OCR@UC Lab

LESSON TITLE: **Lab 4- Packet Analysis and Sniffing**

WARNING:

Warning: Any use of penetration testing techniques on a live network could result in expulsion and/or criminal prosecution. Techniques are to be used in lab environments, for educational use only or on networks for which you have explicit permission to test its defenses.

Level:

☐Beginner ☐Advanced

☒Intermediate

Audience: ☒Instructor-led ☐Self-taught

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

- Analyze data from a packet capture
- Demonstrate an ARP poising attack to capture traffic between two systems

Materials List:

- Computers with Internet connection
- Browsers: Firefox (preferred), Google Chrome, or Internet Explorer
- Intro to Ethical Hacking lab environment

Introduction

In this lab we will take a look at how to analyze and sniff packets on the network with techniques such as ARP poisoning.

Systems/tools used:

- Kali Linux *(u: root, p: toor)*
- Metasploit2 *(u:msfadmin, p:msfadmin)*
- Windows 7 *(u:administrator, p: Pa$$w0rd)* + Wireshark
- Power down all other systems

Module Activity Description:

Part One: Packet Analysis

Open each of the packet captures from the “Packet Captures” folder on the Windows 7 Desktop with Wireshark and answer the following questions.

File: Challenge101-0.pcapng

1. **How many packets are in this trace file?**
   20
2. **What IP hosts are making a TCP connection in frames 1, 2 and 3?**
   192.168.1.108 and 50.19.229.205
3. **What HTTP command is sent in frame 4?**
   GET
4. **What is the length of the largest frame in this trace file?**
   1428
5. **What protocols are seen in protocol column?**
   HTTP and TCP
6. **What responses are sent by the HTTP server?**
   HTTP/1.1 302 Found

File: Challenge101-1.pcapng

7. **In what frame number does the client request the default root web page (“/”)?**
   13
8. **What response does the server send in frame 17?**
   HTTP/1.1 200 OK
9. **What is the largest TCP delta (delay) value seen in this trace file?**
   6.006083000 seconds
10. **How many SYN packets arrived after at least 1 second delay?**
    4

File: Challenge101-3.pcapng

11. **How many frames travel to or from 80.78.246.209?**
    32
12. **How many DNS packets are in the trace file?**
    8
13. **How many frames have the TCP SYN bit set to 1?**
    12
14. **How many frames contain the string “set-cookie” in upper case or lower case?**
    Frame 9, 471, 475 and 82= 4 frames
15. **How many frames contain a TCP delta time greater than 1 second?**
    8

Module Activity Description:

Part Two: Capturing Packets using ARP poisoning

- *On your **Windows 7** system, install **WinSCP, Filezilla**, or your favorite FTP client.*
- *On you **Kali Linux** system, start a packet capture with **Wireshark** on the **eth0** interface.*
- *Turn on packet forwarding with the following command:*

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

- *Start ARP poisoning your Windows 7 and metaploitable2 systems:*

```
arpspoof –i eth0 –t <IP of Windows 7> <IP of metasploitable2>
```

In a new terminal run the same command, but rearrange the IP addresses so you are capturing both sides of the conversation.

- *On you **Windows 7** system, connect to **FTP** on your **metaploitable2** system using **port 21**.*
- *Login with user: **msfadmin** password: **msfadmin***
- *Create a text file on your Windows 7 system with the words "**Hello World**" in the text.*
- *Transfer this file to the metasploitable2 system using ftp.*
- *Stop the packet capture and hit **ctrl-c** in both terminal windows to stop the ARP poisoning.*
- *Analyze the packet capture and answer the following questions/paste screen shots.*

Find the packets that contain the username and password for the ftp server

16. **Paste a screen shot showing each of these packets.**

Find the packet that contains the text file you transferred.

17. **Paste a screen shot showing the FTP Data for this file.**

18. **Are there any packets that might send up a red flag that an ARP poisoning attack is occurring?**

Yes