writeup

Kevin Turkington

I. Overview

In Cedric Cochin's lectures he reviews alot of materials that have been said in previous lectures such as man in the middle attacks, network policys, and several browser exploits. However he expands on these methods to slightly to use as a segway into a non technical form of infection for users computers. He describes any companies least secure layer despite top notch security at every other layer to be the users (employees) themselves. Because the security analyst or networking admin may be versed in social engineering attacks, doesnt mean the employee themselves are as protected and aware too.

II. Non technical attacks

There is a number of non technical attacks that prey on a variety of different user tendencies and behaviors. The most prevalent and a method I have fallen for is simply clicking on links that have been served to the user. In these click bait like attacks a url pointing to a domain infected by malicous JavaScript is sent to the target user in the form of an email, instant message, or general link on a forum. Another click based attack is enticing users with clickable objects or animations, preying on user curiosity. Malwaretising is a significant problem in cyber security because of its prevalence in ads and masquerading as anti-viruses or updates for windows machines. When in reality the software being downloading is full of malware ranging from spyware to trojans and rootkits.

For a more complex approach to user infection ofuscated of URLs this can be a collection of different ways to manipulate a URL. Such as making similar looking urls, matching characters together that look like another, or even hiding malicious content though the use of long query strings. Some examples can look like combinations of Google, docs, drive, or gmail.

The most interesting of all the attacks is Social Engineering, often preying on unknowing employees of target companies to gain physical access to machiens. A great example is Jack Morse Article "Even the best passwords are no match for social engineering" describes a hackers ability to trick employees of apple that s/he was a reproter named Mat Honan gaining access to the reporters iCloud. Simply by answering security questions and making accurate guesses to what they may be. Without any knowledge to the reporters password what so ever.

Complete Compiled list of attacks:

- Click bait links
- Fast moving animations

- Obfuscated URLs
- Social Engineering
- Malwaretising
- Waterhole targeting

III. Technical Attacks

As for the new content given by Cedric Cochin in terms of technical attacks was his in depth analysis on taking advantage of programming mistakes during development. Specifically mistakes and loopholes in web development that can lead to SQL injection, click jacking, and other general man in the browser attacks. For example if a field seems to be using eval for parsing information that field can be used to place a number of different types of malicious content like the following:

```
--Source: https://stackoverflow.com/questions
--        /3476765/mysql-drop-all-tables-ignoring-foreign-keys

SELECT concat('DROP TABLE IF EXISTS ', table_name, ';')
FROM information_schema.tables
WHERE table_schema = 'MyDatabaseName';
```

IV. URL Defense

As for the various defenses methods described in Cedric's lecture as a combination of different high and low throughput methods. Such as the following:

- Manual
- Low Interaction
- Static
- High Interaction
- lexical

Each having their own strengths and weaknesses. Manual has low throughput because of the general use of web research on the website. Low interaction is simplifying loading the website on a virtual browser and waiting for scripts to load or execute. High interaction requires the virtual environment to randomly or programatically click and access content within the page. And lexical classification makes a educated guess based of certain weights from known sets of data similar to this weeks lab.