**Personal Vulnerability Investigation**

Mohammed Nasser Alshukaili.

ICT, Fontys University of Applied Sciences.

Cyber Security, Semester 4.

2022

Contents

[**SCOPE** 3](#_Toc117985484)

[**Main Question** 3](#_Toc117985485)

[**How safe is it to only rely on routers to stay away from hackers?** 3](#_Toc117985486)

[**Sub Questions** 3](#_Toc117985487)

[1- What is the difference between router and modem? 3](#_Toc117985488)

[2- What are most popular routers used nowadays? 3](#_Toc117985489)

[3- How routers work? 3](#_Toc117985490)

[4- How can a hacker take over routers systems? 3](#_Toc117985491)

[**My Plan** 4](#_Toc117985492)

[**Results** 5](#_Toc117985493)

[**1.** **What is the difference between router and modem?** 5](#_Toc117985494)

[**3.** **How routers work?** 7](#_Toc117985495)

[**References** 12](#_Toc117985496)

“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**

### **How safe is it to only rely on routers to stay away from hackers?**

# **Sub Questions**

### What is the difference between router and modem?

### What are most popular routers used nowadays?

### How routers work?

### How can a hacker take over routers’ systems?

# **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:

Table

Description automatically generated

# **Results**

### **What is the difference between router and modem?**

* **Modem**

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.

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.

1. **What are most popular routers used nowadays?**

### **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.

They can have 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

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.

Chart, bar chart

Description automatically generated

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

1. **How can a hacker take over routers systems?**

I got a new tp-link router from ISSD, and I will showcase the steps to get inside the system.

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:

Text

Description automatically generated

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**

Let me see whether I can ping it or not:

Text

Description automatically generated

I can ping to the target router.

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

![Graphical user interface, table

Description automatically generated]()

And it has 4 open ports.

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

Graphical user interface, application, website

Description automatically generated

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

Google can help me with this:

Graphical user interface

Description automatically generated

I got this page

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

![Graphical user interface, text, application, Word

Description automatically generated]()

Now let me to try these credentials to log in.

Graphical user interface, application, website

Description automatically generated

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.

**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:

Text

Description automatically generated

I got the routersploit terminal and I entered this:

Text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

I got this result:

Text

Description automatically generated

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.

# **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>
* 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>
* *NVD - Home*. (n.d.). Retrieved October 28, 2022, from <https://nvd.nist.gov/>