# Assignment #4: DNS Pharming Attack Lab

CSC 574 – Computer and Network Security
Spring 2013 – Prof. Enck
Assignment Value: 100 points

**Due date: April 9, 2013**

The goal is this assignment is to familiarize students with attacks on the Domain Name System (DNS). This is an assignment for individuals - no group work or collaboration allowed. Violations of the NCSU Code of Student Conduct will be reported to the Office of Student Conduct Immediately, and students will fail the course.

## 1 Assignment Details

In this assignment, students will complete a series of excercises designed to show several ways that DNS cache poisoning attacks can be accomplished.
A PDF describing the exact steps students must follow can be here:

http://www.csc.ncsu.edu/faculty/enck/csc574-s13/docs/DNS.pdf

A VM image with all of the necessary tools can be found here:

http://www.cis.syr.edu/~wedu/seed/lab_env.html

The zone files from the PDF description can be found here:

http://www.cis.syr.edu/~wedu/seed/Labs/Attacks_DNS/

Note that our PDF instructions are slightly different than the PDF instructions on that page.

## 2 Grading

The submission for this assignment will be a report detailing the steps taken to achieve the goals for each of the four attacks outlined in the assignment. For each of the four attacks, the report must provide the following information:

1. **/etc/hosts file attack (10points)**
   - Describe the exact steps you took to alter the the IP address that was resolved for a given host.
   - Provide screen shots, commands executed, and command output to explain what took place.
   - Explain how a real-world attacker could leverage this sort of attack.
   - Discuss whether you feel this is a viable attack in the real world. What factors contribute to your answer?
2. **Host-Level Response Spoofing (20 points)**
   - Describe the exact steps you took to alter the the IP address that was resolved for a given host. Be sure to provide evidence that shows that the host did, indeed, resolve an incorrect IP address. This should come in the form of packet captures, command line results, etc.
   - Provide screen shots, commands executed, and command output to explain what took place.
   - Explain how a real-world attacker could leverage this sort of attack.
   - Discuss whether you feel this is a viable attack in the real world. What limitations about this attack contribute to your answer?
3. **Server-Level Response Spoofing (20 points)**
   - Describe the exact steps you took to alter the the IP address that was resolved for a given host. Be sure to provide evidence that shows that the host did, indeed, resolve an incorrect IP address. This should come in the form of packet captures, command line results, etc.

- Provide screen shots, commands executed, and command output to explain what took place.
- Explain how a real-world attacker could leverage this sort of attack.
- Discuss whether you feel this is a viable attack in the real world. What limitations about this attack contribute to your answer?

4. **Kaminsky Attack (50 points)**

   - Describe the exact steps you took to alter the the IP address that was resolved for a given host. Be sure to provide evidence that shows that the host did, indeed, resolve an incorrect IP address. This should come in the form of packet captures, command line results, etc.
   - Provide screen shots, commands executed, and command output to explain what took place.
   - Describe, in plain English, how the attack tool you wrote for this portion of the assignment is structured and functions.
   - How successful was your attack tool? Did you have to run it several times? Why? What could you do to increase its level of success?
   - **Describe, in detail, the steps you took to prevent any packets associated with this attack from reaching the Internet. Failure to provide a sufficient explanation will result in 0 points awarded for this portion of the report.**
   - Explain how a real-world attacker could leverage this sort of attack.
   - Discuss whether you feel this is a viable attack in the real world.

# 3 Submission Instructions

You **must** turn in one `.tar.gz` or `.zip` file named `lastname-assign4.tar.gz` or `lastname-assign4.zip`, respectively. No other archive file formats (e.g., RAR) will be accepted. The archive should contain the following:

1. `lastname-assign4.pdf`: This is a PDF that documents your work and experiences.
2. `survey.pdf`: This is a PDF of the lab survey: http://www.cis.syr.edu/~wedu/seed/Survey_Questionnaires/DNS_Questionnaire.doc
3. Source code for the Kaminsky attack tool. Please remember to include any payload files assosiated with your tool. Your tool must build on the SEED Unbuntu VMWare image by simply executing an install script like the one included with the pacgen source. Please remember to include your install.sh in the tarball.

# 4 Tips

- The fourth portion of the excercise is much more difficult than the first three portions. Budget your time accordingly.
- Remember to explain the steps you took to ensure your Kaminsky Attack tool did not leak packets onto the Internet. Failure to provide a sufficient explanation will result in 0 points awarded for this portion of the report.
- Students may find that the VM downloaded from the SEED site has difficulty connecting to the Internet. If you need access to the Internet for your lab setup to work (except for the fourth portion), you can make the image connect by setting the network to NAT mode.