Secure Home Network

First I wanted to check my public IP address which in windows command line is used this command:

```
C:\Users\Jake>nslookup myip.opendns.com resolver1.opendns.com
```

I then went onto my kali linux virtual machine to perform an nmap scan on my own public IP address to see if it had any open ports i could be vulnerable to

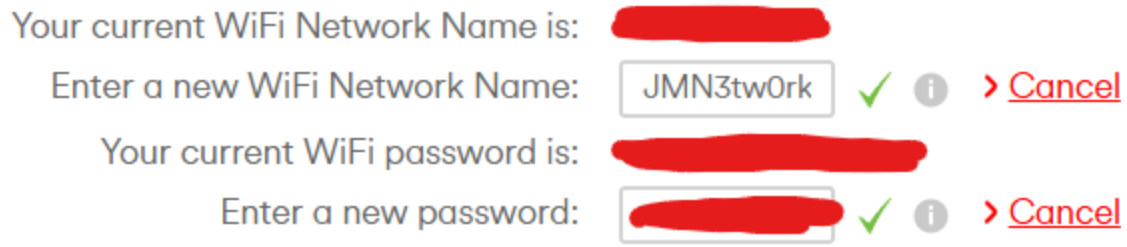
```
┌──(jakemallaby㉿HackingPractice)-[~]
└─$ sudo nmap -sS [redacted] -F
Starting Nmap 7.92 ( https://nmap.org ) at 2026-01-17 09:55 GMT
Nmap scan report for cpc1-cmbg20-2-0-[redacted]
Host is up (0.014s latency).
All 100 scanned ports on cpc1-cmbg20-2-0-[redacted] are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 2.01 seconds
┌──(jakemallaby㉿HackingPractice)-[~]
└─$ sudo nmap -sS [redacted] -T4
Starting Nmap 7.92 ( https://nmap.org ) at 2026-01-17 09:58 GMT
Nmap scan report for cpc1-cmbg20-2-0-[redacted]
Host is up (0.00087s latency).
All 1000 scanned ports on cpc1-cmbg20-2-0-[redacted] are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

No ports are listed which is a good sign to see that there are no potential ports that could be exploited

I did 2 scans 1 was a fast scan to test the top 100 common ports then I conducted a second T4 aggressive scan to test the top 1000 ports.

Securing the Network

I went on the admin page for my router and changed the network name and password



I changed the network name so passers by cannot identify the provider and do any sort of drive by attacks and then changed the password that came with the router even though it was secure I changed it for extra hardening.

Port Forwarding

I then looked more on my networks admin page and checked that there was no port forwarding set up as we don't want to leave port holes within the network

Local		External			
IP address	Port range	Port range	Protocol	Enabled	Delete
No forwarding rule applied!					

Firewall

I Made sure the firewall is active and that this does not allow respond to pings as if someone pings a public ip we dont want our device to respond so it doesnt show up if an attacker pings the public IP address.

This page allows the configuration of firewall options.
It is recommended that firewall protection is always enabled.

IPv4 firewall

Firewall protection	☑ Enabled
Block fragmented IP packets	☐ Enabled
Port scan detection	☑ Enabled
IP flood detection	☑ Enabled

Wireless security

checked my wireless to make sure that it was using a the best security protocol and noticed that there was a WPA3 option over the WPA2 option that was already selected

Security: WPA2-PSK

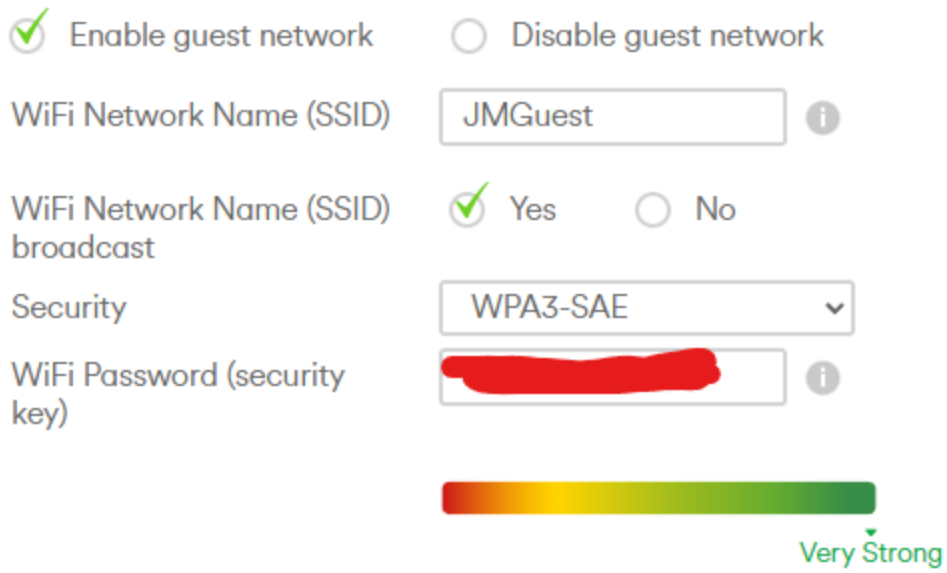
WiFi password (security key)

- Disabled
- WPA2-PSK
- WPA3-SAE
- WPA2-PSK/WPA3-SAE

so I changed to WPA 3 as this is a more secure standard for WiFi security

Guest Network

I configured a guest network as this feature was off then gave a name and set its security and password.



Having a guest network within your home network is essential to make sure friends devices are isolated from the core network as no one knows if their devices are secure. We don't want their devices interacting with the core so its best to separate them for best security practices.