CUDA CRACKING

PRESENTED BY: ROHIT SHAW
XIARCH SOLUTIONS PVT LTD
NEW DELHI
CUDA Cracking

**Compute Unified Device Architecture** (CUDA) is a parallel computing architecture developed by Nvidia for graphics processing. CUDA is the computing engine in Nvidia graphics processing units (GPUs) that is accessible to software developers through variants of industry standard programming languages.

**Introduction:** Cuda cracking means cracking passwords with the help of Graphics card which have GPU, it means the speed of password cracking is much faster than CPU speed.

**Building a CUDA Machine:** For building a monster cuda machine we have to invest a huge amount on it. First we have to select a motherboard which supports more than one GPU because the more GPU means the process of password cracking is much faster. I suggest MSI Big Bang Marshall Motherboard which supports multiple GPUs up to 8 graphic cards. Another unique feature of this motherboard that it is cross platform GPU supportable it means it can support both ATI and Nvidia graphic cards at a time. Use Quad core processors or Intel’s I family processors for better performance. RAM up to 16 GB is efficient for this motherboard. Another important thing to keep in mind that is the power supply system we have to supply up to 1250 watt power to this machine. Also use cooling fans as much as possible because during process graphic cards heats very intensively.
**Graphic Card Selection:** Graphic card selection is the core important thing before assembling a cuda machine. Before investing in graphic card first decides which graphic cards has much cuda cores. Graphics card runs on cuda core it means the number of core is high then the password cracking performance is also high. Also keep in mind which motherboard is you are using because all graphic cards did not compatible with all motherboards. We can see the list of GPU estimations and map the performance of card according to your budget.

<table>
<thead>
<tr>
<th>ATI Radeon HD 5XXX/68XX series</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GPU Name</strong></td>
</tr>
<tr>
<td><strong>SP/ALU count</strong></td>
</tr>
<tr>
<td><strong>Clock rate</strong></td>
</tr>
<tr>
<td><strong>Peak perf with integers</strong></td>
</tr>
<tr>
<td><strong>Single MD5 speed</strong></td>
</tr>
<tr>
<td><strong>Single SHA1 speed</strong></td>
</tr>
<tr>
<td><strong>MS Office 2007 speed</strong></td>
</tr>
<tr>
<td><strong>WinZip/ AES speed</strong></td>
</tr>
<tr>
<td><strong>WPA speed</strong></td>
</tr>
<tr>
<td><strong>BL3 unclock time</strong></td>
</tr>
<tr>
<td><strong>Price</strong></td>
</tr>
<tr>
<td><strong>SHA1 perf. per s</strong></td>
</tr>
</tbody>
</table>

We can see the list above here you see that SP/ALU count column it refers the no. of cuda cores and also see the cracking speed of hashes like MD5, SHA1, WPA and more. Here we are using Radeon HD 5970 and it has 3200 cuda cores that why the cracking speed is much pretty good.
Now after card selection you have to select a proper GPU supported tool from which you will able to crack hash. There are many tools which supports GPU processor. Tools are based on operating systems some tools are Windows Supported and some of them are Linux supported. We are going to now describe some tools according to operating system compatibility.

**WindowsSupported Tools:**

**IGHASHGPU:** This tool is developed by Ivan Golubev. This tool can crack only three hashes SHA1, MD5 and MD4. It is compatible with ATI and Nvidia cards. The ATI cards which supports are Radeon HD 4550, 4670, 4830, 4730, 4770, 4850, 4870, 4890, 5750, 5770, 5850, 5870, 5970 and Nvidia cards with CUDA support.

**BarsWF:** BarsWF is developed by Svarichevsky Mikhail. It supports on Nvidia cards and also known as world’s fastest MD5 cracker. Hash supports only MD5.

**Extreme GPU Bruteforcer:** It is a commercial tool developed by InsidePro. It supports total 58 types of hashes MD5, MD4, NTLM, SHA-1, SHA-512 and many more. Utilizing the power of multiple graphics cards running simultaneously (supports up to 32 GPU), the software allows reaching incredible search speeds of billions of passwords per second. It supports only Nvidia cards.

**Lightning Hash Cracker:** Lightning Hash Cracker is developed by Elcomsoft and it is a freeware tool. It supports only MD5 hashes and Nvidia compatible.

**Oclhashcat Plus:** It is a popular hash cracker tool and it supports ATI and Nvidia cards simultaneously. It works on Windows and Linux based operating systems. Multi GPU supports up to 128 cards. It supports 57 types of hashes.

**Cryptohaze Multiforcer:** It is an open source tool. This is only a tool which can used on network based password cracking so multiple systems can work on the same. It supports 17 types of hashes MD5, MD4, NTLM, LM and more. It supports only Nvidia cards are 8000 series, 9000 series, GTX200 series, GTX400/500 series.

**LinuxSupported Tools:**

**New Multiforcer:** New Multiforcer is the new version for Cryptohaze Multiforcer and an open source tool which supports ATI and Nvidia cards. The older version means Cryptohaze Multiforcer does not supports ATI cards. New Multiforcer supports only 9 types of hashes.

**Oclhashcat Plus:** It is a muti platform working tools runs on Windows and Linux based operating systems. It also supports a large number of hashes and GPU enabled cards up to 128 GPU cards. Works on both Cards ATI and Nvidia.
**Whitepixel:** Whitepixel is an open source tool supports only MD5 hash and runs only on ATI cards. The ATI cards which supported are AMD Radeon HD 5000 series and above series. It is also a Multi GPU supportable program upto 8 GPU cards.

**Hashkill:** Hashkill is an open source tool. It works on both AMD and Nvidia cards. It has 40 plugins for different type of passwords ranging from simple hashes MD5, SHA1 to private SSL key passphrases.

We can see now the description of all tools which are GPU supported but we can’t identify that which tool is good and fast for hash cracking. So we will now test some of the tools on both Operating Systems (Windows & Linux) by cracking a MD5 hash and point out the cracking speed.

**Windows CUDA Machine:** For configuring cuda machine on Windows operating systems we have to install first ATI drivers the R.G catalyst according to your graphic card model.

![Catalyst Control Center](image)

**Tools Demonstration on Windows CUDA Machine:** We are going to use IGHASHGPU. It is very simple command line tool now we will the usage command of IGHASHGPU.
By executing ighashgpu.exe from command line it will show the all command options with
detail some of the syntax we will describe here which is necessary.

-c: for character sets defining (caps, small, digits, special, space, all)

-h: hash value

-t: type of hash (MD5, MD4 or SHA1)

-min: minimum password length

-max: maximum password length

Now let us test our CUDA machine. We require a MD5 hash of a password let make it. Go to
online md5 hash generator service like here we are using www.md5.cz and as password we are
giving Xi4rCh and generate a MD5 hash of it.
Now we can continue to further cracking process. Run ighashgpu.exe and type in these commands

`ighashgpu.exe /h:a52a81807a28e5f92893dd5106c9ce65 /t:md5 /c:csda /max:7 /cpudontcare`

We already know about the syntax usage so we will not describe the syntax function here. The cracking process starts

Now in above figure we can see average password cracking speed is 1116.8 million per second and estimated time is showing approximately 11 min. But we in our case the password found in 5
minutes which we can see in below figure. The cracking speed is increases to 1119.1 million. Now we can see here that alphanumeric password (Uppercase, Lowercase, Digits) within 6 character can be cracked in 5 minutes.

Let us try that if we crack the same MD5 hash with CPU power then what is the efficiency? So we are using here Cain n Able for cracking MD5 hash and see what happens.
In the above screenshot we can see the average time it will take to crack 1.32945 years so we can see the difference between the GPU and CPU efficiency.

**BarsWF:** It supports only Nvidia card so we are going to crack on CPU power. Execute the BarsWF.exe from command line and it will show all the command options in details some of the commands we will demonstrate here which we are going to use.

![Command Line Output](image)

Usage Syntax:

- **-c:** for character set defining (A—for caps, a—for small, 0-digit, ~—for special characters)
- **-h:** hash here
- **-min_len:** minimum password length

So here we will using the same MD5 hash and type in **BarsWF_SSE2_x64.exe --c A0a --h a52a81807a28e5f92893dd5106c9ce65 --min_len 8**

![Output](image)
We can see in above figure the estimate time it will take 27 days it means it is faster than Cain n Abel where it takes a year to crack this hash, BarsWF will take some days.

**LinuxCUDA Machine:** Configuring CUDA machine in Linux system is not easy as Windows. The driver installation process is different in ATI and Nvidia cards.

**ATIDriverinstallation:**

1. Remove the old AMD drivers

```
sudo sh /usr/share/ati/fglrx-uninstall.sh
```

```
sudo apt-get remove --purge fglrx fglrx_* fglrx-amdccele* fglrx-dev* xorg-driver-fglx
```

2. Download the AMD drivers

Download from AMD website

Or via terminal

```
cd ~/.; mkdir catalyst12.4; cd catalyst12.4/
wget -O amd-driver-installer-12-4-x86.x86_64.run http://goo.gl/VGYWP
```

3. Installing Drivers

```
chmod +x amd-driver-installer-12-4-x86.x86_64.run

sudo sh ./amd-driver-installer-12-4-x86.x86_64.run
```

Now continue the installation wizard.
**Nvidia Driver Installation:**

1. Edit the configuration files

   `gedit /etc/modprobe.d/blacklist.conf`

   ![Editing blacklist.conf file](image1)

   add these line in blacklist.conf file

   ```
   blacklist vga16fb
   blacklist nouveau
   blacklist rivafb
   blacklist nvidiafb
   blacklist rivatv
   ```

2. `apt-get --purge remove nvidia-*`

   ![Removing Nvidia drivers](image2)

3. Reboot the system.

4. Installing Drivers
add-apt-repository ppa:ubuntu-x-swat/x-updates

apt-get update && apt-get install nvidia-current nvidia-current-modaliases nvidia-settings

5. Again reboot and you will Nvidia option in your utilities.

![NVIDIA X Server Settings](image)

**Tools Demonstration on Linux CUDA Machine:**

In Linux operating system we are going to use Nvidia cards with has less cuda cores than ATI Radeon card.

**Cryptohaze Linux:** Now let’s see the usage command for Cryptohaze. Type in this command
We have to use only three commands for cracking a hash, which is:

- c (For charset files)
- h (For defining hash type)
- f (For hash file location)

**Charset:** The term charset is short form of character set. It is a defined list of characters recognized by the computer hardware and software. Like you create a text document and define characters in lower case a-z and save it. Now you can create many charset file by defining own characters 0-9, A-Z and more like shown in below Figure.

Now let’s start cracking. Type in:

```
./Cryptohaze-Multiforcer -c /root/Desktop/Cryptohaze-Linux/charsets/charsetall -h MD5 -f /root/Desktop/hash.txt
```

Then press enter and cracking process starts.
See in top right corner side there shows my GPU cracking speed is only 36.64M/s it’s very slow because my Nvidia card has only 16 cuda cores. After successfully cracking it shows the password from your hash which is p@ssw
**New Multiforcer**: New Multiforcer is new revision version of Cryptohaze Multiforcer which supports ATI cards. The usage command is same as Cryptohaze Multiforcer. We have to pass these commands -openclplatform=0, --opencldevice=1 -bfi_init 

`.NewMultiforcer --openclplatform=0 --opencldevice=1 -bfi_init -h Hash type -c my charsets dir -f my file dir`

![Image of Multiforcer output]

**Which is better ATI or Nvidia?**

![Image of ATI and Nvidia logos]

Now which card is better it depends on many factors like price, tools and Cuda cores. If we are matching the speed of password cracking then we see ATI cards are better than Nvidia because the number of cuda cores is greater than Nvidia cards. Nvidia cards are expensive than ATI cards. But nvidia provides a high performance cards like Tesla cards and Titan cards which are very expensive but very fast performance. Maximum tools are Nvidia compatible on both platforms Windows and Linux. We found that very few tools are support ATI cards. We found
that if you don’t care of money then definitely go through with Nvidia cards but if you have small budget then go for ATI cards.

**Conclusions:** Hence we conclude that if we used a high performance graphic card with high cores which is greater than 512 cores and also use more than one card than the cracking speed of our machine is much faster than this machine, here we see the efficiency of both ATI and Nvidia cards. When we are using ATI card which has 3200 cuda cores it gives a speed of 1116.8 Million/second and when we were using only Nvidia card which has only 16 cuda cores it gives only 36 Million/second. Now you can understand the difference and importance of Cuda cores.

**References:**

http://en.wikipedia.org/wiki/CUDA

http://golubev.com/gpuest.htm

http://cyruslab.wordpress.com/2012/01/26/installing-nvidia-on-backtrack5r1/

**About Me:**
Rohit Shaw is a Certified Ethical Hacker works as a penetration tester with Xiarch AAG Group. He has experience in pentesting, social engineering, password cracking and malware obfuscation.