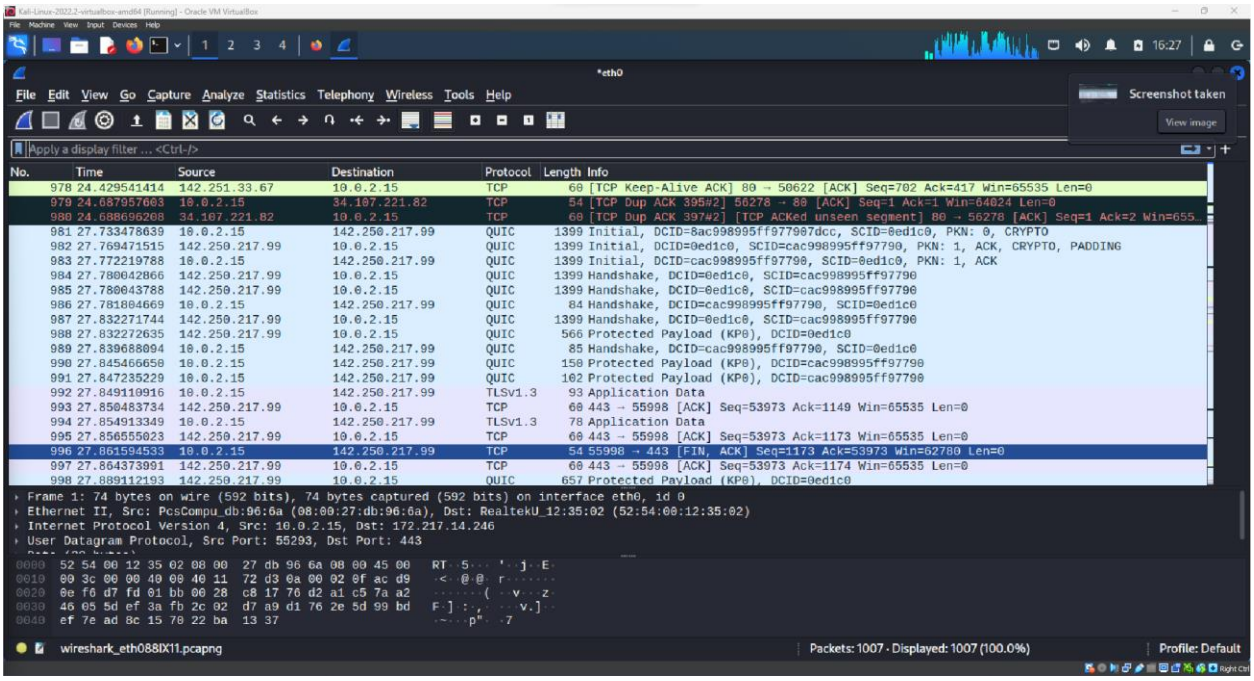
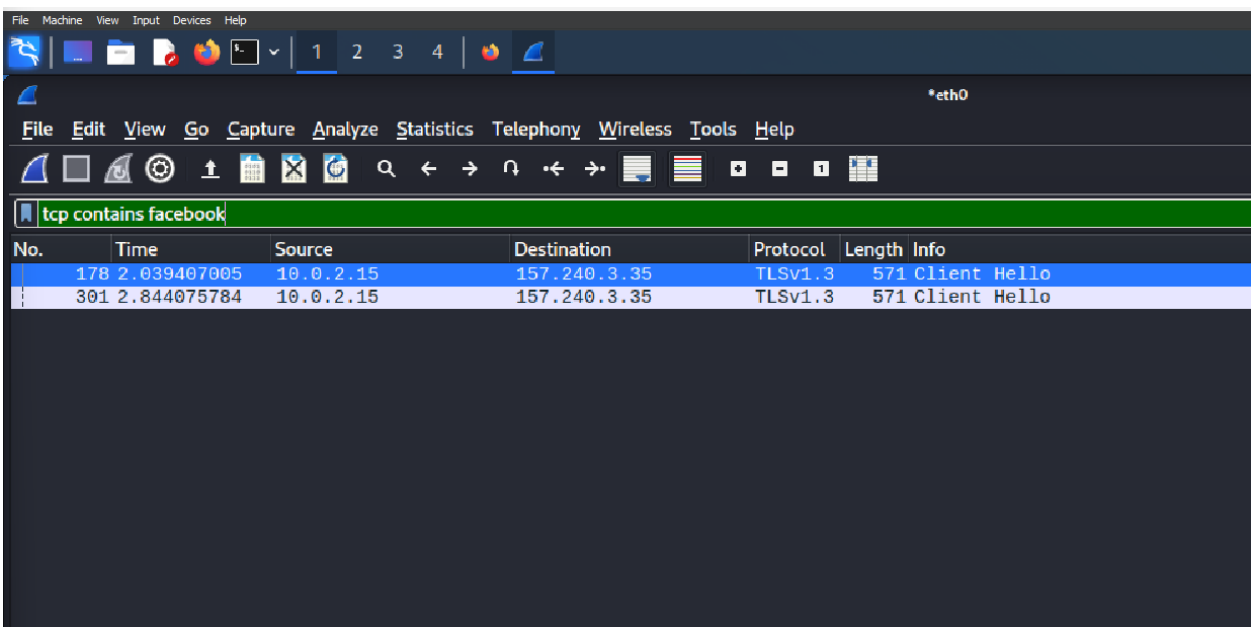
Sniffing and Spoofing

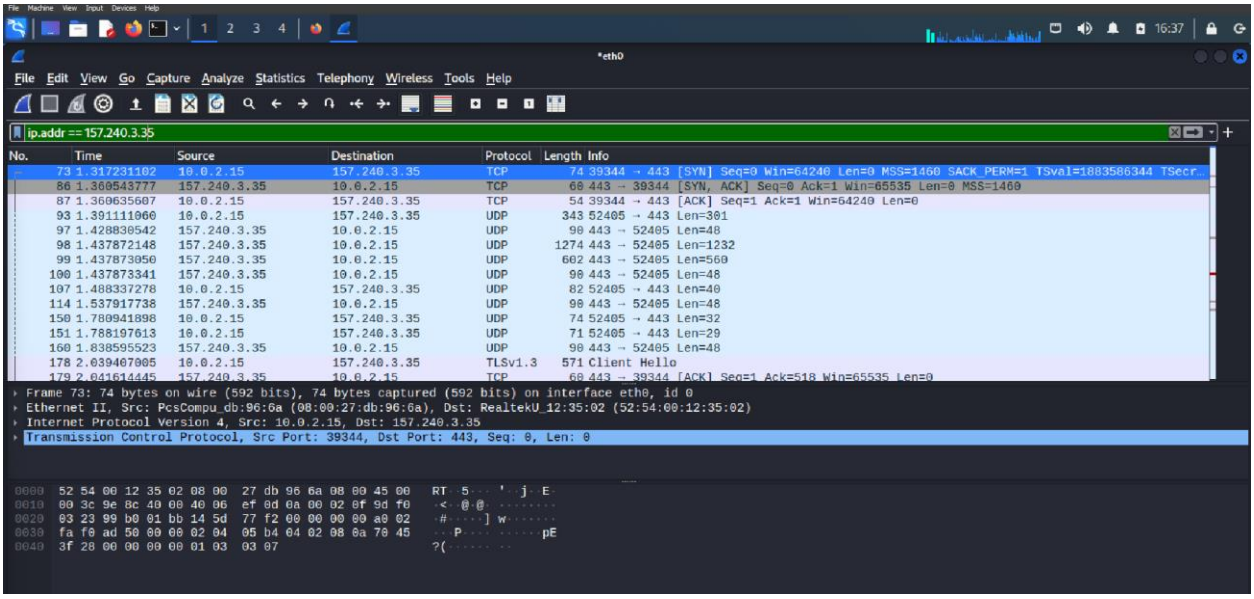
Wireshark:



A number of packets captured by Wireshark



A filter for all packets that contain word Facebook

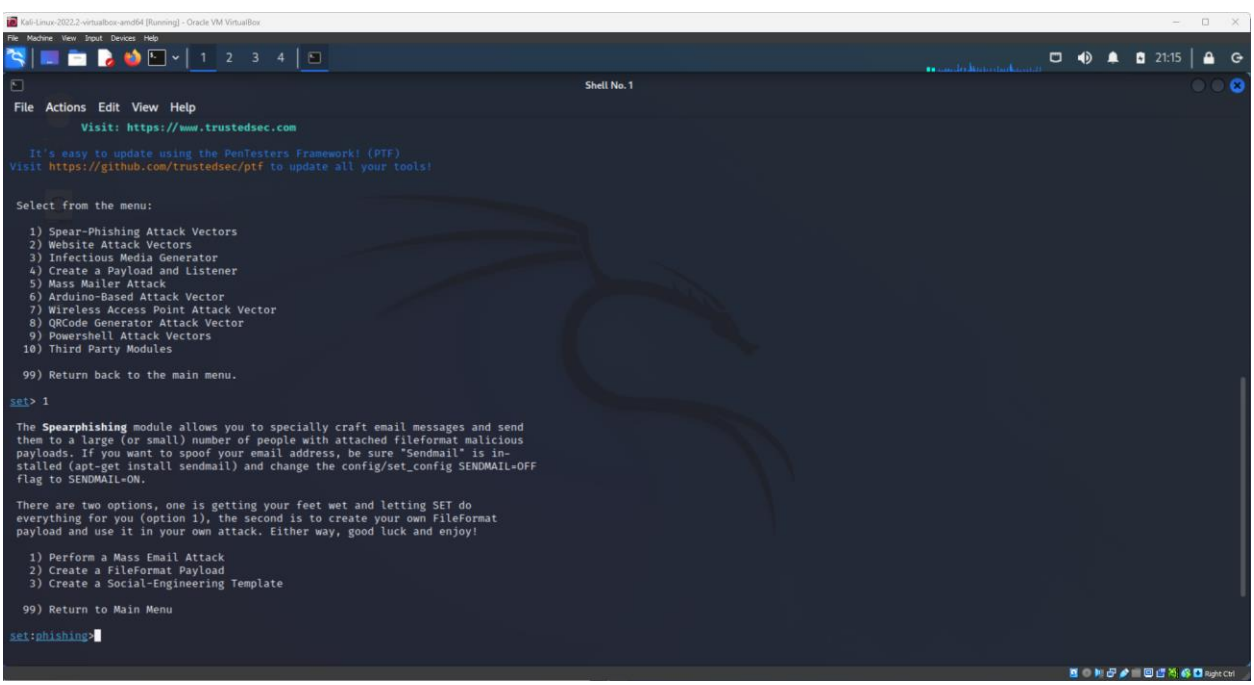


All the packages sent to this IP address server

Password Attack

John the Ripper is an Open Source password security auditing and password recovery tool available for many operating systems. John the Ripper jumbo supports hundreds of hash and cipher types.

Social Engineering Tools



The Spearphishing module allows you to specially craft email messages and send them to a large (or small) number of people with attached fileformat malicious payloads. If you want to spoof your email address, be sure "Sendmail" is installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do everything for you (option 1), the second is to create your own FileFormat payload and use it in your own attack. Either way, good luck and enjoy!

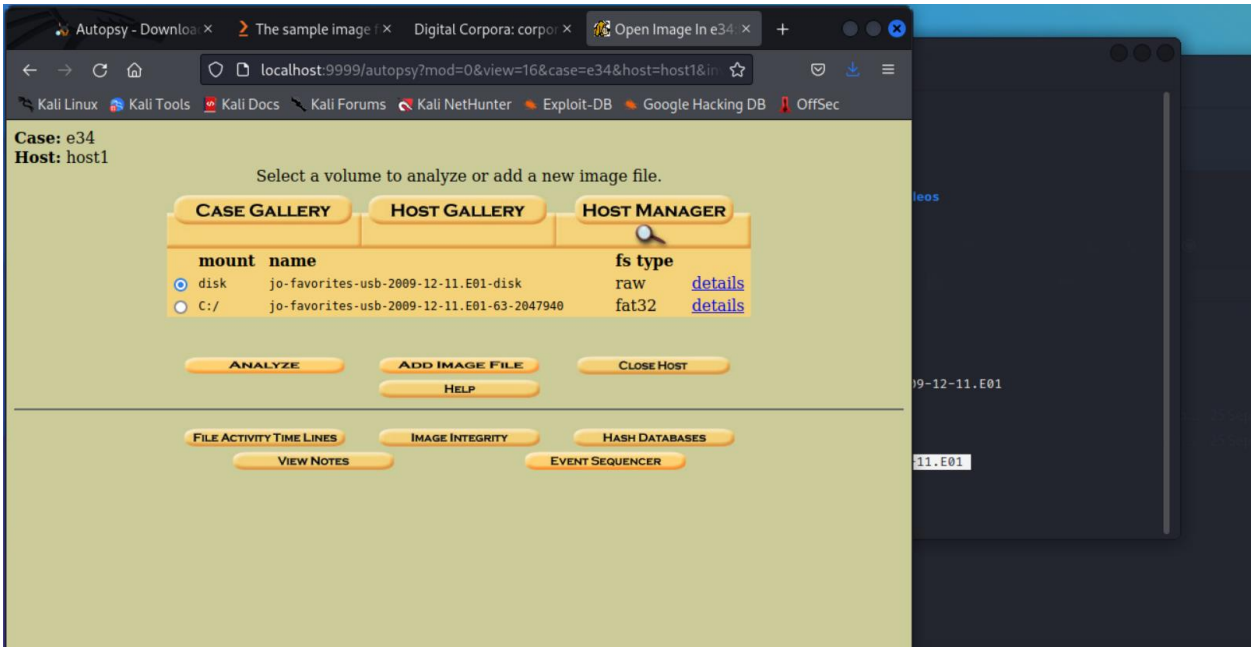
```
   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>1
/usr/share/metasploit-framework/

 Select the file format exploit you want.
 The default is the PDF embedded EXE.

           ********** PAYLOADS **********

   1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
   2) SET Custom Written Document UNC LM SMB Capture Attack
   3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
   4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
   5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
   6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
   7) Adobe Flash Player "Button" Remote Code Execution
   8) Adobe CoolType SING Table "uniqueName" Overflow
   9) Adobe Flash Player "newfunction" Invalid Pointer Use
  10) Adobe Collab.collectEmailInfo Buffer Overflow
  11) Adobe Collab.getIcon Buffer Overflow
  12) Adobe JBIG2Decode Memory Corruption Exploit
  13) Adobe PDF Embedded EXE Social Engineering
  14) Adobe util.printf() Buffer Overflow
  15) Custom EXE to VBA (sent via RAR) (RAR required)
  16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
  17) Adobe PDF Embedded EXE Social Engineering (NOJS)
  18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
  19) Apple QuickTime PICT PnSize Buffer Overflow
  20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
  21) Adobe Reader u3D Memory Corruption Vulnerability
  22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>
```

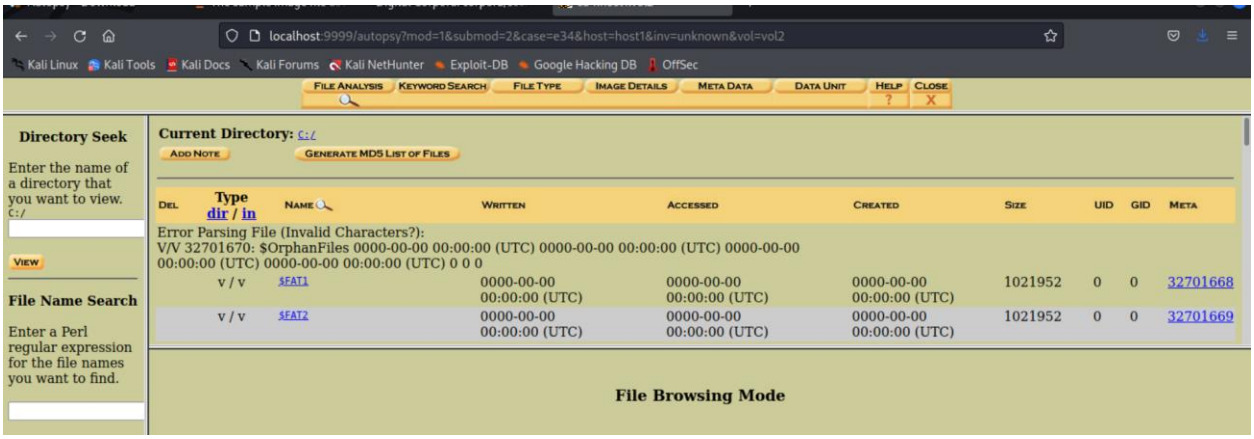
```
set:payloads> Enter the IP address for the payload (reverse):10.0.2.255

What payload do you want to generate:

  Name:                                        Description:

   1) Meterpreter Memory Injection (DEFAULT)  This will drop a meterpreter payload through powershell injection
   2) Meterpreter Multi-Memory Injection      This will drop multiple Metasploit payloads via powershell injection
   3) SE Toolkit Interactive Shell            Custom interactive reverse toolkit designed for SET
   4) SE Toolkit HTTP Reverse Shell           Purely native HTTP shell with AES encryption support
   5) RATTE HTTP Tunneling Payload            Security bypass payload that will tunnel all comms over HTTP
   6) ShellCodeExec Alphanum Shellcode        This will drop a meterpreter payload through shellcodeexec
   7) Import your own executable              Specify a path for your own executable
   8) Import your own commands.txt            Specify payloads to be sent via command line

set:payloads>
```

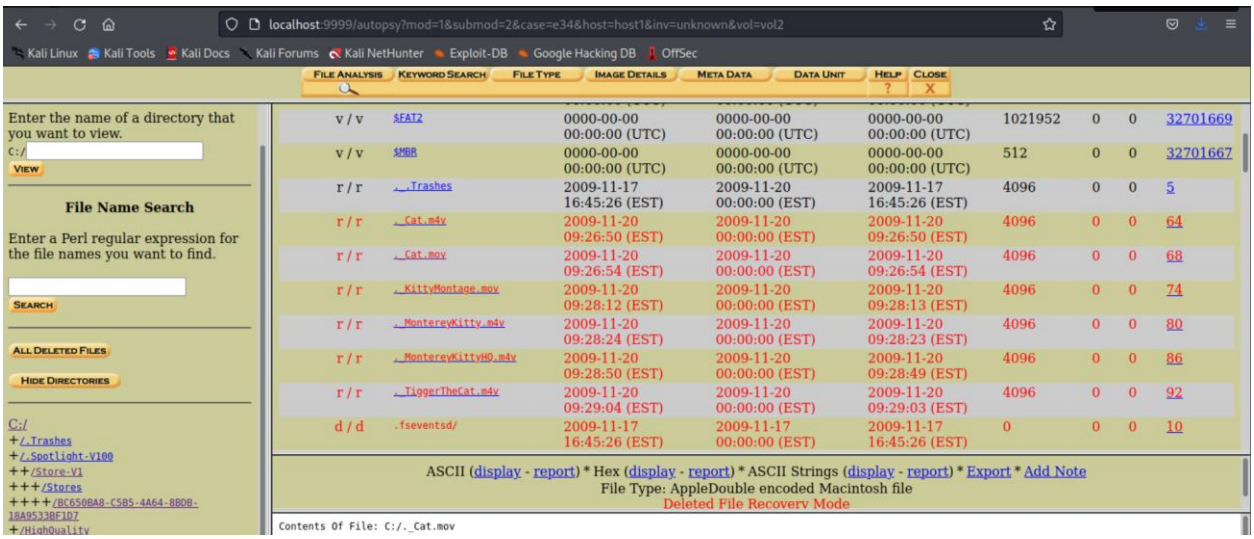
```
File  Actions  Edit  View  Help
9: Order Confirmation
10: Have you seen this?
11: How long has it been?
set:phishing>2
set:phishing> Send email to:dovave4480@loongwin.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:dovave4480@loongwin.com
set:phishing> The FROM NAME user will see:joak,m
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:y
set:phishing> Does your server support TLS? [yes|no]:y
[*] Unable to connect to mail server. Try again (Internet issues?)
/usr/lib/x86_64-linux-gnu/ruby/3.0.0/readline.so: warning: already initialized constant Readline::HISTORY
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/rb-readline-0.5.5/lib/readline.rb:468: warning: previo
us definition of HISTORY was here
/usr/lib/x86_64-linux-gnu/ruby/3.0.0/readline.so: warning: already initialized constant Readline::FILENAME_COMPLETIO
N_PROC
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/rb-readline-0.5.5/lib/readline.rb:496: warning: previo
us definition of FILENAME_COMPLETION_PROC was here
/usr/lib/x86_64-linux-gnu/ruby/3.0.0/readline.so: warning: already initialized constant Readline::USERNAME_COMPLETIO
N_PROC
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/rb-readline-0.5.5/lib/readline.rb:527: warning: previo
us definition of USERNAME_COMPLETION_PROC was here
/usr/lib/x86_64-linux-gnu/ruby/3.0.0/readline.so: warning: already initialized constant Readline::VERSION
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/rb-readline-0.5.5/lib/readline.rb:533: warning: previo
us definition of VERSION was here
[*] StArting the Metasploit Framework console...
```

Forensics

Autopsy linix







shows some deleted data in red

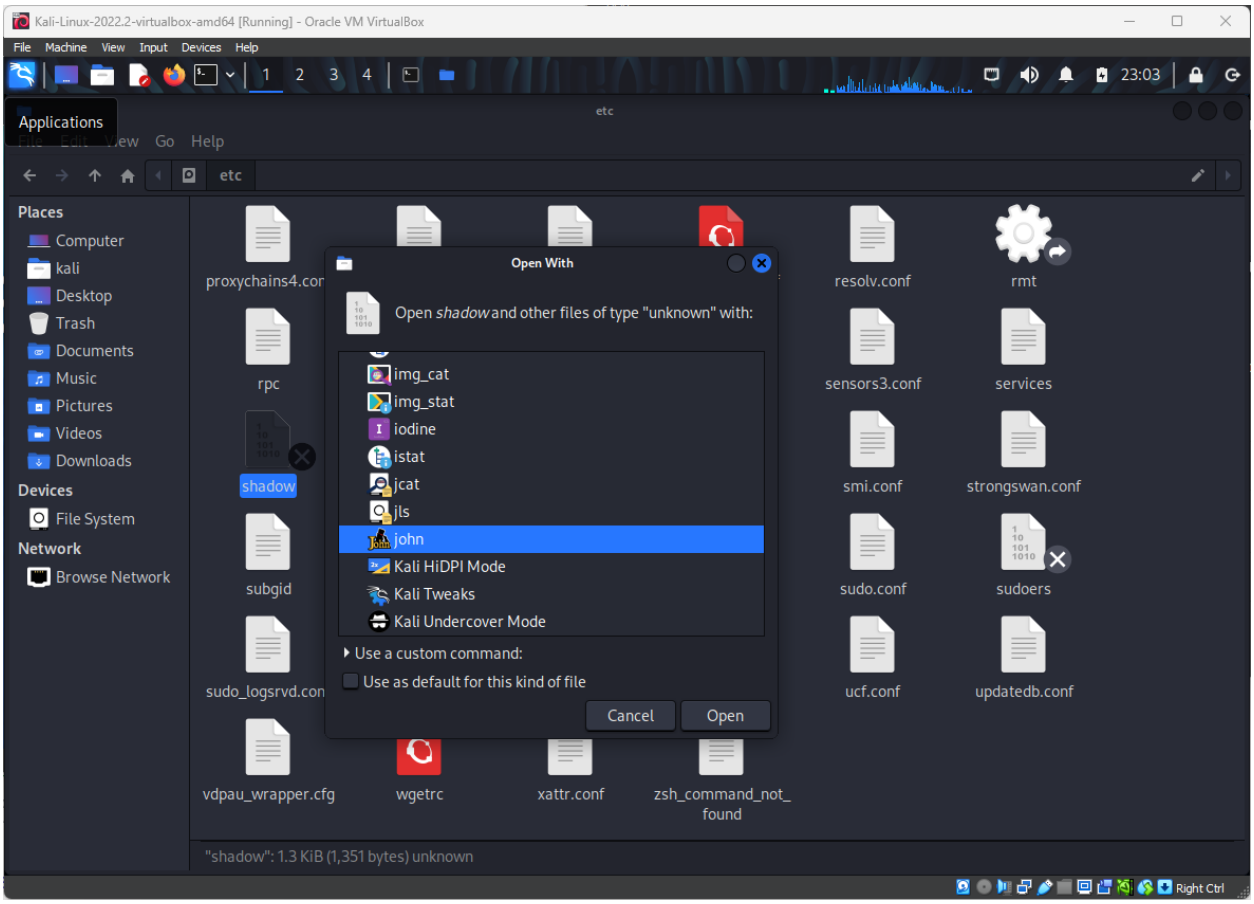
Vulnerability Analysis

Nikto

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×

┌──(kali㉿kali)-[~]
└─$ nikto -h https://www.facebook.com/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          157.240.3.35
+ Target Hostname:    www.facebook.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=Menlo Park/O=Meta Platform
s, Inc./CN=*.facebook.com
                   Ciphers:  TLS_CHACHA20_POLY1305_SHA256
                   Issuer:   /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=Digi
Cert SHA2 High Assurance Server CA
+ Start Time:         2023-03-29 15:03:08 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ X-XSS-Protection header has been set to disable XSS Protection. There is un
likely to be a good reason for this.
+ Uncommon header 'cross-origin-opener-policy' found, with contents: same-ori
gin-allow-popups
+ Uncommon header 'x-fb-rlafr' found, with contents: 0
+ Uncommon header 'report-to' found, with contents: {"max_age":259200,"endpoi
nts":[{"url":"https:\/\/www.facebook.com\/ajax\/browser_error_reports\/?devic
e_level=unknown"}]}
+ Uncommon header 'x-fb-debug' found, with contents: hPS0VnUO2c2J8lStJOQMiBxx
6/hvYD9btNhkH3XAaLiZKcjwOKRNhA5VxJps8y3bXMAm42ZYYM+/wgaluBjqeQ==
+ Uncommon header 'alt-svc' found, with contents: h3=":443"; ma=86400
+ Uncommon header 'document-policy' found, with contents: force-load-at-top
+ The site uses SSL and Expect-CT header is not present.
+ Uncommon header 'cross-origin-embedder-policy-report-only' found, with cont
```

On Facebook no sever os was given

Password Attacks



Checks algorithm being used

```
┌──(root㉿kali)-[~]
└─# john /etc/shadow
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

┌──(root㉿kali)-[~]
└─#
```

```
No password hashes loaded (see FAQ)

┌──(root㉿kali)-[~]
└─# john /etc/shadow --show
0 password hashes cracked, 0 left

┌──(root㉿kali)-[~]
└─#
```

Shows no password being used

I created an encrypted file and set out to get its password

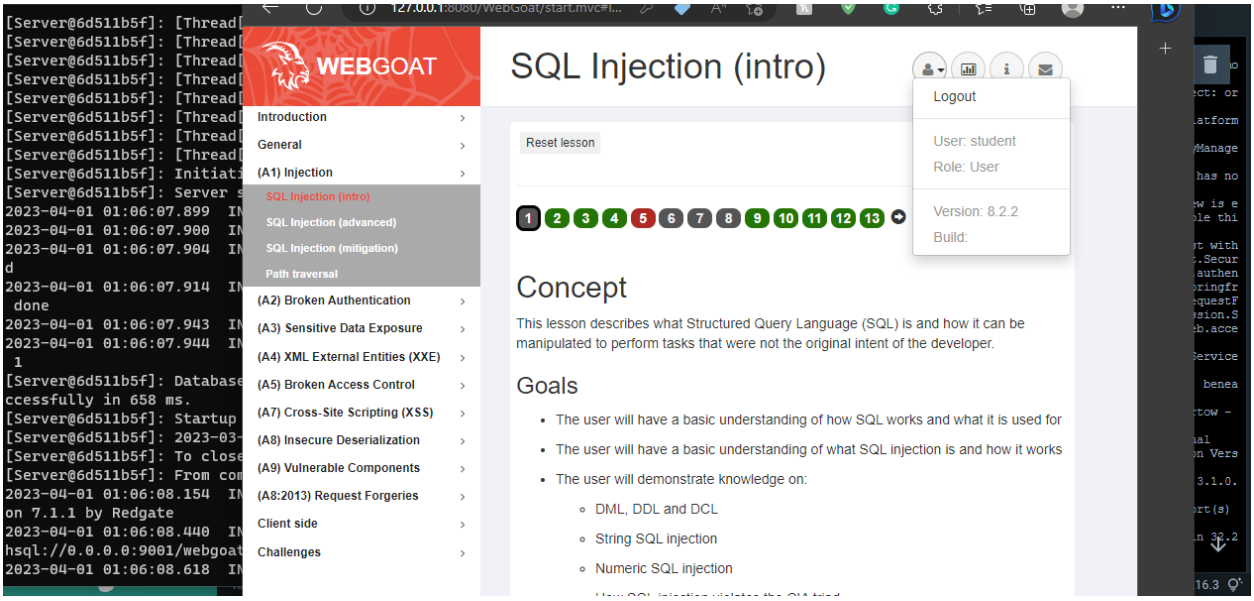
```
┌──(root㉿kali)-[~]
└─# john /home/kali/Documents/LAb_report.docx
Warning: invalid UTF-8 seen reading /home/kali/Documents/LAb_report.docx
Warning: detected hash type "HMAC-SHA256", but the string is also recognized as "HMAC-SHA512"
Use the "--format=HMAC-SHA512" option to force loading these as that type instead
Warning: UTF-16 BOM seen in password hash file. File may not be read properly unless you re-encode
it
oracle: Input file is not UTF-8. Please use --input-enc to specify a codepage.
Warning: only loading hashes of type "HMAC-SHA256", but also saw type "HMAC-SHA224"
Use the "--format=HMAC-SHA224" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 194 password hashes with 194 different salts (HMAC-SHA256 [password is key, SHA256 128/128 S
SE2 4x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
```

This shows 27 password hashes cracked, 202 left

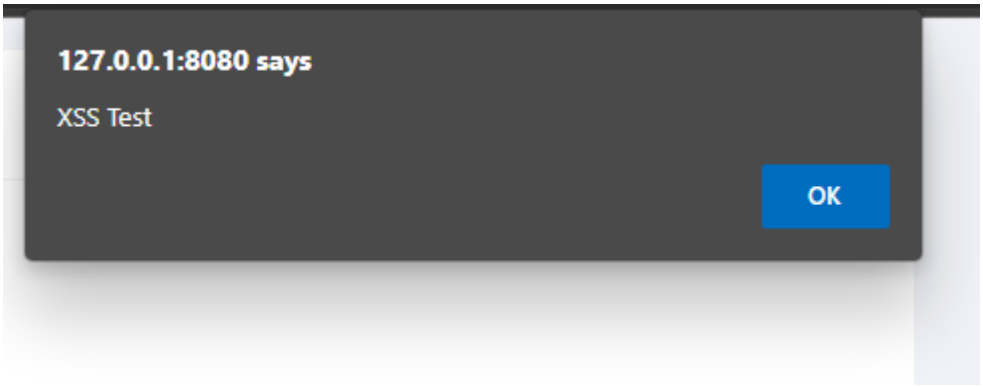
```
H'M◆◆v◆qGv◆%u◆◆ş:NO PASSWORD:◆q◆Tf◆xsNμ#◆
7◆J~◆!◆o@Lr◆[%◆◆◆hYry>◆1◆%w[#(◆◆[◆fK◆^[]◆p◆◆◆^L◆,L◆B◆E◆{◆◆$◆◆◆?Ĭ◆9冕◆◆◆?◆◆◆1I◆◆k◆◆qm◆D◆◆)◆◆▯◆Ƹ◆◆h:◆◆u◆◆◆|◆◆◆b1◆◆Is◆◆0◆◆◆◆H▯◆bŠ2◆◆Q◆◆+'
                                                                                                                                                IH◆◆▒◆◆;.-◆f}N◆lp◆◆S◆◆+◆◆◆~◆v◆R

Ri]◆Ꝓ◆◆ę◆i◆◆T^na◆◆>`◆v◆◆◆ɾ◡Oz◆'
                                ◆◆◆◆4◆◆◆J◆◆◆o◆◆-◆T◆v◆◆CL◆Fx3T3k◆◆◆◆\udĬz◆◆9◆◆I◆◆◆g◆0◆◆Cg
W6Q◆◆◆◆                                                                                                u_◆"◆◆◆◆◆◆ŋ>E◆g◆◆-◆?N(◆◆◆lP:NO PASSWORD:◆h◆zeG◆k
        ?◆v;◆◆u▒◆B}B      ◆L◆◆
                                ◆[d◆x◆◆5YX?t◆◆◆q4◆9~N◆dLQ◆wXZ◆◆/tT",ɥ◆◆
◆◆◆U6Sh◆!◆<◆◆v◆◆◆oB◆◆`^◆◆D5◆◆◆◆L◆◆◆◆Q◆,◆I◆◆`6◆◆S◆罵◆a◆◆◆◆!◆.◆i◆Z◆◆◆◆gV◆g◆q4Yõ◆◆←Ꝑ◆LX◆
◆ɔ◆:o猟.◆d◆R◆◆3◆◆N◆◆◆◆Ys87*◆m◆◆X5fh◆3<[pc$:◆◆n4T◆f◆$g◆]◆_N◆◆0◆[◆◆01ȼf◆◆◆◆◆◆◆◆▒<◆=D◆>
                                                                                                ◆◆◆◆◆<▒◆◆WP]◆FPh◆◆◆◆8◆◆◆◆=U◆▒◆
>J◆+r◆A◆◆`
          @81G:NO PASSWORD:E(pY◆◆◆◆i◆◆◆
l◆~◆◆a◆b◆◆◆◆◆◆◆L◆◆◆◆b◆j◆T◆◆(◆◆P◆C◆◆6◆9ɥ
                                a=E◆K4◆cf◆.◆◆◆◆O5)◆◆7◆iD:NO PASSWORD:◆`yIO5◆◆▒◆Ꝺ◆c◆◆◆U◆▯ ◆◆▒+G6◆sMd◆◆T◆◆
                                                                                                                :n◆ &◆◆◆e◆◆>◆◆]◆[◆◆Dk◆◆nJv
                                                                                                                                        IčkP◆◆Z
b!◆◆ !◆◆@%V\◆◆◆F▒◆{◆,,◆$4?◆◆X◆p◆$+◆◆◆◆3Fc◆◆▒◆◆◆z◆◆◆%◆◆^◆◆4◆◆R◆r◆^h▯#M◆◆P)◆◆◆◆j
                                                                                                ◆◆◆◆F◆g◆X◆EL◆>◆c_◆>.M8◆"◆2◆Y◆◆7qFLP;"◆◆◆H◆@◆~B◆◆

j◆◆K,◆◆◆&B3◆<◆◆m)◆◆it+◆◆◆◆X◆+◆^W♭:NO PASSWORD:@◆◆◆#◆◆1(<
◆=*h◆◆1◆@       e"◆VrD▒C◆R◆9 ◆◆2V◆◆=a>◆\◆◆<◆◆BO=◆l◆,◆3◆◆{13◆◆◆ ◆^◆◆◆(O!HXDL)E◆◆[◆Jw◆|◆u#
                                                                                                  ◆Q◆g◆◆ Ĭ
◆◆◆$◆◆  ◆       R◆◆f◆◆T-k◆◆◆p◆◆δ◆<◆◆qav$◆y$◆◆◆eБ◆◆◆4s◆◆◆◆◆◆◆=◆.{◆◆◆                          A-m◆O◆◆◆◆t◆/l◆◆I◆:dlJ◆◆K◆es▯◆◆◆A◆w

27 password hashes cracked, 202 left

┌──(root㉿kali)-[~]
└─#
```

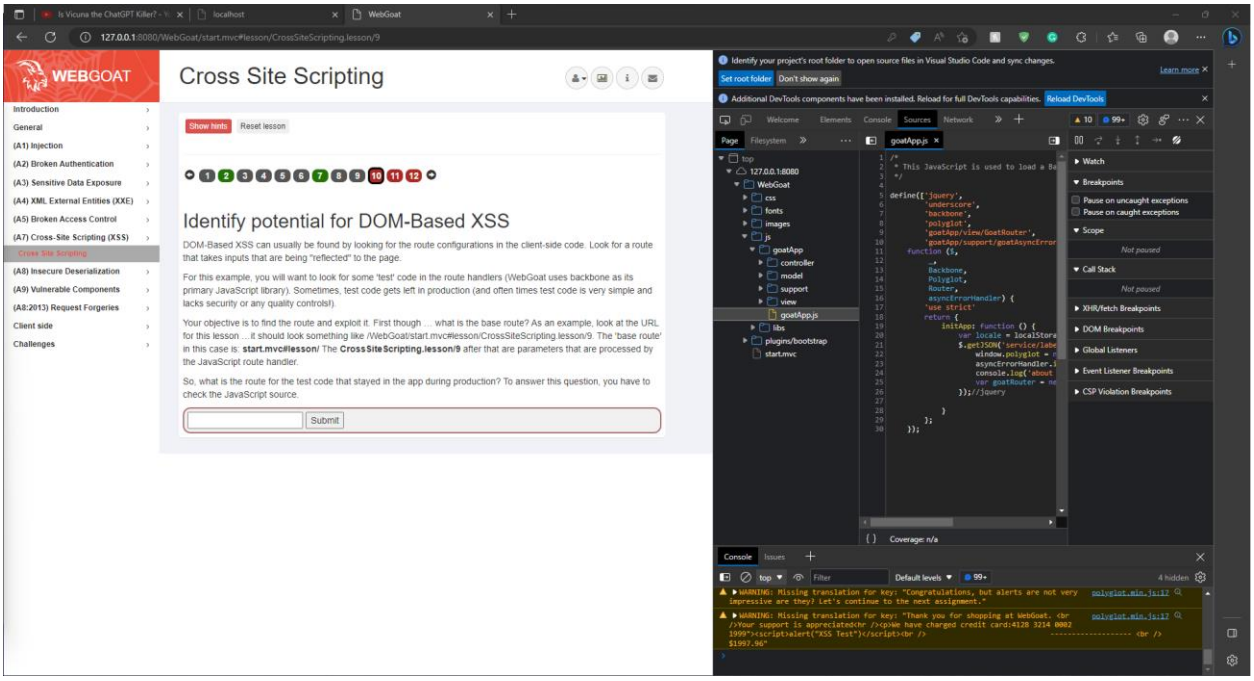
Database Assessment

Web Goat Challenges



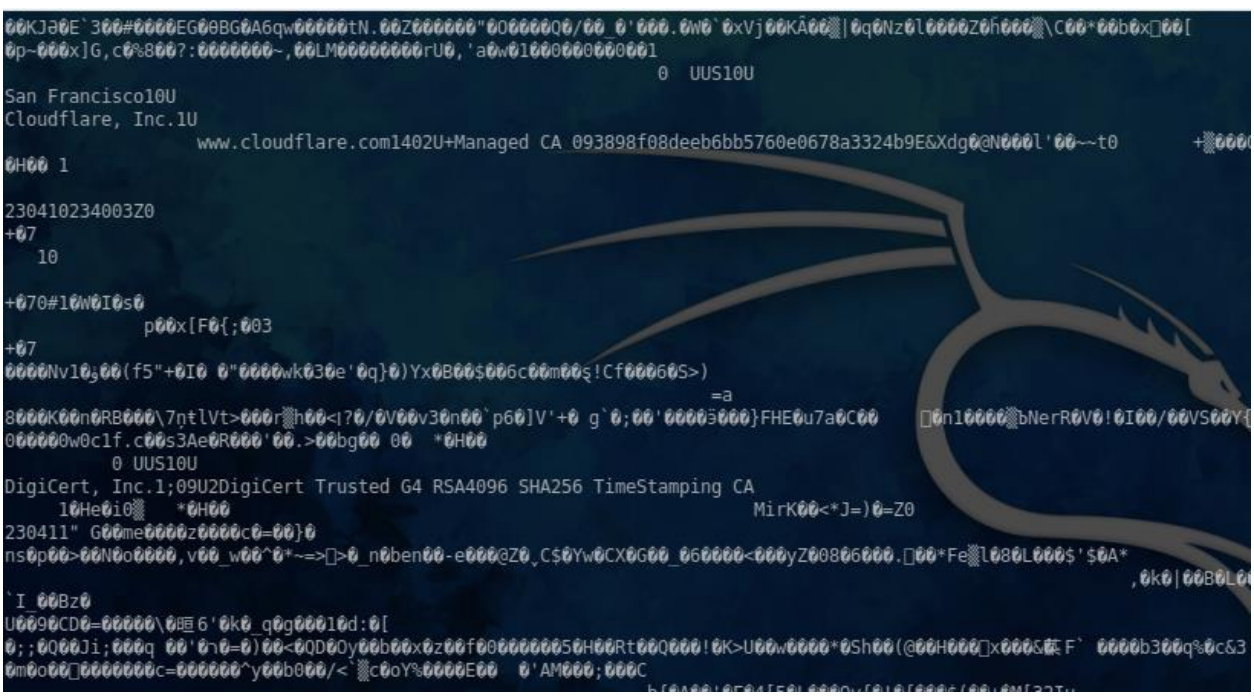
Cross-Site Scripting



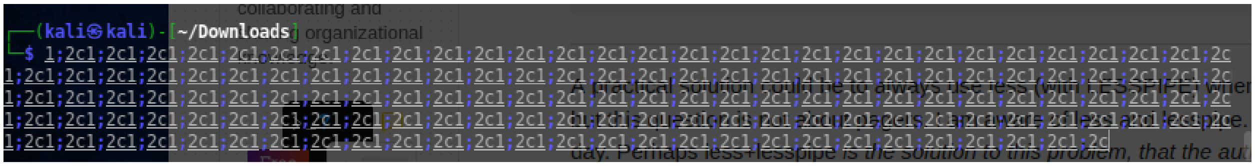


Malware analysis of a .exe file

Commands used in order and CYberchef
ruuning cmd cat on .exe

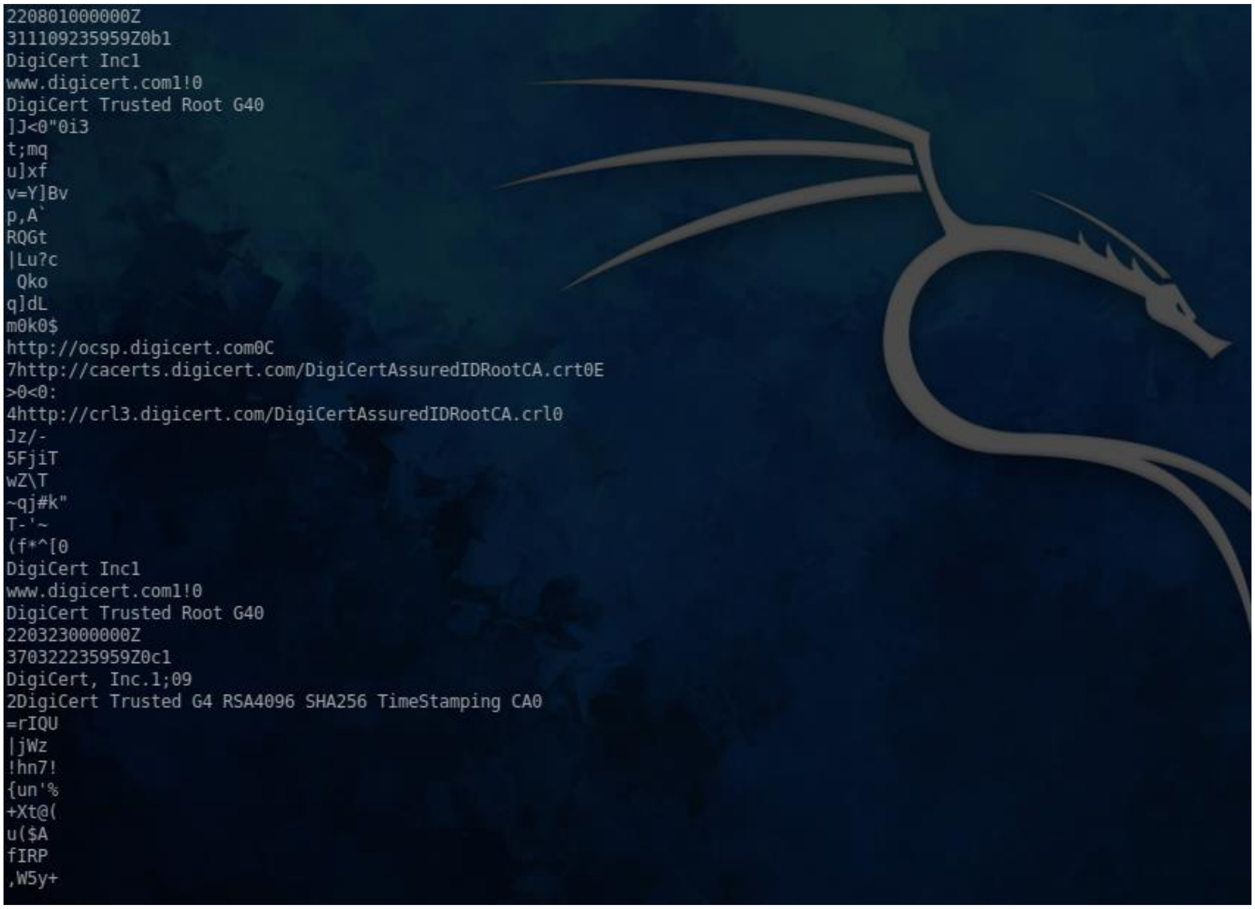


after cat FileApp.exe



```
┌──(kali㉿kali)-[~/Downloads]
└─$ 1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c
1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c
1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c
1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c
1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c
```

Strings fileapp.exe



```
220801000000Z
311109235959Z0b1
DigiCert Inc1
www.digicert.com1!0
DigiCert Trusted Root G40
]J<0"0i3
t;mq
u]xf
v=Y]Bv
p,A`
RQGt
|Lu?c
 Qko
q]dL
m0k0$
http://ocsp.digicert.com0C
7http://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt0E
>0<0:
4http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl0
Jz/-
5FjiT
wZ\T
~qj#k"
T-'~
(f*^[0
DigiCert Inc1
www.digicert.com1!0
DigiCert Trusted Root G40
220323000000Z
370322235959Z0c1
DigiCert, Inc.1;09
2DigiCert Trusted G4 RSA4096 SHA256 TimeStamping CA0
=rIQU
|jWz
!hn7!
{un'%
+Xt@(
u($A
fIRP
,W5y+
```

Noticeable strings

WakeConditionVariable, GetProcessId, __setusermatherr,

CreateFileW

Potential; back door

```
__imp___p__commode
anon.6c9e483745a37be0a8aa77c8906b07c4.131.llvm.1911975304064522615
__mingw_oldexcpt_handler
anon.69cc5c110623d7751034bb5e6ac8568a.0.llvm.7757141689514655956
__imp_DeleteFileW
anon.0098efba999acdb3b38472ad58df1512.8.llvm.15253526931182900225
__imp_GetNamedPipeInfo
anon.97d8ec71871cf1c3bf30bfec2170203c.55.llvm.6288554224869990037
anon.9436f07a512ede7759195d78c28932cf.22.llvm.17561971399798398629
GetLogicalProcessorInformationEx
anon.4ea29b27ce180e74196a71516a32d3bd.50.llvm.14433657592466225512
__imp_anon.59a61f859131d011f5eb8dfd977546d9.1.llvm.13229109604451086328
anon.f3e9258b25bc993ae873893c6b5b8970.72.llvm.1987990312968812729
__imp_CreateNamedPipeW
__imp_anon.620352fc6fe9a2276165ad05f440a228.4.llvm.10042983051580347279
__imp_anon.97d8ec71871cf1c3bf30bfec2170203c.102.llvm.6288554224869990037
GetFileInformationByHandle
__imp_DisconnectNamedPipe
WSACleanup
__imp_anon.d2741634b8c08b66e6e63ca6849e7fab.5.llvm.1726911837090103872
anon.d2741634b8c08b66e6e63ca6849e7fab.103.llvm.1726911837090103872
getsockopt
anon.83e834912982303ad8613e279d4faca0.4.llvm.2682911246271467334
anon.12898464f48fe852843e17b2c0560c95.14.llvm.13552914103641071867
anon.3d5836dca8dc835fd633aebf745ca887.3.llvm.15484446257880030433
anon.5614e1bca7685013b3281be8876a885d.23.llvm.5832775023738784549
anon.d2741634b8c08b66e6e63ca6849e7fab.144.llvm.1726911837090103872
anon.9dc7e76e9b336bfa0cab67fa7a9942b9.19.llvm.7755934173861450816
anon.9dc7e76e9b336bfa0cab67fa7a9942b9.20.llvm.7755934173861450816
__imp_getpeername
anon.43dba236849122e565528771b9b85298.115.llvm.14416331236661328312
anon.9b5e953ea16ad9d3f913cea93685a073.0.llvm.5624815963520901825
__imp_anon.d33b7cc8140b86b3e7241c0314b36227.2.llvm.4802628890652054 98
anon.18ef20037f355fe071b366f2f44d019e.4.llvm.2550592327363295536
CoInitializeEx
__size_of_stack_commit__
__imp_anon.4ea29b27ce180e74196a71516a32d3bd.82.llvm.14433657592466225512
__lib64_libkernel32_a_iname
anon.4ea29b27ce180e74196a71516a32d3bd.78.llvm.14433657592466225512
__imp_anon.bf433d4d99fca62c9b04a68851db5e92.4.llvm.4108042338411055726
```

objdump FileApp.exe

```
┌──(kali㉿kali)-[~/Downloads]
└─$ objdump -x FileApp.exe

FileApp.exe:     file format pei-x86-64
FileApp.exe
architecture: i386:x86-64, flags 0x0000013b:
HAS_RELOC, EXEC_P, HAS_DEBUG, HAS_SYMS, HAS_LOCALS, D_PAGED
start address 0x00000001412f9058

Characteristics 0x26
     executable
     line numbers stripped
     large address aware

Time/Date    Mon Apr 10 19:15:39 2023
Magic       020b (PE32+)
MajorLinkerVersion   2
MinorLinkerVersion   38
SizeOfCode   00000000001b1400
SizeOfInitializedData 0000000000238800
SizeOfUninitializedData 0000000000000600
AddressOfEntryPoint  00000000012f9058
BaseOfCode   0000000000001000
ImageBase    0000000140000000
SectionAlignment 00001000
FileAlignment    00000200
MajorOSystemVersion  4
MinorOSystemVersion  0
MajorImageVersion 0
MinorImageVersion 0
MajorSubsystemVersion 5
MinorSubsystemVersion 2
Win32Version    00000000
SizeOfImage  01acb000
SizeOfHeaders    00000600
CheckSum     00b333df
Subsystem    00000002 (Windows GUI)
```

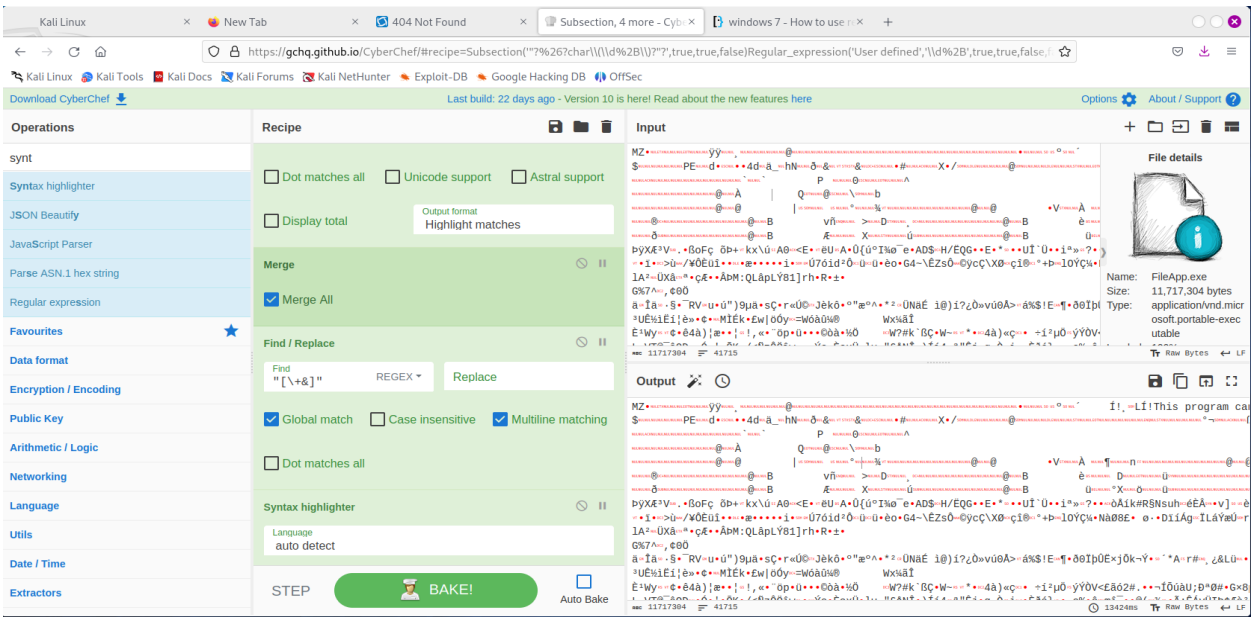
```
┌──(kali㉿kali)-[~/Downloads]
└─$ objdump -f FileApp.exe

FileApp.exe:     file format pei-x86-64
architecture: i386:x86-64, flags 0x0000013b:
HAS_RELOC, EXEC_P, HAS_DEBUG, HAS_SYMS, HAS_LOCALS, D_PAGED
start address 0x00000001412f9058
```

File fileapp.exe

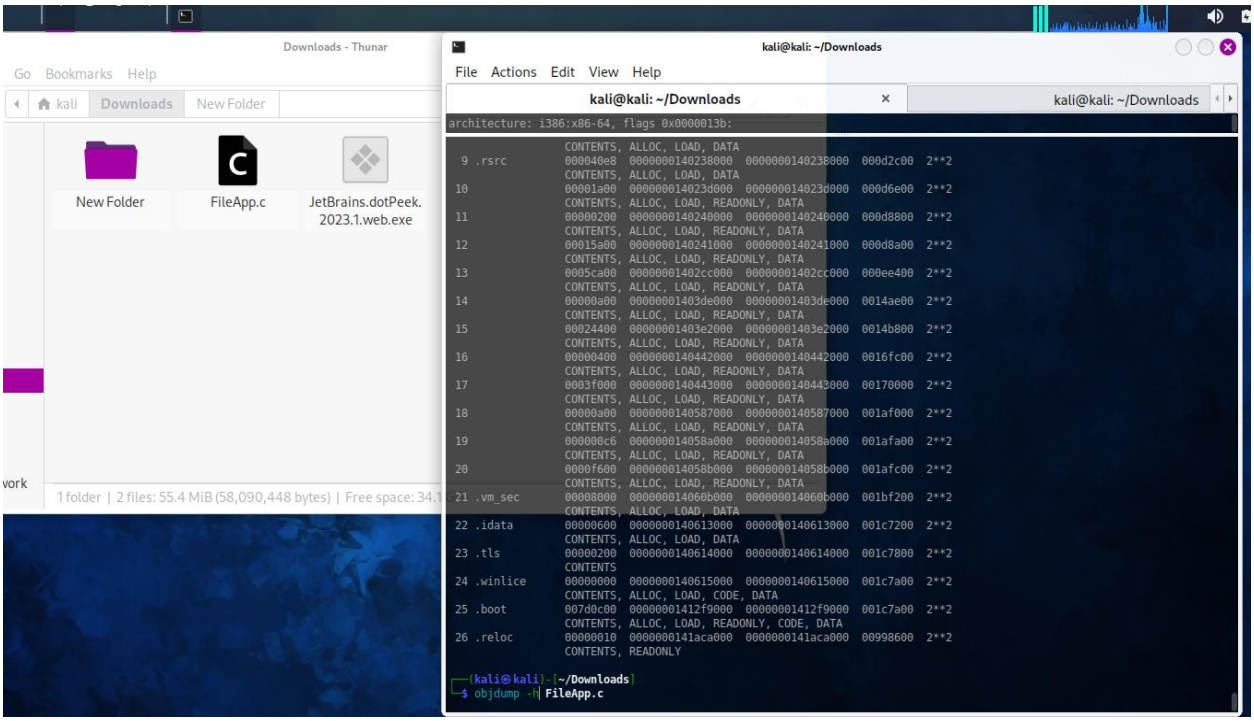
```
┌──(kali㉿kali)-[~/Downloads]
└─$ file FileApp.exe
FileApp.exe: PE32+ executable (GUI) x86-64, for MS Windows, 27 sections
```

Results reads as executable

Fileapp.exe in cyberchef



Change from .exe to .c file


Downloads - Thunar
Go Bookmarks Help
kali Downloads New Folder
New Folder
FileApp.c
JetBrains.dotPeek.
2023.1.web.exe
1 folder | 2 files: 55.4 MiB (58,090,448 bytes) | Free space: 34.1
kali@kali: ~/Downloads
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~/Downloads
architecture: i386:x86-64, flags 0x0000013b:
9 .rsrc 000040e8 0000000140238000 0000000140238000 000d2c00 2**2
CONTENTS, ALLOC, LOAD, DATA
10 00001a00 000000014023d000 000000014023d000 000d6e00 2**2
CONTENTS, ALLOC, LOAD, READONLY, DATA
11 00000200 0000000140240000 0000000140240000 000d8800 2**2
CONTENTS, ALLOC, LOAD, READONLY, DATA
12 00015a00 0000000140241000 0000000140241000 000d8a00 2**2
CONTENTS, ALLOC, LOAD, READONLY, DATA
13 0005ca00 00000001402cc000 00000001402cc000 000ee400 2**2
CONTENTS, ALLOC, LOAD, READONLY, DATA
14 00000a00 00000001403de000 00000001403de000 0014ae00 2**2
CONTENTS, ALLOC, LOAD, READONLY, DATA
15 00024400 00000001403e2000 00000001403e2000 0014b800 2**2
CONTENTS, ALLOC, LOAD, READONLY, DATA
16 00000400 0000000140442000 0000000140442000 0016fc00 2**2
CONTENTS, ALLOC, LOAD, READONLY, DATA
17 0003f000 0000000140443000 0000000140443000 00170000 2**2
CONTENTS, ALLOC, LOAD, READONLY, DATA
18 00000a00 0000000140587000 0000000140587000 001af000 2**2
CONTENTS, ALLOC, LOAD, READONLY, DATA
19 000000c6 000000014058a000 000000014058a000 001afa00 2**2
CONTENTS, ALLOC, LOAD, READONLY, DATA
20 0000f600 000000014058b000 000000014058b000 001afc00 2**2
CONTENTS, ALLOC, LOAD, READONLY, DATA
21 .vm_sec 00008000 000000014060b000 000000014060b000 001bf200 2**2
CONTENTS, ALLOC, LOAD, DATA
22 .idata 00000600 0000000140613000 0000000140613000 001c7200 2**2
CONTENTS, ALLOC, LOAD, DATA
23 .tls 00000200 0000000140614000 0000000140614000 001c7800 2**2
CONTENTS
24 .winlice 00000000 0000000140615000 0000000140615000 001c7a00 2**2
CONTENTS, ALLOC, LOAD, CODE, DATA
25 .boot 007d0c00 00000001412f9000 00000001412f9000 001c7a00 2**2
CONTENTS, ALLOC, LOAD, READONLY, CODE, DATA
26 .reloc 00000010 0000000141aca000 0000000141aca000 00998600 2**2
CONTENTS, READONLY
┌──(kali㉿kali)-[~/Downloads]
└─$ objdump -h FileApp.c