**Lesson 2.3 – Server Exploits**

**\*\*Instructions:** Please change the text color of your responses to red text. Please organize the endings to each page.

**Activity 2.3.4 – Find the Exploits**

1. Document the XSS stored exploit script: Use the View Source feature of the web page and create a screenshot of the few lines of code that could have prevented an XSS stored exploit had the programmer used them. (Show just the relevant lines of code, not the entire script.) (Step #7)
2. Save a screenshot of your entire Wireshark window with the Packet List showing the suspicious packet and the Packets Detail pane showing the exploited content. (Step #8)
3. Document the command execution exploit: Use the View Source feature of the web page, highlight the few lines of code that could have prevented a command execution/injection exploit (not the entire script), and save a screenshot of the script. (Step #10)
4. Save a screenshot of your entire Wireshark window with the suspicious packet in the Packet List and the exploited results in Packet Details. (Step #11)

**FIND THE EXPLOITS**

**EXPLOIT #1**

1. **Find the suspicious packet**
* **Hint 1: Ask, “Which page might an attacker use to run their script?” (XSS reflected or XSS stored)**
* **Hint 2: Find existing content on that web page in Wireshark’s packet details.**
* **Hint 3: Existing content could be, “This is a test comment.” You can find this string in Packet Details.**
* **Hint 4: Look for suspicious content following the legitimate content you searched for. Since you suspect a script attack, the suspicious content may not look like the output generated by the script, but rather the script itself.**
1. **Identify the web page and the few lines of code that prevent this vulnerability.**
* **Hint 1: Consider that a script was used and appears to be (stored) in the contents of the web page.**
* **Hint 2: Use the Find feature in Packet Details to search for the contents of the web page you suspect was used for the exploit.**
1. **Document your work. Sample answer: The compromised information is the cookie data of the user who’s visiting this page.**

**EXPLOIT #2**

1. **Find the suspicious packet**
* **Hint 1: Ask, “Which page might an attacker use to illegally access a web server’s database?” (SQL Injection)**
* **Hint 2: Search for existing content on that page.**
* **Hint 3: Existing content could be “User ID”. You can find this string in Packet Details.**
* **Hint 4: Legitimate SQL queries may be used to hide the suspicious one.**
* **Hint 5: Look for large blocks of data that don’t appear in the other legitimate queries.**
1. **Identify the web page and the few lines of code that prevent this vulnerability.**
* **Hint 1: The attack appears to be a complex SQL command (select ... from ... where ...).**
1. **Document your work. Sample answer: The compromised Information is a bit difficult to determine. However, looking carefully at packet 265 Packet Details, admin data may have been stolen, including a phone number and an address. Observing packet 298 Packet Details, user information could have been stolen, including usernames, passwords, phone numbers, and addresses.**

**EXPLOIT #3**

1. **Find the suspicious packet**
* **Hint 1: You should know the output of the ping command (shown in Packet Details) to identify suspicious output.**
* **Hint 2: Find the string "ping" in Packet details to find the output of the command.**
* **Hint 3: Look at the output ("ping statistics") in Packet Details and compare legitimate results to suspicious results.**
1. **Identify the web page and the few lines of code that prevent this vulnerability.**
* **Hint 1: What kind of exploit do you think this was? Was a command executed? (yes, the ping command)**
1. **Document your work. Sample answer: Compromised information: The compromised information appears to be network architecture information including the Ethernet addresses and IP addresses of the system.**