HOW TO CREATE A CAPTIVE PORTAL

Rachitpandya · Follow

7 min read · Jul 21, 2019

Listen Share More

This article will tell you how you can create a captive portal for yourself but before that lets first go through a small introduction

WHAT IS A CAPTIVE PORTAL ??

The captive portal feature is a software implementation that blocks clients from accessing the network until user verification has been established. The captive portal configuration provides the network administrator control over verification and authentication, assignment to interfaces, client sessions, and Web page customization.

In simple terms Captive portal authentication is a method where a web page is presented to the guest users when they try to access the Internet whether in hotels, conference centres or Wi-Fi hotspots. The web page can also prompt the guest users to authenticate or accept the usage policy and terms.

Now Lets clear one more concept before we actually dive into creating our very own captive portal page and that concept is of “IPTABLES”.

WHAT ARE IPTABLES ??

Firewall decides the fate of packets incoming and outgoing in the system. IPTables is a rule-based firewall and it is pre-installed on most of Linux operating system. By default, it runs without any rules but we will soon change it and add our rules to it. Whether you’re a novice Linux geek or a complete master, there’s probably some way that iptables can be a great use to you.

iptables is a command-line firewall utility that uses policy chains to allow or block traffic. When a connection tries to establish itself on your system, iptables looks for a rule in its list to match it to. If it doesn't find one, it resorts to the default action.(Always remember the order of the rule set in chains are important because iptables start checking from the first rule and goes down the chain .)

iptables uses three main chains: input, forward, and output.

Input — This chain is used to control the behavior for incoming connections.

Forward — This chain is used for incoming connections that aren't actually being delivered locally.

Output — This chain is used for outgoing connections.

To see what your policy chains are currently configured to do with unmatched traffic, run the

```
iptables -L
```

command.

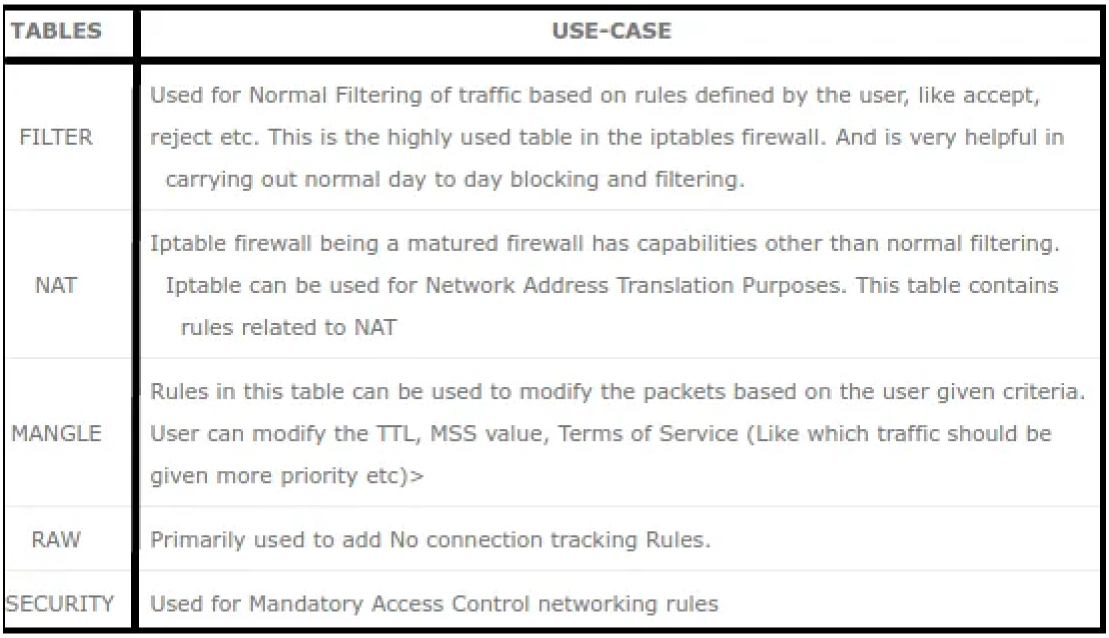
IPTABLES main files are:

1. /etc/init.d/iptables — init script to start|stop|restart and save rulesets.

2. /etc/sysconfig/iptables — where Rulesets are saved.

3. /sbin/iptables — binary.

IPTables has the following 5 built-in tables:



TABLES	USE-CASE
FILTER	Used for Normal Filtering of traffic based on rules defined by the user, like accept, reject etc. This is the highly used table in the iptables firewall. And is very helpful in carrying out normal day to day blocking and filtering.
NAT	Iptable firewall being a matured firewall has capabilities other than normal filtering. Iptable can be used for Network Address Translation Purposes. This table contains rules related to NAT
MANGLE	Rules in this table can be used to modify the packets based on the user given criteria. User can modify the TTL, MSS value, Terms of Service (Like which traffic should be given more priority etc)>
RAW	Primarily used to add No connection tracking Rules.
SECURITY	Used for Mandatory Access Control networking rules

To start, stop and restart Iptabe Firewall use the following commands :

```
# /etc/init.d/iptables start
```

```
# /etc/init.d/iptables stop
```

```
# /etc/init.d/iptables restart
```

Now, let’s see some useful commands:

- **To see all the rules,** we can type:

```
sudo iptables -t <table-name> -L
```

where,
-*t* is used to specify the table name,
-*v* for verbose and
-*L* for listing the chains and rules

- **To add a rule inside a chain of a table**, we can type:

```
sudo iptables -t <table-name> -A <chain-name> -d <destination-address> -p
<protocol> -j <action>
```

where,
-*A* to append one or more rules to the end of the selected chain
-*d* for specifying a destination

-p protocol of the rule or of the packet to check
-j specifies the target of the rule; i.e., what to do if the packet matches it

- To flush all the rules:

```
sudo iptables -t <table-name> -F
```

where,
-F to flush the selected table rules

- **To create a new chain:**

```
sudo iptables -t <table-name> -N <chain-name>
```

where,
-N for adding a new chain to a particular table

- **To delete a chain:**

```
sudo iptables -t <table-name> -X <chain-name>
```

where,
-X is for deleting the optional user-defined chain specified

To know more about different rules of the IPTABLES and explore more about the power of this tool go through this link to get few of the IPTABLE rules which u can use to do various types of tasks.

rachit57/BASIC-IP-TABLE-RULESET
This is a basic set of IPTABLE rules to implement diffrent features as mentioned (Default assumed to ACCEPT traffic)...
github.com

Now let's move ahead and create our captive portal 😊

CREATING THE CAPTIVE PORTAL :

So now let's get started .....

DNS configuration and basic settings :

For creating a captive portal page for your hotspot, the first thing you need to do is the basic configuration settings.

Firstly connect your Linux machine to your router through ethernet (this would generally show as the Eth0 interface in your machine .) now connect your machine's wifi to your hotspot (this would generally show as the Wlan0 interface .)

Now go to your wifi setting page (use default credentials username: admin, password: admin if you haven't changed them) and turn off the DHCP server (after this no one will be able to connect to your wifi).

DNS redirection works as the simple DNS hijacking where all the user DNS requests are hijacked and resolved to the captive portal login page.

Before going any further run these commands so that you won't face any kind of error while following this article.

· apt-get update

· apt-get install hostapd dnsmasq apache2 -y

(NOTE -> use the "sudo" command if you are not a root user)

Configuring and setting hostapd.conf file :

nano hostapd.conf

(this command will open the file "hostapd.conf", nano is just a text editor you can use any text editor like vim , gedit etc.I have used nano throughout this article .)

Make sure your hosapd.conf file looks like this

interface=**wlan0** (your desired interface name)

ssid=**Captive Portal** (your desired access-point name)

hw_mode=g

channel=**6**

macaddr_acl=0

auth_algs=1

```
ignore_broadcast_ssid=0
```

make sure you update these settings every time you are setting this up (especially the channel).

Configuring and setting dnsmasq.conf file :

```
nano dnsmasq.conf
```

Make sure your dnsmasq.conf file looks like this

```
dhcp-option=3,10.0.0.1 ( 3 -> code for default gateway )

dhcp-option=6,10.0.0.1 ( 6 -> code for DNS server )

server=8.8.8.8

log-queries

listen-address=127.0.0.1
```

Now we are ready to run our hostapd file it will be problematic if we directly run the file just now. WHY ??

Because if we run it right now network manager will try to interfere with our process so first, we have to get rid with this issue… so we will go ahead and kill it.

```
$ killall network-manager
```

Now we will go ahead and run our file

- $ hostapd hostapd.conf

Now we will allocate an IP address to the victims but before that we first need to set the IP address of our network interface so here it goes

```
$ ifconfig wlan0 10.0.0.1

$ dnsmasq -C dnsmasq.conf -d
```

Now is the time when you can enable NAT by setting up your firewall rules using the iptables rulesets (To know how to do that please go to the git-hub link mentioned previously in this article)

And also here we will disable the internet access for the victims

```
$ echo 0 > /proc/sys/net/ipv4/ip_forward
```

GREAT!!!!

Now your fake access point is all set.

Just a few more things and we will have our captive portal running.

Now let's go ahead and configure the captive portal using the APACHE WEB SERVER

Configuring captive portal :

Before diving into how to configure up your captive portal you have to create a web page for your captive portal, you can use any language of your choice like HTML , CSS , JAVA , JS , PHP to create your webpage. Or you can get online templates and edit those to have your captive portal page as per your requirements.

For example :

https://cdn.rootsh3ll.com/captive-portal/rootsh3ll-captive-portal-template.tar.xz

Once done… let's continue

Now, this final step will be done in 2 parts, one for the android devices and second for the windows devices -:

For android devices :

Firstly we have to create a directory for android in apache to do that use the following commands :

```
· $ cd /var/www/html/
```

```
· $ mkdir android
```

Now copy your captive portal page template to this directory

```
$ < Address > -C /var/www/html/android/
```

Here “Address” refers to the path of your template folder

Now we will create an android.conf file

```
$ nano /etc/apache2/sites-enabled/android.conf
```

Now copy the following code and save it in this file to create the redirection rules for android.

```
<VirtualHost *:80>

Servername connectivitycheck.gstatic.com

ServerAdmin webmaster@localhost

DocumentRoot /var/www/html/android

RedirectMatch 302 /generate_204 /index.html

ErrorLog ${APACHE_LOG_DIR}/android_error.log

CustomLog ${APACHE_LOG_DIR}/android_access.log combined

</VirtualHost>
```

ALL SET !!

Let's move towards the second part of it

For Windows devices :

Firstly we have to create a directory for windows in apache to do that use the following commands :

- $ cd /var/www/html/

- $ mkdir windows

Now copy your captive portal page template to this directory

```
$ < Address > -C /var/www/html/windows/
```

Here “Address” refers to the path of your template folder

Now we will create windows.conf file

```
$ nano /etc/apache2/sites-enabled/windows.conf
```

Now copy the following code and save it in this file to create the redirection rules for windows.

```
<VirtualHost *:80>

ServerAdmin webmaster@localhost

ServerName www.msftconnecttest.com

ServerAlias msftconnecttest.com

DocumentRoot /var/www/html/windows

RedirectMatch 302 /connecttest.txt index.html

RedirectMatch 302 /redirect index.html

RewriteRule /redirect index.html [R=302,L]

ErrorLog ${APACHE_LOG_DIR}/windows_error.log

CustomLog ${APACHE_LOG_DIR}/windows_access.log combined

</VirtualHost>
```

Now that both of these are done go ahead and set up the IPTABLE rules for redirection.

To know more about different rules of the IPTABLES and explore more about the power of this tool go through this link to get few of the IPTABLE rules which u can use to do various types of tasks.

rachit57/BASIC-IP-TABLE-RULESET

This is a basic set of IPTABLE rules to implement diffrent features as mentioned (Default assumed to ACCEPT traffic)…

github.com

before finishing up the things we have to enable the mod_rewrite to do that :

```
$ a2enmode rewrite
```

Now let's restart the apache server

```
$ service apache2 restart
```

And here comes the final step all we have to do now is to redirect the traffic to localhost, to do that :

```
$ dnsspoof -i wlan0
```

This completes the process and your very own captive portal should be up and running.

To verify you can see the apache logs here /var/log/apache2/android_access.log

Hope this article will be of some use to you.

Thanks for reading.

Tech Cybersecurity Captive Portal Technology Dnsmasq

Follow

Written by Rachitpandya

12 Followers

Learning new things is just a synonym of living.

More from Rachitpandya

Rachitpandya

What Are Backdoors And How they work ??

Many of you might have come across the term “Backdoors” especially if you talk to someone interested in the field of cybersecurity. Ever...

4 min read · Oct 4, 2020

6

Rachitpandya

How To Dual-Boot Your System

A lot of people are confused about how to switch from there current operating system to a different one. Few of them are confused due to...

3 min read · May 10, 2021

1

Rachitpandya

Protein Bars are Healthy: Truth or Hype

Who says avoiding junk food and transitioning to a healthier diet is simple? It's impossible to say no to fast food, chocolates, and...

2 min read · Apr 29, 2021

Rachitpandya

THINGS TO KNOW BEFORE DECIDING YOUR SERVICE FEE

This is a question which a lot of people face and are unable to find a satisfactory answer for. So let's see what the owner of Profrea has...

2 min read · Apr 25, 2021

See all from Rachitpandya

Recommended from Medium

Kallol Mazumdar in ILLUMINATION

I Went on the Dark Web and Instantly Regretted It

Accessing the forbidden parts of the World Wide Web, only to realize the depravity of humanity

8 min read · Mar 13, 2024

17.3K 318

Hazel Paradise

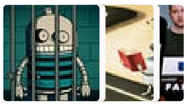
How I Create Passive Income With No Money

many ways to start a passive income today

5 min read · Mar 27, 2024

9.91K 234

Lists

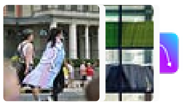


AI Regulation

6 stories · 433 saves

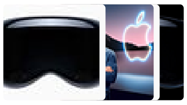
ChatGPT prompts

47 stories · 1506 saves



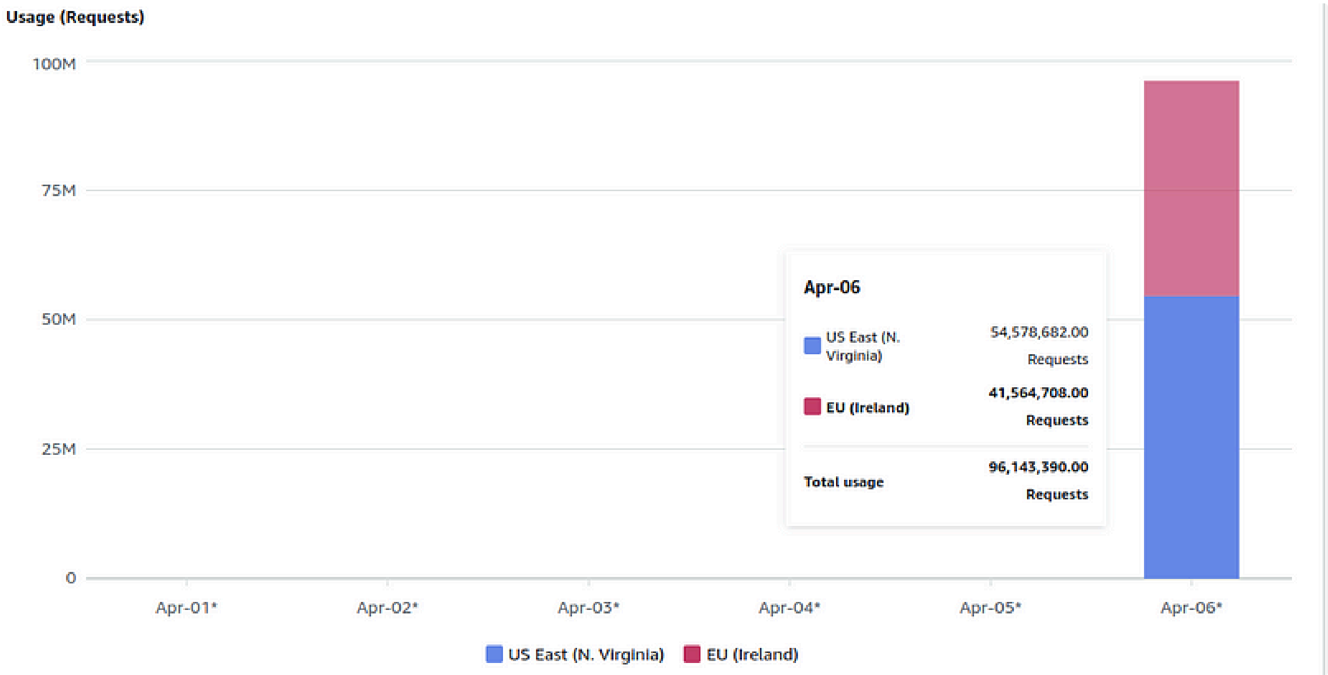
Generative AI Recommended Reading

52 stories · 990 saves



Apple's Vision Pro

7 stories · 67 saves



Maciej Pocwierz

How an empty S3 bucket can make your AWS bill explode

Imagine you create an empty, private AWS S3 bucket in a region of your preference. What will your AWS bill be the next morning?

4 min read · 4 days ago

7.2K 95

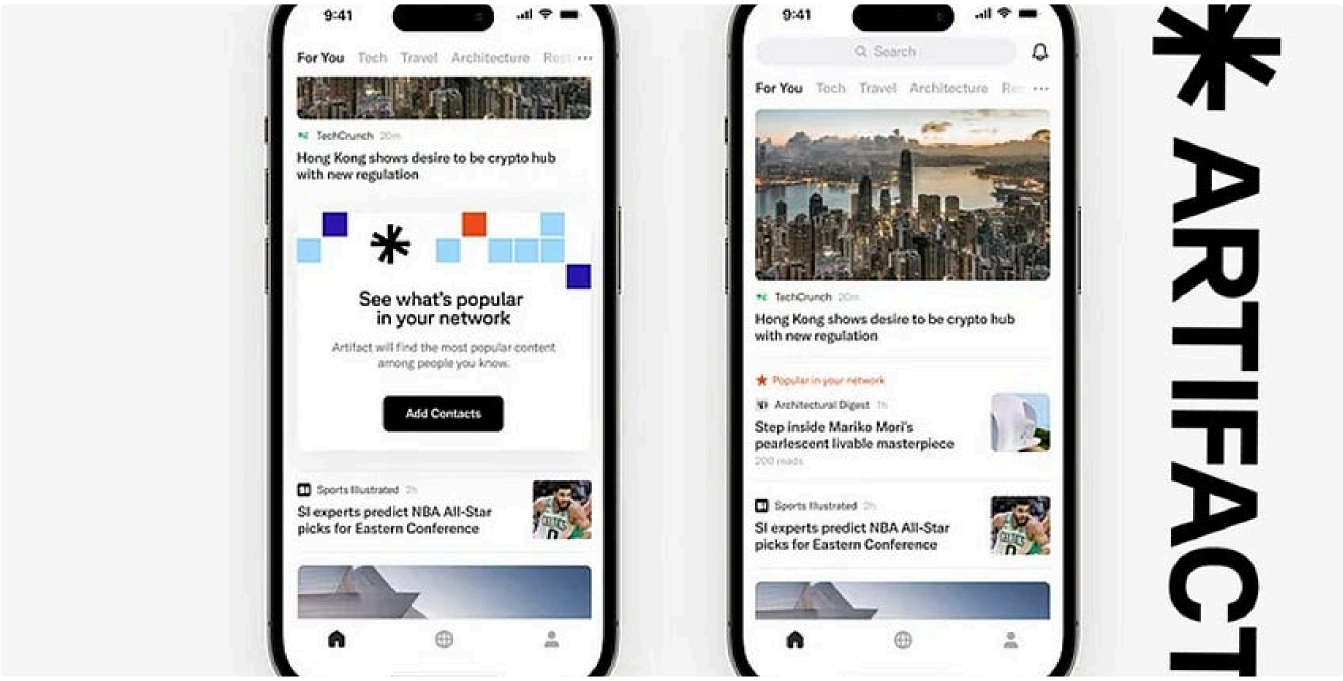
Somnath Singh in Level Up Coding

The Era of High-Paying Tech Jobs is Over

The Death of Tech Jobs.

✦ · 14 min read · Apr 1, 2024

10.1K 260



9:41
For You Tech Travel Architecture Real
TechCrunch 20m
Hong Kong shows desire to be crypto hub with new regulation
See what's popular in your network
Artifact will find the most popular content among people you know.
Add Contacts
Sports Illustrated 2h
SI experts predict NBA All-Star picks for Eastern Conference
9:41
Search
For You Tech Travel Architecture Re
TechCrunch 20m
Hong Kong shows desire to be crypto hub with new regulation
Popular in your network
Architectural Digest 1h
Step inside Mariko Mori's pearlescent livable masterpiece
200 reads
Sports Illustrated 2h
SI experts predict NBA All-Star picks for Eastern Conference
ARTIFACT

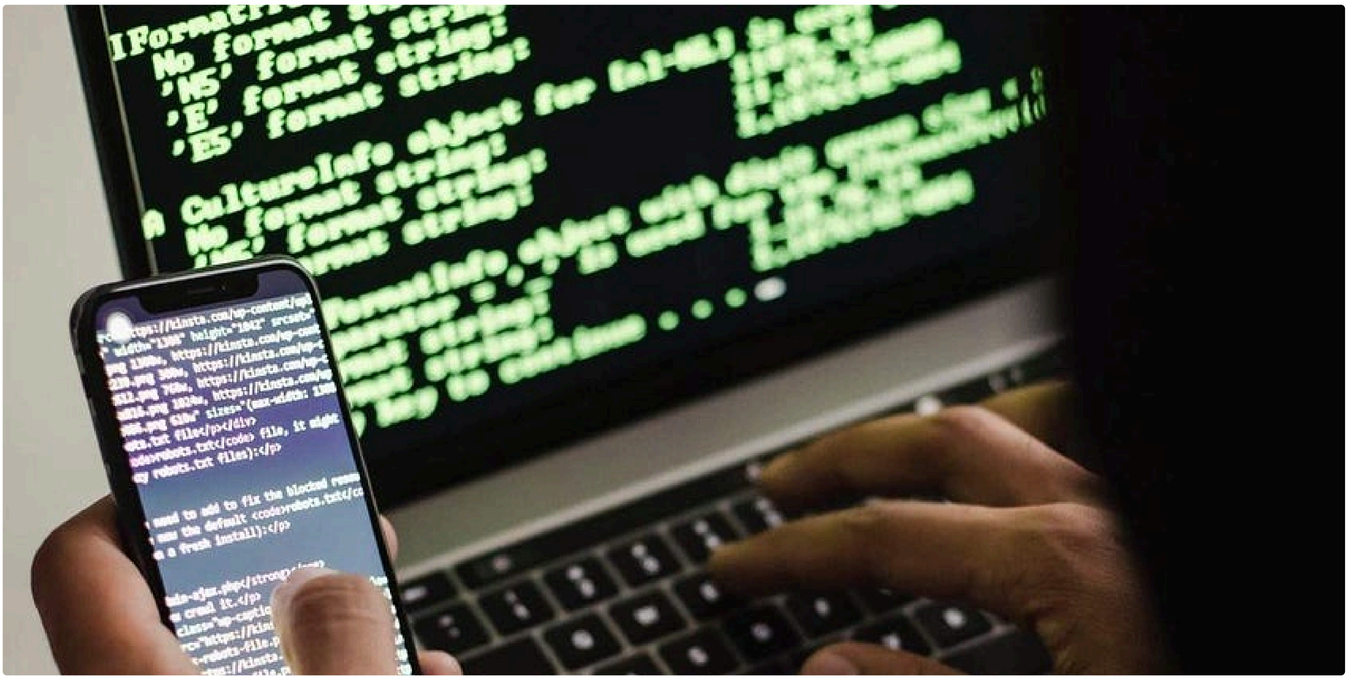
Gowtham Oleti

Apps I Use And Why You Should Too.

Let’s skip past the usual suspects like YouTube, WhatsApp and Instagram. I want to share with you some less familiar apps that have become…

11 min read · Nov 14, 2023

22K 407



Pine Damian

Mobile Phone Hacking

Disclaimer!

7 min read · Apr 18, 2024

289 6

See more recommendations