International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Penetration Testing Toolkit

Sandhiya R

Dr MGR Educational and Research Institute , Maduravoyal, Chennai-600095, India

ABSTRACT

Cyber security is a collection of defensive techniques in order to protect electronic devices, servers, computers, networks, databases, mobile phones and more, from malicious attacks and hackers.Here we develop a software which is collection of penetration testing tools. It is a collection of independent programs that test vulnerabilities on different areas like computer systems, files, and websites. The application will be a desktop app aiming to work on Windows operating system

Keywords: Python, Penetration Testing, Cyber security

1. Introduction

1.1 Penetration Testing

Pen-testing can help prevent this by providing very valuable information, enabling an organization to always be one step ahead. Apart from identifying any possible vulnerabilities pen-testing can lead to a ranking between them, helping the organization prioritize measures against those with the higher risk of being exploited and also the higher chances of causing harm. There are various cases where certain organizations had to pay huge amounts of money in law-suits and recovery efforts, after their systems have been breached. Apart from the revenue, an organization’s credibility greatly depends on how secure its users’ information.

1.2 Proposed System

The process of pen-testing usually involves a security expert who tries to gain unauthorized access with various ways in an information system. To do that, the expert employs automated, manual (and sometimes both) tools in order to identify possible vulnerabilities in different parts of the system. In this various other tools are combined to form a collective penetration testing that can be done using the windows. Tools are easy to access and gain the targeted information without a long time taken.

1.3 Proposed System Advantages

There are various cases where certain organizations had to pay huge amounts of money in law-suits and recovery efforts, after their systems have been breached. Apart from the revenue, an organization’s credibility greatly depends on how secure its users’ information is. Pen-testing can help prevent this by providing very valuable information, enabling an organization to always be one step ahead.Apart from identifying any possible vulnerabilities pen-testing can lead to a ranking between them, helping the organization prioritize measures against those with the higher risk of being exploited and also the higher chances of causing harm

2. System Design And Developement

In this by using the codings and the commands the software is developed. Each tools have inbuild working process. By giving value inputs to the toolsoutputs can be gained. Python language is the base which is used to develop the software.

* *Sandhiya R*
E-mail address: sandhiyaravi1117@gmail.com

3 .Existing System

Penetration Testing is the process of identifying security vulnerabilities in an application by evaluating the system or network with various malicious techniques. The weak points of a system are exploited in this process through an authorized simulated attack.The purpose of this test is to secure important data from outsiders like hackers who can have unauthorized access to the system. Once the vulnerability is identified, it is used to exploit the system to gain access to sensitive information.

Existing System Disadvantages

Penetration testing can be very complex and expensive. You have to determine the test conditions and scope that are worth the risks and resources associated with this tactic.If you wish to conduct a penetration test on your entire network and infrastructure, however, you'll need to make sure your pentesters are prepared to explore every aspect of your IT. This takes even more effort, detail, and resources.At the same time, some businesses plan too heavily for a penetration test. Real cyberattacks occur with little to no warning. Make sure your network and systems face the most realistic test conditions possible for the most accurate results.

3. Conclusion

Thus the penetration testing toolkit can be successfully developed using the python. Which includes many tools which are combined in a single source which can be usefull for penetration testing.

REFERENCES

Bacudio, A., Yuan, X., Bill Chu, B. and Jones, M., (2011) . [Book] An Overview of Penetration Testing. *International Journal of Network Security & Its Applications*, 3(6), pp.19-38. (online) Available at: https://www.researchgate.net/publication/274174058_An_Overview_of_Penetration_Testing
[Accessed 18 April 2021]

Cyber Security Services (Sep, 2019). *The Purpose of Cybersecurity Services.* (online) Available at: https://globalcybersecurity.medium.com/the-purpose-of-cybersecurity-services-30d2baddd62c
[Accessed 20 April 2021]

Galov, N., (Feb, 2021). *40 Worrisome Hacking Statistics that Concern US All in 2020.* (online) Available at: https://hostingtribunal.com/blog/hacking-statistics/#gref
[Accessed 20 April 2021]

Phong, C., T., (Oct, 2014). [PDF] *A Study in Penetration Testing Tools and Approaches.* (online) Available at :
http://openrepository.aut.ac.nz/bitstream/handle/10292/7801/ChiemTP.pdf?sequence=3&isAllowed=y
[Accessed 20 April 2021]

Sobers, R., (Mar, 2021). *134 Cybersecuriy Statistics and Trends for 2021.* (online) Available at: https://www.varonis.com/blog/cybersecurity-statistics/
[Accessed 20 April 2021]