Cyber Security Tools and Technologies

Dr. Arshad Ali
Associate Professor
NUCES Lahore

Cyber Threats

A **Cyber threat**

- is any malicious act that attempts to gain access to a computer network without authorization or permission from the owners.

- refers to the wide range of malicious activities that can damage or disrupt a computer system, a network or the information it contain.

- **Most common cyber threats**: Social Engineered Trojans, Unpatched Software, Phishing, Network worms, etc.

Cyber Threats Sources

- Anyone with a motive and the needed technology can create cyber threats.

- Cyber threats can come from a wide variety of sources, some notable examples include:
    - National governments.
    - Terrorists.
    - Industrial secret agents.
    - Rogue employees.
    - Hackers.
    - Business competitors.
    - Organization insiders.

Cyber Threat Classifications

- Threats can be classified by multiple criteria:
  - Attacker's Resources
  - Attacker's Organization
  - Attacker's Funding

- On basis of these criteria, threats are of 3 types:
  - Unstructured Threats
  - Structured Threats
  - Highly Structured threats

Unstructured Cyber Threats

- **Resources:** Individual or small group.
- **Organization:** Little or no organization.
- **Funding:** Negligible.
- **Attack:** Easy to detect and make use of freely available cyberattack tool.
- Exploitation based on documented vulnerabilities.

Structured Cyber Threats

- **Resources:** Well trained individual or group.
- **Organization:** Well planned.
- **Funding:** Available.
- **Attack:** Against particular individual or organizations.

❖

- Exploitation based on information Gathering.

Highly Structured Cyber Threats

- Extensive organization, resources and planning over time.
- Attack: Long term attack on particular machine or data.
- Exploitation with multiple methods:
    - Technical, social and insider help.

Cyber Security Threat Index Level

- Cyber threats are evaluated daily by the CTU (counter threat unit) and associated with a threat index level.
- The indicator shows the current level of malicious cyber activity and reflects the potential for, or actua damage.
- The threat index levels are:
  - Low
  - **Blue or Guarded**
  - **Elevated**
  - **High**
  - **Severe**

Cyber Security Threat Index Level

- **Green or Low:** indicates a low risk

- **Blue or Guarded:** Indicates a **general risk** of increased hacking, virus or other malicious activity.
  - The potential exists for malicious cyber activities,
    - but no known exploits have been identified or
    - known exploits have been identified but no significant impact has occurred.
- **Yellow or Elevated:** Indicates a significant risk
- There are known vulnerabilities that are being exploited wit a moderate level of damage/disruption or
- The potential for significant damage or disruption is high.

Cyber Security Threat Index Level

Orange or High: Indicates a high risk of increased hacking, or any other malicious cyber activity which

- targets or compromises core infrastructure,
- causes multiple service outages, multiple system compromises or compromises critical infrastructure
- At this level, vulnerabilities are being exploited with high level of damage or disruption or the potential for severe damage or disruption is high.

Cyber Security Threat Index Level

Red or Severe: Indicates a severe risk of increased hacking, virus or any other malicious cyber activity which

- results in wide-spread outages and/or significantly destructive compromises to systems with no known remedy or weakens one or more critical infrastructure sectors.
- At this level, vulnerabilities are being exploited with severe level or wide spread level of damage or disruption of Critical Infrastructure Assets.

Types of Cyber Security

Types of Cyber Security

Advanced Persistent Threat (APT):

- A network attack in which an unauthorized person gains access to network and stays there undetected for a long period of time.

Backdoor:

- Method of bypassing normal authentication and gaining access in OS or application.

Buffer Overflow:

An exploit that takes advantage of the program that is waiting for a user's input.

Types of Cyber Security

Man-in-the-middle Attack

- This attack intercepts and relays messages between two parties who are communicating directly with each other.

Cross-Site Scripting (XSS):

- A code injection attack that allows an attacker to execute malicious JavaScript in another user's browser.

Denial of Service Attack:

- Any attack where the attackers attempt to prevent the authorized users from accessing the service.

Types of Cyber Security

SQL injection:

- A very common exploited web application vulnerability that allows malicious hacker to steal an alter data in website's database.

Zero-day exploit:

- A vulnerability in a system or device that has been disclosed but is not yet patched.

Impacts of Cyber Attacks

- A successful cyber attack can cause major damage to organizations or systems, as well as to business reputation and consumer trust.

- Some potential results include:
    - Financial loss.
    - Reputational damage.
    - Legal consequences.

Malicious Code

Types of Malicious Code

Virus:

- Malicious software program, when it is executed, it replicates itself by modifying other computer programs and inserting its own code.

Network Worm:

- Standalone malware which replicates itself in order to spread to other computers.

Trojan Horse:

- A program that claims to free your computer from viruses but instead introduces viruses onto your system.

Types of Malicious Code

Botnet:

- Used to perform distributed denial-of-service attack (DDoS attack), steal data, send spam, and allow the attacker access to the device and its connection.

Keylogger:

- A type of surveillance technology used to monitor and record each keystroke typed on specific computer's keyboard.

Rootkit:

- Collection of tools or programs that enable administrator-level access to computer or computer network.

Types of Malicious Code

Spyware:

- Software that is hidden from the user in order to gather information about internet interaction, keystrokes, passwords, and other valuable data.

Adware:

- Designed to display advertisements on your comput and redirect your search requests to advertising websites to collect marketing data about you.

Ransomware:

- Malware that prevents or limits users from accessing their system, either by locking the system's screen o by locking the user's files unless a ransom is paid.

Vulnerabilities

What is a Vulnerability?

- A cyber-security term that refers to a flaw in a syste that can leave it open to attack.

Vulnerability is the composition of three elements:

- A flaw in system.
- Access of attacker to that flaw.
- Capability of attacker to exploit the flaw.

Classification of Vulnerabilities

Vulnerabilities are classified according to the assets

- Hardware
- Software.
- Network.
- Personal.
- Physical site.
- Organizational.

Vulnerability Causes

Some of the vulnerability in the system occur due to:

- Missing patches.
- Cleartext credentials.
- Using unencrypted channels.
- **RF Emanation**
  - electromagnetic radiations that all electric devices emit.
  - If such radiations are disclosed,
  - there is a risk that information carried by radiations may leak out to unauthorized persons.

Cyber Security Careers

What careers are there?

A short description of a few **offensive** security roles:

- **Penetration Tester -** Responsible for testing technology products for finding exploitable security vulnerabilities.
- **Red Teamer -** Plays the role of an adversary, attacking an organization and providing feedback from an enemy's perspective.
- **Security Engineer -** Design, monitor, and maintain security controls, networks, and systems to help prevent cyberattacks.

Penetration Testers

- A **Penetration test** or pentest is an ethically-driven attempt to test and analyse the security defences to protect assets (devices) and pieces of information.

- A penetration test involves using the same tools, techniques, and methodologies that someone with malicious intent would use and is similar to an audit.
- According to a cybersecurity industry magazine, there are over 2,200 cyber attacks every day - 1 attack every 39 seconds (2017).

Penetration Testers

- perform authorised tests on organisation's computer systems
  - to identify security weaknesses (vulnerabilities) that could be exploited by cyber criminals.

- find and report security holes before an attacker does.

Responsible for testing technology products for finding exploitable security vulnerabilities.

Penetration Testers: Responsibilities

A penetration tester will likely be required to:

- Work with clients to determine their **requirements** and **scope** of the security assessment (what specifically **-attempting to hack**)

- Perform **physical** security assessments of systems, servers and other network devices to identify areas that require physical protection

- Enumerate and **identify** vulnerabilities in clients computer systems, networks and applications

Penetration Testers: Responsibilities

- Determine the **root cause** of technical and non-technical security issues
- Establish **improvements** for existing security services, including hardware, software, policies and procedures
- Create **reports** detailing vulnerability findings including the risks levels, impacts of the attacks on the business and mitigation methods