Programme Educational Objectives(PEOs)

PEO1 (Core Competency): Graduates will acquire a strong foundation in mathematical, scientific and engineering fundamentals necessary to formulate, solve and analyze Computer Science and Engineering problems.

PEO2 (Professionalism): Graduates will practice the profession with ethics, integrity and leadership to relate engineering to global perspective issues and social context.

PEO3 (Higher Studies and Entrepreneurship): Graduates will be prepared for their careers in the software industry or in higher studies leading to research and for applying the spirit of innovation and entrepreneurship in their career and continuing to develop their professional knowledge on a life long basis.

Programme Outcomes(POs)

PO1: Engineering knowledge: Ability to apply the knowledge of mathematics, physical sciences and computer science and engineering specialization to the solution of complex engineering problems.

PO2: Problem analysis: Ability to identify, formulate and analyze complex real life problems in order to provide meaningful solutions by applying knowledge acquired in computer science and engineering.

PO3: Design/development of solutions: Ability to design cost effective software / hardware solutions to meet desired needs of customers/clients.

PO4: Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions in the field of computer science and engineering.

PO5: Modern tool usage: Create, select and apply appropriate techniques, resources and modern computer science and engineering tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO6: The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO7: Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO8: Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO9: Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO10: Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO11: Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO12: Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Programme Specific Outcomes (PSOs)

PSO1: Software System Design and Development: The ability to apply software development life cycle principles to design and develop the application software that meet the automation needs of society and industry.
PSO2: Computing and Research ability: The ability to employ modern computer languages, environments and platforms in creating innovative career paths in SMAC (Social, Mobile, Analytics and Cloud) technologies.

Hacking Terms: Phishing | Malware | Ransomware | Spoofing | Encryption | Adware | Zero Day threat

K S R INSTITUTE FOR ENGINEERING AND TECHNOLOGY
K.S.R KALVI NAGAR, TIRUCHENGODE - 637 215
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

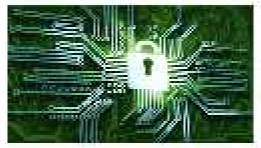
Tech Zest

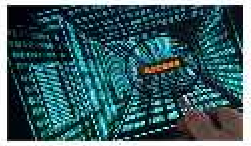
Fuel Your Mind

Jan - 2016 - Volume III / Issue II

PAGE 2 Ethical Hacking
PAGE 3 System Hardening
PAGE 4 Code Review
PAGE 5 War Dialing
PAGE 6 Quiz Time
PAGE 7 Student Article

ETHICAL HACKING





K S R Institute for Engineering and Technology

Vision

To become a globalLy recognized Institution in Engineering Education, Research and Entrepreneurship.

Mission

IM1: Accomplish quality education through improved teaching learning process.
IM2: Enrich technical skills with state of the art laboratories and facilities.
IM3: Enhance research and entrepreneurship activities to meet the industrial and societal needs

Department of Computer Science and Engineering

Vision

To produce globally competitive Computer Science Engineers and Entrepreneurs with moral values.

Mission

DM1 (Quality Education) : Provide quality education to enhance problem solving skills, leadership qualities, team spirit and ethical responsibilities.

DM2 (State of art Laboratory) : Enable the students to adapt to the rapidly changing technologies by providing advanced laboratories and facilities.

DM3 (Research and Development) : Promote research based activities in the emerging areas of techno-environment in order to meet industrial and societal needs.

Hacking Terms: Brute Force Attack | Botnets | DDOS | Firewall | Payload | White hat | Rootkit | SPAM| Worm

Ethical Hacking

Introduction to Ethical Hacking

Ethical hacking and ethical hacker are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network. An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the organization to improve the system security, to minimize or eliminate any potential attacks.

What constitutes ethical hacking?

For hacking to be deemed ethical, the hacker must obey the following rules:

☒ Expressed (often written) permission to probe the network and attempt to identify potential security risks.
☒ You respect the individual's or company's privacy.
☒ You close out your work, not leaving anything open for you or someone else to exploit at a later time.

The term "ethical hacker" has received criticism at times from people who say that there is no such thing as an "ethical" hacker. Hacking is hacking, no matter how you look at it and those who do the hacking are commonly referred to as computer criminals or cyber criminals. However, the work that ethical hackers do for organizations has helped improve system security and can be said to be quite effective and successful. Individuals interested in becoming an ethical hacker can work towards a certification to become a Certified Ethical Hacker or CEH. This certification is provided by the International Council of EC-Council (E-Commerce Consultants).

S.Lingaraj , IV / CSE

Application of Ethical Hacking Network Testing

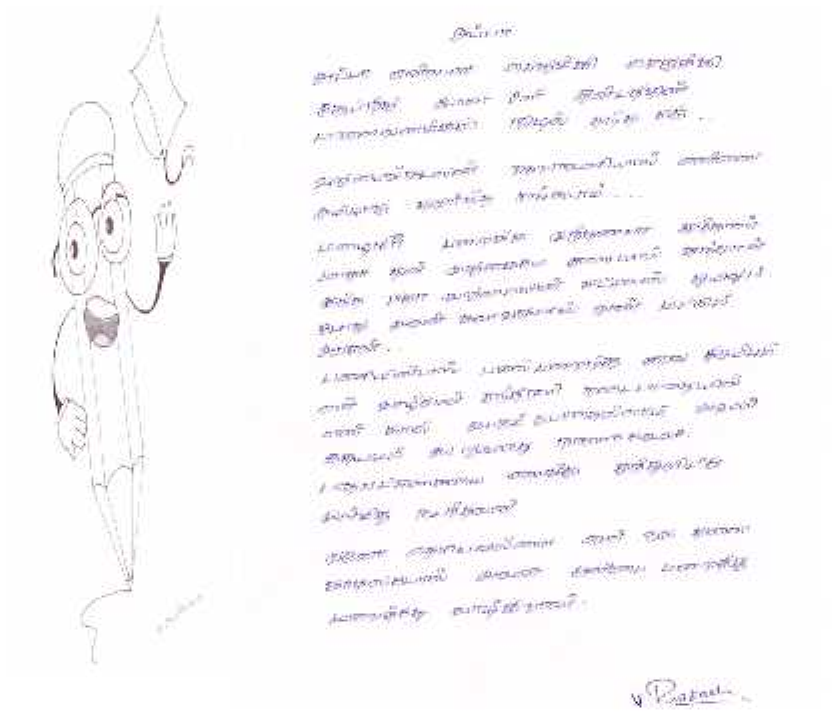
A network performance test primarily tests the uplink and downlink speed of a network. It defines how quick and responsive a network is to user/data communication. It is done by uploading and downloading a data object from the network and measuring both upload and download speeds, throughput, successful message delivery rate and more.

Cracking techniques on networks include creating worms, initiating a denial of service (DoS) attacks, and establishing unauthorized remote access connections to a device. Protecting a network and the computers attached to it from malware, phishing, Trojans, and unauthorized access is a full-time job and vitally important. Hacking on computer networks is often done through scripts and other network software. These specially-designed software programs generally manipulate data passing through a network connection in ways designed to obtain more information about how the target system works.

S.Navaneethan, IV / CSE

☢ Currently, encryption is the most practical and easy way to protect electronically stored, processed or transmitted data. ☢

Student Article



[illegible]

Try this!

- Use exactly four 4's to form every integer from 0 to 50, using only the operators +, -, x, /, () (brackets), . (decimal point), x2 (square), square root and ! (factorial).
  Example: 0 – 44-44

- Using the numerals 1,7,7,7 and 7 (a "1" and four "7"s) create the number 100.
  As well as the five numerals you can use the usual mathematical operations +, −, ×, ÷ and brackets ().
  For example: (7+1) × (7+7) = 112 would be a good attempt, but not right, because it is not 100.

- This is a Magic Square. This means that the numbers add up to the same total in every direction. Every row, column and diagonal should add up to 111. But there are some numbers missing! Fill in the missing numbers. They are all different.

		7
13	37	

D.Sharmila, III / CSE

☢ The very word cryptography has Greek origins. "Kryptos" means hidden and "Graphein" – word. ☢

How Does Bugs Affect Softwares?

Most bugs arise from mistakes and errors made in either a program's source code or its design, or in components and operating systems used by such programs. A few are caused by compilers producing incorrect code. A program that contains a large number of bugs, and/or bugs that seriously interfere with its functionality, is said to be buggy (defective). Bugs can trigger errors that may have ripple effects. Bugs may have subtle effects or cause the program to crash or freeze the computer. Other bugs qualify as security bugs and might, for example, enable a malicious user to bypass access controls in order to obtain unauthorized privileges.

Impact and Severity

This impact may be data loss, financial, loss of goodwill and wasted effort. Severity levels are not standardized. Impacts differ across industry. A crash in a video game has a totally different impact than a crash in a web browser, or real time monitoring system. For example, bug severity levels might be "crash or hang", "no workaround" (meaning there is no way the customer can accomplish a given task), "has workaround" (meaning the user can still accomplish the task), "visual defect" (for example, a missing image or displaced button or form element), or "documentation error". Some software publishers use more qualified severities such as "critical".

G.Janani, II / CSE

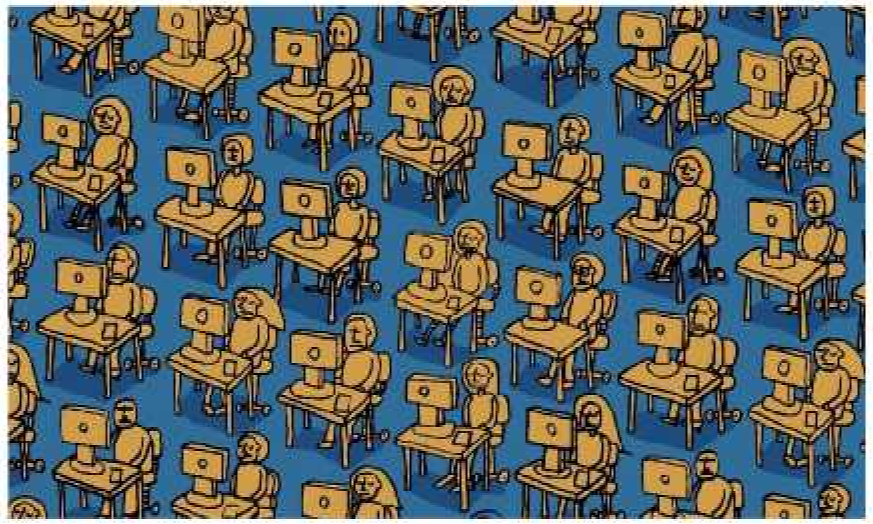
Code Review

Code review (sometimes referred to as peer review) is a software quality assurance activity in which one or several humans check a program mainly by viewing and reading parts of its source code, and they do so after implementation or as an interruption of implementation. At least one of the humans must not be the code's author. The humans performing the checking, excluding the author, are called "reviewers"

Source code, please? Don't hand hackers your vulnerabilities on a silver platter

In code review process the source code plays an important roles. Source code analysis tools tests code at its raw state to validate proper business logic, functionality and code security best and common practices. While hackers use a variety of tools and techniques to infiltrate and recognize weak spots within an application, tools that require the source code itself, like source code analysis tools and other Static Application Security Testing (SAST) solutions, are used less frequently than other solutions as they require both the source code and additional skills

Even if the source code is obtained, a good source code analysis solution that covers multiple programming languages and frameworks would not be something a hacker could easily put their hands on. Considering the above, it is quite safe to say that source code analysis and access to the full application code is a significant edge organizations have over hackers. It may be the only edge.



D.Keerthana, II / CSE

☢ The art and science of breaking the cipher text is known as cryptanalysis. ☢

War Dialing

War dialing is a technique to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for modems, computers, bulletin board systems (computer servers) and fax machines. Hackers use the resulting lists for various purposes: hobbyists for exploration, and crackers – malicious hackers who specialize in breaching computer security – for guessing user accounts.

War Dialing In Hacker's Point Of View

A single war dialing call would involve calling an unknown number, and waiting for one or two rings, since answering computers usually pick up on the first ring. If the phone rings twice, the modem hangs up and tries the next number. If a modem or fax machine answers, the war dialer program makes a note of the number. If a human or answering machine answers, the war dialer program hangs up. Depending on the time of day, war dialing 10,000 numbers in a given area code might annoy dozens or hundreds of people, some who attempt and fail to answer a phone in two rings, and some who succeed, only to hear the war dialing modem's carrier tone and hang up. The repeated incoming calls are especially annoying to businesses that have many consecutively numbered lines in the exchange, such as used with a Centrex telephone system.

Some newer war dialing software, such as War VOX, does not require a modem to conduct war dialing. Rather, such programs can use VOIP - Voice Over IP connections, which can speed up the number of calls that a war dialer can make.

How do hackers get benefited?

Hackers and crackers make use of several methods in order to satisfy their motives and one of the known procedures used by these experts is war dialing. Hackers make use of the resulting list of the war dialing for a wide range of reasons. On the other hand, hobbyists use the list that they have made simply to gratify their curiosity and also to complete their investigation. However, the crackers apply war dialing in their evil schemes like guessing of passwords.

A.Kishore Kumar, IV / CSE

Cloud Bleed

What is cloudbleed ?

Cloudbleed is the name of a major security breach from the internet company Cloudflare that leaked user passwords, and other potentially sensitive information to thousands of websites over six months. In effects, Cloudbleed is similar to the 2014 Heart bleed bug in allowing unauthorized third parties to access data in the memory of programs running on web servers, including data shielded by TLS. The extent of Cloudbleed also could have impacted as many users as Heartbleed since it affected a security and content delivery service used by close to 2 million websites.

Is cloudbleed still actively dangerous?

No. Think of Cloudbleed like a person surviving a heart attack. It's scary and it will require changes to prevent it from happening again. But the worst of it is over. The Cloudflare stopped the bug within 44 minutes of finding out about it and fixed the problem completely within 7 hours. So there will be ripples of consequential fallout as companies learn about the bug and whether their customers' information was involved.

J.Vijayakumar, III / CSE

☢ Cryptography is the art and science of making a cryptosystem that is capable of providing information security. ☢

What should i do?

The first thing to do is change the passwords for any of your accounts that use Cloudflare. Fitbit, OKCupid and Medium are a few, And, if any of those websites or services offer two-step verification, use it. It ensures that even if someone were to get a hold of your password, they would not be able to access your account. As worried about Cloudbleed as some people might be, companies will be pretty worried too and hearing from their customers can go a long way toward improving things for everyone.

A.Sathish Kumar, III / CSE

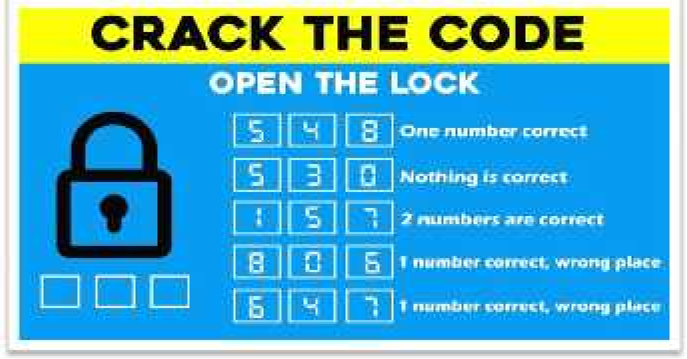
1. A(n) is the logical, not physical, component of a TCP connection.
 a. ISN
 b. Socket
 c. Port
 d. SYN

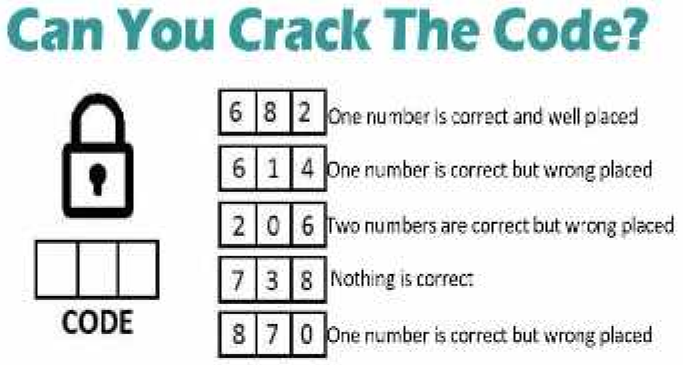
2. Each Class C IP address supports up to host computers.
 a. 254
 b. 512
 c. 65, 000
 d.16 million

3. How is ethical hacking different from simple hacking?
 a. Ethical hackers never launch exploits.
 b. Ethical hackers have written permission.
 c. Ethical hackers act with malice.
 d. Ethical hackers have permission.

4. Which type of hacker performs both ethical and unethical activities?
 a. White hat
 b. Gray hat
 c. Black hat
 d. Suicide hacker

5. Which type of testing occurs when you have no knowledge of the network?
 a. Black box
 b. White box
 c. Gray box
 d. Blind testing


CRACK THE CODE
OPEN THE LOCK
5 4 8 One number correct
5 3 0 Nothing is correct
1 5 7 2 numbers are correct
8 0 6 1 number correct, wrong place
6 4 7 1 number correct, wrong place


Can You Crack The Code?
6 8 2 One number is correct and well placed
6 1 4 One number is correct but wrong placed
2 0 6 Two numbers are correct but wrong placed
7 3 8 Nothing is correct
8 7 0 One number is correct but wrong placed
CODE

R.Priyanka, II / CSE

Richard Matthew Stallman wrote GNU General Public License ☢ In 2014, Yahoo! suffered the largest Cyber Attack.

System Hardening

Most computers offer network security features to limit outside access to the system. Software such as antivirus programs and spyware blockers prevent malicious software from running on the machine. Yet, even with these security measures in place, computers are often still vulnerable to outside access. System hardening, also called Operating System hardening, helps minimize these security vulnerabilities.

How such vulnarabilities occurs?

1. Clicking Questionable Links

Clicking on a questionable link can add malware to your system that could give away access to your personal information, including bank accounts and credit card numbers. To stay safe, always stick to reputable sites before you click through. Generally the most secure links will appear at the top of any Google search, but if you're ever in doubt don't click the link.

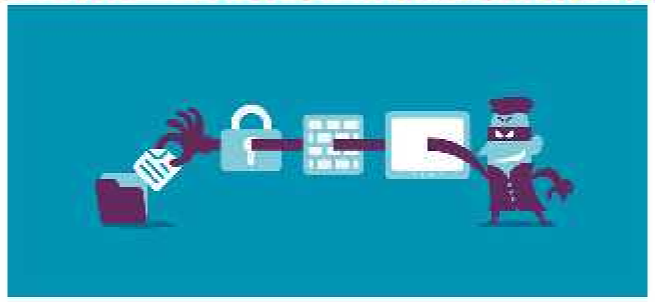
2. Using Unknown Flash Drives

Backing-up your files and your system is important, but always be careful when inserting someone else's flash or USB drive into your computer. External drives can be filled with malware, and all it takes is for one well-placed "left behind" drive to infect an entire network.

3. Downloading Unsolicited Antivirus Software

Everyone has stumbled upon a pop-up warning that "your PC will be at risk unless you download free antivirus software immediately". Hackers are experts at getting you to download files before you know what's happening, and one of their favorite tricks is to pretend their infectious code is actually a virus-scanning program to help you defend against online threats. However, clicking on this malware could actually block your computer from using legitimate antivirus solutions

4. Using the Same Password Without the Two -Factor Authentication



When you make all of your passwords for e-commerce, banking and government websites the same, you're really making a hacker's day. This so-called "daisy chaining" allows all of your accounts to be compromised by breaking into just one. Make sure you have multiple passwords for your various accounts, and try out new variations every six months or so.

J.Karthik Raja II / CSE

Software Testing

Software testing is an investigation conducted to provide stakeholders with information about the quality of the software product or service under test. Software testing can also provide an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation. Test techniques include the process of executing a program or application with the intent of finding software bugs(errors or other defects), and verifying that the software product is fit for use

V.S.Ramyasri, II / CSE

Hacker culture can be traced to 1959 ☢ Hacker's Memorandum was published on leap day 1972.