ISEC 325 Homework 09

Answer the following questions based on your reading of the text books, the module key points, and the instructor's presentation this week.

1. [3 points] What is SMTP used for? What are some common attacks against SMTP servers?

   SMTP is used to send Internet mail. Some of the main attacks against SMTP servers are attackers or malicious software using email servers to send messages. If an email server administrator does not restrict who can use the SMTP server, it is called an open relay where attackers can search the internet and find the open relay and utilize the server to send messages unauthorized. The attacker using the open relay is anonymous and worms can also utilize open relays to spread themselves. Mail bombing is another type of attack on a SMTP server, mail bombing is the equivalent of a denial of service attack on the mail server. The attacker sends a flood of email to the server in order to crash it in a mail bomb.

2. [3 points] What is LDAP used for? What are the common attacks against LDAP servers?

   LDAP is lightweight directory access protocol and is a communication framework with centralized directories that hold a variety of useful data. There are six different standard operations that LDAP performs: authenticating to the directory, searching the directory, reading attributes from the directory, adding entries to the directory, modifying entries in the directory and removing entries from the directory. LDAP is like active directory and holds sensitive data. The common attacks used against LDAP are similar to SQL injection attacks, LDAP injection attacks are made from a web browser where the attacker attempts to use (inject) code into server to modify, insert, and delete data from the LDAP server without proper authentication.

3. [2 points] What are the typical teams involved in contingency planning and contingency operations? What are their responsibilities?

   The typical teams involved in contingency planning and contingency operations are The CP management team who's responsibilities are developing a master plan for all contingency planning operations, collecting information about information systems and the threats they face, conducting business impact analysis, organizing and staffing the leadership for the subordinate teams, and providing guidance to and integrating the work of the subordinate teams. The incident response team develops, tests, manages and executes the incident response plan by detecting, evaluating and responding to incidents. The disaster recovery team develops, tests, manages, and executes the disaster recovery plan by detecting, evaluating, and responding to disasters and by reestablishing operations at the primary business site. The last is the business continuity team which develops, tests, manages, and executes the business continuity plan by setting up and starting off-site operations in the event of an incident response or disaster.

4. [3 points] What is SQL injection and how does it work? What are some recommended methods to combat SQL injection?

   SQL injection is a type of attack where the attacker attempts to use SQL code in entry fields of a web application to modify, delete, insert, get or any other type of SQL command to gain access or manipulate data on the SQL server. The deadliest command would be to drop the database which will delete the database. In order to combat SQL or any other type of injection the programmer or developer must use code sanitation where special characters are sanitized. Sanitizing is the process of making those characters which hold programming meaning into a typical ascii standard character that holds no programming ability. For example, an attacker may use any field of a form to enter <banner> Don't use this website the owner has scammed several people out of money</banner>. By using the command, a banner message comes up on the website when it is accessed. If you sanitize the code it removes the ability of the tags and just types the message in the field. Some other things that help against SQL injection are making sure there is limited access to the web application within the database. Using prebuilt statements that do not take user input, instead of sending SQL queries to the database, invoke stored procedures to take the appropriate actions on the database data, Scrubbing the data is the process I described above, and using white lists which indicate which type of data is acceptable and discard the rest which is part of the program and process of sanitizing the code.

5. [3 points] What is an XSS attack and how does it work? What are ways to prevent XSS attacks?

   Cross side scripting is when a server sends unverified data to the client and the client in turn executes the code that exploits the web browser. Attackers find web sites that display user input back so they can see if the results are scrubbed or not. Attackers can use the web sites to redirect users to malicious sites with cross side scripting. Ways of preventing cross side scripting attacks are making sure that untrusted data cannot be inserted into the HTML that is returned to a client or into URL parameters passed to the Web application. Scrubbing the data so that script tags and special character code does not function. You can also scrub the data inputted of special characters.

6. [2 points] What are the major steps in a business impact analysis? Briefly describe what happens in each step.

   1. Determine mission/business processes and recovery criticality. Mission/Business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum time that an organization can tolerate while still maintaining the mission.

2. Identify resource requirements. Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.

3. Identify recovery priorities for system resources. Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources.

7. [3 points] What are some ways to harden a web server?

Upgrade and patch the underlying operating system and web server software, limit user accounts, enforce a strong password policy and monitor user activity, remove or disable unnecessary applications, services and communications, limit access to sensitive OS and web resources, make sure applications do not run with administrator privileges, do not use links in the public web content to point to other fields or directories on the host or other network systems, don't allow search engine indexing on sensitive web directories, and control access to specific pages and directories to ensure proper authorization.

8. [6 points] Watch this video on BeEF (the Browser Exploitation Framework) for remotely attacking a web browser via XSS: http://www.youtube.com/watch?v=utPBQOZS_TU. Also, do some research into BeEF (http://beefproject.com/).

a. What are your observations about how this process works and the tools used to carry out the attack?

Beef is a cross side scripting tool where you use predetermined web address code to cross side script with JavaScript connecting the target web site to your instance of the beef software. From the beef software you are able to execute a wide variety of cross side scripting attacks on the web site.

b. Who must take steps to prevent a browser from being exploited by XSS?

The programmers and developers must prevent the browser from being exploited by scrubbing the data that is entered into fields on the web site.

c. Since BeEF hooks to Metasploit, is there any safe way to use the web today? Explain.

The safest way to use the web today is to use anti-virus, firewalls, vpns, and ensure you are connecting via https. Keeping your browser up to date with the best security add ons and plug ins also helps. Common sense is what most users are short on but can also go a long way, you can stay away from web sites that are magnets for trouble.

9. [5 points] In two to three paragraphs of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered in the class session this week. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you're still confused about. In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Feel free to ask questions in this as well since it will be returned to you with answers.

I have been sick and quarantined so that is why I wasn't at the MEET session on Thursday. I listened to it and got a lot out of it. The MEET sessions are nice because they provide insight the book does not. I took WEBD236 last semester where you work with applications using php and html. I wasn't a big fan with the way the coursework was set up however I learned a lot about SQL and SQL injection as well as hashes. We used code to scrub input data by making functions set on the php controller that sanitized the code. We briefly talked about cross side scripting however I have a much deeper understanding of how it works now. One thing that we also covered was ensuring that an attacker could not manipulate the URL to access areas of your website you did not want them too. We also covered cookies and protecting them with HTTPS connections so that an attacker could not obtain cookies to gain access to sessions.

The BEEF tutorial was very interesting to me. I feel like we are living in the wild west right now. I can't believe that developers openly develop tools and code that appear to be directly used for malicious purposes. Those developers are like arms dealers who are selling weapons to both sides. I cannot believe there has not been any regulation against them. Even if an attack can be traced back to the attacker and that attacker is apprehended millions of dollars can be lost. When I attended the 614 con hacking convention, I had an awesome opportunity to talk with mentors from many different organizations and a cool security professional told me that API security was blowing up. The cross-side scripting attacks and injection attacks must still be a major part of cyber security. I am glad I have learned about them in both the classes I have taken. This is turning out to be my favorite cyber security class so far. I have learned more in the course than the ones I have taken in the past.

References

Engebretson, P. (2013). *Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Elsevier Science and Technology Books.

Whitman, M. E. (2012). *Guide to Network Security, 1e.* Cengage Learning.