Network Security Theory and Practice

Lab 01

Due March 31, 2021

POLICIES:

1. **Coverage**
   Packet sniffing, packet crafting, and port scanning
2. **Grade**
   All lab assignments account 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
6. **Late Submission**
   20% deduction for late submission till April 07, 2021;
   Deduction ceases upon zero;
   Late submissions after April 07 23:59 will NOT be graded.

PREPARATION:

1. **Lab Goal**
   Lab 01 aims to practice commonly used tools for packet sniffing, packet crafting, and port scanning.
   For packet sniffing and packet crafting, we use basic web exploitation CTF challenges for example. Solving these challenges helps to understand the HTTP protocol and technologies involved in information transfer and display over the internet like PHP, CMS's (e.g., Django), SQL, Javascript, and more.
   For port scanning, we use Nmap to determine which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.
2. **Recommended Tools**
   Curl
   Curl is a command-line tool for transferring data specified with URL syntax. Find out how to use curl by reading the curl.1 man page or the MANUAL document. Find out how to install Curl by reading the INSTALL document.
   Burp Suite
   Burp Suite supports reviewing/editing the data sent and received among other things. It functions as a proxy, typically configured to listen on 127.0.01 loopback

address. An application such as a web browser or sqlmap is configured to use Burp Suite as a Proxy. This enables the review/editing of what is transmitted and received. Here is a link to a tutorial.

Nmap

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

LAB REQUIREMENTS:

1. **https://actf.lol/challenges#Game1-97**
   hints:
   step 1. view page source
   step 2. view page source
   step 3. capture RESONSE-packet header using Burp Suite
2. **https://actf.lol/challenges#Game2-98**
   hints:
   step 1. view page source
   step 2. understand 302 redirection
   step 3. locate redirected pages and find password
   step 4. understand HTTP Referer field
   step 5. capture GET-packet and rewrite Referer field using Burp Suite
   step 6. capture GET-packet and rewrite Coookie field with admin privilege using Burp Suite
3. **https://zjusec.com/play?q=19**
   hints:
   step 1. view page source
   step 2. get link from .bak file
   step 3. capture GET-packet and null Referer field using Burp Suite
   step 4. capture RESONSE-packet header with next link included using Burp Suite
   step 5. view page source and craft POST packet with button click effect using curl or Burp Suite
4. **https://zjusec.com/play?q=2**
   hints:
   This one is relatively straightforward. Just scan with Nmap.

REPORT REQUIREMENTS:

1. **Report Template**

NetSec-Lab-Report-Template.doc

2. **Language**

   English

3. **Content Highlights**

   For each of lab requirements 1~4, 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**

   HTTP packet header format:

   https://blog.csdn.net/selinda001/article/details/79338766

   Nmap tutorial:

   https://blog.csdn.net/smli_ng/article/details/105964486