DOI https://doi.org/10.30525/978-9934-26-459-7-5

AN EXPERIMENTAL APPROACH TO SECURING SERVERS BY THE PORT KNOCKING METHOD WITH ROUTEROS

Armando Jesus Ventura[1*], José Jasnau Caeiro[1]
[1]Polytechnic University of Beja, Rua Pedro Soares, 7800-295 BEJA, Portugal
**Corresponding author's e-mail: ajventura@ipbeja.pt*

Received 1 March 2024, www.isma.lv

Abstract

In computer networks the access to services is commonly provided by opening ports in the router firewall. This paper will focus on the port knocking method for augmenting the computer security of networks. It provides an overview of the technique and discusses some of the modern implementations, namely using Software Defined Networking and P4. A discussion of the implementation of port knocking with routers running RouterOS, supplied by MikroTik, is also presented with some experimental details. The knockd implementation is also shortly discussed. Although the port knocking technique greatly enhances the computer security of network access to services, even with poor implementations, there are advices to follow that are listed in this paper.

Key words: *computer security, internet firewall, port knocking, routing, software defined networking.*

1. Introduction

The port knocking method was proposed in 2003 by Martin Kryzwinski [1], but it remains a technique more relevant than ever before. A large number of cyberattacks start with a port scanning to the computers and routers attached to a certain network. The scanning purpose is to determine which services and operating system versions are running in the computer servers in the network. This knowledge allows the attackers to exploit eventual vulnerabilities of these computer systems. Internet-connected machines may be protected by filtering packets, or trust application-level security. Firewalls implement the first method and are Internet devices with software designed to filter or produce log files reporting unwanted network traffic. However, firewalls do not protect against the exploitation of application-level software vulnerabilities. The Internet architecture is designed in a way that services attached to a port should be accessible by any machine using the Internet protocols.

Another set of sotware is based on the deployment of strong application-level security mechanisms. These are usually built above the network level and are subject to attacks when discovered on a server. A very useful method to avoid many cyberattacks is to have all the server or router service ports initially closed and to only open the port of the router/server for connection to a client after a certain well defined sequence of connection requests to certain ports is performed. This method is designated by port knocking and although *per se* it is already very secure, additional techniques further the safety.

A short enumeration of the advantages of port knocking are:

- the practical impossibility to assert whether port knocking is implemented on the router/server;
- intrusion detection systems (IDS) and firewalls providing access control;
- the enormous challenge to detection by sniffing;
- the room available for improving the technique.

Nevertheless there authors pointing to the shortcomings of port knocking, namely Sristava *et al.* [5] and Pali and Amin [6], among others. Some solutions are based on black listing after wrong scan, dynamic change of port knocking sequences after some sort of assymetric ciphered message exchange [8]. Another proposal for improvement is a two level host authentication [7].

In this paper a short review of the port knocking method is presented. Several implementations such as the *knockd* server, or only *firewall* based port knocking, such as *iptables* or *nftables* are discussed. Modern Software Defined Networking (SDN) proposals are briefly discussed, namely with P4. An implementation with the RouterOS firewall is detailed and discussed and some examples are given, along with some Python port knocking scripts.

The document has the following structure. The first section defines the problem, presents the authors contributions and the contents of each part of the paper. In the second section the authors present a short review of the state of the art. In the third section the experimental details of the RouterOS implementation of port knocking is discussed. Finally the last section is devoted to the conclusions.

References

1. Krzywinski, M., 2003. Port knocking– network authentication across closed ports. *SysAdmin Magazine* 12, 12–17.

2. Mursyidah, Husaini, Atthariq, Arhami, M., Hidayat, H. T., Anita, Ramadhona, 2019. Analysis and implementation of the port knocking method using firewall-based Mikrotik RouterOS. *IOP Conference Series: Materials Science and Engineering* 536, 012129. https://doi.org/10.1088/1757-899x/536/1/012129

3. Zia, U., Yar, M. A., Naeem, T., Amin, M., Zeeshan, M., Sima, M. W. U., 2022. Security technique to prevent port knocking and illegal access in SDN, in: 2022 International Conference on Electrical Engineering and Sustainable Technologies (ICEEST). IEEE. https://doi.org/10.1109/iceest56292.2022.10077876

4. Zaballa, E.O., Franco, D., Zhou, Z., Berger, M.S., 2020. P4Knocking: Offloading host-based firewall functionalities to the network, in: *2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*. IEEE. https://doi.org/10.1109/icin48450.2020.9059298

5. Srivastava, V., Keshri, A. K., Roy, A. D., Chaurasiya, V. K., Gupta, R., 2011. Advanced port knocking authentication scheme with QRC using AES, in: *2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*. IEEE. https://doi.org/10.1109/etncc.2011.5958506

6. Pali, I., Amin, R., 2022. PortSec: Securing port knocking system using sequence mechanism in SDN environment, in: *2022 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE. https://doi.org/10.1109/iwcmc55113.2022.9824343

7. Bhattacharya, A., Rana, R., Datta, S., U., V., 2022. P4-sKnock: A two level host authentication and access control mechanism in P4 based SDN, in: *2022 27th Asia Pacific Conference on Communications (APCC)*. IEEE. https://doi.org/10.1109/apcc55198.2022.9943765

8. Saxena, A., Muttreja, R., Upadhyay, S., Kumar, K.S., U., V., 2021. P4Filter: A two level defensive mechanism against attacks in SDN using P4, in: *2021 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE. https://doi.org/10.1109/ants52808.2021.9937010

Authors

Armando Jesus Ventura, 16/02/1978, Santiago do Cacém

Current position, grades: Assistant Professor, Msc
University studies: Msc in Computer Science
Scientific interest: Networking, system administration, computer programming, cybersecurity
Publications (number or main): 4
Experience: Assistant Professor IPBeja(6y), Assistant Professor IPBeja(11y), Assistant Professor Piaget(2y), Computer Science technician (20y). Member of the UBINET Lab(httpd://ubinet.ipbeja.pt)

José Jasnau Caeiro, 15/03/1963, Lisboa

Current position, grades: Associate Professor, PhD
University studies: Msc and PhD in Electrical and Computer Engineering, Lic. Physics Engineering
Scientific interest: Internet of Things, computer programming, image processing
Publications (number or main): 30
Experience: Associate Professor IPBeja (3y), Assistant Professor IPBeja (23y), Assistant Professor ENIDH (1y), Assistant Professor IP Setúbal (1y), Assistant Teacher FCT-UNL (1), University Teacher (2y), Electronics and Telecomunications technician (1y). Member of IEEE (32y), Member of the SEPSI Lab (http://sepsi.ipbeja.pt/jasnau.html)