GoodSecurity Penetration Test Report

will\_koznarek[@GoodSecurity.com](mailto:YOURNAMEHERE@GoodSecurity.com)

DATE

02/14/2021

# 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 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:

MSEDGEWIN10

Vulnerability Exploited:

Icecast Header Overwrite

Vulnerability Explanation:

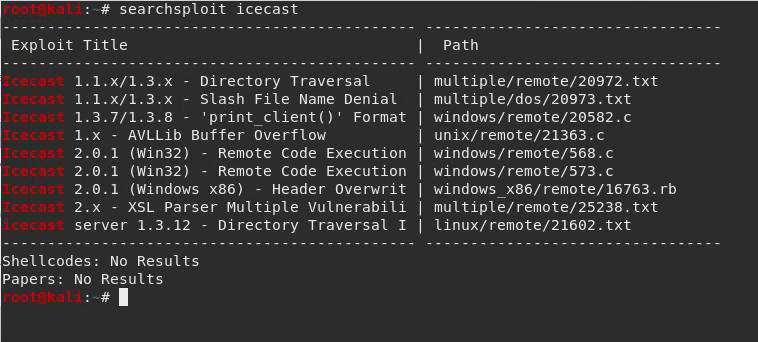
Icecast versions 2.0.1 and older with this vulnerability are succeptible to a buffer overflow that may allow arbitrary code to be executed on the remote host with the priviledges of the Icecase server process. This is exploited by a special crafted HTTP header that will overwrite the server’s stack contents, leading to the code execution.

Severity:

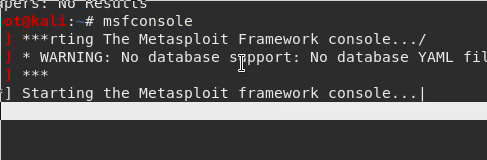
With a CVSS score of 8.1, this vulnerability is pretty severe.

Proof of Concept:

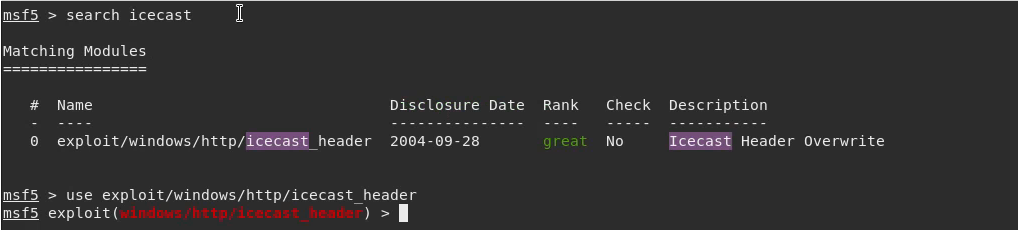
1. nmap Service & Version scan with “Aggressive” OS detection.

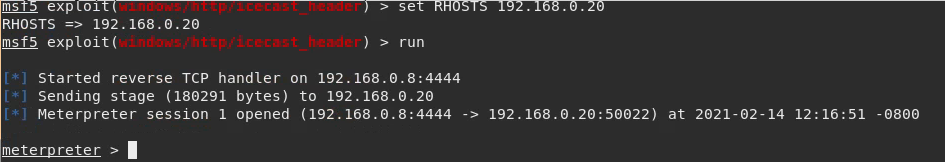
2. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:

3. Start ‘metasploit’



4. Search for the Icecast module and load it for use.

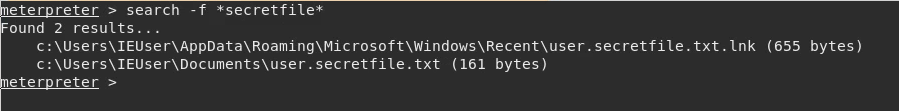
5. Set the ‘RHOST’ to the target machine. (included step 6 in this screenshot)

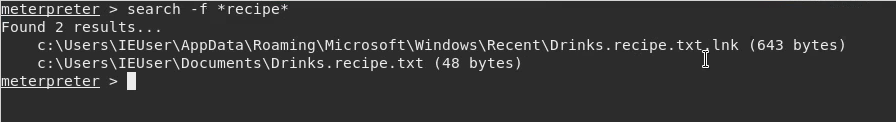


6. Run the Icecast exploit (see above screenshot)

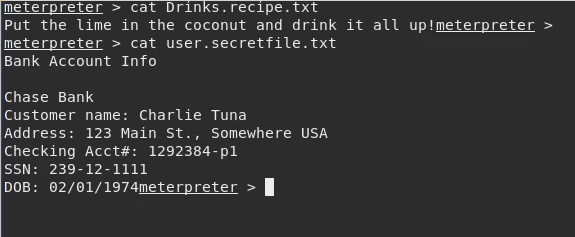
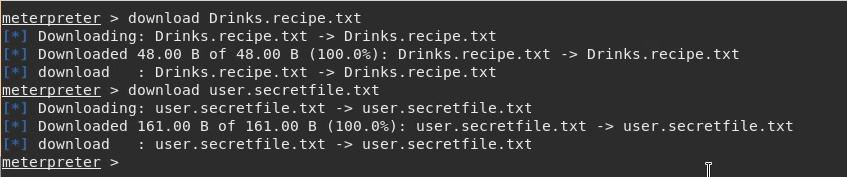
7. You should now have a Meterpreter session open.

- Search for a file containing the string ‘secretfile’ on target.

 - Search for a file containing the string ‘recipe’ on target.

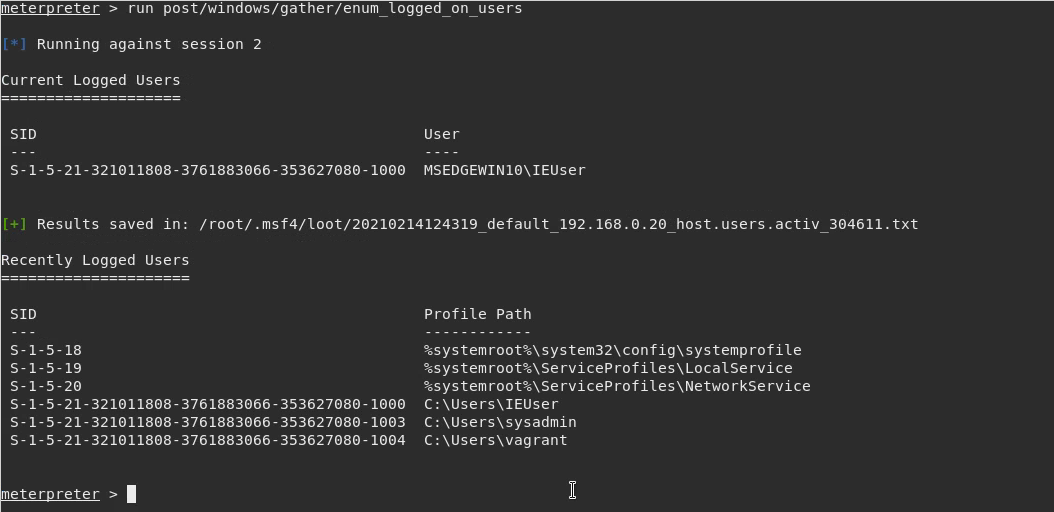


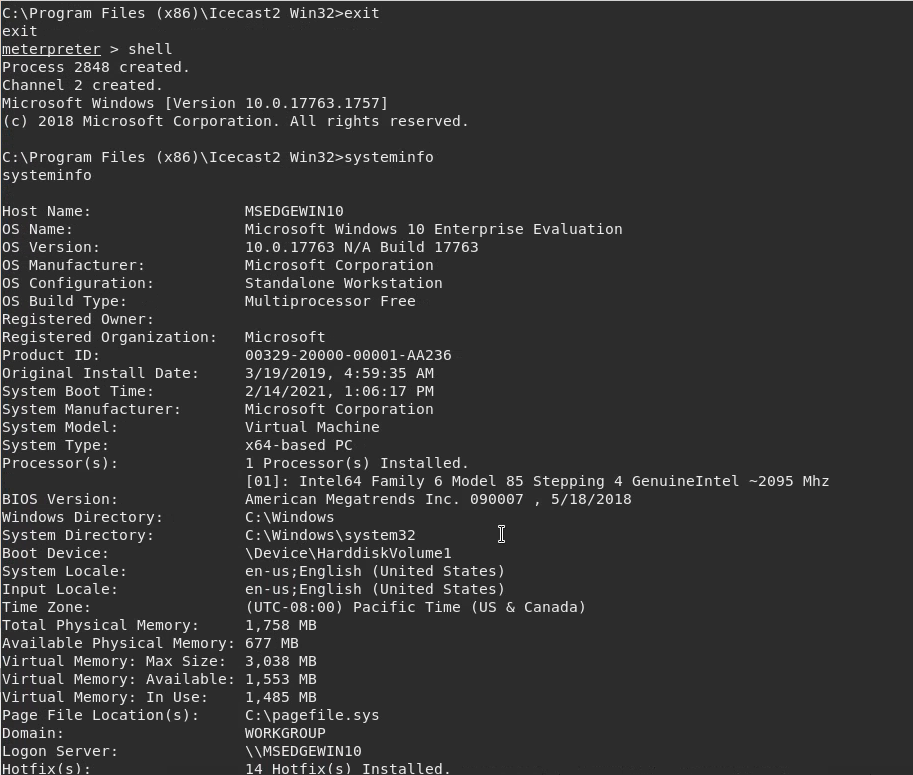
- Run the command(s) that exfiltrates the files you found above and view their contents



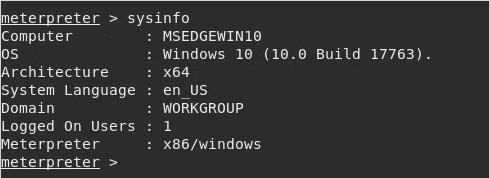
# Bonus

1. Run a Meterpreter post script that enumerates all logged on users.

2. Open a Meterpreter shell and gather system information for the target.



3. Run the command that displays the target's computer system information



# Recommendations

Update the Icecast server to 2.0.2 or higher.