



Colombia Hack Agent (CHackA)



Colombia Hack Agent (CHackA)

```
[...] Developer:      Jairo A. García H.      [...]  
[...] Version:       1.0.                  [...]  
[...] Codename:      HACKLAB SANS - Dungeon Server  [...]  
[...] Report to:     chacka0101 @ gmail.com  [...]  
[...] Homepage:      https://github.com/chacka0101/HACKLABS  [...]  
[...] Publication Date: 5/JAN/2017          [...]
```

HACKLAB SANS - Dungeon Server

← → ↻ ⓘ Not secure | dungeon.northpolewonderland.com

About Dungeon

You are near a large dungeon, which is reputed to contain vast quantities of treasure. Naturally, you wish to acquire some of it. In order to do so, you must of course remove it from the dungeon. To receive full credit for it, you must deposit it safely in the trophy case in the living room of the house.

In addition to valuables, the dungeon contains various objects which may or may not be useful in your attempt to get rich. You may need sources of light, since dungeons are often dark, and weapons, since dungeons often have unfriendly things wandering about. Reading material is scattered around the dungeon as well, some of it is rumored to be useful.

Recent adventurers report a new passage has been installed which leads to the North Pole and the lair of a mischievous Elf who will trade for secrets he holds that may aid your quest.

To help you on your quest, here are some commands to get you started:

Overview commands

Command	Action
Help	More information about playing the game
Info	Game Overview, sets the stage

Move commands

Command	Shortcut	Action
North	n	Move north
South	s	Move south
East	e	Move east
West	w	Move west

Hostname:

IP: <http://dungeon.northpolewonderland.com/>

Walkthrough

Download the game:

```
kali@kali:~$ sudo wget -O dungeon.zip  
https://github.com/chacka0101/Hacking_Software/raw/master/dungeon.zip
```

```
kali@kali:~/Downloads$ sudo wget -O dungeon.zip https://github.com/chacka0101/Hacking_Software/raw/master/dungeon.zip  
--2020-03-23 19:20:41-- https://github.com/chacka0101/Hacking_Software/raw/master/dungeon.zip  
Resolving github.com (github.com)... 140.82.114.3  
Connecting to github.com (github.com)|140.82.114.3|:443... connected.  
HTTP request sent, awaiting response... 302 Found  
Location: https://raw.githubusercontent.com/chacka0101/Hacking_Software/master/dungeon.zip [following]  
--2020-03-23 19:20:42-- https://raw.githubusercontent.com/chacka0101/Hacking_Software/master/dungeon.zip  
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 199.232.48.133  
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|199.232.48.133|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 179226 (175K) [application/zip]  
Saving to: 'dungeon.zip'  
  
dungeon.zip          100%[=====>] 175.03K  --.-KB/s   in 0.02s  
2020-03-23 19:20:42 (9.89 MB/s) - 'dungeon.zip' saved [179226/179226]
```

Copy to personal directory:

```
kali@kali:~/Downloads$ cp dungeon.zip /home/kali/Desktop/chacka
```

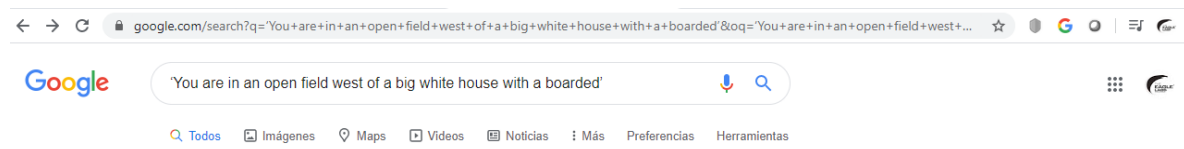
```
kali@kali:~/Desktop/chacka$ unzip dungeon.zip  
Archive:  dungeon.zip  
  creating:  dungeon/  
    inflating:  dungeon/dtextc.dat  
    inflating:  dungeon/dungeon
```

Nos permite interactuar con el texto del juego:

```
kali@kali:~/Desktop/chacka/dungeon$ ./dungeon  
chroot: No such file or directory  
Welcome to Dungeon.                This version created 11-MAR-78.  
You are in an open field west of a big white house with a boarded  
front door.  
There is a small wrapped mailbox here.  
>
```

Ahora debemos averiguar cuales son los comandos de consulta o de debugging:

Googleamos esto: 'You are in an open field west of a big white house with a boarded'



The screenshot shows a Google search interface. The address bar contains the URL 'google.com/search?q=You+are+in+an+open+field+west+of+a+big+white+house+with+a+boarded&loq=You+are+in+an+open+field+west+...'. The search bar contains the text 'You are in an open field west of a big white house with a boarded'. Below the search bar, there are links for 'Todos', 'Imágenes', 'Maps', 'Videos', 'Noticias', 'Más', 'Preferencias', and 'Herramientas'.



Colombia Hack Agent (CheckA)

Squakenet
YouTube - 24 nov. 2014

Pat the NES Punk
YouTube - 11 abr. 2015

Squakenet
YouTube - 25 ago. 2015

es.wikipedia.org › wiki › Zork

Zork - Wikipedia, la enciclopedia libre

Desarrollo[editar]. "Zork" era originalmente una jerga hacker del MIT para un programa inacabado. Los que lo implementaron llamaron al juego completo ...

Plataforma(s): PDP-10, Apple II, Commodore 6...

Modos de juego: Un jugador

Género(s): Aventura conversacional

Desarrolladora(s): Infocom

en.wikipedia.org › wiki › Zork Traducir esta página

Zork - Wikipedia

Zork is one of the earliest interactive fiction computer games, with roots drawn from the original ... Return to Zork (1993, Infocom/Activision), the first fully graphical Zork adventure, with a point-and-click ... Beyond Zork - Zork Zero - Return to Zork - Zork Nemesis - Zork: Grand Inquisitor - Zork: The Undiscovered Underground - Legends of Zork ...

Release: 1977 (PDP-10); 1980 (Zork I); 1981 ...

Engine: ZIL

Developer(s): Infocom

Mode(s): Single-player

Zork I: The Great Underground ... - Return to Zork - Zork Nemesis - Zork II

textadventures.co.uk › games › view › zork Traducir esta página

Zork - Play online at textadventures.co.uk

13 ene. 2014 - Information in this game listing is copyright Erik Temple, Emily Short, Paul O'Brian, is taken from IFDB, and is licensed under a Creative Commons ...

store.steampowered.com › app › Zork_Anthology Traducir esta página

Zork Anthology on Steam

popularizado. Zork también ha sido adaptado a una extensa serie de libros. Wikipedia

Modos de juego: Un jugador

Desarrolladora(s): Infocom

Fecha(s) de lanzamiento: 1977 - 1979

Género: Aventura conversacional

Diseñadores: Marc Blank, Dave Lebling, Brian Moriarty, Steve Meretzky, Tim Anderson, William Crowther, Bruce Daniels

También se buscó

Ver 15 más



King's Quest



Leisure Suit Larry



Quest for Glory



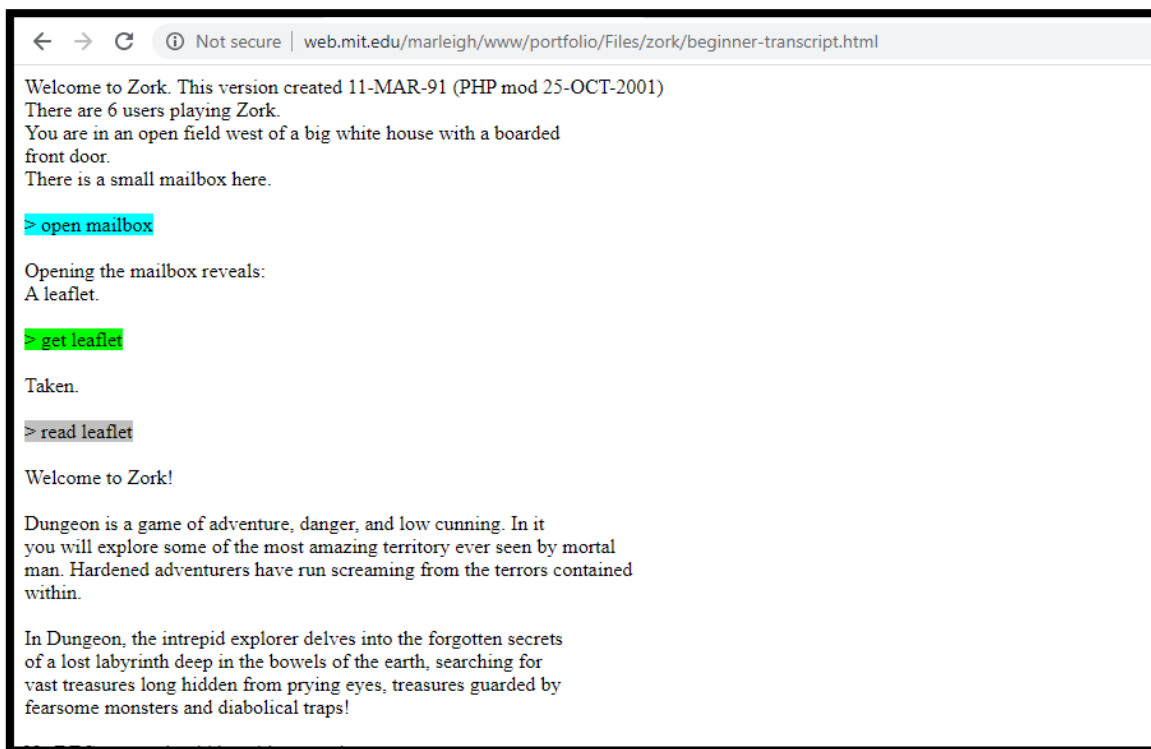
Monkey Island

Reclamar panel de conocimiento

Comentarios

También tenía un comando del *gdt* (game debugging technique) (técnica de depuración de juego) una referencia al DDT debugger que permitía al jugador mover cualquier objeto (incluyendo al mismo jugador) a cualquier cuarto. El uso del gdt requería contestar a una pregunta al azar que necesitaba del conocimiento profundo del juego. La respuesta del juego a una respuesta incorrecta ("una voz explosiva decía 'Error, cretino' y te dabas cuenta que habías sido convertido en una pila de polvo") aparecía en muchas "galletas de la fortuna" de bases de datos.

<http://web.mit.edu/marleigh/www/portfolio/Files/zork/beginner-transcript.html>





Verify GDT (Game Debbuging Technique):

```
kali@kali:~/Desktop/chacka/dungeon$ ./dungeon
chroot: No such file or directory
Welcome to Dungeon.                This version created 11-MAR-78.
You are in an open field west of a big white house with a boarded
front door.
There is a small wrapped mailbox here.
>GDT
GDT>help
Valid commands are:
AA- Alter ADVS          DR- Display ROOMS
AC- Alter CEVENT        DS- Display state
AF- Alter FINDEX        DT- Display text
AH- Alter HERE          DV- Display VILLS
AN- Alter switches      DX- Display EXITS
AO- Alter OBJECTS       DZ- Display PUZZLE
AR- Alter ROOMS         D2- Display ROOM2
AV- Alter VILLS         EX- Exit
AX- Alter EXITS         HE- Type this message
AZ- Alter PUZZLE        NC- No cyclops
DA- Display ADVS        ND- No deaths
DC- Display CEVENT      NR- No robber
DF- Display FINDEX      NT- No troll
DH- Display HACKS       PD- Program detail
DL- Display lengths     RC- Restore cyclops
DM- Display RTEXT       RD- Restore deaths
DN- Display switches    RR- Restore robber
DO- Display OBJECTS     RT- Restore troll
DP- Display parser      TK- Take
GDT>
```

Nos permite interactuar con el texto del juego, pero poder saber el texto completo, nos llevaría mucho tiempo, así que lo mejor es crear un script:

```
kali@kali:~/Desktop/chacka/dungeon$ ./dungeon
chroot: No such file or directory
Welcome to Dungeon.                This version created 11-MAR-78.
You are in an open field west of a big white house with a boarded
front door.
There is a small wrapped mailbox here.
>GDT
GDT>DT
Entry: 1
Welcome to Dungeon.                This version created 11-MAR-78.
GDT>2
?
GDT>3
?
GDT>4
?
GDT>
```

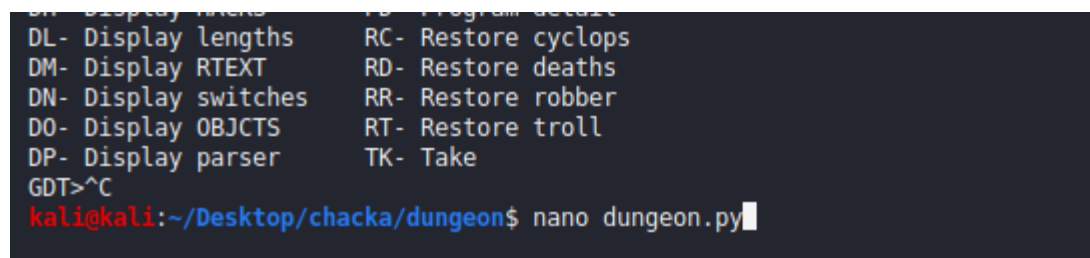
Debemos crear un script en Python para extraer todo el texto del juego y poder comprender así mejor su funcionamiento. Para facilitar el proceso lo vamos a realizar con el módulo de python pwntools:

Requerimiento, instalar:

<https://docs.pwntools.com/en/stable/install.html>

```
$ apt-get update
$ apt-get install python2.7 python-pip python-dev git libssl-dev libffi-
dev build-essential
$ pip install --upgrade pip
$ pip install --upgrade pwntools
```

Creamos el script:



```
DL- Display lengths      RC- Restore cyclops
DM- Display RTEXT        RD- Restore deaths
DN- Display switches     RR- Restore robber
DO- Display OBJECTS      RT- Restore troll
DP- Display parser       TK- Take
GDT>^C
kali@kali:~/Desktop/chacka/dungeon$ nano dungeon.py
```

```
#!/usr/bin/env python
import sys
from pwn import *

binary = './dungeon'
p = process(binary)

p.recvuntil('>')
p.sendline("GDT")
p.recvuntil('GDT>')
i=8
while True:
    i+=1
    p.sendline('DT')
    p.recvuntil('Entry')
    p.sendline(str(i))
    print i
    print p.recvuntil('GDT>')[:-5]
```



```
kali@kali: ~/Desktop/chacka/dungeon
File Actions Edit View Help
GNU nano 4.8 dungeon.py
#!/usr/bin/env python
import sys
from pwn import *

binary = './dungeon'
p = process(binary)

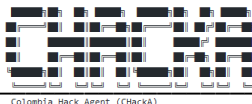
p.recvuntil('>')
p.sendline("GDT")
p.recvuntil('GDT>')
i=8
while True:
    i+=1
    p.sendline('DT')
    p.recvuntil('Entry')
    p.sendline(str(i))
    print i
    print p.recvuntil('GDT>')[:-5]
```

```
DN- Display switches      RR- Restore robber
DO- Display OBJECTS      RT- Restore troll
DP- Display parser       TK- Take
GDT>^C
kali@kali:~/Desktop/chacka/dungeon$ nano dungeon.py
kali@kali:~/Desktop/chacka/dungeon$ sudo python ./dungeon.py
```

Ejecutamos el script y nos permite revisar todo el texto:

```
kali@kali:~/Desktop/chacka/dungeon$ sudo python ./dungeon.py
```

```
1268
:
1269
:
1270
:
1271
:
1272
:
1273
:
1274
:
1275
:
1276
:
1277
:
1278
:
1279
[*] Process './dungeon' stopped with exit code -11 (SIGSEGV) (pid 20645)
Traceback (most recent call last):
  File "./dungeon.py", line 18, in <module>
    print p.recvuntil('GDT>')[:-5]
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/tube.py", line 310, in recvuntil
    res = self.recv(timeout=self.timeout)
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/tube.py", line 82, in recv
    return self._recv(numb, timeout) or b''
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/tube.py", line 160, in _recv
    if not self.buffer and not self._fillbuffer(timeout):
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/tube.py", line 131, in _fillbuffer
    data = self.recv_raw(self.buffer.get_fill_size())
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/process.py", line 707, in recv_raw
    raise EOFError
EOFError
kali@kali:~/Desktop/chacka/dungeon$
```



Columbia Hack Agent (Checka)

En la linea 1024 aparece una pista:

1024

: The elf, satisfied with the trade says -
Try the online version for the true prize

```
kali@kali: ~/Desktop/chacka/dungeon
File Actions Edit View Help
1016
: Avoiding the thief's stiletto, you stumble to the floor, dropping
your #.
1017
: The thief, a man of good breeding, refrains from attacking a helpless
opponent.
1018
: The thief amuses himself by searching your pockets.
1019
: The thief entertains himself by rifling your pack.
1020
: The thief, noticing you beginning to stir, reluctantly finishes you off.
1021
: The thief, forgetting his essentially genteel upbringing, cuts your
throat.
1022
: The thief, who is essentially a pragmatist, dispatches you as a threat
to his livelihood.
1023
: The elf, willing to bargain, says "What's in it for me?"
1024
: The elf, satisfied with the trade says -
Try the online version for the true prize
1025
: "That wasn't quite what I had in mind", he says, tossing
the # into the fire, where it vanishes.
1026
: The elf appears increasingly impatient.
1027
: The elf says - you have conquered this challenge - the game will now end.
1028
:
1029
:
1030
:
1031
:
1032
:
```

La version online es dungeon.northpolewonderland.com, escanemos los puertos de dungeon.northpolewonderland.com y encontramos un Puerto asociado a Zork:

kali@kali:~/Desktop/chacka/dungeon\$ nmap -sV -sC -vvv
dungeon.northpolewonderland.com

```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh      syn-ack OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 a5:e0:ff:71:97:3f:79:59:82:cf:2c:f5:7b:cf:f7:e4 (DSA)
|_ ssh-dss AAAAB3NzaC1kc3MAAACBAJTH4sm1IKpkzTJbAYn30IKJgoXXsYR3uACsTJxxPqqsDFKIDxHlbnk10zy+4gIXre16T8cB43gupKG4WfKye3Hque+I5eg/6qKNLch4kHJdJ2R1z4H6Dxi9DRif92xPhKt
in5H5G7btsZsGvOkZ9nTgQpJWR7EhNCnt/HTAAAFQClpGBZWyPbrGkQXSEJBMtotsFpHQAAIA00J0A0+aE62H0nE1o5bCLK8zPhPv+uPgsaHg0Geg011Vad1aBYcdqnIPWhh3G4opovL5tVRWuAtVo+cdYKtm5N
GvgChvzE4XVXG9R9SUDMS6H0v+PKZZi+j9L+QeetPXDFHFd30csnovavh0rBHXH5Wj0Crmm8n39yP1bw1N0AAAB1B1actxY4w+2Kz2J5ayYUPGAR7pmFR+DXTw64ks+NN0YwZvRgtax28WaaJ1RnzaRP30J1ij20HqG
s50dn/nkSbmW9Rw03jw1V011n3B1t7700jsvstVK+whhP7z0UBPK8FpQZcnbbdRhmGera0VL9ZyACSSXzq9nrdJtg==
|_ 2048 4e:8e:42:5a:07:57:82:16:4c:55:00:70:5c:52:fe:9f (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCG6yVZ/i1C4k1aJUScNKPOFNx3VTh6AIKlB+0VdJ+gpbcd4dxBilGTaCmmu3h2/0wjfPKucJUULOVbYtAib6/F6T/wdLU2S29YL6197g810n/uQcaeHVuCIF6k
jqtUNE7W7guTxBMMCA1m9e9gu0ge6t8JbA060+LK8GGqLHaH0Pvd3iulJPZz40GXzKIYpmqnc0Zgi3618SH9Tnbgclcy0SPsN0fk/+Yy4vNtjR4LT/GXP1bw2/j3oeQxjsMzPsFS7CL68YwR4B0Yg7jjN+TgHpx0QV8z
Rk4a0Y4rizGFCokwZ/H0lt/qnKMaHLLF7jE5fo9se3VR7zPHkeshXD
|_ 256 e9:d6:97:d3:f7:03:54:75:67:8d:96:d3:36:90:6a:eb (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBhZ7bnMn3UvOk+4VUqyG8+Cx8HaL68Kajn981PagRJi6LnpN4rgmSyGfqPYFVCVPI8Qt1shGikmdTJ4BtetQk=
|_ 256 63:63:ca:cc:93:35:01:b3:dd:da:94:e9:0d:28:d2:27 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDtIpJg+5XpfaaBYKqGv8IDchwR02Lo+ic94LSGL+Xcd
25/tcp    open  smtp     syn-ack
|_ smtp-command: Couldn't establish connection on port 25
80/tcp    open  http     syn-ack nginx 1.6.2
|_ http-methods:
|_ Supported Methods: GET HEAD
|_ http-server-header: nginx/1.6.2
|_ http-title: About Dungeon
|_ 1111/tcp open  mud      syn-ack Zork Dungeon MUD (11-MAR-78)
Service info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



Colombia Hack Agent (Checka)

Intentamos hacer un banner grabbing con netcat y nos permite ejecutar el debugger GDT, por lo que le vamos a enviar el dato 1024 que es el dato de la línea misteriosa:

```
kali@kali:~/Desktop/chacka/dungeon$ nc dungeon.northpolewonderland.com
11111
```

Finalmente logramos el objetivo que es el de obtener el correo electrónico:

```
kali@kali:~/Desktop/chacka/dungeon$ nc dungeon.northpolewonderland.com 11111
Welcome to Dungeon.                This version created 11-MAR-78.
You are in an open field west of a big white house with a boarded
front door.
There is a small wrapped mailbox here.
>GDT
GDT>help
Valid commands are:
AA- Alter ADVS          DR- Display ROOMS
AC- Alter CEVENT        DS- Display state
AF- Alter FINDEX        DT- Display text
AH- Alter HERE          DV- Display VILLS
AN- Alter switches      DX- Display EXITS
AO- Alter OBJECTS       DZ- Display PUZZLE
AR- Alter ROOMS         D2- Display ROOM2
AV- Alter VILLS         EX- Exit
AX- Alter EXITS         HE- Type this message
AZ- Alter PUZZLE        NC- No cyclops
DA- Display ADVS        ND- No deaths
DC- Display CEVENT      NR- No robber
DF- Display FINDEX      NT- No troll
DH- Display HACKS       PD- Program detail
DL- Display lengths     RC- Restore cyclops
DM- Display RTEXT       RD- Restore deaths
DN- Display switches    RR- Restore robber
DO- Display OBJECTS     RT- Restore troll
DP- Display parser      TK- Take
GDT>DT
Entry: 1024
The elf, satisfied with the trade says -
send email to "peppermint@northpolewonderland.com" for that which you seek.
GDT>
```

Agradecimientos a:

SANS - <https://holidayhackchallenge.com/2016/>
IppSec - <https://www.youtube.com/watch?v=hWC7mlIYOtU>

-END-