**CIS3360: Security in Computing**

**Homework 2**

1. **(35 points) Knowledge-based Questions:**
   1. 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 of the bot machines in a botnet?
   2. Give the name of a real rootkit that utilizes Direct Kernel Object Manipulation (DKOM) technique?
   3. What is Trojan malware? What is a backdoor?
   4. What is ARP? In what network layer is ARP being used?
   5. What is a Smurf attack? What is a SYN flooding attack?
   6. What are the two major DNS query modes? How many types of resource records are saved on a DNS server?
   7. Why it is easy for attacker to send out spoofed packets in the “thin pipe/thick pipe” method while it is very hard for an attacker to inject spoofed packets in a normal TCP communication session?
2. **(15 points) DNS Query:**

The following shows the result when I use “dig mx knights.ucf.edu” (unrelated text has been cut).

Please answer the following questions:

1). What is the email server 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?

jlazar@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

1. **(15 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?

1. **(20 points) IP Address conversion:**

The flashNetwork network admin is creating a subnet within the company. Convert the IP address 192.168.0.1 to binary for the admin so that they can apply a subnet mask and make sure that the resulting binary code resolves appropriately. Binary result is worth 1 point. Showing all work to get to binary result is worth 19 points.

1. **(15 points) Malware**:

a. What are the differences between polymorphic viruses and metamorphic viruses?

b. Why did the Slammer worm spread much faster than Code Red worm?

c. According to the worm propagation differential equation model, why does a worm slows down its infection speed after it infects more than 80% of vulnerable hosts?