Week 7 writeup – Brennan Giles

Lecture 1

This was my new favorite week of material as we talked primarily about web based attacks and security with our new lecturer, Cedric. Our main topics were the web/ how it works (Jscript, PHP, etc), web as a threat delivery mechanism, web attack vectors, and how to analyze web weaknesses as well as protect against those vulnerabilities.

The web is the primary method of delivering malware as 95% of it is delivered through the web. It can be delivered through browser extensions, scripts, raw html, or into http injection points. Most web attacks are targeting the user as they are almost always the weakest link; users are impatient, lazy, think they are smarter than they are, and most importantly love to click places they shouldn’t. Malevolent forces can take advantage of these shortcomings through many different avenues of attack such as Phishing, SEO poisoning, Fake AV “updates”, Social Media Link Insertion, Forum Link Insertion, and Malvertising. Two of these I wasn’t aware of directly and I will expand on them; SEO poisoning is when trending topics are gamed so that users looking for the latest gossip on hot topics are suggested to go to malicious sites, which soar to the top 20 google suggestions thanks to a botnet encouraging its popularity. Malvertising is when advertising networks targeting specific demographics are taken advantage of so that Malware can be delivered to the most vulnerable individuals.

Some ways to protect against these attacks are through URL/Domain Reputation systems, certification systems, safe URL shorteners, Content provider education, and End user education. Putting a big red X next to dangerous sites helps non-internet savvy people avoid clicking the wrong links.

My favorite part of the lecture included SQL injection, which was fun to go more in depth about. The idea behind SQL injection is that since most sites are DB-driven, we can use unprotected SQL queries that we put in unintended places to access and parse their database for our own gains. An example he used was ‘ or ‘1’=’1’ – ‘ which appends to the original query that if 1=1 that the person should be granted access. Since most of the time these fields are protected (at least in more modern websites) there are other ways to access as well, such as removing fields with no error handling by inspecting the html code. XSS is an interesting interpretation of injection, where instead of manipulating the SQL to get access to the website we instead manipulate the JS of the website (or the DB of the website so we can put our own JS in) so that other users that trust the website access our malicious script. URLs can also be manipulated to appear trustworthy but be hiding script tags inside that redirect you to bad sites.

Lecture 2

For the second lecture we finished up some ideas from the last lecture and continued our discussion about web as a threat delivery mechanism and how users can be fooled into clicking your evil link. For this lecture we learned about how to investigate website weaknesses, automate SQL injection, learn more about website vulnerabilities, and how URL classification works. Some excellent research tools are PhantomJS and burp suite (I’ve used burp before its great) as well as firebug and web scarab. Cedric also went into how URLs and site activity can be used to automatically analyze whether or not it is to be trusted and try to suggest to users how to proceed based on those findings. I really enjoyed this week’s topic and I look forward to completing the hw assignment…