

Name:Shrinivas D

Course:Cyber-Security

Topic:2

Activity:

Test the System Security by using metasploit Tool from kali linux and hack the windows 7 / win dows10. Execute the commands to get the keystrokes / screenshots / Webcam and etc., Write a report on vulnerability issue along with screenshots how you performed and suggest th security patch to avoid these type of attacks Hacker Machine : Kali Linux Victim machine : Windows XP / Windows 7

Victim Machine:Windows7

Payload: windows/meterpreter/reverse\_tcp(trojan)

Attack type: Escalating control over victim machine

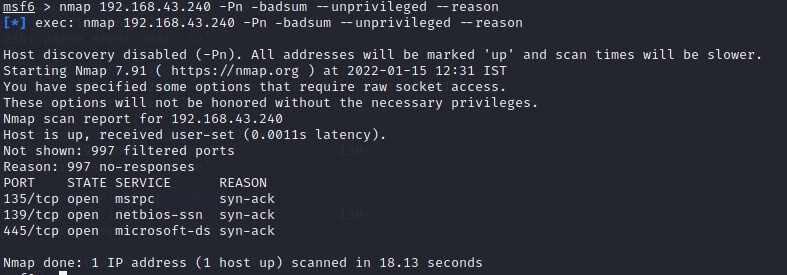
Payload injection: via link(on click starts to download)

Attacker Machine: KaliLinux

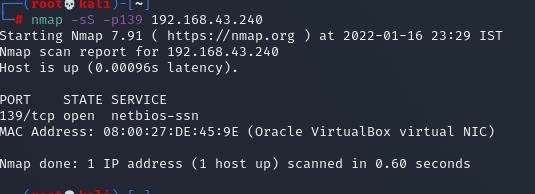
* Using the nmap tool scanned the victim(windows10) and got some open ports “—badsum” used was necessary otherwise it showed all ports filtered

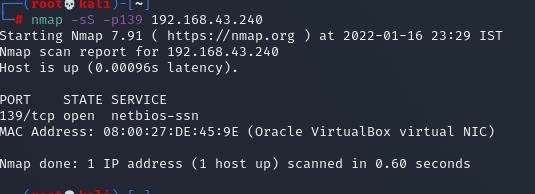
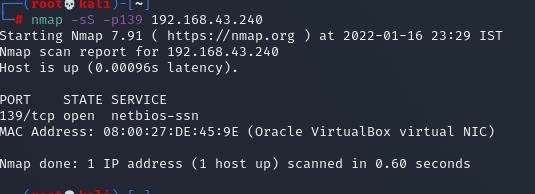
//unfortunately the windows 10 was able to detect the payload and chrome detected it quickly

But exploiting worked for windows 10 via ssh tunel and once all antivirus was disabled meterpreter trojan could be used.



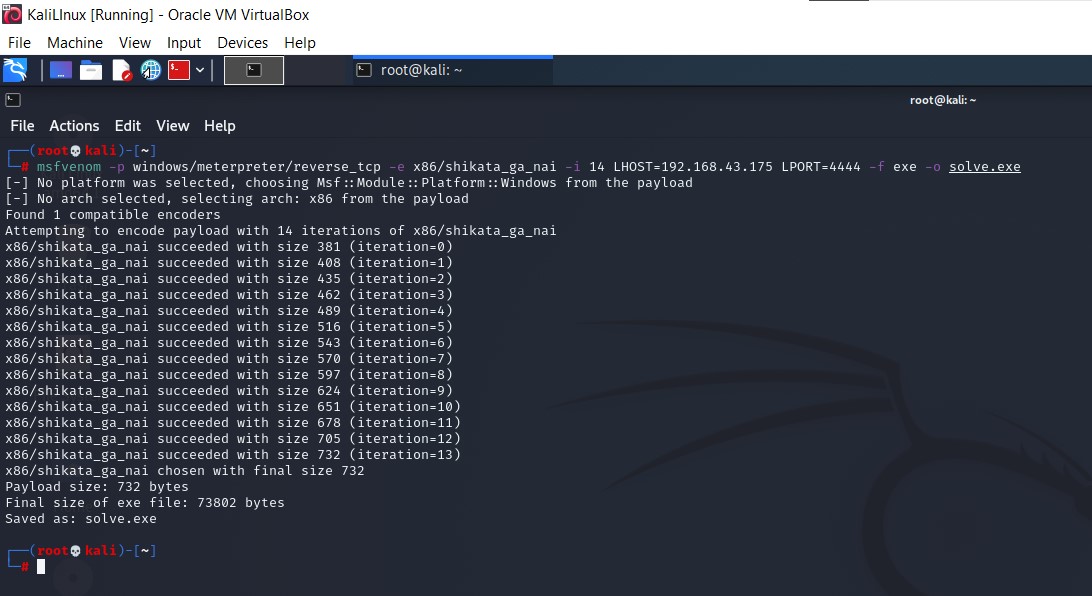
* **Scanning particular port(stealth scanning “-sS”)**





* **Creating the payload:**

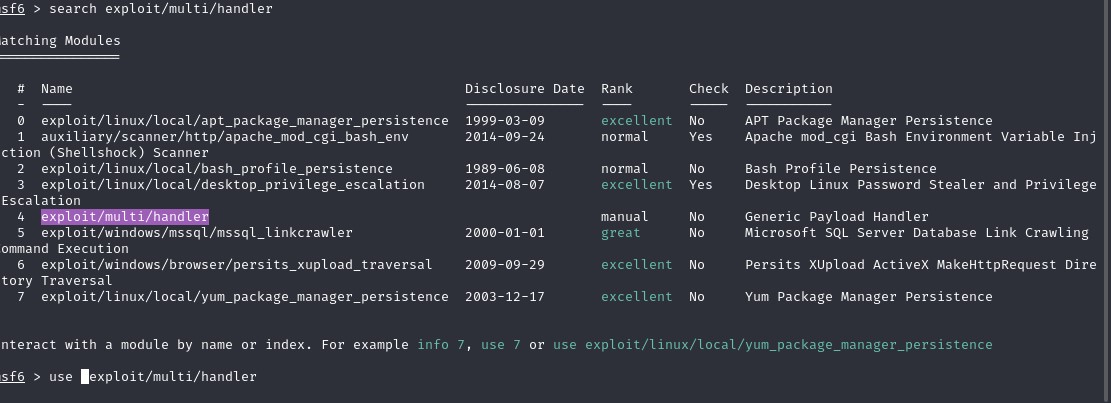
**Created a trojan as payload using msfvenom, used meterpreter as it escalates the privilages of getting full control of victim machine. Also encoding the payload 14 times with 32 bit encoder**



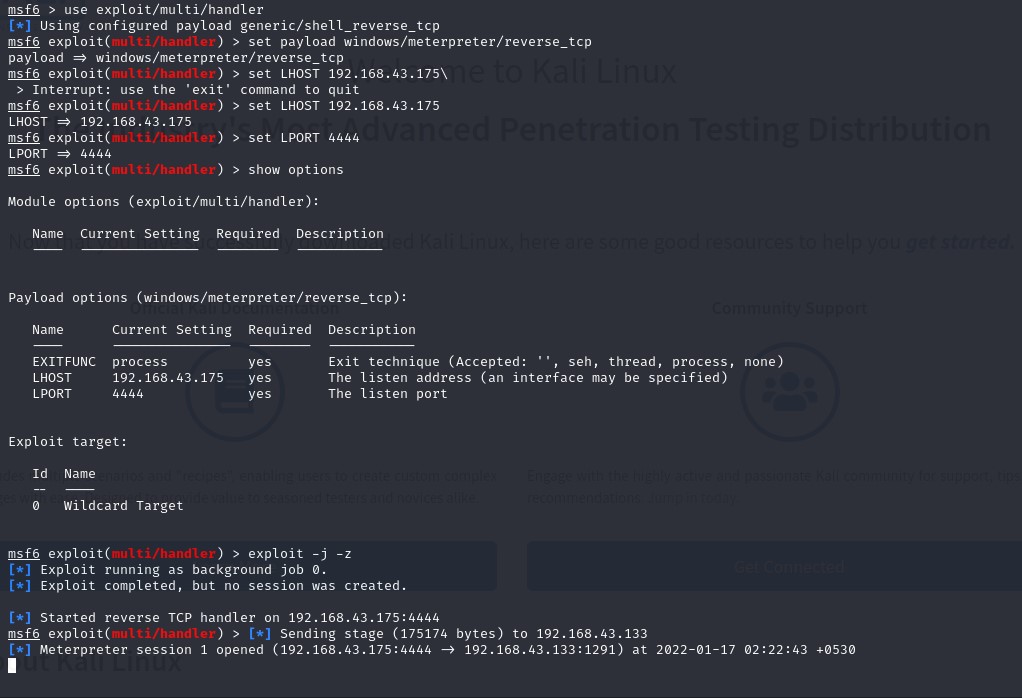
* Uploading the payload to apache server in kali linux and copying the link and adding suffix /”payload filename” to the copied link and start the apache2 service on kali linux and adding adding prefix as http:// iff the copied link is not in http format.

This new modified link is sent to victim machine via gmail(for example) if the victim clicks this link the it automatically downloads the payload via that link from apache server. By encoding the payload the antivirus was unable to detect the virus file

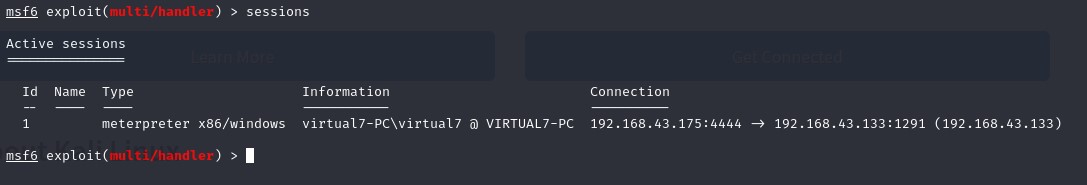
# ➢ Used multi handler exploit via Metasploit

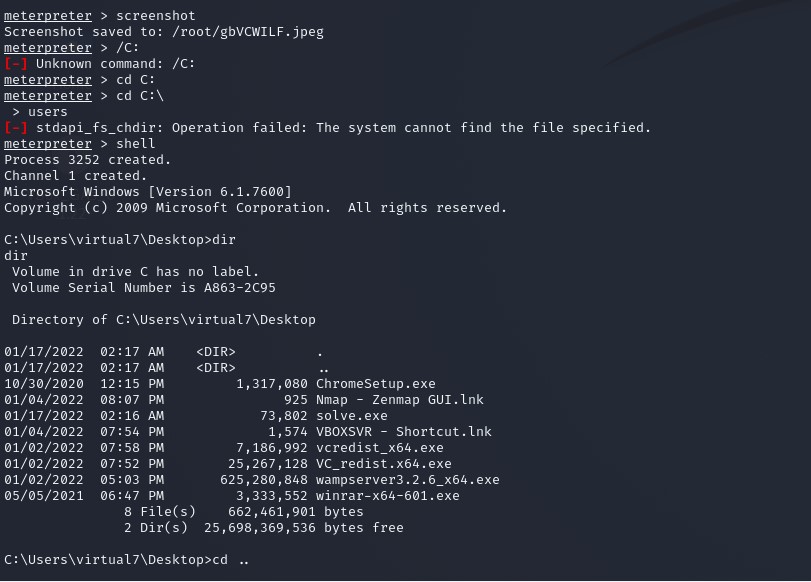


* Setting up the Metasploit for that particular payload(metrepreter,reverse\_tcp)
* Setting the lhost and lport
* Checking whether the settings are correct
* Turn off the apache2 service
* Running the exploit in background using the exploit command with appropriate options
* Waiting for the victim to run the payload that was downloaded on victim machine
* Victim runs the file but there is no action seen by victim on victim machine ➢ As soon the payload runs on victim machine a session is created and we can use that session to get the full control over victim machine and can take screen shots,traverse trouh the entire file/directories download or delete or make modification in victims machine .Also can get keystrokes i.e; whatever the victim is typing on a platform it is got traced out and we can see those key strokes in kali linux

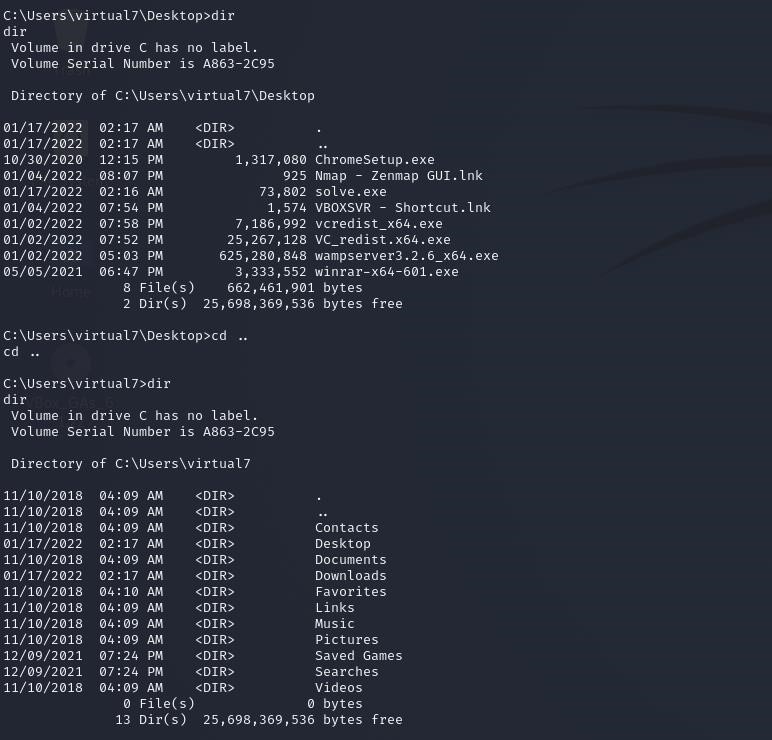


* Session was created

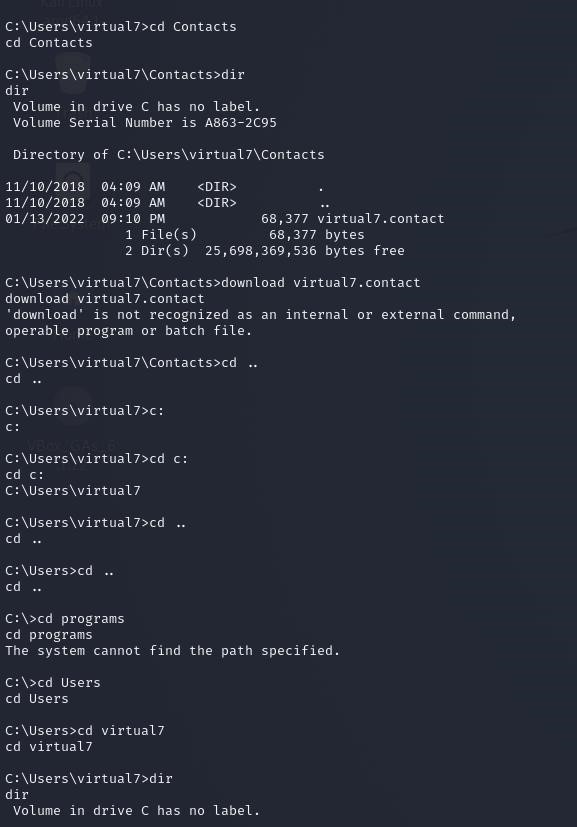


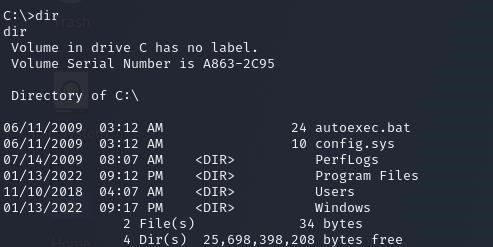
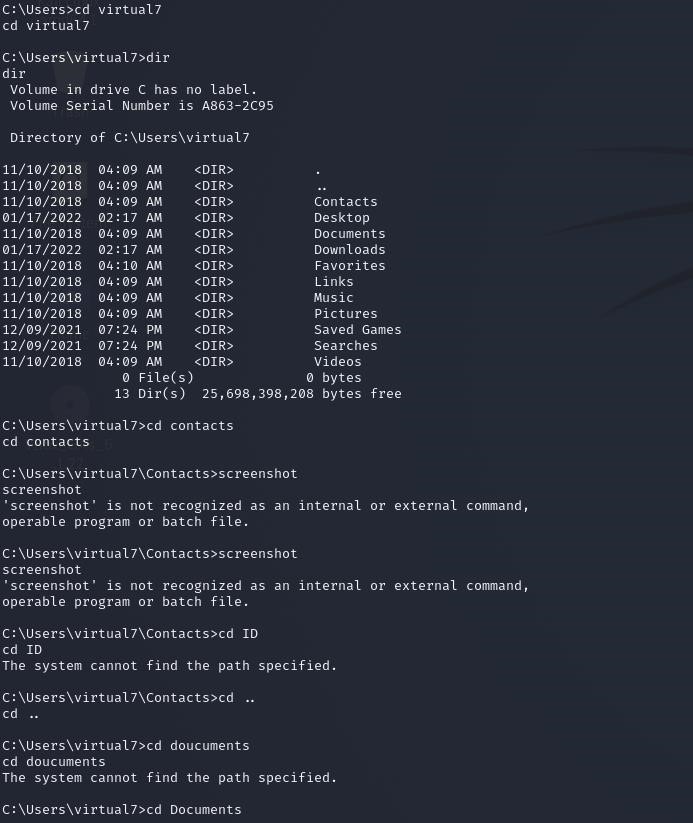


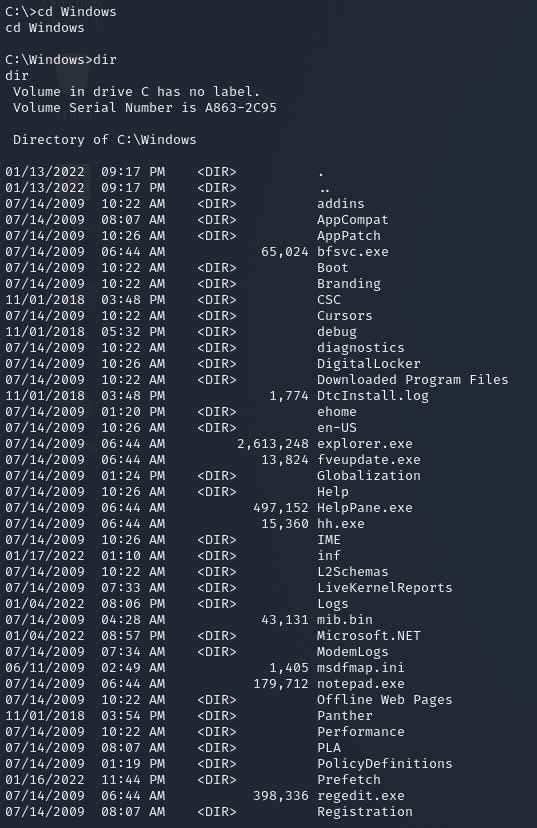
Screen shot was taken ,system configuration was seen , traversed trough directories listed all files directory had

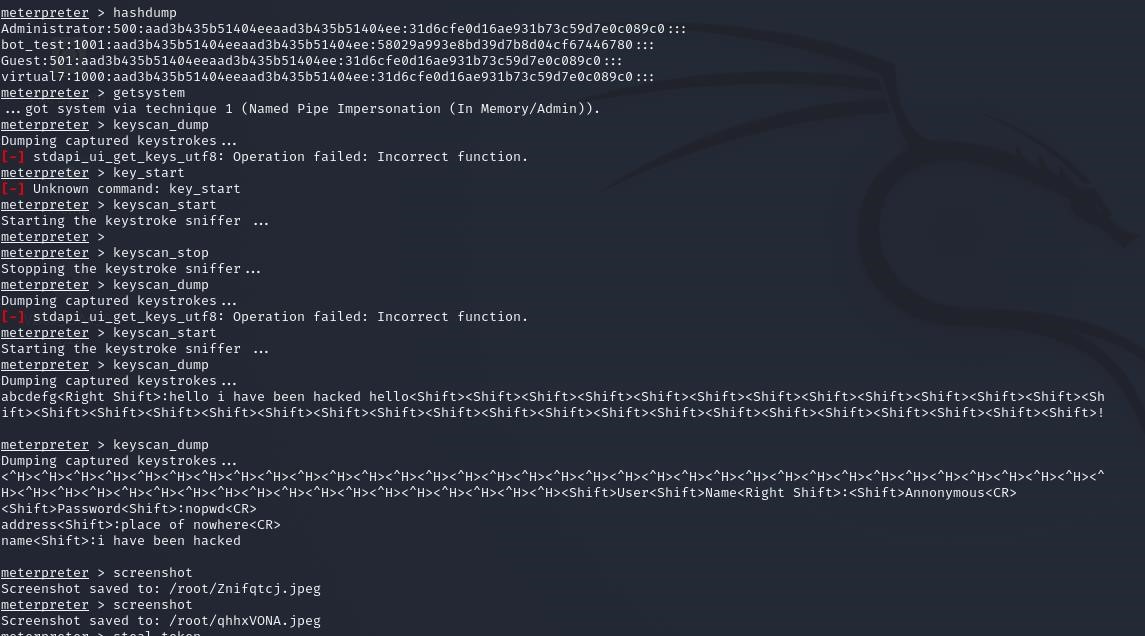


# Traveling through directories files and desktop

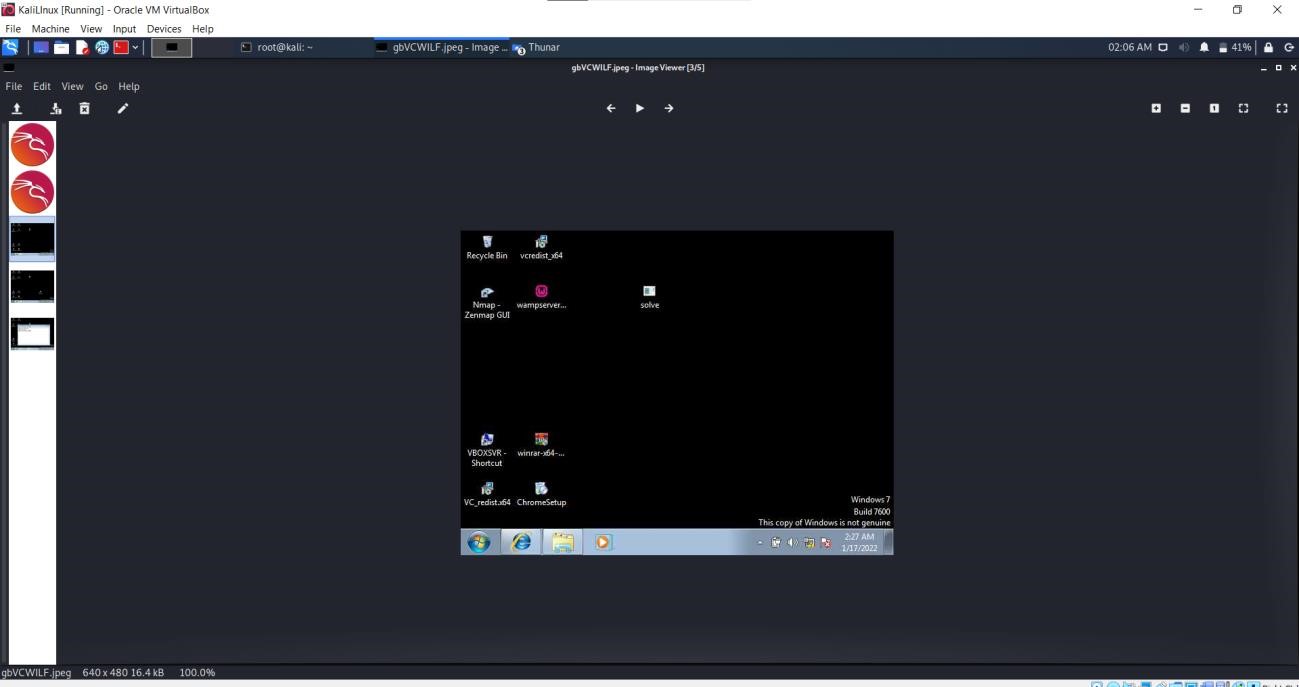
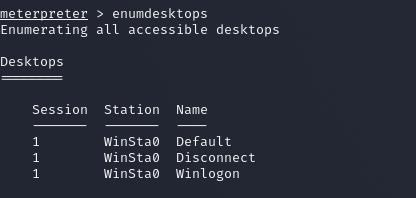
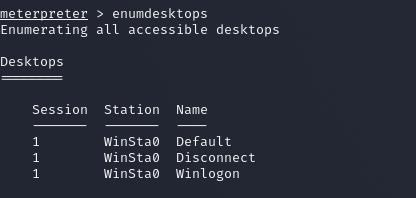




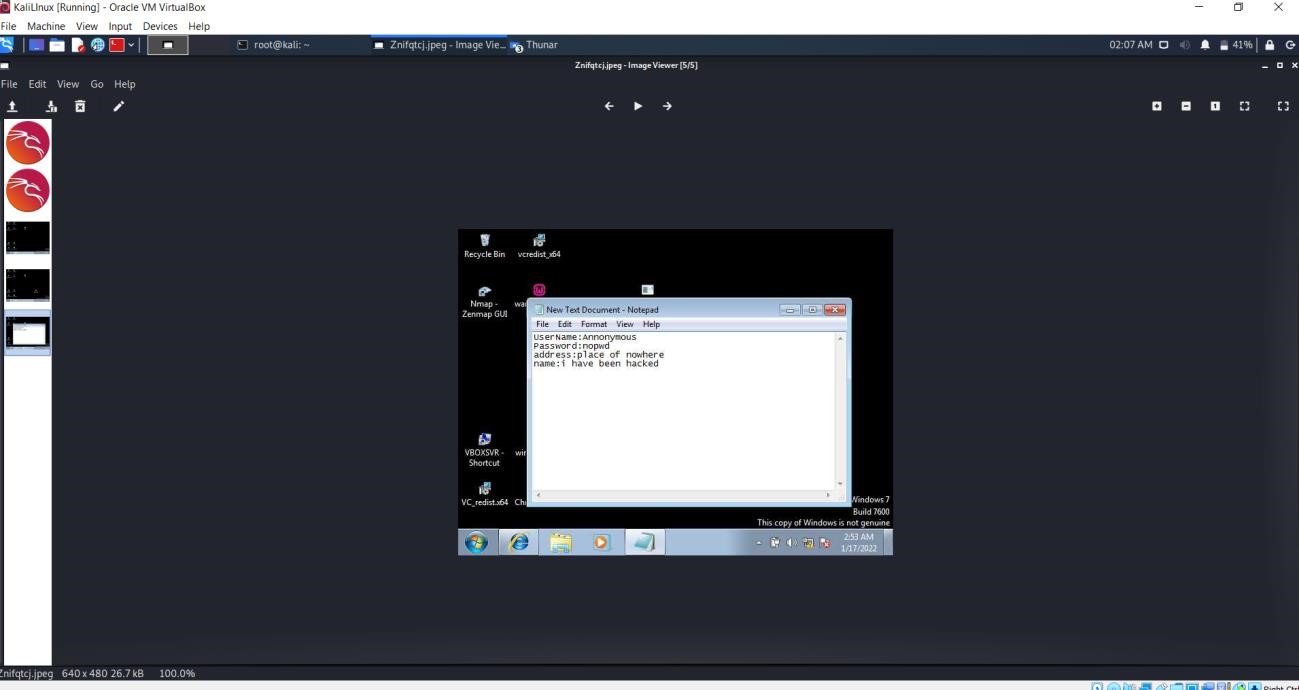
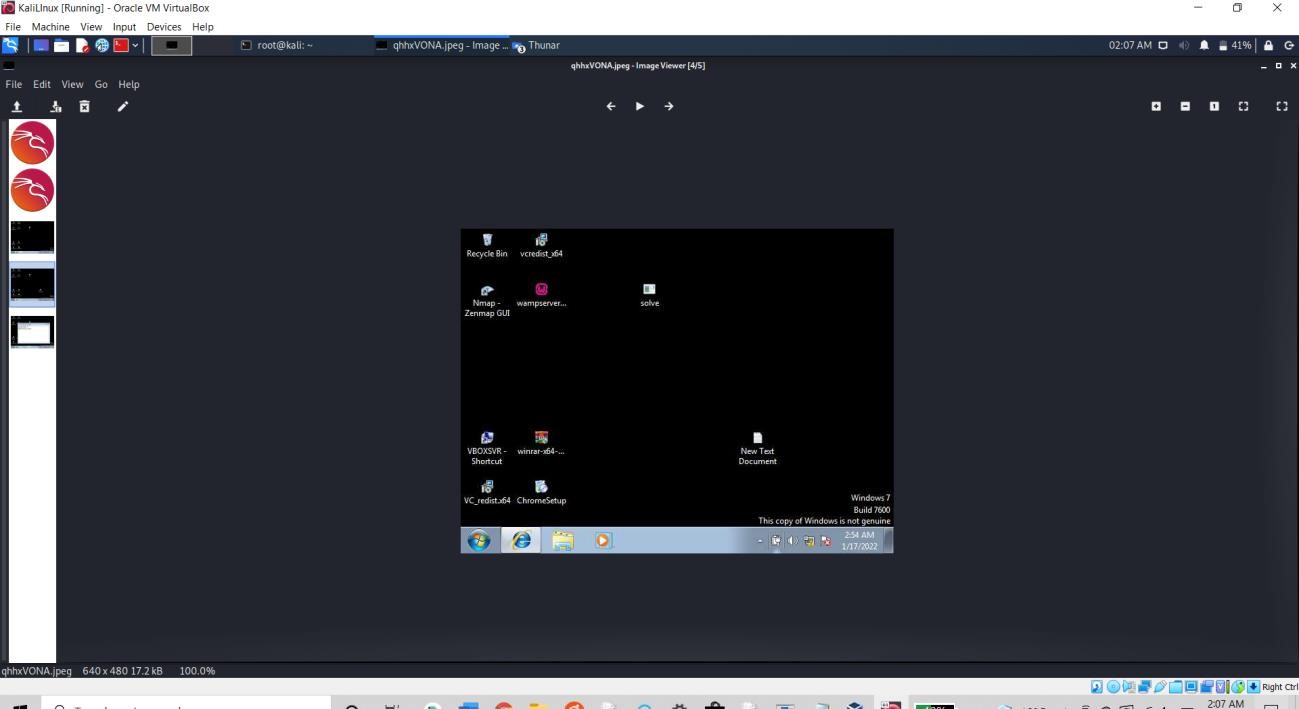


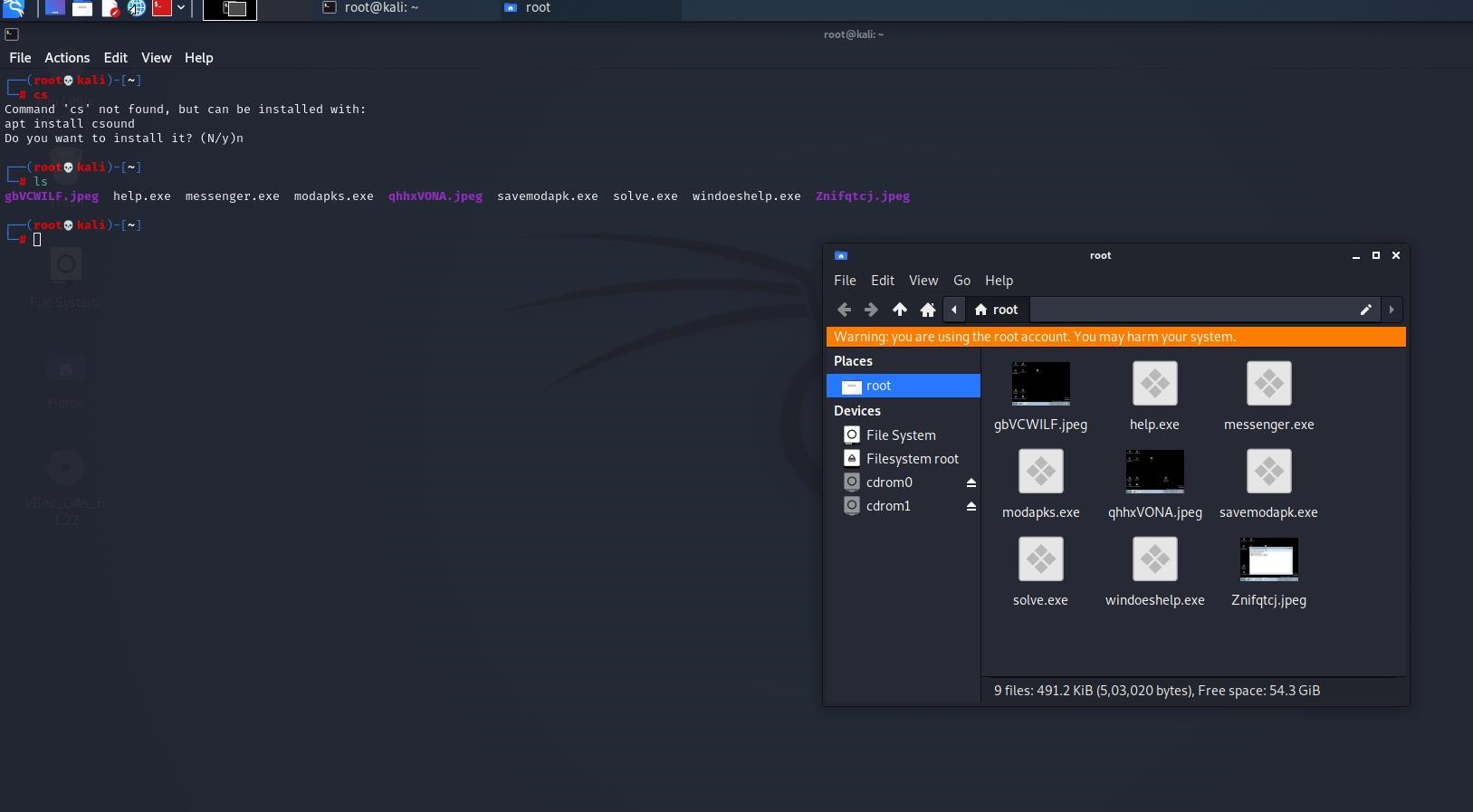


* **Got administrative information interms of hash**
* **Got keyStrokes by scanning**



# Some Screen shots taken via kali linux





# Screen shots were saved in root directory of kali linux

**Conclusion:**

* Never click over unknown links or any links from unknown sources, as the current real world attacks are more powefull than above simulated test.
* Never download any application or module,etc from third party websites or unsecured websites.
* Keep browser and system security and anti-viurs updated and use browsers that provide well and optimum security
* Never turn off or lower the browser settings as the virus file can easily get downloaded without getting detected.
* Never turn off system security services like anti-virus and firewalls
* Perform security scan of entire system atleast 4 thrice or more in a month
* Don’t give permissions to applications which they don’t require and still ask for the permission, for example a drawing application named paint asks access location permission and contacts permission.