GoodSecurity Penetration Test Report

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

05/28/2020

# 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:

DVW10

Vulnerability Exploited:

Icecast\_header

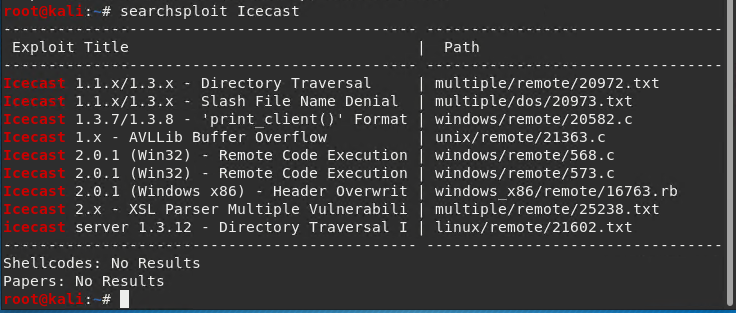
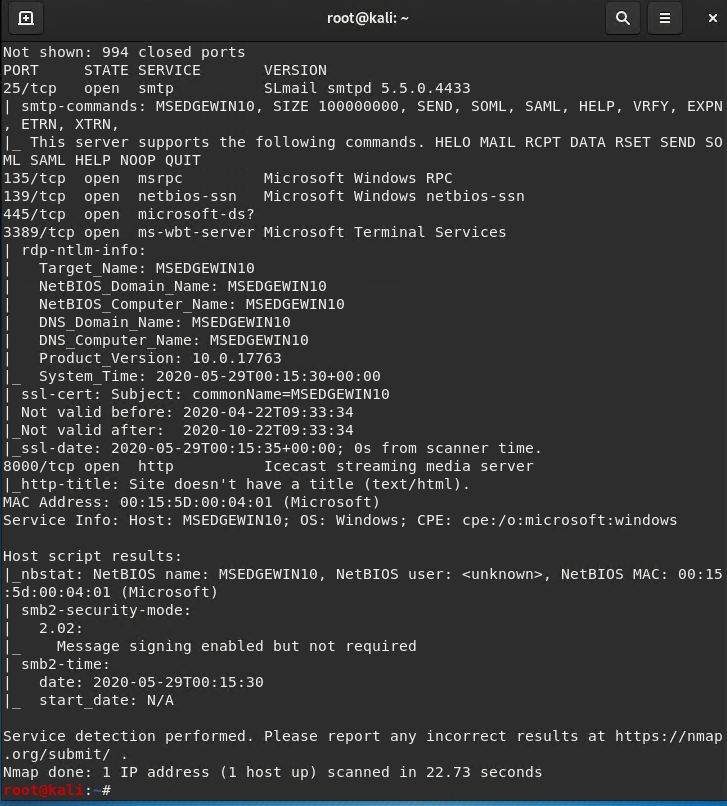
Vulnerability Explanation:

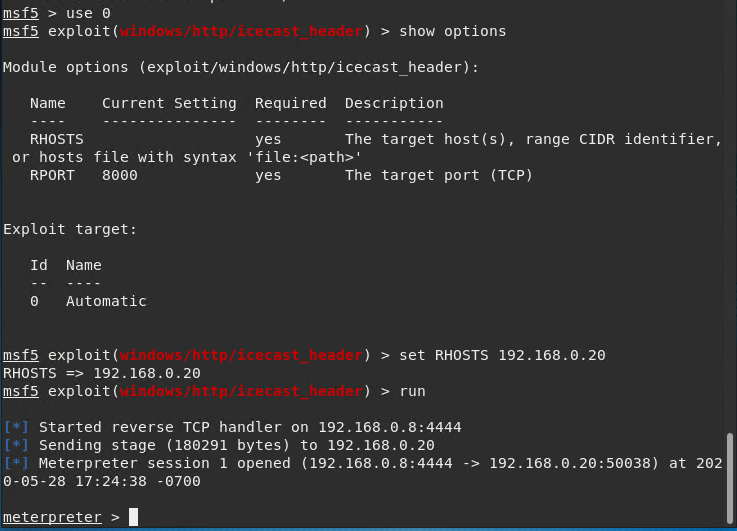
Icecast Header Overwrite is a buffer overflow in the header parsing of icecast versions 2.0.1 and earlier. Sending 32 HTTP headers will cause a write one past the end of a pointer array, which overwrites the saved instruction pointer.

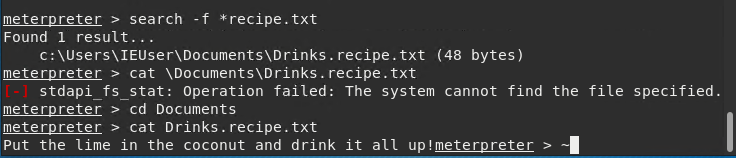
Severity:

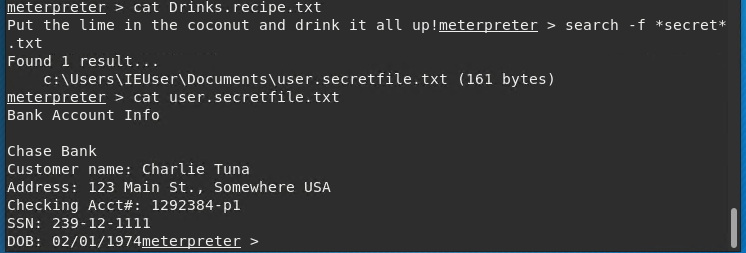
In my expert opinion this is extremely sever and needs to be taken care of prompt as anyone with a knowledge of Metasploit can take advantage of this and gain access.

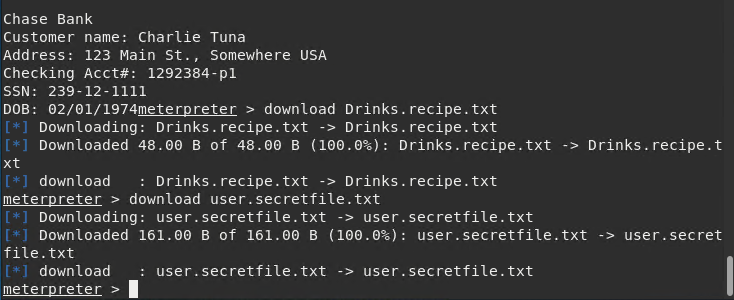
Proof of Concept:











# Recommendations

I would highly recommend regularly updating your software, Icecast immediately, as this vulnerability is only applicable to older versions. I would also recommend either closing some ports or preventing port scanning in your fire wall.