GoodSecurity Penetration Test Report

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

DATE

# 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:

MSEDGEWWIN10

Vulnerability Exploited:

exploit/windows/http/icecast\_header\_info

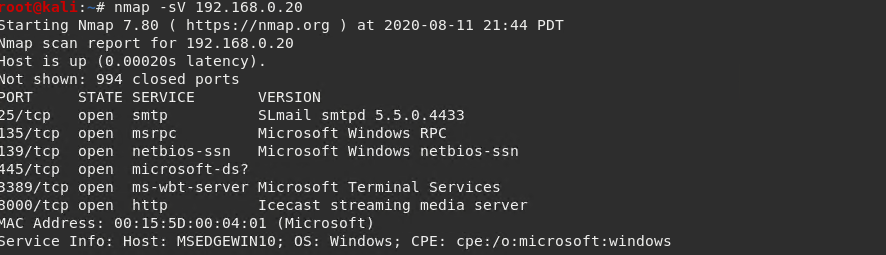
Vulnerability Explanation:

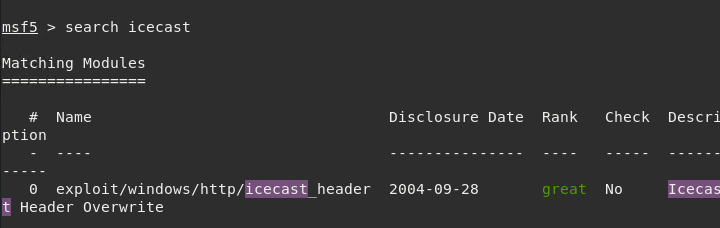
The vulnerability is exploited by a buffer overflow attack. A buffer overflow attack is when extra information overflows to adjacent memory not designated to the initial information. By sending 32 HTTP headers you can overwrite preset instructions and access the machine.

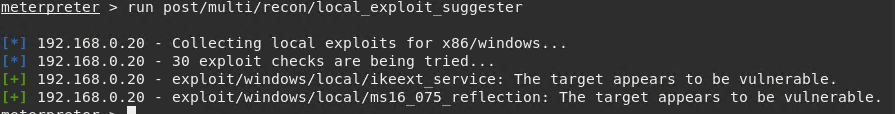
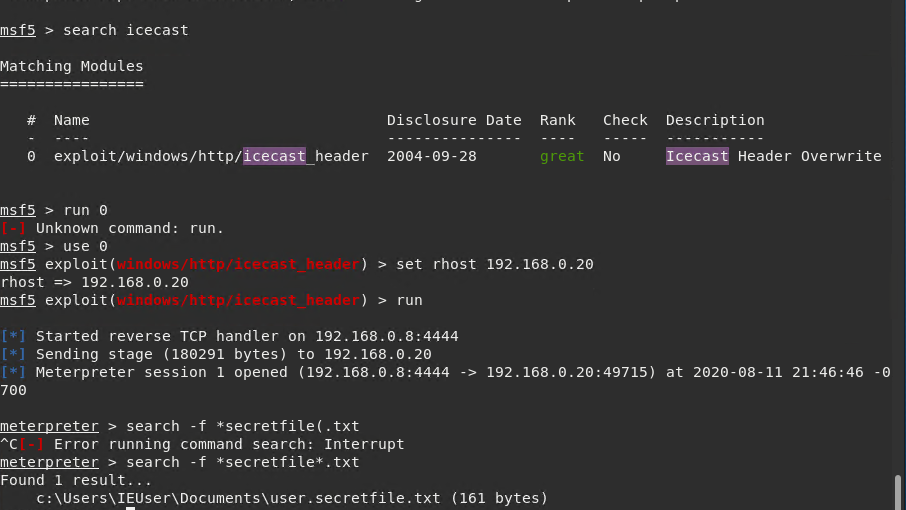
Severity:

In terms of what the attacker can access, it stands as a glaring security flaw. After exploiting icecast, the attacker was able to search through files without any issues for whatever data the attacker was seeking. The nice part of the exploit is it’s quite outdated and can easily be resolved with an update as it only exploits versions 2.0.1 and under while the current released version is 2.4.4.

Proof of Concept:







# Recommendations

The first recommendation for tightening the security would be to either update icecast or delete it altogether depending on reliance of the software. This would be the immediate resolution for the existing exploit. A further recommendation would be to have firewall rules added to whitelist/blacklist IP ranges that should be allowed to access machines. This would be a preventative measure for any potential exploitation that could come across in the future.