HACKING

Presented By:
Reena Sharma
Assistant professor
Computer dept

. Introduction to Hacking

The Internet, like any other new media historically, provides new methods of engaging in illegal activities. That is not to say that the Internet is intrinsically 'bad', as many tabloid journalists would have us to believe, it is simply a means for human beings to express themselves and share common interests. Unfortunately, many of these common interests include pornography (writing, picturing), trading Warez (pirated software), trading illegal MP3 files, and engaging in all kinds of fraud such as credit card fraud.

TYPES OF HACKING

- **White -Hat Hackers**
  This type of hacker enjoys learning and working with computer systems, and consequently gains a deeper understanding of the subject. Such people normally go on to use their hacking skills in legitimate ways, such as becoming security consultants. The word 'hacker' was originally used to describe people such as these.

- **Black-Hat Hackers**
  This is the more conventional understanding of the term 'hacker', one that is portrayed in newspapers and films as being essentially 'chaotic', an obsessive social misfit hell-bent on the destruction of everything good about the Internet. White-hat hackers often call this kind of hacker a 'cracker', as they spend most of their time finding and exploiting system insecurities.
  In reality, nobody really fits into either camp neatly. It is down to the individual's set of ethics to decide what path that they will take in their hacking career. Not all of the activities of white-hat hackers may be legal, while not all of the black-hat hackers activities are illegal, so many shades of

- **2. Hacker Motivation & Hackers Attacking**
  The factors that affect the motivation of someone who is drawn to illegal hacker activities are not always clear. It is well known, for example, that few hackers are motivated by financial gain. Most hacker activity is of a nature were money is rarely involved.
  2.1 Factors of Motivation
  Few studies have been carried out into hacker motivation, although much has been gained by interviewing former hackers who have now gone 'white-hat' (i.e. hacking for security companies etc.). Here are some of the factors that may motivate a person into becoming a hacker:

  Curiosity:

  Money:

  Spying:

  Anarchy:

  Money:

- **Why Do Hackers Attack?**
  There are many reasons why a hacker might attack a system. Some possibilities may include:
  •Obtain a company's secrets or insider information
  • Use the system's hard drive for storage, often for pornography or stolen software
  •Steal credit card numbers
  •Steal passwords to other systems
  •Use the computer in an attack on another computer or system
  •To steal programs or files
  •Read others' email
  •Stalking
  •A challenge, or "to see if I can"
  •To impress other hackers

3. Hacking Techniques

- **3.1 Overview of Hacking Techniques**
  The depth and variety of techniques employed by hackers to illegally enter a computer system are vast, for this reason I intend to provide a brief overview of some of the more common techniques involved, without going into to much detail on any particular technique.
  Hacking a system is a two-step process, Gathering Information and Launching an Attack.
  3.2 Gathering Information
  A dedicated hacker may spend several months gathering information on the intended target before launching an attack armed with this new information ", but there are also more remote methods available to the hacker.

- **Port Scanning**: A port scanner is a program that automatically detects security weaknesses in a remote system. Scanners are TCP port scanners, that attack TCP/IP ports and services (Telnet or FTP, for example), and record the response from the target. In this way, they learn valuable information about the targeted system such as if whether or not the remote system will allow an anonymous user to log in, or indeed if the system is protected by a firewall.

  Many hackers simply type large amounts of IP addresses into a port-scanning program and launch random attacks on many users simultaneously, hoping to strike it lucky with that one system that shows a serious weakness.

Packet Sniffing: A sniffer is a piece of software that grabs information 'packets' that travel along a network. That network could be running a protocol, such as Ethernet, TCP/IP, IPX or others. The purpose of the sniffer is to place the network interface into 'promiscuous' mode and by doing so, capture all network traffic. Looking into packets can reveal valuable information like usernames, passwords, addresses or the contents of e-mails

Password Cracking: A password cracker is a program that attempts to decrypt or otherwise disable password protection. Often simulation tools are used to simulate the same algorithm as the original password program. Through a comparative analysis, these tools try to match encrypted versions of the password to the original. Many password crackers are simply brute-force engines that try word after word from a dictionary, often at very high speeds

THANKYOU