International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

Review on Phishing Attack and Ethical Hacking

Yerraballi Krishna Prasad & Mr. D. Venkata Siva Reddy
[1]M.Sc. (Computer Science) Besant Theosophical College, Madanapalle.
krishnaprasad2607@gmail.com
[2]HEAD Dept of Computer Science. Besant Theosophical College, Madanapalle.

Abstract:

Ethical hackers use hacking techniques so as to produce security. They are legally authorized hackers. Various tools area unit utilized in order to hold out hacking. The most common hacking technique used is phishing. Since, there is a rapid growth in the number of attack, Phishing is one such type of attack in which users are tricked by the phishers using social engineering methods to steal their personal or confidential information. Detection of phishing attack with high accuracy is a challenging research issue. Our experimental results show that Gemini can achieve zero false negative rate and less than 1% false positive rate, and Gemini can effectively block the access to a phishing site before a victim user begins to enter in a password.

Keywords: *Ethical Hacking, Phishing attack, Gemini, fake e-mails,*

I. INTRODUCTION

Instead of detecting a phishing site based on its appearance including contents and URLs, we leverage the important information a victim user already typed in username for more accurate phishing detection. For a legitimate web site that needs online authentication, every registered user should have a novel username. The tuple of (username, domain name) provides very useful information for detecting phishing sites. Given an entire list of (username, domain name) pairs, if the username in the current login form is a valid username but the currently visited domain name does not match any corresponding domain names associated with the username in the list, we can infer that the currently visited website is a phishing site with very high confidence. For example, say a user has “monkey” as the username on the legitimate websites of domainA.com, domainB.com, and domainC.com. When the user is detected to use ”monkey” because the username within the login variety of a fresh appeared web site domainX.com, it is highly likely that the website of domainX.com is a phishing site.

Based on the observation on top of, we develop a browser extension called Gemini to protect victim users from phishing attacks. To make Gemini work well in the real world, we have to build a complete list of mappings. We first initialize the mapping list by collecting the majority of ground truth data and then continue to accumulate the newly appeared and least-frequently used mappings while Gemini is in action. Thus, Gemini will acquire most mappings inside a brief amount and keep track of fresh appeared and least-frequently-used mappings throughout its period.

To validate the efficacy of Gemini, we implement different prototypes of Gemini as a browser extension for IE, Firefox, and Chrome, respectively, and conduct extensive experiments over various legitimate and phishing websites. Our experimental results show that Gemini can achieve zero false negative rate and less than 1% false positive rate; and Gemini can

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

effectively block the access to a phishing site before a victim user begins to enter a positive identification. Moreover, Gemini is clear to users and complementary to existing anti-phishing tools. The iatrogenic overhead of Gemini is minor and has negligible result upon user browsing.

Security is the condition of being protected in opposition to danger or loss. In the case of networks, it is also called the information security. Computer security is required because most organizations can be damaged by antagonistic software or intruders. There may be several forms of damage which are interrelated which are produced by the intruders.

Types of Hackers:

1) As per working

- White Hat Hackers
- Black Hat Hackers
- Grey Hat Hackers
- Hactivists
- State Sponsored Hackers
- Suicide Hackers

2) As per knowledge

- Script Kiddies
- Admins
- Coders

II. EXISTING TECHNOLOGIES:

Planned a theme to rescue the passwords purloined by phishers through client-side reportage and server-side aggregation. However, their answer takes impact solely once an exact variety of users become victims of a phishing attack. Birk et al. Proposed a technique to inject fingerprinted credentials to phishing sites in order to trace those stolen credentials and reveal the phisher's identity.

There are several large online databases such as phish tank [8] and OpenDNS [6] that maintain lists of reported phishing sites. These blacklists area unit inhabited by thought browsers [4], [5] and commercial security tools such as umbrella [13]. Once an internet site is detected to be at intervals a blacklist, the site will be blocked and users will be alerted. There are also some studies to enhance the effectiveness of blacklists [18].

The uniform resource locator data and page contents are wide wont to establish a phishing web site. The structural, lexical options, additionally as host-based options, like informatics address and time of registration of URLs at intervals a site, will be wont to classify legitimate sites and malicious sites [20]. Some existing approaches are able to detect a phishing site based on its content information, such as lexical features, layout similarity with legitimate sites, and content anomaly. Many machine learning primarily based approaches will determine phishing sites supported each URL info and page contents.

When compared to the existing techniques, Gemini does not require any other devices. Some anti-phishing techniques such as Antiphish and Webwallet identify the actual intention of user browsing to help users from falling prey to phishing attacks. Apart from all these techniques that concentrate more on password information, this research work take advantage of the username input to activate the anti-phishing methodology to stop consumer from entering their credentials. Gemini is more transparent to users. Yue et al. Designed a clear way that is

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

free of deceit to safeguard the consumer personal information leaked to a phishing site by hiding the real information among fake documents. This methodology makes the intruder very difficult to retrieve vital information before the consumers are noticed the fake site. Some password management techniques like PwdHash, Password Multiplier, and passpet provide password hashing for enforcing security to passwords.

Phishing:

Phishing is a form of social engineering in which an attacker tries to fraudulently acquire sensitive information from a victim by impersonating a reliable third party. It is worth noting that the phishers are getting smarter. Observing the trends in other online crimes, it is inevitable that future phishing attacks will incorporate greater elements of context to become more effective and thus more hazardous for society.

Fig.1 the Process of Phishing attack

The above figure shows the process of phishing attack. The attack is basically done using a fake page which is similar to the trusty webpage. The attacker sends the fake page link via email. This includes the fake mailing process. Once the user clicks on the fake page link and login using his/her credentials, which directly reaches the attacker and the user is phished.

III. IMPLIMENTATION:

Learning the concepts of hacking and applying them for securing any system, organization or for any good cause is what defines ethical hacking.

3.1 Reconnaissance

Reconnaissance is a set of processes and techniques used to secretly discover and collect information about a target system. During reconnaissance, an ethical hacker attempts to collect as much information about a target system as possible, following the seven steps listed below

- Gather preliminary information
- Identifying active machines
- Determine open ports and access points
- OS fingerprinting
- Reveal all the services on ports
- Network mapping

3.3 Scanning and Enumeration

The second step of ethical hacking and penetration testing involves two terms that is scanning and enumeration. Scanning is a common technique used by a pen tester to discover the open doors. Scanning is used to find out the vulnerabilities in the services running on a port. During this process you have to find out the alive host, operating systems involved, firewalls, intrusion detection systems, servers/services, perimeter devices, routing and general network topology (physical layout of network), that are part of the target organization. Enumeration is the initial attack on target network. Enumeration is that the method to collect the data a few target machine by actively connecting to that.

3.4 Gaining Access

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

Once the reconnaissance is done and all the vulnerabilities are scanned, the hacker then tries to gain he access with the help of certain tools and techniques. It basically focuses on the password retrieval. For this hacker can either use bypassing techniques (like using konboot) or password cracking techniques (like pwdump7).

3.5 Maintaining access

Once an attacker has gained the access of the targeted system, he/she can exploit both the system and its resources and furthermore use the system as a launch pad to scan and harm other systems, or he/she can keep a low profile and continue exploiting the system without the actual user noticing all these acts. Both these actions can destroy the organization leading to a catastrophe. Root kits gain access at the OS level whereas a bug gains access at the appliance level. Attackers can use Trojan horses to transfer user names, passwords, and even credit card information stored on the system. Organizations can use intrusion detection systems or deploy honeypots to detect intruders. The latter though is not recommended unless the organization has the required security professionals to leverage the concept of protection.

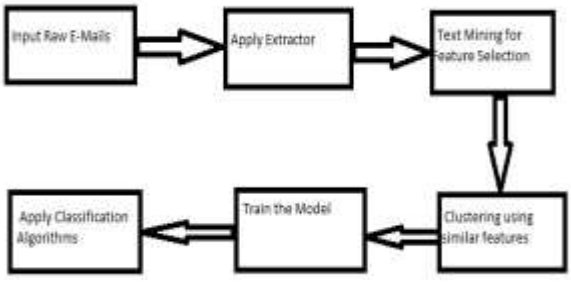
3.6 Clearing Tracks

An attacker needs to destroy evidence of his presence and activities for several reasons like evading detection and further punishment for the intrusion. Erasing evidence often known as ‘clearing tracks’ is a requirement for any attacker who wants to remain obscure and evade trace back. This step usually starts by erasing the contaminated logins or any other possible error messages that may have been generated on the victims system from the attack process. For instance, a buffer overflow attack usually leaves a message in the system logs which needs to be cleared. Next, attention is turned to touching changes in order that future logins don't seem to be logged.

The first thing a system administrator does to monitor the unusual activity happening in the system is by checking all the system log files, it is important for intruders to use a utility to modify the system logs so that they cannot be traced by the administrator. It is necessary for attackers to create the system appear as if it did before they gained access and established backdoors for his or her use. Any files that were modified need to be changed back to their original attributes so that there is no doubt in administrators mind that the system has been intruded.

A. The System Architecture:

As shown in figure below, the system consists of six sub modules as input raw E-mails, Apply Extractor, Text Mining, Clustering, Training Phase and Apply classification for the test data set.



B. Proposed Algorithm:

1. Input emails
2. Apply extractor to extract text from e-mail.

3. Text mining to selected text for feature selection.
4. Partitioning into clusters based on similar features.
5. Train the classifier using known values
6. Apply classifier to classify e-mails.
7. Output as fake or real e-mails
8. End.

IV. Conclusion:

This research work aims to presents a data mining methods to construct a model in order to protect against phishing attacks. The architectural model provides a powerful approach to identify phishing sites without inducing high overhead over the browser and work effectively. Identifying different features helped in recognizing the different E-mails into different clusters and able to detect the cluster specially designed by the phishers.

V. REFERENCES:

[1] Alexa: Top sites in United States. http://www.alexa.com/topsites/countries/ US.
[2] Algorithm implementation of levenshtein distance. http://en.wikibooks.org/wiki/Algorithmimplementation/Strings/Levenshtein distance JavaScript.
[3] Bank of America, sign up for the site key service. http://www. bankofamerica.com/privacy/pass mark/.
[4] Firefox: phishing and malware protection. http://www.mozilla.org/en-US/ firefox/phishing-protection/.
[5] https://en.wikipedia.org/wiki/Certified_Ethical_Hacker
[6] Opendns. http://www.opendns.com/.
[7] The past, present & future of local storage for web applications. http://diveintohtml5.info/storage.html.
[8] Phish tank. http://www.phishtank.com /.
[9] Phishing activity trends report, 2012 1st quarter. http://docs.apwg.org/ Reports/apwgtrendsreportq12012.pdf.
[10] Phishing activity trends report, 2012 2nd quarter. http://docs.apwg.org/ Reports/apwgtrendsreportq22012.pdf.
[11] Phishing in season: A look at online fraud in 2012. http://blogs.rsa.com/ Phishing-in-season-a-look-at-online-fraud-in-2012/.
[12] Rsa: Phishing attacks net 687 m to date in 2012. http://threatpost.com/ Enus/blogs/rsa-phishing-attacks-net-687m-date-2012-082412.
[13] Umbrella: Block malware, contain botnets and stop phishing. http://www. umbrella.com/explore/internet-security/.
[14] Rsa site key solution for enterprise. http://www.RsaSecurity.com, 2007. [15] BIRK, D., GAJEK, S., GROBERT, F., AND SADEGHI, A.-R. Phishing Phishers - observing and tracing organized cybercrime. In Proceedings *Of the Second International Conference on Internet Monitoring and Protection* (2007), IEEE, pp. 3–11.
[16] CHIASSON, S., VAN OORSCHOT, P., AND BIDDLE, R. A usability study and critique of two password managers. In Proceedings *of the 15th USENIX Security Symposium* (2006), pp. 1–16.
[17] DHAMIJA, R., AND TYGAR, J. The battle against phishing: Dynamic security skins. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)* (2005), ACM, pp. 77–88.
[18] FELEGYHAZI, M., KREIBICH, C., AND PAXSON, V. On the potential of proactive domain blacklisting. In Proceedings *of the 3rd USENIX con- ference on Large-scale Exploits and Emergent Threats* (2010), USENIX, pp. 6–6.

[19] FLOREˆ NCIO, D., AND HERLEY, C. Password rescue: a new approach to phishing prevention. In *Proceedings of the 1st USENIX Workshop on Hot Topics in Security* (2006), USENIX, pp. 2–2.

[20] GARERA, S., PROVOS, N., CHEW, M., AND RUBIN, A. A framework for detection and measurement of phishing attacks. In *Proceedings of the 2007 ACM Workshop on Recurring Malcode* (2007), ACM, pp. 1–8.

[21] HALDERMAN, J., WATERS, B., AND FELTEN, E. A convenient method for securely managing passwords. In Proceedings *of the 14th international conference on World Wide Web (WWW)* (2005), ACM, pp. 471–479.

About the Authors:

YERRABALLI KRISHNA PRASAD,
M.Sc. (Computer Science),
Besant Theosophical College Madanapalle.

Mr. D. Venkata Siva Reddy
HEAD of Dept Computer Science,
Besant Theosophical College Madanapalle.