

# Retro

## Working Theory

## Enumeration

## Tools

### nmap

```
nobodyatall@0xB105F00D:~/tryhackme/retro$ sudo nmap -sC -sV -oN portScn -Pn 10.10.104.151
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-22 13:17 +08
Nmap scan report for 10.10.104.151
Host is up (0.20s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: IIS Windows Server
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| 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: 2020-05-22T05:18:24+00:00
| ssl-cert: Subject: commonName=RetroWeb
| Not valid before: 2020-05-21T05:16:39
|_ Not valid after: 2020-11-20T05:16:39
```

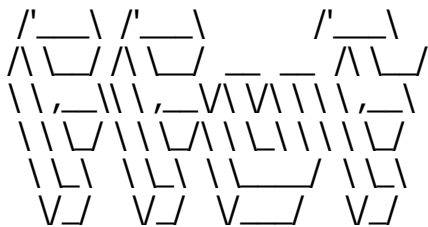
|\_ssl-date: 2020-05-22T05:18:28+00:00; +4s from scanner time.  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:  
|\_clock-skew: mean: 4s, deviation: 0s, median: 3s

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 30.70 seconds

## fuzz

~/script/reconnaissance/ffuf/ffuf -u http://10.10.43.187/FUZZ -w /usr/share/wordlists/dirb/big.txt



v0.12

---

:: Method : GET  
:: URL : http://10.10.43.187/FUZZ  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout : 10  
:: Threads : 40  
:: Matcher : Response status: 200,204,301,302,307,401,403

---

retro [Status: 301, Size: 149, Words: 9, Lines: 2]  
:: Progress: [20469/20469] :: 196 req/sec :: Duration: [0:01:44] :: Errors: 0 ::

## Targets

### http port 80

Found interesting directory  
=====  
/retro

/retro

=====

Found User: Wade

found interesting post: Ready Player One

potential credential: parzival

## Post Exploitation

## Privilege Escalation

<https://nvd.nist.gov/vuln/detail/CVE-2019-1388>

the user checking about the privilege escalation method on his machine and bookmarked the cve page on his chrome.

he did download the installer to perform the testing too and didnt clean the recycle bin

get the isntaller from recycle bin

perform privilege escalation with Windows Certificate Dialog by right click and run as Admin user to prompt a browser window by clicking the certificate issuer link, then prompt a cmd.exe shell with the save as(page) windows as a NT authority User.

## Creds

RDP Credential

=====

Wade:parzival

## Flags

## Write-up Images