Retro

Enumeration

Nmap Scan

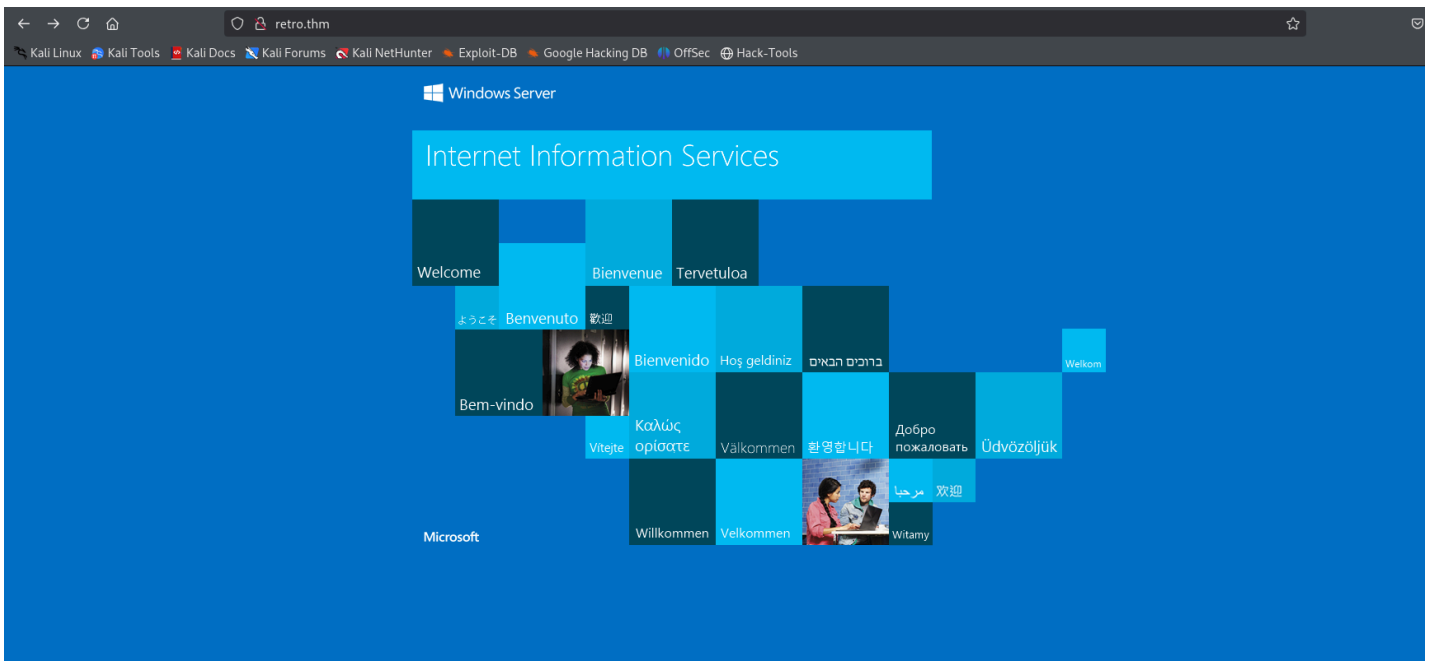
```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE

3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-04-23T07:40:19+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: RETROWEB
|   NetBIOS_Domain_Name: RETROWEB
|   NetBIOS_Computer_Name: RETROWEB
|   DNS_Domain_Name: RetroWeb
|   DNS_Computer_Name: RetroWeb
|   Product_Version: 10.0.14393
|_  System_Time: 2025-04-23T07:40:12+00:00
| ssl-cert: Subject: commonName=RetroWeb
| Not valid before: 2025-04-22T07:30:10
|_Not valid after:  2025-10-22T07:30:10
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

- Fuzz the HTTP port
- Find the credentials (username and password) to log in to the RDP port

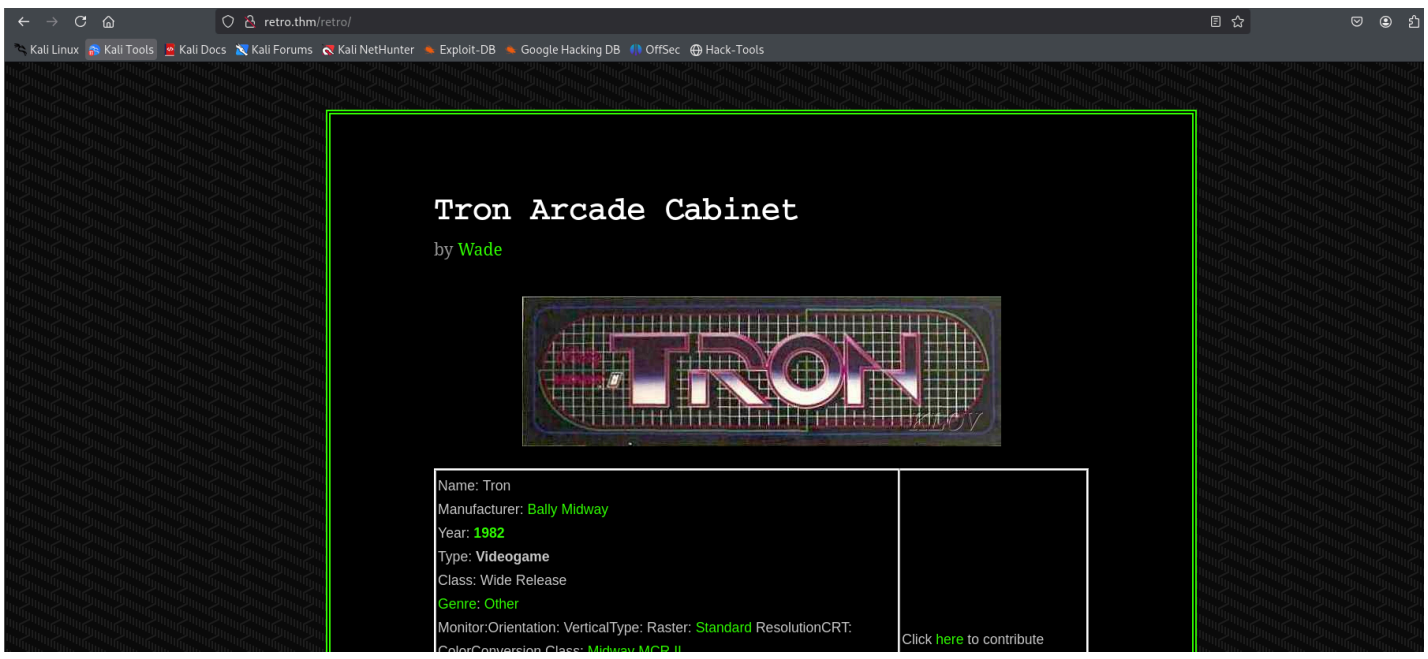
HTTP (80)

FFUF Scanning

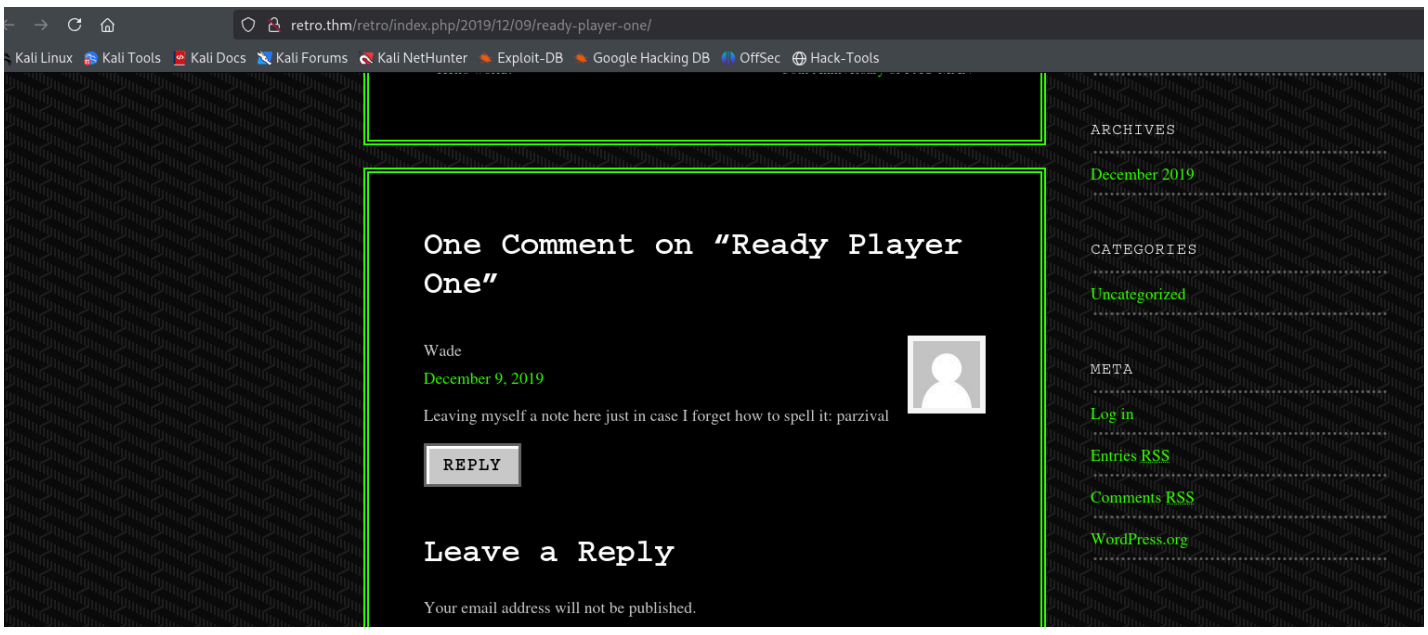
```
retro                   [Status: 301, Size: 146, Words: 9, Lines: 2, Duration: 590ms]
```



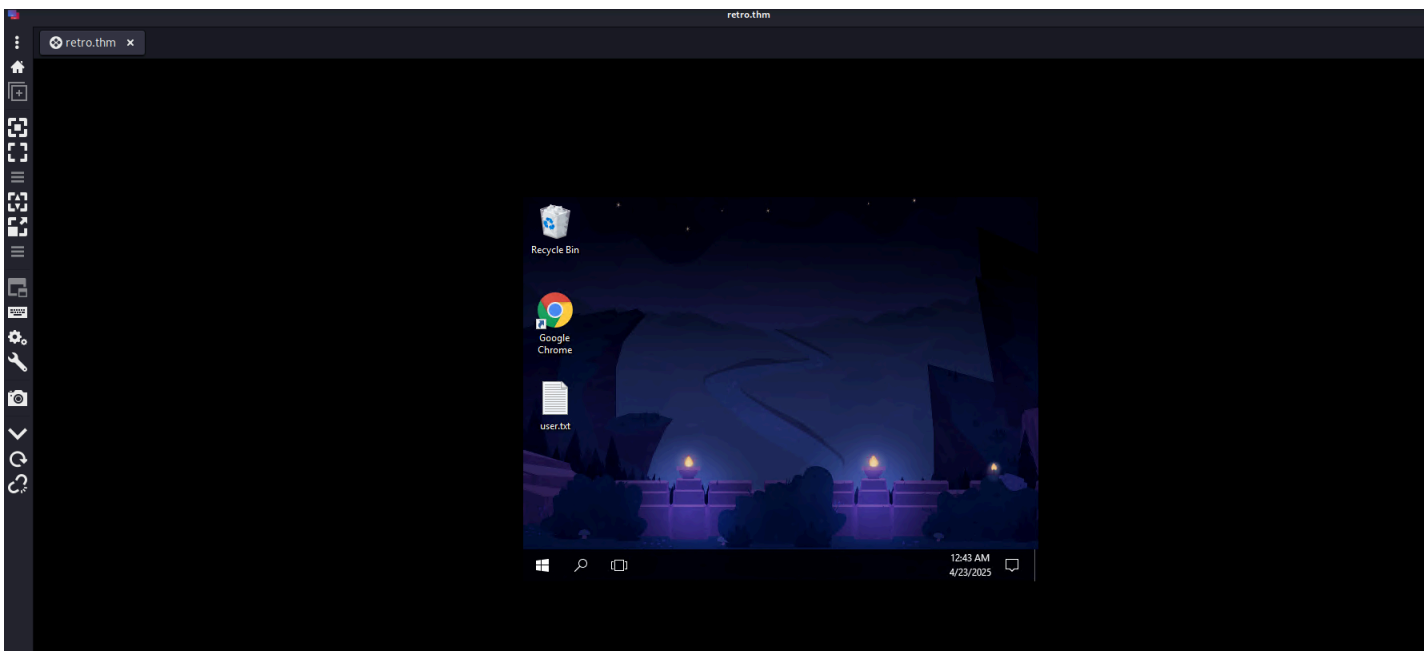
The webpage- IIS Server



/retro- Some blog webpage

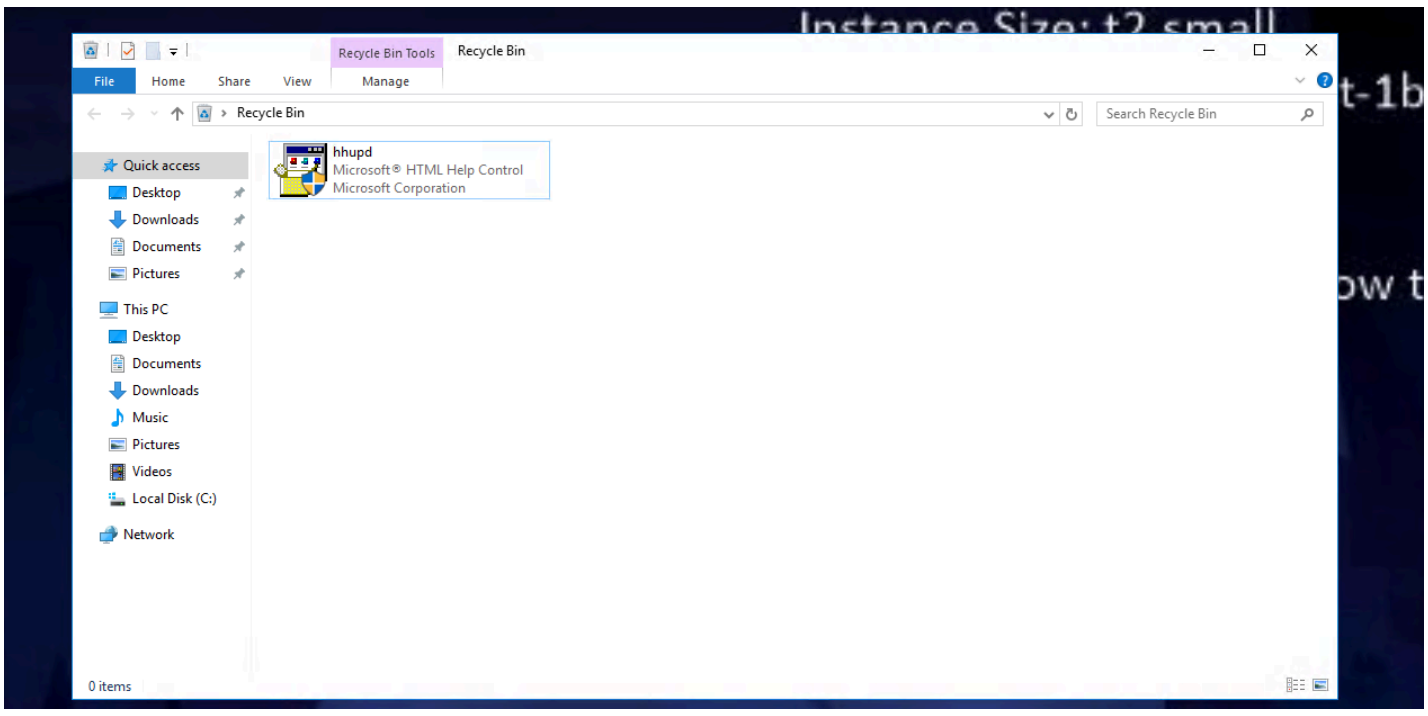


Password: parzival (RDP password)

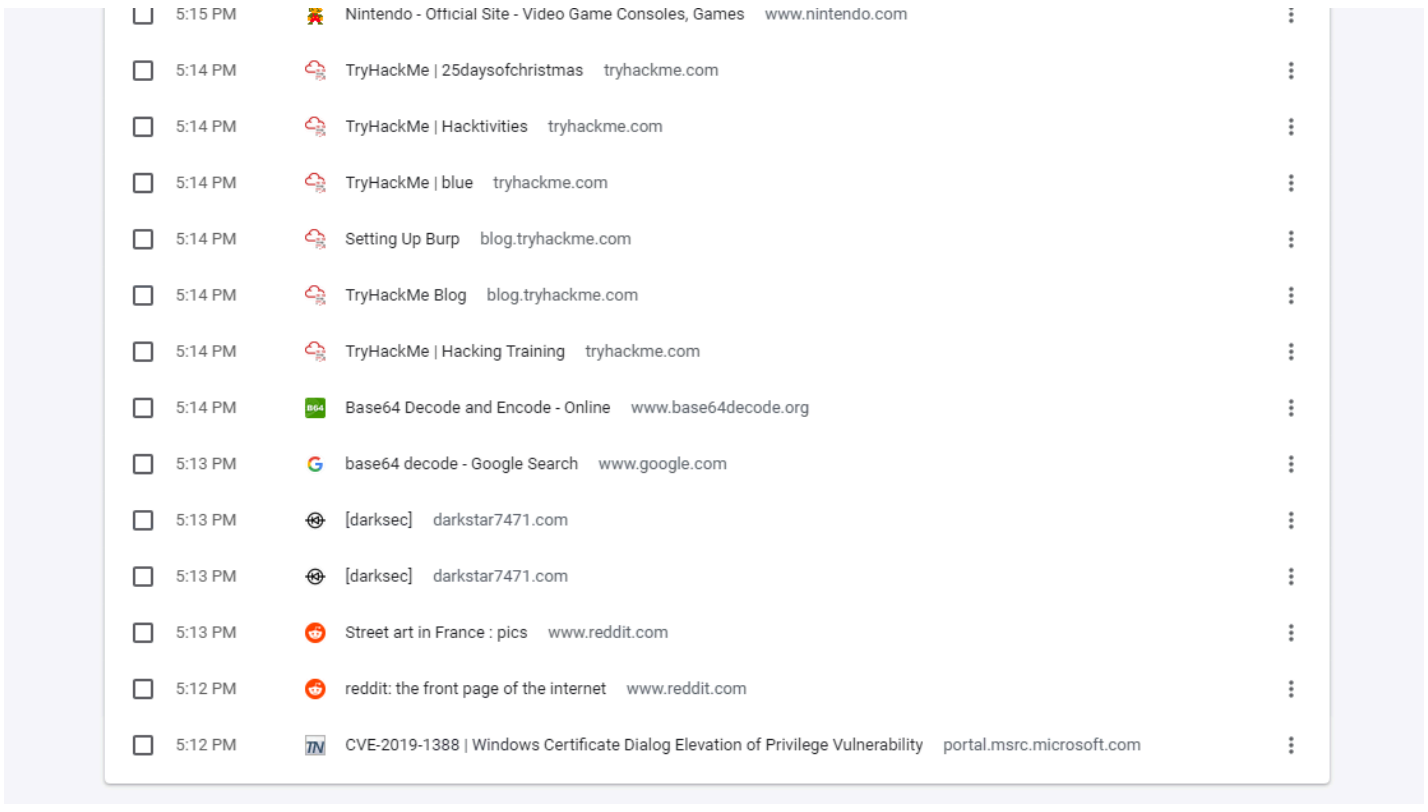


RDP credentials- wade:parzival

Root Flag/Privilege Escalation



Found this in the Recycle Bin. This has a privilege escalation technique (CVE–2019–1388).



The Chrome history does reveal some information on the CVE.

But this didn’t work.

This method will take some attempts as the browsers won’t be shown when opening the hhupd.exe as an administrator. So the machine has to be restarted multiple times to finally get the root shell.