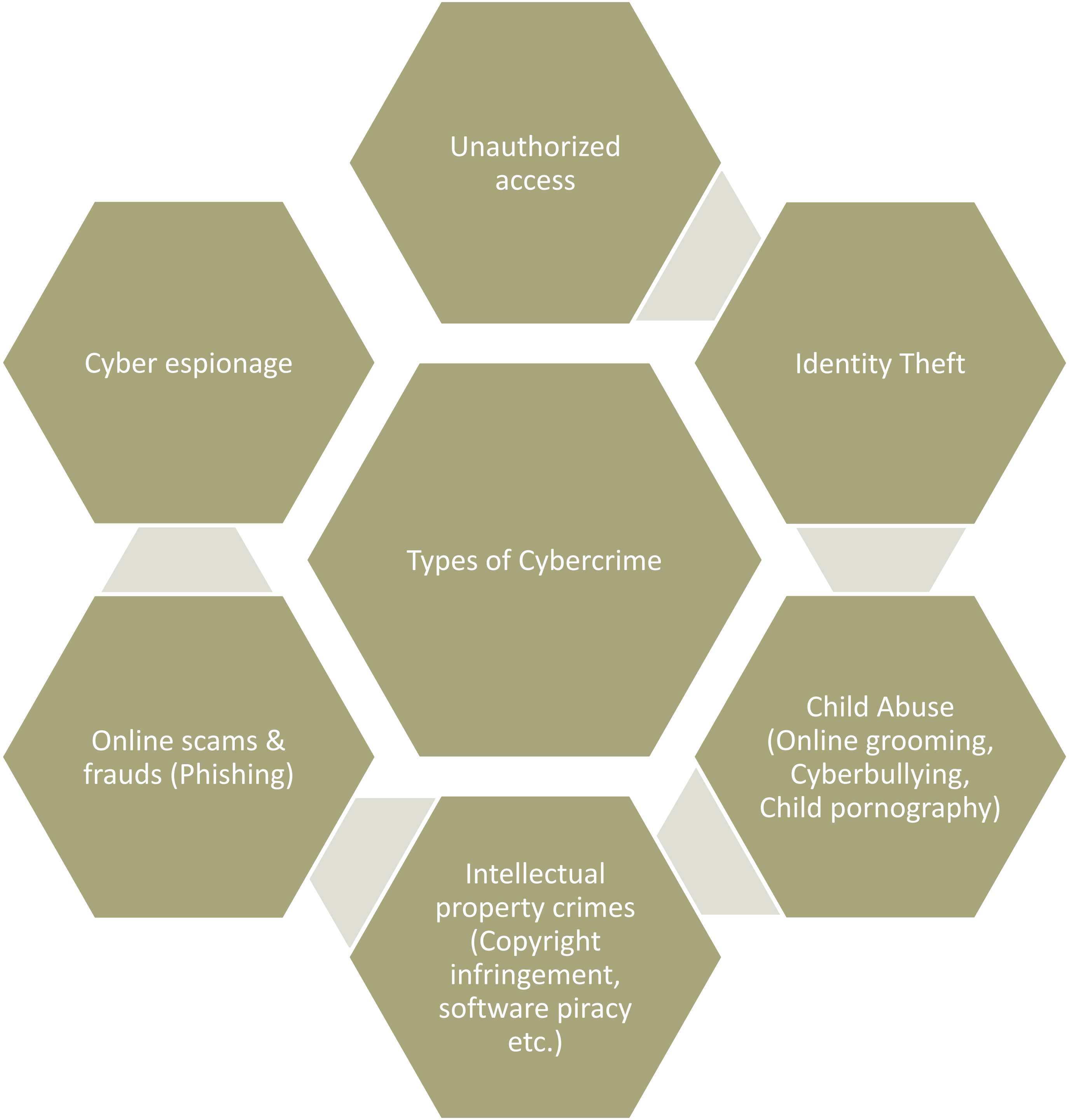
CYBERCRIME?

There should be a:

Computing device

Person involved

Intent to harm



Types of Cybercrime

Unauthorized access

Identity Theft

Child Abuse (Online grooming, Cyberbullying, Child pornography)

Intellectual property crimes (Copyright infringement, software piracy etc.)

Online scams & frauds (Phishing)

Cyber espionage

Digital evidence

- Any information stored/transmitted in digital forms that can be used in legal proceedings.
- System and network logs
- Email and messaging
- Files and documents
- Browser and internet history

Evidence Preservation

- Data imaging
- Secure storage
- Write blocking devices

Importance:

- Chain of custody
- Integrity
- Avoiding contaminations

Acquisition and analysis

- Practical

Networking

- IP address (192.168.0.1)
- Types of IP: IPv4 and IPv6
- MAC address

Both IPv4 and IPv6 addresses come from **finite pools** of numbers. For **IPv4**, this pool is 32-bits (232) in size and contains **4,294,967,296 IPv4 addresses**.

The maximum number of **IPv6** addresses is **340 undecillion**, or **2^128**, which is more than **100 times the number of atoms on Earth.**

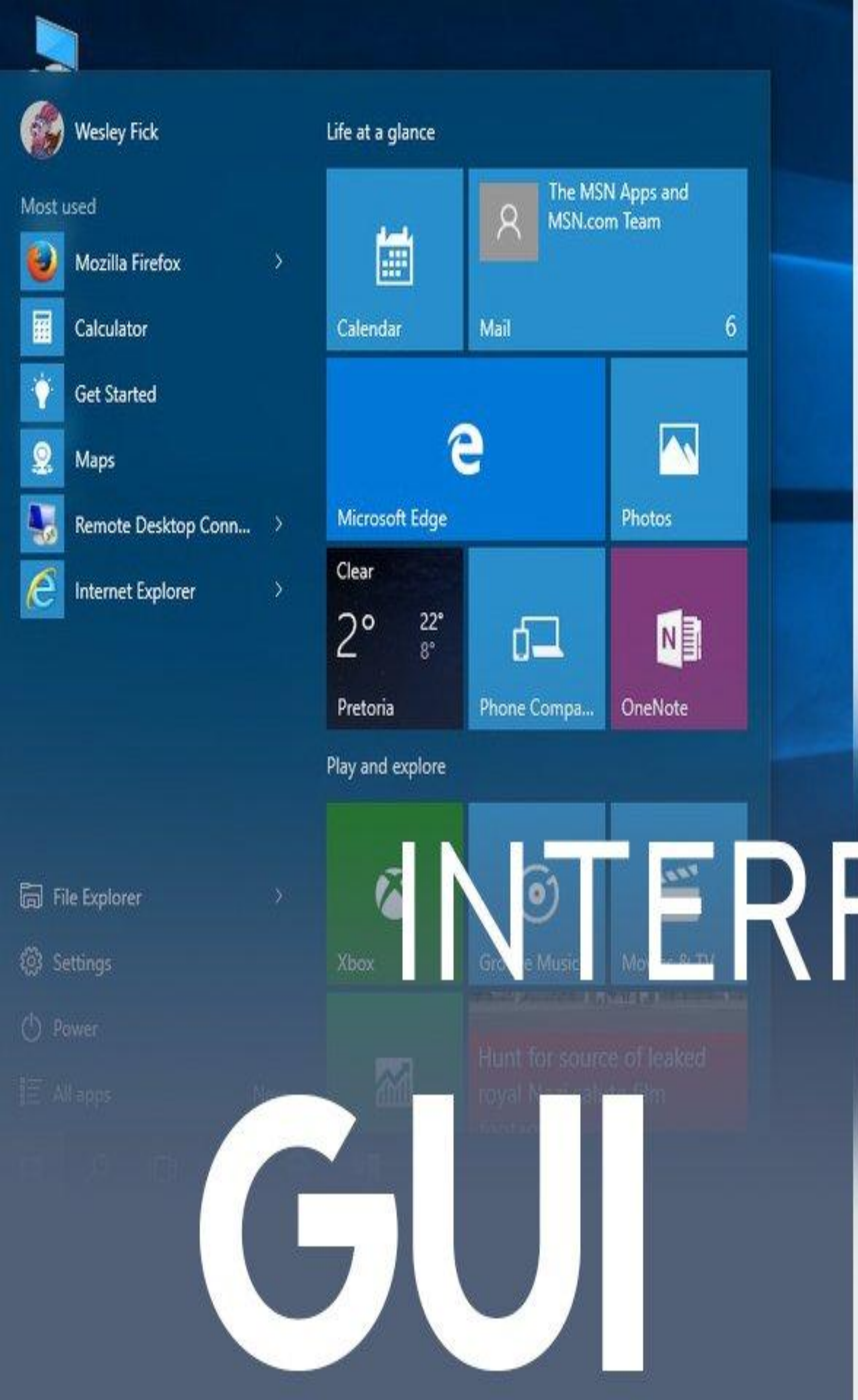
TCP port numbers:

The maximum TCP port number is **65,535** for both **IPv4** and **IPv6.**

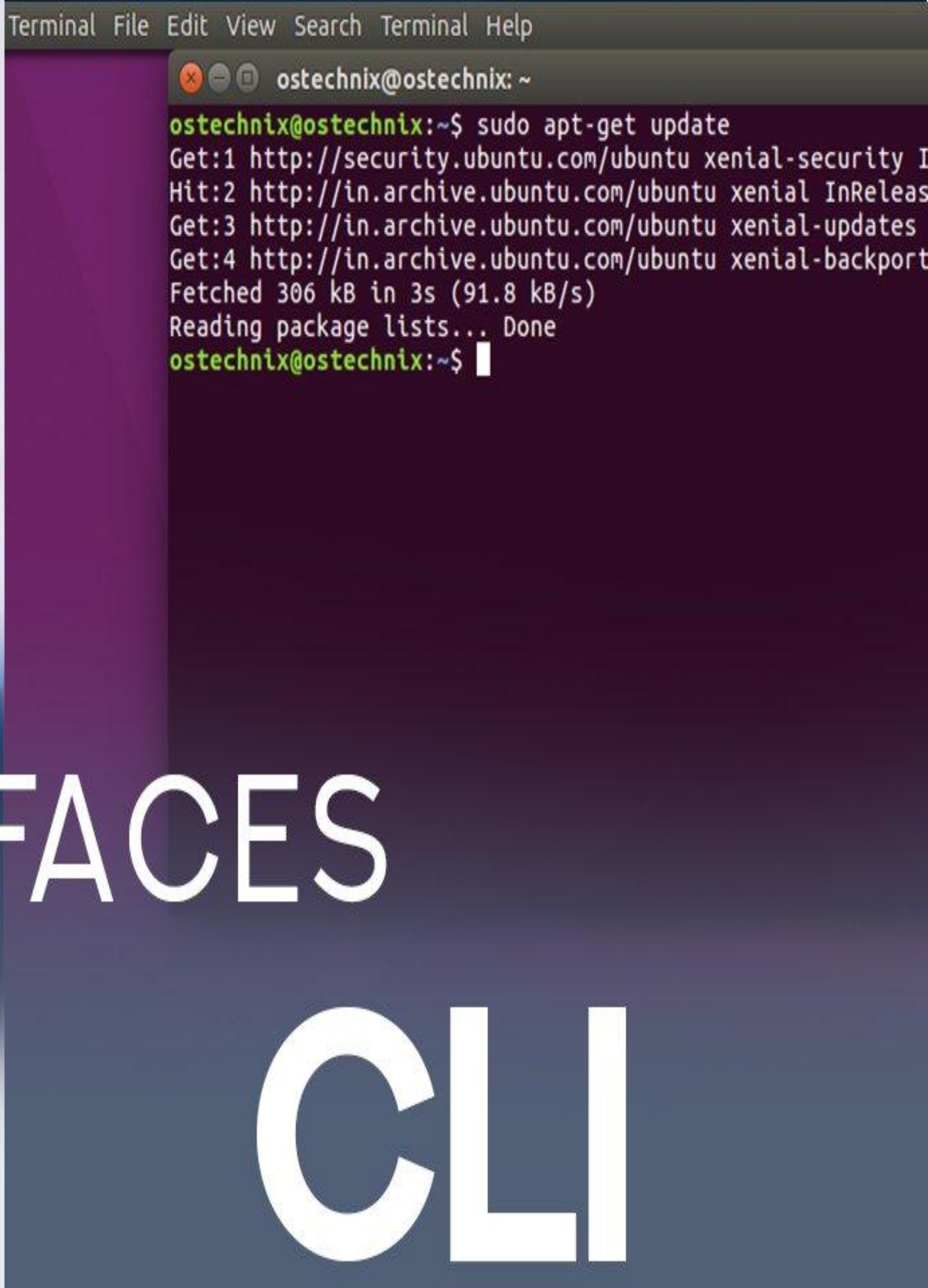
Ethical Hacking

- Ethical hacking involves the probing and testing of computer systems, networks, and applications purposely to identify and make amends on security vulnerabilities, an ethical hacker alias white-hat or pen tester, is mandated with similar goals to enhance security within an organization.

INTERFACES



GUI



```
ostechnix@ostechnix:~$ sudo apt-get update
Get:1 http://security.ubuntu.com/ubuntu xenial-security I
Hit:2 http://in.archive.ubuntu.com/ubuntu xenial InReleas
Get:3 http://in.archive.ubuntu.com/ubuntu xenial-updates
Get:4 http://in.archive.ubuntu.com/ubuntu xenial-backport
Fetched 306 kB in 3s (91.8 kB/s)
Reading package lists... Done
ostechnix@ostechnix:~$ 
```

CLI

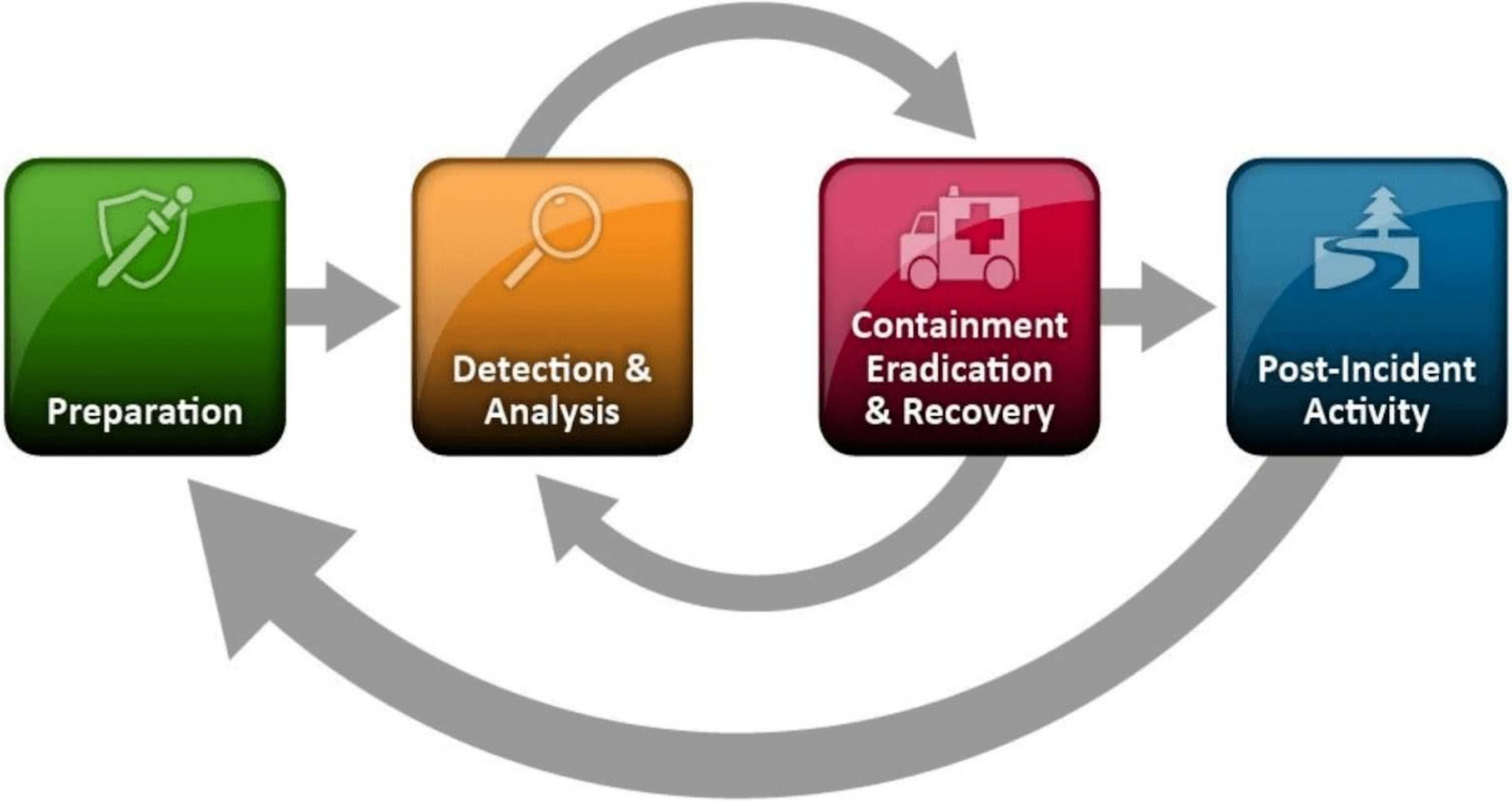
Basic commands

- **ls** : List directory contents
- **cd** : Change directory
- **pwd** : Print working directory
- **mkdir** : Create a new directory
- **rmdir** : Remove a directory
- **touch** : Create a file
- **rm** : Remove files
- **cp** : Copy files or directories
- **nano**: Open file in text editor

Virtual machines

- Practical Setup Kali Linux

Incident Response



Incident response team

- Incident commander
- Technical Lead
- Communication officer
- Legal and compliance officer
- Forensic experts
- IT support and system admins
- Public Relations

Incident Handling

Identifying:

- Monitoring alerts
- User and system reports
- Behavioral analysis

Containment: Short term / Long term

- Network isolation
- Account lockdown
- Service suspension

Investigation

- Data collection
- Forensic analysis
- Root cause analysis
- Impact assessment

Tools and Techniques

- EnCase
- FTK
- Autopsy
- Security logs
- Wireshark

Types of Hackers

White Hat Hackers

Ethical hackers improve security systems.

Black Hat Hackers

Malicious hackers exploit systems for gain.

Gray Hat Hackers

Blend of both Black hat & White hat Activities.

Script Kiddies

Inexperienced use pre-written tools.

Hacktivists

Promote political or social messages.

State-Sponsored Hacker

Conduct cyber espionage

Cyber Terrorists

Create fear and disruption for political/ideological reasons.

Key aspects of ethical hacking

Reporting: Ethical hackers report back to the organization with the results of the tests.

Permission-Based: This permission becomes necessary to differentiate their job from criminal hacking jobs

Objective: The main goal is to find the holes before hostile attackers can penetrate them. This includes discovering system, application, and network vulnerabilities that an attacker could exploit.

Methodology: Ethical hackers are given access to essential information about the systems, network architecture, data flow mechanisms in the organization etc. This assists with the testing and helps enhance security.

Benefits of Ethical Hacking

White hat hacking provides numerous benefits to organizations, individuals, and society as a whole. Some of the key advantages include:

- **Improved security**
- **Proactive defense**
- **Compliance**
- **Trust and reputation**
- **Cost savings**
- **Knowledge sharing**
- **Education and training**

White Hat Security Techniques

- Vulnerability scanning
- Penetration testing
- Social engineering
- Web application testing
- Network traffic analysis

White Hat Security Techniques

- Password cracking
- Reverse engineering
- Static and dynamic code analysis
- Security frameworks and platforms

Ethical Hacking: Legal Considerations and Limitations

The Five Phases Of Ethical Hacking

Reconnaissance/ Footprinting

Scanning

Gaining Access

Maintaining Access

Clearing Tracks

techjury

Key Terminologies

Attack OR Attack Vector

An attack vector is defined as the technique by which unauthorized access is gained inside the computer or network for a criminal purpose by exploiting the vulnerabilities in the system.

Risk

It can be defined as the probability of the loss from any particular threat from the threat landscape, which can exploit the system and gain the benefits from it such as loss of private and confidential information such as username and password, sensitive organization data, also the loss of the reputation which has occurred can be considered. Also, the loss occurred in terms of damage or destruction of hardware and software assets can be considered as Risk.

Threat

Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset

Vulnerability

Weaknesses or gaps in a systems security program, design policies and implementation that can be exploited by different threats to gain unauthorized access of a computer system or network.

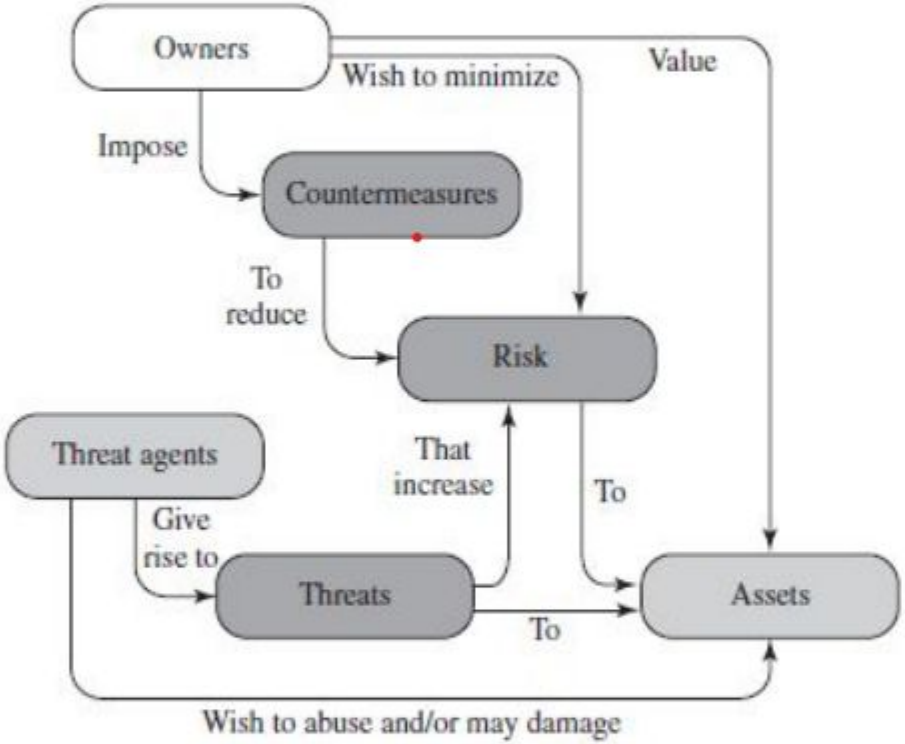
Asset

People, property, and information. People may include employees and customers. Property assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include reputation and proprietary information. Information may include databases, software code, critical company records, and many other intangible items.

Countermeasure

An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, or by minimizing the harm it can cause, or by discovering and reporting it so that corrective and proactive action can be taken. Here in the below image, we will the relationship between all the different terminologies we have seen

SECURITY CONCEPTS AND RELATIONS



ATTACKS

Attack

1. Active Attack

2. Passive Attack

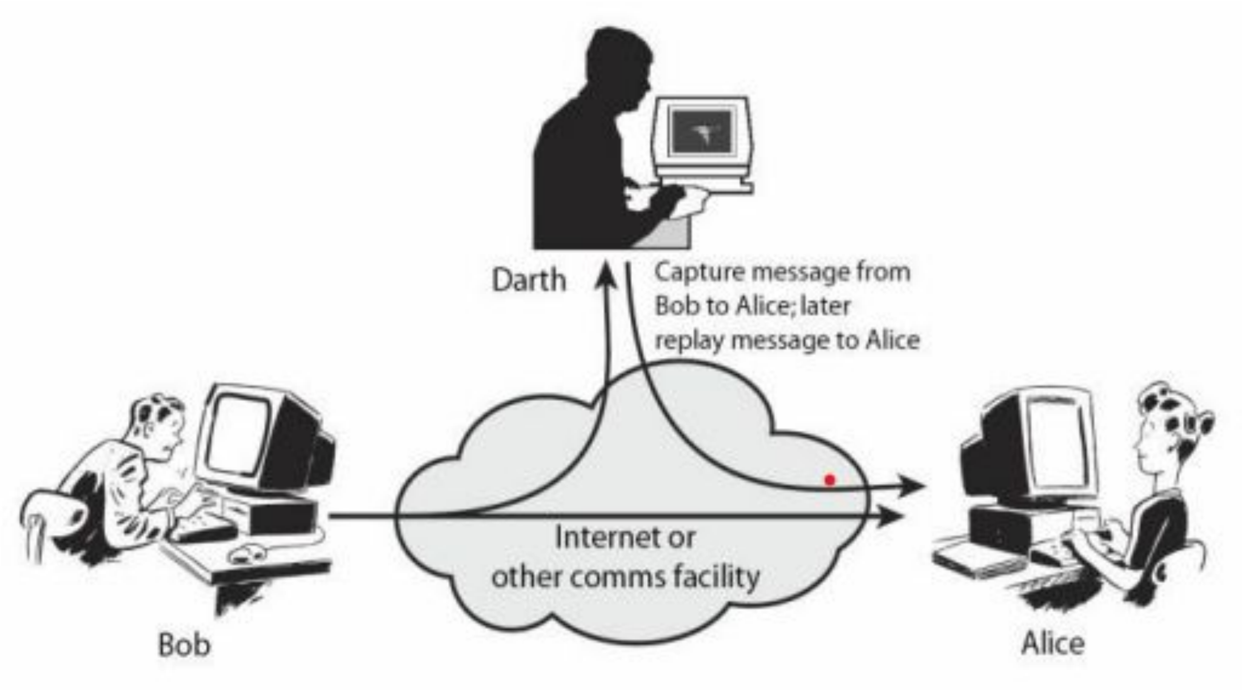
Classification based on Origin

1. Inside Attack :If the origin of the threat agent is from the inside the organization, which may have the authorization and access granted to the resources, but uses it with the criminal intent.

2. Outside Attack: Origin or source of the attack is from the outside of the organization and gains the unauthorized access to the system or resources with the criminal intent

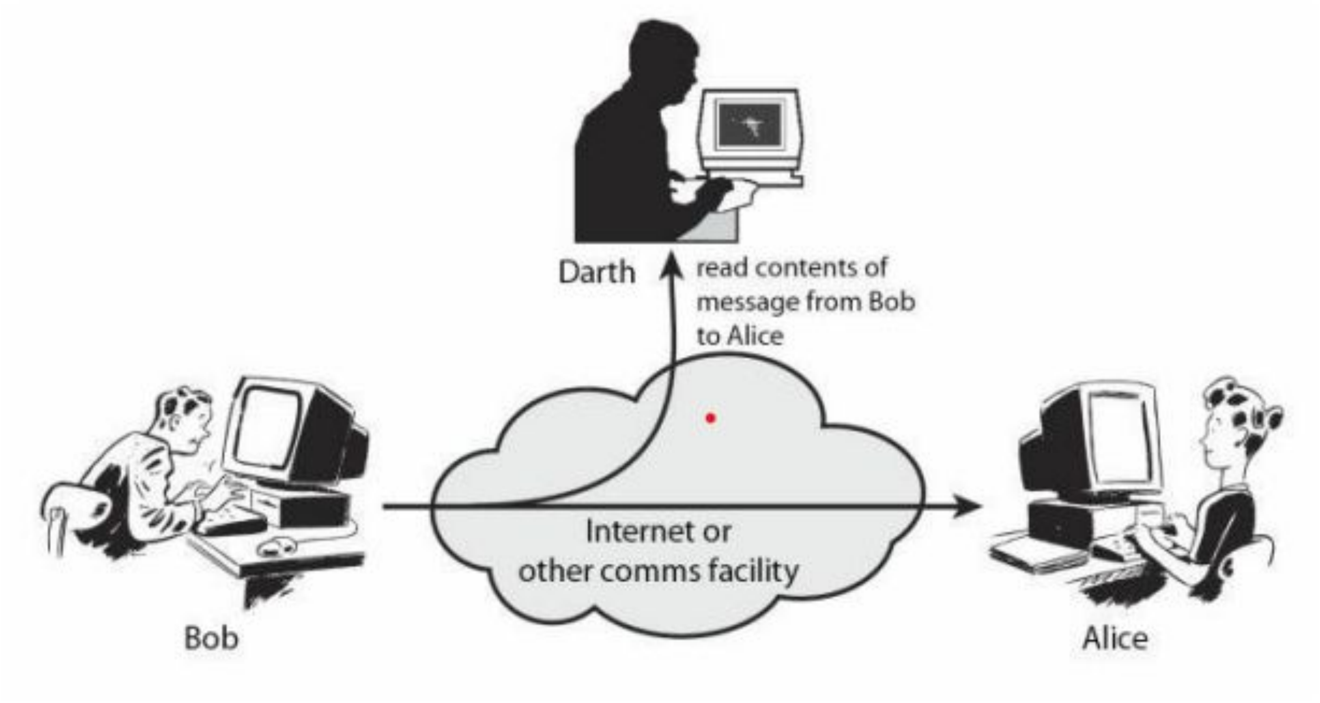
ACTIVE ATTACKS

In an active attack, the attacker intercepts the connection and then modifies information. An active attack can be divided further into Masquerade, Replay attack, Modification of messages


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

PASSIVE ATTACK

In a passive attack, the attacker intercepts the information but with the intent of reading the information and not modifying it. It can further be divided as Traffic Analysis and Release of Message content.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

1. Phishing

 a. Spear Phishing

2. SQL Injections

a. Blind SQL Injection b. Out of Bound SQL Injection

3. DoS and DDoS

4. Man-In-The-Middle attack and Session Hijacking

5. Brute-Force Attack

6. Malware Attack a. Virus / Worms / Trojons / Droppers b. Ransomware / Adware / Spywar