**KNOCKD**

knockd è un demone (daemon) per Linux che implementa una funzionalità chiamata "port knocking". Il port knocking è una tecnica di sicurezza utilizzata per nascondere i servizi di rete dietro un firewall e permettere l'accesso solo a chi conosce una sequenza segreta di tentativi di connessione a determinate porte.

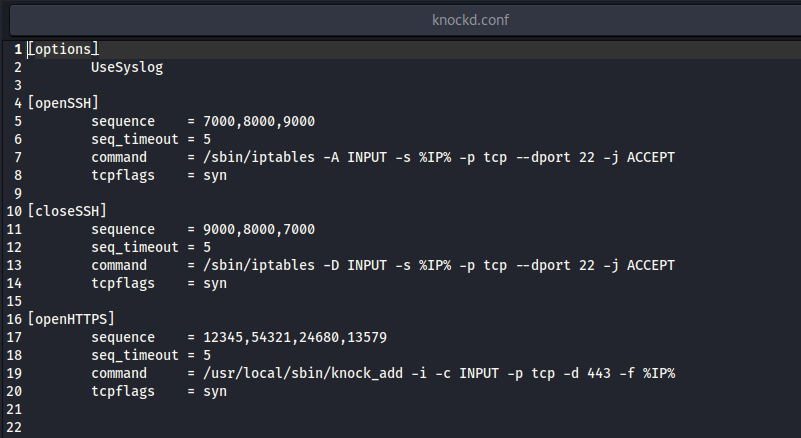
Quando knockd è in esecuzione su un server, ascolta passivamente il traffico di rete su un'interfaccia specifica. Non apre alcuna porta di per sé, ma monitora i tentativi di connessione (knocks) su porte chiuse. Se un utente tenta di connettersi a una serie di porte nell'ordine corretto, knockd eseguirà un comando predefinito, che potrebbe essere l'apertura di una porta del firewall per consentire l'accesso a un servizio (come SSH).

Questo approccio permette di "nascondere" un servizio di rete finché non viene utilizzata la sequenza corretta di knock per rivelarlo temporaneamente.

Per installare knockd basta eseguire il seguente comando

**sudo apt-get install knockd**

Successivamente all’installazione abbiamo il file di configurazione principale sotto al path : **/etc/knockd.conf**



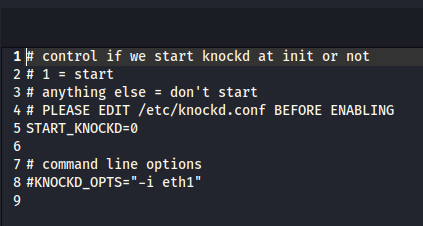
1 **[options]**: Sezione per le opzioni generali; UseSyslog significa che knockd invierà i suoi log a syslog.

2 **[openSSH]**:

* **sequence**: La sequenza di porte da "bussare" in ordine per attivare il comando associato. In questo caso, l'utente deve connettersi alle porte 7000, 8000 e 9000 in questo ordine.
* **seq\_timeout**: Il tempo massimo (in secondi) per completare la sequenza. Se il tempo supera questo limite, la sequenza viene ignorata.
* **command**: Il comando da eseguire quando la sequenza viene rilevata correttamente. In questo esempio, aggiunge una regola iptables per consentire l'accesso SSH alla porta 22 dall'indirizzo IP che ha eseguito il knock.
* **tcpflags**: Specifica che il knock deve essere effettuato con pacchetti TCP con il flag SYN (sincronizzazione) impostato.

3 **[closeSSH]**: Una configurazione simile alla precedente, ma in questo caso la sequenza inversa (9000, 8000, 7000) chiude la porta SSH rimuovendo la regola iptables.

Per abilitare knockd bisogna modificare il file al path **/etc/default/knockd**:



Cambiare **START\_KNOCKD=0** in **START\_KNOCKD=1**

Dopo aver abilitato knockd eseguire il seguente comando per avviare:

**sudo systemctl start knockd**

Per inviare i knock al server basta eseguire il comando:

**knock <ip\_del\_server> 7000 8000 9000**

Dopo aver eseguito questo comando, se la configurazione è corretta e la sequenza è eseguita correttamente, la porta SSH (22) dovrebbe essere aperta e accessibile.

**Sicurezza e Considerazioni**

**1 Protezione di Base e Offuscamento del Servizio:**

* Il port knocking aggiunge un livello di sicurezza basato sul principio di "security through obscurity" (sicurezza tramite offuscamento). I servizi di rete come SSH, che di solito sono direttamente accessibili su porte conosciute, possono essere nascosti dietro il firewall.
* Finché l'attaccante non conosce la sequenza corretta di porte da "bussare", il servizio rimane inaccessibile, riducendo la superficie di attacco. Questo può prevenire gli attacchi automatizzati e gli scanner di rete che cercano vulnerabilità su porte aperte.

**2 Mitigazione degli Attacchi di Forza Bruta:**

* Un servizio come SSH spesso subisce attacchi di forza bruta che tentano di indovinare le credenziali. Nascondendo la porta SSH dietro una sequenza di knock, questi attacchi possono **essere** completamente evitati poiché la porta stessa è chiusa fino a quando la sequenza corretta non viene eseguita.

**3 Compatibilità con Altri Meccanismi di Sicurezza:**

* Il port knocking può essere combinato con altre misure di sicurezza, come firewall dinamici, VPN, autenticazione a chiave pubblica SSH, e strumenti come fail2ban, che blocca gli IP dopo tentativi di accesso falliti. Questa combinazione di tecniche crea una difesa multilivello (defense-in-depth), rendendo un sistema più robusto.

**4 Debolezze e Considerazioni di Sicurezza:**

* Susceptibilità agli Attacchi di Replay: Un attaccante che riesce a monitorare il traffico di rete può catturare la sequenza di knock corretta e tentare un attacco di replay, inviando la stessa sequenza per ottenere accesso al servizio. Questo può essere mitigato utilizzando tecniche di autenticazione a doppio fattore o cambiando la sequenza periodicamente.
* Monitoraggio del Traffico e Rilevamento della Sequenza: Se un attaccante riesce a posizionarsi come "man-in-the-middle" o può monitorare il traffico di rete, potrebbe rilevare le sequenze di knock e usarle per accedere al sistema. Pertanto, il port knocking è più sicuro in reti in cui il traffico non è facilmente intercettabile.
* Attacchi DoS (Denial of Service): Se knockd è configurato per monitorare molte porte o se la sequenza richiede un numero significativo di tentativi, può essere vulnerabile a un attacco di tipo Denial of Service. Un attaccante potrebbe inviare un gran numero di pacchetti knock per consumare le risorse di sistema.
* Configurazione Inadeguata: Errori nella configurazione di knockd o del firewall possono portare a vulnerabilità che un attaccante può sfruttare. È fondamentale configurare correttamente i timeout, le regole di iptables e le sequenze di knock.

**5 Log e Monitoraggio:**

* È importante monitorare i log generati da knockd e dal firewall per rilevare tentativi sospetti di knock. La presenza di sequenze incomplete o tentativi di accesso non autorizzati potrebbe indicare un tentativo di attacco.

**6 Sequenze di Knock Dinamiche e One-Time Password (OTP):**

* Una buona pratica di sicurezza è utilizzare sequenze di knock dinamiche o basate su OTP (One-Time Password) che cambiano nel tempo. Questo approccio può migliorare la sicurezza del port knocking prevenendo attacchi di replay e rendendo più difficile prevedere la sequenza successiva.

**7 Segmentazione e Controllo degli Accessi:**

* Il port knocking non dovrebbe essere l'unica misura di sicurezza utilizzata. Dovrebbe essere parte di una strategia più ampia che include la segmentazione della rete, controlli di accesso basati sui ruoli (RBAC), monitoraggio continuo e risposta agli incidenti.

**8 Non è una Soluzione Perfetta:**

* Mentre il port knocking può fornire un livello aggiuntivo di sicurezza, non sostituisce altre misure di sicurezza fondamentali come la gestione degli aggiornamenti, la configurazione sicura dei servizi, l'uso di password forti e la protezione contro exploit di sicurezza. Il port knocking è utile principalmente per ridurre l'esposizione agli attacchi, ma deve essere combinato con altre difese.

**9 Utilizzo di knockd su Reti Pubbliche:**

* Su reti pubbliche o in situazioni in cui il traffico di rete può essere monitorato da terzi, l'uso di knockd dovrebbe essere attentamente valutato. L'uso di crittografia o tunnel VPN può aumentare la sicurezza.

**10 Gestione degli Errori e Timeout:**

* La configurazione del timeout per la sequenza di knock è cruciale. Un timeout troppo lungo può consentire ad un attaccante di "forzare" la sequenza con tentativi ripetuti nel tempo, mentre un timeout troppo breve potrebbe impedire l'accesso agli utenti legittimi.

**Conclusione**

Il port knocking e l'utilizzo di knockd rappresentano un'interessante tecnica di sicurezza per proteggere i servizi di rete. Tuttavia ha i suoi limiti e deve essere utilizzato con consapevolezza dei suoi punti deboli e dei possibili attacchi. È particolarmente utile in combinazione con altre tecniche di sicurezza per creare una difesa multilivello. La chiave è un'implementazione attenta e un monitoraggio continuo per garantire la sicurezza e la reattività agli eventuali tentativi di attacco.