**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra informačních technologií**


**Teze bakalářské práce**

# Honeypot a jeho možnosti zvýšení zabezpečení serveru

**Marek Šišák**

# Souhrn

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

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

# 1. Cíl a metodika

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

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

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

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

# 2. Výsledky a diskuze

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

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

Z nashromážděných jedinečných hesel mělo největší čestnost **heslo 123456 s hodnotou 17 pokusů**. Nejčastějšími kombinacemi uživatelského jména a hesla byly v 15 případech root/1234, root/wubao a root/jiamina. **Nejdelší heslo mělo 100 znaků**, nejkratší 1, nejčetnější byla hesla s 8 znaky. Z 94 IP adres, se kterými přišlo během provozu Kippo do kontaktu, byla nejaktivnější adresa **103.41.124.63 s 1104 relacemi**.

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

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

Z výsledků práce vyplývá, že aktivita útočníků je opravdu obrovská a proudí z celého světa. První radou, se kterou se uživatel PC v oblasti bezpečnosti setkává, se týká kvalitně

nastaveného hesla. Kolikrát lidé neznalý možností zneužití počítačů nejsou řádně informováni o hrozbách, které na ně číhají a díky slabému heslu přicházejí o cenné informace. Každý bezpečnostní technik nabádá uživatele k vytvoření hesla kombinujícího písmena různých velikostí, s číselnými hodnotami a speciálními znaky. V práci je jasně vidět, že pokud správce serveru nastaví častého uživatele typu root, se slabým heslem, má zaručeno, že se mu na server dostane třetí strana, o kterou nestojí.

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

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

# Seznam použitých zdrojů


1. LANCE, Spitzner. *Honeypots: Tracking hackers*. Boston: Addison-Wesley, 2003. ISBN 03-211-0895-7.
2. *The Honeynet Project* [online]. [cit. 2013-12-02]. Dostupné z: https://www.honeynet.org/
3. Honeypot Background. [online]. [cit. 2015-01-13]. Dostupné z: http://www.honeyd.org/background.php
4. Kippo-Graph - BruteForce Labs Blog. [online]. [cit. 2015-03-03]. Dostupné z: http://bruteforce.gr/kippo-graph
5. Bezpečnost - Root.cz. [online]. [cit. 2015-03-15]. Dostupné z: http://www.root.cz/bezpecnost/