*DEPARTMENT OF INFORMATION TECHNOLOGY* Experiment No. 7

|  |  |
| --- | --- |
| Semester | T.E. Semester VI – Information Technology |
| Subject | Systems and Web Security |
| Subject Professor In-charge | Prof. Chintan Shah |
| Assisting Teachers | Prof. Mohit Gujjar |
| Laboratory | L05B |

|  |  |  |
| --- | --- | --- |
| Student Name | Ashutosh Engavle | |
| Roll Number | 15101B0042 | |
| Grade and Subject Teacher’s Signature |  |  |

|  |  |
| --- | --- |
| Experiment Number | 7 |
| Experiment Title | To Implement Phishing Attack |
| Objectives  (Skill Set / Knowledge Tested / Imparted) | The objective of this experiment is to study the concept of Phishing attack and its various techniques. |
| Theory: | WHAT IS A PHISHING ATTACK Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransom ware attack or the revealing of sensitive information.  An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identifies theft.  Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.  An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.  **PHISHING TECHNIQUES** EMAIL PHISHING SCAMS: Email phishing is a numbers game. An attacker sending out thousands of fraudulent messages can net significant information and sums of money, even if only a small percentage of recipients fall for the scam. As seen above, there are some techniques attackers use to increase their success rates.  For one, they will go to great lengths in designing phishing messages to mimic actual emails from a spoofed organization. Using the same phrasing, typefaces, logos, and signatures makes the messages appear legitimate.  In addition, attackers will usually try to push users into action by creating a sense of urgency. For example, an email could threaten account expiration and place the recipient on a timer. Applying such pressure causes the user to be less diligent and more prone to error.  Lastly, links inside messages resemble their legitimate counterparts, but typically have a misspelled domain name or extra subdomains. In the above example, the myuniversity.edu/renewal URL was changed to myuniversity.edurenewal.com. Similarities between the two addresses offer the impression of a secure link, making the recipient less aware that an attack is taking place.  Phishing techniques - Phishing link example SPEAR PHISHING:Spear phishing targets a specific person or enterprise, as opposed to random application users. It's a more in depth version of phishing that requires special knowledge about an organization, including its power structure. For example:  1. A link in the email redirects to a password-protected internal document, which is in actuality a spoofed version of a stolen invoice. 2. The PM is requested to log in to view the document. The attacker steals his credentials, gaining full access to sensitive areas within the organization’s network.   By providing an attacker with valid login credentials, spear phishing is an effective method for executing the first stage of an APT. |
| Output | C:\Users\logon\Downloads\Screenshot from 2018-01-12 15-49-17.png  C:\Users\logon\Downloads\Screenshot from 2018-01-12 15-49-25.png  C:\Users\logon\Downloads\Screenshot from 2018-01-12 15-49-31.png  C:\Users\logon\Downloads\Screenshot from 2018-01-12 15-49-37.png  C:\Users\logon\Downloads\Screenshot from 2018-01-12 15-49-54.png  C:\Users\logon\Downloads\Screenshot from 2018-01-12 15-50-08.png  C:\Users\logon\Downloads\Screenshot from 2018-01-12 15-50-38.png  C:\Users\logon\Downloads\Screenshot from 2018-01-12 15-50-47.png |
| Conclusion | In this experiment, we studied how phishing attack takes place and that one has to be aware of the various techniques used by the malicious users for the same. |