

Disertační práce rozšiřuje možnosti systému honeypotů. Byly implementovány další funkce pro zvýšení efektivity zvoleného řešení. Následně byla porovnána efektivita původního systému se systémem, který byl rozšířen o nové funkce.

- Realizace zpracování detekce online hrozeb za účelem nalezení vhodných postupů a nástrojů využitelných v oblasti zabezpečení informačních systémů.

Vytvoření systému detekce pomocí honeypotů, byla realizována vhodnými dostupnými nástroji. Dále bylo nutno provést jejich modifikace a doprogramovat vhodné propojení. Na zvoleném systému pak byly ověřeny vhodné postupy pro efektivní nasazení. Hlavními novými prvky jsou:

- Koncept systému

Pojetí celého systému honeypotů, se liší od dosud zveřejněných systémů. Bylo vyvíjeno a přizpůsobována aktuálním podmínkám. Z původního hlavního cíle, zkoumat a rozebírat jednotlivé incidenty, bylo změněno určení, na detekci incidentů a detekci kompromitovaných uživatelských účtů. To znamená, že z původního studijního účelu se systém transformoval na produkční systém, určený k praktickým úkolům.

- Rozšíření Agent

Modifikace standartní verze honeypotů, je implementace dalšího prvku, který vylepší možnosti detekce incidentu. V disertační práci jej nazýváme Agent. Tento prvek nasazený ve vybraném uživatelském systému implementuje nadbytečné informace, které nejsou zajímavé pro uživatele. Ale pokud je systém kompromitován, útočník nedovede rozlišit, zda se jedná o nadbytečné informace. Pokud jej použije v další fázi, je vysoce pravděpodobné, že bude detekován pomocí systému honeypotů. V laboratorních podmínkách bylo prokázáno, že Agent zvyšuje efektivitu detekce incidentu.

- Analyzovat možnosti aplikace navrženého systému a vyhodnocení experimentů na vybraných systémech v laboratorních podmínkách na aktuálních hrozbách.

Byla vytvořena virtuální experimentální laboratoř, v níž byl implementován systém honeypotů. Byly stanoveny hypotézy a následně statisticky vyhodnoceny. Vyhodnocení experimentu se nachází v předcházející kapitole,

13 PŘÍNOS PRÁCE PRO VĚDU A PRAXI

Cílem této disertační práce je zvýšení bezpečnosti v informačních systémech a předcházení útokům, jejž by ohrožovaly stávající systémy. Firmám a organizacím tento systém snižuje finanční náklady a zvýšit účinnost zabečení jejich systémů. Hlavním výsledkem je vytvoření systému detekce na principu honeypotů. Bylo implementováno rozšíření stávajících systémů detekce na principu honeypotů a následně laboratorně ověřeno na aktuálních hrozbách.

13.1 Přínos pro vědu

Navržený systém detekce on-line hrozeb ve virtuálním prostředí pomocí systému senzorů, nabízí široké možnosti uplatnění v oblasti počítačové bezpečnosti. Výzkum provedený při zpracování disertační práce se zaměřuje na možnosti využití honeypotů v oblasti detekce hrozeb a jeho účinné nasazení. Přínos pro teorii spočívá v návrhu metodiky systému detekce pomocí honeypotů a zvýšení efektivity systému detekce pomocí rozšíření Agent. Vhodnou kombinací zvolených detekčních metod se otvírají nové možnosti, přenést tento systém z teoretické roviny do praxe.

13.2 Návrh řešení pro praxi

Přínosem pro praxi je vytvoření komplexního sytému na detekci incidentů, jenž řeší stávající a budoucí hrozby ve virtuálním prostředí. Tento systém jde jednoduše modifikovat a rozšířit jak do mobilních aplikací, tak směrem ke cloudovým a řešením.

13.3 Implementace honeypotů v praxi

Tento systém dle předchozí metodiky je implementován jako služba ve dvou organizacích. První implementace byla provedena v roce 2008, a za tu dobu se hodně vyvíjela dle zaměření hrozeb. V této disertační práci byly použity a vylepšeny metody a softwarové nástroje vycházejí z praktického nasazení. Systém detekce incidentu pomocí honeypotů usnadňuje řešit vzniklé bezpečnostní incidenty a upozorňuje na konkrétní aktuální nedostatky v provozu počítačových systémů. Pokud se incident podaří detekovat včas, šetří to i finanční prostředky, které byly vynaloženy na jeho odstranění.

ZÁVĚR

Detekce hrozeb je trvalý trend a zároveň nutnou součástí každého informačního systému. Proto jsem si také vybral tuto problematiku k řešení. Ačkoliv vývoj v této oblasti je uspokojivý a bylo dosaženo hodnotných cílů, tyto systémy nejsou a nemohou být dokonalé. Existuje velké množství nových možností, nové postupy a přístupy ke zdokonalení těchto metod. Nepřestávají se objevovat nové případy hrozeb, které nejsou jednoduše detekovány a nové možnosti obcházení těchto metod detekce související s vývojem technologií. Současný stav této problematiky je velmi dynamický.

V této disertační práci na téma „Metody detekce on-line hrozeb ve virtuálním prostředí“ jsem se snažil nastínit složitou problematiku detekce hrozeb ve virtuálním prostředí a zhodnotit popsané metody. Toto velké množství technik detekce míří k rozmanitému testování různých systémů na detekci hrozeb, k novým návrhům na vylepšení těchto systémů a na optimalizaci bezpečnostních postupů.

Cílem této disertační práce je zmenšení nebezpečí a omezení vybraných rizik, které hrozí počítačovým systémům ve virtuálním prostředí, a navržení vhodného řešení této problematiky. Hlavní část této práce je zaměřena na využití systémů detekce k vyhledávání aktuálních hrozeb. Aktuální systémy detekce již spolehlivě detekují většinu incidentů, ale jsou většinou neúčinné proti cíleným útokům na konkrétní počítačové systémy. V úvodní části se práce zabývá komplexním rozdělením bezpečnostních řešení, jejich rozdělením a přístupem k detekci hrozeb. Jsou zde popsány jejich výhody a nevýhody. Dále se zabýváme detekcí incidentů za využití systému honeypotů. Následně se zaměřuje na hrozby, které se snažíme detekovat. Je zde popsána metodika incidentů. Jsou zde definována její slabá místa, kde můžeme uplatit systém detekce za využití honeypotů.

V další části je navržen systém detekce incidentů pomocí honeypotů. Původní teoretický koncept je přepracován na aktuální situace a rozšířen o nové možnosti. Z původního hlavního cíle, zkoumat a rozebírat jednotlivé incidenty, bylo změněno určení, na detekci incidentů a detekci kompromitovaných uživatelských účtů. To znamená, že z původního studijního účelu se systém transformoval na produkční systém určený k praktickým úkolům. Dále bylo použito rozšíření Agent, které zvyšuji úroveň detekce incidentů.

Následně byla sestavena experimentální laboratoř, kde byl implementován navržený způsob detekce. Experiment byl proveden na aktuálních hrozbách a bylo prokázáno, že rozšíření Agent zvyšuje efektivitu detekce incidentu.

Hlavní přínos práce lze spatřovat v systému detekce incidentů, pomocí honeypotů. Tento systém je schopen detekovat jak aktuální, tak neznámé typy hrozeb. Z dlouhodobého hlediska je to silný nástroj na bezpečnost ve virtuálním prostředí a vynikající pomůcka k podrobnějšímu studiu bezpečnostních incidentů. Vhodnou kombinací zvolených detekčních metod se otvírají nové možnosti, přenést

tento koncept z teoretické roviny do praxe. Nasazením tohoto řešení v praxi, zvýší zabezpečení počítačových systémů a sníží prostředky na řešení případných incidentů. Domnívám se, že disertační práce na toto aktuální téma je v mnohém přínosná a inspirativní nejen pro mě osobně, ale také pro kolegy zabývající se informační bezpečností.

SEZNAM POUŽITÉ LITERATURY

[1] ABBASI, F.H. a R.J. HARRIS, 2009. Experiences with a Generation III virtual Honeynet. 2009, s. 6.

[2] ADAM, Christian SEIFERT a Shaun VLASHEF. *Network Sinkhole* [online]. 2006-2013 [cit. 2013-10-23]. Dostupné z: https://redmine.honeynet.org/projects/sinkhole

[3] ALPEROVITCH, Dmitri. Operation Shady RAT. *Blog Ventral* [online]. 2012. [cit. 2013-10-07]. Dostupné z: http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat

[4] *Amun: Python Honeypot* [online]. 2012. vyd. [cit. 2013-10-09]. Dostupné z: http://amunhoney.sourceforge.net/

[5] BACHER, P., T. HOLZ, M. KOTTER a G. WICHERSKI. Know Your Enemy: Tracking Botnets. [online]. [cit. 2013-10-08]. Dostupné z: http://www.honeynet.org/papers/bots

[6] BARTEL, Petr. Analýza dat získaných honeynety. 2009.

[7] BOUŠKA, Petr. VLAN - Virtual Local Area Network. PRANGE, Gordon W a DILLON. *SAMURAJ-cz.com* [online]. [cit. 2013-10-08]. Dostupné z: http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

[8] BODÓ, Radoslav a Michal KOSTĚNEC. Experiences with IDS and Honeypots: Best Practice Document. 2012, s. 48. Dostupné z: http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-cbpd135.pdf

[9] COHEN, Fred. *Deception ToolKit* [online]. [cit. 2013-10-23]. Dostupné z: http://www.all.net/dtk/

[10] COMMAND FIVE PTY LTD. Advanced Persistent Threats: A Decade in Review. [online]. 2011, s. 13 [cit. 2013-09-11]. Dostupné z: http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf

[11] COMMAND FIVE PTY. Command and Control in the Fifth Domain. 2012, s. 30.

[12] DAMBALLA. Advanced Persistent Threats (APT): What's an APT? A Brief Definition. DAMBALLA. [online]. 2010 [cit. 2013-09-11]. Dostupné z: https://www.damballa.com/knowledge/advanced-persistent-threats.php

[13] DELL. Anatomy of a cyber-attack. 2012. Dostupné z: http://www.sonicwall.com/downloads/EB_Anatomy_of_a_CyberAttack_Final.pdf

[14] DELL SECUREWORKS. Lifecycle of the Advanced Persistent Threat. [online]. 2012, s. 16 [cit. 2013-09-11]. Dostupné z: http://go.secureworks.com/advancedthreats

[15] *Dionae - catches bugs* [online]. 2012. vyd. [cit. 2013-10-09]. Dostupné z: http://dionaea.carnivore.it/

[16] ENDORF, Carl. *Detekce a prevence počítačového útoku*. 1. vyd. Praha: Grada, 2005, 355 s. ISBN 80-247-1035-8.

[17] ESET. *ESET - Antivirus | spolehlivá ochrana počítače a dalších zařízení :: O nás :: ESET Technologie* [online]. 2013 [cit. 2013-09-13]. Dostupné z: http://www.eset.com/cz/firmy/proc-eset/technologie/

[18] GÓMEZ, Diego González. Installing a virtual honeywall using vmware. *Spanish Honeynet Project*, 2004.

[19] HOLZ, T. a F. RAYNAL. *Detecting honeypots and other suspicious environments*. ISBN 0-7803-9290-6. DOI: 10.1109/IAW.2005.1495930.

[20] CHRÁSKA, Miroslav. *Metody pedagogického výzkumu: základy kvantitativního výzkumu*. Vydání 1. Praha: Grada Publishing, 2007, 265 s. ISBN 978-80-247-1369-4.

[21] CHANDOLA, Varun, Arindam BANERJEE a Vipin KUMAR. Anomaly Detection : A Survey. [online]. 2007, s. 74 [cit. 2013-10-07]. Dostupné z: http://www.cs.umn.edu/tech_reports_upload/tr2007/07-017.pdf

[22] CHECK POINT SOFTWARE TECHNOLOGIES, Inc. *OPSEC: Open Platform for Security* [online]. 2013 [cit. 2013-10-23].

[23] CHESWICK, Bill. An Evening with Berferd in which a cracker is Lured, Endured, and Studied. In: Proc. Winter USENIX Conference, San Francisco. 1992.

[24] INFOBLOX. How a DNS Firewall Helps in the Battle against Advanced Persistent Threat and Similar Malware. 2013, s. 7.

[25] JONES, A.K. a SIELKEN, R.S. Computer system intrusion detection: a survey. In *Intrusion Detection Research* [online]. Charlottesville : University of Virginia, 9.2.2000 [cit. 2013-09-08]. Dostupné z WWW: http://www.cs.virginia.edu/~jones/IDS-research/Documents/jones-sielken-survey-v11.pdf.

[26] KASPERSKY LAB. Global Corporate IT Security Risks : 2013. *Kaspersky Lab* [online]. 2013, s. 26 [cit. 2013-10-07]. Dostupné z: http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf

[27] KAZIENKO, Przemyslaw a Piotr DOROSZ. Intrusion Detection Systems (IDS) Part 2 - Classification; methods; techniques. In: *WindowSecurity.com* [online]. 2004 [cit. 2013-10-07]. Dostupné z: http://www.windowsecurity.com/articles-tutorials/intrusion_detection/IDS-Part2-Classification-methods-techniques.html

[28] KLÍMEK, Petr a Martin KOVÁŘÍK. *Aplikovaná statistika v programu XLStatistics*. 1. vyd. Bučovice: Martin Stříž, 2009, 164 s. ISBN 978-80-87106-24-2.

[29] *Know your enemy: learning about security threats*. 2nd ed. Boston: Addison-Wesley, c2004, xxix, 768 p. ISBN 03-211-6646-9.

[30] LEWIS, Nick. The updated Makadocs malware: How to protect users locally. TECHTARGET. *TechTarget* [online]. 2013 [cit. 2013-10-10]. Dostupné z: http://searchsecurity.techtarget.com/answer/The-updated-Makadocs-malware-How-to-protect-users-locally?asrc=EM_ERU_24041181&utm_medium=EM&utm_source=ERU&utm_campaign=20131010_ERU%20Transmission%20for%2010/10/2013%20(UserUniverse:%20578602)_myka-reports@techtarget.com&src=5171436

[31] LUMENSION. Preventing Weaponized Malware Payloads in Advanced Persistent Threats: Strategies for Layered Endpoint Defense Against the APT Kill Chain. 2012, s. 13.

[32] LYON, Gordon Fyodor. *Nmap network scanning: official Nmap project guide to network discovery and security scanning*. 1st ed. Sunnyvale, CA: Insecure.Com, LLC, c2008, xxix, 434 p. ISBN 09-799-5871-7

[33] MACHÁLEK, Jiří. Honeynet: útoky na přelomu roku. *Blog sdružení CZ.NIC* [online]. 2013 [cit. 2013-10-23]. Dostupné z: http://blog.nic.cz/2013/02/19/honeynet-utoky-na-prelomu-roku/

[34] MANDIANT. APT1 Exposing One of China's Cyber Espionage Units. [online]. 2013, s. 74 [cit. 2013-09-11]. Dostupné z: http://www.mandiant.com

[35] MICHAL, Jindřich. Historie počítačových virů. [online]. 2001. vyd. [cit. 2013-10-07]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2001/xmichal1.htm

[36] NAGARAJAN, Ajay, Quyen NGUYEN, Robert BANKS a Arun SOOD. Combining Intrusion Detection and Recovery for Enhancing System Dependability. 2012, s. 6.

[37] NAGARAJAN, Ajay a Arun SOOD. SCIT and IDS Architectures for Reduced Data Ex - filtration. 2010, s. 6.

[38] NITHIN CHANDRA, S.R a T.M MADHURI. Cloud Security using Honeypot Systems. 2012. Dostupné z: http://www.ijser.org/researchpaper/Cloud-Security-using-Honeypot-Systems.pdf

[39] NEWMAN, Robert C. *Computer security: protecting digital resources*. Sudbury: Jones and Bartlett Publishers, c2010, xxviii, 453 s. ISBN 978-0-7637-5994-0.

[40] OPENVPN TECHNOLOGIES, Inc. *OpenVPN - Open Source VPN* [online]. 2013 [cit. 2013-10-10].

[41] PROVOS, Niels. *Developments of the Honeyd Virtual Honeypot* [online]. 1999-2004 [cit. 2013-10-23]. Dostupné z: http://www.honeyd.org

[42] PROVOS, Niels a Thorsten HOLZ. *Virtual honeypots: from botnet tracking to intrusion dedction*. Upper Saddle River: Addison-Wesley, 2008, xxiii, 440 s. ISBN 978-0-321-33632-3.

[43] RAYNAL, F., Y. BERTHIER, P. BIONDI a D. KAMINSKY. *Honeypot forensics: workshop papers : June 10-11, 2004, West Point, New York*. Piscataway, N.J.: IEEE, c2003. ISBN 0780385721. DOI: 10.1109/IAW.2004.1437793.

[44] RIST, Lukas. *Glastopf Project* [online]. 2012 [cit. 2013-10-23]. Dostupné z: http://glastopf.org/

[45] SCARFONE, Karen; MELL, Peter. Guide to Intrusion Detection and Prevention Systems (IDPS) : Recommendations of the National Institute of Standards and Technology [online]. Gaithersburg : National Institute of Standards and Technology, 2007 [cit. 2013-07-30]. Dostupné z WWW: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[46] SCHNEIER, Bruce. *Advanced Persistent Threat (APT)* [online]. 2011 [cit. 2013-10-08]. Dostupné z: https://www.schneier.com/blog/archives/2011/11/advanced_persis.html

[47] SOURCEFIRE. *Snort* [online]. 2010 [cit. 2013-10-10]. Dostupné z: http://www.snort.org/

[48] SPITZNER, Lance. *Honeypots tracking hackers*. Boston: Addison-Wesley, 2003, xxvi, 452 s. ISBN 03-211-0895-7.

[49] SPITZNER, Lance. Honeypots: Definitions and Value of Honeypots. *Virtual honeypots: from botnet tracking to intrusion dedction* [online]. Upper Saddle River: Addison-Wesley, 2008 [cit. 2013-09-11].

[50] STOLL, Cliff. *The cuckoo's egg: tracking a spy through the maze of computer espionage*. New York: Pocket Books, 2005. ISBN 14-165-0778-7.

[51] *SURFcert IDS* [online]. 2012 [cit. 2013-10-08]. Dostupné z: http://ids.surfnet.nl/wiki/doku.php

[52] THE HONEYNET PROJECT. *The Honeynet Project* [online]. 2013 [cit. 2013-10-23]. Dostupné z: http://www.honeynet.org/

[53] THE PROFTPD PROJECT. *The ProFTPD Project* [online]. 1999 - 2013 [cit. 2013-10-23]. Dostupné z: http://www.proftpd.org/

[54] THE SQUIRRELMAIL PROJECT TEAM. *SquirrelMail - Webmail for Nuts!* [online]. 1999-2010 [cit. 2013-10-23]. Dostupné z: http://squirrelmail.org/

[55] TREND MICRO. Targeted Attack Entry Points: Are Your Business Communications Secure?. [online]. 2012, s. 5 [cit. 2013-09-11].

[56] UNSPAM TECHNOLOGIES, Inc. *Project Honey Pot: The Web's Largest Community Tracking Online Fraud & Abuse* [online]. 2004–13 [cit. 2013-10-23]. Dostupné z: https://www.projecthoneypot.org/

[57] VERIZONE. 2013 Data Breach Investigations Report. 2013, s. 63. Dostupné z: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

[58] VRABLE, Michael. Scalability, fidelity, and containment in the potemkin virtual honeyfarm. *ACM SIGOPS Operating Systems Review*. 2005, roč. 39, č. 5.

[59] WEAVER, Nicholas; PAXSON, Vern; STANIFORD, Stuart. Wormholes and a honeyfarm: Automatically detecting novel worms. *DIMACS Large Scale Attacks Workshop*, 2003.

[60] WENKE Lee, Cliff Wang and David Dagon. *Botnet detection countering the largest security threat*. Online-Ausg. New York: Springer, 2007. ISBN 978-038-7687-681.

[61] WICHERSKI, Georg. *Oxff's Blog* [online]. 2012 [cit. 2013-10-23]. Dostupné z: http://blog.oxff.net/#anvszwpmjdyizhsqgngq

[62] ZALEWSKI, Michal. *P0f v3* [online]. 2012 [cit. 2013-10-09]. Dostupné z: http://lcamtuf.coredump.cx/p0f3/

SEZNAM PUBLIKACÍ AUTORA

VÝMOLA, Tomáš. *Konverze textových souborů*, Bakalářská práce, Masarykova Universita – Fakulta informatiky, Brno, 2002, vedoucí bakalářské práce doc. Ing. Jiří Sochor, CSc.

VÝMOLA, Tomáš. *Projekt řešení vybraných bezpečnostních rizik serverů organizace*, Diplomová práce, Univerzita Tomáše Bati ve Zlíně – Fakulta aplikované informatiky, Zlín, 2007, 89 s., vedoucí diplomové práce doc. Mgr. Roman Jašek, Ph.D.

ŠKODÁKOVÁ, Petra, PAVELKOVÁ Drahomíra a Tomáš VÝMOLA, T. *ICT application for benchmarking of financial performance of clusters.* Center for in Vestigations into Information Systems (CVIS) [online]. 2008 [cit. 01-12-2008]. ISSN 1214-9489.

VÝMOLA, Tomáš. *Detekce hrozeb pomocí systémů honeypotů*, Informační a datová bezpečnost ve vazbě na strategické rozhodování ve znalostní společnosti Zlín, 24. – 25. 3. 2009, [1. vyd.]. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. ISBN-ISSN 80-238-6782-7.

VÝMOLA, Tomáš. *BEZPEČNOSTNÍ HROZBY BOTNETŮ*, Internet, bezpečnost a konkurenceschopnost organizací, Zlín, 17. – 18. 3. 2010, [1. vyd.]. Zlín : Univerzita Tomáše Bati ve Zlíně, 2010. 496 s. ISBN-ISSN 978-83-61645-16-0.

VÝMOLA, Tomáš. *Tolerantní přístup k obraně ve virtuálním prostředí*, Internet, bezpečnost a konkurenceschopnost organizací, Zlín, 16. – 17. 3. 2011, [1. vyd.]. Zlín : Univerzita Tomáše Bati ve Zlíně, 2011. ISBN-ISSN 978-80-7454-012-7 CD-ROM.

JAROŠ, Jiří a Tomáš VÝMOLA. *Řešení krizových situací v případě ddos útoku,* International Conference of Crisis Management in Public and Private Sector, Uherské Hradiště, 23. – 24. 6. 2011, [1. vyd.]. Zlín : Univerzita Tomáše Bati ve Zlíně, 2011. ISBN-ISSN 978-83-7454-027-1 CD-ROM.

VÝMOLA, Tomáš. *Detection Of Security Incidents In The Server Log Using Neural Network.* In: *INTERNET, COMPETITIVENESS AND ORGANIZATIONAL SECURITY: Process Management and the Use of Modern Technologies Zlín,*. Zlín: Tomas Bata University in Zlín, Faculty of Applied Informatics, 2012. ISBN 978-80-7454-142-1.

JAŠEK, Roman, Martin KOLAŘÍK a Tomáš VÝMOLA. *APT Detection System using Honeypots*. In: RECENT ADVANCES in AUTOMATIC CONTROL, INFORMATION and COMMUNICATIONS. 2013. vyd. Valencia, Spain: WSEAS Press, 2013. ISBN 978-960-474-316-2ISSN 1790-5117.

CV AUTORA

Jméno a příjmení:	Ing. Tomáš Výmola
Datum narození:	26. 8. 1977
Bydliště:	Stará Cesta 507, 763 14 Zlín-Štípa (Česká republika)
E-mail:	vymola@fame.utb.cz

Dosažené vzdělání:

1996 – 2002	Masarykova univerzita, Fakulta informatiky; obor Informatika, bakalářské studium
2006 – 2008	Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky; obor Inženýrská informatika, magisterské studium
2008 – dosud	Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky; obor Inženýrská informatika, doktorské studium

Pracovní zkušenosti:

1.2.1999 – 30. 09. 2002	Avex Computer Systems – správa systémů, programátor
1. 10. 2002 – 28. 2. 2004	Univerzita Tomáše Bati ve Zlíně, Fakulta managementu a ekonomiky – civilní služba
1. 3. 2004 – dosud	Univerzita Tomáše Bati ve Zlíně, Fakulta managementu a ekonomiky – Správce sítě a WWW stránek FAME

Jazykové znalosti:

Angličtina:	středně pokročilý
Ruština:	začátečník

2009 – Jazykový kurz CL English Language School Brighton

Další znalosti a dovednosti:

- Programování:
  - Profesionální: PHP, HTML
  - Střední: PERL, C, C++, Visual Basic, Delphi
  - Základní: Oracle, Java, .Net

- Databáze:
    - Profesionální: MySQL
    - Střední: MSSQL
    - Základní: Oracle
- Datové modelování
- Správa sítí
- Operační systémy: Windows, Linux
- Administrace systémů: Novell, VmWare, ARIS, Lotus, Microsoft Exchange, Navision, Palstat, Witness, Plant Simulation, Jack, IS SAFIR

Spolupráce na projektech:

- „RIUS - ROZBĚH INTERUNIVERZITNÍHO STUDIA V SÍTI VYBRANÝCH UNIVERZIT“, ČR - CZ.04.1.03/3.2.15.1/0067
- „EVENE - Erasmus Virtual Economics & Management Studies Exchange, eLearning program, Agreement Number“ - 2005 - 3837 / 001 - 001 ELE-ELEB127
- „Inovace předmětů zaměřených na finanční řízení podniku s důrazem na aplikaci praktických postupů, poznatků a nástrojů“, ESF OP VK CZ.1.07/2.2.00/07.0358
- „Vzdělávání v oblasti účetnictví a daní“, ESF OP VK CZ.1.07/2.2.00/07.0050
- „CreaClust - Přeshraniční klastrová iniciativa pro rozvoj kreativního průmyslu“ – 22410420020
- „Merlingo - MEdia-rich Repository of Learning Objects“
- Integrovaná strategická koncepce pro řízení zdravotnictví a rozvoj zdravotnických služeb ve Zlínském kraji, Zlínský kraj
- „KLIN - Inovace klíčových předmětů bakalářských a magisterských studijních programů na FAME UTB ve Zlíně“ – CZ.1.07/2.2.00/15.0104
- „SVI - Štíhlá výroba a inovace“ – CZ.1.07/2.4.00/31.0096