Acta Informatica Pragensia
2(1), 2013, 39–56, DOI: 10.18267/j.aip.12
Online: aip.vse.cz

Sekce / Section:
Recenzované stati / Peer-reviewed papers

Vplyv sofistikovaného hybridného Honeypotu na efektivitu architektúry systému detekcie prieniku v distribuovaných počítačových systémoch

Peter Fanfara[1], Martin Chovanec[2]

[1] Katedra počítačov a informatiky, Fakulta elektrotechniky a informatiky
Technická univerzita v Košiciach, Letná 9, 04001 Košice, Slovenská republika
[2] Ústav Výpočtovej Techniky, Technická univerzita v Košiciach
Boženy Němcovej 3, 04001 Košice, Slovenská republika

{peter.fanfara, martin.chovanec}@tuke.sk

Abstrakt: Pri súčasnom vývoji technológií, rapídnom raste počítačových sietí a distribuovaných systémov, je reálne riziko útoku čoraz pravdepodobnejšie. Pre zvýšenie samotnej bezpečnosti systémov už bolo vytvorených a implementovaných množstvo riešení, ktoré mali slúžiť na detekciu a/alebo prevenciu pred samotnými útokmi. Najpoužívanejšie riešenie predstavuje použitie systému na detekciu prieniku (IDS) v kooperácii s firewallom. Avšak ani IDS a ani firewall nedokážu reagovať v reálnom čase, pokiaľ sa jedná o špecifický typ útoku. Táto práca sa zaoberá detekčným mechanizmom na báze technológie Honeypot a jeho využitím v navrhovanej architektúre pre zvýšenie bezpečnosti v počítačových systémoch. Podstatou práce je poukázať na to, ako dokáže sofistikovaný hybridný Honeypot vplývať na dizajn architektúry IDS a tým zvýšiť jej efektivitu.

Klíčová slova: bezpečnosť počítačových systémov, honeypot, systém detekcie prienikov, škodlivý kód

Title: Influence of Sophisticated Hybrid Honeypot on Efficiency of Intrusion Detection System Architecture in Distributed Computer Systems

Abstract: In the current development of technologies, rapid growth of computer networks and distributed systems still exist a very probable risk of attack. There have been developed and implemented a number of solutions to help in detecting and/or preventing attacks and to improve the actual system security. The most common solution is to use Intrusion Detection System (IDS) in cooperation with the firewall. Neither the IDS nor firewall can respond in real time to a specific type of attack. This paper deals with the detection mechanism based on Honeypot technology and its use in the proposed architecture to improve security of computer systems. The essence of the work is to show how can sophisticated hybrid Honeypot influence the design of IDS architecture and thus increase its efficiency.

Keywords: Intrusion Detection System (IDS), Honeypot, Malicious code, Security

1 ÚVOD

Vzhľadom k rýchlemu šíreniu internetu a webových technológií môžu ľudia ľahko a jednoducho vyhľadávať informácie a zároveň rýchlo posielať správy. Avšak, ak nebudeme súčasne klásť dostatočne veľký dôraz, adekvátny rýchlemu rozvoju internetu, na základné zabezpečenie systémov, hackeri môžu poľahky ovládnuť zabezpečenie systému použitím škodlivého kódu, využitím existujúcich zraniteľností systému alebo programových slabín. Potom invázia, ničenie a krádeže, ako aj falšovanie informácií spôsobia veľké škody väčšine podnikov a na majetku osôb. Dôsledkom potenciálnej hrozby vzniká v dnešnej dobe čoraz väčší záujem o zvýšenie bezpečnosti informácií, ako aj detekciu prienikov.

Začiatky detekcie prienikov priniesli so sebou aj komplikácie. Medzi teoretickou a praktickou rovinou detekcie prienikov stále existuje priepasť. Táto situácia vytvorila všetky druhy skúšok pre skúmané a rozvíjajúce sa produkty v tejto oblasti. Sú tu pokusy definovať priebežne termíny a vyvíjať adekvátne riešenia, ktoré kooperujú s ostatnými časťami bezpečnostného systému alebo s riadiacou infraštruktúrou. Ďalší významný pokus je požiadavka, aby preferované riešenie alebo prístup riešili všetky problémy bez ohľadu na platnosť tvrdenia.

Zaužívaná obrana siete/systému je postavená na použití firewallu a systému na detekciu prienikov (*Intrusion Detection System* – IDS). Tieto dva systémy prinášajú zo sebou dva druhy otázok. Akonáhle sú útočníci informovaní o tom, že firewall má povolenú bezpečnostnú výnimku pre vonkajšiu službu, dokážu využitím tejto služby získať prístup k interným serverom a prostredníctvom brány firewall uskutočniť ďalší útok. Za druhé, systém na detekciu prienikov nedokáže poskytnúť dodatočné informácie pre zistenie nepriateľských útokov, ako aj nedokáže priamo znížiť straty spôsobené takýmito útokmi [1].

Ak by sme boli, hneď pri prvom útoku, schopný okamžite zaznamenať neznámu zraniteľnosť a možný útok na počítač v systéme, analyzovať neznámy útok a postúpiť výsledky o podobných varovaniach bezpečnostným špecialistom, bola by niekoľkonásobne vyššia šanca vydať výstrahy pre zabezpečenie systémov, nájsť analyzované vzory útokov, možných rizík, metód a nástrojov, a tak v predstihu zabrániť potencionálnym útokom i ďalším poškodeniam. Takýmto postupom by sme dokázali v predstihu účinne znížiť a zmierniť riziko bezpečnosti informácií.

Tradičný prístup k zabezpečeniu je značne mierne zameraný na obranu, ale záujem je čím ďalej, tým viac venovaný agresívnejším formám obrany pred potencionálnymi útočníkmi a narušiteľmi. Takouto formou je aj ochrana pred vniknutím založená na návnade prostredníctvom technológie lákadla (*Honeypot*).

2 SYSTÉMY NA DETEKCIU PRIENIKOV (IDS)

Systém na detekciu prienikov možno definovať ako nástroj alebo softvérovú aplikáciu, ktorá monitoruje činnosti počítačového systému a/alebo siete kvôli potencionálnemu výskytu nebezpečných aktivít alebo porušenia bezpečnostnej politiky. Produkuje správy pre riadiacu stanicu. Primárne je zameraný na identifikáciu a zaznamenávanie informácií o prípadných udalostiach, ako aj hlásenie takýchto pokusov.

2.1 KLASIFIKÁCIA SYSTÉMOV NA DETEKCIU PRIENIKOV

Vzhľadom k rozličným aplikačným prostrediam je možné IDS klasifikovať do dvoch hlavných typov [2]:

- **Hostiteľský** (*host-based*) – pozostáva z agenta umiestneného na hostiteľskom počítači, ktorý pre kontinuálne monitorovanie používa informácie získané zo samotného auditného systému hostiteľského počítača alebo záznamy sieťových aktivít. V takomto IDS senzor zvyčajne obsahuje aj softvérového agenta. Ak nastanú neobvyklé okolnosti systém automaticky vygeneruje a odošle upozornenie. Nevýhodou je zvyčajne veľké množstvo dát určené na monitorovanie.
- **Sieťový** (*network-based*) – predstavuje nezávislú platformu pre identifikovanie prienikov prostredníctvom priameho zachytenia prenášaných paketov v sieti a monitorovanie viacerých počítačov na identifikovanie, či sa jedná o útok alebo inváziu na základe sledovania hlavičky a obsahu jednotlivých paketov. Sieťové systémy detekcie prienikov (*NIDSs*) získavajú prístup k sieťovej prevádzke pripojením sa k sieťovému rozbočovaču (*network hub*), sieťovému prepínaču (*network switch*) nakonfigurovanom na zrkadlenie portov. V NIDS sú senzory na detekciu umiestňované na kritické miesta v sieti, vo väčšine prípadov sú to hranice siete alebo tzv. demilitarizované zóny. Tieto senzory zachytávajú všetku sieťovú prevádzku a analyzujú obsah jednotlivých paketov kvôli výskytu nebezpečnej prevádzky. Nevýhodou je konzumácia väčšiny systémových prostriedkov a sieťovej prevádzky. Príliš veľká sieťová prevádzka zapríčiní nemožnosť alebo nesprávnosť spracovania paketov systémom na detekciu prienikov.

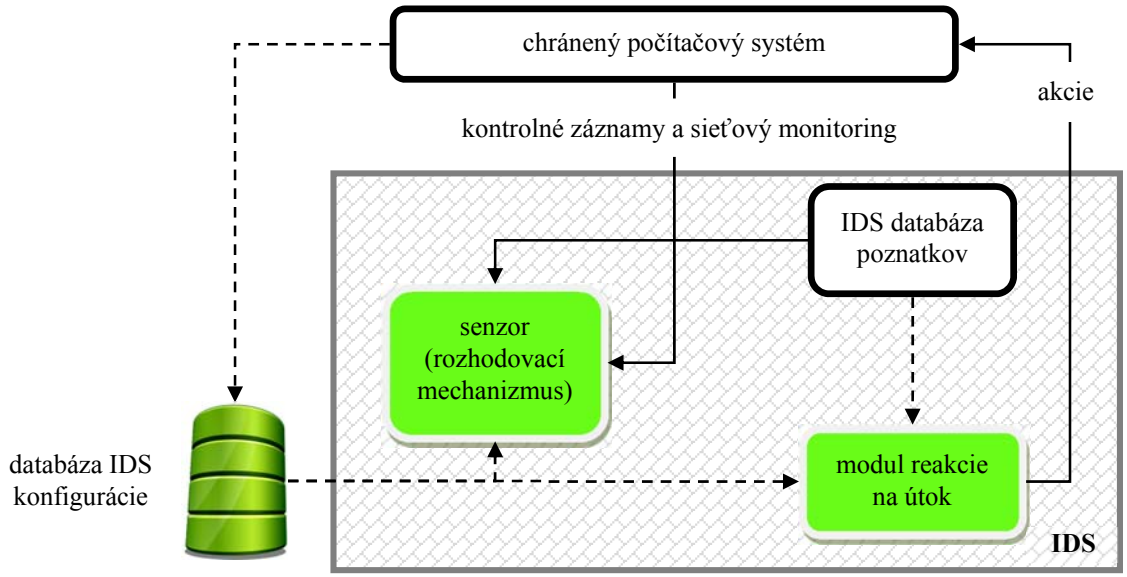
Vzhľadom na metódy detekcie je možné IDS rozdeliť na tri základné typy [3]:

- **Detekcia anomálií** (*anomaly detection*) – odkazuje na zistenie štruktúry v danom súbore dát, ktoré nie sú v súlade s bežným správaním. Takto zistené štruktúry sa nazývajú anomálie. Detekcia anomálií stanovuje základný výkon pre normálnu prevádzku v sieti. Poplach zaznie len v prípade, ak je aktuálna prevádzka v sieti mimo základných parametrov – vyskytla sa anomália.
- **Detekcia zneužitia** (*misuse detection*) – zhromažďuje charakteristiky a vzory predchádzajúceho útoku hackera a pričom ich ukladá do databázy medzi základné znalosti útoku. Následne dokáže identifikovať útok, ktorý má rovnaké vzory a charakteristiky, ako už predtým zaznamenaný útok. V prípade, ak hacker použite na útok novú metódu, ktorá ešte nebola pred tým zaznamenaná, IDS nedokáže spustiť poplach a vznikne hlásenie typu falošné negatívum (*false negative*).
- **Hybridný mód detekcie** (*hybrid mode detection*) – predstavuje detegovanie útoku za pomoci oboch predchádzajúcich typov detekcie, čo má za následok zníženie generovania falošného poplachu, aj keď sa nič nedeje (*false positives*), ako aj negenerovanie poplachu pri nezachytení útoku (*false negatives*).

2.2 ŠTRUKTÚRA A ARCHITEKTÚRA IDS

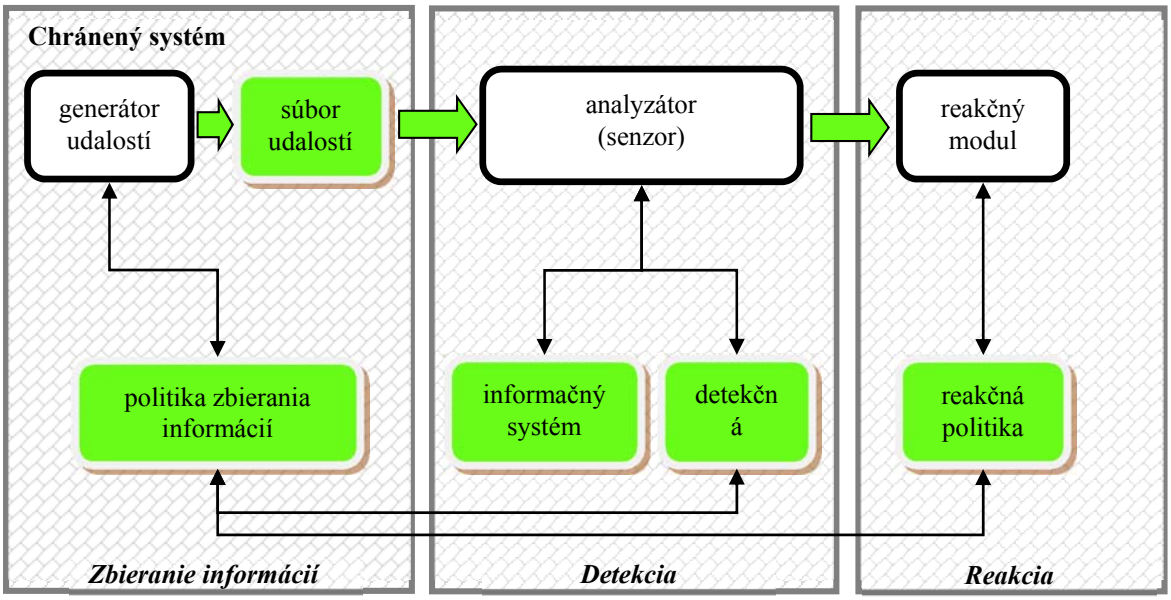
Systém na detekciu prienikov pozostáva z viacerých prvkov, znázornených na Obr. 1, kde hlavným prvkom je senzor (mechanizmus analýzy), ktorý je zodpovedný za detekciu narušenia. Tento snímač obsahuje mechanizmus, ktorý generuje rozhodnutia týkajúce sa narušenia. Senzor príjme dáta z troch hlavných zdrojov informácií: vlastná IDS databáza poznatkov, logovacie záznamy systému a kontrolné záznamy. Logovacie záznamy systému môžu zahŕňať, napr. konfiguráciu súborového

systému a používateľské oprávnenia. Tieto informácie tvoria základ pre ďalšie rozhodovanie pri detekcii narušenia.



Obr. 1. Systém na detekciu prienikov.

Senzor, spolu s ostatnými prvkami znázornenými na Obr. 2, je integrovaný spolu s prvkom zodpovedným za zber dát – generátor udalostí. Spôsob zbierania dát je určený politikou generátora udalostí, ktorý definuje spôsob filtrovania informácií notifikovania o udalostiach. Generátor udalostí (operačný systém, siete, aplikácie) produkuje v súlade s bezpečnostnou politikou súbor udalostí, ktorý môže byť logovacím záznamom systémových udalostí, prípadne sieťových paketov. Tieto udalosti môžu byť spolu s informačnou politikou uložené buď v chránenom systéme alebo mimo neho. V prípade sieťových paketov sa prúdy udalostí neukladajú, nakoľko sú prenášané priamo do analyzátora.



Obr. 2. Prvky systému detekcie prieniku.

Úlohou senzora je filtrovanie informácií a odignorovanie všetkých irelevantných údajov získaných zo súboru udalostí súvisiacich s chráneným systémom a tým odhaliť podozrivé aktivity. Na tento účel využíva databázu detekčnej politiky, ktorá sa skladá z nasledujúcich prvkov: útok podľa vzoru, normálne správanie, profily a potrebné parametre. Okrem toho databáza obsahuje aj parametre IDS konfigurácie a spôsob komunikácie s reakčným modulom. Vlastnú databázu má aj senzor, ktorá obsahuje dynamickú históriu komplexu potenciálnych prienikov.

2.3 NÁSTROJE DETEKCIE PRIENIKOV

Systémov na detekciu prienikov existuje veľké množstvo a môžu byť špecifické pre systém použitím vlastných nástrojov. Najčastejšie používaný je multiplatformový nástroj Snort, ktorý má navyše výborné predpoklady pre použitie na zvýšenie bezpečnosti distribuovaných systémov v kombinácii s Honeypotom.

Snort

Nástroj Snort predstavuje open-source systém na detekciu prieniku, ktorý dokáže nielen detegovať a upozorniť na útok, napr. proti Honeypotu, ale dokáže aj zachytiť pakety a zaťaženie siete danými paketmi zahrnutými do útoku. Tieto informácie sa môžu ukázať ako kritické pri analýze aktivít útočníkov. Pre projektovanie používa modulárnu architektúru a pravidlami riadený jazyk. Kombinuje abnormálne správanie, detekciu podpisu a rôzne metódy detekcie protokolu [4].

Aby bolo možné čo najúspešnejšie sledovať činnosti hackerov v distribuovaných počítačových systémoch, udomácnila sa metodika klamania a podvádzania, prostredníctvom poskytnutia a emulovania niektorých služieb systému, ktorý sa na prvý pohľad zdá byť legitímny. Z dôvodu preniknutia a objasnenia jednotlivých taktík útočníkov je potom možné všetky aktivity hackerov zaznamenať a monitorovať. Táto idea je prijatá použitím pokročilého bezpečnostného nástroja zvaného Honeypot.

3 HONEYPOT

Honeypot je zložité definovať, pretože sa jedná o novú a stále sa vyvíjajúcu technológiu, ktorú je možné zahrnúť do rôznych aspektov bezpečnosti, ako je prevencia, odhaľovanie a zhromažďovanie informácií. Jedinečnosť technológie spočíva v jej všeobecnosti a nie v konkrétnosti – nerieši špecifický bezpečnostný problém. Práve naopak, Honeypot je vysoko-flexibilný nástroj s aplikáciami v rôznych oblastiach. Všetko záleží na tom, čo chceme dosiahnuť. Niektorými lákadlami možno zabrániť útokom, iné možno použiť na detekciu útokov, zatiaľ čo ostatné lákadlá môžu byť použité pre zhromažďovanie informácií a výskum.

Lákadlá, ako sa niekedy Honeypoty nazývajú, sú pozorne monitorované sieťové návnady, existujúce v rôznych tvaroch a veľkostiach, slúžiace rôznym účelom. Je možné ich umiestniť v počítačovej sieti, s firewallom, pred firewall aj za firewall. Toto sú najfrekventovanejšie miesta, z ktorých získavajú útočníci prístup do systému a aj odkiaľ je o nich možné najlepšie získať maximum informácií. Cieľom je získať informácie ohrozením dát systému takým spôsobom, že v budúcnosti bude infiltrovanie akýchkoľvek dát systému nerealizovateľné.

Dáta získané z Honeypotov je možné využiť pri zlepšení súčasného zabezpečenia a obrany, alebo rekonfiguráciu systému s prípravou na budúce hrozby.

3.1 ROZDELENIE HONEYPOTOV

Honeypoty môžu byť klasifikované podľa rôznych spôsobov. Najčastejšie je zaužívané ich rozdeľovanie podľa účelu a úrovne interakcie.

3.1.1 ÚČEL HONEYPOTU

Toto základné delenie rozdeľuje lákadlá na základe oblasti nasadenia a dôvodu použitia.

Výskumný Honeypot

Hlavným cieľom, nakoľko sú používané výhradne v oblastiach výskumu, je získať čo najviac informácií o útočníkoch spôsobom, že sa im plne umožní infiltrovať a preniknúť do bezpečnostného systému. Používa sa na získanie informácií a rozpoznávanie nových metód a druhov nástrojov používaných pri útoku na iné systémy, ako aj analyzovanie stôp hackerov, ako je totožnosť útočníkov a ich spôsob práce (*modus operandi*).

Výskumný Honeypot je navrhnutý na získanie informácií o ľubovoľnej komunite útočníkov, pričom nepridáva žiadnu priamu hodnotu, ktorá by mohla zvýšiť riziko útoku. Používa sa na zhromažďovanie informácií o útokoch, ktorým môžu organizácie čeliť a tým im umožní, lepšie sa pred danými hrozbami chrániť. Primárnou funkciou je skúmať spôsob, akým útočníci postupujú a vedú útok. Pomáha pochopiť ich motívy, správanie a organizáciu. Výskumné lákadlá sú komplexné, čo sa týka nasadenia, udržiavania a zachytenia rozsiahleho množstva dát. Na druhej strane ale môžu byť z časového hľadiska veľmi rozsiahle [5].

Aj napriek informáciám získaným z jedného výskumného Honeypotu, ktoré sa môžu použiť na zlepšenie prevencie proti útoku, zlepšenie detekcie a odpovedi na útok, výskumný Honeypot prispieva

celkovo k priamej bezpečnosti len veľmi málo. Výskumné Honeypoty pridávajú obrovskú hodnotu pre výskum, nakoľko poskytujú platformu pre skúmanie kybernetických hrozieb. Útočníkov je možné sledovať priamo pri čine, zaznamenávať ich útok a narušenie systému krok po kroku. Takéto zhromažďovanie informácií je jednou z jedinečných a ohromujúcich vlastností Honeypotu. Taktiež je to vysoko-prospešný bezpečnostný nástroj v oblasti rozvoja analyzovania a forenzných schopností [6].

Produkčný Honeypot

Jedná sa o typ lákadla, ktoré je použité v prostredí organizácie na jej ochranu a pomoc pri znížení miery rizika. Poskytuje okamžité zabezpečenie lokality výrobných kapacít a nástrojov. Vzhľadom k tomu, že nevyžaduje takú funkcionalitu ako výskumný Honeypot, je zvyčajne jeho vývoj a nasadenie značne jednoduchšie. Hoci dokáže identifikovať rôzne spôsoby útokov, poskytuje menej informácií o útočníkovi ako výskumné Honeypoty. Jeho použitím je možné určiť z ktorého systému útočníci pochádzajú, ktorú konkrétnu činnosť vykonali, ale nemožno určiť ich identitu alebo aké nástroje používajú [5].

Používa sa na ochranu siete pred nebezpečnými aktivitami útočníkov, detekciu a izolovanie útokov vonkajších narušiteľov a spomalenie útoku na skutočné ciele systému, ako aj na zníženie rizík informačnej bezpečnosti. Umiestňuje sa v sieťach z dôvodu zvýšenia celkovej bezpečnosti spoločnosti, kde pomáhajú pri odhaľovaní útokov. Majú tendenciu zrkadliť časti siete spoločnosti alebo špecifické služby a ich simuláciou prilákať pozornosť útočníkov, aby s nimi zahájili interakciu s cieľom odhaliť aktuálne zraniteľné. Odhaľovanie týchto bezpečnostných nedostatkov a upozornením administrátora o útoku môžu poskytnúť včasné varovanie pred útokom a výrazne redukovať riziko prieniku do systému [7].

Je potrebné zdôrazniť, že produkčný Honeypot má ako preventívny mechanizmus minimálnu hodnotu. Najvhodnejšími postupmi implementovania Honeypotu je využitie firewallu, systémov na detekciu prieniku (IDS), mechanizmus na uzamknutie a opravu systému [8].

3.1.2 ÚROVEŇ INTERAKCIE

Úroveň interakcie môže byť definovaná ako maximálny rozsah dostupných možností útoku, umožnený samotným Honeypotom, ktorý má útočník k dispozícii. Hodnota technológie závisí na úrovni interakcie s útočníkmi. Všetky Honeypoty fungujú na rovnakom koncepte – nikto by nemal prísť do styku s lákadlom a preto akékoľvek transakcie alebo interakcie sú, na základe definície, neoprávnené. Okrem základného rozdelenia na výskumný a produktívny Honeypot je možné lákadlá kategorizovať aj podľa stupňa interakcie medzi narušiteľom a systémom. Je to akási pomôcka pri výbere správneho typu lákadla pre nasadenie do systému.

Nízka interakcia

Lákadlo na tejto úrovni interakcie neobsahuje žiadny operačný systém, s ktorým by útočník mohol komunikovať. Všetky nástroje sú nainštalované výhradne k emulovaniu operačného systému a jeho najzákladnejších služieb, ktoré nemôžu byť využité k získaniu úplného prístupu k/do Honeypotu tak, aby spolupracovali s útočníkmi a škodlivým kódom [9][10].

Interakcia systému s útočníkmi je limitovaná a len počas krátkej doby, takže útočníci majú niekoľkonásobne sťažené preniknutie do systému. Útočníci môžu daný Honeypot len skenovať a pripojiť sa na niekoľko portov. Tento typ lákadla sa používa na zabezpečenie systému pred potenciálnymi útočníkmi, čo na druhej strane spôsobuje získanie obmedzeného počtu informácií o narušiteľoch. Lákadlá s nízkou interakciou môžu byť porovnávané k pasívnym systémom na detekciu prieniku, nakoľko žiadnym spôsobom neovplyvňujú prevádzku v systéme a takisto nedokážu ani komunikovať s útočníkom. Hoci takéto riešenie minimalizuje mieru ohrozenia Honeypotu, je na druhej strane, z dôvodu schopnosti nízkej interakcie útočníka s lákadlom, získavanie informácií o útočníkoch veľmi obmedzené. Avšak stále je možné ho použiť pri analyzovaní spamerov a ako aktívne protiopatrenie proti červom. Honeypoty s nízkou interakciou sú charakteristické možnosťou ľahkého nasadenia a udržiavania [8].

Stredná interakcia

V porovnaní s predchádzajúcim typom interakcie sú stredné Honeypoty trochu sofistikovanejšie. Ani tento typ nemá nainštalovaný operačný systém, ale simulované služby na tomto type lákadla sú technicky viac komplexnejšie. Aj keď sa pravdepobnosť, že útočník nájde slabinu v zabezpečení systému zvyšuje, je stále málo pravdepodobné, že systém bude ohrozený. Lákadlá so strednou interakciou poskytujú útočníkovi ilúziu operačného systému, pretože obsahujú viacero emulovaných služieb, s ktorými môže vzájomne komunikovať. Dôsledkom toho môžu byť zaznamenané a analyzované aj zložitejšie typy útokov [8].

Vysoká interakcia

Jedná sa o najmodernejšie typy lákadiel, ktoré predstavujú riešenie s najkomplexnejším a časovo-náročným dizajnom s najvyššou mierou rizika, pretože v sebe zahŕňajú aj funkčný operačný systém [10]. Cieľom Honeypotov s vysokou interakciou je poskytnúť útočníkovi možnosť komunikovať so skutočným operačným systémom, v ktorom nie je nič simulované, emulované alebo obmedzené. Umožňuje zber najväčšieho množstva informácií, nakoľko dokáže zaznamenať a analyzovať všetky vykonané aktivity [1].

Vzhľadom k tomu, že útočník má k dispozícii viac zdrojov, malo by byť lákadlo s vysokou interakciou pod neustálym monitorovaním, aj z dôvodu zníženia nebezpečenstva alebo vzniknutia bezpečnostnej diery. Hlavný dôraz je kladený na získanie cenných informácií o narušiteľoch, sprístupnením celého systému alebo dokonca umožnením manipulácie s ním. Pomocou tohto rýdzo výskumne-orientovaného lákadla je možné objaviť nové techniky používané narušiteľmi [10].

3.2 ARCHITEKTÚRA HYBRIDNÉHO HONEYPOTU

Hybridné lákadlo predstavuje kombináciu dvoch lákadiel s rôznou úrovňou interakcie. Kombinácia dvoch rôznych Honeypotov predstavuje bezpečné riešenie, nakoľko je možné využiť výhody obidvoch lákadiel, znázornené v Tabulka 1, tak, že sa navzájom dopĺňajú a tým obmedzujú svoje nevýhody. Ideálnym riešením je kombinácia Honeypotu s nízkou a vysokou interakciou. Honeypot s nízkou interakciou vystupuje ako ľahké proxy, čím odbremeňuje Honeypot s vysokou interakciou – nezapája ho do všetkých útočníkových aktivít ako je automatizovaný proces skenovania samotného systému, čím mu umožňuje zamerať sa na spracovanie podstatných

útočníkových aktivít spojených s procesom prieniku do systému a prenosov smerovaných k špecifickému IP adresného priestoru, na ktorom je hybridný Honeypot nainštalovaný [11]. Akonáhle Honeypot s nízkou interakciou vyhodnotí/deteguje, že sa nejedná o žiadny automatizovaný proces, aktivuje sa Honeypot s vysokou interakciou pre záznam informácií, na základe ktorých je možné zlepšiť samotnú bezpečnosť systému.

Honeypot s vysokou interakciou	**Honeypot s nízkou interakciou**	**Hybridný Honeypot**
- pomalý	+ rýchly	+ rýchly
+ možnosť detegovania neznámych útokov	- absencia možnosti detegovania neznámych útokov	+ možnosť detegovania neznámych útokov
+ 0 falošne detegovaných útokov		+ 0 falošne detegovaných útokov
- neschopný odolať časovým bombám, plytvanie výkonu pri automatizovaných procesoch útočníkov	+ odolá časovým bombám a postačujúci pre interakciu s automatizovanými procesmi útočníkov	+ odolá časovým bombám a postačujúci pre interakciu s automatizovanými procesmi útočníkov
- drahý	+ lacný	+ relatívne drahý
- zložitý na nastavenie a ovládanie	+ jednoduchý na nastavenie aj ovládanie	- zložitý na nastavenie a ovládanie

Tab. 1. Podstata hybridných Honeypotov.

Pri každom návrhu lákadla sa jeho implementovanie do systému nezaobíde bez použitia jedného alebo viacerých implementačných nástrojov, ktoré majú značný význam v oblasti zvyšovania zabezpečenia systémov:

- **Dionaea** je modulárna architektúra využívajúca Honeypot s nízkou interakciou, ktorá umožňuje simulovať hlavné služby i zraniteľnosť serverov a takýmto spôsobom upútať útočníkovu pozornosť alebo zachytiť škodlivý kód [12].
- **Sebek** je najpokročilejší komplexný nástroj pre zhromažďovanie dát, ktorého cieľom je zachytiť z Honeypotu čo najviac informácií o činnosti útočníka, zastavením konkrétneho systémové volania (*syscalls*) na úrovni jadra (*kernel level*) [12].

3.3 VÝHODY A NEVÝHODY POUŽÍVANIA HONEYPOTOV

Všetky bezpečnostné technológie majú určité riziko. Pokiaľ znalosti a skúsenosti predstavujú výhodu pre útočníkov, platí to takisto aj pre bezpečnostných odborníkov. Je nutné ovládať jednotlivé výhody

aj nevýhody lákadiel, nakoľko uvedomenením si vlastného rizika Honeypotu je možné použiť tieto znalosti na zmiernenie rizík a obídenie, resp. maximálne minimalizovanie možných nevýhod [8].

Použitie Honeypotov má niekoľko významných výhod v porovnaní so súčasnými najčastejšie používanými bezpečnostnými mechanizmami [11]:

- **Malé dátové sady** (*small data sets*) – Honeypoty dokážu sledovať len prevádzku, ktorá prichádza priamo do nich. Dátové sady lákadla môžu byť malé, ale na druhej strane môžu obsahovať informácie vysokej hodnoty.
- **Jednoduchosť** (*simplicity*) – lákadlá sú veľmi jednoduché a flexibilné. Pre plnenie správnej funkčnosti v počítačovej bezpečnosti nepotrebujú návrhy komplikovaných algoritmov, aktualizovanie a udržiavanie stavových tabuliek alebo signatúr.
- **Objavenie nových nástrojov a taktík** (*discovery of new tools and tactics*) – Honeypoty zachytia všetko, čo sa dostane s nimi do interakcie, ako aj pred tým ešte nepoužité nástroje a taktiky útočníkov.
- **Šifrovanie alebo IPv6** (*encryption or IPv6*) – implementácia lákadiel funguje aj v šifrovanom alebo IPv6 prostredí.
- **Minimálne zdroje** (*minimal resources*) – vzhľadom k tomu, že zachytávajú len škodlivé aktivity, potrebujú k správnej funkčnosti minimálne systémové zdroje. Ako lákadlo je tým pádom možné použiť už vyradený alebo low–end systém.

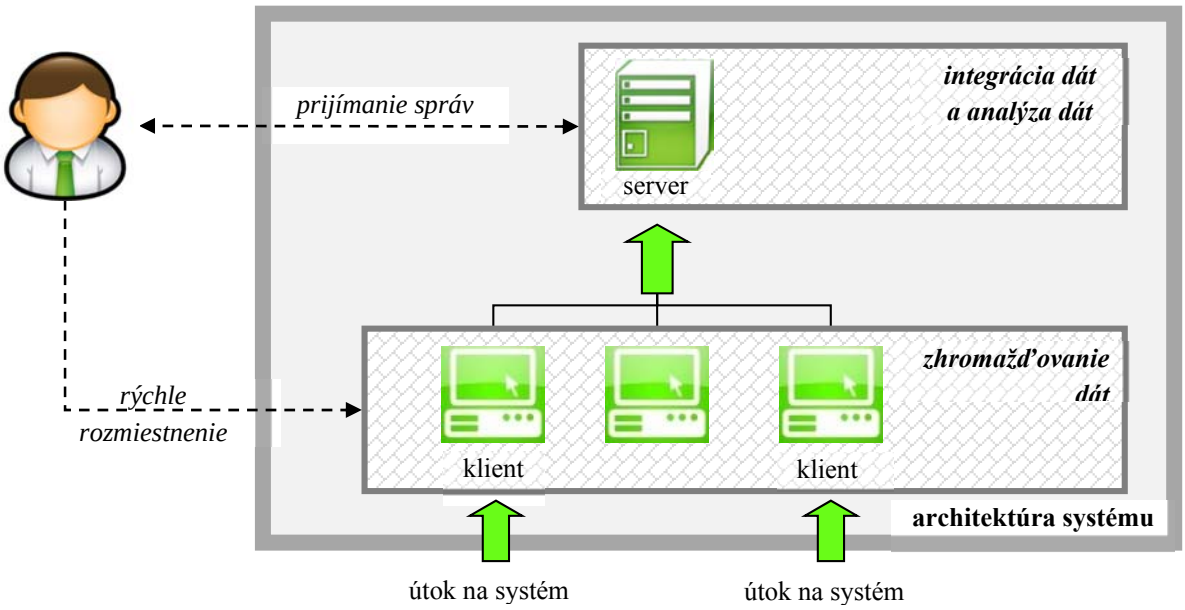
Podobne ako ostatné bezpečnostné riešenia, tak aj technológia na báze lákadiel, má špecifické nevýhody [1]:

- **Obmedzené videnie** (*limited view*) – jediným spôsobom, kedy Honeypot dokáže aktivity útočníka zachytiť a sledovať, je ten keď s ním útočník priamo komunikuje. Útoky na ostatné časti systému nebudú zaznamenané, pokiaľ nebude Honeypot tiež ohrozený.
- **Prezradenie identity Honeypotu** (*discovery and fingerprinting*) – Honeypot má určité očakávateľné vlastnosti alebo správania, kvôli ktorým útočník môže zistiť skutočnú totožnosť lákadla. Aj jednoduchá chyba, ako je nesprávne napísané slovo v emulácii služby, môže byť pre útočníka signálom interakcie s Honeypotom [8].
- **Riziko prevzatia** (*risk of takeover*) – ak nad Honeypotom získa útočník kontrolu, môže ho zneužiť pri útoku na iné systémy vo vnútri alebo mimo organizácie.

4 ARCHITEKTÚRA SYSTÉMU DETEKCIE VYUŽÍVAJÚCA HYBRIDNÝ HONEYPOT

Hlavnú slabinu IDS predstavuje problém pri detegovaní nového typu útoku, ako aj použitie odlišnej stratégie pri útoku alebo nového nástroja. Aby bolo možné zachytiť aj takéto útoky je nutné každý nový útok zaznamenať do konfiguračnej databázy IDS. Navrhovaný systém detekcie využíva sofistikovaný hybridný Honeypot pre zníženie záťaže pri budovaní a navrhovaní bezpečnostných prvkov distribuovaných systémov a rozsiahleho zhromažďovania dát, ako aj minimalizovanie ktorejkoľvek hrozby prieniku do systému. Hybridný Honeypot kombinuje niekoľko nástrojov (Snort, Dionaea a Sebek) pracujúcich ako jeden celok. Kvôli rýchlej odozve na daný útok navrhovaný systém, znázornený na Obr. 19, analyzuje všetky zachytené dáta v rôznych formátoch. Pri výskyte/začatí

interakcie s Honeypotom zároveň poskytuje, prostredníctvom webového rozhrania, aj varovný systém správ pre systémového administrátora.



Obr. 3 Architektúra navrhovaného systému detekcie.

Navrhovaná architektúra pozostáva z niekoľkých klientov a servera. Klient zhromažďuje informácie o útoku a zachytený škodlivý kód následne odosiela späť na server. Server zaznamená a analyzuje útok, vydá varovanie a pomocou webového rozhrania zobrazí celkovú informáciu. Architektúra je navrhnutá na dosiahnutie efektu centralizovaného riadenia distribuovaných informácií a vybudovania kompletného distribuovaného systému včasného varovania.

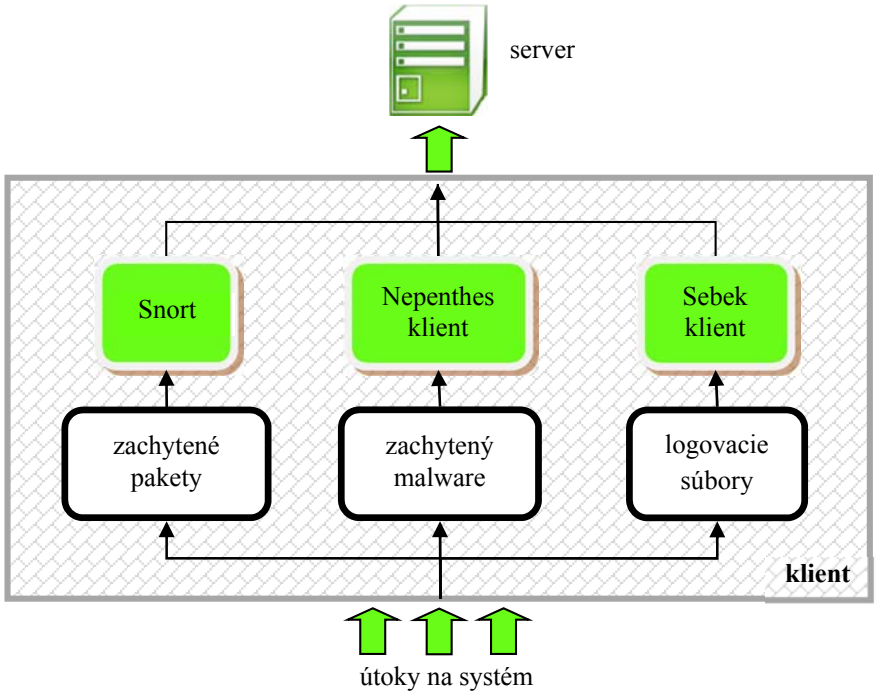
4.1 ARCHITEKTÚRA – KLIENT

Z dôvodu zhromažďovania dát o útočníkových aktivitách počas samotného útoku sú nainštalovaní klienti umiestnení v rovnakej doméne. Pri kyberútoku sa, v závislosti od typu, aktivujú rôzne súčasti systému pre zber množiny dát a ich spätné doručenie serveru na uľahčenie následnej analýzy a pre následné aktualizovanie systémovej bezpečnosti. Architektúra klienta, zobrazená na Obr. 4, pozostáva z troch súčastí:

Snort – monitoruje a filtruje pakety pri detegovaní prieniku. Identifikuje vzory jednotlivých útokov, informácie a varovné správy.

Nepenthes klient – simulovaním všeobecných služieb a zraniteľných miest láka útočníkov, pričom zachytáva vzory škodlivých kódov.

Sebek klient – zaznamenáva správanie útočníka počas interakcie s Honeypotom do logovacích súborov.



Obr. 4 Architektúra klienta.

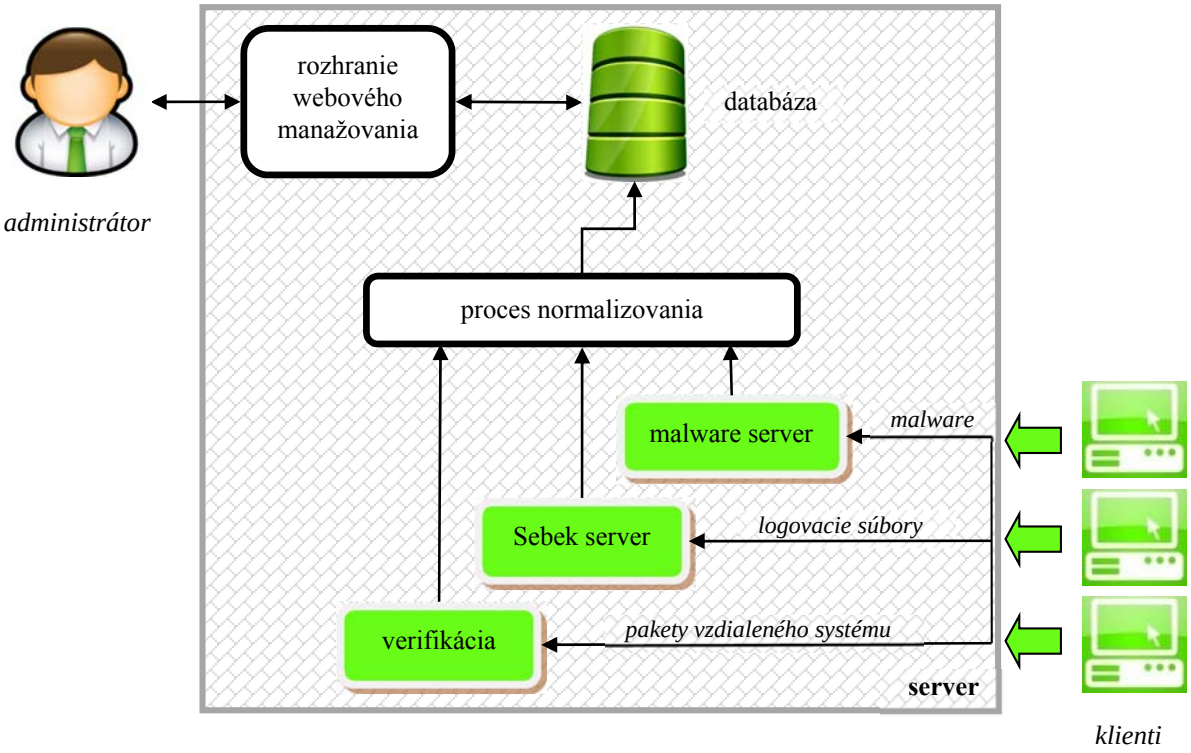
4.2 ARCHITEKTÚRA – SERVER

Z dôvodu centralizácie zozbieraných údajov je server súčasne pripojený k viacerým klientom a nastavený prijímať všetky odosielané správy, ktoré následne ukladá do databázy. Architektúra servera je znázornená na Obr. 5. Previazanosťou jednotlivých správ indikuje zámer útočníkov napadnúť cielené oblasti počítačov rozsiahlymi útokmi alebo skenovaním. Navrhovaná architektúra servera pozostáva z troch častí, ktoré ešte pred uložením do databázy absolvujú proces normalizovania vstupných formátov:

Malware server – prijíma vzory malwaru odosielané časťou Nepenthes klient.

Sebek server – súčasne prijíma a filtruje viacero zdrojov dát predstavujúce inštrukciu alebo spojenie odosielaných dát na uloženie.

Verifikácia – modulárny návrh open-source hybridného systému na detekciu prieniku, využívajúci štandardný komunikačný formát. Dokáže sa prispôsobiť potrebám rozsiahleho systému z akéhokoľvek bodu nasadenia, prijímať množstvo údajov od klientov a integrovať rôznorodé dátové formáty.



Obr. 5 Architektúra servera.

Webové rozhranie servera zobrazuje celú analýzu informácie o útoku, získanej z databázy. Súčasne monitoruje útoky a výskyt neobvyklých okolností. V prípade ich výskytu sa zvýraznia konkrétne správy, aby správca systému dokázal správne a včas reagovať. Najideálnejšie riešenie predstavuje koncept použitia navrhovaného autonómneho sofistikovaného Honeypotu pre proces detegovania.

4.3 NÁVRH SOFISTIKOVANÉHO HONEYPOTU

4.3.1 IDEÁLNY STAV

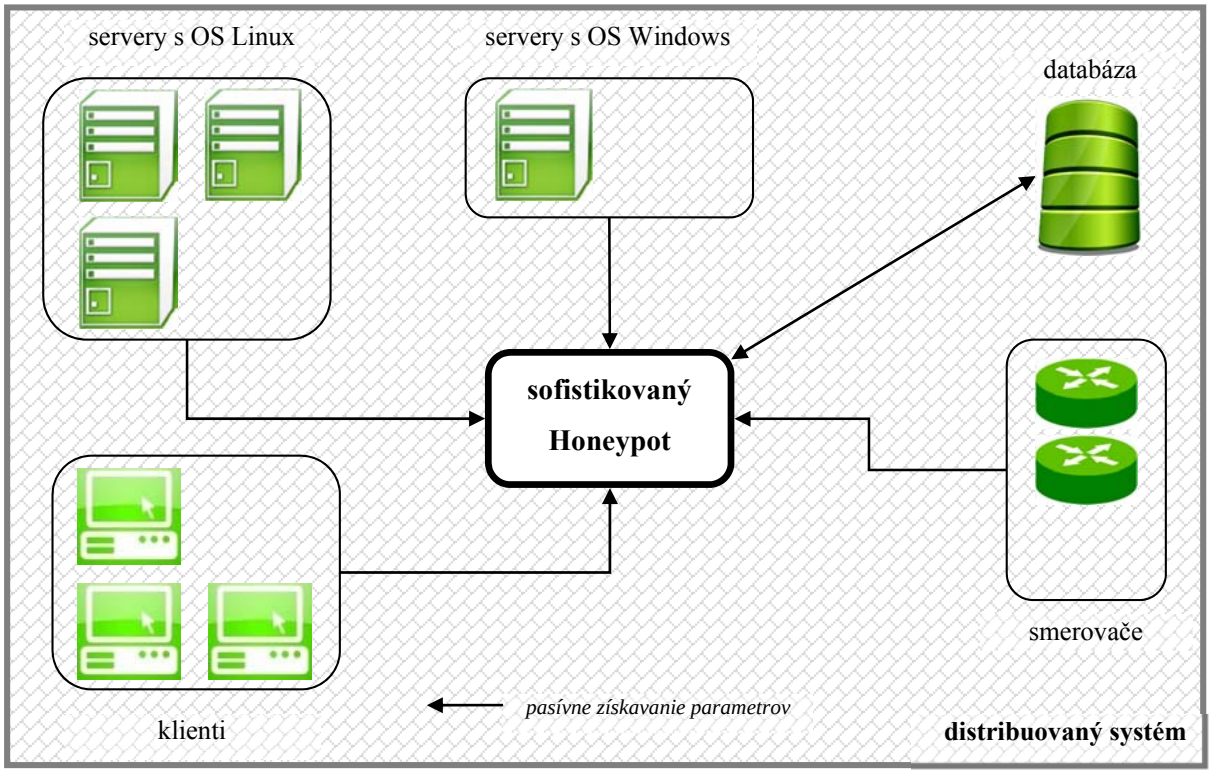
Riešenie súčasného stavu predstavuje návrh sofistikovaného Honeypotu, ktorý funguje na princípe plug-&-play. Optimálny stav nastáva, ak po zapojení lákadlo vykoná všetky konfigurácie úplne samostatne. Napr. po nainštalovaní OS Linux do distribuovaného systému, budeme mať linuxový Honeypot, alebo pri odstránení ľubovoľnej služby, sa súvisiaca služba odstráni aj spomedzi zoznamu emulovaných služieb. Pri výmene smerovačov, napr. Hewlett-Packard za smerovače Cisco, sa lákadlo tváriace ako smerovač samostatne nakonfiguruje a aktualizuje.

Riešením je zariadenie, ktoré jednoducho stačí len pripojiť do siete a samé sa naučí topológiu systému, presne určí počet Honeypotov, ako aj ich konfiguráciu a dokáže sa v reálnom čase adaptovať na akúkoľvek zmenu v systéme.

4.3.2 PROBLÉM

Prvou a najkritickejšou časťou sofistikovaného Honeypotu je spôsob, akým dokáže získavať informácie o sieti, v ktorej je nasadený, napr. aké systémy sú využívané a ako sa používajú v danom prostredí – znázornené na Obr. 6. Po získaní týchto parametrov bude sofistikovaný Honeypot

inteligentne mapovať a promptne reagovať na dané prostredie. Jeden z možných a najjednoduchších spôsobov je použiť aktívne sondovanie a takto určiť používané systémy, ich typ i používané služby. Použitím aktívnej metódy získavania údajov, ktorá má svoje nedostatky v podobe zvýšenej záťaže siete, vzniká riziko ohrozujúce prevádzku systému.



Obr. 6. Pasívne získavanie systémových parametrov sofistikovaným Honeypotom pre determinovanie spôsobu rozmiestnenia virtuálnych Honeypotov.

Pre kontinuálnu a korektnú funkčnosť v distribuovanom systéme by sofistikovaný Honeypot musel neustále aktívne skenovať celé prostredie nasadenia, čo nepredstavuje najvhodnejší prístup.

4.3.3 RIEŠENIE PROBLÉMU

Riešením nevýhod aktívneho skenovania predstavuje pasívny prístup, konkrétne metóda pasívneho získavania odtlačkov a mapovania (*passive fingerprinting and mapping*) [13].

Metóda pasívneho získavania odtlačkov nie je nová. Ideou je zmapovanie a získanie prehľadu systémov v nasadenom prostredí. Rozdiel oproti aktívnej metóde predstavuje spôsob mapovania, ktorý je pasívne získavaný odchytávaním sieťovej komunikácie, jej analyzovaním a následným určením identity systémov. Pasívny spôsob používa rovnaké metódy ako aktívny. Nástroje ako, napr. Nmap [13], vytvoria databázu signatúr o známych operačných systémoch a službách. Po vytvorení databázy tieto nástroje aktívne vysielajú pakety, vyžadujúce odpoveď, od cieľových zariadení. Prichádzajúce odpovede, unikátne pre väčšinu operačných systémov a služieb, sú porovnávané s databázou z dôvodu jednoznačného identifikovania operačného systému a používaných služieb.

Pasívne získavanie odtlačkov používa rovnaký prístup ako vyššie popísaná databáza, ibaže dáta získava pasívne. Namiesto aktívneho sondovania systému odchytáva prevádzku zo siete a analyzuje odchytené pakety, ktoré následne porovnáva s databázou signatúr identifikácie vzdialeného systému. Metóda pasívneho získavania odtlačkov nie je limitovaná použitím výhradne TCP protokolu, čo umožňuje využitie iných protokolov. Tým, že je metóda kontinuálna – zmeny v sieti zachytáva v reálnom čase, sa jej výhoda stáva kritickou pre udržiavanie realistického Honeypotu počas dlhého obdobia. Jedinú nevýhodu pre pasívne získanie predstavuje správnosť fungovania cez smerované siete – efektívnejšie je pri použití v lokálnych sieťach.

4.3.4 KONCEPT

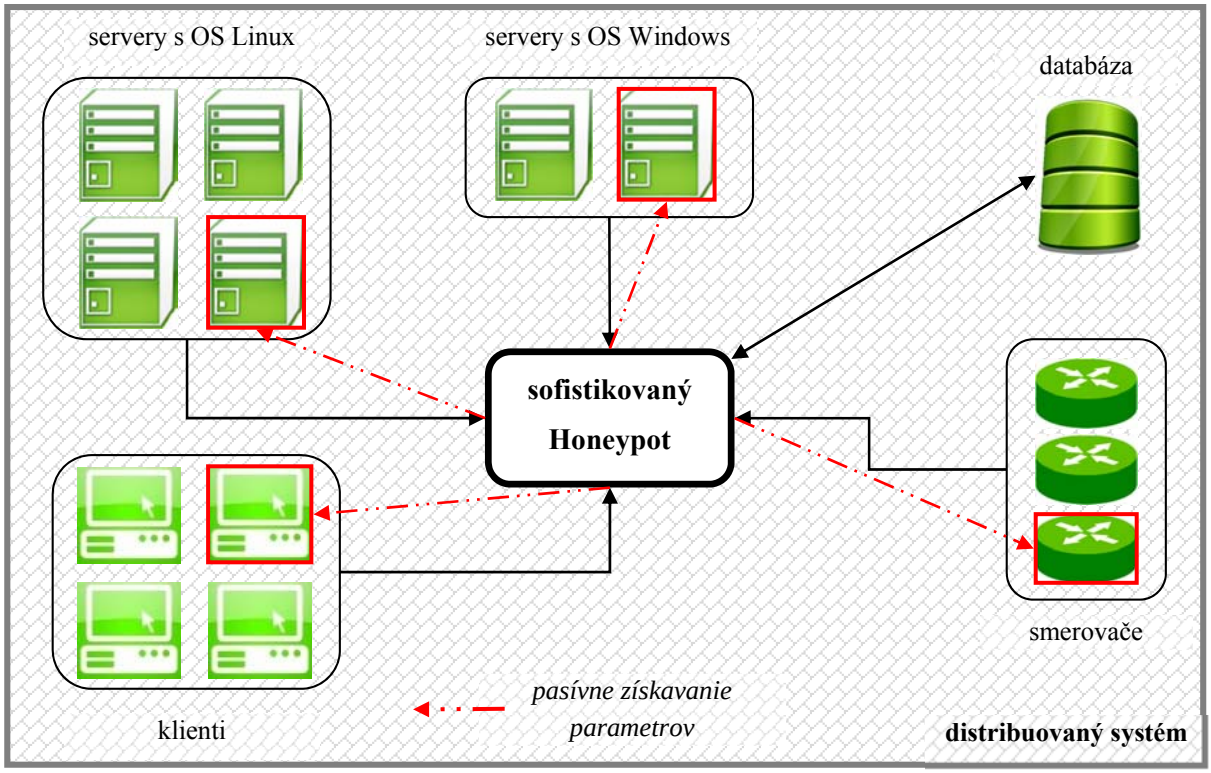
Navrhovaný Honeypot používa pri získavaní údajov o sieti koncept založený na pasívnom získavaní odtlačkov. Honeypot je nasadený ako samostatné zariadenie, ktoré je fyzicky pripojené do počítačovej siete distribuovaného systému. Pasívnym analyzovaním sieťovej prevádzky determinuje počet používaných systémov, typ operačných systémov, druh spustených a poskytovaných služieb, po prípade zistí, s kým a ako často komunikuje konkrétny systém. Tieto informácie slúžia pre mapovanie a získanie znalostí o sieti. Akonáhle Honeypot zozbiera všetky potrebné informácie, môže začať s rozmiestňovaním Honeypotov Obr. 7, ktoré sú vytvorené pre zrkadlenie celého systému. Honeypoty so schopnosťou výzoru a správania sa rovnakým spôsobom ako produkčné prostredie, dokážu bez problémov splynúť s okolím, čo robí ich identifikáciu alebo vypátranie útočníkom omnoho zložitejším. Pasívne získavanie informácií však nekončí, ale prebieha kontinuálne, čím monitoruje celú sieť systému a predstavuje zvýšenie flexibility, nakoľko pri akejkoľvek zmene je táto v reálnom čase identifikovaná a, v systéme rozmiestnenými Honeypotmi, v čo najrýchlejšom čase realizovaná.

4.3.5 ROZMIESTNENIE HONEYPOTOV V SYSTÉME

Tradičné riešenie otázky implementovania lákadlá do systému vyžaduje jeho fyzické umiestnenie pre každú monitorovanú IP adresu, čo predstavuje značné časové obdobie i prácu. Jednoduchším autonómnym riešením, napr. typu vystreľ a zabudni (*fire-&-forget*), je neimplementovať fyzické Honeypoty, ale virtuálne, ktoré v dostatočnom množstve dokážu monitorovať všetky nevyužívané IP adresy. Virtuálne lákadlá sledujú identický IP adresný priestor, ako samotný systém. Všetky virtuálne lákadlá sú vytvorené, umiestnené a spravované jedným fyzickým zariadením – navrhovaným sofistikovaným Honeypotom, ktorého princíp fungovania je znázornený na Obr. 7.

Nakoľko virtuálne Honeypoty monitorujú nevyužívané IP adresy v počítačovej sieti, je takmer isté, že akákoľvek aktivita daných IP adries je z najväčšou pravdepodobnosťou škodlivým alebo neautorizovaným správaním. Pomocou informácií získaných prostredníctvom pasívneho mapovania prostredia je možné stanoviť potrebné množstvo, typ a rozmiestnenie Honeypotov.

Schopnosť dynamicky vytvárať a rozmiestňovať virtuálne lákadla už existuje. Open-source riešenie Honeypotu s nízkou interakciou – Honeyd umožňuje nasadiť virtuálne lákadlá v celom prostredí organizácie. Kombináciou možností riešenia ako je Honeyd a schopnosťami metódy pasívneho získavania odtlačkov, je možné realizovať návrh autonómneho sofistikovaného Honeypotu s dynamickým vytváraním a rozmiestňovaním virtuálnych lákadiel, ktoré splynutím s okolitým prostredím systému minimalizujú riziko identifikovania a odhalenia útočníkom [14].



Obr. 7. Rozmiestnenie virtuálnych Honeypotov na základe získaných parametrov.

5 ZÁVER

V súčasnosti je bezpečnosť informačných technológií obzvlášť dôležitá v spoločnostiach, ktoré sú závislé od informácií. Preto sa, pri tvorbe systémov, kladie nemalý dôraz práve na ochranu údajov a informačných zdrojov. Ochrana prístupu, dostupnosť a integrita údajov reprezentujú základné bezpečnostné vlastnosti požadované od informačných zdrojov. Narušenie niektorej z uvedených vlastností by znamenalo prienik do systému a s tým súvisiace bezpečnostné riziko. Existuje niekoľko spôsobov ochrany systémov, kam radíme aj rôzne metódy na zabezpečenie, obsahujúce bezpečnostné pravidlá a popisujúce jednotlivé úrovne možného správania.

Ďalším spôsobom obrany sú rôznorodé systémy, ktoré detegujú neobvyklé a podozrivé správanie. Medzi tieto systémy zahŕňame aj systémy na detekciu prienikov. Pri systémoch na detekciu prienikov predstavuje hlavný problém riziko nedetegovania prieniku.

Riešením daného problému detekcie predstavuje použitie lákadiel, ktoré sú relatívne novou, čoraz populárnejšou a používanejšou, technológiou. Technológia nazývaná Honeypot má obrovský potenciál pre bezpečnostnú komunitu a môže dosiahnuť niekoľko cieľov iných technológií, čo ju robí takmer univerzálnou. Použitie lákadiel predstavuje cenovo-efektívne riešenie pre zvýšenie bezpečnostného postavenia organizácie. Z tohto dôvodu sú rastúcou mierou nasadzované v systémoch, avšak väčšinou pasívne, nakoľko administrátori sledujú situáciu v systéme a akonáhle bol Honeypot napadnutý, manuálne vykonajú analýzu a implementujú riešenie.

Tak ako akákoľvek nová technológia, aj lákadlá majú určité nedostatky, ktoré potrebujú prekonať a odstrániť. Takže ani Honeypot nepredstavuje všeliek na prelomenie bezpečnosti. Vzhľadom k tomu, že sa používa na zber informácií o útočníkoch a iných hrozbách, je užitočný ako nástroj pre forenzné činnosti v sieti a detekciu prienikov v počítačových systémoch.

Budúcnosť Honeypotov a počítačovej bezpečnosti v detekcii prienikov predstavujú sofistikované lákadlá, pretože majú predpoklad radikálnej revolúcie autonómneho nasadenia a údržby. Štúdovaním a monitorovaním siete v reálnom čase, sa stávajú vysoko-flexibilným riešením. Nielenže ich nasadenie a spravovanie sa stáva cenovo efektívnejším, ale poskytuje aj omnoho lepšiu integráciu do systému, čím sa minimalizuje riziko chyby ľudského faktora počas manuálneho konfigurovania. Splynutím s okolitým prostredím systému navyše minimalizuje riziko identifikovania útočníkom.

POĎAKOVANIE

Táto práca bola podporovaná Agentúrou na podporu výskumu a vývoja na základe zmluvy č. APVV-0008-10 (50%) a vznikla aj vďaka podpore v rámci operačného programu Výskum a vývoj pre projekt: Centrum výskumu účinnosti integrácie kombinovaných systémov obnoviteľných zdrojov energií, s kódom ITMS: 26220220064, spolufinancovaný zo zdrojov Európskeho fondu regionálneho rozvoja (50%).

6 ZOZNAM POUŽITÝCH ZDROJOV

[1] MCGRAW, Gary a Greg MORRISETT. Attacking Malicious Code: A Report to the Infosec Research Council. *IEEE Software: A report to the Infosec Research Council*. 2000, vol. 17, issue 5, s. 33-41. DOI: 10.1109/52.877857.

[2] MCHUGH, John, Alan CHRISTIE a Julia ALLEN. Defending Yourself: The Role of Intrusion Detection Systems. *IEEE Software: A report to the Infosec Research Council*. 2000, vol. 17, issue 5, s. 42-51. DOI: 10.1109/52.877859.

[3] *Know your enemy: revealing the security tools, tactics, and motives of the blackhat community*. Boston: Addison-Wesley, c2002, xvii, 328 s. ISBN 02-017-4613-1.

[4] Snort. [online]. [cit. 2013-03-03]. Dostupné z: http://www.snort.org.

[5] CHUVAKIN, Anton. "Honeynets: High Value Security Data". *Network Security*. 2003, vol. 2003, issue 8, s. 11-15. DOI: 10.1016/S1353-4858(03)00808-0.

[6] Symantec Corporation. SPITZNER, Lance a Marty ROESCH. *The Value of Honeypots: Part One: Definitions and Values of Honeypots* [online]. 2001, 3.11.2010 [cit. 2013-03-03]. Dostupné z: http://www.symantec.com/connect/articles/value-honeypots-part-one-definitions-and-values-honeypots.

[7] KECIA, Gubbels. Hands in the Honeypot. In: *SANS Institute: InfoSec Reading Room* [online]. 2002 [cit. 2013-06-03]. Dostupné z: http://www.sans.org/reading_room/whitepapers/detection/hands-honeypot_365.

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

[9] BAECHER, Paul, Markus KOETTER, Thorsten HOLZ, Maximillian DORNSEIF a Felix FREILING. The Nepenthes Platform: An Efficient Approach to Collect Malware. s. 165. DOI: 10.1007/11856214_9.

[10] BAUMANN, Reto a PLATTNER. White Paper: Honeypots. 2002. Dostupné z: http://www.rbaumann.net/download/whitepaper.pdf.

[11] SPITZNER, L. a PLATTNER. The honeynet project: trapping the hackers. *IEEE Security*. 2003, vol. 1, issue 2, s. 15-23. DOI: 10.1109/MSECP.2003.1193207.

[12] SINGH, Ram Kumar a T. RAMANUJAM. Intrusion Detection System Using Advanced Honeypots. *(IJCSIS) International Journal of Comput er Science and Info rmation Security* [online]. 2009, roč. 2, č. 1 [cit. 2013-06-03]. Dostupné z: http://arxiv.org/ftp/arxiv/papers/0906/0906.5031.pdf.

[13] 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.

[14] PROVOS, Niels. Honeyd: A Virtual Honeypot Daemon. Dostupné z: http://www.citi.umich.edu/u/provos/papers/honeyd-eabstract.pdf.

[15] Symantec Corporation. In: SPITZNER, Lance. *Open Source Honeypots: Learning with Honeyd* [online]. 2003, 2.11.2010 [cit. 2013-06-03]. Dostupné z: http://www.symantec.com/connect/articles/open-source-honeypots-learning-honeyd.

[16] SUTTON, Raplh Edvard Jr. Section 1: How to Build and Use a Honeypot. In: *Docstoc: Documents & Resources for Small Businesses & Professionals* [online]. 2008 [cit. 2013-06-03]. Dostupné z: http://www.docstoc.com/docs/1953205/How-to-build-and-use-a-Honeypot-By-Ralph-Edward-Sutton-Jr-DTEC.

[17] BALAZ, Anton a Liberios VOKOROKOS. Intrusion detection system based on partially ordered events and patterns. *2009 International Conference on Intelligent Engineering Systems*. IEEE, 2009, s. 233-238. DOI: 10.1109/INES.2009.4924768.

[18] VOKOROKOS, Liberios, Norbert ÁDÁM a Anton BALÁŽ. *Application Of Intrusion Detection Systems In Distributed Computer Systems And Dynamic Networks* [online]. Košice, 2008[cit. 2013-03-03]. ISBN 978-80-8086-100-1. Dostupné z: http://kpi1.fei.tuke.sk/CST08/CSetTRS08.pdf#page=23.