Cyber Security – lecture 2

“The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb”

National Research Council, U S A "Computers at Risk” (1991)

Contents

- Hacking
- Types of Hackers
- Tips to get protected from Cyber Crime
- Attack Vectors
- Introduction to incident response
- Digital Forensics

Hacking

- What is Hacking?
  - The Process of attempting to gain or successfully gaining, unauthorized access to computer resources is called Hacking.
- Who is a hacker?
  - In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network.
  - The term hacker is reclaimed by computer programmers who argue that someone breaking into computers is better called a cracker.

Hacking – Contd.

- Why do hackers hack?
  - Just for fun.
  - Show off.
  - Hack other systems secretly.
  - Notify many people their thought.
  - Steal important information.
  - Destroy enemy’s computer network during the war.

Hacking – Contd.

- Types of Hacking
  - Website Hacking
    - Hacking a website means taking control from the website owner to a person who hacks the website.
  - Network Hacking
    - Network Hacking is generally means gathering information about domain by using tools like Telnet, Ns look UP, Ping, Tracert, Netstat, etc… over the network.
  - Ethical Hacking
    - Ethical hacking is where a person hacks to find weaknesses in a system and then usually strengthen them.
  - Email Hacking
    - Email hacking is illicit access to an email account or email correspondence.

Hacking – Contd.

- Types of Hacking
  - Password Hacking
    - Password Hacking or cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
  - Online Banking Hacking
    - Online banking Hacking Unauthorized accessing bank accounts without knowing the password or without permission of account holder is known as online banking hacking.
  - Computer Hacking
    - Computer Hacking is when files on your computer are viewed, created, or edited without your authorization.

Hacking – Contd.

- What should do after hacked?
  - Shutdown the system – Or turn off the system
  - Separate the system from network
  - Restore the system with the backup– Or reinstall all programs
  - Connect the system to the network
  - It can be good to call the police

Hacking – Contd.

- Advantages of hacking
  - Can be used to recover lost information where the computer password has been lost.
  - Teaches you that no technology is 100% secure.
  - To test how good security is on your own network. They call it white hat computer hacking.
- Disadvantages of Hacking
  - Criminals can use it to their advantage.
  - It can harm someone's privacy
  - It's Illegal

TYPES OF CYBER HACKERS

- White hat hacker:
  - White hat hackers, also known as ethical hackers are the cybersecurity experts who help the Govt and organizations by performing penetration testing and identifying loopholes in their cybersecurity.
  - They even do other methodologies and ensure protection from black hat hackers and other malicious cyber crimes.
  - They will hack into your system with the good intention of finding vulnerabilities and help you remove virus and malware from your system.
- Black hat hacker:
  - These hackers look for vulnerabilities in individual PCs, organizations and bank systems. Using any loopholes they may find, they can hack into your network and get access to your personal, business and financial information.

TYPES OF CYBER HACKERS

- Gray hat hacker:
  - Gray hat hackers fall somewhere in between white hat and black hat hackers.
  - Hacker who hacks into an organization and finds some vulnerability may leak it over the Internet or inform the organization about it.
  - A gray hat hacker doesn't use his skills for personal gain, he is not a black hat hacker. Also, because he is not legally authorized to hack the organization's cybersecurity, he can't be considered a white hat either.
- Script Kiddies
  - These hackers usually download tools or use available hacking codes written by other developers and hackers. Their primary purpose is often to impress their friends or gain attention.
  - However, they don't care about learning. By using off-the-shelf codes and tools, these hackers may launch some attacks without bothering for the quality of the attack.

TYPES OF CYBER HACKERS

- Red hat hacker:
  - Red Hat Hackers have an agenda similar to white hat hackers.
  - Instead of reporting a malicious attack, they believe in taking down the black hat hacker completely.
  - Red hat hacker will launch a series of aggressive cyber attacks on the black hat hacker so that the hacker may have to replace the whole system.
- State/Nation Sponsored Hackers
  - State or Nation sponsored hackers are those who have been employed by their state or nation's government to snoop in and penetrate through full security to gain confidential information from other governments to stay at the top online.
  - They have an endless budget and extremely advanced tools at their disposal to target individuals, companies or rival nations.

Tips to get protected from Cyber Crime

- Some easy tips to protect computers from the growing threats:
  - Terminate Online Session Completely
    - Always terminate your online session by clicking on the "Log out or Sign Out" button.
    - Avoid using the option of "remember" your username and password information.
  - Create Backup of Important Data
    - Backup of all the important files whether personal or professional should be created.
  - Use Security Programs
    - If your system does not have data protection software to protect online, then by all means buy internet security program for your computer.
  - Protect Your Password
    - Try creating a password that consists of a combination of letters, numbers and special characters. Password should be changed regularly. Do not share your password with other people.

Tips to get protected from Cyber Crime – Contd.

- Some easy tips to protect computers from the growing threats:
  - Participation in Social Networking
    - While participating in most social networking sites do not expose the personal information to others.
  - Use Your Own Computer
    - It's generally safer to access your financial accounts from your own computer only. If you use some others computer, always delete all the "Temporary Internet Files", and clear all your "History" after logging off your account.
  - Update Your Software Package Regularly
    - Frequent online updates are needed for all the Internet security software installed on your computer system.
  - Using Email
    - Do not any links in emails from people you do not know. Hackers do use E-mail as the main target seeking to steal personal information, financial data, security codes and other.

Attack Vectors

- An attack vector is a path or means by which a hacker can gain access to a computer or network server in order to deliver a malicious payload or malware.
- Attack vectors enable hackers to exploit system vulnerabilities, including the human element.
- Attack vectors include viruses, e-mail attachments, Web pages, pop-up windows, instant messages, chat rooms, and deception.
- All of these methods involve programming except deception
- In deception a human operator is fooled into removing or weakening system defenses.

Attack Vectors – Contd.

- To some extent, firewalls and anti-virus software can block attack vectors. But no protection method is totally attack-proof.
- A defense method that is effective today may not remain so for long, because hackers are constantly updating attack vectors, and seeking new ones to gain unauthorized access to computers and servers.
- The most common malicious payloads are viruses, Trojan horses, worms, and spyware.
- If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.

Introduction to incident response

- Incident response is an organized approach to addressing and managing the after effect of cyberattack, also known as an IT incident, computer incident or security incident.
- The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.
- Ideally, incident response activities are conducted by the organization's computer security incident response team (CSIRT)

Introduction to incident response – Contd.

- CSIRT is a group that has been previously selected to include information security and general IT staff as well as C-suite level members.
- The team may also include representatives from the legal, human resources and public relations departments.
- The CSIRT response should match with the organization's incident response plan (IRP)
- IRP is aa set of written instructions that outline the organization's response to a cyberattack.

Introduction to incident response – Contd.

- Importance of incident response
  - Any incident that is not properly contained and handled can escalate into a bigger problem that can ultimately lead to a damaging data or system collapse.
  - Responding to an incident quickly will help an organization minimize losses, reduce exploited vulnerabilities, restore services and processes, and reduce the risks that come in future.
  - Incident response enables an organization to be prepared for the unknown as well as the known and is a reliable method for identifying a security incident immediately when it occurs.
  - Incident response also allows an organization to establish a series of best practices to stop an intrusion before it causes damage.

Introduction to incident response – Contd.

- Who is responsible for incident response?
  - To properly prepare for and address incidents across the business, an organization should form a CSIRT. This team is responsible for analyzing security breaches and responding appropriately. An incident response team may include:
    - An incident response manager, usually the director of IT, who oversees and prioritizes actions during the detection.
    - Security analysts who support the manager and work directly with the affected network to research the time, location and details of an incident.
    - Threat researchers that provide threat intelligence and context for an incident.
    - Management support is key to securing the necessary resources, funding, staff and time commitment for incident response planning and execution.
    - The incident response team may also include a human resources representative, especially if the investigation reveals that an employee is involved with an incident;
    - Including the organization's general council can ensure that the collected evidence maintains its forensic value in case the organization decides to take legal action;

Introduction to incident response – Contd.

- Incident response plan - IRP
  - An IRP should include procedures for detecting, responding to and limiting the effects of a data security breach.
  - Incident response plans usually include instructions on how to respond to potential attack scenarios, including data breaches, denial of service/distributed denial of service attacks, network intrusions, virus, worms or malware outbreaks or insider threats.
  - Without an incident response plan in place, an organization may not detect the attack, or it may not follow proper protocol to contain the threat and recover from it when a breach is detected.

Introduction to incident response – Contd.

- Incident response plan - IRP
  - An incident response plan can benefit an enterprise by outlining how to minimize the duration of and damage from a security incident, identifying participating stakeholders, streamlining forensic analysis, hastening recovery time, reducing negative publicity and ultimately increasing the confidence of corporate executives, owners and shareholders.
  - The plan should identify and describe the roles and responsibilities of the incident response team members who are responsible for testing the plan and putting it into action.
  - The plan should also specify the tools, technologies and physical resources that must be in place to recover breached information.

Introduction to incident response – Contd.

- There are six key phases of an incident response plan [IRP]:
  - Preparation: Preparing users and IT staff to handle potential incidents that may arise
  - Identification: Determining whether an event is really a security incident
  - Containment: Limiting the damage of the incident and isolating affected systems to prevent further damage
  - Eradication: Finding the root cause of the incident, removing affected systems from the production environment
  - Recovery: Permitting affected systems back into the production environment, ensuring no threat remains
  - Lessons learned: Completing incident documentation, performing analysis to learn from the incident and potentially improve future response efforts

Digital Forensics

- What is digital forensic?
  - Digital Forensics is the preservation, identification, extraction, interpretation and documentation of computer evidence which can be used in the court of law.
  - Digital forensics is a branch of forensic science which includes the recovery and investigation of material found in digital devices, often in relation to cyber crime.
  - Technically, the term computer forensics refers to the investigation of computers. Digital forensics includes not only computers but also any digital device, such as digital networks, cell phones, flash drives and digital cameras.
- Branches of Digital Forensics include:
  - Network Forensics
  - Firewall Forensics
  - Database Forensics
  - Mobile Device forensics

Digital Forensics - Contd

- Benefits of Digital Forensics:
  - Digital Forensics help to protect from and solve cases involving:
    - Theft of intellectual property-
      - This related to any act that allows access to trade secrets, customer data, and any confidential information.
    - Financial Fraud-
      - This related to anything that uses victims information to conduct illegal transactions.
    - Hacker system penetration-
      - Taking advantage of vulnerabilities of systems or software using tools such as rootkits and sniffers.
    - Distribution and execution of viruses and worms-
      - These are the most common forms of cyber crime and often cost the most damage.

Digital Forensics - Contd

- Challenges faced by Digital Forensics:
  - The increase of PC's and internet access has made the exchange of information quick and inexpensive.
  - Easy availability of Hacking Tools.
  - Lack of physical evidence makes crimes harder to prosecute.
  - The large amount of storage space available to suspects, up to over 10 Terabytes.
  - The rapid technological changes requires constant upgrade or changes to solutions.

Digital Forensics - Contd

- Digital Forensic Process- 5 Major Steps
  - Identification
    - The first step in the forensic process:
      - What evidence is present
      - Where it is stored and
      - How it is stored Preservation
  - Preservation
    - Isolate, secure and preserve the state of physical and digital evidence.
    - This includes preventing people from using the digital device or allowing other electromagnetic devices to be used within an affected radius.

Digital Forensics - Contd

- Digital Forensic Process.
  - Analysis
    - Determine significance, reconstruct fragments of data and draw conclusions based on evidence found.
    - It may take several iterations of examination and analysis to support a crime theory.
  - Documentation
    - A record of all visible data must be created, which helps in recreating the scene and reviewing it any time
    - Involves proper documentation of the crime scene along with photographing, sketching and crime-scene mapping.
  - Presentation
    - Summarize and provide explanation of conclusions.
    - This should be written in a layman's language using abstracted terminologies.
    - All abstracted terminologies should reference the specific details.

Digital Forensics - Contd

- Need for Digital Forensics
  - To ensure the integrity of digital system.
  - To focus on the response to hi-tech offenses, started to intervene the system.
  - Digital forensics has been efficiently used to track down the terrorists from the various parts of the world.
  - To produce evidence in the court that can lead to the punishment of the criminal.

Digital Forensics - Contd

- Skills required for Digital Forensics
  - Application of Programming or computer-related experience
  - Broad understanding of operating systems and applications
  - Strong analytical skills
  - Strong computer science fundamentals
  - Strong system administrative skills
  - Knowledge of the latest intruder tools
  - Knowledge of cryptography and steganography
  - Strong understanding of the rules of evidence and evidence handling
  - Ability to be an expert witness in a court of law

Digital Forensics - Contd

- Digital Forensic Software Tools
  - Logicube:
    - One of the Leading digital forensic hard drive data recovery technology.
    - Widely used by cybercrime experts and corporate security personnel.
  - DIBS:
    - Hardware and software, specifically designed to copy, analyze and present computer data in a forensically sound manner.
  - AcessData:
    - A pioneer in digital investigations since 1987.
    - Provide state of the art cyber security, password cracking, eDiscovery and decryption solutions.
  - BACKTRACK 5R3, Kali Linux etc……