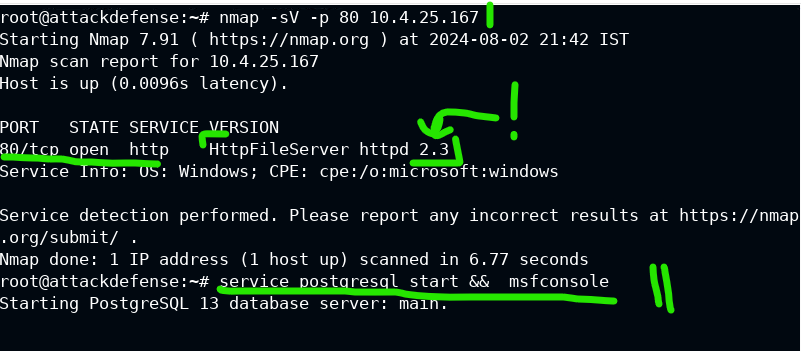
HTTP file server vulnerability lab:

Goal: the admin casually left an important document on his desktop. We don’t have access to the physical machine, but we know it’s running HTTP over port 80. Retrieve the contents of that file on the target machine (10.4.25.167)

Process:

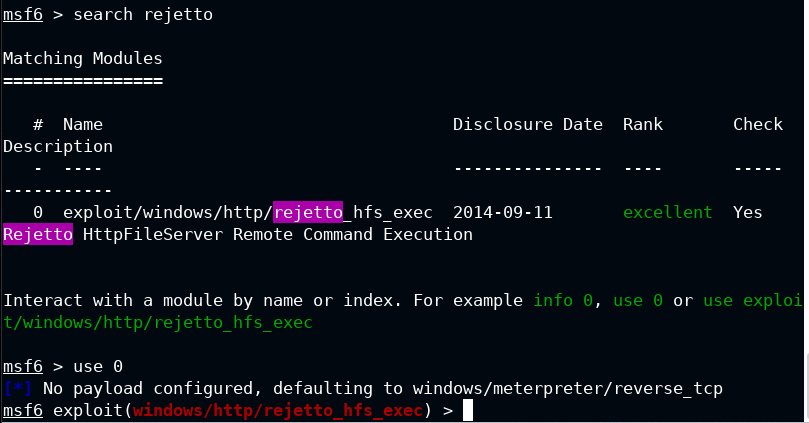
Run nmap service-version scan over port 80. We got a tip that HTTP is working, so we want to see what version is running



With this version 2.3 in mind, open Metasploit with msfconsole.

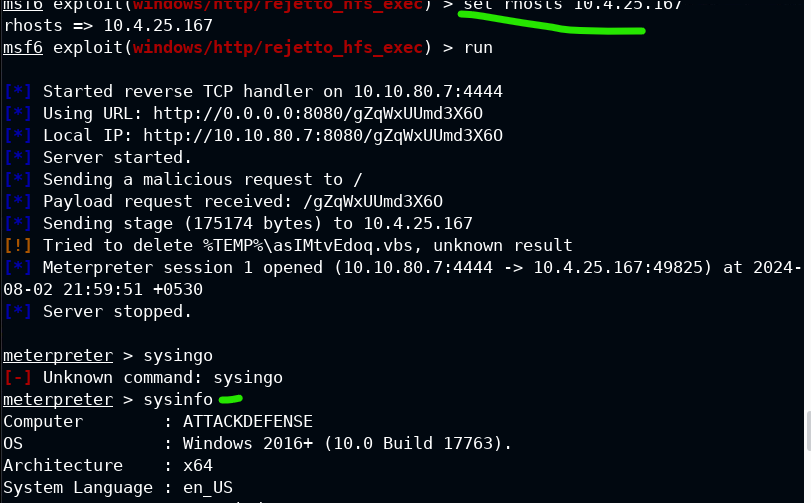
Remember that Rejetto helps get us in with HTTP File Server (HFS).

Let’s search for it.



Set the rhosts to the target and run exploit. This will give us a meterpreter session.

Then check sysinfo to see what kind of machine we’re dealing with.

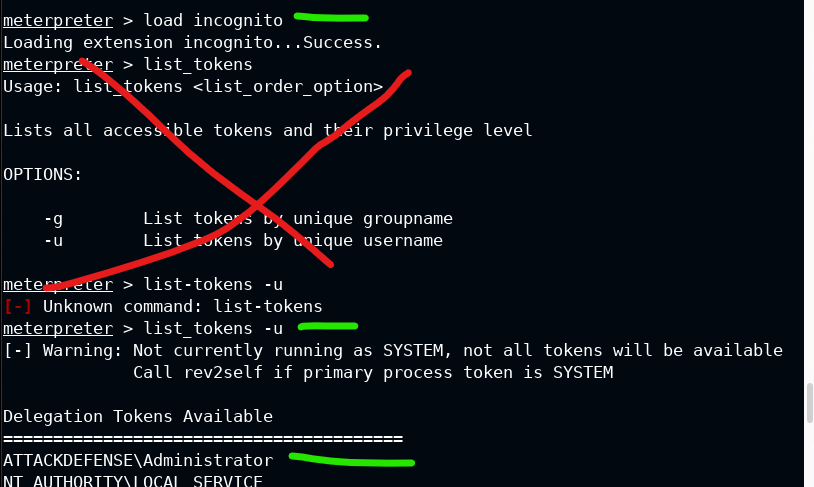


Check priveleges with command: getprivs

We have the ability to impersonate another user…



Load incognito, find the admin by lust\_tokens -u

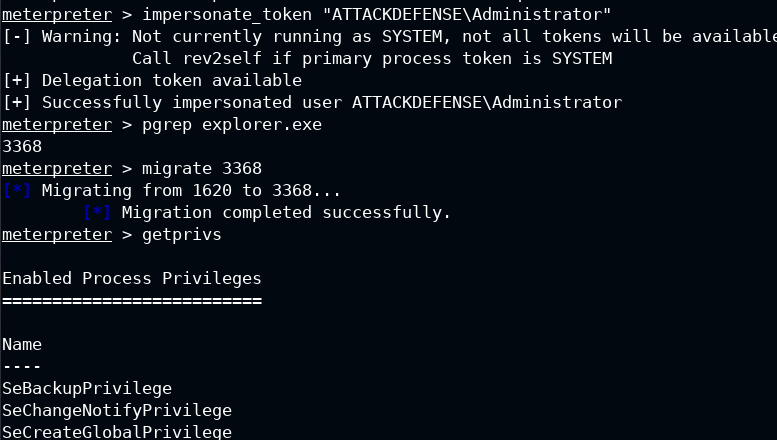


We use impersonation privs to become ‘like’ an administrator with the following command:

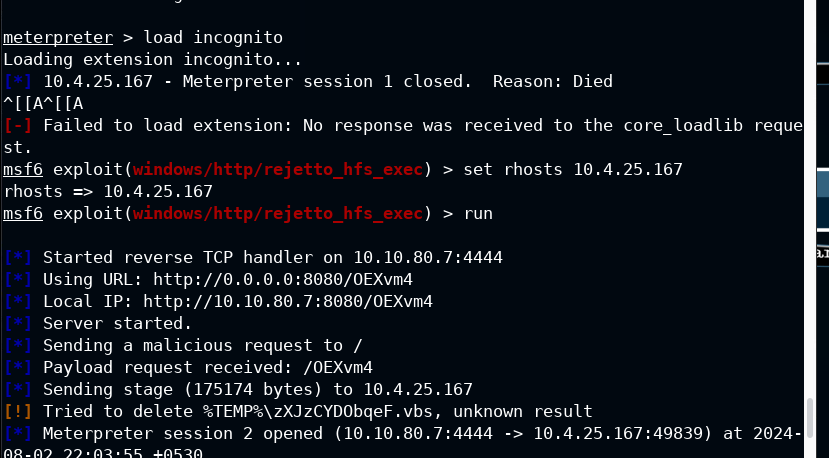
Impersonate\_token “admin name”

Then, use pgrep to find a process, and migrate to something like explorer.exe for meterpreter session stability.

\*Warning, to counteract, check logs when there are sessions activated for explorer.exe migration after an impersonation token is done. This smells malicious.



After migrating the process, meterpreter session may close down; run the exploit again to regenerate it



Now we can see that we are the admin, essentially, and can go to the Admin’s desktop and get the flag file.

