fail2ban

(shorty)

Worum gehts?

- Was ist fail2ban und wie funktioniert das?
- Wie ich darauf gekommen bin und was es mir gebracht hat.
- Was man sonst noch so damit machen kann ...

Was ist fail2ban

- fail2ban ist ein in Python geschriebenes IPS
- Eher rudimentäres IPS (reicht auf jeden Fall für Scriptkiddies und viele automatisierte Angriffsversuche)
- Client zum Steuern, Server der die Arbeit macht und Hilfsprogramm zu Regexp testen

Wie funktioniert fail2ban

- Liest Log-Dateien aus und überprüft auf verdächtiges Verhalten von Quell-IPs
- Wird ein Angriffsversuch festgestellt wird die IP via "iptables" oder über das Routing mit "ip" für einen festgelegten Zeitraum gebannt (gesperrt)
- Nach einem definierten Zeitraum wird die IP wieder freigeschaltet

Wie funktioniert fail2ban

- Whitlisten von IPs ist möglich
- Zu beobachtende Dienste werden i.d.R in sog. Jails organisiert
  - Filter: Enthalten Filterregeln (Regexp) um in den Logfiles bestimmte Verhaltensmuster zu identifizieren und IP-Adressen zu extrahieren
  - Actions: Sind die Befehle die ausgeführt werden um i.d.R. IPs zu sperren

Wie bin ich auf fail2ban gekommen bin

- Problem: Täglich mehrere Tausend SSH-Zugriffsversuche auf meine Server, teilweise im fünfstelligen Bereich
  - Benutzernamen: root, pi, user, ubuntu, ...
  - Diese Fehlversuche von Anmeldungen werden protokolliert(!), die logfiles sind dann damit "zugemüllt"

Wie bin ich auf fail2ban gekommen bin

- Hab da mal was von Kollegen drüber gehört und google sagts auch :-D
- fail2ban bietet hier eine fast vollständig vorkonfigurierte Lösung (debian GNU/Linux)
- OK, ein anderer SSH-Port und entfernen "schwacher" Cyphers hättens wohl auch getan
- Mit fail2ban werden SMTP, IMAP, HTTPS, etc. gleich mit "abgesichert"

Was hats mir gebracht?

- Einfacher Schutz meiner Rechner (automatisierte Angriffen und Scriptkiddies)
- Lesbarere Logfiles - da steht jetzt das wesentliche drin ;-)
- Eine weitere Komponente in meinem Sicherheitskonzept (-wahnsinn)

Was man sonst noch damit machen kann...

- Samba-Shares vor Krypto-Trojanern schützen (Backup ist immer noch erforderlich!)
  - https://www.heise.de/security/artikel/Erpressungs-Trojaner-wie-Locky-aussperren-3120956.html
- Verteiltes fail2ban-System um mehrere Rechner zeitgleich in einem Netzwerk zu schützen (interessant bei zentraler Benutzerverwaltung)
  - https://www.blackhillsinfosec.com/configure-distributed-fail2ban/
    - Danke Martin für den Tipp :-)

… und wenn man sich versehentlich selbst ausgesperrt hat?

- Dann kann man mit "Port knocking" sich wieder freischalten
  - https://wiki.archlinux.org/index.php/Port_knocking
- Oder einfach 10 Minute warten und einen Kaffee trinken
- Falls man noch eine SSH-Sitzung offen hat kann man den Bann mit `fail2ban-client set [JAILNAME] unbanip [IP]` wieder aufheben

Lesenswertes

- https://wiki.ubuntuusers.de/fail2ban/
- https://www.fail2ban.org/wiki/index.php/Main_Page
- https://www.heise.de/security/artikel/Erpressungs-Trojaner-wie-Locky-aussperren-3120956.html
- https://www.blackhillsinfosec.com/configure-distributed-fail2ban/
- https://wiki.archlinux.org/index.php/Port_knocking
- und natürlich `man fail2ban`