GoodSecurity Penetration Test Report

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

04/28/2022

# 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:

198.162.0.20

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

Exploit(windows/http/icecast\_header) = Icecast Header Overwrite

Vulnerability Explanation:

This vulnerability is a buffer overflow attack. Specifically, it overwrites the HTTP header buffer and inserts code that allows an attacker to gain access to the server. Because the buffer is only designed to handle a certain size of input, the extra input gets written into the protocol memory and then overwrites existing code allowing the attacker to insert commands that gives them access.

Severity:

This is a severe vulnerability since the attacker can initiate the attack and gain access to the target computer without any interaction from the user. The attack does not require the user to click on a link or open a file. The attacker can gain complete and immediate access to the computer and can insert and extract information at will. This also gives them the ability to laterally move through the system and since this is the CEO’s computer, the level of access is high.

Proof of Concept:

1. Since we had full network access for this engagement, I was able to map the network very easily. An outside attacker would have to find a way into the network prior to being able to completely map the network in this way. Using NMAP I performed a service and version search to determine any open ports and what services they were runningText

   Description automatically generated

Text

Description automatically generated

1. I identified the CEO server as having IP address 192.168.0.20 and saw they were running an icecast media server on port 8000. I recognized this as a possible vulnerability and started Metasploit to search for a possible exploit.

Graphical user interface, text

Description automatically generated

1. Using this vuln, I moved into the module and set the option parameters for my attack. This included setting the RHOST to the target IP (192.168.0.20) and the RPORT to the Icecast media port (8000).

Text

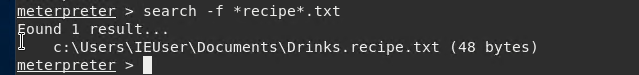
Description automatically generated

1. After setting options, I ran the exploit and was able to launch a meterpreter shell. I ran the sysinfo command to confirm I has gained access to the computer.

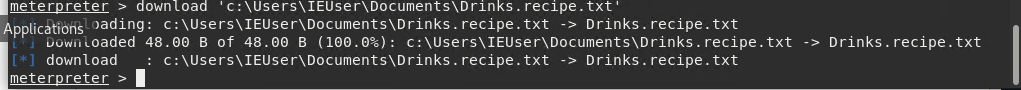
Text

Description automatically generated

1. I performed a search action from the meterpreter shell to find the target file.



1. As requested by the engagement scope, I extracted the ‘Drinks.recipe.txt’ file from the CEO’s computer to my attacker computer.



Text

Description automatically generated

# Recommendations

During the engagement, I noticed several open ports with out-of-date services that have known vulnerabilities. I exploited the Icecast vulnerability since it required no interaction from the user to gain access to the target computer. My recommendation would be to close any unnecessary ports as well as update any services that are running to the latest fully patched version. In the case of Icecast.

In general, a full audit of any services and programs running should be updated to the latest patched version.