CS 161 – Computer Security
Instructor: Tygar
20 October 2015

Homework 6

Notes

- Homework 6 is due on 27 October 2015 at 3PM.
- Please work on this homework individually – no collaboration allowed.
- **Please list your name, student ID, section, and TA at the top of your solution**
- Submit this homework using Gradescope

Please start the answer to each question (including subquestions) on a new page.

1. Download `Wireshark` here: http://www.wireshark.org/. Alternatively, if you're running Linux, you can `sudo apt-get install wireshark` as well. It's also installed on the Hive machines in Soda.
Once you install and open Wireshark, select the option to "Open an existing packet capture". Select `phishingemail.pcap` from the class resource page https://piazza.com/berkeley/fall2015/cs161/resources and open it. You should see a large amount of packets once the capture successfully opens. It contains the packet capture of the actions taken by malware downloaded from a phishing email. The following exercises are to get you accustomed to reading packets in Wireshark.

    a. Initially, a few DNS requests are made. Which name is requested in the first (time = 0) DNS request?

    sgb-sy.com

    b. What is the DNS response to the requested name in part (a)? This should be an IP address.

    46.149.110.103

    c. The 11th packet sent is an HTTP POST request. What is the source IP, destination IP, source port, and destination port of the request?

    srcIP = 192.168.56.102, srcPort = 1066, destIP = 46.149.110.103, destPort = 80

    d. Note that you can actually see the sequence numbers of the TCP packets being sent. What is the sequence number of packet #49?

    11726

e. The HTTP POST requests (like the one mentioned in Part c) are made by the malware, which is transferring data to the attacker. How many total HTTP POST requests are made?

5 HTTP POST requests are made.

f. Packet #772 is an HTTP GET request. Which domain (hostname) is it to, and what resource is it requesting?

It is to google.com, and it requests /webhp.

2. Now you are ready for analysis using the skills you learned in Question 1. Open `compromise.pcap` (again, on the class resource page) in Wireshark. This is a packet capture submitted to a website that collects information on malicious sites.

a. The victim's IP is 192.168.22.10. What is the IP of the DNS resolver that the victim is using?
4.2.2.3

b. Let's figure out where the exploit came from. You can infer this from the first site that the victim requests in the packet capture. He or she visits their webpage, and later some malware is delivered. What is the URL of this site?
almorakib.com

c. Shockwave2 programs are often used to display animated graphics on webpages (using Adobe Flash). They can also be used in a malicious manner, so naturally, we should look for evidence of it being used. What port do these programs use? What is the first packet number and destination (IP) in the first packet in the capture involving Shockwave2?

Port 1257. Packet number is 14008, and destination is 46.101.165.112. Can also accept packet 13880, which is when the Shockwave file is requested

d. What hostname (not IP address) is delivering the Shockwave2 data that the victim's computer is now requesting?
udashdghajsdjkasdahsjkasd.cf

e. A main goal in an attack would be to get the user's computer to run an executable, such as a .exe file on Windows. Is there any evidence that this was accomplished? If so, what host, packet number, and file provide the evidence?
In packet 14377, harsh02.exe is delivered from 89.28.47.100

3. Use `phpnetcompromise.pcap` for this problem. Packets #1 to #6 constitute the (untampered) DHCP request. Assuming that your IP address is 198.168.40.69, and your assign your victim the same IP as it is currently assigned, show what a DHCP spoof packet capture would look like. You should only need to work with packets #1 to #6, plus any others you choose to add. Assume that the victim accepts the first DHCP Offer it gets, and your attack succeeds.

   Fill out a table containing the Packet Number, Source IP, Dest IP, Protocol, Info fields. Don't include the transaction ID from the info field. Each row corresponds to one packet in the Wireshark packet capture.

No.	**Source IP**	**Dest IP**	**Protocol**	**Info**
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
2	198.168.40.69	192.168.40.10	DHCP	DHCP Offer
3	192.168.40.1	192.168.40.10	DHCP	DHCP Offer
4	0.0.0.0	255.255.255.255	DHCP	DHCP Request
5	198.168.40.69	192.168.40.10	DHCP	DHCP ACK
6	192.168.40.10	198.168.40.69	DHCP	DHCP Request
7	198.168.40.69	192.168.40.10	DHCP	DHCP ACK

4. Load `chat.pcap` into Wireshark for this problem. This packet involves communication from a popular chat client.

   a. Try following TCP stream 5 and examining the first packet sent. What country is this connection from?
   AU (Australia) or US for partial credit, based on other methods

   b. You can find the user's ID as well from this trace. What is it? (Hint: it was transferred as "uic" in the data stream.)

   aaaaaaaa123 or spoonfed123

c. As you may have figured out, this packet capture is from a Skype messaging client and contains all kinds of information. So Skype uses a TCP stream, but at least the original packets were probably encrypted with SSL. We can't change the Skype program or how it encrypts its data. How do you think someone created this unencrypted packet capture? (Hint: Can you manipulate Skype on your computer into using a public key for which you know the private key?)

- Skype user must trust a certificate authority which the attacker can persuade to sign a Skype certificate
- Execute a MITM attack, listening to the Skype using the private key corresponding to the certificate's public key (can decrypt any traffic sent by Skype)