CIS 6930/4930: Practical Cyber Security

Assignment 2: Web Hijack

Due Date: 04/02/2018

Objective

You come across a very popular website visited by many people every day. Your task is to hijack as many of the visitors' devices as you can.

Assignment Setup

You are given a Windows XP SP 2 VM. Please import it into VMware and run it. You should find a file exploit.html on the desktop. Test the PoC exploit on the VM and make sure it works. You need to first replace the shellcode with the one that will deliver the shell to your local machine.

The target website IP address will be emailed to you. Please only use the IP assigned to you and do not try to attack other IPs.

Download the windows xp virtual machine from following link:
https://drive.google.com/open?id=1iMFy3I1L0FWhVgW9U_-i3q01bIDbT3dC

Assignment Requirements

We know the following:

- Many of the people who visit this website are still running Windows XP SP2 and use Internet Explorer (IE) for browsing.
- You must be able to compromise the machines of anyone who visits this website using XP SP2 (like the provided VM). For the purpose of this assignment, your shell needs to be returned to a C&C server at **10.247.49.159**, at a port number assigned to you
- You must do this as stealthily as possible, i.e., the person visiting the website must not suspect that there is something fishy going on. This ensures that you pwn the maximum number of devices before being discovered.

What you need to submit

1. A one-page report that documents the steps you took to accomplish the task.
2. Source code of the webpage exploit.

Testing in Grading

We will visit the website you took over using Internet Explorer and hope to get a shell back on the C&C server under the port assigned to you.