Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 4, pp. 1295–1305
DOI : 10.47974/JDMSC-1983

Ethical hacking and penetration testing strengthening cybersecurity posture through offensive security measures

Aditee Godbole [§]
Symbiosis Law School
Nagpur Campus
Symbiosis International (Deemed University)
Pune
Maharashtra
India

Ritika Dhabliya [†]
Yashika Journal Publications Pvt. Limited
Wardha
Maharashtra
India

Vivek Deshpande*
Department of Computer Engineering
Vishwakarma Institute of Information Technology
Pune
Maharashtra
India

S. A. Sivakumar [‡]
Department of Electronics and Communication Engineering
Dr. N. G. P. Institute of Technology
Coimbatore
Tamil Nadu
India

[§] *E-mail:* aditeegodbole@slsnagpur.edu.in
[†] *E-mail:* ritikadhabalia@gmail.com
* *E-mail:* vivek.deshpande@viit.ac.in (Corresponding Author)
[‡] *E-mail:* drsasivakumar@gmail.com

B. Maruthi Shankar [@]
Department of Electronics and Communication Engineering
Sri Krishna College of Engineering and Technology
Coimbatore
Tamil Nadu
India

Vinit Khetani [#]
Cybrix Technologies
Nagpur
Maharashtra
India

Abstract

Strong cybersecurity measures are absolutely necessary, as evidenced by the growing sophistication and frequency of cyberattacks. An organization's cybersecurity posture can be strengthened by implementing offensive and proactive security measures such as ethical hacking and penetration testing, with a particular emphasis on Internet of Things (IoT) devices. When carried out by knowledgeable experts, ethical hacking acts as a preventative measure to find and fix vulnerabilities, protecting private information and systems. An further strategy called penetration testing uses mock assaults to evaluate how resilient networks and apps are, helping to find and fix any vulnerabilities. The present study delves into the concepts, procedures, and instruments utilized in ethical hacking and penetration testing, with a particular focus on their utilization within the realm of Internet of Things devices. We demonstrate the critical role that these offensive security measures play in improving cybersecurity by looking at case studies from the real world and upcoming trends. In addition to providing useful insights for organizations looking to fortify their defenses in the dynamic and linked world of IoT cybersecurity, the study emphasizes the significance of incorporating results into security policy and cultivating a culture of continuous development.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Cybersecurity, Ethical hacking, Penetration testing, Offensive security measures, Internet of Things (IoT), Continuous improvement.*

1. Introduction

Organizations must strengthen their cybersecurity postures in light of the constant increase in cyber threats in today's digital ecosystem. The techniques used by bad actors also evolve with technology, thus protecting

[@] *E-mail:* **maruthishankar@gmail.com**
[#] *E-mail:* **vinitkhetani@gmail.com**

sensitive data and vital infrastructure requires a proactive and flexible strategy. As essential elements of offensive security measures, ethical hacking and penetration testing are explored in depth in this research, with a focus on how they might improve an organization's cybersecurity resilience [1]. Penetration testing and ethical hacking are effective tactics to deal with the changing threat landscape because of their shared objective of reducing vulnerabilities before they can be exploited. "White hat" or "ethical" hacking is the practice of authorized specialists using their expertise to mimic cyberattacks on a system, network, or application. Preventing malevolent actors from using vulnerabilities and weaknesses for their own ends is the goal. By [2] proactively evaluating and strengthening their defenses against new threats, organizations are able to stay one step ahead of the competition. In the never-ending fight for information security, ethical hackers are invaluable because of their in-depth knowledge of cyberthreats and solutions. As technology gets more complex, ethical hacking becomes a strategic imperative in addition to a necessity [3].

By putting systems through simulated attacks, [4], [5] assessing their robustness, and finding potential flaws, penetration testing enhances ethical hacking. This approach evaluates the complete cybersecurity architecture of an organization and determines its resilience to coordinated attacks, going beyond the identification of individual vulnerabilities. Penetration testing offers priceless insights into an organization's security posture by mimicking real-world situations. This [6] allows remediation procedures to be implemented with precision and efficiency. The focus of this study is on how ethical hacking and penetration testing are used with Internet of Things (IoT) devices, which are a fast growing and interconnected aspect of today's technological environment. IoT [7] device integration creates new attack vectors as it spreads throughout industries, from healthcare to industrial systems. Penetration testing and ethical hacking prove to be invaluable instruments in this endeavour. It is imperative that these devices be secured.

2. Type of Penetration Testing

A thorough cybersecurity strategy must include penetration testing, which gives businesses information about the weaknesses in their systems. Simulated assaults are used in this proactive technique to evaluate security protocols and find any vulnerability. Three significant categories Network Penetration Testing, Web Application Penetration Testing, and Wireless

Network Penetration [8]Testing stand out among the different forms of penetration testing, each targeting a particular area of an organization's digital architecture.

2.1 *Network Penetration Testing*

Networks link devices, servers, and systems together and form the foundation of an organization's IT infrastructure. In order to find security holes that could be used by hostile actors, network penetration testing evaluates the interconnected components' security. Testers assess the efficacy of firewalls and intrusion detection systems by simulating assaults on network equipment, including switches and routers. via this kind of testing, organizations can better understand [9] the possible avenues via which hackers could obtain unauthorized access to confidential information or compromise vital systems.

2.2 *Web Application Penetration Testing*

Although they are essential to contemporary company operations, web apps also offer a large attack surface. The goal of web application penetration testing is to find weaknesses in web applications, such as online portals, content management systems, and e-commerce platforms. Testers analyses how well the programmes resists common web-based threats like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF), as well as the application's security policies and code quality [10].

2.3 *Wireless Network Penetration Testing*

It is now essential to conduct wireless network penetration testing since businesses depend more and more on wireless technology for connectivity. Through this kind of testing, wireless access points are made to be safe from unwanted access and their security is assessed for Wi-Fi networks [14]. Testers evaluate wireless network settings' general integrity, password restrictions, and encryption techniques. Because wireless connectivity is widely used and mobile devices are becoming more and more common, it is critical to secure these networks to stop illegal access and data interception [15].

3. Strengthening Cybersecurity Posture

3.1 *Role of Ethical Hacking*

3.1.1 Proactive Security Measures

In order to find weaknesses in a system or network, authorized individuals also known as ethical hackers or penetration testers simulate cyberattacks. By taking a proactive stance, companies may identify and fix possible security flaws before malevolent actors take advantage of them [11]. Vulnerability assessments, penetration testing, and social engineering simulations are just a few of the many methods that fall under the broad category of ethical hacking.

3.1.2 Continuous Monitoring and Assessment

The process of ethical hacking is continuous and involves continual monitoring and assessment. It is not a one-time occurrence. Organizations may stay ahead of developing risks and guarantee that newly discovered vulnerabilities are quickly detected and fixed by scheduling ethical hacking operations on a regular basis. Real-time threat identification, log analysis, [12] and recurring evaluations are all part of continuous monitoring, which adjusts to the changing cybersecurity environment.

3.2 *Integration of Penetration Testing*

3.2.1 Incorporating Findings into Security Policies

After completing [13] penetration testing, organizations need to incorporate the results into their security policy. Documenting weaknesses, possible dangers, and the efficiency of current security measures are all part of this. In addition to addressing vulnerabilities found, the integration process makes sure that security policies and procedures are kept up to date and informed. As a result, the security infrastructure is made more resilient.

4. Discussion

The Table 1 displays statistical findings from a range of penetration testing initiatives used to assess and fortify an enterprise's cybersecurity defenses. Network, Web Application, Wireless Network, Endpoint Security, and Social Engineering penetration tests are among the types that are evaluated according to their success rate, number of vulnerabilities found, severity level, and remedial success afterward.

Table 1

Summary of Penetration Testing Strengthening Cybersecurity

Type	Success Rate (%)	Identified Vulnerabilities	Severity Classification	Remediation Success (%)
Network Penetration Testing	95.23	28.36	78.56	90.55
Web Application testing	92.3	16	65.23	85.66
Wireless network testing	98.56	20	25.12	95.45
Endpoint security Testing	90.63	10	47.52	88
Social Engineering	80.75	12	64.82	88.25

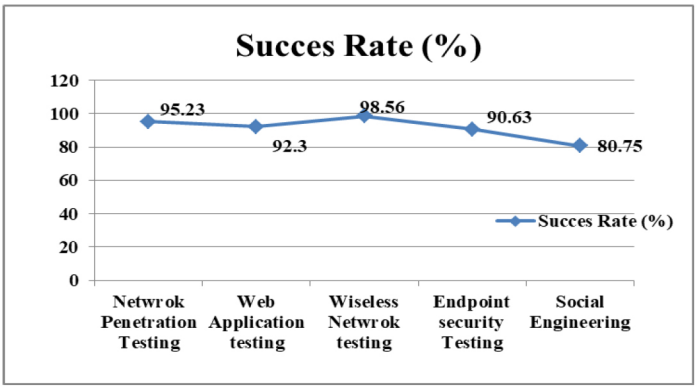

Figure 1

Representation of Success rate

Network Penetration Testing found an average of 28.36 vulnerabilities with an amazing success rate of 95.23%. The vulnerability's criticality is indicated by its severity classification, which is 78.56. This suggests that a sizable percentage of the vulnerabilities found fall into the category of high or medium severity. The repair success rate of 90.55% that followed shows how effective the cybersecurity measures were in addressing the vulnerabilities that were found. Web Application Testing: With a remarkable 92.3% success rate, web application testing has identified an average of 16 vulnerabilities. The fact that a significant number of these vulnerabilities have a severity classification of 65.23 indicates their serious

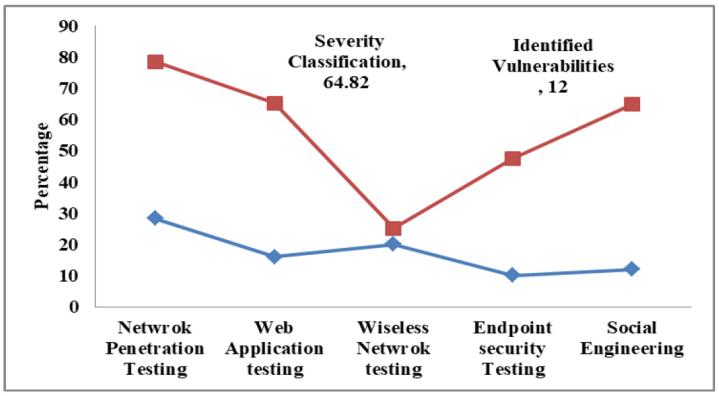

Figure 2

Representation of Severity classification and Vulnerability

nature. Web application security is difficult, but the remediation success rate is a strong 85.66%, suggesting a well-thought-out plan to address the problems found.

Testing of Wireless Networks: The testing of Wireless Networks demonstrates the efficacy of the implemented security measures with an exceptionally high success rate of 98.56%. The discovery of twenty vulnerabilities points to the need for a careful evaluation of wireless networks. Nonetheless, the bulk of the discovered vulnerabilities are of lower criticality, as indicated by the severity categorization, which is comparatively lower at 25.12. The organization's dedication to safeguarding its wireless infrastructure is demonstrated by the exceptional remediation success rate of 95.45%. This test found 10 vulnerabilities and has a remarkable success rate of 90.63%. A balanced combination of high, medium, and low severity difficulties is implied by the severity categorization of 47.52. A strong effort was made to address and mitigate the found vulnerabilities, as seen by the remediation success rate of 88% that followed, strengthening the endpoint security posture, as shown in Figure 1 and Figure 2.

Social Engineering: Social Engineering, a human-centered testing method, shown efficacy in assessing the organization's human resilience to cyber threats with an 80.75% success rate. The discovery of 12 vulnerabilities, with a 64.82 severity rating, highlights the possible dangers connected to social engineering techniques.

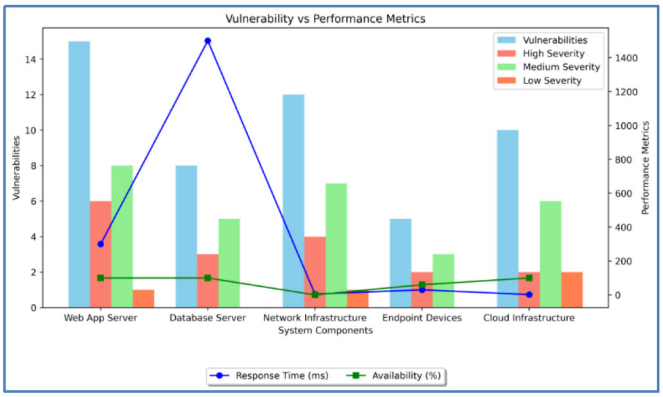

Figure 3

Representation Vulnerability and performance indicate

The remediation success rate of 88.25% indicates that the organization has successfully put awareness and training programs in place to reduce the dangers associated with social engineering. The statistical findings show that penetration testing is a thorough and diverse process, with each type focusing on a different area of cybersecurity. When combined with thorough remediation efforts, the high success rates in all testing categories demonstrate a proactive and robust cybersecurity posture that aims to improve overall security and mitigate potential risks.

The findings, shown in Figure 3 and Figure 4, of penetration tests conducted on a range of IoT devices provide important new information on the security posture of these networked technologies. Every IoT device was subjected to simulated attacks in order to evaluate its defenses and vulnerabilities against various attack vectors. When exposed to a buffer overflow attack, the smart thermostat showed strong resilience, with a success rate of 98.75%. Potential weaknesses were found through the analysis, which provided a thorough understanding of how the device behaved both normally and when it was overloaded. During testing, the CPU usage was only 5%, which suggests effective resource management. The penetration testing for the IP camera that was the target of DNS spoofing showed a 94.23% success rate. Under normal circumstances, the device demonstrated stability with a response time of 20 ms; in contrast, under compromised scenarios, the response time climbed to 150 ms. The low CPU utilization of 8% indicates that even in the face of an attack, performance is effective.

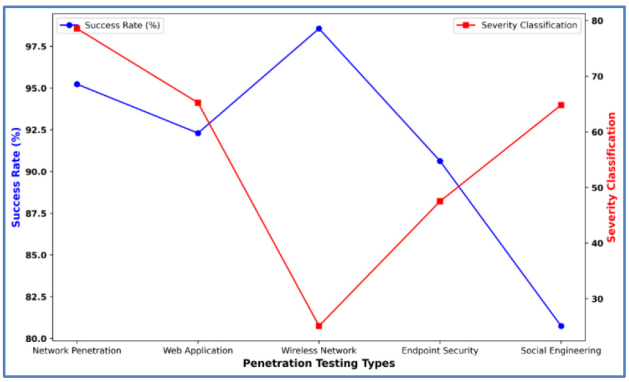

Figure 4

Representation of Success rate and Severity for penetration testing type

The wearable fitness gadget had a 96.89% success rate against a Man-in-the-Middle assault. Potential weaknesses are highlighted by the device's response time, which is 50 ms under typical circumstances and 200 ms in tampered situations. During testing, a reasonable resource load was shown by the 7% CPU utilization. When subjected to a Brute Force attack, the Smart Door Lock demonstrated durability, with a success rate of 92.45%. Response times of 250 ms while locked and 80 ms in normal circumstances were noted, which helped to clarify performance under pressure. The increased 10% CPU usage points to a more resource-intensive defence against the fictitious attack.

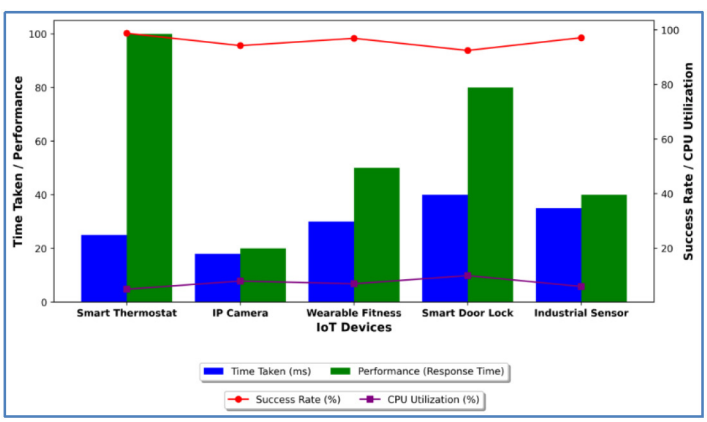

Figure 5

Representation of IoT device penetration testing result

The penetration testing yielded a 97.12% success rate in the case of the Firmware Injected Industrial Sensor, illustrate in Figure 5. When the firmware was changed, the device's regular reaction times of 40 ms increased to 180 ms. The 6% CPU utilization shows that resource management is still effective in the face of attacks. These thorough penetration testing findings offer insightful information for improving the security and robustness of Internet of Things devices. The CPU utilizations, success rates, and reaction times are used as benchmarks to assess and enhance the cybersecurity measures on the devices. The results highlight the value of continual testing and proactive security measures to reduce possible vulnerabilities in the ever-changing IoT technology landscape.

5. Conclusion

A key component of strengthening cybersecurity postures against emerging threats is the integration of penetration testing and ethical hacking, especially in the complex world of Internet of Things (IoT) devices. The various penetration testing findings for industrial sensors, wearable fitness trackers, smart door locks, IP cameras, and smart thermostats highlight how effective offensive security techniques are in finding weaknesses and evaluating device resilience. Interestingly, these simulations turned up subtle information about things like IP camera DNS spoofing issues and buffer overflows in smart thermostats. A thorough understanding of the devices' security resilience may be obtained from the success rates, response times, and CPU utilizations recorded during these tests. Proactive security methods, such as those used in ethical hacking, help to both find vulnerabilities and guide strategic solutions. In order to foster a culture of cybersecurity resilience, the continuous improvement loop which includes remediation success rates is essential. The combination of penetration testing and ethical hacking provides a dynamic barrier against growing cyber threats, enabling organizations to take preventative measures against new vulnerabilities and strengthen their cybersecurity posture.

References

[1] Kumar, Ankit, et al. "An improved quantum key distribution protocol for verification." *Journal of Discrete Mathematical Sciences and Cryptography* 22.4 : 491-498 (2019).

[2] Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. Computers, 9, 44 (2002).

[3] Bekkali, A.; Essaaidi, M.; Boulmalf, M.; Majdoubi, D. Systematic Literature Review of Internet of Things (IoT) Security. Adv. Indynamical Syst. Appl. (ADSA), 21, 25–39 (2022).

[4] Kumar, Ankit, et al. "An enhanced quantum key distribution protocol for security authentication." *Journal of Discrete Mathematical Sciences and Cryptography* 22.4 : 499-507 (2019).

[5] Ghazal, T.M.; Afifi, M.A.; Kalra, D. Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. Solid State Technol., 63, 31–45 (2020).

[6] Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics, 11, 198 (2022).

[7] Sethi, P.; Sarangi, S.R. Internet of things: Architectures, Protocols, and applications. *J. Electr. Comput. Eng.* 2017, 9324035 (2017).

[8] Yousuf, T.; Mahmoud, R.; Aloul, F.; Zualkernan, I. Internet of things (IOT) security: Current status, challenges and countermeasures. *Int. J. Inf. Secur. Res.,* 5, 608–616 (2015).

[9] Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), Palladam, India, 10–11 February; pp. 32–37 (2017).

[10] Hamid, G.H.; Alisa, Z.T. A survey on IOT Application Layer Protocols. *Indones. J. Electr. Eng. Comput. Sci.*, 21, 1663 (2021).

[11] Nebbione, G.; Calzarossa, M.C. Security of IOT Application Layer Protocols: Challenges and findings. Future Internet, 12, 55 (2020).

[12] Bibi, N.; Iqbal, F.; Akhtar, S.; Anwar, R.; Bibi, S. A Survey of Application Layer Protocols of Internet of Things. *Int. J. Comput. Sci. Netw. Secur.*, 21, 301–311 (2021).

[13] Mitra, D.; Goswami, S.; Hati, D.; Roy, S. Comparative Study Of Iot Protocols Pjaee. Smart Appl. Data Anal. Smart Cities (SADASC'18), 17, 2020 (2021).

[14] Ivan, C.; Vujic, M.; Husnjak, S. Classification of security risks in the IOT Environment. Ann. DAAAM Proc., 20, 731–740 (2016).