

NAME-ANMOL KANT

NOW WE TALK ABOUT HACKING TOOLS OF KALI LINUX

1) INFORMATION GATHERING (IG)

LET'S FIRST TALK ABOUT WHAT IS THIS BASICALLY A PROCESS FOLLOWED BY EVERY HACKER BEFORE THEY HACK THE SYSTEM SUPPOSE THEY WANT TO HACK A SERVER FOR THAT THEY WANT TO FIND INFORMATION ABOUT THAT SERVER LIKE IP, MAC ADDRESS WHICH PORTS ARE OPEN STUFF AFTER THAT YOU KIND OF HACK THE SERVER OR FOR ANYTHING YOU WANT TO HACK YOU NEED INFORMATION THAT STUFF SO ITS EASY FOR YOU TO EXPLOIT THEIR VULNERABILITIES. IG IS THE FIRST PHASE OF ETHICAL HACKING. WE GATHER INFORMATION ABOUT THE HOST, SERVER, CLIENT, TARGETED SYSTEM ETC.

TWO TYPES OF INFORMATION GATHERING

- 1) ACTIVE INFORMATION GATHERING
- 2) PASSIVE INFORMATION GATHERING

2) WHATEVER INFORMATION IS PUBLICALLY AVAILABLE WE COLLECT THIS INFORMATION WITH THE HELP OF SOME TOOLS. EXAMPLE OF TOOLS IS **MALTEGO** IT DID NOT HARM THE PRIVACY OF ANYONE AND YOU GATHER THE INFORMATION.

1) THINGS THAT ARE NOT PUBLICALLY AVAILABLE LIKE PORTS WHEN I SCAN YOUR SYSTEM THEN I KNOW HOW MANY PORTS ARE OPEN YOU HAVE A BIG SERVER YOU ARE WORKING ON WHICH IS AN IP-LIKE KIND OF STUFF. WE FIND OUT THESE THINGS USING TOOLS.

SO NOW WE SEE SOME TOOLS IT'S VERY DIFFICULT TO TALK ABOUT EVERY TOOL BUT AT LEAST WE SAW MORE THAN TWO OR THREE TOOLS WE NOW ALL TOOLS WORK FOR THE SAME THING WHICH IS IG.

1) Nmap

It is a kind of tool that finds out ports from your website and server what your machine version which port is open or closed. Nmap is used for port scanning.

```
nmap -sV -O --script vuln
```

If we want to know more tools and how they work, we simply click on them and see how they work what is their script and all things. We use sudo word for putting any tool information.

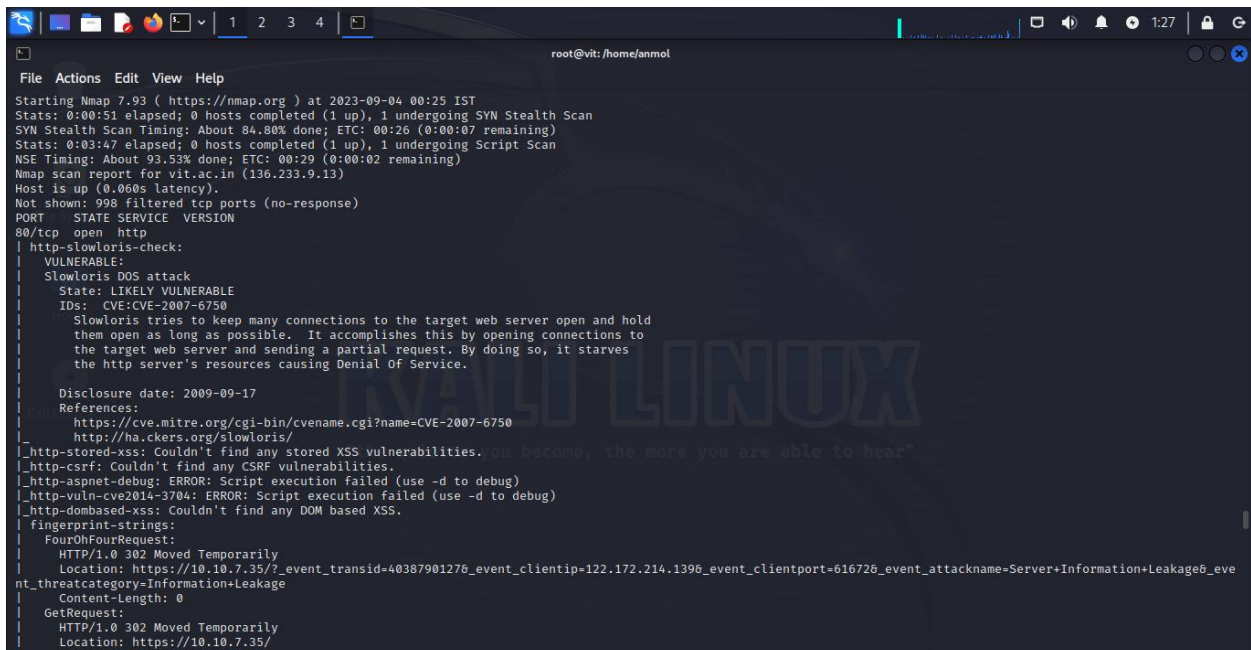
Sudo -i used it to open the Kali terminal's root server.

We also used a harvester to find IP, email, host, etc.

We use netdiscover,autopasswd, and spider foot which type of tools for information gathering.

2) VULNERABILITY ANALYSIS

We gather information about a particular server and domain(website) after that we find the vulnerability of the following server or domain so that we exploit the vulnerability to enter the system. For this, we used nmap previously that is `nmap -sV -O -script -vuln` and we found vuln but we now see some other tools to find vuln so that attackers take advantage of these loopholes.



```
File Actions Edit View Help
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-04 00:25 IST
Stats: 0:00:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.80% done; ETC: 00:26 (0:00:07 remaining)
Stats: 0:03:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.53% done; ETC: 00:29 (0:00:02 remaining)
Nmap scan report for vitae.in (136.233.9.13)
Host is up (0.060s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http
| http-slowloris-check:
|   VULNERABLE:
|     Slowloris DOS attack
|       State: LIKELY VULNERABLE
|       IDs: CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible. It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|       http://hackers.org/slowloris/
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_ http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 302 Moved Temporarily
|     Location: https://10.10.7.35/?_event_transid=40387901276_event_clientip=122.172.214.1396_event_clientport=616726_event_attackname=Server+Information+Leakage6_eve
|_ nt_threatcategory=Information+Leakage
|   Content-Length: 0
|_ GetRequest:
|     HTTP/1.0 302 Moved Temporarily
|     Location: https://10.10.7.35/
```

3) Web application analysis

The collection of web pages is called a website. the web application is considered a website. So basically what we do here we find the vulnerability in the website or web application.

We see some tools regarding this. many websites are built on different languages like php, python, java,jascript,wordpress, etc.

We see some tools like wpscan and sqlmap for web application analysis.

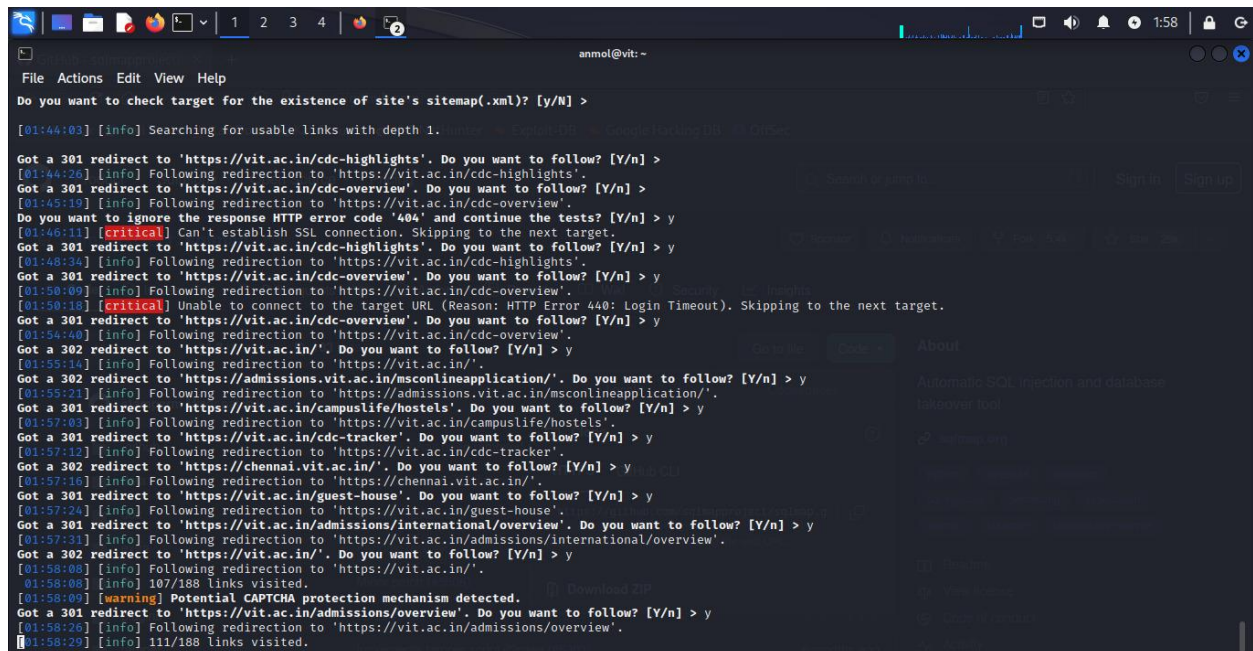
We all say that we can hack the website through wpscan.

By using wpscan we just use any domain or IP to scan and basically, if it is not working then we use wpscan - - url - - force to know about vulnerabilities.

I am using sqlmap tools to find the vuln on the website. (ls=list)

Zap is also a web application tool for finding vuln, for using zap tool Your website not be a php,html,wppress, or CSS.you use every website except this programming language. website. It basically attacks or scans using a URL

Only the WPscan-made website used the wpscan we see tomorrow



```
anmol@vit: ~  
File Actions Edit View Help  
Do you want to check target for the existence of site's sitemap(.xml)? [y/N] >  
[01:44:03] [info] Searching for usable links with depth 1.  
Got a 301 redirect to 'https://vit.ac.in/cdc-highlights'. Do you want to follow? [Y/n] > y  
[01:44:26] [info] Following redirection to 'https://vit.ac.in/cdc-highlights'.  
Got a 301 redirect to 'https://vit.ac.in/cdc-overview'. Do you want to follow? [Y/n] > y  
[01:45:19] [info] Following redirection to 'https://vit.ac.in/cdc-overview'.  
Do you want to ignore the response HTTP error code '404' and continue the tests? [Y/n] > y  
[01:46:11] [critical] Can't establish SSL connection. Skipping to the next target.  
Got a 301 redirect to 'https://vit.ac.in/cdc-highlights'. Do you want to follow? [Y/n] > y  
[01:48:34] [info] Following redirection to 'https://vit.ac.in/cdc-highlights'.  
Got a 301 redirect to 'https://vit.ac.in/cdc-overview'. Do you want to follow? [Y/n] > y  
[01:50:09] [info] Following redirection to 'https://vit.ac.in/cdc-overview'.  
[01:50:18] [critical] Unable to connect to the target URL (Reason: HTTP Error 440: Login Timeout). Skipping to the next target.  
Got a 301 redirect to 'https://vit.ac.in/cdc-overview'. Do you want to follow? [Y/n] > y  
[01:54:40] [info] Following redirection to 'https://vit.ac.in/cdc-overview'.  
Got a 302 redirect to 'https://vit.ac.in/'. Do you want to follow? [Y/n] > y  
[01:55:14] [info] Following redirection to 'https://vit.ac.in/'.  
Got a 302 redirect to 'https://admissions.vit.ac.in/msconlineapplication/'. Do you want to follow? [Y/n] > y  
[01:55:21] [info] Following redirection to 'https://admissions.vit.ac.in/msconlineapplication/'.  
Got a 301 redirect to 'https://vit.ac.in/campuslife/hostels'. Do you want to follow? [Y/n] > y  
[01:57:03] [info] Following redirection to 'https://vit.ac.in/campuslife/hostels'.  
Got a 301 redirect to 'https://vit.ac.in/cdc-tracker'. Do you want to follow? [Y/n] > y  
[01:57:12] [info] Following redirection to 'https://vit.ac.in/cdc-tracker'.  
Got a 302 redirect to 'https://chennai.vit.ac.in/'. Do you want to follow? [Y/n] > y  
[01:57:16] [info] Following redirection to 'https://chennai.vit.ac.in/'.  
Got a 301 redirect to 'https://vit.ac.in/guest-house'. Do you want to follow? [Y/n] > y  
[01:57:24] [info] Following redirection to 'https://vit.ac.in/guest-house'.  
Got a 301 redirect to 'https://vit.ac.in/admissions/international/overview'. Do you want to follow? [Y/n] > y  
[01:57:31] [info] Following redirection to 'https://vit.ac.in/admissions/international/overview'.  
Got a 302 redirect to 'https://vit.ac.in/'. Do you want to follow? [Y/n] > y  
[01:58:08] [info] Following redirection to 'https://vit.ac.in/'.  
[01:58:08] [info] 107/188 links visited.  
[01:58:08] [warning] Potential CAPTCHA protection mechanism detected.  
Got a 301 redirect to 'https://vit.ac.in/admissions/overview'. Do you want to follow? [Y/n] > y  
[01:58:26] [info] Following redirection to 'https://vit.ac.in/admissions/overview'.  
[01:58:29] [info] 111/188 links visited.
```

4) Password attack

In Hydra, two things are CLI with terminal and GUI with graphical.

We see two tools one for online and another for offline attacks.

The online attack is hydra => `hydra ssh://ip:port num -L`

HOW WE WRITE = `hydra [some command line option] protocol://target:port/module-options.`

Syntax breakdown-

`hydra ftp://192.63.12.0:2221 -l admin -p list.txt`

Which protocol do we want to use

1)FTP

2)MySQL

3)ssh

4)any login form we want to do brute force.

generate target-based Wordlists / Password List in Kali Linux

If you want to download a tool then you simply copy the link to your gp terminal and type `cd desktop` then `git clone` then `cd/filename` that is `cupp` (`cd cupp/` then `ls`). If you want to see any time on the terminal then simply type `./cupp.py`

First, we made a txt file or we say password directory.

Leet mode = when people use numbers between words for example `t3ch=tech`.

leet in number is 1337.

`-t=` how many connections we send per time in my case that is 2 because the firewall detects them and blocks our IP if we succeed more than 4. If you do not do it send 16 per time. If the firewall is there then it a chance you will be blocked.

The main syntax is this

`Hydra ssh://192.168.0.104:2222 -L /home/anmol/temp/word.txt -P /home/anmol/temp/word.txt -v -f -t 2`

So we made a password list with Cupp.

Now we use crunch to make some more password lists.

We just type `crunch 3 4 123456789 -o roman.txt`

Hydra is used for proxy brute forcing.

