Analysis and implementation of the Port Knocking method using Firewall-based Mikrotik RouterOS

Mursyidah, Husaini, Atthariq, Muhammad Arhami, Hari Toha Hidayat, Anita, Ramadhona

Department of Information Computer Technology, Politeknik Negeri Lhokseumawe, Lhokseumawe, 24301, Indonesia

E-mail: mursyidah@pnl.ac.id

Abstract. Static firewalls such as packet filtering that restrict access based on addresses on NIC (Network Interface Card) devices in the form of MAC addresses will make dependence on the device, this will make it difficult for administrators. This type of firewall is vulnerable to packet spoofing in the form of MAC address spoofing. Firewall port knocking in some previous research, port Knocking using third-party applications that must be installed and dependence on certain. This port knocking method with port programming based on socket programming aims to provide easy access without dependence on IP addresses and Mac addresses or operating systems as well as better security through a tap format that must go through 4 stages, namely having to use the correct protocol type, port number correct, correct order and send the correct string to obtain access rights. The Port knocking method only allows access to clients who have performed the correct and complete knocking port. Knocking port applications are made using socket-based programming that can run on Windows and Linux operating systems and do not need the installation process so that the authentication process is less than 2 seconds. The compatibility of the port Knocking application makes access easier and faster. The port knocking method firewall has a filter effectiveness of 66.7% and better resistance to DDoS attacks than packet filtering based on data service quality. Port Knocking gets RTT value of 380 ms (Medium Category) and Packet loss of 8.3% (Good Category), while packet filtering gets RTT value of 2858 (Poor Category) and Packet Loss of 56.3% (Poor Category).

1. Introduction

Firewall is a computer network protection solution in preventing attacks and intrusions that can endanger the confidentiality of data and damage to the infrastructure of a network [1]. Some previous studies about security systems built with firewalls use the port knocking method that is "Increasing the Security of VPN Server with RouterOS Microtic Port-Based Knocking Method". The method is applied to VPN Server, port knocking authentication using the Cygwin and knock.exe applications and testing using the BackTrack Linux operating system [2]. The Port Knocking method is also applied to the Linux operating system Ubuntu Server 12.04 LTS. Port Knocking process using knocked application and port knocking is used to secure SSH Server services, FTP Server, and MySQL Server [3]. The use of third-party applications is less efficient because it must be installed first, the port Knocking process is done manually by typing the command line.

Dependence on time limits (timeouts), as well as dependence on the operating system that is used because of different operating systems, different applications for Knocking the port. This will take up a lot of time for the Administrator to access the router and certain services run by the router.
Based on the problems discussed above, to overcome them, "Analysis and Implementation of Firewalls using the MikroTik RouterOS-based Knocking Port method" is made. With the port Knocking process using an application made with socket-based programming so that the authentication process does not require a long time. In addition to the convenience provided to legitimate parties (Administrators), this system will also provide multiple layers of security by detecting attacks and by Knocking formats that must go through 4 stages, namely Knocking the correct port number, protocol type, correct sequence / sequence, and must send text (strings) to each beat. This security system uses the Kali Linux operating system with 3 forms of attacks in the form of DDoS (Distributed Denial of Services), Port Scanning and Brute Force. This port knocking is used to secure FTP (File Transfer Protocol), SSH (Secure Shell), Telnet (Telecommunications Network, API, Winbox and WebFig services on routers).

2. Experimental
2.1 Research Stages
The research stage is presented in the form of a flowchart which can be seen in Figure 1.

![Figure 1. Flowchart Stages of Research.](image)

The research phase begins with analyzing needs including the needs of hardware and software. The hardware used in the form of several PCs/laptops, MikroTik RB951Ui-2nd Router board, USB modem, 1 Sim Card and UTP (Unshielded Twisted Pair) cable. There is software needed in research, namely Windows 7 / 8.1 operating system for Administrators, Kali Linux for Attacker, Putty application, Winbox, API, Browser, Automate Scite Script Editor, Wireshark, Nmap, Hydra, and Hping3 Tools.
2.2 System Design
The network system used in the study is a hotspot system with an internet connection originating from a GSM modem. Hotspot network system can be done by configuring Interfaces, Bridge, PPP (Point to Point), IP (Internet Protocol) Configuration, and Hotspot Configuration. Figure 2 illustrates the System that was built using the Mikrotik RB951Ui-2nd Router board is a hotspot system with an internal Access Point, the internet source comes from a GSM modem that is connected via a USB port through the PPP interface (Point to Point). Interfaces used are ether2, wlan1 and PPP-out1 Ether2 interface for local area network (LAN), wireless (wireless LAN) to distribution networks for clients via wireless with AP Bridge mode. The IP address used for Bridge Hotspot interfaces is the class C IP address, which is 192.168.10.1/24. for the hotspot in the form of bridge hotspot, Hotspot server address 192.168.10.1 and DNS Name: tmjprl.hotspot.ac.id. The next step is the creation of a port Knocking application using the Autoit Scite Script Editor. Knocking ports based on socket programming can be done with UDPOpen and UDPSend functions.

![Figure 2. Designing a Hotspot Network System.](image)

2.3 Firewall Port Knocking configuration
The basic principles of port knocking can easily be explained as follows:
- The client connects to a remote system that applies firewall rules as follows: the client cannot connect to any remote port on the remote system at all, in other words, all ports are closed by a firewall,
- The client tries to connect by sending UDP data packets to the remote system through several ports sequentially,
- The client will not get any response from the server during this phase,
- Port knock daemon records the connection attempt and then authenticates the experiment if the authentication is successful, in this case, the order of ports that are attempted to connect according to certain rules in the daemon knock port, then the daemon will overwrite the firewall configuration file to allow port n to opened to the client with authenticated IP address,
- The client connects to port n using the application. [4]

The following firewall flowchart port knocking method can be seen in Figure 3.
At first, the firewall will perform detection against the traffic packet data. UDP data packets sent to the client towards a server will be logged by the firewall as a form of experimental connection. The format of the beats according to the rules on the firewall will be included in the address list's Knock with a time limit runs out of 1 second. If the knocking is done is correct and complete appropriate rules on the firewall then the client will obtain access to services FTP, SSH, Telnet, Winbox, WebFig and fire with a time limit of 1 day. The details of firewall port knocking method schema can be seen in Figure 4. A shown in the figure, the Firewall allows only the Address list in the IP range within 192.168.10.20 until 192.168.10.250 for getting accessibility to services/services (FTP, SSH, Telnet, WebFig, Winbox and fire) on the router. Address list access obtained by doing 7 keystrokes along with the delivery of the

**Figure 3.** Flowchart Firewall Port Knocking Method.

![Flowchart Firewall Port Knocking Method](image-url)
string at each knock against ports (1490, 343, 2914, 9203, 90, 3430, 29). Each of the beats will be in the
address list's Knock with a time limit runs out (timeout) 1 second. Access service which not under this
IP Address range will be rejected and marked by the firewall as a Blacklist.

Firewall Port Knocking method only allows access to the services SSH (port 22), FTP (port 21),
Telnet (port 23), WebFig (port 1491), Winbox (port 8291) and fire (port 8728) against the IP address of
the client who has conducted percussion port/port knocking in full and true. The correct format of a
knock in the form protocol type to UDP destination port, be 1490, 343, 2914, 9203, 90, 3430 and 29,
the order/sequence right and send the string on each of his knock.

![Port knocking firewall scheme.](image)

Figure 4. Port knocking firewall scheme.

Figure 5 shows a schema type of packet filtering firewall. It shows, that the firewall allows access to
services FTP, SSH, Telnet, WebFig, Winbox and fire only from the MAC address that has a definition
by the firewall from any IP address. Access which not under this MAC Address will be rejected.

![Packet filtering firewall scheme.](image)

Figure 5. Packet filtering firewall scheme.

2.4 Testing Firewalls against attacks
There are 3 stages of testing that are testing the application, test access port percussion services as well
as testing of the attack on the port knocking method and firewall packet filtering.

- Application Testing percussion port
  Testing applications on the operating system port percussion Windows and Linux. Testing conducted
to know the performance of the application as well as application compatibility on the operating
system.
- Testing of access services
Testing access to services FTP, SSH, Telnet, Winbox, Webfig as well as the API before and after doing a port knocking.

- **Testing the attack**
  
The attack is carried out using the operating system Linux version 2017.2 Time. The testing flowchart can be seen in Figure 6 below.

![Flowchart](image)

**Figure 6. Flowchart Firewall Packet Filtering Against Attacks.**

Figure 6 shows that before the main attack DDoS, Port Scanning and Brute force attacks are performed, starting with the MAC Spoofing (IP Address Forgery) by the attacker. Mac spoofing can be done with the tool on an operating system mac changer Time Linux. DDoS attacks do with fashion-- Hping3 flood using a tool. Tool Nmap used to process the Port Scanning attacks. A Brute Force attack can be done with a tool to do a Hydra login with username and password list arrangement made with tool Crunch [6]. Following the attack on the testing flowchart firewall port knocking method can be seen in Figure 7.

These tests are done to find out the capabilities of the firewall the port knocking method and system resilience built good port knocking or packet filtering with 3 main types of DDOS attack (tool Hping3), Brute Force (tool Crunch & Hydra) as well as Port Scanning (Network Mapper tool). The attack starts with MAC Spoofing (counterfeiting the Mac Address) with the tool on an operating system macchanger Time Linux. After Mac Spoofing IP Spoofing will do (counterfeiting IP Address) with the tool to DDoS Hping3, Nmap to Port Scanning. A Brute Force attack cannot be done IP address forgery [6].
3. Results and Discussion

3.1 Application Testing Results Percussion Port

Testing the application using Knocking Port percussion port that has been created using socket-based programming with the Autoit Scite Editor Script. Application testing can be done by Knocking the server port through the application tool Wireshark. The following flowchart process conducted by the client port percussion can be seen through the tool Wireshark on Linux operating system Time as shown in Figure 8. Based on Figure 8, the port can build percussion application communication between client (IP address: 192.168.10.239) and the server (IP address: 192.168.10.1) with the original client port (58072, 47732, 38580, 58652, 54625, 54625, 46149, and 40877) and the destination port of the server (1490, 39214, 9203, 90, 3430, and 29). the application can also handle the sending of your data in the form of a string that is the data type for the text that combines letters, numbers, whitespace (space), and various other characters. Application of percussion port can be run on the Windows operating system 7, 8.1, 10 and Linux.
3.2 Results of the Testing Service Access

Services/Services FTP, SSH, Telnet, Winbox, WebFig, and fire can only be accessed by a client who's been doing the first port knocking as can be seen in Table 1.

| No | Knocking Port | Services |
|----|---------------|----------|
|    | Before        | FTP      | SSH      | Telnet   | WebFig   | Winbox | API  |
| 1  | Failed        | Failed   | Failed   | Failed   | Failed   | Failed |
| 2  | Succeed       | Succeed  | Succeed  | Succeed  | Succeed  | Succeed|

Table 1 shows that access services cannot be done without doing percussion port first.

A. Attack test results

1) Testing Firewalls Against Port Scanning Attack this test to know the security format beats against port scanning or port scanning. The test results can be seen in Table 2.

| No | Port     | Level space | Timeout space | Regex | Attack time | Scanned | Succeeds space | Access to service |
|----|----------|-------------|---------------|-------|-------------|---------|----------------|-------------------|
| 1  | 273-2391 | 7           | 10m           | -     | 288 s       | 3       | 4              | Failed            |
| 2  | 29-9203  | 7           | 10m           | -     | 2076.46s    | 3       | 2              | Failed            |
| 3  | 29-9203  | 7           | 1s            | √     | 2071.95s    | 3       | 0              | Failed            |
On the basis of table 2 indicates that the timeout high beats in a minute will create opportunities for attackers to perform port scanning over and over again so that it can submit beats to all port. Without using regexp layer7 filter firewall, NMap will do scanning port so that port will receive a knock from the attacker through the scanning process port. With the use of a number of stages that many beats, timeout (time constraints) are a little bit and use the regexp for string data on each delivery beats will provide better security in the absence of a successful knock done by Nmap.

2) Test attack on firewall use port knocking method or packet filtering An attack on the test results firewall port knocking or packet filtering can be seen in table 3.

| No | Firewall      | Spoof MAC | Spoof IP | Status Host | Knocking Port | DDoS  | Port Scanning | Brute Force |
|----|---------------|-----------|----------|-------------|---------------|-------|--------------|-------------|
| 1  | Packet Filtering | Yes       | -        | Not Active  | -             | √     | √            | √           |
| 2  | Port Knocking  | Yes       | Yes      | Active      | No            | X     | X            | X           |

Based on table 3 indicates that the DDoS attacks, Port Scanning and Brute Force against the firewall packet filtering successfully done only by Spoofing (Forgery) MAC address only. The attacker will gain access to services only with MAC Spoofing, while the success of the attack on the port knocking method depending on the firewall towards the target host status already/not yet doing the port knocking. Kerberhasilan attacks have to be Spoofing the MAC and IP Address. Obtained values the effectiveness of filters the results for the number of attacks failed with the total number of attacks obtained for port knocking is a method of 66.7% while packet filtering is 0%.

Although the DDoS attacks and Port Scanning successfully against the target host have done the port knocking, the attacker still will not get the rights of access to the service without making a port knocking.

3) Testing the resilience of the servers against DDoS (Distributed Denial of Service) based on the quality of the data service.

Service quality measurement data using the parameters of the RTT (Round Trip Time) and Packet Loss through Ping to Google servers [5]. The measurement is done in 1-hour time range from 20:46 to 21:46 and from 09:48 to 10:48 at the time of the occurrence of DDoS attacks. Following the results of the quality of service, data can be seen in table 4.

| No | Firewall      | AVG RTT (ms) | Packet Loss (%) | Categories |
|----|---------------|--------------|-----------------|------------|
| 1  | Port Knocking | 380          | 8.3             | Good       |
| 2  | Packet filtering | 2858        | 56.3            | Bad        |
Based on the value of the RTT and Packet Loss shows that the resilience of the firewall with port knocking server better than packet filtering with remained in good standing (good quality data service) at the time of the occurrence of DDoS attacks.

4. Conclusions
The firewall that is using the port knocking method with a format of a knock in the form of 7 stages of beats, timeout (timeout) 1s as well as using regexp safe against port scanning attacks. Firewall port knocking method a value filter effectiveness of 66.7% and. resistance better than packet filtering based on the quality of the data service. Port Knocking gets an RTT of 380 ms (category medium) and Packet loss of 8.3% (Both Categories), while packet filtering gets an RTT of 2858 (Poor Category) and Packet Loss amounted to 56.3% (Poor Category). Application port knocking does not need installation can run on Windows and Linux operating system so that it will provide ease of access for administrators. The concept of port knocking does not cause an administrator to rely on against MAC Address as well as the operating system.

References

[1] Sukaridhoto, S. 2014. Buku Jaringan Komputer I & II. Online. dhoto.lecturer.pens.ac.id/publications/book/2014/Dhoto-JaringanKomputer1.pdf. Diakses 20 Mei 2018.
[2] Budiman, A. D. 2014 (Agustus). Meningkatkan Keamanan VPN Server dengan Menggunakan Metode Port Knocking berbasis MikroTik RouterOS. Online. https://repository.unikom.ac.id/28652.
[3] Fajri M. S, Rahmad Suhatman & Eka Y. E. 2014 (April). “Analisa Port Knocking Pada Sistem Operasi Linux Ubuntu Server 12.04 LTS”. Online. https://journal.pcr.ac.id. Diakses 22 Mei 2018.
[4] Richard, Josefh P. Dan Susanto, B (2007). Seminar Nasional Teknologi. Sistem Autentikasi Port Knocking. Online. http://p3m.amikom.ac.id. Diakses pada 30 Maret 2018.
[5] Susandi, H., Maksum, P. 2014 (Agustus). Analisis Kualitas Layanan Data pada Jaringan Telekomunikasi berbasis CDMA EFD0 Rev.A. Online.https://jurnal.usu.ac.id/singuda_ensikom/article/viewFile/5086/2936. Diakses pada 21 Mei 2018.
[6] Kali Linux Penetration Testing Tools. 2018. Online. https://tools.kali.org/. Diakses 29 Juli 2018.