Nmap

Let's run a quick nmap scan:

```
sudo nmap -sC -sV -p53,135,139,445,593,49152,49153,49154,49155,49158,49160,49170,49179,49180 -oN blackfield.nmap -vvv -Pn -n -T4 10.10.10.192
```

and then follow it up with a deeper nmap scan on the found ports:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-06 15:28:08 +0100
Initiating Parallel DNS resolution of 1 host. at 15:28:08, 0.00s elapsed
DNS resolution for 1 hosts finished.
Initiating SYN Stealth Scan at 15:28:08
Scanning 10.10.10.192 [17 ports]
Discovered open port 135/tcp on 10.10.10.192
Discovered open port 53/tcp on 10.10.10.192
Discovered open port 139/tcp on 10.10.10.192
Discovered open port 445/tcp on 10.10.10.192
Discovered open port 49152/tcp on 10.10.10.192
Discovered open port 593/tcp on 10.10.10.192
Discovered open port 49153/tcp on 10.10.10.192
Discovered open port 49154/tcp on 10.10.10.192
Discovered open port 49155/tcp on 10.10.10.192
Discovered open port 49158/tcp on 10.10.10.192
Discovered open port 49160/tcp on 10.10.10.192
Discovered open port 49170/tcp on 10.10.10.192
Discovered open port 49179/tcp on 10.10.10.192
Discovered open port 49180/tcp on 10.10.10.192
Completed SYN Stealth Scan at 15:28:08, 0.03s elapsed (17 total ports)
Nmap scan report for 10.10.10.192
Host is up, received reply-to-ping (0.0s latency).
Scanned at 2020-09-06 15:28:08 BST for 0s
PORT     STATE SERVICE      REASON      VERSION
53/tcp   open  domain       syn-ack ttl 127 Microsoft Windows Active Directory DNS 6.0 (6.1DB7A9A)
135/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp  open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds syn-ack ttl 127 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
593/tcp  open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49152/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
49158/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
49160/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
49170/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
49179/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
49180/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
Read data files from: /usr/bin/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
           Raw packets sent: 17 (680B) | Rcvd: 17 (680B)
```

SMB Enum

`smbclient` doesn't find anything interesting without a password:

```
smbclient -L 10.10.10.192
```

```
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        profiles$       Disk
        SYSVOL          Disk      Logon server share
        forensic        Disk
SMB1 disabled -- no workgroup available
```

(profiles$)

If we connect to **profiles$**, we get a load of subdirectories:

```
smbclient \\10.10.10.192\profiles$
```

```
Enter WORKGROUP\root's password:
Anonymous login successful
  .                   D        0  Wed Jun 03 16:47:12 2020
  ..                  D        0  Wed Jun 03 16:47:12 2020
  AAD3B435B51404EEAAD3B435B51404EE.HTA    A     1954  Wed Jun 03 16:47:12 2020
  AAD3B435B51404EEAAD3B435B51404EE.TxR    A    70554  Wed Jun 03 16:47:12 2020
  AAD3B435B51404EEAAD3B435B51404EE.TxR    A    70554  Wed Jun 03 16:47:12 2020
  ...
  ...
  ...
```