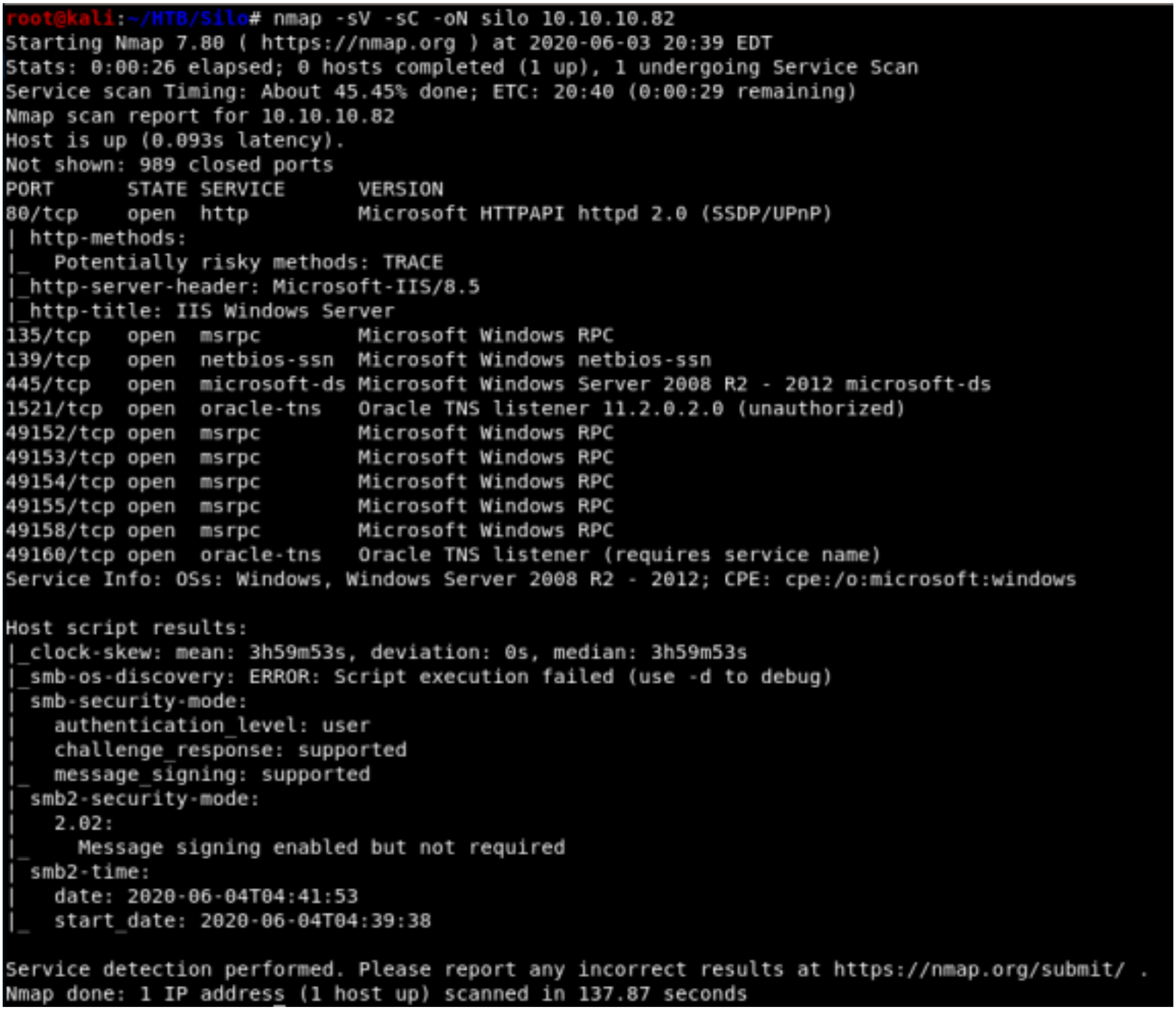
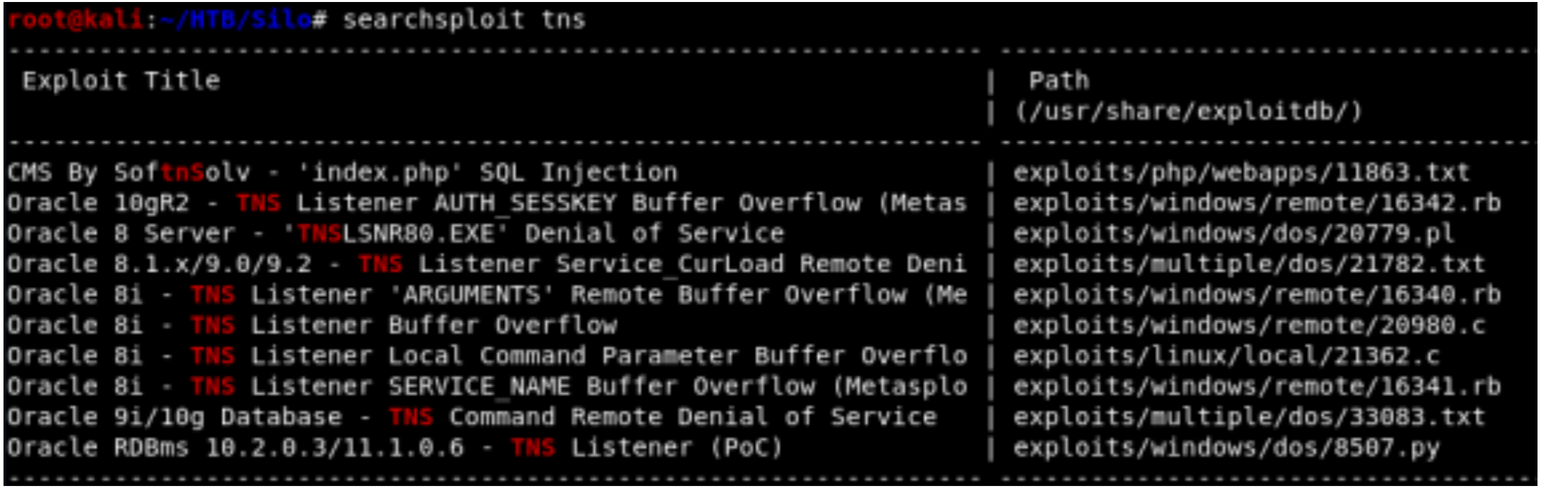
nmap scan



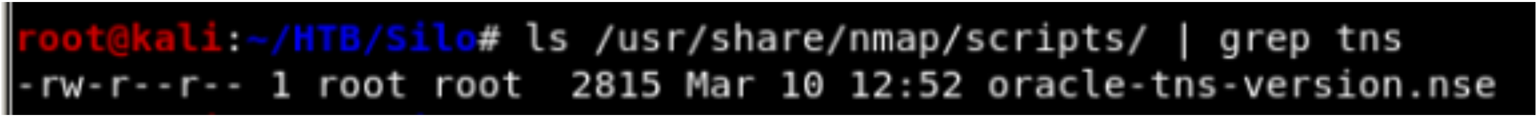
```
root@kali:~/HTB/Silo# nmap -sV -sC -oN silo 10.10.10.82
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-03 20:39 EDT
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 45.45% done; ETC: 20:40 (0:00:29 remaining)
Nmap scan report for 10.10.10.82
Host is up (0.093s latency).
Not shown: 989 closed ports
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)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 3h59m53s, deviation: 0s, median: 3h59m53s
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
| 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: 2020-06-04T04:41:53
|_  start_date: 2020-06-04T04:39:38

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 137.87 seconds
```

TNS possibly vulnerable



```
root@kali:~/HTB/Silo# searchsploit tns
--------------------------------------------------------------- ---------------------------------
 Exploit Title                                                 |  Path
                                                               | (/usr/share/exploitdb/)
--------------------------------------------------------------- ---------------------------------
CMS By SoftnSolv - 'index.php' SQL Injection                   | exploits/php/webapps/11863.txt
Oracle 10gR2 - TNS Listener AUTH_SESSKEY Buffer Overflow (Metas | exploits/windows/remote/16342.rb
Oracle 8 Server - 'TNSLSNR80.EXE' Denial of Service            | exploits/windows/dos/20779.pl
Oracle 8.1.x/9.0/9.2 - TNS Listener Service_CurLoad Remote Deni | exploits/multiple/dos/21782.txt
Oracle 8i - TNS Listener 'ARGUMENTS' Remote Buffer Overflow (Me | exploits/windows/remote/16340.rb
Oracle 8i - TNS Listener Buffer Overflow                       | exploits/windows/remote/20980.c
Oracle 8i - TNS Listener Local Command Parameter Buffer Overflo | exploits/linux/local/21362.c
Oracle 8i - TNS Listener SERVICE_NAME Buffer Overflow (Metasplo | exploits/windows/remote/16341.rb
Oracle 9i/10g Database - TNS Command Remote Denial of Service   | exploits/multiple/dos/33083.txt
Oracle RDBms 10.2.0.3/11.1.0.6 - TNS Listener (PoC)            | exploits/windows/dos/8507.py
--------------------------------------------------------------- ---------------------------------
```

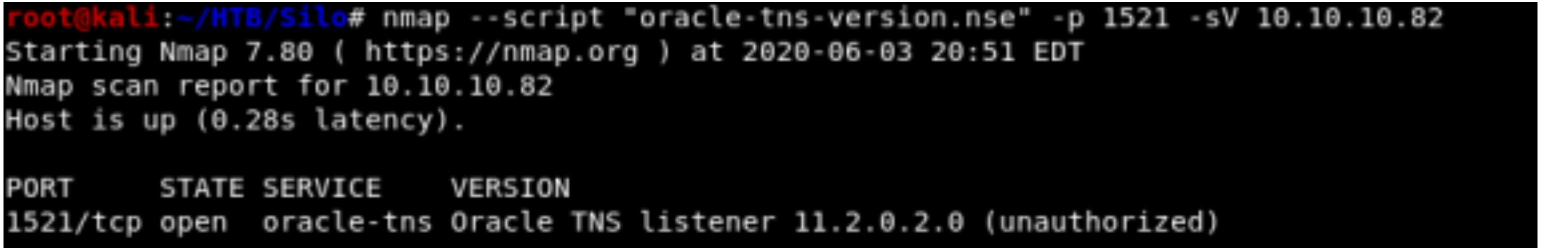
tns enumeration script



```
root@kali:~/HTB/Silo# ls /usr/share/nmap/scripts/ | grep tns
-rw-r--r-- 1 root root  2815 Mar 10 12:52 oracle-tns-version.nse
```

Well run this on ports 1521 and 49160

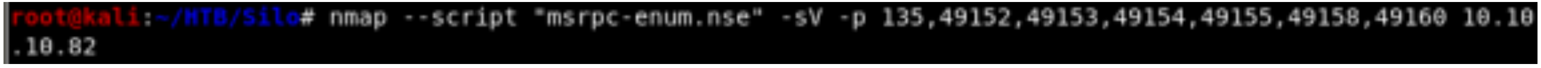
Turns out the version number was given to us in the original nmap scan



```
root@kali:~/HTB/Silo# nmap --script "oracle-tns-version.nse" -p 1521 -sV 10.10.10.82
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-03 20:51 EDT
Nmap scan report for 10.10.10.82
Host is up (0.28s latency).

PORT     STATE SERVICE    VERSION
1521/tcp open  oracle-tns Oracle TNS listener 11.2.0.2.0 (unauthorized)
```

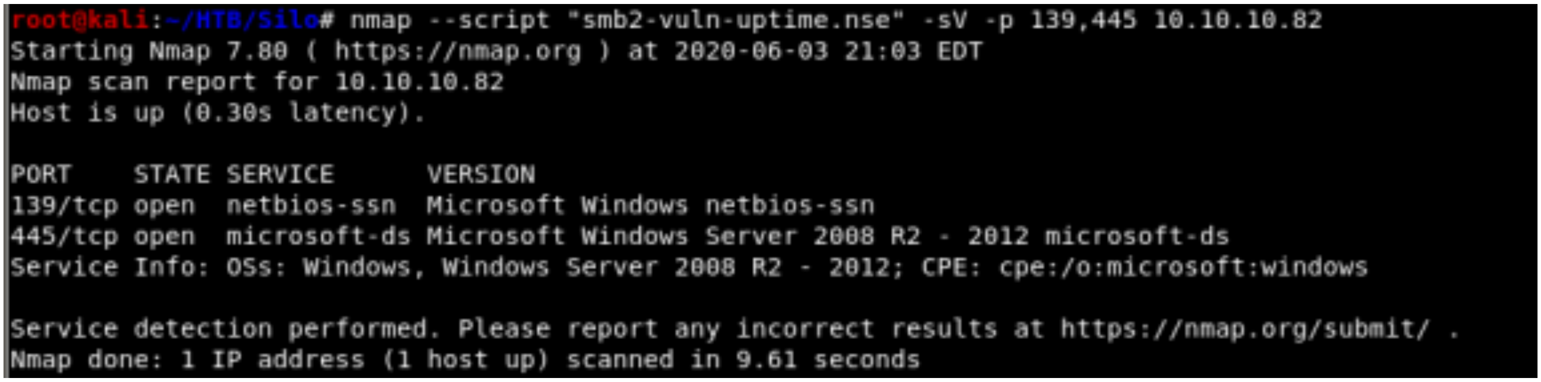
Quick google search for vulns shows that this version of TNS could be vulnerable! Possibly will come back to this

Enumerating msrpc with this scan



```
root@kali:~/HTB/Silo# nmap --script "msrpc-enum.nse" -sV -p 135,49152,49153,49154,49155,49158,49160 10.10
.10.82
```

this script didnt give any output which was unique from the first nmap scan

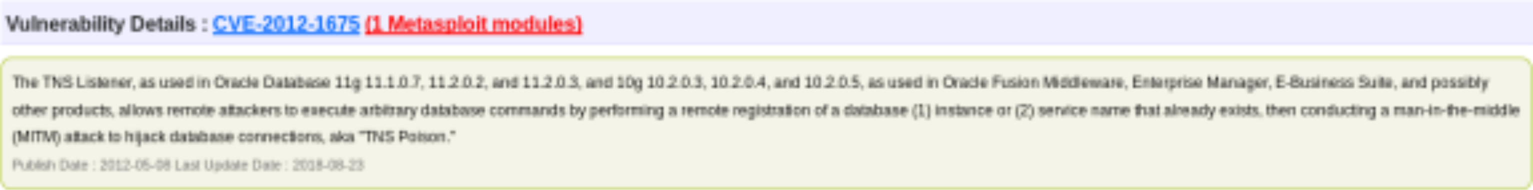


```
root@kali:~/HTB/Silo# nmap --script "smb2-vuln-uptime.nse" -sV -p 139,445 10.10.10.82
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-03 21:03 EDT
Nmap scan report for 10.10.10.82
Host is up (0.30s latency).

PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.61 seconds
```

It doesnt look like this machine is vulnerable to Eternal Blue or any other obvious smb/samba exploits either.... It now seems very likely that the TNS listener is what we need to target

Looking into CVEs related to TNS 11.2.0.2 might reveal our attack vector

This could possibly be useful to us

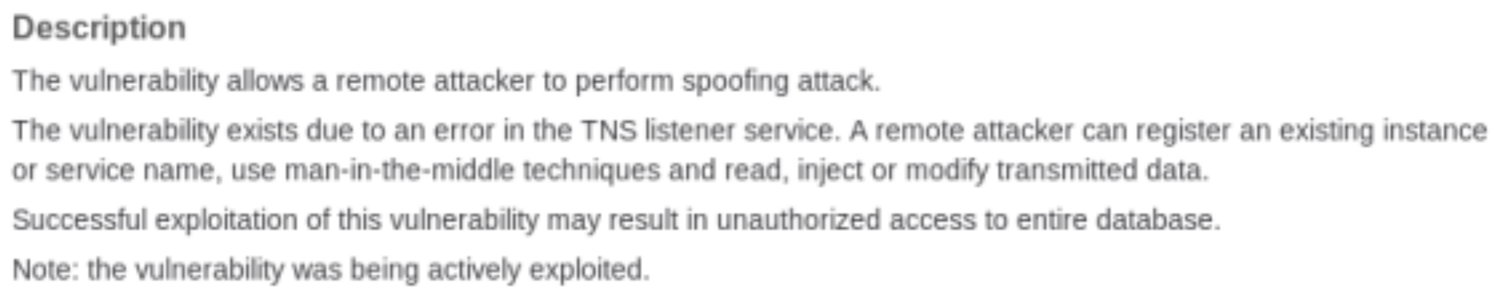


Vulnerability Details : CVE-2012-1675 (1 Metasploit modules)

The TNS Listener, as used in Oracle Database 11g 11.1.0.7, 11.2.0.2, and 11.2.0.3, and 10g 10.2.0.3, 10.2.0.4, and 10.2.0.5, as used in Oracle Fusion Middleware, Enterprise Manager, E-Business Suite, and possibly other products, allows remote attackers to execute arbitrary database commands by performing a remote registration of a database (1) instance or (2) service name that already exists, then conducting a man-in-the-middle (MITM) attack to hijack database connections, aka "TNS Poison."

Publish Date : 2012-05-08 Last Update Date : 2018-08-23

Reading more into this cve... it definitely seems like it can be useful



Description

The vulnerability allows a remote attacker to perform spoofing attack.

The vulnerability exists due to an error in the TNS listener service. A remote attacker can register an existing instance or service name, use man-in-the-middle techniques and read, inject or modify transmitted data.

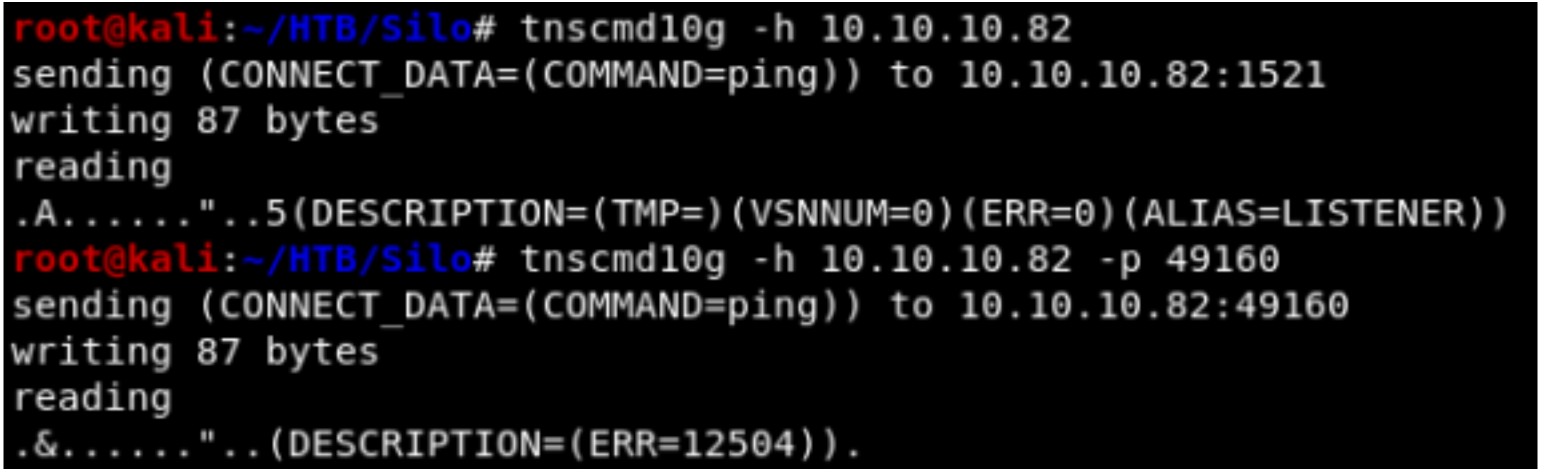
Successful exploitation of this vulnerability may result in unauthorized access to entire database.

Note: the vulnerability was being actively exploited.

Two tools which are useful for enumerating the oracle TNS listener are: tnscmd10g and https://github.com/-quentinhardy/odat

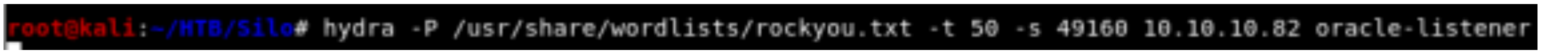
TNS enumeration:

Connecting to both ports shows us that one seems to return some information (which I dont understand yet), and the other port sends an error (thankfully I know what those are :^))



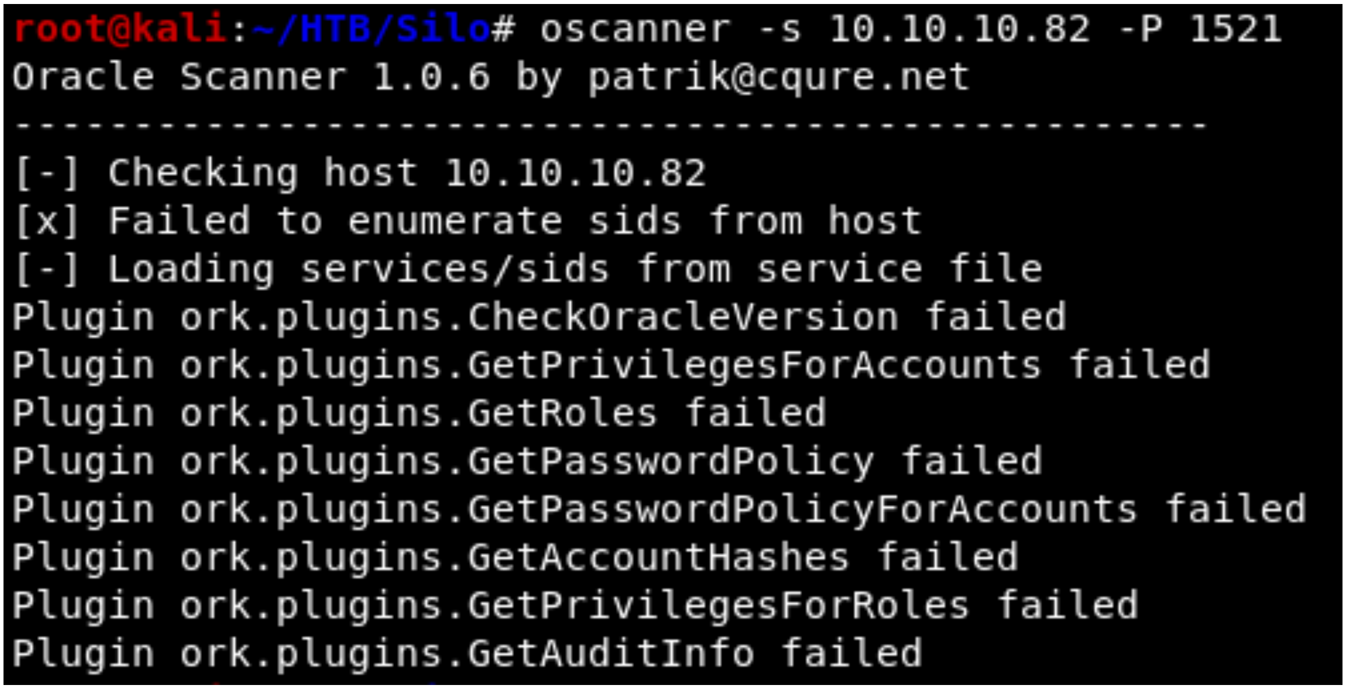
```
root@kali:~/HTB/Silo# tnscmd10g -h 10.10.10.82
sending (CONNECT_DATA=(COMMAND=ping)) to 10.10.10.82:1521
writing 87 bytes
reading
.A......"..5(DESCRIPTION=(TMP=)(VSNNUM=0)(ERR=0)(ALIAS=LISTENER))
root@kali:~/HTB/Silo# tnscmd10g -h 10.10.10.82 -p 49160
sending (CONNECT_DATA=(COMMAND=ping)) to 10.10.10.82:49160
writing 87 bytes
reading
.&......"..(DESCRIPTION=(ERR=12504)).
```

This command can supposedly be useful for brute forcing TNS auth creds



```
root@kali:~/HTB/Silo# hydra -P /usr/share/wordlists/rockyou.txt -t 50 -s 49160 10.10.10.82 oracle-listener
```

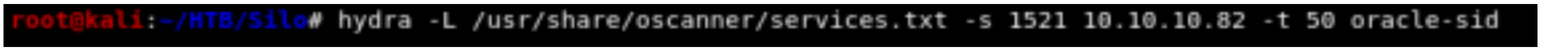
Apparently the next step in enumerating this service needs to be to get SID's from the host so theres a tool called oscanner which seems to let us grab this info



```
root@kali:~/HTB/Silo# oscanner -s 10.10.10.82 -P 1521
Oracle Scanner 1.0.6 by patrik@cqure.net
--------------------------------------------------
[-] Checking host 10.10.10.82
[x] Failed to enumerate sids from host
[-] Loading services/sids from service file
Plugin ork.plugins.CheckOracleVersion failed
Plugin ork.plugins.GetPrivilegesForAccounts failed
Plugin ork.plugins.GetRoles failed
Plugin ork.plugins.GetPasswordPolicy failed
Plugin ork.plugins.GetPasswordPolicyForAccounts failed
Plugin ork.plugins.GetAccountHashes failed
Plugin ork.plugins.GetPrivilegesForRoles failed
Plugin ork.plugins.GetAuditInfo failed
```

After running the script we weren't able to get any info... meaning that we probably need to get the password to communicate with the other TNS Listener port

While trying to brute force the password, we can also try to brute force SID's with this command



```
root@kali:~/HTB/Silo# hydra -L /usr/share/oscanner/services.txt -s 1521 10.10.10.82 -t 50 oracle-sid
```