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

Nicola Bena (matricola 870103)

RELATORE
Prof. Marco Anisetti

CORRELATORI
Prof. Claudio A. Ardagna
Dott. Filippo Gaudenzi

Il successo del cloud computing ha richiesto un nuovo modo di svolgere *Security Assessment* e *Security Assurance*: modelli basati sulla raccolta continua di evidenze per valutare lo stato effettivo della sicurezza si stanno dimostrando sempre più utili ed efficaci.

Tra essi vi è MoonCloud, spin-off dell'Università di Milano, i cui target iniziali sono stati proprio i sistemi cloud. L'ambito di questa tesi è stata una collaborazione con tale azienda, al fine di espanderne i target anche a sistemi IT tradizionali o cloud privati, comunque confinati nell'ambito di una o più reti aziendali (dette *reti target*). Per fare ciò, è necessario disporre di *hook dall'interno* di tali reti, mentre per sistemi cloud si sfruttano hook messi a disposizione dal cloud provider. Inoltre, MoonCloud viene erogato come un servizio, ovvero l'utente finale non deve installare niente per analizzare i propri asset nella cloud, e nella transizione verso sistemi IT tradizionali si è cercato di mantenere questa caratteristica.

Il cosìdetto *hook dall'interno* è una VPN tra MoonCloud e le reti da analizzare, mediante un device che viene portato presso i clienti e responsabile di instaurare il collegamento. E' molto importante che questa soluzione di VPN sia trasparente per il cliente finale (oltre che sicura), ovvero richieda di effettuare il minor numero di configurazioni possibili, possibilmente nessuna.
Il lavoro svolto si può articolare in tre parti principali:

1. Uno studio sulle tecnologie VPN esistenti e delle topologie realizzabili con esse, al fine di valutare quali fossero le più adatte. La scelta è stata *OpenVPN*, un software consolidato e molto flessibile: in MoonCloud si posizionano i VPN server, mentre il device che si porta nella rete target funge da VPN client.

2. Un'analisi delle problematiche di configurazione, derivanti anche dall'uso altamente automatizzato della VPN. In particolare, poiché si vuole far sì che un server possa servire il maggior numero di client possibili, è stato necessario dover gestire la possibilità che diversi client abbiano gli stessi indirizzi IP, causando quindi dei conflitti. L'innovativa soluzione è stata chiamata *IP mapping*, e consiste nel *mappare* le reti dei clienti su nuove reti garantite univoche, il tutto in maniera trasparente.
   Sempre ai fini della trasparenza di configurazioni per il cliente, è stato introdotto il concetto di *NAT al contrario*.

3. La creazione di un microservizio a supporto dell'automazione della gestione della VPN. Esso è scritto in Python ed espone API REST che assolvono ai seguenti compiti:

- creazione di tutti i file di configurazione per la VPN
- gestione dei certificati mediante i quali avviene l'autenticazione nella VPN
- gestione dell'*IP mapping*: assegnare correttamente le reti ai client e, dato un indirizzo IP originale, ritornare la sua versione mappata
- trasferimento dei file di configurazione per i server verso i server stessi, mantenendone la coerenza.

Come prospettiva futura si sta studiando un'architettura distribuita, basata sempre su VPN, ma che sposti parte della computazione direttamente nelle reti target, per evitare di generare troppo traffico rallentando la connessione Internet dei clienti.