

PROJECT- 1_ SYSTEM HACKING

Name: Anuraag Maity

E mail: anuragmaity16@gmail.com

Contents

PASSWORD ATTACK	1
i. ABSTRACT.....	1
ii. OBJECTIVE	1
iii. INTRODUCTION.....	2
iv. METHODOLOGY	2
v. SCREENSHOT OF PASSWORD ATTACK	3
vi. CONCLUSION.....	5

PASSWORD ATTACK

i. ABSTRACT

This report offers a comprehensive exploration of tools and techniques used in ethical hacking, specifically focusing on system security assessment. It provides insights into five critical components: Hydra for password attacks, auxiliary modules in Metasploit, NSE Scripts in Nmap, John the Ripper for password cracking, and password generation using Crunch.

This report provides a comprehensive exploration of password attacks, a pervasive threat in the realm of cybersecurity. It investigates five key elements central to the art of password manipulation: Hydra, Auxiliary Modules, NSE Scripts, John the Ripper, and password generation using Crunch. Each element is meticulously examined for its role in identifying weak access points, assessing network vulnerabilities, and enhancing password security. By shedding light on the tactics and tools employed in password attacks, this report equips readers with valuable insights into defending against one of the most common and potentially devastating cyber threats.

ii. OBJECTIVE

- a. **Explaining Tools and Techniques:** We want to help people understand important tools and techniques used in ethical hacking, like Hydra, auxiliary modules, NSE Scripts, John the Ripper, and Crunch, in simple terms.
- b. **Ethical and Legal Use:** We want to stress the importance of using these tools and techniques responsibly and legally. We aim to make readers aware of ethical and legal considerations when using them.
- c. **Understanding Techniques:** Make it easy for readers to understand how ethical hackers use these tools to check if a computer system is secure.

iii. INTRODUCTION

This report seeks to the world of ethical hacking, offering a comprehensive introduction to the tools and techniques used in the field of system security assessment. By shedding light on these essential components, we aim to empower individuals and organizations to enhance their cybersecurity.

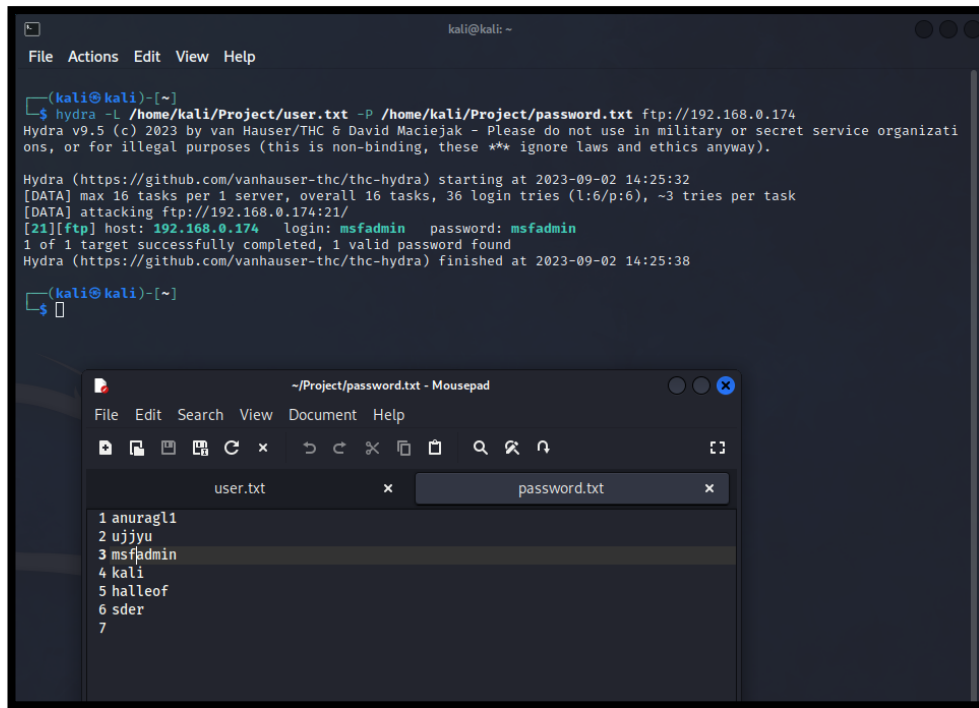
Throughout this report, we will explore five pivotal elements of ethical hacking:

- a. **Hydra:** A versatile password-cracking tool that assists in identifying weak points in access control systems.
- b. **Auxiliary Modules:** Part of the Metasploit framework, these modules play a crucial role in assessing network vulnerabilities and gathering essential information.
- c. **NSE Scripts:** Nmap Scripting Engine scripts enable targeted and thorough network scanning, aiding in the discovery of potential security flaws.
- d. **John the Ripper:** A potent password-cracking utility known for its ability to decipher password hashes and evaluate password strength.
- e. **Password Generation Using Crunch:** A tool for creating customized wordlists and generating secure passwords, a cornerstone in bolstering digital defences.

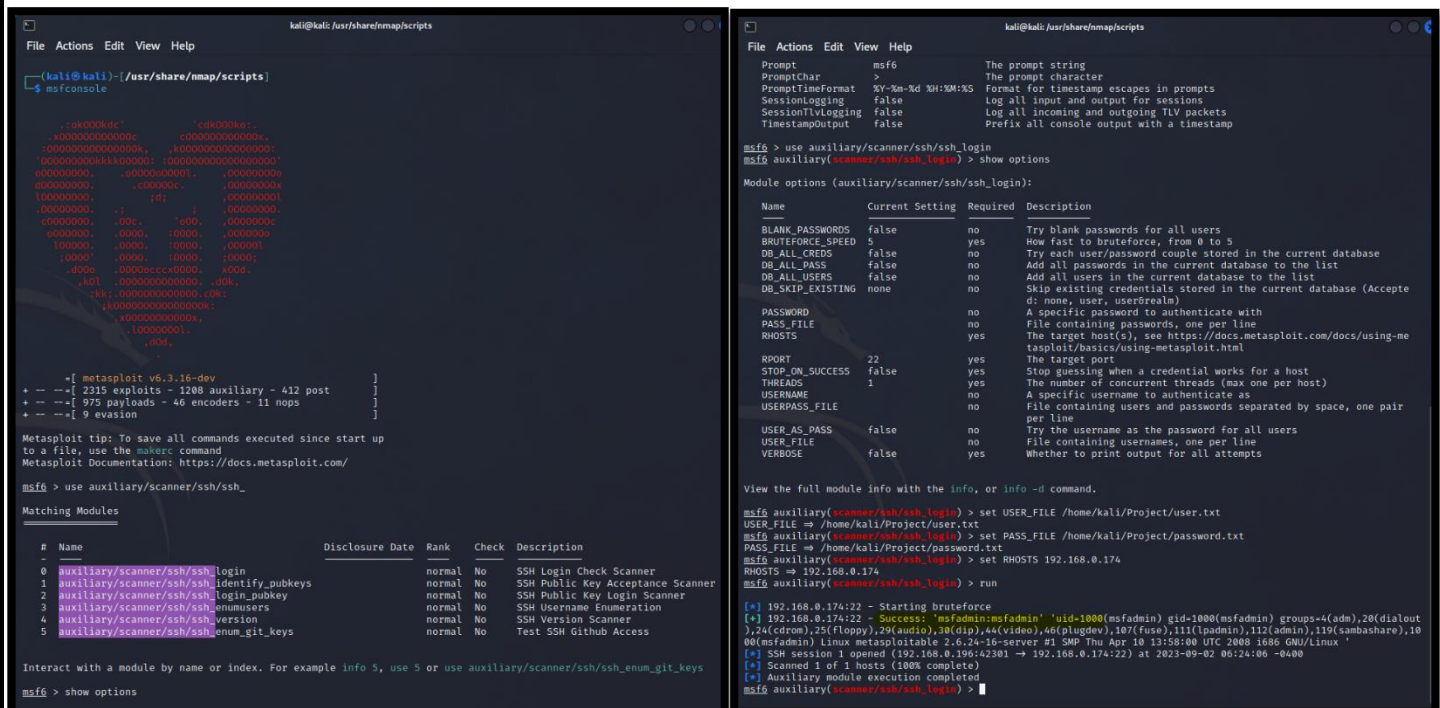
iv. METHODOLOGY

- a. Password attacks are a significant concern, as they can compromise sensitive data and systems. To mitigate such risks, it is crucial to understand the methodologies employed by attackers. The methodology for password attacks typically involves several stages.
- b. Password List Creation: Attackers compile a list of potential passwords that the target might use. This list can be generated using common password dictionaries, brute-force techniques, or by analysing the target's online presence for clues like pet names, birthdays, or favourite sports teams.
- c. Password Cracking: Attackers utilize various password cracking techniques to guess the correct password.

v. SCREENSHOT OF PASSWORD ATTACK



Task 1: Hydra Tool



Task 2: Auxiliary Modules Using Metasploit

```
kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help
ip-geolocation-geoplugin.nse

(kali@kali)-[/usr/share/nmap/scripts]
$ ls -l |grep ssh
-rw-r--r-- 1 root root 5391 Mar 28 05:20 ssh2-enum-algos.nse
-rw-r--r-- 1 root root 1200 Mar 28 05:20 ssh-auth-methods.nse
-rw-r--r-- 1 root root 3045 Mar 28 05:20 ssh-brute.nse
-rw-r--r-- 1 root root 16036 Mar 28 05:20 ssh-hostkey.nse
-rw-r--r-- 1 root root 5948 Mar 28 05:20 ssh-publickey-acceptance.nse
-rw-r--r-- 1 root root 3781 Mar 28 05:20 ssh-run.nse
-rw-r--r-- 1 root root 1423 Mar 28 05:20 sshv1.nse

(kali@kali)-[/usr/share/nmap/scripts]
$ nmap --script ssh-brute.nse -p 22 192.168.0.174
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-02 06:12 EDT
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: webadmin:
NSE: [ssh-brute] Trying username/password pair: sysadmin:
NSE: [ssh-brute] Trying username/password pair: netadmin:
NSE: [ssh-brute] Trying username/password pair: guest:
NSE: [ssh-brute] Trying username/password pair: web:
NSE: [ssh-brute] Trying username/password pair: test:
NSE: [ssh-brute] Trying username/password pair: root:123456
NSE: [ssh-brute] Trying username/password pair: admin:123456
NSE: [ssh-brute] Trying username/password pair: administrator:123456
NSE: [ssh-brute] Trying username/password pair: webadmin:123456
NSE: [ssh-brute] Trying username/password pair: sysadmin:123456
NSE: [ssh-brute] Trying username/password pair: netadmin:123456
NSE: [ssh-brute] Trying username/password pair: guest:123456
NSE: [ssh-brute] Trying username/password pair: web:123456
NSE: [ssh-brute] Trying username/password pair: test:123456
NSE: [ssh-brute] Trying username/password pair: root:12345
NSE: [ssh-brute] Trying username/password pair: admin:12345
NSE: [ssh-brute] Trying username/password pair: administrator:12345
NSE: [ssh-brute] Trying username/password pair: webadmin:12345
NSE: [ssh-brute] Trying username/password pair: sysadmin:12345
NSE: [ssh-brute] Trying username/password pair: netadmin:12345
NSE: [ssh-brute] Trying username/password pair: guest:12345
NSE: [ssh-brute] Trying username/password pair: web:12345
NSE: [ssh-brute] Trying username/password pair: test:12345
NSE: [ssh-brute] Trying username/password pair: root:123456789
NSE: [ssh-brute] Trying username/password pair: admin:123456789
```

Task 3: NSE Scripts

```
(kali@kali)-[~/Downloads]
$ zip2john zoro.zip > zoro.hashes
ver 2.0 zoro.zip/zoro/ is not encrypted, or stored with non-handled compression type

(kali@kali)-[~/Downloads]
$ john zoro.hashes
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 369605 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
0987654321 (zoro.zip/zoro/Screenshot_2023-06-30_09_20_54.png)
1g 0:00:00:01 DONE 2/3 (2023-08-25 09:22) 0.9090g/s 44287p/s 44287c/s 44287C/s 123456..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~/Downloads]
$ jhon --show
Command 'jhon' not found, did you mean:
  command 'john' from snap john-the-ripper (roll+15b3b7c)
  command 'john' from deb john
  command 'jshon' from deb jshon
See 'snap info <snapname>' for additional versions.

(kali@kali)-[~/Downloads]
$ john zoro.hashes --show
zoro.zip/zoro/Screenshot_2023-06-30_09_20_54.png:0987654321:zoro/Screenshot_2023-06-30_09_20_54.png:zoro.zip:zoro.zi
p

1 password hash cracked, 0 left

(kali@kali)-[~/Downloads]
$
```

Task 4: John The Ripper

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ crunch 5 8 cafegedrgqw1234 -o pass.txt  
Crunch will now generate the following amount of data: 7879580046 bytes  
7514 MB  
7 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 883677340  
  
crunch: 7% completed generating output  
crunch: 12% completed generating output  
crunch: 17% completed generating output
```

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ crunch 8 8 -t ,000^%% pass1.txt  
Crunch will now generate the following amount of data: 135721872000 bytes  
129434 MB  
126 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 15080208000  
Aaaa!000  
Aaaa!001  
Aaaa!002  
Aaaa!003  
Aaaa!004  
Aaaa!005  
Aaaa!006  
Aaaa!007  
Aaaa!008  
Aaaa!009  
Aaaa!010  
Aaaa!011  
Aaaa!012  
Aaaa!013  
Aaaa!014  
Aaaa!015  
Aaaa!016  
Aaaa!017  
Aaaa!018
```

Task 5: Password Generation Using Crunch

vi. CONCLUSION

In summary, this report has explored five crucial elements of ethical hacking: Hydra for password cracking, Auxiliary Modules for network vulnerability assessment, NSE Scripts for targeted network scanning, John the Ripper for password strength evaluation, and Crunch for secure password generation. These tools and techniques collectively strengthen cybersecurity by identifying vulnerabilities, enhancing access control, and promoting robust password security. Ethical hacking, conducted responsibly, is a proactive approach to safeguarding digital assets in an interconnected world.