PORT DETECTOR

Detect ports easily

Created By F.K

Apache License

Version 2.0, January 2004

Source Codes

https://github.com/firatkaya1/port-detector

GNU/Linux

Version 19.10

We are detect to your operation system is GNU/Linux . Under the these page all suggestions re-write for you personal computer. Feel free.

Please before the start check out dependencies for firewall settings. If you do not have these dependencies, open the original documentation(github.com/firatkaya1) and install to your operation system.

•*We are using iptables command on linux.*

• *sudo apt-get update && sudo apt-get install iptables*

Settings

Extract Path

/home/kaya/Desktop/port-detector.pdf

Language

English

Created Date

2021/01/04 14:16:04

#	Host	Port	Status	?
1	0.0.0.0	631	Listening	IPP
2	0.0.0.0	5939	Listening	TCP
3	0.0.0.0	36477	Listening	UNKNOWN
4	0.0.0.0	57621	Listening	UNKNOWN

We are detecting 4 ports and 2 port came from unknown, if you are considering these ports not expected, please forbid these ports.

Why should you close unused ports?

Open ports on a server are a security vulnerability that can potentially allow a hacker to exploit services on your network. If those services are unpatched, a hacker can easily take advantage of the system by running a simple port scan using free software like nmap to discover the open ports. It’s important that you understand some basics about port security and how to manage ports with the principal of least privilege.

How to block a port?

In linux worlds, we recommend to you use commands which is help you to understand and managed your firewall.

Step 1

Install iptables library to your machine.

- *sudo apt-get update && sudo apt-get install iptables*

Step 2

Block the incoming request which is protect to you from unknown resources.

- *sudo iptables -I OUTPUT -p tcp --dport {YOUR-PORT-NUMBER} -j DROP*

Step 3

Check the ports, are they closed from outside request?

- *sudo iptables -L -nv*

Frequently Asked Questions

1-Why I should close open ports?

Open ports can accept outside request to your machine and represent vulnerability of your information. We are recommended to close outside request for protect itself.

2-Why should some ports be open?

Even we want to control all the ports, we have to continue our communication between machine and world. For example, we do not want to close 80 port because this port working with HTTP and connect to other machine. Another example is 22 port. This port helps to us connect our machine via SSH.

3-What happen if i close all ports?

Definitely worst idea. You can not contact your machine if machine is a server. All communication will lose.

4-How can i close all ports only one command ?

```
iptables -A INPUT -p tcp -m tcp -m multiport ! --dports 80,443 -j DROP
```

5-How can i open a port that i closed?

Let's we assume, we closed 22 port after that we wants to open same port again.

```
iptables -I INPUT -p tcp --dport 22 --syn -j ACCEPT
```

6-What is iptables command ?

Iptables is a Linux command line firewall that allows system administrators to manage incoming and outgoing traffic via a set of configurable table rules. Iptables uses a set of tables which have chains that contain set of built-in or user defined rules

7-What is extract path in this document?

Extract path is represent your document where will save.

8-What is the language?

Language is represent main language of this document. You can change before create this document.

8-What is the name?

Name is represent file name of document. You can change before create this document.

'10-What is ' sudo iptables -L -nv' ?

Command	Explain
-I	Append this rule to a rule chain. Valid chains for what we're doing are INPUT, FORWARD and OUTPUT, but we mostly deal with INPUT in this tutorial, which affects only incoming traffic.
OUTPUT	Represent incoming traffic.
-p	The connection protocol used.
tcp	Represent Transmission Control Protocol
--dport	The destination port(s) required for this rule. A single port may be given, or a range may be given as start:end, which will match all ports from start to end, inclusive.
{YOUR-PORT-NUMBER}	Which port do you want to block ?
-j	Jump to the specified target. By default, iptables allows four targets:ACCEPT,REJECT,DROP,LOG
ACCEPT	Accept the packet and stop processing rules in this chain.
REJECT	Reject the packet and notify the sender that we did so, and stop processing rules in this chain.
DROP	Silently ignore the packet, and stop processing rules in this chain.
LOG	Log the packet, and continue processing more rules in this chain. Allows the use of the --log-prefix and --log-level options.

'10-What is ' sudo iptables -L -nv' ?

This command list of all rules in iptables.

Command	Explain
-L	List of current rules in iptables.
-nv	Filter only invalid rules.

Most Common Ports and Services

Port	Service	Explain
20,21	FTP	File Transfer Protocol
22	SSH	Secure Shell (SSH)
23	TELNET	Unencrypted text communication
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name System
80	HTTP	Hyper Text Transfer Protocol
110	POP3	Post Office Protocol
119	NNTP	Network News Transfer Protocol
123	NTP	Network Time Protocol
143	IMAP	Internet Message Access Protocol
443	HTTPS	Hyper Text Transfer Protocol Security
465	SMTPS	Simple Mail Transfer Protocol Over SSL
3306	mysql	MySQL Database Service
5432	postgres	PostgreSQL Database
8080	Tomcat	Apache Tomcat Server