

# Premessa

Negli ultimi anni si è osservato un interesse crescente nei confronti delle Honeynet, che nascono nell'ottica di ribaltare l'impostazione tradizionale della sicurezza: il loro scopo è quello di fornire informazioni dettagliate sulle metodologie di un'intrusione e sulle motivazioni, strumenti e tecniche di attacco utilizzate dagli intrusi. L'esperienza infatti insegna che, per quanto la gestione della sicurezza di un sistema informatico sia precisa ed accurata, non si otterrà mai la certezza di una protezione completa: "il sistema maggiormente sicuro è infatti -come si usa dire nell'ambiente informatico- quello spento". Fino ad oggi, nel mondo informatico, la difesa dei sistemi ha sempre avuto un approccio passivo: è la scoperta di un attacco che porta alla correzione degli errori che lo hanno reso possibile e alla generazione di procedure difensive. Le Honeynet ribaltano questo punto di vista e puntano ad un approccio attivo della difesa informatica: il nemico per essere sconfitto deve essere conosciuto, studiato, osservato per carpirne i punti deboli, e poter "virtualmente" sferrare l'attacco, che in questo significa erigere delle giuste barriere difensive prima di essere colpiti.

Questa mia tesi vuole porre lo sguardo su cosa sia una Honeynet, cercando di illustrarne i concetti generali e di descriverne alcune tipologie di soluzioni disponibili, valutandone il valore aggiunto e i rischi che esse presentano per le organizzazioni che ne vogliono usufruire. Cercherò infatti di mostrare, nell'ambito di questa mia dissertazione, le varie tipologie di Honeynet e Honeygot, anche con l'ausilio di esempi e di test effettuati, i rischi che esse possono apportare e soprattutto il loro valore nell'ambito della ricerca. In sintesi, gli obiettivi principali ed anche gli argomenti fondamentali trattati in questo testo riguardano:

- *Descrizione e definizione di Honeygot e Honeynet.* Viene fornita una descrizione dei concetti generali di Honeygot e Honeynet e la storia, si fornisce una definizione dettagliata e si analizzano i vantaggi e gli svantaggi correlati. In merito alle Honeynet, si descrivono e si analizzano i principi di funzionamento, le specifiche e i rischi ad esse correlate. Si introduce il concetto di generazioni di Honeynet e si analizzano le architetture ed i principi di funzionamento delle stesse, evidenziando le loro peculiarità in base ai requisiti fondamentali di una Honeynet.
- *Analisi delle Tipologie di Honeygot.* Si analizzano sei tipologie specifiche Honeygot, ognuna delle quali presenta un differente livello di interazione. Lo scopo è quello di effettuare una panoramica per capirne il valore ed i principi di funzionamento. Si approfondisce il concetto di Honeygot a diverso livello di interazione grazie all'ausilio di esempi e test dei differenti software.
- *Progettazione e implementazione di una Honeygot.* Al fine di dimostrare l'efficacia di questa tecnologia nell'analisi comportamentale tecnica dei malicious hacker e alla

raccolta di dati agli attacchi è stata realizzata una Honeypot a bassa interazione con l'utilizzo di Honeyd.

- *Analisi dei log raccolti.* Utilizzando tecniche e metodologie della Network Forensic sono stati analizzati i log raccolti grazie alla Honeypot implementata. Dalle analisi effettuate dei log raccolti sono emersi dati relativi alle connessioni ricevute dalla Honeypot che mostrano i vantaggi connessi all'implementazione di una Honeypot sia di ricerca che di produzione.

Il valore di ricerca delle Honeypot è molto elevato, in quanto permette di studiare ed analizzare, come si è mostrato in questo caso di studio, gli attacchi automatizzati, le vulnerabilità più colpite nella rete ed il comportamento degli intrusi in rete. Si dimostra che il valore di produzione delle Honeypot è strettamente correlato al concetto di “difesa attiva”, volto a proteggere il patrimonio informativo aziendale.

La tesi è organizzata come segue:

- nel *Capitolo 1* vengono definiti i concetti generali di Honeypot e HoneyNet e si analizzano i vantaggi e gli svantaggi correlati. In merito alle HoneyNet, si esaminano i principi di funzionamento, le specifiche e i rischi;
  - nel *Capitolo 2* si classificano le Honeypot in base al loro livello di interazione, si introduce il concetto di generazioni di HoneyNet e si analizzano le architetture ed i principi di funzionamento delle stesse, evidenziando le loro peculiarità in base ai requisiti fondamentali di una HoneyNet introdotti nel Capitolo 1. Si descrive, infine, l'innovativo concetto di HoneyToken;
  - nel *Capitolo 3* si descrivono e si approfondiscono, mediante esempi e test sul campo, sei tipologie specifiche Honeypot, ognuna delle quali presenta un differente livello di interazione;
  - nel *Capitolo 4* si analizzano i requisiti che i log devono garantire per essere utilizzati nell'ambito di analisi di Network Forensic;
  - nel *Capitolo 5* viene mostrata l'implementazione di una Honeypot a bassa interazione con l'utilizzo di Honeyd e si effettua l'analisi dei log raccolti.
  - Il *Capitolo 6* è il capitolo conclusivo nel quale si espongono anche i possibili sviluppi futuri di questa tesi.
-