Ethical Hacking(Unit 5) VelTech Technical University Chennai

Presentation · April 2024

DOI: 10.13140/RG.2.2.35481.22885

1 author:

Arun Anoop Mandankandy
Vivekananda College of Engineering & Technology

Ethical Hacking(Unit 5)

Dr.Arun Anoop M CEH CHFI
Associate Professor
Dept. of CSE
SoC, Veltech University, Chennai.

UNIT – 5 Reporting and Cyber Law **L-9 Hours**

Skills required for an ethical hacker – Incident Handling - CVE and CVSS – Report Writing – Laws of Land – Ethics Vs Law – Indian IT Policy 2000 – Compliance and Risk Assessment - Case Studies (Ransomware Attacks/Stuxnet/DataBreach/Pegasus).

Skills Required to Become a Ethical Hacker

Skills allow you to achieve your desired goals within the available time and resources. As a hacker, you will need to develop skills that will help you get the job done. These skills include learning how to program, use the internet, good at solving problems, and taking advantage of existing security tools.

In this article, we will introduce you to the common programming languages and skills that you must know as a hacker.

- **Top Ethical Hacking Skills**
  - Excellent Computer Skills. ...
  - Programming Skills. ...
  - Database Skills. ...
  - SQL Skills. ...
  - Linux Skills. ...
  - Cryptography. ...
  - Social Engineering Skills. ...
  - Web Applications.

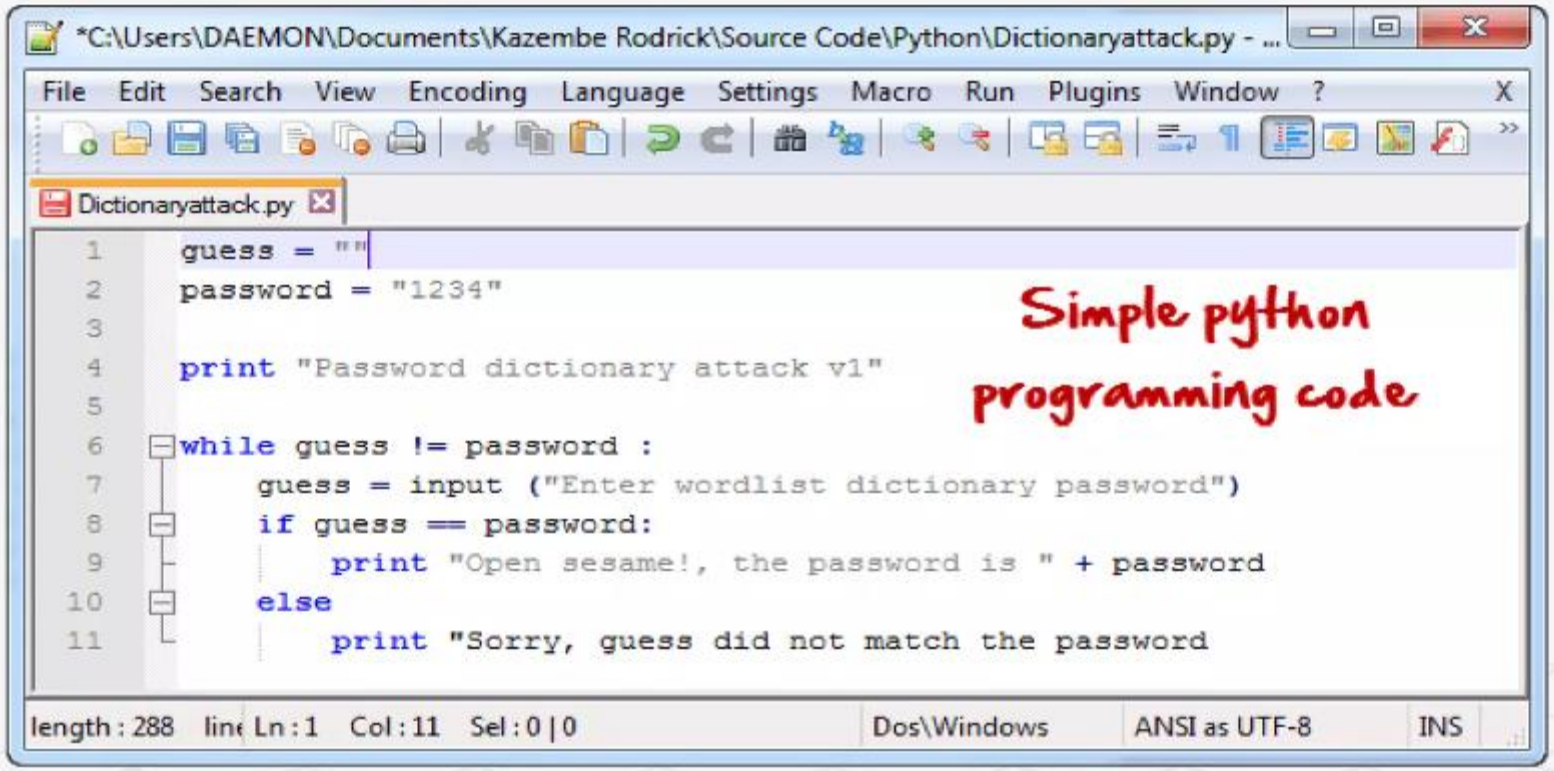
1. Excellent Computer Skills

Computer skills are abilities and knowledge which allow you to use computers and related technology.

But do you know which computer skills to list on a resume to get hired?

2. Programming Skills

A programming language is a language that is used to develop computer programs. The programs developed can range from operating systems; data based applications through to networking solutions.



Why should you learn how to program?

- Hackers are the problem solver and tool builders, learning how to program will help you implement solutions to problems. It also differentiates you from script kiddies.
- Writing programs as a hacker will help you to automate many tasks which would usually take lots of time to complete.
- Writing programs can also help you identify and exploit programming errors in applications that you will be targeting.
- You don't have to reinvent the wheel all the time, and there are a number of open source programs that are readily usable. You can **customize the already existing applications and add your methods to suit your needs**.

What languages should I learn?

COMPUTER LANGUAGES	DESCRIPTION	PURPOSE
HTML	Language used to write web pages.	Web hacking Login forms and other data entry methods on the web use HTML forms to get data. Being able to write and interpret HTML, makes it easy for you to identify and exploit weaknesses in the code.
JavaScript	Client side scripting language	Web Hacking JavaScript code is executed on the client browse. You can use it to read saved cookies and perform cross site scripting etc.
PHP	Server side scripting language	Web Hacking PHP is one of the most used web programming languages. It is used to process HTML forms and performs other custom tasks. You could write a custom application in PHP that modifies settings on a web server and makes the server vulnerable to attacks.
SQL	Language used to communicate with database	Web Hacking Using SQL injection, to by-pass web application login algorithms that are weak, delete data from the database, etc.
Python Ruby Bash Perl	High level programming languages	Building tools & scripts They come in handy when you need to develop automation tools and scripts. The knowledge gained can also be used in understand and customization the already available tools.
C & C++	Low Level Programming	Writing exploits, shell codes, etc. They come in handy when you need to write your own shell codes, exploits, root kits or understanding and expanding on existing ones.
Java,CSharp Visual Basic VBScript	Other languages	**Other uses** The usefulness of these languages depends on your scenario.

3. Database Skills

- Ethical hacking requires a number of different skills to be successful. One of the most important ethical hacker skills is the ability to work with databases.
- Hackers need to be able to understand how databases are structured and how they work in order to be able to find security vulnerabilities.
- In addition, hackers need to be able to use database management tools in order to manipulate data and access restricted information. Without these skills, it would be very difficult for ethical hackers to do their job.

4. SQL Skills

- Ethical hacking is an increasingly popular profession that calls for a very specific set of skills. Perhaps one of the essential ethical hacking skills required for an ethical hacker is the ability to write and understand SQL queries.
- SQL, or Structured Query Language, is a programming language specifically designed for working with databases.
- To find vulnerable information in a database, an ethical hacker needs to be able to craft SQL queries that can extract the desired data.

5. Linux Skills

- Anyone in information technology systems, such as administrators and network engineers, software developers or engineers, and some cybersecurity professionals, should learn Linux. It's an important skill to learn because Linux is the foundation of many servers and supercomputers.
- For ethical hackers, Linux skills are essential, as they allow you to access the inner workings of a system and identify potential vulnerabilities.
- In addition, Linux skills provide you with the ability to create custom scripts and programs that can be used to automate various tasks.

What is Social Engineering? Attacks,Techniques & Prevention

- Social engineering is the art of manipulating users of a computing system into revealing confidential information that can be used to gain unauthorized access to a computer system. The term can also include activities

  such as exploiting human kindness, greed, and curiosity to gain access to restricted access buildings or getting the users to installing backdoor software.

Social Engineering attacks

- **Phishing**: Phishing uses emails that appear to come from legitimate sources to trick people into providing their information or clicking on malicious links and put end users into one of the emotional states that causes them to act without thinking.
- **Vishing:** Attackers use phone calls to trick victims into handling over data. They may pose as bank managers or other trusted entities to supply your credentials and other important data.
- **Smishing**: Uses SMS text messaging to get you to divulge information or click on a malicious link.
- **Spear Phishing:** Similar to phishing but the attacker customizes the email specifically for an individual to make the phish seem more real. They often target key employees with access to critical and/or confidential data

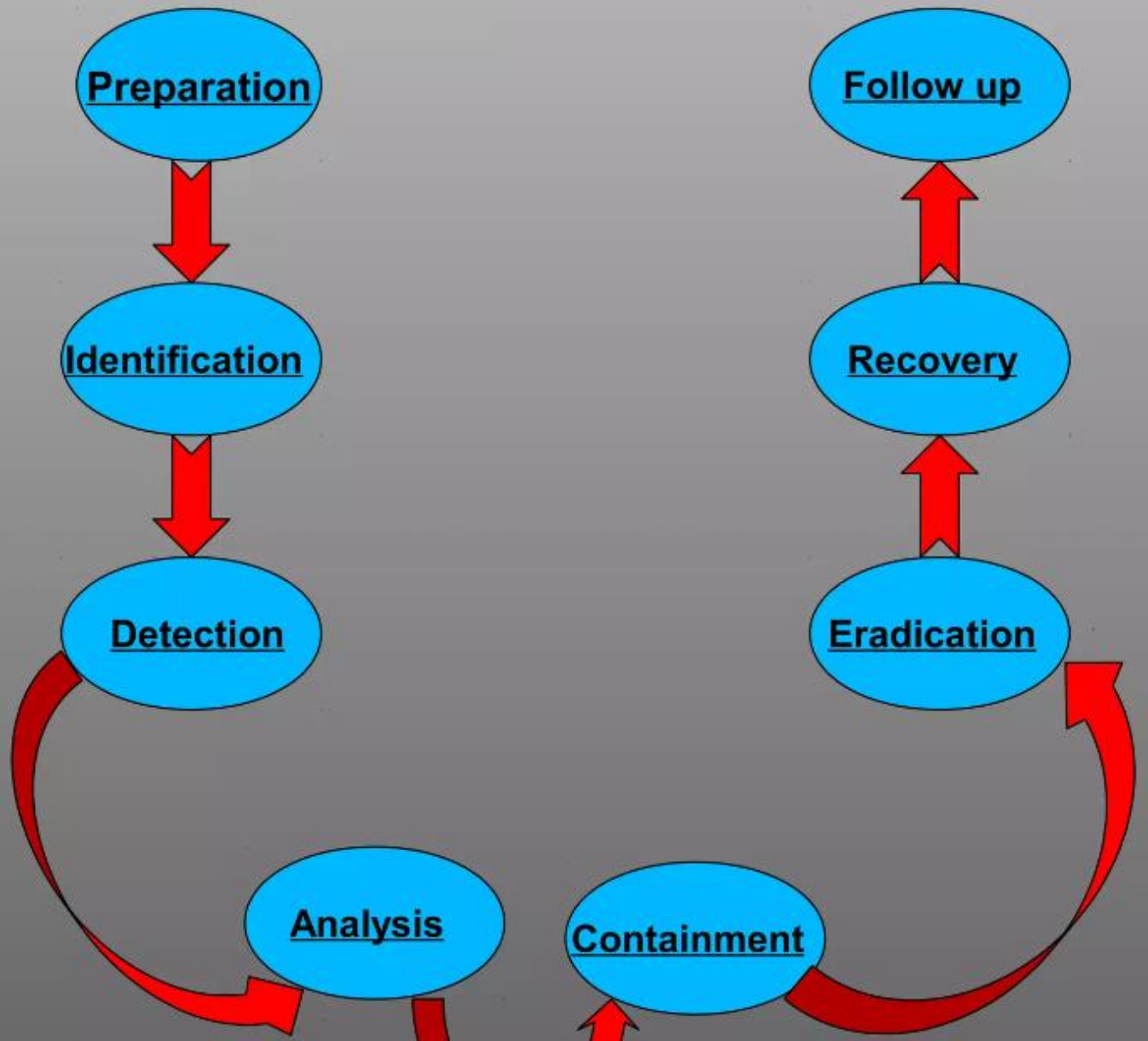
What is Incident Handling?

- Incident Handling is an **action plan for dealing with** intrusions, cyber-theft, denial of service (DoS), malicious code, fire, floods, and other security-related events.

- Having **procedures** and **policies** in place so you know what to do when an incident occurs.

Incidents Handling(IH) Life-Cycle

Important



(1)Preparation

**Preparation is one of the most important step in the Incident Handling(IH) lifecycle, because If a system is not initially prepared for an attack, it is extremely vulnerable and if attacked, the potential destruction will be greater.

**In order to help prevent an intrusion, it is necessary that a company plans and prepares for any possible intrusion, This includes:-

-creating a **security plan** and **policy**.

-developing an **emergency communication plan**.

-**selecting** and **training** incident handling team members.

-providing **easy reporting facilities**.

-**routinely practicing** and **improving** upon the incident response plan.

Preparation Key Points

- Take Notes,Logs,etc….
  - Hand Written Notes are a great Help.
  - Use Time Stamps in the Notes.
- Management Support
  - Regular Reports (Preferred Monthly).
  - Graphically illustrated Reports.
- Build An Incident Handling Team
  - Identify qualified People.
  - Multi- disciplinary Team is the best
    - Network
    - Security
    - Operations
    - Systems
    - HR

(2)Identification

- Usually **the first step** to identification is **Noticing something unusual on a system**.

- Identification involves **perpetual monitoring**, which will help determine whether **an event has really occurred,** and **the nature of this event.**

- **Examining the system logs regularly** will help a system administrator be more aware of an intrusion or some unusual activity,**The system logs can show** denied access messages, messages referring to old vulnerabilities, and blocked accesses to specific services.

- An **intrusion detection system (IDS)** is a tool that can help in the **identification** and **detection** of activities of an attack, The **IDS's purpose** is to detect an attack by a hacker by monitoring incoming traffic while the attack is actually occurring.

- **the IDS** will sound an **alarm** and **alert** the system administrator, If there is **an obvious violation**.

- By using **a Host-based intrusion detection tool**, you can **prevent** a worm from infecting your system by blocking it from entering the system.

- **Finally** **it should be kept in mind that** only secure communication channels should be **used to** prevent the intruder from overhearing the communication.

(3)Detection

- **The Goal** is to gather events ,analyze them, and determine if it is ***an Incident***.
- **Signs of an Incident:-**
  - IDS tool has an alert.
  - Unexplained entries in a log file.
  - Failed events, such as logon.
  - Unexplained events (new accounts).
  - System reboots.
  - Poor performance.

(4)Analysis

- Would be easy if all precursors were indications **But they are not**, User-provided indications are often incorrect, Even **if indication is accurate**, Doesn't necessarily mean anything is going on.

- Indicator may be an **issue**, just not a security issue.
- **Example:** Web server that is down due to non-malicious cause.

- ***Remember***, **skilled attackers** cover their tracks, It is likely that there may be no precursors or indications until after the incident has occurred, **Unskilled attackers** are being able to be as quiet as skilled attackers with the tools being released.

(5)Containment

- **The Goal** is to stop the bleeding and Stop the attacker to get any deeper.
- **In order to contain the incident**, there are a few steps that should be followed to make sure the problem does not expand,

First, an on-site team should survey the incident and secure the area, if possible, while making sure to keep the system in the exact state that it was found.

second, Securing the area includes isolating the compromised system and keeping all non-essential persons away from the system.

Another important step, is to back up the system using new media and stored in a safe place to prevent tampering.

It is also important to keep all the log files containing information regarding the intrusion to use as a reference in an investigation.

The final step in containment is determining whether the organization should continue operating in the compromised situation.

(6)Eradication

- **Eradication** is the removal of any changes or unwanted data put on the system, Such as deleting malicious code or disabling breached user accounts.

- Once an incident has occurred, it is important to make sure it is not repeated. **In order to do this**, the problem needs to be eradicated.

- **To eradicate the problem,** the cause needs to be identified in order to improve the system's defenses.

- **Vulnerability analysis** should take place to search for any additional vulnerability on the system and prevent any future incidents of the same nature.

(7)Recovery

- **The goal** of recovery is to put the impacted system back to production in safe manner.
- **The first reaction**, once the recovery stage has been reached, will be to **restore the System**.
- **the system will require** analysis to determine how the system can be improved so that the same kind of attack does not reoccur.
- **The system may need** to have its antivirus software updated, or the IDS updated with new policies.

(8)Follow up

- **When the incident is under control**, it is important to look back and reflect on how the incident occurred, and how effective the ensuing handling of the situation was.

- **During the follow-up stage**,

- strategy meetings should be held.
- analytical reports should be written.
- IT security-related policies should be updated.

- **Important points to consider are**

- whether to change the placement of firewalls.
- move the compromised system to a more secure location.
- change the IP address of the compromised system, or update the routers and firewalls.

Incident Types

- Hardware/software failures.
- Cyber-theft, Intellectual property theft.
- Viruses, worms or other malicious software.
- Unauthorized use.
- Intrusions, Internal or external attack.
- Denial of Service.
- Strikes, Employees unavailable.
- Power outages, Storms.
- Hazard material spills.
- Bombings, Explosions.
- Earthquakes, Fires, Floods.

Incident Categories

- ***Denial of Service:***
  - Prevents or impairs authorized use by exhausting resources.
- ***Malicious Code:***
  - Virus, worm, Trojan horse, etc…….
- ***Unauthorized Access:***
  - Logical or physical access without permission.
- ***Inappropriate Usage:***
  - Violates acceptable use policies.
- ***Multiple Component:***
  - One incident encompassing one or more incidents.

*Multiple Category Incidents:

- Should be categorized by transmission mechanism.
- ***Example:***
  - Virus creates backdoor.
  - Handle as malicious code, since the virus was the transmission mechanism.

- **CVSS** – The Common Vulnerability Scoring System (CVSS) is a system widely used in vulnerability management programs. CVSS indicates the severity of an information security vulnerability, and is an integral component of many vulnerability scanning tools.
- **CVE –** Common Vulnerabilities and Exposures (CVE) is a list of publicly disclosed vulnerabilities and exposures that is maintained by MITRE.

HACKTHEBOX

7 steps to master the incident reporting process

1. **Initial incident detection**
   Detect and acknowledge the incident.
2. **Preliminary analysis**
   Determine the scope and potential ramifications.
3. **Incident logging**
   Precisely log every action and observation related to the incident.
4. **Notification of relevant parties**
   Bring security incidents to the attention of stakeholders and wider teams.
5. **Detailed investigation & reporting**
   Conduct a comprehensive technical analysis to understand tactics and techniques used, coupled with a compilation of all findings.
6. **Final report creation**
   Provide regulators, insurers, and executive leadership with a detailed account of the incident, why it happened, and how it was fixed.
7. **Feedback loop**
   Revisit and analyze the incident to identify areas for improvement.

LAND LAW

Introduction

The Unit is designed to introduce the fundamental principles of land law. It builds upon the study of concepts related to land since pre-colonial to the current system.

Definition of terms

Land law is the form of **law** that deals with the rights to use, alienate, or exclude others from **land**. In many jurisdictions, these kinds of property are referred to as real estate or real property, as distinct from personal property.

Ethics vs. Law

Law	Ethics
Formal, written document	Unwritten principles
Interpreted by courts	Interpreted by each individual
Established by legislatures	Presented by philosophers, religious, professional groups
Applicable to everyone	Personal choice
Priority decided by court	Priority determined by individual
Court makes final decision	No external decision maker
Enforceable by police and courts	Limited enforcement

The [Indian] Information Technology Act, 2000

Information Technology Act 2000

- Section 43 [a]

  Penalty for unauthorised access to a computer system

- Section 43 [b] -

  Penalty for unauthorised downloading or copying of data without permission

- Section 72 -

  Offence of accessing any electronic record, book, register, correspondence, information, document or other material and, without the consent of the person concerned, disclosing such information to another person

CVE system is a widely used catalog of known vulnerabilities, where each entry is assigned ~~a~~ a ~~assigned a~~ unique identifier & corresponding CVSS score to denote its severity.

Case Studies.
- Stuxnet
- Ransomeware
- Data Breach
- Pegasus.

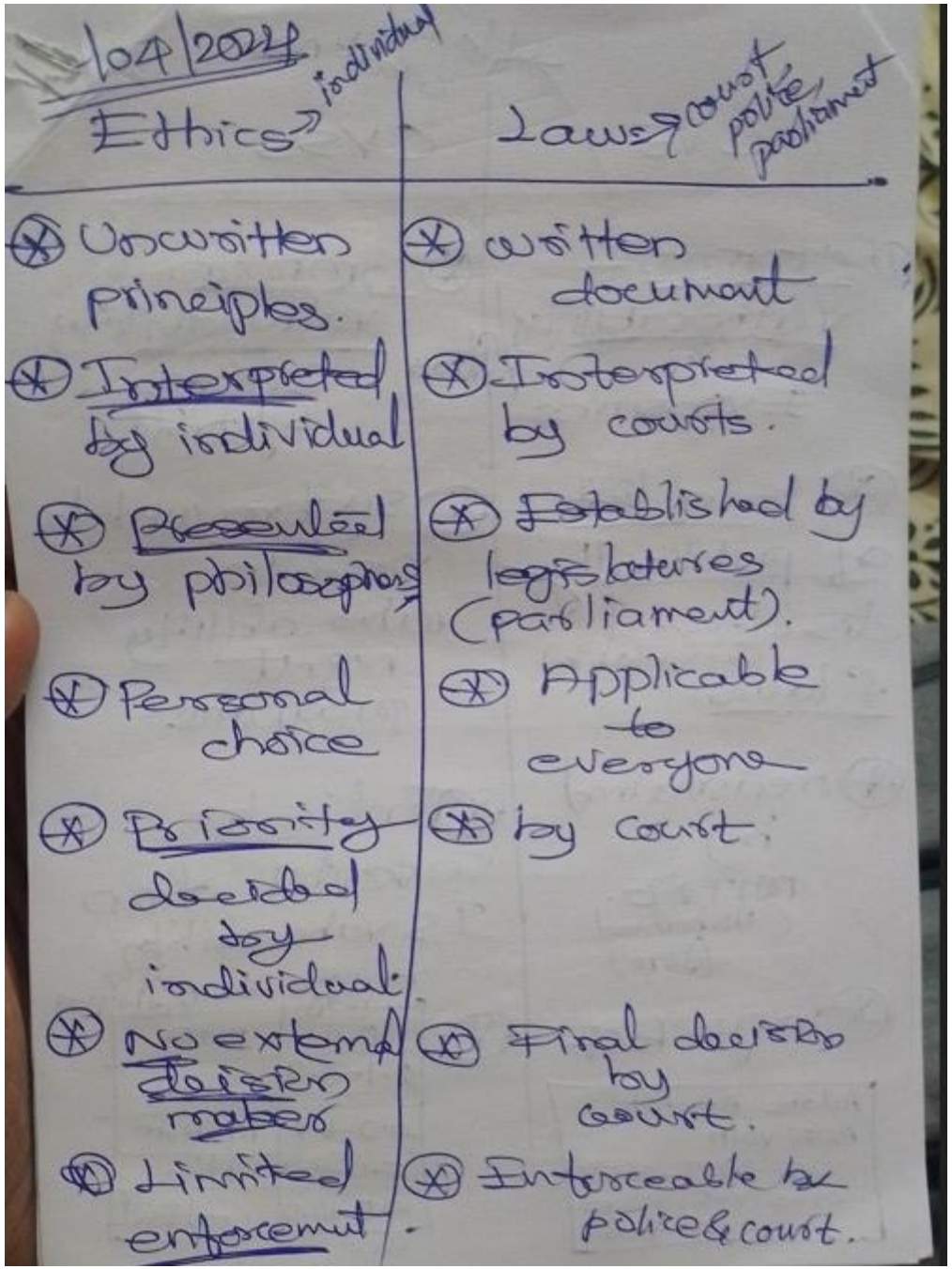
CVE	CVSS
Common vulnerability & Exposures.	Common vulnerability scoring system.
is a list of publically disclosed (available) flaws.	system widely used in vulnerability mgmt programs.
maintained by MITRE (sponsored firm)	indicate severity of an IS vulnerability
eg:- BOF	

Adobe Acrobat BOF vuln
CVE-2009-0658
CVSS V3 Base score is 7.8

Base score range	Severity category
0.0	None
0.1-3.9	Low
4.0-6.9	Medium
7.0-8.9	High
9.0-10.0	Critical

Important

Important



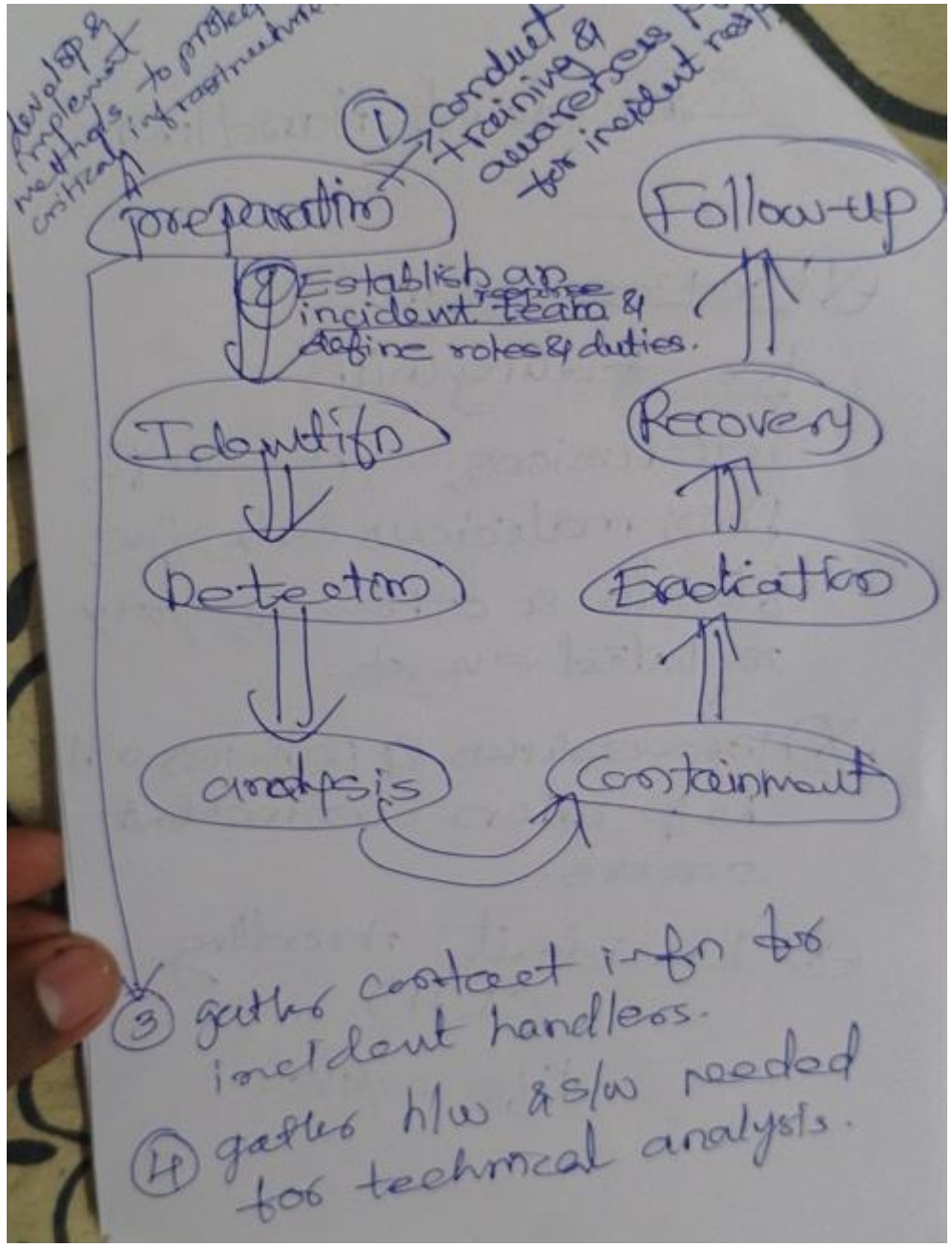
Ethics → individual	Laws → court, police, parliament
Unwritten principles.	written document
Interpreted by individual	Interpreted by courts.
Presented by philosophers	Established by legislatures (parliament).
Personal choice	Applicable to everyone
Priority decided by individual	by court.
No external decision maker	Final decision by court.
Limited enforcement.	Enforceable by police & court.

Incident Handling

- action plan for dealing with intrusions, cyber-theft, DoS, malicious code, fire, floods & other security related events.
- procedures & policies will help when an incident occurs.
- Incident Handling (IH) life cycle.

Incident Types.

- h/w or s/w failures
- intellectual property theft.
- viruses/worms/malicious s/w
- unauthorised use.
- intrusions internal, external attack
- DoS
- earthquakes, fires, floods.



Eradication

① Eliminate component of the incident such as detecting malicious code & disabling breached (hacked) user a/cs, if applicable.

To restore affected s/ms in minimal time.

Recovery

via appropriate tech actions such as

① Restore s/ms (restoring from clean backups; rebuilding systems from scratch; replacing compromised files with clean versions installing patches, changing passwords, and tightening n/w perimeter security.

To keep regarded on sys assets & many other sues

Detection & Analysis

① Monitor infn sys protection mechanisms & sys logs.

② Investigate reports of suspected breaches.

③ Notify authorities.

Containment

① choose & implement strategy for preventing further loss based on level of risk.

② Gather & preserve technical evidence if applicable.

Identifn.

* Detect & identify security incidents through monitoring, logging, IDs, & user reports.

* classify & categorize incidents based on severity.

Detection

* goal is to gather events, analyze them & determine if it is an incident.

IDS tool has an alert → sys reboots unexplained entries in log file. → poor performance

Follow up

Post incident activity: To take necessary st to avoid such incide

- Strategy meetings should be held.
- Analytical reports should be written.
- IT security related policies should be updated.
- Move the compromised s/m to more secure location.
- Change IP addres of compromised s/m.
- Update the IP of routers & firewalls.

Pegasus.

- is a spyware developed by Israeli cyberarms firm NSO group that can be covertly installed on mobile phones running most versions of iOS & android.

- malicious a sw that gathers info about person / firm & send it to attkr (3rd party) without our knowledge in way that harms the user.

Adware
Sim monitor
Web tracking
Trojans.

flaws

CVE-

2016-4655 → info leak in kernel.

2016-4656 → kernel memory corruption

4657 → memory corruption.

Pegasus exposes all msgs, calls, emails, audio, videos, ...

Staxnet

- Most sophisticated malware ever seen in public.
- It's code is ~1.5MB (very large) big
- Has 3 rootkits (~~root~~ user mode, kernel mode & PLC rootkits)
- Spreads via USB flash memory & n/w shares.
- It updates itself by connecting HTTP.
- Infects SSDPA svcs.
- 1st malware that has a physical payload.

Colourful Thank You Slide Design

THANK YOU