Johns Hopkins CS600.424: Network Security Spring 2012

Homework 3

The following homework specification sheet will serve as your own personal checklist as you move through the simulation. When writing up your results, you may simply create a scheme that lists the heading and then addresses each task item highlighted below.

For example:

Practical Web Security

Task 1.	I have…itidentifiedis…oftypethe vulnerability in this problem
Task 2.	<script>malicious script here.</script>
Task 3.	The vulnerability in

You will be provided with an Ubuntu Server 10.10 virtual machine that contains all required dependencies to complete this assignment.

The virtual machine image can be downloaded from:
http://dl.dropbox.com/u/65446573/Net%20Sec/Ubuntu-Server.vmwarevm.zip
VM login credentials: user/user.

VMWare 8 for Windows
http://dl.dropbox.com/u/65446573/Net%20Sec/VMware-workstation-full-8.0.0-471780.exe
Serial: JM211-Q830K-189Y4-AUCU4-0HN4J

VMWare Fusion for Mac OSX
http://dl.dropbox.com/u/65446573/Net%20Sec/VMware-Fusion-4.0.1-474597-light.dmg
Serial: 10083-Z9311-N81Y4-AH82M-14ZNJ

Congratulations,

We would like to officially extend an offer of full-time employment to you as our sole network security consultant! As you may know, Freedom of the Fish, a new subsidiary of Awesome Corp, has been charged with the practical implementation of a customer service portal that provides guarantees of high availability, usability, and security. These guarantees enable us to meet our end goal of providing an accessible online application that enables professional services on the practice of caring for *really expensive fish*.

Your new boss and CEO, Ms. Alice, is very invested in the security and privacy of our customers, and as such she has a few initial assignments for you to complete in a timely manner. To begin your assignment, simply follow the instructions below. Good luck!

Practical Web Security

Freedom of the Fish is planning to implement a Linux Apache2 MySQL PHP Perl (LAMPP) server, via Any-OS Apache2 MySQL PHP Perl (XAMPP) software package, to provide potential web service(s) to their customers. Your first assignment is to:

1. Execute the ~/start.sh script to start the appropriate web services, and receive your specific URL to visit on the host machine.

2. Choose a language at the top to start the navigation of the default pages. Now that we have access to the default pages, it is time to brush up on your Cross Site Scripting skills (XSS)!

3. Navigate to the Guest Book page from the left hand navigation menu.

a. There is a known XSS vulnerability on this page.

b. To find this vulnerability, we will take the naive approach of fuzzing with the following string <script>alert('found it');</script>

c. **TASK 1*** Once you have identified the vulnerability, write 1-3 sentences as to what type of XSS this is (persistent or non-persistent), and what security implications it has (i.e. what is its effect on other viewers).

d. **TASK 2*** Now that we have identified the vulnerability, let's do something a bit more malicious with it. First notice that this is a Perl script; so without looking at the Perl source directly in the terminal, use your browser to view the source. Look around at the form, and than execute a script injection that will automatically play a wave audio file anytime a user accesses the guest book page. (Hint: Take a look at the html tag "embed" and a wave file named warning.wav is already provided in the XAMPP folder).

e. **TASK 3*** Having successfully brushed up on your XSS scripting skills, follow the XAMPP symbolic link in your home directory, locate the source of guestbook-en.pl, and then open it with your favorite editor (i.e. nano or vim). Reviewing the source, write 1-2 sentences identifying the vulnerability that allowed the attack and how to mitigate it.

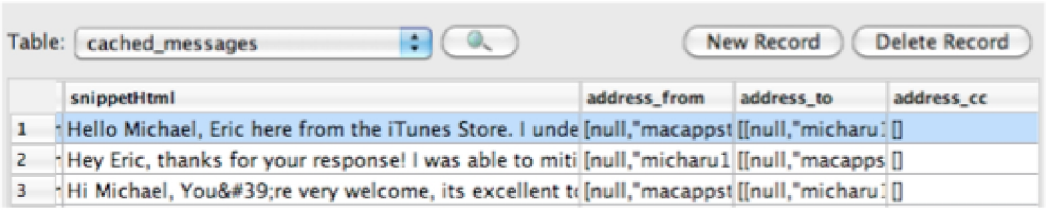
1. Navigate to the CD Collection Page from the left hand navigation menu.
   a. There is a known SQL Injection vulnerability on this page.

   b. A SQL injection vulnerability presents itself through an unsanitized input form field that manipulates a back-end database. Being that all input is accepted, a malicious user could provide a string that closes the form's intended query, and executes SQL of the user's choice.

   c. **TASK 4*** Your job is to examine the vulnerable form field, the one which allows the end user to view soon to be added CD records by providing the artist of the CD, and provide an injection script that will print all the CDs in the database without knowing the artist. Please provide your injection string, as well as a 1-2 sentence description of how to mitigate such a vulnerability. (Hint: The Wikipedia page http://en.wikipedia.org/wiki/SQL_injection is a good starting place on learning basic SQL injection)

Just as you finish your security review of the above, you are approached by a frantic member of the company's web application development team. The team has been charged with the completion of an early design phase objective that will provide an official recommendation of application resources/development framework(s), providing the final foundation for the company's online application.

The group is currently caught in a debate of whether they should include the latest supported HTML5 tags, or wait for the implementation to be solidified later on. You, having already experimented with HTML5 local storage, argue that such tags need to better scrutinized and standards improved prior to implementation on a commercial application. To prove the point, you took the following screenshot of a Safari local storage for Gmail. Carefully take note of what information is collected on the local machine:



1. **TASK 5*** The web team asks that you provide a formal write up, one paragraph, concerning the implications of HTML5 local storage, and how might they be mitigated. For more information check out the following resources:

a. http://michael-coates.blogspot.com/2010/07/html5-local-storage-and-xss.html

b. http://www.veracode.com/blog/2010/05/html5-security-in-a-nutshell/

c. http://www.eweek.com/c/a/Security/HTML5-Security-Facts-Developers-Should-Keep-in-Mind-551353/

2. Note that these references take varying positions, and you should do the same. This task depends on your interpretation, and hopefully it will lead to you to explore HTML5 in more depth.

Practical Network Security

There have been complaints filed by employees that co-workers have been download applications from Internet from 4shared.com. As such, you are asked to:

1. Disallow access to the site providing the applications, .

   a. In Linux we can restrict access to specific websites by adding 0.0.0.0 <site root url> to the /etc/hosts file.

   b. To begin, let us use the terminal command: lynx 4shared.com. Notice that the web page is rendered in text because we have not yet disallowed it. Also, ping 4shared.com, and note the ip address.

   c. **TASK 1*** Next, modify the /etc/hosts file using the convention described above, with DNS translation of 4shared.com, to disallow access to 4Shared for all users. Again, lynx 4shared.com, and ping 4shared.com. Please provide one-two sentences of what you see, and why this is the expected result.

   d. **TASK 2*** Finally, you are to report back to management that even though we have disallowed 4shared.com, employees may still be able to access the website via a web proxy. You will be tasked with explaining a proxy in depth during a later task, so for now you are tasked with writing a simple list of steps to connect to a web proxy (i.e. hidemyass.com/proxy) via lynx, and than using the proxy to successfully connect to the www.reddit.com page.

2. Configure our server's firewall to disallow unintended usage.

   a. Take a look at netstat –a(n). Note the active connections for our web application, and open sockets that couple with that application.

   b. While scanning the list, you should notice one active connection that is running on port 9999. This is a python server that is ran whenever you run your start.sh, and thus not malicious. However, the intention of this script is to help you consider the broad surface of (non) malicious applications that establish services, sockets, daemons, etc. on some port - even though you might not want them too.

   c. As such, you are to block all incoming/outgoing connections except those for ssh, http, and ftp (for everyone) using Linux iptables.

      i. **TASK 3*** Write a script (Python / Perl / BASH) that will automatically setup the appropriate iptables configuration to meet the above specification. Be sure to test your implementation by attempting an FTP connection and trying to connect to a https web page such as https://google.com using lynx. Please provide the full script in your submission. In case you need to reset the iptable rules to their defaults a BASH file is provided fixIP.sh

ii. **TASK 4*** After completing the above, consider the different approaches to writing firewall rules. Do you prefer a whitelist approach appropriate where you block certain connections as needed; or do you prefer a blacklist approach appropriate where you block all connections, and open ports as needed. Please provide 1-3 sentences concerning your preference, and why.

You should be able to find a good amount of information concerning iptables all over the web. To get you started, here is a simple script skeleton:

```
#!/bin/sh

# Flushing all rules.
# -F (flush) ; -X (delete policy chain)
iptables --flush
iptables –delete-chain

# Setting default filter policy
# -P (policy, chain target)
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Allow ssh

iptables -A INPUT -p tcp --sport 513:65535 --dport 22 -j ACCEPT

iptables -A OUTPUT -p tcp --sport 22 --dport 513:65535 -j ACCEPT

# Nothing comes or goes out of this box.

iptables –A INPUT –j DROP

iptables –A OUTPUT –j DROP
```

Proxies

Your final assignment has to do with a recent issue that HR has reported to Ms. Alice. It would seem that employees have been using web proxies to access restricted content over the network, FTP proxies to bring in content from their home network, and other sorts of mischievousness. She would like for you to provide her a written summary, 1-2 paragraphs, covering the following:

1. **TASK 1*** The purpose of a proxy;
2. **TASK 2*** High-level of how a common proxy works
3. **TASK 3*** High-level explanation on how onion routing used in the Tor Project allows privacy when surfing the web
4. **TASK 4*** What are the implications of privacy while using a proxy?