

ASSIGNMENT 2:

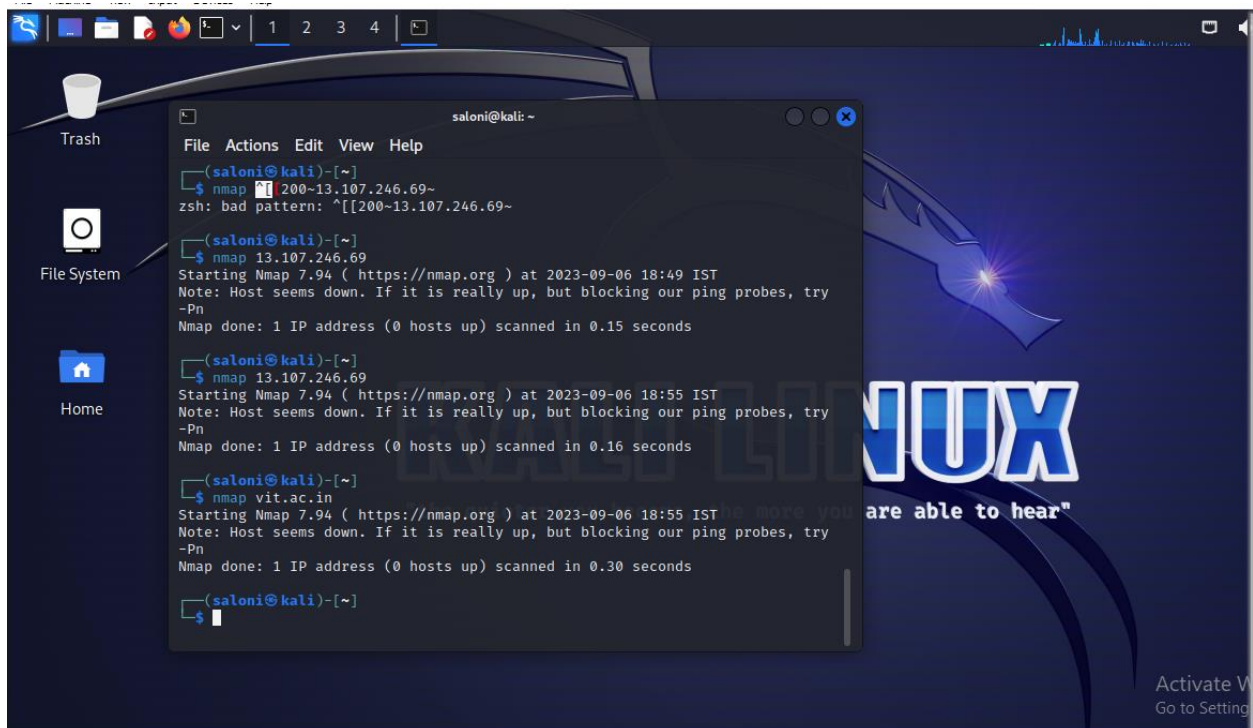
KALI LINUX

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.

```

kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

saloni@kali: ~
File Actions Edit View Help

Version 3.8.24
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: https://www.elegantthemes.com/blog/ [2606:4700:83b1:74db:1bca:5c5:68
11:883e]
[+] Started: Wed Sep 6 21:03:09 2023

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - x-turbo-charged-by: LiteSpeed
| - cf-cache-status: HIT
| - server: cloudflare
| - cf-ray: 8027c49d4e153a7b-BOM
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] A backup directory has been found: https://www.elegantthemes.com/blog/wp-
content/backup-db/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 70%
| Reference: https://github.com/wpscanteam/wpscan/issues/422

[+] This site has 'Must Use Plugins': https://www.elegantthemes.com/blog/wp-c
ontent/mu-plugins/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 80%
| Reference: http://codex.wordpress.org/Must_Use_Plugins

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

4. Database assessment :

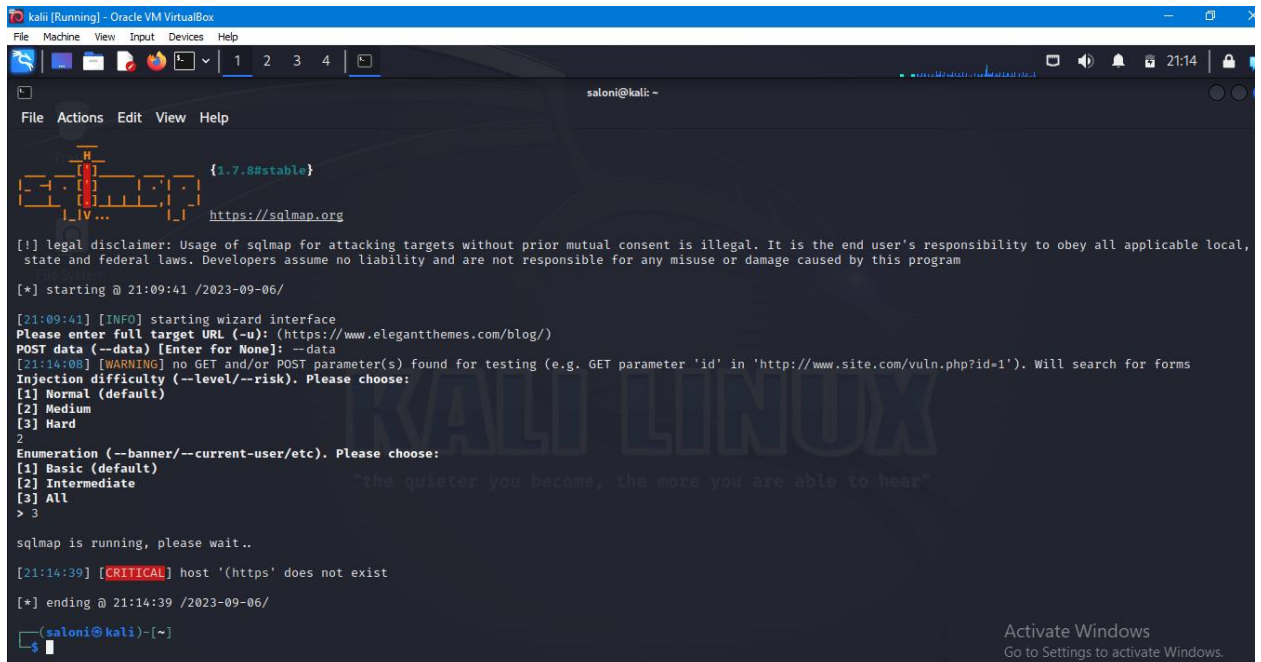
These applications are made to access the database and analyze it for different attacks and security issues. These assessment shows some opportunities for improvement and changes. They develop a report of the analysis done on the database system. They perform:

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

Some of the tools are:

- Bbqsl
- Jsqli injection
- Oscanner
- Sqlmap
- Sqlninja
- Tmscmd10g

SQLMAP



```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

saloni@kali: ~
File Actions Edit View Help

[1] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 21:09:41 /2023-09-06/

[21:09:41] [INFO] starting wizard interface
Please enter full target URL (-u): (https://www.elegantthemes.com/blog/)
POST data (--data) [Enter for None]: --data
[21:14:08] [WARNING] no GET and/or POST parameter(s) found for testing (e.g. GET parameter 'id' in 'http://www.site.com/vuln.php?id=1'). Will search for forms
Injection difficulty (--level/--risk). Please choose:
[1] Normal (default)
[2] Medium
[3] Hard
2
Enumeration (--banner/--current-user/etc). Please choose:
[1] Basic (default)
[2] Intermediate
[3] All
> 3

sqlmap is running, please wait..

[21:14:39] [CRITICAL] host '(https' does not exist

[*] ending @ 21:14:39 /2023-09-06/

saloni@kali)~$
```

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:

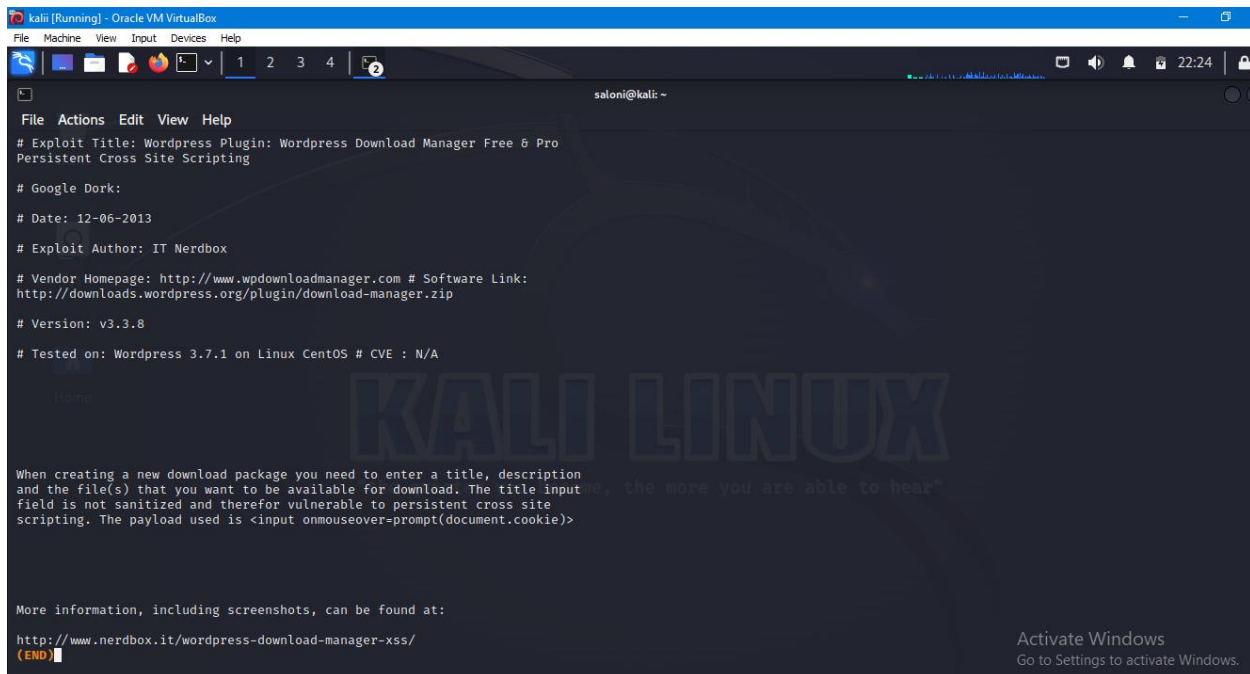
Reverse Engineering is to break down the layers of the applications or software. This is used in creating cracks and patches for different software and services. These tools reach the source code of the application, understand its working and manipulate according to needs. For example, Reverse engineering 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
- terminator
- Social engineering toolkit(root)



```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 5
saloni@kali: ~
File Actions Edit View Help
# Exploit Title: Wordpress Plugin: Wordpress Download Manager Free & Pro
Persistent Cross Site Scripting
# Google Dork:
# Date: 12-06-2013
# Exploit Author: IT Nerdbox
# Vendor Homepage: http://www.wpdowndownmanager.com # Software Link:
http://downloads.wordpress.org/plugin/download-manager.zip
# Version: v3.3.8
# Tested on: Wordpress 3.7.1 on Linux CentOS # CVE : N/A

When creating a new download package you need to enter a title, description
and the file(s) that you want to be available for download. The title input
field is not sanitized and therefor vulnerable to persistent cross site
scripting. The payload used is <input onmouseover=prompt(document.cookie)>

More information, including screenshots, can be found at:
http://www.nerdbox.it/wordpress-download-manager-xss/
(END)
```

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

```

kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
saloni@kali: ~
File Actions Edit View Help
-k secret default is: -c on
override default phrase to use for encryption (secret must be
shared between client and server)
-q hush, quiet, don't print anything (overrides -v)
-v be verbose
-n toggle numeric-only IP addresses (don't do DNS resolution). if
you specify -n twice, original state will be active (i.e. -n
works like a on/off switch)
-m toggle monitoring (snooping) on/off (only used with the -e
option). snooping can also be turned on by specifying -vv (-v
two times)
-P prefix add prefix (+ a hardcoded separator) to all outbound data.
this option is mostly only useful for dbd in "chat mode" (to
prefix lines you send with your nickname)
-H onloff highlight incoming data with a hardcoded (color) escape
sequence (for e.g. chatting). default is: -H off
-V print version banner and exit (include that output in your
bug report and send bug report to michel.blomgren@tigerteam.se)
unix-like OS specific options:
-s invoke a shell, nothing else. if dbd is setuid 0, it'll invoke
a root shell
-w n "immobility timeout" in seconds for idle read/write operations
and program execution (the -e option)
-D onloff fork and run in background (daemonize). default: -D off
(saloni@kali)-[~]
$ sudo apt install dbd
[sudo] password for saloni:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
dbd is already the newest version (1.50-1kali7).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
(saloni@kali)-[~]
$

```

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
- Volafax
- 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 5
Shell No. 1
File Actions Edit View Help

0101100101101111011101010010000001100
100110010101100001011010001011000111
1001001000000110100001100001011011001
100101001000000110100010111100100000
011011011110101011000101101000001000
00011101000101001011010101100100010
000001101111011011000100000011100101
101111011010101100100010000001101000
01100001011011001001000111001001000
00001101000101101001001001000000101
010001101000011000010110110011010101
1100110010000001100110011110110010
0010000001110101011001010100101011
100110011001000000111010001010000110
01010010000010100101101110110001101
10100101100001011011000010110101000101
011011001100110110100010110110011001
010110010101110010001000000101000110
11110110111011010001010110110100101
110100001000000010100110100001110101
01100110111001100101010

[---] The Social-Engineer Toolkit (SET) the quieter you become, the more you are able to hear
[---] 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 5
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

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
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/ "the more you are able to hear"
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-XXXX):
```

Activate Windows
Go to Settings to activate Windows.