



Game name: Hacker Evolution
Developer: exosyphen studios
Website: <http://www.exosyphen.com>
E-mail: office@exosyphen.com

Hacker Evolution – Complete game walkthrough

First level – Tutorial

There is no need for a walkthrough for this level, as everything is self explanatory in this level.

Level 1 - The beginning

Your first objective is to retrieve the connection log file from the New York Exchange server. The server is visible on the map, under the name:

ny-exchange.com

If you run a scan on it (scan ny-exchange.com), you will notice there are 2 open ports:

Port 80, running a standard http service (you can connect on this port),

Port 99, running a file manager service

You will need access on port 99, in order to be able to download the connection.log file. Don't try the crack command, as you will be most likely traced. There are 2 ways in which you can hack the password for this service.

If you connect to ny-exchange.com (on port 80), you can follow the server of the company who designed the page (see the bottom line of the screen displayed after connecting). The server is xenti-design.com. Scan it, so it will show up on your target map. It's unprotected, so you can bounce through it. Click on it, to add it to the bounced link. Now you can crack the password for the file manager service on port 99, by typing:

crack ny-exchange.com 99

The second way is to locate the hackers server. You can find it if you look through the files available on port 80 on ny-exchange.com (The server is : dot-hackers.net) Scan it, to reveal it on the target map. It has only port 80 open, but it's only protected by a 4 characters password which you can easily crack. It's also encrypted by with a 128 bits key, which you can easily decrypt. You can use this server to bounce through, and crack the password on port 99 on ny-exchange.com, but it's recommended that you download the x-filemanager.exploit from it, and use that instead. Also, there is \$2000 available on the server, so you might want to transfer that money into your account.

Note: Using an exploit instead of the crack command, ads less global trace percentage to your total trace.

Once you downloaded the exploit, use it like this: exec x-filemanager.exploit ny-exchange.com

All done now. Connect to ny-exchange.com on port 99: and download the connection.log file:

connect ny-exchange.com 99

download.connection.log

Next, look inside the connection.log file (Type: cat connection.log), and attempt to identify the source of the attack. You will find several hostnames inside. Use the scan command to see which hosts actually exist (it will show up on the map).

Once the server shows up on the map, your second objective is completed.

Next, you must upload a copy of the connection.log file, to the FSA file server. This is simple:

connect files.fsa.gov 81

upload connection.log

The third objective is now completed.

For the next objective, you must retrieve the users.log file from terminal-83.xenti.com. You must crack and decrypt this host before being able to connect to it. Don't try it directly, as you will get traced. Setup a bounced link first, by clicking on as many hosts as possible, on the target map. After the bounced link is setup, type:

decrypt terminal-83.xenti.com

crack terminal-83.xenti.com

After it's finished, you have to connect to it, and download the users.log file. First, notice that there isn't enough space on your server to download the file. You can either upgrade your memory modules, or deleted some unneeded files. Delete the connection.log file. Type:

delete connection.log

Next, you must identify which user was logged into terminal-83.xenti.com at the time of the attack. The time of the attack was: [12/20/2015][11:59:44]. You can deduct this from the following line in the connection.log

file:

[12/20/2015][11:59:44] - authorized connection from terminal-83.xenti.com

Next, see the users.log file, and see who was logged in at that time. The username is: tjohn. Keep this in mind. Type:

scan xenti.com

to reveal the host on the map, as this is your next target.

You must decrypt and hack xenti.com. Setup a bounced link first, as you will get traced if you do it directly.

Type:

decrypt xenti.com

crack xenti.com 210

Note: If you have trouble hacking this host (you are being traced), you can use the available money to either upgrade your firewall, or reduce your trace time (use the KILLTRACE command).

Tip: When using bounced links, don't use more hosts than needed. You can only bounce through a host, 3 times.

Now, connect to xenti.com and download tjohn's profile:

connect xenti.com 210

download tjohn.profile

Logout, and connect to files.fsa.gov to upload the file and complete the last objective.

logout

connect files.fsa.gov

upload tjohn.profile

Level 2 – Xenti Space Station

It is worth to upgrade firewall in this level. In order to upgrade your firewall to level 1, use the following command :

upgrade fw1

You can alternatively upgrade your CPU (**upgrade cpu0**). In both cases you will be able to crack 8 characters passwords and decrypt 256 bit encryptions .

After this upgrade you can decrypt and crack 99 port of control-center.xenti.com. If you don't have any upgrades you can crack and decrypt **xenti.com** first and use it in a bounced link. Retrieve **connection.log** from this server. The first objective is now completed.

Note: If you delete this file from your localhost, the objective remain completed. Use this trick if you don't have enough free space.

When you download **connection.log** you will see a message from root@dot-hackers.net which offers you a good deal. Scan **dot-hackers.net** to reveal it on the map, and upload the file for them:

scan dot-hackers.net
connect dot-hackers.net 99
upload connection.log

Hackers fulfill their promise and give you **atm.ce-bank.com**. Scan and crack it. It has a very low protection, so you even don't need bounce links. Transfer all the money from it. Also you can download **connection.log** and spot **terminal-83.xenti.com**. The other way to spot **terminal-83.xenti.com** is inside the **connection.log** file on **files.fsa.gov server**. There are several unsuccessful attempts to login from this server.

Note: All files with the same name are equal for the game objectives. You can download **connection.log** from : control-center.xenti.com, atm.ce-bank.com or even files.fsa.gov to complete the first objective.

Now you have more than enough servers for bounced links.

Hack : **control-center.xenti.com**. Connect to the server, type **ls** and spot **tj.bin** file. Delete it to complete the second objective.

The next objectives is **xenti.com**. It has low protection, so you can crack and decrypt it without bounce links. Download **history.log** from this server and upload it to **files.fsa.gov**.

You receive message from john.davis@fsa-gov.main. He noticed that the source of the attack was the same, as in the attack on ny-exchange.com. So it is **terminal-84.xenti.com** as you should remember. Scan it and finish the level.

Level 3 – Checkpoint

In order to complete this level you must have a firewall or cpu upgrade.

First objective. In order to retrieve the **connection.log** file from **interlink.net**, you need to find a password on the secure authorization server. Its name can be easily guessed: **sec.interlink.net**. Scan, decrypt and crack it. Connect to the server and type ls. You will see the **passwd** file. You will find the password, inside the file.

Decrypt the **interlink.net** server using 1 server in the bounced link and then use the login command with the password you have. You will see that the password has matched the service on 150. Connect on this port and download the **connection.log** file. Also, transfer the \$3000 available here.

You receive a message from dot-hackers. They will offer you useful information in exchange for the file. Scan **dot-hackers.net** and upload the file on port 99.

The interesting information is on **xterm.xenti.com**. Use 1 server in the bounced link to decrypt it and crack the service on port 151. Port 23 is lightly protected and it can be cracked without the use of bounced links. This server has some interesting files. You have to download **e-receipt.log** for the second objective, **monitor.bin** for the third objective and **conmanager.bin** for the last objective. Also read xconmanager.bin file. You will have to delete this file.

The last objective is **interlink.net**. Crack the service running on port 152, using 1 server in the bounced link. Connect on this port, and replace **xconmanager.bin** file with **conmanager.bin**. This allow server to reestablish the links and you will complete the level.

Tip: You can find **terminal-83.xenti.com** by looking inside the **connection.log** file on **interlink.net**. If you crack it, you can see **ns1.sdb.com** in the **remote.log** file. It has \$5000 and moderate protection. This is the rewarding way mentioned in the second objective.

Level 4 – Nothing is random

Issue a scan on **cb-asia.com**. You will notice a service linking to **atm.au-bank.com.au**
Hack **atm.au-bank.com.au** and transfer \$4000 from it

Upgrade to a second 1 Ghz cpu (**upgrade cpu0**) and use the remaining money to reduce your trace.

Decrypt cb-asia.com. Crack cb-asia.com (port 80). Connect, and download the connection.log file. Your first objective is completed.

On the welcome screen of cb-asia.com, you will notice an email address : **services@ns.cb-asia.com**

Scan **ns.cb-asia.com**. Crack and decrypt it and then transfer the \$4000 from it.
Now, connect to **dot-hackers.net** on port 99, and upload a copy of **connection.log**.

You will receive a message with a hint. Crack the service running on port 110, on **cb-asia.com**
Connect on port 110, and download the hash file.
View it's content (cat), and reconstruct the password based on the instructions.
Use the login command to gain access to the transaction manager service

```
sdsd  3434  ddfd  dasd  
[txty] dsdd  xcef  3342  
edcv  [qwsa] 4322  dssd  
sads  dwed  [1324] dedx  
[fdsz] dsds  ewwe  sdsd
```

login cb-asia.com txtyqwsa1324fdsz

Now, connect on port 110 on cb-asia.com, and download the transaction.log file
(Before connecting, delete some files from your localhost, to have room for the download).
Your second objective is now completed.

Upload a copy of the file to the dot-hackers.com server. You will then receive a password wich you can use to connect to their server and download a report.

connect dot-hackers.net 98 download report

Read it ... it's interesting.

Next, you might want to crack dot-hackers.net (port 80) and look around. (Use the killtrace command to reduce your trace level).

In the **news.txt** file, you will learn about a contest at **black-haxors.com**
Also, there are some exploits available. Download them.
Hack black-haxors.com and transfer the money from there.

Next, look inside the transaction.log file

The suspicious transaction is this :

```
43545456546456      USD 1.232.002.123      ch548755
```

Reconstruct the hostname : **scan ch548755.bank.com**

The 3rd objective is now completed.

Next, hack the service running on port 100 on **cb-asia.com**, connect on port 100, and delete the **tj.bin** file.
The 4th objective and the level are now completed.

Tip: before completing the 4th objective, you can go ahead and hack all services on all servers, to receive a special achievement bonus at the end of the level (500 score points).

Level 5 – Rundown

In this level, you have to hack the 4 firewalls, in the correct order. The order is not random and there is a logic behind it.

Issue a scan on all 4 firewalls. If you sort them based on the strength of the encryption key size, and password length, you will notice that the correct order in which you must hack them is:

firewall-2.xenti.com
firewall-1.xenti.com
firewall-4.xenti.com
firewall-3.xenti.com

Hack the 4 firewalls, in the above order.

Tips:

- Transfer the money from each firewall, and use it to reduce your trace level
- If you connect to firewall-1.xenti.com, you will notice a hint about : firewall.xenti.com scan it, and keep it for later.
- Use bounced links to easily crack and decrypt the firewalls that have stronger encryption.

Next, scroll back to the first message, to construct the password for core.xenti.com

Type:

login core.xenti.com

in your console, and scroll through the messages, and type in each 8 character sequence

login core.xenti.com 11111111999999992222222277777777

After that, decrypt the encryption key for core.xenti.com

Next, crack the password on port 402 on core.xenti.com

Now, connect to core.xenti.com on port 402.

Before deleting the core.code file, look inside it.

You will find a hint to : **n e s s i e . c o r e - x e n t i . c o m**

Scan, and then hack nessie.core-xenti.com to complete another level objective.

This is the Xenti Corporation backup server.

Next, crack and decrypt, **firewall.xenti.com** After that, connect to it and transfer the available money. Also, download the **serverfreeze.code** file.

Now, connect to core.xenti.com and upload the serverfreeze.code file.

The level is now completed.

Level 6 – The chase

The first step is to decrypt and hack all services on **xterm.xenti.com**

decrypt xterm.xenti.com

crack xenti.com 23

crack xenti.com 115

crack xenti.com 151

Next, connect to xterm.xenti.com on port 23.

Look inside the activity.log file. You will find a reference to **wi-fi.jd.xenti.com**. Scan to reveal it on the map. Also, transfer the money from **xterm.xenti.com**

Add xterm.xenti.com to the bounced link setup, and then proceed to decrypt wi-fi.jd.xenti.com

Next, crack the service running on port 808 on **wi-fi.jd.xenti.com**

Now, logout, and connect again on port 23 to xterm.xenti.com.

Look inside the **e-receipt.doc** file.

You will find a reference to **atm-5.sdb.ch**. Scan it to reveal it on the map.

Now, setup a bounced link through xterm.xenti.com and wi-fi.jd.xenti.com

Decrypt and crack atm-5.sdb.ch

Transfer the money from it.

Buy a 2Gb memory module upgrade:

upgrade mem1

Now, connect to wi-fi.jd.xenti.com and download the **dhcptable** file. The first objective is now completed.

If you look inside the dhcptable, you will notice that laptop-nessie is the name of John Davis's laptop. Next,

connect to xterm.xenti.com on port 115. Look inside the mail file. You will find a hint to **flyblue-air.com**.

Scan it to reveal it on the map.

Decrypt it's encryption key.

Next, hack the service running on port 99 on flyblue-air.com

Next, connect on port 99 to flyblue-air.com and look inside the index.old file

You will find a reference to **wifi.flyblue-air.com**

Scan it to reveal it on the map

Decrypt and crack **wifi.flyblue-air.com**

Connect to it on port 808 and look inside the dhcptable1.file

You will find John Davis's laptop connected and his IP address : **192.168.1.120**

Scan it to reveal it on the map. Decrypt and crack it. Connect to it on port 102, and download the archive.bin file.

Next, connect to dot-hackers.net on port 99, and upload the archive.bin file to their server.

The second level objective is now completed.

You will need a copy of the monitoring trojan.

You can find it on **atm-5.sdb.ch**. Connect to it, and download the monitor.bin file.

Next, connect to **192.168.0.120** and upload a copy there. The third level objective is now completed.

Next, crack the reservations service running on port 100 on **flyblue-air.com**.

Connect to **xterm.xenti.com** on port 115, and in the emails you will find the reservation id number.(34723).

Connect to flyblue-air.com on port 100, and delete the 34723 file. The fourth objective is now completed.

Reduce your trace level below 20% to complete the level.

Level 7 – Deja vu

When you start the level, you have one target on the map: **c-core.worldmed.com**

It's encryption is too strong to be decrypted by default. You can risk a trace, or, if you look at the level intro text, and the message, that arrives after the level is started, you can discover a new host:

ns.dot-hackers.net

Hack it. Connect to ns.dot-hackers.net, and look inside the files. Inside **named.conf**, you will find a reference to **atm-3.sdb.ch**.

Hack it and transfer the money from it.

(You can also download a good exploit : **x-filemanager.exploit**)

Use the exploit to hack the service running on port 181 on **c-core.worldmed.com**

You can use atm-3.sdb.ch and ns.dot-hackers.net, to setup a bounced link, and hack into **c-core.worldmed.com**.

Now, connect to c-core.worldmed.com on port 180, and look inside the call_records file.

You will notice a data call lasting 30 minutes, exactly the duration of the attack.

The number is : **555-3234-1122**

Next connect on port 181, and look inside the call_config file. You will notice the logic of modem hosts, associated with phone numbers : **NUMBER.nphone.com**

Run a scan on **555-3234-1122.nphone.com**.

Your first objective is now completed.

Next, hack into **555-3234-1122.nphone.com** and then connect to it. In the modem.conf file, you will find a reference to xenti.nphone.com. Scan it and hack it.

Connect to **xenti.xphone.com**

Download the **worldmed-dna.seq** file.

Your second objective is now completed.

Delete the worldmed-dna.seq file and your third objective is completed.

Make sure your trace level is reduced below 10%, to be able to finish the level.

Level 8 – The Maze

When you start the level, you receive a hint that you should have started this yesterday. Today is the 29th, so **28.xmaze.net** is the entry in the maze. Hack it, and the first objective is completed.

Connect to **28.xmaze.net**

Look inside the **hint-28** file. There is a hint to download it. Download it, and you will receive a message. You will notice the number 24 in the message. Your next host is : **24.xmaze.net**. Hack it, and the second objective is completed.

Connect to **24.xmaze.net** Look inside the hint file, and try to find the next 2 digits. You will notice it's 26, from this line :

```
if [ $? -ne 26 ] ; then
    echo "Failed" ;
    exit -1 ;
fi ;
echo "OK" ;
echo "Connect" ;
nice 26 pppd call adsl updetach
if [ $? -ne 0 ] ; then
    echo "Connexion failed" ;
    exit -1 ;
fi ;
```

The next server is **26.xmaze.net**. Hack it, and the 3rd objective is completed.

Connect to 26.xmaze.net and look inside the hint file. You have a matrix:

```
// The column that has the smallest number and
// the line that has the biggest number, are your next step in the maze
6 [2] 3 4 5 3
5 4 5 6 3 3
3 3 6 4 5 4
6 6 5 4 4 3
5 3 4 5 3 6
4 6 6 5 5 4
[7] 3 4 4 5 6
```

The smallest numbers is 2, on column 2. The biggest numbers is 7, on line 7
So, the next server is : **27.xmaze.net**

Hack it, and the fourth objective is completed. This server also contains a hint to xmaze.net. Hack it, and grab the money from there.

Connect to 25.xmaze.net

If you look inside the hint file, and solve the math code, the result will be 22, so the next server is **22.xmaze.net**. Hack it, and your fifth objective is completed.

Connect to **22.xmaze.net** and look inside the hint file.

There is a riddle :

"If you add the next server's digits, the result will be half the number of servers in the maze"

There are 16 server in the maze.

Half, is 8.

The only server which's sum of digits it's 8, is : **35.xmaze.net**

Hack it, and download the dnaseq-35 file. The sixth objective and the game level are now completed.

Level 9 – End

After starting the level, you receive a message. Notice the hostname in the email address :

ns.dot-hackers.net

Hack it, and transfer the money from there. Use the money to reduce your trace level.

Connect to **ns.dot-hackers.net**. Look inside the named.conf file. You will notice a link to:

ns2.dot-hackers.net

Also, download the **name_services.exploit** file

Decrypt ns2.dot-hackers.net. Use the exploit to hack the service on port 53. Crack the password on port 80.

Connect to ns2.dot-hackers.net and look in the cache file.

You will find the 4 firewalls, and their order (notice the word REVERSE).

The correct order to hack them is :

fwall-00.xenti.com

fwall-64.xenti.com

fwall-23.xenti.com

fwall-34.xenti.com

Hack all 4 firewalls.

When you connect to the last firewall, you will notice a hint to **aicore.xenti.com**. Decrypt it.

Next, concatenate the strings from the 4 messages to obtain the password, and use it to hack into:

aicore.xenti.com

login aicore.xenti.com tty3322xxzz4455uupp8888kkcc7777

connect to aicore.xenti.com and download : **tty3322xxzz4455uupp8888kkcc7777.bin**

Your first objective is now completed.

Next, delete tty3322xxzz4455uupp8888kkcc7777.bin from aicore.xenti.com.

The game is now completed.