IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 11, November 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311040|

Ethical Hacking and Web Security: Approach Interpretation

Sunil J, Darshan A N, Harshithgowda S

Assistant Professor, Department of Computer Science and Engineering, CIT, Gubbi, Tumkur, Karnataka, India

U.G. Student, Department of Computer Science and Engineering, CIT, Gubbi, Tumkur, Karnataka, India

U.G. Student, Department of Computer Science and Engineering, CIT, Gubbi, Tumkur, Karnataka, India

ABSTRACT: The two most important components of cyber security training are Web safety and hacking ethics. Developing good web security would be challenging without acknowledging the shortcomings of computer technology to prevent intrusions in the real world. The education of hacking ethics and vulnerability assessment is therefore an essential component of a competent cyber security program. A well-known marketing slogan is "growth hacking." This research investigates the hacking method as well as the hacking trend. A single setback could result in cyber-vandalism, disappointment, lost money, mental anguish, or worse in each of these domains. Every new technology comes with pros and cons. Consumers must do this even though ethical hackers help them better understand their security needs.

KEYWORDS: Security, Network defense, System, Cryptography, Cyber-attack.

I. INTRODUCTION

Our computer network infrastructure faces new and evolving threats every day. According to CNBC News,

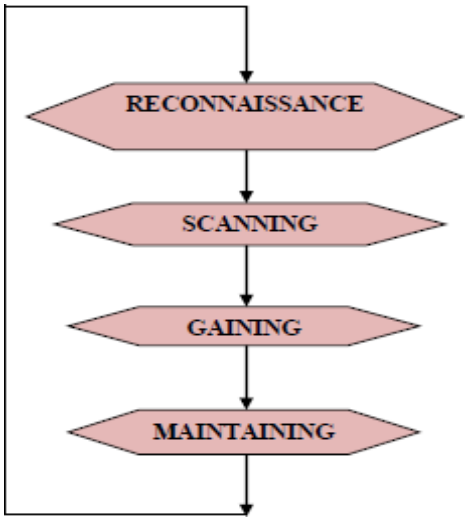


Fig 1: Steps involved in hacking

Global security specialist Derek Manky stated, "We see over a half a million cyber-attack attempts every minute" [1]. Furthermore, hackers target all of our computer network weaknesses in an effort to undermine or harm our more advanced security system. The various stages of hacking are depicted in Fig. 1. We must train more cyber security experts in order to protect our networks and stop intrusions. Network security training and hands-on ethical hacking are now crucial.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311040|

We have discovered that priority scanning vulnerabilities is a crucial stage in ethical hacking and defense-related training based on our experience teaching our students about cyber security [1]. Students that possess these fundamentals will be better equipped to defend computer systems, undertake ethical hacking, and defend networks in the real world [2]. This study examines and discusses real-world laboratory problems related to network vulnerability scanning. The following are the contributions this study makes:

After thoroughly describing the biggest open-source networks, we examine definitions and techniques of network vulnerability scanning. Next, we present our interactive vulnerability scanning labs, which we created especially to enhance the cyber security curriculum in ethical hacking and network advocacy.

Cyber safety education seminars cover defense tactics such as cryptography, intrusion detection, firewall control, and access control, as well as buffer overflow attacks, post-exploitation, and experimentation.

II. ETHICAL HACKING

Computer security has grown to be a significant concern for businesses and governments as Internet usage increases. Although they are still worried about hacking, they wish to use the Internet for electronic commerce, advertising, information dissemination, and other objectives. Conversely, potential clients worry about the retention of control over personal information, including addresses, social security numbers, and credit card details. In their search for a solution, businesses discovered that one of the best methods to determine the intrusion risk in their best interests is for independent computer security experts to attempt to breach their computer systems [3]. Like sending out impartial auditors to visit a business and look over its financial records. In order to protect computer security, these "tiger teams" would employ the same instruments and techniques as intruder systems, but they would not harm or steal information from the target systems. Rather, they would assess the security of the target systems, inform their owners of the flaws they found, and offer guidance on how to fix them. Originally posted to Usenet 9 in December 1993, the most popular pieces were eight pieces by Farmer and Vene Ma. The possibility of using hacker techniques to assess system security was discussed in public, maybe for the first time [4]. The number of active hackers on various social networking sites is displayed in Table 1, and the graph in Fig. 2 below illustrates the rise in hacking in line form.

Table 1: Number of active intruders executing hacking activity ondifferent sites

Websites	Number of Hackers
Yahoo	2525
My space	1792
LinkedIn	1486
Facebook	1091
Slide share	2756
Adobe	1749

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

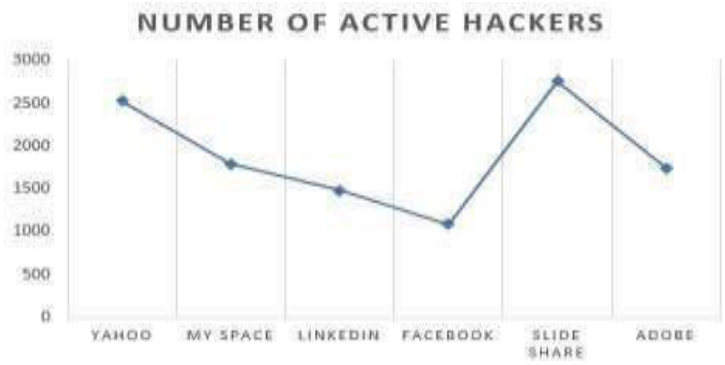
Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311040|

Fig 2: Graphical representation of number of active hackers on different



They went on to describe how they might learn enough about their goals to compromise security in order to improve intranet and Internet security in general. They provided a number of examples of how this data could be obtained and used to gain control over the victim and prevent such an attack. In order for everyone to read and utilize their report, Farmer and Vene Ma decided to make it freely available online [5]. However, they came to the realization that gauging their level of learning might be too difficult.

They gathered all the tools they used, combined them into a single user-friendly package, and made them available to anyone who wanted to use them [6–7]. The Network Auditing Security Analysis Tool, their program, has received extensive international news coverage. Most of the initial attention was negative because of misconceptions about the instrument's capabilities. An automated hacker capable of breaking into networks and stealing data has not been created by this technology. On the contrary, the computer conducted an audit, found, and notified users of system defects [8–10]. Computer systems must regularly audit their operations and balances, much like banks do. The SATAN application not only completed the audit but also provided the user with information on how to fix any problems that were discovered [7]. The application didn't tell the user how to take advantage of the bug because it wouldn't be useful.

III. FUNCTIONING OF ETHICAL HACKING

An ethical hacker's assessment of a system's security looks for answers to three fundamental questions: What data could an intruder obtain from a target system? How would a thief benefit from this knowledge? Is anyone aware of the intruder's endeavors and accomplishments? The third is far more crucial, even though the first and second are unquestionably significant: The intruders will usually succeed and attempt to gain access for weeks or months if the target system owners or operators are unaware that they are being targeted. There must be a significant amount of conversation and paperwork before a customer may receive an assessment. A client and Spafford start the conversation by asking, "What are you trying to protect?" What are you attempting to defend against? How much time, money, and effort are you willing to invest in getting the right protection? Surprisingly, many customers find it difficult to provide appropriate answers to the first question. For example, a medical facility may say "our patient information," an engineering firm might say "our new product ideas," and an online retailer might say "our customer database." Since these answers only list objectives in general terms, they are all inadequate. The various steps in the entire ethical hacking process are shown in Fig. 3 below.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

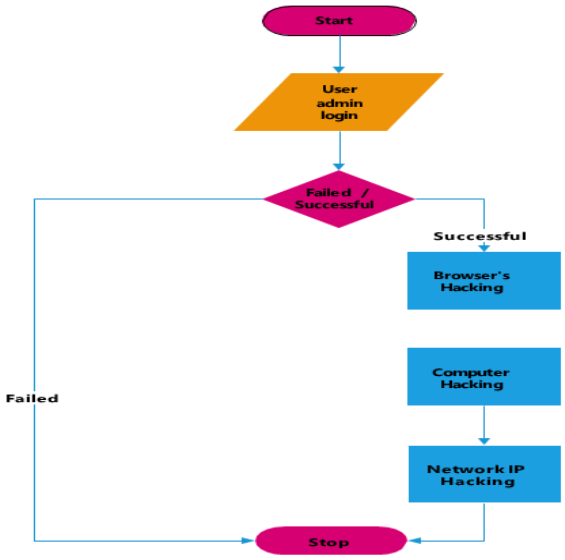
Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311040|

Fig. 3: Steps involved in the whole ethical hacking process



Typically, the customer should be requested to list all of the important information assets whose loss might negatively affect the business or its clients. Secondary sources of information should also be included, such as computer and network information (which could aid an intruder), employee names and addresses (which pose a privacy and security risk), and other organizations working with this organization (subject to a potentially less secure system partner, which could offer alternate routes to the target systems). Once the contractual agreement has been achieved, the testing can begin in accordance with the terms of the agreement [11]. Clients are at danger during the testing process since the same information might be obtained by a criminal hacker who observes transmissions from ethical hackers. If the ethical hackers find a weakness in the customer's security, the criminal hacker may exploit this vulnerability [12]. This is especially perplexing because ethical hackers' work can be mistaken for that of criminal hackers. The easiest way to deal with this issue is to use the Internet to identify different addresses that the ethical hacker uses to send messages and to switch the addresses of origin. For the final report and in the event of strange occurrences, full records of ethical hacker testing are always kept. In extreme cases, additional intrusion monitoring software may be targeted to guarantee that every test originates from the workstation of an ethical hacker. . However, it is difficult to do so without informing the information the customer's staff and the customer's internet service provider may need cooperation.

IV. CONCLUSION

In order to help students absorb the theories and facts taught in the classroom, hands-on laboratories are essential. Money, potential, availability, and impact must all be balanced in any practical laboratory run by an organization, especially when it comes to offensive safety laboratory operations. To learn how hackers identify flaws in a target host before launching an attack, network security training and hands-on ethical hacking, including vulnerability scanning, are necessary. An essential component of a quality cyber security curriculum is the instruction of hacking ethics and vulnerability assessment. Frequent audits, which include close intrusion detection, superior system administration, and knowledge of computer security, are all essential components of an organization's security operations.

REFERENCES

1. Stoner, Jessie. "Foundations of Information Ethics Book Review." School of Information Student Research Journal 11.1 (2021): 8.
2. Montreuil, Marjorie, et al. "A Review of Approaches, Strategies and Ethical Considerations in Participatory Research With Children." International Journal of Qualitative Methods 20 (2021): 1609406920987962.
3. Radoilska, Lubomira, and Emanuela Ceva. "Ethical Theory and Moral Practice at 24." Ethical Theoryand Moral Practice 24.1 (2021): 1-3.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311040|

4. Oosman, Bushra Siddiqua, and Ravishankar Dudhe. "Review on the ethical and legal challenges with IoT." 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE). IEEE, 2021.
5. Iantorno, Michael. "Book Review: Coding Democracy: How Hackers Are Disrupting Power, Surveillance, and Authoritarianism." (2021): 1461444821999815.
6. Hensher, Martin, et al. "Scoping review: Development and assessment of evaluation frameworks of mobile health apps for recommendations to consumers." Journal of the American Medical Informatics Association (2021).
7. Rodriguez, Emily, Challace Pahlevan-Lbrekic, and Elaine L. Larson. "Facilitating Timely Institutional Review Board Review: Common Issues and Recommendations." Journal of Empirical Research on Human Research Ethics (2021): 15562646211009680.
8. Christner, Clara, et al. "Automated Tracking Approaches for Studying Online Media Use: A Critical Review and Recommendations." Communication methods and measures (2021): 1-17.
9. Kim, Hakpyeong, et al. "A systematic review of the smart energy conservation system: From smart homes to sustainable smart cities." Renewable and Sustainable Energy Reviews 140 (2021): 110755.
10. Sohrabi, Soheil, et al. "Quantifying the automated vehicle safety performance: A scoping review of the literature, evaluation of methods, and directions for future research." Accident Analysis & Prevention 152 (2021): 106003.
11. Sathesh, A. “Enhanced soft computing approaches for intrusion detection schemes in social media networks.” Journal of Soft Computing Paradigm (JSCP) 1, no. 02 (2019): 69-79.
12. Kirubakaran, S. Stewart. “ Study of Security Mechanisms to Create a Secure Cloud in a Virtual Environment with the Support of Cloud Service Providers.” Journal of trends in Computer Science and Smart technology (TCSST) 2, no. 03 (2020): 148-154.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details