Strategies of Ethical Hacking and Penetration Testing

Adam Lee¹, Timothy Randhir²

1. Student: Springfield Technical Community College, Springfield, MA
2. Mentor: Professor, Springfield Technical Community College, Springfield, MA

Introduction

The digital age has brought up new issues and vulnerabilities to personal and professional information. With computers networked into almost every object, information is accessible anytime and anywhere. This access also allows outsiders to access without authorization. From 2014 to 2018, the total financial loss from cybercrime throughout the world increased from $8 million to $2.7 billion. The average cost of a data breach was $3.92 million in 2019 for a business, and an average of 279 days is spent to detect a breach. There is a need for proactive methods to prevent cybercrime. This study evaluates the use of ethical hacking to protect networks from cybercrime.

Methods

- A review of literature will be used to study the increase in cyber crime and to identify the potential of ethical hacking and penetration testing.
- Review the principle and theory of ethical hacking and determine pros and cons.
- Discuss how and why ethical hacking is an effective approach to deter cybercrime.

Results

1. Cross-site Scripting
2. SQL Injection
3. Buffer Overflow
4. Information Disclosure
5. SQL Injection
6. Cross Site Request Forgery

Discussion

The first documented case of “hacking” was back in the 1970’s when computerized phones were becoming targeted. Since then it has shown that the more complex the system is, the more susceptible and vulnerable to cybercrime they became. In 2020, a cybersecurity firm, Trustwave, uncovered a backdoor malware named “GoldenSpy” that was embedded in mandatory Chinese tax software suites that foreign companies, doing business in China, must use to pay their taxes. By way of social engineering, Twitter had a major breach in their systems and hackers were able to swindle numerous individuals of roughly $120,000 using Twitter. Cybercriminals posed as Amazon employees to steal money and personal information from unsuspecting customers. These two examples were accomplished not by attacking the system, but rather by exploiting one of the only open-ended variables in the equation, the human factor.

Conceptual model

1. Gather Data
2. Exploit
3. Report

Advantage

- Helping in closing the open holes in the system network
- Provides security to banking and financial establishments
- Prevents water leak events
- Fight against terrorism and criminal security breaches
- Having a computer system that prevents cybercriminals from gaining access

Disadvantage

- All depends upon the trustworthiness of the ethical hacker
- Hiring professionals is expensive
- The ethical hackers that know the knowledge they gain to do malicious hacking activities
- Allowing the company’s financial and banking details to be seen by malicious security breaches

Conclusions

Cyber crime is predicted to increase exponentially. A proactive approach to counter security is needed and reactive security measures are not enough. Ethical hacking fills that void.

Acknowledgements

I want to thank STEM SSA Director Dr. Reena Randhir and DHE for the encouragement and support. I also want to thank all the staff and guest speakers that shared their time and expertise.