



Capture The Flags

NAMA TIM	VHS_CyberTech - SMK Negeri 22 Jakarta
KETUA	Andi Syahrudin
ANGGOTA	Muhamat Anwar Dwi Yanto

MISC

Challenge : QRCOD3

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}

Answer

Diberikan sebuah file Qrcode. yang pertama saya lakukan adalah mendecode file qrcode tersebut dengan bantuan website setelah itu didapatkan raw text binary. Raw text binary itu

```
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
```

Setelah didapat Raw binary tersebut, dilakukanlah binary decode

Keamanan komputer atau dikenal juga dengan sebutan cybersecurity atau IT security adalah keamanan informasi yang diaplikasikan kepada komputer dan jaringannya. Keamanan komputer bertujuan membantu pengguna LKSSMK28{IT_s3cuR1Ty_2020} agar dapat mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem yang @

FLAG: LKSSMK28{IT_s3cuR1Ty_2020}

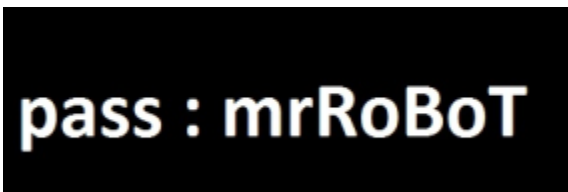
Challenge : URL IMAGE

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

Format Flag : LKSSMK28{FLAG}

Answer

Diberikan sebuah gambar, disana kita suruh memecahkan hal rahasia yang terdapat pada image tersebut. Yang pertama kami lakukan membuka gambar tersebut dan terlihat ada kata pass



Setelah kami meneliti gambar lagi dengan menggunakan command **exiftool** ditemukan keanehan pada informasi copyright yang berisikan link

Copyright : <https://pastebin.com/kwfWbHcb>

Setelah informasi sudah cukup kami buka link tersebut dan ditemukan flag

FLAG: LKSSMK28{Hid3n_URL_onImag3}

WEB

Challenge : PSWEB

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

Link: <http://202.148.27.84/psweb/>

Answer

Diberikan sebuah link website dan berupa hint yaitu *bagaimana cara melihat source code*, maka dari itu kami membuka source code dari website tersebut dan mencari flagnya, flag tersebut berada di file *amber.css*

```
float: left;
margin-top: 24px;
margin-left: 260px;
}
/* Flag : LKSSMK28{Mr_r0b0t_E03} */
#upcoming-101b {
width: 300px;
color: #CCCCCC;
font-family: "Trebuchet MS", verdana,
```

Flag : LKSSMK28{Mr_r0b0t_E03}

Challenge : Bypass Administrator

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

Link: <http://202.148.27.84:10002/>

Answer

Diberikan sebuah link website dan berupa hint yaitu bagaimana anda sebagai *administrator*, setelah dilakukan percobaan ada hint

Login successful!

Setting cookie: `auth=username=guest&date=2020-10-21T09:43:06+0000&`

Click [here](#) to continue!

Setelah itu kami mencoba bypass cookie dengan mengganti username dengan administrator dan mendapatkan flag

Welcome administrator!

Congratulations!

`LKSSMK28{3e671ea34dcac32e7e9e7c67ee8cfc0b}`

[Log out](#)

Flag : `LKSSMK28{3e671ea34dcac32e7e9e7c67ee8cfc0b}`

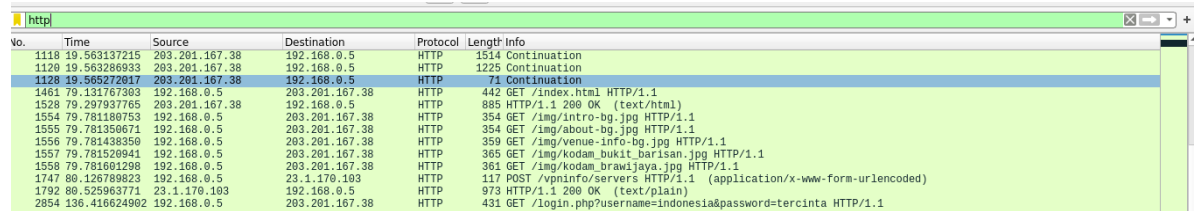
Challenge : Web Login

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

<http://202.148.27.84:10009/>

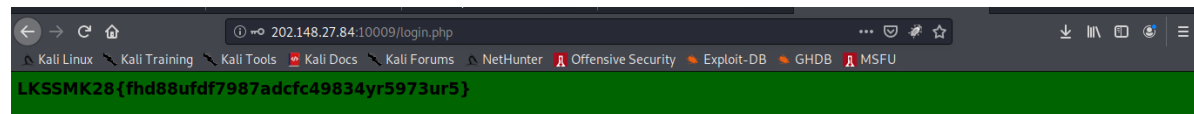
Answer

Diberikan sebuah link website dan file pcap (file wireshark) setelah itu kami melakukan exploit terhadap file pcap menggunakan aplikasi wireshark dan ditemukan username yaitu **indonesia** dan **tercinta**



No.	Time	Source	Destination	Protocol	Length	Info
1118	19.563137215	203.201.167.38	192.168.0.5	HTTP	1514	Continuation
1120	19.563286933	203.201.167.38	192.168.0.5	HTTP	1225	Continuation
1128	19.565272917	203.201.167.38	192.168.0.5	HTTP	71	Continuation
1461	79.131767393	192.168.0.5	203.201.167.38	HTTP	442	GET /index.html HTTP/1.1
1528	79.297937765	203.201.167.38	192.168.0.5	HTTP	885	HTTP/1.1 200 OK (text/html)
1554	79.781180753	192.168.0.5	203.201.167.38	HTTP	354	GET /img/intro-bg.jpg HTTP/1.1
1555	79.781350671	192.168.0.5	203.201.167.38	HTTP	354	GET /img/about-bg.jpg HTTP/1.1
1556	79.781438350	192.168.0.5	203.201.167.38	HTTP	359	GET /img/venue-info-bg.jpg HTTP/1.1
1557	79.781520941	192.168.0.5	203.201.167.38	HTTP	365	GET /img/kodam_bukit_barisan.jpg HTTP/1.1
1558	79.781601298	192.168.0.5	203.201.167.38	HTTP	361	GET /img/kodam_brawijaya.jpg HTTP/1.1
1747	80.126799823	192.168.0.5	23.1.170.193	HTTP	117	POST /vpninfo/servers HTTP/1.1 (application/x-www-form-urlencoded)
1792	80.525963771	23.1.170.193	192.168.0.5	HTTP	973	HTTP/1.1 200 OK (text/plain)
2854	136.416624902	192.168.0.5	203.201.167.38	HTTP	431	GET /login.php?username=indonesia&password=tercinta HTTP/1.1

Dan saya mencoba login dengan username dan password tersebut dan ditemukan file



Flag : LKSSMK28{fhd88ufdf7987adcf49834yr5973ur5}

Challenge : Remote Code Execution

Panjang command yang diperbolehkan hanya 11 karakter saja.

Link: <http://202.148.27.84:10007/>

Answer

Diberikan sebuah link website dan judul soal yang mengarah ke exploit, setelah itu kami mencoba beberapa command dan hasil null, tidak ada sama kami mencoba hal lain dengan menggunakan beberapa function yang ada di php salah satunya function system, kami coba command tersebut **system(ls)**

flag_gfshgRYTRYRTYSGS74rhf index.php logo.jpg

Submit

Setelah itu kami mengakses file tersebut dengan link
http://202.148.27.84:10007/flag_gfshgRYTRYRTYSGS74rhf

FLAG: LKSSMK28{eb0ccf7987adcfc4a08b10db23d62da9}

Revers Engineering

Challenge : Simple Brain Encrypt

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

Format Flag : LKSSMK28{FLAG}

Answer

Diberikan sebuah Document tentang spoiler warning, ada beberapa petunjuk

1. Baca Dengan Teliti
2. Kata Simple Brain yang bertuju ke hash pada brainfuck

Setelah saya baca dengan teliti ada sebuah link yang bertuju ke pastebin dan link

Elliot yang hampir menguasai segala sesuatu mengenai jaringan internet bahkan dengan semua arsitektur tertanam yang menggunakan jaringan internet pastebin.com/TzcBcjg3 untuk beroperasi membuatnya menjadi salah satu orang paling ditakuti sekaligus paling lemah karena kejiwaannya yang tidak stabil.

tersebut saya buka dan muncul encrypt brainfuck

```
-[----->+<]>+++.-.+++++++..-----.-.[--->+<]>.+++++.-[--->+<]>+.[--->+<]>+.-----  
.++++.+++.-.-[--->+<]>+.-[->+<]>-.+++++.+++++.-.-----[->+++++<]>.[--  
>++++<]>--.-[--->+<]>..++++..[->++++<]>.-.
```

Setelah itu saya decrypt atau decode dengan bantuan website

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

FLAG: LKSSMK28{SIMPL3_encRyPPTT}

Challenge : SimPle Encrypt

Gabungkan Enkripsi di bawah ini :

TEtTU01LMjh7Y mFzZTY0X0VuY3 J5cHQxMDBufQ==

Format Flag : LKSSMK28{FLAG}

Answer

Diberikan suatu kata encrypt yang harus kita pecahkan, pertama yang harus kita lakukan adalah menganalisis kata tersebut dan ketika sudah dianalisis kata tersebut adalah encrypt base64, cara menyelesaikannya dengan satu command yaitu

```
Echo "TEtTU01LMjh7YmFzZTY0X0VuY3J5cHQxMDBufQ==" | base64 -d
```

FLAG : LKSSMK28{base64_Encrypt100n}

Challenge : Crack PDF File

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

Answer

Diberikan sebuah file dengan extension executable, yang pertama kita lakukan adalah menganalisis file tersebut dengan command

```
root@me:~/Downloads# file file.exe
file.exe: Zip archive data, at least v2.0 to extract
```

Ternyata bukan file executable setelah itu kami extract file tersebut dengan command **unzip file.exe**

Ada file pdf yang harus dicrack dan wordlist maka dari itu kami mengambil kesimpulan bahwa kami bias membrute force dengan cara

```
/usr/share/john/pdf2john.pl files_secret.pdf > pdf.hash
```

```
John pdf.hash --wordlist=rockyou-20.txt
```

Dan didapatkan password hellokitty, untuk membuka file_secret.pdf tersebut

TEtTU01LMjh7Y3JhY2sxbjlfZG9jdW0zblR9==

decrypt kata tersebut menggunakan decrypt base64 dan didapatkan flag

FLAG: LKSSMK28{crack1n9_docum3nT}

Challenge : Reverse 1

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

Answer

Diberikan sebuah file executable, disana saya disuruh untuk mereverse application tersebut, yang pertama saya lakukan adalah mereverse file dengan ghidra tool

Dan ditemukan function strcmp

```
local_c = strcmp(local_118, local_155);
```

Saya mencoba menggunakan tools ltrace yang berfungsi untuk melakukan tracing terhadap pemanggilan **fungsi** dari library.

```
strcat("k0opi_h", "ita")
strcat("k0opi_hita", "m_pht")
strcmp("asd", "k0opi_hitam_pht")
```

dimasukan password tersebut dan ditemukan flag

FLAG: LKSSMK28{01c9fsd3gt34zxxcb0eb8a42d3c534rf3c570703e3t}

FORENSIC

Challenge : File Signature

tim analisa menemukan sebuah file yang mencurigakan, diperkirakan file ini extention nya diganti dan ada data yang hilang di file signature nya.

bisakah kalian membantu tim analis untuk membetulkan file tersebut

Answer

Diberikan file dengan banyak extension, yang pertama kami lakukan lah adalah apakah file tersebut benar dengan command **file flag.jpg.exe.doc.rar**

```
root@me:~/Downloads# file flag.jpg.exe.doc.rar
flag.jpg.exe.doc.rar: RAR archive data, v5
```

Setelah itu file tersebut saya extrack dan muncul file baru dengan nama flag.jpg.exe.doc.pdf

```
root@me:~/Downloads# file flag.jpg.exe.doc.pdf
flag.jpg.exe.doc.pdf: data
```

Mungkin dicheck type file tersebut adalah data saya tidak percaya saya check kembali header nya dengan command xxd

```
root@me:~/Downloads# xxd -l 12 flag.jpg.exe.doc.pdf
00000000: 0000 0000 0010 4a46 4946 0001          .....JFIF..
```

Ada kesalahan di hex header tersebut, maka dari saya membenarkan header hex tersebut dengan bantuan Wikipedia, setelah sudah di benarkan maka didapatkan flag

flag = Yuu-kita-ke-jakarta

FLAG: LKSSMK28{Yuu-kita-ke-jakarta}

Challenge : gambar1

tim analisis sedang menganalisis / forensic sebuah file gambar.

langkah pertama bantu analisis dengan menemukan hash MD5 gambar tersebut.

flag = LKSSMK28{MD5}

Answer

FLAG: LKSSMK28{Yuu-kita-ke-jakarta} Menggunakan md5sum files

```
root@kali:~/Downloads# md5sum 2018-09-22_09.31.07.jpg
c0b7d53ada2ad6858df4ada15f40b550 2018-09-22_09.31.07.jpg
root@kali:~/Downloads#
```

Jadi tinggal isi aja c0b7d53ada2ad6858df4ada15f40b550

Flag= LKSSMK28{c0b7d53ada2ad6858df4ada15f40b550}

Challenge : gambar2

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}

Answer

Menggunakan exiftool nama files

```
: 2018:09:22
```

Jadi kita tinggal ganti jadi 22-09-2018

Flag= LKSSMK28={22-09-2018}

Challenge : gambar3

masih analisis di gambar pertama

kali ini dengan mencari latitude dan longitude.

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

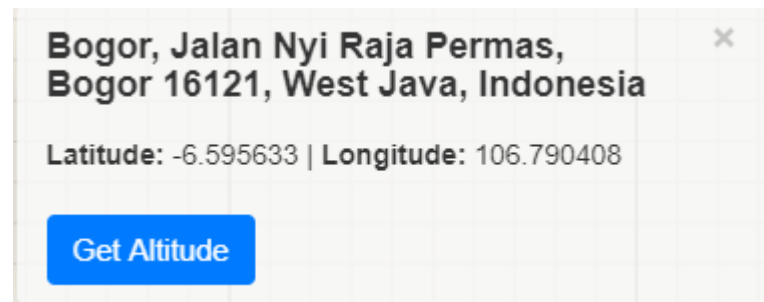
flag=LKSSMK28{KOTA} = huruf kapital

Answer

Menggunakan exiftools nama files

```
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
root@kali:~/Downloads# exiftool 2018-09-22_09.31.07.jpg
```

Tapi saya menggunakan untuk check GPS di <https://www.gps-coordinates.net/>



Flag= LKSSMK28{BOGOR}