M1W4D4

Assegnare IP a macchina virtuale Kali con indirizzo 192.168.32.100, assegnare IP a macchina virtuale Windows 10 con indiirzzo 192.168.32.101, Servizio HTTPS e DNS attivo su entrambe le macchine. Poi simulare in ambiente virtuale che la macchina Windows 10 richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo di Kali. Fare questo passaggio sia con HHTP che HTTPS

Di seguito intercettare tramite Wireshark le comunicazioni evidenziando l’indirizzo MAC sorgente destinazione ed il contenuto della richiesta sia HTTP sia HTTPS evidenziando le eventuali differenze.

Primo passaggio: impostare indirizzo statico di Kali (192.168.32.100) scrivendo sulla riga di comando: *sudo nano /etc/network/interfaces*

*sudo*: permette le operazioni come amministratore di Sistema, *nano*: è l’editor di testo col quale modifichiamo il file all’interno del *path* (percorso) */etc/network/interfaces*.

Una volta aperto l’editor di testo bisogna scrivere le seguenti righe:

auto eth0

iface eth0 inet static

address 192.168.32.100/24

gateway 192.168.32.1

oppure

address 192.168.32.100

netmask 255.255.255.0

Cliccare *Ctrl-O* per salvare e premere *Enter* per confermare, inoltre per assicurarsi che il processo vada in porto eseguire il seguente comando per riavviare il servizio di rete: *sudo systemctl restart networking*

Immagine che contiene nero, oscurità

Descrizione generata automaticamenteSecondo passaggio: impostare indirizzo statico di Windows 10 (192.168.32.101) andando su simbolo dell’Ethernet in basso a destra -> Centro Connessioni -> Modifica Opzioni Scheda -> (Su Ethernet) Proprietà -> Protocollo IPv4 e inserire come di seguito:

IP: 192.168.32.101

Subnet Mask: 255.255.255.0

Gateway predefinito: 192.168.32.1

DNS preferito: 192.168.32.100

Di entrambe le connessioni assicurarsi che siano entrambe su NAT con rete privata (se si vuole che abbiamo la connessione Internet sfruttata dalla propria macchina host) o Internal in modo tale che comunichino tra loro in un’ambiente completamente chiuso e senza accesso ad Internet. -> Per farlo bisogno andare su Oracle Virtual Box e sulla Home selezionare le macchine in questione -> Impostazioni -> Rete -> NAT o Internal.

Possiamo fare la simulazione di richieste tramite l’app INetSim all’interno di Kali

Prima di tutto controlliamo aggiornamenti su Kali tramite il comando: *sudo apt update* e nel caso *sudo apt upgrade*.

Controllare che sia installato INetSim *sudo apt install inetsim*

Configuriamo ora il servizio tramite il comando: sudo nano /etc/intetsim/inetsim.conf

Configurare l’indirizzo IP di Kali con i seguenti comandi:

*service\_bind\_address 192.168.32.100*

*service\_bind\_port\_dns 53*

Abilitare il servizio DNS personalizzato con l’indirizzo di Kali: *dns\_default\_ip 192.168.32.100*

Il servizio HTTPS lo si abilita tramite il certificato e la chiave annessa:

*ssl\_certificate /etc/inetsim/certs/server-cert.pem*

*ssl\_private\_key /etc/inetsim/certs/server-key.pem*

Per poterlo mettere in atto bisogna autofirmarlo con il comando: *sudo inetsim-make-cert*

Ed infine avviare INetSim col comando: *sudo inetsim*

Bisogna assicurarsi la configurazione del DNS su Win10 tramite il comando: *nslookup epicode.internal* e deve avere come risultato l’IP 192.168.32.100

La richiesta viene fatta andando sul browser e digitando <http://epicode.internal> per l’http mentre è: <https://epicode.internal> per l’HTTPS

Nel caso non vada potrebbe essere un problema del Firewall di W10 che blocca le connessioni della porta 80 per l’HTTP e 443 per l’HTTPS.

La prima azione preliminare è pingare le due macchine per assicurarsi che siano connesse: ping 192.168.32.100 da Windows 10 verso Kali e ping 192.168.32.101 per Kali verso Windows 10.

Selezionare l’interfaccia di rete corretta: eth0 nella fattispecie

Poi si cattura il traffico HTTP filtrando *http or tcp.port == 80* e cliccando su “start capture”.

Generare la richiesta da W10 scrivendo dal browser [*http://epicode.internal*](http://epicode.internal) o dal promt dei comandi con: *curl* [*http://epicode.internal*](http://epicode.internal)

Per il traffico HTTPS il discorso è diverso essendo crittografato, filtriamo da Wireshark su Kali: tl*s or tcp.port == 443* mentre da W10 scriviamo sul browser: [*https://epicode.internal*](https://epicode.internal)

Una volta fatto bisogna decrittografare il traffico, bisogna ottenere la chiave privata e il certificato nel percorso: */etc/inetsim/certs*

Bisogna poi configurare Wireshark per la crittazione *TLS* seguendo i seguenti passaggi: *Edit -> Preferences -> Protocols -> TLS -> (Pre-)Master -Secret log filename* specificando o il percorso del file per chiavi private o si inserisce manualmente la chiave.

Si filtra *TLS* e si osserva il tutto.