

1. Introduction

Corporate data has become an essential aspect for businesses. The reason is that attackers can comprise company's sensitive data. Security has appeared to be a massive issue for many companies due to lack of safety and protection.

As there is little knowledge given to students and others who are interested in security, the author provides an extension to display the vulnerabilities a network may have.

2. Aim & Objectives

➤ Run experiments based on high level security attacks/threats in an ethical hacking environment. The author devises a set of objectives to support the aim and to maintain a steady procedure for the project to advance into succession;

- Evaluate relevant literature
- Review various threats and attacks such as Malware (Eavesdropping, Data Modification, Trojans etc.)
- Practice the use of Kali Linux distribution (Pen testing usage)
- Attempt ethical hacking techniques
- Password cracking on WLAN networks (WPA2)
- Port scanning to analyse various vulnerabilities on a network

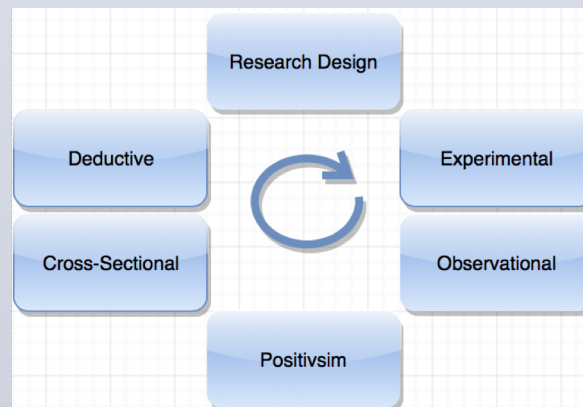
3. Research Literature & Methodology

The author conducted various academic literature which is known as Related Works, this was conducted to support the hypothesis. It demonstrates the how the author understands the field in which they are research and has allowed them to position the project into context. Some of the related works are shown below;

- *Evaluation of portable penetration testing on smart cities applications using Raspberry Pi iii [1]*
- *Faster detection and prediction of DDoS attacks using MapReduce and Time Series Analysis [2]*
- *Man-In-The-Middle attack in Wireless and Computer Networking [3]*
- *Advances in Password Cracking and Countermeasures in Computer Security [4]*

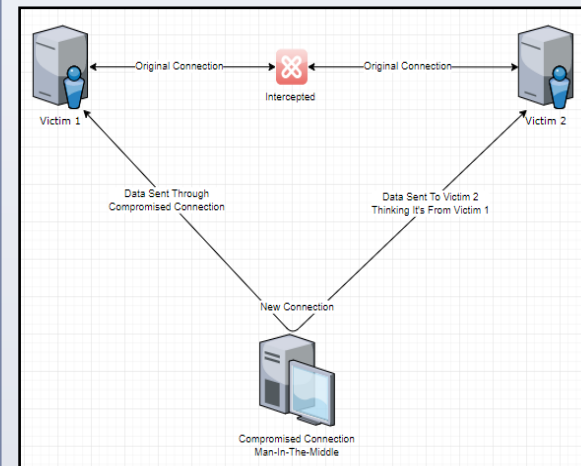
4. Methodology & Research Design

The concept of research design refers to the idea of the way that the research is yet to be constructed. It alludes to a systematic method that incorporates the distinctive parts of a hypothesis.

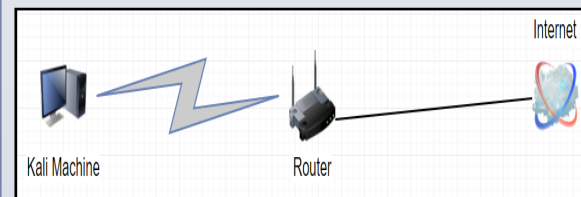


5. Design & Implementation

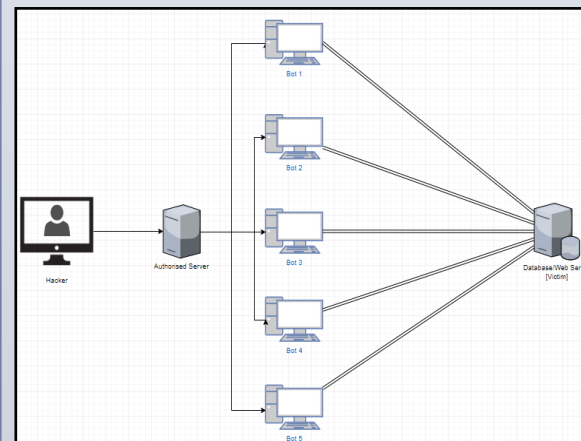
Conceptual designs will require the creation of a blueprint of multiple designs relating the infrastructure of the implementations needed.



Man-In-The-Middle



WPA2 Cracking



DDoS Design Model

6. Results & Findings

Below the author provides the results of the implementations below;

```

root@kali: ~
File Edit View Search Terminal Help

Aircrack-ng 1.2 rc4

[00:00:17] 24740/31147 keys tested (1430.57 k/s)

Time left: 4 seconds 79.43%

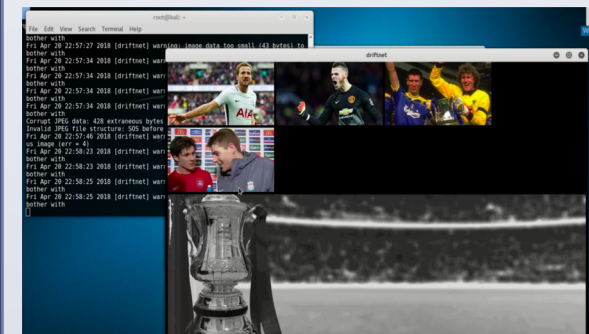
KEY FOUND! [ setting_breakpoint ]

Master Key : 42 23 F1 86 09 CD 53 3B 8A 98 8F 81 53 CF ED 6F
            AA BA CB 0F 1B 63 49 E2 11 6F 15 47 E9 05 F7 C4

Transient Key : 4D F8 56 05 51 62 DE 6D 7A 6E 80 F7 2C 59 F6
               84 96 F3 67 FE D3 40 7F EE C1 A9 4D B6 C3 77 ED
               4E BF 9F 7D 8E FD B1 BE FC AA 6F 8A 24 22 A8 E1
               05 CB D9 13 61 22 43 E4 6B 4E 1F 5C C9 1A 21 B8

EAPOL HMAC : DC 6A FD F4 BC B9 69 B9 9D 94 0E 25 40 75 F0 BA

WPA2 Cracked
  
```



MITM Content Captured

7. Conclusion

The author demonstrates multiple attacks to illustrates the vulnerabilities within a networking infrastructure. The display of high level attacks approached the project with a substantial closure.

References

- N. B. Al Barghuthi, M. Saleh, S. Alsuwaidi, and S. Alhammadi, "Evaluation of portable penetration testing on smart cities applications using Raspberry Pi III," in *2017 Fourth HCT Information Technology Trends (ITT)*, 2017, pp. 67–72. [1]
- V. Maheshwari, A. Bhatia, and K. Rai, "Faster detection and prediction of DDoS attacks using MapReduce and time series analysis," in *2018 International Conference on Information Networking (ICOIN)*, 2018, pp. 556–561. [2]
- B. Bhushan, G. Sahoo, and A. K. Rai, "Man-in-the-middle attack in wireless and computer networking — A review," in *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall)*, 2017, pp. 1–6. [3]
- A. L.-F. Han, D. F. Wong, and L. S. Chao, "Password Cracking and Countermeasures in Computer Security: A Survey," *arXiv Prepr. arXiv1411.7803*, 2014. [4]