

# Blaster

## Enumeration

### tools

```
# Nmap 7.80 scan initiated Thu May 21 15:15:29 2020 as: nmap -sC -sV -oN portScn -Pn 10.10.43.187
Nmap scan report for 10.10.43.187
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: 2020-05-21T07:15:56+00:00
| ssl-cert: Subject: commonName=RetroWeb
| Not valid before: 2020-05-20T07:10:40
|_ Not valid after: 2020-11-19T07:10:40
|_ ssl-date: 2020-05-21T07:15:59+00:00; 0s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

```
# Nmap done at Thu May 21 15:16:00 2020 -- 1 IP address (1 host up) scanned in 30.39 seconds
```

### nmap

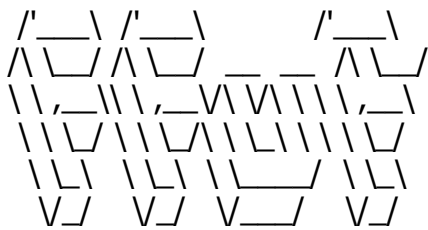
```
# Nmap 7.80 scan initiated Thu May 21 15:15:29 2020 as: nmap -sC -sV -oN portScn -Pn 10.10.43.187
Nmap scan report for 10.10.43.187
Host is up (0.20s latency).
Not shown: 998 filtered ports
```

```
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: 2020-05-21T07:15:56+00:00
| ssl-cert: Subject: commonName=RetroWeb
| Not valid before: 2020-05-20T07:10:40
|_ Not valid after: 2020-11-19T07:10:40
|_ ssl-date: 2020-05-21T07:15:59+00:00; 0s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
# Nmap done at Thu May 21 15:16:00 2020 -- 1 IP address (1 host up) scanned in 30.39 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 ::

## services

### port 80

directory /retro

=====

Username found: Wade

found potential credential in /retro/index.php/2019/12/09/ready-player-one/

Wade: parzival

## Post Exploitation

### privilege escalation

Found CVE-2019-1388: abuse UAC Windows Certificate Dialog (Windows Local Privilege Escalation)

grab the installer out from the recycle bin and test the local privilege escalation vector

### creds

RDP

===

Wade: parzival

### imgPOC