Ethical Hacking

Module – 2

- **What are the types of hackers?**

Hackers fall into three general categories:

- ✓ black hat hackers
- ✓ white hat hackers
- ✓ Gray hat hackers.

- **Explain in brief - Ethical hacking and cyber security.**

Ethical Hacking

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers.

Cyber Security

cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security

- **Explain Footprinting Methodology**

Footprinting is an ethical hacking technique used to gather as much data as possible about a specific targeted computer system, an infrastructure and networks to identify opportunities to penetrate them. It is one of the best methods of finding vulnerabilities.

There are two types of foot printing in ethical hacking:

- ✓ active footprinting
- ✓ passive footprinting

Active footprinting

Active foot printing describes the process of using tools and techniques, like using the traceroute commands or a ping sweep -- Internet Control Message Protocol sweep -- to collect data about a specific target. This often triggers the target's intrusion detection system (IDS). It takes a certain level of stealth and creativity to evade detection successfully.

Passive footprinting

As the name implies, passive footprinting involves collecting data about a specific target using innocuous methods, like performing a Google search, looking through Archive.org, using Neo Trace, browsing through employees' social media profiles, looking at job sites and using Whois, a website that provides the domain names and associated networks fora specific organization. It is a stealthier approach to footprinting because it does not trigger the target's IDS.

- **Find basic information using Google advance search operator and Pipl search**
  - ✓ site:topsint.com
  - ✓ site:topsint.com erp
  - ✓ site:topsint.com filetype:pdf

- **Find vulnerability tool and check open port and service.**
  - ✓ Nmap
  - ✓ Wireshark
  - ✓ Angry IP Scanner
  - ✓ NetCat
  - ✓ Advanced IP Scanner