GoodSecurity Penetration Test Report

[ILHAMBUHARIE@GoodSecurity.com](mailto:YOURNAMEHERE@GoodSecurity.com)

07102020

# 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 HTTP Header Buffer Overflow

## Vulnerability Explanation:

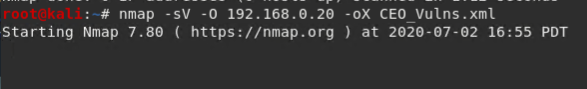
Icecast is a free streaming media package. The service allows users to listen to audio or view video over a local area network or the Internet. The exploit is on a buffer overflow in the header parsing of icecast versions 2.0.1 and earlier. The exploit sends 32 HTTP headers will cause a write one past the end of a pointer array. On windows machines this overwrites the saved instruction pointer. This exploit uses ExitThread(), this will leave icecast leaving the thread in use, and the thread counter won't be decremented.

## Severity:

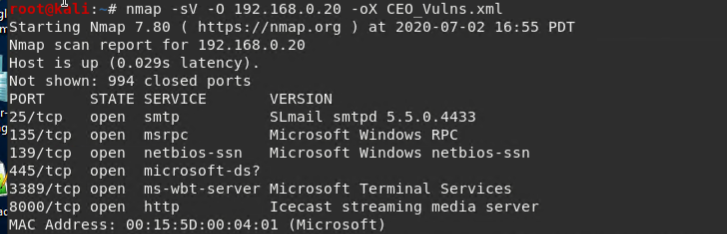
Critical

## Proof of Concept:

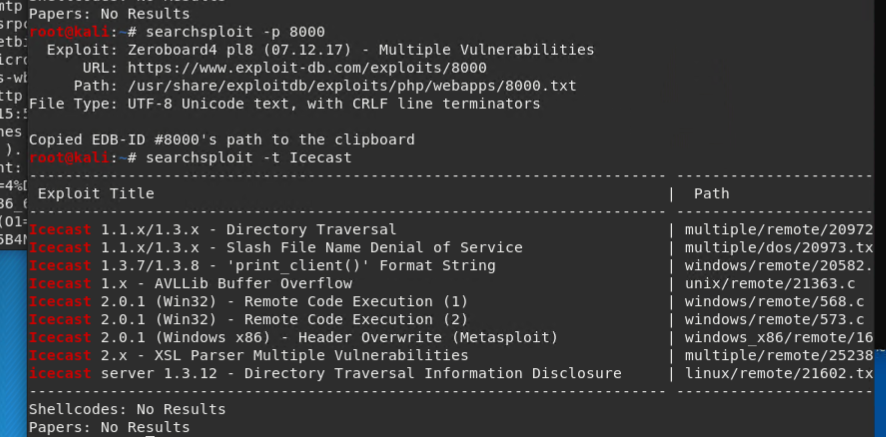
Step1: Run a nmap search on the victim machine that scans for open ports that will include versions of available ports' applications and the operating system version. The command also outputs the results to an xml file.

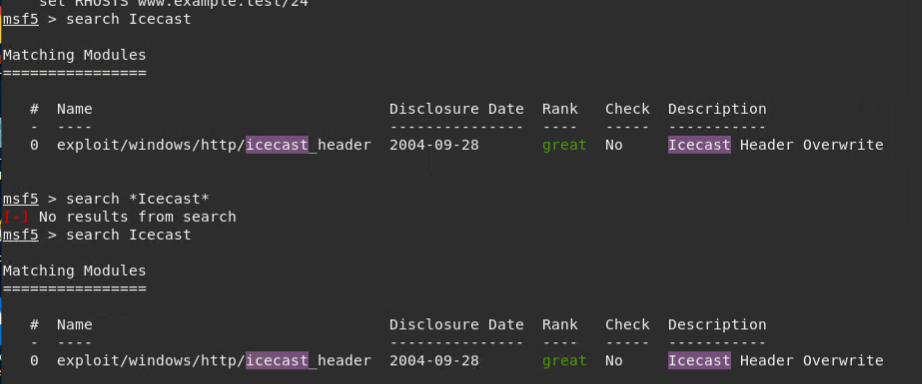


Step2: See list of open Ports and the applications (including versions) running on those ports.

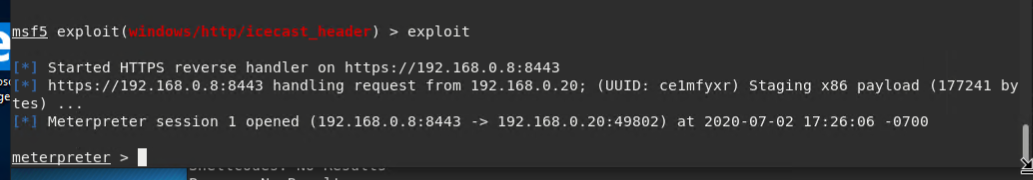


Step3: Search for an exploit on the service running on port 8000.

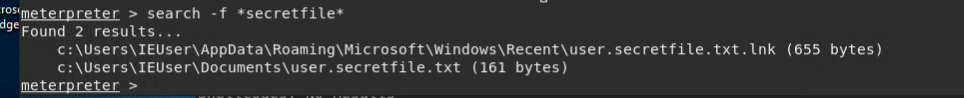




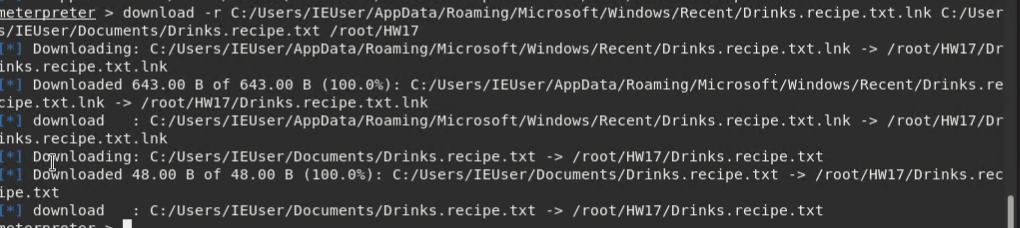
Step3: Set the IP address and port oo the victim to exploit. Run the exploit.



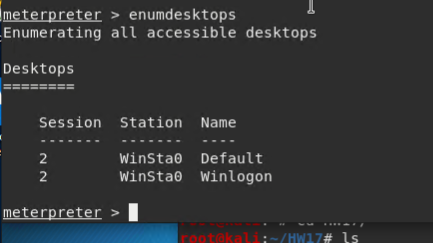
Step4: Once the meterpreter shell is available, the attacker has gained access to the victim machine. First action was to look for the secret file.

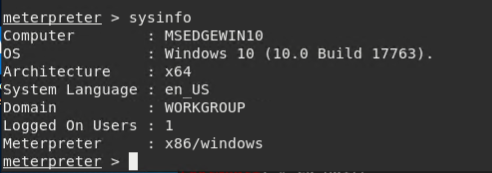


Step5: Once the secret file is found, download the secret file.



Step6: Snooping around the machine to look for other system information that can be useful to an attacker like logged in users, operating system information.





Step7: With the shell access an attacker has full command line access to the victim machine and can access all the information on the victim machine.



NetBIOS was another potential vulnerability; however, after failing at seven different NetBIOS exploits on port 139, the NetBIOS service is safe for now.

# Recommendations

Close port 8000 if ICECast is not being used. If the ICECast application is used by the business, it is recommended that ICECast be upgraded/patched to version 2.0.2. or above.