GoodSecurity Penetration Test Report

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

11/10/21

# 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 Overwrite

Vulnerability Explanation:

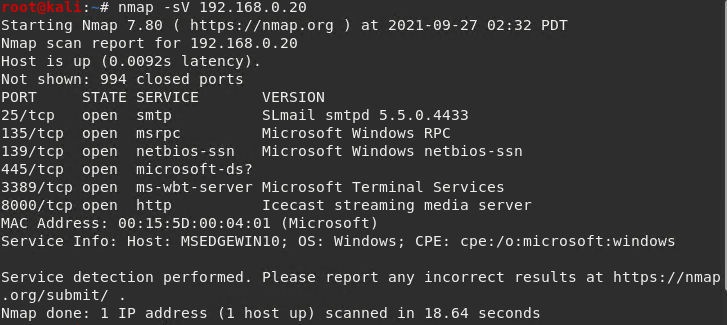
Version 2.0.1 of the Icecast media streaming server has a buffer overflow exploit.

Because Icecast will only take a maximum of 32 headers in a HTTP request, so a request containing more than 31 headers causes the headers to be overwritten with a pointer to the 32nd header. With this exploit it is possible to execute remote code using the normal HTTP request with an extra 31 headers followed by a shell code.

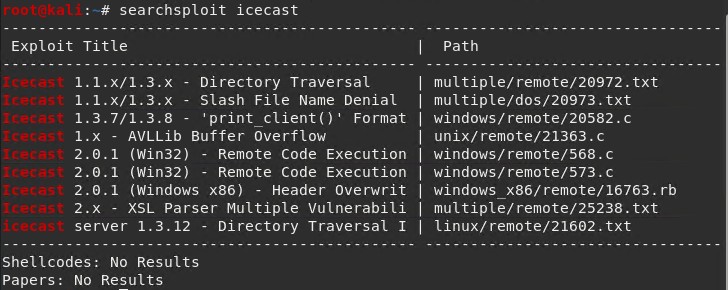
Severity:

According to Nist (<https://nvd.nist.gov/vuln/detail/CVE-2018-18820>) this exploit has a Base Severity score of 8.1, meaning this is a severe exploit with terrible consequences.

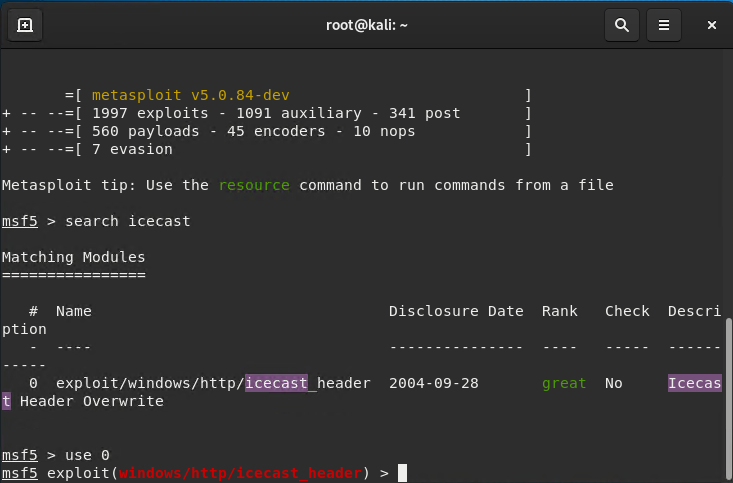
Proof of Concept:

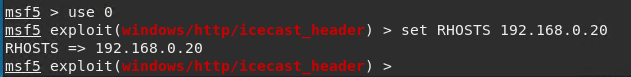
After Performing an NMAP scan of the CEO’s workstation IP from the attacking Kali machine we can see that the Icecast media streaming server is open.  


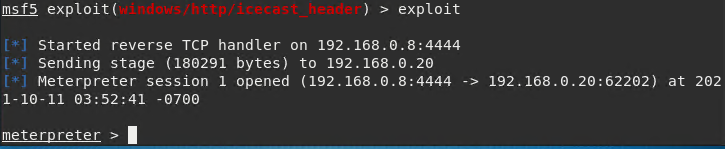
Using searchsploit we can see the following exploits available for Icecast;



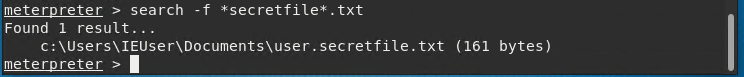
After launching Metasploit using msfconsole we can then search for and launch the relevant exploit;

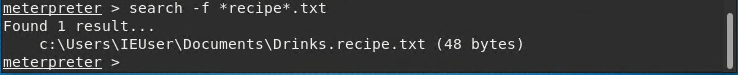




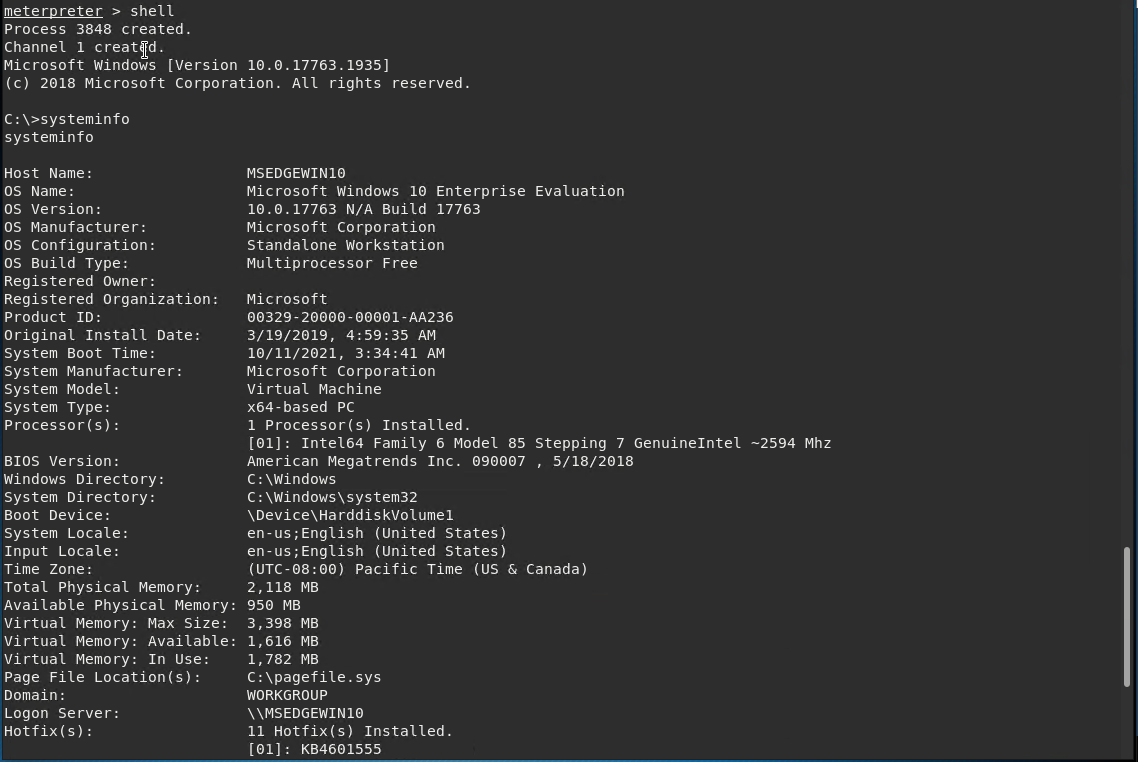


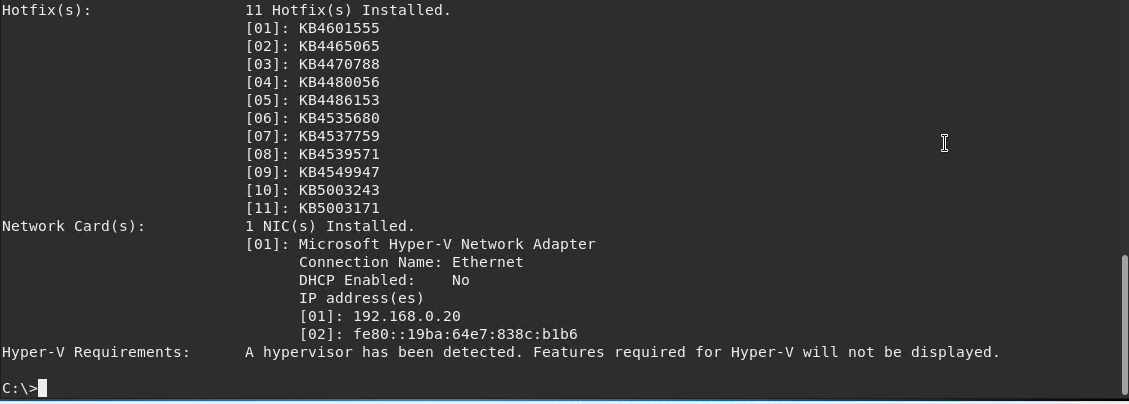
Now that we have a meterpreter session we have access and control of the CEO’s workstation. This is a serious problem as the amount of damage that can be done from here is substantial. To demonstrate I have located the 2 target files in the system: Secretrefile.txt and recipe.txt

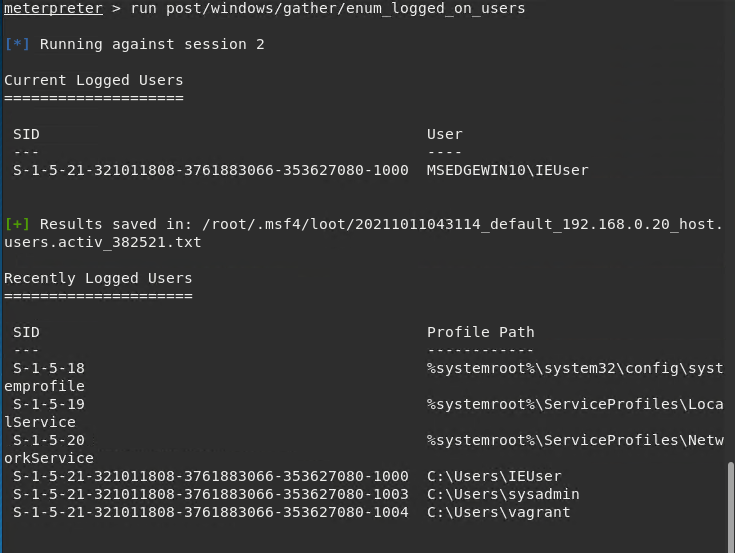




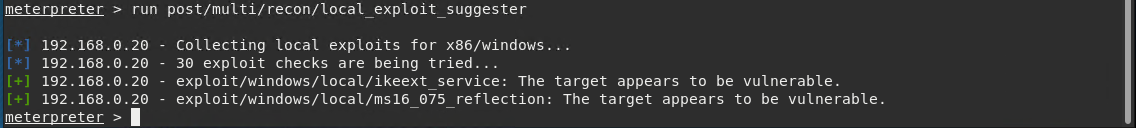
To further demonstrate the severity of this exploit I’ve also run a few post exploits to show how much information can be gathered.







And using the Metasploit exploit suggester we can also see there are other vulnerabilities that arise also;



# Recommendations

My Main recommendation is to update icecast to a later version (2.4.4 or higher) as the server is currently running on version 2.0.1 which houses the HTTP buffer overflow vulnerability and can allow attackers to gain illegitimate access to your system, by patching Icecast we can limit the possibility of future attacks in this method.

In addition to updating Icecast to a later date it is also my recommendation to improve personal security on this system by doing the following;

* Encrypt at risk or sensitive information on the system so only those with the correct key can view said file.
* Have firewall rules in place that limit who can access this media streaming service, that way this vulnerability can be mitigated to a degree.

Additionally if there is no need for this service to be in place in the organization then it can also be an option to remove this service all together or replace it with a more secure option such as Ampache, Subsonic, SHOUTcast Radio, Rocket Streaming Audio Server or Gnump3d, though it should be noted no software designed to share media will be completely secure and these alternatives may have their own problems also.