GoodSecurity Penetration Test Report

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

04/11/2020

# 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 exploit two programs that had major vulnerabilities. The details of the attack can be found in the ‘Findings’ category.

# Findings

Machine IP:

**192.168.0.20**

Hostname:

As per evidence screenshot **penetration-1701.png** the Host name is

**MSEDGEWIN10**

Vulnerability Exploited:

As per evidence screenshot **penetration-1703.png** the Exploit Title is

**Icecast 2.0.1 (Windows x86) – Header Overwrite**

Vulnerability Explanation:

By definition, an attack is possible when the Icecast Server has not been patched to latest versions, which leaves Icecast Server versions up to 2.0.1 susceptible to buffer overflow vulnerabilities.

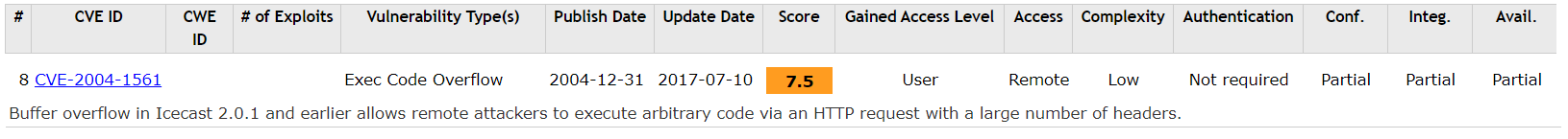
The vulnerability allows for code to be executed remotely when the Icecast server is running.

Buffer overflow in Icecast 2.0.1 and earlier allows remote attackers to execute arbitrary code via an HTTP request with a large number of headers.

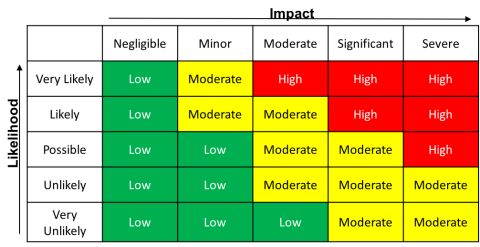
The vulnerability is only exploitable when code is remotely executed on Microsoft Operating Systems, however the buffer overflow affects all platforms, and is only exploitable when a sensitive IP address is located adjacent to the affected buffer.

Severity:

According to <https://www.cvedetails.com/vulnerability-list/vendor_id-693/Icecast.html> the version 2.0.1 of Icecast Server has a **Security Vulnerability score of 7.5**



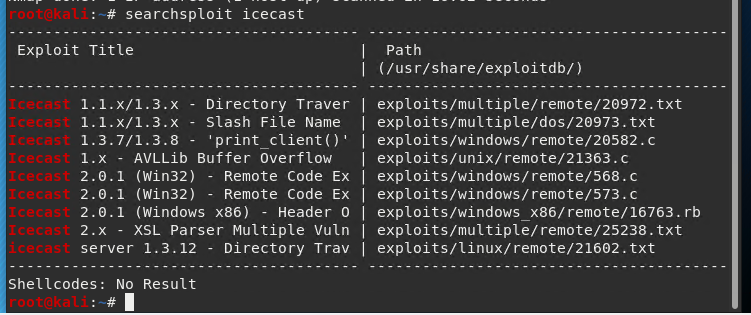
Based on my expert opinion, the vulnerability risk is **HIGH.** The likelihood of a data breach is **Very Likely,** and the impact to the business will be **Significant.** In my opinion, it is not **if the vulnerability will be exploited, but when.**



Proof of Concept:

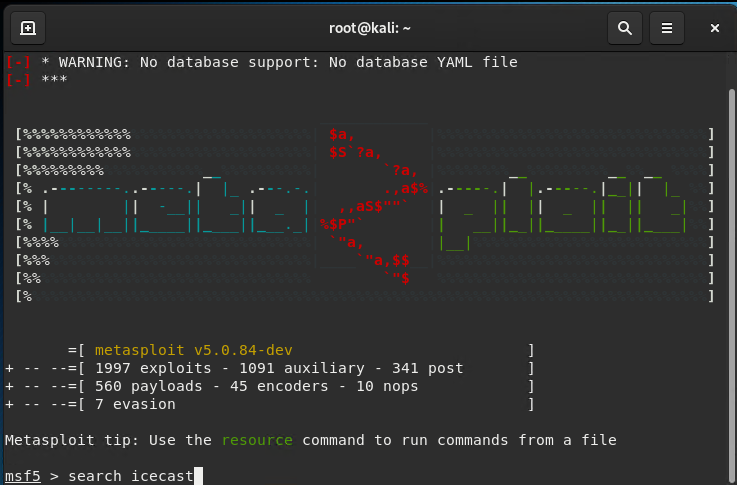
Terminal commands have been **highlighted.**

**Searchsploit icecast**

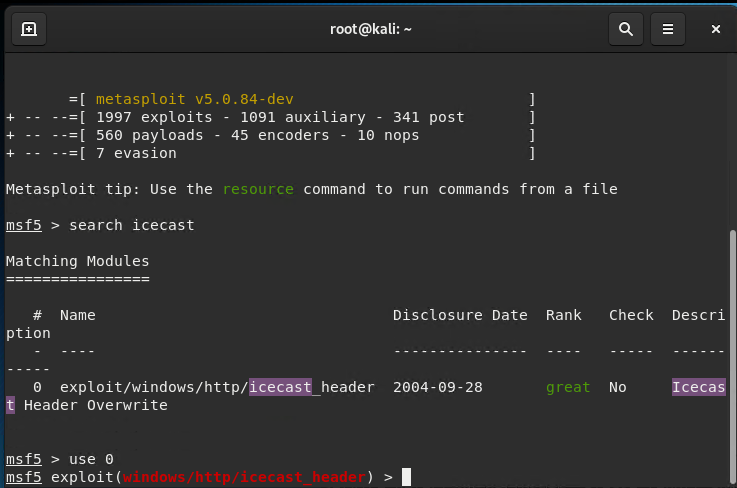


then using Metasploit,

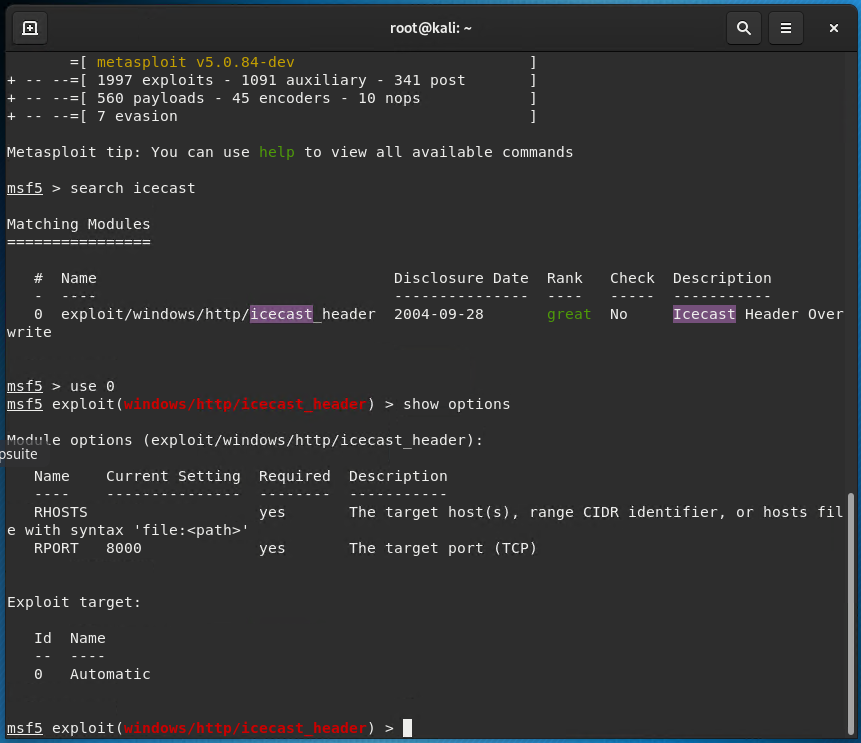
**search icecast**



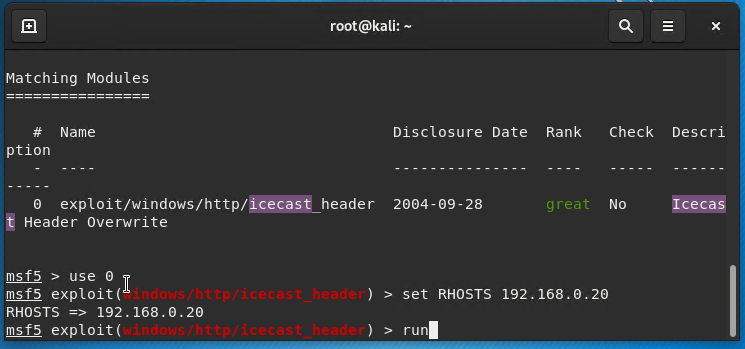
**use 0**



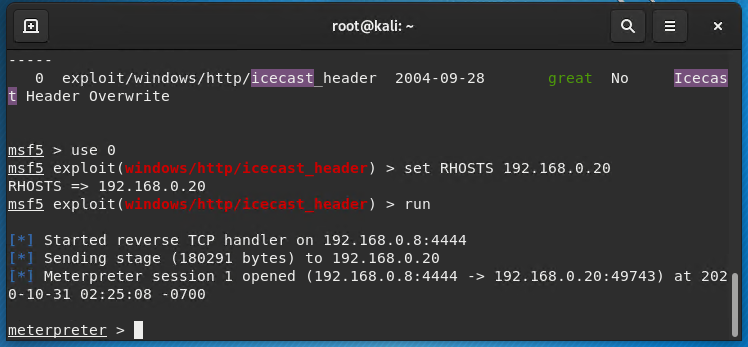
**show options**

****

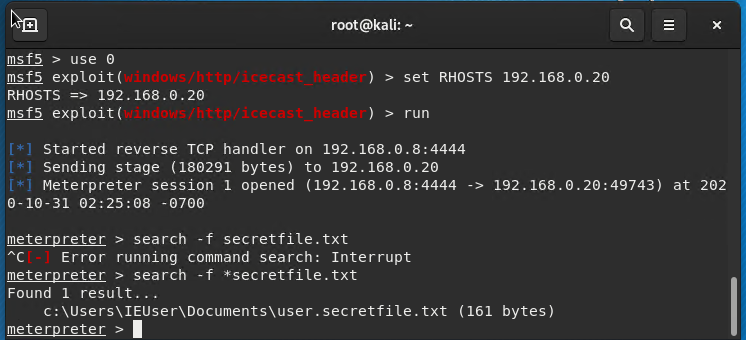
**set RHOSTS 192.168.0.20**



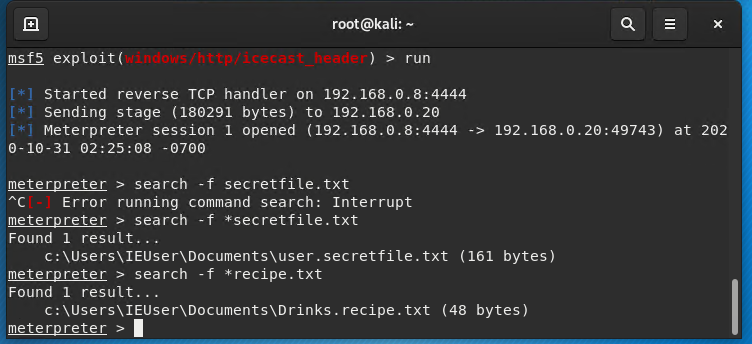
**run**



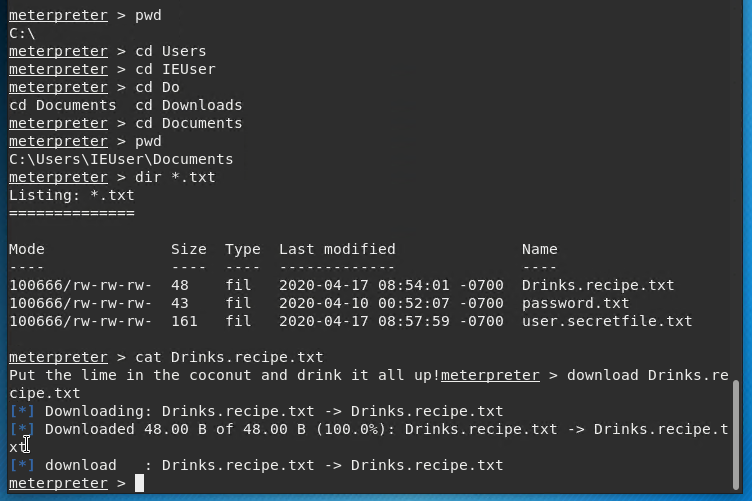
**search -f \*secretfile.txt**



**search -f \*recipe.txt**



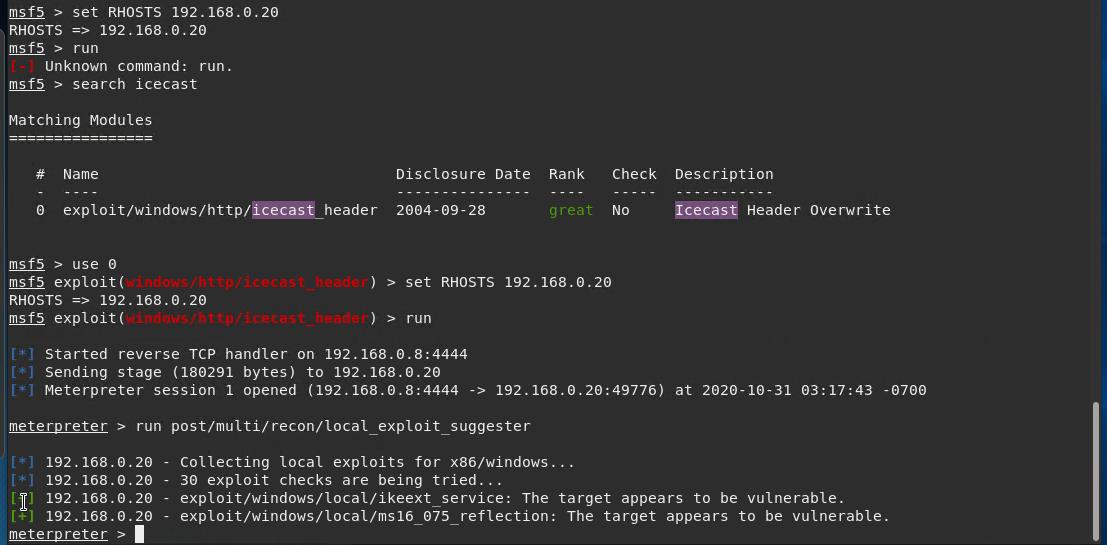
**download Drinks.recipe.txt**



**Vulnerabilities Found:**

**run post/multi/recon/local\_exploit\_suggester**

Meterpreter discovered two possible vulnerabilities:

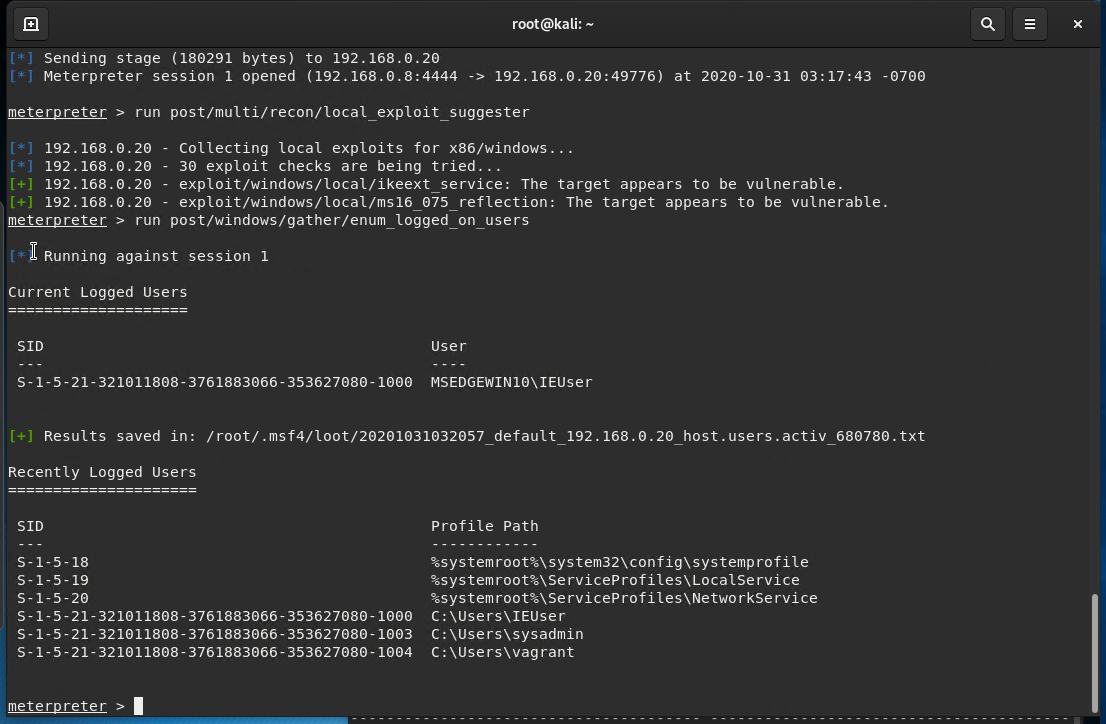


The two exploits of concern are

* ikeext\_service
* ms16-075

The ikeext services exploit 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. It requires an insecure bin path to plant the DLL payload.

The 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.



# Recommendations

1. I recommend that the Icecast Server is immediately patched to the latest release. According to icecast.org the current release is 2.4.4 (October 2020).
2. Choice of filenames
   1. I suggest either encrypting sensitive data files, and
   2. Use an internal file naming protocol that only senior management are aware of – something much less obvious than “Drinks.Recipe” and “secret”