Homework 7

CIS 4930 / CIS 5930
Offensive Computer Security
Spring 2014

Due **April 4th**, 2014, by *MIDNIGHT*
Worth: 100 points

Electronic turn in (Turn in via email to the TA. Email address is raiaan@cs.fsu.edu)
The email must be titled in the following format:
[OCS2014] hw7 <your last name>
(where <your last name> is your last name)
i.e.: [OCS2014] hw7 redwood
Download the files for this homework from: http://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/hw/hw7_pcaps.zip

A useful and concise Wireshark Tutorial can be found here:
http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

A brief tutorial video has been uploaded here:
https://www.youtube.com/watch?v=tls99yZLzn4&feature=youtu.be

Part A: [79 points]
Answer the following questions below by viewing **vm1.pcap**

1. What protocol is responsible for assigning an adapter an IPv4 address?
   a. **[2 points]** Does an attacker need to launch a MitM attack to be able to receive adapter information for other adapters on the Local Area Network (LAN) which utilize this protocol to obtain an IPv4 address? Why?
   b. **[2 points]** What is the IPv4 address of the adapter assigning IPv4 addresses?
   c. **[2 points]** What information can the attacker infer about the LAN by observing these packets? (IP address range and subnet)
2. What are the **assigned** IPv4 addresses for the adapters with these MACs?
   a. **[1 point]** 08:00:27:8F:4C:61
   b. **[1 point]** 08:00:27:76:1F:7C
   c. **[1 point]** 08:00:27:0C:66:53
3. **[4 points]** Did all of the above adapters receive their IPv4 address from the protocol described in question 1? If not, which adapters were not assigned their IPv4 address and what is the IPv4 address and MAC address of these adapters?
4. **[2 points]** Does an attacker need to have an assigned IPv4 address to interact on a LAN? Why?
5. **[3 points]** What DNS protocols are used in this file?
6. Frames **102-109** utilize the ICMP protocol

    a. **[2 points]** What is the ICMP protocol being used for in these frames?
    b. **[2 points]** Did the source gather any new information from these ICMP requests?
    c. **[2 points]** What happened to the replies?

7. A series of SYN packets are sent to a destination between frames **120** and **2121**
    a. **[2 points]** What is the purpose of these SYN packets?
    b. **[2 points]** What new information about the destination was obtained by these SYN packets?
8. A series of SYN packets are sent to a destination between frames **2241** and **4250**
    a. **[2 points]** What is the purpose of these SYN packets?
    b. **[2 points]** What new information about the destination was obtained by these SYN packets?
9. **[8 points]** From 7 and 8, what type of packet was returned to the source from the destination to indicate this new information?
10. Between frames **4365** and **4368** an adapter utilizes the ARP protocol (Request/Reply)
    a. **[4 points]** What is the purpose of the ARP protocol?
    b. **[2 points]** Which adapter is collecting this information (IP and MAC)?
11. Between frames **4371** and **4382** an adapter floods the LAN with ARP replies
    a. **[4 points]** Is this valid without an ARP request? Why?
    b. **[4 points]** What is suspicious about these ARP replies?
    c. **[4 points]** Which adapters (IP and MAC) are these ARP replies effecting and what is the purpose behind these ARP replies?
12. An adapter accesses a HTTP server
    a. **[2 points]** What kind of HTTP server was accessed?
    b. **[2 points]** What is the IP and MAC address of the HTTP server host?
13. One of the clients downloaded a document from the server
    a. **[5 points]** Was the attacker able to successfully intercept the entire document and would the attacker have been able to intercept this document without the actions taken in question 11?
    b. **[2 points]** What is the document media type?
    c. What content is in this document?
        i. **[2 points]** What is the title in the document (HINT: not the filename)?
        ii. **[2 points]**What is the month and year the document was published?
        iii. **[2 points]** Who was the authority that issued the document?
    d. **[2 points]**Does the victim have any indication this file was intercepted?
    a. **[2 points]** Could the interception of this file be completely prevented by using HTTPS?

Part B: [21 points (Plus extra credit)]

Answer the following questions using **p2.pcap**. This is a packet capture (from the attacker's machine) of a targeted, man in the middle attack using sslstrip to steal a username and password.

1. The arp spoof activity begins at packet #3:

a. **[2 points]** Who is the attacker (What is his/her MAC address?)?
b. **[2 points]** What is the attackers ACTUAL IP? This will be easy to find given the MAC address. Do not confuse it for the IP that the attacker is trying to impersonate!
c. **[2 points]** Who is the attacker trying to impersonate (What IP address)?
d. **[2 points]** Who is the victim IP? Hint: See the target IP address in the spoofed arp packets.

2. The victim begins browsing the web at packet 11
   a. **[5 points]** Packets 11 through 168 represent the traffic generated by google's instant search mechanism (i.e. results updated per keystroke). Packet 169 was his final query in this search, as he had finished typing the query string. What was his search string that he submitted to google?
   b. **[4 points]** How many GET requests between packet 11 and 170 did the client's browser generate? Hint: Use "contains" as part of a filter in the HTTP headers to find this.
3. After google.com, the victim next visits a website that does not enforce Strict Transport Security. The victims traffic begins around packet
   a. **[2 points]** There is a lot of advertising traffic in the packet capture. What is the second website the victim visits (domain name will suffice)? Hint: it's easiest to search by looking at the SSL traffic handshake messages. Use the following filter:
   (ssl.handshake.type == 2)
   b. **[2 points]** A HTTPS session is established in packets 1303 - 1322. Is this SSL handshake between the victim and the website; or between the attacker and the website?
   c. **[EXTRA CREDIT 5 points]** Packet 3284 is a plaintext HTTP POST request generated by the victim pressing the login button on the website form. What is the victim's username and password?