Network Security Theory and Practice

Lab 02

Due March 21, 2024

POLICIES:

1. **Coverage**
   ARP spoofing
2. **Grade**
   Lab 02 accounts for 10% of the final grade
3. **Individual or Group**
   Individual based, but group discussion is allowed and encouraged
4. **Academic Honesty**
   Violation of academic honesty may result in a penalty more severe than zero credit for an assignment, a test, and/or an exam.
5. **Submission**
   Submit your_name-Lab02.pdf on course.zju.edu.cn
6. **Late Submission**
   Late submissions after April 3 23:59 will NOT be graded.

PREPARATION:

1. **Lab Goal**
   Lab 02 aims to understand the principle of ARP deception and implement ARP deception through tools.
2. **Recommended Tools**

   arpspoof & dnsspoof

   ARP & DNS Spoofing tool, which comes with Kali Linux. In Ubuntu, you only need to run the command to install it:

   sudo apt-get install dsniff

   scapy

   Scapy is a python program that enables users to send, sniff, parse, and forge network packets. This feature allows you to build tools that can detect, scan or attack networks.

LAB REQUIREMENTS:

1. **Create a virtual machine**
2. **Configure virtual machine IP address**
   1、 Set the network connection mode to bridge mode.
   2、 modify the IP address and DNS address of the virtual machine to make it in the same network segment as the host network.
   3、Ensure that the virtual machine and the host can ping each other.
   (Note that you may need to turn off the host firewall. If you use the wireless network, it is recommended to turn on the hotspot. There may be problems when using the ZJUWLAN.)
   3、 Install arpspoof in the virtual machine.
3. **Start the ARP Spoofing**
   1、 Enter 'arp -a' in the host computer to view the ARP cache.
   2、 Run the instruction 'sudo arpspoof -i [network card] -t [target IP] [host IP]'
   You can find help here: arpspoof instruction usage.
   3、 Surf the Internet on the host computer and observe the network status
   4、 Enter 'arp -a' in the host computer to view the ARP cache. Compare the gateway MAC address and the virtual machine MAC address.
   5、 Using 'ctrl+c' to interrupt the command in VM and check the host network status

   Use scapy

   You can write a script to craft an ARP packet and send it to the victim. This can help you understand the attack principles and lay the foundation for what comes next.
4. **Start the DNS Spoofing**

   Find tools to realize the dns spoof, liking dnsspoof instruction.

REPORT REQUIREMENTS:

1. **Report Template**

   NetSec-Lab-Report-Template.doc
2. **Language**

   English
3. **Content Highlights**

   For each of lab requirements, please use screenshots to showcase the correct processes for solving each challenge.

   For certain steps, necessary discussions may be provided to demonstrate your understanding.
4. **Page Limit**

   Please keep the report as concise as possible.
5. **References**

   IP configuration of Virtual machine: https://www.jianshu.com/p/440b000dacbf

   Scapy document: https://scapy.readthedocs.io/en/latest/