Ethereal

Synopsis

Etheral showcases how DNS can be used to exfiltrate information from a system, and is applicable to many externally facing applications. It also features a very restrictive environment, which is made more hospitable by the use of the OpenSSL "LOLBIN". It highlights how malicious shortcut files can be used to move laterally and vertically within a system or network. Finally, it shows how an attacker would be able use trusted certificates to defeat a stringent application whitelisting configuration. Finally, it showcases techniques for creating and signing Windows Installer (MSI) files.

Skills

- Knowledge of Internet protocols
- Knowledge of Windows
- DNS data exfiltration
- OpenSSL eagress check
- Malicious shortcut testing and creation
- Malicious MSI testing and creation
- Enumeration and replication of AppLocker policy

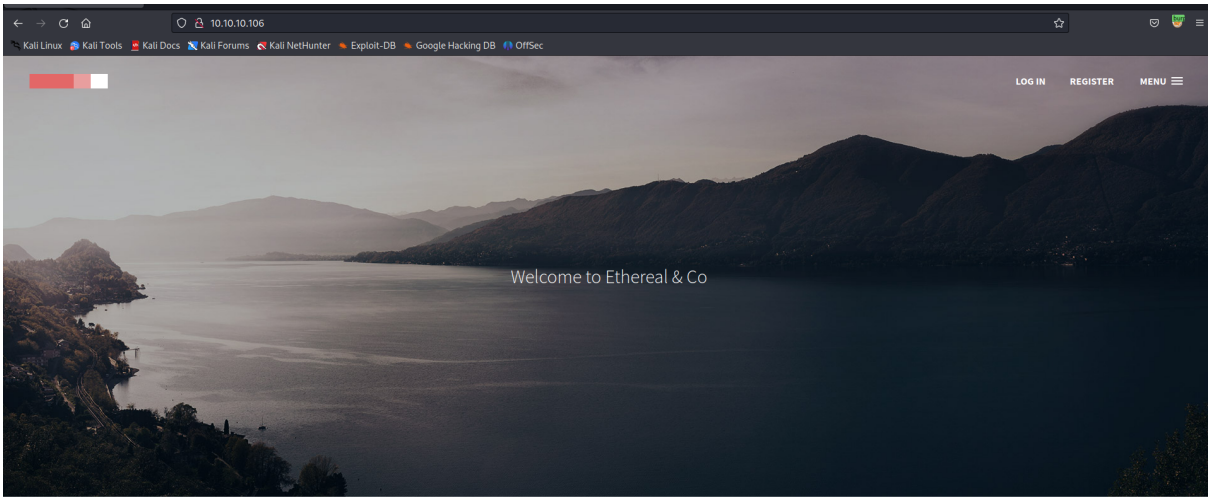
Exploitation

As always we start with the nmap to check what services/ports are open

```
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.16.249.135 is not the same as 10.10.10.106
80/tcp   open  http    Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Ethereal
|_http-server-header: Microsoft-IIS/10.0
8080/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Bad Request
|_http-server-header: Microsoft-HTTPAPI/2.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016|2012|2008|10 (91%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microso
Aggressive OS guesses: Microsoft Windows Server 2016 (91%), Microsoft Windows Server 2012 (85%), Microsoft Windows Server 2012 or Window
), Microsoft Windows Server 2012 R2 (85%), Microsoft Windows Server 2008 R2 (85%), Microsoft Windows 10 1607 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

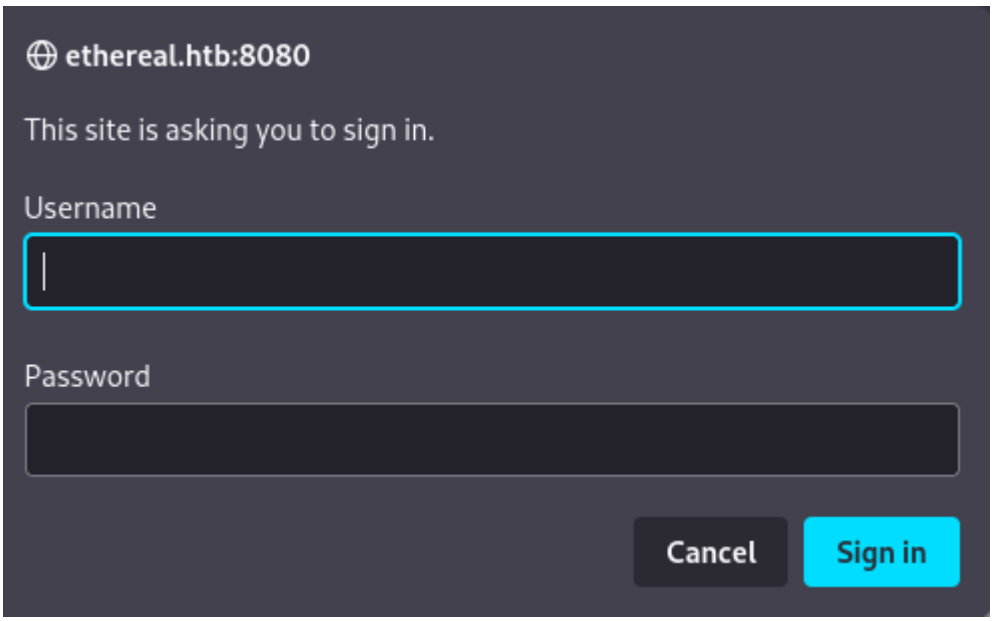
We can see a few ports open, but we decided to start form the web port because web has the broadest attack surface

Opening browser gave us the following web app

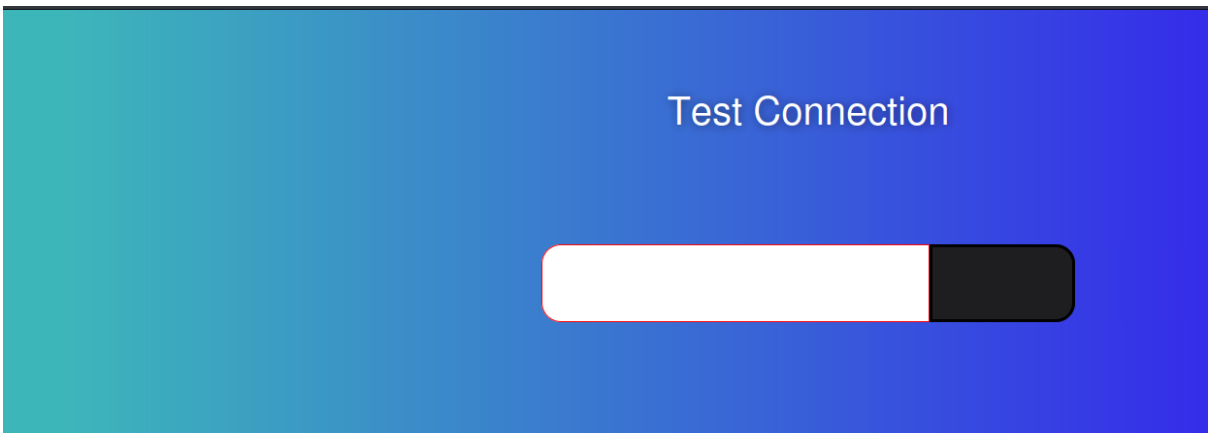


Incepted in 2003, Ethereal & Co (Pvt) Ltd is a leading Development & Design expert company

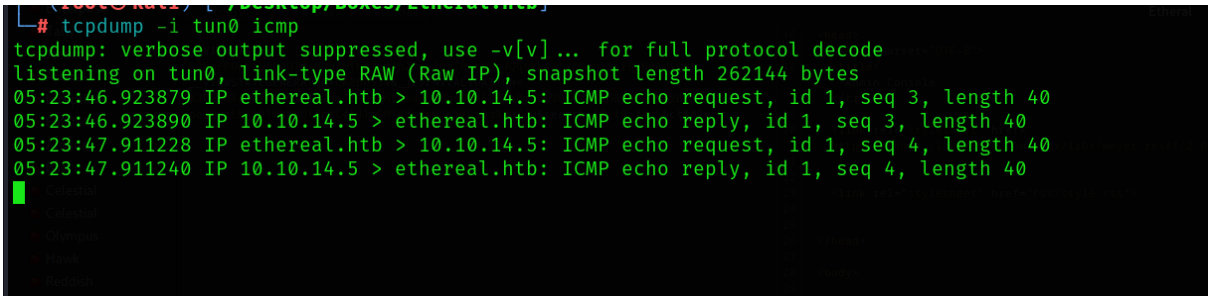
When we tried to access an administrator pane we were asked for credentials



So we launched hydra and after a while we found a valid combination what allowed us to get an unauthorised access, this provided us with the test connection functionality

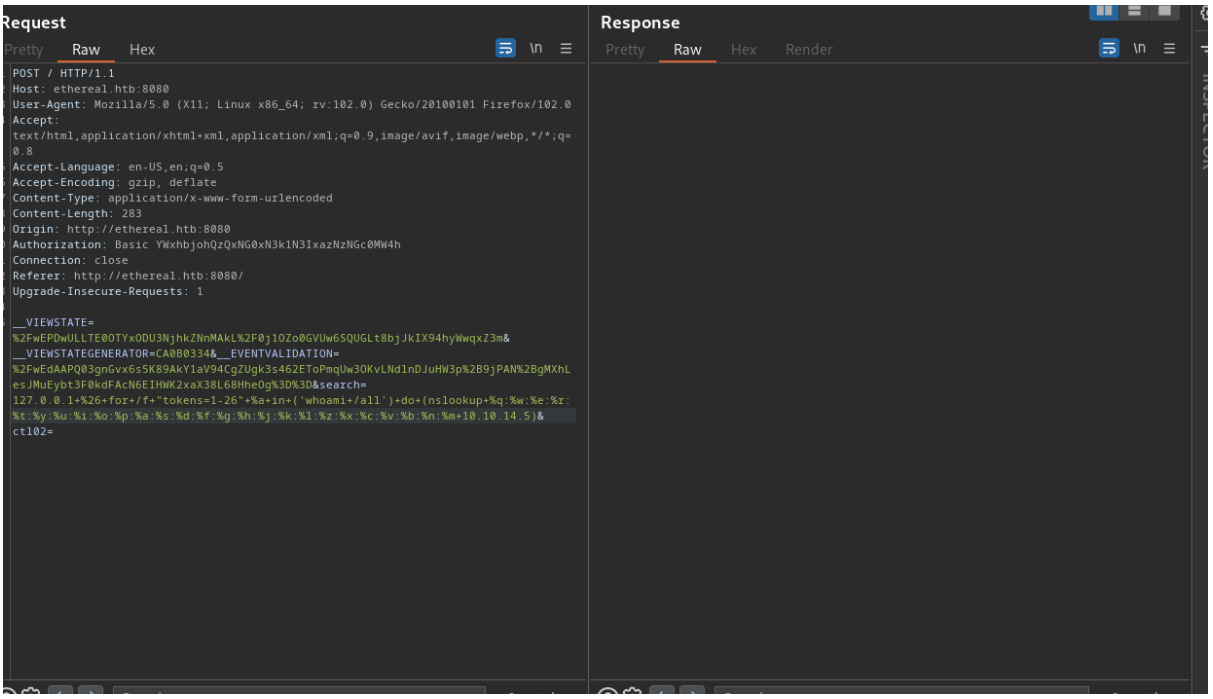


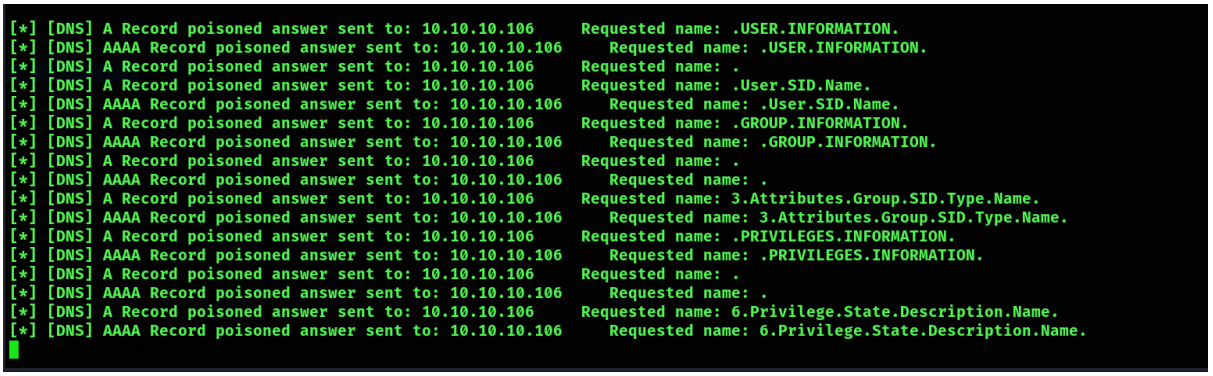
We confirmed that we can abused this functionality to ping our attacker's machine



Next we tried to get a reverse shell but all attempts failed due to the very strict firewall rules

So, the next thing we tried was poisoning DNS via malicious nslookup command to enumerate directories on the system





And we successfully poisoned DNS services what allowed us to read files from the system

Next step as to automate is via python code so everything will be looking much better