PROGETTO 1

Gelosa Matteo

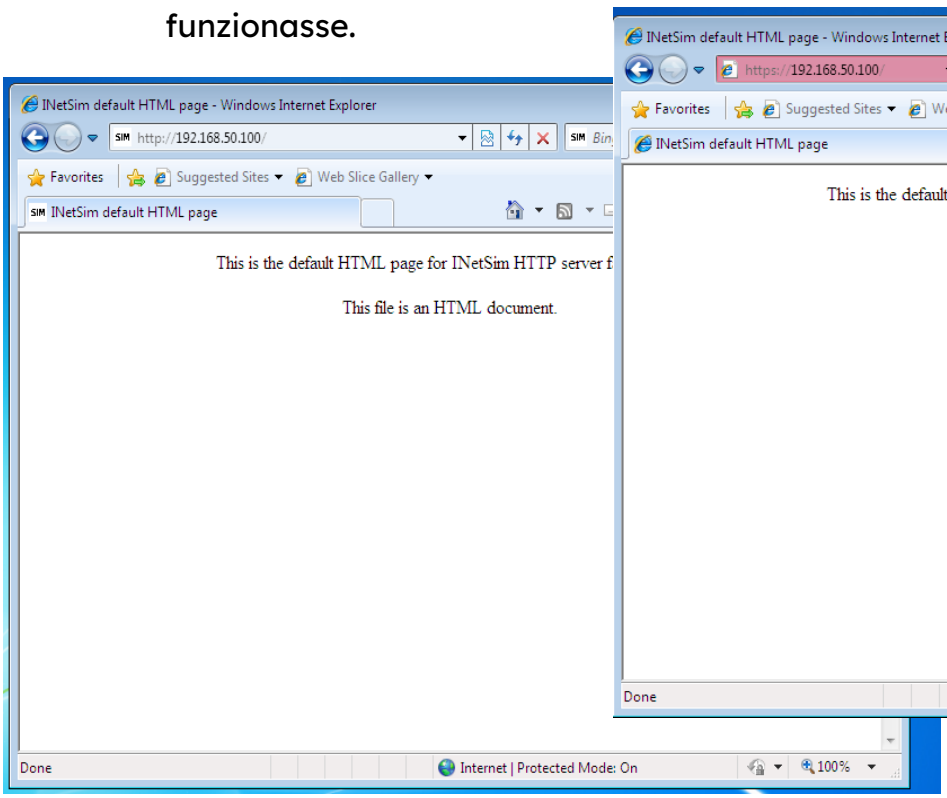
Per questo esercizio,ho inizialmente verificato che le due macchine Kali(192.168.50.100) e Win7(192.168.50.102) comunicassero tra loro tramite il comando ping essendo su rete interna. Il risultato è stato positivo, con questo breve test mi sono assicurato di poter procedere correttamente con l'esercizio.

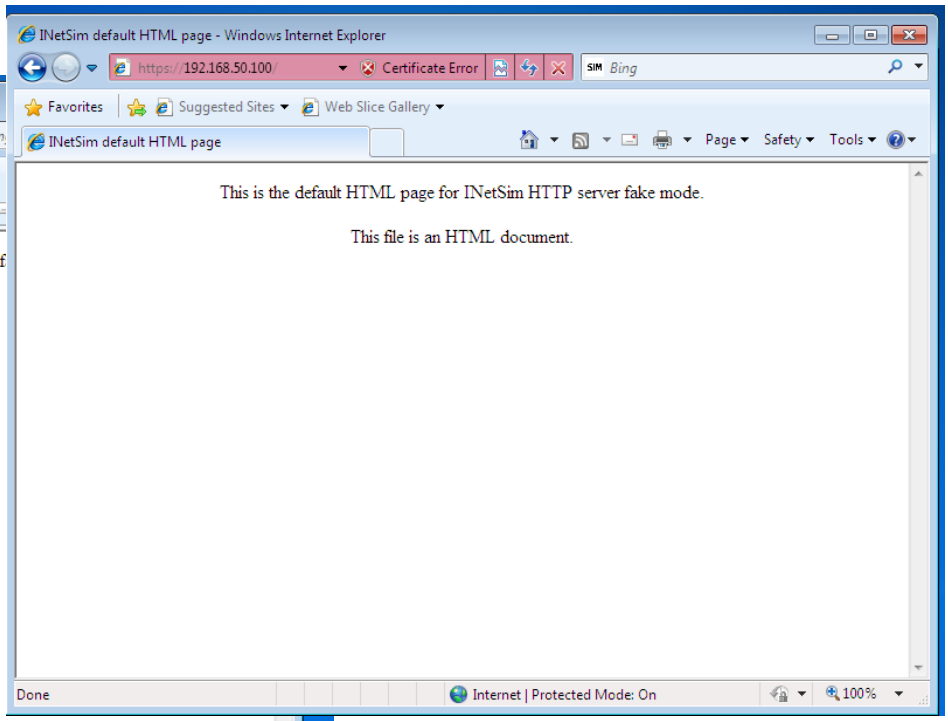
Successivamente, grazie al tool Inetsim presente su Kali Linux (Esso è in grado di simulare molteplici server sulla nostra rete interna) ho configurato il tool in modo che simulasse server http,https e dns.

```
#
start_service dns
start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service ftps
#start_service tftp
```

Ho rimosso il cancelletto che ha il compito di commentare il testo e non renderlo eseguibile. Rimuovendolo dal testo desiderato esso può essere eseguito.

Successivamente ho eseguito richieste http e https dalla macchina Win7 per verificare che il tutto
funzionasse.

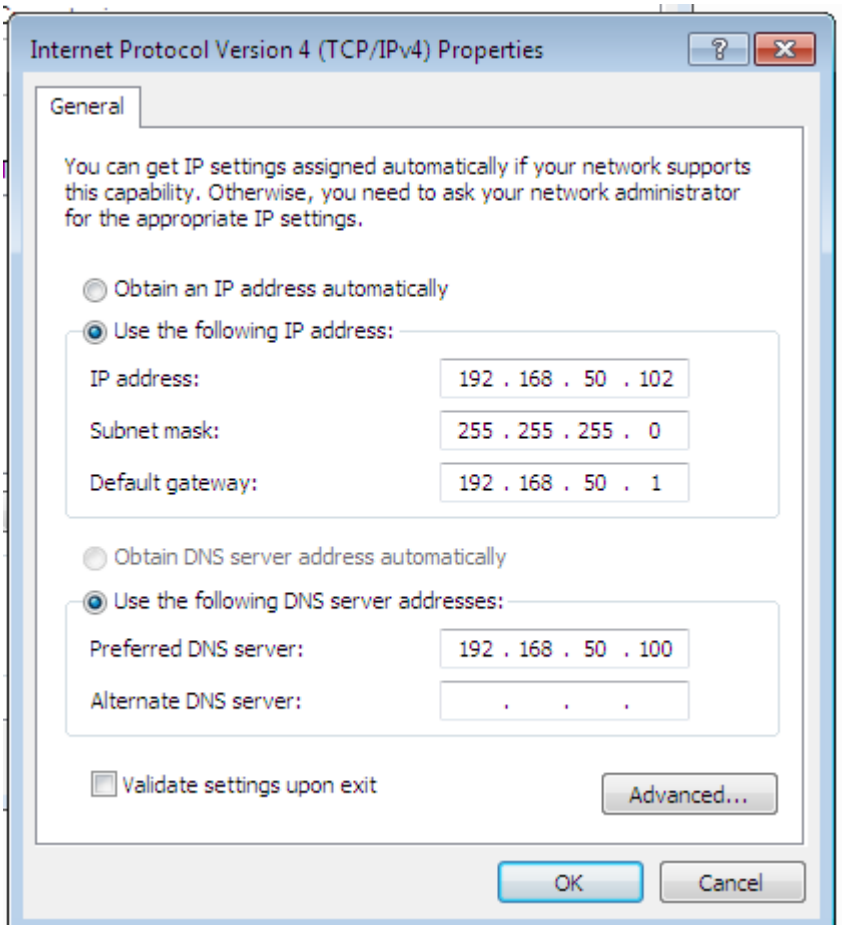




Per far sì che la macchina Win7 riuscisse a visualizzare il “server” http e https ho dovuto impostare un bind address di 0.0.0.0 . Quest’ultimo infatti permette a tutti gli ip della rete interna di visualizzare il server quando si effettua la richiesta.

```
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 0.0.0.0
```

Successivamente ho impostato il server DNS.
Sulla macchina Win7 ho impostato come indirizzo DNS l’indirizzo della macchina Kali (192.168.50.100) nonchè la macchina che ospita il server.
Eseguendo questo passaggio sono sicuro che digitando il dominio epicode.internal nella barra di ricerca la macchina Win7 sarà in grado di raggiungerlo.



Spostandomi sulla macchina Kali ho effettuato queste modifiche:

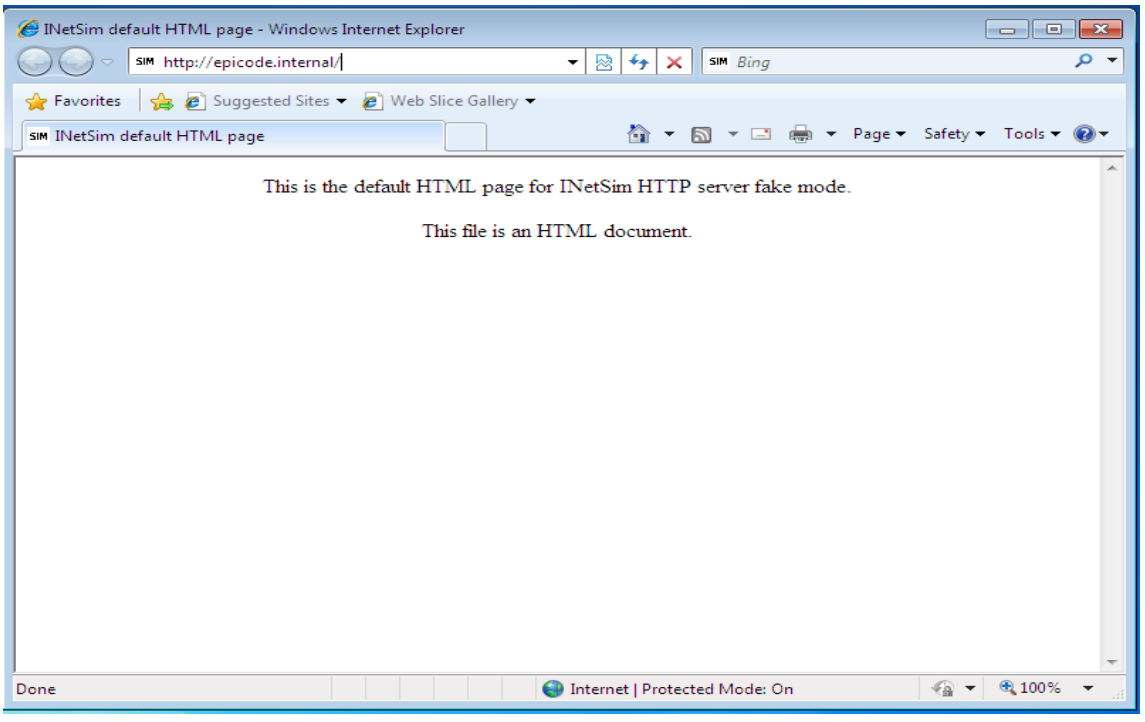
Ho impostato un ip di default al server DNS (192.168.50.100) nonchè l'indirzzo ip della macchina Kali.
Facendo questo chiunque faccia una chiamata col dominio associato all'indirizzo ip del server DNS avrà come risposta la pagina corretta.

```
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip 192.168.50.100
```

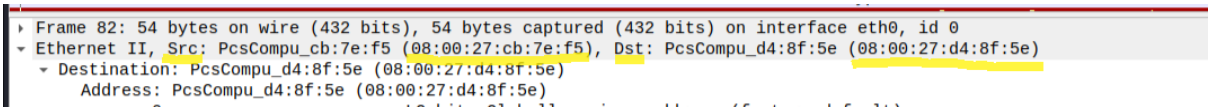
Infine ho impostato il dominio di default per il server DNS (epicode.internal), questo mi ha permesso di poter digitare nella barra di ricerca della macchina win7 il dominio per ricevere come risposta la pagina desiderata.

```
##########################################
# dns_default_domainname
#
# Default domain name to return with DNS replies
#
# Syntax: dns_default_domainname <domain name>
#
# Default: inetsim.org
#
dns_default_domainname epicode.internal
```

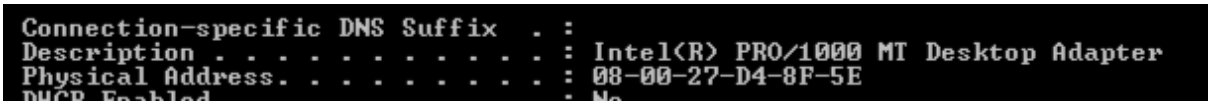
Questa è l'immagine della barra di ricerca con il dominio epicode.internal, come si può notare riscontro risultato positivo.

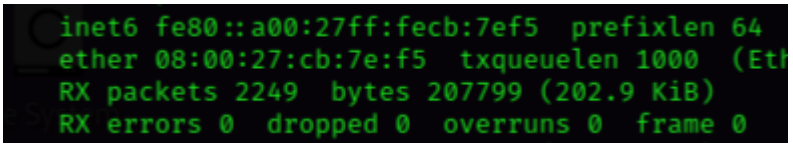


Successivamente ho utilizzato il tool Wireshark per intercettare i pacchetti e per visualizzare i MAC address della macchina sorgente e macchena destinatario.



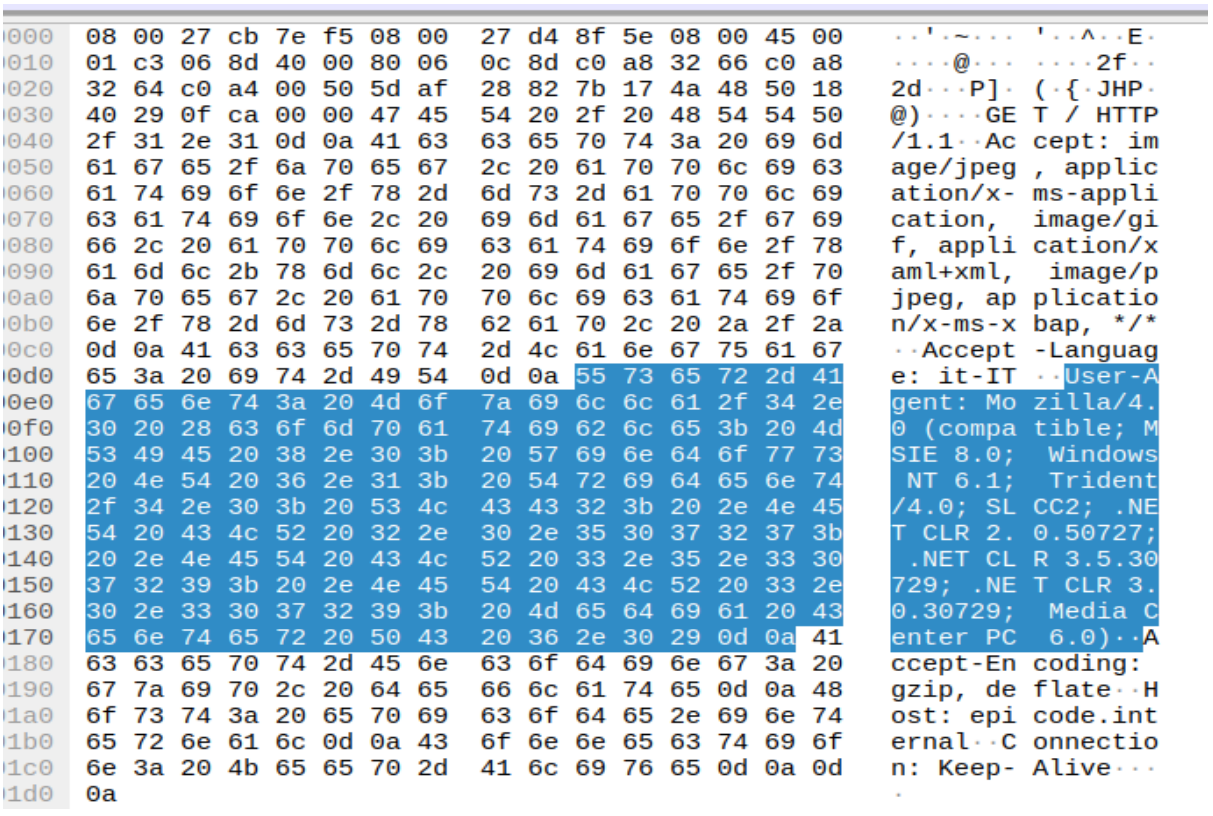
Che corrispondono con quelli della macchina Kali e Win7





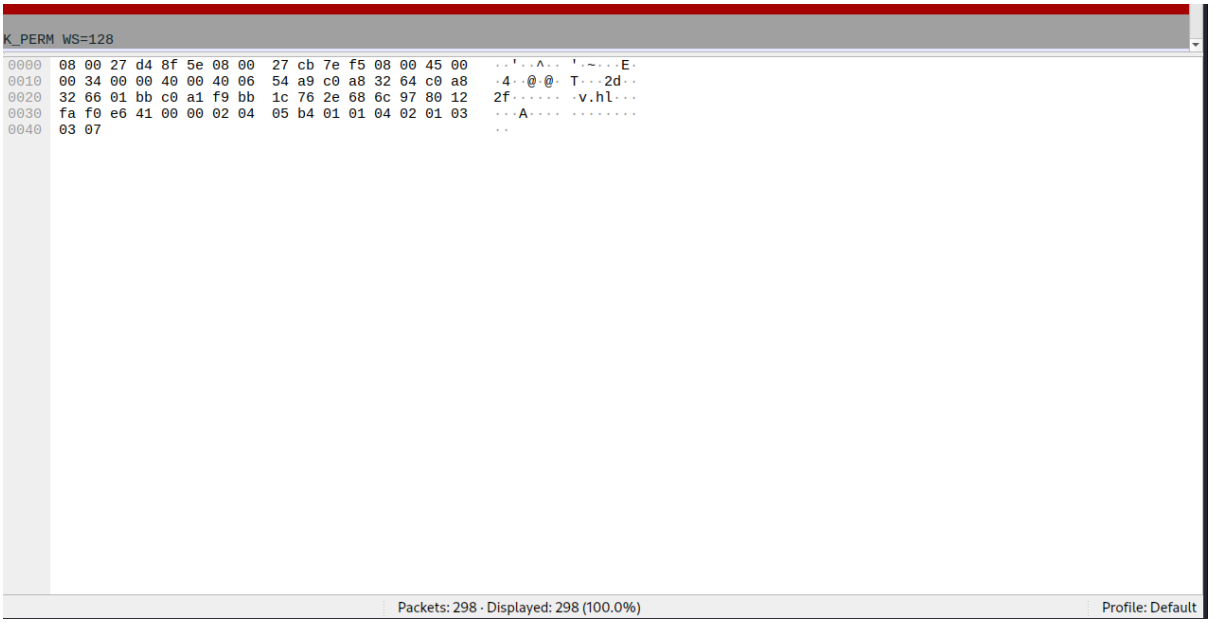
Infine ho provato ad intercettare sempre utilizzando il tool Wireshark lo scambio di pacchetti tra le varie richieste http e https.
Ho notato come nelle richieste http il traffico in transito sia visibile mentre con la richiesta https il traffico viene criptato e dunque non comprensibile.

Richiesta http :



Possiamo notare come alla nostra destra il traffico sia comprensibile.

Richiesta https:



In questo caso possiamo notare come il traffico alla destra sia completamente incomprensibile e quindi cifrato.