DOMANDE NOTE:

Wireshark:

- dimmi se il sito (es. di mediaworld) ha il server del proprio sito gestito da loro o da una terza azienda.
    a. RISPOSTA:
        - lancia nslookup www.mediaworld.it per scoprire l'ip del server;
        - lancia whois mediaworld.it per scoprire le persone e le aziende che gestiscono mediaworld;
        - lancia whois sull'IP ricavato dal punto 1 per vedere se coincide con quanto ottenuto dal punto 2 (una cosa è a chi è affidato il controllo del sito, un altro è chi effettivamente gestisce il lato IT del sistema);
        - Osserviamo dalle foto che sono entrambe gestite da IANA.

```
martin@Martin-HP:~$ whois mediaworld.it

**************************************************
* Please note that the following result could be a
* the data contained in the database.
*
* Additional information can be visualized at:
* http://web-whois.nic.it
**************************************************

Domain:             mediaworld.it
Status:             ok
Signed:             no
Created:            1998-06-10 00:00:00
Last Update:        2024-06-12 01:12:02
Expire Date:        2025-06-12

Registrant
  Organization:     MMS Intangibles GmbH & Co. KG
  Address:          Media-Saturn-Str. 1
```

```
martin@Martin-HP:~$ whois 127.0.0.53

#
# ARIN WHOIS data and services are subject to the Terms of
# available at: https://www.arin.net/resources/registry/who
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_
#
# Copyright 1997-2025, American Registry for Internet Numbe
#


NetRange:       127.0.0.0 - 127.255.255.255
CIDR:           127.0.0.0/8
NetName:        SPECIAL-IPV4-LOOPBACK-IANA-RESERVED
NetHandle:      NET-127-0-0-0-1
Parent:          ()
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:
Updated:        2024-05-24
Comment:        Addresses starting with "127." are used whe
Comment:        Protocol.  127.0.0.1 is the most commonly u
Comment:
Comment:        These addresses were assigned by the IETF,
Comment:        be found here:
Comment:        http://datatracker.ietf.org/doc/rfc1122
Ref:            https://rdap.arin.net/registry/ip/127.0.0.0



OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
```

- perchè WSH ha bisogno di sudo?

    a. RISPOSTA: Perchè WSH deve ordinare alla scheda di rete, quindi interfacciandosi con l'hardware, di entrare in modalità promiscua. In questa modalità, la scheda "ascolta" e inoltra al sistema operativo tutti i pacchetti che vede, indipendentemente dal loro destinatario.
- cos'è il protocollo ARP?
    a. RISPOSTA: ARP (Address Resolution Protocol) è un protocollo che mappa gli indirizzi IP (logici) agli indirizzi MAC (fisici). Serve a un dispositivo per scoprire l'indirizzo MAC di un altro dispositivo che si trova sulla stessa rete locale. Il dispositivo invia un ARP Request (domanda broadcast: "Chi ha questo IP? Dammi il tuo MAC"); il destinatario con quell'IP risponde con un ARP Reply (invio del suo MAC). Il mittente salva la coppia IP-MAC nella sua cache ARP.
- Perché i contenuti della maggior parte dei pacchetti sono illeggibili? Come si può comprenderli?
    a. RISPOSTA: I payload non si possono leggere perché sono cifrati. No, non è possibile comprendere direttamente il contenuto cifrato di un messaggio catturato su Wireshark. È possibile decifrarlo e leggerlo solo se si possiede la chiave di decifratura (es. la chiave simmetrica di sessione per TLS, o la chiave pre-condivisa per WPA2), e la si fornisce a Wireshark che è in grado di eseguire la decifratura in automatico.
- Quali protocolli (es. HTTP, FTP) trasmettono dati in chiaro? Che implicazioni di sicurezza ha questo per le informazioni sensibili catturate con Wireshark?
    a. RISPOSTA: HTTP e FTP trasmettono in chiaro. Implicazione: credenziali e dati sensibili sono visibili a chi intercetta il traffico.
- Confronta la visibilità del contenuto dei dati catturati in una sessione FTP rispetto a una SSH. Perché questa differenza è cruciale dal punto di vista della sicurezza?
    1. RISPOSTA: FTP: dati visibili in chiaro. SSH: dati cifrati e illeggibili. Cruciale perché SSH garantisce riservatezza, FTP no.

- Come possono comandi come ping e traceroute (analizzabili via Wireshark) o nslookup essere utilizzati per la ricognizione di rete da parte di un attaccante? Quali informazioni potrebbero ottenere?
    - RISPOSTA: usati per ricognizione. Ottengono host attivi (ping), topologia/router (traceroute), mappatura IP-dominio (nslookup).

Interfaccia Socket:

1. provare a vedere scambio pacchetti su WireShark durante connessione client-server di questa esercitazione;
2. dove avvengono nei codici l'inizializzazione delle connessioni? le send e le receve? le interfacce socket dove sono?
3. cos'è il socket?
4. quanti protocolli usa? perchè? c'è lo stesso codice?
5. criterio per scegliere TCP o UDP? Vantaggi e svantaggi?

WebServices:

1. viene richiesto di eseguire l'ultimo esercizio. sfruttare le archietture dei microservizi. Che problema esce, se c'è? calcolare il tempo di esecuzione (ottimizzato e non);

WebSocket:

1. eseguire tutti gli esercizi;
2. come è fatta la web chat degli esercizi?
3. cos'è una web socket?
4. cos'è/cosa fa HTTP UPGRADE?
5. a che livello opera websocket?
6. che funzione websocket non si può fare con HTTP?
7. da chi parte la richiesta? -> sempre client
8. cosa permette di fare il websocket?

Modello PUB/SUB:

1. cos'è PUB e SUB? Perchè si usano? Vantaggi e svantaggi?
2. cos'è e cosa fa il broker?
3. quali sono i wizard pattern?

Sicurezza:

1. come si fa a fare riservatezza con un messaggio di posta elettronica;
2. come si fa a fare firma digitale con un messaggio di posta elettronica;
3. come si mettono insieme le due cose (potrebbe anche richiedere schemi disegnati);
4. Come avviene la registrazione sicura di un utente?
5. Backend/Frontend dove avviene lo store e la cifratura (come?) delle psw?
6. l'app di web-chat websocket, che tipo di sicurezza usa?
7. l'esercizio non è sicuro, come potremmo fare per renderlo tale?
8. che proprietà possiede il TLS?
9. come fa a scambiarsi la chiave simmetrica?
10. esempio di vulnerabilità in un sistema pub/sub che non si può risolvere?
11. secondo me che non c'è un metodo di autenticazione per il broker, ossia non c'è modo di sapere se sto effettivamente comunicando con il broker che intendo o uno fittizio. Pov, non c'è modo di sostituire il broker, perchè? ->risposta: certificato autentico sull'ip del broker/server;
12. come posso rendere MQTT più sicuro con poco sforzo?
13. problema che TLS non può risolvere?