GoodSecurity Penetration Test Report

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

12/14/2020

# 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:**

Icecast Header Overwrite

SMTP User Enumeration

SMTP Open Relay

**Vulnerability Explanation:**

Icecast header overwrite

The Icecast header overwrite vulnerability allows a threat actor to send an HTTP request with more than 32 header lines which will generate a buffer overflow and allow the remote party to execute commands on the remote system that has Icecast installed. This vulnerability affects versions 2.0.1 and lower of Icecast server.

SMTP User Enumeration

A module that inspects the VRFY, EXPN and RCPT TO commands to generate a list of all OS and server level user accounts, SMTP server type and version via port 25.

SMTP Open Relay

A module that checks if a system or server can operate as an open SMTP relay.

**Severity:**

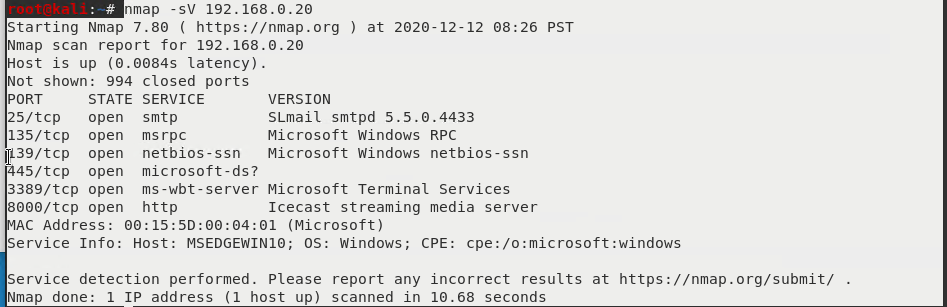
The Icecast header overwrite vulnerability is extremely severe since a threat actor can gain access to the remote system and execute commands, load malicious payload on the remote system and exfiltrate data from the remote system.

SMTP user enumeration is a medium severity risk. It allows a threat actor to probe a remote system and obtain user names for accounts on the remote system via port 25. It does pose a privacy issue if the users for a targeted mail server are to remain private. Since the server type and version are provided, an attacker may be able to exploit the SMTP server if exploits are available for the version that runs on the server or system. It can also allow an attacker to wage brute force attacks easier since the attacker will already have a list of all users on the server or system.

SMTP open relay is a high severity risk. A threat actor can use an open relay for email spoofing and wage spam campaigns from the remote system that acts as an SMTP open relay.

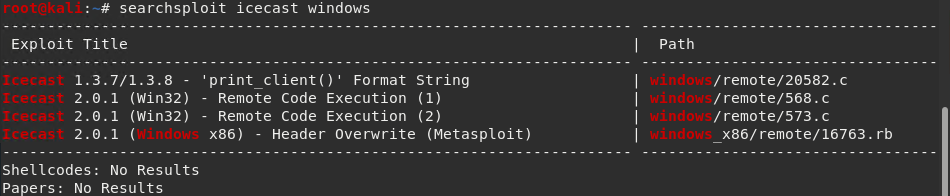
**Proof of Concept:**

Ran an nmap command on the target system to see which ports are open, the services that use the open ports and the operating system of the remote system.

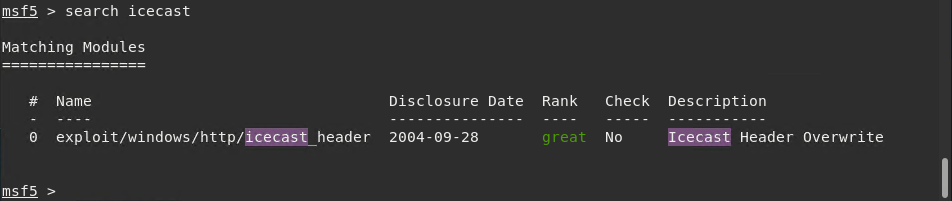


**Icecast Header Overwrite**

Used Searchslpoit to see all exploits available to target Icecast on a Windows system.



Accessed Metasploit and searched for the exploit to target Icecast on the Windows system.



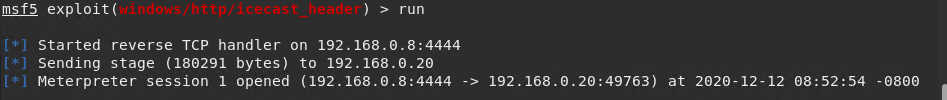
Loaded the exploit from Metasploit.



Set the RHOSTS variable to the IP for the remote system.



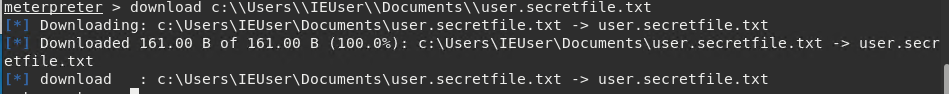
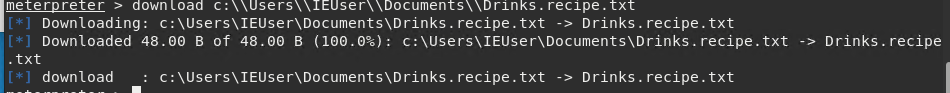
Ran the exploit and established a backdoor into the remote system.

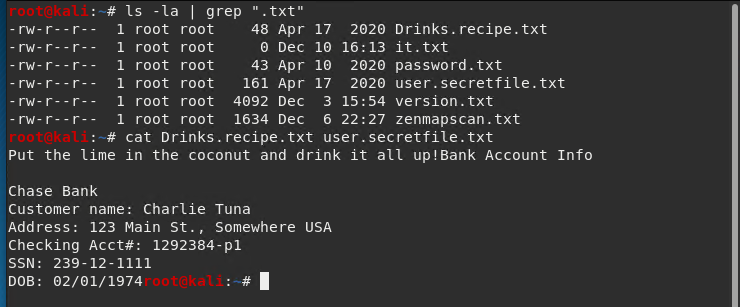


Ran search commands to discover the locations of the secret text files.



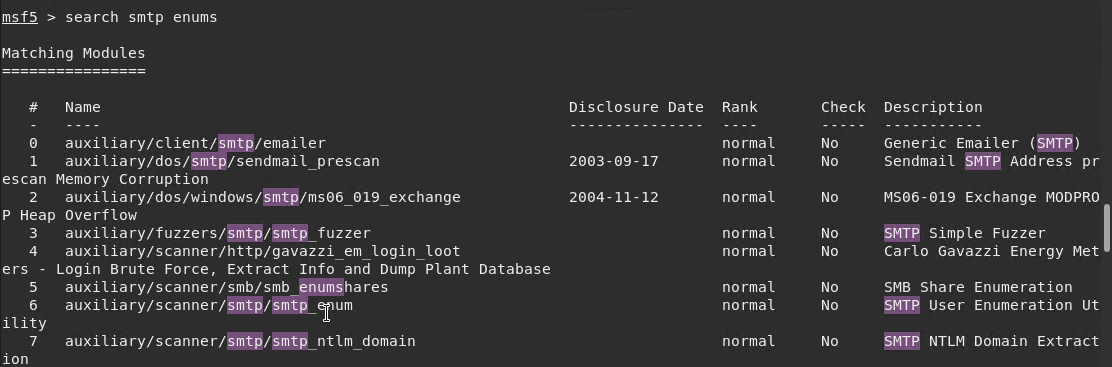
Exfiltrated both secrets files from the remote system to my local system.



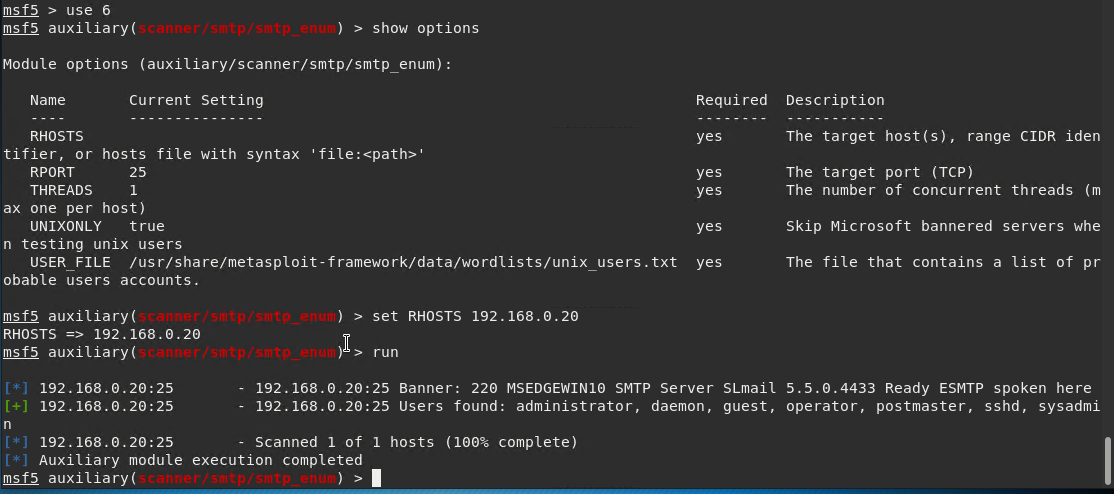


**SMTP User Enumeration**

Searched Metasploit for SMTP enumeration vulnerabilities and utilities.

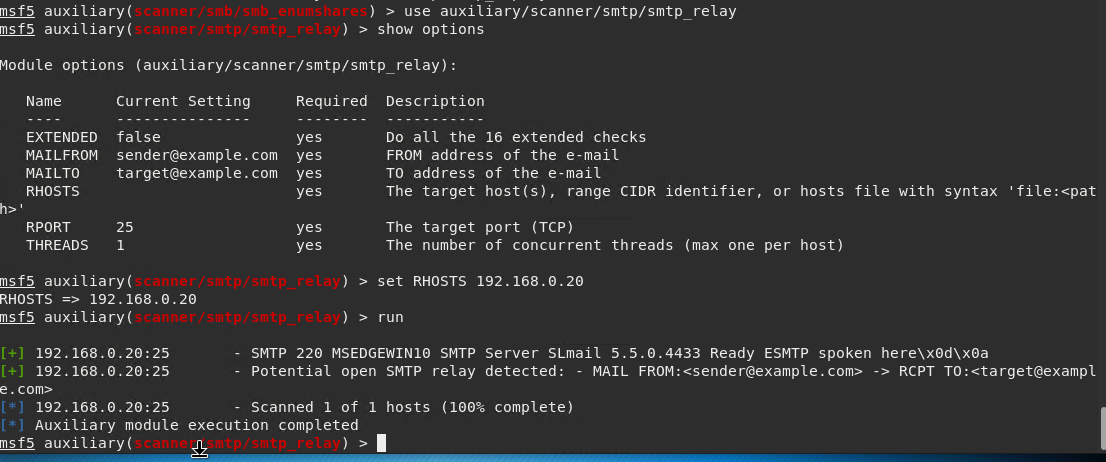


Loaded SMTP enumeration utility, set RHOSTS variable to the remote computer and ran the utility which revealed the user accounts on the system.



**SMTP Open Relay**

Loaded the SMTP open relay utility from Metasploit, set RHOSTS variable to the remote computer and ran the utility which determined that the remote system can operate as an open relay.



# Recommendations

I would recommend that Goodcorp update Icecast to the latest version available to avoid the header overwrite exploit.

Disable the VRFY, EXPN and RCPT TO commands so that the usernames for user accounts, server type and version number are not revealed.

Set the SMTP mail server to only allow mail to be sent from authorized users that supply usernames and passwords when sending mail and/or the server is allowed to send mail from authorized domains and IPs.