Kali Linux Commands

Attacking from kali (attacker) to windows (victim)

For ip address in kali terminal, the command is: ifconfig

For ip address in windows, the command is: ipconfig

Then enter these commands in kali terminal:

For root user: sudo su

Nmap commands:

1) nmap -sS <your-ip> - for performing stealth scan
2) nmap -sT <your-ip> - scans for tcp protocols
3) init 0 – turns off the entire kali terminal
4) nmap -O <your-ip> - for os detection
5) nmap -sU <your-ip> - scans for udp protocols
6) nmap -sV <your-ip> - for service version detection
7) nmap -sP <your-ip> - for ping scan

Phishing using socialphish

Go to: socialphish

In kali linux type these commands:

1) git clone https://github.com/pvanfas/socialphish.git
2) cd socialphish
3) chmod +x socialphish.sh
4) ./socialphish.sh

Then select any one option and enter credentials and you will see it in kali linux terminal

DDos Attack using slowloris

On college pc, go to ADMIN/metasploitable or ADMIN/CS Tools/metaspoitable and open Metaspoitable.vmx to open it in VMWare.

Then enter username and password as msfadmin

Then get the ip address using the command: ifconfig

Note down the ip address.

Then outside the VMWare, open chrome and go to slowloris repository.

Click on code button and copy the url.

Open kali linux terminal and type the command: git clone <url>

Then change directory using command: cd slowloris

Then type the command: python3 slowloris.py <ip of metasploitable>

Open chrome in windows in VMware and enter <ip of metasploitable>

You will see that it will not load and after some time show the error 'site took too long to respond' thus proving that we successfully performed a DDos attack.

Note: If python is not installed in kali linux terminal then type the command: sudo apt install python3

Using 3rd party antivirus (AVG)

AVG antivirus is already installed, if not then install it

On your pc/VMWare (windows) press Ctrl + R and type regedit and select Yes

Then in the registry editor, select HKEY_LOCAL_MACHINE and expand it and then expand the SYSTEM

Whatever the entries we do, it gets stored in CurrentControlSet

After you restart your OS, the changes get stored in ControlSet001

Now open AVG antivirus in windows (VMWare) and click on Run Smart Scan. It will scan windows and give you issues if any.

After the scan is complete, click on Resolve All and if it asks for a free trial, then skip it and complete the scan

Scan PC using Microsoft Baseline Security Analyzer

Make sure antivirus/firewall is disabled

Open Microsoft Baseline Security Analyzer, install if it not there

Download link: MSBA

Select the first option i.e. Scan a computer

For the computer name, click on the dropdown to automatically get the hostname and then click on start scan.

It will then scan the computer and then give you a detailed report

Scan PC using ZAP

Make sure antivirus/firewall is disabled

Open ZAP, install if not there

Download link: ZAP

Then enter the url - http://testphp.vulnweb.com in the url field

Select Always in the Use ajax spider option and then click on Attack

It will then scan the url and give you a detailed report

Go to alerts section to see what were the issues

On the top right click on the Generate Report button (After firefox icon) and click on Generate Report to get a detailed report of the scan

Now you can read the detailed report of the scan in the browser

Check if your password is secure or not

1) Go to this site: security.org

Enter any password to see how secure it is

2) Go to this site: nordpass

Enter any password to see how secure it is

Keylogger using spyrix

Visit spyrix and click on My Account

Sign up with your email account and enter a password of your choice

After that, login with those details and then download the spyrix keylogger for that gmail account (first option)

Then install the setup and then open spyrix with your account

Now select the Screenshots tab to see the recent screenshots.