GoodSecurity Penetration Test Report

[Julie Haynes@GoodSecurity.com](mailto:Julie%20Haynes@GoodSecurity.com)

June 7, 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 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:**

The Icecast Header Overwrite vulnerability allows exploit of a buffer overflow in the header parsing of Icecast version 2.0.1 and earlier. Sending 32 HTTP headers will cause a write one past the end of pointer array - on Win32 - this overwrites the saved instruction pointer. This exploit uses ExitThread() to make a thread appear to still be in use to Icecast so that the thread counter won’t be decremented. Each time a payload exits, the counter will be left incremented so that eventually the threadpool limit will be maximized. After the 32 HTTP headers cause the threadpool limit to reach its limit, the attacker can then leverage this exploit to overwrite a return address on the stack.

The result is that remote attackers can execute arbitrary code using an HTTP request with a large number of headers. The arbitrary code can then be used to open a shell on the

Reference CVE-2004-1561 <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1561>

**Severity:**

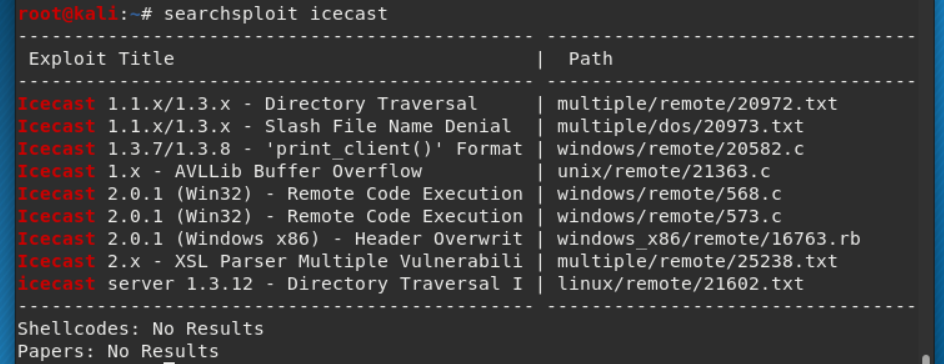
The Icecast Header Overwrite vulnerability is considered high severity. An attacker can use this vulnerability to take over the target. By exploiting this vulnerability I was able to launch a shell on the target system and immediately accomplish the following tasks remotely:

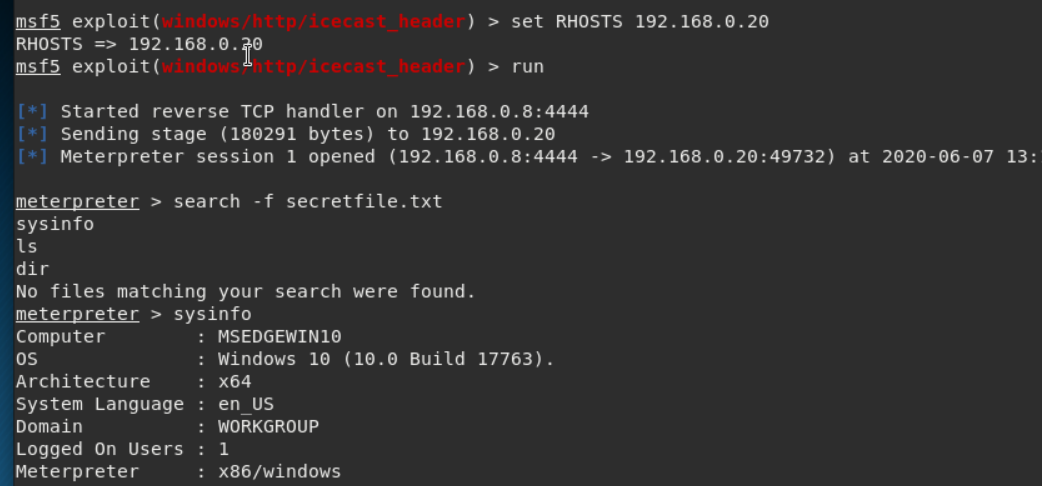
* View a list of currently logged in users
* View a list of all system information
* Access critical files including secretinfo.txt and recipe.txt
* Create a new directory called YouAreHacked and view a list of directories

**Proof of Concept:**

The following steps were used for remote penetration testing of the target

1. Open a Kali Linux command line and run ping 192.168.0.20 to confirm the target host was running.
2. Run the Nmap command nmap -sC -sV 192.168.0.20 to perform a service and version scan against the target. Results of the scan showed the following open ports including availability of Icecast streaming media on port 8000:
   * Port 25/tcp - SMTP service used for email, includes a list of multiple SMTP commands supported, when exposed to the internet this port can be inhabited by multiple Trojan programs
   * Port 135/tcp - MSRPC service for MS Windows, can be leveraged by hacker tools such as epdump when exposed to the internet
   * Port 139/tcp - NETBIOS-SSN service, vulnerable to multiple Trojans
   * Port 445/tcp – Microsoft Directory Services used for sharing MS files via SMB. Port 445 is easy for attackers to use to remotely commandeer Windows machines when it is open to the internet.
   * Port 3389/tcp - MRDP or MS Terminal Services
   * Port 8000/tcp - ice http version Icecast streaming media server, vulnerable to Icecast Header Overwrite exploit
3. Run searchsploit icecast command in Kali to discover available Icecast exploits.

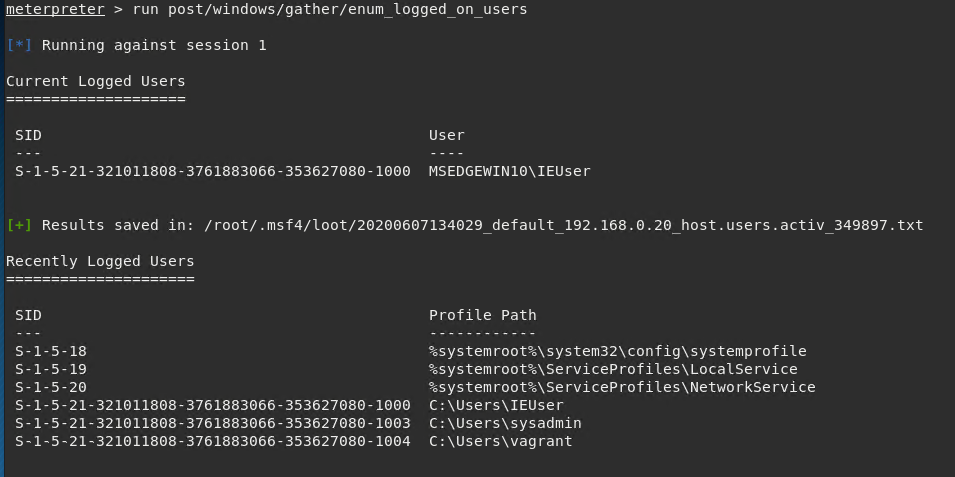


1. Run *msfconsole* to start Metasploit in Kali then run *search icecast* in Metasploit to find the Icecast Header Overwrite exploit available at “exploit/windows/http/icecast\_header” exploit listed.
2. Run *use exploit/windows/http/icecast\_header* in Metasploit to launch the Icecast Header Overwrite exploit
3. Configured the RHOST to the target machine IP address by first running *show options* then running *set RHOSTS 192.168.0.20* in Metasploit.
4. Used the *run* command in Metasploit command line to run the Icecast exploit and open a Meterpreter session.
5. Used multiple search commands including *search -f secretfile.txt*, *search -f recipe.txt*, and *search -f \*.txt* in Metasploit to locate these the “secretfile.txt” and “recipe.txt” files

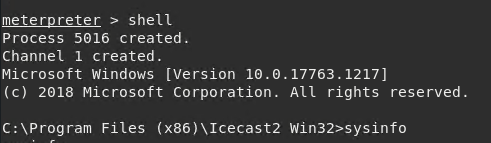


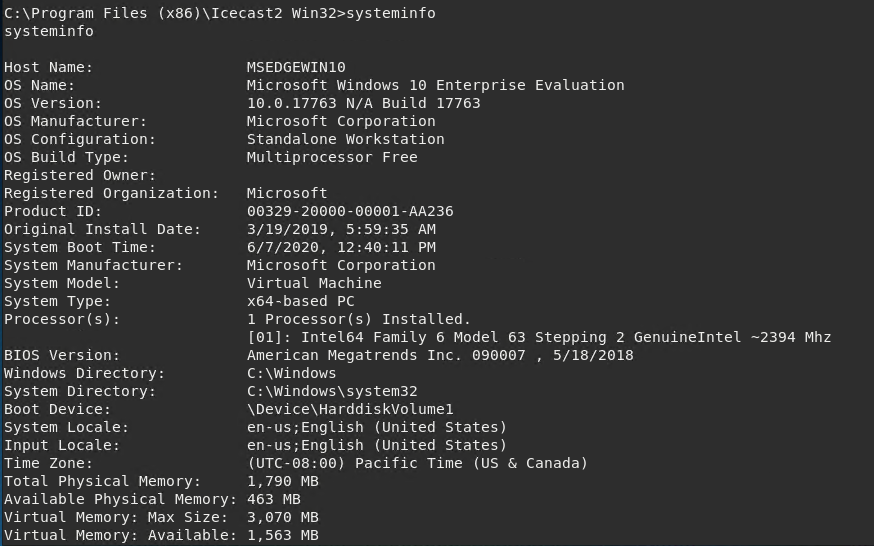


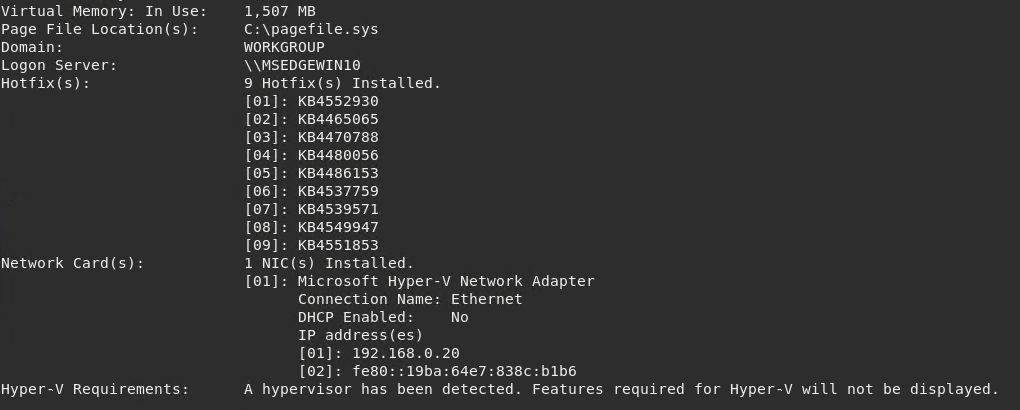
1. Run the Meterpreter post script, *run post/windows/gather/enum\_logged\_on\_users*, to enumerate all logged on users.



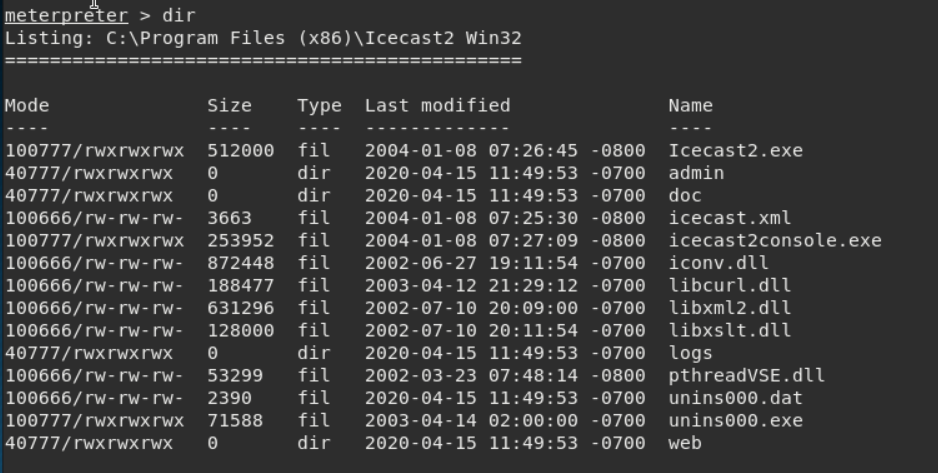
1. Open a Meterpreter shell by running the *shell* command then gather all system info by running the *systeminfo* command.

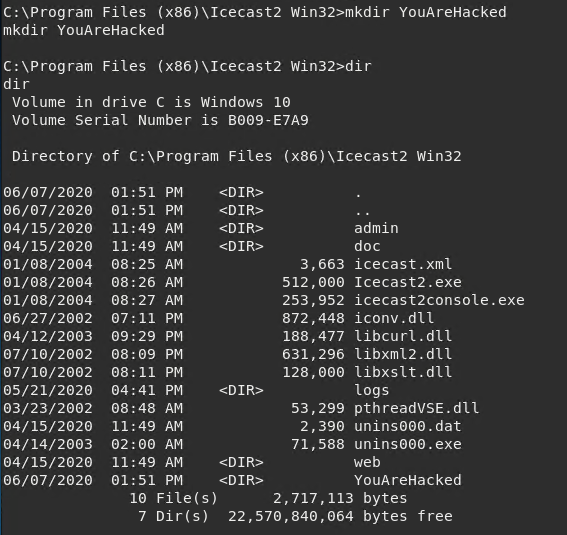






1. Run the *dir* command to view a list of directories on the target host. Run the *mkdir YouAreHacked* to create a new directory on the target host, then run the *dir* command to confirm the new directory was created on the target host.





# Recommendations

1. Upgrade Icecast to 2.0.2 or later so that target host is not vulnerable to the Icecast Header Overwrite exploit.
2. Ensure that port 445 is not exposed to the internet by blocking it with a firewall or NAT router.
3. Prevent global exposure of port 3389 by only allowing access to this port from specific IP addresses.
4. Review whether the remaining open ports, 25, 135, and 139 need to remain open to the internet and close them to the internet if possible.