



GALGOTIAS  
UNIVERSITY

**School of Computing  
Science and Engineering**

Program: B.Tech - Specialization

Course Code: CSCN2020

Course Name: Ethical Hacking

## Course Outcomes

CO's	CO Statement
CO1	Understand the concept of BIOS setup and browser's tools
CO2	Learn windows tricks and tips with commands and registry editor
CO3	Understand the basic technique to crack windows and application passwords
CO4	Learn and understanding basics of Perl programming language
CO5	Understanding about MBR, Disc access and the basics of viruses with prevention methods
CO6	Able to perform NMAP and Penetration testing techniques
CON	Applying hacking technique with Kali linux OS

## Course Prerequisites

S. No	Prerequisites
1.	Basics of Operating System (Windows and Kali Linux)
2.	Basics of Hardware Technology
3.	Basics of Networking
4.	Basics of CISCO's Packet Tracer

## Syllabus

<b>Module I</b>	<b>Hacking Windows</b>	<b>8</b>
<p>BIOS Passwords, Windows Login Passwords, Changing Windows Visuals, Cleaning Your Tracks, Internet Explorer Users, Cookies, URL Address Bar, Netscape Communicator, Cookies, URL History, The Registry, Baby Sitter Programs.</p>		
<b>Module II</b>	<b>Advanced Windows Hacking</b>	<b>12</b>
<p>Editing your Operating Systems by editing Explorer.exe, The Registry, The Registry Editor, Description of .reg file, Command Line Registry Arguments, Other System Files, Some Windows &amp; DOS Tricks, Customize DOS, Clearing the CMOS without opening your PC, The Untold Windows Tips and Tricks Manual, Exiting Windows the Cool and Quick Way, Ban Shutdowns: A Trick to Play, Disabling Display of Drives in My Computer, Take Over the Screen Saver, Pop a Banner each time Windows Boots, Change the Default Locations, Secure your Desktop Icons and Settings.</p>		
<b>Module III</b>	<b>Getting Past the Password</b>	<b>8</b>
<p>Passwords: An Introduction, Password Cracking, Cracking the Windows Login Password, The Glide Code, Windows Screen Saver Password, XOR, Internet Connection Password, Sam Attacks, Cracking Unix Password Files, HTTP Basic Authentication, BIOS Passwords, Cracking Other Passwords</p>		

<b>Module IV</b>	<b>The Perl Manual</b>	<b>12</b>
<p>Perl: The Basics, Scalars, Interacting with User by getting Input, Chomp() and Chop(), Operators, Binary Arithmetic Operators, The Exponentiation Operator(**), The Unary Arithmetic Operators, Other General Operators, Conditional Statements, Assignment Operators. The?: Operator, Loops, The While Loop, The For Loop, Arrays, THE FOR EACH LOOP: Moving through an Array, Functions Associated with Arrays, Push() and Pop(), Unshift() and Shift(), Splice(), Default Variables, \$_, @ARGV, Input Output, Opening Files for Reading, Another Special VariableS.</p>		
<b>Module V</b>	<b>How does a Virus Work</b>	<b>8</b>
<p>What is a Virus?, Boot Sector Viruses (MBR or Master Boot Record), File or Program Viruses, Multipartite Viruses, Stealth Viruses, Polymorphic Viruses, Macro Viruses, Blocking Direct Disk Access, Recognizing Master Boot Record (MBR) Modifications, Identifying Unknown Device Drivers, How do I make my own Virus?, Macro Viruses, Using Assembly to Create your own Virus, How to Modify a Virus so Scan won't Catch it, How to Create New Virus Strains, Simple Encryption Methods.</p>		
<b>Module VI</b>	<b>Recent trends in ethical hacking</b>	<b>8</b>
<p>Ethical Hacking Tools and Techniques, Penetration Techniques, NMAP, Web Penetration, Ethical Hacking as Network Defense, Ethics in Ethical Hacking</p>		

## **Recommended Books**

### **Text books**

1. Ankit Fadia, An unofficial guide to Ethical Hacking, Second edition.
2. W. Stallings, Cryptography and Network Security: Principles and Practice, 5th Ed. Boston: Prentice Hall, 2010. (ISBN No.: 978-0-13-609704-4)
3. C. Kaufman, R. Perlman, and M. Speciner, Network Security: Private Communication in a Public.

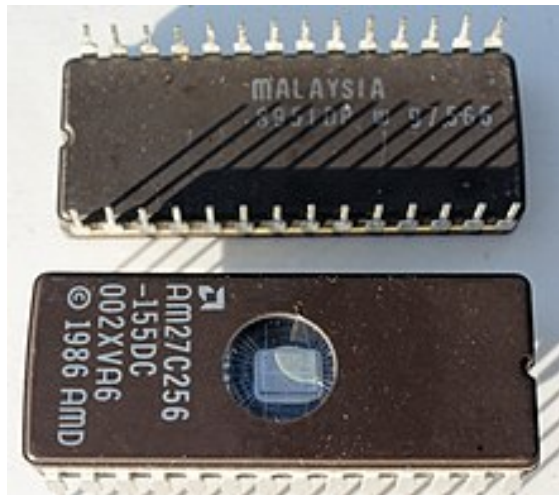
### **Reference Books**

1. Atul Kahate, Cryptography and Network Security, 2nd ed., Tata Mcgraw Hill education Private Limited, 2011.
2. Computer Security, Dieter Gollman, 3rd ed, Wiley Publications, 2011.
3. Introduction to Computer Security, Matt Bishop, 1st ed, Addison-Wesley Professional, 2004.
4. Windows Hacking, Ethical hacking series, Ankit Fadia.

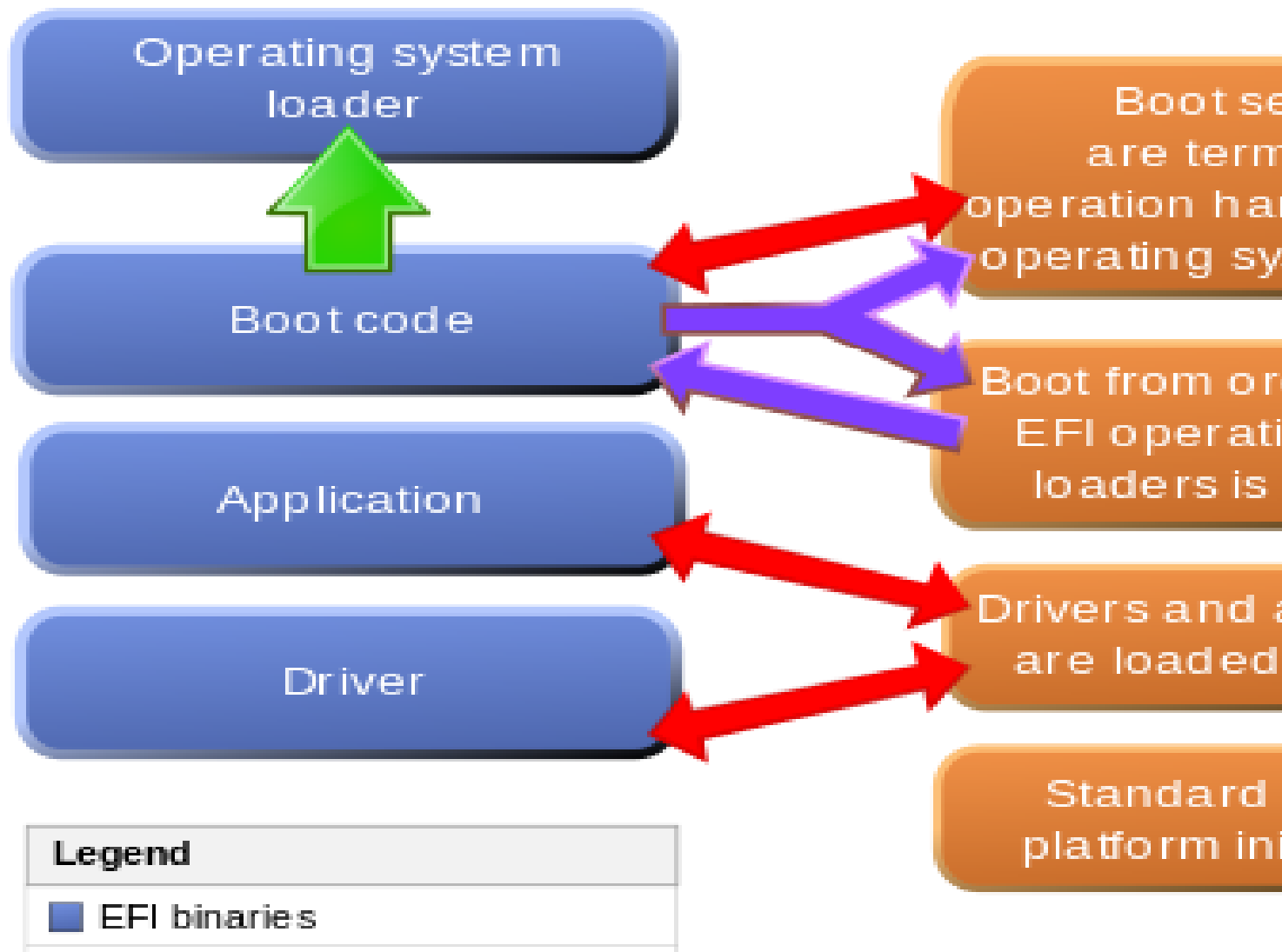
### **Additional online materials: -**

## BIOS

- Hardware initialization
- Data flow between OS and Devices
- Flash Memory
- BIOS rootkits
- UEFI
- MBR and GPT



Interaction between EFI boot manager and Driver





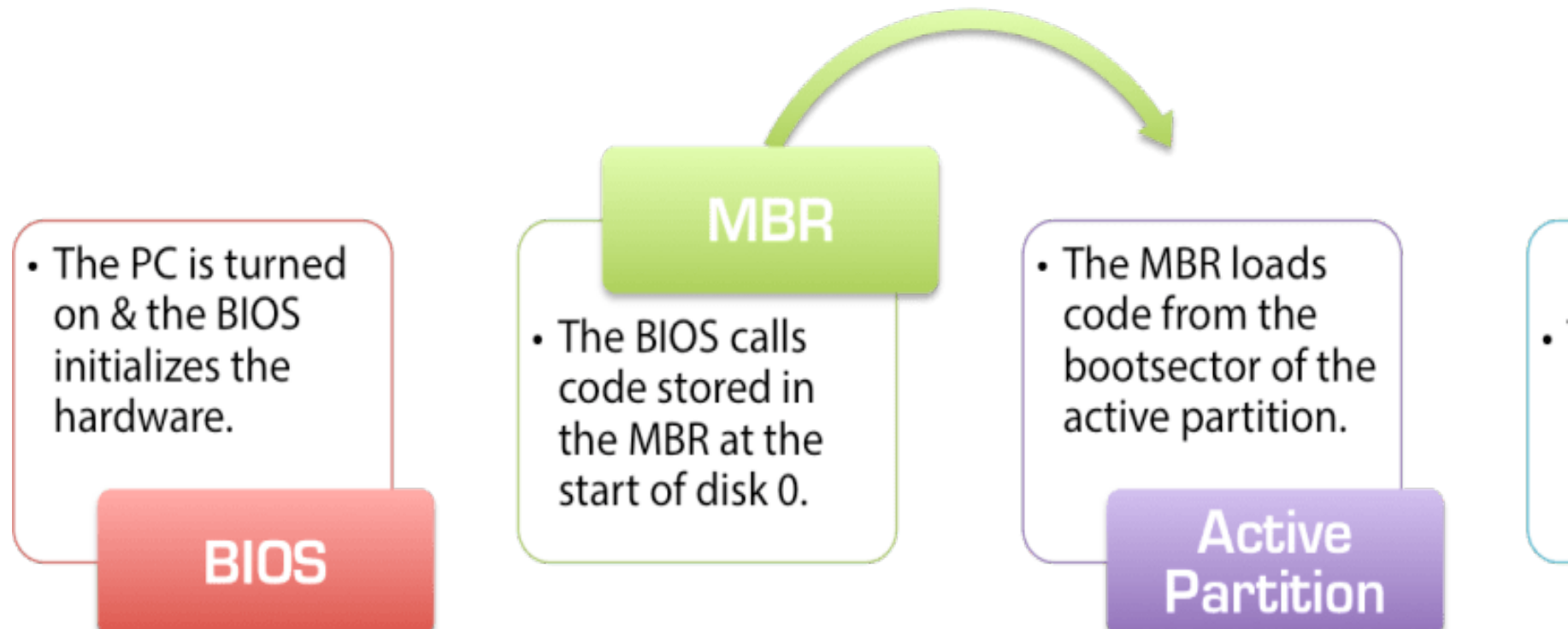
## UEFI classes

- Class 0: Legacy BIOS
- Class 1: UEFI in CSM-only mode
- Class 2: UEFI with CSM
- Class 3: UEFI without CSM
- Class 3+: UEFI with Secure Boot Enabled

## The following is a list of commands supported by the EFI shell

•help	•guid	•set	•alias	•dh	•bcfg
•unload	•map	•mount	•cd	•echo	•edit
•pause	•ls	•mkdir	•mode	•cp	•Edd30
•comp	•rm	•memmap	•type	•dmpstore	•dblk
•load	•ver	•err	•time	•date	•pci
•stall	•reset	•vol	•attrib	•cls	•mem

## Overview of the BIOS/MBR Boot Process

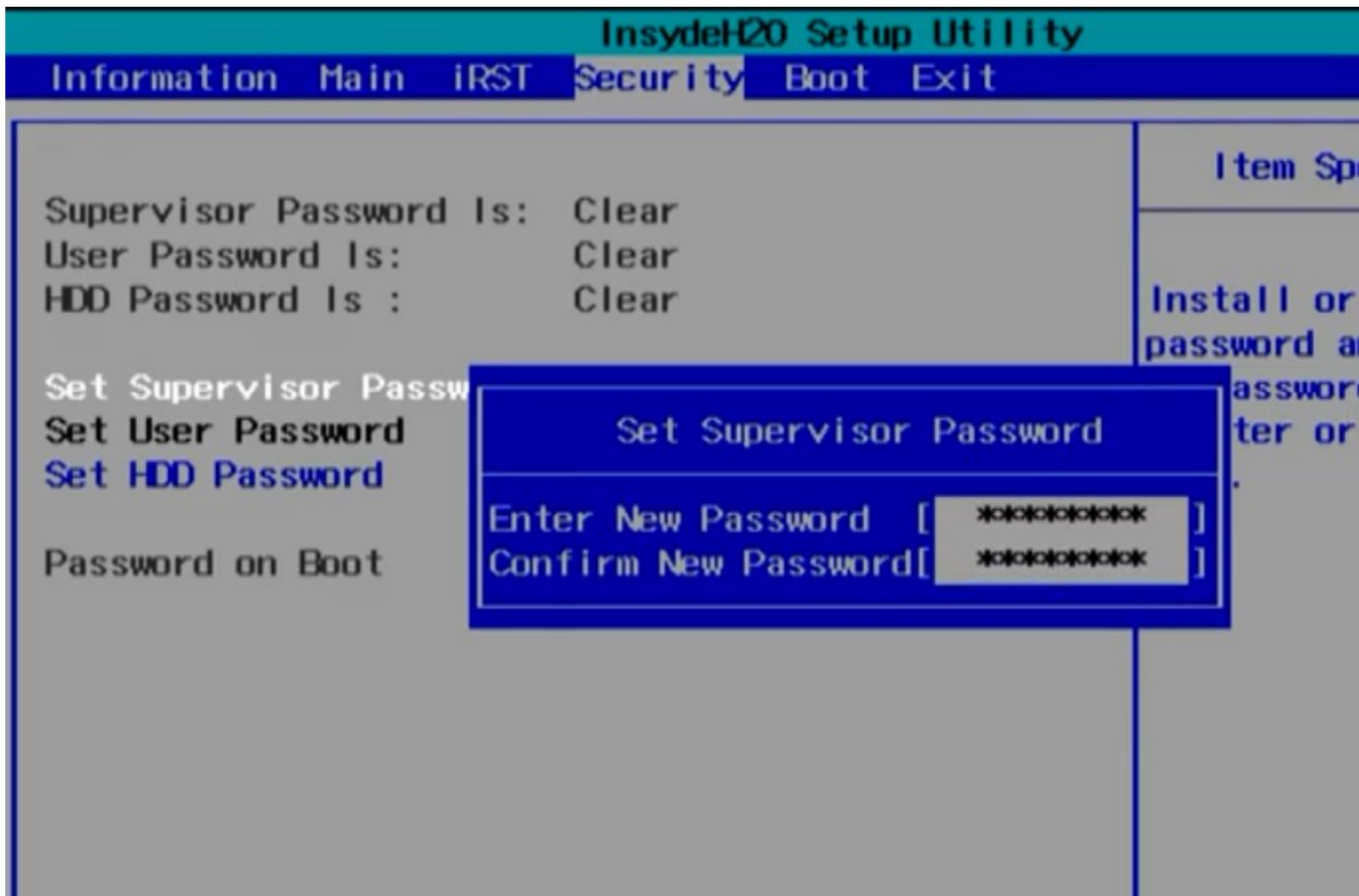


## The BIOS password

The BIOS password is stored in complementary metal-oxide semiconductor (CMOS) memory. In some computers, a small battery attached to the motherboard maintains the memory when the computer is off.

## System Passwords

- BIOS Password
- Login Password
  - ✓ Admin Password
  - ✓ User Password



## Crack BIOS password

**Step 1** The first option will be to change the Password Jumper Settings on the BIOS. There is a specific jumper on the motherboard which is meant for this. However, it is advisable to read the product manual first before trying this step, because the position of the Jumper will differ from one motherboard to another.

**Step 2** To perform this one has to turn off the computer, make sure the power cable is out of the wall outlet. Unscrew the screws located on the Side Panel of the CPU.

**Step 3** Once, you do that, identify the location of the BIOS jumper on the motherboard by checking in product documentation and reset the same.

The jumper might be labeled as CLEARCMOS or JCMOS1. However, the best will be to always refer to the product documentation.

**Step 4** Once this is done, restart the computer and check whether the password is cleared or not. Now once the password is cleared, turn off the computer once again, and put back the jumper to its original position.





## **Bypass BIOS password**

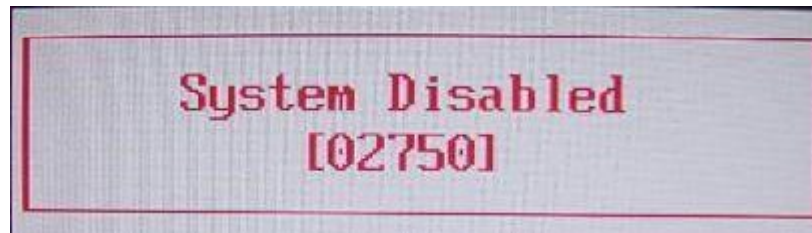
Another situation similar to the scenarios we discussed above can be solved by bypassing the BIOS password. The methods which can be used here are similar to the methods used in previous scenarios. In addition to that, we can use these two methods as well:

### **Method:** Overloading the keyboard buffer

This method is specific to some of the old system boards, and the newer systems might not be able to implement this. This is done by booting the system without mouse or keyboard, or in certain BIOS architectures, it might work by hitting the ESC key in quick succession.

## For laptop users :

For **laptop** users, the process will be entirely different, since they have to use a backdoor password entry option. Enter the wrong password thrice on the screen, which will show an error like this.

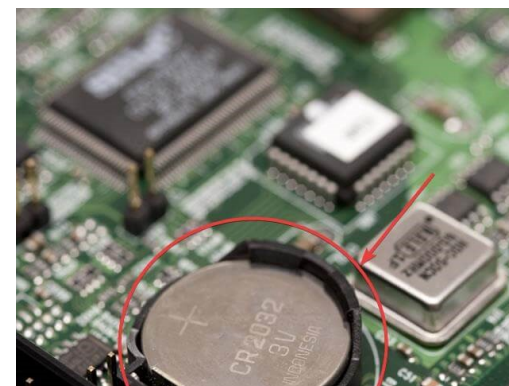




## Reset BIOS password

### Method 1. Reset your BIOS by removing the CMOS battery

1. First **disconnect your PC** from any power source.
  - 1.1. If you are using a laptop, this includes **removing the battery**
2. Remove your PC's cover, and locate the **CMOS battery**
3. **Remove** the battery
4. **Press the power button** for around 10 seconds
5. Put the CMOS battery **back in place**
6. Put the cover back, or reassemble the laptop
7. **Boot** the PC



## Method 2. Remove BIOS password using an MS-DOS Command

1. **Reboot** your PC
2. Enter the **Boot menu**
3. Choose **Safe Mode with Command Prompt**
4. While in MS-DOS mode, a black dialogue box of cmd will turn up with a C:WINDOWS> prompt
5. Type in **Debug**
6. Hit **Enter**
7. Enter the following command given below and press **Enter**:
  1. **debug**
  2. **o70 2E**
  3. **o71 FF**
  4. **quit**
8. Type in **Exit**, and hit **Enter**
9. **Reboot** your PC

### **AMI/AWARD BIOS**

D

O 70 17

O 71 17

Q

### **PHOENIX BIOS**

D

O 70 FF

O 71 17

Q

**Method 3: Use Backdoor BIOS password****AWARD BIOS Passwords:**

01322222

589589

589721

595595

598598

ALFAROME

ALLy

aLly

aLLY

ALLY

aPAf

\_award

award

AWARD\_SW

AWARD?SW

AWARD SW

AWARD PW

AWKWARD

awkward

BIOSTAR

CONCAT

CONDO

Condo

d8on

djonet

HLT

J64

J256

J262

j332

j322

KDD

Lkwpeter

LKWPETER

PINT

pint

SER

SKY\_FOX

SYXZ

syxz

shift + syxz

TTPTHA

ZAAADA

ZBAAACA

ZJAAADC

**Misc Common Passwords:**

ALFAROME  
BIOSTAR  
biostar  
biosstar  
CMOS  
cmos  
LKWPETER  
lkwpete  
setup  
SETUP  
Syxz  
Wodj

**PHOENIX BIOS Passwords:**

BIOS  
CMOS  
phoenix  
PHOENIX

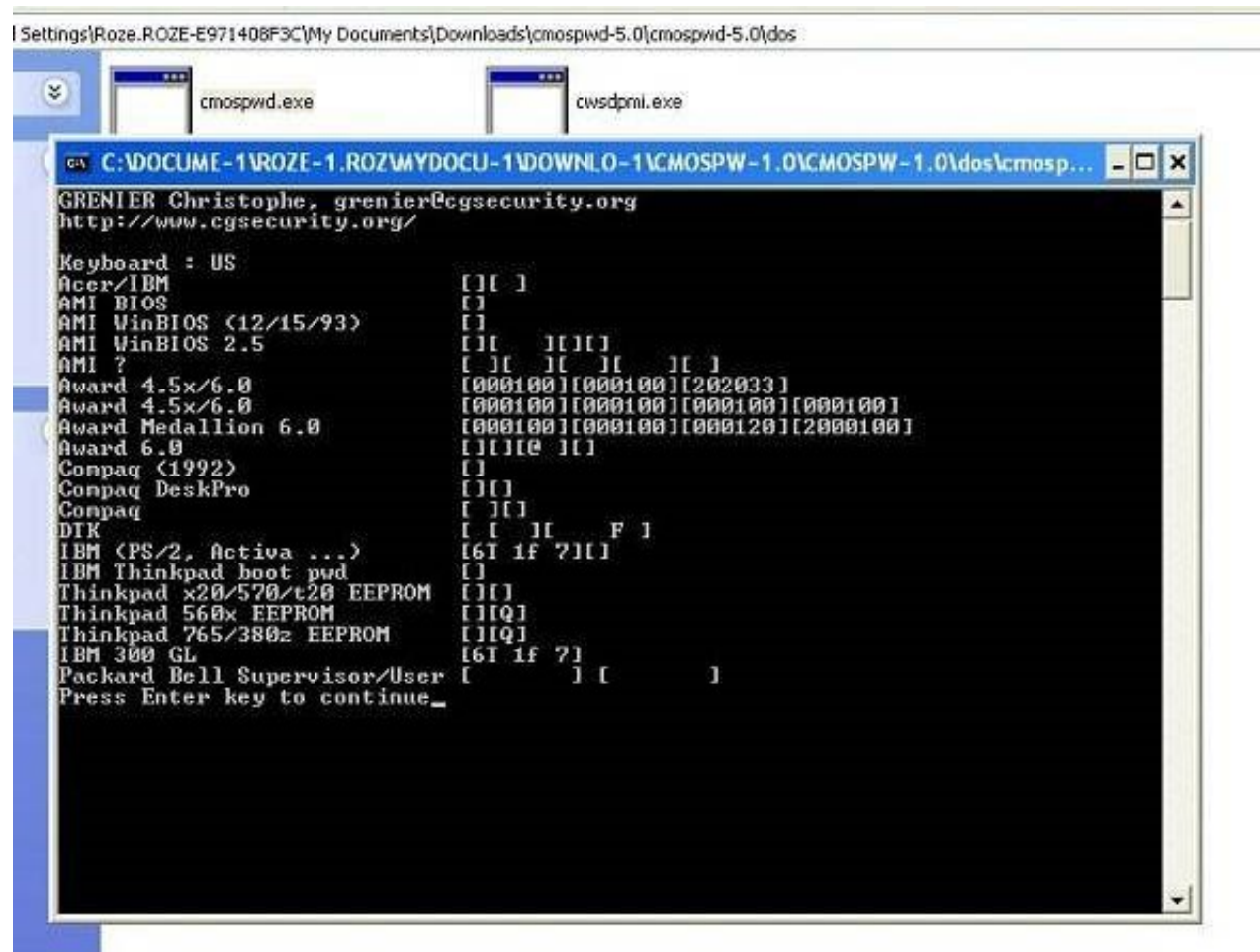
**AWARD BIOS Passwords:**

01322222  
589589  
589721  
595595  
598598  
ALFAROME  
ALLy  
aLLy  
aLLY  
ALLY  
aPAf  
\_award  
award  
AWARD\_SW  
AWARD?SW  
AWARD SW  
AWARD PW

**Other Manufacturer BIOS Passwords:**

Biostar – Biostar  
Compaq – Compaq  
Dell – Dell  
Enox – xo11nE  
Epox – central  
Freetech – Posterie  
IWill – iwill  
Jetway – spooml  
Packard Bell – bell9  
QDI – QDI  
Siemens – SKY\_FOX  
TMC – BIGO  
Toshiba – Toshiba  
VOBIS & IBM – merlin

## Method 4: Use Third-Party Software



```
Settings\Roze.ROZE-E971408F3C\My Documents\Downloads\cmospwd-5.0\cmospwd-5.0\dos
cmospwd.exe  cwsdpml.exe

C:\DOCUME~1\ROZE~1\ROZ\WYDOCU~1\DOWNLO~1\CMOSPW~1.0\CMOSPW~1.0\dos\cmosp...
GRENIER Christophe, grenier@cgsecurity.org
http://www.cgsecurity.org/

Keyboard : US
Acer/IBM          [[] ]
AMI BIOS         [[]]
AMI WinBIOS (12/15/93) [[]]
AMI WinBIOS 2.5  [[] ][][]
AMI ?           [ ][] [] [] [] []
Award 4.5x/6.0  [000100][000100][202033]
Award 4.5x/6.0  [000100][000100][000100][000100]
Award Medallion 6.0 [000100][000100][000120][2000100]
Award 6.0       [[]][@ []]
Compaq (1992)   [[]]
Compaq DeskPro  [[]]
Compaq         [ ][]
DTK            [ [ ][] F ]
IBM (PS/2, Activa ...) [6T if ?][]
IBM Thinkpad boot pwd  [[]]
Thinkpad x20/570/t20 EEPROM [[]]
Thinkpad 560x EEPROM  [][Q]
Thinkpad 765/380z EEPROM [][Q]
IBM 300 GL      [6T if ?]
Packard Bell Supervisor/User [ ] [ ]

Press Enter key to continue_
```

## Method 5. Reset your BIOS password with a backdoor password

1. **Boot** your PC
2. Try to access the Boot Menu and intentionally type in the **wrong BIOS password 3 times**
  1. This will force your PC to go into a lockdown mode along with a System disabled message paired with a code
3. Note the code down
4. Go to [bios-pw.org/](https://bios-pw.org/) and enter the code
5. Press **Get Password**
6. The website will generate passwords similar to the one you used

## Windows Registry Editor

The Windows Registry Editor (regedit) is a graphical tool in the Windows operating system (OS) that allows Import/export .Reg files or create, delete or make changes to corrupt registry keys and subkeys

Handle to Registry Key (HKEY)

The Registry

**HKEY\_User** - contains the user information for each user of the system.

**HKEY\_Current\_User** - has all the preferences for the current user.

**HKEY\_Current\_Configuration** - stores settings for the display and printers.

**HKEY\_Classes\_Root** - includes file associations and OLE information.

**HKEY\_Local\_Machine** - has the settings for the hardware, operating system, and installed applications.

**HKEY\_Dyn\_Data** - includes performance data.



## ***Windows registry features and advantages are as follows:***

- ✓ All low-level and third-party OS components and applications, like device drivers and kernels, can access the registry.
- ✓ To profile system performance, it facilitates access to the necessary counters.
- ✓ It stores and reflects user changes to configurations, preferences, policies and applications.
- ✓ Depending on the Windows version, it stores physical registry files in different locations.
- ✓ It contains two elements: keys, which are similar in concept to Windows folders, and values, which are similar to files.
- ✓ Registry files must be edited with the registry editor or another third-party application, as file modifications cannot be directly applied.
- ✓ Although it is possible to physically delete registry values and keys, Microsoft provides the RegClean tool to automate this process.

### REGISTRY VALUE DATA TYPES

1. REG\_BINARY
2. REG\_DWORD
3. REG\_EXPAND\_SZ
4. REG\_MULTI\_SZ
5. REG\_SZ

### *Other Data Types*

1. REG\_DWORD\_LITTLE\_ENDIAN
2. REG\_DWORD\_BIG\_ENDIAN
3. REG\_LINK
4. REG\_NONE
5. REG\_QWORD
6. REG\_QWORD\_LITTLE\_ENDIAN
7. REG\_RESOURCE\_LIST

**Windows registry disadvantages :**

- ✓ Transferring program user settings between Windows machines
- ✓ Transaction log files
- ✓ It needs a dedicated uninstaller to remove registry entries

**Syntax for REGEDIT.EXE**

REGEDIT [/v|-v] [/s|-s] <FILENAME>

## REGEDIT

Import, export or delete registry settings from a text (.REG) file.

### ***Syntax***

Export the Registry (all HKLM plus current user)

REGEDIT /E *pathname* (Drive + Path + Filename = Pathname)

Export part of the Registry

REGEDIT /E *pathname* "RegPath"

Export part of the Registry in ANSI mode

REGEDIT /A *pathname* "RegPath"

(This is undocumented and will not support unicode-only keys/values.)

Import a reg script

REGEDIT *pathname*

Silent import

REGEDIT /S [pathname](#)

Start the regedit GUI

REGEDIT

Open multiple copies of regedit

REGEDIT /m

## Disabling Drives:

- Device Manager
- Registry Editor
- Group Policy Editor
- USB Storage Enabler Through Registry Editor
- Third Party Software

## Ban Shutdown:

1. Open Microsoft Management Console
2. Select Add/Remove Snap – in from File Menu
3. Select Group policy object module
4. Browse to select users and under users select Non Administrative Users
5. Click finish and Go back to “MMC”
6. Select from newly created Local Computer \ Non-Administrators policy object in the left pane, navigate to User Configuration > Administrative Templates > Start Menu and Taskbar
7. In the right pane select **Remove and prevent access to the shutdown, restart, sleep, and hibernate commands** and double-click on it. Select Enable > Apply/OK. **(Or)**
8. gpedit.msc → Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment > **Shut Down the System.**

## CHANGE THE DEFAULT LOCATIONS:

1. Start Registry Editor by entering “Regedit” in the search All programs.

2. Locate the following:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion*

3. Right click on the value named **ProgramFilesDir** & change the default value *C:\Program Files* to the path you want to install all your programs in.

4. Click OK and Exit.





# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking





# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking





# School of Computing Science and Engineering

Course Code : CSCN 2020

Course Name: Ethical Hacking



Thank You