

Implementing a Secure Network Solution for Home and Organisational Use

Introduction

The main focus of this report is to provide an in-depth overview on how to implement a secure network whilst containing and maintaining measures such as creating, testing, updating and redeploying.

The creation of the network will look into fundamentals such as simulations, equipment, resources and the overall cost.

The testing of the network will look at key features such as penetration, security and its measures, efficiency, flexibility and scalability.

Testing & Evaluation

An ARP Scan was one of the network attacks chosen as it shows the vulnerability of router security issues that are not configured initially to provide ultimate protection of a network and its devices allowing for unauthorised user to gain information on devices and target them individually for various different gains.

Kali Linux's ARP Scanning tool was used.

Below is a scan completed on the authors home network, showing the devices connected to the router as well as their network addresses.

```
Report bugs or send suggestions at https://github.com/royhills/arp-scan
See the arp-scan homepage at https://github.com/royhills/arp-scan
root@kali:/home/kali# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:1f:30:76, IPv4: 10.0.2.15
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.2    52:54:00:12:35:02    QEMU
10.0.2.3    52:54:00:12:35:03    QEMU
10.0.2.4    52:54:00:12:35:04    QEMU

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.488 seconds (102.89 hosts/sec). 3 responded
root@kali:/home/kali#
```

Aim & Objectives

The aim of this project is to be able to implement a secure network for home and organisational use whilst considering vulnerabilities and how to overcome them whilst providing an analysis of both types of networks.

- Analysis of historical, current and future network infrastructure and trends
- Constructing an evaluation assessment of risks and issues related to constructing a network and providing successful resolutions
- Design and creation of networking environments in simulation and physical locations
- Research into threat identification and providing security measures for data protection within a network
- Ethically attempt to attack a network device via an unauthorised method
 - Analysis of penetration testing

Research Overview

What makes a feasible network?

- Quality of Service
- Ability for Scalability
- Complete Security
- Ease of Maintenance

Common Network Types

- Local Area Network (LAN)
- Wireless Local Area Network (WLAN)
- Wide Area Network (WAN)

Cybersecurity Issues

- Information & Network Security
 - Denial of Service (DoS)
 - Sniffing & Spoofing
 - Hackers
- Organised Crime Syndicates
 - Disgruntled Insiders

Conclusion

To conclude this project report and its chapters, the main focus was to arise issues that are faced by network users in terms of cybersecurity and network security related issues that comprehend a user from having an effective, usable network for daily use.

Overall, this project is able to display the security issues that come with the creation of a network in the environments stated above.

The different types of networks have been looked at in relation to the given environments and recommendations were provided on the different types of attacks that can occur against such networks with plans on how to prevent or reduce the risk of them happening.

Recommendations

For further research within this area of study, different types of network related attacks such as data mining and information gathering can be executed to gather data on a network users' area and attack them to discover files and other documents.

References

- [1] A. D'Amico and A. Whitley, "The Real Work of Computer Network Defense Analysts," Springer, Berlin, 2008.

Design & Implementation

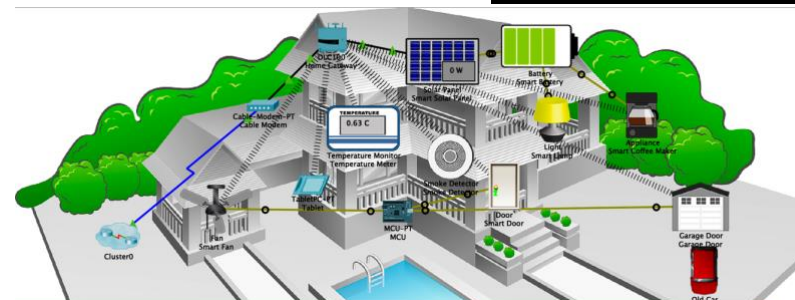
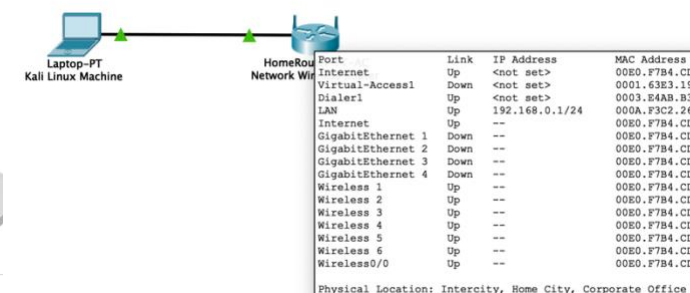


Figure 1 - Smart Home Network



Port	Link	IP Address	MAC Address
Internet	Up	<not set>	00E0.F7B4.CD01
Virtual-Access1	Down	<not set>	0001.63E3.19EC
Dialer1	Up	<not set>	0003.E4AB.B399
LAN	Up	192.168.0.1/24	000A.F3C2.26CB
Internet	Up	--	00E0.F7B4.CD01
GigabitEthernet 1	Down	--	00E0.F7B4.CD02
GigabitEthernet 2	Down	--	00E0.F7B4.CD03
GigabitEthernet 3	Down	--	00E0.F7B4.CD04
GigabitEthernet 4	Down	--	00E0.F7B4.CD05
Wireless 1	Up	--	00E0.F7B4.CD06
Wireless 2	Up	--	00E0.F7B4.CD07
Wireless 3	Up	--	00E0.F7B4.CD08
Wireless 4	Up	--	00E0.F7B4.CD09
Wireless 5	Up	--	00E0.F7B4.CD0A
Wireless 6	Up	--	00E0.F7B4.CD0B
Wireless0/0	Up	--	00E0.F7B4.CD0C

Physical Location: Intercity, Home City, Corporate Office

Figure 2 - ARP Scan

A typical smart home network would consist of devices such as a server, router with wireless and wired capabilities, smart devices, computer system. Figure 1 above displays a typical home layout of smart devices connected to a single WLAN network.

Figure 2 displays the design of an ARP Scan network attack and the typical information discovered from this attack; where a router is attacked to display all connected user devices and their network addresses.