GoodSecurity Penetration Test Report

Richard.Brantsch[@GoodSecurity.com](mailto:Richard.Brantsch@GoodSecurity.com)

27 September 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 goal of this test is to perform attacks similar to those of a hacker and attempt to infiltrate Hans’ computer to determine if it is at risk. GoodSecurity’s overall objective was to exploit any vulnerable software, find a secret recipe file on Hans’ computer, and report the findings back to GoodCorp.

The internal penetration test found several alarming vulnerabilities on Hans’ computer: When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting two programs with major vulnerabilities. The details of the attack are below.

# Findings

*Machine IP:*

IPv4: 192.168.0.20

IPv6: fe80::19ba:64e7:838c:b1b6

*Hostname:*

MSEDGEWIN10

*Vulnerability Exploited:*

Icecast Header Overwrite  
MSF: EXPLOIT/WINDOWS/HTTP/ICECAST\_HEADER

*Vulnerability Explanation:*

The version 2.0.1 of the Icecast streaming media server allows for a buffer overflow exploit.

The Icecast server accepts a maximum of 32 headers in the clients HTTP Request, a request with more than 31 headers cause the overwriting of the return address of the vulnerable function with a pointer to the beginning of the 32th header.

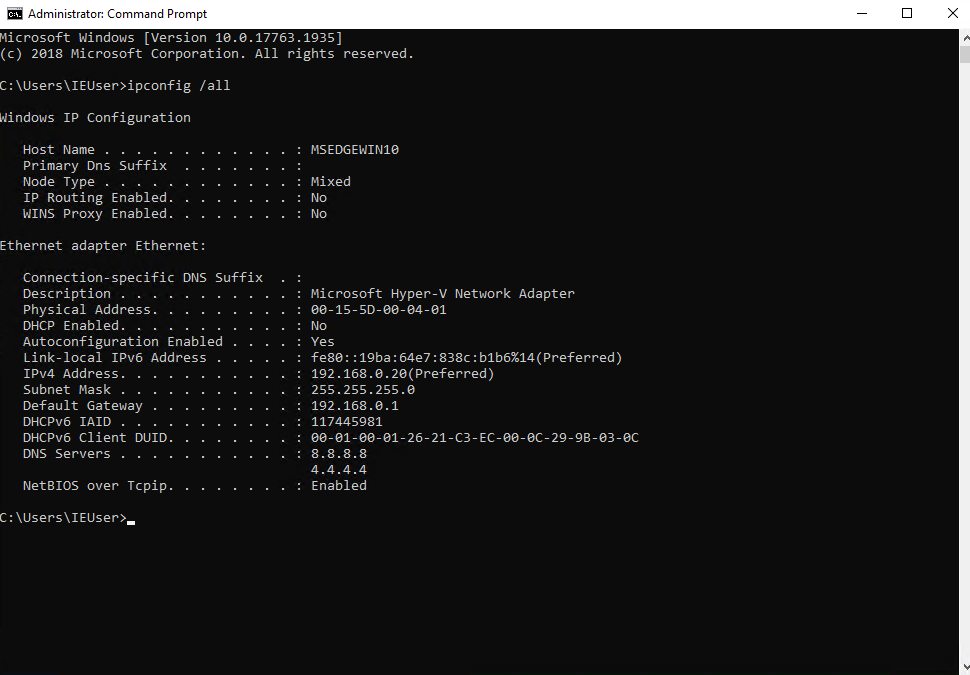
Utilizing this exploit makes it possible to execute remote code simply using the normal HTTP request plus 31 headers followed by a shellcode that will be executed.

Link: [Icecast Header Overwrite](https://vulners.com/metasploit/MSF:EXPLOIT/WINDOWS/HTTP/ICECAST_HEADER)

*Severity:*

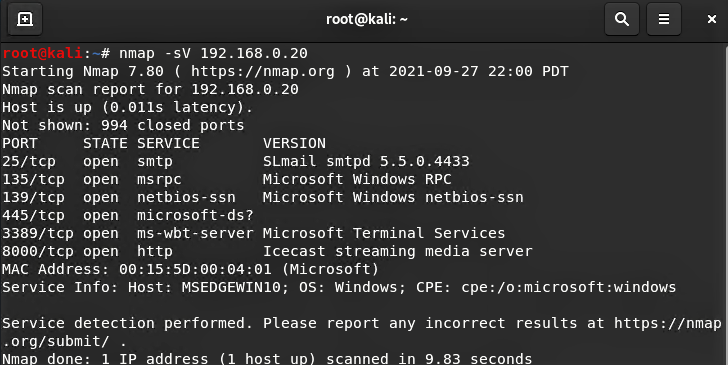
CVSS 7.5 High

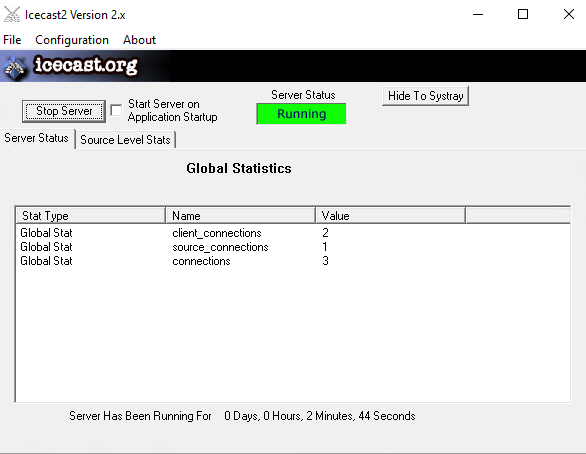
*Proof of Concept:*

On the CEO’s workstation (DVW10) I performed an IP lookup to determine the target IP:

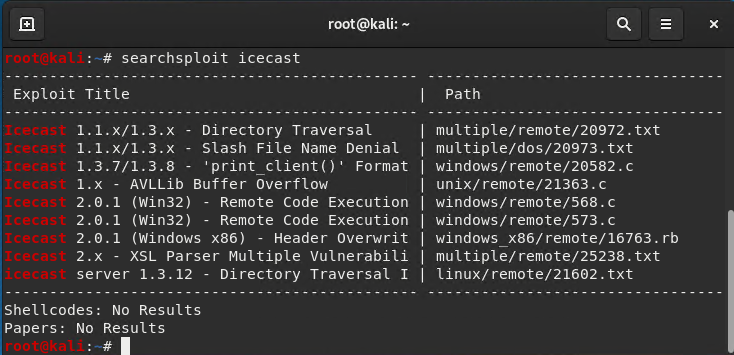


On the attacker machine (Kali) I performed a service and version scan using Nmap, this revealed which services are up and running:

****

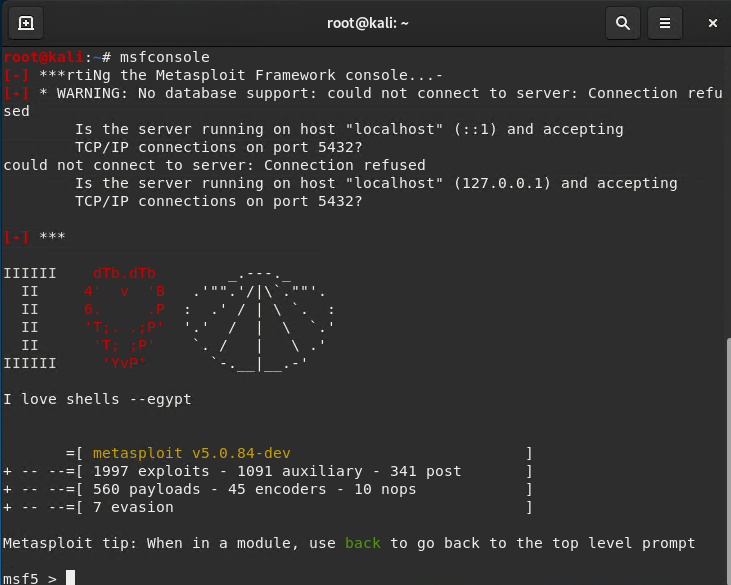
Simultaneously on the target machine (DVW10) Icecast`s Global Statistics showed me following:

Searching for exploits with Searchsploit on the attacker (Kali) machine with the information I retrieved from the service and version lookup:

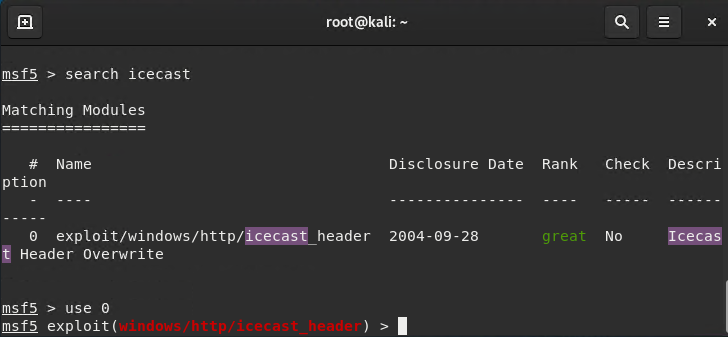


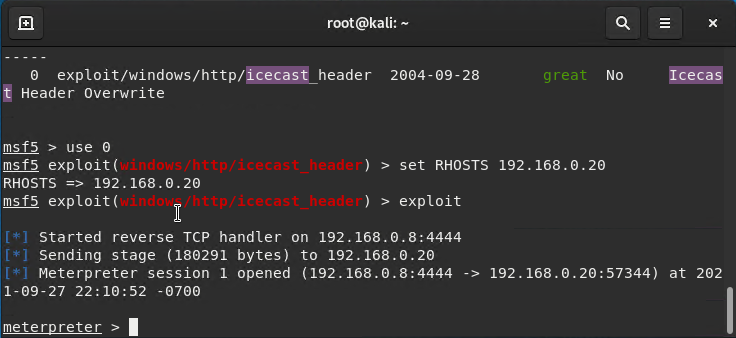
**The relevant exploit for us is the windows\_x86/remote/16763.rb**

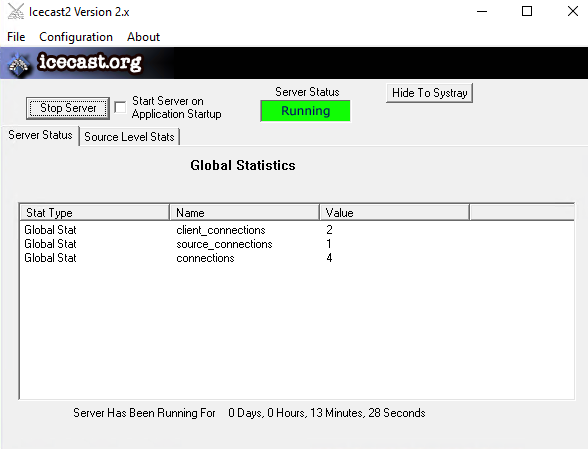
Starting a Metasploit (Attacker’s tool) session:



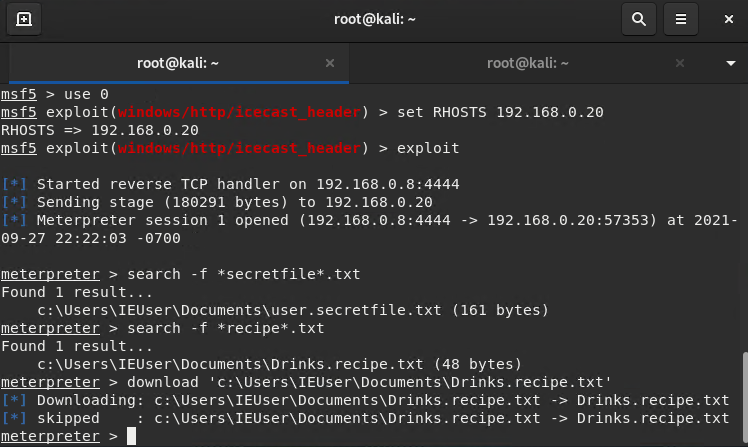
Locating the exploit in Metasploit and selecting it:

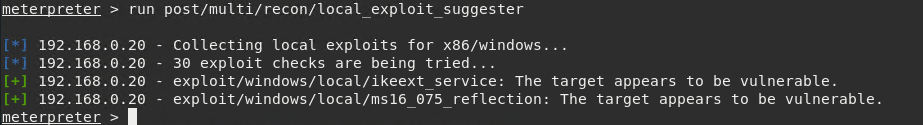
****

Setting the targets IP address:

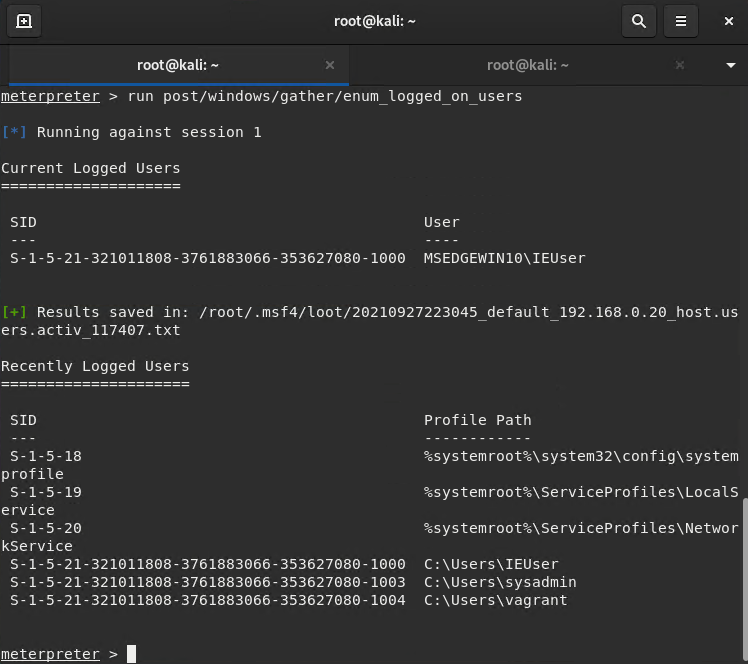
Checking the Icecast Global Statistics showed that the Value on connections changed from 3 to 4 which confirms the attack was successful:

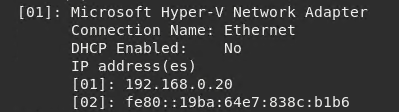
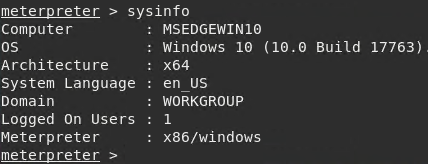
Connection to the DVW10 machine is established, search for the secretfile.txt and for the `recipe.txt` on the target and download the file:

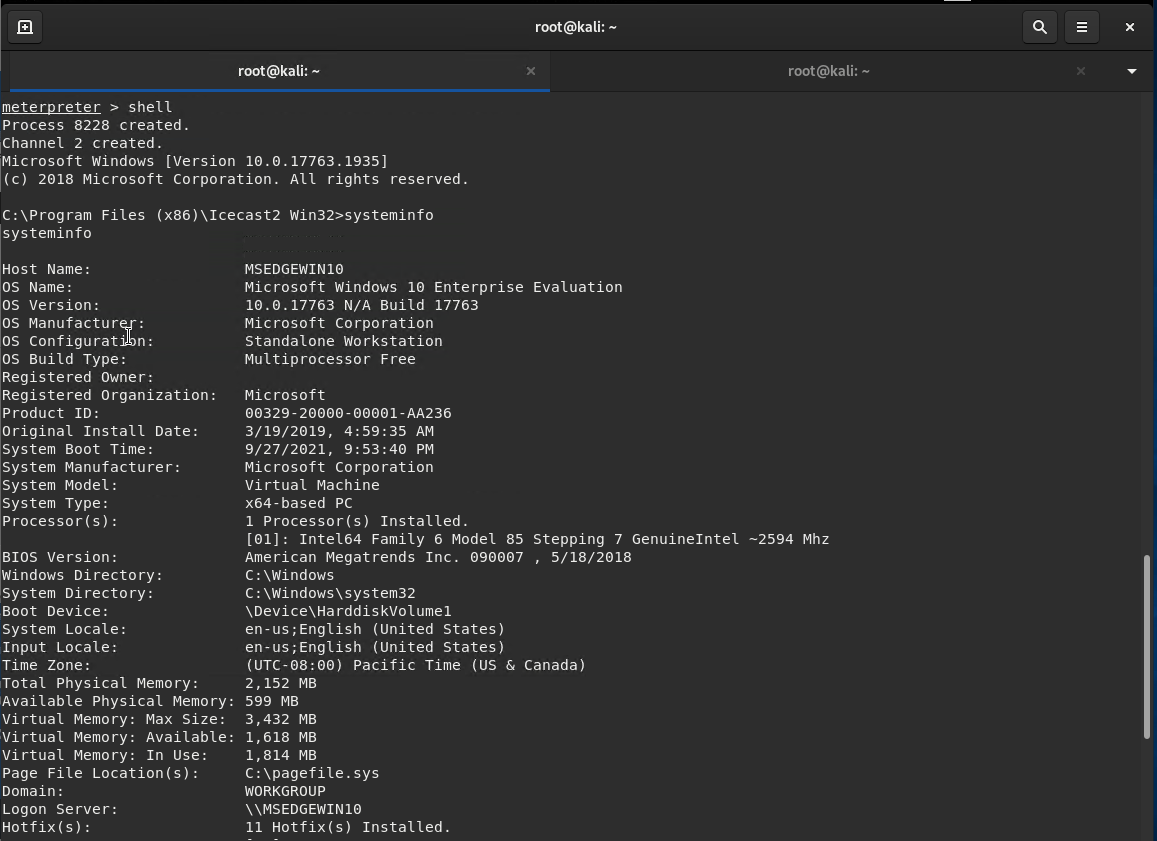


Additional findings while in control of the DVW10 machine were following:   
Scan for additional vulnerabilities/exploits:

Enumerates all logged on users:

****

Displaying computer system information:

****

# Findings

*Machine IP:*

IPv4: 192.168.0.20

IPv6: fe80::19ba:64e7:838c:b1b6

*Hostname:*

MSEDGEWIN10

*Vulnerability Exploited:*

*Windows Net-NTLMv2 Reflection DCOM/RPC   
MSF: EXPLOIT/WINDOWS/LOCAL/MS16\_075\_REFLECTION*

*Vulnerability Explanation:*

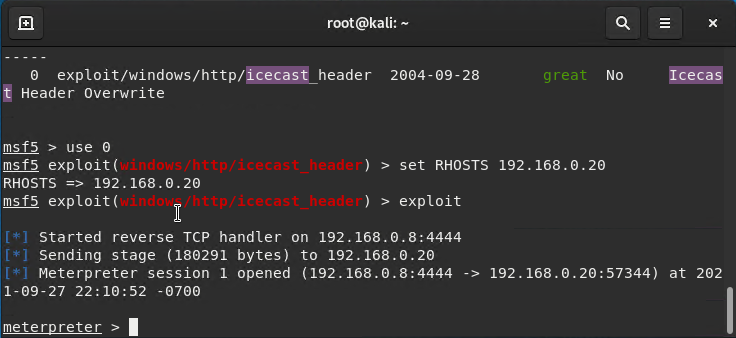
The remote Windows host is missing a security update. It is, therefore, affected by an elevation of privilege vulnerability in the Microsoft Server Message Block (SMB) server when handling forwarded credential requests that are intended for another service running on the same host. An authenticated attacker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

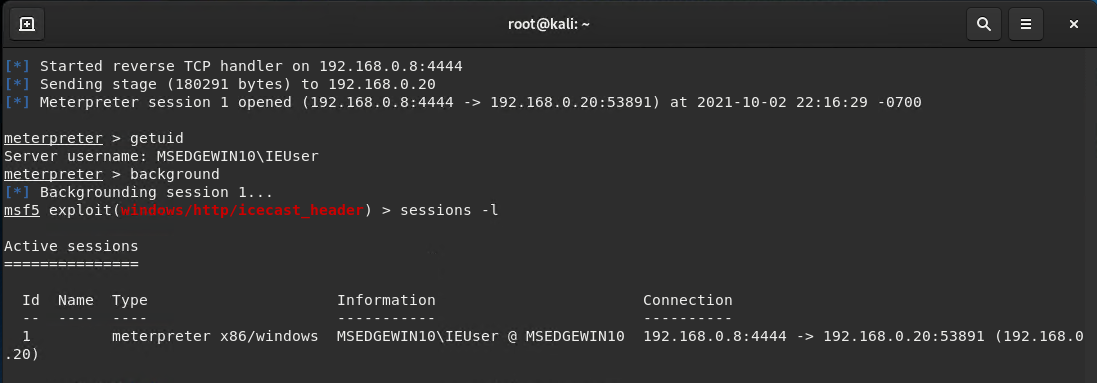
Link: [Windows Net-NTLMv2 Reflection DCOM/RPC](https://vulners.com/metasploit/MSF:EXPLOIT/WINDOWS/LOCAL/MS16_075_REFLECTION)

*Severity:*

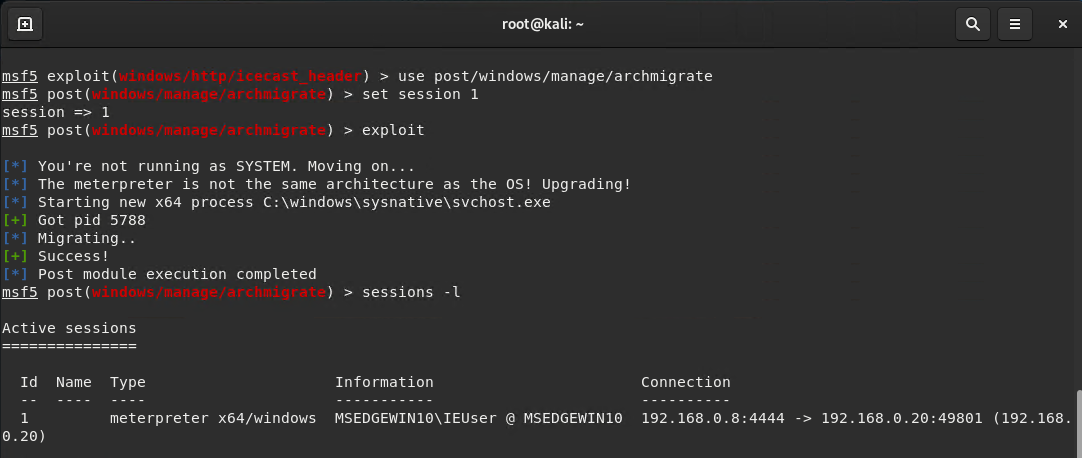
CVSS 7.2 High

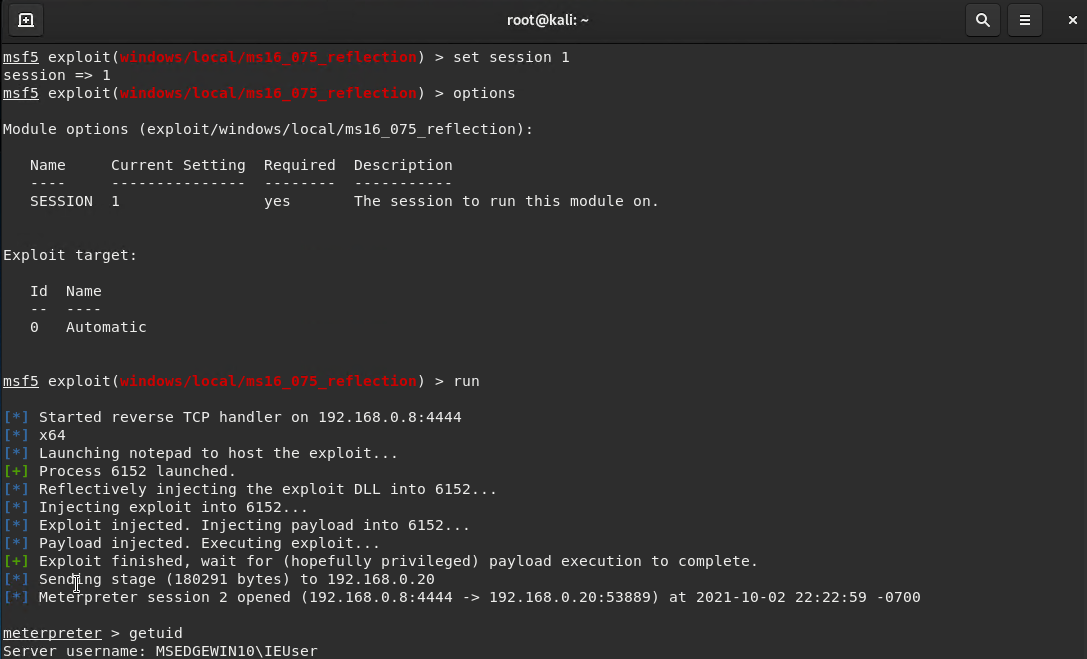
*Proof of Concept:*

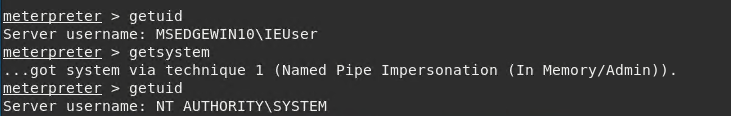
Using the Icecast exploit to gain access to the DVW10 Machine:

Displaying server username, launching a background session\* and displaying current sessions:

***\* For the next step I need to be in a background session to be able to load new modules for the initial attack.***

I used a module called archmigrate, this module checks if the architecture of meterpreter is as same as the architecture of OS and if it is not, spawns a new process with the correct architecture and migrates into that process.

Loading the *Windows Net-NTLMv2 Reflection DCOM/RPC | /MS16\_075\_REFLECTION exploit and creating a new session, in this case we did not gain SYSTEM although the exploit did run successfully:*

Although the *MS16\_075\_REFLECTION* exploit did not create a session with elevated privileges it created a new meterpreter session, in this case we can gain SYSTEM (elevated privileges) with an inbuild function of meterpreter:

# Findings

*Machine IP:*

IPv4: 192.168.0.20

IPv6: fe80::19ba:64e7:838c:b1b6

*Hostname:*

MSEDGEWIN10

*Vulnerability Exploited:*

IKE and AuthIP IPsec Keyring Modules Service (IKEEXT) Missing DLL |   
MSF: EXPLOIT/WINDOWS/LOCAL/IKEEXT\_SERVICE

*Vulnerability Explanation:*

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.

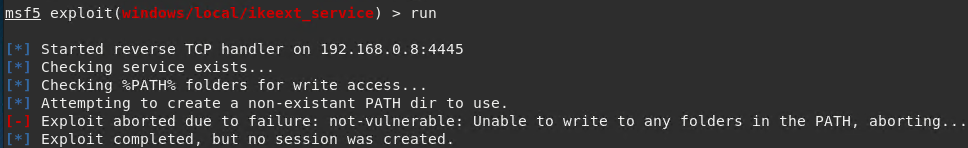
Link: [IKE and AuthIP IPsec Keyring Modules Service (IKEEXT) Missing DLL](https://vulners.com/metasploit/MSF:EXPLOIT/WINDOWS/LOCAL/IKEEXT_SERVICE)

*Severity:*

CVSS 6.0 Medium

*Proof of Concept:*

Using the Icecast exploit to gain access to the DVW10 Machine as demonstrated in Findings 2.0 and 2.1, combined with the archmigrate module used in Findings 2.1 (this module checks if the architecture of meterpreter is as same as the architecture of OS and if it is not, spawns a new process with the correct architecture and migrates into that process).

Loading the: *IKE and AuthIP IPsec Keyring Modules Service (IKEEXT) Missing DLL |   
MSF: EXPLOIT/WINDOWS/LOCAL/IKEEXT\_SERVICE*

The exploit was unsuccessful and could not find any files in %PATH% to write access to.

# Recommendations

**Vulnerability:**

**Icecast Header Overwrite | MSF: EXPLOIT/WINDOWS/HTTP/ICECAST\_HEADER**

The remote web server runs Icecast version 2.0.1. Such versions are affected by an HTTP header buffer overflow vulnerability that may allow an attacker to execute arbitrary code on the remote host with the privileges of the Icecast server process.

This Icecast exploit is an old vulnerability that can be fixed with a patch.   
Update Icecast to the latest version and all other software on the system.

Link: [Icecast Current Release (2.4.4)](https://icecast.org/download/)

Additionally Encrypt all files/folders that are valuable to your company. **Enable your windows firewall with rules to only explicitly allow traffic on needed ports.**

Remove Icecast: If Icecast is not a valued business resource, consider removing altogether.

**Vulnerability:**

**Windows Net-NTLMv2 Reflection DCOM/RPC MSF: EXPLOIT/WINDOWS/LOCAL/  
MS16\_075\_REFLECTION**

Although the exploit did not elevate the privileges it was still able to establish a connection to the DVW10 Machine which is dangerous per se since Meterpreter is a powerful attacking tool like demonstrated on the last page of Findings 2.1. Therefore, I would strongly recommend to update the system software immediately since it still is an active vulnerability.

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Link: [Windows 10 May 2021 Update](https://www.microsoft.com/en-au/software-download/windows10)

**Vulnerability:**

**IKE and AuthIP IPsec Keyring Modules Service (IKEEXT) Missing DLL | MSF: EXPLOIT/WINDOWS  
/LOCAL/IKEEXT\_SERVICE**

This specific exploit is more vulnerable to Microsoft Windows versions older than Windows 10 nevertheless there is always a risk having an unpatched vulnerability on your system. I would recommend to apply an update immediately.

Link: [Windows 10 May 2021 Update](https://www.microsoft.com/en-au/software-download/windows10)

If you are using Windows Update, the latest SSU (Service Stack Update) will be offered to you automatically.