Vulnerability Research and Exploits

Part A

Security engineers see the world differently than other engineers. Instead of focusing on how the systems work, they focus on how the systems fail, how they can be made to fail, and how to prevent or protect against those failures. Most software vulnerabilities don't ever appear in normal operations, only when an attacker deliberately exploits them. So security engineers need to think like attackers. This mindset is difficult to teach, and may be something you are born with or not. But in order to train people possessing the mindset, they need to search for and find security vulnerabilities again and again and again. And this is true regardless of the domain. Good Cryptographers discover vulnerabilities in other's algorithms and protocols. Good software security experts find vulnerabilities in other's code. Good airport security designers figure out new ways to subvert airport security.

Vulnerabilities are weaknesses in the system design, implementation, software or code, or the lack of a mechanism. Vulnerabilities and weaknesses are common with software mainly because there isn't any perfect software or code in existence. Vulnerabilities in software can be found in: firmware, operating systems, configuration files, application software and patches.

An exploit refers to a piece of software, tool, or technique that takes advantage of a vulnerability that leads to privilege escalation, loss of integrity, or denial of service on a computer system.

In this assignment you will be required to search for vulnerabilities that are found in applications, network, and protocols. Identify ten vulnerabilities and find exploits that can take advantage of these vulnerabilities. You will be required to demonstrate how the exploit will work. Please note that some of the exploits are malicious, therefore, the demonstration is just being able to compile and run the exploit. You can use search, Google Hacking techniques or vulnerability assessment tools such as Metasploit (www.metasploit.com/), Nikto (http://cirt.net/nikto2), Firebug (https://getfirebug.com/), SAINT (http://www.saintcorporation.com/) and OpenVAS (http://www0.atomicorp.com/index.html) to identify vulnerabilities.

Part B

In this part you will be required to demonstrate the use of the following vulnerability assessment tools:

1. Metasploit - http://www.metasploit.com/
2. Nessus – http://www.nessus.org/products/nessus
3. Identify one vulnerability scanner and demonstrate its use in the presentation.

Part C

In this part of the assignment you will be required to identify and list major vulnerability databases and/or repositories in use currently in vulnerability research. If possible identify and list databases and/or repositories of exploits. Finally, include in your report anything (video, software, shell command etc) related to vulnerabilities and exploits that you think the rest of the class may find useful when they join the workforce as penetration testers or ethical hackers.

Each student will be required to submit a report of at most five pages describing what you have achieved in this assignment. The presentations for this assignment will be done in the lab at the date we will agree during the lecture.