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

Con l'avvento del cloud computing risulta necessario rivoluzionare il modo di svolgere pratiche quali il *Security Assessment* e la *Security Assurance*. I più efficaci approcci proposti nel panorama scientifico ed industriale risultano essere quelli basati su raccolta continua di evidenze per valutare l'evoluzione dello stato della sicurezza del sistema target. Tra essi vi è MoonCloud, spin-off dell'Università di Milano, che fornisce una soluzione di security governance per la cloud *as a Service*, basata su raccolta di evidenze. La tesi è stata sviluppata in collaborazione con tale azienda, al fine di poter eseguire le verifiche di sicurezza anche in ambiti di cloud private o reti aziendali tradizionali, senza sconvolgere il paradigma *as a Service*.

Il lavoro svolto si può articolare come segue:

1. Studio delle possibili soluzioni architetturali basate su appliance VPN che permettano di istaurare un ponte tra MoonCloud e la rete privata da ispezionare, mantenendo il paradigma *as a Service*. Si è effettuato uno studio approfondito sulle tecnologie VPN esistenti e sulle topologie realizzabili con esse, al fine di valutare quali fossero le più adatte.

2. Design e realizzazione di una architettura VPN non standard basata su *OpenVPN* tra VPN appliance e MoonCloud. Vengono individuate e descritte diverse soluzioni innovative per la gestione delle reti target (*NAT al contrario* e *IP Mapping*). Il *NAT al contrario* serve per evitare di impostare rotte presso il cliente, mentre l'*IP Mapping* consiste nel *mappare* gli indirizzi IP delle reti target in nuovi indirizzi garantiti univoci e quindi utilizzabili dalle sonde MoonCloud per identificare i target dell'ispezione. Ciò consente di gestire tutti i possibili conflitti di indirizzi IP tra le reti dei clienti. Il sistema sviluppato ha la caratteristica di essere completamente trasparente al cliente finale oltre ad essere estremamente automatizzato.

3. La creazione di microservizi a supporto dell'automazione della gestione della VPN, per svolgere le seguenti principali operazioni: *i)* creazione di tutti i file di configurazione per *OpenVPN*, *ii)* gestione dei certificati mediante i quali avviene l'autenticazione nella VPN, *iii)* gestione dell'*IP Mapping*, *iv)* trasferimento coerente dei file di configurazione per e verso i server VPN in MoonCloud.

Come prospettiva futura si sta studiando un'architettura distribuita, basata sempre su VPN, che sposti parte della computazione richiesta per l'ispezione direttamente nelle reti target. In questo modo le componenti di

MoonCloud che effettivamente raccolgono evidenze agiscono direttamente dal cliente, e sulla VPN transitano solo richieste e risposte, diminuendo quindi il traffico generato.