Penetration Testing Using a Triangular Approach

Jordan Christian, jachris 15@earlham.edu
Earlham College Department of Computer Science
Richmond, Indiana, 47374

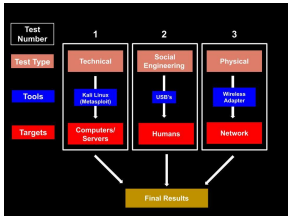
As we move farther along into the 21st century, securing computers has become more vital than ever. Daily, hackers around the world attempt to breach devices and steal important data. Penetration testing is a method by attacking the integrity of a network and reporting the findings to the owner of that network. However, penetration testing can be expensive. We tried to develop a method by which small organizations could develop their own testing and in turn strengthen their security to protect their data.

Motivation

- Security is essential to protect the data of a company
- Penetration testing is expensive
- Needed to be a better way to make these types of tests available to small scale organizations
- Current testing approaches focus solely on technical aspects and not physical or social engineering

Design & Implementation

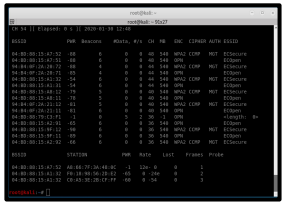
- Three separate tests were conducted to fully test the integrity of the system at Earlham college



- Results of each test were put into a written report
- This report was given to the appropriate people for them to make changes

Physical testing using WiFi Adapter

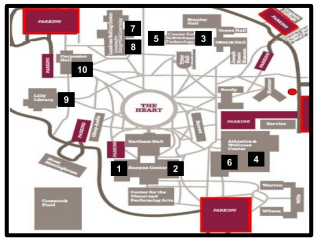
- Using Kali Linux and a wireless adapter, tests were conducted to try and gain access to information under a secure network



- This was done on a virtual machine not connected to any WiFi network

Social Engineering

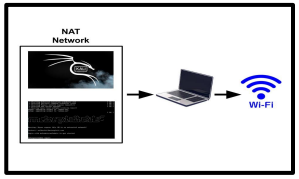
- USB's were placed around campus for deception. This was done to try and entice others to pick and use them



- Upon opening, there was a text file explaining the purpose of this project
- Participants were asked to fill out a survey to explain their awareness of hacking

Technical testing using VirtualBox

- Virtualization was needed for this part of the experiment. Kali and Metasploit servers were operating under the same NAT network



- Kali is able to use known exploits to attack a server
- Similar tests can be done on one's own server

Future Work

We wanted our work to be reproducible for use by other companies. Future work would include testing other businesses in our local area.

Acknowledgements

I would like to thank Dr. Charles Peck, Dr. Xunfei Jiang, Mr. Craig Earley, Mr. Jason Elliot, and Mr. Byron Roosa for providing varying levels of support for this project.

*This poster is based on work described in "Penetration Testing Using a Triangular Approach", Jordan Christian, available at https://portfolios.cs.earlham.edu/index.php/author/jachris15/