Silo

Nmap

I ran a quick scan (`nmap -p- -Pn -T5 10.10.10.82`) and then started some basic enumeration whilst the second, deeper scan ran:
`nmap -p 80,135,139,445,1521,5985,47001,49153-49162 -Pn -A 10.10.10.82` . There's probably a smarter way to run that second scan, I just don't know it.

```
PORT      STATE  SERVICE      VERSION
80/tcp    open   http         Microsoft IIS httpd 8.5
| 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)
5985/tcp  open   http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open   http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49153/tcp open   msrpc        Microsoft Windows RPC
49154/tcp open   mpc        Microsoft Windows RPC
49155/tcp open   msrpc        Microsoft Windows RPC
49156/tcp closed unknown
49157/tcp closed unknown
49158/tcp open   msrpc        Microsoft Windows RPC
49159/tcp closed unknown
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
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:w

Host script results:
|_clock-skew: mean: 3m32s, deviation: 0s, median: 3m32s
|_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: 2020-07-05T13:54:53
|_  start_date: 2020-07-05T13:40:36
```

Initial Enum: Fail

We can't enumerate the SMB service, so will maybe have to wait till we get some creds?

Taking a look at the website, we can determine it's written in **.aspx** by going **/index.[X]**, and swapping [X] for the usual .php, htm, etc etc until we find one that works.

I used `gobuster` but didn't get nothing interesting.

Let's look at the Oracle service

Oracle

I'm not to familar with port **1521**, so I turned to HackTricks to guide me:
https://book.hacktricks.xyz/pentesting/1521-1522-1529-pentesting-oracle-listener

Odat Installation

It seems the best tool for the job is **Odat**, however it's a pain to install. Following this guide works to a certain extent, but needs some editing here and there. I've tried my best to make things clear.
https://dastinia.io/tutorial/2018/07/31/installing-oracle-database-attacking-tool-on-kali/ .

Oh and make sure you do everything as root by going `su` . It makes life easier.

Setup Troubleshooting

When (**not if**) you encounter problems following this guide when it comes to executing **sqlplus,** try this: