GoodSecurity Penetration Test Report

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

Friday April 30,2021

# 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 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:

MSEDGEWIN10

Vulnerability Exploited:

Icecast Header Overwrite (buffer overflow)

Vulnerability Explanation:

The Icecast application an attacker to send 32 HTTP headers through buffer overflow exploit. It allows control of the victims system by overwriting the memory using Icecast flaw, that writes past the end of a pointer array.

Severity:

Severity: Critical level 10.0

Proof of Concept:

Locating Icecast IP address:

Text

Description automatically generated

Ping for response from Icecast:

Text

Description automatically generated

Using nmap to scan for open and vulnerable ports of the IP address:

Text

Description automatically generated

Icecast exploits: Text

Description automatically generated

Establishing Metasploit session:

Text

Description automatically generated

Set RHOST:

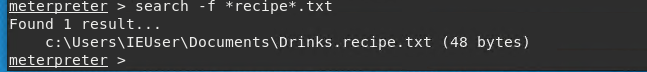


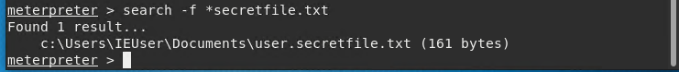
Run exploit:

Text

Description automatically generated

Exposing secret filte.txt and recipe.txt:

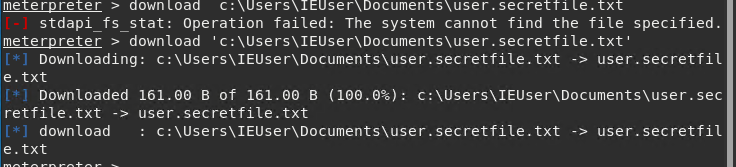




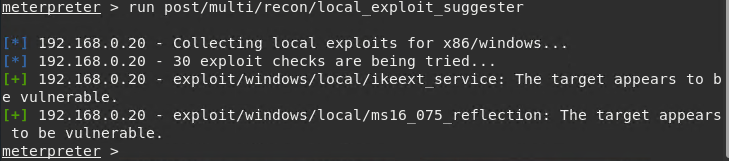
Files downloaded:

Text

Description automatically generated



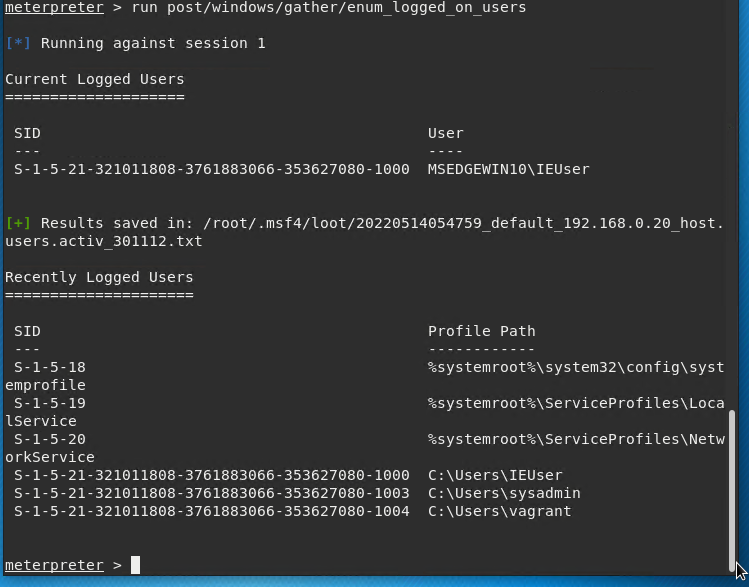
Additional Vulnerabilties:



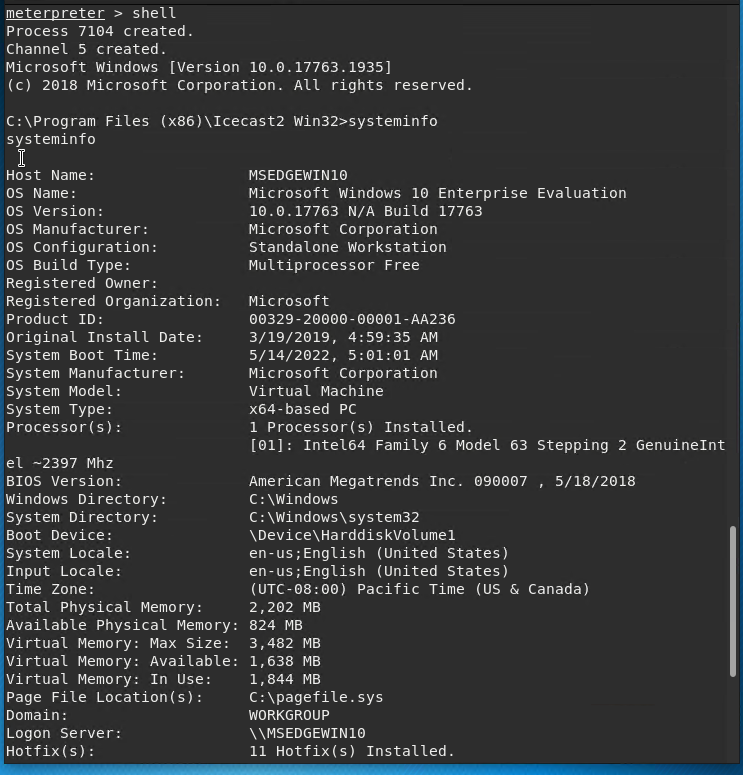
The following additional vulnerabilities were found:

1. Exploit/windows/local/ikeext\_service
2. Exploit/windows/local/ms16\_075\_reflection

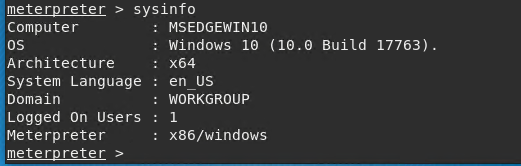
Logged on users:



System Information from shell:



Sysinfo from meterpreter:



# Recommendations

1. I would start with patching to the latest version of Icecast immediately.
2. It is important to perform regular updates to your system and to have good checks and balances to ensure all systems are up to date with the updated software. For all software that is being run it is best practice to set up a schedule for monthly patches to keep your system hardened against possible attacks like this one in the future.
3. The IKEEXT and the ms16\_075 exploits are more difficult to expose than Icecast is. However, it is still a vulnerability and can be prevented with the regular patches.