Instructor Demo: +

SY306 Lab 13

Credential Harvesting

Introduction

As the last lab in the course, this assignment will require you to demonstrate and tie together various technical concepts, using team initiative and research to come up with appropriate technical solutions. This lab will be directed at a target already identified and researched as part of a SY304 project from Spring 2019. Teams should consist of 2 or 3 members, one of which must be presently enrolled in SY304. **Once decided, let your instructor know the membership of your team for this lab**.

Section 4341 & 5551 team assignment information.

Requirements

A. Phishing Email: [20 points]

1. Create a phishing e-mail specifically directed at people or a person from one of the targets chosen by the SY306 team member presently enrolled in SY304 (i.e. TFES.org, Rutabaga Juicery & Eats, Buddy's Crabs & Ribs, Starbucks, 49 West Coffeehouse, Winebar & Gallery, Taco Bell, SeaWorld, or others...)
2. The email should be drafted in HTML, use an effective social engineering approach and have a format similar to the following:

```
Date: Wed, 10 Apr 2019 20:34:42
-0400
Subject: [SUBJECT HERE]
From: [SENDER ADDRESS]
To: [RECIPIENT ADDRESS]

Lorem ipsum dolor sit amet,
consectetur adipisicing elit, sed do
eiusmod tempor incididunt ut labore
et dolore magna aliqua. Ut enim ad
minim veniam, quis nostrud
exercitation ullamco laboris nisi ut
aliquip ex ea commodo consequat.
Duis aute irure dolor in
```

```
reprehenderit in voluptate velit
esse cillum dolore eu fugiat nulla
pariatur. Excepteur sint occaecat
cupidatat non proident, sunt in
culpa qui officia deserunt mollit
anim id est laborum.

Lorem ipsum dolor sit amet,
consectetur adipisicing elit, sed do
eiusmod tempor incididunt ut labore
et dolore magna aliqua. Ut enim ad
minim veniam, quis nostrud
exercitation ullamco laboris nisi ut
aliquip ex ea commodo consequat.
Duis aute irure dolor in
reprehenderit in voluptate velit
esse cillum dolore eu fugiat nulla
pariatur. Excepteur sint occaecat
cupidatat non proident, sunt in
culpa qui officia deserunt mollit
anim id est laborum.

Click here for more information.

Sincereley,

Sender
```

3. The link in the email should take the 'victim' to the website you will make next.

B. fake / spoof website to harvest credentials [30 points]

1. Create a spoofed website of a real site that has the ability to steal and harvest credentials.

2. Ensure the spoofed website looks as similar to the real site as possible and maintains normal functionality. At a minimum it should have:

    a. A username and password login.

    b. An exact visual appearance to the original site.

    c. The exact same favicon in the browser tab.

    d. 'Normal' behavior when the user provides their credentials.

3. **For 20 points extra credit:** Research and successfully implement tab nabbing as part of the process to steal the user's credentials.

Instructor - Sample Tab Nab Code: +

C. python script to receive credentials and write them to persistent storage (file, db, etc.) [40 points]

1. Create a Python script to receive the credentials from your spoofed side and write them to persistent storage (file, db, etc.)

D. Final Steps [10 points]

1. **Documentation:** Ensure you have appropriate comments in your Python script.

2. You should have the following four links on your `default.html` under the heading **Lab 13**.

   a. A link to the phishing e-mail.

   b. A link to the spoofed website.

   c. A link to the real/original (non-spoofed) website.

   d. A link to the file/db collecting all the harvested data.

NOTE: Each of the four links need to be on each team member's `default.html`

Additional Guidance

- Grading will be based on the effective use of social engineering tactics to draft the phishing e-mail, proper website / server-side script functionality, similarity of spoofed website to the orignal, technical difficulty, and proper use of a SY304 project target.
- While current SY304 students have used Social-Engineer Toolkit (SET) to demonstrate attacks this semester, SET can **NOT** be used in this lab. Use this lab as an opportunity to demonstrate the technical skills you have learned this semester in SY306!
- If necessary, research a tool called `wget` to clone / scrape websites.
- The Navy Federal website **can not** be used / spoofed in this lab to meet the requirement of part B above

Deliverables

1. You should have all the pieces working as described in parts A, B, and C of the "Requirements" section above.

2. You should four links in your `default.html` as specified in part D of the "Requirements" section above.

3. All of your files should be in a folder called "Lab13" (without the quotes) in your `public_html`. Your instructor will assume that your files viewable at http://midn.cs.usna.edu/~m21xxxx/Lab13/

4. **Turn in:**

    1. **Paper submission:** turn in the following hardcopy at the beginning of class on Monday, April 22nd, stapled together in the following order (coversheet on top):

        1. A completed assignment coversheet. Your comments will help us improve the course.

    2. **Electronic submission:** Submit all Lab13 files via the online system: `submit.cs.usna.edu` by 23:59, Sunday, April 21st