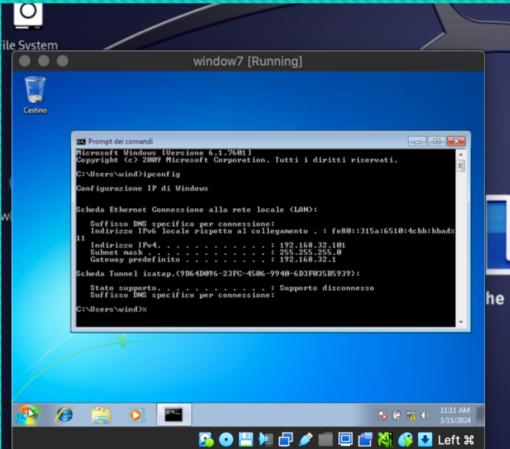


# W4D4 – Nicholas Di Angelo –

Configurazione e Programmazione Indirizzo IP sulla Macchina Linux (192.168.32.100)



A CONFIGURAZIONE IP SU WINDOWS7

A CONFIGURAZIONE IP SU KALI LINUX

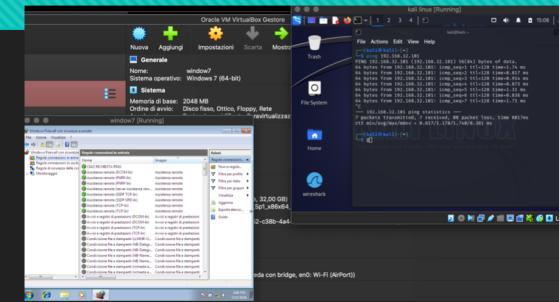
PER CONFIGURARE UNA POLICY CHE CONSENTA DI FAR COMUNICARE LE MACCHINE LINUX ANDANDO AD INSERIRE GLI INDIRIZZI IP DI DESTINAZIONE E QUELLO DI PARTENZA DELLE MACCHINE, CONSENTENDO SUCCESSIVAMENTE, LA CONNESSIONE SENZA AVER BISOGNO DI AUTORIZZAZIONI DI ALCUN TIPO

## Configurazione Regole sul Firewall Win7 - “CIAO RICHIESTA PING” E PROVE PING

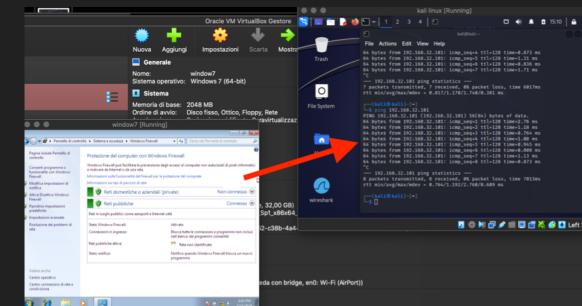
PER CONFIGURARE UNA POLICY CHE CONSENTA DI FAR COMUNICARE LE MACCHINELINUX BASED CON WINDOWS CON FIREWALL ATTIVO BISOGNA MODIFICARE I PERMESSI DI CONNESSIONE ALL' INTERNO DELLE IMPOSTAZIONI AVANZATE DI WINDOWS, ANDANDO AD INSERIRE GLI IP DI DESTINAZIONE E QUELLO DI PARTENZA DELLE MACCHINE, CONSENTENDO SUCCESSIVAMENTE, LA CONNESSIONE SENZA AVER BISOGNO DI AUTORIZZAZIONI DI ALCUN TIPO. RISPETTIVAMENTE LE 2 MACCHINE HANNO I SEGUENTI IP: - WINDOWS: 192.168.32.101; - KALI LINUX: 192.168.32.100;



PROVA PING TRA 192.168.32.100 - 192.168.32.101



CONFIGURAZIONE REGOLE SUL FIREWALL WIN7 -  
“CIAO RICHIESTA PING”



PROVA PING 192.168.32.100 CON REGOLA FIREWALL  
ATTIVO SU 192.168.32.101

# Configurazione Inetsim Start Device - DNS, HTTP, HTTPS

APRENDO LA MACCHINA VIRTUALE BASTERÀ DIGITARE IN PROMPT DEI COMANDI IL PERCORSO "SUDO NANO /ETC/INETSIM/INETSIM.CONF", ATTIVANDO COSÌ LO START SERVICE ALLE VOCI DNS,HTTP,HTTPS

N.B. I PARAMETRI IN BIANCO SONO QUELLI ATTIVI MENTRE QUELLI IN CELESTINO SONO QUELLI CHE ABBIAMO DISATTIVATO ANDANDO A METTERE UN '#' AVANTI AD OGNI RIGA DI PARAMETRO CHE NON CI INTERESSA UTILIZZARE, IN QUESTO CASO I SERVIZI ATTIVI SONO DNS ,HTTP E HTTPS.

IN QUESTA FASE ANDREMO A CONFIGURARE IP DEL SERVER INTERNO CHE CI SERVIRÀ PER LA COMUNICAZIONE DEL PACCHETTO IN LOOPBAK. NELLO SPECIFICO BISOGNERÀ TOGLIERE IL '#' DALLA VOCE SERVICE\_BIND\_ADDRESS ED INSERIRE L'INDIRIZZO IP DELLA MACCHINA KALI LINUX CHE FUNGERÀ DA DNS

LA CONFIGURAZIONE DEL DNS AVVIENE ATTIVANDO LA VOCE DNS\_DEFAULT\_IP INSERENDO L'INDIRIZZO DELLA MACCHINA DI KALI

IN QUESTA ULTIMA FASE DI CONFIGURAZIONE ANDREMO A CONFIGURARE NEL DNS\_STATIC LA STRINGA EPICODE.INTERNAL NONCHÈ L'INDIRIZZO DELLA MACCHINA DNS 192.168.32.100 .

SALVANDO LA CONFIGURAZIONE DI CUI ALLE PAGINE G(H)I)L DEL PRESENTE ELABORATO ATTRAVERSO L'USO DEL SEGUENTE PROCESSO DI PROGRAMMAZIONE  
CTRL + X -> Y + INVIO

```
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
#start_service irc
#start_service nntp
#start_service finger
#start_service ident
#start_service syslog
#start_service time_tcp
#start_service time_udp
#start_service daytime_tcp
#start_service daytime_udp

#dns
# dns_static
# Static mappings for DNS
#
# Syntax: dns_static <epicode.internal> <192.168.32.100>
#
# Default: none
#
dns_static epicode.internal 192.168.32.100
dns_static ns1.foo.com 10.70.50.30
dns_static ftp.bar.net 10.10.20.30

#dns_version
```

CONFIGURAZIONE INETSIM START DEVICE - DNS, HTTP, HTTPS

```
#dns
# dns_bind_port 53
#
#dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 192.168.32.100

#dns_default_hostname
#
# dns_default_hostname
```

CONFIGURAZIONE INDIRIZZO IP SERVICE BIND ADDRESS 192.168.32.100

```
#dns
# dns_bind_port 53
#
#dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 192.168.32.100

#dns_default_hostname
#
# dns_default_hostname
```

CONFIGURAZIONE DNS DI DEFAULT 192.168.32.100

```
#dns
# dns_bind_port 53
#
#dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 192.168.32.100

#dns_default_hostname
#
# dns_default_hostname
```

CONFIGURAZIONE DNS EPICODE.INTERNAL SU IP 192.168.32.100

# AVVIO DELL'APPLICATIVO INTESINET CONNESSIONE HTTP – EPICODE.INTERNAL

Questo paragrafo descrive l'avvio del programma Inetsim per avviare il servizio di loopback

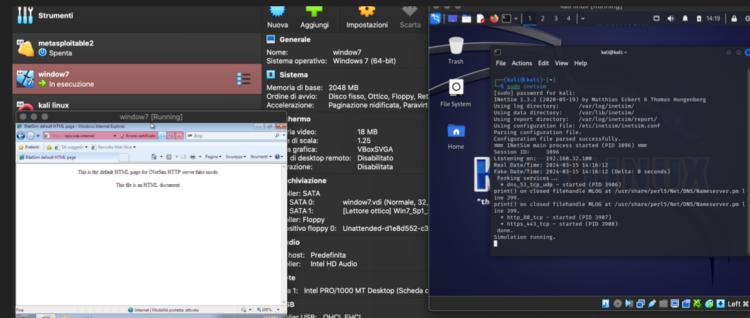
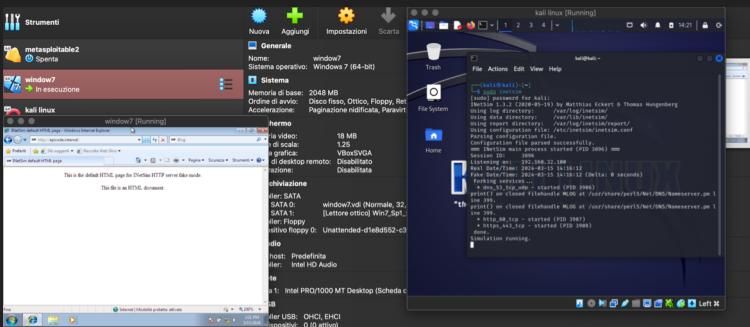
Avviata la simulazione si aprirà il browser di windows7 Explorer e digitare: <http://localhost> Ci apparirà una pagina come la seguente FOTO 1

Avviata la simulazione si aprirà il browser di windows7 Explorer e digitare: <https://localhost> Ci apparirà una pagina come la seguente FOTO 2

```
kali@kali: ~
File Actions Edit View Help
Parsing configuration file.
Use of uninitialized value $args[1] in lc at /usr/share/perl5/INetSim/Config.pm line 529, <CONFIGFILE> line 13.
Warning: Unknown service name '' in configuration file '/etc/inetsim/inetsim.conf' line 13
Warning: Unknown option 'start' in configuration file '/etc/inetsim/inetsim.conf' line 30
Configuration file parsed successfully.
== INetSim main process started (PID 6857) ==
Session ID: 6857
Listening on: 192.168.32.100
Real Date/Time: 2024-03-15 11:15:49
Fake Date/Time: 2024-03-15 11:15:49 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 6867)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/NAMEServer.pm line 399.
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/NAMEServer.pm line 399.
* https_443_tcp - started (PID 6868)
done.
Simulation running.
```

3) AVVIO DEL PROGRAMMA INETSIM  
SIMULATION RUNNING

1) COLLEGAMENTO WEB HTTP:// EPICODE.INTERNAL DA WIN7 INTERNET EXLORER



2) COLLEGAMENTO WEB HTTPS://EPICODE.INTERNAL DA WIN7 INTERNET EXLORER

# Avvio Scansione Wireshark Individuazione Pacchetti HTTP

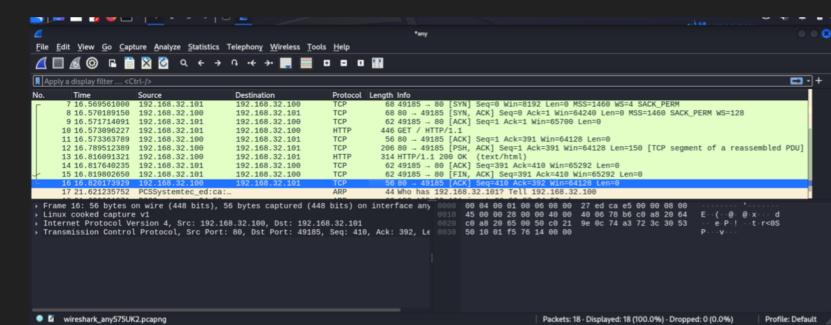
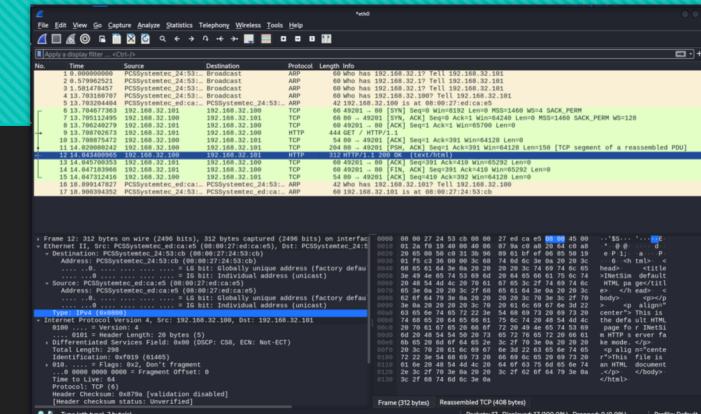
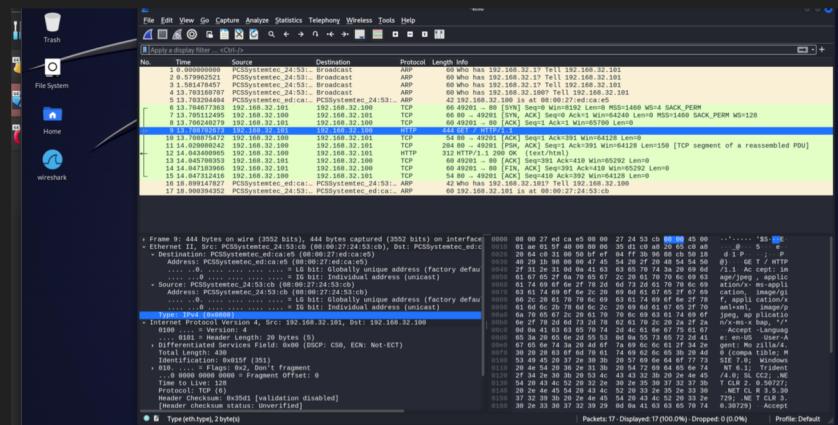
ATTRAVERSO IL PROGRAMMA WIRESHARK AVVIEREMO UNA SCANSIONE DI RETE ETH0 AL FINE DI INDIVIDUARE I PROTOCOLLI HTTP (SYN,SYN,ACK,ACK)

LA SEQUENZA DELLE AZIONI ESPOSTE NELL'ESEMPIO È QUELLA CHE AVVIENE IN UN AMBIENTE DI WEB DINAMICO, QUANDO IL SERVER WEB, COME IN QUESTO CASO, INTERAGISCE PER MEZZO DEL LINGUAGGIO DI SCRIPTING PHP, CON UN DATABASE E COSTRUISCE LA PAGINA DA RESTITUIRE AL CLIENT, IN BASE ALLE RISPOSTE RICEVUTE DAL SERVER

Dopo aver richiesto la prima pagina, inserito il nome da cercare e aver ricevuto, è visualizzato nel browser, la seconda pagina di risposta, si può fermare la cattura dei frame

La comunicazione inizia con pacchetti che trasportano richieste.

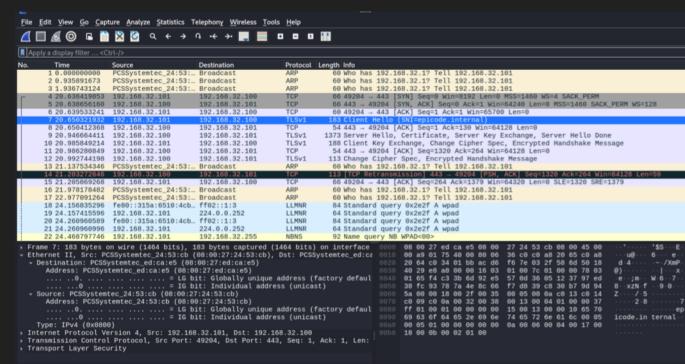
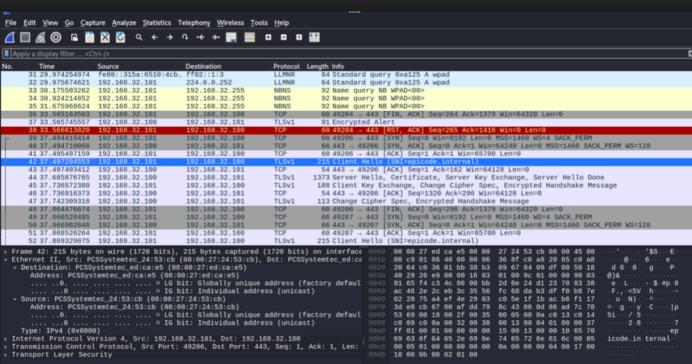
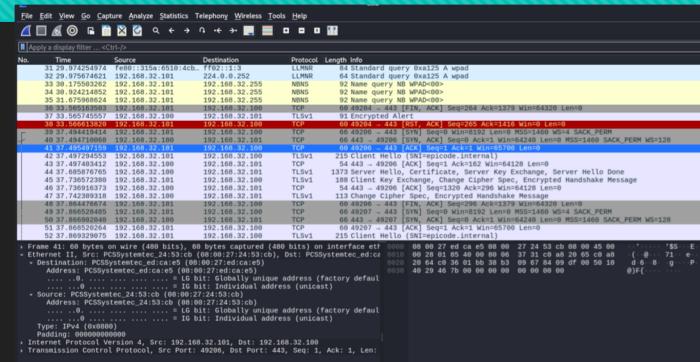
(SYN del richiedente, SYN e ACK del destinatario e successivo ACK del richiedente) La conversazione può essere avviata. Un pacchetto di tipo **SYN** (Synchronization) chiama l'interlocutore che, se accetta la conversazione, ritorna un pacchetto **ACK** (Acknowledge). A questo punto anche il richiedente invia un ACK e la conversazione vera e propria può essere avviata. Quella descritta è comunemente nota come **NEGOZIAZIONE DEI PACCHETTI**. I pacchetti successivi contenenti i dati della conversazione fra i due host saranno seguiti da pacchetti di tipo ACK per attestare l'avvenuta ricezione



# AVVIO SCANSIONE WIRESHARK INDIVIDUAZIONE PACCHETTI HTTPS

ATTRAVERSO IL PROGRAMMA WIRESHARK AVVIEREMO UNA SCANSIONE DI RETE ETH0 AL FINE DI INDIVIDUARE I PROTOCOLLI HTTPS ALLA VOCE TLSV1

SEGUE L'ANALISI E DIFFERENZE DELLE SCANSIONI HTTP - HTTPS



## evidenzE tra il traffico catturato in HTTP ed il traffico precedente in HTTPS. SpiegaZIONE, motivaZIONE Eprincipali differenze.

### HTTP-HTTPS

L'HTTP (Hypertext Transfer Protocol) è un protocollo STATELESS ovvero non mantiene la connessione, agisce secondo il modello CLIENT/SERVER ovvero il client invia una richiesta e il server risponde alla stessa richiesta. Volendo inviare una chiamata ad un sito web ci saranno quindi 2 richieste:

- RICHIESTA HTTP (HTTP Request)
- RISPOSTA HTTP (HTTP Response)

La versione "sicura" del protocollo HTTP si chiama HTTPS e utilizza una serie di protocolli, algoritmi e librerie di sicurezza con lo scopo di rendere cifrato il traffico web, warning che appare cliccando sulla "i" del browser EXPLORER "la tua connessione a questo sito non è protetta". Viceversa facciamo riferimento ad un sito che utilizza il protocollo sicuro HTTPS In questo caso "la connessione è protetta" e le informazioni inviate tramite questo protocollo restano PRIVATE.

Come abbiamo potuto osservare tutto il traffico HTTP è in chiaro, possiamo vedere tutti i pacchetti generati e il loro contenuto, comprese le informazioni che abbiamo inserito nel momento dell'accesso al sito web , questo quindi il motivo per cui i siti HTTP sono considerati NON SICURI: se intercettiamo il traffico web siamo sempre in grado di leggere il contenuto dei pacchetti.

Nelle scansioni HTTPS contrariamente a quanto sopra vediamo solo dei generici pacchetti "Application Data" ma quello che è presente all'interno di essi, a noi è completamente sconosciuto.