Assignment 2

Exploring tools available on Kali Linux
for System Security Purpose

Atharva Vaidya
121942024

Kali Linux is an open source distribution based on Debian focused on providing security auditing tools. Actively developed by Offensive Security, it's one of the most popular security distributions in use by infosec companies and ethical hackers. It includes numerous security-hacker tools for information gathering, vulnerability analysis, wireless attacks, web applications, exploitation tools, stress testing, forensic tools, sniffing and spoofing, password cracking, reverse engineering, hardware hacking and much more.
In this activity students are expected to practically learn following available tools on Kali Linux and prepare abstract report of all the tools and brief report (with screen shorts) of 15 tools (10 Red and 5 of their own choice and exclude this from brief report):

Contents

NMAP

Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks. Nmap can be used to monitor single hosts as well as vast networks that encompass hundreds of thousands of devices and multitudes of subnets. While the basis of Nmap's functionality is port scanning, it allows for a variety of related capabilities including:

- **Network mapping** : Nmap can identify the devices on a network (also called host discovery), including servers, routers and switches, and how they're physically connected.
- **OS detection** : Nmap can detect the operating systems running on network devices (also called OS fingerprinting), providing the vendor name, the underlying operating system, the version of the software and even an estimate of devices' uptime.
- **Service discovery** : Nmap can not only identify hosts on the network, but whether they're acting as mail, web or name servers, and the particular applications and versions of the related software they're running.
- **Security auditing** : Figuring out what versions of operating systems and applications are running on network hosts lets network managers determine their vulnerability to specific flaws. If a network admin receives an alert about a vulnerability in a particular version of an application, for example, she can scan her network to identify whether that software version is running on the network and take steps to patch or update the relevant hosts. Scripts can also automate tasks such as detecting specific vulnerabilities.

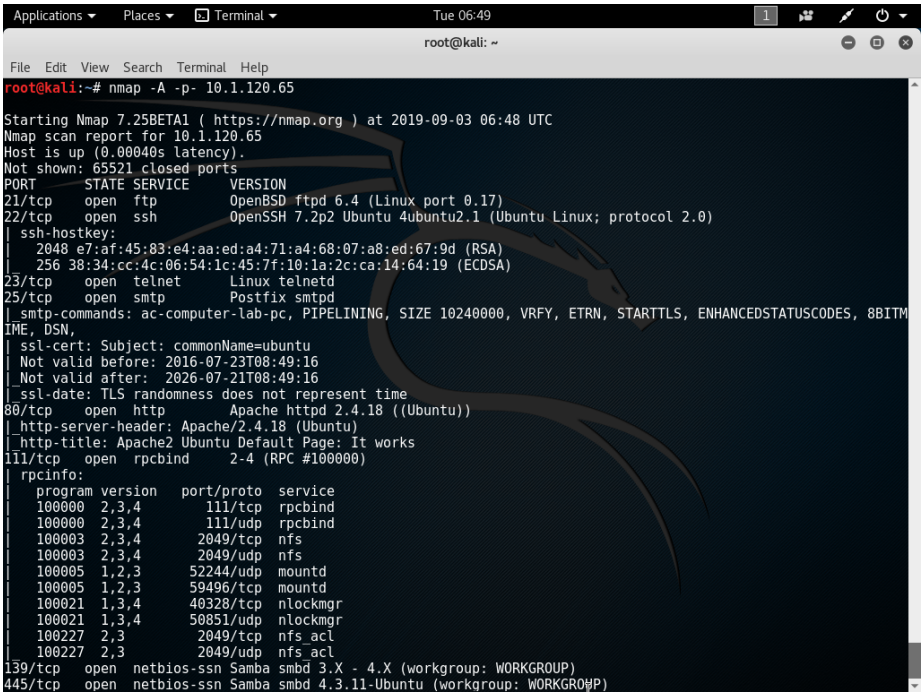

Figure 1: Scanning a PC on LAN.(1)

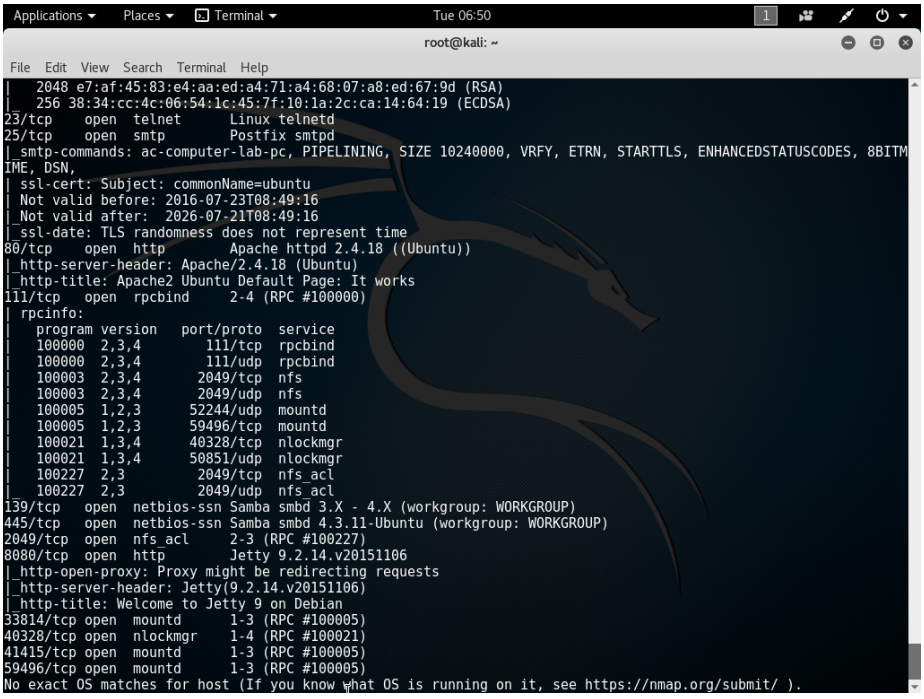

Figure 2: Scanning a PC on LAN.(2)

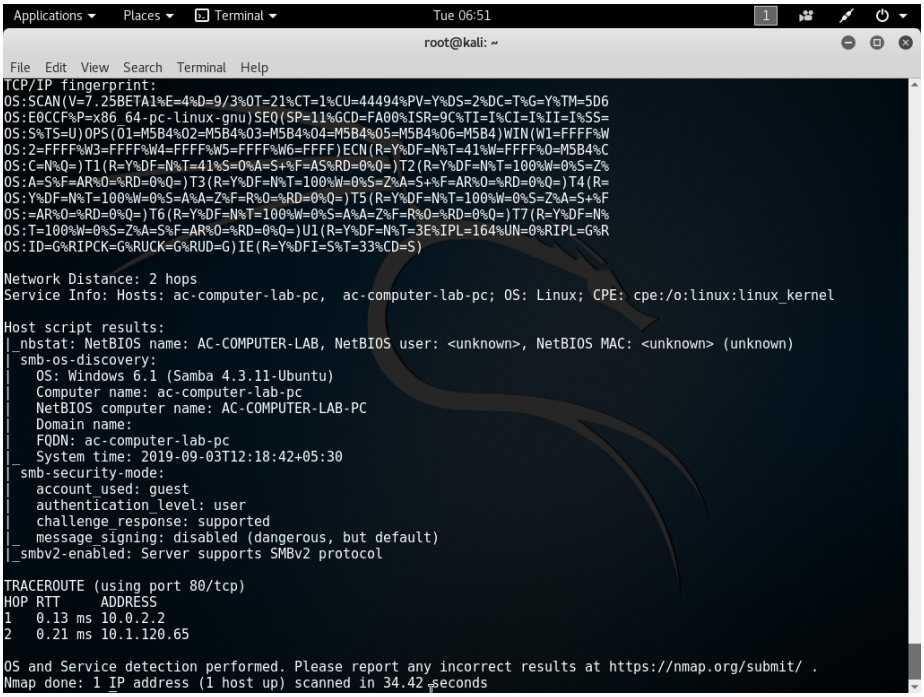

Figure 3: Scanning a PC on LAN.3

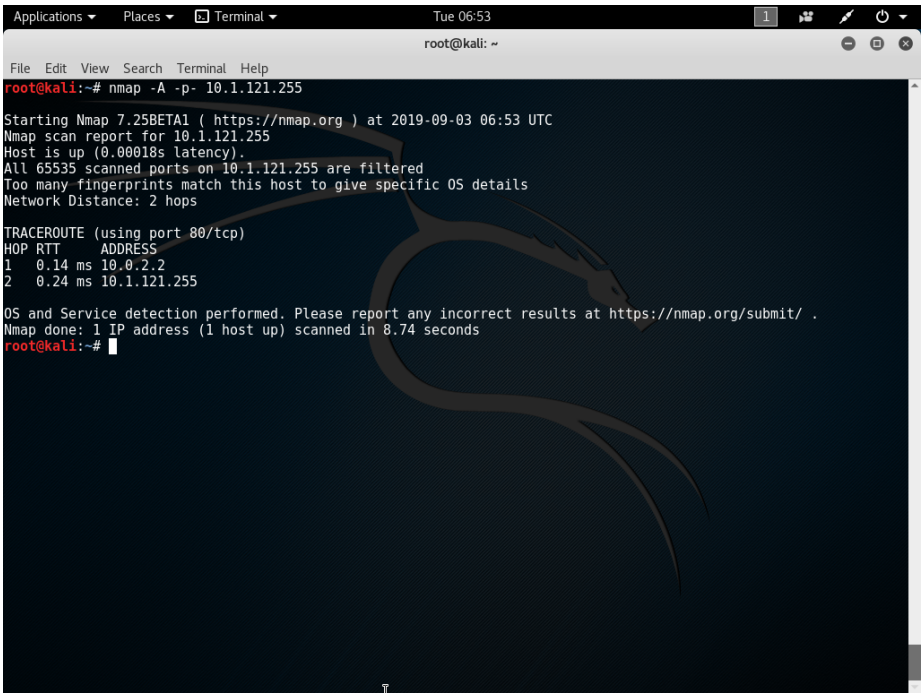

Figure 4: Scanning a PC on Virtual Machine.

Nessus

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.
Working Each computer has thousands of ports, all of which may or may not have services (ie: a server for a specific high-level protocol) listening on them. Nessus works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack. Nessus is called a "remote scanner" because it does not need to be installed on a computer for it to test that computer. Instead, you can install it on only one computer and test as many computers as you would like.

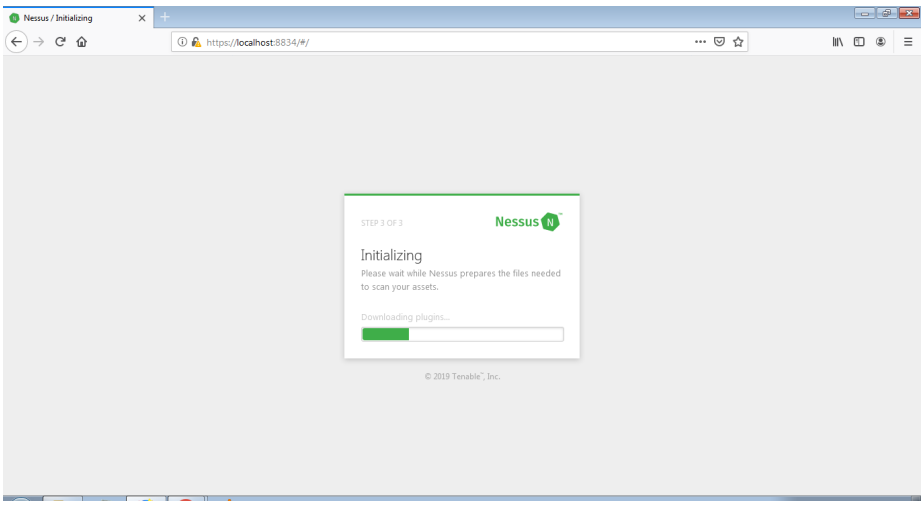

Figure 5: Nessus Initialization

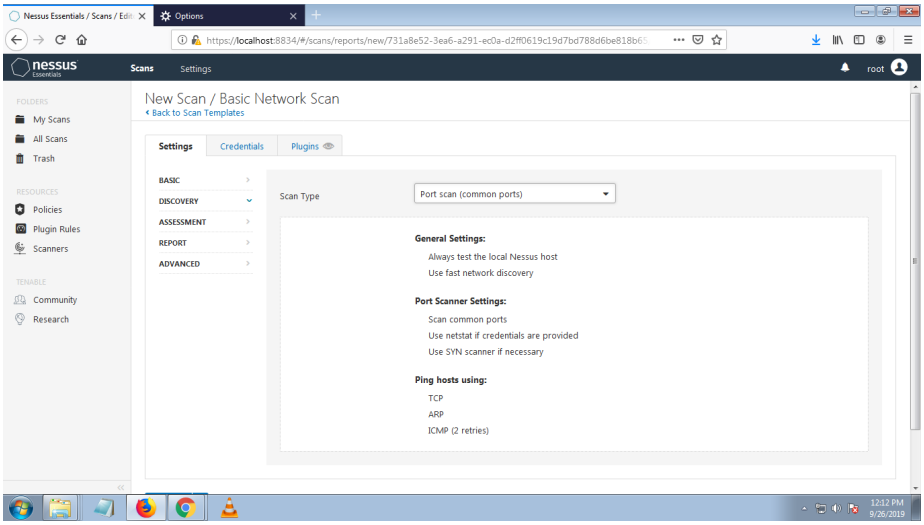

Figure 6: Settings Page

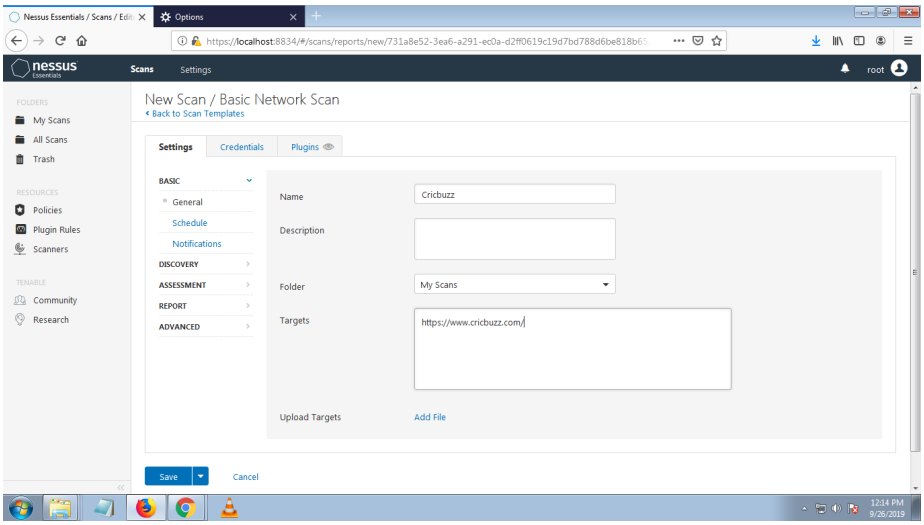

Figure 7: General Settings Page

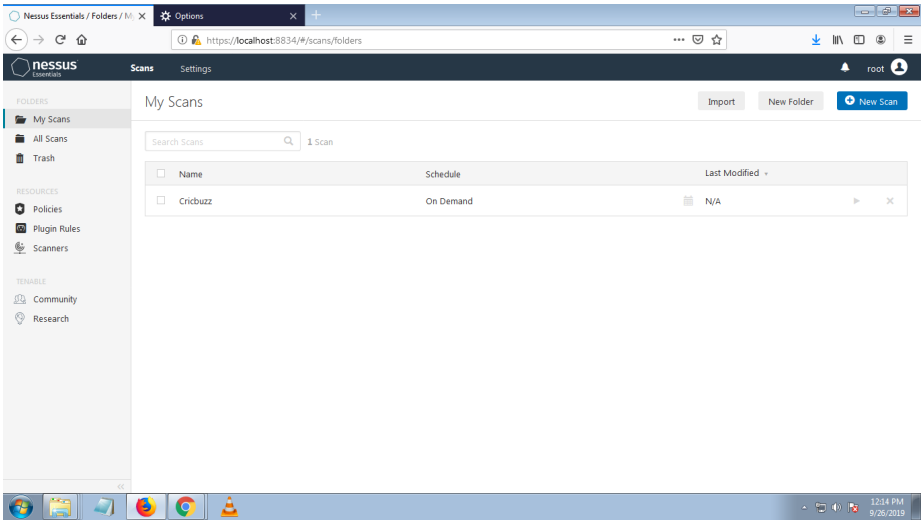

Figure 8: Scans List Page

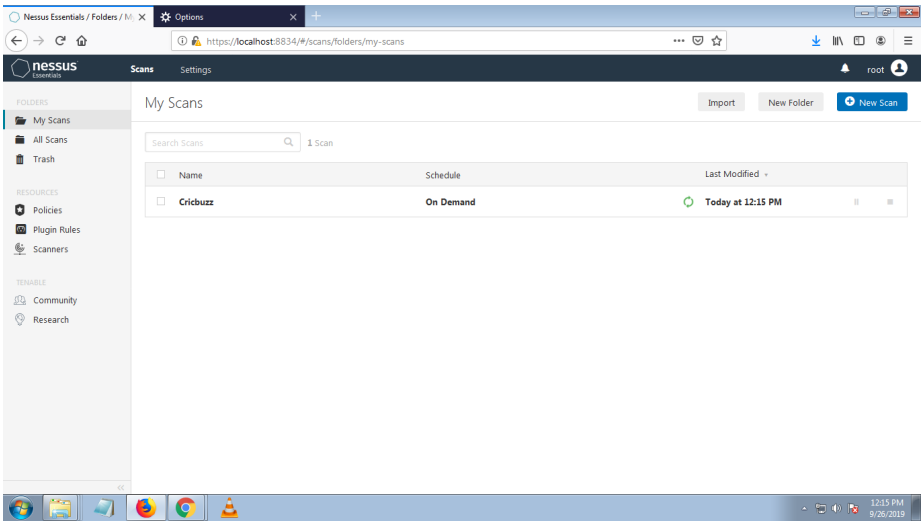

Figure 9: Scan Started

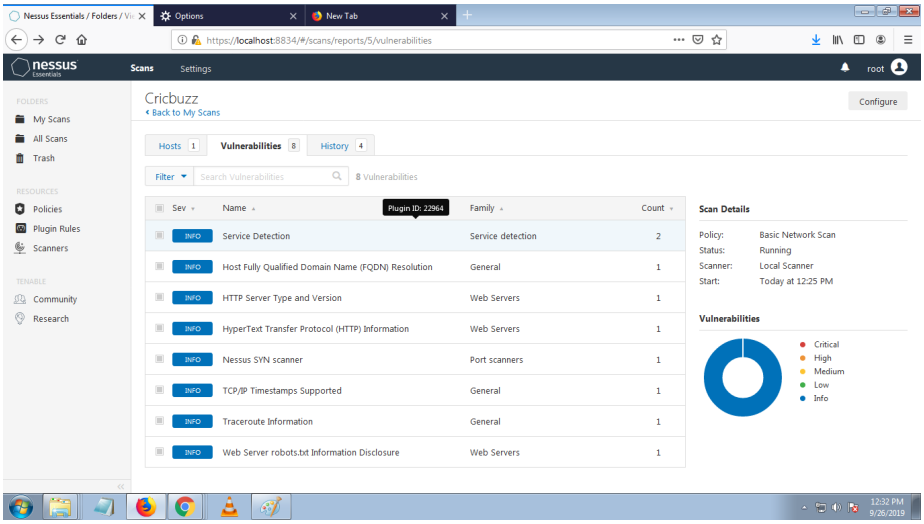

Figure 10: Vulnerabilities List

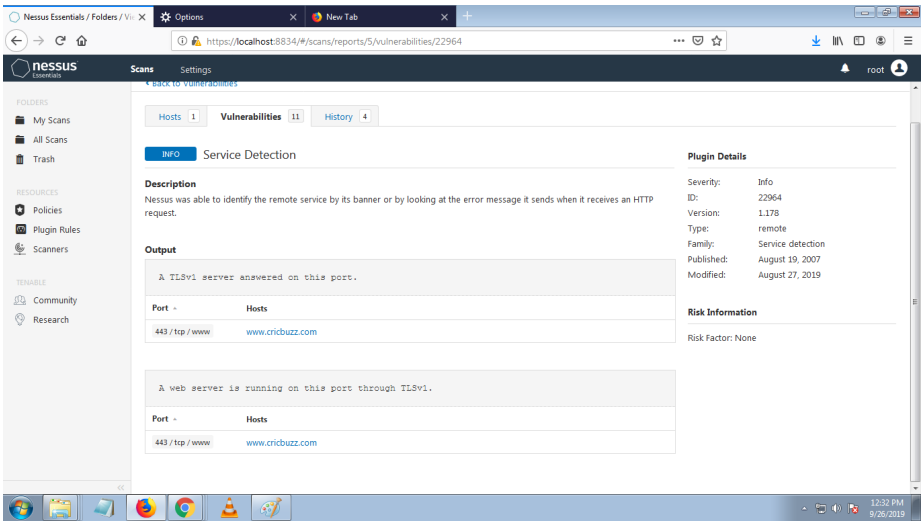

Figure 11: Service Detection Information

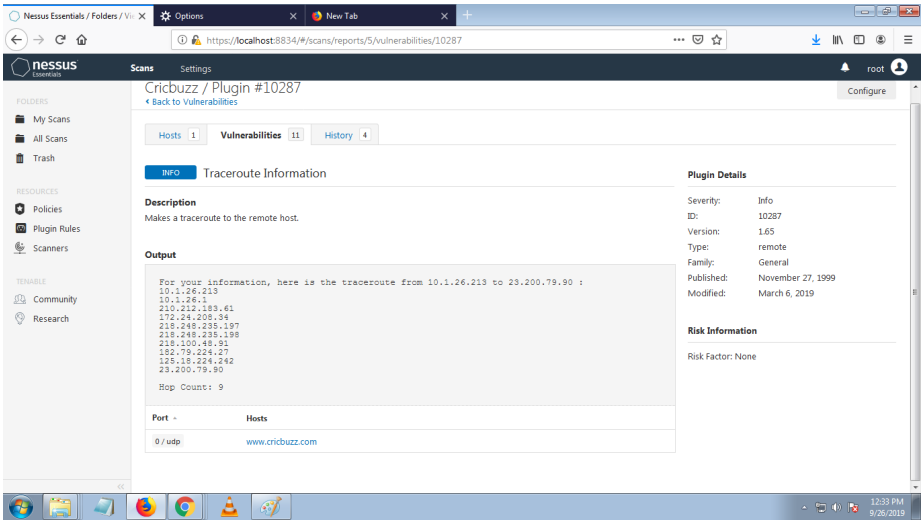

Figure 12: Traceroute Information

Lynis

Lynis is a security tool for systems running Linux, macOS, or Unix-based operating system. It performs an extensive health scan of your systems to support system hardening and compliance testing.
Lynis scanning is modular. It will only use and test the components that it can find, such as the available system tools and its libraries.No installation of other tools is needed.

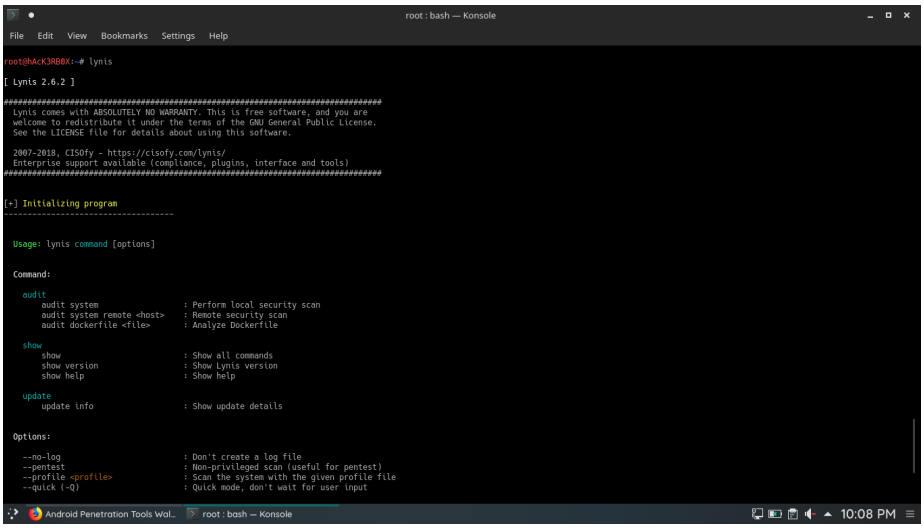

Figure 13: Lynis

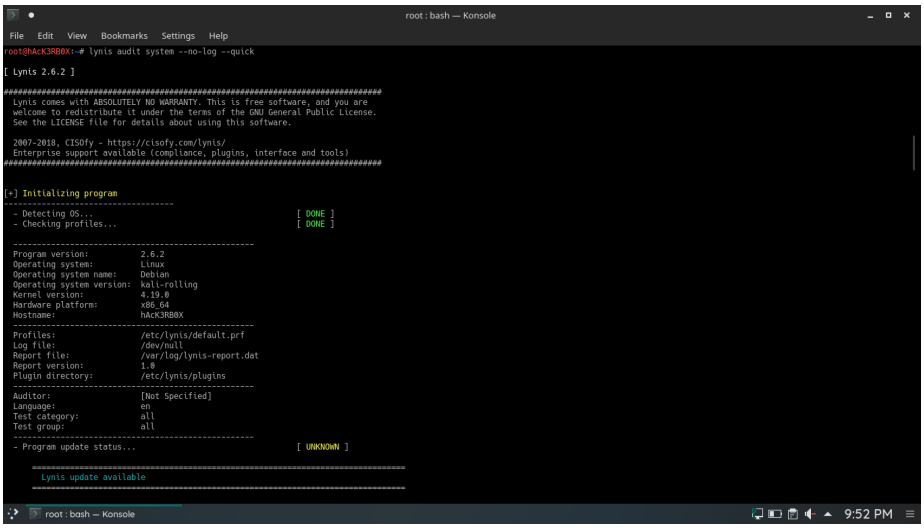

Figure 14: Lynis System Audit - OS Detection

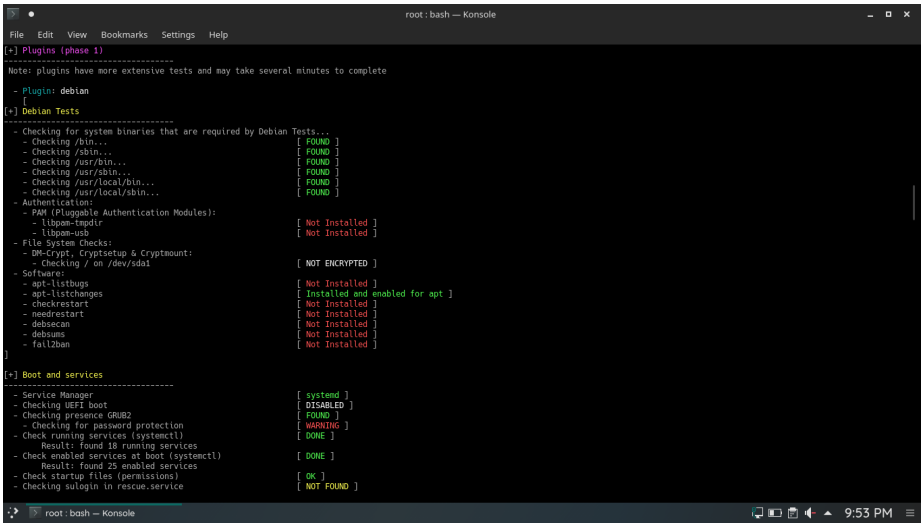

Figure 15: Lynis System Audit - Debian Tests and Boot Services

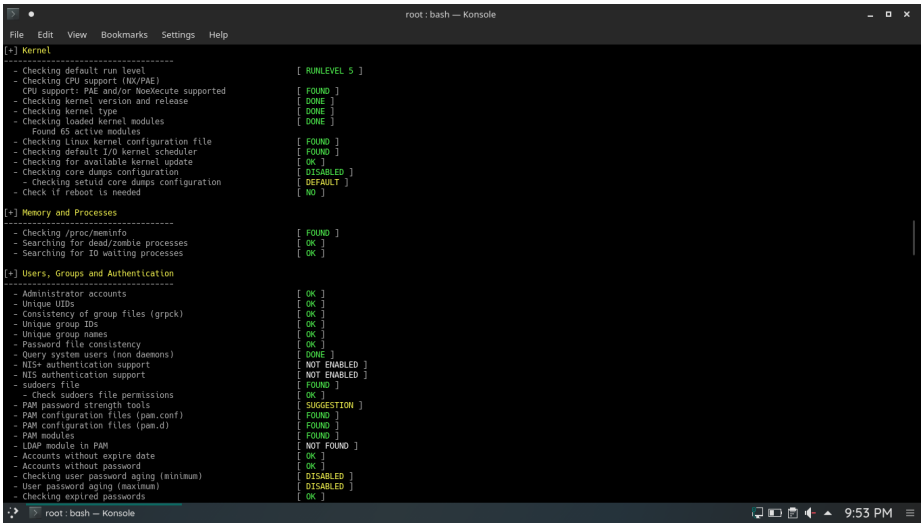

Figure 16: Lynis System Audit - Kernel, Memory and Processes, Users and Group

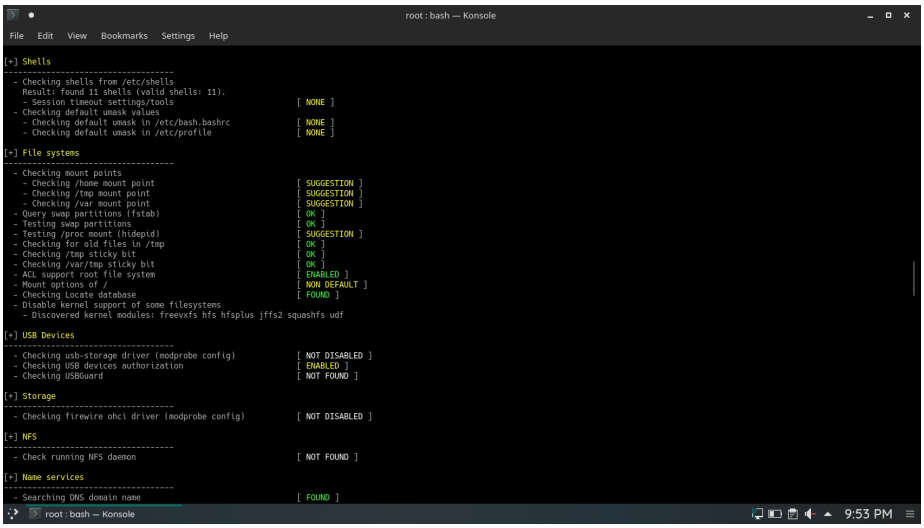

Figure 17: Lynis System Audit - Shell, Filesystems and Devices

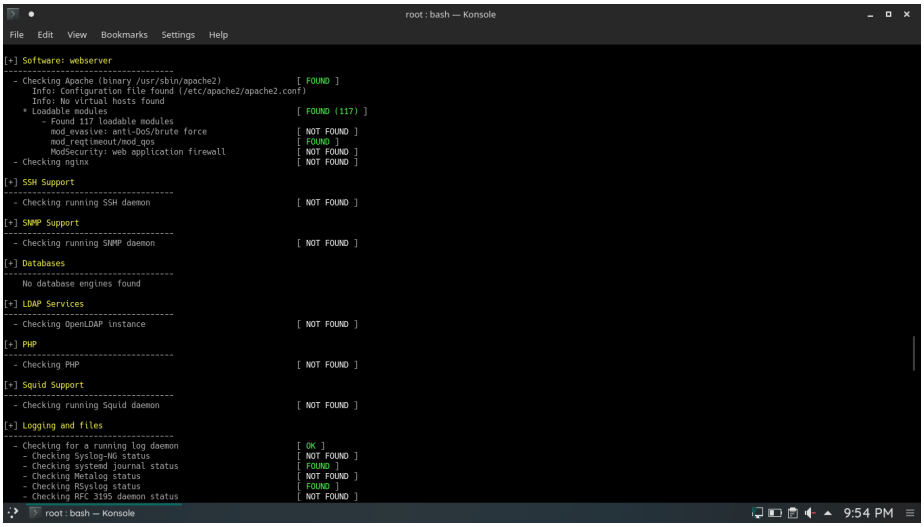

Figure 18: Lynis System Audit - SSH, LDAP, Logging

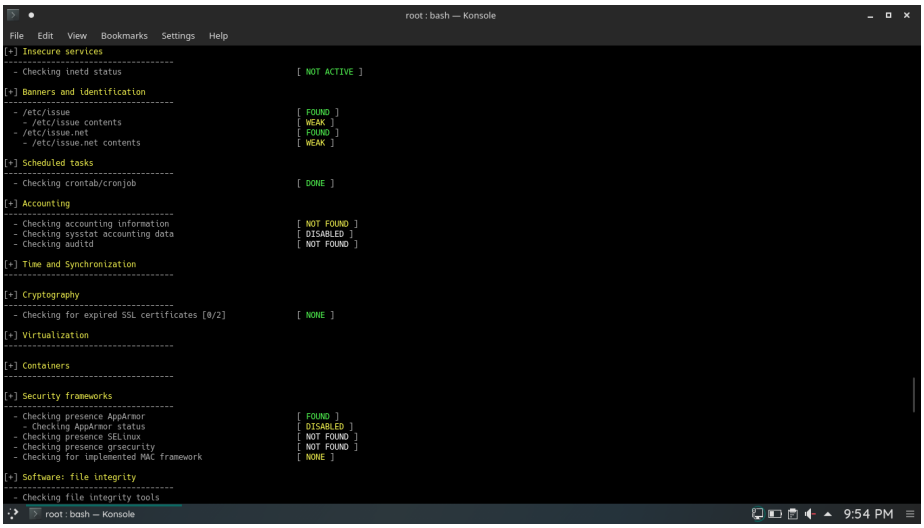

Figure 19: Lynis System Audit - Security Frameworks

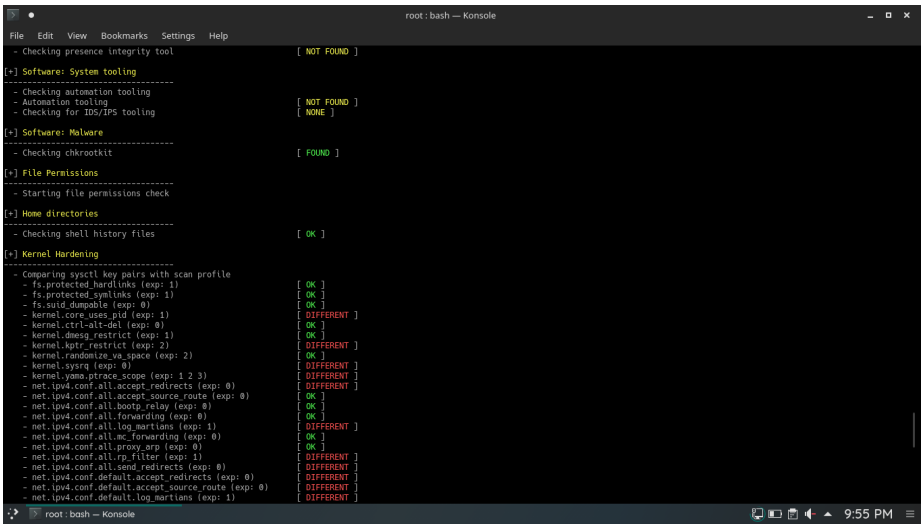

Figure 20: Lynis System Audit - Kernel Hardening

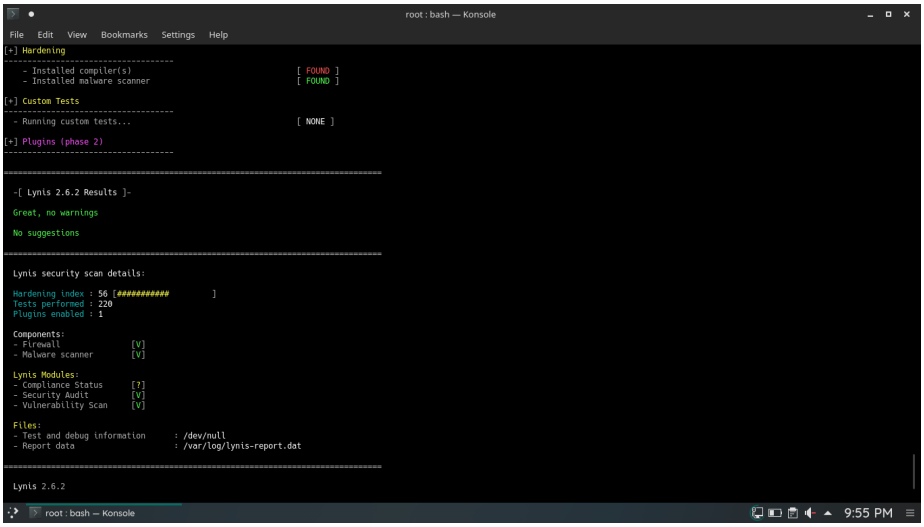

Figure 21: Lynis System Audit - Suggestions

John the Ripper

John the Ripper is a fast password cracker. It is an old but a very good password cracker that uses wordlists to crack given hash. This software is available in two versions such as paid version and free version. It is totally cross-platform.
John the Ripper works in 3 distinct modes to crack the passwords:

- **Single Crack Mode** : In this mode John the ripper makes use of the information available to it in the form of a username and other information.
- **Wordlist Crack Mode** : In this mode John the ripper uses a wordlist that can also be called a Dictionary and it compares the hashes of the words present in the Dictionary with the password hash. We can use any desired wordlist.
- **Incremental Mode** : This is the most powerful cracking mode, it can try all possible character combinations as passwords. However, it is assumed that cracking with this mode will never terminate because of the number of combinations being too large (actually, it will terminate if you set a low password length limit or make it use a small charset), and you'll have to interrupt it earlier.

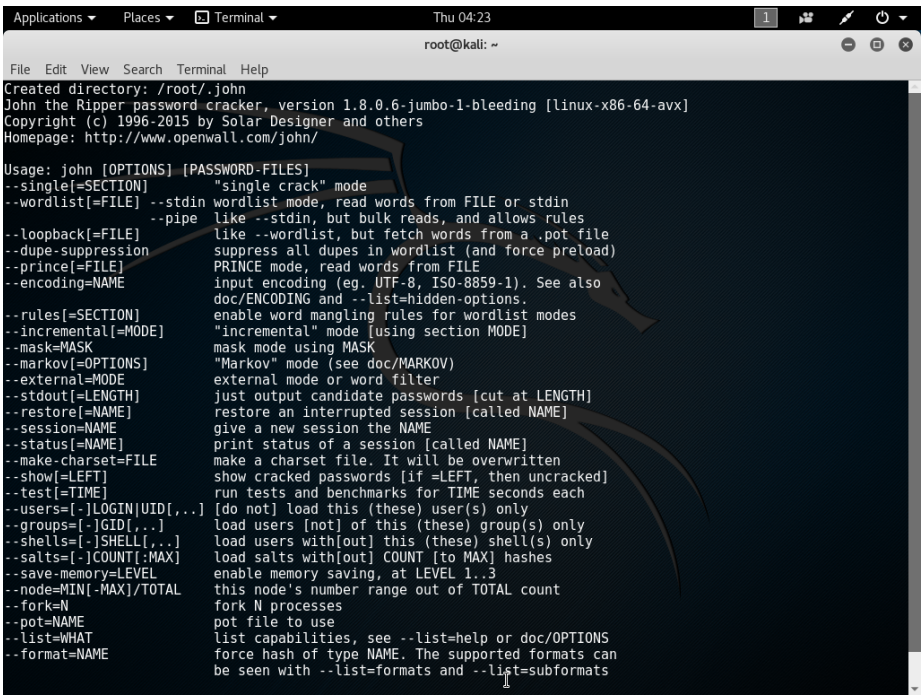

Figure 22: John The Ripper

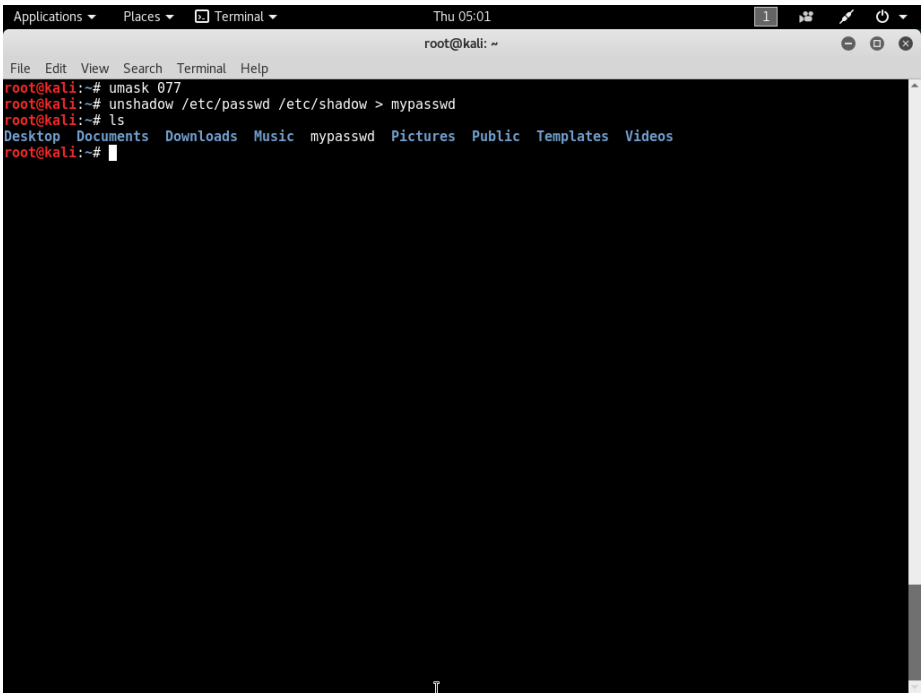

Figure 23: Unshadowing the shadow file and copying to PWD

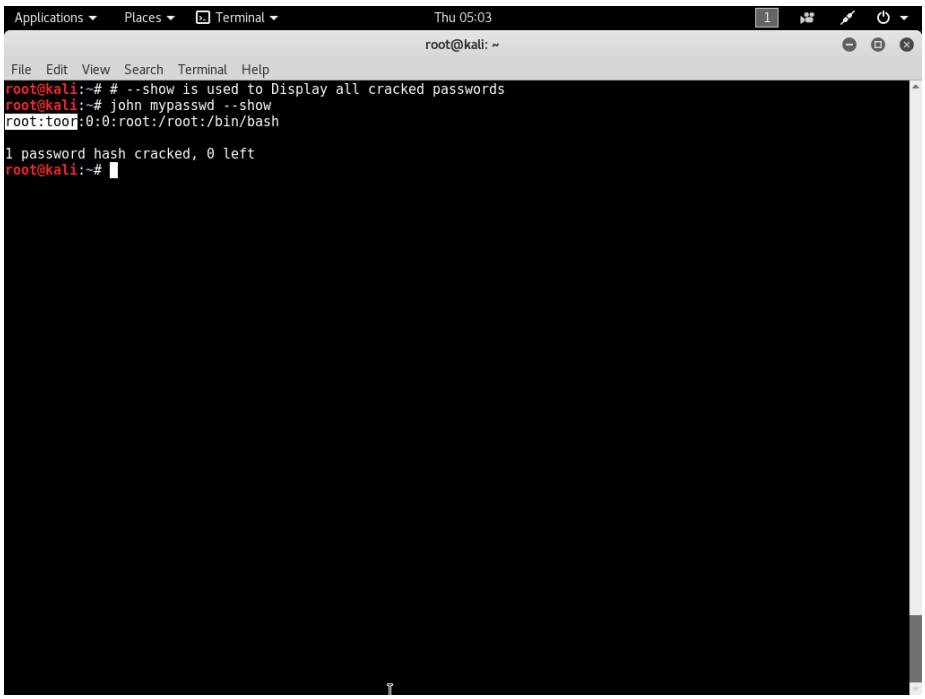

Figure 24: Cracking the Passwords of users

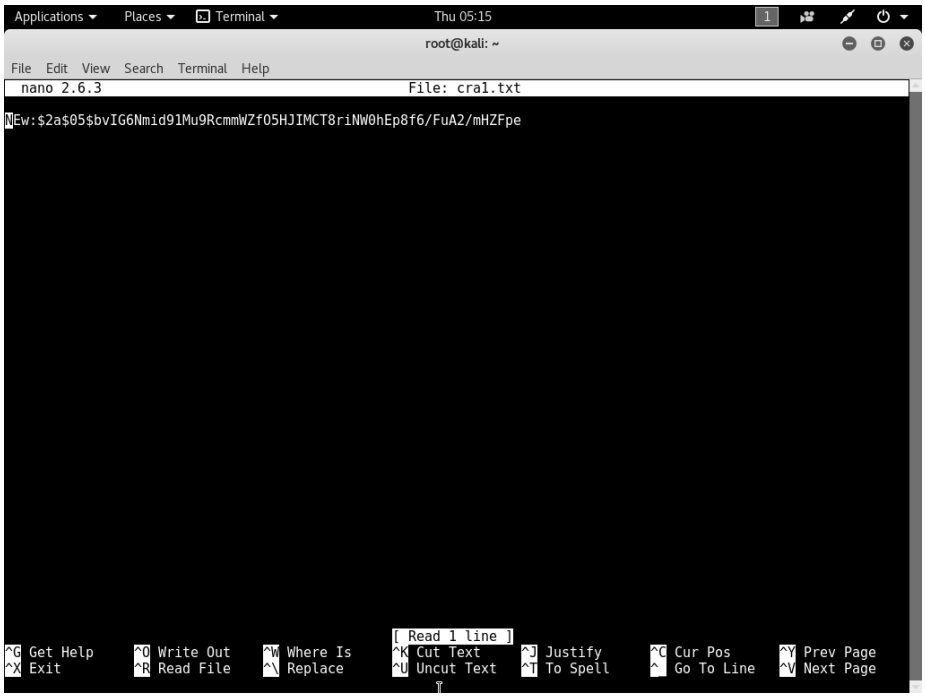

Figure 25: Contents of a Text File containing Hash

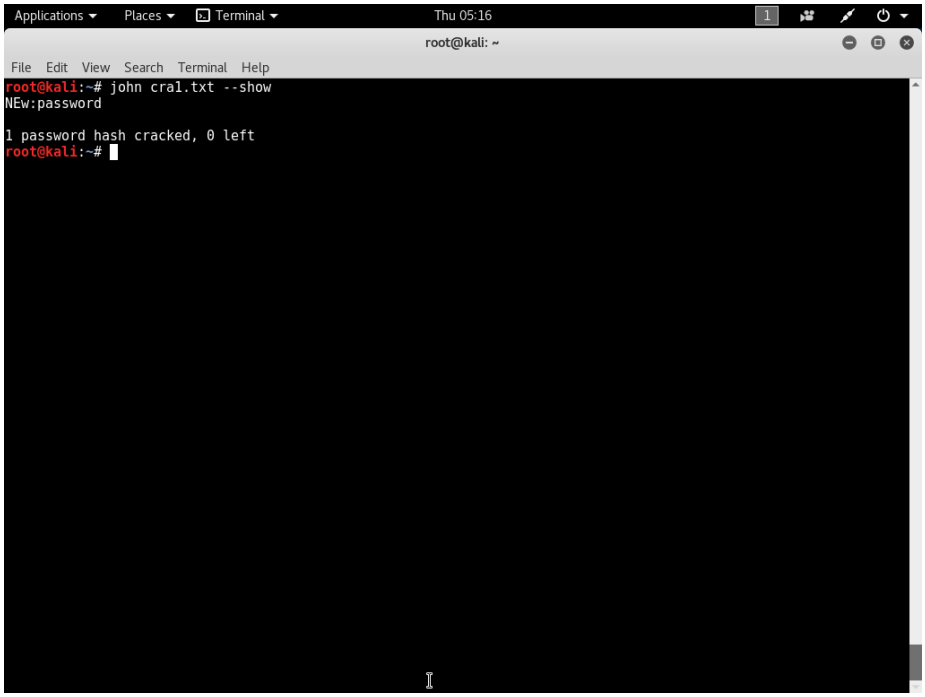

Figure 26: Cracking the Hash of the Text file

Apktool

Apktool is a tool for reverse engineering 3rd party, closed, binary Android apps. It can decode resources to nearly original form and rebuild them after making some modifications. It also makes working with an app easier because of the project like file structure and automation of some repetitive tasks like building apk, etc. Decompiling an APK enables to view the content inside an apk file and various aspects of an app or game can be modified. APKTool is used to port applications to previously unsupported devices, theme some of your favorite applications, look into the strings of APK files to see what may be coming in future updates, and provide translations for applications.

Decode APK Resources

In the illustration below, I am using vulnerable APK file **(diva-beta.apk)** Decoding can be done using the command:

apktool d diva-beta.apk

The **res** folder contains all the media files including images, ringtones and many more. It also contains the front-end XML files which can be used to alter the look and feel of the app you have decompiled.

Original folder contains META-INF and original AndroidManifest.xml, META-INF has APK signatures. After modifying the APK, it is no longer signed.

The **AndroidManifest.xml** file describes essential information about your app to the Android build tools, the Android operating system, and Google Play.

The **Smali** folder is the important part, Apktool decodes compiled java files in the form of .smali files (Read more on smali here). These Smali files are responsible for the functionality of the app and handling them would create direct impacts to the app.

Rebuilding decoded resources back to binary APK

Once done with the modification to the APK source, the APK file can be rebuilt from the source files using the command:

apktool b diva-beta

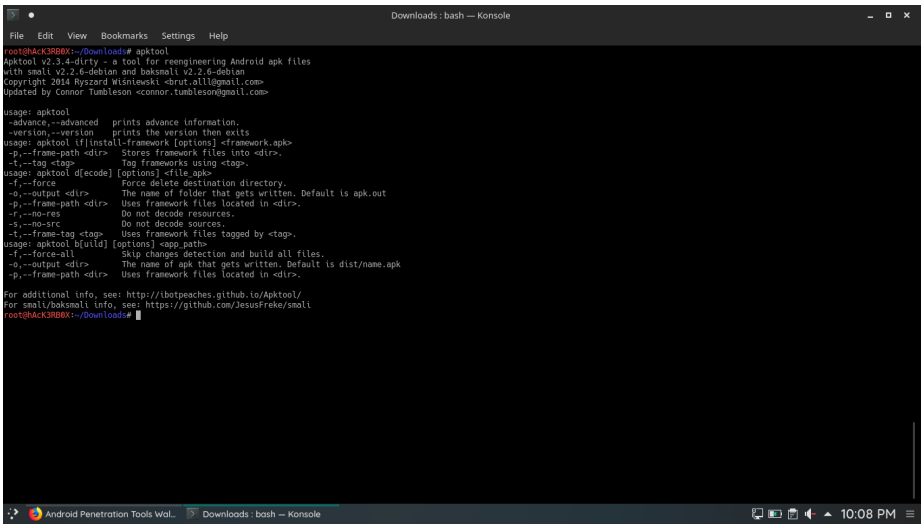

Figure 27: Apktool

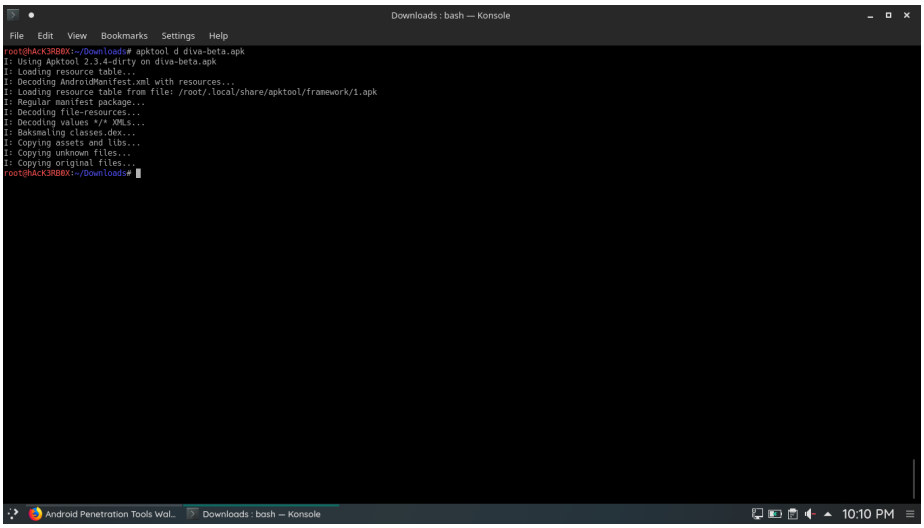

Figure 28: Decoding the diva-beta APK File

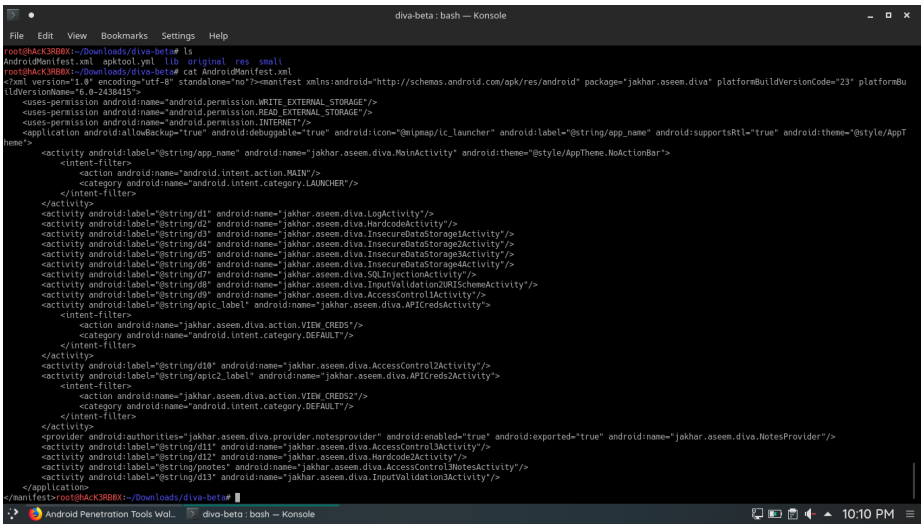

Figure 29: Displaying AndroidManifest.xml file

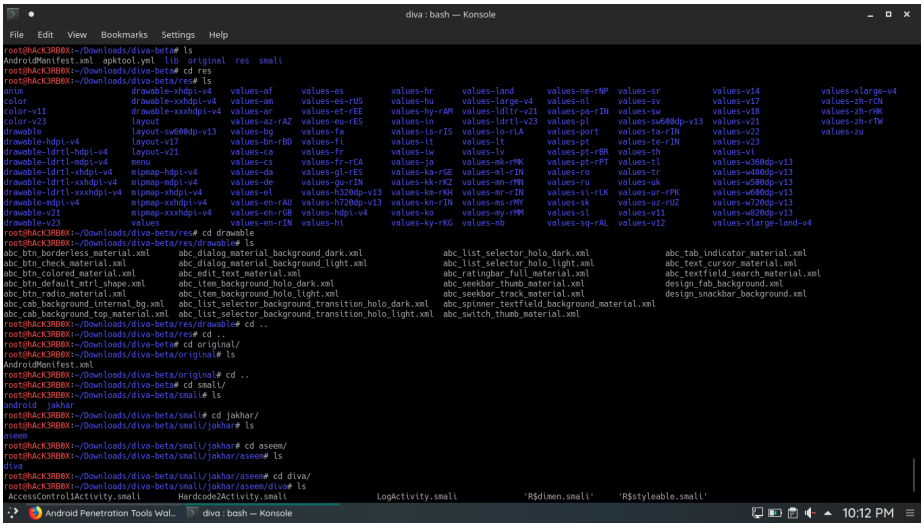

Figure 30: Browsing the Decompiled App Directory

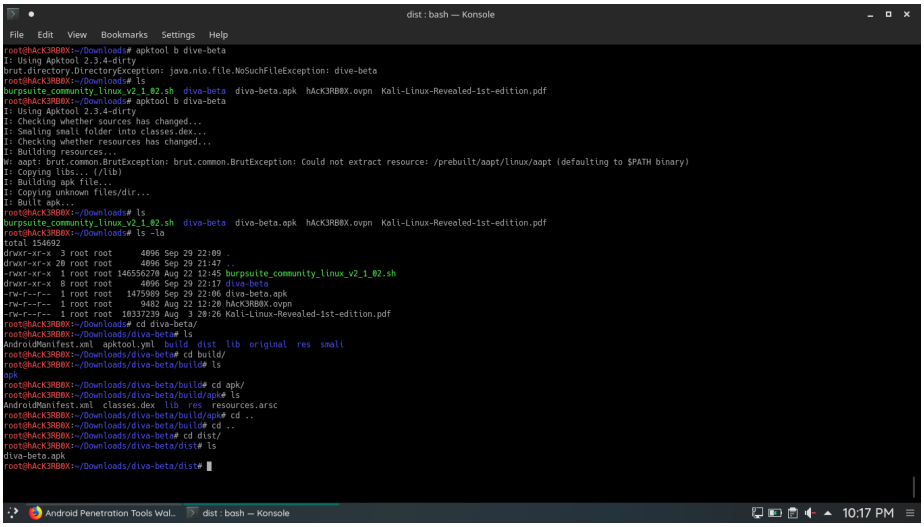

Figure 31: Recompiling the App from the Decompiled Directory

Hydra

Hydra (better known as “thc-hydra”) is an online password attack tool.It is very fast and flexible, and new modules are easy to add.This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.It brute forces various combinations on live services like telnet, ssh, http, https, smb, snmp, smtp etc.Hydra supports 30+ protocols including their SSL enabled ones.It brute forces on services we specify by using user-lists & wordlists.
Hydra works in 4 modes:

- One username & one password
- User-list & One password
- One username & Password list
- User-list & Password list

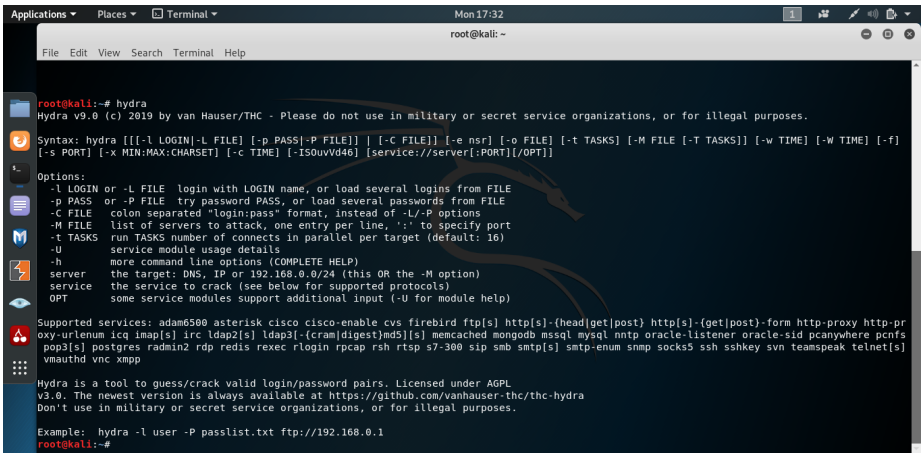

Figure 32: Hydra

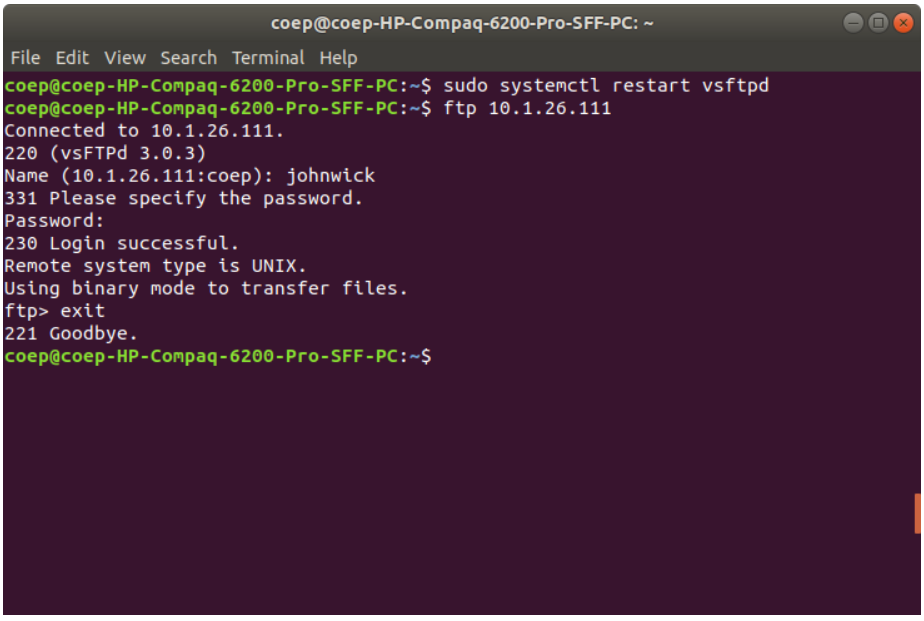

Figure 33: Creating FTP Server

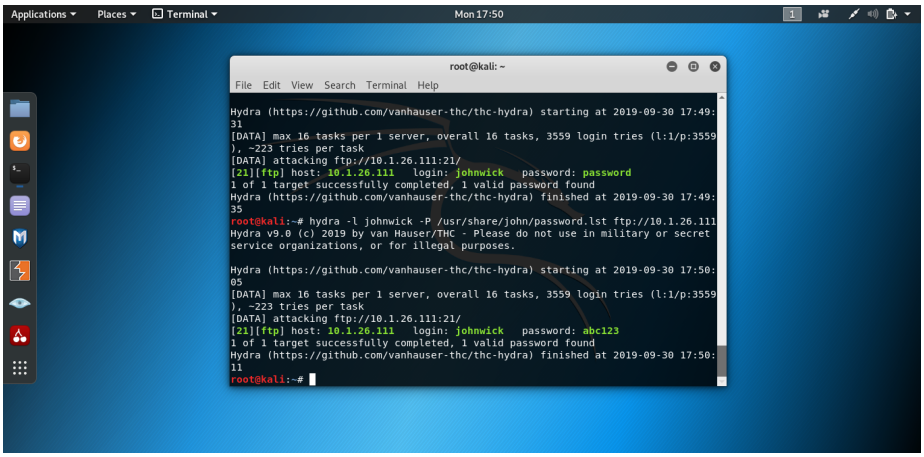

Figure 34: Cracking FTP Server

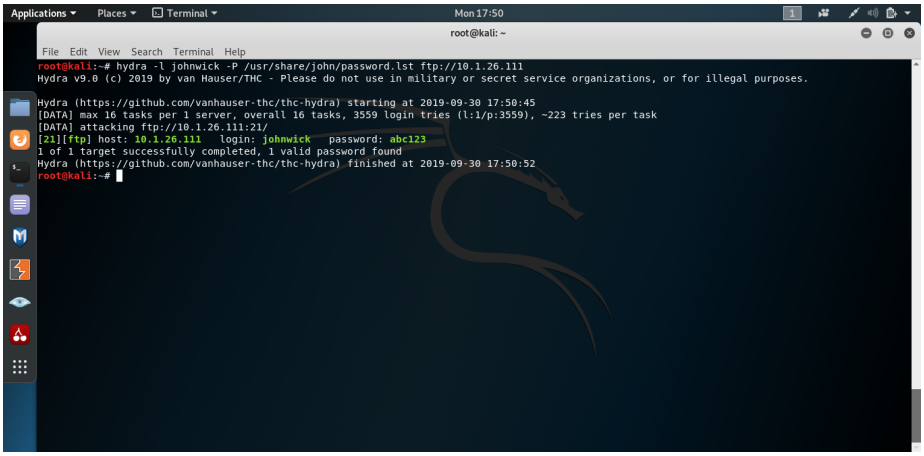

Figure 35: Cracking FTP Server

RainbowCrack

RainbowCrack is a revolutionary hash cracker that we have shared on this page along with Rainbow Tables free to download. It allows user to decrypt a hashed password into understandable plain text. With this software, a password of any length can be cracked in a matter of minutes no matter how strong the opposite security encryption is.

Working

RainbowCrack does not uses brute force attacks like other software.It uses time-memory tradeoff algorithm which uses more storage in order to reduce time. It first requires a pre-computation stage in which all plaintext/hash pairs are computed and stored in rainbow table. There are Terabytes of Rainbow Tables available online, some are free while some paid.It cracks a hash in few minutes that would take up to 4 weeks using brute force attack.

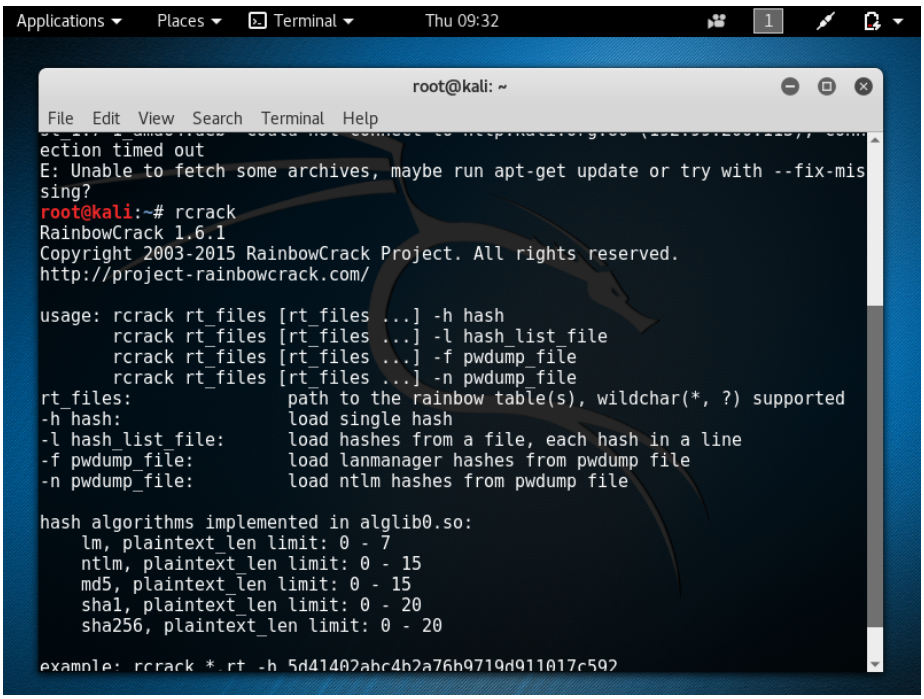

Figure 36: RainbowCrack

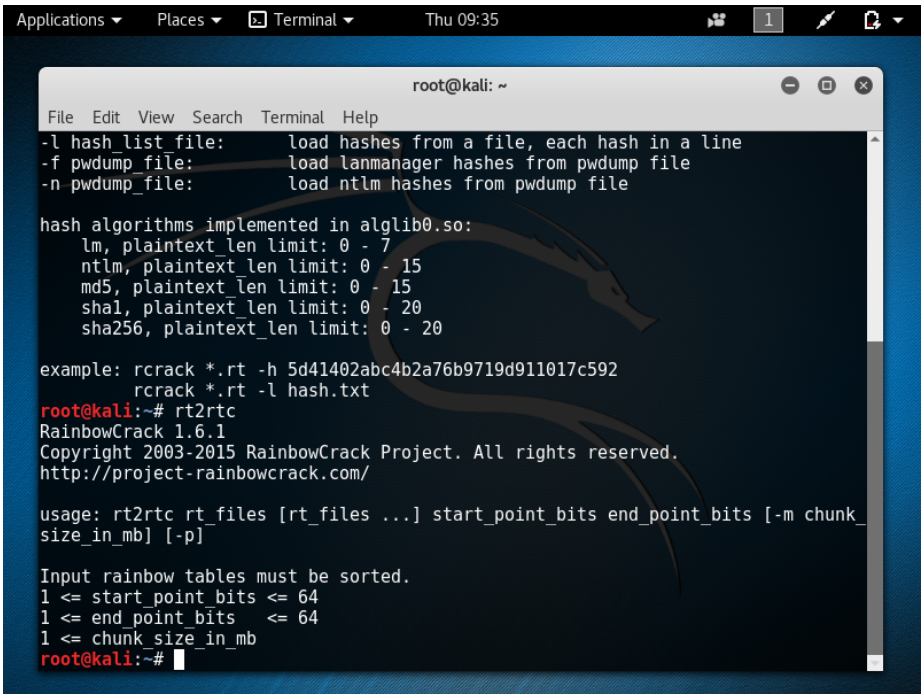

Figure 37: RainbowCrack

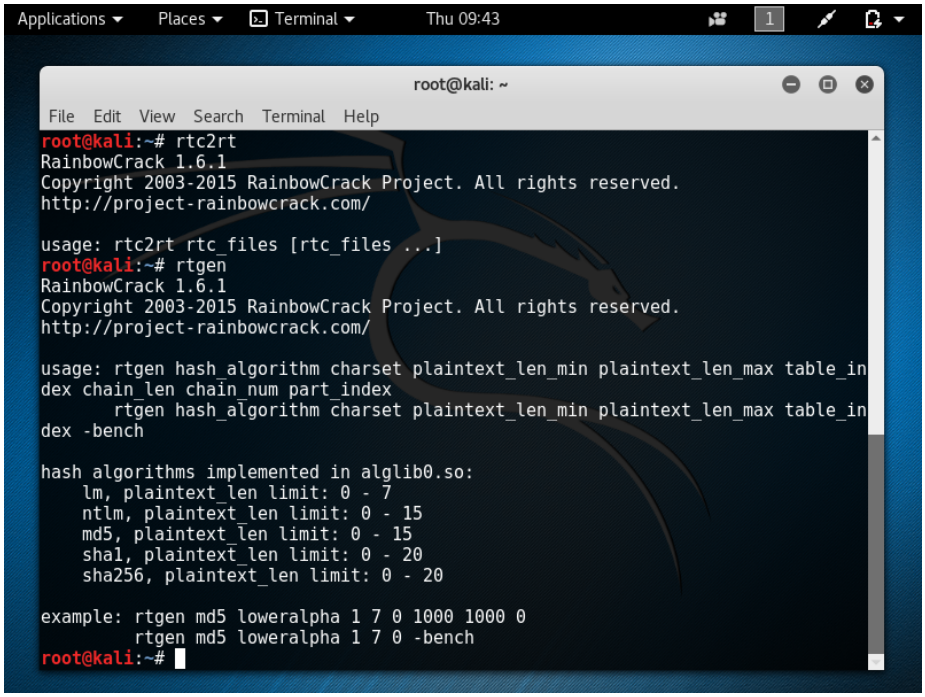

Figure 38: RainbowCrack

UnicornScan

Unicornscan is a sophisticated, powerful and stateless port scanner that uses stimulus into and measuring a response from any TCP/IP enabled device.One of the key features of unicornscan that sets it apart of nmap and other port scanners is that it has its own TCP/IP stack. The other port scanners all use the underlying host operating system's TCP/IP stack. This enables unicornscan to scan much more quickly than the others as it can, for instance, send out SYN packets with one thread and receive the responses with another thread. This can make a huge difference when scanning very large networks as a security researcher/ pentester where we might be scanning thousands of IP addresses and be even more important to an attacker who may be scanning millions of addresses looking for a particular open port or vulnerability. In addition, because it has its own TCP/IP stack, it is capable of sending packets with different OS fingerprints that the operating system of your host. This can be very useful for obscuring your identity, especially combined with IP spoofing.

This simple syntax will return for us the open TCP ports on the target system, very similar to the nmap -sS scan, but without the default ICMP that nmap uses. As you can see, unicornscan reports back to us that ports 80 are open on the target system.

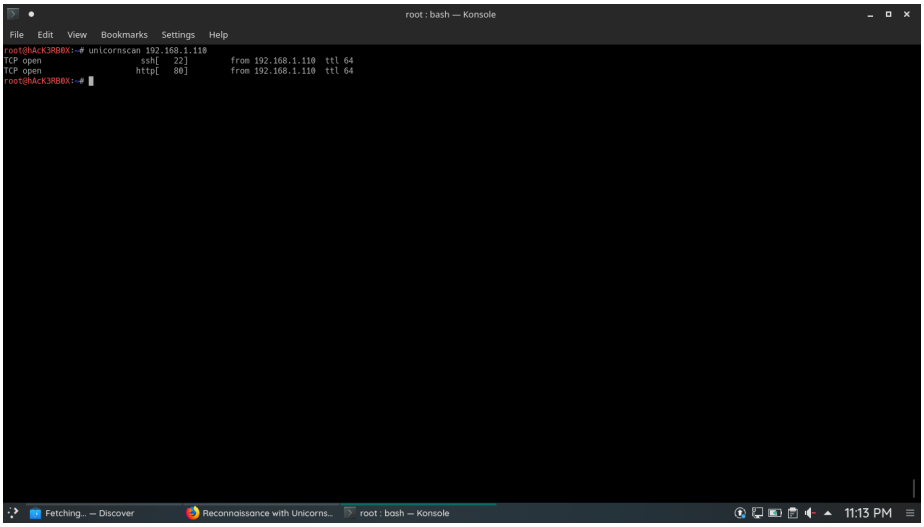

Figure 39: Unicorn Scan

WPScan

WPScan is a vulnerability scanner sponsored by SUCURI used to identify the security-related problems on WordPress website. WPScan is useful if the website is on a private network or Intranet where the Internet is not available. WPScan is basically used to find for known vulnerabilities within the core version, plugins, and themes. It is also used to find out if any weak passwords, users, and security configuration issues are present. The database at wpvulndb.com is used to check for vulnerable software and the WPScan team maintains the ever-growing list of vulnerabilities.

Running the basic command above will perform a quick scan of the website to identify your active theme and basic issues, such as exposed WordPress version numbers.

Checking for Vulnerable Plugins

Adding the *–enumerate vp* argument checks the WordPress website for vulnerable plugins.

If vulnerable plugins are found you will see red exclamation icons and references to further information. Any vulnerable plugin should be replaced and removed if you cannot update it to patch the vulnerability.

Checking User Enumeration

When hackers know your WordPress usernames it becomes easier for them to perform a successful brute force attack. If attackers gain access to one of your users with sufficient permissions, they can gain control of your WordPress installation.

To find out the login names of users on your WordPress website, we will use the argument *–enumerate u* at the end of the command.

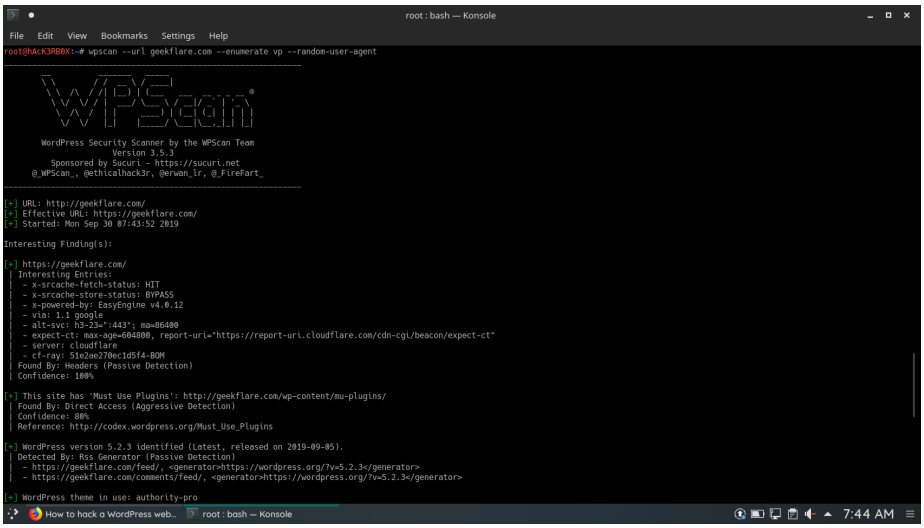

Figure 40: Scanning a Wordpress site for Vulnerability - 1

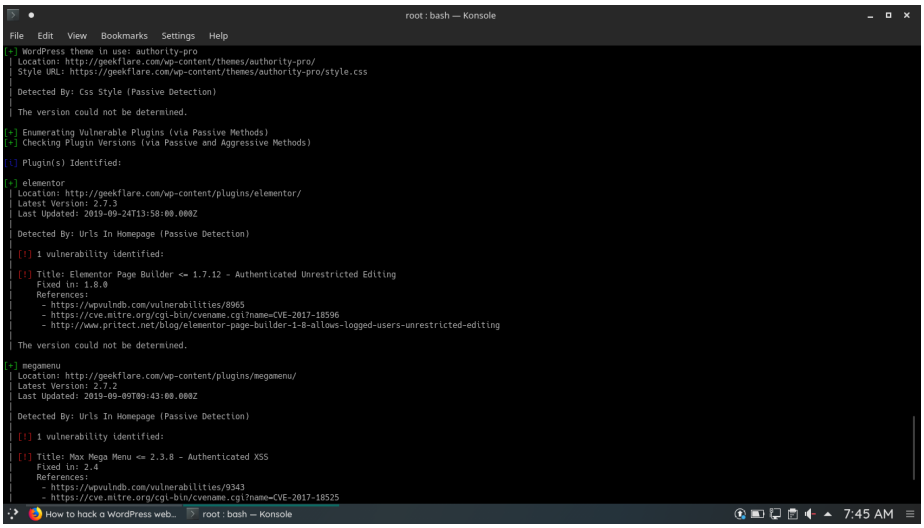

Figure 41: Scanning a Wordpress site for Vulnerability - 2

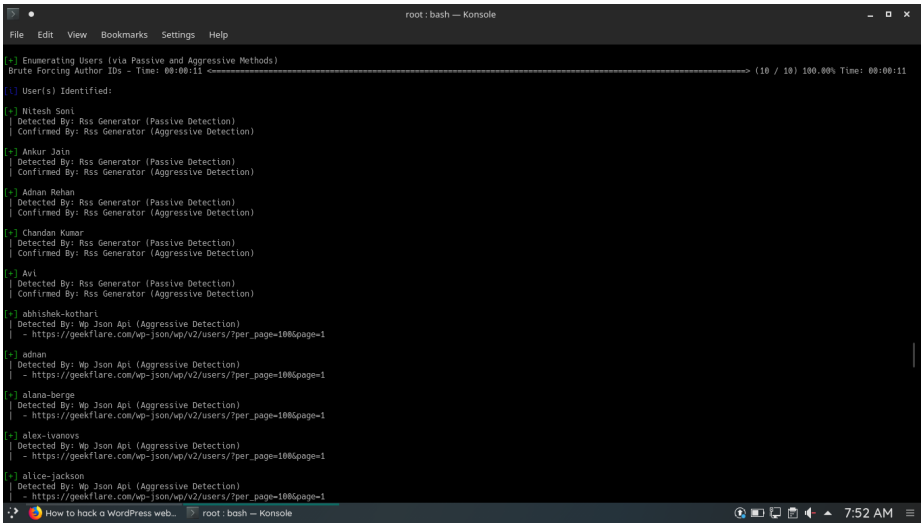

Figure 42: Listing all users from a Particular Wordpress Site

SlowHTTPTest

SlowHTTPTest is a highly configurable tool that simulates some Application Layer Denial of Service attacks by prolonging HTTP connections in different ways.Currently, the supported attacks by the slowhttptest library are:

- Slowloris
- Slow HTTP POST
- Apache Range Header
- Slow Read

Slowloris and Slow HTTP POST DoS attacks rely on the fact that the HTTP protocol, by design, requires requests to be completely received by the server before they are processed. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. If the server keeps too many resources busy, this creates a denial of service. This tool is sending partial HTTP requests, trying to get denial of service from target HTTP server.
Slow Read DoS attack aims the same resources as slowloris and slow POST, but instead of prolonging the request, it sends legitimate HTTP request and reads the response slowly. As you can see, our target is our own website, however even with 100 connections, our server doesn't hang at all because we do have protection against this kind of attacks. The service available will be always YES if the target is reachable. You can test with another computer/network if the website is still up indeed. The generate output in HTML created by our options, will be the following one:

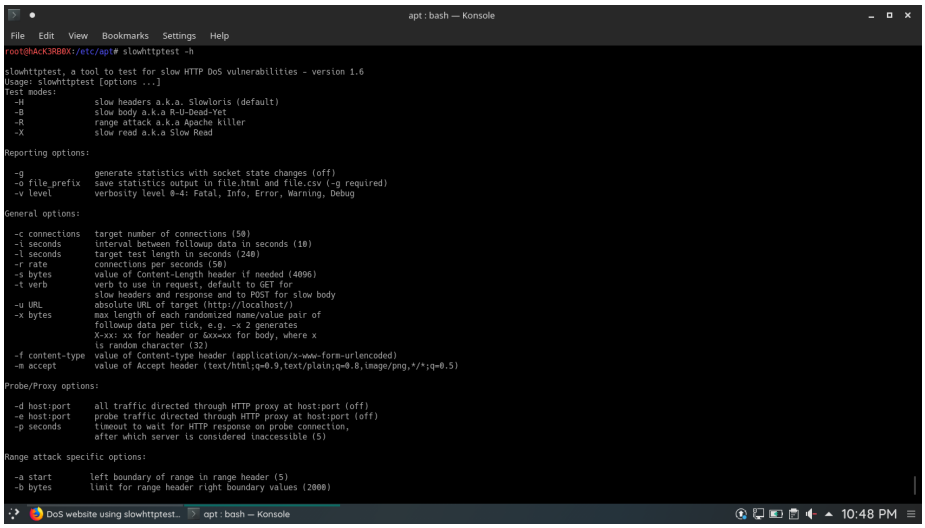

Figure 43: SlowHTTPTest

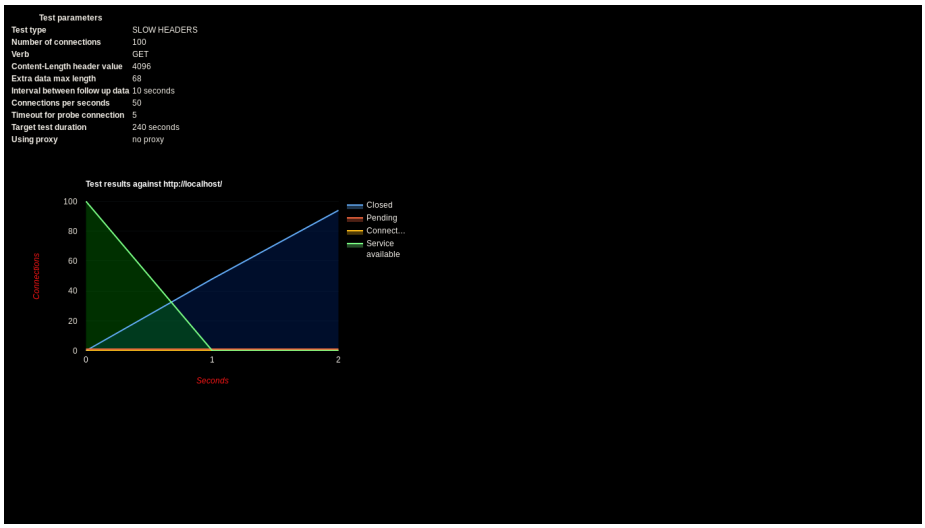

Figure 44: Result Generated after performing a small DOS Attack

Nikto

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 3500 potentially dangerous files/CGIs, versions on over 900 servers, and version specific problems on over 250 servers. Scan items and plugins are frequently updated and can be automatically updated. Nikto is not designed as an overly stealthy tool. It will test a web server in the shortest timespan possible, and it's fairly obvious in log files.

Lengthy Nikto run time

Due to the number of security checks that this tool performs a scan can take 45 mins or even longer, depending on the speed of your web server.

False Positives with Nikto

Nikto does quite well in detecting web server configurations that return HTTP 200 OK on actual "page not found" results. Since Nikto is checking hundreds of URL's for the presence of old scripts, vulnerable applications and other problems. This can sometimes result in many false positives if the detection of the 404 -¿ 200 is not discovered by Nikto. It is not difficult to spot as you will receive a great deal of invalid urls as positives. These are easily checked manually to ensure they are actual false positives.

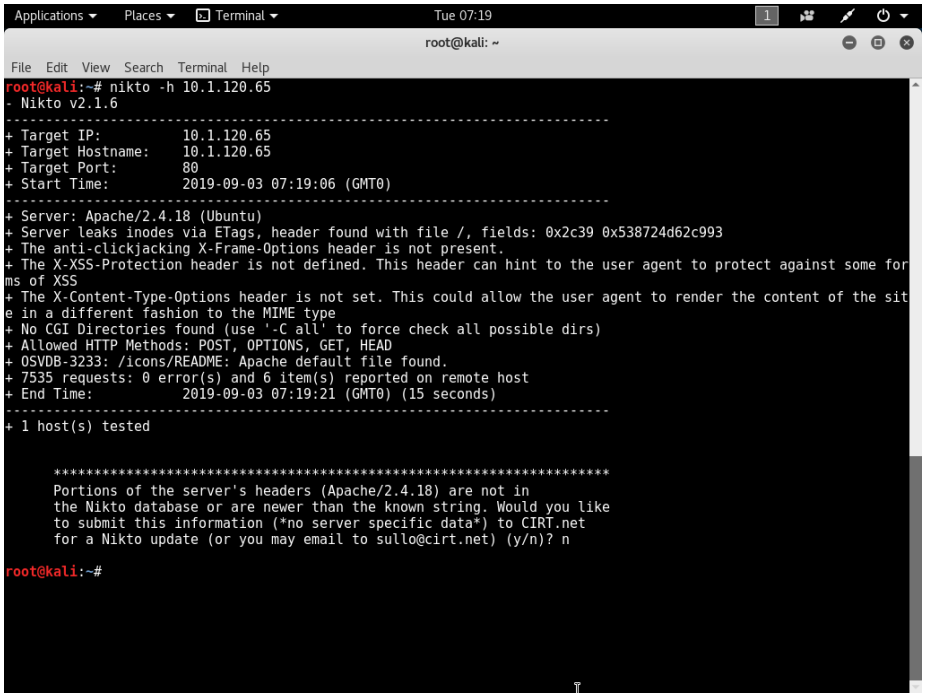

Figure 45: Nikto Sample Scan

Fluxion

Fluxion is a security auditing and social-engineering research tool. It is a remake of linset by vk496 with (hopefully) fewer bugs and more functionality. The script attempts to retrieve the WPA/WPA2 key from a target access point by means of a social engineering (phishing) attack.

Working

- Scan for a target wireless network.
- Launch the Handshake Snooper attack.
- Capture a handshake (necessary for password verification).
- Launch Captive Portal attack.
- Spawns a rogue (fake) AP, imitating the original access point.
- Spawns a DNS server, redirecting all requests to the attacker's host running the captive portal.
- Spawns a web server, serving the captive portal which prompts users for their WPA/WPA2 key.
- Spawns a jammer, deauthenticating all clients from original AP and luring them to the rogue AP.
- All authentication attempts at the captive portal are checked against the handshake file captured earlier.
- The attack will automatically terminate once a correct key has been submitted.
- The key will be logged and clients will be allowed to reconnect to the target access point.

findmyhash

findmyhash is a python script that connects to different online resources to find cracked hashes. It currently supports following hashes:

- MD4
- MD5
- SHA1
- SHA256
- RMD160
- LM
- NTLM
- MYSQL
- CISCO7
- JUNIPER

Syntax
python findmyash.py ¡algorithm¿ [OPTIONS]

Wireshark

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.

Features

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and
- many other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Save packet data captured.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics.

Common Misconceptions of Wireshark

- Wireshark isn't an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.
- Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except domain name resolution, but that can be disabled).

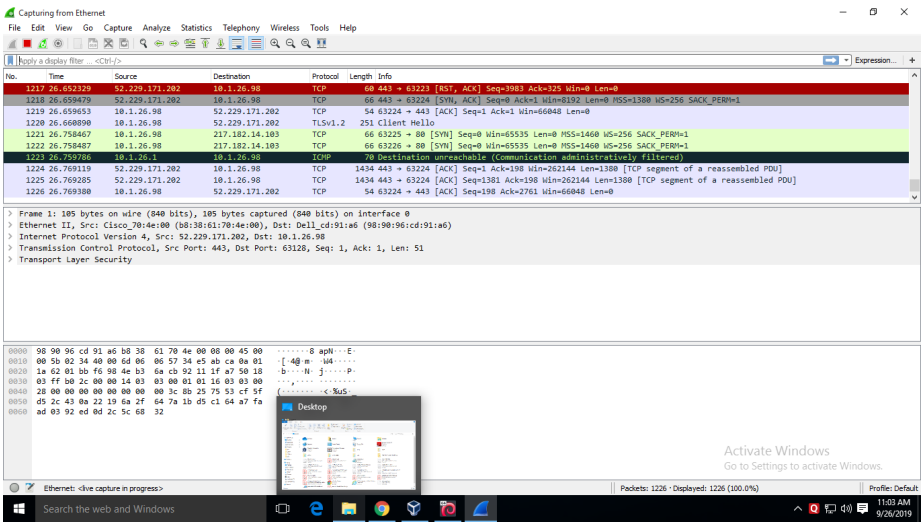

Figure 46: Wireshark Sample Packet Capture

Metasploit Framework

Metasploit offers developers and ethical hackers with a platform which is dedicated to exploit testing. It is a great platform which offers testers a free of cost but a potent way to Pentest systems, websites, and networks. An expert tester can utilize this tool to check for any vulnerabilities and possible loopholes which can be exploited by malicious attackers.
This amazing platform has the ability to highlight such false positive threats and other loopholes, it identifies such threats in no time. The administrator can opt for automatic analysis of threats and vulnerabilities and prioritize the task accordingly. Even there is an option for real-time scanning and testing.

Metasploit Pro Features

- It conducts a thorough test of your web app and provides you with a complete audit report.
- Validate vulnerabilities and bugs found in applications.
- You can measure the possible exposure to phishing attacks as well

BurpSuite

Burp Suite is a Java based Web Penetration Testing framework.Burp Suite helps you identify vulnerabilities and verify attack vectors that are affecting web applications.Burp Suite can be classified as an Interception Proxy. While browsing their target application, a penetration tester can configure their internet browser to route traffic through the Burp Suite proxy server. Burp Suite then acts as a Man In The Middle by capturing and analyzing each request to and from the target web application so that they can be analyzed. Penetration testers can pause, manipulate and replay individual HTTP requests in order to analyze potential parameters or injection points. Injection points can be specified for manual as well as automated fuzzing attacks to discover potentially unintended application behaviors, crashes and error messages.

- **HTTP Proxy** : It operates as a web proxy server, and sits as a man-in-the-middle between the browser and destination web servers. This allows the interception, inspection and modification of the raw traffic passing in both directions.
- **Scanner** : A web application security scanner, used for performing automated vulnerability scans of web applications.
- **Intruder** : This tool can perform automated attacks on web applications. The tool offers a configurable algorithm that can generate malicious HTTP requests.The intruder tool can test and detect SQL injections, cross-site scripting, parameter manipulation and vulnerabilities susceptible to brute-force attacks.
- **Spider** : A tool for automatically crawling web applications. It can be used in conjunction with manual mapping techniques to speed up the process of mapping an application's content and functionality.
- **Repeater** : A simple tool that can be used to manually test an application. It can be used to modify requests to the server, resend them, and observe the results.
- **Decoder** : A tool for transforming encoded data into its canonical form, or for transforming raw data into various encoded and hashed forms. It is capable of intelligently recognizing several encoding formats using heuristic techniques.
- **Comparer** : A tool for performing a comparison (a visual "diff") between any two items of data.
- **Extender** : Allows the security tester to load Burp extensions, to extend Burp's functionality using the security testers own or third-party code (BAppStore)
- **Sequencer** : A tool for analyzing the quality of randomness in a sample of data items. It can be used to test an application's session tokens or

other important data items that are intended to be unpredictable, such as anti-CSRF tokens, password reset tokens, etc.