



Cyber security and Ethical Hacking



About me

I'm a Postgraduate

I'm a Certified Ethical Hacker [CEH v11]

I've completed multiple certification from EC council, Cisco, CodeRed etc.

My area of expertise is Cyber security-Ethical Hacking

I've hacked all my family personal electronic devices only for testing

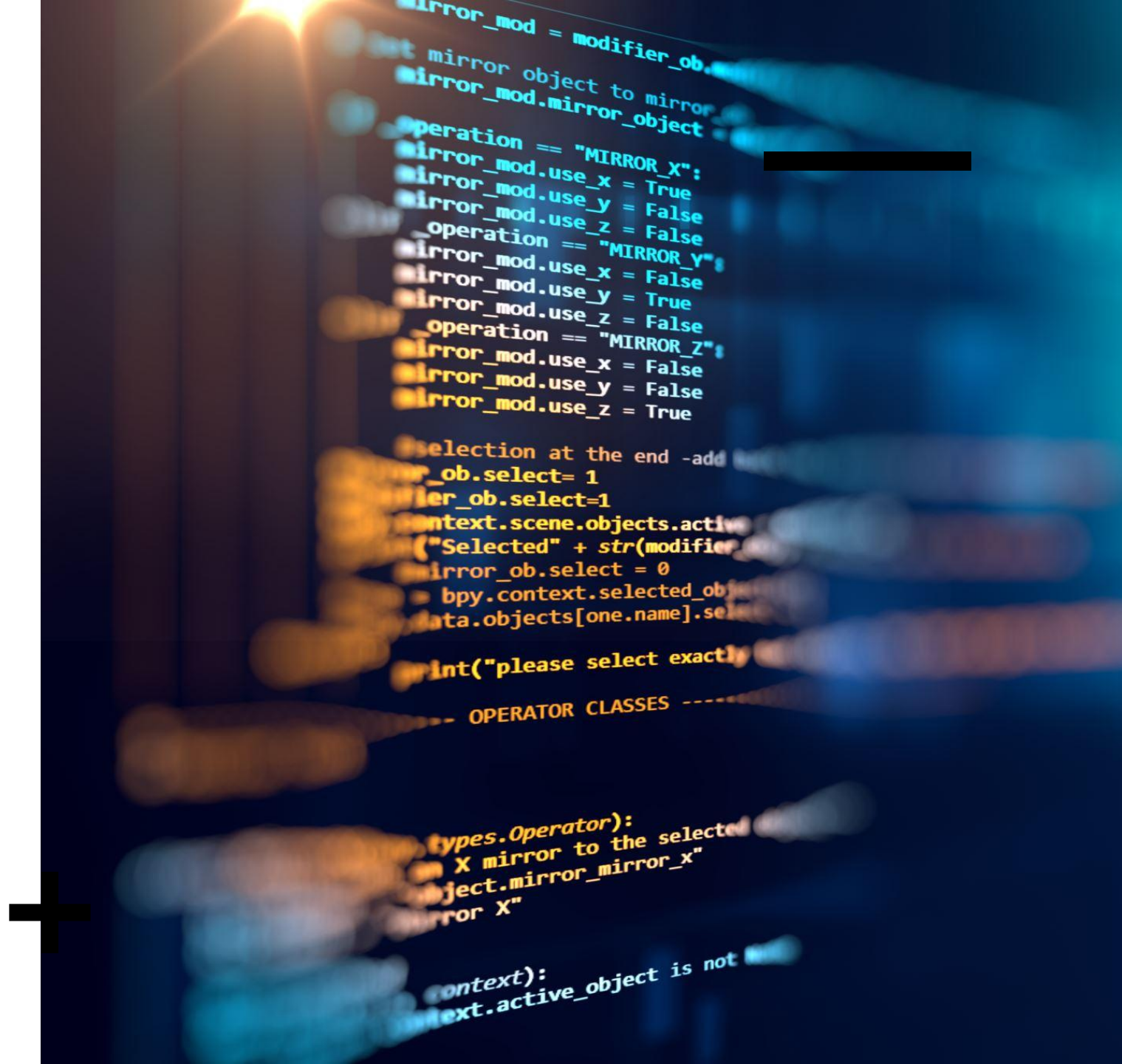
I work on many projects as well

Apart from testing I love hacking neighbour Wi-Fi's, testing other tools etc



Introduction to Cyber Security and Ethical Hacking

- Cyber security is broad term in which the ethical hacking exists.
- Ethical hacking specifically concerns with the security part.
- Cyber security cover all the remaining portions like strategies, analysis, planning etc.



What is cyber security?





What is cyber security?

- Cybersecurity refers to the practice of protecting computer systems, networks, software, and data from unauthorized access, use, disclosure, disruption, or destruction.
- It involves the implementation of measures and countermeasures to prevent, detect, respond to, and recover from incidents or attacks targeting digital infrastructure.

What is actual "Hacking"

2 days ago I named my WiFi
"Hack it if you can" and..



yesterday, it was changed to
"Challenge accepted"

When you use CTRL + C instead
of copying using right click



Me searching..

How to hack Microsoft like
Anonymous"

MEMECHAT APP

Kyuki apun ko "Profesnal Hecker" ban
na hai

Or this —
hacking?
?

Hacking

- Well, it simply means breaking into someone else system without their permission. It is illegal to do that around the world including India and you may go to Jail for this.
- So how to do it or practice it legally??

Incognito mode: *exists*
Me: *enables incognito*



What is Ethical Hacking?





What is Ethical Hacking?

- It is the practice of deliberately and legally attempting to identify vulnerabilities and weaknesses in computer systems, networks, applications, or websites.
- The main objective of ethical hacking is to help organizations improve their security posture by proactively identifying and addressing vulnerabilities.





Why do we really
concern for this?



From Individual
perspective



Need for cyber security

- Endless opportunities
- Security
- Keeping private things “private”
- Stopping any sort of frauds or crimes





From any business
perspective





Need for cyber security

- Maintaining Customer and Employee Trust
- Securing financial position of the organisation
- Preserve the Organization's Ability to Function
- Staying Strong Amidst Competition
- Reducing Risk



Cybersecurity is a universal challenge

By 2020, there will be...

20.8 billion

“things” to secure

5 billion

personal data records stolen

\$8 trillion

lost to cybercrime

...while security pressures continue to grow



**COMPLIANCE
MANDATES**

GDPR fines can cost

billions

for large global companies



**SKILLS
SHORTAGE**

By 2022, there will be

1.8 million

unfulfilled cybersecurity jobs



**TOO MANY
TOOLS**

Organizations are using

too many

tools from too many vendors

Reality of Hacking in movies and shows

+

```
Starting Hack....  
Hacking FBI 0%  
Hacking FBI 20%  
Hacking FBI 40%  
Hacking FBI 60%  
Hacking FBI 80%  
Hacking FBI 100%  
FBI Hacked Successfully
```

In the movies

```
1 print("Starting Hack....");  
2 print("Hacking FBI 0%");  
3 print("Hacking FBI 20%");  
4 print("Hacking FBI 40%");  
5 print("Hacking FBI 60%");  
6 print("Hacking FBI 80%");  
7 print("Hacking FBI 100%");
```

Behind the scenes



Benefits
of
hacking

Getting called a hacker



+

Types of Hackers

HACKERS

Types of Hackers:

- Black Hat Hackers: These hackers mainly involve in bad and illegal practices. It can be stealing money from bank to data leak of big organizations[Fig 1]
- White Hat Hackers: These hackers work legally to protect the client's businesses from cyber-attacks.[Fig 3]
- Grey Hat Hackers: These hackers are neither bad nor good. They work what they think right thing to do.[Fig 2]
- And some others...



Fig. 1

Fig. 2

Fig. 3





White Hat Hacker



Black Hat Hacker



Script Kiddie



Red Hat Hacker



Gray Hat Hacker



Hacktivist



Few most
recent data
breaches of
2023



| Material Information (2377 MSI) | | | | | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|--------------|----------------------|----------|
| SEQ_NO | 1 | Date of announcement | 2023/04/07 | Time of announcement | 12:03:41 |
| Subject | Announcement regarding some information service systems affected by cyberattack | | | | |
| Date of events | 2023/04/07 | To which item it meets | paragraph 26 | | |
| Statement | 1.Date of occurrence of the event:2023/04/07 2.Cause of occurrence:Some information service systems affected by cyberattack. 3.Handling procedure:After detecting some information systems being attacked by hackers,MSI's IT department has initiated information security defense mechanism and recovery procedures. The Company also has been reported the anomaly to the relevant government authorities. 4.Anticipated possible loss or impact:No significant impact our business in terms of financial and operational currently. 5.Amount of insurance claims that might be obtained:N/A 6.Improvement status and future countermeasures:The Company is also enhancing the information security control measures of its network and infrastructure to ensure data security. 7.Any other matters that need to be specified:None. | | | | |

Data breach on April 6,2023



Data breach on April 10,2023

Data breach on April 3, 2023




HiFishCH @HiFishCH · Apr 3

Does anyone know more about this breach?

[bleepingcomputer.com/news/security/...](https://bleepingcomputer.com/news/security/)

The shutdown of any CloudServices @westerndigital is severe: My dad can't access any of the data stored on his WD MyCloud Home.



Western Digital

bleepingcomputer.com

Western Digital discloses network breach, My Cloud service down

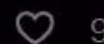
Western Digital announced today that its network has been breached and an unauthorized party gained access to multiple company ...



7



2



9



3,663



Why we need security ??

- ▶ we need it -- personal data, sensitive info from being leaked
- ▶ company need it --- security to protect our data
- ▶ they failed to secure the data --- they have to heavy fines to regulatory bodies ,
- ▶ eg instagram ...all of you have your data on instagram, suddenly u came to know that the data is not at all secure
- ▶ personal posts are being leaked .
- ▶ instagram ---> they will public interest --->business impact
- ▶ --> they have to heavy fines
- ▶ ---> they to implement security protocols --- hardware for the security -- expense

CIA Triad in Cyber Security

- ▶ The CIA Triad is an information security model, which is widely popular. It guides an organization's efforts towards ensuring data security. The three principles—confidentiality, integrity, and availability which is also the full for CIA in cybersecurity, form the cornerstone of a security infrastructure. In fact, it is ideal to apply these principles to any security program.
- ▶ **Confidentiality** makes sure that only authorized personnel are given access or permission to modify data
- ▶ **Integrity** helps maintain the trustworthiness of data by having it in the correct state and immune to any improper modifications
- ▶ **Availability** means that the authorized users should be able to access data whenever required

Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation



Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation (often abbreviated as "CIA" or "CIAAN") are the five core security properties that are used to ensure the security and reliability of information systems. Together, they form the foundation of information security and are the key elements that must be protected in order to ensure the safe and secure handling of sensitive information.

1. **Confidentiality** is important to protect sensitive information from being disclosed to unauthorized parties. This includes protecting data at rest, in transit, and in use. Common techniques used to maintain confidentiality include encryption, access controls, and data masking.
2. **Integrity** is important to ensure that information has not been tampered with or modified in an unauthorized way. This includes protecting data from unauthorized modification, deletion or addition. Common techniques used to maintain integrity include digital signatures, message authentication codes, and data hashing.
3. **Availability** is important to ensure that information and systems are accessible to authorized users when they need them. This includes protecting against denial of service attacks and ensuring that systems are highly available and can withstand failures. Common techniques used to maintain availability include load balancing, redundancy, and disaster recovery planning.

4 Authenticity is important to ensure that information and communication come from a trusted source. This includes protecting against impersonation, spoofing and other types of identity fraud. Common techniques used to establish authenticity include authentication, digital certificates, and biometric identification.

5 Non-repudiation is important to ensure that a party cannot deny having sent or received a message or transaction. This includes protecting against message tampering and replay attacks. Common techniques used to establish non-repudiation include digital signatures, message authentication codes and timestamps.

3 aaa cyber security



Authentication

Who is allowed to access ?

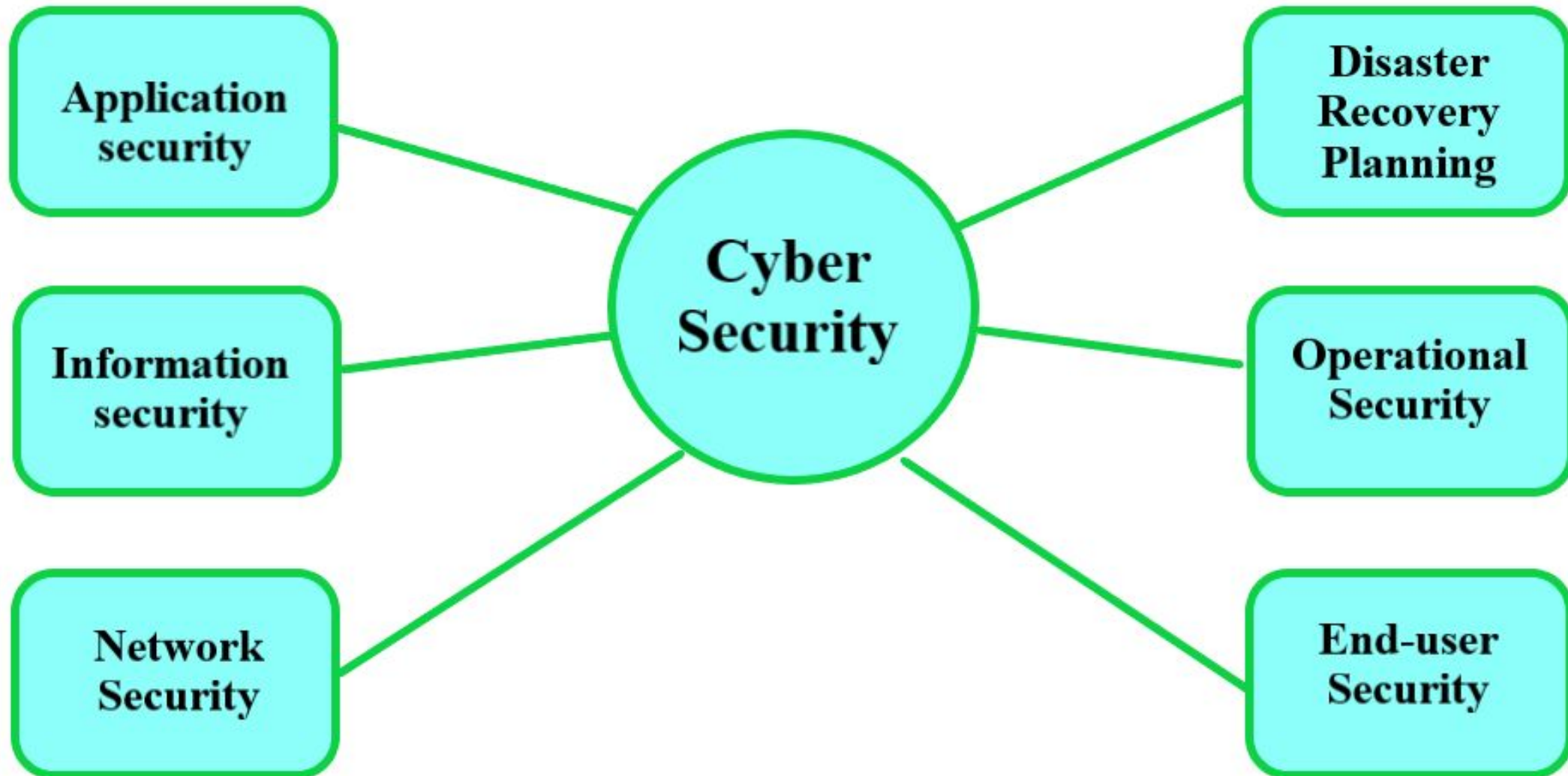
Authorization

What resources allowed to access ?

Accounting

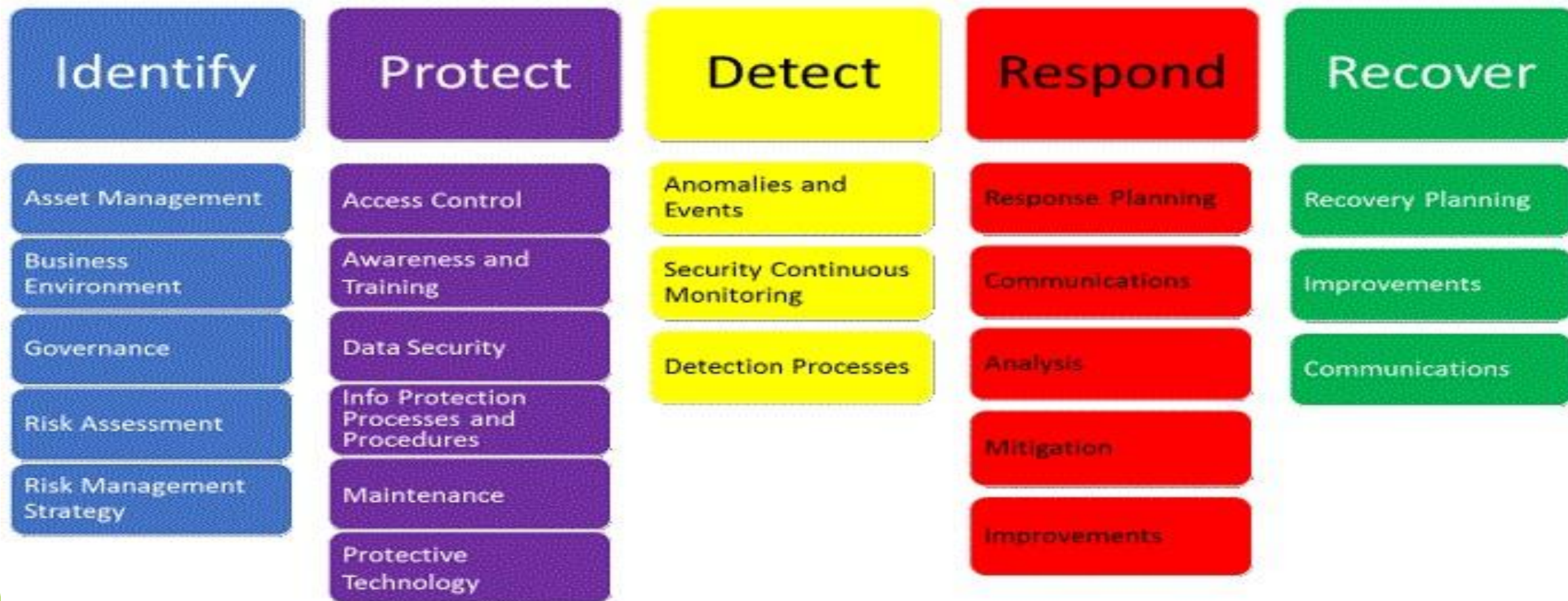
What is being accessed?

Elements of Cyber security



National Institute of Standards and Technology

NIST Cyber Security Framework



Common Terminologies :

- ▶ Hacking : unauthorized access to any device , gain insights access the personal or sensitive you dont have permission
- ▶ eg. in college / uni ---> you are doing some work on your laptop
you got a call you went out for 5 mins...meanwhile a friend of you or anyone else access your laptop and gains some personal information

- ▶ Ethical Hacking : permitted to do that ...ethical hacking -- companys hires you as ethical hacker
- ▶ give you a permission to hack their systems, websites, networks ,database to find out the loopflaws
- ▶ proper documentation is there before this between the EH and the company ..
---> security testing
- ▶ hackers are not the bad guys --- crackers are the one

- ▶ Who are Hackers::::: a hacker is a person who use a device or particular stuff other then the purpose for which it is meant for.
- ▶ They are the ones who are challenging the limits of everything , using the stuff beyond their use.
- ▶ plagiarism checker tools : while you are doing any kind of research ...submit research work --> they will is it 100% authenticate
- ▶ it should be copied from any website on internet
- ▶ for this purpose they use a tool ---> plagiarism checker

► Types of hackers

=====

- BHH -- black hat hackers --- exceptionally talented individuals --> exploit the systems for financial gains ---> never report the bug -- just exploit
- WHH -- white hat hackers --- talented individuals -- use their knowledge to protect the data and fight against BHH-- > never exploit a bug --- direct report it
- GHH -- -combination of both BHH + WHH ==> GHH -- sometimes they are offensive (BHH) and sometimes defensive(WHH)
- Script Kiddies -- newbies in the cyber world-- they have the names of the tools used -- don't have the necessary skills
- State sponsored Hackers --- hired by Govt
- Hacktivists -- hackers activist --- fight for a cause ---> anonymous, shadow breakers etc

- ▶ 3 very important terminologies

=====

- ▶ Vulnerability : it means any kind of weakness , flaw, loophole in the system design, architecture which compromise the security of entire applications
- ▶ Exploit : practical process of vuln
 - like- A vulnerability is a gap in the armor or weakness that allows people to enter. The exploit is the mechanism that someone uses to get in. For example, a door with a fragile lock has a vulnerability. The exploit uses the keys, hammer, or lockpick to break the lock.
- ▶ Payload : the shell or the code used to exploit the websites is called payload (weapon used for hacking)
 - like- A payload is a piece of code that executes when hackers exploit a vulnerability. In other words, it's an exploit module. It's usually composed of a few commands that will run on the targeted operating system (e.g., key-loggers) to steal data and other malicious acts.

VULNERABILITY RISK THREAT



Threat:

Something
that can damage
or destroy an
asset



Vulnerability:

A weakness
or gap in
your
protection



Risk:

Where assets,
threats, and
vulnerabilities
intersect

- ▶ Phases of hacking :
- ▶ 1. Information Gathering gathering the infor which is public in nature which is present on internet
- ▶ 2. Scanning ---> gathering the infor which is private in nature --> ip of machines. mac of address-- services are running in machine, ports are open
- ▶ 70 % of the entire attack scenaios covered this -----> 70%
- ▶ 3. Gaining Access
- ▶ 4. Maintaining Access
- ▶ 5. Clearing the Tracks

- ▶ information gathering + scanning ==>> Recon

- ▶ Information Gathering :

- ▶ =====

- ▶ information gathering means getting the information which is public in nature
....

- ▶ access the info from internet ---> platforms like fb , insta , website

► Practical

- Data breach (check Gmail data breach)
- <https://haveibeenpwned.com/>
- - Kali installation-
- <https://www.kali.org/>
- <https://www.kali.org/get-kali/#kali-installer-images>
- The professional version is not free of VM and the workstation is free.
- <https://www.virtualbox.org/wiki/Downloads>

At the end conclusion is ---

**Its all fight for Asset : means
which has value**

-

so should Do anything