CIS3360: Security in Computing (online session, Spring 2012)

Homework 4: Chapter 4, 5, 6

(assigned 04/9, due on webcourse by 3AM 04/18, i.e., late night in 04/17)

Question 1 should be submitted to Assignment 4.1
(TA for 4.1: Dmytro Dondyk dmytrodondyk@gmail.com)

1. (56 points) Knowledge-based Questions:

a. Although the majority of current botnets use the centralized C&C communication architecture, why they are very hard to shut down even if defenders know all bot machines in a botnet?

b. What are the two botnet monitoring techniques introduced in the lectures?

c. Give the name of a real rootkit that utilizes Direct Kernel Object Manipulation (DKOM) technique?

d. What is a Trojan malware? What is a backdoor?

e. What is ARP? In what network layer is ARP being used?

f. What is Smurf attack? What is SYN flooding attack?

g. What are the two major DNS query modes? How many types of resource records are saved on a DNS server?

h. Why it is easy for attacker to send out spoofed packets in “thin pipe/thick pipe” method while it is very hard for attacker to inject spoofed packets in a normal TCP communication session?

Question 2-3 should be submitted to Assignment 4.2
(TA for 4.2: Jonathan Warner despoteuodia@knights.ucf.edu)

2. **(20 points) DNS Query:**
   The following shows the result when I use "dig mx knights.ucf.edu" (unrelated text has been cut). Please answer the question:
   1). What is the email server's name that in charge of UCF student email account of username@knights.ucf.edu?
   2). What are the IP addresses used for this email server?
   3). What are the IP addresses of UCF authoritative DNS servers?

```
czou@eustis:~$ dig mx knights.ucf.edu
;; QUESTION SECTION:
;knights.ucf.edu.            IN      MX

;; ANSWER SECTION:
knights.ucf.edu.      154    IN      MX      0 680526354.pamx1.hotmail.com.

;; AUTHORITY SECTION:
ucf.edu.              1794   IN      NS      ucf3.ucf.edu.
ucf.edu.              1794   IN      NS      ucf1.ucf.edu.
ucf.edu.              1794   IN      NS      ucf2.ucf.edu.

;; ADDITIONAL SECTION:
680526354.pamx1.hotmail.com. 1086 IN   A      65.54.188.78
680526354.pamx1.hotmail.com. 1086 IN   A      65.54.188.109
ucf1.ucf.edu.         1589   IN      A       10.171.12.5
ucf2.ucf.edu.         1794   IN      A       10.171.12.37
ucf3.ucf.edu.         1794   IN      A       10.171.12.69
```

3. **(24 points) DNS Resource Records:**

Suppose you open a startup company "flashNetwork" and want to set up your company network. Your network has the following servers:

Authoritative DNS server: "dns.flashNetwork.com" with IP as "128.119.12.40"

Web server: "flashNetwork.com" with two IP as "128.119.12.55" and "128.119.12.56". Internet users can also access the web server by the domain name of "www.flashNetwork.com".

Email server: "mail.flashNetwork.com" with IP as "128.119.12.60"

Your company's email address is "username@flashNetwork.com".

a). What resource records (RRs) do you need to provide to the upper-level ".com" Registrar?

b). What RRs do you need to put in your company's authoritative DNS server?