GoodSecurity Penetration Test Report

[justin.cremer@GoodSecurity.com](mailto:justin.cremer@GoodSecurity.com)

01-31-2021

# 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:

192.168.0.20

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

Exploit/windows/http/icecast\_header

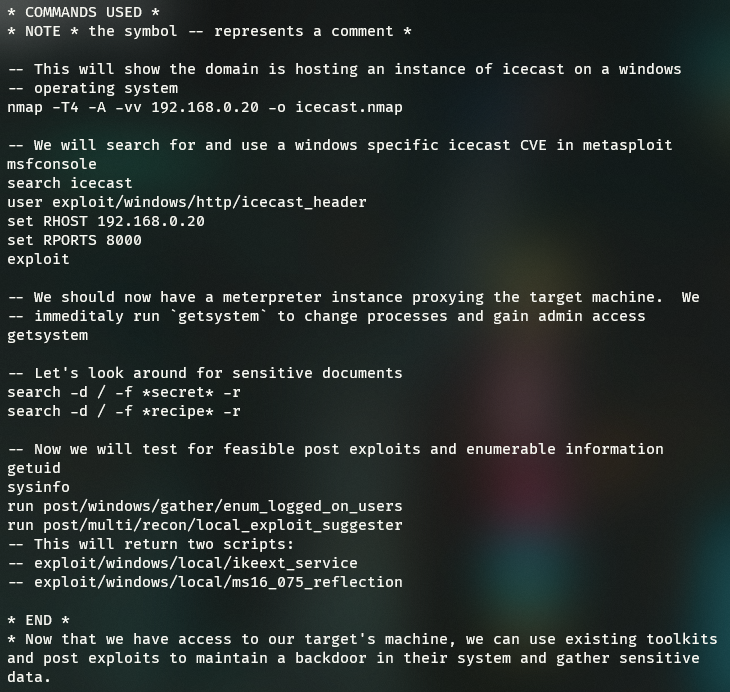
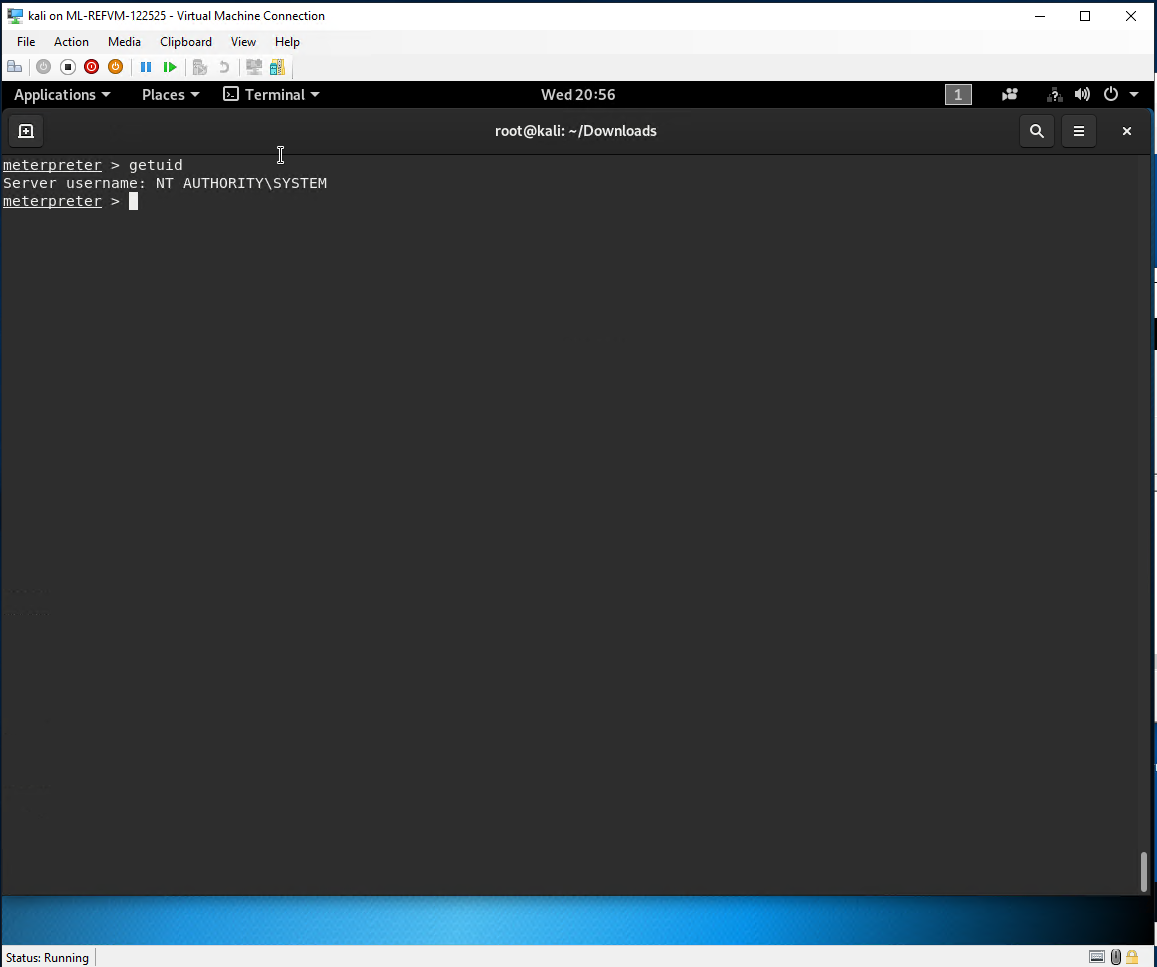
Vulnerability Explanation:

Icecast\_header (CVE-2004-1561) exploits a buffer overflow in Icecast’s header parsing protocol. In sending 32 request headers, Icecast appends an extra ‘header’ to the pointer address one byte outside of the array. On windows systems, this will overwrite the saved instruction pointer and leave Icecast thinking one of the processor threads is still occupied by one of its methods; in reality, the running process is a malicious payload. This exploit effects versions <= 2.0.1 of Icecast.

Severity:

This exploit is quite severe, as it allows malicious actors to run any manor of arbitrary code on the host’s machine.

Concept: Proof:



# Recommendations

More than anything, I strongly suggest upgrade Icecast to its latest version. Since this attack occurs over http, I also suggest e2e encryption using rotating ssl certs on employee machines. Blacklisting all traffic by default and adding employee DNSs to network firewall rules is a great way to avoid immediate targeted service attacks such as this one.