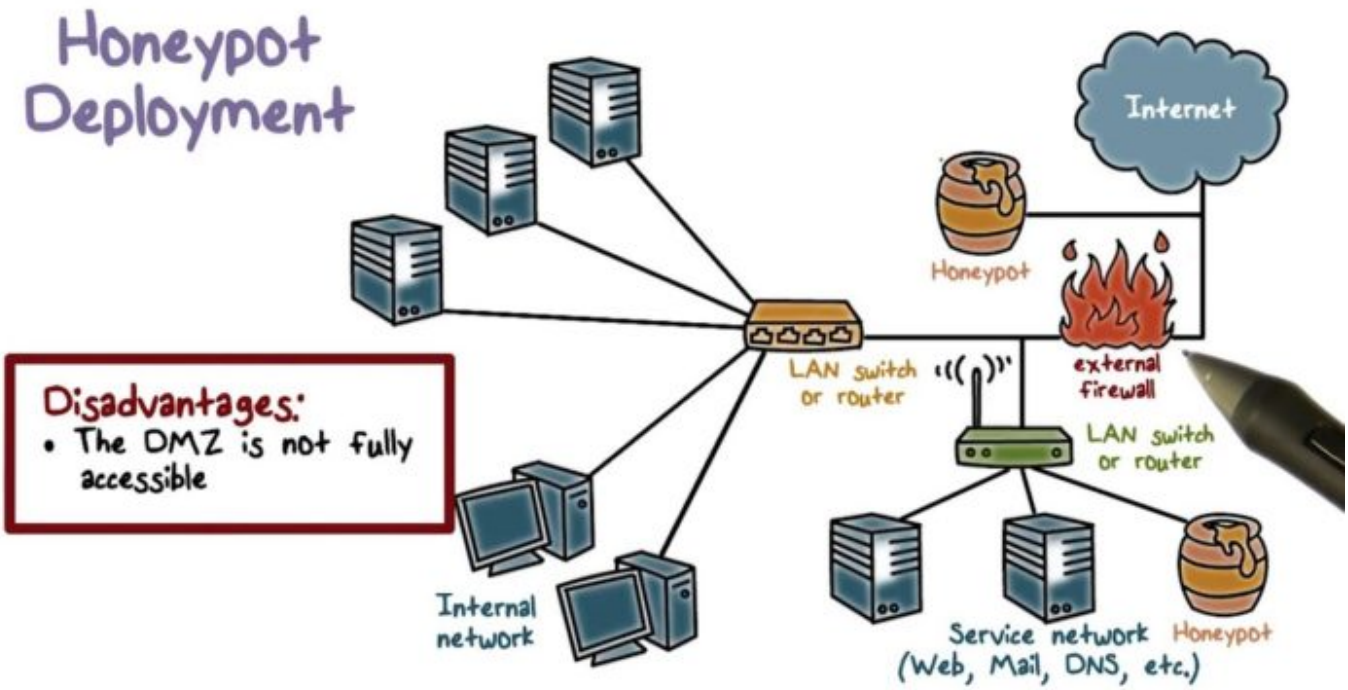
Honeypot - Barattoli di miele per cracker

Author : Fabio Carletti aka Ryuw

Date : 13 Febbraio 2019

Per gli addetti ai lavori di IT, con il termine “HoneyPot” si intende **una trappola contro gli attacchi di pirati informatici**. Il termine deriva dal personaggio dei cartoni **Winnie the Pooh**, orso goloso di miele. Nel mondo della sicurezza informatica si usano queste esche per identificare intromissioni abusive. Sono utili per trovare, ad esempio, un cracker entrato in una rete LAN, un NAS o un server web interno. Queste risorse sono un’esca allettante da bucare e usare per attacchi su internet o per spionaggio industriale. **Queste trappole simulano un bottino interessante** per chi è intento a bucare workstation e permettono al responsabile IT di **monitorare, tramite allarmi, il comportamento di botnet e attaccanti**, analizzando i log dei movimenti fatti. Le trappole sono finte, quindi non si usano pc potenti o server costosi ma vps e vecchi pc ancora funzionanti, contenenti file fasulli e/o insignificanti.

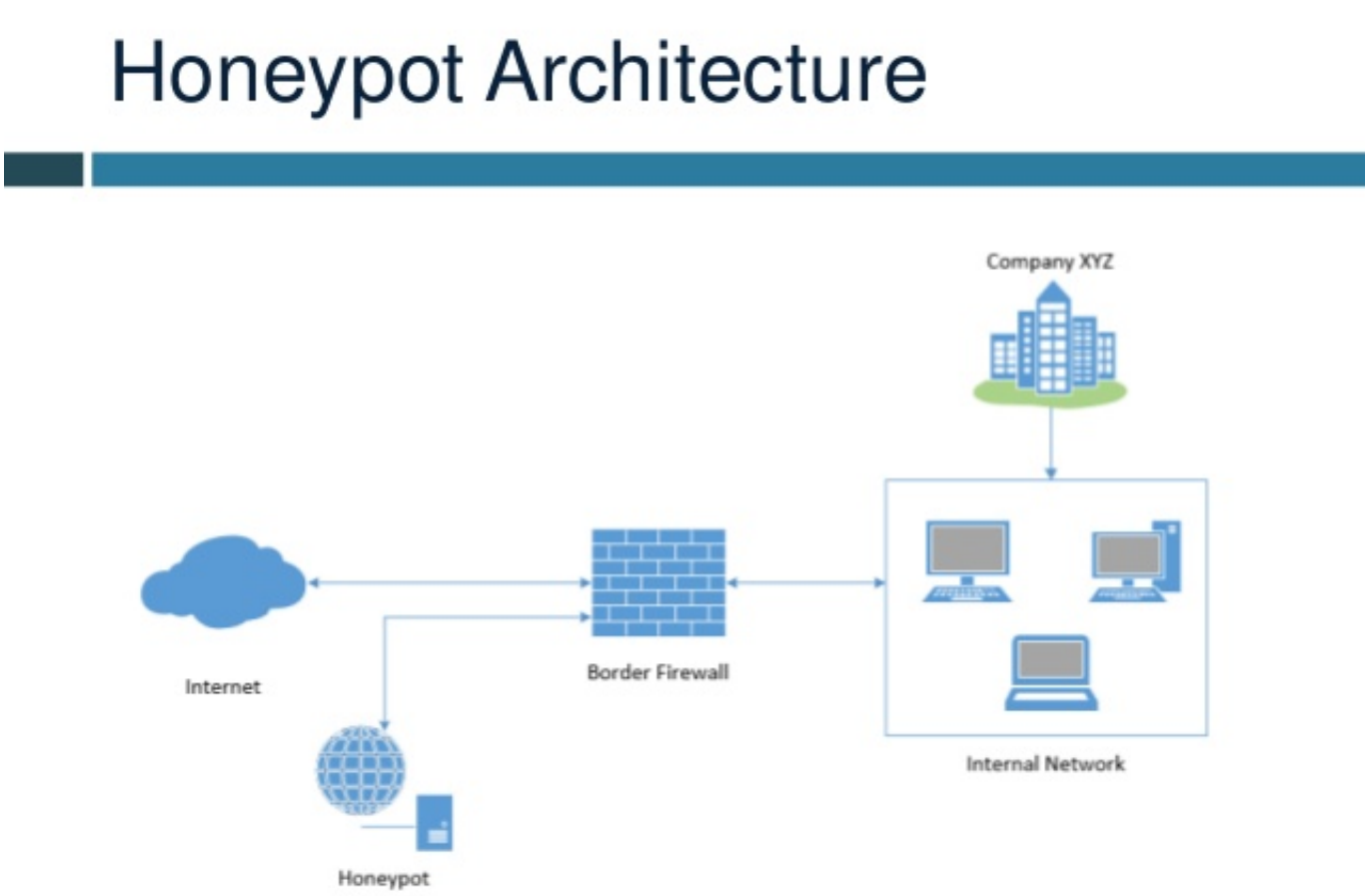
Con l’arrivo di pc lowcost come raspberry e simili, molti usano questi mini-pc che, avendo un basso impatto energetico, sono sempre più utilizzati dalle aziende. Sostanzialmente **una macchina HoneyPot è un server che simula un server reale in una rete che attira l’attaccante a entrare** attratto da dati riservati, password, account e informazioni per prendere il controllo dei sistemi informatici o ricattare con malware cryptolocker. In ambienti con sotto-reti e grandi realtà si vedono anche HoneyNet in cui termini come *prevention/detection/response*, DMZ e intranet sono da controllare tutti i giorni da un apposito addetto security ITC specialist.



L’approccio delle **HoneyPot fisiche** permette di avere macchine reali e un alto livello di interazione, mentre per le **esche virtuali** - quindi simulando i PC - si può rispondere al traffico verso la trappola e simulare differenti tipologie di HoneyPot. L’amministratore di sistema punta a ottenere dall’esca informazioni su come limitare i rischi dell’organizzazione e ricercare come le attuali botnet scansionano gli IP esposti a internet e agiscono verso di essi.

Esistono appositi servizi offerti da Symantec, kfsensor, honeynets, honeytrap, honeystick, nebula, nepenthes, pehunter, phoneyC e altri vendor che mettono a disposizione software a pagamento o free e, spesso, opensource per questo genere di attività, catturando pacchetti sospetti verso l’esca. Questa attività di monitoraggio ha il vantaggio di richiedere poche risorse, aiuta a controllare i falsi positivi ed è utilizzabile con IPv6.

HoneyWall è un progetto simile, basato su linux, per questo genere di attività, con tool per catturare e analizzare il traffico di rete abilitando ALL nelle regole di traffico verso la HoneyNet. La restrizione del traffico in uscita, strategia orientata ad evitare il rischio di attacco di ulteriori sistemi a partire da un honeypot compromesso, può essere facilmente rilevata attivando un elevato numero di connessioni in uscita e osservando la presenza di una qualche limitazione.



Un progetto molto dinamico, completo e facile da usare è **OpenCanary**, disponibile su [github] con utility da configurare per gli alert tramite email e il monitoraggio di vulnerabilità e metodi di attacco. Una risorsa dove trovare link a progetti simili più specifici in settori di esca informatica è presso il sito **Honeynet Project** (honeynet.org). Il sito è una fonte realizzata da **studenti appassionati di sicurezza informatica** dove trovare lezioni e info riguardanti honypot/honeynet. Ci sono **due livelli di interazione:** uno basso, in cui l'esca potrebbe essere scoperta da un attaccante esperto poiché non viene usato un server reale; e un livello alto, in cui c'è il pieno accesso al sistema operativo, una macchina creata per apparire simile alle altre nella rete. Ma questa scelta comporta un maggior rischio di sicurezza e necessita di un constante supervisione, risultando un lavoro complesso e dispendioso.

Un'alta interazione cattura più informazioni - compresi nuovi tool e nuovi tipi di attacco - e pregiudica l'approccio del tecnico, che deve avere skill anche in ambito *forensics*. Pacchetto disponibile per Debian è **Kippo,** che emula un servizio ssh protetto da password debole, raccogliendo informazioni sugli attacchi a forza bruta e a dizionario, loggando ogni input dell'attaccante.

Uno strumento spesso usato insieme ad una honeypot/honeynet è **Snort**, famoso IDS/IPS per

proteggere e monitorare, tramite regole assegnate dalla comunità snort, traffico di rete e richieste IP. Snort è rilasciato sotto GNU license - quindi liberamente utilizzabile - e multipiattaforma usando librerie libpcap per analizzare protocolli e controllare i contenuti dei pacchetti. **Nelle honeynet la presenza di un honeywall è indispensabile** per svolgere un'azione di contenimento degli attacchi che possono sfruttare il sistema compromesso come testa di ponte e, allo stesso tempo, per acquisire maggiore informazioni in maniera trasparente.

L'adozione di particolari misure di sicurezza, come si può capire, può rivelarsi **un'arma a doppio taglio** in grado di facilitare il lavoro di riconoscimento di un sistema-trappola da parte di un cracker preparato. Un aggressore esperto potrebbe intuire la presenza di un honeywall, costruendo dei pacchetti *ad hoc* contenenti un payload dannoso che sicuramente comporterebbe la loro eliminazione da parte di SnortInline. Inviando pacchetti "maliziosi" verso un sistema target di cui si ha il controllo, è possibile stabilire se tali pacchetti sono stati alterati in qualche modo o scartati. Questo tool, messo in modalità IPS, previene minacce di port scanner, buffer overflow e IP da bannare.

Gli HoneyPot vanno maneggiati con cura, poiché potrebbero diventare il punto di ingresso alla nostra rete: quindi **la scelta deve essere oculata** e bisogna, innanzitutto, valutare se occorre realmente. Inutile in piccole realtà, maggiormente utile in grandi contesti dove più persone si occupano della sicurezza della rete con pentest regolari e titolari sensibili a tematiche di sicurezza informatica e *disaster recovery*.

L'utilità di questi sistemi è che si possono rilevare o impedire attacchi verso macchine reali e **spesso la sua efficienza dipende da dove viene collocato**. L'attaccante, fino a quando non si rende conto di essere in trappola, perderà tempo per impadronirsi del sistema OS. I network admin più attenti attuano le honeypot per proteggere e monitorare maggiormente la rete lan, così da avere un accertamento in tempo reale dell'utilizzo del traffico da internet.

Nello scorso anno è capitato a un cliente che monitorando una honeypot (una vps con debian GNU/linux) e simulando un webserver con account dei dipendenti, l'admin ha notato che l'attaccante provava account con le email aziendali dei dipendenti - segno evidente che già le possedeva - e cercava, quindi, possibili server di posta interni per mandare email manipolate verso clienti esteri. La vicenda si è conclusa tra i vari accorgimenti con il **cambio di tutte le password e indirizzi di email interne e la blacklist di IP sospetti**.

Altro caso: un'azienda che ha preparato una HoneyNet tramite una rete wifi "fake/esca", con ID amministrazione e password WPA2. Monitorando i dispositivi a cui si connettevano, si è studiato il loro modo di agire per organizzare misure di **controspionaggio industriale**.

Le honeypot sono **uno strumento ingegnoso per distogliere l'attenzione, in alcuni casi, dal tesoro dell'azienda**. La sicurezza informatica non è un prodotto, ma un processo; e solo la ricerca continua, da parte del tecnico sensibile a queste tematiche, può - attraverso tecniche e tool - proteggere le macchine PC e la rete.

Spesso nella piccola e media azienda non c'è questa figura di riferimento, considerando la sicurezza come un optional e non come punto di riferimento e di necessaria attenzione per la

produttività. **Il nuovo GDPR sta costringendo le attività commerciali ad alzare il livello di sicurezza informatica** e ad adottare password più complicate. **Il vero problema è l'utente non attento**, che adopera la tecnologia prendendo con leggerezza privacy e sicurezza informatica così lasciando spesso, inconsapevolmente, vettori di attacco a potenziali cracker.

Articolo a cura di **Fabio Carletti aka Ryuw**