CSC347 Introduction to Information Security Assignment 2

Due: November 8, 2015 at 11:59 PM

Late penalty: 10% for 1 day, 20% for 2 days

Hand in: Electronic submit a2.zip here. a2 has the following structure.

```
a2
        members.txt
        SoftwareSecurity/
                1a/
                        report.txt
                        # any other files you want to include
                1b/
                        report.txt
                        # any other files you want to include
                1c/
                        report.txt
                        # any other files you want to include
        SystemSecurity
                1/
                        report.txt
                        # any other files you want to include

                2/
                        report.txt
                        # any other files you want to include
                3/
                        report.txt
                        # any other files you want to include
```

Marking:

Groups: Groups of size 2. Both students receive the same mark.

All parts of this assignment involve /virtual/arnold/Ubuntu804Server_2015a2.zip (md5sum 7e69edab980956ba6f2743db7fe92d5a) VM on your lab computer, or at least in dh2020pc01.utm.utoronto.ca:/virtual/arnold/Ubuntu804Server_2015a2.zip. You may also need the /virtual/arnold/kali.zip VM on your lab computer, or at least dh2020pc01.utm.utoronto.ca:/virtual/arnold/kali.zip. (root/toor)

Software Security

1. **[25 Marks]** Ubuntu804Server_2015a2 is running a very small web application which, when run on a lab machine, is available at http://192.168.0.100/fourFours/. You should run there unless you know how to configure networking for vmware at home.
   a. **[10 Marks]**

   The fourFours web application may be vulnerable. Using only a web browser or other remote tools (on the host machine), find out as much about the application as you can. Write a report on what you have discovered. If there are any vulnerabilits/exploits, document them in your report, as in assignment 1. The more you know about the application, its internals, its users etc. the better. Provide step by step instructions detailing how you discovered information and how to carry out exploits. Marks for this problem are based on the amount of detail discovered and the collection of vulnerabilities and exploits listed (both number and type). All attacks are to be remote, you should assume that you do not have direct access to the machine running the web application.

   The above is called penetration testing.

   Your report should describe, step by step, what you did and what you discovered. You can build your own tools or use others to investigate the application at 192.168.0.100, your investigations should not assume any form of access to the machine other than over port 80 (ie, through a web browser). Don't assume that you can attempt to login to the guest VM, that you have 'physical' access to the guest vm etc. Imagine that the guest VM is being hosted by a company on the web, you do not have control over this machine, you can only see it via port 80 (http).

   For reference, please take a look at The OWASP Top 10. I see vulnerabilities in at least 4 of the categories listed. We studied SQL Injection, XSS and XSRF. A single vulnerability might lead to many exploits. An example of an exploit might be:

   - Make an entry in the four fours application as another user.
   - Extract all passwords
   - Change a users password
   - Delete all posted four fours entries
   - Prevent a user from loggin in
   - Login without proper credentials
   - ...

b. **[10 Marks]**

You can log into the web server using arnold/bpbthisisvulnerable2015. That is, before part b this is vulnerable 2015.

For this question, you are to look at fourFours application vulnerabilities and then fix them, hardening the application. That is, fix any of the issues you found with the application and the server that made it easy for you to get your job done as a hacker. Submit a writeup of what you did to harden the application. Submit any modified code etc.

Some pointers: To change to root, execute

```
sudo bash
```

entering arnolds password. I am in the sudoers group. You can find the web application at `/var/www`. You can (and should) do whatever you think is necessary to lock down this application. Your writeup should include the steps you took to lock it down.

c. **[5 Marks]** (Could be considered system security) Review the software running on the server to determine if some or all of it should be updated. Take a look at, for example, cvedetails. List relevant software, current versions, vulnerabilities and advice (whether to upgrade or not).

System Security

1. **[10 Marks]** Run through the System Hardening tutorial, only run it against the Ubuntu804 FourFours server. Write a report outlining the status of each Vulnerability and the Resolution if necessary. For example,

```
Vulnerability: linux single (GRUB):
Status:
    This vulnerability has been removed from the Ubuntu804 server, as outlined in the tutorial,
Resolution: No action taken at this time.

Vulnerability: (List the Vulnerability)
Status: (List the status of the VM with respect to this vulnerability)
Resolution: (If some action needs to be taken, describe it in detail, for example, a set of instructions, or a script)
...

(make sure to include the following)

Vulnerability: Weak passwords
Procedure: I loaded Kali linux, copied /etc/shadow and /etc/passwd to the Kali vm
    and ran john on the unshadowed file.

Status: (list all accounts with logins and which have weak passwords
    (what are they), which have strong passwords.)

Resolution: (advice for users, password policy, procedures)
```

2. **[5 Marks]** You have the VM, so you essentially have physical access to the system. Figure out one or two very different ways to get /etc/shadow and /etc/passwd from the VM, without initially having any accounts or passwords. Document your approach. Is there any way to prevent these attacks?
3. **[10 Marks]** Detection: You are wondering if someone has broken into the server, look around for evidence, declaring it compromised or not. If compromised, describe how, and what the attacker appears to be doing. In your report, outline the tools and techniques you used to audit the system. Outline what appears to be compromised, what the atackers appear to be doing. Describe how to remove the attacker from the system.
    - Look through the logs
    - See who has been using the system
    - Determine what processes are normally running
    - Take a look at commands users are executing (history)
    - Check file dates/times.
    - ...

Questions and Answers

Question:

I need to create my own website to explore vulnerabilites associated with the Four Fours application.

Answer:

You have space at cslinux.utm.utoronto.ca. To use it,

```
cd ~
mkdir www
chmod 711 .
chmod 711 www
cd www
# edit index.html
echo "Got HERE!!" >> index.html
chmod 644 index.html
```

Access your webspace via http://cslinux.utm.utoronto.ca/~UTORID/

Question:

What do I have to do to get the VM working?

Answer:

Tapan has a set of notes

Question:

Can I use SQLMAP?

Answer:

```
Some people are using SQLMAP to SQLInject fourFours, since
the assignment states that you can build or use any tools,
this is allowed. We will give more credit to those that
demonstrate they can SQLInject the application themselves.

Another way to look at it is, if you use SQLMAP you should
have more time to explore additional vulnerabilities, so we
will expect that.
```

Question:

How do I reset the database when trying to cross site script the virtual machine.

Answer:

You can either just unzip the VM again starting it in a new state. Alternatively, you can go in using postgresql and reset the database. Finally, because I know that you are swamped, I have added a reset script to the fourFours application. You can find them in a new VM at

```
scp UTORID@dh2020pc01.utm.utoronto.ca:/virtual/arnold/Ubuntu804Server_2015a2v2.zip .
and also at pc02 to pc10

and you can verify the integrity of the download ...

md5sum Ubuntu804Server_2015a2v2.zip
6b86b34cc72afb68f5889192f90ef9e4  Ubuntu804Server_2015a2v2.zip

http://192.168.0.128/fourFours/reset.php (use your own ip)

Also this VM already has the networking setup as well.
```

Question:

Some of the System Hardening exercises do not seem to apply to the Ubuntu804 VM

Answer:

For the following, just verify that you can't interact with the boot loader, etc. I have already locked the following down.

```
Vulnerability: linux single (GRUB)
Vulnerability: linux GRUB
Vulnerability: User tries to boot off another device (they pressed F2 during boot) (CD, USB, etc)
Vulnerability: User opens up box, removes battery from system to clear BIOS settings
```

Everything else should apply.

Question:

Hints for System Security, question 2?

Answer:

Take a look at ... Physical Security lecture. You have physical access to the VM (you have the data behind it). This is just like having physical access to the computer. Now go down the list of things that could be done if users can touch the system, do any apply to the VM.

Question:

Can you give us some hints/advice on the current assignment.

Answer:

- DO NOT FIXATE ON ONE PART OF THE ASSIGNMENT!!! Do a bit on each, and come back if you feel you can add more.
- For Software Security 1a. Don't spend too much time on any one issue, ie SQL Injection, or XSS, there is more, so explore some of the other OWASP top 10.
- For Software Security 1b. You can write down advice vs actually fixing the application. But for the advice, be concrete. For example, don't just say 'whitelist' say how you will do it and what you will restrict to. For questionable world writable files, pay attention to who owns them, how they are being used, whether it is really necessary that they be world writable etc. Your advice should show that you have thought about them, researched them to some extent.
- For Software Security 1c. What I am looking for is your ability to assess the software surrounding an application. For

example, in the FourFours application there is a postgresql database involved. What version is it? Are there serious issues with that version of Postgresql, what are they. The report should make a case for either continuing to use that version while understanding the risks or for upgrading. Do this for other software involved with the application.

- For System Security 1. Your report should outine any questionable results and some direction for dealing with them. You should be concrete, indicating that you know what has to be done, but don't have to carry out the change. For example, in the assignment, I list "(advice for users, password policy, procedures)" you can talk about the modification to the policy file (name it, identify which fields would change to which values). Let me give one away, how many processes should a user be allowed to run? You should have some limit, what should it be? Well take a look at the system right now, run ps, see how many processes each user is using. Then decide a reasonable number. Is 100/150 ok?
- For System Security 2. Imagine that you had physical access to a computer, then what could you do. Take some of that and translate that to the world of VMs. See the System Security lecture, Physical Security section. This is a very concrete hint!!
- For System Security 3. OK, I'll tell you. The system was compromised. There should be some evidence of the compromise. This can take the form of odd static state (files, directories, history, logs) or odd behavior (processes running, odd behaviour of commands).

Question:

We are working on the System security and have john the ripper running on /etc/shadow and /etc/passwd, and we are wondering what the importance of having /etc/passwd as a parameter. From what it seems like to us, /etc/shadow already has all the required information. Could you please clarify the importance of the inputs of John the Ripper and what exactly it is trying to do in this case?

Answer:

You unshadow /etc/password and /etc/shadow to create the old style password file. John likes to run on that best.

Question:

I had a question about the weak passwords part on System Security section. How do I transfer the /etc/shadow and /etc/passwd files to the Kali Linux. I have no access to the internet from the VM itself. Me running (sudo dhclient eth0) is not getting any results. And running john in the Ubuntu804Server is only promting to install.

Answer:

You should have at least a connection between the vm and the host machine. At least you should be able to scp from Ubuntu804 to the host and then from host to Kali linux. I did it directly, Terminal in Kali, scp from the Ubuntu804 machine.

Question:

For the first question in the System Security portion of A2, are we only supposed to determine and resolve the statuses of the vulnerabilities you provided or are we to also find our own on top of that to receive full marks?

Answer:

Only those that are in the tutorial. It is good that you are thinking beyond, but we should put a limit on it. You should demonstrate that you put thought into your answers, vs

```
here is the output from

find / -perm -04000 -uid 0 -print > Set-UID-root-programs
```

So you should look at the results, consider what should be changed, is all software needed? Your goal is to write up the advice for the systems admins to follow.