BUSINESS SCHOOL by EEBU	Procédure de mise en place Fail2Ban	Document Doc- Fail2Ban	
		Date 04/12/2024	Version 0.10
		Rédacteur : KORKMAZ Eren	

Procédure Interne

Version	Date	Commentaires	Rédacteur
0.10	04/12/2024	Création de la procédure	Korkmaz Eren

BUSINESS SCHOOL by 3SIS	Procédure de mise en place Fail2Ban	Document Doc- Fail2Ban	
		Date 04/12/2024	Version 0.10
		Rédacteur : KORKMAZ Eren	

Table des matières

1- Introduction

1.1 Qu’est-ce que Fail2Ban ?

Fail2Ban est un outil essentiel pour renforcer la sécurité des serveurs en bloquant les adresses IP des attaquants après des tentatives répétées de connexion échouées.

1.2 Principales caractéristiques de Fail2Ban

Fail2Ban est un outil puissant et flexible pour protéger un serveur contre des attaques répétées, comme celles par force brute. Grâce à sa capacité à surveiller différents services, à bloquer automatiquement les IP malveillantes et à être configuré de manière personnalisée, il est très populaire parmi les administrateurs de serveurs pour renforcer la sécurité des systèmes en ligne.

2- Procédure

2.1 L’installation

BUSINESS SCHOOL by EEMI	Procédure de mise en place Fail2Ban	Document Doc- Fail2Ban	
		Date 04/12/2024	Version 0.10
		Rédacteur : KORKMAZ Eren	

```
eren@debianattaquant:~$ sudo apt install nmap hydra fail2ban -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  firebird3.0-common firebird3.0-common-doc fontconfig fontconfig-config fonts-dejavu-core
  i965-va-driver intel-media-va-driver libaom3 libapr1 libaprutil1 libavcodec59 libavutil57 libblas3
  libbson-1.0-0 libcairo-gobject2 libcairo2 libcodec2-1.0 libdatrie1 libdav1d6 libdeflate0
  libdrm-amdgpu1 libdrm-intel1 libdrm-nouveau2 libdrm-radeon1 libfbclient2 libfontconfig1
  libfreerdp2-2 libfribidi0 libgdk-pixbuf-2.0-0 libgdk-pixbuf2.0-bin libgdk-pixbuf2.0-common libgl1
  libgl1-mesa-dri libglapi-mesa libglvnd0 libglx-mesa0 libglx0 libgomp1 libgraphite2-3 libgsm1
  libharfbuzz0b libhashkit2 libhwy1 libidn12 libigdgmm12 libjbig0 libjpeg62-turbo libjxl0.7
  liblcms2-2 liblerc4 liblinear4 libllvm15 liblua5.3-0 libmariadb3 libmemcached11 libmfx1
  libmongoc-1.0-0 libmongocrypt0 libmp3lame0 libnuma1 libogg0 libopenjp2-7 libopus0 libpango-1.0-0
  libpangocairo-1.0-0 libpangoft2-1.0-0 libpcap0.8 libpciaccess0 libpcre3 libpixman-1-0 libpq5
  librav1e0 librsvg2-2 librsvg2-common libsensors-config libsensors5 libserf-1-1 libshine3
  libsnappy1v5 libsoxr0 libspeex1 libssh-4 libsvn1 libsvtav1enc1 libswresample4 libswscale6
  libthai-data libthai0 libtheora0 libtiff6 libtommath1 libtwolame0 libutf8proc2 libva-drm2
  libva-x11-2 libva2 libvdpau-va-gl1 libvdpau1 libvorbis0a libvorbisenc2 libvpx7 libwebp7
  libwebpmux3 libwinpr2-2 libx11-xcb1 libx264-164 libx265-199 libxcb-dri2-0 libxcb-dri3-0
  libxcb-glx0 libxcb-present0 libxcb-randr0 libxcb-render0 libxcb-shm0 libxcb-sync1 libxcb-xfixes0
  libxfixes3 libxkbfile1 libxrender1 libxshmfence1 libxvidcore4 libxxf86vm1 libz3-4 libzvbi-common
  libzvbi0 lua-lpeg mariadb-common mesa-va-drivers mesa-vdpau-drivers mysql-common nmap-common
  ocl-icd-libopencl1 python3-pyinotify python3-systemd va-driver-all vdpau-driver-all whois
Paquets suggérés :
  mailx system-log-daemon monit sqlite3 hydra-gtk i965-va-driver-shaders libcuda1 libnvcuvid1
  libnvidia-encode1 freerdp2-x11 liblcms2-utils liblinear-tools liblinear-dev opus-tools
  librsvg2-bin lm-sensors speex ncat ndiff zenmap opencl-icd python-pyinotify-doc
  nvidia-vdpau-driver nvidia-tesla-440-vdpau-driver nvidia-tesla-418-vdpau-driver
  nvidia-legacy-390xx-vdpau-driver nvidia-legacy-340xx-vdpau-driver
Les NOUVEAUX paquets suivants seront installés :
  fail2ban firebird3.0-common firebird3.0-common-doc fontconfig fontconfig-config fonts-dejavu-core
  hydra i965-va-driver intel-media-va-driver libaom3 libapr1 libaprutil1 libavcodec59 libavutil57
  libblas3 libbson-1.0-0 libcairo-gobject2 libcairo2 libcodec2-1.0 libdatrie1 libdav1d6 libdeflate0
  libdrm-amdgpu1 libdrm-intel1 libdrm-nouveau2 libdrm-radeon1 libfbclient2 libfontconfig1
  libfreerdp2-2 libfribidi0 libgdk-pixbuf-2.0-0 libgdk-pixbuf2.0-bin libgdk-pixbuf2.0-common libgl1
  libgl1-mesa-dri libglapi-mesa libglvnd0 libglx-mesa0 libglx0 libgomp1 libgraphite2-3 libgsm1
  libharfbuzz0b libhashkit2 libhwy1 libidn12 libigdgmm12 libjbig0 libjpeg62-turbo libjxl0.7
  liblcms2-2 liblerc4 liblinear4 libllvm15 liblua5.3-0 libmariadb3 libmemcached11 libmfx1
  libmongoc-1.0-0 libmongocrypt0 libmp3lame0 libnuma1 libogg0 libopenjp2-7 libopus0 libpango-1.0-0
  libpangocairo-1.0-0 libpangoft2-1.0-0 libpcap0.8 libpciaccess0 libpcre3 libpixman-1-0 libpq5
  librav1e0 librsvg2-2 librsvg2-common libsensors-config libsensors5 libserf-1-1 libshine3
  libsnappy1v5 libsoxr0 libspeex1 libssh-4 libsvn1 libsvtav1enc1 libswresample4 libswscale6
```

```
eren@debianattaquant:~$ sudo nmap -sS -p- 192.168.25.12
Starting Nmap 7.93 ( https://nmap.org ) at 2024-12-04 10:31 CET
Nmap scan report for 192.168.25.12
Host is up (0.0034s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:CD:E5:9C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 8.68 seconds
eren@debianattaquant:~$
```

```
eren@debianattaquant:~$ sudo systemctl start ssh
eren@debianattaquant:~$
```

```
eren@debianattaquant:~$ sudo hydra -l eren -P /usr/share/wordlists/rockyou1.txt ssh://192.168.25.12
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-04 10:58:38
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 19 login tries (l:1/p:19), ~2 tries per task
[DATA] attacking ssh://192.168.25.12:22/
[22][ssh] host: 192.168.25.12   login: eren   password: 123456
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-04 10:58:45
eren@debianattaquant:~$
```

```
eren@debianattaquant:~$ sudo cp /etc/fail2ban/jail(conf,local)
-bash: erreur de syntaxe près du symbole inattendu « ( »
eren@debianattaquant:~$ sudo cp /etc/fail2ban/jail.local
cp: opérande de fichier cible manquant après '/etc/fail2ban/jail.local'
Saisissez « cp --help » pour plus d'informations.
eren@debianattaquant:~$ sudo cp /etc/fail2ban/jail.conf
cp: opérande de fichier cible manquant après '/etc/fail2ban/jail.conf'
Saisissez « cp --help » pour plus d'informations.
eren@debianattaquant:~$ sudo cd /etc/fail2ban/jail.conf
sudo: cd : commande introuvable
sudo: « cd » est une commande interne du shell, elle ne peut pas être exécutée directement.
sudo: l'option -s peut être utilisée pour exécuter un shell privilégié.
sudo: l'option -D peut être utilisée pour exécuter une commande dans un répertoire spécifique.
eren@debianattaquant:~$ sudo cp /etc/fail2ban/jail[conf,local]
eren@debianattaquant:~$
Saisissez « cp --help » pour plus d'informations.
eren@debianattaquant:~$ sudo cp /etc/fail2ban/jail.{conf,local}
eren@debianattaquant:~$ sudo touch /var/log/auth.log
eren@debianattaquant:~$ sudo systemctl restart fail2ban
eren@debianattaquant:~$
```

```
eren@debianattaquant:~$ sudo hydra -l eren -P /usr/share/wordlists/rockyou1.txt ssh://192.168.25.12
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics any
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-04 11:42:30
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce th
tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 19 login tries (l:1/p:19), ~2 tries per task
[DATA] attacking ssh://192.168.25.12:22/
[ERROR] could not connect to ssh://192.168.25.12:22 - Connection refused
```

2.2 Schéma réseau

BUSINESS SCHOOL	Procédure de mise en place Fail2Ban	Document Doc- Fail2Ban	
		Date 04/12/2024	Version 0.10
		Rédacteur : KORKMAZ Eren