

Introduction

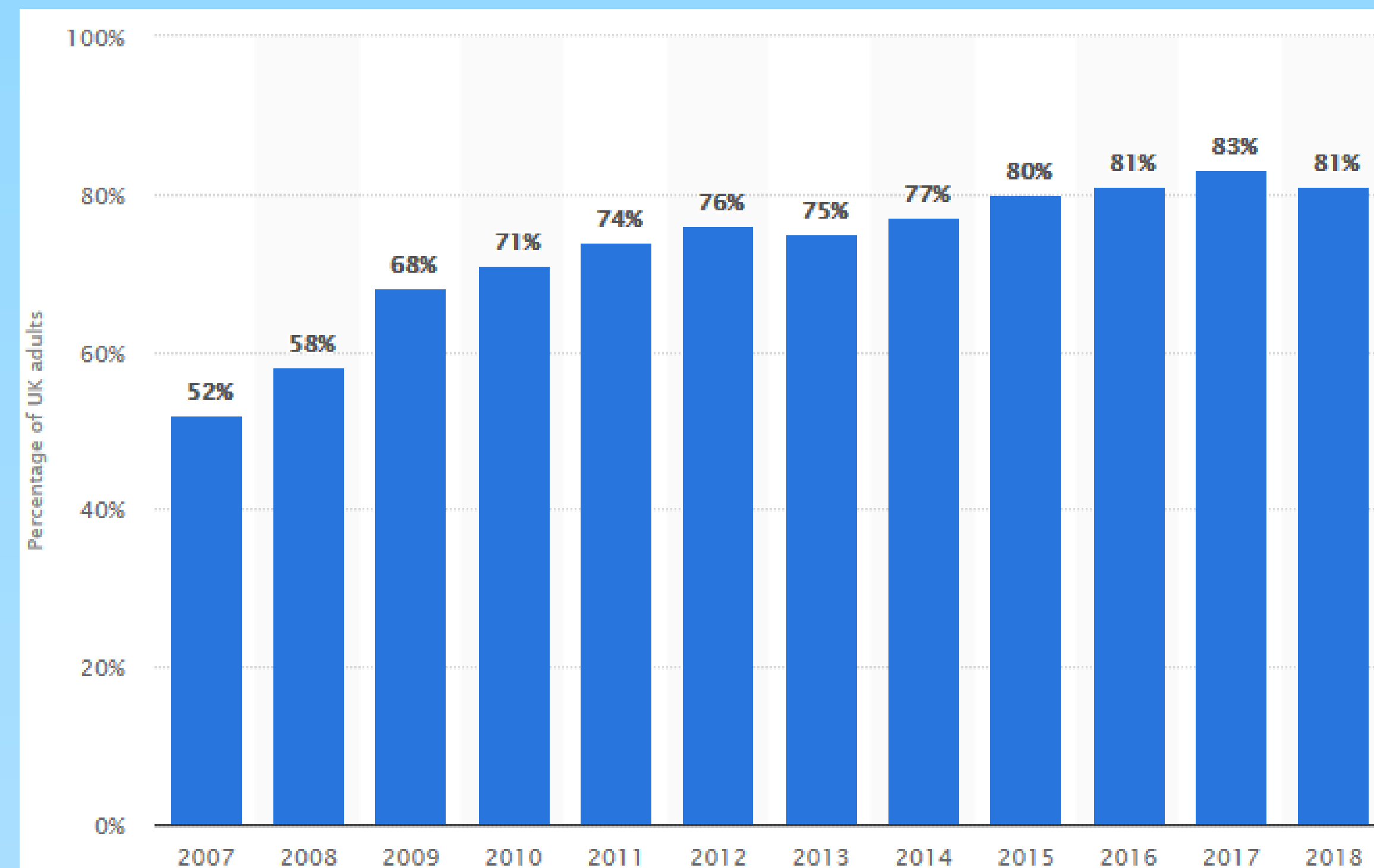
The home network has, over the past decade, become a permanent and required utility in the large majority of British homes and becoming an essential to said homes. That being said, despite this reliance and requirement of the internet access a home network provides, users do very little to secure it, usually only wanting the internet access it provides, and caring not at all for the security concerns that accompany this thought process. This lack of foresight on the dangers of a relatively unsecured home network can lead to all manner of attacks to be carried out against it. This inherit danger will only grow as networking becomes more predominant with devices such as the Internet Of Things becoming more popular and invasive. Therefore this project aims to *secure* a home network environment to the degree without sacrificing the ease of use descriptive of a home network environment.

Implementation Methodology

Of course, as part of the securing of the home network, some changes had to be made to the actual router itself. While some of these changes made aren't effective in later testing, in a real-life scenario they would be. The implementations put in place were;

- Installation of DD-WRT custom firmware
- Hiding and changing of the Service Set Identifier
- Changing all access points to WPA2 protocol
- Changing of passwords both access point and admin access to unique passwords following guide in documentation.
- Creation of Guest networks to segment network
- Activation of Stateful Packet Inspection Firewall
- Disabling of WPS authentication
- Creation of MAC filter list
- Deactivation of Dynamic Host Configuration Protocol and use of static routing to replace it
- Disabling of all remote access features
- Enabling of HTTPS when accessing router
- Checking for firmware updates
- Disabling of Universal Plug and Play
- Limitation of signal strength outside house

While some of these may have an effect on the following tests, some don't, but all of them help improve the security of an otherwise insecure network.



Number of UK homes with home broadband circa 2018 [3]

Testing Methodology

Once the implementation of the security tools and methods was put in place, it would then be tested against real-time commonly used attacks against home network environments. This physical testing environment consists of a singular home router and two devices, an attacking and defending device, with internet access depending on the attack. This better secured router was then attacked via three different methods, these three attacks tested against said home network are; A wordlist attack, a Man in the Middle attack and a denial of service attack. Each of these attacks were done via software available within Kali Linux to show that these attacks can be easily done using free accessible software, while the router itself is running the DD-WRT custom firmware, also freely and easily available. To be more specific, the software used for the Wordlist attack was 'Fern Wi-fi Cracker', the MITM attack was carried out via 'Websploit' and the DOS attack was done by using Metasploit, while all three attacks saw usage of Nmap for it's network scanning capabilities.



Testing Equipment Used

Results

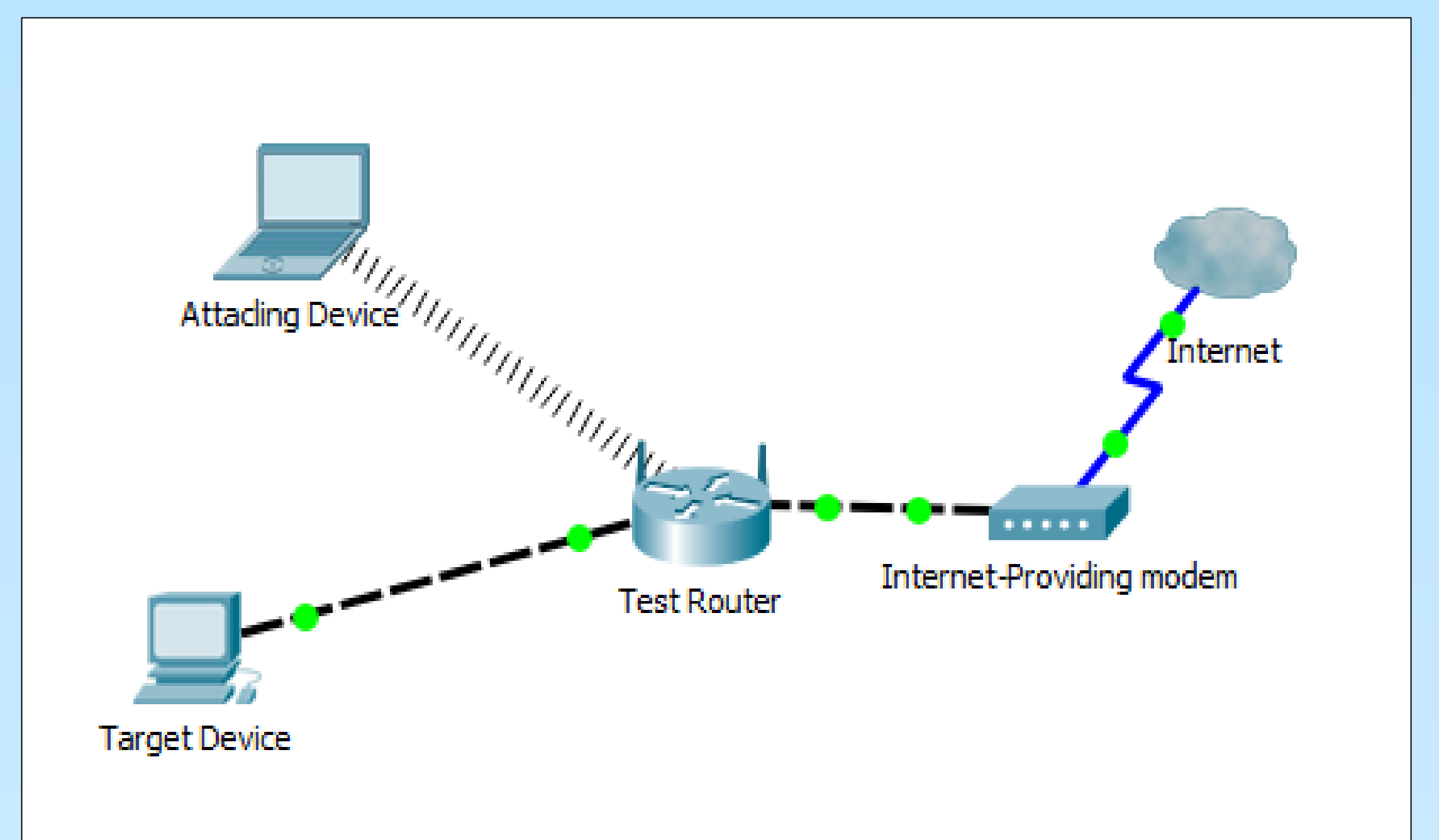
The result of the tests differed depending on the attack. Starting with the password/ Wordlist attack, this attack uses a large text file with hundreds of thousands of possible passwords to 'crack' it. When using a password of "Password1", the attack took ~4 hours to crack, on the other hand the password of "P@s5w0rd1", that is closer to the guidelines given in the associated documentation of this poster, took more than seven days, an exact amount couldn't be determined due to the computer trying to crack it froze on the seventh day. Important to note is that the wordlist attack wouldn't work against the more secure latter password due to lack of words or commonality that is required for wordlist attacks and as such a hashing attack was carried out instead, hashing being a simpler way of trying out *every perceivable possibility*. Suffice to say the network with such a password or similar on it's access points should more than suffice for home security.

The Man in the Middle is an attack by which the target's connection is intercepted and relayed by the attacker, meaning the target device should have no idea it is being intercepted. This attack requires network access to work correctly, but given this is a testing scenario, the password need was waived. Anyway, the MITM attack was relatively successful, barring the use of clientside VPNs and HTTPS, both of which did reduce the amount of data intercepted by the attacking MITM device, the Virtual Private Network especially so. This being said, the only results incepted from the defending device were URLs those of which were using the HTTP protocol, which (un)luckily are quite few and far between, not to mention the use of The HTTP Strict Transport Security that is in most internet browsers nowadays such as Firefox and Chrome. What this protocol does is help defend against SSLstripping, a technique of which helps bypass HTTPS by redirecting it to the HTTP version, allowing for the attacking device to read the newly intercepted redirected version.

The third and last attack was a Denial Of Service attack, while not as well known as the similar Distributed DOS attack, it is none-the-less well known to the average person. The aim of this attack is to spam the target with a large number of information packets in order to bring it down, how it does this is dependent on the type. While the attack was performed in-network to maximize the effect, the attack was successful to a degree, but not successful enough to fully use up the networking resources on the target device, as is the method of a SYN flood DOS attack. Well this was likely due in part to bandwidth limitations on a wireless medium, it was also due to the router having an Stateful Packet Inspection firewall, helping to reduce the amount of SYN packets that were able to reach the targeted device and therefore reducing the effectiveness of the attack.

Conclusions

In conclusion, the test attacks were successful to a degree, but not enough to fully work. Bear in mind for these tests to actually be performed some requirements were waived, it is highly likely that the MITM an DOS attack wouldn't get to this stage in a real-life scenario. Therefore, while there are more than enough ways to further secure the home network against attacks, be it on an ISP provided router or third party, most of which are available to the average home user. The biggest factor towards *why* home networks are at such risk is largely due to the attitude of said users, preferring to take a responsive approach rather than the far safer preemptive approach to security. If anything, both the lack of knowledge in the area and belief that the company that provided the router has added sufficient security beforehand, tend to be the biggest reasons for unsecure or default security within a home network router. So, while there are many security features and tools that can be used to secure a network, it is ultimately left up to the user to know the risks of an unsecured network and to take action, for which there are hundreds of guides online as well as the associated documentation for this poster board.



Logical Testing Network Diagram

References

- {1}- N. Publications, "Security Tip (ST15-002) Home Network Security," *US-Cert.gov*, 2018. [Online]. Available: <https://www.us-cert.gov/ncas/tips/ST15-002>.
- {2}- Symtanec, "Internet Security Threat Report Volume 23," 2018.
- {3}- Statistica, "Broadband Penetration in the UK." [Online]. Available: <https://www.statista.com/statistics/272228/broadband-penetration-in-the-united-kingdom-uk/>.