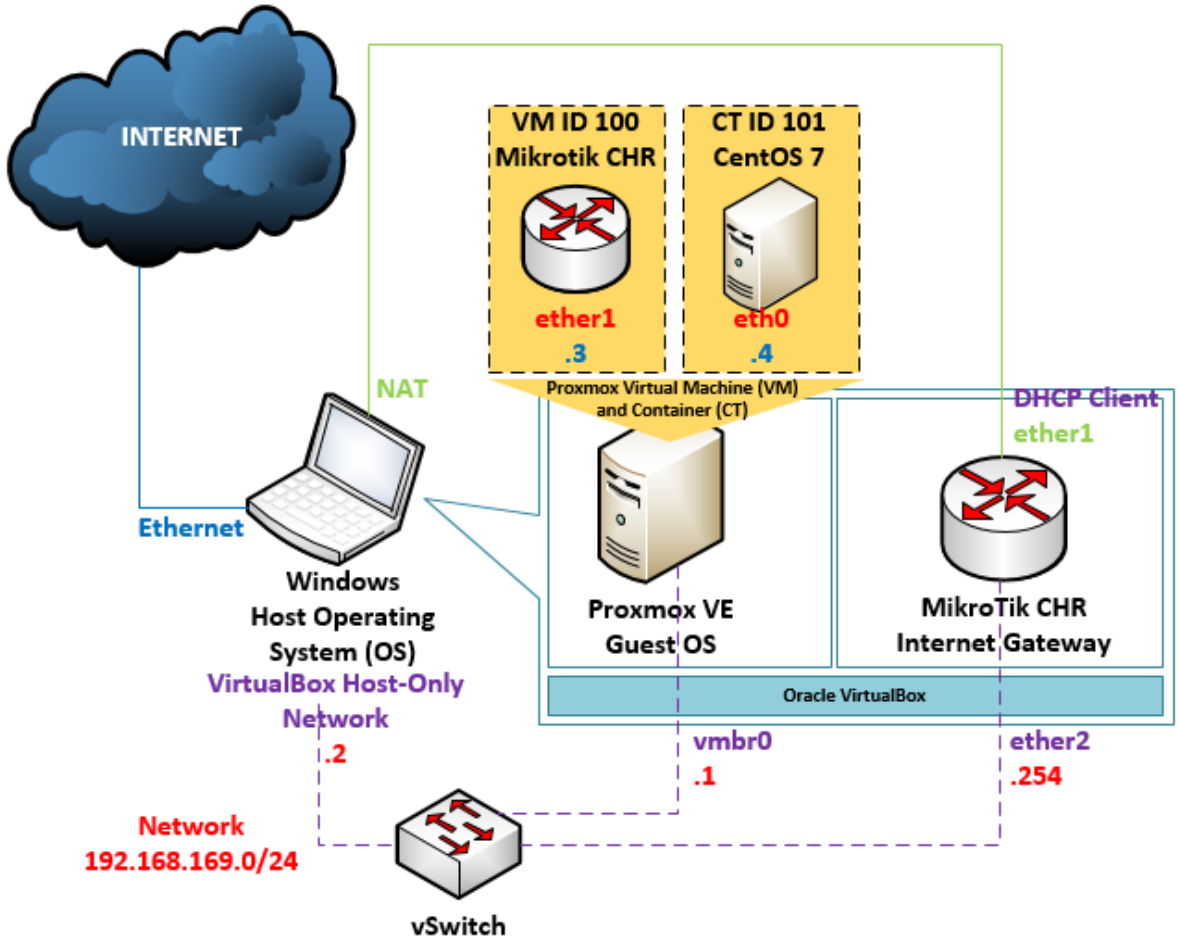
PROTEKSI BRUTE FORCE PADA PROXMOX VIRTUAL ENVIRONMENT (PVE) MENGGUNAKAN FAIL2BAN

Oleh I Putu Hariyadi (admin@iputuhariyadi.net)

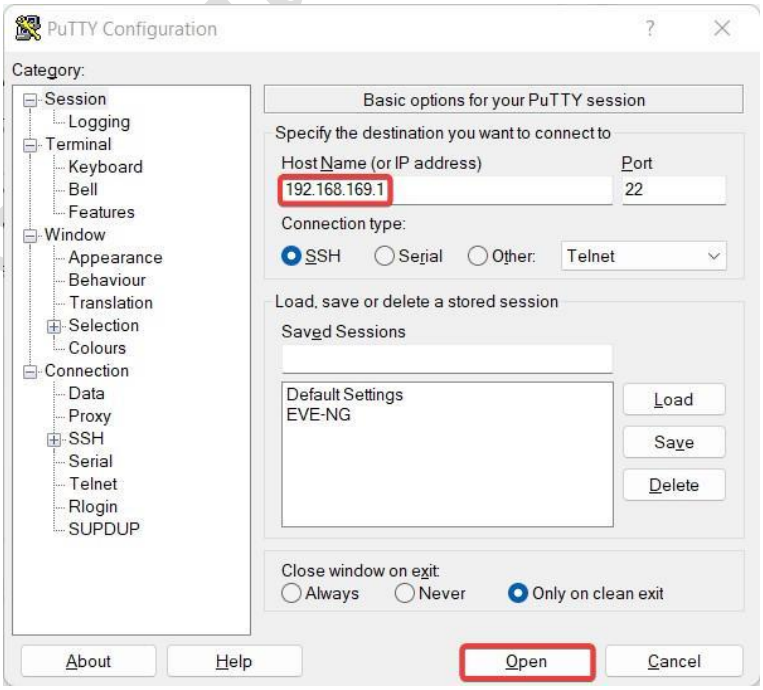
Fail2ban merupakan aplikasi yang dapat melakukan pemindaian (**scan**) *file log* dan melarang atau memblokir (**ban**) alamat **Internet Protocol (IP)** yang menunjukkan tanda-tanda berbahaya berdasarkan pada seperangkat aturan (**rules**) dan pemfilteran (**filter**) yang dapat dikelola. *Fail2ban* dapat diterapkan pada **server Proxmox Virtual Environment (PVE)** untuk memproteksi terhadap serangan *brute force* pada layanan seperti *Secure Shell (SSH), HyperText Transfer Protocol (HTTP)* dan *HyperText Transfer Protocol Secure (HTTPS)*. Rancangan jaringan yang digunakan untuk mensimulasikan proteksi *brute force* pada *server Proxmox*, seperti terlihat pada gambar berikut:



Terlihat pada *Windows Host Operating System (OS)* diinstalasi *Oracle VirtualBox* dan didalamnya dibuat 2 (dua) *Guest Machine* atau *Virtual Machine (VM)* yaitu **Proxmox VE** dan **Mikrotik CHR**. **VM Mikrotik CHR** pada *VirtualBox* difungsikan sebagai *Internet Gateway* sehingga menjembatani berbagi pakai koneksi Internet baik untuk *server Proxmox* maupun VM dan Container (CT) didalamnya. Alamat *network* yang digunakan untuk pengalamatan adalah **192.168.169.0/24**. Alamat *Internet Protocol (IP)* pertama dari alamat *network* tersebut yaitu 192.168.169.1/24 dialokasikan untuk *interface vmbr0* di *server Proxmox*. Sedangkan alamat IP kedua yaitu 192.168.169.2/24 dialokasikan untuk *interface VirtualBox Host-Only Network* di *Windows*. Sebaliknya alamat IP terakhir yaitu 192.168.169.254/24 dialokasikan untuk *interface ether2* di VM *Mikrotik CHR Internet Gateway*. Selain itu pada *VM Mikrotik CHR Internet Gateway* juga memiliki *interface ether1* diatur sebagai *DHCP Client*. Terakhir untuk VM dan CT pada server Proxmox masing-masing dialokasikan alamat IP 192.168.169.3/24 dan 192.168.169.4/24.

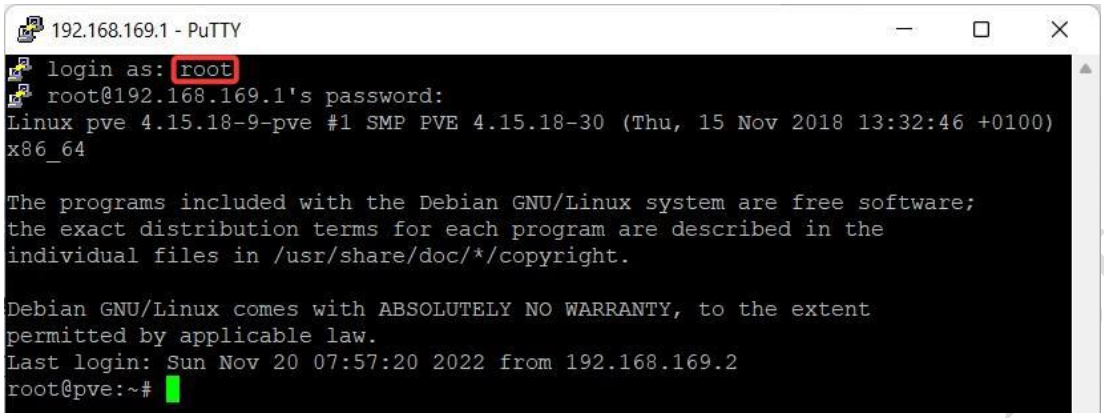
Adapun langkah-langkah dalam menginstalasi dan mengkonfigurasi *fail2ban* untuk memproteksi *brute force* pada *server Proxmox* melalui SSH adalah sebagai berikut:

1. Jalankan aplikasi *SSH Client*, sebagai contoh menggunakan *Putty*. Tampil kotak dialog *Putty Configuration*. Pada isian **Host Name (or IP Address)**, masukkan alamat IP dari *Server Proxmox* yaitu **192.168.169.1**, seperti terlihat pada gambar berikut:



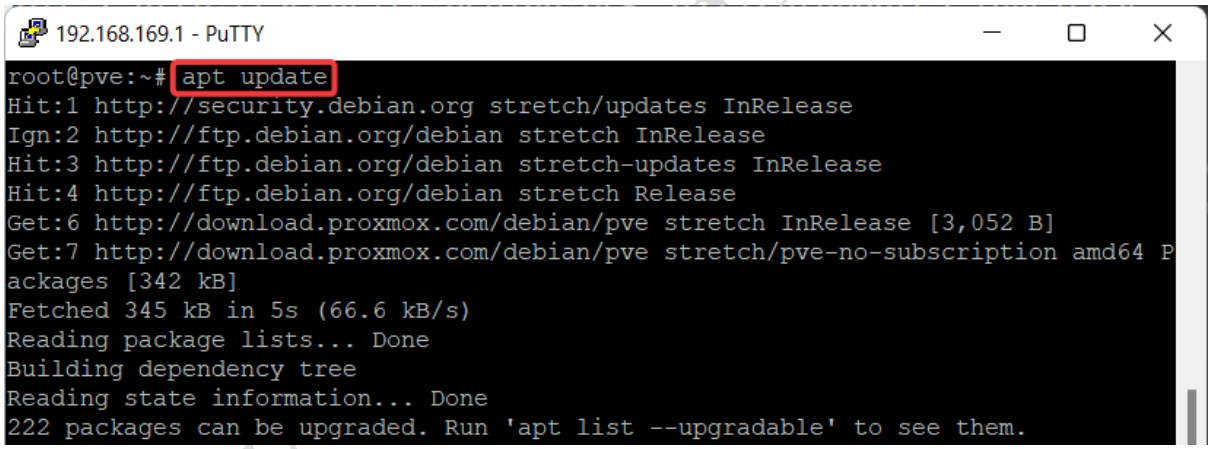
   Klik tombol **Open**.

2. Tampil kotak dialog *Putty* yang meminta pengguna untuk melakukan proses otentikasi login ke *Server Proxmox*, seperti terlihat pada gambar berikut:



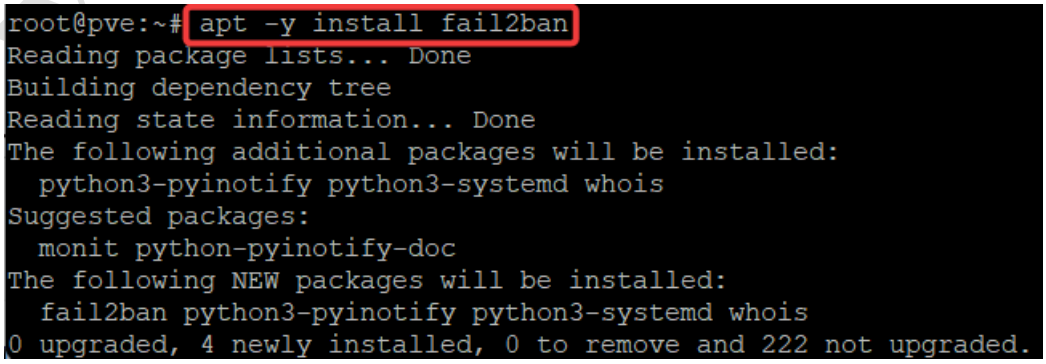
Pada inputan **login as:,** masukkan "**root**" dan tekan tombol **Enter**. Selanjutnya tampil inputan **password:**, masukkan "**12345678**" dan tekan tombol **Enter**. Apabila proses otentikasi berhasil dilakukan maka akan tampil *shell prompt* #.

3. Memperbaharui *server Proxmox* dengan mengeksekusi perintah "`apt update`".

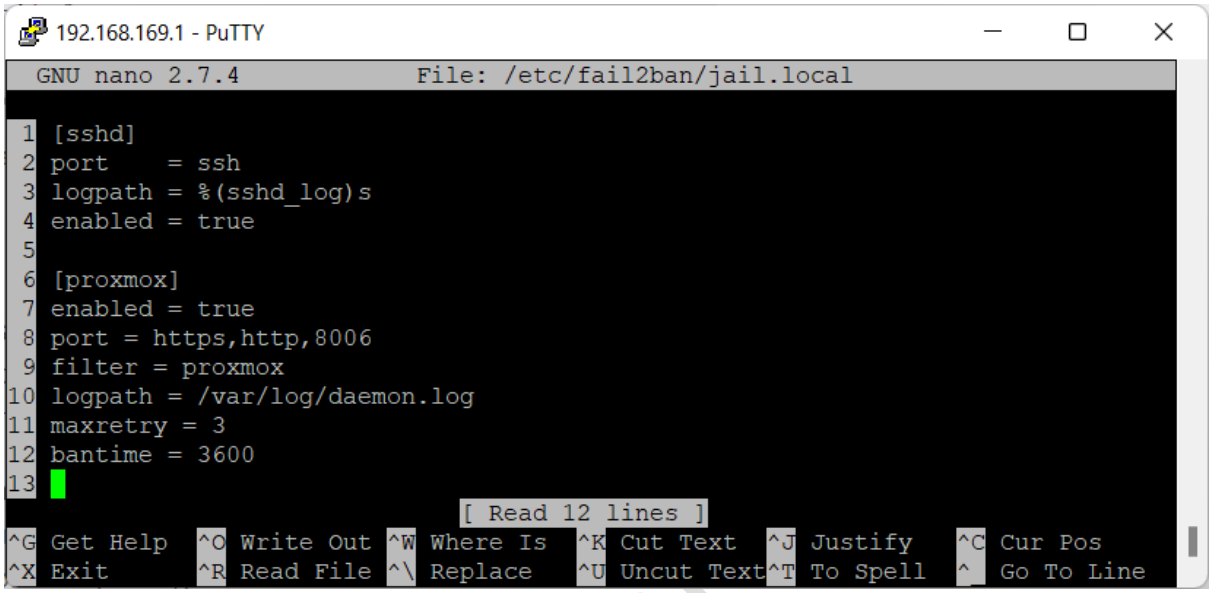


Tunggu hingga proses pembaharuan selesai dilakukan.

4. Menginstalasi paket aplikasi **fail2ban** dengan mengeksekusi perintah "`apt -y install fail2ban`".



5. Membuat *file* `jail.local` yang menampung konfigurasi dari **fail2ban server** terkait pemblokiran serangan **brute force** pada **port** dari layanan **SSH**, **HTTPS** dan **HTTP** serta **WEBGUI Proxmox** dan disimpan di direktori "`/etc/fail2ban`" dengan mengeksekusi perintah "`nano -l /etc/fail2ban/jail.local`".



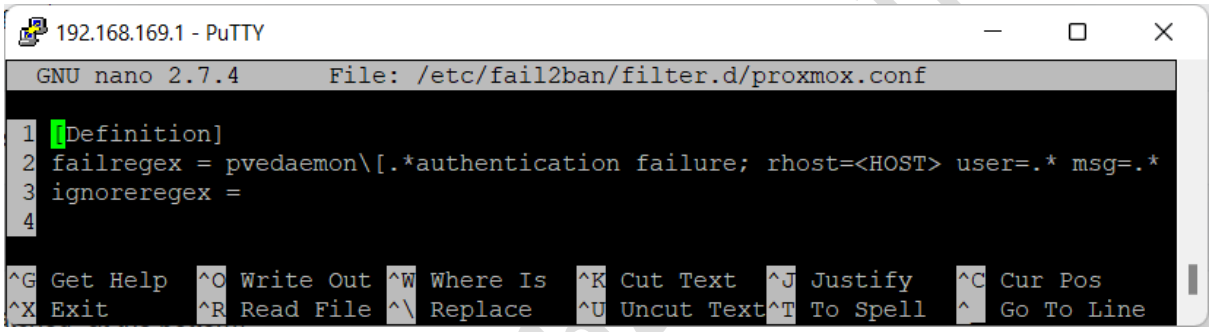
Baris pertama sampai dengan ke empat merupakan *section* (bagian) dengan nama "**sshd**" yang merupakan konfigurasi *jail* terkait layanan **sshd**. Baris kedua yaitu `port = ssh` digunakan untuk merujuk ke layanan `ssh` dengan menggunakan nama dari *service*-nya. Sedangkan baris ketiga yaitu `logpath` digunakan untuk menentukan lokasi log yang digunakan. Terakhir baris ke empat yaitu **enabled = true** digunakan untuk mengaktifkan *jail*.

Baris ke enam hingga ke duabelas merupakan konfigurasi *jail* terkait layanan **proxmox**. Diawali dengan nama *section* yaitu **`proxmox`** di baris ke enam. Baris ketujuh `enabled = true` digunakan untuk mengaktifkan *jail*. Baris ke delapan `port = https,http,8006` digunakan untuk merujuk ke layanan **HTTPS, HTTP** menggunakan nama *service*-nya dan **WEBGUI Proxmox** yang menggunakan nomor **port 8006**. Baris ke Sembilan filter=proxmox menentukan nama dari *file* yang ditemukan di direktori **/etc/fail2ban/filter.d** yang memuat informasi terkait *fail regex* untuk melakukan *parsing log* dengan tepat. Baris ke sepuluh yaitu `logpath = /var/log/daemon.log` merupakan lokasi dari *file log*. Sedangkan baris ke sebelas **maxretry=3** digunakan untuk menentukan jumlah kecocokan atau nilai penghitung yang

memicu tindakan pelarangan pada IP yaitu 3 (tiga). Terakhir baris ke duabelas yaitu **bantime=3600** digunakan untuk menentukan durasi waktu dalam detik untuk alamat IP tersebut diblokir (*banned*) yaitu 60 menit.

Simpan perubahan dengan menekan tombol **CTRL+O** dan tekan **Enter**. Tekan tombol **CTRL+X** untuk keluar dari editor *nano*.

6. Membuat *file* `proxmox.conf` yang memuat pola (**pattern**) atau **regular expression** terkait bagaimana menemukan *event* atau peristiwa pada *file log* yaitu terkait usaha kegagalan login dan disimpan di direktori "`/etc/fail2ban/filter.d`" dengan mengeksekusi perintah "`nano -l /etc/fail2ban/filter.d/proxmox.conf`".



Baris pertama merupakan **section Definition**. Sedangkan baris kedua, **failregex** digunakan untuk mencocokkan dengan teks yang ditulis oleh **Proxmox** ke *file log* dengan nama "**daemon.log**" ketika terdeteksi kegagalan *login*. Nilai dari **rhost** yaitu **<HOST>** menampung alamat IP dari *remote host* yang gagal melakukan *login* sehingga nilai tersebut dijadikan acuan oleh *fail2ban* untuk melakukan pemblokiran. Terakhir baris ketiga, **ignoreregex** digunakan mengidentifikasi entri *log* yang harus diabaikan oleh *Fail2Ban*, meskipun cocok dengan *failregex*.

Simpan perubahan dengan menekan tombol **CTRL+O** dan tekan **Enter**. Tekan tombol **CTRL+X** untuk keluar dari editor *nano*.

7. Merestart *service fail2ban* agar perubahan konfigurasi yang telah dilakukan berdampak dengan mengeksekusi perintah "`systemctl restart fail2ban`".

```
root@pve:~# systemctl restart fail2ban
```

8. Memverifikasi status *service fail2ban* dengan mengeksekusi perintah "`systemctl status fail2ban`".

```
root@pve:~# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset
     Active: active (running) since Sun 2022-11-20 09:19:12 WITA; 9s ago
       Docs: man:fail2ban(1)
    Process: 27154 ExecStop=/usr/bin/fail2ban-client stop (code=exited, status=0/
    Process: 27162 ExecStart=/usr/bin/fail2ban-client -x start (code=exited, statu
   Main PID: 27186 (fail2ban-server)
      Tasks: 5 (limit: 4915)
     Memory: 10.6M
        CPU: 3.556s
     CGroup: /system.slice/fail2ban.service
             └─27186 /usr/bin/python3 /usr/bin/fail2ban-server -s /var/run/fail2ba

Nov 20 09:19:11 pve systemd[1]: Starting Fail2Ban Service...
Nov 20 09:19:12 pve fail2ban-client[27162]: 2022-11-20 09:19:12,349 fail2ban.se
Nov 20 09:19:12 pve fail2ban-client[27162]: 2022-11-20 09:19:12,354 fail2ban.se
Nov 20 09:19:12 pve systemd[1]: Started Fail2Ban Service.
```

9. Memverifikasi *service fail2ban* aktif ketika *booting server Proxmox* dengan mengeksekusi perintah "`systemctl is-enabled fail2ban`".

```
root@pve:~# systemctl is-enabled fail2ban
enabled
```

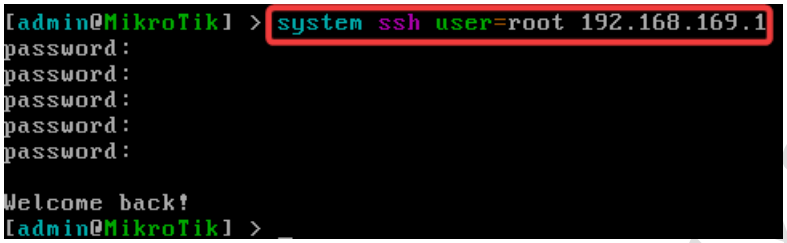
10. Memverifikasi apakah **ban** terkait **sshd** telah berfungsi dengan mengeksekusi perintah "`fail2ban-client status sshd`".

```
root@pve:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```

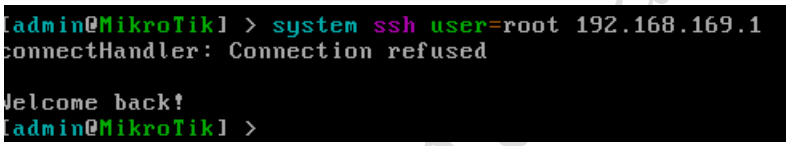
11. Memverifikasi apakah **ban** terkait **proxmox** telah berfungsi dengan mengeksekusi perintah "`fail2ban-client status proxmox`".

```
root@pve:~# fail2ban-client status proxmox
Status for the jail: proxmox
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/daemon.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```

12. Menampilkan informasi terkait **log** dari **fail2ban** yang tersimpan di *file* **/var/log/fail2ban.log** dengan mengeksekusi perintah "`tail /var/log/fail2ban.log`".
13. Memverifikasi hasil konfigurasi **fail2ban** dengan melakukan ujicoba **brute force attack** terkait layanan **SSH** di **server Proxmox** melalui **VM Mikrotik CHR Internet Gateway** dengan mengeksekusi perintah "`system ssh 192.168.169.1 user=root`". Pada inputan **password:**, dengan sengaja masukkan sandi yang salah. Ulangi sampai 5 (lima) kali percobaan dan memunculkan pesan **Welcome back!** serta menunjukkan *prompt Mikrotik* kembali**,** seperti terlihat pada gambar berikut:

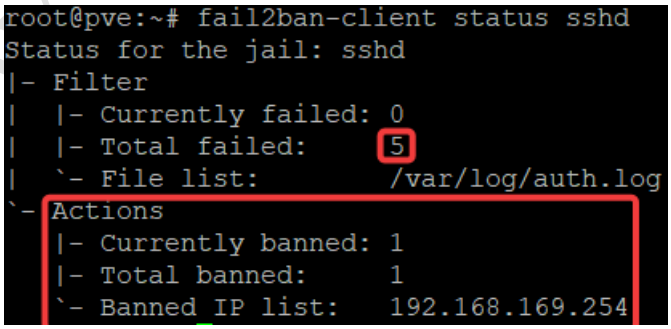


Sedangkan ketika dilakukan percobaan akses SSH kembali maka akan memunculkan pesan **connectHandler: Connection refused**, seperti terlihat pada gambar berikut:



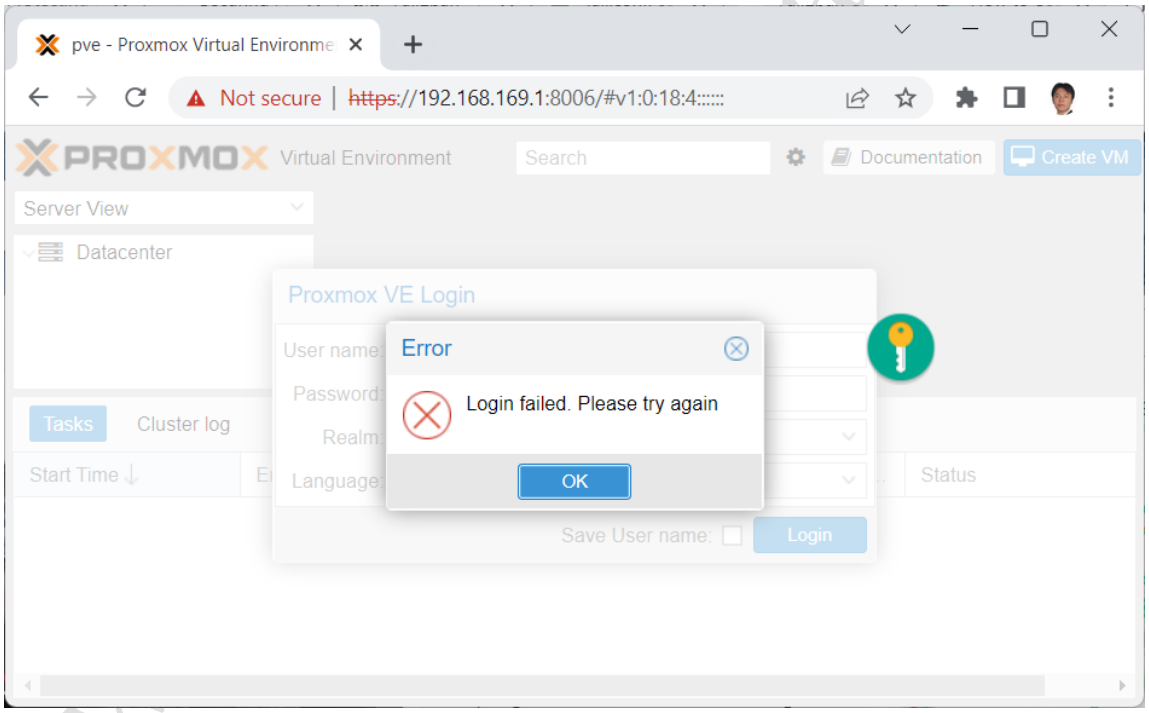
Ini menandakan bahwa koneksi SSH telah ditolak oleh **server Proxmox** karena secara *default* pada *file* konfigurasi **/etc/fail2ban/jail.conf** memuat maksimal percobaan yang diijinkan adalah 5 (**maxretry**) dan jika gagal akan melarang usaha SSH selama **600 detik** atau **10 menit (bantime)**.

14. Memverifikasi dampak dari **brute force attack** yang telah dilakukan ke layanan SSH sebelumnya melalui terminal (**Putty**) dari **server Proxmox** dengan mengeksekusi perintah "`fail2ban-client status sshd`".



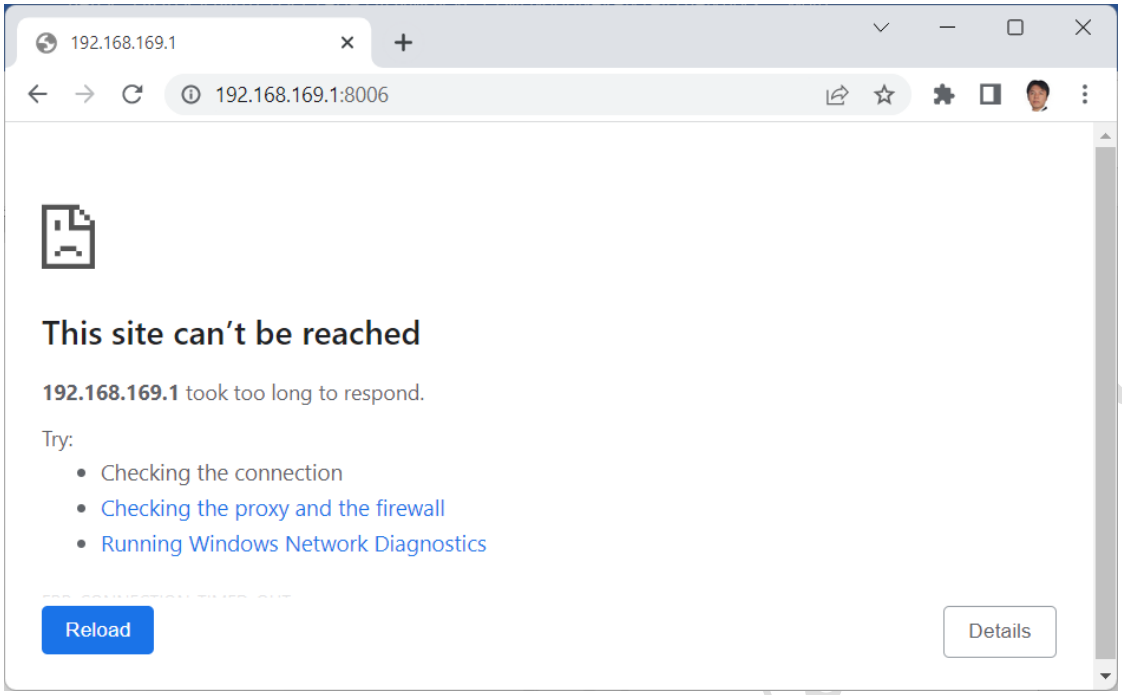
Terlihat nilai dari parameter **Total failed** pada bagian **Filter** adalah **5** sesuai dengan jumlah usaha **brute force attack** dari **VM Mikrotik CHR Internet Gateway**. Sedangkan pada parameter **Currently banned** dan **Total banned** di bagian **Actions** memperlihatkan jumlah yang di *banned* yaitu 1 (satu). Terakhir pada parameter **Banned_IP list** dari bagian **Actions**, terlihat nilai dari alamat IP yang di **banned** yaitu **192.168.169.254** yang merupakan alamat IP dari **VM Mikrotik CHR Internet Gateway**.

15. Memverifikasi hasil konfigurasi **fail2ban** dengan melakukan ujicoba **brute force attack** terkait layanan **WEBGUI** dari **server Proxmox** menggunakan *browser* pada **Windows** yaitu dengan mengakses alamat https://192.168.169.1:8006 sehingga memunculkan halaman **login** dari **Proxmox**. Lakukan usaha *login* menggunakan **user name "root"** dengan **password** yang sengaja disalahkan sehingga memunculkan pesan **Login failed. Please try again**, seperti terlihat pada gambar berikut**:**



Ulangi usaha *login* dengan *password* yang sengaja disalahkan tersebut sebanyak 3 (tiga) kali.

16. Melakukan percobaan akses kembali ke **WEBGUI Proxmox** melalui *browser* menggunakan alamat https://192.168.169.1:8006 maka akan memunculkan pesan **This site can't be reached**, seperti terlihat pada gambar berikut:



Ini menandakan bahwa koneksi ke **WEBGUI** telah ditolak oleh **server Proxmox** karena secara *default* pada *file* konfigurasi **/etc/fail2ban/jail.local** memuat maksimal percobaan yang diijinkan adalah 3 (**maxretry**) dan jika gagal akan melarang usaha akses melalui **HTTP, HTTPS dan 8006 (WEBGUI)** selama 3**600 detik** atau **60 menit (bantime)**.

17. Memverifikasi dampak dari **brute force attack** yang telah dilakukan ke layanan **WEBGUI** sebelumnya melalui terminal (**Putty**) dari **server Proxmox** dengan mengeksekusi perintah "`fail2ban-client status proxmox`".

```
root@pve:~# fail2ban-client status proxmox
Status for the jail: proxmox
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     4
|  `- File list:        /var/log/daemon.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.169.2
```

Terlihat nilai dari parameter **Total failed** pada bagian **Filter** adalah **4** sesuai dengan jumlah usaha **brute force attack** dari *browser* pada **system Windows**. Sedangkan pada parameter **Currently banned** dan **Total banned** di bagian **Actions** memperlihatkan jumlah yang di *banned* yaitu 1 (satu). Terakhir pada parameter **Banned_IP list** dari bagian **Actions**, terlihat nilai dari alamat IP yang di **banned** yaitu **192.168.169.2** yang merupakan alamat IP dari **system Windows**.

18. Membatalkan larangan (**unban**) untuk alamat IP **192.168.169.2** secara manual sebelum masa berakhir larangan sehingga **WEBGUI Proxmox** dapat diakses melalui **system Windows** dengan mengeksekusi perintah "`fail2ban-client set proxmox unbanip 192.168.169.2`", seperti terlihat pada gambar berikut:

```
root@pve:~# fail2ban-client set proxmox unbanip 192.168.169.2
192.168.169.2
```

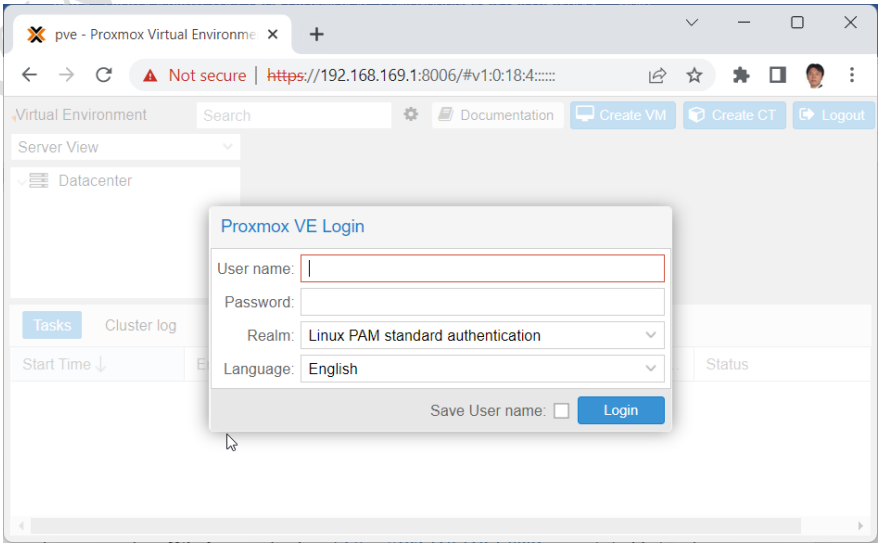
Parameter `proxmox` pada perintah tersebut merupakan nama dari **jail** yang terdapat pada *file* **jail.local**.

19. Memverifikasi konfigurasi **unban** yang telah dilakukan sebelumnya melalui *terminal* (**Putty**) dari **server Proxmox** dengan mengeksekusi perintah "`fail2ban-client status proxmox`".

```
root@pve:~# fail2ban-client status proxmox
Status for the jail: proxmox
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     4
|  `- File list:        /var/log/daemon.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
```

Terlihat pada parameter **Currently banned** dari bagian **Actions**, bernilai **0** (nol) dan pada parameter **Banned_IP list** sudah tidak terlihat alamat IP dari **system Windows** yang di **banned** sebelumnya yaitu **192.168.169.2**.

20. Memverifikasi hasil **unban** dengan mengakses kembali **WEBGUI Proxmox** melalui *browser* **system Windows** pada alamat https://192.168.169.1:8006, seperti terlihat pada gambar berikut:



Terlihat halaman login dari **Proxmox** sehingga membuktikan proses *unban* berhasil dilakukan.