International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 4 ǁ 2022 ǁ PP. 37-39

Identifying Hacked Web Application Using Weblink

Prof. Sanjay Kadam, Rashmi Khogare, Vighnesha Shelar, Bhushan Nagaonkar
Information Technology, Bharati Vidyapeeth College of Engineering, Maharashtra, India

Abstract - Cyber attacks refer to those attacks launched on unsuspecting online users either using a computer as the object of the crime (hacking, phishing, spamming etc.), or as a tool to advance other criminal activities (cyber stalking, identity theft, child pornography etc.). Cyber attacks are increasing exponentially hence making cyber security to be a challenge in this digital age. Cyber attacks when successfully launched can result in monumental losses to businesses and individual hence quick incident responses are required to salvaged the situation in case of an occurrence of cyber attacks.
Keywords - Cyber Attacks, Cyber Crime, Cyber Security, Strategies, Variations.

Date of Submission: 11-04-2022 Date of acceptance: 28-04-2022

I. INTRODUCTION

In recent days, the demand for cyber security and protection against various types of cyber-attacks has been ever increasing. It is essential to prevent and protect our data from such hackers.. Therefore we have create an Website which will help to detect such kind of attacks . Identifying hacked Web application using Web link website will help to detect whether our application is been attacked or not so that the user/customer will know that their data is been stolen & they can take action according .

Concept of Cyber Attacks/Cyber Crimes

Cyber attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft. Simply put, a cyber attack is an attack launched from one computer or more computers against another computer, multiple computers or network.

A. Targeted Attacks

Targeted Cyber attacks refer to those attacks that aregeared at particular organizations, services, and individuals to obtain private, technical, and institutional information, and other intellectual assets for the purpose of vandalism or monetary gain. In atargeted attack, an organization is singled out because the attacker has a specific interest in their business, or has been paid to target the victim. A targeted attack is often more damaging than an un-targeted one because it hasbeen specifically tailored to attack specific systems,processes or personnel, in the office and sometimes athome. Targeted attacks are becoming increasinglysophisticated as they go through different stages asstated below, Targeted attacks may include:

1. Spear-phishing - sending emails to targeted individuals that could contain an attachment with malicious software, or a link that downloads malicious software.
2. Botnet Attacks- Deploying a botnet to deliver a DDOS (Distributed Denial of Service) attack, spread malware, used in eavesdropping on a user network or used to launch a web phishing attack. Botnets are always under the control of a botmaster.

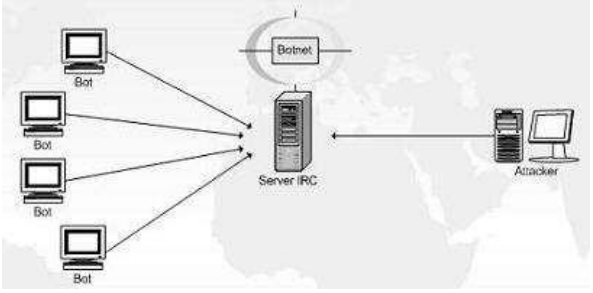

Figure 1. A sample botnet attack.

B

Other forms of targeted attacks include Cyber-Espionage, Intrusion, Internal spread Attack and Elimination of traces of activity.

B. Un-targeted attacks

In un-targeted attacks, attackers indiscriminatelytarget as many devices, services or users as possible. They do not care about who the victim is as there will be a number of machines or services with vulnerabilities. To do this, they use techniques that take advantage of the openness of the Internet, which include:

1. **Phishing** - sending emails to large numbers of people asking for sensitive information them to visit a fake website.
2. **Water holing** - setting up a fake website or compromising a legitimate one in order to exploit visiting users.
3. **Ransomware** - This could include disseminating disk encrypting extortion malware.
4. **Worms** – these are self replication malwares that can exist undetected in a system whilst causing harvoc

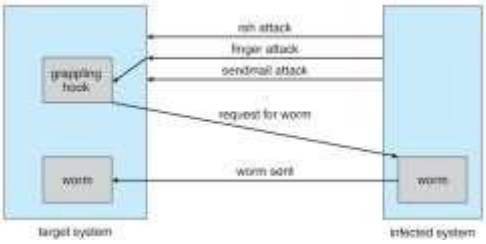

Figure 2: A worm attack.

II. Literature Review

Web applications have become one of the most popular targets of attacks during the last years. The objective is to detect vulnerabilities in Web applications and their dependencies and to generate attack scenarios that reflect such dependencies. Our approach aims to move a step forward toward the automation of this process .

we presents the main concepts behind the proposed approach and an example that illustrates the main steps of the algorithm leading to the identification of the vulnerabilities of a Web application and their dependencies.

III. Diagram

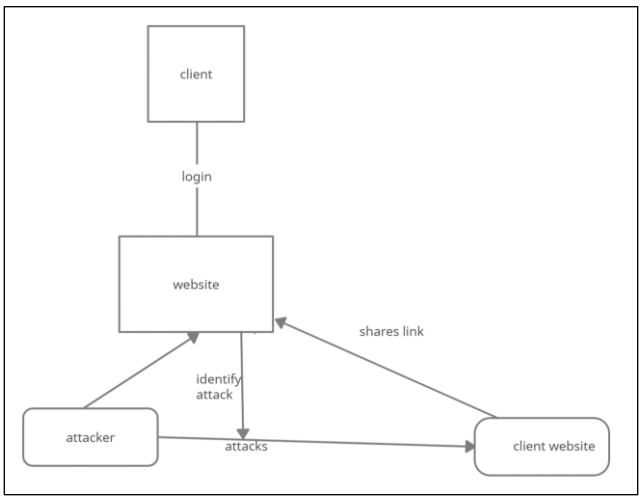

Figure 3 . System Architecture

In our system architecture the client needs to login in our system if the client is new to our website ialert the he needs to sign in to ialert after login the client shares the application link which he wants to check whether has been attacked or not after this the ialert check using python scripting whether the application is

been attacked or not if yes then the information regarding attack and the attacker will be displayed on the screen of ialert.

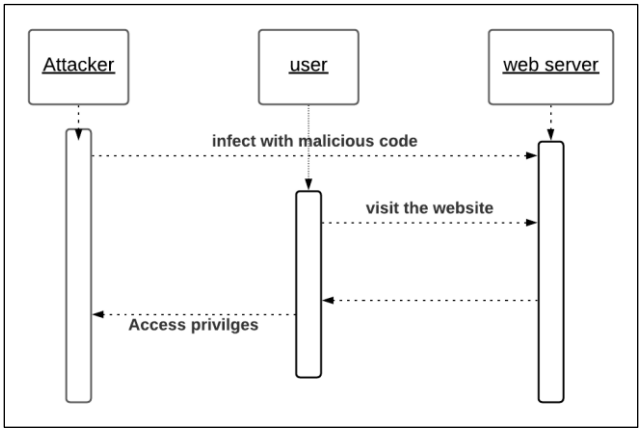

Figure 4 : Interaction Diagram

IV. Conclusion

As technology and the internet continue to evolve, the world is rapidly becoming a global village, with almost everything running on the cyber space affecting most aspects of human lives, enabling growth, dismantling barriers to commerce and allowing people across the globe to communicate, collaborate and exchange ideas. But hackers are becoming more sophisticated by the day. This places the burden of securing IT infrastructure and users on us IT professionals hence the need to be vigilant and prompt in responding to incidents of cyber attacks as well as proactive in ensuring that cyber attacks are mitigated against in all its entirety. Cyber crimes are growing increasingly and as such require even faster growth in cyber security if we hope to keep online and system users safe. The main aim of cyber security is the security of systems, applications and people on the internet from malicious cyber criminals. Cyber security awareness is key to reducing cyber crimes and promotes cyber security.

V. Future Scope

For future work in this regard there is need to developframeworks and strategies to combat cyber crimes in real time. This is due to the rapid evolution and elusivenature of these attacks. Furthermore future research inthis area additionally should focus on development ofreal time cyber attacks detection, mitigation and incident recovery systems.

References

[1]. US Data Vault (n.d). " Types of cyber attacks- and how to prevent them. Available from www.usdatavault.com. Extracted 10/5/2018.
[2]. Technopeia (n.d). " What does Cyber Attack Mean?". Available fromwww.technopedia.com.
[3]. Josh Fruhlinger, (2018). "What is a cyber attack? Recent Examples showing disturbingtrends". Available from www.csoonline.com.
[4]. The windows club (n.d). " Cyber attacks- definition, types, prevention". Available from www.thewindowsclub.com.
[5]. Pooja Aggarwal , Neha, Piyush Arora , Poonam , "REVIEW ON CYBER CRIME AND SECURITY", IJREAS, Vol. 02, Issue 01, Jan 2014.
[6]. Seema Vijay Rane & Pankaj Anil Choudhary, April 2012-September 2012,"Cyber Crime and Cyber Law in India", Cyber Times International Journal ofTechnology and Management, Vol. 5 Issue 2.
[7]. BinaKotiyal, R H Goudar, and Senior Member, A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India PritiSaxena, IACSITInternational Journal of Information and Education Technology, Vol. 2, No. 2, April 2012.
[8]. Amit Wadhwa, and Neerja Arora. A Review on Cyber Crime: Major Threats and Solutions. International Journal of Advanced Research in Computer Science. Volume 8, No. 5, May – June 2017
[9]. NEC (n.d). "What constitutes a cyber attack?". Available from www.nec.com.
[10]. Soumya Tiwari, Anshika Bhalla, and Ritu Rawat. Cyber Crime and Security. International Journal of Advanced Research in Computer Science and SoftwareEngineering Volume 6, Issue 4, April 2016
[11]. Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific& Engineering Research, Volume 3, Issue 6,June-2012 1 ISSN 2229-5518 IJSER © 2012.