GoodSecurity Penetration Test Report

IgorAcevski@GoodSecurity.com

10/12/2021

1.0 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 exploiting two programs that had major vulnerabilities. The details of the attack can be found in the 'Findings' category.

2.0 Findings

Machine IP:

192.168.0.20

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

Icecast streaming media server

Vulnerability Explanation:

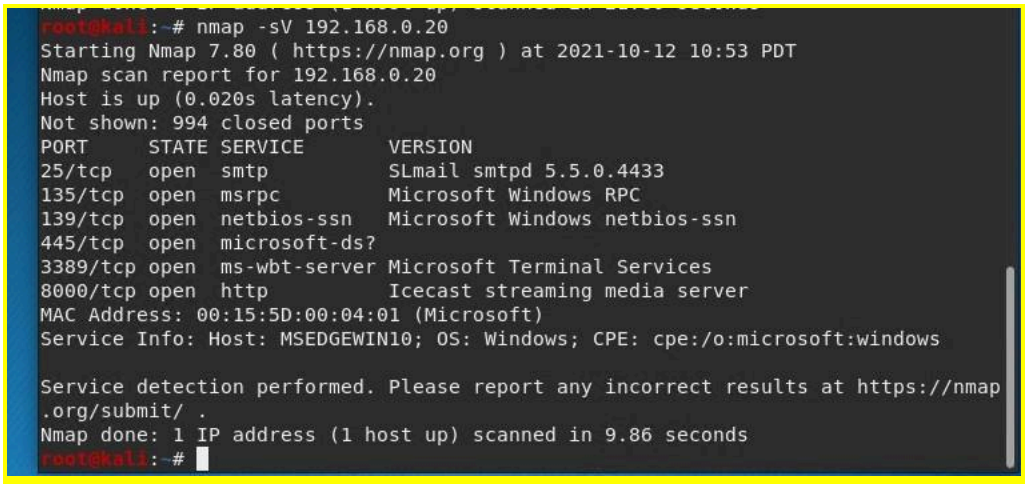
IceCast is a buffer overflow where the attacker can take over the control of the server and write codes which can trigger buffer overflow and crash the server.

Severity:

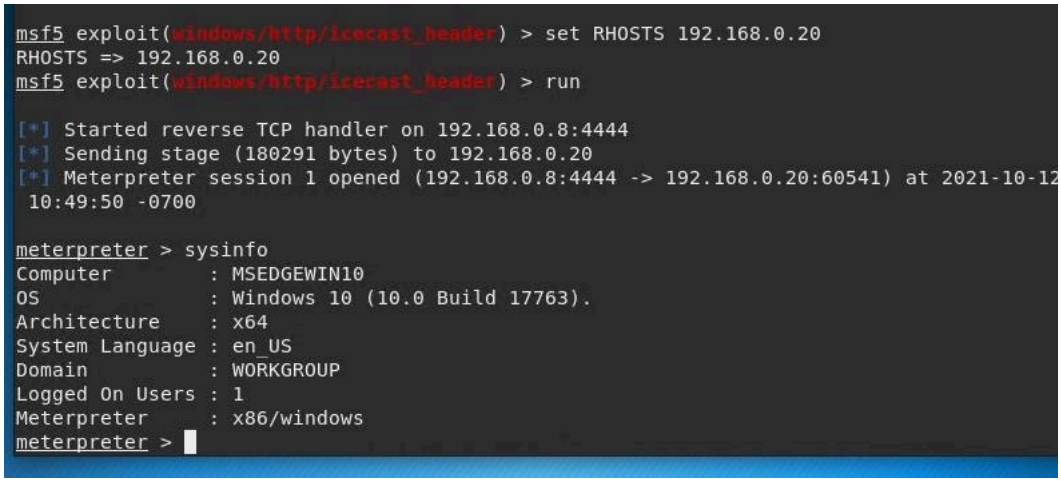
This Is a very high severity

Proof of Concept:

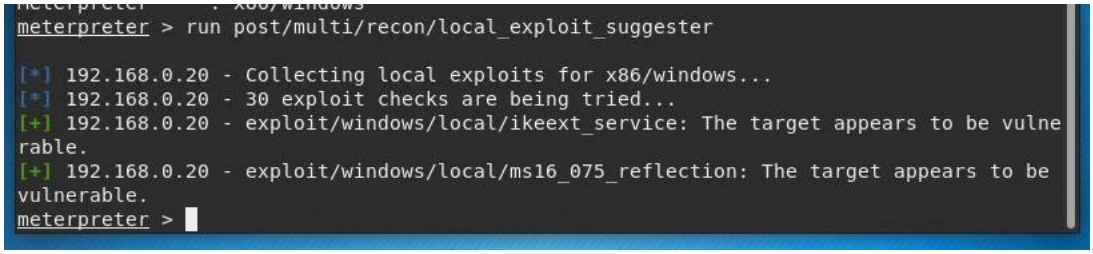
Using nmap I scan all open ports from Hans' computer and find the icecast vulnerable.



Using Metasploit, I use an icecast exploit to gain access to Hans' computer and find information about the machine.



Gaining access to Hans' computer gave us one more option to look for more vulnerabilities using local exploit suggester.



And I find two more vulnerabilities:

Ikeext_service

ms16_075_reflection

3.0 Recommendations

The best recommended IceCast vulnerability is to fully update the IceCast server with the last update and monitor for new updates.