Progetto Finale M1

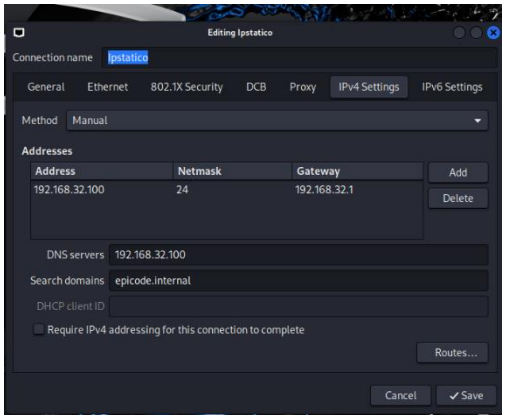
Requsiti e servizi attivi:

- Kali Linux : IP 192.168.32.100
- Windows: IP 192.168.32.101
- HTTPS Server :ATTIVO
- Servizio DNS per risoluzione nomi di domini: ATTIVO

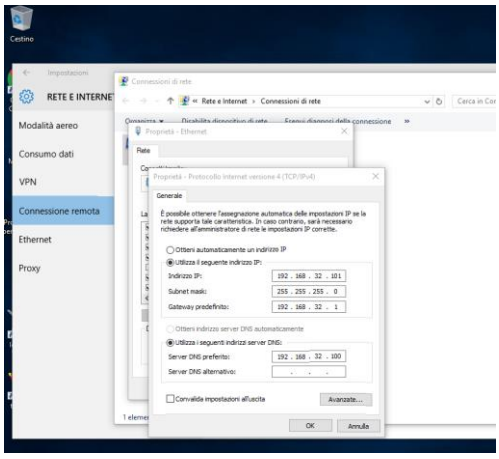
Procedimento con relativi screen.

Con il progetto finale andremmo a lavorare su due macchine virtuali installate in precedenza su Virtual Box, Kali Linux che sarà il nostro Server ed in fine Windows 10 che sarà il Client.

Per prima cosa ho avviato le due macchine e sono andato subito ad impostare i relativi indirizzi IP prima su Kali Linux e poi su Windows



CONFIGURAZIONE IP KALI

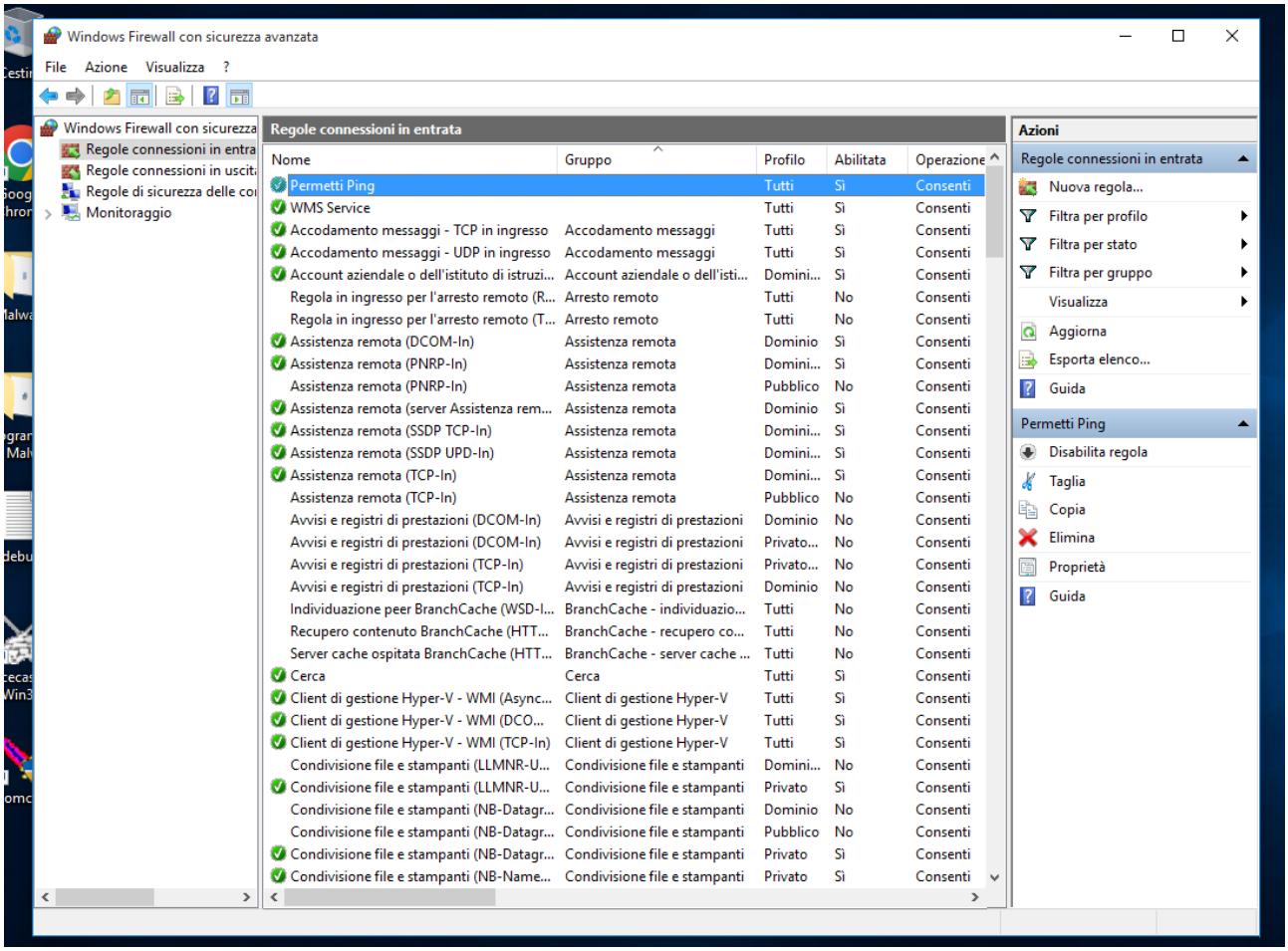


CONFIGURAZIONE IP E DNS WINDOWS

Nelle foto qui di sopra possiamo osservare la configurazione degli IP e DNS sulle due macchine.

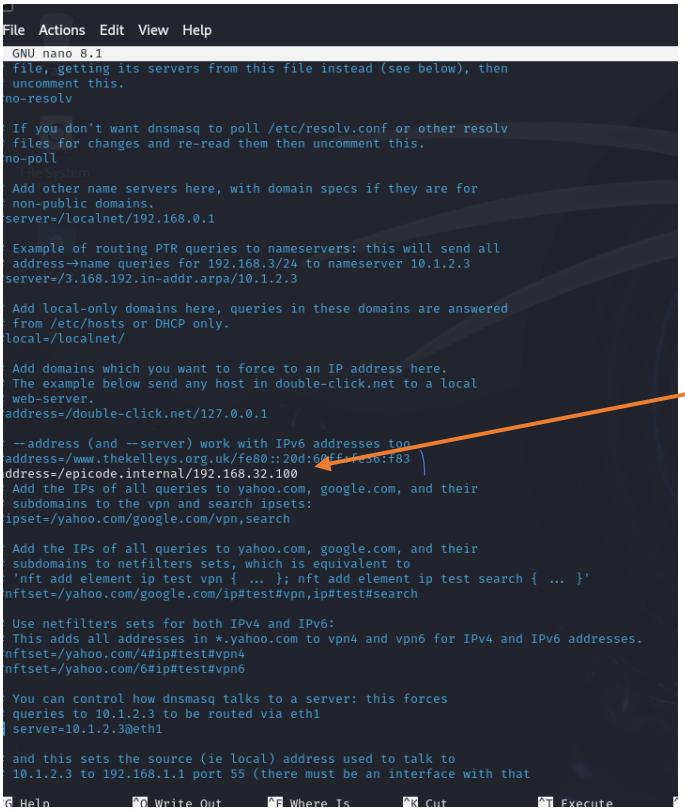
Sopra sono possiamo osservare la configurazione degli IP e D

Dopo la configurazione degli IP ho cambiato la policy del firewall di windows per permettere la comunicazione delle due macchine tra di loro

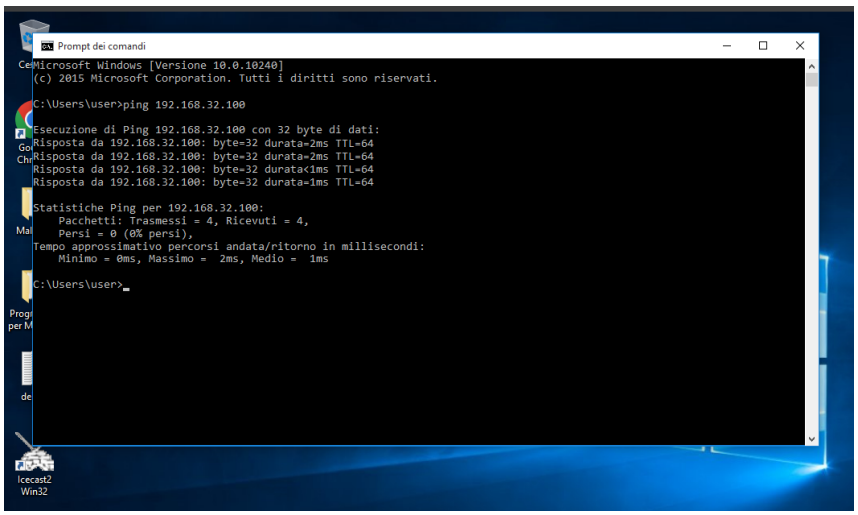


Quindi ho dato al Firewall una nuova regola autorizzandolo a far passare gli IP dati da me in fase di configurazione .

Sopra sono possiamo osservare la configurazione degli IP e D



Nella foto qui di fianco, sono ritornato nuovamente sulla macchina Kali Linux, ma questa volta per andare a configurare Inetsim per poter attivare il DNS (epicode.internal) con indirizzo IP:192.168.32.100



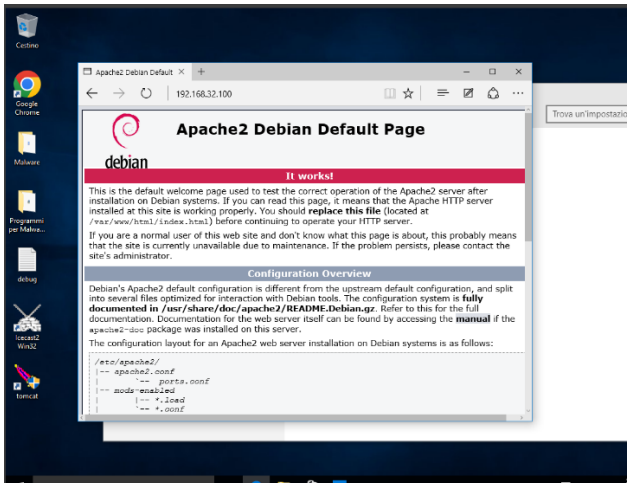
Successivamente dopo aver configurato le due macchine, attivando le policy del firewall windows e impostando il DNS epicode.internal, sono ritornato sulla macchina Windows come si evince da foto, ho aperto il prompt dei comandi per lanciare il comando PING da Windows a Kali Linux .

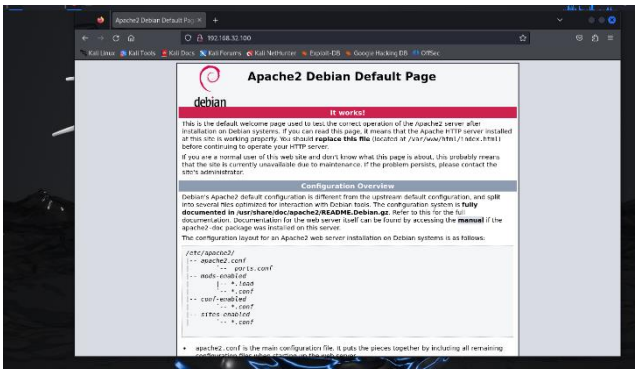
Sopra sono possiamo osservare la configurazione degli IP e D

```
└─$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 122047) ===
Session ID:     122047
Listening on:   127.0.0.1
Real Date/Time: 2024-11-29 15:02:33
Fake Date/Time: 2024-11-29 15:02:33 (Delta: 0 seconds)
 Forking services...
  * https_443_tcp - started (PID 122049)
 done.
Simulation running.
```

Dop aver costato che le due macchine tra di loro riescono a comunicare, ho aperto Kali Linux e lanciato tramite il terminale ho lanciato il comando inetsim come si può vedere nella foto qui di sopra.Tale comando viene comunemente usato come simulatore per servizi internet ,ma viene anche usato in ambienti sicuri come Laboratori virtuali dove poter testare malware o file sospetti in modo da non recare danno.

Tornando al nostro esercizio questo comando una volta avviato ci darà la possibilità di andarci a collegare direttamente al nostro DNS precedentemente configurato sotto l'url di epicode.internal.

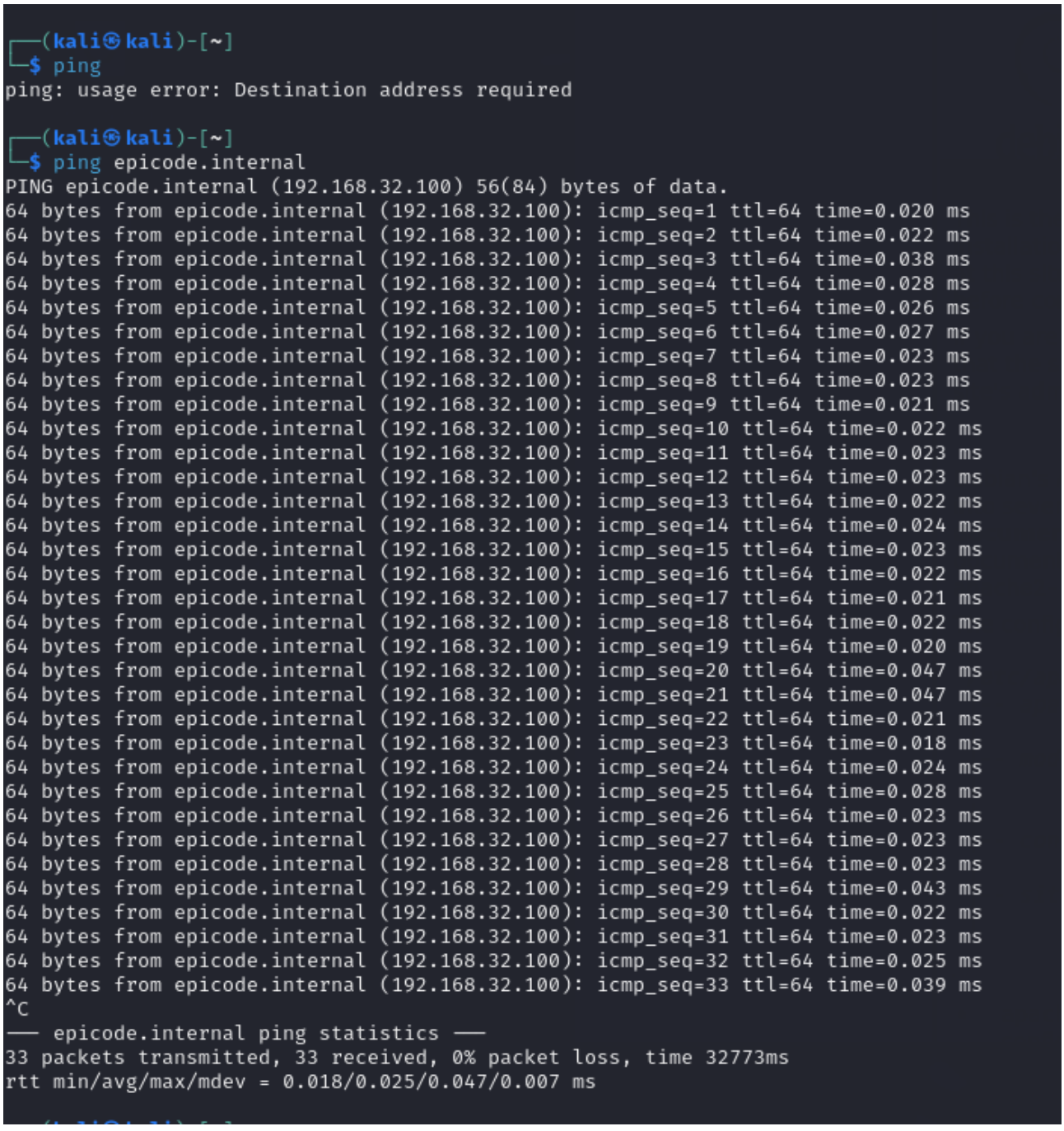




Queste sono le due macchine Kali Linux sulla nostra dx dove abbiamo inserito IP 192.168.32.100 nella barra degli indirizzi per poi portarci sul

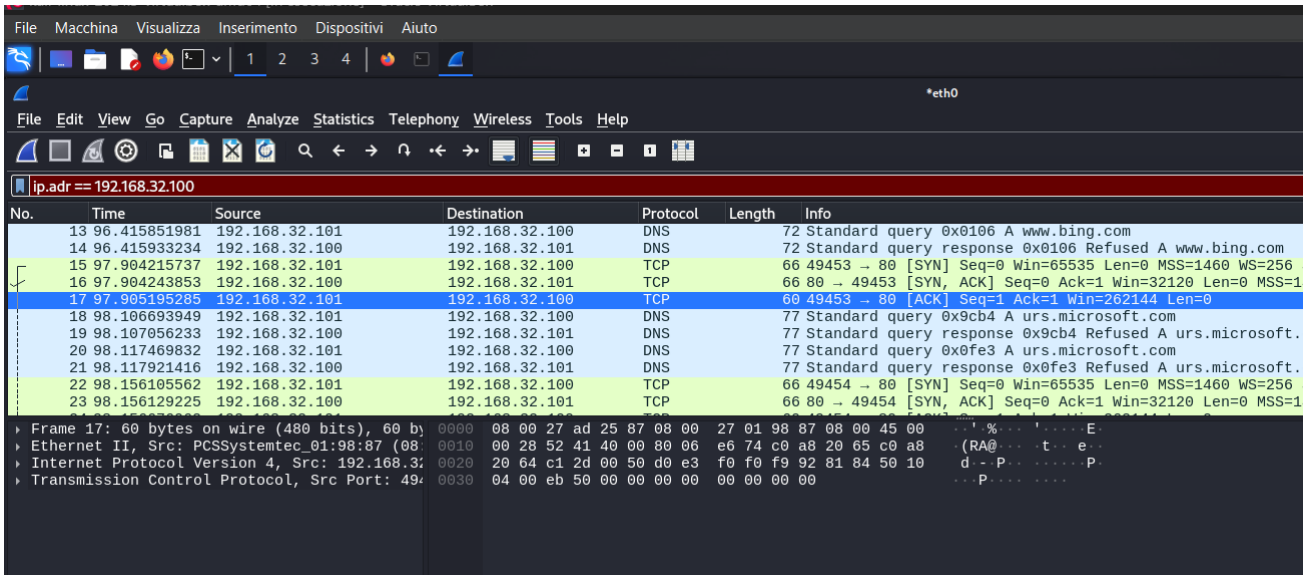
Sopra sono possiamo osservare la configurazione degli IP e D

sito internet epicode.iternal e mentre nella schermata di sx abbiamo la macchina di windows anche lei collegata all'indirizzo IP 192.168.32.100



Come si nota oltre a provarci a collegare direttamente tramite Browser web abbiamo fatto un 'ulteriore test da terminale sempre con il comando ping ma stavolta anziché di inserire l' IP abbiamo inserito il seguente comando :ping epicode.internal. Ricordo anche che il comando PING può

rivelarsi un’ ottimo strumento di diagnostica per capire se è tutto ok nella nostra configurazione.



Sempre con inetsim attivo e provandoci a collegare alla nostra pagina in questione epicode.internal ho eseguito il tool WireShark.

Proprio quest’ultimo serve per andare ad analizzare tutto il traffico di rete e la cattura di pacchetti in transito ed andarli ad analizzare ,infatti wire shark è uno strumento di analisi.

Sopra sono possiamo osservare la configurazione degli IP e D