Studio ed implementazione di una architettura avanzata basata su VPN per Security Assessment

Nicola Bena

Ottobre 2018

MoonCloud

- Framework per la valutazione ed il monitoraggio continuo di servizi cloud
- valutazione che certe proprietà (non solo di sicurezza) siano rispettate mediante raccolta continua di evidenze
- per l'utente finale MoonCloud è offerto as-a-service
  - inserisce informazioni sul target
  - MoonCloud effettua valutazione
  - mostra risultati

Non solo cloud

Obiettivo della tesi: estendere MoonCloud per poter analizzare reti aziendali classiche o cloud private

- cercando di rimanere ancora as-a-service
- la rete target è protetta da almeno un firewall/NAT, le sue risorse non sono accessibili dall'esterno
- soluzione: utilizzare una VPN tra MoonCloud e le reti dei clienti

Soluzione

La VPN deve:

- essere flessibile
- ligthweight per il cliente: non deve configurare niente

Soluzione:

- device Linux portato nella rete target che fa da VPN client
- in MoonCloud i VPN server
- OpenVPN per il collegamento VPN
- nftables (successore di iptables) per risolvere problemi di configurazione

Sfida 1 – NAT al contrario

- IP src dei pacchetti MoonCloud verso la rete target appartiene alla rete MoonCloud
- la rete target deve inviare le risposte al VPN client, ma senza rotte configurate le invierebbe al proprio default gateway

NAT al contrario: tutti i pacchetti provenienti dalla VPN vengono immessi nella rete target usando come IP sorgente quello del client VPN

- stesso NET ID della rete target
- quindi le risposte possono tornargli senza problemi
- realizzato con nftables

Sfida 2 – IP mapping

"*Ogni rete connessa alla VPN deve stare in reti IP diverse*"[1]

- si vuole che un server gestisca il maggior numero di reti target diverse
- alta probabilità che due reti abbiano lo stesso NET ID

IP mapping: *mappare* ogni rete target in una nuova rete garantita univoca perché scelta da MoonCloud

- tutta MoonCloud conosce solo indirizzi mappati quindi unici

[1] `https://openvpn.net`

Sfida 2 – IP mapping (2)

1. Quando si registra un nuovo cliente, le sue reti vengono mappate in reti nuove ed univoche
2. il cliente specifica il target dell'analisi usando l'indirizzo IP reale
3. MoonCloud ne ottiene la versione mappata in maniera tutto trasparente: è il l'IP dst dell'analisi
4. l'analisi parte, nel VPN client
   - richieste MoonCloud $\rightarrow$ host target:
     1. modifica IP dst mappato $\rightarrow$ IP originale
     2. applica *NAT al contario* ed invia ai target
   - risposte target $\rightarrow$ MoonCloud:
     1. applica inverso di *NAT al contrario*
     2. modifica IP src originale $\rightarrow$ IP mappato

- per fare il mapping lato client si usa nftables

Altre sfide

- Staticità configurazione server
  - OpenVPN si configura con file di testo letti all'avvio
  - necessità di specificare per ogni client quali reti raggiunge per inserire rotte nel kernel dell'OS
  - Soluzione: sfruttare hook `client-connect` per eseguire uno script che aggiunga le rotte all'OS ogni volta che un client si connette
    - lo script viene riletto ad ogni nuova connessione
    - client-disconnect per rimuoverle
- Rotte server-side
  - il client deve conoscere le reti presenti *dietro* il server per questioni di routing
  - non è possibile sapere a priori quali siano
  - Soluzione: il server applica NAT sui pacchetti verso la VPN

Considerazioni di sicurezza

La VPN potrebbe essere sfruttata da attaccanti. Si usano le seguenti contromisure:

- lato server si usano regole di firewalling che consentono di passare alle richieste di MoonCloud ed alle sole risposte ad esse
  - No richieste provenienti dalla rete target
- un host malevolo nella rete target dovrebbe passare due livelli di NAT e le regole lato server

MoonCloud_VPN

Microservizio integrato in MoonCloud per gestire la soluzione VPN

- creazione file di configurazione per OpenVPN
  - trasferimento via SSH ai server
- gestione certificati di client e server
  - creazione
  - revoca e rinnovo mediante CRL
- gestione IP mapping
  - assegnazione nuove reti ai client
  - creazione file di configurazione per nftables
  - dato un IP originale ritornare quello mappato