ASSIGNMENT 2:

KALI LINUX

Saloni Ghule

Website: https://vit.ac.in

1. Information Gathering:

Information gathering, or data collection, is a process where you follow a series of steps to conduct research and answer questions or resolve problems you have. Though information gathering isn't bound by cybersecurity, it is an essential skill to have in the field.

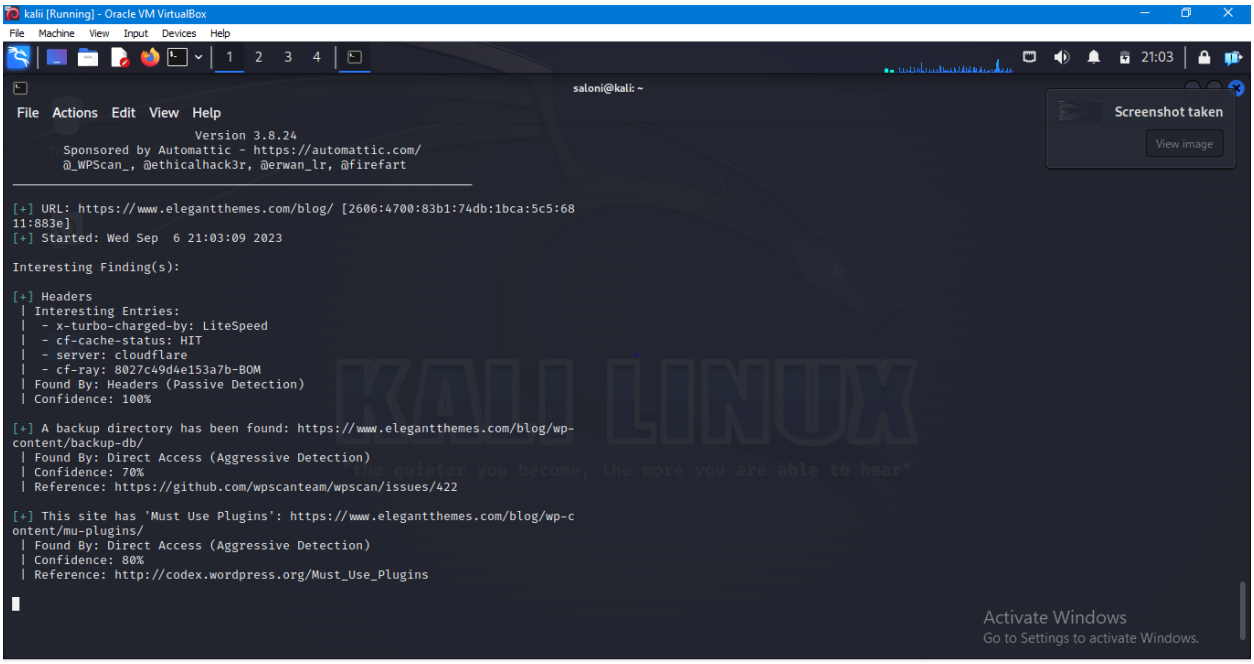
2. Vulnerability Analysis:

A vulnerability assessment is the testing process used to identify and assign severity levels to as many security defects as possible in a given timeframe. This process may involve automated and manual techniques with varying degrees of rigor and an emphasis on comprehensive coverage.

3. Web application analysis:

The process involves an active analysis of the application for any weaknesses, technical flaws, or vulnerabilities. Any security issues that are found will be presented to the system owner, together with an assessment of the impact, a proposal for mitigation or a technical solution.

wpscan



4. Databse assessment :

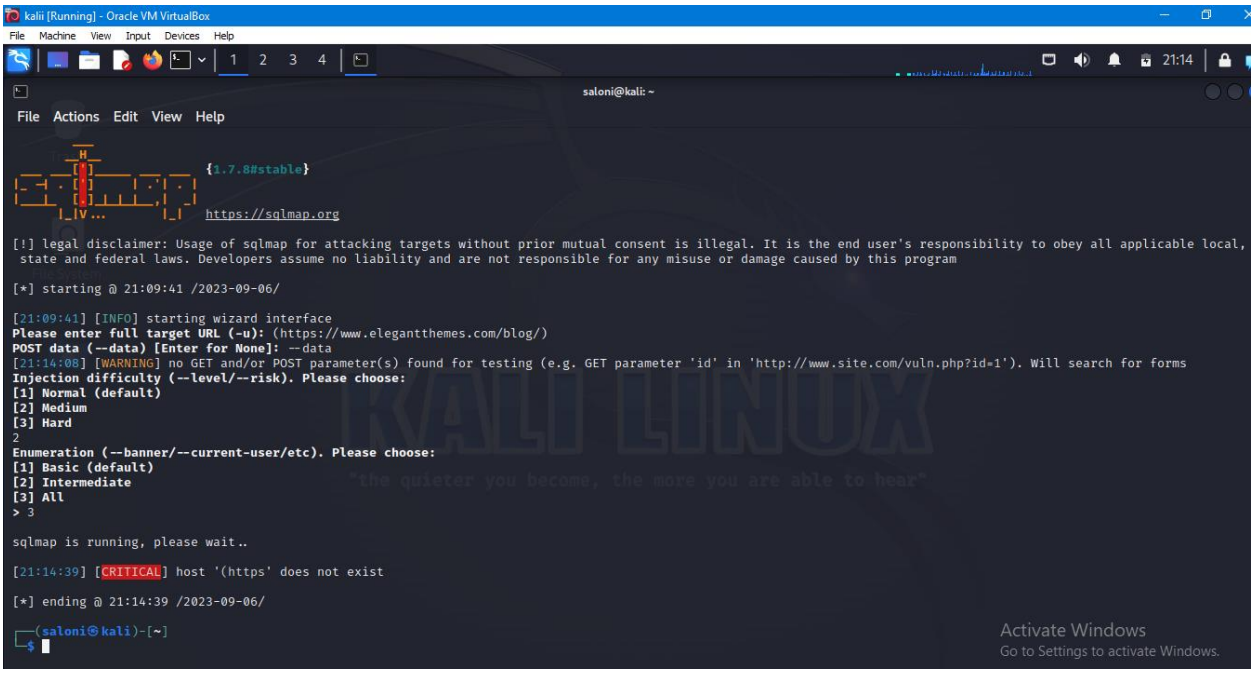
These applications are made to access the database and analyze it for different attacks and security issues. These assessment shows some opportunities for improvement and changes. They develop a report of the analysis done on the database system. They perform:

- Configuration checking
- Examining user account
- Privilege and role grants
- Authorization control
- Key management
- Data encryption

Some of the tools are:

- Bbqsl
- Jsql injection
- Oscanner
- Sqlmap
- Sqlninja
- Tmscmd10g

SQLMAP



5. Password attacks:

These are basically a collection of tools that could handle the wordlist or password list to be checked on any login credentials through different services and protocols. Some tools are wordlist collectors and some of them are the attacker. Some of the tools are:

- Cewl
- Crunch
- Hashcat
- John
- Johnny
- Medusa
- Ncrack

6. Wireless attacks:

These tools are wireless security crackers, like breaking wifi – routers, working and manipulating access points. Wireless attacks are not limited to password cracking these are also used in information gathering and knowing behavior of victims over the internet. For example, the Victim is connected to a compromised access point or a fake access point then it can be used as a Man-in-The-Middle attack. Some of the tools are:

- Aircrack-ng
- Fern- wifi –cracker
- Kismet
- Ghost Phisher
- Wifite

7. Reverse Engineering:

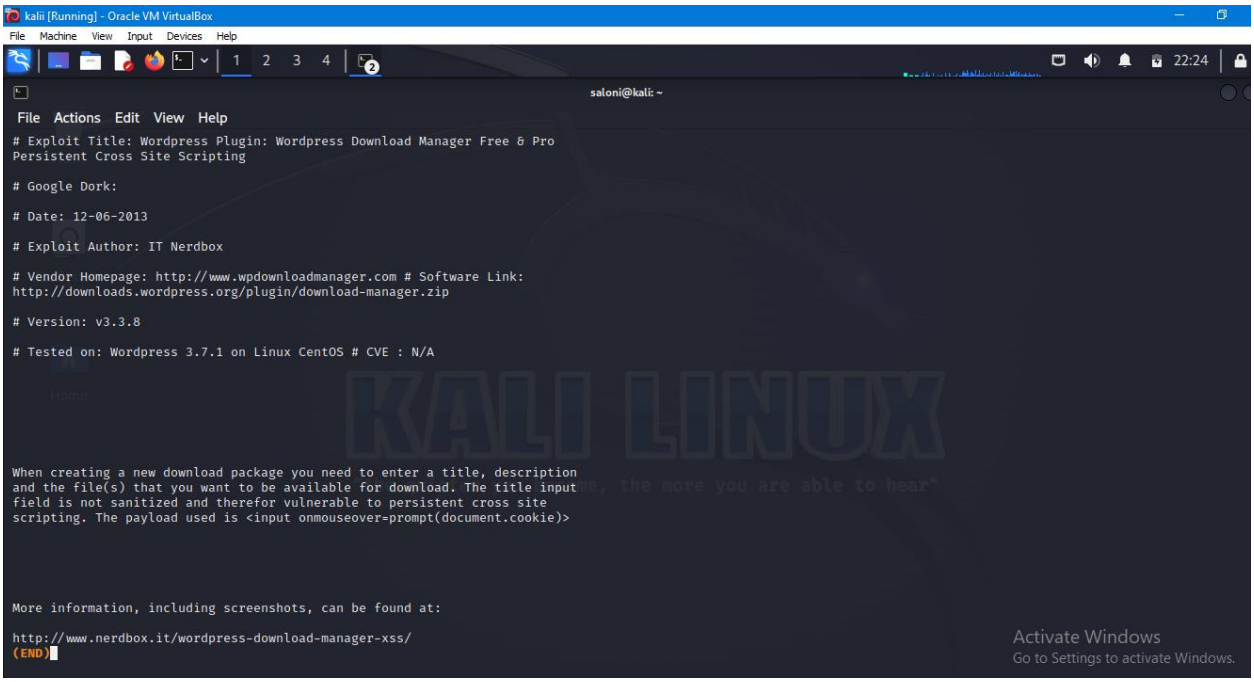
Reverse Engineering is to break down the layers of the applications or software. This is used in creating cracks and patches for different software and services. These tools reach the source code of the application, understand its working and manipulate according to needs. For example, Reverse engineering tools are also used by High-End companies to know the logic and idea behind the software. Some of the tools are:

- Apktools
- Ollydbg
- Flasm
- nasm shell

8. Exploitation Tools:

These tools are used to exploit different systems like personal computers and mobile phones. These tools can generate payloads for the vulnerable system and through those payloads information from the devices can be exploited. For example, the Victim's system is compromised using payloads over internet or installing it if physically accessible. Some of the tools are:

- Armitage
- Metasploit
- Searchsploit
- Beef xss framework
- termineter
- Social engineering toolkit(root)



9. Sniffing and Spoofing:

Secretly accessing any unauthorized data over network is sniffing. Hiding real identity and creating fake identity and use it for any illegal or unauthorized work is spoofing. IP spoofing and MAC spoofing are two famous and mostly used attacks. Some of the tools are:

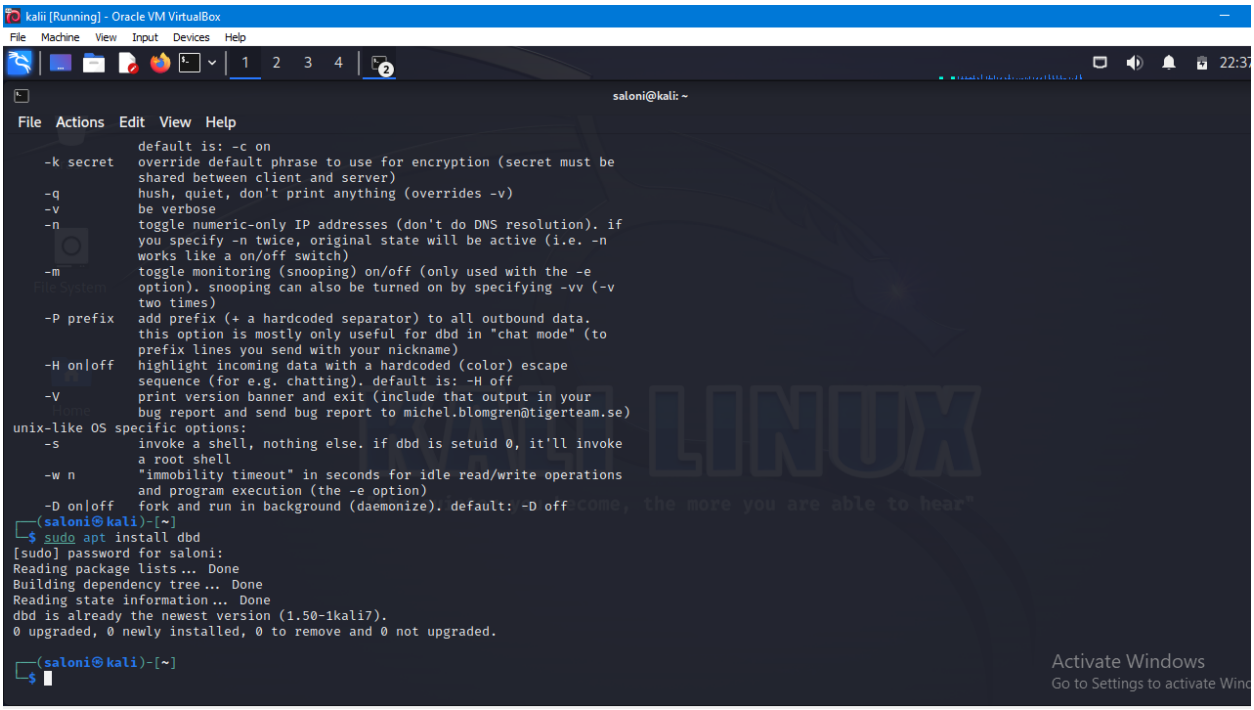
10. Wireshark
11. Bettercap
12. Ettercap
13. Hamster
14. Driftnet
15. responder
16. macchanger

10. Post Exploitation:

These tools use back doors to get back to the vulnerable system i.e. to maintain access to the machine. As the name suggests these are useful or mostly used after an attack has previously been made on the victim's machine. For example, After an attack victim removed the vulnerability from the system, in this situation if attacker wants to access data again, then these tools are helpful. Some of the tools are:

- MSF
- Veil –Pillage framework

- Powersploit
- Powershell empire



11. Forensics:

These tools are used by forensic specialist to recover information from any system or storage devices. This helps in collecting information during evidence searching for any cybercrime. Some of the tools are:

- Autopsy
- Binwalk
- Galleta
- Hashdeep
- Volafox
- Volatility

12 Reporting Tools:

After all the assessment and vulnerability testing analysts have to report all those to the client in an organised and authenticated way. These tools develop statistics and information to help in analysing. Some of the tools are:

- Dradis
- Faraday IDE
- Pipal
- Magictree
- metagoofil

13. Social Engineering:

As the name suggests these tools generate similar services that people use in daily life and extract personal information using those fake services. These tools use and manipulate human behavior for information gathering. For example, Phishing is one of the example of social engineering, in this, a similar looking home page of any social platform is created and then login details are compromised. Some of the tools are:

- SET
- Backdoor-f
- U3-pwn
- Ghost Phisher
- msf payload creator
- SET(social engineering toolkit

```
File  Machine  View  Input  Devices  Help
1  2  3  4                                                    22:54
Shell No. 1
File  Actions  Edit  View  Help

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                     Version: 8.0.3
                  Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

Activate Windows
Go to Settings to activate Windows.
```

```
File  Machine  View  Input  Devices  Help
1  2  3  4
Shell No. 1
File  Actions  Edit  View  Help

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

 Unable to check for new version of SET (is your network up?)

 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

 set> 10


  [-] Social-Engineer Toolkit Third Party Modules menu.
  [-] Please read the readme/modules.txt for information on how to create your own modules.

  1. RATTE Java Applet Attack (Remote Administration Tool Tommy Edition) - Read the readme/RATTE_README.txt first
  2. Google Analytics Attack by @ZonkSec
  3. RATTE (Remote Administration Tool Tommy Edition) Create Payload only. Read the readme/RATTE-Readme.txt first
```

```
  99) Return back to the main menu.

set> 10


  [-] Social-Engineer Toolkit Third Party Modules menu.
  [-] Please read the readme/modules.txt for information on how to create your own modules.

  1. RATTE Java Applet Attack (Remote Administration Tool Tommy Edition) - Read the readme/RATTE_README.txt first
  2. Google Analytics Attack by @ZonkSec
  3. RATTE (Remote Administration Tool Tommy Edition) Create Payload only. Read the readme/RATTE-Readme.txt first

  99. Return to the previous menu

set:modules>2
Loading module. Please wait ...
_______________________________
     Google Analytics Attack
    By Tyler Rosonke (@ZonkSec)
_______________________________

User-Guide: http://www.zonksec.com/blog/social-engineering-google-analytics/

References:
-https://developers.google.com/analytics/devguides/collection/protocol/v1/reference
-https://developers.google.com/analytics/devguides/collection/protocol/v1/parameters


[*] Choose mode (automatic/manual): manual

[*] Entering manual mode.

[*] Enter TrackingID (tid)(UA-XXXXX):
```