Network Security Theory and Practice

Lab 02

Due March 22, 2022

POLICIES:

1. **Coverage**
   ARP spoofing, DNS 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**
   Soft copy of report.pdf on course.zju.edu.cn by March 25 23:59
6. **Late Submission**
   20% deduction for late submission till March 27, 2022;
   Deduction ceases upon zero;
   Late submissions after March 27, 2022 will NOT be graded.

PREPARATION:

1. **Lab Goal**
   Lab 02 aims to understand the principle of ARP deception and DNS deception, and practice these attacks through tools such as WinCap and Cain.

2. **Recommended Tools**
   WinCap
   WinPcap (Windows packet capture) is a free and public network access system under Windows platform. The purpose of developing WinPcap is to provide Win32 applications with the ability to access the bottom of the network. It is used for direct network programming under Windows system.
   Cain and Abel
   Cain and Abel is a free password recovery tool for Microsoft operating system developed by oxid.it. Its function is very powerful. It can sniff the network, cheat the network, crack the encrypted password, decode the disrupted password, display the password box, display the cached password and analyze the routing protocol.

LAB REQUIREMENTS:

1. **Create a virtual machine**
2. **Configure IP address of the virtual machine**

   hints:

   step 1. set the network connection mode to bridge mode.

   step 2. modify the IP address and DNS address of the virtual machine to make them in the same network segment as the host network.

   step 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 wireless network, it is recommended to turn on the hotspot; different behaviors may appear when using the ZJUWLAN.)

   step 4. install WinPcap & Cain and Abel in the virtual machine
3. **Run Cain and Abel for MAC sniffing**

   hints:

   step 1. click Configure and select the network adapter of the corresponding IP of the virtual machine.

   step 2. click sniffer and select the label host.

   step 3. click start sniffing, then right-click in the blank space and select scan MAC address.

   step 4. observe the MAC address of the current network segment.
4. **Practice ARP spoofing attack**

   hints:

   step 1. add a spoofing object and create an ARP spoofing; select the gateway on the left and the spoofed IP on the right.

   step 2. enter 'ARP - a' in the host to view the ARP cache; compare the gateway’s MAC address and the virtual machine’s MAC address.
5. **Practice DNS spoofing attack**

   hints:

   step 1. fill in the DNS spoofing with the requested DNS name and the IP address of the response package.

   step 2. enter 'ipconfig/flushdns' from the host command line to empty the cache; open the browser and visit the cheated website address.

REPORT REQUIREMENTS:

1. **Report Template**

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

   English
3. **Content Highlights**

   For each of the lab requirements, please use screenshots to showcase the correct processes for launching the corresponding attacks.

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

ARP spoofing:
https://jingyan.baidu.com/artice/d2b1d1029636b05c7e37d491.html