Securimag

TOOLS UP !

OUTILS À CONNAÎTRE POUR S'EN SORTIR EN CTF

iggy - Oct 23, 2019

INTRODUCTION

- Pléthore
- CTF
- Linux

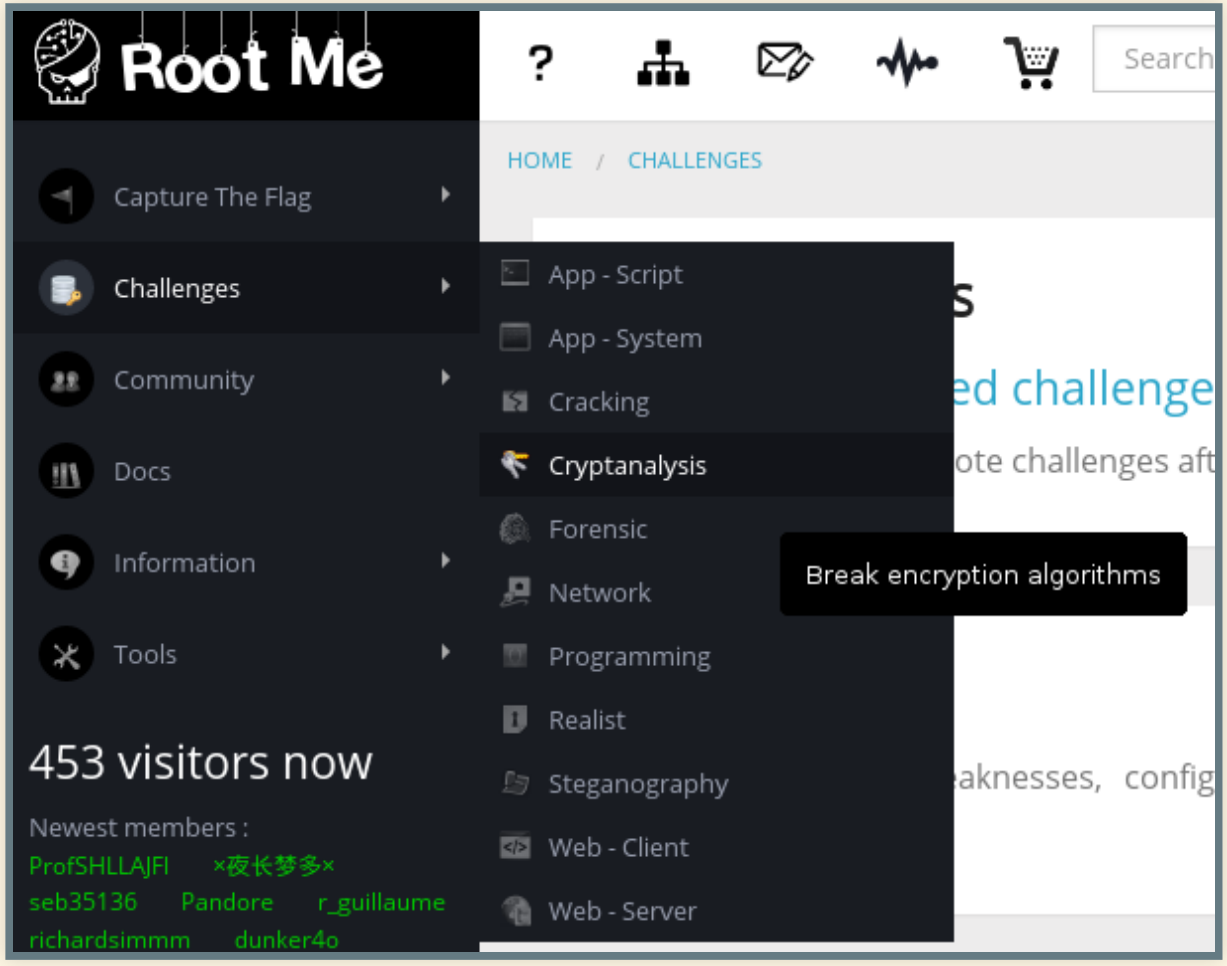
AGENDA

- Ressources
- VM
- Scripting
- Bruteforce
- Cryptography
- Exploitation
- Forensics
- Mobile
- Networking
- Reversing
- Steganography
- Web
- Bordel

RESSOURCES

- Liste complète https://github.com/apsdehal/awesome-ctf
- Challenges tout niveau root-me.org
- Write up (2014-2017) https://github.com/ctfs/
- Write up https://ctftime.org/writeups

RESSOURCES


Root Me
Search
HOME / CHALLENGES
Capture The Flag
Challenges
Community
Docs
Information
Tools
App - Script
App - System
Cracking
Cryptanalysis
Forensic
Network
Programming
Realist
Steganography
Web - Client
Web - Server
Break encryption algorithms
453 visitors now
Newest members :
ProfSHLLAJFI
×夜长梦多×
seb35136
Pandore
r_guillaume
richardsimmm
dunker4o

RESSOURCES

Code - Pseudo Random Number Generator

20 Points

Strange encryption.

Author

Tosh, 19 December 2012

Level

Validations

1699 Challengers 2%

Statement

Here is an archive containing an encrypted file, and the program which has been used for encryption. Your goal is to get back

Clue : according to our information, the file was encrypted during the month of december 2012.

Start the challenge

Validation

Enter password :

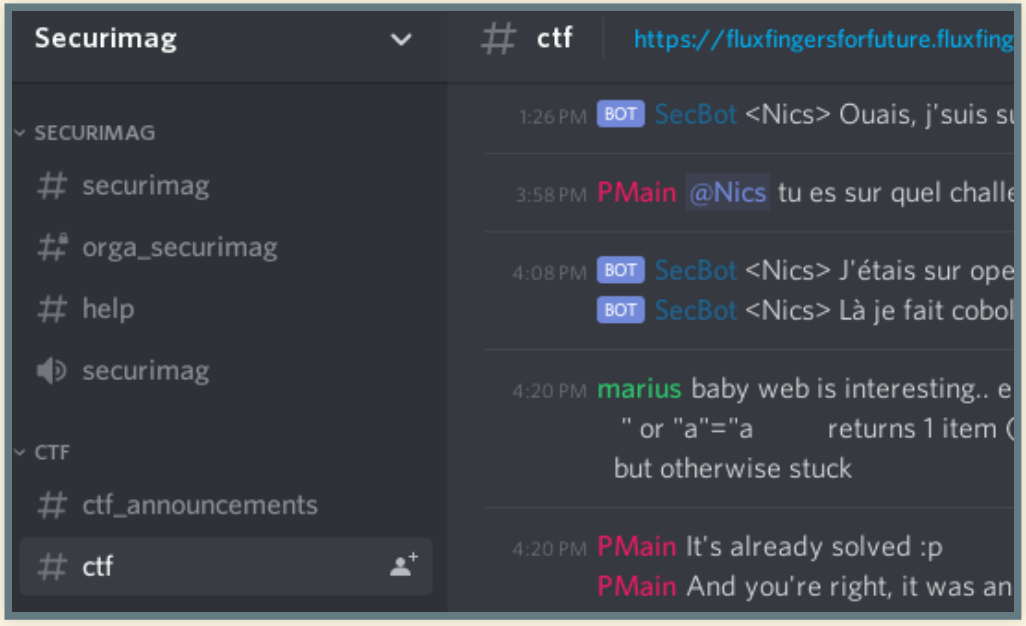
Send

4 related ressource(s)

- Pseudo Random Number Generators for cryptographic applications (Cryptographie)
- Good practice in PRNG (Cryptographie)
- NIST Pseudo Random Number Generators for cryptographic applications (Cryptographie)
- rfc1750 (RFC)

RESSOURCES

- Securimag discord / #ctf



VIRTUAL MACHINE (VM)

```
Virtualbox                  https://www.virtualbox.org/wiki/Downloads
Qemu                        https://www.qemu.org/
openvz / vmware / xen

Kali Linux                  https://www.kali.org/downloads/
La votre...
```

SCRIPTING

```
bash          |
zcsh          |_ Apprendre le "Bourrinage Minimum Syndical" (BMS)
sh            |
whatever      |

python        |
ruby          |_ "Le python c'est bon" (c) Monty 2015
perl          |
go            |
```

BRUTEFORCE

Rare en CTF... donc bon

```
hashcat  Advanced password recovery    https://hashcat.net/hashcat/
john     Tool to find weak passwords   http://www.openwall.com/john/
```

CRYPTOGRAPHY

Quand vous jouez avec RSA...

```
RsaCtfTool  Uncipher data from weak public key
            and try to recover private key
            https://github.com/Ganapati/RsaCtfTool

RSATool     https://github.com/ius/rsatool
```

... sinon

CRYPTOGRAPHY

```
10:24:11 Nics | Un stylo et une feuille de papier !
10:24:17 Nics | Et un interpreteur python
```

EXPLOITS

```
pwntools    CTF framework and exploit development library
            https://github.com/Gallopsled/pwntools

ROPgadget   Sarch your gadgets on your binaries
            https://github.com/JonathanSalwan/ROPgadget

one_gadget  Only search for execve('/bin/sh', NULL, NULL)
            https://github.com/david942j/one_gadget
```

FORENSICS

Audacity	Audio editor http://sourceforge.net/projects/audacity
exiftool	Meta informations http://www.sno.phy.queensu.ca/~phil/exiftool/
testdisk	Scan and repair disk partitions https://www.cgsecurity.org/wiki/TestDisk_Download
foremost	Recover files using headers, footers, structures http://foremost.sourceforge.net/
Volatility	Memory extraction utility framework https://github.com/volatilityfoundation/volatility
PDFextract	Extracts various data out of PDF http://github.com/gdelugre/origam
binwalk	Search binary files https://github.com/devttys0/binwalk

MOBILE

Android tools

```
Google SDK      Android development kit (que 10G)
                https://developer.android.com/studio/

Drozer          Security testing framework for Android
                https://github.com/mwrlabs/drozer

MARA            Mobile Application Reverse engineering and Analysis Frame
                https://github.com/xtiankisutsa/MARA_Framework

Frida           Dynamic instrumentation toolkit
                https://www.frida.re/

androidre       docker image for the reverse engineering of Android appli
                https://github.com/cryptax/androidre
```

NETWORKING

```
wireshark   Dump and analyze network traffic
            https://www.wireshark.org/

nmap        Network exploration tool... port scanner
            https://nmap.org/

netcat      TCP/IP swiss army knife

tcpdump     Dump traffic on a network
```

REVERSING

gdb	The GNU debugger https://www.gnu.org/software/gdb/
gdb-peda	Python Exploit Development Assistance for GDB https://github.com/longld/peda
radare2	Reverse engineering framework and commandline tools https://github.com/radare/radare2
cutter	Reverse Engineering Platform powered by radare2 https://github.com/radareorg/cutter
ghidra	https://ghidra-sre.org/
IDA	(payant)
BinNinja	(payant)

STEGANOGRAPHY

```
PNGcheck    Test PNG image files for corruption
            http://www.libpng.org/pub/png/apps/pngcheck.html

Stegsolve   Stegano solver for challenge
            http://www.caesum.com/handbook/Stegsolve.jar

zsteg       Detect stegano-hidden data in PNG and BMP
            https://github.com/zed-0xff/zsteg/

steghide    Steganography program - embed/extract
            http://steghide.sourceforge.net/
```

WEB

Burp	THE tool for web security research Burp Suite Community Edition https://portswigger.net/burp
curl	Command line request https://curl.haxx.se/
sqlmap	Automated sql injection https://github.com/sqlmapproject/sqlmap
requestbin	Inspect HTTP events https://requestbin.com/

WEB

```
jq          Command-line JSON processor
xmllint     command line XML tool
html2text   HTML-to-text converter

Encode input to URL
python -c "import sys, urllib as ul; print ul.unquote_plus(sys.argv[1])"

Decode input to URL
python -c "import sys, urllib as ul; print ul.quote_plus(sys.argv[1])"

Quick http server
python -m http.server 8000
```

BORDEL

```
xxd          Make a hexdump or do the reverse
bvi          Visual editor for binary files
base64       Base64 encode/decode data
qrencode     Encode input data in a QR Code
zbarimg      Scan and decode bar codes
xdotool      Command-line X11 automation
```

QUESTIONS ?