General Statement

I was going to investigate other potential vulnerabilities and exploits besides the noted Icecast vulnerability but my lab virtual machine allotted time ran out. I ran vulnerability searches (on my own Kali Linux box) on the other services enumerated in the “nmap” scan and I’ve included those results in this file. I didn’t include these findings in the report as I wasn’t able to perform any attempted exploits on the services.

SL Mail

```
┌──(justin㉿kali)-[~]
└─$ searchsploit slmail
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' R | windows/remote/16399.rb
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' R | windows/remote/638.py
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' R | windows/remote/643.c
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' R | windows/remote/646.c
SLmail Pro 6.3.1.0 - Multiple Remote Denial o | windows/dos/31563.txt
---------------------------------------------- ---------------------------------
Shellcodes: No Results
```

The SLmail service running on Hans’ machine is SMTP and not POP3. So, I don’t think there’s a vulnerability here.

NetBIOS-SSN

I found the following results for NetBIOS:

```
┌──(justin㉿kali)-[~]
└─$ searchsploit netbios
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
BEA WebLogic 7.0 - Hostname/NetBIOS Name Remo | windows/remote/22448.txt
Cyberoam Transparent Authentication Suite 2.1 | windows/dos/46926.py
Microsoft Windows 95/98 - NetBIOS NULL Name   | windows/remote/19889.c
Microsoft Windows NT 4.0/2000 - NetBIOS Name  | windows/remote/20106.cpp
netBIOS - 'newsid' SQL Injection              | php/webapps/5852.txt
---------------------------------------------- ---------------------------------
Shellcodes: No Results
```

However, I didn't find any vulnerabilities for NetBIOS-SSN. So, I don't think there's a vulnerability here.

Microsoft Terminal Services

I found the following results for Microsoft Terminal Services:

```
┌──(justin㉿kali)-[~]
└─$ searchsploit Terminal Services
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
Microsoft Terminal Services - Use-After-Free  | windows/dos/18606.txt
Palo Alto Networks Terminal Services Agent 7. | windows/local/41176.c
Terminal Services Manager 3.1 - Local Buffer  | windows_x86/local/46058.py
Terminal Services Manager 3.2.1 - Denial of S | windows/dos/46911.py
---------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Had I had more time on my Pentesting lab machine I would have explored these potential vulnerabilities and they're associated exploits.