

[Capture The Flag]

NAMA TIM : [AJIS]

Rabu, 21 Oktober 2020

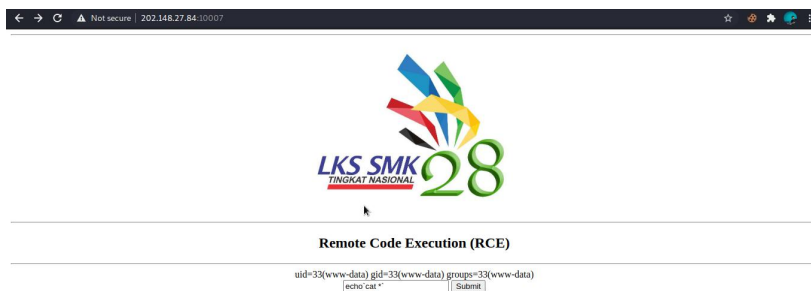
Ketua Tim	
1.	Abdul Rozaqi Wildan
Member	
1.	Muhammad Farhan Iqbal
2.	Abdul Rozaqi Wildan

Remote Code Execution (LKS SMK28)

Pertama kita disuguhkan dengan tampilan web dan ada fitur search disitu.

Disini sangat stuck karena memasang payload berjam-jam tidak dapet hasil sehingga saya, saya memasukkan payload ini :

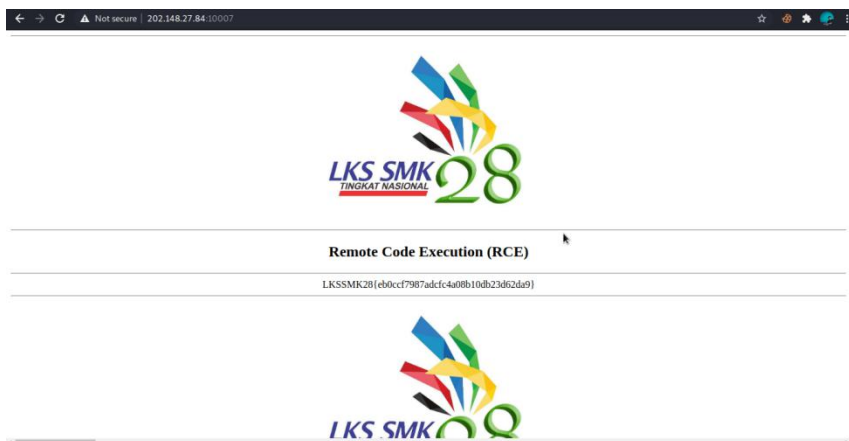
`echo `id``



Dan ada hasilnya

Lalu kita tampilkan semuanya dengan perintah :

`echo`cat *``



Dan dapat flagnya : `LKSSMK28{eb0ccf7987adcf4a08b10db23d62da9}`

PSWEB (LKS SMK28)

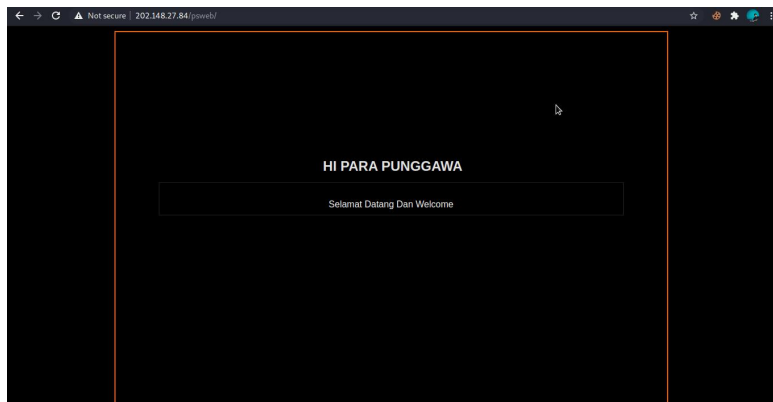
Flag di soal ini berhubungan dengan website. Sangat gampang untuk menyelesaikan soal, jika teman-teman paham website dan bagaimana cara melihat source code pasti bisa dengan mudah menyelesaikan dan mendapatkan flag

<http://202.148.27.84/psweb/>

Format Flag : LKSSMK28{FLAG}

Solvednya :

Kita masuk ke webnya :



Lalu sesuai dengan hint nya, kita view source dengan ctrl + u

```
view-source:202.148.27.84/psweb/
1 <html xmlns="http://www.w3.org/1999/xhtml">
2 <head>
3 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
4 <title>Page Source</title>
5 <link href="/psweb/amber.css" rel="stylesheet" type="text/css" />
6 <!--
7 -->
8 </style>
9 </head>
10 <body>
11
12
13
14
15
16 <!-- Begin Wrapper -->
17 <div id="wrapper">
18 <div id="logo"></div>
19 <!-- end logo div -->
20 <!-- begin tag div -->
21 <div id="tag"></div>
22 <!-- end tag div -->
23 <!-- begin nav bar -->
24 <div id="nav-bar">
25 <div id="nav-buttons">
26 </div>
27 </div>
28 <!-- end nav bar -->
29 <div class="intro-text-base">
30
31 <h1 style="text-align:center;">HI PARA PUNGGANA</h1>
32 <div id="random">
33 <br>
34 <center>Selamat Datang Dan Welcome</center>
35 </div>
36 </body>
37 </html>
38
```

202.148.27.84/psweb/amber.css

Dan klik link CSS nya

```
view-source:202.148.27.84/psweb/amber.css
margin-top: 10px;
float: left;
color: #f0f0f0;
}
#upcoming4c {
width: 526px;
color: #CCCCCC;
font-family: "Trebuchet MS", verdana, Arial, sans-serif;
font-size: 10pt;
float: left;
margin-top: 24px;
margin-left: 300px;
}
#upcoming-101a {
width: 300px;
color: #CCCCCC;
font-family: "Trebuchet MS", verdana, Arial, sans-serif;
font-size: 10pt;
float: left;
margin-top: 24px;
margin-left: 260px;
}
/* Flag : LKS-MK28(Mr_r0b0T_E03) */
#upcoming-101b {
width: 300px;
color: #CCCCCC;
font-family: "Trebuchet MS", verdana, Arial, sans-serif;
font-size: 10pt;
float: left;
margin-top: 24px;
margin-left: 11px;
}

table.thr {
margin: 0 0 0 0;
padding: 0 0 0 0;
}
td.tright{
border: 0px;
text-align: right;
color: #FFFFFF;
}
td.tleft{
border: 0px;
}
```

Lalu search LKS

Dan dapet flagnya :

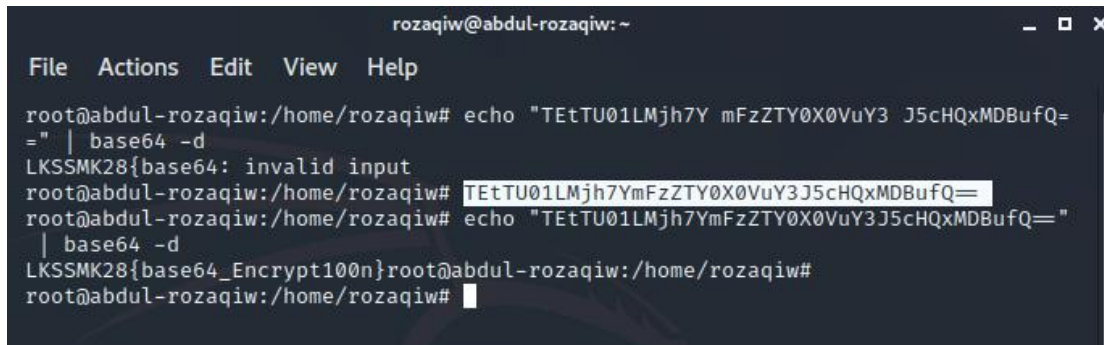
Simple Encrypt (LKS SMK28)

Gabungkan Enkripsi di bawah ini :

TETtU01LMjh7Y mFzZTY0X0VuY3 J5cHQxMDBufQ==

Format Flag : LKSSMK28{FLAG}

Kita decode saja menggunakan terminal di kali



```
rozaqiw@abdul-rozaqiw: ~  
File Actions Edit View Help  
root@abdul-rozaqiw:/home/rozaqiw# echo "TETtU01LMjh7Y mFzZTY0X0VuY3 J5cHQxMDBufQ=  
=" | base64 -d  
LKSSMK28{base64: invalid input  
root@abdul-rozaqiw:/home/rozaqiw# TETtU01LMjh7YmFzZTY0X0VuY3J5cHQxMDBufQ==  
root@abdul-rozaqiw:/home/rozaqiw# echo "TETtU01LMjh7YmFzZTY0X0VuY3J5cHQxMDBufQ=  
=" | base64 -d  
LKSSMK28{base64_Encrypt100n}root@abdul-rozaqiw:/home/rozaqiw#  
root@abdul-rozaqiw:/home/rozaqiw#
```

Dapet Flag : LKSSMK28{base64_Encrypt100n}

SimPLe Brain Encrypt (LKS SMK28)

300

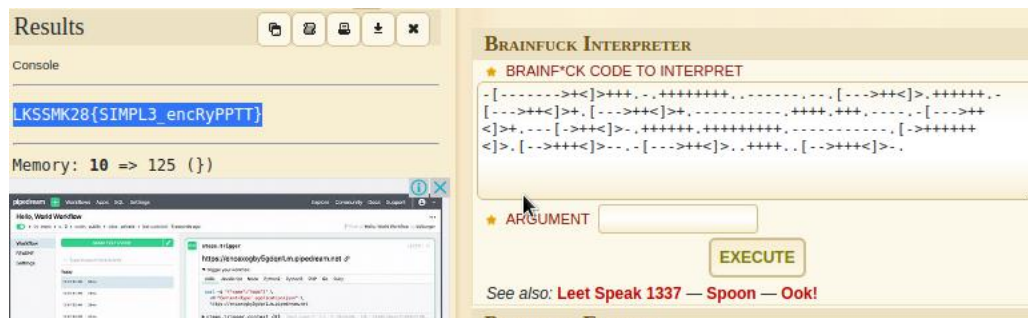
Teman-teman diberikan file tentang spoiler warning. yang jika dibaca dengan teliti akan menemukan link untuk memecahkan soal.

Format Flag : LKSSMK28{FLAG}

Setelah ada link tersembunyi <http://pastebin.com/TzcBcJg3> dan dibuka di browser ada enkripsi brainfuck

Masuk ke sini untuk decodenya

<https://www.dcode.fr/brainfuck-language>



LKSSMK28{SIMPL3_encRyPPTT}

Bypass Administrator (LKS SMK28)

500

silahkan login menggunakan user "guest" dan password "guest" tetapi untuk mendapatkan "flag" anda harus login sebagai administrator.

[Link Soal](#)

Format Flag : LKSSMK28{FLAG}

Masuk ke link soal <http://202.148.27.84:10002/> lalu masukan username dan password dengan guest



Bypass Administrator

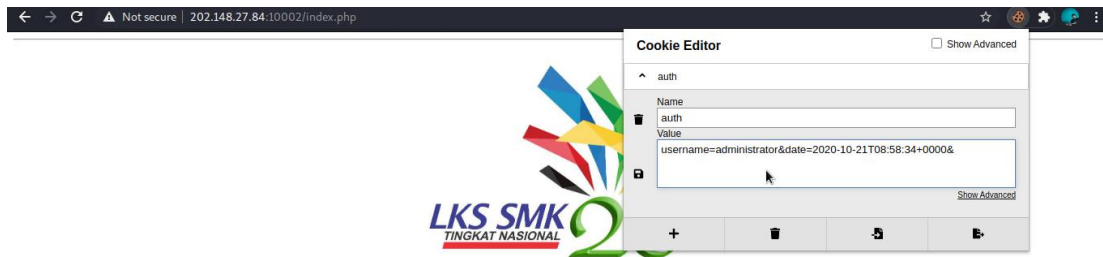
Warning: Cannot modify header information - headers already sent by (output started at /var/www/html/index.php:1) in /var/www/html/index.php on line 23

Login successful!

Setting cookie: auth=username=guest&date=2020-10-21T08:58:34+0000&

Click [here](#) to continue!

Dan berhasil masuk disana dapet hint lagi harus admin, saya menggunakan extension chrome cookie editor, masukin auth di name terus copas ini nya username=guest&date=2020-10-21T08:58:34+0000& dan ganti guest nya jadi administrator lalu save dan reload



Bypass Administrator

Welcome administrator!

Congratulations!

LKSSMK28{3e671ea34dcac32e7e9e7c67ee8cfc0b}

[Log out](#)

Dan dapet Flagnya :

LKSSMK28{3e671ea34dcac32e7e9e7c67ee8cfc0b}

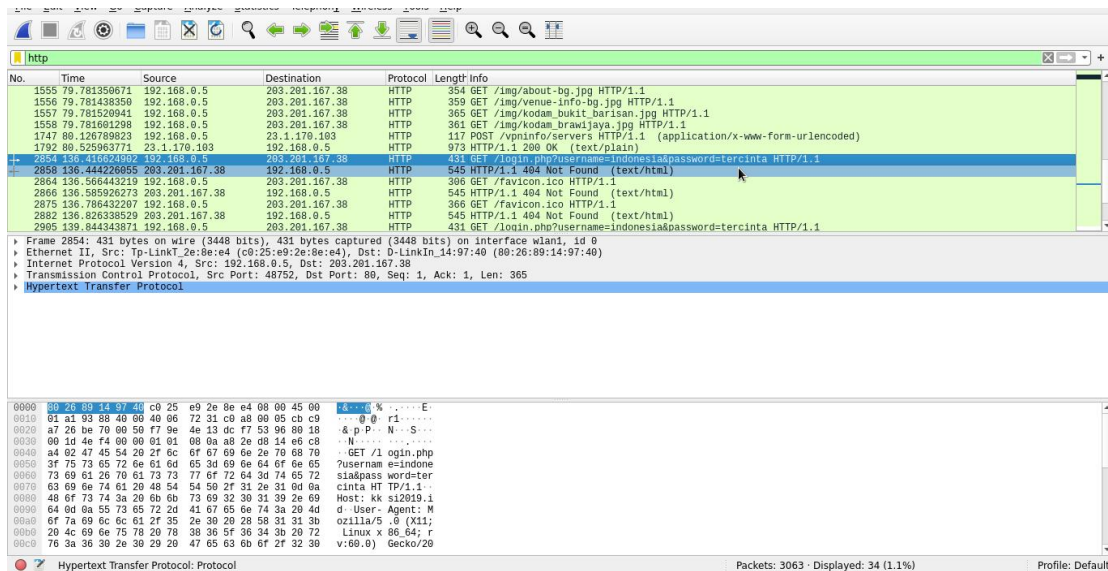
Web Login (LKS SMK28)

500

Lakukan analisa pada file pcap, untuk mendapatkan akses kedalam url berikut ini:

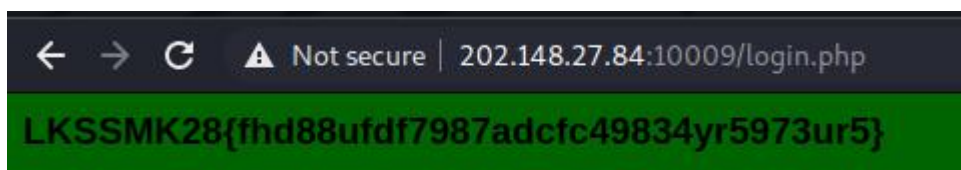
<http://202.148.27.84:10009/>

Download file pcap nya dan buka lewat wireshark dan filter dengan http dan ada protokol yang ada username dan password nya



Dan ada username = indonesia, password = tercinta

Dan masuk ke link web yg tadi dan masukan username dan passwordnya dan dapet flag :



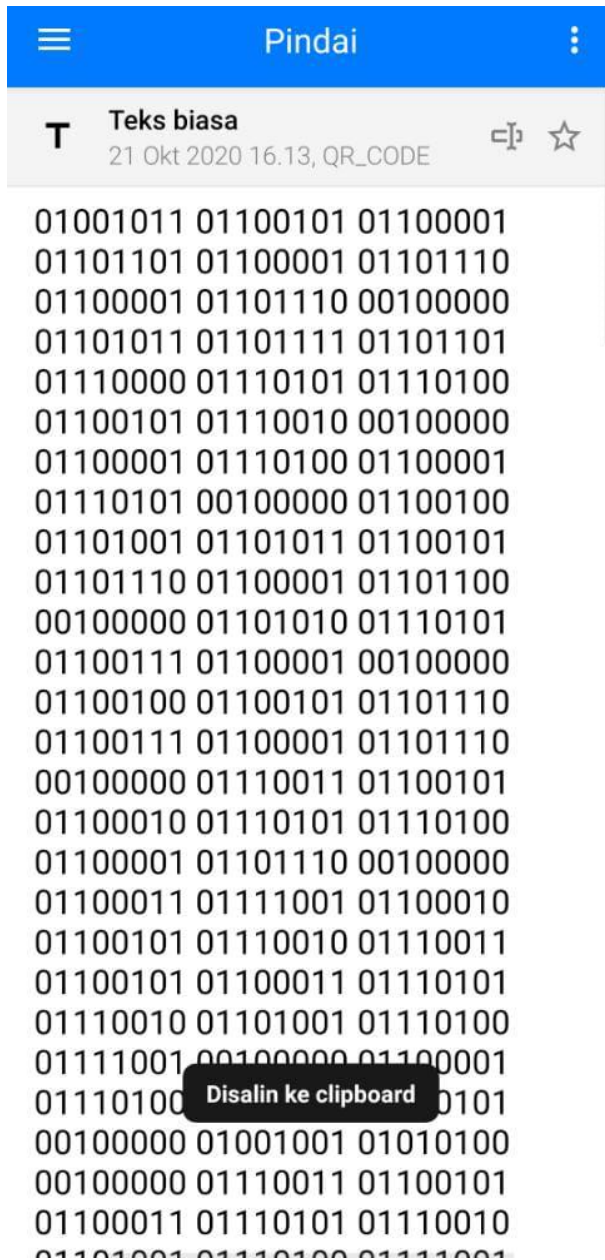
QR COD3 (LKS SMK28)

250

Kode QR atau biasa dikenal dengan istilah QR Code adalah bentuk evolusi kode batang dari satu dimensi menjadi dua dimensi.

Terdapat pesan rahasia enkripsi Binary yang terdapat di file qrC0d3.png

Format Flag : LKSSMK28{FLAG}

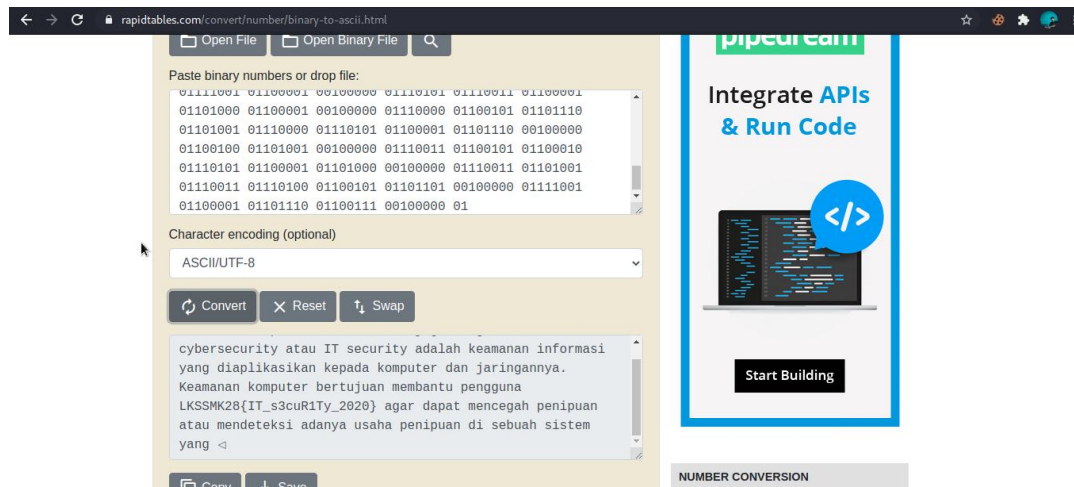


Lalu scan dengan qr code aplikasi scanner dan dapet data binary

```
01001011 01100101 01100001 01101101 01100001 01101110 01100001
01101110 00100000 01101011 01101111 01101101 01110000 01110101
01110100 01100101 01110010 00100000 01100001 01110100 01100001
01110101 00100000 01100100 01101001 01101011 01100101 01101110
01100001 01101100 00100000 01101010 01110101 01100111 01100001
00100000 01100100 01100101 01101110 01100111 01100001 01101110
00100000 01110011 01100101 01100010 01110101 01110100 01100001
01101110 00100000 01100011 01111001 01100010 01100101 01110010
01110011 01100101 01100011 01110101 01110010 01101001 01110100
01111001 00100000 01100001 01110100 01100001 01110101 00100000
01001001 01010100 00100000 01110011 01100101 01100011 01110101
01110010 01101001 01110100 01111001 00100000 01100001 01100100
01100001 01101100 01100001 01101000 00100000 01101011 01100101
01100001 01101101 01100001 01101110 01100001 01101110 00100000
01101001 01101110 01100110 01101111 01110010 01101101 01100001
01110011 01101001 00100000 01111001 01100001 01101110 01100111
00100000 01100100 01101001 01100001 01110000 01101100 01101001
01101011 01100001 01110011 01101001 01101011 01100001 01101110
00100000 01101011 01100101 01110000 01100001 01100100 01100001
00100000 01101011 01101111 01101101 01110000 01110101 01110100
01100101 01110010 00100000 01100100 01100001 01101110 00100000
01101010 01100001 01110010 01101001 01101110 01100111 01100001
01101110 01101110 01111001 01100001 00101110 00100000 01001011
01100101 01100001 01101101 01100001 01101110 01100001 01101110
00100000 01101011 01101111 01101101 01110000 01110101 01110100
01100101 01110010 00100000 01100010 01100101 01110010 01110100
01110101 01101010 01110101 01100001 01101110 00100000 01101101
01100101 01101101 01100010 01100001 01101110 01110100 01110101
00100000 01110000 01100101 01101110 01100111 01100111 01110101
01101110 01100001 00100000 01001100 01001011 01010011 01010011
01001101 01001011 00110010 00111000 01111011 01001001 01010100
01011111 01110011 00110011 01100011 01110101 01010010 00110001
01010100 01111001 01011111 00110010 00110000 00110010 00110000
01111101 00100000 01100001 01100111 01100001 01110010 00100000
01100100 01100001 01110000 01100001 01110100 00100000 01101101
01100101 01101110 01100011 01100101 01100111 01100001 01101000
00100000 01110000 01100101 01101110 01101001 01110000 01110101
01100001 01101110 00100000 01100001 01110100 01100001 01110101
00100000 01101101 01100101 01101110 01100100 01100101 01110100
01100101 01101011 01110011 01101001 00100000 01100001 01100100
01100001 01101110 01111001 01100001 00100000 01110101 01110011
01100001 01101000 01100001 00100000 01110000 01100101 01101110
01101001 01110000 01110101 01100001 01101110 00100000 01100100
01101001 00100000 01110011 01100101 01100010 01110101 01100001
```

```
01101000 00100000 01110011 01101001 01110011 01110100 01100101
01101101 00100000 01111001 01100001 01101110 01100111 00100000 01
```

Lalu kita decode saja di <https://www.rapidtables.com/convert/number/binary-to-ascii.html>



Dan dapat flag :

LKSSMK28{IT_s3cuR1Ty_2020}

gambar1

250

tim analisis sedang menganalisis / forensic sebuah file gambar.

langkah pertama bantu analisis dengan menemukan hash MD5 gambar tersebut.

flag = LKSSMK28{MD5}

Tinggal download gambarnya dan masukan ke perintah linux md5sum namafile

```
rozaqi@abdul-rozaqi: ~  
File Actions Edit View Help  
root@abdul-rozaqi:/home/rozaqi/Downloads# md5sum 2018-09-22_09.31.07.jpg  
c0b7d53ada2ad6858df4ada15f40b550 2018-09-22_09.31.07.jpg  
root@abdul-rozaqi:/home/rozaqi/Downloads#
```

Lalu masukan md5 nya

Flag : LKSSMK28{c0b7d53ada2ad6858df4ada15f40b550}

FORENSIC

Gambar2

Challenge

10 Solves

×

gambar2

250

bantu lagi tim analisis yah.

kali ini masih dengan file di gambar1.

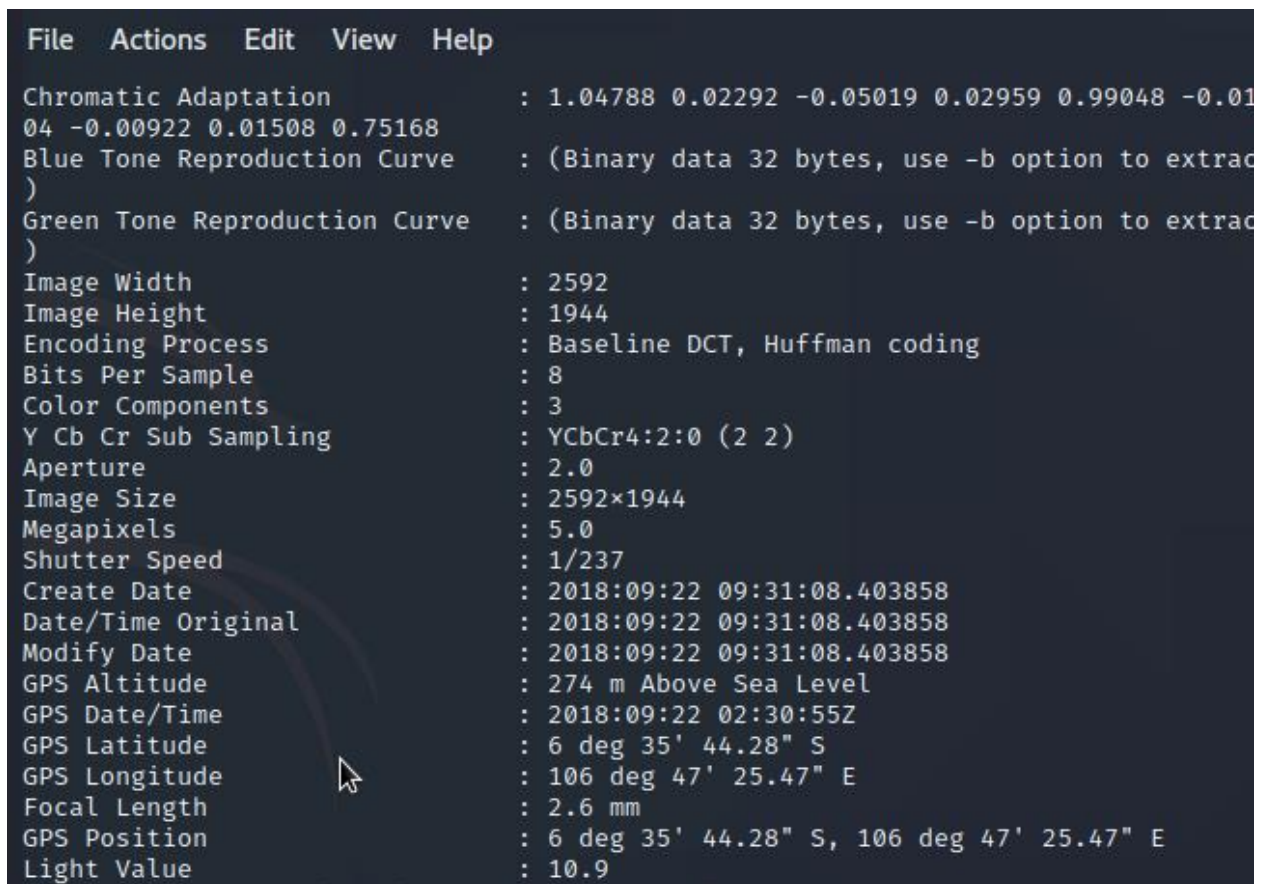
langkah selanjutnya adalah mencari tanggal berapa photo ini dibuat.

flag = {DD-MM-YYYY}

Flag

Submit

Diberikan sebuah foto yang sama seperti gambar1, untuk mencari waktu diambilnya gambar tersebut, bisa menggunakan **exiftool**



dan didapat tanggalnya yaitu 22-09-2018

LKSSMK28{22-09-2018}

Gambar3

Challenge

9 Solves



gambar3 250

masih analisis di gambar pertama

kali ini dengan mencari latitude dan longitude.

bisakah bantu tim analisis, di Kota apakah photo ini di buat.

flag=LKSSMK28{KOTA} = huruf kapital

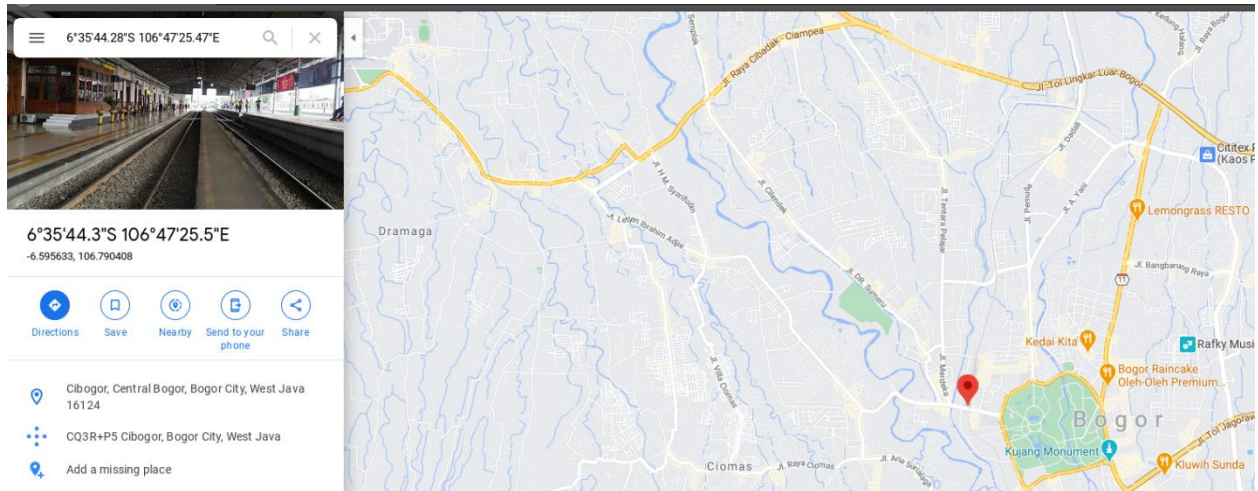
Flag

Submit

Dengan foto yang sama dengan soal sebelumnya, untuk mencari lokasi gambar tersebut didapatkan dengan sintaks **exiftool**

```
Modify Date      : 2018:09:22 09:31:08.403858
GPS Altitude     : 274 m Above Sea Level
GPS Date/Time    : 2018:09:22 02:30:55Z
GPS Latitude     : 6 deg 35' 44.28" S
GPS Longitude    : 106 deg 47' 25.47" E
Focal Length     : 2.6 mm
GPS Position     : 6 deg 35' 44.28" S, 106 deg 47' 25.47" E
Light Value      : 10.9
```

Koordinat tersebut dapat ditranslate ke dalam peta menggunakan google



Dilihat dari peta, maka dapat diketahui posisi pengambilan foto berada di kota
BOGOR

LKSSMK28{BOGOR}

MISC

URL IMAGE

Challenge

11 Solves




URL IMAGE (LKS SMK28)

250

Selain memperhatikan jenis file gambar. Para IT juga diharuskan mengecek data image dengan detail.

Format Flag : LKSSMK28{FLAG}

 image_passw...

Flag

Submit

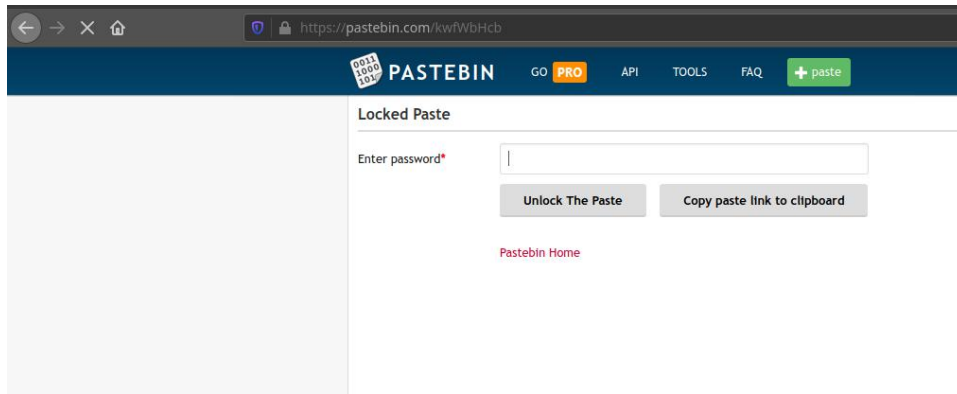
Diberikan sebuah gambar seperti berikut



Dan ketika saya membedah gambar tersebut dengan **exiftool**, ada sebuah link yang ditanamkan

```
MIME Type           : image/jpeg
JFIF Version         : 1.01
Resolution Unit      : inches
X Resolution         : 96
Y Resolution         : 96
Exif Byte Order      : Big-endian (Motorola, MM)
Copyright            : https://pastebin.com/kwfWbHcb
Padding              : (Binary data 2060 bytes, use -b option to extra
ct)
About                : uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Rights               : https://pastebin.com/kwfWbHcb
Image Width          : 1460
Image Height         : 958
Encoding Process     : Baseline DCT, Huffman coding
Bits Per Sample      : 8
Color Components     : 3
Cb Cr Sub Sampling   : YCbCr4:2:0 (2 2)
Image Size           : 1460x958
Megapixels           : 1.4
root@mfarhan-iqbal:/#
```

Saya membuka link tersebut dan mendapatkan sebuah file yang terkunci dengan password, maka saya inputkan password yang di-embed pada gambar



text	0.03 KB
1.	LKSSMK28{Hid3n_URL_onImag3}

RAW Paste Data

```
LKSSMK28{Hid3n_URL_onImag3}
```

LKSSMK28{Hid3n_URL_onImag3}

REVERSE

CRACK PDF FILE

Challenge

6 Solves



Crack PDF File (LKS SMK28)

400

hai teman-teman semua. terdapat file yang harus di crack untuk mendapatkan Flag Teliti terlebih dahulu file yang dikirim sebelum teman-teman mendapatkan file PDF untuk di crack

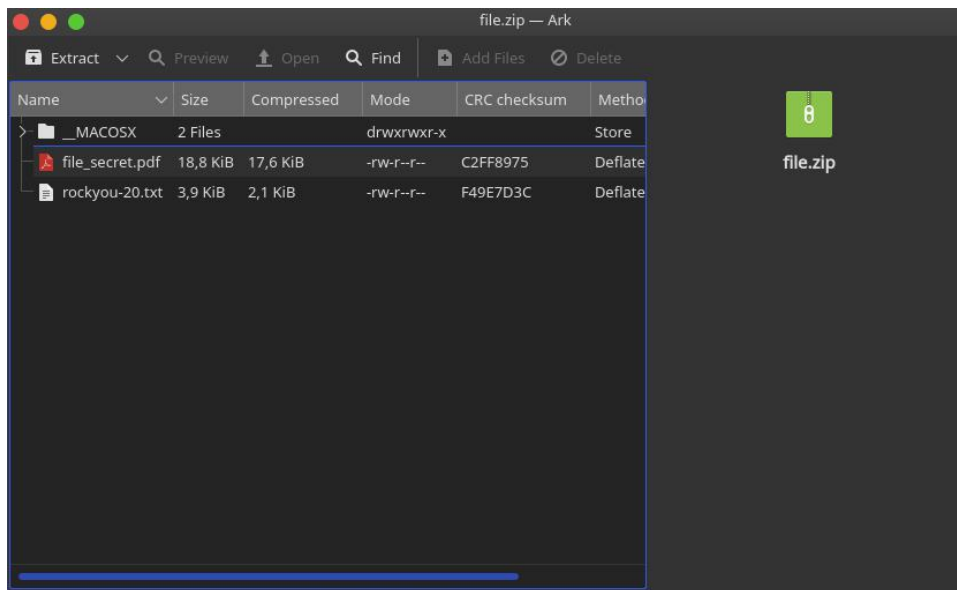
Format Flag : LKSSMK28{FLAG}

 file.exe

Flag

Submit

Diberikan file berbentuk zip yang berisi seperti berikut



Diekstraklah file tersebut dan saya mendapati file pdfnya terkunci, dan diberikan pula wordlist untuk melakukan brute, langsung saja saya scripting

```
import pikepdf
```

```
from tqdm import tqdm
```

```
passwords = [ line.strip() for line in open("rockyou-20.txt") ]
```

```
for password in tqdm(passwords, "Decrypting PDF"):
```

```
    try:
```

```
        with pikepdf.open("file_secret.pdf", password=password) as pdf:
```

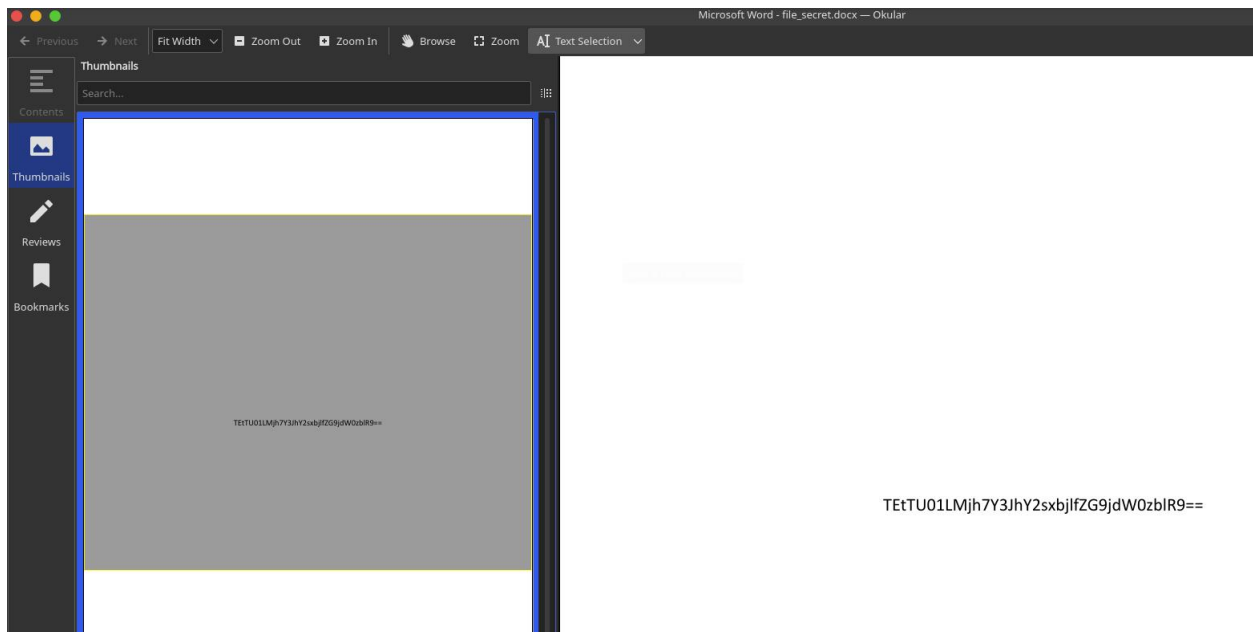
```
            print("[+] Password found:", password)
```

```
            break
```

```
        except pikepdf._qpdf.PasswordError as e:
```

```
            continue
```

Didapatkanlah passwordnya yaitu hellokitty, dan langsung dimasukkan ke file pdf



Didapatkan string yang saya rasa bukanlah flag. Karena stringnya mirip dengan base64, saya coba decode dari base64

```
File Actions Edit View Help
root@mfarhan-iqbal:/# echo "TETtU01LMjh7Y3JhY2sxbjlfZG9jdW0zblR9==" | base64 -d
LKSSMK28{crack1n9_docum3nT}base64: invalid input
root@mfarhan-iqbal:/#
```

LKSSMK28{crack1n9_docum3nT}

REVERSE1

Challenge

4 Solves



Reverse 1 (LKS SMK28) 750

Di dalam digital forensic, reversing berguna untuk menganalisis malicious file (malware atau exploit). Dapatkah Anda melakukan reverse dan mendapatkan Flag dari tantangan ini.

 reverse1

Flag

Submit

Diberikan file executable bernama **reverse1**, maka saya coba buka dengan IDA64

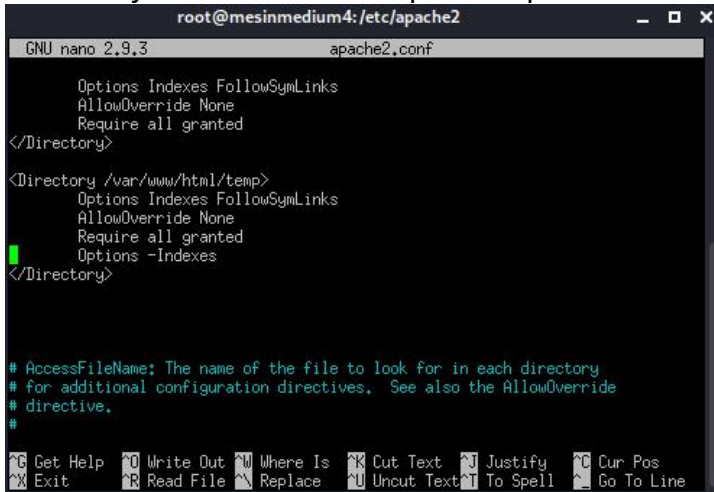
TEMPLATE LAPORAN FINAL HARDENING (LINUX) LKS - KEAMANAN SIBER 2020

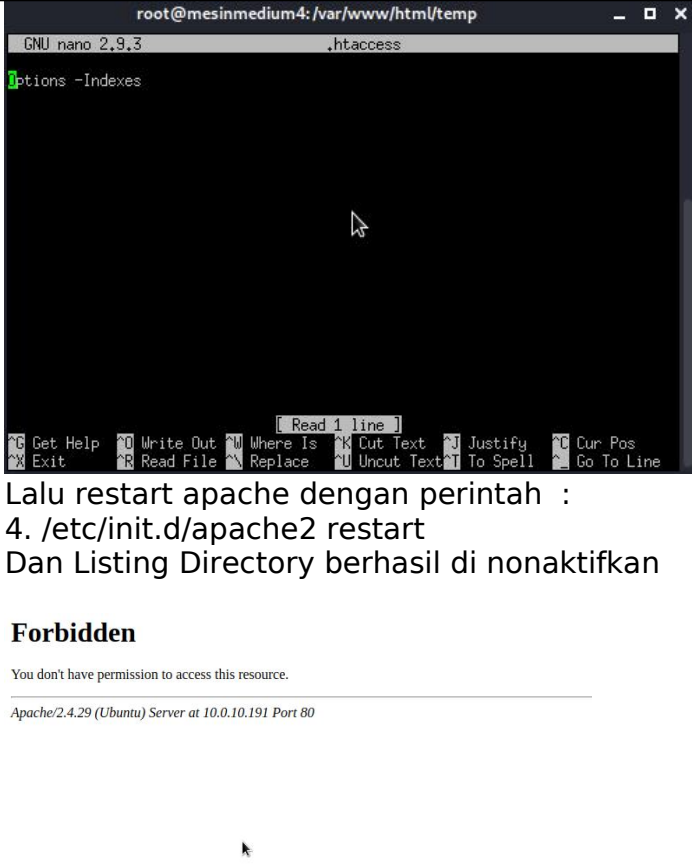
nama tim : **AJIS**

nama anggota : **Abdul Rozaqi Wildan**

Muhammad Farhan Iqbal

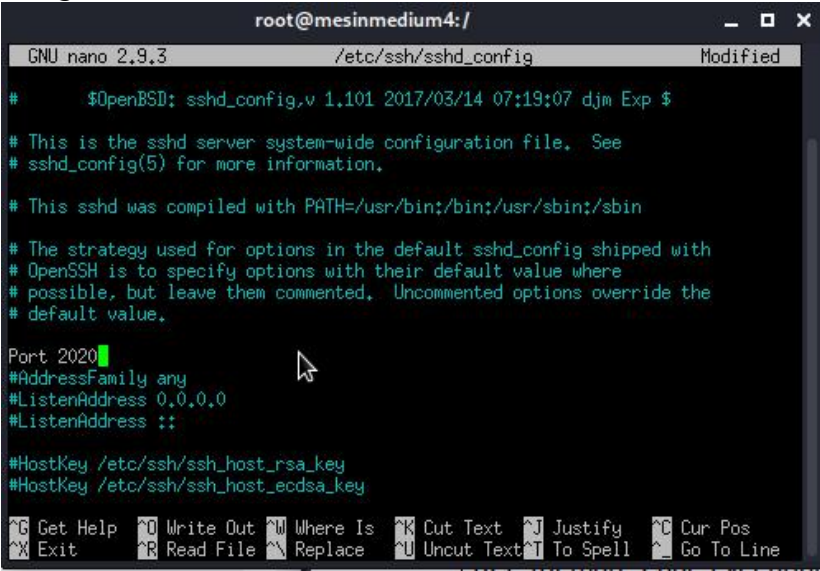
HARDENING

NO	ITEM	PENJELASAN
1	Jenis Celah Keamanan/Kesalahan Konfigurasi	Directory Listing
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/var/www/html/temp
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Di directory temp terlihat sebuah dir list yang mengakibatkan penyerang bisa melihat file yang penting pada website
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	<div>1. Caranya masuk ke /etc/apache/apache2.conf</div>  <div>2. Dan tambahkan Direktori yang temp dan masukan perintah Options -Indexes seperti gambar di atas 3. Membuat file .htaccess di dir temp dan masukan perintah Options -Indexes</div>

		 <p>Lalu restart apache dengan perintah : 4. /etc/init.d/apache2 restart Dan Listing Directory berhasil di nonaktifkan</p> <p>Forbidden</p> <p>You don't have permission to access this resource.</p> <p>Apache/2.4.29 (Ubuntu) Server at 10.0.10.191 Port 80</p>
--	--	---

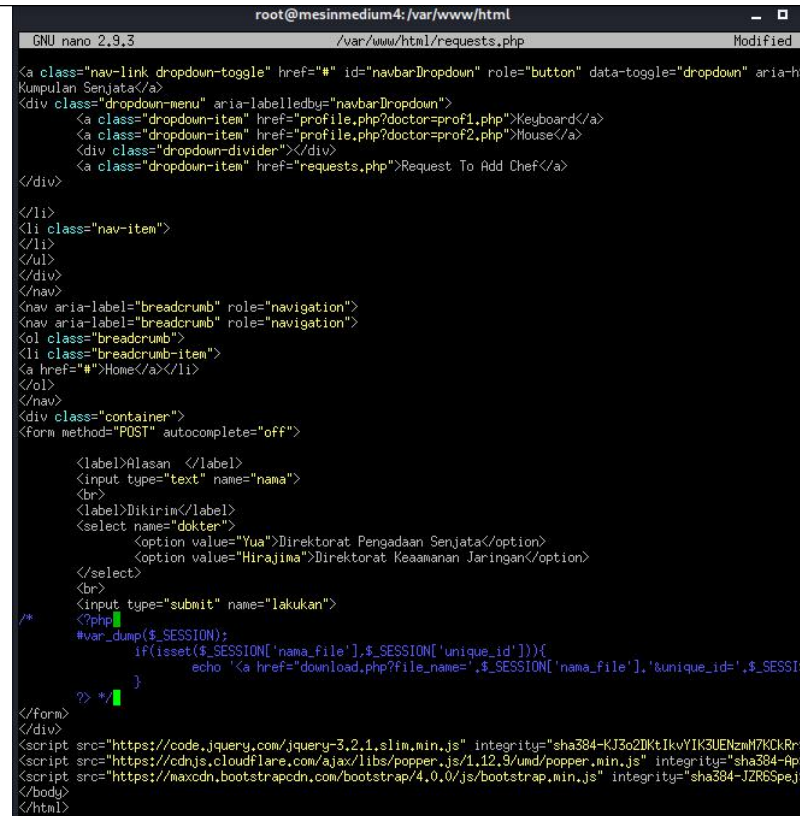
NO	ITEM	PENJELASAN
2	Jenis Celah Keamanan/Kesalahan Konfigurasi	Weak Password
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	Kelemahan password terletak pada Port SSH
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Password yang lemah mudah diserang oleh Attacker
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Sehingga password dari user maupun root harus kuat 1. Menggunakan campuran password 2. Jangan pernah menggunakan informasi pribadi 3. Gunakan password yang panjang 4. Gunakan kombinasi angka Dengan perintah di linux : passwd root

--	--	--

NO	ITEM	PENJELASAN
3	Jenis Celah Keamanan/Kesalahan Konfigurasi	Default Port SSH
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/var/www/html/temp
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	pada Linux secara default akan aktif mendengarkan pada port 22 dan karena semua orang tahu maka banyak sekali usaha brute force password root menujunya.
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	<p>1. Buka file sshd_config di direktori /etc/ssh/ dengan perintah : Nano /etc/ssh/sshd_config 2. Lalu hilangkan tanda pagar di Port dan ganti portnya dengan 2020</p>  <p>3. Lalu save dan restart dengan perintah : /etc/init.d/ssh restart</p>

		<pre> root@mesinmedium4:/ root@mesinmedium4:/# /etc/init.d/ssh restart [ok] Restarting ssh (via systemctl): ssh.service. root@mesinmedium4:/# </pre> <p>Lalu kita cek dengan nmap server dan berhasil diganti</p> <pre> rozaqi@abdu-rozaqi: ~ File Actions Edit View Help rozaqi@abdu-rozaqi:~\$ su Password: root@abdu-rozaqi:/home/rozaqi# nmap 10.0.10.191 Starting Nmap 7.80 (https://nmap.org) at 2020-10-21 12:08 WIB Stats: 0:00:09 elapsed; 0 hosts completed (0 up), 1 undergoing Ping S Parallel DNS resolution of 1 host. Timing: About 0.00% done Stats: 0:00:10 elapsed; 0 hosts completed (0 up), 1 undergoing Ping S Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 10.0.10.191 Host is up (0.063s latency). Not shown: 998 closed ports PORT STATE SERVICE 80/tcp open http 2020/tcp open xinupageserver Nmap done: 1 IP address (1 host up) scanned in 14.38 seconds root@abdu-rozaqi:/home/rozaqi# </pre>
--	--	---

NO	ITEM	PENJELASAN
4	Jenis Celah Keamanan/Kesalahan Konfigurasi	Local File Download
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/var/www/html/request.php
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Di dalam file request.php terdapat sebuah link yang dapat mendownload file penting, jika file penting ini di download oleh attacker, si attacker ini dapat mengetahui informasi token atau config, dan lain-lain.
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Menghilangkan Perintah yang dapat mendownload file dengan cara : 1. Masuk ke file request.php dan kita beri komentar seperti ini

		 <pre> root@mesinmedium4:/var/www/html GNU nano 2.9.3 /var/www/html/requests.php Modified <a class="nav-link dropdown-toggle" href="#" id="navbardropdown" role="button" data-toggle="dropdown" aria-h Kumpulan Senjata <div class="dropdown-menu" aria-labelledby="navbardropdown"> Keyboard House <div class="dropdown-divider"></div> Request To Add Chef </div> <li class="nav-item"> </div> </nav> <nav aria-label="breadcrumb" role="navigation"> <nav aria-label="breadcrumb" role="navigation"> <ol class="breadcrumb"> <li class="breadcrumb-item"> Home </nav> <div class="container"> <form method="POST" autocomplete="off"> <label>Alasan </label> <input type="text" name="nama">
 <label>Dikirim</label> <select name="dokter"> <option value="Yua">Direktorat Pengadaan Senjata</option> <option value="Hirajima">Direktorat Keamanan Jaringan</option> </select>
 <input type="submit" name="lakukan"> </div> </form> </div> <script src="https://code.jquery.com/jquery-3.2.1.slim.min.js" integrity="sha384-KJ3o2DKtIkvYIK3UENzmM7KcRn" <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity="sha384-Ap" <script src="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js" integrity="sha384-JZR6Spej" </body> </html> </pre> <p>Maka tidak ada file yang akan terdownload</p>
--	--	--

NO	ITEM	PENJELASAN
5	Jenis Celah Keamanan/Kesalahan Konfigurasi	RCE (Remote Code Execution)
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/var/www/html/class.php
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Di dalam file /var/www/html/class.php memiliki fungsi passthru() yang parameternya diambil di metode GET dan tidak memiliki filtering, sehingga attacker dapat memasukkan perintah lainnya yang akan dieksekusi pada sisi server
	Mitigasi/Solusi yang telah dilakukan. Jelaskan	Membatasi agar fungsi passthru() dalam file /var/www/html/class.php (pada baris 4) hanya bisa

	<p>secara rinci step by step (jangan dalam bentuk narasi)</p>	<p>menjalankan satu perintah tertentu (hard coded dalam baris baris pemrograman) seperti di bawah ini:</p> <pre><?php \$cmd = \$_GET['cmd']; \$cmd = 'ls'; echo passthru(\$cmd);</pre> <p>Cara lain yang bisa dilakukan adalah menonaktifkan fungsi passthru() melalui konfigurasi php.ini seperti di bawah ini:</p> <p>Disable_functions = passthru</p>
--	---	---

Contoh Lain template HARDENING:

NO	ITEM	PENJELASAN
6	Jenis Celah Keamanan/Kesalahan Konfigurasi	SSH
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/root/.ssh/authorized_keys, /root/KEYS/root.pem
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Berkas root.pem dapat digunakan oleh attacker untuk melakukan SSH ke server tanpa harus menggunakan password. Hal ini dapat dibuktikan bahwa public key sudah terpasang pada berkas /root/.ssh/authorized_keys
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Mitigasi yang telah dilakukan antara lain: Menghapus berkas /root/KEYS/root.pem Menghapus berkas /root/.ssh/authorized_keys Membuat ulang SSH Key dengan menggunakan perintah ssh-key

Laporan Attack :

1. Untuk server sendiri tinggal masuk ke terminal kali [ssh messi@10.0.10.191](ssh:10.0.10.191) dan masukkan password user {USER}.

```
messi@mesinmedium4: /home/flag
File Actions Edit View Help
messi@mesinmedium4:/home/flag$ ls
flag.txt
messi@mesinmedium4:/home/flag$ cat flag.txt
LKSSMK28{799e4b07faec485cacb09388823ce2ab}
messi@mesinmedium4:/home/flag$
```

Flag : LKSSMK28{799e4b07faec485cacb09388823ce2ab}

Untuk yang root masuk su dan masukan password root :

```
root@mesinmedium4: ~
File Actions Edit View Help
messi@mesinmedium4:/home/flag$ su
Password:
root@mesinmedium4:/home/flag# ls
flag.txt
root@mesinmedium4:/home/flag# cd /root/
root@mesinmedium4:~# ls
root.txt
root@mesinmedium4:~# cat root.txt
LKSSMK28{338d811d532553557ca33be45b6bde55}
root@mesinmedium4:~#
```

Flag : LKSSMK28{338d811d532553557ca33be45b6bde55}

2. Untuk Server lawan masuk ke ssh lawan yang SMK Negeri 3 Lampung dan masuk menggunakan user mane dan password default.

```
rozaqi@abdu-rozaqi: ~  
File Actions Edit View Help  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
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.  
  
Last login: Wed Oct 21 06:46:13 2020 from 10.0.10.83  
Could not chdir to home directory /home/mane: No such file or directory  
$ ls  
bin      etc      lib      mnt      run      swap.img  var  
boot     home     lib64    opt      sbin     sys       vmlinuz  
cdrom    initrd.img  lost+found  proc    snap     tmp       vmlinuz.old  
dev      initrd.img.old  media      root    srv      usr  
$ cd home  
$ ls  
flag messi  
$ cd flag  
$ ls  
flag.txt  
$ cat flag.txt  
LKSSMK28{7e475036d69fe4a87659d3423702182f}  
$
```

3. Untuk Server lawan masuk ke ssh lawan yang root dan masukan password default dan dapet flagnya :

LKSSMK28{d12b9d374f1868cbcaa2879c89fd8487}

4. Untuk Server lawan masuk ke ssh lawan yang root dan masukan password default dan dapet flagnya :

```
bale@bale: ~  
File Actions Edit View Help  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
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.  
  
Last login: Wed Oct 21 06:38:37 2020 from 10.0.10.83  
Could not chdir to home directory /home/mane: No such file or directory  
$ ls  
bin      etc      lib      mnt      run      swap.img  var  
boot     home     lib64    opt      sbin     sys       vmlinuz  
cdrom    initrd.img  lost+found  proc    snap     tmp       vmlinuz.old  
dev      initrd.img.old  media      root    srv      usr  
$ cd home  
$ ls  
flag messi  
$ cd flag  
$ ls  
flag.txt  
$ cat flag.txt  
LKSSMK28{9387a9c1bd92239372e8149e2c48ad16}  
$
```


HARDENING WINDOWS 7

NAMA TIM	AJIS
KETUA	Abdul Rozaqi Wildan
ANGGOTA	Muhammad Farhan Iqbal

1. Security banner (Windows machines)

Challenge : On random windows machine go to login screen
<p>Windows 7 mempunyai fitur untuk menambahkan pesan yang ditampilkan di layar saat pengguna masuk.</p> <p>Untuk memberikan pesan bagi pengguna yang masuk ke komputer Windows 7 yang akan masuk/login. Pesan tersebut bersifat informatif dan tidak memberikan keamanan yang sebenarnya.</p>

Buatlah Security Banner Pesan sebelum login ke Komputer Windows 7

Answer

Tulis Jawaban Langkah-langkah pengerjaan

1. Membuka gpedit.msc
2. Buka Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Option
3. Terdapat 2 file untuk banner pada Interactive logon : Message text for users attempting logon dan Message title for users attempting logon

Message text for users attempting logon : Text pada banner

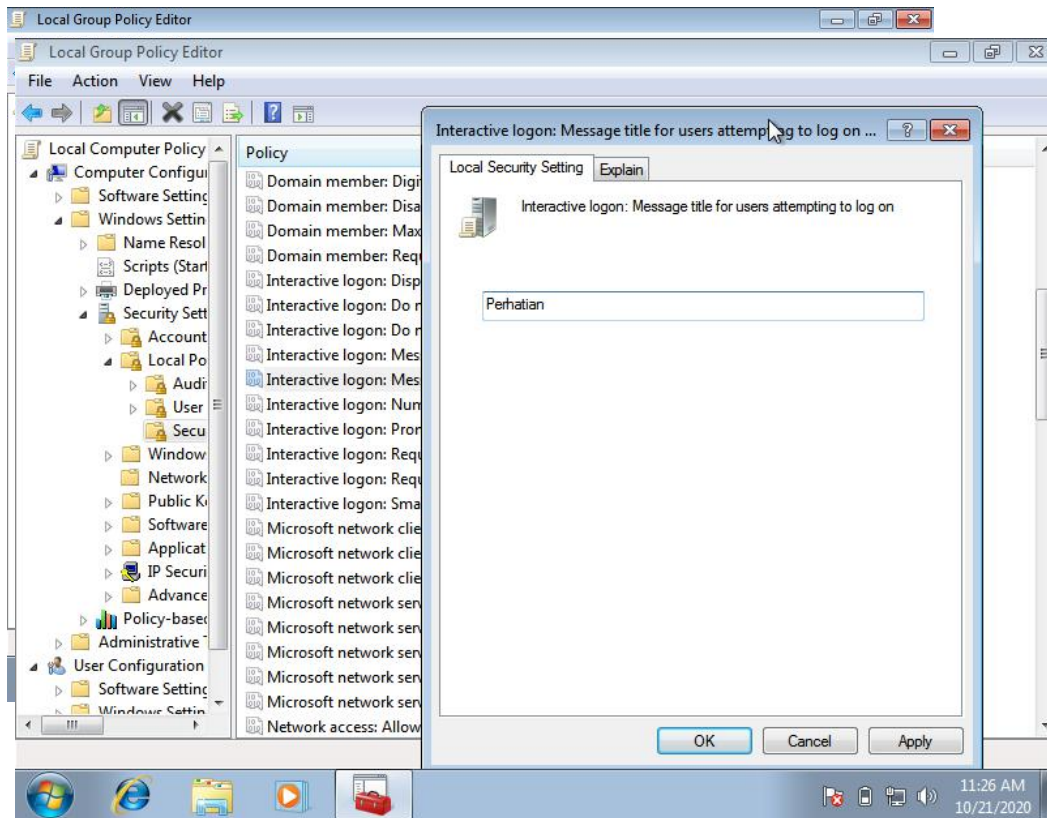
Message title for users attempting logon : Title pada banner

4. Kami mengedit file text dengan PC ini hanya digunakan oleh bagian Sales!
5. File title : Perhatian
6. Merestart windows untuk melihat banner yang telah diubah

ScrenShoot

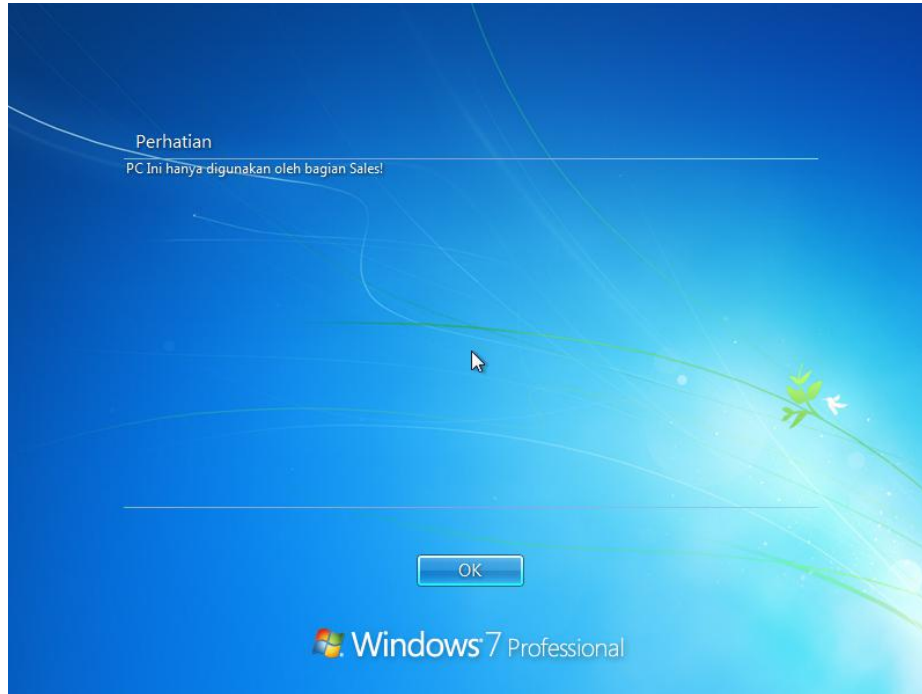
Masukan screenshot penyelesaian

1. Lokasi banner Windows 7

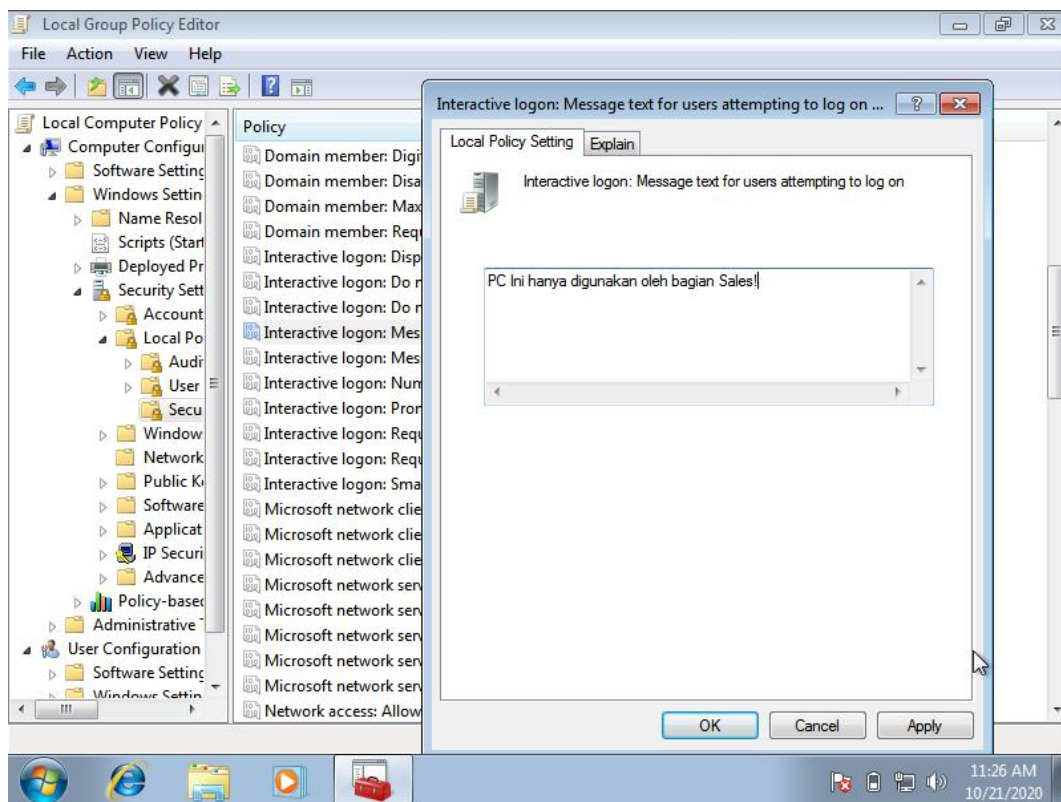


2. edit title screen

3. edit text screen
4. Login ke Windows 7



- 5.



2. Password minimum length (Windows machines)

Challenge : Pick random preconfigured account, change password to random one with length of 8 (which meets complexity requirements)

Windows 7 mempunyai Security Police yang mengatur setiap user membuat password dengan minimal berapa karakter.

Di Challenge nomor 2 para peserta membuat kebijakan setiap password untuk user di Windows 7 diharuskan memasukan password dengan 8 karakter.

Answer

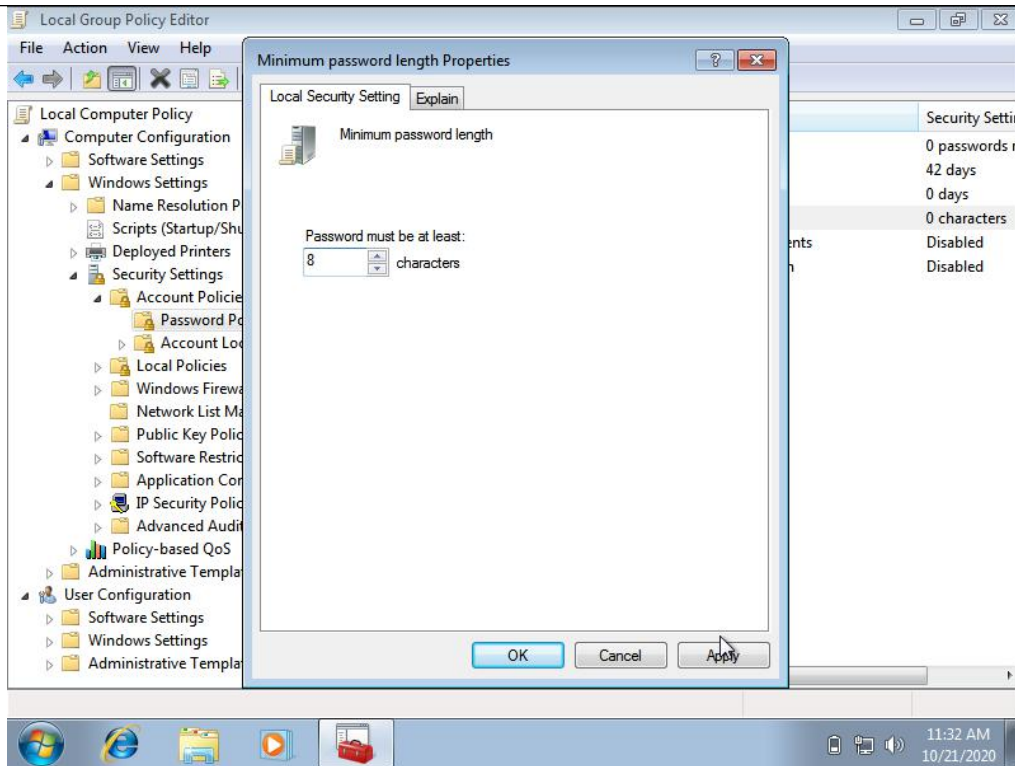
Tulis Jawaban Langkah-langkah pengerjaan

1. Membuka gpedit.msc
2. Buka Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy
3. mengedit file Minimum password length diisi menjadi 8 characters

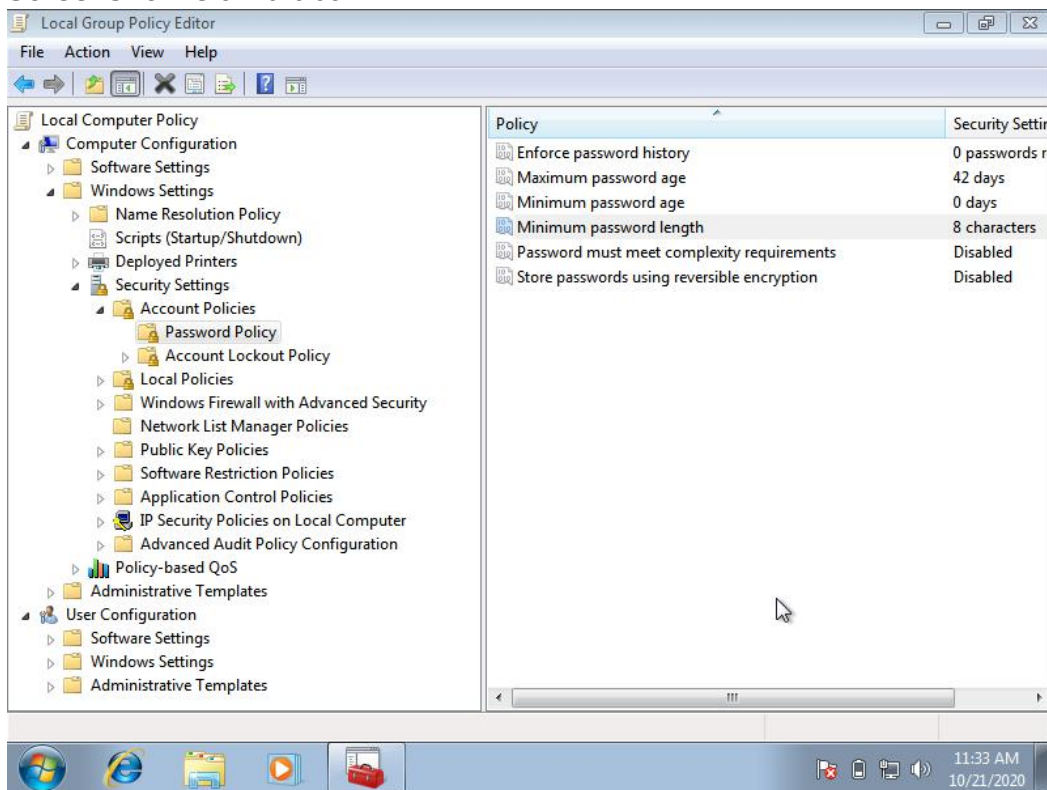
ScrenShoot

Masukan screenshot penyelesaian

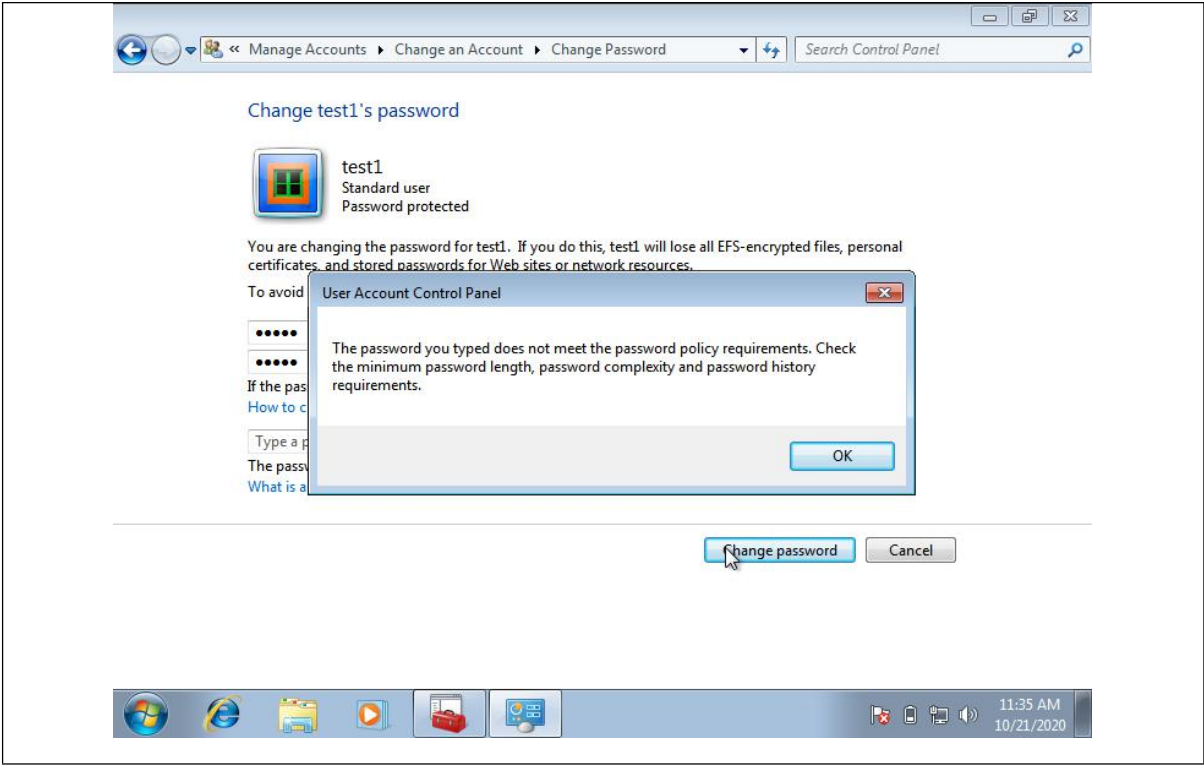
1. Mengedit Password length



2. Screenshot telah diubah



3. Hasil gagal saat user mengubah password kurang dari 8 karakter



3. Password complexity (Windows machines)

Challenge : Pick random preconfigured account, change password to random one with length of 8 (which meets complexity requirements)

Challenge no 3 adalah mengaktifkan fitur complexity requirements di Windows 7.

Pengaturan keamanan ini menentukan apakah kata sandi harus memenuhi persyaratan kompleksitas.

Jika kebijakan ini diaktifkan, kata sandi harus memenuhi persyaratan minimum berikut:

- Tidak mengandung nama akun pengguna atau bagian dari nama lengkap pengguna yang melebihi dua karakter berturut-turut
- Panjangnya setidaknya delapan karakter
- Berisi karakter dari tiga dari empat kategori berikut:
 - Huruf besar Bahasa Inggris (A sampai Z)
 - Huruf kecil Bahasa Inggris (a hingga z)
 - Basis 10 digit (0 hingga 9)

Karakter non-alfabet (misalnya,!, \$, #,%)

Answer

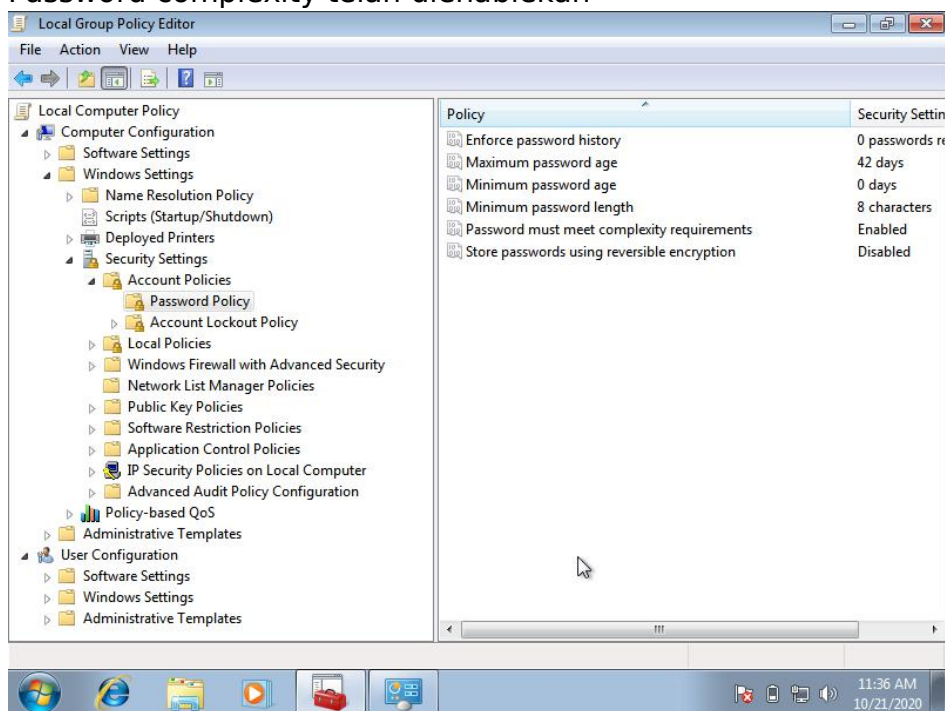
Tulis Jawaban Langkah-langkah pengerjaan

1. Membuka gpedit.msc
2. Buka Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy
3. mengedit file password must meet complexity requirements
4. menenablekan file

ScrenShoot

Masukan screenshot penyelesaian

1. Password complexity telah dienablekan



2. User mengganti password dengan smkbisa2020. Hasilnya tak dapat diubah karena tak memenuhi syarat

Change test1's password



test1
Standard user
Password protected

You are changing the password for test1. If you do this, test1 will lose all EFS-encrypted files, personal certificates, and stored passwords for Web sites or network resources.

To avoid

.....
.....

If the pas

How to c

Type a p

The passw

What is a

User Account Control Panel

The password you typed does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.

OK

Change password

Cancel

4. Cached logins (Windows machines)

Challenge : On random windows client machine - login with random account, logoff, shutdown vNIC, try to login again with the same account

Chaced Login ke computer Windows 7 kredensial akun tersimpan di cached Login system dari Windows 7.

Data cache disimpan dalam kunci registri HKLM\ SECURITY\Cache, yang hanya dapat diakses oleh akun SYSTEM. Penting juga untuk menyebutkan bahwa masa cache ini di komputer tidak terbatas.

Setting Security di cached login Windows 7 yang hanya memperbolehkan user yang terakhir yang hanya dapat login ke dalam Windows 7.

Secara teori, jika ada akses fisik ke komputer, penyerang memiliki kesempatan untuk menggunakan kredensial yang disimpan, disarankan untuk menonaktifkan cache lokal untuk keamanan yang lebih baik.

Setting Logons cached yang disimpan diatur ke nilai value 1.

Ini memungkinkan hanya pengguna terakhir untuk masuk ke sistem.

Answer

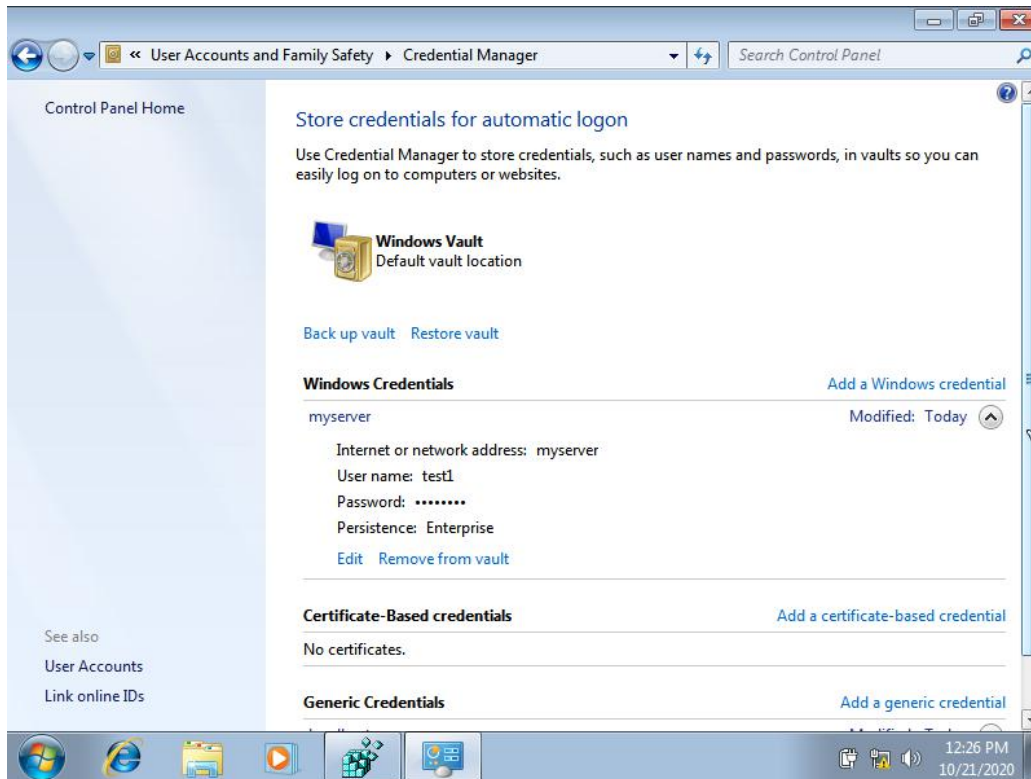
Tulis Jawaban Langkah-langkah pengerjaan

1. Membuat cache credential pada control panel > user >
2. Mengubah value cachedlogons pada regedit
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS
NT\CURRENTVERSION\WINLOGOON\

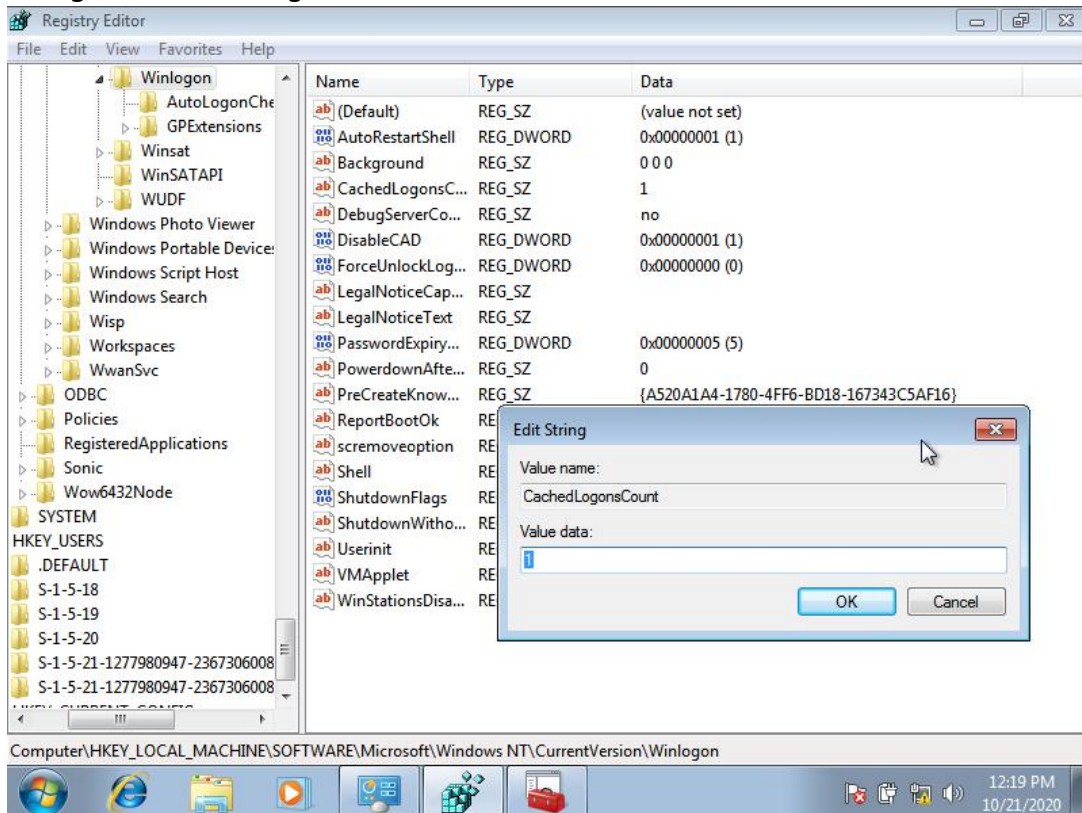
ScrenShoot

Masukan screenshot penyelesaian

1. Membuat cache



2. Mengubah value logons



3.

5. Account lockdown (Windows machines)

Challenge : On random windows machine - try to login 3 times with incorrect password

Untuk menghindari serangan Brute Force pada akun windows 7 berilah security pada menu login user.

Gunakan security jika salah memasukan password sebanyak 3 kali user akan diblok selama 1 menit.

Answer

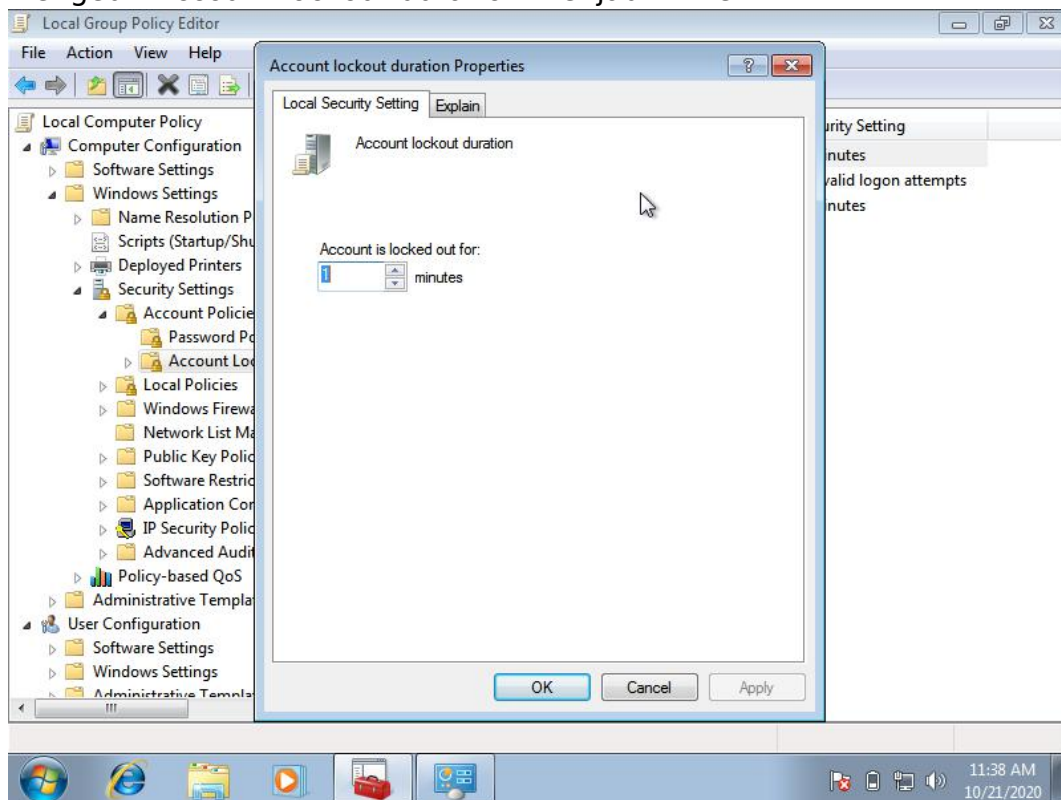
Tulis Jawaban Langkah-langkah pengerjaan

1. Membuka gpedit.msc
 2. Computer Configuration > Windows Settings > Security Settings > Account Policies > Account lockout Policy
 3. Mengedit file Account lockout duration dan Account lockout threshold
- Account lockout duration : 1 minutes
Account lockout threshold : 3 invalid logon attempts

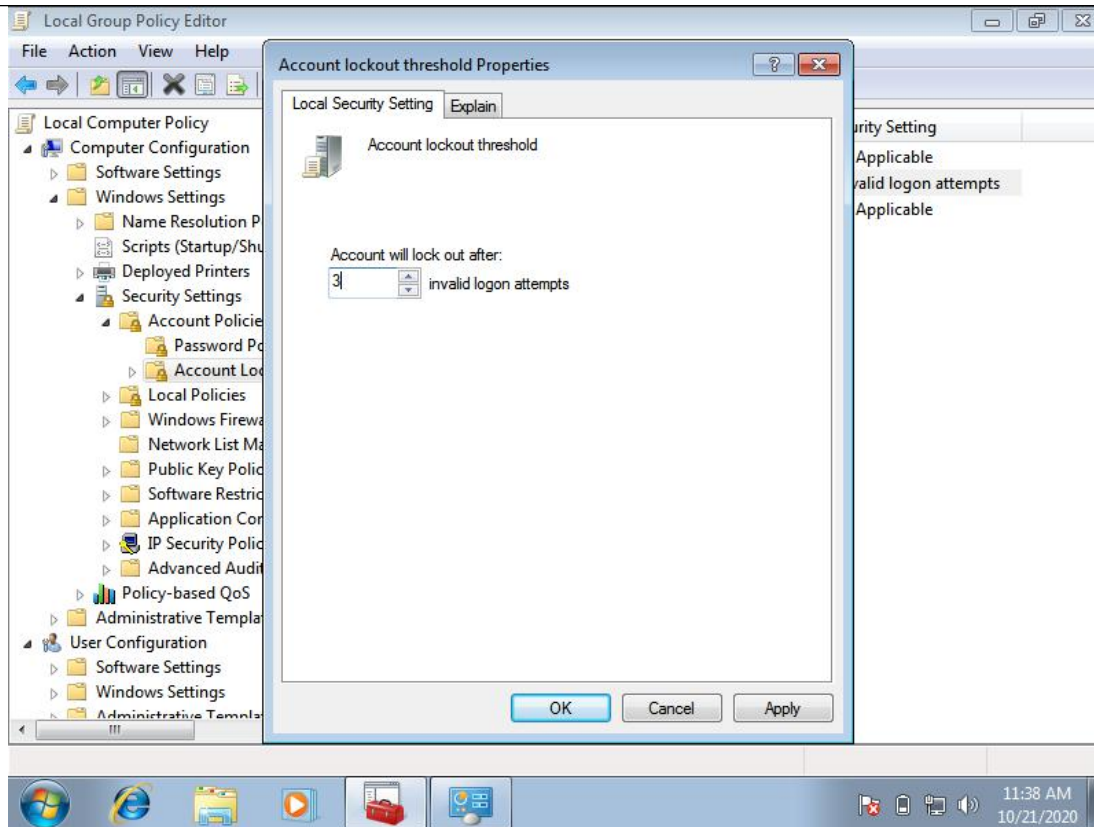
ScrenShoot

Masukan screenshot penyelesaian

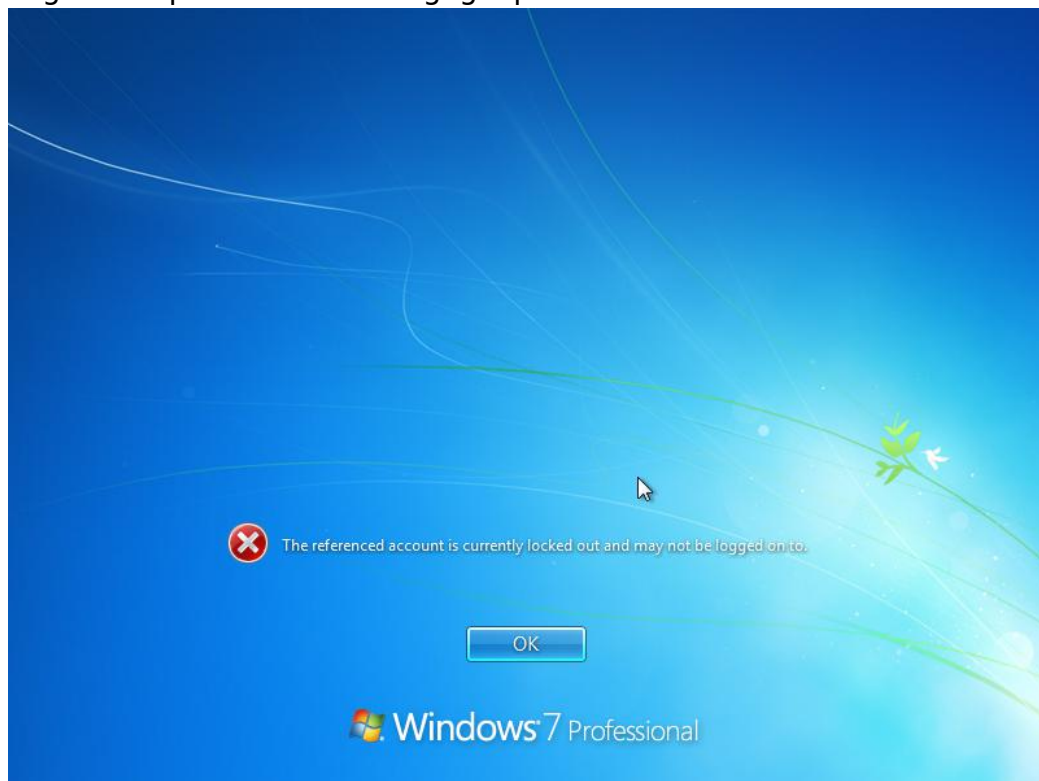
1. Mengedit Account lockout duration menjadi 1 menit



2. Mengedit Account lockout threshold menjadi 3 kali percobaan



3. Login saat percobaan 3 kali gagal pada akun test



4.

6. Inactivity timeout (Windows machines)

Challenge : On random windows machine login and wait for 1 min

Pada challenge No 6 disini peserta diharuskan membuat setting security pada Windows 7

Jika selama 1 menit tidak ada aktifitas di Windows 7 akan otomatis terkunci/lock.

Untuk masuk Kembali ke Windows 7 diharuskan untuk Login Kembali dengan user yang aktif.

Answer

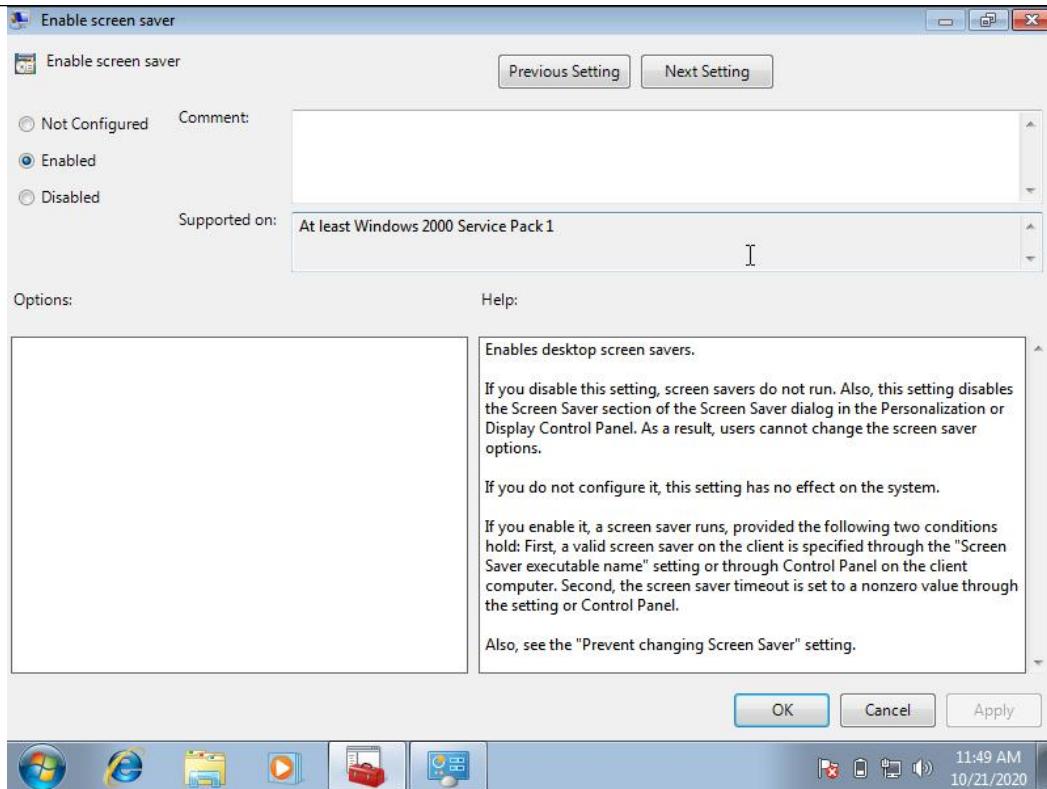
Tulis Jawaban Langkah-langkah pengerjaan

1. Membuka gpedit.msc
2. User Configuration Administrative Templates > Control panel > Personalitation
3. Mengedit Enable screen saver
4. Mengedit Screen saver timeout

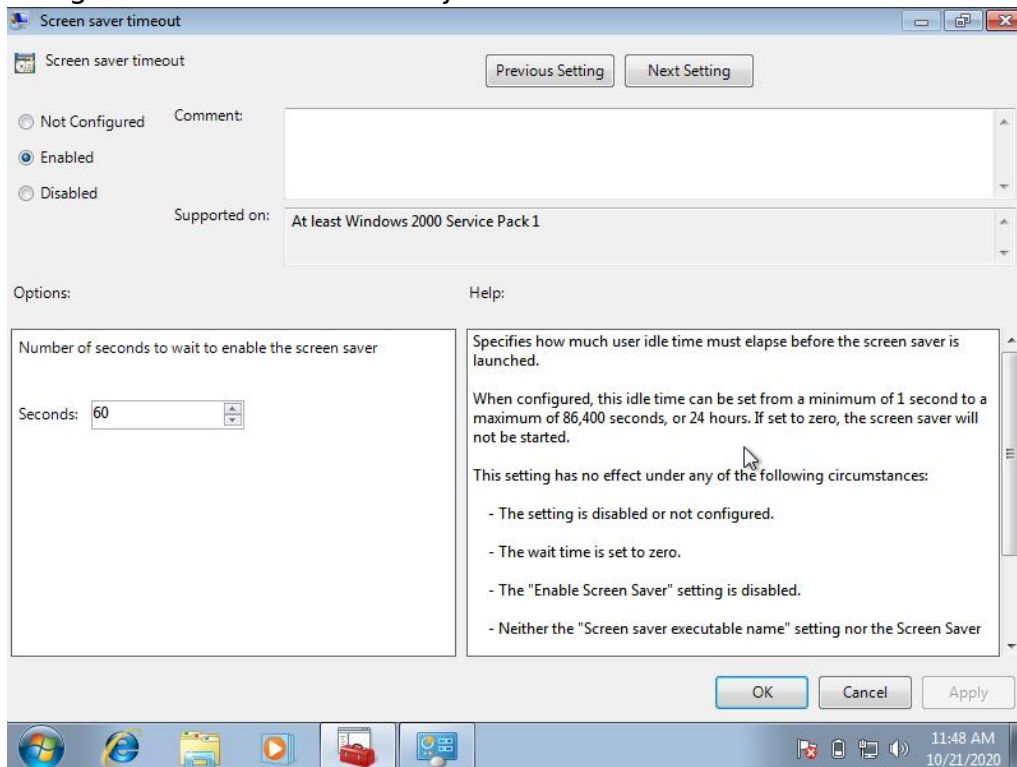
ScrenShoot

Masukan screenshot penyelesaian

1. Menenablekan screen saver



2. Mengatur waktu timeout menjadi 60 detik



3.

--