

Personal Vulnerability Investigation

Mohammed Nasser Alshukaili.

ICT, Fontys University of Applied Sciences.

Cyber Security, Semester 4.

2022

Contents

SCOPE	3
Main Question	3
What are the vulnerabilities in the tp-link WR841N router?	3
Sub Questions	3
1- What is the difference between router and modem?	3
2- What type of routers do big companies use in their buildings?	3
3- How routers work?	3
4- How can a hacker take over tp-link wr841n's system?	3
My Plan	4
Results	5
1. What is the difference between router and modem?	5
2. What type of routers do big companies use in their buildings?	6
3. How routers work?	7
4. How can a hacker take over tp-link WR841N's system?	8
References	17

“Despite the speed with which technology is coming into our lives, the level of cybersecurity hasn’t kept pace. Many employees have been working from home for the past two years, but the security of routers hasn’t improved over this time – they’re still rarely updated. Therefore, the risk that router vulnerabilities could be abused by cybercriminals remains a concern in 2022. What’s important is to prevent a threat as early as possible, since people usually find out about an attack when it’s too late – after money has been stolen,” comments Maria Namestnikova, Head of the Russian Global Research and Analysis Team (GReAT) at Kaspersky.

SCOPE

The aim of this research is to investigate how vulnerable the modern routers are. I will be taking advantage of the available resources that my school offers (ISSD), and I will try to use online open-source tools to hack the router. The whole process can take up to 3 weeks.

Main Question

What are the vulnerabilities in the tp-link WR841N router?

Sub Questions

- 1- What is the difference between router and modem?
- 2- What type of routers do big companies use in their buildings?
- 3- How routers work?
- 4- How can a hacker take over tp-link wr841n’s system?

My Plan

In this research, I will be using the DOT framework to answer my questions.











(<https://ictresearchmethods.nl/Methods>)

DOT framework consists of 5 strategies:

- 1- Library
- 2- Field
- 3- Lab
- 4- Showroom
- 5- Workshop

Each strategy offers several methods.

Here is my plan for this research:

  	
Sub Question	Methods
1 - What is the difference between router and modem?	 Available product analysis Community research Literature study
2 - What type of routers do big companies use in their buildings ?	 Interview
3 - How routers work?	 Available product analysis Literature study
4 - How can a hacker take over tp-link WR841N's system?	  Available product analysis Security test Unit test
<div>  <div>LIBRARY</div> <div>FIELD</div> <div>LAB</div>  </div>	

Results

1. What is the difference between router and modem?

- **Modem**

In research from Brain the internet uses **Analog signal** to send data, the computer can only read **Digital signal**. Therefore, we need a device that translates **Analog signal** to **Digital signal** and vice versa, here comes the modem.

The modem **demodulates** the incoming analog signals into digital signals for the computer to understand.

It also **modulates** the outgoing digital signals into analog signals for the internet to understand. (2021)

Modem is perfect to bring the internet for one device. However, connecting only one device to the internet is not realistic. Nowadays, people tend to have more than one device to connect to the internet.

Unfortunately, the modem was not built to connect to more than one device. Therefore, the router comes in.

- **Router**

Router is placed between the modem and the clients to manage the routing for the incoming and outgoing data.

It knows the Mac and the ip addresses for the devices, this would help it to organize the packets.

There are a few types for routers:

- **Wired Router**

Connects with the clients using wires.

- **Wireless Router**

Has wireless capabilities built-in. Most of these routers will also offer ports for wired connections as well.

- **Core Router**

Forwards packets to hosts within a network, but not between networks. (Ellis, 2022)

Conclusion

To sum up, the modem only gives the access to the internet, where routers route the packets to the right destination

2. What type of routers do big companies use in their buildings?

An interview with a cyber security specialist would help me to answer this question.

Interview

I decided to interview an intern that works for Surf in Utrecht.

The purpose of this interview is to give myself a good insight about routers from a cyber security experienced point of view.

I will aim to extract general information from him, as well as what kind of routers are they using at Surf.

Interviewer: Good afternoon, welcome to this interview and thank you for accepting the request. Can you please introduce yourself?

Mustafa: Good afternoon Mohammed, I am really glad to share my humble knowledge with you today. My name is Mustafa and I am doing my internship at Surf in Utrecht.

Interviewer: Great! Can you please tell us about the company and what it does?

Mustafa: Sure, Surf is a well-known company in The Netherlands that works in the technology industry. It tends to improve the quality of the education in the ICT industry.

Interviewer: I brought you today to talk about the router. What do you know about it in general? And have you worked with it?

Mustafa: Interesting topic, I do know the router and what it does, it simply makes the internet accessible for many devices at the same time. And yes, I have worked with many routers and I am using a Linksys one for my room.

Interviewer: Good choice. Now please explain to me how you use routers at Surf and what kind of routers do you prefer there?

Mustafa: At Surf, I have seen many routers that offer different services. In my office, I am using a D-Link that works as an access point for me and for the visitors to use. My boss uses a weird router from Google, but he says that it is the perfect router for him. And there is a room that has many Cisco routers that do not work as access points, they are just there if someone wants to use the internet using ethernet connection.

Overall, I think Surf has many more brands for routers and this is just what I have seen.

Interviewer: Thank you so much Mustafa for your time and for sharing this information with me.

Mustafa: You're welcome.

Conclusion

The interview illustrates how professional employees look at routers. I managed to get a general view about the usage of routers inside a big company (Surf).

3. How routers work?

Routers connect the Local Area Network devices with each other. It allows them to communicate with each other without having to travel to the outside internet.

Routers also connect the devices with the outer world, when requesting an online page, data packets are being sent from the client to the local router, then the router forwards the packet to the outer world using a public ip address, the data packets will go to the requested ip and get the web page for example from the destination router.

Kumar states that routers can have many vulnerabilities. Such as:

- Outdated VPN and multi-media functions
- Outdated Linux kernel in the firmware
- Presence of hardcore credentials in a plain text format
- Over-dependence on older BusyBox functions
- Use of weak default passwords, such as 'admin'
- Use of WPS
- Router Broadcasts the Model Number

(2022).

But do users actually care about these things?

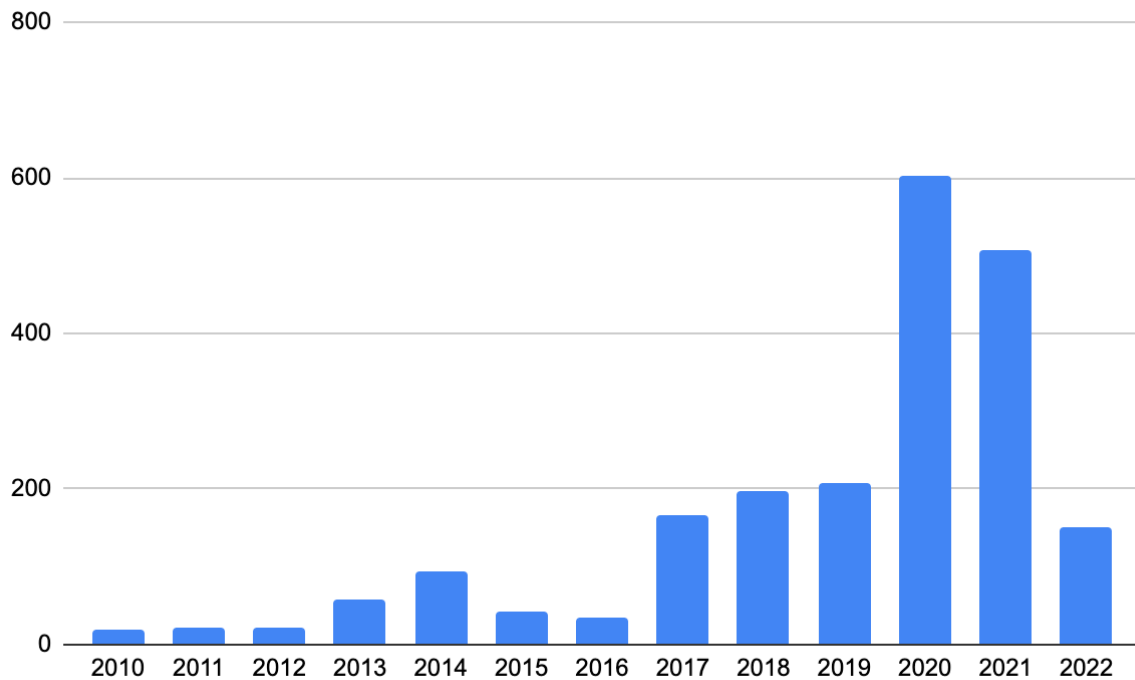
In research from Kaspersky, people rarely think about the security of their devices.

According to the research, 73% of users have never thought about upgrading or securing their router, making it one of the biggest threats impacting the Internet of Things today (2022).

The number of vulnerabilities found in routers increased sharply by almost 600 in the last decade. In 2021, around 500 vulnerabilities were discovered, 87 of them were critical.

Critical vulnerabilities are the most dangerous holes that gives the attackers the chance to get inside any system.

PVI



Number of router vulnerabilities according to <https://nvd.nist.gov>, 2010 – May 2022

4. How can a hacker take over tp-link WR841N's system?

I got a new tp-link WR841N router from ISSD, and I will showcase the steps to find the vulnerabilities that this router has.

I turned on the router and now I need to find its ip and mac addresses.

I will do a simple nmap scan on my network:

```
C:\Users\Admin>nmap 192.168.0.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-30 02:51 Arabian Standard Time

Nmap scan report for 192.168.0.1
Host is up (0.0019s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown
MAC Address: 30:B5:C2:22:5C:1C (Tp-link Technologies)
```

From this respond, I can tell that the target (router) has the following ip and mac addresses:

Target IP address: 192.168.0.1

Target MAC address: 30:B5:C2:22:5C:1D

PVI

Let me see whether I can ping it or not:

```
C:\Users\Admin>ping 192.168.0.1

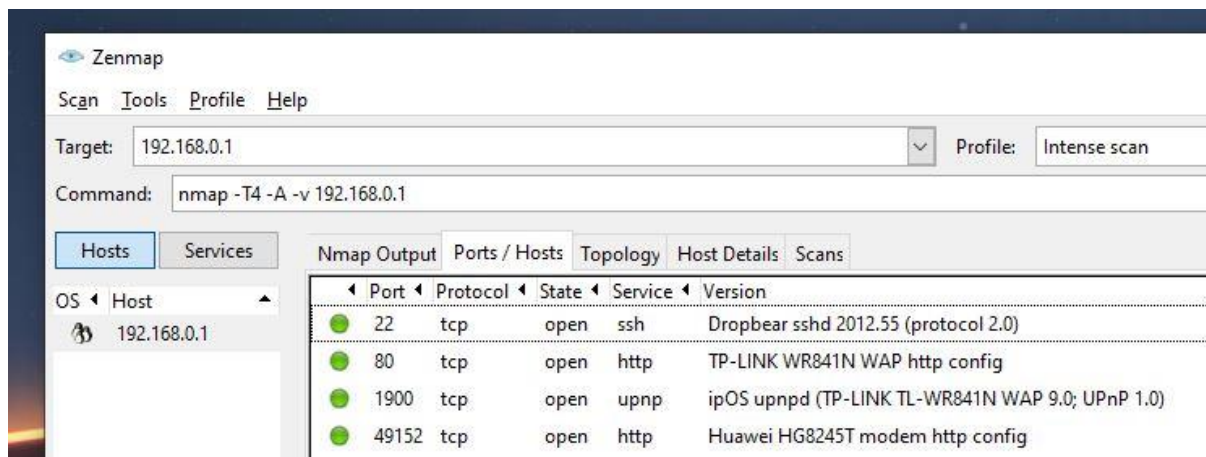
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Admin>
```

I can ping to the target router.

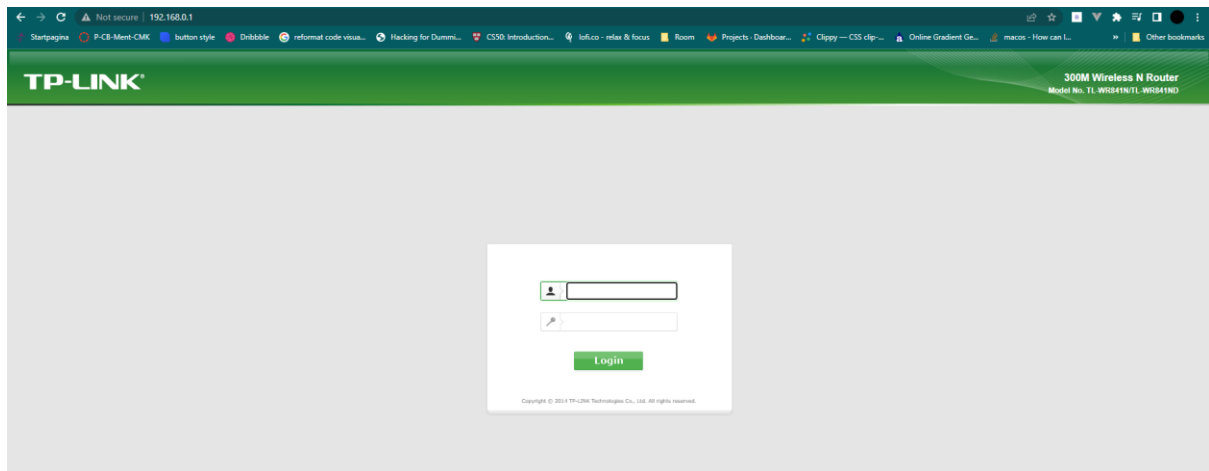
I also got that the target is running Linux operating system:



And it has 4 open ports.

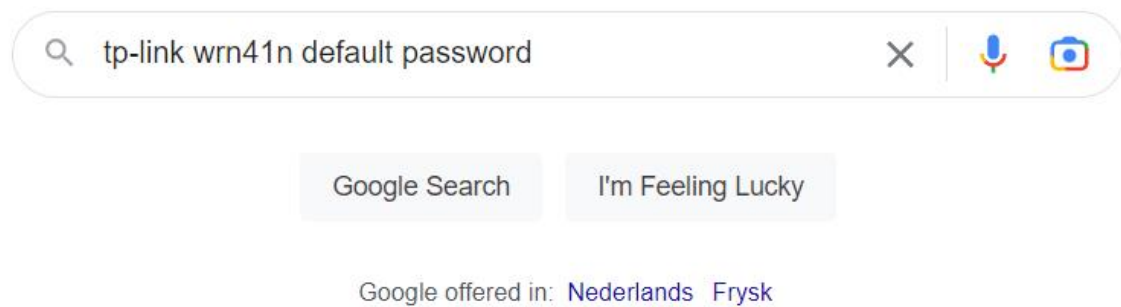
Let me try to take advantage of the open port 80 and see what is there:

PVI



I got this login page. I just need to find the credentials for this router.

Google can help me with this:



I got this page

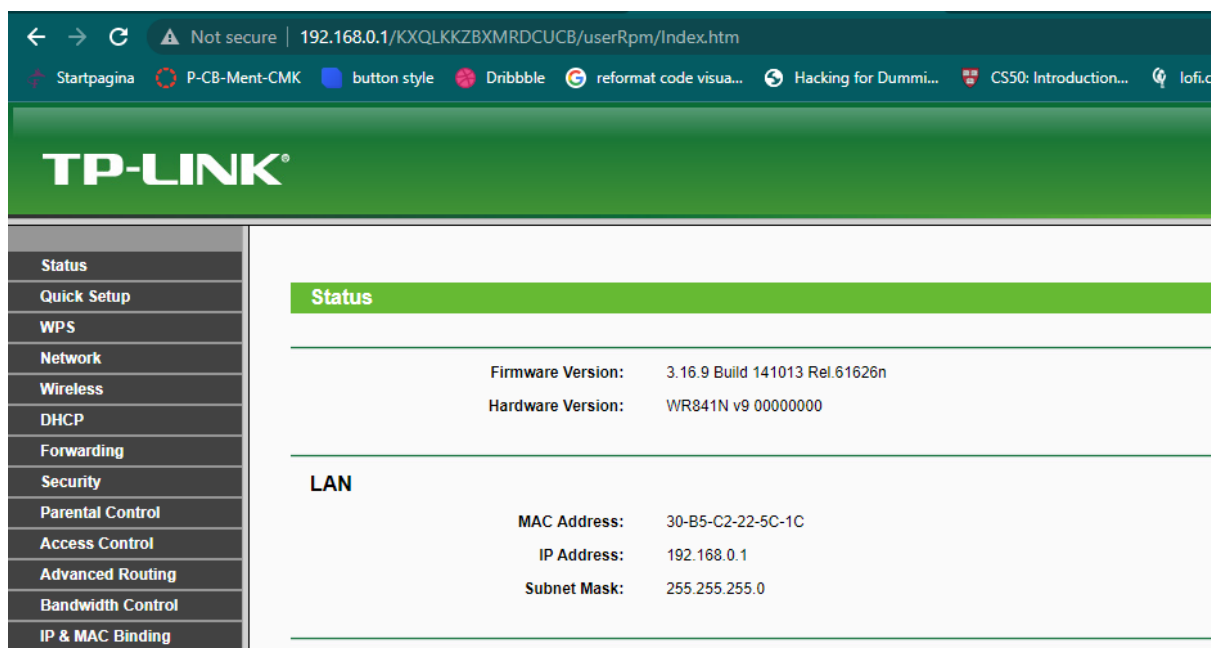
<https://www.192-168-1-1-ip.co/router/tp-link/tl-wr841n/8196/>

TP-Link TL-WR841N Login Guide

1. Open your web browser (e.g. Chrome, Firefox, Opera or any other browser)
2. Type **192.168.1.1** (the default IP to access the admin interface) in the address bar of your internet browser to access the router's web-based user interface.
3. You should see 2 text fields where you can enter a username and a password.
4. The default username for your TP-Link TL-WR841N is **admin**.
The default password is **admin**.
5. Enter the username & password, hit "Enter" and now you should see the control panel of your router.



Now let me to try these credentials to log in.



As you can see it worked, and now I can change any settings for the router.

Most users do not pay attention to changing the default credentials of the router.

To avoid this kind of hack, users need to change the credentials to strong usernames and passwords.

I also found this vulnerability

Nmap Output		Ports / Hosts	Topology	Host Details	Scans
	Port	Protocol	State	Service	Version
✓	22	tcp	open	ssh	Dropbear sshd 2012.55 (protocol 2.0)

It allows remote authenticated users to execute arbitrary code and bypass command restrictions via multiple crafted command requests, related to "channels concurrency."

How to fix it?

Upgrade the Debian version.

Routersploit

Routersploit is a tool that digs deep into the IoT devices to find vulnerabilities in them. It is a free open-source tool, and this is what I want to try against the router.

On their page in Github, I can download the tool:

<https://github.com/threat9/routersploit>

I installed the tool:

```

Installation on Kali Linux

apt-get install python3-pip
git clone https://www.github.com/threat9/routersploit
cd routersploit
python3 -m pip install -r requirements.txt
python3 rsf.py

```

I got the routersploit terminal and I entered this:

```

rsf > use scanners/autopwn
rsf (AutoPwn) > show info

Name:
AutoPwn

Description:
Module scans for all vulnerablities and weaknesses.

Devices:
- Multi

Authors:
- Marcin Bury <marcin[at]threat9.com>

rsf (AutoPwn) >

```

```
rsf (AutoPwn) > set target 10.89.206.108
[+] target => 10.89.206.108
rsf (AutoPwn) > run
```

I got this result:

```
[*] 10.89.206.108 Could not verify exploitability:
- 10.89.206.108:80 http exploits/routers/3com/officeconnect_rce
- 10.89.206.108:80 http exploits/routers/billion/billion_5200w_rce
- 10.89.206.108:23 custom/tcp exploits/routers/cisco/catalyst_2960_rocem
- 10.89.206.108:80 http exploits/routers/cisco/secure_acs_bypass
- 10.89.206.108:80 http exploits/routers/asus/asuswrt_lan_rce
- 10.89.206.108:80 http exploits/routers/dlink/dsl_2740r_dns_change
- 10.89.206.108:80 http exploits/routers/dlink/dsl_2640b_dns_change
- 10.89.206.108:1900 custom/udp exploits/routers/dlink/dir_815_850l_rce
- 10.89.206.108:80 http exploits/routers/dlink/dsl_2730b_2780b_526b_dns_change
- 10.89.206.108:80 http exploits/routers/shuttle/915wm_dns_change
- 10.89.206.108:80 http exploits/routers/netgear/dgn2200_dnslookup_cgi_rce

[-] 10.89.206.108 Could not confirm any vulnerability

[-] 10.89.206.108 Could not find default credentials
rsf (AutoPwn) >
```

It says that it could not confirm any vulnerabilities. However, there are chances that the router is vulnerable to one of the modules above. Therefore, I will be trying each one to find out.

Metasploit

Metasploit is an exploitation framework. It can be accessed using the CLI command:

```
Metasploit tip: Enable verbose logging with set VERBOSE true

msf5 > ls
[*] exec: ls

auxiliary encoders evasion exploits nops payloads post
msf5 > ping 8.8.8.8
[*] exec: ping 8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=104 time=1.36 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=104 time=1.48 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.363/1.424/1.485/0.061 ms
Interrupt: use the 'exit' command to quit
msf5 > 
```

Msfconsole also supports tab completion.

Metasploit offers modules that scan open ports on the target system. We can look at the available modules using this command:

```
msf5 > search portscan

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/http/wordpress_pingback_access  normal No    Wordpress Pingback Locator
1  auxiliary/scanner/natpmp/natpmp_portscan          normal No    NAT-PMP External Port Scanner
2  auxiliary/scanner/portscan/ack                    normal No    TCP ACK Firewall Scanner
3  auxiliary/scanner/portscan/ftpbounce              normal No    FTP Bounce Port Scanner
4  auxiliary/scanner/portscan/syn                    normal No    TCP SYN Port Scanner
5  auxiliary/scanner/portscan/tcp                    normal No    TCP Port Scanner
6  auxiliary/scanner/portscan/xmas                   normal No    TCP "XMas" Port Scanner
7  auxiliary/scanner/sap/sap_router_portscanner      normal No    SAPRouter Port Scanner

Interact with a module by name or index, for example use 7 or use auxiliary/scanner/sap/sap_router_portscanner

msf5 > 
```

Let us **show options** `auxiliary/scanner/portscan/tcp` for example.


```

msf5 > use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

  Name      Current Setting  Required  Description
  ----      -
  CONCURRENCY 10              yes       The number of concurrent ports to check per host
  DELAY       0               yes       The delay between connections, per thread, in milliseconds
  JITTER      0               yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds
  PORTS       1-10000         yes       Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS      <path>          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:
  THREADS     1               yes       The number of concurrent threads (max one per host)
  TIMEOUT     1000            yes       The socket connect timeout in milliseconds

msf5 auxiliary(scanner/portscan/tcp) >

```

- **CONCURRENCY:** Number of targets to be scanned simultaneously.
- **PORTS:** Port range to be scanned. Please note that 1-1000 here will not be the same as using Nmap with the default configuration. Nmap will scan the 1000 most used ports, while Metasploit will scan port numbers from 1 to 10000.
- **RHOSTS:** Target or target network to be scanned.
- **THREADS:** Number of threads that will be used simultaneously. More threads will result in faster scans.

I will try to scan the open ports against the target router using Metasploit.

```

msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.0.1
RHOSTS => 192.168.0.1
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

  Name      Current Setting  Required  Description
  ----      -
  CONCURRENCY 10              yes       The number of concurrent ports to check per host
  DELAY       0               yes       The delay between connections, per thread, in milliseconds
  JITTER      0               yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds
  PORTS       1-10000         yes       Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS      192.168.0.1     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  THREADS     1               yes       The number of concurrent threads (max one per host)
  TIMEOUT     1000            yes       The socket connect timeout in milliseconds

```

```

msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.0.1: - 192.168.0.1:22 - TCP OPEN
[+] 192.168.0.1: - 192.168.0.1:80 - TCP OPEN
[+] 192.168.0.1: - 192.168.0.1:1900 - TCP OPEN
[*] 192.168.0.1: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >

```

As seen above, Metasploit found 3 open ports which are 22, 80, and 1900.

Conclusion

In conclusion, this research managed to give a closer look about routers. Many vulnerabilities were found. Such as, open ports and default credentials. For further investigation, I would suggest targeting the firmware of the router itself. OS vulnerabilities are always there if you are looking at the right details.

References

- Ellis, J. (2022, August 22). *What Is A Router And How Does It Work?* Retrieved October 21, 2022, from <https://www.comms-express.com/blog/what-is-a-router-and-how-does-it-work/>
- *What is a router, and how does it work?* (n.d.). Retrieved October 26, 2022, from <https://us.norton.com/blog/iot/smarter-home-what-is-router>
- Brain, M. (2021, August 25). *How Modems Work*. HowStuffWorks.
<https://computer.howstuffworks.com/modem1.htm>
- Kumar, S. (2022, April 8). *Vulnerabilities in Modern Routers, Netgear, Cisco, Linksys, etc.* ReadWrite. <https://readwrite.com/vulnerabilities-in-modern-routers-netgear-cisco-linksys-etc/>
- Kaspersky. (2022, June 8). *87 critical vulnerabilities discovered in routers in 2021*. [www.kaspersky.com. https://www.kaspersky.com/about/press-releases/2022_87-critical-vulnerabilities-discovered-in-routers-in-2021](https://www.kaspersky.com/about/press-releases/2022_87-critical-vulnerabilities-discovered-in-routers-in-2021)
- *NVD - Home*. (n.d.). Retrieved October 28, 2022, from <https://nvd.nist.gov/>
- *GitHub - threat9/routersploit: Exploitation Framework for Embedded Devices*. (n.d.). GitHub. Retrieved November 6, 2022, from <https://github.com/threat9/routersploit>
- */ Penetration Testing Software, Pen Testing Security*. (n.d.). Metasploit.
<https://www.metasploit.com/>
- TryHackMe. (n.d.). *TryHackMe / Metasploit: Introduction*.
<https://tryhackme.com/room/metasploitintro>
- *CVE - CVE-2012-0920*. (n.d.). <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-0920>

- Offensive Security. (2019, November 1). *Scanner SSH Auxiliary Modules - Metasploit Unleashed*. <https://www.offensive-security.com/metasploit-unleashed/scanner-ssh-auxiliary-modules/>