Politechnika Wrocławska

Zarządzanie infrastrukturą teleinformatyczną

Aplikacji uruchamiająca plik binarny ELF bez używania wywołań systemowych

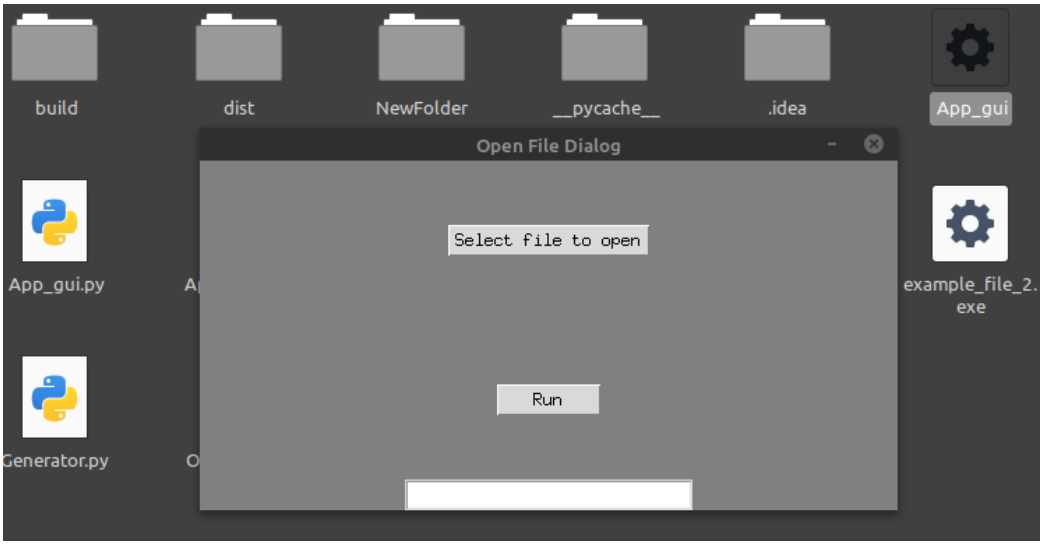
Piotr Potomski

1. Aplikacja

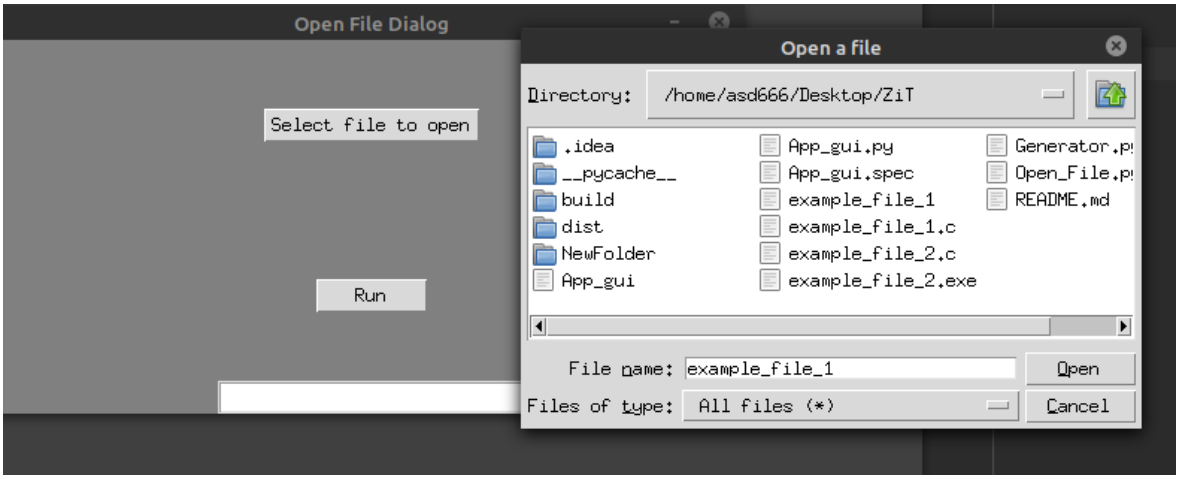
Aplikacja generuje interpretowalny kod pliku ELF jako plik w pamięci i wykonuje go nie pozostawiając śladów na dysku. W projekcie możliwe jest uruchomienie okienkowej wersji aplikacji (*App_gui*) oraz z uruchomienie z poziomu skryptu (*Open_File.py*). Sposób otwarcia oraz użycia zapisany został w pliku *README.md* oraz poniżej. W aplikacji użyte zostało wywołanie memfd_create, które zapewnia łatwy sposób na uzyskanie deskryptora pliku dla anonimowej pamięci.

2. Użycie

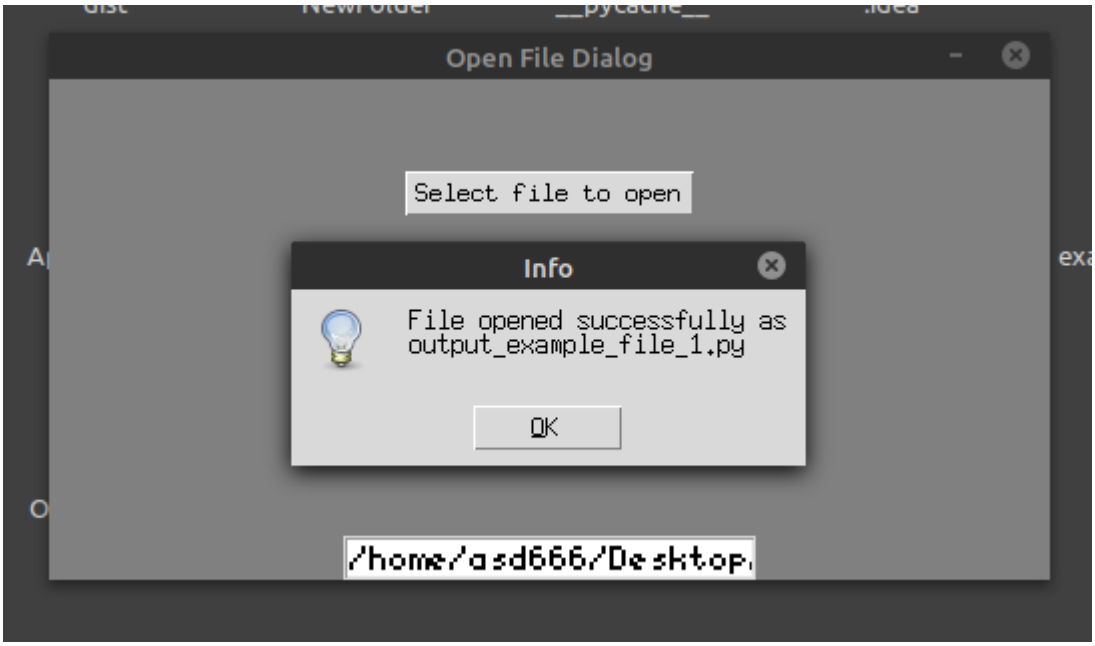
Należy otworzyć aplikację *App_gui*:

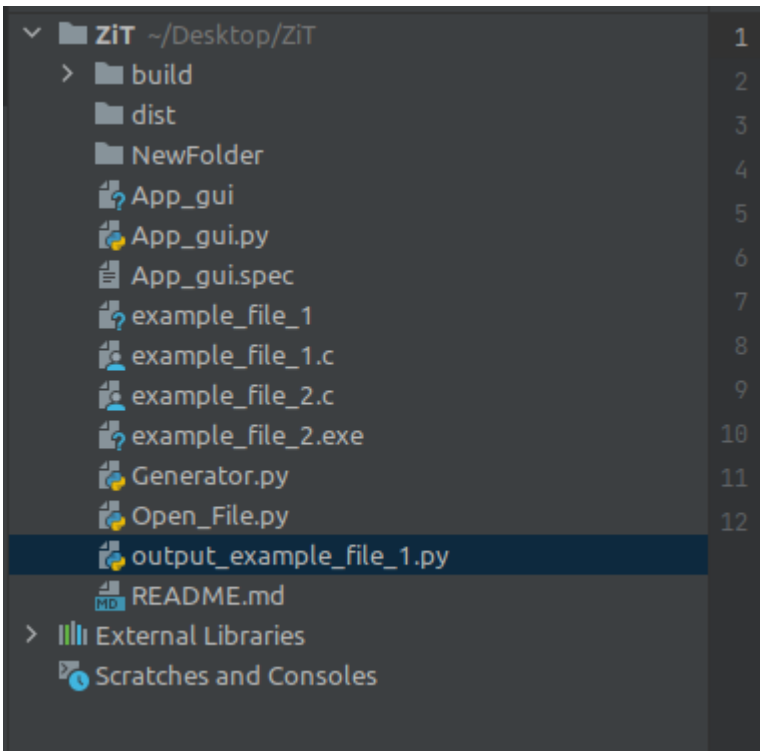


Następnie należy wybrać plik i kliknąć *Run*.



Po kliknięciu przycisku *Run* wyświetli się komunikat jeśli poprawnie otworzony zostanie plik i dodany do projektu zostanie plik wyjściowy.





3. Strace

Wybrane wyniki komendy *strace* dla *example_file_1*:

```
(ZiT) asd666@asd666:~/Desktop/ZiT$ strace -e trace=mkdir,uname,write,clock_nanosleep,mkdir -c ./example_file_1
Hello, World!
system name = Linux
node name   = asd666
release     = 5.4.0-74-generic
version     = #83-Ubuntu SMP Sat May 8 02:35:39 UTC 2021
machine     = x86_64
Hello, World!
system name = Linux
node name   = asd666
release     = 5.4.0-74-generic
version     = #83-Ubuntu SMP Sat May 8 02:35:39 UTC 2021
machine     = x86_64
Hello, World!
system name = Linux
node name   = asd666
release     = 5.4.0-74-generic
version     = #83-Ubuntu SMP Sat May 8 02:35:39 UTC 2021
machine     = x86_64
Hello, World!
system name = Linux
node name   = asd666
release     = 5.4.0-74-generic
version     = #83-Ubuntu SMP Sat May 8 02:35:39 UTC 2021
machine     = x86_64
Hello, World!
system name = Linux
node name   = asd666
release     = 5.4.0-74-generic
version     = #83-Ubuntu SMP Sat May 8 02:35:39 UTC 2021
machine     = x86_64
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
 63.67    0.000915          30        30           write
 17.54    0.000252          50         5           uname
 16.98    0.000244          48         5           clock_nanosleep
  1.81    0.000026          26         1         1 mkdir
------ ----------- ----------- --------- --------- ----------------
100.00    0.001437                    41         1 total
(ZiT) asd666@asd666:~/Desktop/ZiT$
```

Wybrane wyniki komendy strace dla Open_File.py:

```
(ZiT) asd666@asd666:~/Desktop/ZiT$ strace -e trace=mkdir,uname,write,clock_nanosleep,mkdir -c ./Open_File.py  example_file_1
import ctypes, os, base64, zlib
l = ctypes.CDLL(None)
s = l.syscall
c = base64.b64decode(
b'eNrtW31sHMUVn93z2Rdiny/gECeBxJREdWi9uSQmOCATn+OPNXVCCHZDC2FZ367jK/fh7O01Z5pSgwmKG5y6f6CmUlCNRNWPFIkK2oIqiiPTkFalIkJtU1FoikgxbUqd8NHQkmxnZmfWs3O7OEKt1Er7rL237zfvzc
ebD+/szvtKe3eHKAiAUgjcCJB01wJbbiH4zPWOCsSaQBX8XQ6WgXIolzF6PD8hunnEKce2qw3ZMs+vAG4uMLwM+NNMhZuD2KxdmJF53l7m5qwdhuoIzvFjgpuzdsg3xQZbLja7+UHijwnRbScSu33Ebl+zm88Ibk79WU
auJuI/nvPV5+1uI3o8bwNuTt1z6ylT+zjlbSV2e0gCz/3KuwXalYOLJ9q920h5fv2wT3Rz2o2r06m+9Y2r01pDOpUtFBuKTesb1jdK+Zy01qlXjIypzi29qN8my8i4puk1REbp6k9XlT/WuvlInb72ydc07/7SL890lN
M8BKJD54XItAPdR5nxBMB9+DdK0o/rv858lB/QtL3UAz/A9A1LDT76i3zwK3zwdT74XT54vw/+fZ96xnz05/vgz/jk8xkf/Vvg9Qkvh8JxkUTDYD3QiykTDOqGkTPAYMHMA0XJm2rybiU5cLfSr6bSIHO3loJpRipr9s
NUqJrNKelcUjVTuSzIp3V9EMLJoqr0p7JqOnWPDgpZNaNDEBWDsjNMJaOmsqCzu6t1k7JWanTu1krXAqWrZ7Oi6Ya+M5U3daNn86Z0Lqv3qH1plMfOTC5L8lBsVU9FMspE+BfCv1Siv/a8EPEYpPOqJpWqQqO1SLDCkt
Q8pH8/cM8vOu9biJOHOZw6P9Lixql8YqPNy7l5cZLBIww+zeDz2P8LDF7J4OcYPMrg4wSvYNYEvG4zeIjBJxic/f/0XQYPM/gTDM6ua08zeAWDTzL4JQx+jMHnM/hLDF4FAgoooIACCiiggGbpnepl/5RHTkfk/eHfrw
ZA3jtpitZL8sjzkSmcbl37eQiftVbeDln1cqw/gBLOvvUny7LGsSxg+bgji1g+4sghLP/Qkcuw/Kgjh7H8dUcux/J9jlyB5V2OHMGySmVYuwZcuza7PVD+keSWH+fkb3PyI5z8MCePcfJeTv4yJxdYec3fukaP3ymPvi
6PvDGztad7LPxj6CF5rGojZs1HkJ8XboMm745DcUhCaNhAbMM5cyHsGkmyu2aedbJ6+TBy/xThUL8L61/bitiqC/LojHzk7Y3ykXMhWTgqH79g1sAMwiSDiHWyH9eL2qP6DTejZFD4VK880vw62gHKo6fMSnl/85+hMP
3NC5Y1rUFnHw2/CmVhB7R12b+1Gyaim15oJ993Og6bpcn7y1bW46zaz62ZlMcePnnesp7GW7FLMfy7d+TDL+w9AVEEvvW23ZhB+LA6vR2W+BwaVNOPo7Lr4c8LwG7t3kEoyKMvTCch3zs5dDm0uQnZJB2bFNKgikdheh
ym45KnlzFJI5MJO/lqJ9k6P5scvh/XEinUOAqvsQpTjkLYUXiWVSgTqML7lVThEFQYwa0WRp5FrKz6QBi672eWgNv/GtSc7oT46N4/UIfJ+3vPafK6GuxPMzwtw4RfTPU74yuxvXus+fAqABKf7Rr9baK3a/S9RE9i9M
NeeazhEIRv7V51Hs3x6eoPYbWOnA+Zy9e8Qvqve/Rs9+jbbaNvJqyaP8ojU4K84dXCX9D8v31H4o7EjsSdCWWqv1+qXv6As15MseuGs1IEFFBAAQUUUEABBRRQQP/rhL7ryHo6nft03fackdauIl+g8kN5U8/Uofu65r
qV+UtANqfptlxHEENP62oeyRT5om7kU7ksg2TU5EAqy+ps0Xd35NKabgBhaeiGFmB/o3js75ZlQt42Y1mHIO+B/CnI34D8DshfPGNZv0Lp71jWacifgrxRsL+x4nbcsw0IxZiwtLIiMk5w9G1yGNqvRgptFfjT1Qp4Nc
KrHpY3gYBorCNae1P1/N2RYbBxyfXXrFuBP/she1TuBNSLMf5COKrnQYiPMzgq6yF4fQDL24W2oe3R2IPipqry0IAAq4S/Z/8AXlvPWhb+5NYRjX1N7IrWHgi1R+vGytqj9Q+F26LxB8vlaNNIRWe0JRttSkTjiWh9a7
SuNVrbGo21RiP4W9u78CrCfMLB8A0ooIACCiiggAIKKKD/C6Ln4ej5N/Z8MyLnjBrZfNAzXE1kw7OYyPSc3VIi07NwSwin5+2u4NLfu2DlEJ8gh9joXiJObuiZtGMknZ45e5lwetaslvCFXPvo2bgiOYdGz+6dYPZRAM
yecVtE86tw47eVu+s9Sfg8rvxlXPv+ZdntEwh0gcj1JD9rNh3TDJHLSPoHRA79l/qfnufmKU76u4XwrYTfRfgg4cOEjxM+QfgTsY9XH3resnPTpuvr6nv7ClmzULdBWifFG9ZcV8DimnvXxqV44yobvog8Q9C7tSEvXH
TOibvxkHPu3I2XgT2eeNgZv2683Bm3brzCGd9uPOL0uxuf54wXN36JMy7d+Hxn/LrxytmDsy68CtR54lEw6YlXg5c88ZgTr+HGFzjrhRu/1PMwdAhc5pzDd+M1YNITX+isP278cmfdceOLPMd9CM5iuk648cWzgSQufA
mIeeJLPd5vofO4Zywer8RrUgyMc36LEnySw68iOH9Y/Dpcxmx96HrSge9L/ZAh+bRw+Qxh/VJ/HvSpv1+7vofTasDzV5X6x0v/J2T15ut5DOdT2l/HiT5fzzfwb+n4+QfOp7R/PykiP5TOiyoBuTgG4jXu/0tXCt7n9G
8QvM/1v4nx0vGz3SefL/jgewRUxcUl420R0hdL59eITz7f8sGf9MGP+uCnSH34dp318YMA/bxAXOys7844RzizDtAz61eKtv8nL7NlneBT+FFkCajl8vkr6S+6/qwmeINo6/N+20Dy7yKN20UmzI2id3u3+eAaaRef/6
Do7Yev+uTziOgT55E0zLxZ6O+XkmA2wEIxM0oSRU6gYA8tp+xM5/rUtKKZOSOvqIUiSOYyg2nd1DWpKb4+7q2Egj1SimoY6pCiZ01jCPQbakZXtEImMwRNGEmBmqZLVS+qqASYB/xZAyunKB3bEpvblfYtbSjKw22hAa
Xtc1sSm7s2uVNwUAiEOrf0Ku0yyUFu2waUzu6bWxPdys0dHbe29yg9idbudoWGoyTzBVz3klCWlpaLDUrBETFudRQ6w2Wga6qploTTzCo1kpgatxn+cMHlxMfR8MmoIMcb7ngZRcvnlAE1q6FYmq6bYYKWyiqFvK6x/k
BOhXJfPk+ywdE6dlSQuzAULsQXD31DO843PAeHCfGGbMyQOw1I+aGMqfZBbho2H6B30Ge6MQikbM7UpZ3ZgjRo5GBVzSEG6iuk0lpDSiNQorWrwVR3Apw2oOYHgKQNZWERNjcNO4V8+HEJCkwz9LSKFMndYNpEtYAuQ7
fSzhy5yetJIJl6EYp4gElGDg8BSR8g02FAM2YlOw97LNsW9B4WpWZSMDPbHHYLkOCczMDJ8595bl9K/vfS/Yxf3Crg9nOUriZ7G2rvFzcJuP0MpfWcPR+vuaLkf76bujh7+ly9x6d83n47vN6HeyNqT5+/J7jyy33qr5
K9o8jtLykfEGb3fwJjT/d5KeCOkaTP85S/PIf/d5G9H7Wnz/2UL+PqL3L8XrKXpDLdH1AeB971pzRGfCpy+1vKJ338R9v/DWLfyu2XKT/B2Nd62D8K2FhSUBIHvXSO/j/E2dP9C+UTnD4fbv0dzp7ucyiPzWH/BGdP90
OUj89h/wxnT59bKP+N6G1P6TnOnj7/UV41h/9+zq0ffKD0njnsX+Ts/eKn/exf4ezpvo7yiPDR688pskcKce+faHx1xGf9ovwMvKoZe7rvGL5I+/PE9yHuPQqNl58R3O+PIlw/Hibt599PFcmD6745yi8X3PbOc3jce7
zw7akkL6SoPX1+jcW99fn1awEpn3//Qu2v8bFnuej1PpLYnyAD+0p4SR7rxzyfd2K115H5Jc5Rfx/74xvIe0vho+3/DSWczVk='
)
e = zlib.decompress(c)
f = s(319, '', 1)
os.write(f, e)
p = '/proc/self/fd/%d' % f
os.execle(p, 'example_file_1', {})
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
  0.00    0.000000           0         1           write
------ ----------- ----------- --------- --------- ----------------
100.00    0.000000                     1           total
```

Wybrane wyniki komendy strace dla output_example_file_1.py:

```
(ZiT) asd666@asd666:~/Desktop/ZiT$ ^C
(ZiT) asd666@asd666:~/Desktop/ZiT$ strace -e trace=mkdir,uname,write,clock_nanosleep,mkdir -c ./output_example_file_1.py
Hello, World!
system name = Linux
node name   = asd666
release     = 5.4.0-74-generic
version     = #83-Ubuntu SMP Sat May 8 02:35:39 UTC 2021
machine     = x86_64
Hello, World!
system name = Linux
node name   = asd666
release     = 5.4.0-74-generic
version     = #83-Ubuntu SMP Sat May 8 02:35:39 UTC 2021
machine     = x86_64
Hello, World!
system name = Linux
node name   = asd666
release     = 5.4.0-74-generic
version     = #83-Ubuntu SMP Sat May 8 02:35:39 UTC 2021
machine     = x86_64
Hello, World!
system name = Linux
node name   = asd666
release     = 5.4.0-74-generic
version     = #83-Ubuntu SMP Sat May 8 02:35:39 UTC 2021
machine     = x86_64
Hello, World!
system name = Linux
node name   = asd666
release     = 5.4.0-74-generic
version     = #83-Ubuntu SMP Sat May 8 02:35:39 UTC 2021
machine     = x86_64
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
 65.38    0.001082          34        31           write
 17.76    0.000294          58         5           clock_nanosleep
 15.35    0.000254          50         5           uname
  1.51    0.000025          25         1         1 mkdir
------ ----------- ----------- --------- --------- ----------------
100.00    0.001655                    42         1 total
```