GoodSecurity Penetration Test Report

JeffPeterson@GoodSecurity.com

01/16/21

# 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.

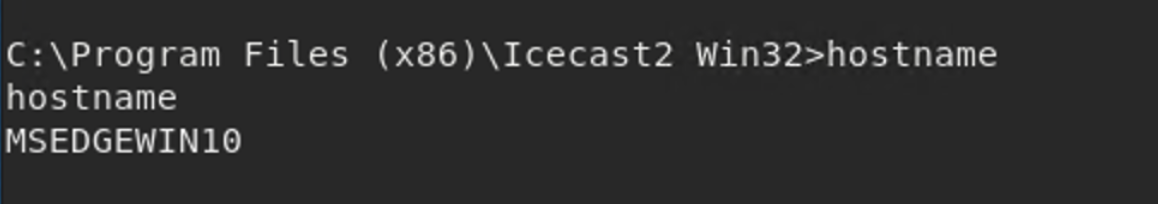
# Findings

**Machine IP:**

192.168.0.20

**Hostname:**

MSEDGEWIN10



**Vulnerability Exploited:**

icecast\_header

**Vulnerability Explanation:**

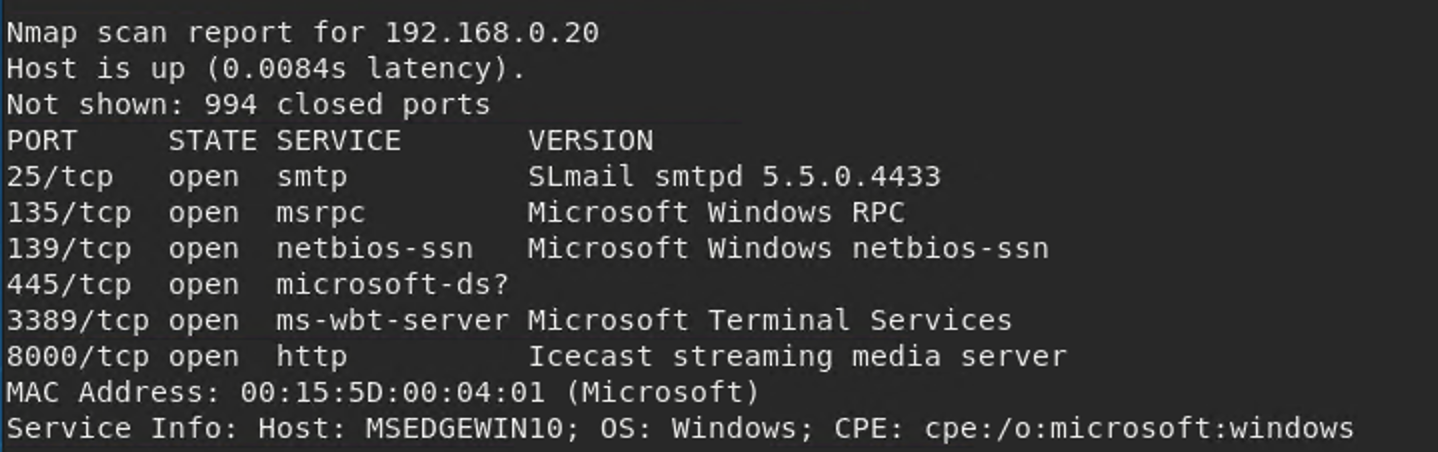
This vulnerability is due to an issue in the header parsing of Icecast versions 2.0.1 and earlier. Icecast\_header is a buffer overflow exploit that sends 32 HTTP headers which is one past the end of the buffer and allows remote attackers to execute arbitrary code via an HTTP request.

**Severity:**

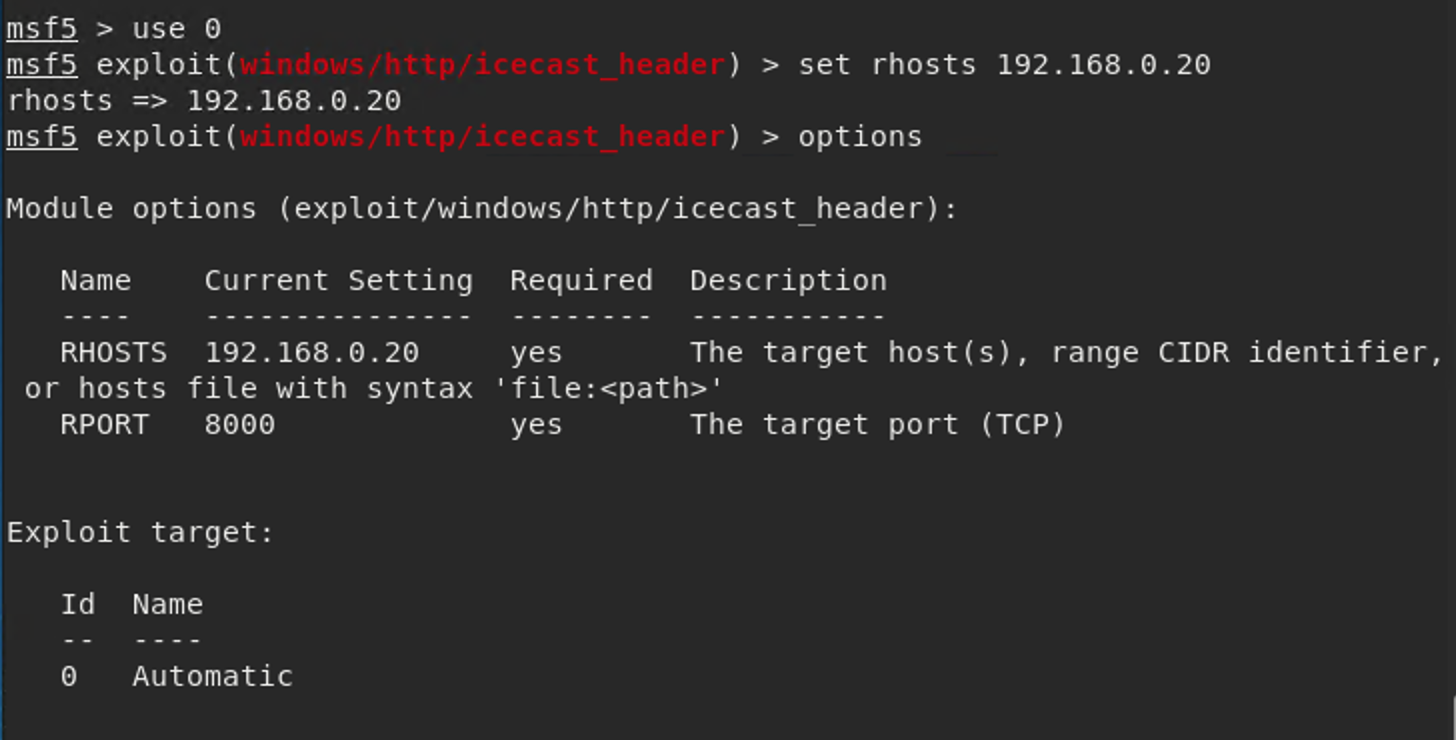
The severity of this is pretty high. Once the exploit is executed, the attacker has access to the whole system and can search through for sensitive documents and download them. The attacker can also upload and execute more malicious code.

**Proof of Concept:**

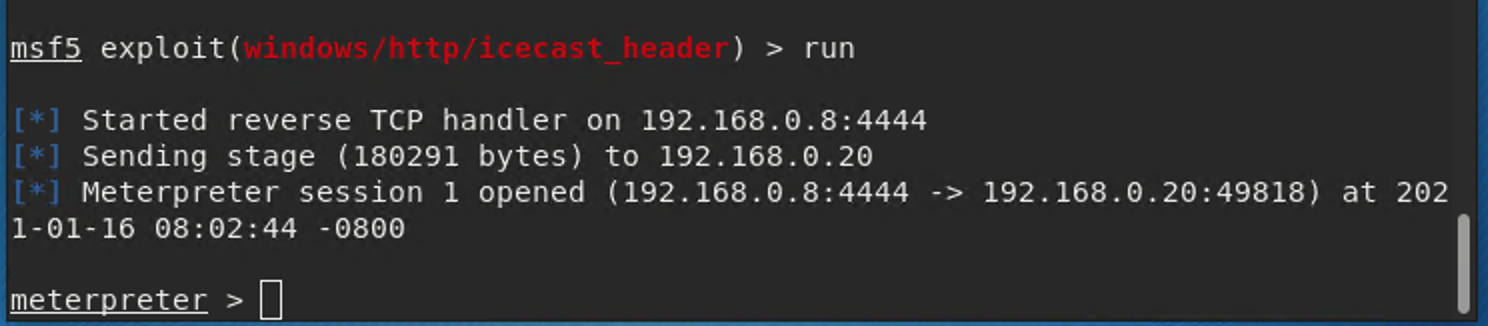
The first step taken was to scan the IP address of the machine to discover which services are running and which ports might be open.



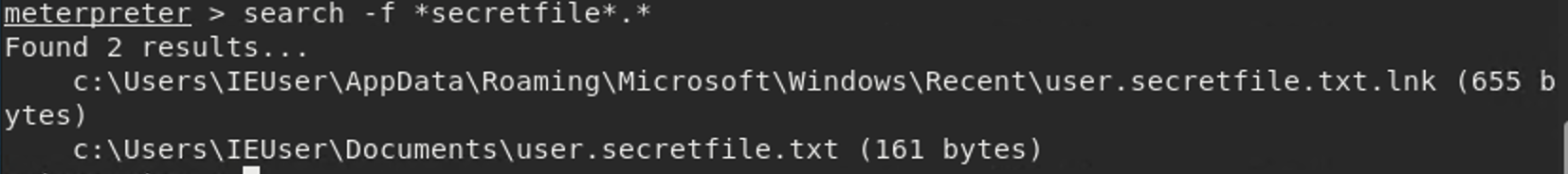
After noticing Icecast was running on port 8000 over HTTP, I attempted to execute the icecast\_header exploit to see if I could get a connection.

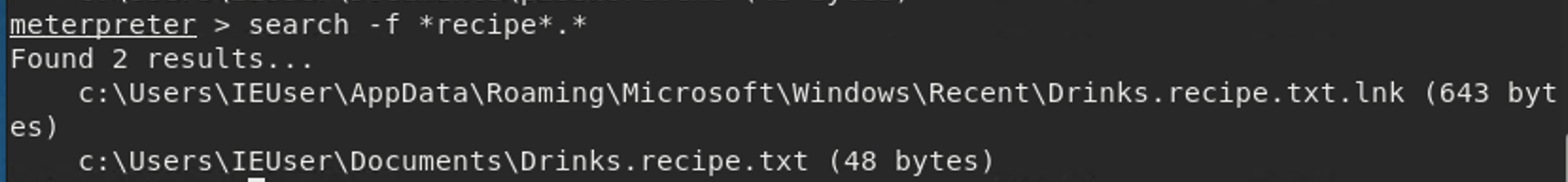


The exploit was run successfully and I was able to get a meterpreter session to the victim machine.

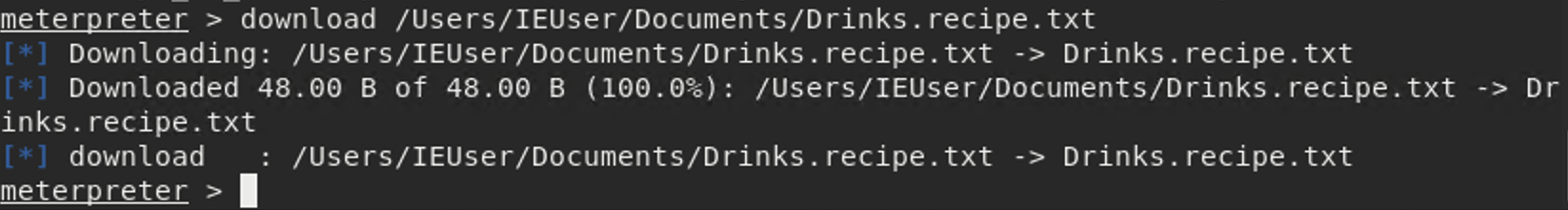


From this session, I was able to search for the requested files: sercretfile and recipe. I wasn’t sure which file type to search for but through the meterpreter session, I was able to search the entire system and the results are below.

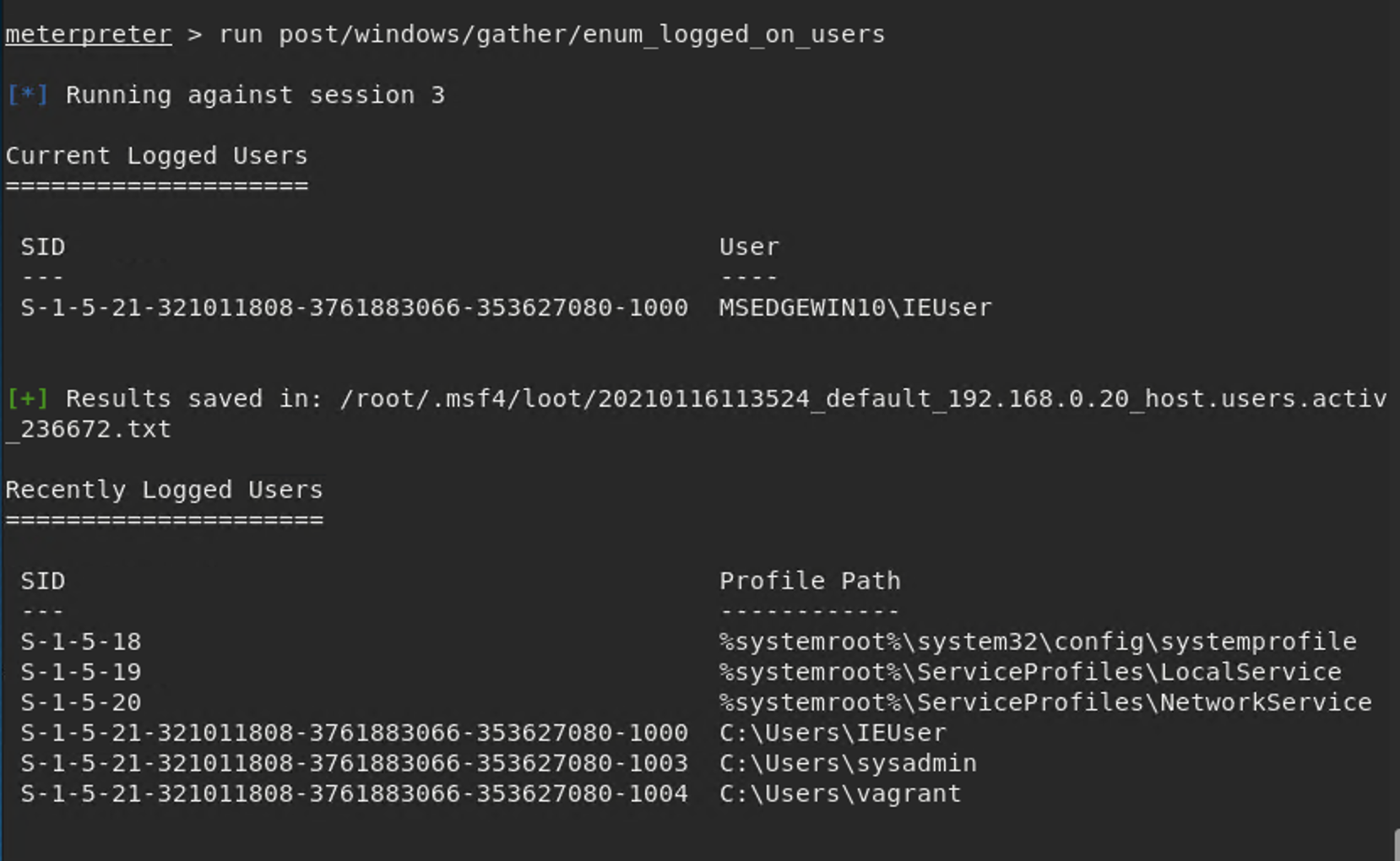




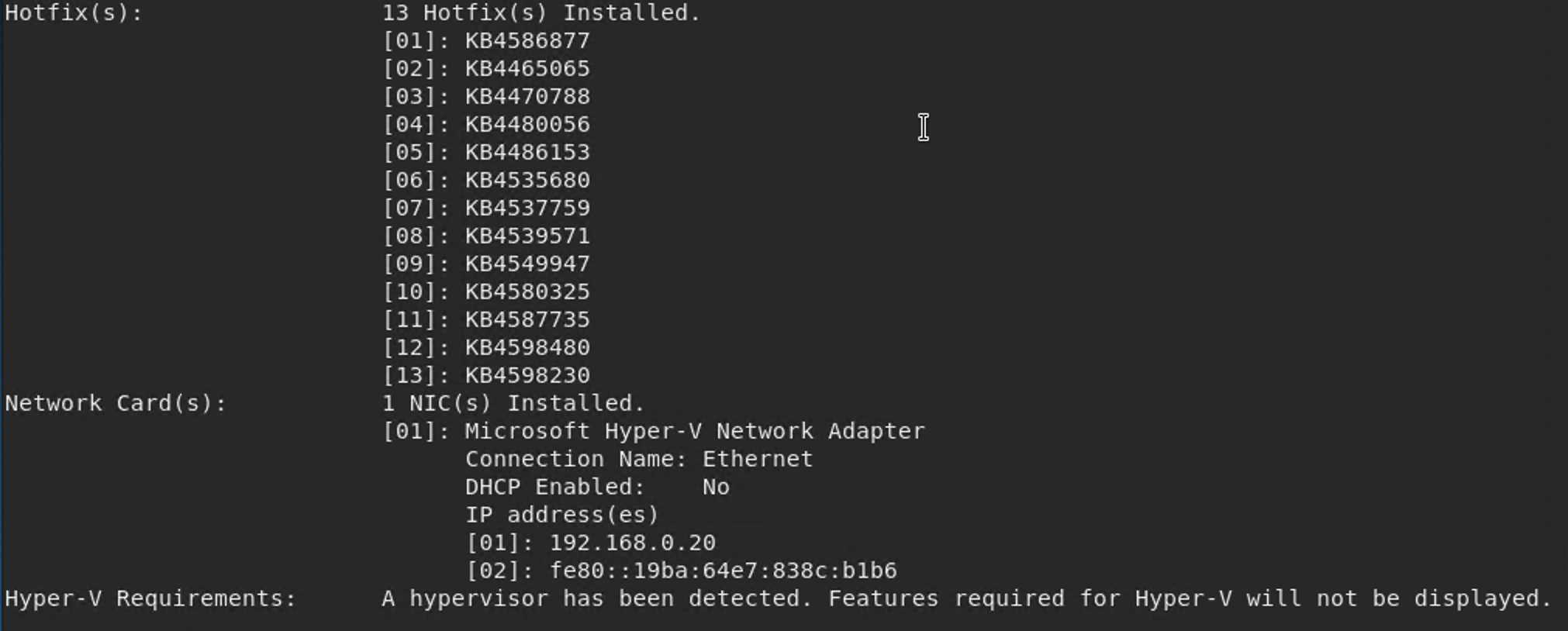
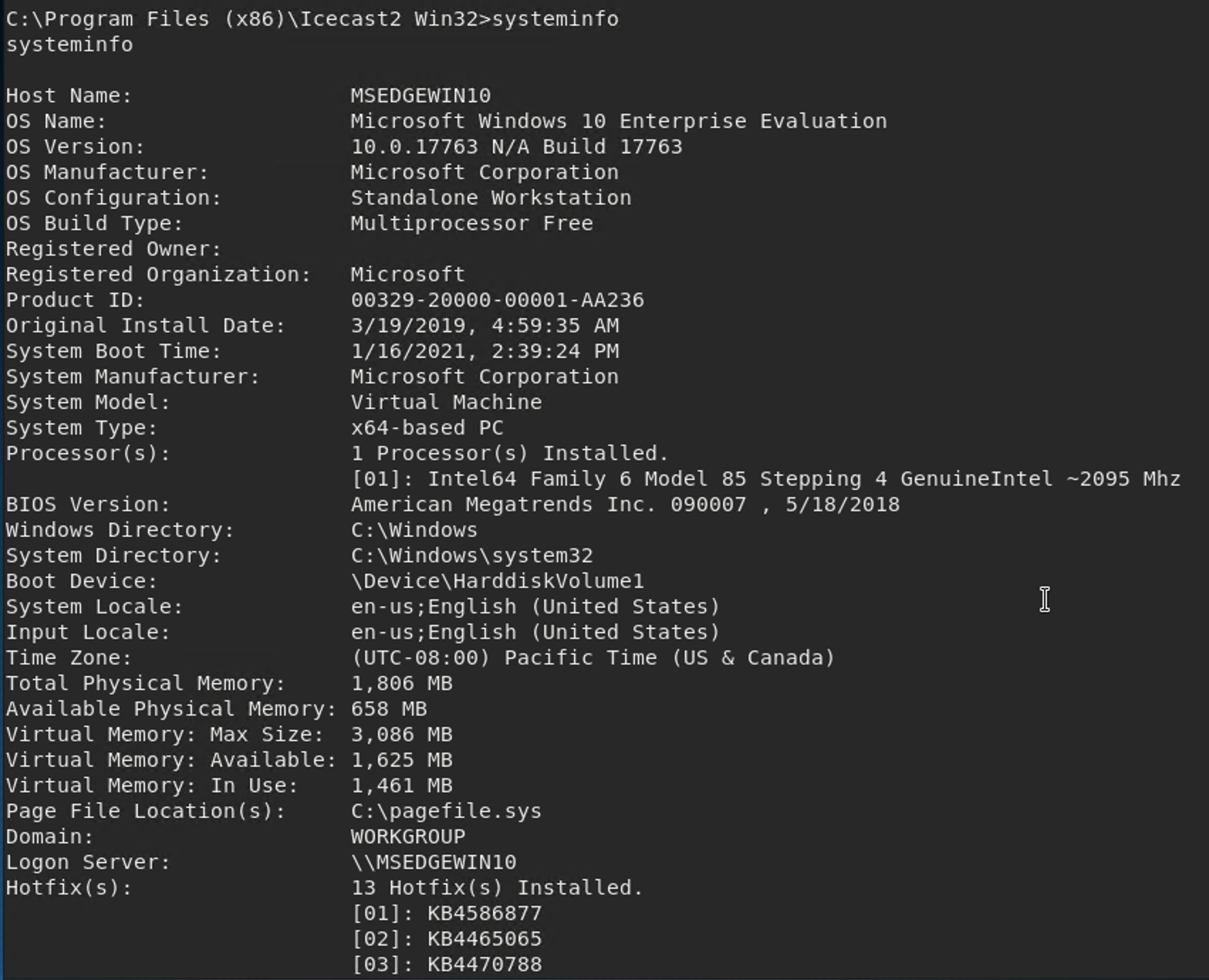
Once I found the location of the files, I was able to download them locally. I only downloaded the recipe file for demonstration purposes.



From the meterpreter session, I was able to run another exploit to find which users were logged in to the system.



Next, I opened a meterpreter shell to grab some system information on the target.



# Recommendations

The first thing I would recommend is to make sure your system is up to date and update the Icecast application. The Icecast vulnerability affects versions 2.0.1 and earlier and they are currently on version 2.4.1. If there are vulnerabilities in an unpatched system, a strong password still might not save you. Suggest using a Web Application Firewall or a local IPS to help protect against buffer overflow attacks. For sensitive files, instead of saving them locally, you could store them in a secure server with access controls and require multi-factor authentication to access that server. Also suggest setting up a cybersecurity awareness/best practices program to educate the company employees to gain a better understanding of the types of threats that exist and how to prevent them.