GHOST PROTOCOL - PORT KNOCKING // knockd

Le Port Knocking : Le Protocole Fantôme

On veux savoir comment fonctionne cette magie noire ? C'est littéralement le concept de la "Porte Dérobée" ou du passage secret dans les films d'espionnage.

Le Concept Visuel

Imagine ton serveur comme un bunker en béton. Il n'y a **aucune porte visible**.

- Si un scanner (Nmap, Shodan, Bot Russe) passe, il voit un mur lisse. Tous les ports (même le SSH) répondent "Absents" ou "Fermés".
- Il n'y a pas de serrure à crocheter puisqu'il n'y a pas de porte.

La Séquence (Le "Toc-Toc-Toc")

Pour faire apparaître la porte, on dois "frapper" à des endroits précis du mur, dans un ordre précis.

Concrètement, ton client (ton PC) envoie des paquets réseau (des tentatives de connexion SYN) sur des ports fermés, mais surveillés par un démon silencieux (knockd).

Exemple de séquence "Sésame Ouvre-toi" :

1. On tentes de te connecter au port **7000** (Ça échoue, normal).
2. On tentes le port **8000** (Ça échoue).
3. On tentes le port **9000** (Ça échoue).

La Magie (L'Ouverture)

Le démon knockd sur le serveur analyse les logs du pare-feu en temps réel.

- Il se dit : *"Tiens, l'IP 92.155.xx.xx a touché le 7000, puis le 8000, puis le 9000 en moins de 5 secondes..."*
- **ACTION :** Il insère *instantanément* une règle iptables temporaire : ALLOW TCP FROM 92.155.xx.xx TO PORT 22

L'Infiltration

Soudain, pour **toi seul** (ton IP), le port 22 devient visible.

- On lances ta commande ssh user@lab-debian-99.
- On te connectes.
- Au bout de 10 secondes (réglage timer), le démon supprime la règle.
- La porte disparaît. Le port 22 est de nouveau fermé pour le monde entier.
- **Subtilité :** Ta connexion établie reste active (car le pare-feu autorise les connexions *déjà établies*), mais plus personne ne peut entrer, même toi, sans refrapper.

✓ Les Avantages (Le Style)	× Les Inconvénients (La Galère)
Furtivité Totale : Ton serveur n'existe pas sur les radars. Zéro log d'attaque brute-force dans Fail2Ban car personne ne voit le SSH.	**Complexité Client :** On ne peux pas juste ouvrir ton terminal et taper ssh. Il faut lancer un script de "toc" avant (knock lab-debian-99 7000 8000 9000).
Surface d'attaque Nulle : Même une faille 0-day sur OpenSSH ne peut pas être exploitée si le port est inaccessible.	**Le "Lag" :** Si ta connexion est instable et qu'un des 3 "tocs" se perd en route, la porte ne s'ouvre pas. C'est frustrant.
Cool Factor : C'est très satisfaisant techniquement.	**Risque de Lock-out :** Si le démon knockd plante, on es dehors. Il faut impérativement un accès console de secours (via ton hébergeur VPS).

L'Installation (Le Matériel d'Écoute)

⚠ **AVERTISSEMENT DE SÉCURITÉ (LA RÈGLE D'OR)**

> **Ne jamais configurer ça à distance sur un serveur de Prod sans un accès KVM/Console de secours.** Si le démon knockd plante ou si tu oublies la séquence, tu es enfermé dehors. Comme c'est une VM, tu es safe (tu as la console Proxmox/VMware).

```
admin@lab-debian-99:~$ sudo apt update && sudo apt install knockd iptables
[sudo] password for admin:
Hit:1 http://deb.debian.org/debian trixie InRelease
Get:2 http://deb.debian.org/debian trixie-updates InRelease [47.3 kB]
Get:3 http://security.debian.org/debian-security trixie-security InRelease [43.4 kB]
Get:4 http://security.debian.org/debian-security trixie-security/main Sources [119 kB]
Get:5 http://security.debian.org/debian-security trixie-security/main amd64 Packages [97.9 kB]
Fetched 308 kB in 0s (1,270 kB/s)
5 packages can be upgraded. Run 'apt list --upgradable' to see them.
Installing:
  iptables  knockd

Installing dependencies:
  libip4tc2  libip6tc2  libnetfilter-conntrack3  libnfnetlink0  libpcap0.8t64

Suggested packages:
  firewalld

Summary:
  Upgrading: 0, Installing: 7, Removing: 0, Not Upgrading: 5
  Download size: 656 kB
  Space needed: 3,311 kB / 21.9 GB available

Continue? [Y/n]
```

On aura besoin d'iptables, même si tu utilises ufw habituellement, knockd parle historiquement en commandes iptables.

La Configuration de la Séquence (Le Code Secret)

C'est ici qu'on définit le mot de passe rythmique

```
admin@lab-debian-99:~$ sudo nano /etc/knockd.conf
```

```
[options]
    UseSyslog

[openSSH]
    # La séquence secrète (Choisis tes propres ports !)
    # Exemple : Toc sur 7000, puis 8000, puis 9000
    sequence    = 7000,8000,9000
    seq_timeout = 5
    # La commande MAGIQUE : On insère (-I) une règle tout en haut pour accepter ton IP
    command     = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
    tcpflags    = syn

[closeSSH]
    # Séquence pour fermer manuellement (Optionnel mais classe)
    sequence    = 9000,8000,7000
    seq_timeout = 5
    # On supprime (-D) la règle
    command     = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
    tcpflags    = syn
```

> **Note :** Dans cet exemple, une fois la porte ouverte, elle reste ouverte jusqu'à ce que on fasses la séquence inverse (closeSSH). On peut aussi mettre un cmd_timeout pour qu'elle se ferme toute seule après 10 secondes. Pour l'instant, restons manuel.

L'Activation du Démon (Le Réveil)

Sur Debian, knockd est désactivé par défaut pour éviter les accidents. Il faut lui dire de démarrer et sur quelle interface écouter.

Trouve ton interface réseau (souvent eth0, ens18 ou enp3s0)

```
admin@lab-debian-99:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:98:b3:1b brd ff:ff:ff:ff:ff:ff
    altname enx52540098b31b
    inet 192.168.100.142/24 brd 192.168.100.255 scope global dynamic noprefixroute enp1s0
       valid_lft 2945sec preferred_lft 2298sec
    inet6 fe80::c540:47fd:7dbb:63ff/64 scope link
       valid_lft forever preferred_lft forever
```

Édite le fichier de démarrage

```
admin@lab-debian-99:~$ sudo nano /etc/default/knockd
```

```
# control if we start knockd at init or not
# 1 = start
# anything else = don't start
# PLEASE EDIT /etc/knockd.conf BEFORE ENABLING
START_KNOCKD=1

# command line options
KNOCKD_OPTS="-i enp1s0"
```

On passe `START_KNOCKD` de 0 à 1

On premplace le `eth0` de `KNOCKD_OPTS` par notre interface

Démarre le service

```
admin@lab-debian-99:~$ sudo systemctl restart knockd
```

```
admin@lab-debian-99:~$ sudo systemctl enable knockd
Synchronizing state of knockd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable knockd
Created symlink '/etc/systemd/system/multi-user.target.wants/knockd.service' →
'/usr/lib/systemd/system/knockd.service'.
```

Le Verrouillage (Fermer la porte à clé)

C'est le moment critique. Pour l'instant, le SSH est encore ouvert à tous. On va dire au pare-feu : **"Rejette TOUT le monde sur le port 22, sauf ceux qui sont déjà connectés."**

Attention : Ne coupe pas ta connexion actuelle !

Tape ces commandes une par une :

1. **Accepter les connexions déjà établies** (Pour ne pas te faire éjecter maintenant)

```
admin@lab-debian-99:~$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

2. Fermer le port 22 au reste du monde

```
admin@lab-debian-99:~$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```

À ce stade, si on essaies d'ouvrir un **nouveau** terminal SSH vers la VM, ça doit tourner dans le vide (Timeout). Le mur est en place.

```
admin@lab-debian-51:~$ ssh user@192.168.100.142
ssh: connect to host 192.168.100.142 port 22: Connection timed out
```

L'Infiltration (Le Test)

Depuis le **un autre pc**, il te faut un outil pour toquer. On peux installer knockd (qui contient le client knock) ou utiliser netcat / telnet.

```
admin@lab-debian-99:~$ sudo apt install knockd
[sudo] password for admin:
Installing:
  knockd

Installing dependencies:
  libpcap0.8t64

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 0
  Download size: 199 kB
  Space needed: 512 kB / 21.9 GB available

Continue? [Y/n]
```

La Procédure d'Entrée

1. **Essaie de te connecter (Ça doit échouer) :** ssh user@lab-debian-99 -> *Connection timed out...*

```
admin@lab-debian-51:~$ ssh user@192.168.100.142
ssh: connect to host 192.168.100.142 port 22: Connection timed out
```

2. **Fais le Code Secret (Toc Toc Toc) :** Remplace l'IP et les ports par ceux de ta config.

```
admin@lab-debian-51:~$ knock -v 192.168.100.142 7000 8000 9000
hitting tcp 192.168.100.142:7000
hitting tcp 192.168.100.142:8000
hitting tcp 192.168.100.142:9000
```

3. On tente la connection SSH !

```
admin@lab-debian-51:~$ ssh user@192.168.100.142
The authenticity of host '192.168.100.142 (192.168.100.142)' can't be established.
ED25519 key fingerprint is SHA256:q+ZBfWi+IQfK/0dnvtqR1FrmtKLEKxasWbRDao//AQ4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.100.142' (ED25519) to the list of known hosts.
user@192.168.100.142's password:
Linux lab-debian-01 6.12.63+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.63-1 (2025-12-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jan 24 13:25:41 2026 from 192.168.100.1
```

Bien joué, **Ghost**. 👻

On viens de faire l'expérience du "Stealth Mode". Pour le reste du monde, le port 22 n'existe pas. Pour toi, il apparaît sur demande. C'est la définition de la classe.

La Commande de Fermeture Manuelle

Si tu as gardé le bloc [closeSSH] de ma configuration précédente, la fermeture manuelle est simplement la **séquence inverse**.

```
admin@lab-debian-51:~$ knock -v 192.168.100.142 9000 8000 7000
hitting tcp 192.168.100.142:9000
hitting tcp 192.168.100.142:8000
hitting tcp 192.168.100.142:7000
```

Le démon va recevoir la séquence inverse, déclencher la commande iptables -D (Delete) et la porte disparaîtra

Vérification

```
admin@lab-debian-51:~$ ssh user@192.168.100.142
ssh: connect to host 192.168.100.142 port 22: Connection timed out
```

La Configuration Automatique (Auto-Close)

C'est la méthode recommandée. On ouvre, on rentre, et le portier referme tout seul après X secondes. Plus de risque d'oublier la porte ouverte.

On va modifier la section [openSSH] pour utiliser start_command (Ouverture) et stop_command (Fermeture) avec un minuteur.

```
admin@lab-debian-99:~$ sudo nano /etc/knockd.conf
```

```
[options]
    UseSyslog

[openSSH]
    sequence      = 7000,8000,9000
    seq_timeout   = 5
    tcpflags      = syn

    # 1. On OUVRE la porte (Insert en haut de la liste)
    start_command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT

    # 2. Le Minuteur (10 secondes)
    cmd_timeout   = 10

    # 3. On FERME la porte (Delete la règle après le temps écoulé)
    stop_command  = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
```

On peux supprimer ou commenter le bloc [closeSSH], il devient inutile

On n’oublie pas de restart le demon

```
admin@lab-debian-99:~$ sudo systemctl restart knockd
```

Le Test Final (Chrono en main)

On vérifie que c'est fermé !

```
admin@lab-debian-51:~$ ssh user@192.168.100.142
ssh: connect to host 192.168.100.142 port 22: Connection timed out
```

1. **Toque :** knock -v ... 7000 8000 9000

```
admin@lab-debian-51:~$ knock -v 192.168.100.142 7000 8000 9000
hitting tcp 192.168.100.142:7000
hitting tcp 192.168.100.142:8000
hitting tcp 192.168.100.142:9000
```

2. **Rentre vite :** ssh -> Connecté ! ✔

```
admin@lab-debian-51:~$ ssh user@192.168.100.142
user@192.168.100.142's password:
Linux lab-debian-01 6.12.63+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.63-1 (2025-12-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jan 24 15:26:21 2026 from 192.168.100.154
```

3. **Attends 10 secondes…**
4. **Ouvre un NOUVEAU terminal et tente ssh :** -> Timeout. **×**

```
admin@lab-debian-51:~$ ssh user@192.168.100.142
ssh: connect to host 192.168.100.142 port 22: Connection timed out
```

La porte s'est refermée toute seule, mais ta session active reste connectée car le pare-feu accepte les connexions ESTABLISHED.