



ESPLORANDO LE POTENZIALITA' DI MITMPROXY

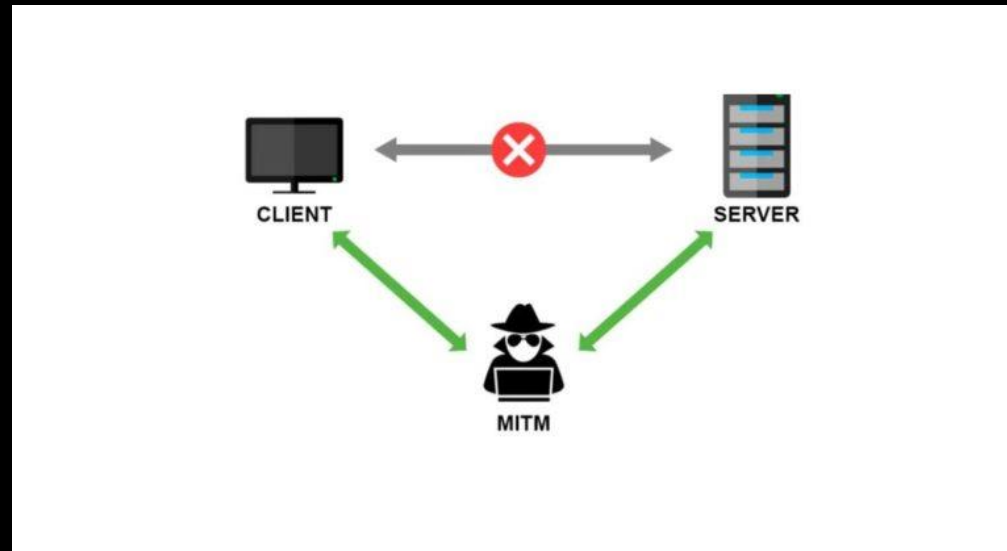
Federica Magliocca

The background features a solid black field. At the top, there is a wavy, translucent shape with a color gradient from yellow and orange on the left to green and blue on the right, resembling a stylized horizon or a liquid surface.

ATTACCO MAN IN THE MIDDLE

CHE COS'E' UN ATTACCO MITM

Un attacco MITM (Man-in-the-Middle) è una forma di attacco informatico in cui un attaccante si inserisce tra due parti comunicanti per intercettare, monitorare e talvolta modificare la comunicazione tra di loro, senza che nessuna delle due parti ne sia consapevole. In pratica, l'attaccante si inserisce in una posizione privilegiata tra la vittima e il destinatario desiderato, facendosi passare per il mittente legittimo verso il destinatario e viceversa.



CHE COS'E' UN ATTACCO MITM

Durante un attacco MITM, l'attaccante può accedere ai dati scambiati tra le due parti, inclusi messaggi, informazioni personali, credenziali di accesso, dettagli finanziari e altro ancora. L'attaccante può anche iniettare dati maligni nella comunicazione per manipolare i messaggi o convincere le parti coinvolte a compiere azioni indesiderate.

Questo tipo di attacco può essere sferrato per esempio:

- all'interno di una rete locale o di una rete Wi-Fi
- su Internet
- durante l'accoppiamento di due dispositivi Bluetooth
- durante un pagamento tramite Pos e carta contactless.

COME FUNZIONA UN ATTACCO MITM

Inizializzazione dell'attacco: L'attaccante crea una connessione con entrambe le parti coinvolte nella comunicazione. Ad esempio, potrebbe configurare una rete WiFi falsa o compromettere un dispositivo di rete.

Interposizione: Una volta che l'attaccante si trova tra le due parti, riesce a intercettare i dati che vengono scambiati tra di loro. L'attaccante può utilizzare varie tecniche per ottenere questo risultato, come lo "sniffing" dei pacchetti di dati che passano attraverso la rete.

COME FUNZIONA UN ATTACCO MITM:

Manipolazione dei dati: L'attaccante ha ora la possibilità di manipolare i dati trasmessi tra le due parti. Ad esempio, può modificare i messaggi inviati, inserire nuovi dati o eliminare parti dei dati. L'obiettivo può essere quello di ottenere informazioni riservate o alterare il contenuto della comunicazione.

Reindirizzamento: In alcuni casi, l'attaccante può anche reindirizzare la comunicazione verso un'altra destinazione. Ad esempio, può dirottare una connessione HTTPS a un server controllato dall'attaccante stesso, dove i dati possono essere intercettati e manipolati.

Nascondere la presenza: Per avere successo, un attacco MITM deve evitare di far sospettare alle parti legittime la sua presenza. L'attaccante può cercare di mantenere la comunicazione tra le parti apparentemente normale, ad esempio generando certificati falsi per garantire connessioni SSL o TLS.

ESEMPIO

Quando due parti iniziano una conversazione, in genere stabiliscono una connessione e si scambiano le cosiddette chiavi pubbliche, utilizzate per crittografare le conversazioni.

Immaginiamo che Alice e Bob “chattino” sul web. Quando Alice si rivolge a Bob, invia la sua chiave pubblica. Bob cripterà tutti i messaggi di Alice con la sua chiave pubblica.

Bob a sua volta invia a Alice la sua chiave pubblica. Quando Alice riceve il messaggio cifrato da Bob, lo decifra con la sua chiave privata e lo legge.

Ora immaginiamo una terza persona tra Alice e Bob. Il suo nome è Peter.

Peter intercetta la chiave pubblica di Alice mentre viaggia verso Bob e la sostituisce con la propria chiave pubblica. Poi intercetta la chiave pubblica di Bob e la sostituisce con la propria mentre viaggia verso Alice.

ESEMPIO

Ora sia Alice che Bob criptano le informazioni con la chiave pubblica di Peter e Peter può decifrarle con la propria chiave privata.

Dopo la decrittazione, legge il messaggio, forse lo altera, quindi lo cripta con la chiave pubblica di Alice intercettata nella prima fase e lo inoltra a Alice.

In questo modo cripta tutte le comunicazioni da e verso Bob o Alice e nessuno dei due sa che sta origliando.

TIPOLOGIE DI MITM: ARP SPOOFING

L'ARP Spoofing è una tecnica di attacco Man-in-the-Middle (MITM) che sfrutta il protocollo Address Resolution Protocol (ARP) per intercettare o manipolare il traffico di rete tra due o più dispositivi all'interno di una rete locale.

Il protocollo ARP viene utilizzato per associare gli indirizzi IP agli indirizzi MAC all'interno di una rete; quando un dispositivo nella rete desidera comunicare con un altro dispositivo, invia una richiesta ARP broadcast chiedendo chi detiene un determinato indirizzo IP. Il dispositivo con l'indirizzo IP corrispondente risponderà con il suo indirizzo MAC, consentendo ai dispositivi di comunicare tra di loro.

Nell'ARP Spoofing, un aggressore invia falsi pacchetti ARP nella rete, facendo credere ai dispositivi che l'indirizzo MAC dell'aggressore corrisponda all'indirizzo IP del dispositivo di destinazione. Di conseguenza, quando i dispositivi nella rete cercano di comunicare con il dispositivo di destinazione, invieranno il traffico di rete all'indirizzo MAC dell'aggressore anziché al dispositivo reale.

TIPOLOGIE DI MITM: DNS SPOOFING

Il DNS Spoofing è un tipo di attacco informatico in cui un aggressore manipola le risposte DNS (Domain Name System) per indirizzare gli utenti verso un indirizzo IP diverso da quello corretto.

Quando un utente cerca di accedere a un sito web utilizzando il suo nome di dominio, il suo dispositivo invia una richiesta DNS a un server DNS per ottenere l'indirizzo IP associato a quel nome di dominio. Il server DNS restituisce quindi la risposta contenente l'indirizzo IP corretto, consentendo al dispositivo di stabilire la connessione con il server web corrispondente.

Nel DNS Spoofing, l'attaccante riesce a modificare o corrompere le risposte DNS in modo che gli utenti vengano indirizzati verso un indirizzo IP controllato dall'attaccante anziché verso l'indirizzo IP reale del server legittimo. Ciò può essere fatto sfruttando vulnerabilità nei server DNS o inserendo informazioni di risoluzione dei nomi false nella cache DNS.

TIPOLOGIE DI MITM: SSL STRIPPING

SSL Stripping è un tipo di attacco Man-in-the-Middle che mira a bypassare o rimuovere la crittografia SSL/TLS (Secure Sockets Layer/Transport Layer Security) tra un client e un server, consentendo all'attaccante di intercettare e manipolare il traffico di rete.

Quando un client si connette a un server tramite HTTPS (HTTP Secure), l'attaccante intercetta la comunicazione e cerca di forzare una connessione non crittografata (HTTP) anziché la connessione crittografata (HTTPS). Ciò può essere fatto manipolando i pacchetti di rete o inserendo modifiche nella comunicazione.

TIPOLOGIE DI MITM: SSL STRIPPING

Il processo avviene tipicamente in tre fasi:

L'attaccante intercetta la richiesta del client al server e invia una risposta falsificata al client, facendogli credere che la connessione sia solo HTTP e non HTTPS.

Il client riceve la risposta falsificata e, a causa della manipolazione, potrebbe convertire la connessione in HTTP invece di mantenere la connessione crittografata.

L'attaccante riesce quindi a intercettare il traffico di rete tra il client e il server, avendo accesso ai dati non crittografati scambiati tra di loro.

TIPOLOGIE DI MITM: SESSION HIJACKING

Il session hijacking, noto anche come session snatching o sidejacking, è un tipo di attacco in cui un aggressore ottiene il controllo di una sessione utente valida per accedere a un sistema o a un'applicazione senza autorizzazione. L'obiettivo principale dell'attacco di session hijacking è assumere l'identità dell'utente legittimo per eseguire operazioni malevole o ottenere informazioni sensibili.

Le sessioni utente vengono utilizzate per mantenere lo stato e l'identità dell'utente durante una sessione di interazione con un'applicazione o un sistema. Una sessione può essere identificata da un token di sessione o da un cookie che viene scambiato tra il client e il server per autenticare e autorizzare l'utente.

TIPOLOGIE DI MITM: SESSION HIJACKING

Esistono diverse tecniche utilizzate per eseguire un attacco di session hijacking:

Sniffing di pacchetti: L'attaccante monitora il traffico di rete per catturare pacchetti contenenti informazioni di autenticazione, come cookie di sessione, e li utilizza per impersonare l'utente legittimo.

Session prediction: L'attaccante tenta di prevedere o generare in modo casuale l'identificatore di sessione valido per ottenere accesso non autorizzato.

Session stealing: L'attaccante ruba il token di sessione o il cookie di un utente legittimo utilizzando tecniche come Cross-Site Scripting (XSS) o Cross-Site Request Forgery (CSRF).

Session fixation: L'attaccante forza l'utente a utilizzare un'identificazione di sessione specifica, che l'attaccante conosce e può sfruttare per assumere il controllo della sessione.

TIPOLOGIE DI MITM: EVIL TWIN

L'Evil Twin, noto anche come attacco Twin AP, è un tipo di attacco informatico in cui un aggressore crea una rete Wi-Fi falsa che appare come una rete legittima al fine di intercettare il traffico di rete degli utenti e condurre attacchi di tipo Man-in-the-Middle (MITM).

Nell'Evil Twin, l'attaccante crea una rete Wi-Fi con un nome di rete (SSID) e un'interfaccia di accesso che corrispondono a quelli di una rete Wi-Fi legittima a cui gli utenti desiderano connettersi. Questo può essere fatto utilizzando strumenti specializzati o dispositivi come router wireless configurati appositamente per l'attacco.

Quando gli utenti cercano di connettersi alla rete Wi-Fi, possono vedere il nome di rete (SSID) legittimo nella lista delle reti disponibili e possono connettersi all'Evil Twin senza rendersi conto che si tratta di una rete falsa.

TIPOLOGIE DI MITM: EVIL TWIN

Alcuni possibili attacchi che possono essere eseguiti tramite un Evil Twin includono:

Sniffing di pacchetti: L'attaccante può intercettare e leggere i pacchetti di dati scambiati tra gli utenti e i server a cui sono connessi, consentendo di raccogliere informazioni sensibili come nomi utente, password o dati personali.

Spoofing di accesso: L'attaccante può intercettare le richieste di login degli utenti e inviare pagine di login falsificate, cercando di raccogliere le credenziali di accesso degli utenti.

Iniezione di contenuti malevoli: L'attaccante può iniettare contenuti malevoli o modificare le pagine web visualizzate dagli utenti, cercando di eseguire attacchi come il **phishing** o l'iniezione di **malware**.

TIPOLOGIE DI MITM: IP SPOOFING

L'IP Spoofing è una tecnica utilizzata per manipolare l'indirizzo IP di origine di un pacchetto di rete in modo da mascherare l'identità dell'attaccante o indirizzarlo a un indirizzo IP falso. Questo tipo di attacco viene spesso utilizzato per condurre attacchi di tipo Denial of Service (DoS) o per nascondere l'origine di un attacco.

Nell'IP Spoofing, l'attaccante modifica manualmente l'indirizzo IP di origine del pacchetto in modo che sembri provenire da un altro indirizzo IP, che può essere un indirizzo IP valido o un indirizzo IP inesistente.

L'obiettivo principale dell'IP Spoofing è quello di ingannare i dispositivi di rete di destinazione facendoli credere che il pacchetto provenga da una fonte affidabile o legittima. Ciò può consentire all'attaccante di bypassare misure di sicurezza, filtraggi o limitazioni basate sull'indirizzo IP.

TIPOLOGIE DI MITM: IP SPOOFING

Gli attacchi di IP Spoofing possono essere utilizzati per:

Denial of Service (DoS): Un attaccante può inviare un grande numero di pacchetti con indirizzi IP falsificati a un sistema o a una rete, sovraccaricandoli e impedendo il normale funzionamento dei servizi.

Smurf Attack: In questo tipo di attacco, l'attaccante invia pacchetti ICMP Echo Request (ping) con un indirizzo IP falsificato come indirizzo di origine a una rete di computer che risponderanno tutti insieme alla vittima reale, creando un effetto di amplificazione del traffico.

Spoofing di identità: Un attaccante può impersonare un indirizzo IP legittimo per eludere le misure di autenticazione o accesso ai sistemi.

Nascondere l'origine: L'IP Spoofing può essere utilizzato per nascondere l'origine di un attacco, rendendo difficile risalire all'attaccante.



CERTIFICATI DIGITALI

INTRODUZIONE AI CERTIFICATI DIGITALI

I certificati digitali sono strumenti crittografici utilizzati per proteggere la comunicazione online, autenticare l'identità delle parti coinvolte in una transazione e garantire la riservatezza delle informazioni.

Un certificato digitale è un file che contiene informazioni relative all'identità del titolare del certificato (ad esempio, nome, indirizzo e-mail) e una chiave pubblica associata.

La chiave pubblica è utilizzata per crittografare i dati, mentre la chiave privata corrispondente, che viene mantenuta segreta dal titolare del certificato, viene utilizzata per decrittografare i dati.

INTRODUZIONE AI CERTIFICATI DIGITALI

I certificati digitali sono ampiamente utilizzati in vari contesti, come il commercio elettronico, l'accesso remoto sicuro, la firma digitale dei documenti e la crittografia delle e-mail.

Consentono di stabilire connessioni sicure e autenticate, contribuendo a proteggere la privacy e la sicurezza delle informazioni trasmesse online.



TIPI DI INFORMAZIONI CONTENUTE NEI CERTIFICATI DIGITALI

Le informazioni che i certificati digitali devono riportare sono stabilite da un protocollo che a livello internazionale ne definisce il formato e il contenuto. Lo standard più popolare è l'ITU-T X.509. In base a tale standard, le informazioni riportate da un certificato digitale sono:

- Versione del certificato
- Numero seriale del certificato
- ID dell'algoritmo (algoritmo e parametri)
- Ente che ha emesso il certificato
- Periodo di validità del certificato (espresso come intervallo di tempo compreso tra un "non prima" e un "non dopo")
- Nome del soggetto
- Informazioni sulla chiave pubblica del soggetto (algoritmo, parametri e chiave pubblica)
- Codice identificativo univoco dell'ente emittente
- Codice identificativo univoco del soggetto
- Estensioni che può avere il certificato
- Algoritmo di firma del certificato
- Parametri di firma
- Firma del certificato

COME OTTENERE UN CERTIFICATO DIGITALE

Per avere un certificato digitale bisogna rivolgersi ai prestatori di servizi fiduciari accreditati, che possono essere pubblici o privati.

Un prestatore di servizi fiduciari accreditato è un'Autorità di Certificazione (**Certification Authority**, anche indicata con l'acronimo CA) che rappresenta una terza parte fidata, cioè un organismo deputato al rilascio dei certificati digitali e che viene riconosciuto affidabile dalle parti che ricorrono a esso per tale servizio.

COME OTTENERE UN CERTIFICATO DIGITALE

La CA firma digitalmente il certificato con la sua chiave privata e lo rende pubblico, affinché tutti possano sapere della sua esistenza e del fatto che vi sia una chiave pubblica associata al soggetto richiedente il certificato.

La pubblicità dei certificati digitali è garantita dal fatto che ogni CA mantiene un registro pubblico dei certificati digitali emessi e tuttora validi.

COME OTTENERE UN CERTIFICATO DIGITALE

Un certificato può essere sospeso o revocato perché, ad esempio, è avvenuta una compromissione della chiave privata oppure è cambiato un dato identificativo del soggetto.

In questi casi il certificato viene rimosso dalla lista dei certificati validi e viene inserito nella lista dei certificati sospesi (Certificate Suspension List) o nella lista dei certificati revocati (**Certificate Revocation List**).

COSA GARANTISCE LA VALIDITÀ DEI CERTIFICATI DIGITALI

Un certificato per essere considerato valido deve, quindi, essere firmato digitalmente con la chiave privata di una Certification Authority (CA) considerata affidabile da entrambe le parti.

Inoltre i certificati digitali hanno una validità temporale specifica, che è indicata nel certificato stesso. Questa validità determina il periodo durante il quale il certificato è considerato affidabile e può essere utilizzato per autenticare le comunicazioni.

La validità di un certificato digitale è determinata da due date:

- **Non prima:** indica il momento in cui il certificato diventa valido. Prima di questa data, il certificato non è ancora considerato affidabile.
- **Non dopo:** indica il termine della validità del certificato. Dopo la data di scadenza, il certificato non è più considerato affidabile e dovrebbe essere rinnovato o sostituito per continuare a garantire la sicurezza delle comunicazioni.



MITMPROXY

INTRODUZIONE AL MITM PROXY

Mitmproxy (Man-in-the-Middle proxy) è un tipo di proxy che, fungendo da intermediario tra un client e un server, consente di controllare, monitorare e manipolare il traffico di rete tra i due.

Il proxy agisce come un server verso il client e come client verso il server, in modo che possa ricevere le richieste del client, analizzarle e inviarle al server di destinazione.

Allo stesso modo, può ricevere le risposte dal server, analizzarle e inoltrarle al client originale.

INTRODUZIONE AL MITM PROXY

Quando Mitmproxy riceve una richiesta per stabilire una comunicazione TLS (sotto forma di un messaggio ClientHello), mette in attesa il client e prima effettua una connessione al server per "sniffare" il contenuto del suo certificato TLS.

Le informazioni ottenute (nome comune, organizzazione, nomi alternativi del soggetto) vengono quindi utilizzate per generare al volo un nuovo certificato di intercettazione, firmato dalla CA di Mitmproxy. Mitmproxy torna quindi al client e continua l'handshake con il certificato appena falsificato.

Questo significa che il browser del dispositivo sul quale verrà utilizzato mitmproxy deve essere configurato in modo tale da riconoscere la CA di mitmproxy come trusted.

INTRODUZIONE AL MITM PROXY

L'intercettazione del traffico consente al MITM proxy di esaminare i dati in transito e di effettuare diverse azioni.

Ad esempio, può filtrare e bloccare determinati tipi di contenuti, come siti web o file specifici, oppure può eseguire l'inserimento di contenuti aggiuntivi nelle risposte del server.

PRINCIPALI SCOPI DI UTILIZZO

MITM proxy può essere utilizzato per vari scopi, sia legittimi che malevoli:

- **Analisi del traffico di rete:** Un MITM proxy può essere utilizzato per analizzare il traffico di rete al fine di identificare potenziali minacce o vulnerabilità. Ad esempio, può essere impiegato per rilevare attacchi informatici, come tentativi di phishing o di infiltrazione nella rete.
- **Debugging e testing delle applicazioni:** I MITM proxy sono utili per il debugging e il testing delle applicazioni web. Consentono di intercettare e analizzare le richieste e le risposte tra il client e il server per individuare eventuali errori o problemi di prestazioni.

PRINCIPALI SCOPI DI UTILIZZO

- **Filtraggio del contenuto:** Un MITM proxy può essere utilizzato per filtrare il contenuto in base a determinati criteri. Ad esempio, può bloccare l'accesso a siti web ritenuti non sicuri o non conformi alle politiche aziendali. Può anche filtrare e bloccare il download di determinati tipi di file, come file eseguibili o contenuti multimediali.
- **Controllo dell'uso della rete:** I MITM proxy possono essere utilizzati per monitorare e controllare l'uso della rete da parte degli utenti. Possono tenere traccia delle attività di navigazione, limitare l'accesso a determinati siti web o controllare la larghezza di banda utilizzata da determinati servizi.

PRINCIPALI SCOPI DI UTILIZZO

- **Manipolazione del traffico:** Un MITM proxy può manipolare il traffico di rete al volo. Ad esempio, può iniettare contenuti aggiuntivi nelle pagine web visualizzate dal client, come annunci pubblicitari o avvisi.
- **Analisi delle prestazioni:** Un MITM proxy può essere utilizzato per monitorare e analizzare le prestazioni delle applicazioni e dei servizi web. Può registrare i tempi di risposta del server, la latenza di rete e altre metriche per identificare eventuali problemi di prestazioni.

QUALI CONTROLLI EFFETTUA MITMPROXY SUI CERTIFICATI

Quando un browser si connette a un server tramite HTTPS, esegue una serie di controlli sul certificato del server per garantire che la comunicazione sia sicura e che il server sia affidabile.

- Validità temporale
- Validità dell'autorità di certificazione (CA)
- Integrità del certificato
- Corrispondenza del nome del dominio
- Revoca del certificato
- Sicurezza del protocollo di crittografia

Se uno qualsiasi di questi controlli fallisce, il browser può avvertire l'utente che la connessione potrebbe non essere sicura o potrebbe richiedere l'interazione dell'utente per confermare la validità del certificato.

QUALI CONTROLLI EFFETTUA MITMPROXY SUI CERTIFICATI

L'obiettivo era verificare che MITM proxy eseguisse gli stessi controlli del browser sui certificati del server. Questo è stato fatto nel seguente modo:

- Creazione di un server web Apache
- Generazione di una Certification Authority(CA) con OpenSSL
- Generazione di un certificato server (non valido) con OpenSSL
- Configurazione del server con il certificato generato
- Installazione della CA come CA trusted nel browser (Google Chrome)
- Installazione della CA come CA trusted in mitmproxy
- Avvio di mitmproxy e verifica del suo comportamento

CREAZIONE SERVER APACHE

Creiamo una cartella per il nostro sito web in /var/www e inseriamo il file HTML:

- `sudo mkdir /var/www/mitm/`
- `cd /var/www/mitm/`
- `nano index.html`

```
GNU nano 6.2 index.html *
<html>

<body>

  <title> MITM </title>
  <h1> Man in the middle attack </h1>
</head>

<body>

  <p> Un attacco MITM (Man-in-the-Middle), tradotto in italiano "uomo n
  <p> In pratica, l'attaccante si inserisce in una posizione privilegiata tra l
  <p> Durante un attacco MITM, l'attaccante puo' accedere ai dati scambiati
  <p> L'attaccante puo' anche iniettare dati maligni nella comunicazione per
  <p> Questo tipo di attacco con tecnica Man In The Middle, puo' essere sferrato p
  <p> all'interno di una rete locale o di una rete domestica Wi-Fi </p>
  <p> su Internet </p>
  <p> durante l'accoppiamento di due dispositivi Bluetooth </p>
  <p> durante un pagamento tramite Pos e carta contacless. </p>

</body>

</html>
```

CREAZIONE SERVER APACHE

Configuriamo i file di configurazione di VirtualHost nella directory `/etc/apache2/sites-available/`:

- `sudo nano mitm.conf`

Puntiamo la direttiva `DocumentRoot` alla directory in cui sono ospitati i file del nostro sito:

- `DocumentRoot /var/www/mitm/`

Forniamo la direttiva `ServerName` con il nome del server:

- `ServerName mitm.local`

Attiviamo il file VirtualHost:

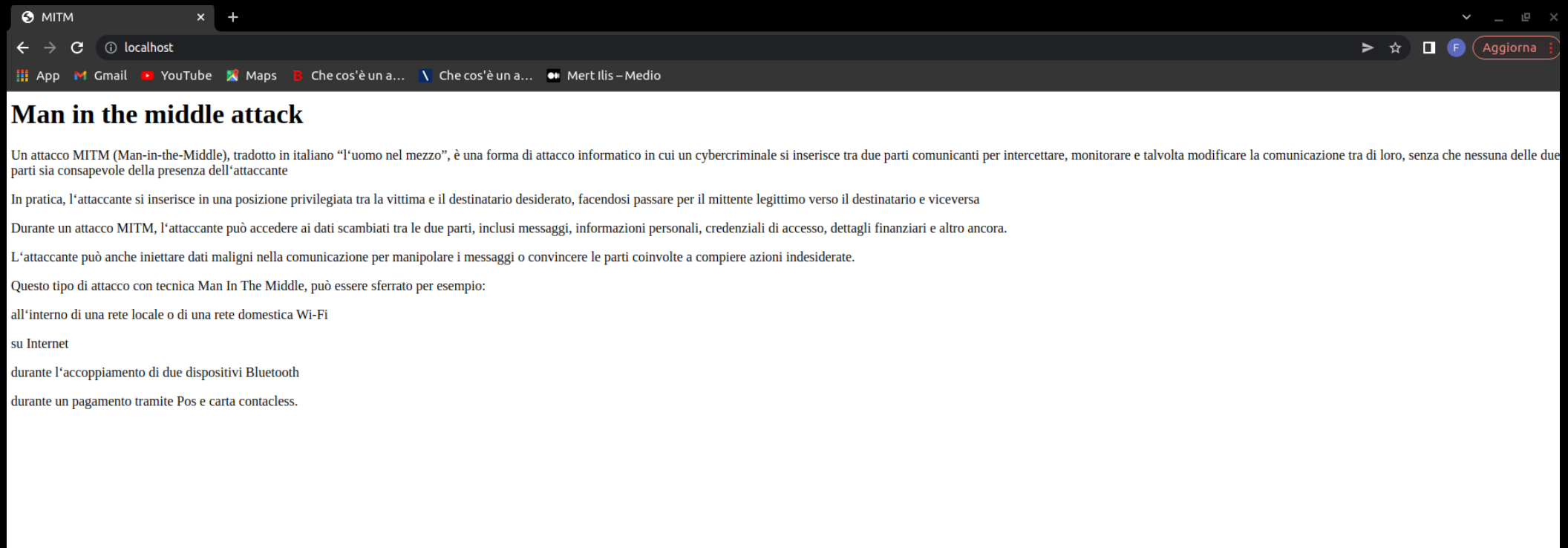
- `sudo a2ensite keliweb.conf`

Riavviamo apache per attivare la nuova configurazione:

- `sudo service apache2 restart`

CREAZIONE SERVER APACHE

- A questo punto digitando *http://localhost* nel browser otteniamo la nostra pagina web:



GENERAZIONE DI UNA CERTIFICATION AUTHORITY (CA) CON OPENSSL

Generiamo la chiave della CA:

- `openssl genrsa -out "root-ca.key" 4096`

Generiamo il certificato della CA:

- `openssl req -new -key "root-ca.key" -out "root-ca.csr" -sha256 -subj '/CN=Local Test Root CA'`

Configuriamo la CA creando un file "root-ca.cnf"

```
[root_ca]
```

```
basicConstraints = critical,CA:TRUE,pathlen:1
```

```
keyUsage = critical, nonRepudiation, cRLSign, keyCertSign
```

```
subjectKeyIdentifier=hash
```

Autofirmiamo il certificato della CA:

- `openssl x509 -req -days 3650 -in "root-ca.csr" -signkey "root-ca.key" -sha256 -out "root-ca.crt" -extfile "root-ca.cnf" -extensions root_ca`

GENERAZIONE DI UN CERTIFICATO SERVER CON OPENSSL

Generiamo la chiave del server:

- `openssl genrsa -out "server.key" 4096`

Generiamo il certificato del server:

- `openssl req -new -key "server.key" -out "server.csr" -sha256 -subj '/CN=mitm.local'`

Configuriamo il certificato del server creando un file "server.cnf":

```
[server]
```

```
authorityKeyIdentifier=keyid,issuer
```

```
basicConstraints = critical,CA:FALSE
```

```
extendedKeyUsage=serverAuth
```

```
keyUsage = critical, digitalSignature, keyEncipherment
```

```
subjectAltName = DNS:mitm.local, DNS:localhost, IP:127.0.0.1
```

```
subjectKeyIdentifier=hash
```

GENERAZIONE DI UN CERTIFICATO SERVER CON OPENSSL

Firmiamo il certificato con la chiave della CA generata in precedenza:

- `openssl x509 -req -days 750 -in "server.csr" -sha256 -CA "root-ca.crt" -CAkey "root-ca.key" -CAcreateserial -out "server.crt" -extfile "server.cnf" -extensions server`

A questo punto possiamo usare la chiave `server.key` e il certificato `server.crt` del server nella configurazione del nostro server Apache per abilitare la comunicazione SSL.

CONFIGURAZIONE DEL SERVER PER LA COMUNICAZIONE SSL

Aggiungiamo ai file di configurazione apache2.conf, default-ssl.conf e mitm.conf la chiave e il certificato del server per la comunicazione SSL:

```
<VirtualHost *:443>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

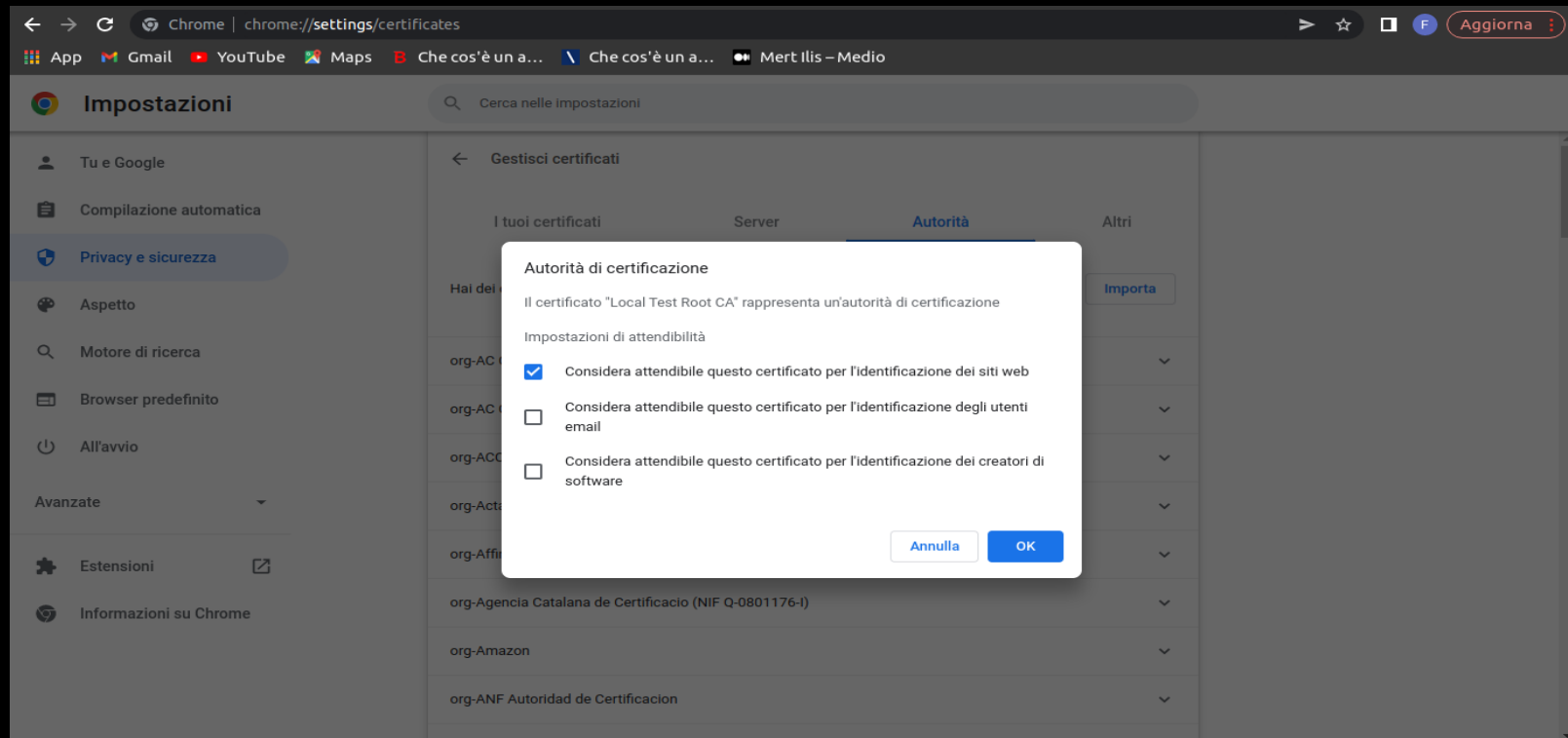
ServerName mitm.local

SSLEngine on
SSLCertificateFile /home/federica/server.crt
SSLCertificateKeyFile /home/federica/server.key

DocumentRoot "/var/www/mitm"
<Directory "/var/www/mitm">
    Options FollowSymLinks
    AllowOverride All
    Require all granted
</Directory>
```

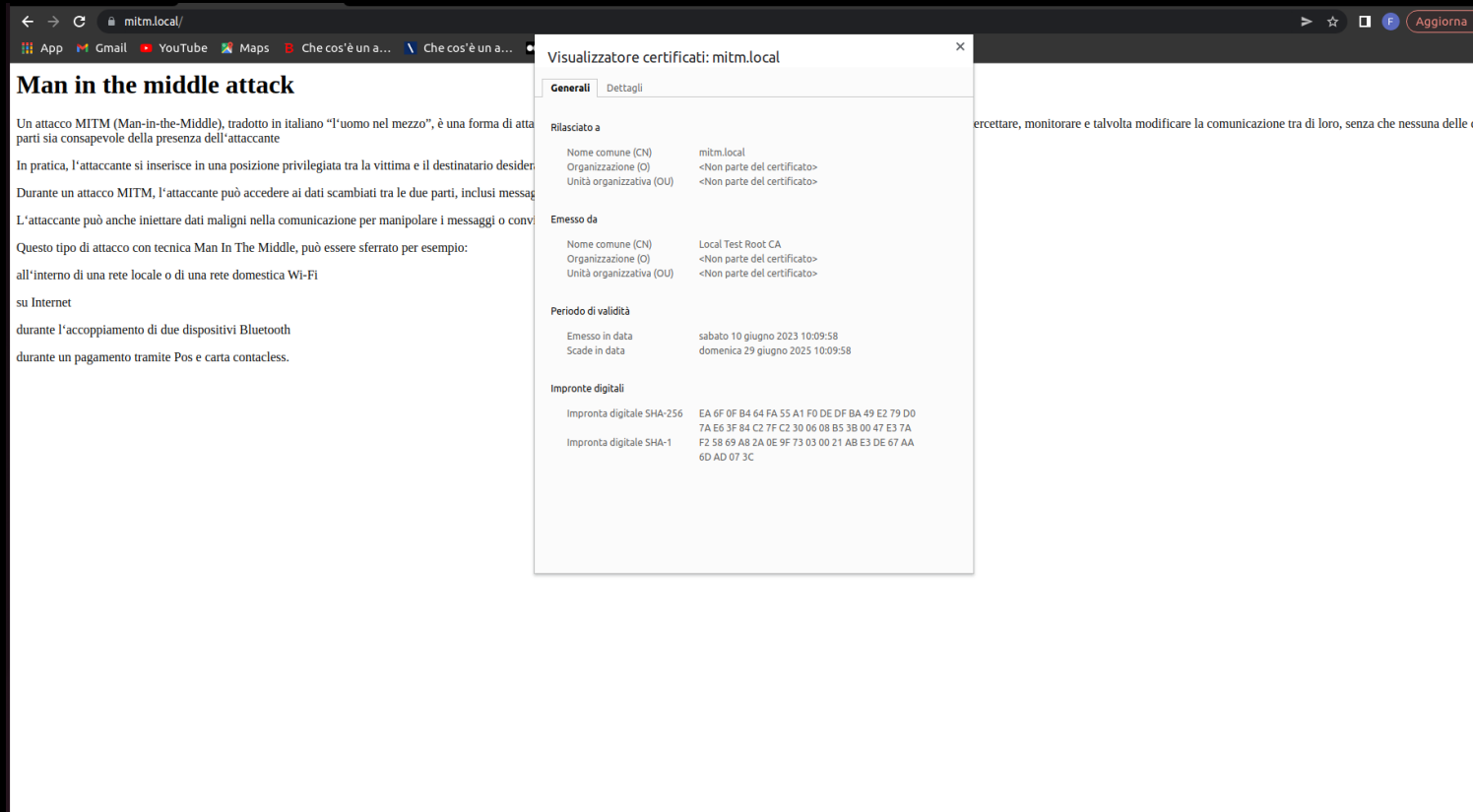
INSTALLAZIONE DELLA CA COME CA TRUSTED NEL BROWSER

Adesso è necessario configurare il browser del dispositivo in modo che riconosca come affidabile la Certification Authority (CA) che ha emesso il nostro certificato.



INSTALLAZIONE DELLA CA COME CA TRUSTED NEL BROWSER

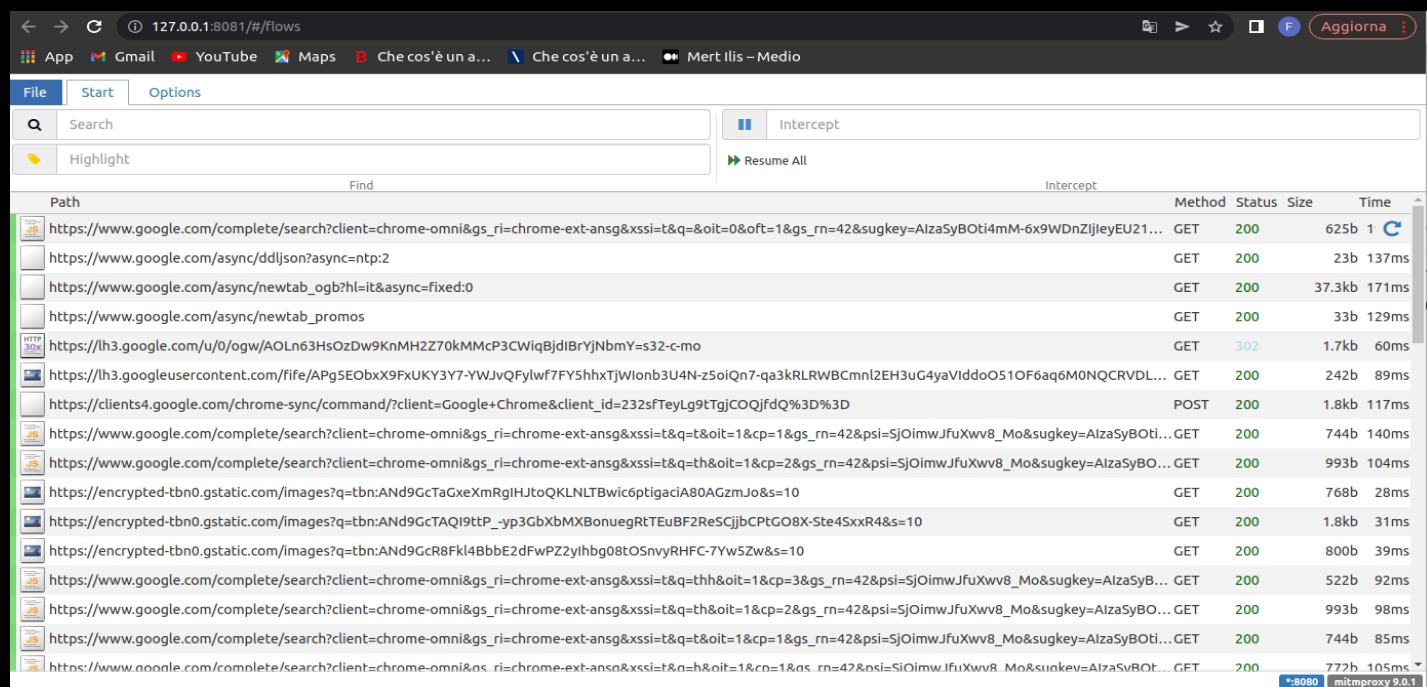
A questo punto se digitiamo nel browser l'indirizzo <https://mitm.local> possiamo accedere al nostro sito web e vedere che il certificato è valido poichè firmato da una CA considerata attendibile dal browser.



INSTALLAZIONE DELLA CA COME CA TRUSTED IN MIMTPROXY

Dopo aver installato mitmproxy e aver inserito la CA di mitmproxy nelle Certification Authority del browser possiamo avviare mitmproxy.

Avviamo l'interfaccia web di mitmproxy con il comando mitmweb per vedere l'analisi del traffico:



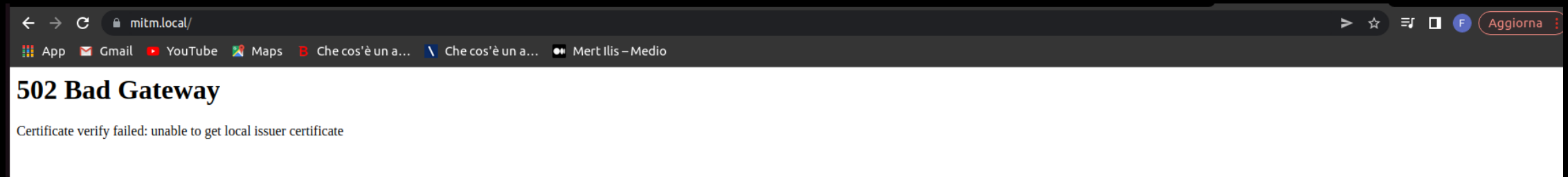
The screenshot shows the mitmproxy web interface in a browser. The address bar displays '127.0.0.1:8081/#/Flows'. The interface includes a search bar, a 'Highlight' button, and a 'Resume All' button. A table lists intercepted HTTP flows with columns for Path, Method, Status, Size, and Time. The table contains 15 entries, mostly GET requests to Google search and static image URLs. The status is consistently 200, and the size and time vary. The bottom right corner shows the mitmproxy version 9.0.1.

Path	Method	Status	Size	Time
https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=&oit=0&oft=1&gs_rn=42&sugkey=AlzaSyBOTi4mM-6x9WDnZijleyEU21...	GET	200	625b	1
https://www.google.com/async/ddljson?async=ntp:2	GET	200	23b	137ms
https://www.google.com/async/newtab_ogb?hl=it&async=fixed:0	GET	200	37.3kb	171ms
https://www.google.com/async/newtab_promos	GET	200	33b	129ms
https://lh3.googleusercontent.com/u/0/ogw/AOLn63HsOzDw9KnMH2Z70kMMcP3CWiqBjdiBrYjNbmY=s32-c-mo	GET	302	1.7kb	60ms
https://lh3.googleusercontent.com/fife/APg5EObx9FxyUKY3Y7-YWJvQFylw7FY5hhxTJWlonb3U4N-z5oiQn7-qa3kRLRWBcmnl2EH3uG4yaVlddoO51OF6aq6M0NQCRVDL...	GET	200	242b	89ms
https://clients4.google.com/chrome-sync/command/?client=Google+Chrome&client_id=232sfTeyLg9tTgJCOQjfdQ%3D%3D	POST	200	1.8kb	117ms
https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=t&oit=1&cp=1&gs_rn=42&psi=SjOimwJfuXwv8_Mo&sugkey=AlzaSyBOTi...	GET	200	744b	140ms
https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=th&oit=1&cp=2&gs_rn=42&psi=SjOimwJfuXwv8_Mo&sugkey=AlzaSyBO...	GET	200	993b	104ms
https://encrypted-tbn0.gstatic.com/images?q=tbn:AND9GcTaGxeXmRgIHJtoQKLNLTBwic6ptigaciA80AGzmJo&s=10	GET	200	768b	28ms
https://encrypted-tbn0.gstatic.com/images?q=tbn:AND9GcTAQI9tP_yp3GbXbMXBonuegRtEuBF2ReSCjibCPTGO8X-Ste4SxxR4&s=10	GET	200	1.8kb	31ms
https://encrypted-tbn0.gstatic.com/images?q=tbn:AND9GcR8Fkl4BbbE2dFwPZ2yIhbg08tOSnvyRHFC-7Yw5Zw&s=10	GET	200	800b	39ms
https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=thh&oit=1&cp=3&gs_rn=42&psi=SjOimwJfuXwv8_Mo&sugkey=AlzaSyB...	GET	200	522b	92ms
https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=th&oit=1&cp=2&gs_rn=42&psi=SjOimwJfuXwv8_Mo&sugkey=AlzaSyBO...	GET	200	993b	98ms
https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=t&oit=1&cp=1&gs_rn=42&psi=SjOimwJfuXwv8_Mo&sugkey=AlzaSyBOTi...	GET	200	744b	85ms
https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=h&oit=1&cp=1&gs_rn=42&psi=SjOimwJfuXwv8_Mo&sugkey=AlzaSyBOTi...	GET	200	772b	105ms

INSTALLAZIONE DELLA CA COME CA TRUSTED IN MIMTPROXY

Tuttavia se andassimo sul nostro sito web otterremo l'errore 502 BAD GATEWAY
(*Certificate verify failed: unable get local issuer certificate*)

Questo accade perchè mitmproxy si accorge che la CA che ha emesso il nostro certificato non è attendibile.



INSTALLAZIONE DELLA CA COME CA TRUSTED IN MIMTPROXY

Dobbiamo quindi inserire la nostra CA nella lista delle Certification Authority di MITM proxy. MITM proxy mantiene la lista delle CA attendibili nel pacchetto *certifi* di python.

Installiamo il pacchetto *certifi*:

- *pip install certifi*

E eseguiamo il seguente script python per inserire la nostra CA nella lista delle CA attendibili di MITMproxy

```
import certifi
import os
from OpenSSL.crypto import load_certificate, FILETYPE_PEM

def add_custom_ca():
    ca_path = "/home/federica/.mitmproxy/root_ca.pem" # Percorso del certificato della tua CA

    with open(ca_path, 'rb') as f:
        ca_cert_data = f.read()

    ca_cert = load_certificate(FILETYPE_PEM, ca_cert_data)

    # Aggiungi il certificato della tua CA al pacchetto certifi
    ca_bundle = certifi.where()
    with open(ca_bundle, 'ab') as f:
        f.write(ca_cert_data)

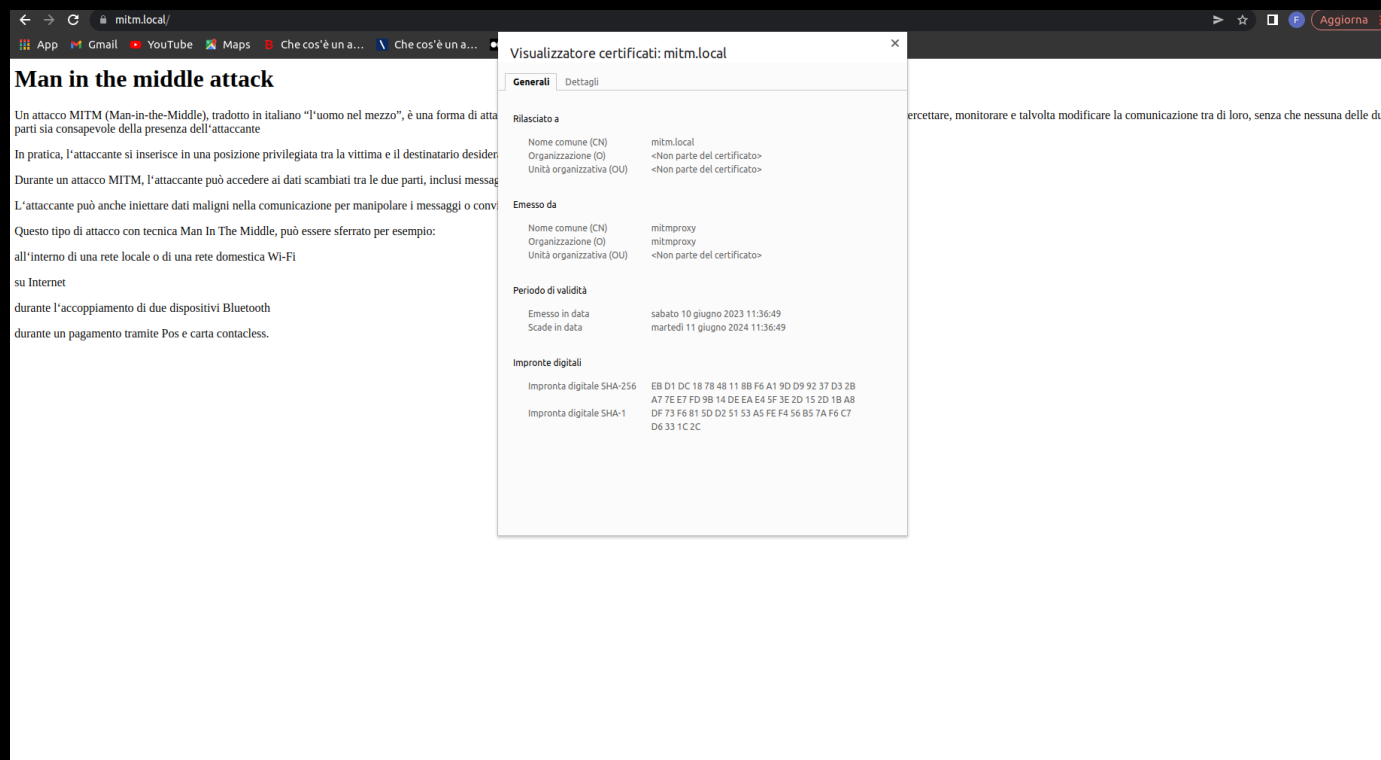
    print("Certificato della tua CA aggiunto correttamente al pacchetto certifi.")

# Esegui la funzione per aggiungere il certificato della tua CA al pacchetto certifi
add_custom_ca()
```

AVVIO DI MITMPROXY

Avviamo mitmproxy e digitiamo nel browser l'indirizzo del nostro sito web.

Vediamo che ora mitmproxy riconosce il certificato del server come valido perchè firmato da una CA attendibile e sostituisce il certificato del server con un certificato emesso dalla sua CA.



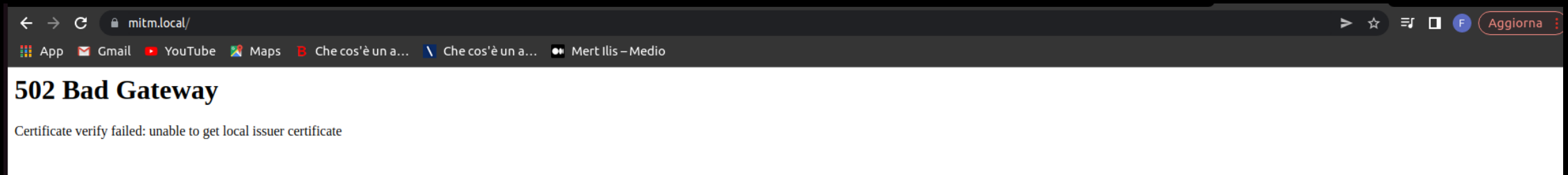
GENERAZIONE CERTIFICATI NON VALIDI

Abbiamo visto che MITM proxy verifica la validità dell'autorità di certificazione (CA), adesso vediamo come si comporta quando il certificato del server non è valido perchè, ad esempio, scaduto.

Generiamo un certificato server scaduto:

- `openssl x509 -req -days -365 -in "expired_certificate.csr" -sha256 -CA "root-ca.crt" -CAkey "root-ca.key" -CAcreateserial -out "expired_certificate.crt" -extfile "expired_certificate.cnf" -extensions expired_certificate`

Se avviamo MITM proxy e andiamo sul nostro sito web notiamo che otteniamo l'errore 502 BAD GATEWAY (Certificate verify failed: unable get local issuer certificate)



GENERAZIONE CERTIFICATI NON VALIDI

Si possono verificare altre situazioni di errore come generare un certificato con un nome di dominio diverso da quello del nostro server.

Anche in questo caso MITM proxy comunica che la verifica del certificato è fallita (502 BAD GATEWAY).

Tuttavia si può forzare MITM proxy a non fare alcuna verifica sui certificati con l'opzione - - ssl - insecure

Per quanto riguarda la revoca del certificato da parte della CA, invece, Mitmproxy non fornisce un modo integrato per gestire una CRL.

CONCLUSIONE

In conclusione, dalla verifica effettuata abbiamo potuto vedere che MITM proxy esegue molti dei controlli effettuati dal browser sui certificati:

- Validità temporale
- Validità dell'autorità di certificazione (CA)
- Corrispondenza del nome del dominio

Ma ci sono alcuni controlli che non esegue, infatti, come abbiamo visto, non è in grado di verificare se un certificato è stato revocato, perchè non gestisce una Certificate Revocation List (CRL).

The background features a solid black field. At the top, there is a decorative, wavy horizontal band with a color gradient. From left to right, the colors transition from a warm orange-red to a bright yellow, then through a green, and finally into a light cyan or blue at the far right edge.

GRAZIE PER L'ATTENZIONE