Autore guida: whistler
Autore Pdf: 51ckb01
Date: 2018.04.10
Link: https://hackerjournal.it/forum/main-forum/riepilogo-laboratorio-di-pentest/#post-211

@whistler

Salve a tutti!
Ho pensato di scrivere un post di riepilogo del laboratorio virtuale descritto a partire dal numero 216 per varie ragioni:

>>Fornire a tutti una copia riepilogativa delle istruzioni del laboratorio sempre a portata di mano;

>>Aiutare chi decidesse tardi di seguire questa rivista rendendo più semplice riallacciarsi alle nozioni dei numeri precedenti;

>>Dare un aiuto aggiuntivo a chiunque si fosse bloccato in qualche passaggio e non ha avuto modo di chiedere sul forum.

Qualunque critica, consiglio o constatazione sarà ben accetta.

Buon divertimento!

1.1 INSTALLAZIONE DI VIRTUALBOX.

link utile: -> **www.virtualbox.org/wiki/Downloads**

Per chi usa Linux:

debian based -> sudo apt install virtualbox
arch based -> sudo pacman -S virtualbox
redhat based -> sudo yum install virtualbox
gentoo based -> sudo equo install virtualbox

In via alternativa visitare il link a inizio paragrafo.

Per chi usa Windows scaricare il file .exe dalla pagina www.virtualbox.org/wiki/Downloads;
Al termine del download seguire la procedura guidata per l'istallazione.

Per chi usa Mac OS:

Non essendo pratico di questo OS, ho trovato un'ottima guida a questo link

https://ie4mac.com/install-virtualbox-macos/

in cui anche in questo caso bisogna scaricare i file per l'installazione da www.virtualbox.org/wiki/Downloads.

1.2 SCARICARE LE ISO LIVE PER LE MACCHINE VIRTUALI.

Elenco qui di seguito le macchine virtuali con le rispettive iso, nomi assegnati nel corso e funzioni:

Kali linux, "Pentester", simula l'attaccante;
Damn small linux, "Backbone" e "Server FTP", router perimetrale e server FTP presente nella SOHO;Zeroshell, "Router", simula il router interno alla rete da testare;Metasploitable, "Server Web", simula un server web presente nella SOHO.

I link da cui scaricare le iso live sono i seguenti:

Kali linux ----------> https://www.kali.org/downloads/
Damn small linux ----------> http://www.damnsmalllinux.org/download.html
Zeroshell ----------> https://zeroshell.org/download/
Metasploitable ----------> https://sourceforge.net/projects/metasploitable/

1.3 CREARE E CONFIGURARE LE MACCHINE VIRTUALI.

Dopo aver installato Virtualbox e aver scaricato tutte le iso non ci resta che creare le macchine virtuali per dar vita al laboratorio di pentest.

>> Macchina "Pentester"

Sistema operativo --------> Linux (Ubuntu a 64 bit);

RAM ----------> 1024 MB;

Disco fisso ----------> Nessuno;

Archiviazione ----------> Dopo aver creato la macchina virtuale, aggiungere un nuovo controller IDE inserendovi l'ISO di Kali Linux;

Rete ----------> Una scheda di rete, connessa alla rete interna chiamata "intnet";

Configurazione di rete----> Eseguire i seguenti comandi con una shell di root:

#ifconfig eth0 210.100.1.1/24
#route default gw 210.100.1.2

>> Macchina "Backbone"

Sistema operativo --------> Linux (Linux 2.4 a 32 bit);

RAM ----------> 64 MB;

Disco fisso ----------> Nessuno;

Archiviazione ----------> Dopo aver creato la macchina virtuale, aggiungere un nuovo controller IDE inserendovi l'ISO di Damn Small Linux;

Rete ----------> Due schede di rete, una connessa alla rete interna chiamata "intnet", l'altra invece sarà connessa alla rete interna chiamata "intnet1";

Configurazione di rete----> Eseguire i seguenti comandi con una shell di root:

#ifconfig eth0 up
#ifconfig eth0 210.100.1.2 netmask 255.255.255.0
#ifconfig eth1 up
#ifconfig eth1 211.100.1.1 netmask 255.255.255.0
#sysctl -w net.ipv4.ip_forward=1
#route add -net 212.100.1.0/24 gw 211.100.1.2

>> Macchina "Router"

Sistema operativo --------> Linux (Other Linux - 32 bit);

RAM ----------> 256 MB;

Disco fisso ----------> Nessuno;

Archiviazione ----------> Dopo aver creato la macchina virtuale, aggiungere un nuovo controller IDE inserendovi l'ISO di ZeroShell;

Rete ----------> Tre schede di rete, una connessa alla rete solo host "vboxnet0",
una connessa alla rete interna chiamata "intnet1",
l'ultima connessa alla rete interna "intnet2";

Configurazione di rete----> Per convenienza seguiremo l'ultima configurazione descritta nel numero 216,
ovvero la configurazione delle interfacce di rete sarà effettuata tramite la
il browser della macchina fisica. All'avvio della macchina virtuale, ZeroShell attribuisce l'indirizzo 192.168.0.75 alla prima scheda di rete. Per creare il collegamento tra la VM e la macchina fisica, nell'interfaccia principale di Virtualbox selezioniamo dal menù la voce "Preferenze", per poi cliccare sull'icona "Rete" e scegliere la scheda "Reti solo host". Clicchiamo su "Aggiungi rete solo host", ovvero sull'icona di una scheda di rete sormontata dal simbolo "+". Nella schermata inseriamo l'indirizzo ip 192.168.0.71 e la netmask 255.255.255.0 e clicchiamo su "Ok"
Assicurasi che il flag "Abilita il server" non sia selezionato. Così facendo verrà creata un'interfaccia di rete virtuale denominata "vboxnet0". Ora come premesso in precedenza configuriamo le interfacce della macchina "Router" collegandoci con un browser della macchina fisica all'ip 192.168.0.75 ed

effettuiamo il log in con username "admin" e password "zeroshell" (senza le virgolette ovviamente). Nell'home page del portale selezioniamo la voce "Setup" all'interno della sezione "System".
Selezioniamo la scheda "ETH01", premiamo il pulsante "Add IP" e inseriamo l'indirizzo 211.100.1.2 e la subnet 255.255.255.0.
Reiteriamo l'operazione per la scheda "ETH02" però con ip 212.100.1.1 e subnet 255.255.255.0.
Infine clicchiamo su "Gateway" in cima alla pagina e inseriamo l'indirizzo 211.100.1.1.

(Le operazioni precedenti, che ci hanno permesso di configurare le interfacce della macchina "Router", sono state riprese dalla guida che spiega come creare una zona DNS con questa VM: quest'ultima la riassumerò più avanti.)

>> Macchina "Server Web"

Sistema operativo --------> Linux (Linux 2.4 a 32 bit);

RAM ----------> 256 MB;

Disco fisso ----------> Nessuno;

Archiviazione ----------> Selezionare l'opzione "Usa disco fisso esistente", per poi scegliere il file con estensione vmdk che avete scaricato insieme agli altri file di metasploitable;

Rete ----------> Una scheda di rete, connessa alla rete interna "intnet2";

Configurazione di rete----> Eseguire i seguenti comandi con una shell di root:

#ifconfig eth0 212.100.1.2 netmask 255.255.255.0;
#route add default gw 212.100.1.1

>> Macchina "Server Ftp"

Sistema operativo --------> Linux (Linux 2.4 a 32 bit);

RAM ----------> 64 MB;

Disco fisso ----------> Nessuno;

Archiviazione ----------> Dopo aver creato la macchina virtuale, aggiungere un nuovo controller IDE inserendovi l'ISO di Damn Small Linux;

Rete ----------> Una scheda di rete, connessa alla rete interna "intnet2";

Configurazione di rete----> Eseguire i seguenti comandi con una shell di root:

#ifconfig eth0 up
#ifconfig eth0 212.100.1.3 netmask 255.255.255.0;
#route add default gw 212.100.1.1

1.4 PRIMI TEST: IL COMANDO PING.

Avviando tutte le VM, lanciamo un terminale sulla macchina Pentester e controlliamo la connettività tramite
il comando "ping":

#ping -c4 212.100.1.1
#ping -c4 212.100.1.2
#ping -c4 212.100.1.3

I comandi precedenti permettono di verificare la connettività con le macchine che formano la SOHO.

Umilmente vorrei proporre un piccolo script per eseguire in una sola riga i comandi precedenti.

#for i in `seq 1 3`;do ping -c4 212.100.1.$i; done

Se la percentuale presente nel campo "packet loss" è pari a 0 allora il test avrà avuto successo.

2.1 CONFIGURAZIONE DELLA ZONA DNS SU ZEROSHELL.

Dopo aver creato e configurato il laboratorio virtuale, nel numero 216 della rivista ci viene spiegato come creare una zona DNS tramite la VM "Router" per poi ricevere istruzioni su come utilizzare due tool (dig e fierce) presenti in Kali Linux per l'interrogazione dei server DNS.

Iniziamo subito collegandoci con un browser della macchina fisica all'indirizzo ip 192.168.0.75 e accediamo all'interfaccia di ZeroShell inserendo username e password, rispettivamente "admin" e "zeroshell";
A sinistra, all'interno della sezione "NETWORK" selezioniamo la scheda "DNS" e facciamo click sul pulsante create in alto a destra;
Si apre una finestra in cui inseriamo i seguenti parametri della zona DNS da creare:

Domain name: labpentest.hj
Master server: 212.100.1.1
Email contact: root@labpentest.hj

Ignoriamo temporaneamente i restanti campi e facciamo click su "Submit".

Adesso inseriamo il primo host, il server web.
Nella sezione "Entry commands", clicchiamo su "New" e nella finestra che si aprirà inseriamo i seguenti campi:
Entry name: www
TTL: 1
address: 212.100.1.2

Clicchiamo su "Save" per confermare la richiesta di creazione dell'entry e ripetiamo la procedura (inserendo valori diversi nei campi ovviamente) per aggiungere il server ftp:Entry name: ftp
TTL: 1
address: 212.100.1.3

Ancora una volta concludiamo premendo su "Save" e avremo popolato la nostra zona DNS.

2.2 MODIFICA DELLE IMPOSTAZIONI DI SICUREZZA DI ZEROSHELL

Prima di passare alla macchina "Pentester" dobbiamo cliccare su "Clients" nella sezione superiore della pagina e aggiungere nella voce "IP" l'ip 210.100.1.1 ovvero l'indirizzo della macchina attaccante, premere "+" e infine "Save".
Ciò é necessario in quanto ZeroShell ha delle funzioni integrate di sicurezza che consentono solo agli host autorizzati di collegarsi al server DNS. Tale modifica serve appunto a consentirci di utilizzare i tool di interrogazione del DNS dalla macchina attaccante.

2.3 UTILIZZO DELLA MACCHINA PENTESTER E DEI TOOL DI KALI LINUX

Ora che la rete di test con zona DNS perfettamente configurata è pronta, ci spostiamo sulla VM "Pentester" e su una shell digitiamo:

echo nameserver 212.100.1.1 > /etc/resolv.conf

Adesso la macchina con Kali Linux risolverà i nomi dei siti web tramite il server DNS configurato su ZeroShell.

Su ternminale lanciamo i seguenti comandi che ci consentiranno di acquisire sempre più informazioni sulla rete target:

#dig labpentest.hj NS
#dig labpentest.hj SOA
#dig labpentest.hj MX
#dig labpentest.hj A
#dig labpentest.hj AXFR
#fierce -dns labpentest.hj

Come si può notare, solo fierce è stato in grado di fornirci un quadro completo della rete target. Per maggiori informazioni riguardo il comando fierce raccomando di leggere la documentazione presente sul seguente link: https://tools.kali.org/information-gathering/fierce

3.1 CREAZIONE DI UNA NUOVA MACCHINA VIRTUALE PER L'UTILIZZO DI WHOIS.

Nel numero 217 viene creata una nuova VM che a differenza della prima, collegata al laboratorio virtuale, sarà in grado di sfruttare la stessa connettività della macchina fisica e pertanto ci consentirà di utilizzare un nuovo strumento presente in Kali Linux, come in tutte le altre distribuzioni Linux in circolazione.

Macchina "Kali"

Sistema operativo --------> Linux (Debian a 64 bit);

RAM ----------> 1024 MB;

Disco fisso ----------> Nessuno;

Archiviazione ----------> Dopo aver creato la macchina virtuale, aggiungere un nuovo controller IDE inserendovi l'ISO di Kali Linux;

Rete ----------> Una scheda di rete, impostata in modalità "Scheda con bridge".

3.2 UTILIZZO E DESCRIZIONE DEL COMANDO WHOIS.

Avviamo la macchina virtuale "Kali" e lanciamo una shell per digitare il comando whois verso google.it.
Naturalmente nessuno di noi qui rischia tre anni di galera (conseguenza legale di cui la rivista ci rende ben consapevoli nel caso in cui vengano utilizzati strumenti di pentesting verso sistemi che non siano di nostra proprietà o senza la manleva del proprietario) poiché con questo semplice comando si ottengono informazioni assolutamente lecite riguardo il proprietario di un dominio presente in rete.

Personalmente consiglio di utilizzare con cautela gli strumenti di questa nuova macchina virtuale soprattutto se collegata in rete (così da poter fare sogni tranquilli senza visite della polizia postale) e di limitarsi alle istruzioni della rivista.

Tornando alla nostra shell:

#whois www.google.it

Come descritto nella rivista, l'output di questo comando fornisce diverse informazioni catalogate nei seguenti campi:

Created ----------> Indica la data di creazione del dominio.

Expire date ----------> La data di scadenza oltre il quale il nome di dominio può essere messo a disposizione di chiunque ne faccia richiesta.

Registrant ----------> Fornisce informazioni sul proprietario del dominio.

Admin Contact -------> Mostra informazioni di contatto del Registrant dell'amministratore del sito.

Techical Contact -----> Mostra informazioni di contatto del Registrant per motivi tecnici relativi al dominio.

Registrar ----------> Visualizza le informazioni riguardanti la società di servizi internet a cui si è rivolto il registrant per la registrazione del dominio.

3.3 USO DI WHOIS CON L'INDIRIZZO IP.

Dopo aver imparato ad usare whois sui nomi di un dominio l'articolo ci mostra come tale comando possa essere usato anche con indirizzi ip numerici:

#dig www.google.it A
#whois 216.58.205.99

Come imparato nel numero precedente, il comando dig usato in questo modo ci fornisce l'ip dell'host che useremo nel comando successivo, rivelandoci l'intera classe di indirizzi appartenenti al registrant (in questo caso 216.58.192.0/19, cioé tutti gli indirizzi compresi tra 216.58.192.0 e 216.58.223.255).