GoodSecurity Penetration Test Report

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

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

# Findings

**Machine’s IP address :** 192.168.0.20

**Hostname:** MSEDGWIN10

**The name of the script or Metasploit module used** : Metasploit:/exploit/windows/http/icecast\_header

**Vulnerability Exploited**: Icecast header overwrite

**Vulnerability Explanation:**

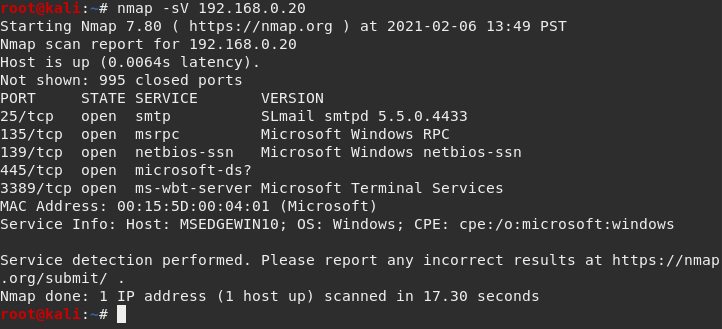
The GoodSecurity found vulnerability called Buffer overflow. Icecast 2.0.1 and earlier allows remote attackers to execute arbitrary code via an HTTP request with a large number of headers.

**Severity:**

This is a very serious vulnerability, as it has been shown to allow exfiltration of sensitive data.

**Proof of Concept:**

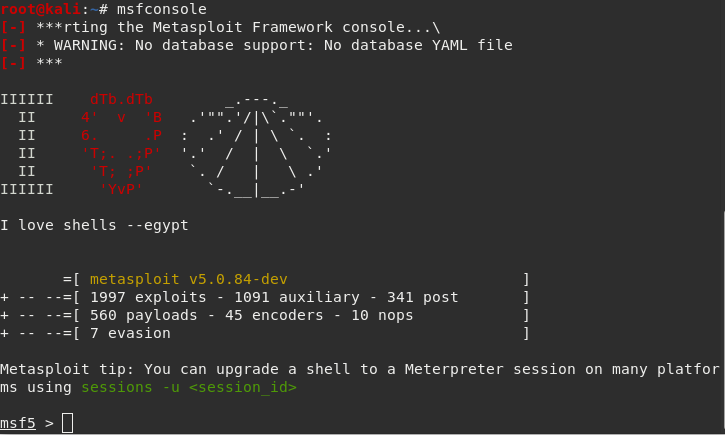
* **Preliminary nmap**

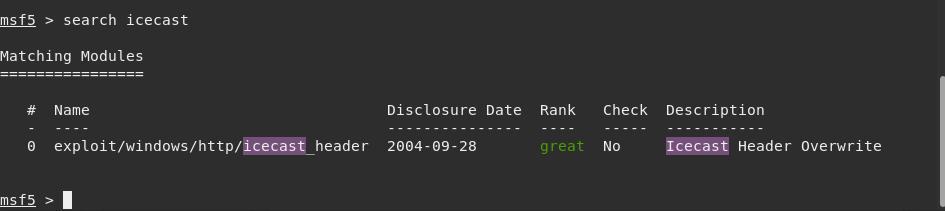
****

* **Service and version scan using Nmap to determine which services are up and running after icecast server**

# 

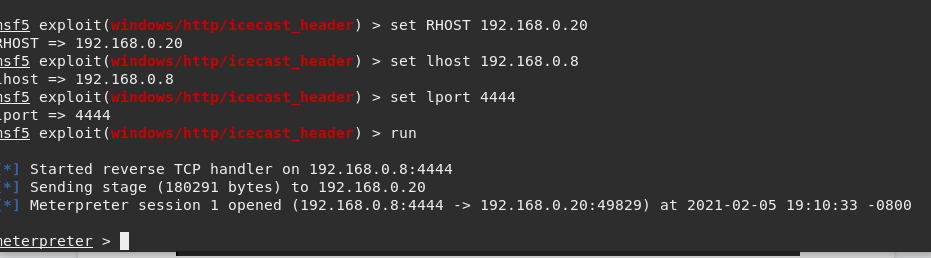
* **Running msfconsole**

****

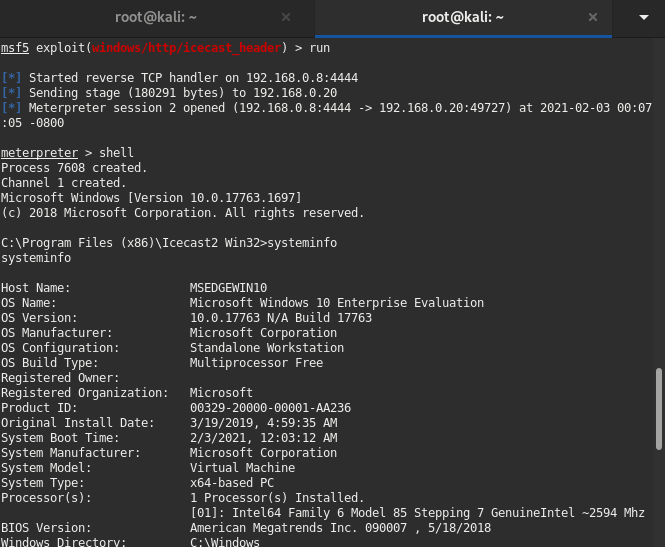
* **SearchSploit commands to show available Icecast exploits**
* **Load icecast module using the command**

use exploit/windows/http/icecast\_header

* **Setting rhost/lhost and running Metasploit**

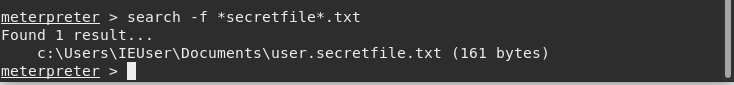
****

* **Running icecast exploit and shell created (systeminfo)**

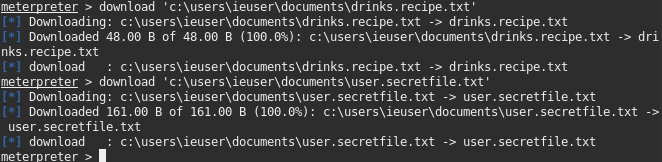
****

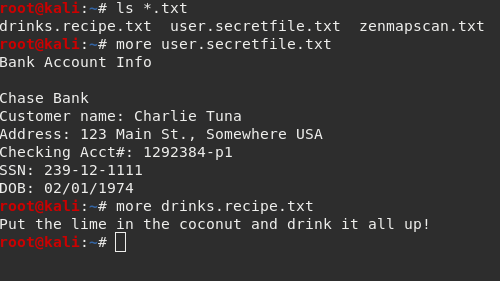
* **suspicious file search**

****

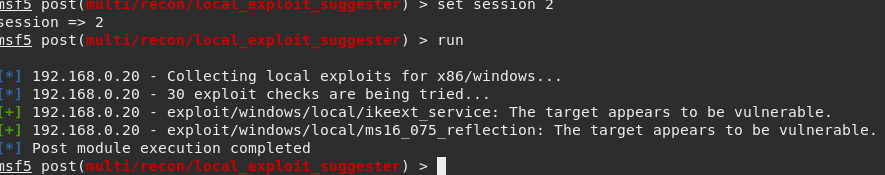
****

* **Extraction of those files**

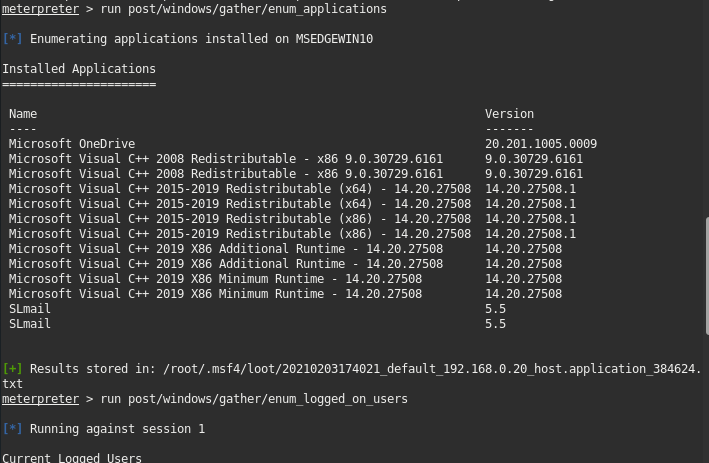
****

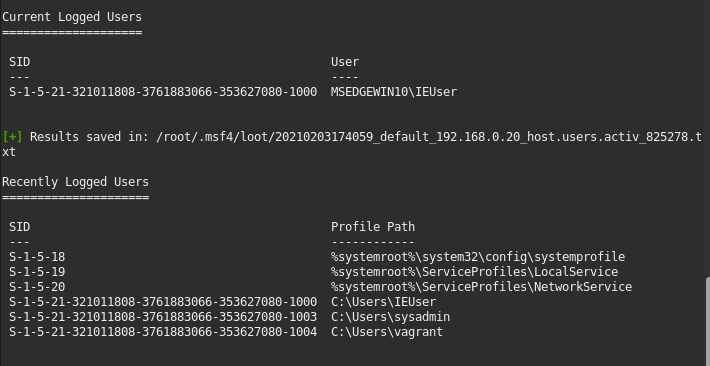
****

* **Meterpreter's local exploit suggester to find possible exploits**

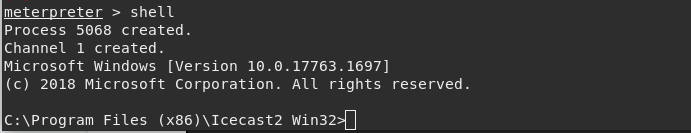
****

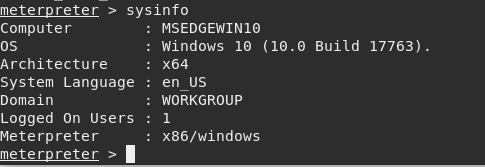
* **Meterpreter post script that enumerates all logged on users and installed apps**

****

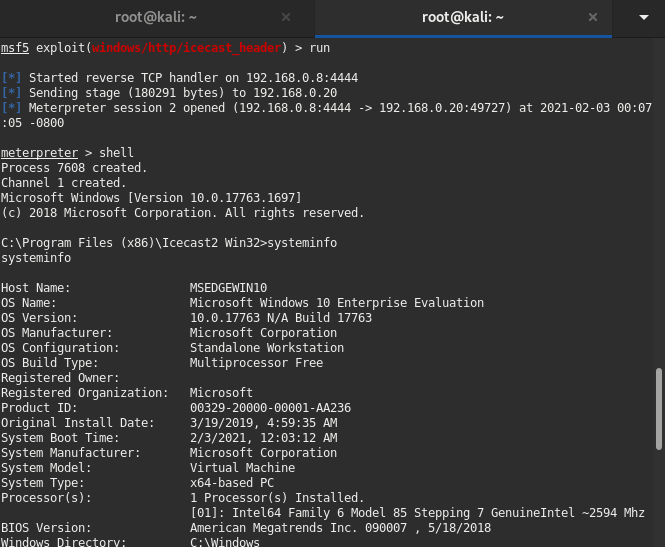
****

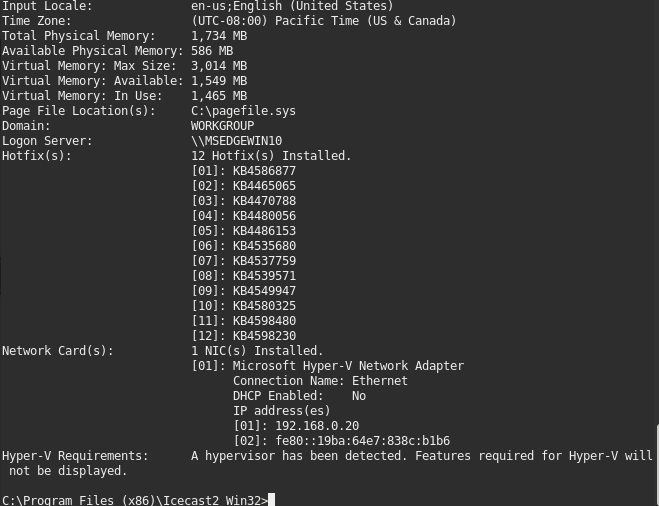
* **Open a Meterpreter shell and gather system information for the target**

****

****

* **target's computer system information:**





# Recommendations

Based on the findings of Good Security the following recommendations were made:

* Update all the installed applications in the CEO’s desktop.
* Especially update Icecast to a newer version as vulnerabilities were found in the older versions (Icecast 2.0.1 and older)
* An effective vulnerability assessment and remediation program must be able to prevent the exploitation of vulnerabilities by detecting and remediating vulnerabilities in covered devices in a timely fashion. Proactively managing vulnerabilities on covered devices will reduce or eliminate the potential for exploitation and save on the resources otherwise needed to respond to incidents after exploitation has occurred.
* Enable all relevant firewalls to pass all IP traffic
* "Minimum necessary" means blocking the least amount of traffic possible to avoid the problem. For example, blocking a specific TCP port rather than all TCP traffic, or blocking a specific IP protocol rather than all IP traffic.
* Establish information resources that will be used to identify relevant vulnerabilities. These information resources should be monitored to keep up-to-date awareness on emerging threats and latest software updates.
* Prioritize the order in which the organization addresses remediating vulnerabilities.
* Non-authenticated vulnerability scans should be performed on covered devices at least once a week.
* Measure the effectiveness of the patch and vulnerability management program and apply corrective actions as necessary.