2022 LZU OSS Information Security Assignments

Author: HexGadget

For everyone who wants to join the C4M31 that belongs to the OSS Security Team, these assignments are set for the qualification of your skill and potential. The contents are mainly scheduled as below:

2022 LZU OSS Information Security Assignments

- Web Security
- Cryptography
- Reverse
- PWN
- Penetration Test
- Forensics
- Appendix

Web Security

In this part, you should set up your own environment for the DVWA lab.

The download link is provided here: DVWA.

You can set up this platform either on your own system or a virtual machine system (e.g., VMWARE, Virtual Box).

All of these labs should be done, and the operations should be recorded for verification.

An example organization is given below (Note: The language can be either English or Simplified Chinese.):

> *Attack 1: The SQL Injection (Level: Easy)*
>
> *The codes are shown below:*
>
> *Some Codes and screenshots for your operations.*

> *The reason that leads to the vulnerability is ... or The reason why attacker can't attack this application is ...*
>
> *Potential mechanisms to fix these vulnerabilities are ... or The mechanism that guarantees the security is ...*
>
> *Attack 2: ...*

Cryptography

For cryptography, several assignments are given below:

1. Write your own Python script to implement at least 10 common encoding mechanisms. (Note: The third-party libraries are banned!)
2. With an algorithm given, try to analyze it and find the plaintext.
3. A simple RSA problem.

The code for assignment 2:

```
import sys
key = '*****CONFIDENTIAL*********'
flag = 'LZUOSS{*****CONFIDENTIAL*********}'
# Ciphertext is:
1355a945343485ec977964015436017600015400 64bceabca7645400da0102ea8a3
3866543fa

if len(key) % 2 == 1:
    print("Key Length Error")
    sys.exit(1)

n = int(len(key) / 2)
encrypted = ''
for c in flag:
    c = ord(c)
    for a, b in zip(key[0:n], key[n:2*n]):
        c = (ord(a) * c + ord(b)) % 251
    encrypted += '%02x' % c

print(encrypted)
```

Information for assignment 3:

> *e= 0x10001*
>
> *n=0xf1f145b9a2e1c88ebbf849402c2feefe4bbcb7b7eb0fb5236a92a34a9402802a316cd7abbae071b13d40fd724719938b657ff519f8443e00ff377c0df7f40e9a9d0929a47eab7c7feb7bfccad715c84b662dbf6721f69c48c32e3513abb924529f715b21c1e2b1044a45a515f6f49f04ad41d05b9da23f4d6cbd726292ff0297*
>
> *c=0xc408c1f631a33ebe1cb6ff7470f6b3739223715d45c750511917732cac30e700368856af03d3f96cc2471e4fc774e6be5bc4fe2a76384ff36d2d0f6f0204b6c65614470078823b51021a2e26a0fcc2bfdce19710b6d17b3c014d04ed6930e85aa4e4708885a75c7d692cf1756556ec199366f9b38c0ded8aa94738ce5e8b5a4a*
>
> *Your mission is finding the plaintext.*

Reverse

Use the CheatEngine to modify a game you like, and three requirements are given below:

1. At least three variables can be modified with the corresponding static address being found.
2. Hook Scripts should be written with assembly language.
3. Export your modification as CT table and import it to test whether it is still available.

PWN

In this part, you should perform a successful buffer overflow attack and gain the control of the system.

The source code is given below:

```
#include<stdio.h>

void vuln()
{
    char s[12];
    gets(s);
    puts(s);
}
```

```
int main()
{
    vuln();
    return 0;
}
```

The platform should be Ubuntu 20.04, and the compiled program should be the 32-bit version.

The organization of the solution is proposed here:

> *Analyze the organization of the memory in the system.*
>
> *Analyze the potential vulnerability in the program based on the source code.*
>
> *Give the full detail of the compiling process.*
>
> *The operation to PWN this program.*
>
> *Your pains and gains.*

Penetration Test

Note: We here only provide the download links of VMs, and you should prepare your own VM platform.

Use Kali Linux as the platform and other tools you like to present a penetration test on the following targets:

1. Target Machine 1
2. Target Machine 2
3. Target Machine 3

Forensics

Use Wireshark to analyze why Telnet is not Secure.

Download link: Wireshark

Appendix

- **All the answers should be written in a proper format and should be submitted in PDF format.**

- **Any cheating behavior will be recorded and reported.**