DISTRIBUTED BRUTE FORCE ATTACKS PROTECTION

Jan Richter
Master Degree Programme (2), FIT BUT
E-mail: xricht14@stud.fit.vutbr.cz

Supervised by: Petr Lampa
E-mail: lampa@fit.vutbr.cz

ABSTRACT

This project deals with analysis of brute force attacks focused on breaking authentication of common services (especially ssh) of Linux and xBSD operating systems. It also examines real attacks, actual tools and ways of detection of these attacks. Finaly there are designed new mechanisms of coordination and evaluation distributed brute force attacks in distributed environment.

1 ÚVOD

Rychlé rozrůstání Internetu v posledních letech spolu s množstvím nových služeb a informací přináší také velké množství nových nástrah a nebezpečí, která na uživatele v síti čekají. Může jít o různé formy sociálního inženýrství, viry, červy, trojské koně, podvržené odpovědi DNS serverů, odposlech dat na nezabezpečených sítích nebo útoky hrubou silou, kdy se útočník pokouší o přihlášení do systému pomocí tipovaní uživatelského jména a hesla. Právě tímto typem útoku a ochranou před ním se tato práce zabývá.

2 ANALÝZA

Pro analýzu útoků byly použity logy ssh démona z několika různých serverů připojených různými poskytovateli na různých místech Evropy, které byly nasbírané za období posledních téměř dvou let. Dále byly výsledky porovnávány s výsledky podobných analýz útoků hrubou silou na ssh[1].

Podrobné výsledky analýzy jsou k dispozici v originále mé diplomové práce.

Existuje velké množství nástrojů, které se snaží problém útoků hrubou silou řešit (blíže byly zkoumány *sshguard*, *fail2ban* a *DenyHosts*). Všechny pracují na v podstatě stejném principu, čtou logy ssh démona (a případně dalších služeb) a pokud naleznou předem stanovený počet neúspěšných pokusů o přihlášení v předem stanoveném časovém rozmezí z jedné ip adresy, vyhodnotí tuto ip adresu jako útočníka a pomocí dostupných nástrojů (iptables, ipfw, tcpwrapper a pod.) zablokují útočníkovi další přístup na předem stanovenou dobu.

Hlavními nedostatky těchto nástrojů jsou:

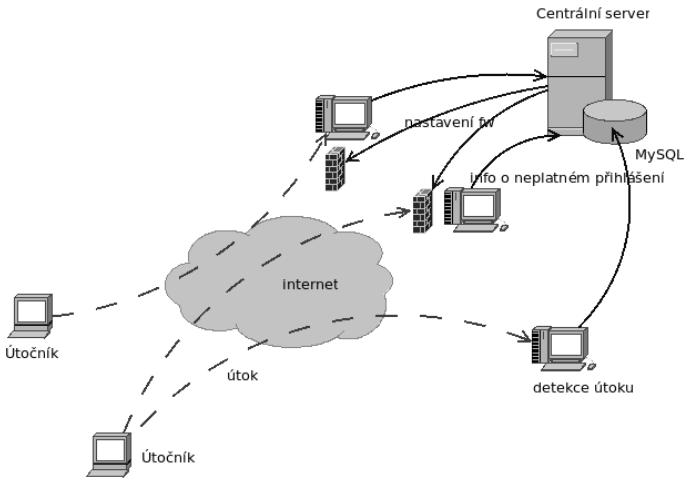
- **běží pouze na jednom stroji** (některé) - omezené možnosti rozpoznání útoků

- nebo naopak **běží globálně** (některé) - probíhá celosvětová výměna odhalených útočníků, ale v tomto měřítku nelze účinně uhlídat podvržené ip adresy
- **neúčinné sdílení informací o útocích** - přestože některé systémy pro detekci a blokování útoků provádějí výměnu informací o zablokovaných adresách, vyhodnocení probíhá vždy pouze na jednotlivých stanicích a nelze proto efektivně odhalit všechny útoky, které by se daly odhalit porovnáváním informací z více stanic vzájemně
- **detekují útoky pouze na základě ip adresy** - často jsou vedeny distribuované útoky, které ale spojuje například použité uživatelské jméno
- **nespojují útočníky do skupin** - neumožňují tak detekci distribuovaných útoků, vhodným vylepšením by bylo inteligentní vytváření vztahů mezi jednotlivými útočícími ip adresami pro pozdější blokování celých skupin na základě několika málo shodných adres

3 NAVRHOVANÉ ŘEŠENÍ

Navrhované řešení má za úkol odstranit uvedené nedostatky současných nástrojů pro detekci útoků hrubou silou. Na jednotlivých počítačích budou detekovány útoky na základě analýzy logů systémových služeb. Informace o jednotlivých bezpečnostních incidentech budou dále předávány na centrální server, na kterém budou ukládány do MySQL databáze, za pomocí které budou dále vyhodnocovány útoky, které by nebylo možné detekovat pomocí pouze jednoho počítače.

Centrální server s databází také bude poskytovat aktuální pravidla pro nastavení firewallu jednotlivých svých klientů. Jednoduché schéma systému je naznačeno na obrázku 1.



Obrázek 1: Schéma systému

Jelikož lze předpokládat, že velké distribuované útoky jsou prováděny z rozsáhlých botnetů, bude se server snažit identifikovat jednotlivé sítě útočníků a spojovat je do skupin, aby na základě příštích pokusů o přihlášení bylo možno zablokovat všechny útočníky ze skupiny bez ohledu na to, zda se pokusí o přihlášení.

Serverová část tedy sestává z MySQL databázového serveru, na který budou klienty zapisovány jednotlivé pokusy o přihlášení, a ty budou pomocí databázových triggerů dále vyhodnocovány a

porovnávány s ostatními záznamy. Při vyhodnocení ip adresy jako útočníka, bude tato zapsána do tabulky blokovaných počítačů včetně údaje od kdy do kdy má být klienty blokována. Doba zablokování dané ip adresy je konfigurovatelná a volitelně také může docházet k prodlužování této doby při opakovaném zablokování a/nebo může být po nastaveném počtu útoků zapsána do tabulky permanentně blokovaných ip adres.

Jak vyplývá z předešlého odstavce, na serveru tedy existuje tabulka dočasně zablokovaných ip adres (*banlist*) a permanentně zablokovaných ip adres (*blacklist*), kromě nich je zde ještě tabulka důvěryhodných ip adres (*whitelist*), do které může správce zadat ip adresy, které nesmí být zablokovány nikdy. Klient si tyto tabulky po svém spuštění přečte a nakonfiguruje podle nich firewall počítače. Po dobu svého běhu si pak se serverem průběžně vyměňuje informace a aktualizuje nastavení firewallu.

Konfigurace systému se nachází na dvou místech. Každý klient potřebuje konfigurační soubor, ve kterém jsou uvedeny údaje pro přihlášení k serveru a údaj zda mají být ostatní položky konfigurace získány ze serveru nebo má být použit zbytek konfiguračního souboru. Volitelně jsou zde potom položky obsahující regulární výrazy pro parsování logů, nastavení používaného typu firewallu a pod.

Čtení logu démona hlídané služby je inspirováno nástrojem *sshguard*, je tedy zapotřebí nakonfigurovat systémový logger tak, aby zapisoval (také) na standardní vstup programu. Tímto je možno se vyhnout zbytečnému pollingu nebo používání dalších nástrojů jako file alternation monitor nad logem zapisovaným na disk. Dále tento přístup umožní rychlejší reakci při volitelně nastavitelném lokálním vyhodnocení útoků.

4 ZÁVĚR

Tato implementace systému by oproti stávajícím implementacím měla umožnit pružnější zabezpečení středně velkých počítačových sítí. Momentálně existují implementace, které buď chrání jeden samostatný počítač, nebo sdílejí informace s celým světem, ale neexistuje žádný mezistupeň. Dále by měla umožnit administrátorovi sítě jednodušší centrální konfiguraci celého systému a v neposlední řadě pokročilejší detekci a zpracování distribuovaných útoků.

PODĚKOVÁNÍ

Tato práce vznikla částečně za podpory grantu VUT FIT, FIT-S-10-2 a specifického výzkumu MSM0021630528.

REFERENCE

[1] Owens, J., Matthews, J.: A Study of Passwords and Methods Used in Brute-Force SSH Attacks, Department of Computer Science Clarkson University, 2008, Potsdam, New York

[2] Malecot, E.L, Hori, Y., Sakurai, K., Ryou, J.C., Lee, H.:(Visually) Tracking Distributed SSH Brute Force Attacks?, 3rd Int'l Joint Workshop on Information Security and Its Applications (IJWISA), pp. 1-8, February 2008, Korea University, Seoul, Korea