Computer Security – Lab 4
Infamous Exploits

Thomas Kerber

November 26, 2016

1 VM Setup

For this exercise, you will be utilising a virtual machine, to make sure your DICE account isn't compromised by running a vulnerable server. Import '`/group/teaching/cs/exploits-lab.ova`' into VirtualBox. Start the virtual machine. You will not be able to login, but the web server running on it should be accessible from DICE, by navigating to `https://localhost:8081`. Your browser will warn you about an insecure connection. Add a security exception and proceed. This is due to various certificate issues, and not the vulnerabilities you will be exploiting in this lab.

2 Heartbleed

The server is vulnerable to the heartbleed exploit. Research how the heartbleed exploit works, then modify the script '`/group/teaching/cs/heartbeat.py`' to perform the exploit. The script executes a TLS hello, followed by a TLS heartbeat. You will need to modify the packets sent, not the code used to send them.

3 Shellshock

The server is also vulnerable to shellshock. The page at `https://localhost:8081/cgi-bin/uptime.sh` uses a vulnerable version of bash to generate the page. Research how the shellshock exploit works, then perform it. Try to deface the main web page using it.