  
  
**Assignment Cover Sheet**

|  |  |
| --- | --- |
| **Subject Code: CSCI369** |  |
| **Subject Name: Ethical Hacking** |  |
| **Submission Type: Turnitin** |  |
| **Assignment Title: Project Proposal** |  |
| **Student Names: Ocean Dsouza , Siam Ali, Uzair Naeem, Youssef Elshafey** |  |
| **Student Number: 6628485, 6482491, 6538654, 7004266** |  |
| **Student Phone/Mobile No. 0503605417, 0505191211, 0563249747, 0501255340** |  |
| **Student E-mail:** [**osd331@uowdubai.ae.ac**](mailto:osd331@uowdubai.ae.ac) **,** [**sa122@uowmail.edu.au**](mailto:sa122@uowmail.edu.au)**,** [**nm690@uowmail.edu.au**](mailto:nm690@uowmail.edu.au) **,** [**ye901@uowmail.edu.au**](mailto:ye901@uowmail.edu.au) |  |
| **Lecturer Name: Dr. May El Barachi** |  |
| **Due Date: 29-May-2022** |  |
| **Date Submitted: 29-May-2022** |  |

|  |  |
| --- | --- |
| **PLAGIARISM:** The penalty for deliberate plagiarism is FAILURE in the subject. Plagiarism is cheating by using the written ideas or submitted work of someone else. UOWD has a strong policy against plagiarism.  The University of Wollongong in Dubai also endorses a policy of non-discriminatory language practice and presentation.  **PLEASE NOTE:**STUDENTS MUST RETAIN A COPY OF ANY WORK SUBMITTED | **DECLARATION:** I/We certify that this is entirely my/our own work, except where I/we have given fully-documented references to the work of others, and that the material contained in this document has not previously been submitted for assessment in any formal course of study. I/we understand the definition and consequences of plagiarism.  **Signature of Student:** |

|  |  |  |
| --- | --- | --- |
| |  | | --- | | **Optional Marks:** | | **Comments:** | |

A close up of a device



Description automatically generated

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Lecturer Assignment Receipt**(To be filled in by student and retained by Lecturer upon return of assignment) | | | **Subject:** CSCI369 | **Assignment Title:** Project Proposal | | **Student Name:** | **Student Number:** | | **Due Date:** | **Date Submitted:** | | **Signature of Student:** | | |

A close up of a device



Description automatically generated

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Student Assignment Receipt** (To be filled in and retained by Student upon submission of assignment) | | | **Subject:** CSCI369 | **Assignment Title:** Project Proposal | | **Student Name:** | **Student Number:** | | **Due Date:** | **Date Submitted:** | | **Signature of Lecturer** | | |

**Title**

The topic we have selected is Social Engineering and Phishing attacks.

**Project scope and objective**

The Scope of this project is to investigate and showcase the various types of social engineering and phishing attacks that may occur by simulating actual attacks and assessing the various factors involved in the attack.

Our objective is to exploit the human inclination to trust individuals to access valuable information. To understand our target and his/her behavioral pattern, we need to observe them. This is where reconnaissance comes into play as we will use various reconnaissance tools to gather intel about our target before performing a social engineering attack. The first social engineering attack vector we select is Phishing and under phishing we are performing spear phishing attacks and our main objective is gaining the targets credentials. The second vector selected is baiting where our objective is to get the victim to plug a flash drive with a seemingly innocent pdf file containing an infectible. Finally, the last advances strategy we will be showcasing is a water hole attack where we infect a vulnerable website with Cross-site-scripting vulnerability and gain access to the user’s system and try to elevate privileges.

**Phase of social engineering attacks addressed**

1. **Reconnaissance-** investigating the intended victim to get background information and the moving to get the trust of the victim so that it can lead to revealing of sensitive information or granting or gaining access to restricted resources. There will be 2 ways in which reconnaissance will be done active and passive

* **Passive reconnaissance-** information is found without actively engaging the target. This means that no requests are sent to the target therefore they have no way to know you are gathering intel on them.

1. **Scanning- This** is the phase where the attacker will try to seek information such as IP addresses, computer names, OS version or user accounts in order to gain access into system.

* **Vulnerability scanning-** This refers to scanning network, application or websites used by the target for vulnerabilities to exploit.

1. **Gaining Access:** This is thew phase where the attacker will try to gain access to the system using various tool and will try to escalate their privileges vertically or horizontally.
2. **Maintaining Access:** This is where the attacker will try to maintain a persistent connection to the victim’s system in the background without them knowing.

The 5 phases of the social engineering attack are explained below-

Social Engineering Life Cycle Diagram 


1. Investigation: Identifying victim(s), Gathering background information and Selecting attack methods
2. Hook: Tricking the victim to gain a grip by engaging the target directly and spinning a story then trying to take control.
3. Play: This is done over a period of time by getting a better grip on the situation and then executing attack and disrupting or stealing the business data.
4. Exit: Closing the interactions, without raising suspicion by removing all traces of malware, covering tracks which were taken in order to steal or disrupt the business or bringing the situation to a natural end.

**Security properties addressed**

**Confidentiality:** The privacy of the system is violated because we will be tricking the user into giving sensitive information

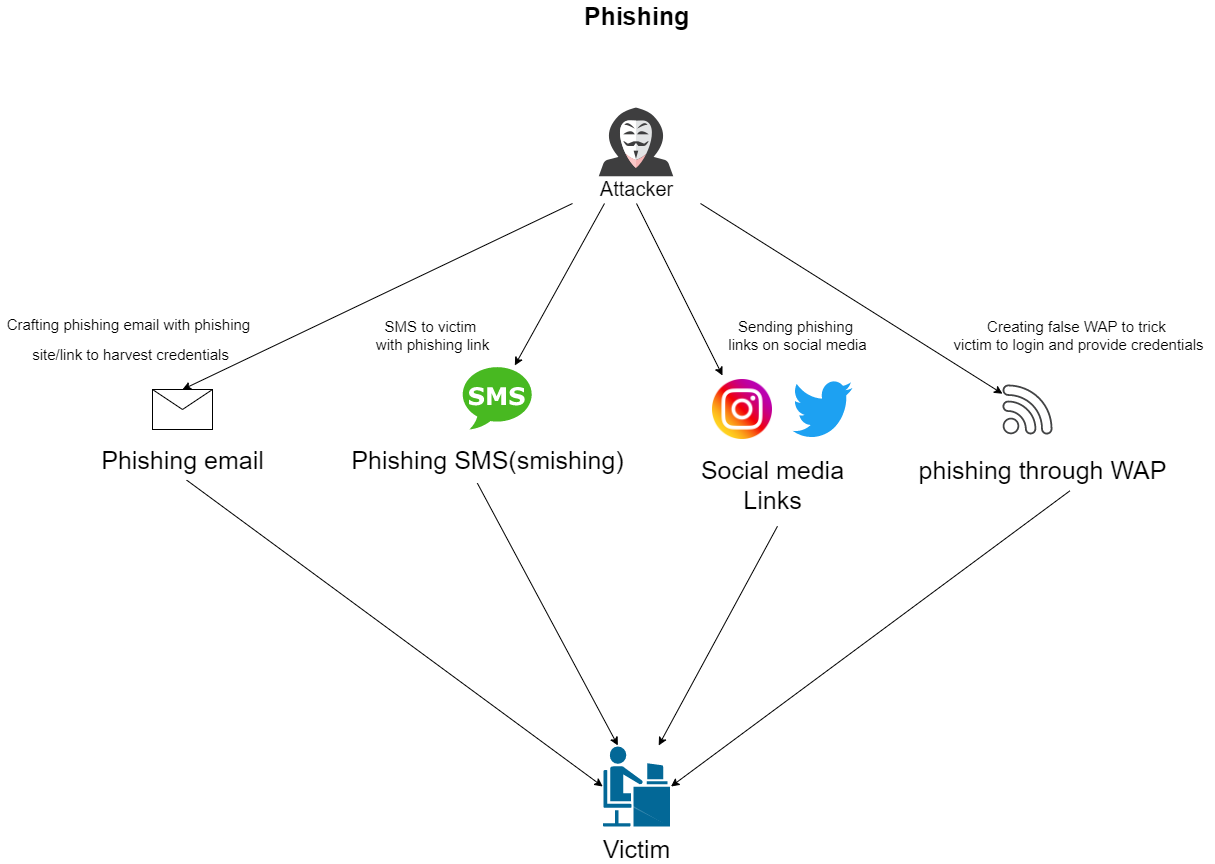
**Integrity**: when we collect the sensitive information, we can modify it to make it corrupt or lost

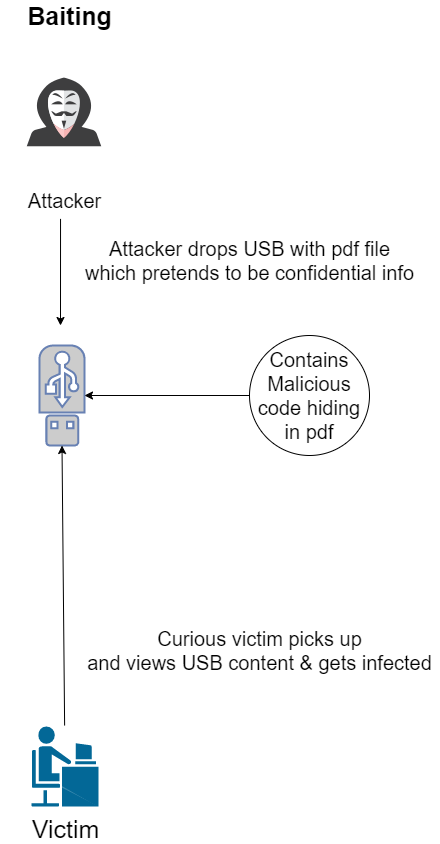
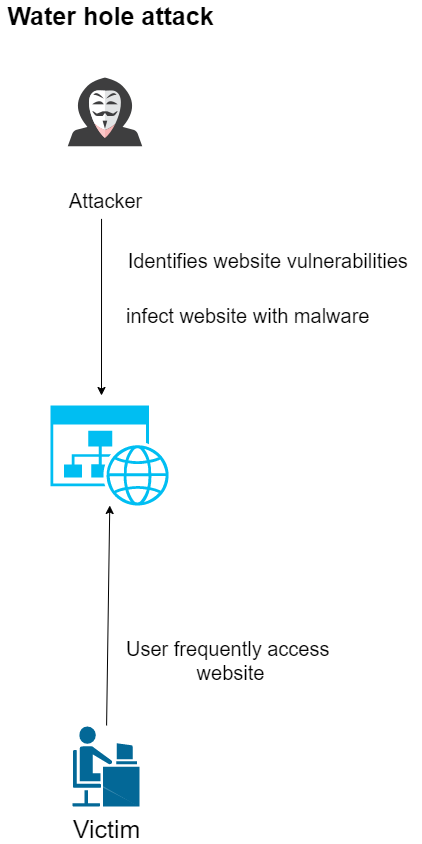
**Availability**: once we have the user data, we can prevent the authorised access of the data

**Platform and tools used**

The platform we will be using is kali Linux as the attacking machine, and other tools such as Blackeye, SET (social engineering toolkit), Wifiphisher and Metasploit. We will utilize passive (Methods that do not engage the target) OSINT tools such as The Harvester, Google Hacking, Sherlock and PhoneInfoga. To simulate our attacks our victim will be running a windows 10 Home x64 as the operating system of choice.

**Experimental setup**





**Test cases/scenarios and expected results**

Most of the scenarios are going to be remote and will be focused primarily on Phishing and the different kinds of phishing as the other

|  |  |  |
| --- | --- | --- |
| Test Case | Scenario | Result |
| Phishing | Phishing mail | Gain credentials |
|  | WIFI phishing | Gain credentials |
|  | Smishing | Gain credentials |
|  | Social media links | Gain credentials |
| Baiting | Dropped USB | Infect Target |
| Water Hole | Infect Xss Vulnerability | Privilege escalation |
|  |  |  |
|  |  |  |

**Tools:**

SET (Social Engineering Toolkit)

<https://null-byte.wonderhowto.com/how-to/use-set-social-engineer-toolkit-0147454/>

Blackeye (social media & Account phishing)

<https://null-byte.wonderhowto.com/how-to/phish-for-social-media-other-account-passwords-with-blackeye-0196790/>

Wifiphisher (Gain access to wireless networks)

<https://null-byte.wonderhowto.com/how-to/hack-wi-fi-get-anyones-wi-fi-password-without-cracking-using-wifiphisher-0165154/>

Metasploit(Discovering vulnrabilities)

<https://www.imperva.com/learn/application-security/metasploit/>

The harvester method to get information entered or credentials

<https://pentestlab.blog/2012/02/24/credential-harvester-attack-method/>

The Sherlock tools

<https://null-byte.wonderhowto.com/how-to/hunt-down-social-media-accounts-by-usernames-with-sherlock-0196138/>

Phoneinfoga

<https://secnhack.in/phoneinfoga-osint-tool-for-phone-numbers/>

**Potential Challenges:**

The Major challenges we might face in regards to phishing is setting up the fake persona of a user and then trying to dig as much information on that particular user. In regards to the Baiting while infecting the Virtual machine we may also infect the host machine therefore we need to be careful and use the virtual machine as a sandbox by not using any shared (host to VM) services. We might also need time to learn the usage of all the tools given to simulate the attacks mentioned.

Time and Milestone:

* 29th - 6th: installation and learning of Tools
* 7th - 15th: Performing simulated attacks
* 15th - 21st: Reporting of Findings