Securing Servers Connections

Document Name :	Securing SSH Connections
Version :	1.0
Version Date :	13/07/2022
Modified By :	Marc MARTINEZ
Creation Date :	13/07/2022
Created by :	Marc MARTINEZ
Approved by :	Marc MARTINEZ
Confidentiality Level :	INTERNAL

Modification History

	Date	Author	Commentary
1.0	13/07/2022	Marc MARTINEZ	Creation of the document

Introduction

This document will give a summary of the method the Security Team suggests using to secure the ssh connections to the servers of the application, as well as all of the others connexions to the servers.

Content

SSH

The Security Team using fail2ban, a free software, to secure the ssh connections to the servers of our systems and infrastructure.

We suggest setting up policy to ban IPs on suspicions of DDoS attemps or brute forces attemps.

The proposed policy is to ban the IPs adresses after 5 unsuccessful attemps and for 86400 seconds (24 hours).

We also suggest changing the ssh port to something else than port 22 to prevent low level brute forces attacks depending on the default port.

Others Ports

The Security Team also would like to add that changing the ports on all of the importants systems used on our infrastructure would have the same protective effects as for changing the ssh port to not leave it on default port.

Firewalls

Furthermore, all unused ports should be closed and used ports must have, if possible, restrictions of IP based on the intended use of the port.

For examples, the ports used to exchange informations between our database server and the application server should only be open for the IPs of those machines, between themselves.

The same thing should be done for the ports that receives informations from the IoT devises. That would allow us to have more trust in the informations received in this ports (ie : not getting wrong data delivered to the systems because something else than our IoT devises with the known IPs addresses tried to connect to those ports).

The default firewall software for debian based systems is ufw.

The default firewall software for centOS based systems is firewalld.

Tools suggested and required budget

- fail2ban (free)
- ufw/firewalld/other unix open source firewall (free)
- Half (0.5) a day of man hours (400€)