SSH szerver biztonságának javítása

Írta AndrzejL

Amikor legutóbb állítottam a szerveremet, több száz bejegyzést találtam a /var/log/auth.log fájlban, sikertelen belépési kísérletekkel, különféle IP-címekről és bejelentkezési nevekkel. Csak találgattam, mi lehet ez, addig amíg nem láttam ezt a videót:

SSH Login törése - Videó

Tanulság? Legalább egy bot van (hiú ábránd...), amelyik az egész IP-tartományt szkenneli, nyitott 22-es portot keresve, és valamilyen brute-force eszközzel próbálja feltörni azt. Hát ez nem valami biztató megállapítás az SSH használók számára.

Mit lehet ezzel kezdeni? Három dolgot tehetünk.

A) Megtiltani a root bejelentkezését.

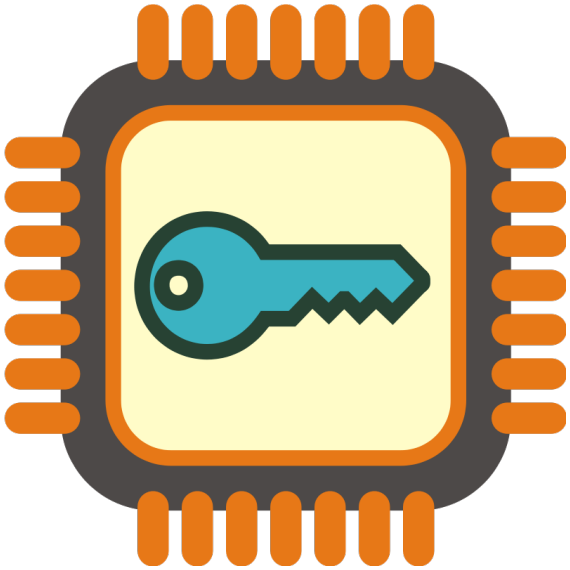
B) Synaptic-kal telepíteni a fail2ban-t.

C) Az SSH port-ot 22-ről 10100 fölöttire cserélni.

Én mindet alkalmazom.

A root bejelentkezésének letiltása kötelező. A root az egyetlen biztos bejelentkező név a Linux alapú rendszerekben. A támadóknak nem kell találgatniuk. Biztosan ott van. Már csak a jelszót kell kitalálniuk. A root belépés tiltása arra kényszeríti, hogy találgassa a belépőnevet és a jelszót egyaránt. Ez így sokkal nehezebb nekik és ez a lényeg.

A PCLinuxOS sajátos beállításokat alkalmaz a config fájlokban. Az /etc/ssh/denyusers-be ha belenézel láthatod, hogy tartalmazza a root kifejezést.



Ez a beállítás megakadályoz minden SSH-ra root-kénti bejelentkezési kísérletet, miközben a kedvedért megengedi a su parancs használatát. Miért? Még ha ismeri is a támadó a root jelszavát, akkor sem képes belépni. Ugyanakkor a rendszerbe SSH-n már bejelentkezett felhasználó megemelheti a jogosultságait a su paranccsal. Ez egyszerre biztonságos és kényelmes. Néha szükség van root jogra, így a PCLinuxOS lehetővé teszi root jog elérését, tehát felhasználóként is be kell jelentkezni és tudni a root-jelszót is a gép fölött teljes ellenőrzést elnyeréséhez.

A másik módszer – Fail2ban – (megtalálod a tárolóinkban) egy tűzfalszabállyal egészíti ki, ami blokkol minden belépési kísérletet az SSH-ra, amennyiben X számú sikertelen kísérletet észlel Y időn belül. Például – az xxx.yyy.zzz.uuu gép próbált bejelentkezni jake, ann és mark néven háromszor 20 percen belül, ezért egy órára letiltotta.

Az X és Y értékét az /etc/fail2ban/jail.conf beállító fájlban lehet megadni.

Emellett, ha beállítod a működő helyi mail szerveredet, akkor a fail2ban a eseményekről értesítést küld.

A fail2ban az SSH mellett védi az (S)FTP-t és az azonosítást alkalmazó protokollokat. Kiváló eszköz.

Továbbá megváltoztatod az SSH szerver portját. A következő videó megmutatja hogyan kell csinálni.

Az SSH Szerver portjának megváltoztatása - Videó.

Miért változtassuk meg a portot és miért 10100 fölé? Az alapbeállítás szerinti port a 22-es. Az összes szkriptelő kölyök, névkereső csúcsfej a bot-jában ezt a portot használja. Még ha okos is a szkriptes fiú, és az IP címedet olyan portszkennerrel támadja mint az nmap, alapbeállításból csak az első 10000 port-ot fogja látni. Az SSH-t e fölé állítva a portszkenner SEMMIT, NULLÁT, SZEMETET, stb.-t talál. Ha ennél is okosabb a kölyök, és mind a 65 ezer portot szkenneli, a nyitott port ismeretlen szolgáltatásként jelenik meg. Néhány további kapcsolót is be kell állítania az nmap-en, hogy kiderüljön, ez egy SSH-szerver. A kölykök többnyire lusták, és a könnyebb préda után néznek. Egy kicsit jobban megnehezíteni a dolgot áldás a biztonságod szempontjából.

Eddig ezt a három dolgot tanultam meg az SSH-szerver biztonságának javítását illetően. Lehet, hogy a jövőben valami újat is tanulok, akkor azt egy újabb cikkben ismertetem.

Vésd az eszedbe, hogy még a leggyengébb védelem is jobb mint a védelem teljes hiánya.