Linuxshell Italia

Honeypot Hacklab

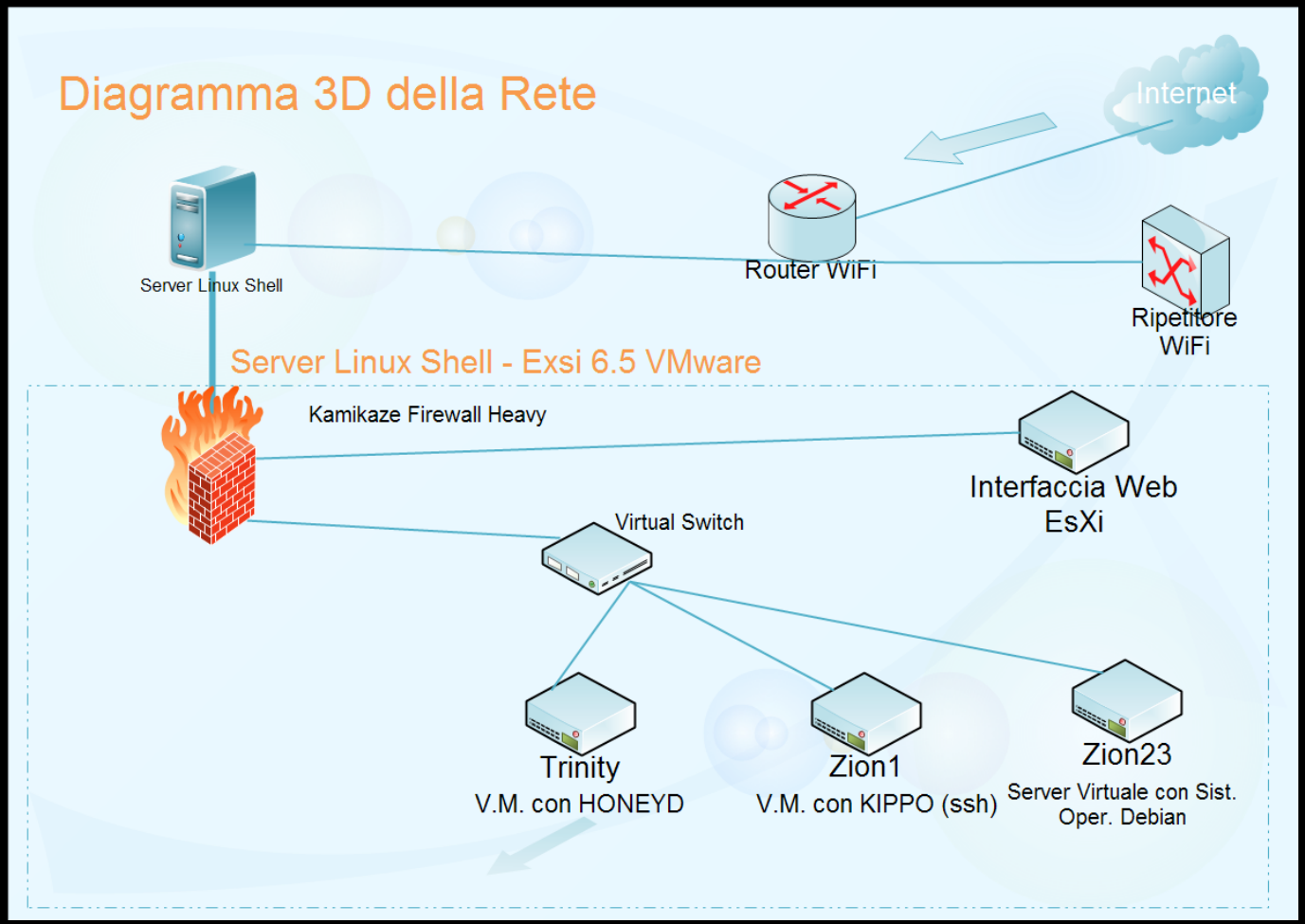
Intro Marco Pantò - Presenta Luca Vidoni - 28 ottobre 2017

Situazione di partenza

- Avevamo un datato HP a disposizione con 6 dischi SAS da 2,5" 32 GB di Ram, due schede di rete e una connesione a Internet.
- Abbiamo installato un **EsXI 6.5**, ovvero un server tramite il quale è possibile creare e gestire macchine virtuali. Questo prodotto è un vero e proprio sistema operativo con all'interno un microkernel linux che analizza l'hardware per poi lasciare il controllo a un modulo vmkernel sviluppato da VMware.
- La gestione del sistema EsXI e delle macchine virtuali avviene mediante interfaccia web (attiva dopo l'installazione).

Situazione di partenza

- Dopo aver attivato questo server abbiamo installato una serie di macchine virtuali linux.



Situazione di partenza

- Così facendo volevamo capire chi o cosa girasse in Internet.
- Il risultato circa 7000 tentativi di accesso in circa 35 giorni in cui il server è restato online. I tentativi provenivano da tutto il Mondo.

Non ci credete?

Che fare?

- Ci siamo fatti una domanda chi c'è dall'altra parte del terminale?
- Come rispondere a questa domanda?
- Installare su due macchine virtuali due **honeypot** diversi e, dirottando il traffico informatico del firewall su queste specifiche trappole, provare a capire chi si ha di fronte.

Cos'E' un honeypot 1/2

- In informatica, un **honeypot** (letteralmente: "barattolo del miele") è un sistema o componente hardware/software usato come "trappola" o "esca" (**decoy**) al fine di proteggere una rete telematica contro gli attacchi informatici da "**hacker**" o "**malware**".
- Il valore primario di un honeypot è **l'informazione** che esso dà sulla natura e sulla frequenza di eventuali attacchi subiti dalla rete.
- Gli honeypot **non** contengono informazioni reali o sensibili e quindi non dovrebbero essere coinvolti nelle normali attività di lavoro.

Cos'E' un honeypot 2/2

- Di fatto cosa succede a chi si imbatte in un honeypot?
- l'attaccante resta intrappolato nell' honeypot senza venirne a capo e senza riuscire a “bucare” il sistema, scoraggiandolo;
- essendo un sistema “fasullo”, è possibile vedere le tecniche impiegate per violare un sistema e porvi rimedio;
- possono rivelare intrusioni non autorizzate o malevole in corso.

Che ti pi di honeypot esistono

- Esistono molti tipi di honeypot. I più famosi sono: Artillery, Artemisa(VoIP), Kippo(ssh), Honeyd, Honeytrap o Nepenthes ecc.
- Dopo un'analisi abbiamo deciso di installare Kippo e Honeyd.
- Abbiamo scelto Kippo perchè nei 7000 attacchi il 95% erano stati portati sulla porta ssh (22).
- In un secondo momento abbiamo deciso di installare anche Honeyd per poter avere un sistema I.D.S. (*Intrusion detection system*) completo in caso di aggiramento del firewall.

Kippo 1/2

- Kippo è un programma scritto in Python un linguaggio di programmazione molto potente.
- Kippo non necessita di essere installato, basta solo che ci siano le librerie necessarie e i permessi adeguati per funzionare.
- Questo lo rende molto facile da utizzare e da inserire anche all'interno di un sistema articolato.
- Di solito Kippo viene utilizzato come honeypot sulla porta **22** (ssh).

Kippo 2/2

- Tramite un comando specifico "*createfs.py*" è possibile "clonare" il file system del computer bersaglio (un generico PC).
- Nelle varie cartelle che articolano il programma Kippo esiste uno script "*passdb.py*" che serve per inserire delle nuove password "*fake*" all'interno del database pass.db .
- Infine, esiste uno script "*playlog.py*" che serve a visualizzare cosa ha fatto l'attacante (hacker) una volta entrato nella trappola e come si è comportato, cosa ha scaricato, che comandi ha eseguito ecc.

Honeyd 1/2

- *Honeyd* è un altro honeypot molto flessibile a bassa interazione. Può essere usato per emulare una gran varietà di servizi e macchine (sia client sia server). Tramite *honeyd* è possibile creare modelli di comportamenti per le macchine e quindi distribuire numerose istanze di questi modelli al fine di creare una rete emulata.
- Per un vincolo del programma non è possibile inserire nella stessa configurazione due diverse tipologie di computer. Si è reso necessario realizzare due file distinti di configurazione uno per l'ambiente Windows e uno per l'ambiente Linux

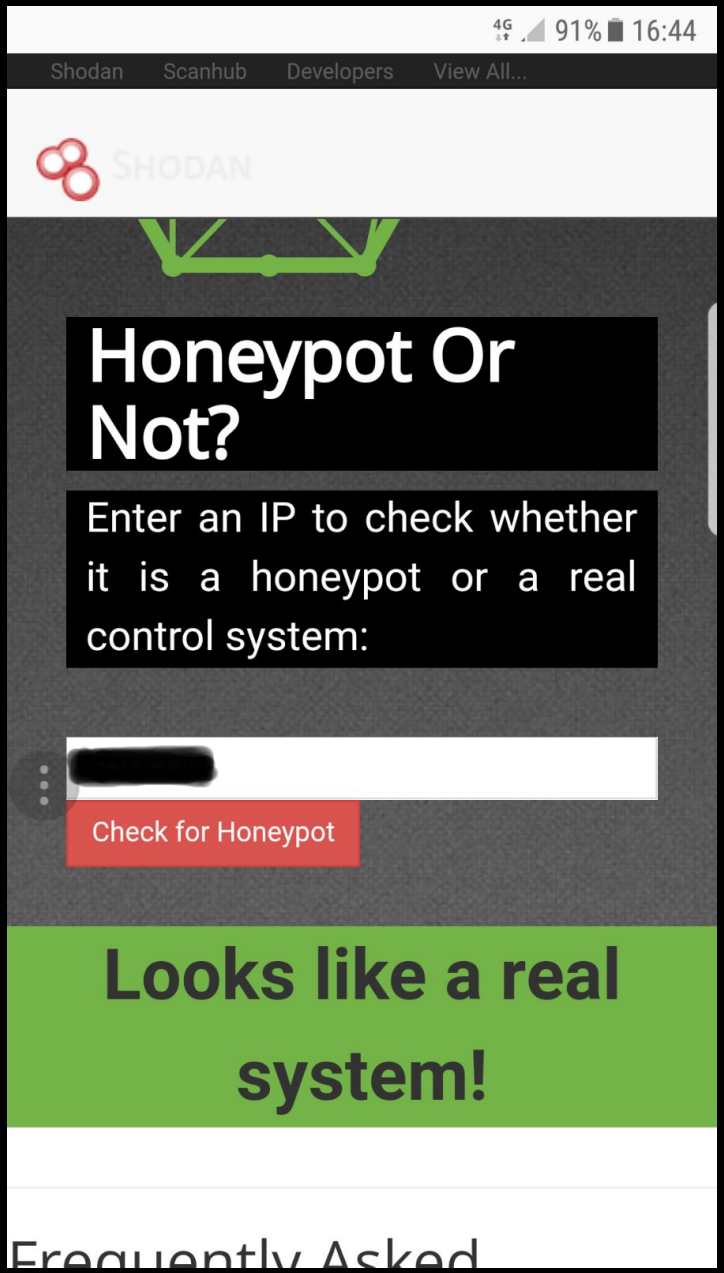
Honeyd 2/2

- Si possono eseguire diverse istanze del *honeyd* in contemporanea.
- Per una maggiore comprensione, è consigliabile inserire (tramite uno script reperibile in rete) tutti i log in una base di dati (MariaDB o MySQL).
- Per analizzare la base di dati vi è anche un programma (*honed2viz*) che installa un server web con una serie di pagine in php nelle quali vi sono grafici e statistiche.

I risultati di kippo

- In circa 95 giorni ci sono stati 850 attacchi informatici sulla porta 22 di cui 843 condotti da dei bot.
- Tramite un programma presente in Internet è stato possibile controllare quanto fosse credibile l'honeypot

I risultati di kippo



I risultati di Honeyd

- Tramite honeyd è stato possibile scoprire un piccolo worm .

Buona serata a tutti

Contattateci sul sito
www.linuxshell.it o www.certificazionilinux.com
per domande sulla presentazione info@linuxshell.it o lukes1582@gmail.com