Information and Cyber Security

BY DR. ASMA ADNANE

Outlines

- Part 1: Introduction to cyber security
  - Definition and origin, Cyber Crime and information security,
  - Types of Cyber Crime,
  - Classification of Cyber Criminals
- Part 2: Examples of Cyber crimes
  - Tools used in Cyber Crime, Challenges, Strategies,
  - The Legal Perspectives: Indian/Global Perspective,
  - Types of Attack, Social Engineering, Cyber stalking, Ransomware.

Part 1 – Introduction to cyber security

What is Cyber security ?

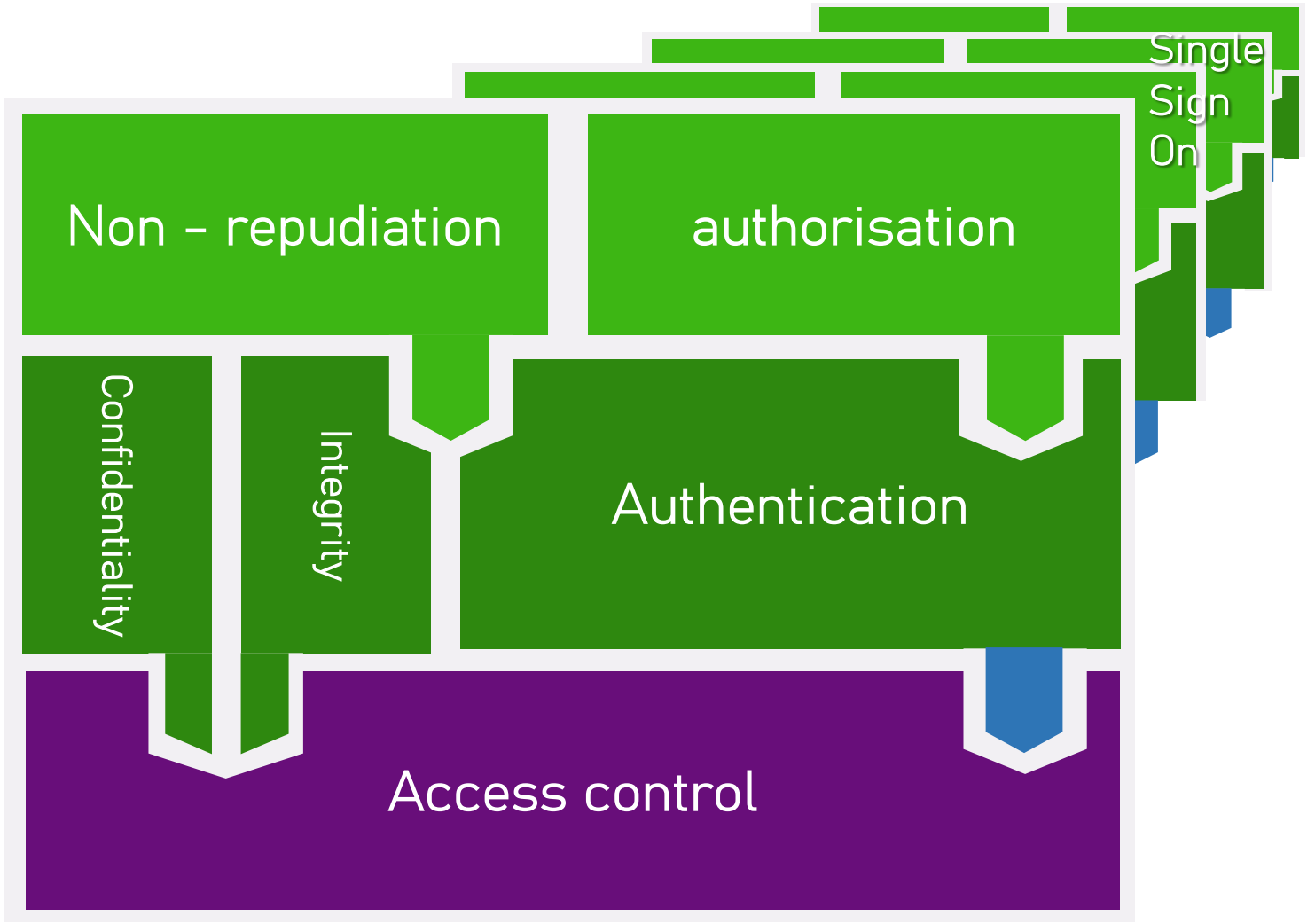
- Information security
- Information assurance
- Data security
- Computer security
- IT security
- Cyber security
  - ➢ **Multiple names, same concept**

Cyber security comprises **technologies and mechanisms that are designed to protect** systems, networks and data from cyber attacks.

Objectives of Cyber security

- Cyber security has several objectives, of course related to the types of data, threats as well as the types of resources, etc … Nevertheless, the main points are:
  - prevent **unauthorized disclosure** of data
  - prevent **unauthorized modification** of data
  - prevent the **unauthorized use** of network or computing resources generally

Security services

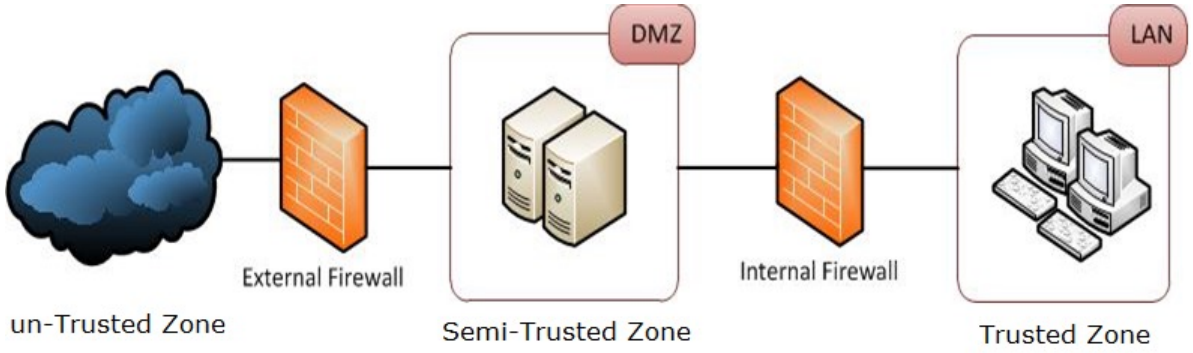


Access control (1/2)

- **Physical/real world filters**

  Security procedure, badges, server rooms with locks

- **Virtual world filters** to identify authorised flow (who ? And what ?)



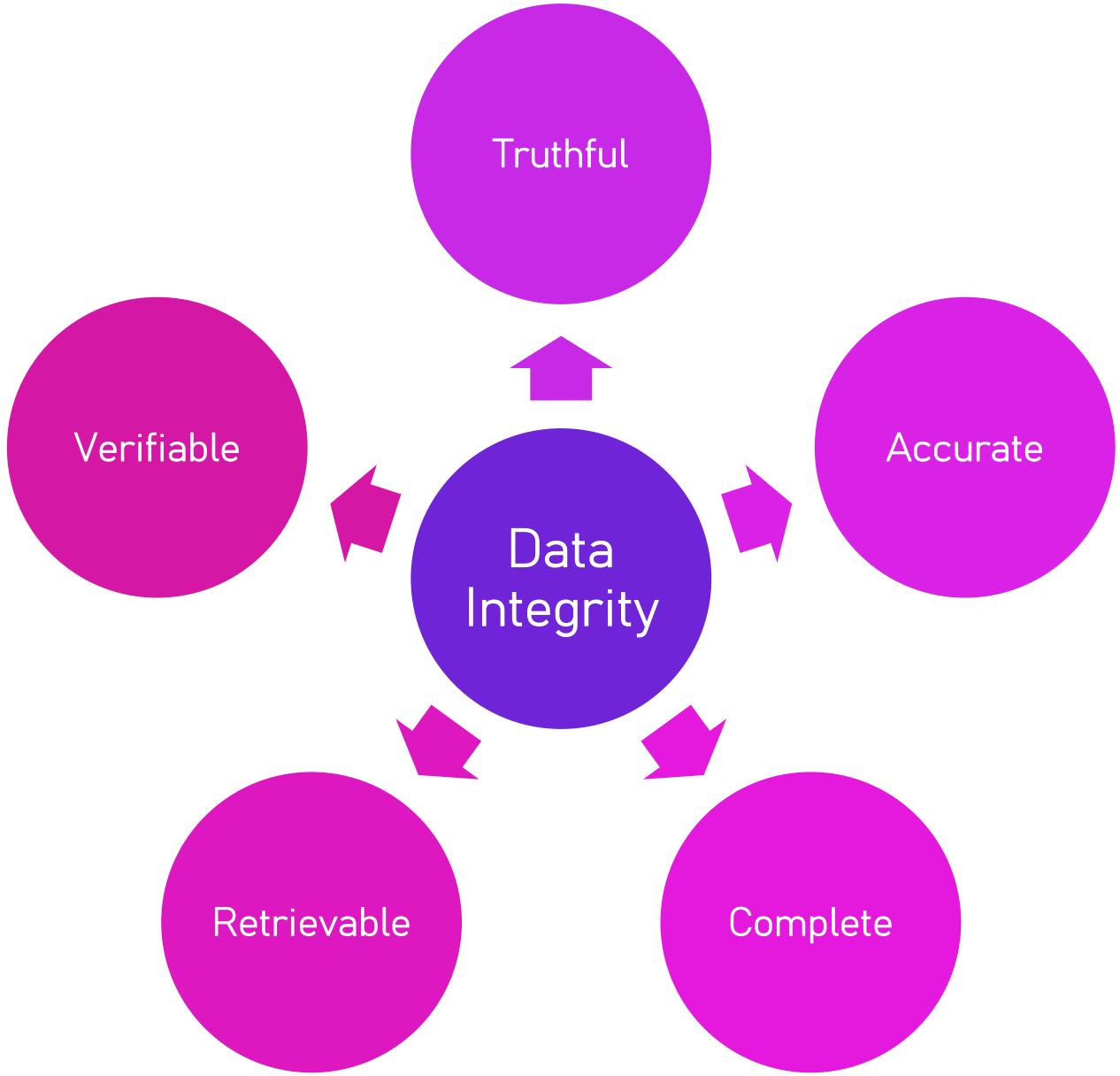
Authentication

- Identify the users
- Ensures that only authorised use
  have access to the
  information/system/service

Integrity

The protection of system information or processes from intentional or accidental modification

➢Digital signature



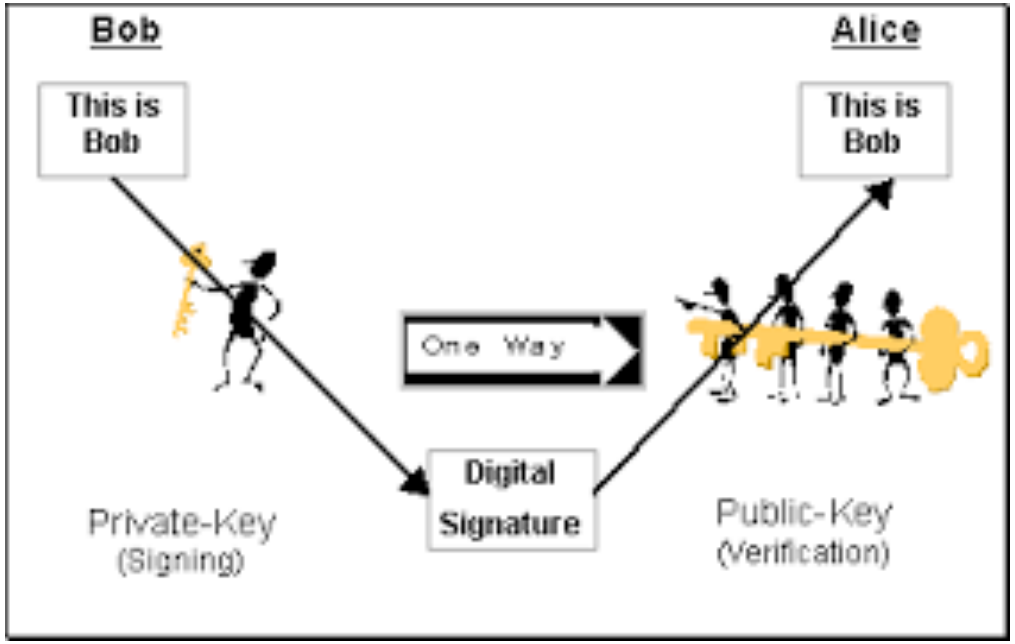
Confidentiality

- Prevent the disclosure of sensitive information from unauthorized people, resources, and processes
- Cryptography

Non-repudiation

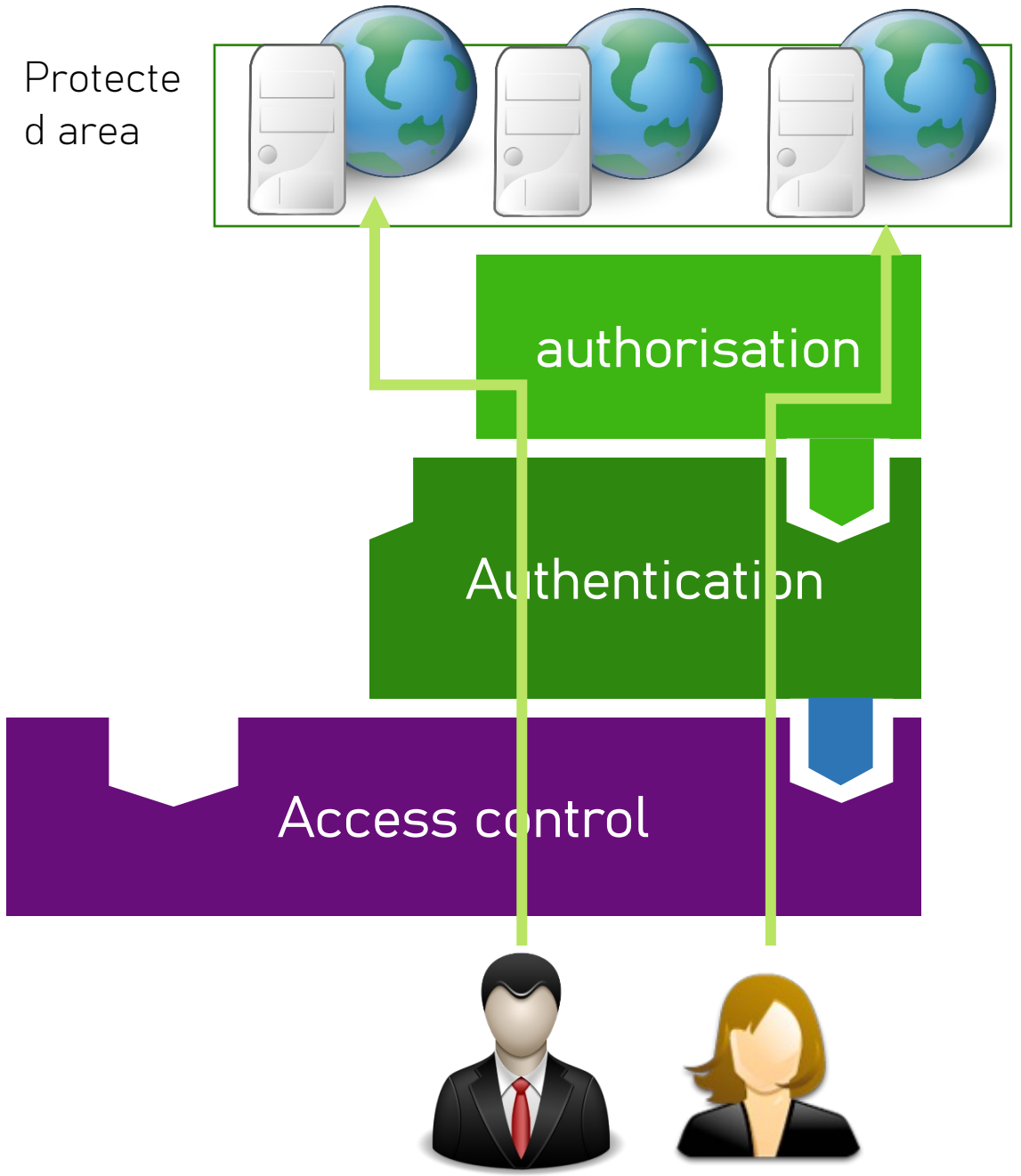
- Concerns the undisputed ownership of information; the originator should be able to prove ownership and not deny ownership for the sake of convenience.

➢ Digital signature



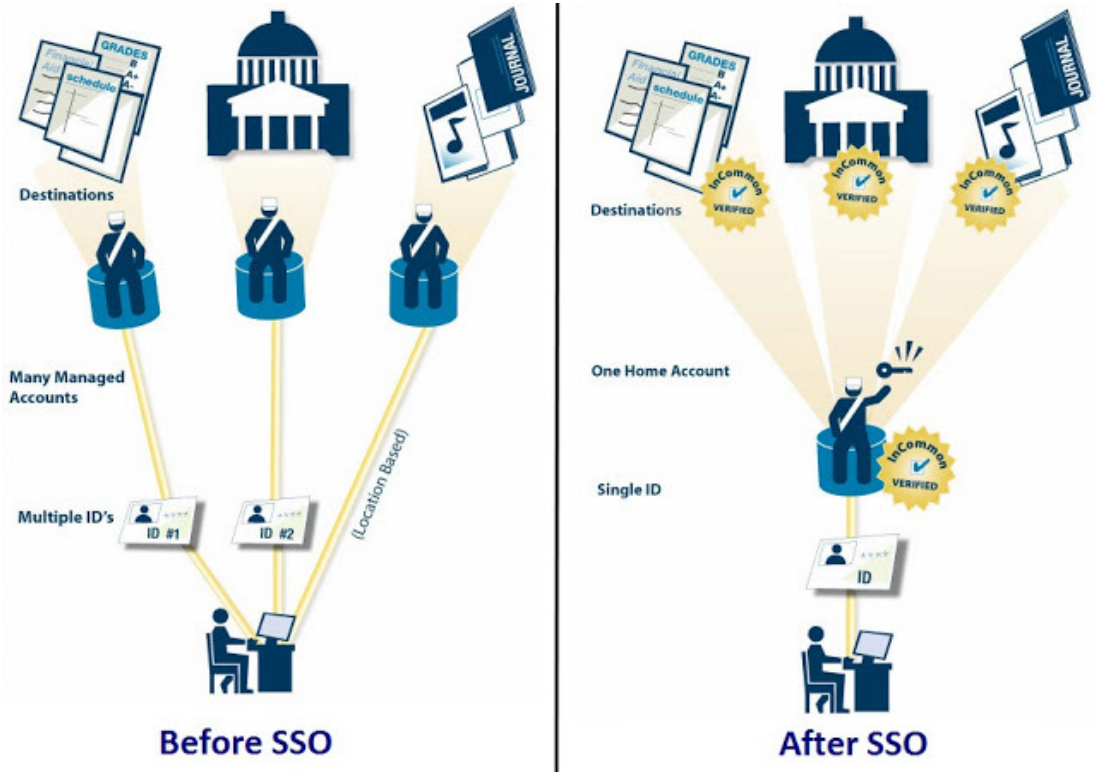
Authorisation

- Manage user's privileges and access rights
- Offers personalised access to resources
- E.g. OS Windows users

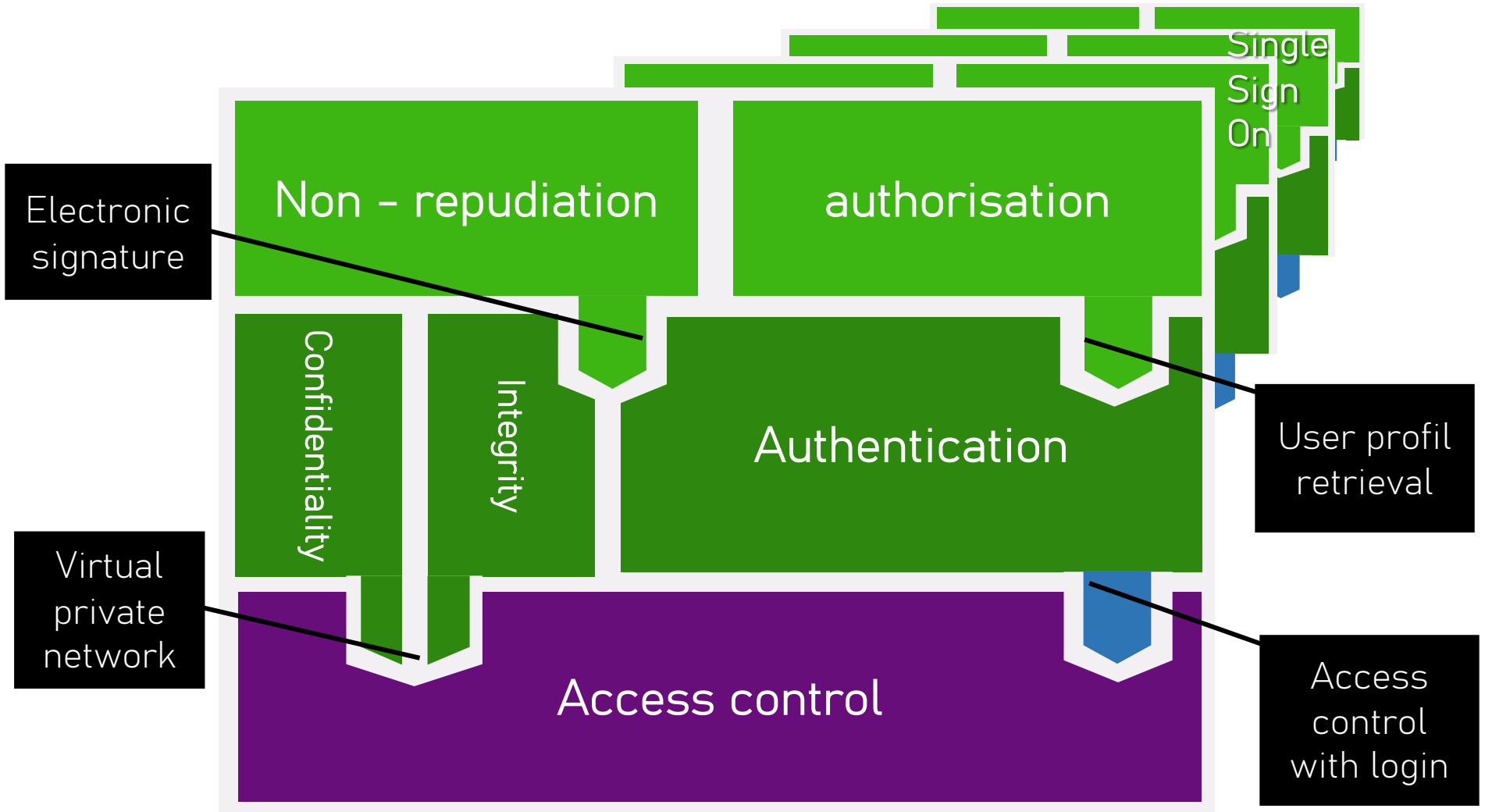


Signle Sign On

- One login, for multiple access
- Ensures transparent authentication in all systems where user has authorised access



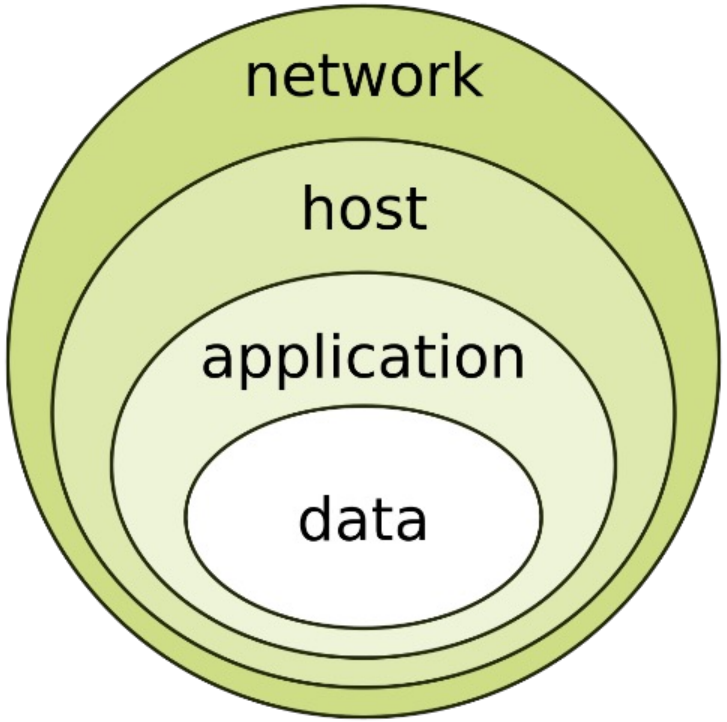
Security services



Two Models of Information Security

- CIA – Overall security of information
  - Confidentiality
  - Integrity
  - Availability

- CAIN – Important for transport
  - Confidentially
  - Authenticity
  - Integrity
  - Non-repudiation



Terminology

Asset

Vulnerability

Threat

Risk

Cyber Attack

Hacker / cyber attacker

Asset

- **Anything** that has value to the organisation and which therefore requires protection, e.g.:
  - network devices (routers, switches, firewalls)
  - resources manipulated by users (desktops/laptops/servers, information)
  - network performance-related details such as bandwidth and throughput
  - information related to network operation (topology, configurations, user addresses)
  - servers and databases that provide services
  - information in transit
  - People/staff

Vulnerability

- Vulnerability is a weakness of an asset or group of assets that might be exploited or triggered by a threat, e.g.:
  - a software bug/error (in a router firmware, a browser)
  - a flaw in a protocol
  - default passwords for managing network devices
  - cables exposed
  - maintenance of access rights upon job termination
- In today's environment, several organizations track, organize and test these vulnerabilities
- The US government has a contract with an organization to track and publish network vulnerabilities
- The common vulnerability exposure (CVE) list also publishes ways to prevent the vulnerability from being attacked

Threat

- **Threat:** cause of harm
  - threats are exercised by threat agents,
  - e.g., a hacker, cyber criminal, insider,
    - malware (i.e., automated 'agents'), hacktivist…
  - threats can be intentional (e.g., virus, social engineering), accidental (e.g., loss of laptop), environmental (e.g., power cut)
- **Common threat agents**:
  - **Internal (Insiders)** who have authorised/privileged access to the network
  - **External (Outsiders)** who have no authorised access to the network
  - **Partner** who represents a class in-between with 'some' authorised/privileged access to the network

Security report 2022

2022 Data Breach investigations Report - Verizon

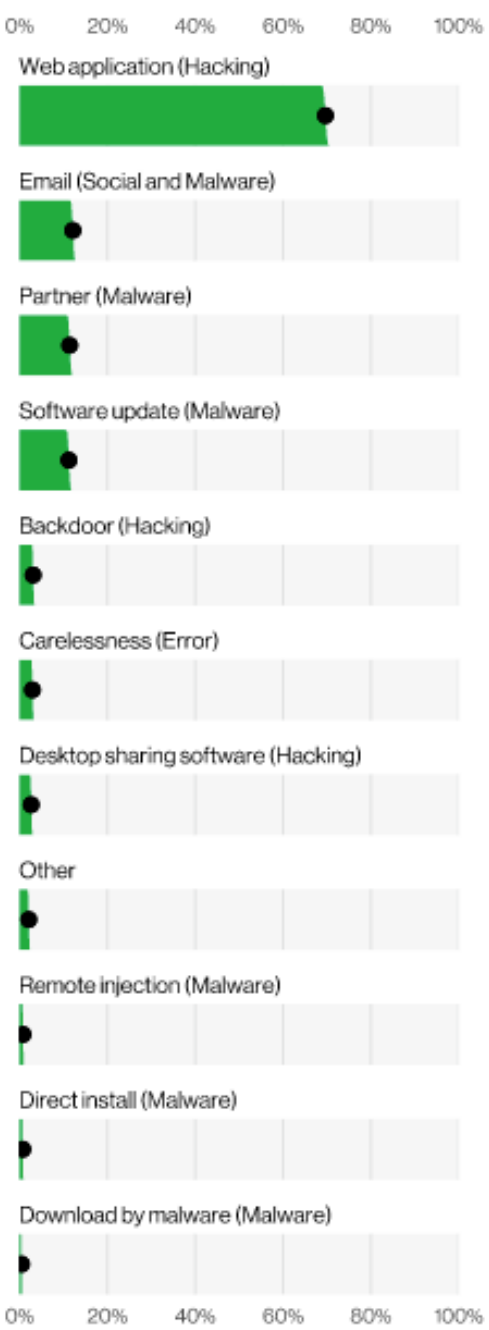


Figure 16. Top action vectors in incidents (n=18,419)

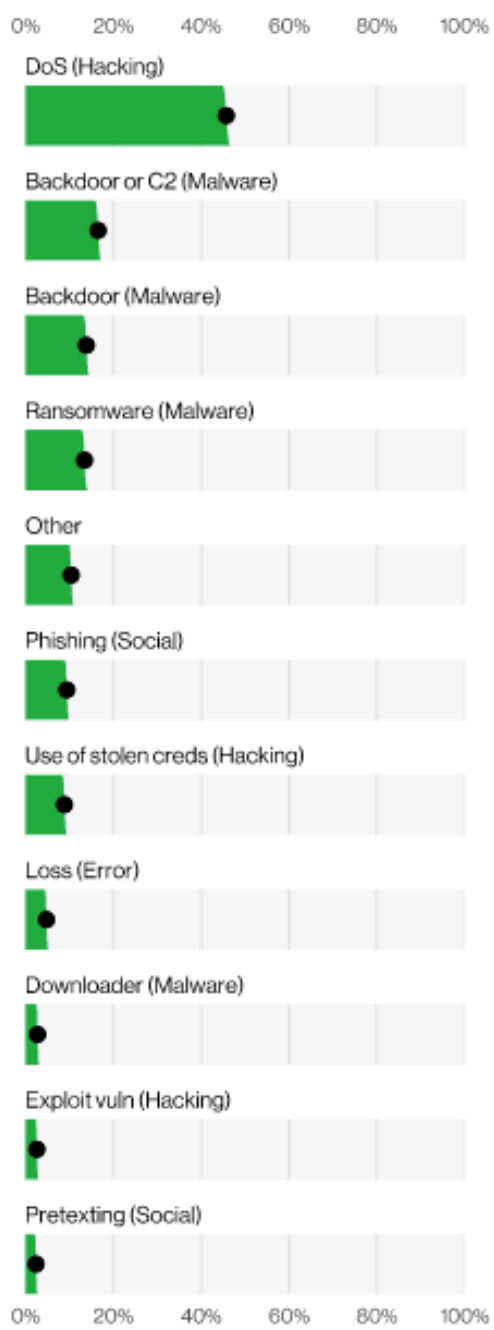
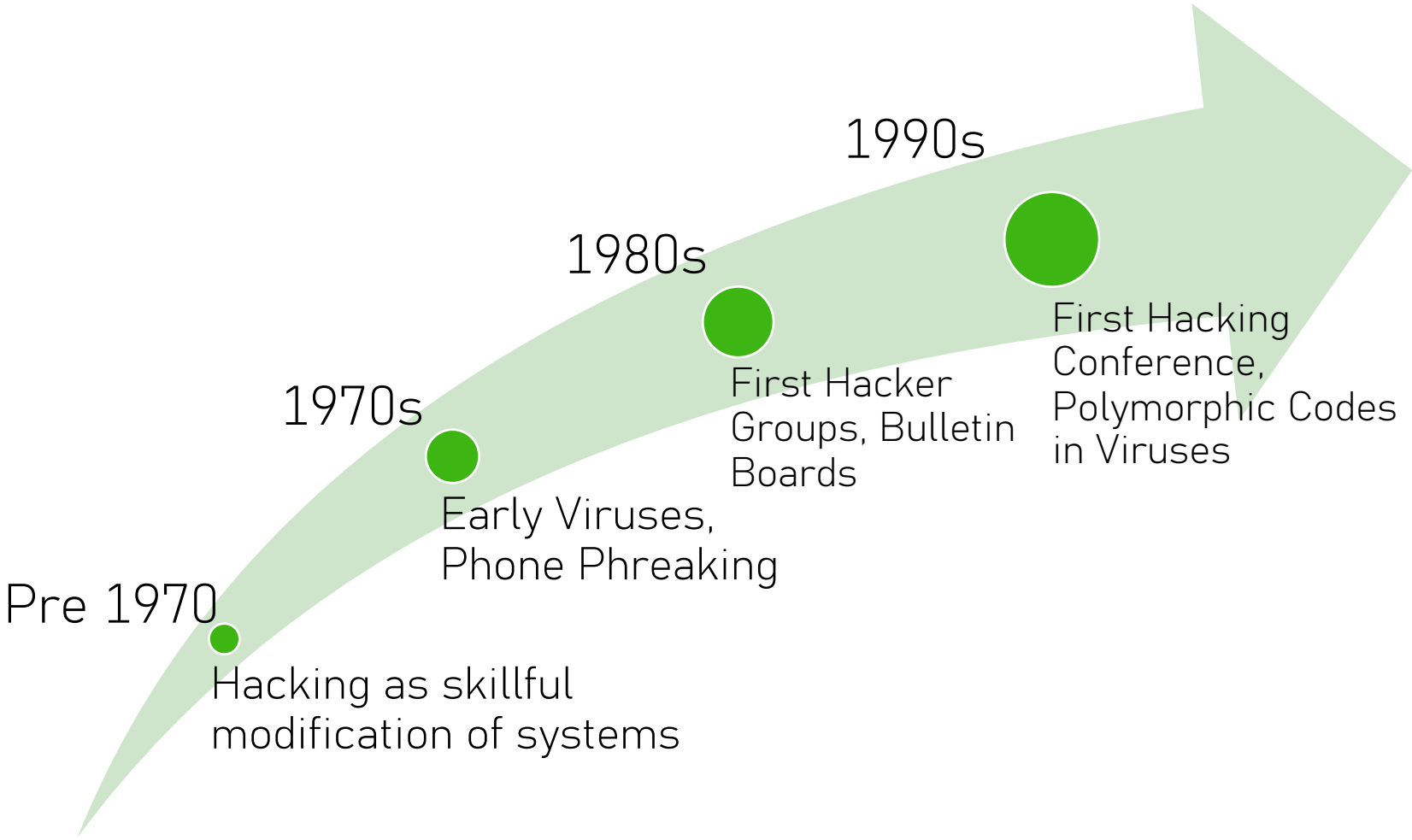


Figure 17. Top action varieties in incidents (n=18,511)

History of Hacking



Hackers

- White hat

  Ethical hackers, or penetration testers.

  Security experts who use their skill for ethical and legal purposes

- Black hat

  Hackers, people who violate computer security for personal gain

  When he finds a new "zero-day" security vulnerability , he will sell it to criminal organizations or use it to compromise computer systems.

- Grey hat

  In between black and white hat hackers

  E.g. they look for vulnerabilities in a system without the owner's permission. If issues are found, they will report them to the owner, sometimes requesting a small fee to fix the issue. If the owner does not respond or comply, then sometimes the hackers will post the newly found exploit online for the world to see.

Other categories

- **Script kiddies** are beginners and possess basic skills.
- **Suicide hackers** do not care if they get caught; goals include political, terrorist, or other aims.

What is cybercrime

- No consensus about a definition
- Broad definition (Casey, 2011):

Wide range of crimes that involve computers (i.e., internet-enabled devices) and networks (LANs and the internet itself)

What is cybercrime

- Cyber crime is an umbrella term used to describe two distinct, but closely related criminal activities (McGuire and Dowling, 2013)

Cyber-dependent crimes are offences that can only be committed by using a computer, computer networks, or other form of ICT. These acts include the spread of viruses and other malicious software, hacking, DDoS.
They are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud.

Cyber-enabled crimes are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT. E.g.:

- fraud (including mass-marketing frauds, 'phishing' e-mails and other scams; online banking and e-commerce frauds);
- theft (including theft of personal information and identification-related data); and
- sexual offending against children (including grooming, and the possession, creation and/or distribution of sexual imagery).

Hacker motivations

- Monetary
- Status
- Terrorism
- Revenge/ grudge
- Hacktivism
- Fun

Modern Hacking and Cybercriminals

- Transformation of hobbyist hacking to cybercrime
- Cybercriminals seeking profits by aiming at financial data, industry information, and other valuable targets
- Emergence of national laws to counter cyber attacks

Hacking in Indian law

- Cybercrimes are covered under Information Technology Act (IT Act) and the Indian Penal Code.
- The IT Act, 2000, deals with cybercrime and electronic commerce. The IT Act was later amended in the year 2008. The Act defines cyber crimes and punishments.
- Amendments to the Indian Penal Code, 1860, The Reserve Bank of India Act were also done under this IT Act. The purpose of this Act is to safeguard e-governance, e-banking, and e-commerce transactions.

Hacking in the Indian IT Act

Section	
Section 65	Tampering with Computer Source Documents. Penalties if found guilty can be **imprisonment up to 3 years and/or up-to Rs 2 lakh fine**.
Section 66	Hacking with computer systems or unauthorised usage of computer system and network. **Punishment if found guilty can be imprisonment up to three years and/or a fine of up to Rs 5 lakh**.
Section 66C	Identity theft using passwords, digital signatures, biometric thumb impressions or other identifying features of another person for fraudulent purposes.
Section 66D	Cheating by Personation Using Computer Resources. **Punishment if found guilty can be imprisonment up to three years and/or up to Rs 1 lakh fine**.
Section 66E	Taking pictures of private areas, publishing or transmitting them without a person's consent is punishable under this section. **Penalties if found guilty can be imprisonment up to three years and/or up to Rs 2 lakh fine.**
Section 66F	Acts of cyber terrorism. Guilty can be served a sentence of **imprisonment up to life**!
Section 67	Publishing Obscene Information in Electronic Form. In this case, the **imprisonment is up to five years and a fine up to Rs 10 lakh**.

Other sections

- Other sections
  - Section 379: Theft, crimes committed with stolen mobile/computer,
  - Section 430: Cheating and dishonestly inducing delivery of property, and bogus websites,
  - Section 463: Making false documents or false electronic records.
  - Section 468: Committing forgery for the intention of cheating attracts imprisonment of up to seven years and/or a fine. Email spoofing is an example of a crime punishable under this section.
- Even with cyber laws in place, the rate of cybercrime is increasing drastically. India reported a rise of 11.8% in cybercrime in the year 2020, during which around 50,000 cases were reported.
- The Police are grappling with solving cybercrimes due to challenges faced by them like underreporting, the jurisdiction of crime, public unawareness and increasing technology costs of investigating crime.

Hacking in the UK law

- Conducting hacking activity against a company or a person without their permission is viewed as an *offence under the Computer Misuse Act 1990* "unauthorised access to computer material".
- There are significant number of acts, directives and regulations to consider when it comes to malicious computer hacking, such as penetration testing

Computer Misuse Act 1990

Police and Justice Act 2006

Serious Crime Act 2015

EU Directive 2013/40/EU

Terrorism Act 2000

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

GDPR 2018

…..etc

Hacking in UK law – Offence and penalty

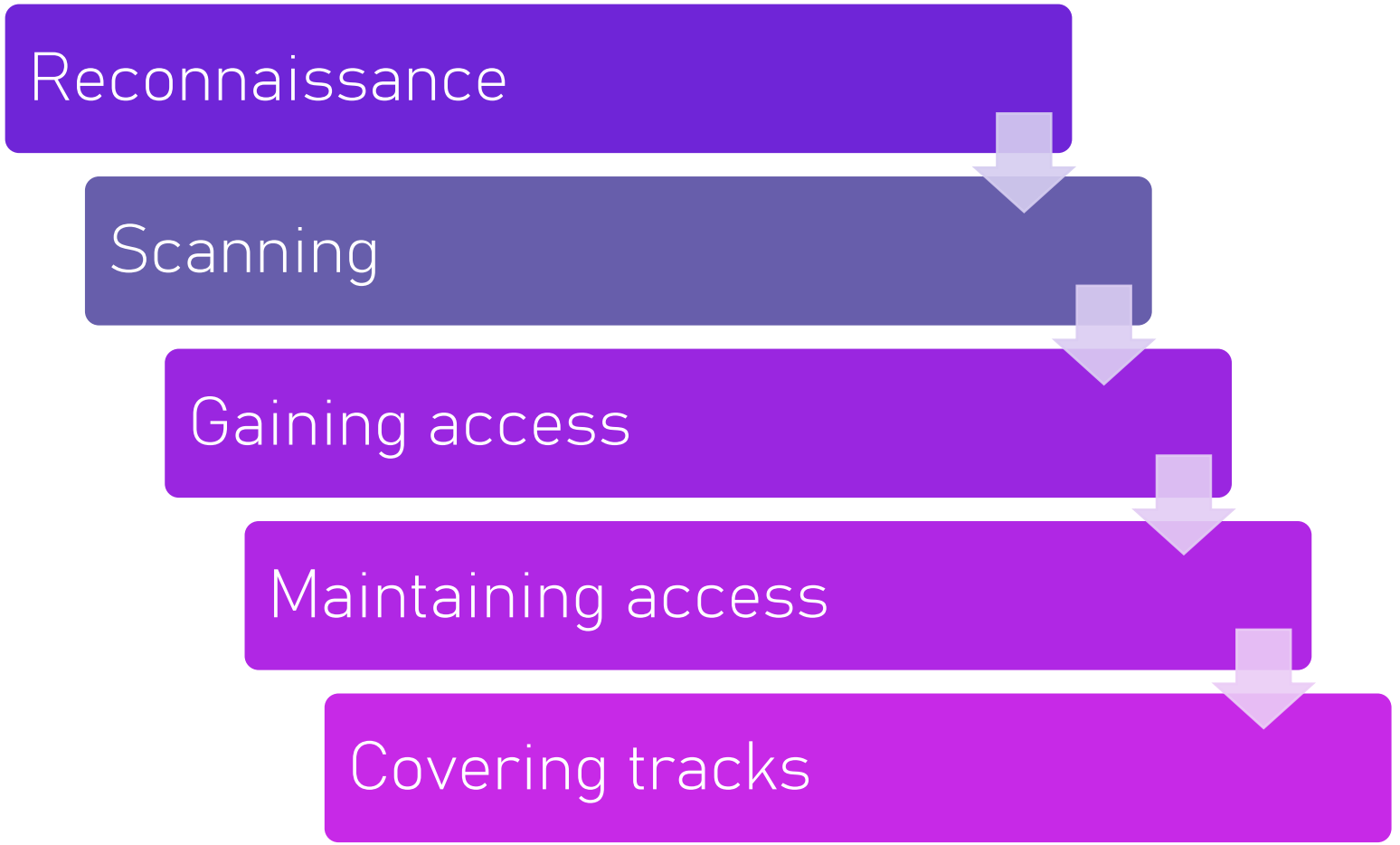
Offence	Penalty
Unauthorised access to computer material	Up to six months in prison and/or an up to a £5,000 fine
Unauthorised access to computer materials with intent to commit a further crime	Up to a five-year prison sentence and/or an unlimited fine
Unauthorised modification of data	Up to a five-year prison sentence and/or an unlimited fine
Making, supplying or obtaining anything which can be used in computer misuse offences	Up to a ten-year prison sentence and/or an unlimited fine

Ethical Hacking and Penetration Testing

- **Ethical hackers** require permission to engage in penetration testing
- **Penetration testing** is the structured and methodical means of investigating, uncovering, attacking, and reporting on a target system's strengths and vulnerabilities
- Penetration tests are commonly part of **IT audits**

Attack steps

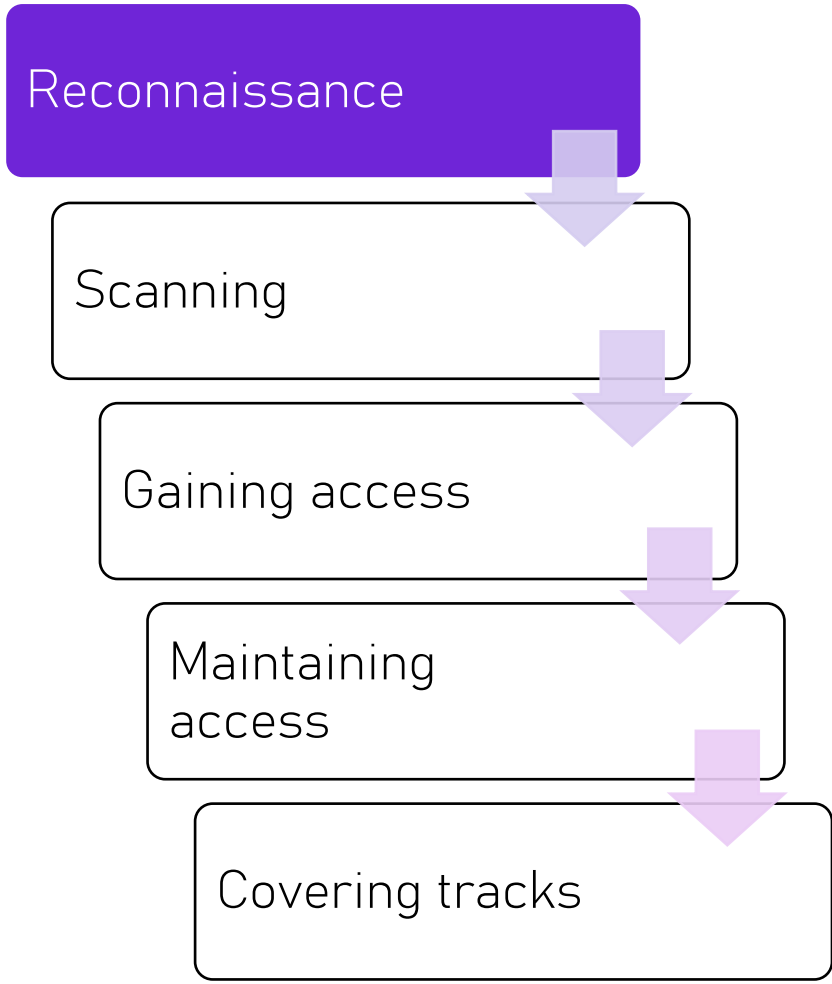
- Pen testing follows the attack steps.
- The objective is to make life hard for any would-be hackers at each step.



What is reconnaissance

- Reconnaissance is about information gathering
- The word *reconnaissance* is borrowed from its military use, where it refers to a mission into enemy territory to obtain information
- Goal: Obtain as much information as possible about the target (network) without raising the attention of defenders

  If you detect and (possibly) stop the reconnaissance, you may be able to avoid an attack



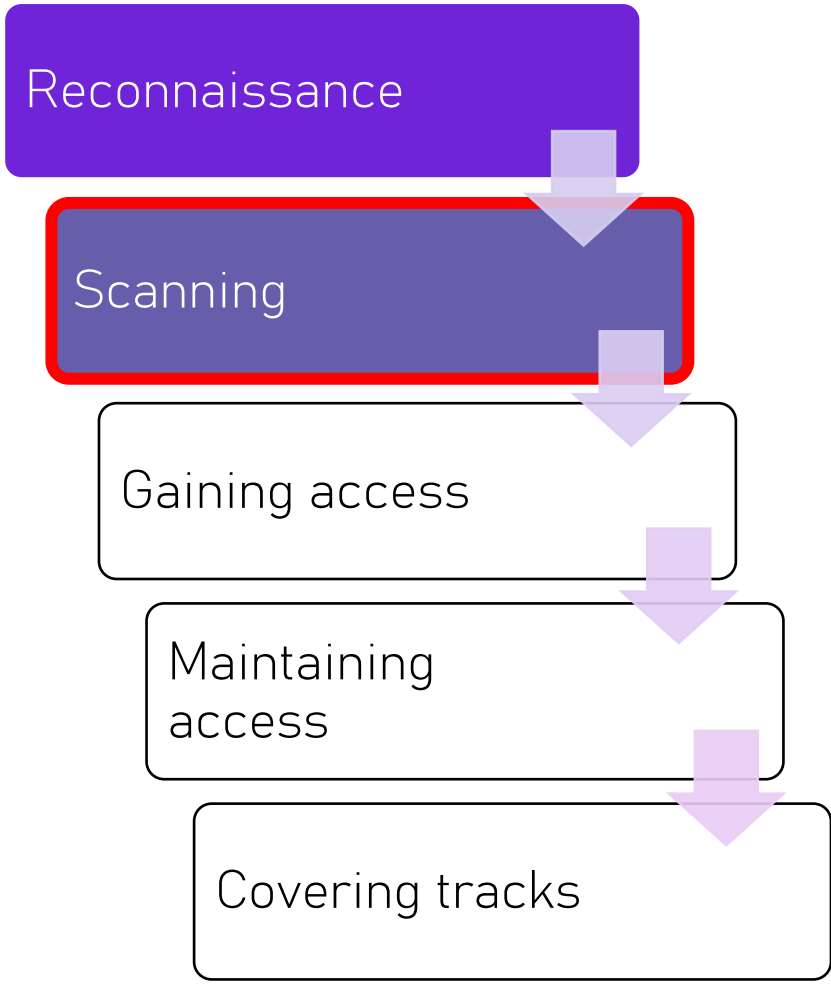
Scanning

- Scanning is about actively probing a system to find '*what is attackable*' → i.e., find entry points to a network / specific target

  In some ways there is a fuzzy line between active reconnaissance & scanning

- Goal: *Obtain a network map and find vulnerabilities*
- If you detect and block scanning activities, you stop the next phase – the actual attack

  If we cut off information at this point a hacker is likely to go elsewhere



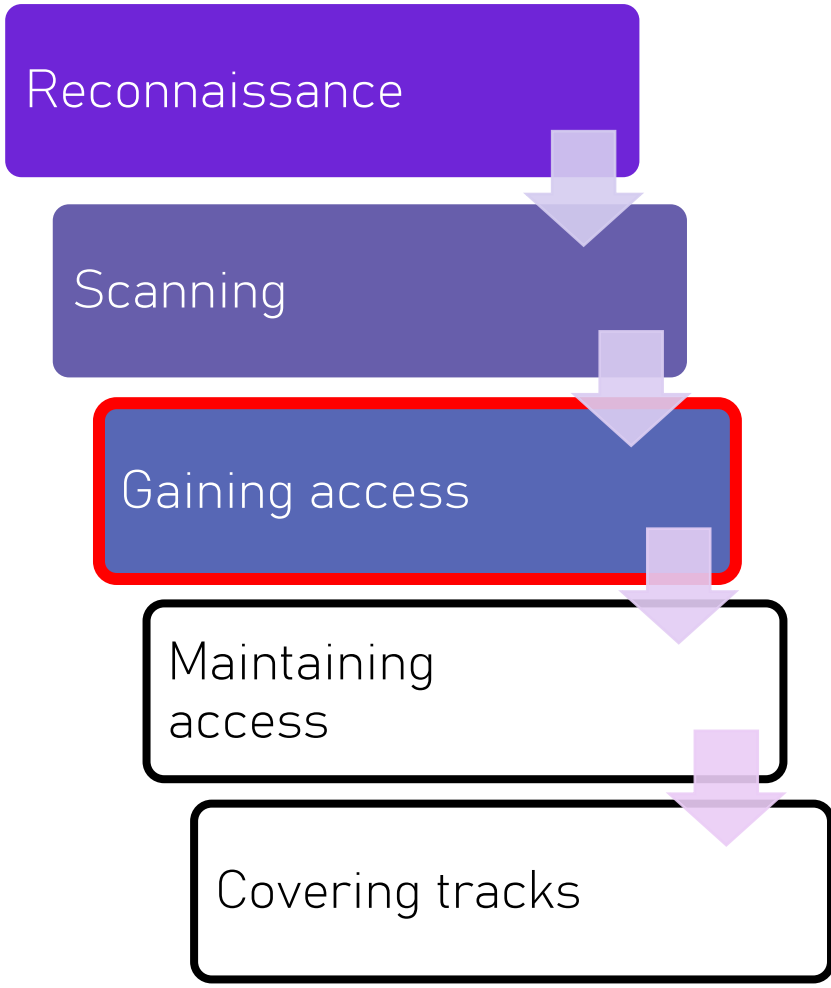
Gaining access

- Gaining access involves exploiting one or more vulnerabilities = The attack

  The previous phase aimed at finding out '*what is attackable*', i.e., entry points to a network / specific target

  This phase is about actually launching an attack

- Goal: *Reach a target for some sort of gain* (e.g., £££, affect reputation, revenge, espionage, raise attention)



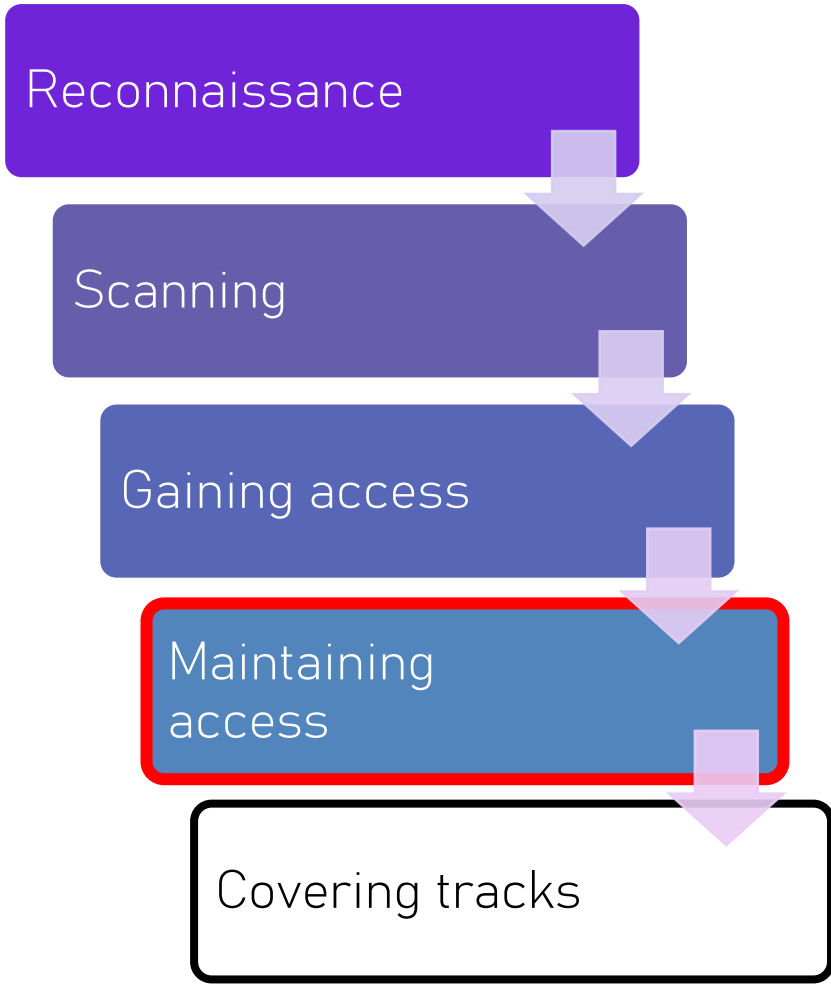
Maintaining access

- Maintaining access is about the ability of attackers to return to a target and/or to install & run malware to harvest something

  This phase involves the setup of a 'way' for attackers to connect to the target at any time (backdoor)

- Goal: Maintain long term access to systems and networks

  If you detect and close this open channel, there is a great chance that the attack will be discontinued



What covering tracks entails

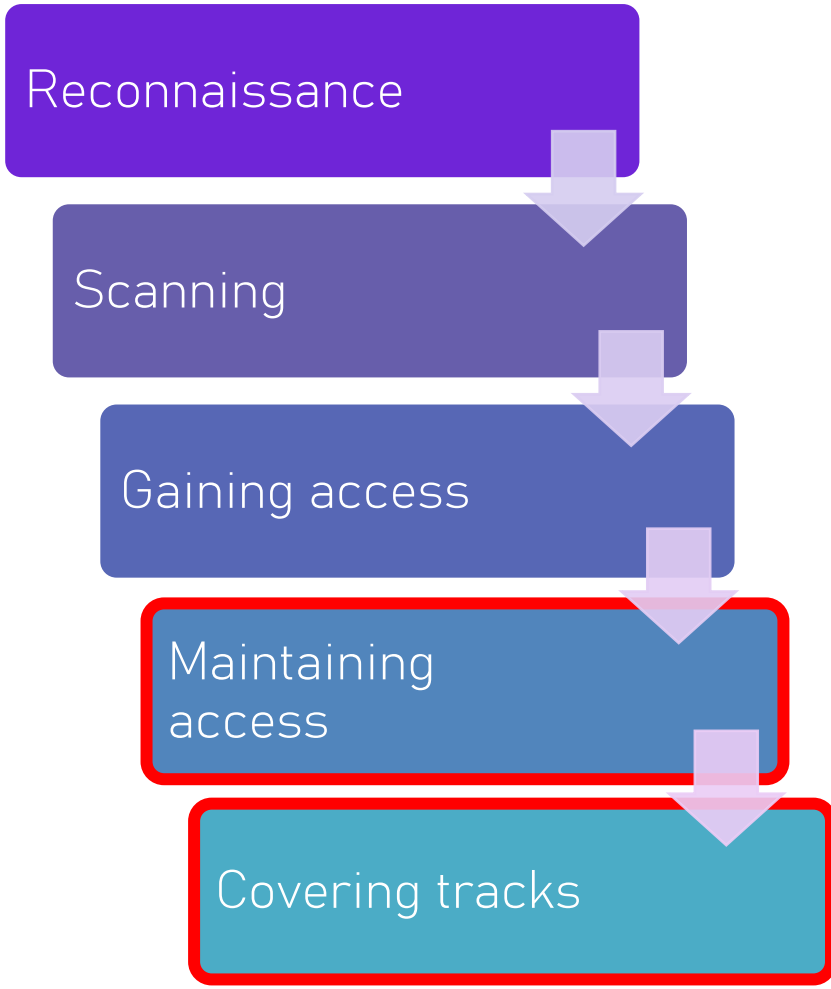
- Covering tracks is about erasing or disguising artefacts related to an attack

  It involves activities such as:

  - clearing logs
  - Hiding/disguising files, processes & activities

    E.g., in the Target data breach, attackers used malware 'svchosts.exe' which resembles Windows service host process 'svchost.exe'
  - embedding malware to the OS kernel or to the BIOS

- Goal: Avoid detection



Examples of security attacks

- Social ingineering
- Phishing
- Malware - Malicious software
- Denial or service (DOS or DDOS)
- Password cracking
- Ransomware
- Attacks that made the news

  Heartbleed

  WannaCry

Ransomware

What is a ransomware ?

- Is a malware.
- Prevents a user from using computing device.

  Freeze the computer or Encrypts files

  Demands payment from user as ransom for Decrypting file, hence the name ransomware

How the attack is done ?

- installs itself into your computing device i.e. Infection. (via, email, file sharing ..etc)
- Connects with its master server (Domain Server) through web
- Does encryption proce
- Pops up a pay page

Defence against ransomware

- No cure but prevention
- Patching
- Active and up-to-date antivirus
- Regular offline backups
- Use

Examples of ransomware

- India ranked 10 th globally in the number of ransomware attacks.
  - “About 42 per cent of total attacks in India are reported in Maharashtra. The top sectors that are being targeted in the country are software and services, capital goods, and the public sector,” the Ransomware Threat Report 2022.
  - The most active ransomware groups in India were Lockbit2.0, Avaddon and Conti.
- UHBVN Ransomware Attack

  Uttar Haryana Bijli Vitran Nigam was hit by a ransomware attack where the hackers gained access to the computer systems of the power company and stole the billing data of customers. The attackers demanded Rs.1 crore or $10 million in return for giving back the data.
- WannaCry

  India was the third worst-hit nation by WannaCry ransomware, affecting more than 2 lakh computer systems. During the first wave of attacks, this ransomware attack had hit banks in India including few enterprises in Tamil Nadu and Gujarat. The ransomware majorly affected the US healthcare system and a well-known French car manufacturing firm.
- Mirai Botnet Malware Attack

  This botnet malware took over the internet, targeting home routers and IoT devices. This malware affected 2.5 million IoT devices including a large number of computer systems in India. This self-propagating malware was capable of using exploitable unpatched vulnerabilities to access networks and systems.

Source: Times of India

Cyberstalking and Harassment

- Using electronic communications to harass or threaten another person
- Criteria for law enforcement officers:
  - Is it possible? Is the threat credible?
  - How frequent?
  - How serious?

Cyberterrorism

- The unlawful use of the Internet to perform terrorist activities
- Can include large-scale disruption of computer networks
- China Eagle Union
  - Group that consists of several thousand Chinese hackers whose stated goal is to infiltrate Western computer systems

Social ingineering

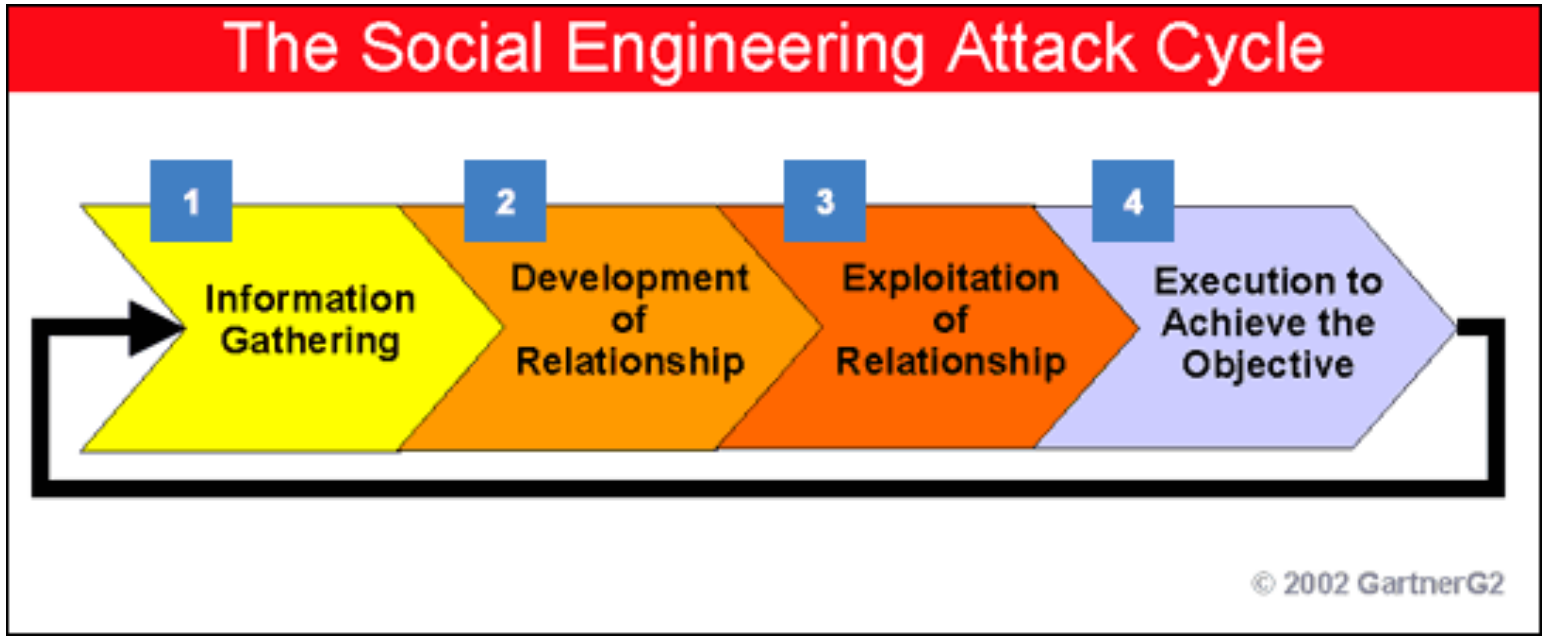
‘Hacking’ the Human instead of Systems

- Social engineering consists of techniques used to manipulate people into performing actions or divulging confidential information (Mitnick & Simon, 2002) …… to be used for illicit financial gains from identity theft.

Mitnick, K., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. New York: John Wiley & Sons.

Hacking of mind

Attack Lifecycle



- **Psychological** techniques such as persuasion that appeal to people's **emotions**
- Create feeling of **trust**
- Commitment
- Promise of a valuable prize
- **Impersonation** (Tech support staff, maintenance technicians, manager, police …etc)

Social Engineering Techniques

- Methods for Information gathering:

  Reconnaissance

  Public information

  Social networking sites

  Dumpster diving

  Cold calling

- Impersonation

  Impersonating who? Tech support staff, maintenance technicians, manager, police …etc

Common Social Media Scams

- “Secret” celeb gossip
- “Please send money”
- “Test your IQ”
- “Tweet for cash!”
- Fake login screens
- Fake Facebook groups
- False news articles
- Charity solicitations
- Sexual solicitation
- Amber alerts

Specific Attacks examples

Pretexting	Phishing	Spear Phishing	Vishing/Phone Phishing	Trojan Horse
Shoulder Surfing	Piggybacking / Tailgating	Dumpster Diving	Road Apples / Baiting	Quid pro quo – Something for something

Dumpster Diving

- The term used for *going through someone's trash*
- What do they want?

  Confidential Information, credit card data, Financial reports, Utility bills

  Banking information – blank credit applications

  A phone list, Calendars with schedules, Company policy, Interoffice memos

  Discarded computer manuals

Pretexting

- Using an *invented scenario over the phone* to gain access to information
- The pretext is the scenario – created with a little valid information to get more

  Insurance Number, mother's maiden name, place of birth
- Often used by private investigators to gain copies of personal records

Phishing

- Via emails, phone calls
- *appear legitimate*
- include a sense of urgency
- threat to your personal safety or security
- You are asked to verify personal data
- Banks and Credit Card Shopping sites are frequent targets

Examples

- **Recently, several scam emails linked to coronavirus have been seen.**
- Cyber-criminals are targeting individuals as well as industries, including aerospace, transport, manufacturing, hospitality, healthcare and insurance.
- Phishing emails written in English, French, Italian, Japanese, and Turkish languages have been found.
- The BBC has tracked five of the campaigns.
- https://www.bbc.co.uk/news/technology-51838468

Awareness Material

- Posters
- Email
- Screensavers
- Open Days
- Videos
- Company's Web pages / Facebook/ twitter
- Social gathering.
- Messages on (e.g., pens, key fobs, post-it notes, notepads, first aid kits, clean-up kits, clocks).

Preventing social engineering

- Via channel of attack (person vs. technology)
- Type of technology (phone, internet)
- User role (secretary, system administrator)

Thank you, questions ?

1

Outlines

- Part 1: Malware and other cyber attacks
  - Phishing, Password Cracking tools, Key-loggers and Spywares,
  - DoS and DDoS, Viruses,
  - Worms, Trapdoors, Salami attack, Man-in-the-middle attacks, Covert channels, SQL injection,
- Part 2: Security protocols
  - Cybersecurity Techniques,
  - Tools and Laws Introduction,
  - Proxy servers and Anonymizers,

2

Phishing

- An attempt to trick a victim into giving up personal information
  - Usually done by emailing the victim and claiming to be from some organization a victim would trust
  - Is generally a process of reaching out to as many people as possible, hoping enough people respond
- More targeted attacks: spear phishing and whaling

3

Phishing

- Via emails, phone calls
- *appear legitimate*
- include a sense of urgency
- threat to your personal safety or security
- You are asked to verify personal data
- Banks

Social Phishing*

Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer
School of Informatics
Indiana University, Bloomington

December 12, 2005

4

4

DDOS : Distributed Denial Of Service

6

6

Definition

- Distributed Denial Of Service is a distributed version of the DOS attack
- The DOS attack makes a service or a network unavailable to its legitimate users.

- It can have different forms:
  - Flooding of a network
  - Disruption of connections between two machines
  - Block the access to a service to a particular machine/person

7

7

Detection and Protection of DDOS

- How can I prevent my servers from being used as DDoS hosts in the future?
- How can I prevent my personal computer from being used as a DDoS host ?
- How do I check my servers to see if they are active DDoS hosts?
- What should I do if I find a DDoS host program on my server?
- How should I configure my routers, firewalls, and intrusion detection systems against DDoS attacks?

10

10

3 lines of defence against DDOS

1. **Before the attack**: Attack prevention and pre-emption
   a. Enforce policy for **resource consumption** (scanning, and filtering)
   b. Providing **backup** resource on-demand
   c. Modify systems and protocols on the internet to reduce the possibility of DDOS attack
   d. Turn off all unnecessary services of the web servers, and use the latest update and resource management services (load balancing)
2. **During the attack**: attack detection and filtering
   a. Try to detect the attack at the beginning by looking for **suspicious patterns of behavior** => the response involves **filtering out packets** likely to be part of the attack
3. **During and after the attack**: Attack source traceback and identification
   a. Identify the source in order to prevent future attacks

DDOS attack is very challenging, because there is a number of ways in which they can operate.

11

11

Password cracking

12

12

Password Cracking

- Most of the password cracking techniques are successful due to weak or easily guessable passwords
- There are two types of password cracking tools

Online password crackers, technique which interacts with a 'live' service or application

→ attempts to brute-force authentication by trying an exhaustive list of password and username combinations

Offline password crackers, technique which do not require the service or application to be running

→ used to obtain a password in plaintext having access to a system's password hash file

13

13

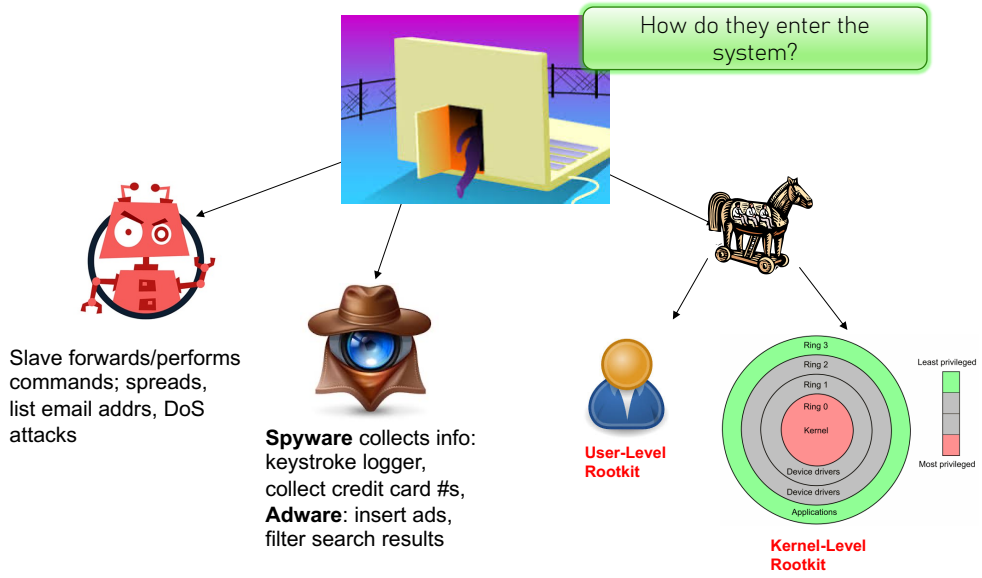
How to prevent password cracking ?

- Use strong passwords.
- Force a password update; always change default passwords.
- Use stronger authentication methods: digital certificate, challenge/response, or smart card.
- Monitor and track password attacks, lock the account after a certain number of attempts (known as password throttling).
- Protect password hashes: for example, using BIOS setting to prevent booting from anything but the primary driver.
- Rename privileged accounts (ROOT, ADMIN), and give them additional protection.

14

14

Backdoor malwares



20

20

What is a backdoor

- Backdoor is a piece of software which resides on a target computer
  - It runs as a hidden process that allows an unauthorized user to control a machine bypassing normal authentication
  - It can often bypass security measures such as firewalls, password protection and intrusion detection systems
    - It provides interactive access via non-standard TCP ports
    - The backdoor is setup as a 'server' (in a target system) which listens to incoming connections from a 'client' (controlled by the attacker)

21

21

Capabilities of a backdoor

Backdoors allow:

- Use of command shells
- File transfers
- Remote shutdown and reboot
- Registry editing
- Keystroke logging & password dumping
- Screen capture
- Encrypted communication
- Mouse and keyboard control
- Upload and download of files & execution of programs

22

22

How to detect and block backdoors

Run antivirus (updated) with Trojan removal tools

Scan attachments and downloads before opening/installing them – use hashes to check integrity of legitimate software (whenever possible)

Keep computers patched

Monitor:

- Processes running
- Open ports
- Alerts from firewall outbound communication
- Unexplained activities (e.g., pop-ups)

Use IDS (limited success)

23

23

Logic Bombs

- Malware designed to harm a system when some logical condition is reached
- Often triggered based on a specific date and time
- Possible to distribute a logic bomb via a Trojan horse

24

Spyware

- Also called Adware
- Any software that can monitor activity on a computer
- May involve taking screenshots or perhaps logging keystrokes
- Can have legal or illegal applications
- May be embedded in other programs
- May masquerade as antimalware product

25

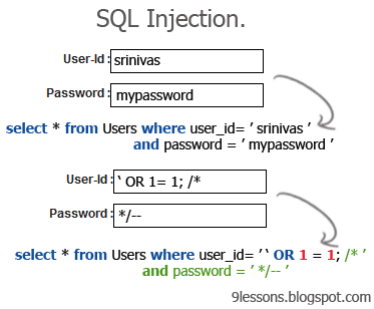
Keystroke Loggers

- Also called "keyloggers"
- Software-based keyloggers can be installed via worms or Trojan horses
- Record keystrokes and transmit them to the attacker
- Hardware-based keyloggers

26

SQL Injection

- Are designed to exploit "holes" in a Web application
- If Web site lacks input validation, you need only a Web browser and SQL knowledge to launch attack
- Are common and serious issues with Web sites that use a database as its back end
- Is carried out by placing special characters into existing SQL commands and modifying behavior to achieve desired result



27

Hacking via SQL Injection

- Typical SQL statement
  - `SELECT * FROM tblUsers WHERE USERNAME = '" + txtUsername.Text +' AND PASSWORD = '" + txtPassword.Text +"'`
- Specific username and password:
  - `SELECT * FROM tblUsers WHERE USERNAME = 'thisuser' AND PASSWORD = 'letmein'`
- SQL injection example:
  - `SELECT * FROM tblUsers WHERE USERNAME = '' or '1' = '1' AND PASSWORD = '' or '1' = '1'`

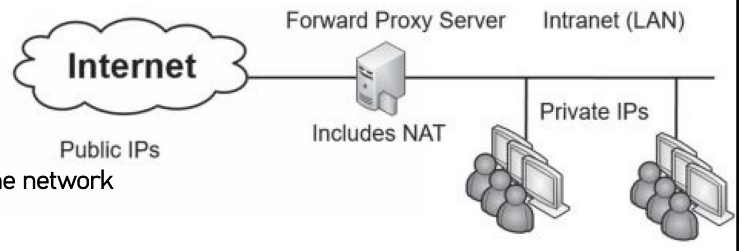
28

Hacking via Cross-Site Scripting

- Perpetrator seeks out someplace on target website that allows end users to post text that other users will see, such as product reviews
- Instead of posting a review or other text, the attacker posts JavaScript
- If website does not filter user input before displaying, other users navigate to this review and script executes

29

Proxy servers and Anonymizers



- Proxy server is located on the edge of the network

bordering the Internet and the intranet,

- A proxy server can filter and cache content from web pages, but it doesn't divert attacks. A web application firewall (WAF) is an additional firewall designed to protect a web application.
- A transparent proxy will accept and forward requests without modifying them.
  - It is the simplest to set up and use and it provides caching.
- nontransparent proxy server can modify or filter requests.
  - Organizations often use nontransparent proxy servers to restrict what users can access with the use of URL filters.
  - A URL filter examines the requested URL and chooses to allow the request or deny the request.
- Employees sometimes try to use anonymizers to bypass proxy servers, but a proxy server usually detects, blocks, and logs these attempts.

30

Cyber security techniques

31

Test Basic

2 approaches of testing

- *Whitebox testing –*

  Full information about the target is shared with the testers. This type of testing confirms the efficacy of internal vulnerability assessment and management controls by identifying the existence of known software vulnerabilities and common misconfigurations in an organisation's systems.

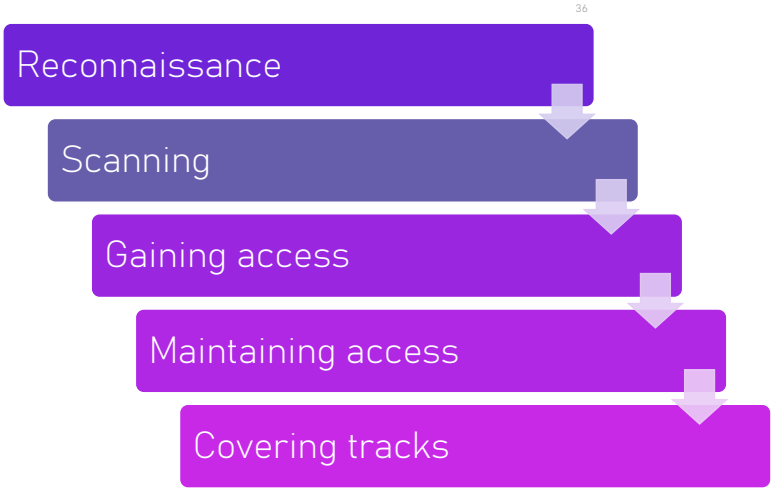
- *Blackbox testing –*

  No information is shared with the testers about the internals of the target. This type of testing is performed from an external perspective and is aimed at identifying ways to access an organisation's internal IT assets. This more accurately models the risk faced from attackers that are unknown or unaffiliated to the target organisation. However, the lack of information can also result in vulnerabilities remaining undiscovered in the time allocated for testing.

32

Attack steps

- Pen testing follows the attack steps.
- The objective is to make life hard for any would-be hackers at each step.

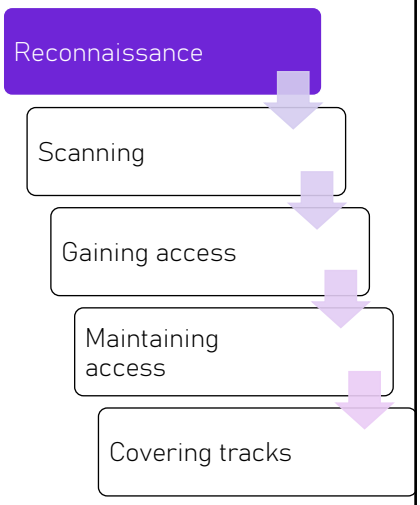


33

33

What is reconnaissance

- Reconnaissance is about information gathering
- The word *reconnaissance* is borrowed from its military use, where it refers to a mission into enemy territory to obtain information
- Goal: Obtain as much information as possible about the target (network) without raising the attention of defenders
  - If you detect and (possibly) stop the reconnaissance, you may be able to avoid an attack



34

34

Types of reconnaissance

There are two methods used to obtain data

1. Passive Reconnaissance:
   - Gather information without engaging any action with the target
   - Uses public information / **public intelligence**
   - May use technical and non-technical tools/techniques
2. Active Reconnaissance:
   - Engage with the target to gather information
   - Typically uses technical tools

35

35

Reconnaissance from public data

Gathering freely available public data from:

- Cached web pages
- Job postings, Job Sites
- Professional profiles
- Troubleshooting mailing lists
- News archives
- Social media
- User groups

36

36

Reconnaissance tools

- WHOis
- Network traffic sniffers
- Maltego
- Other websites:
  - Social media
  - Google
  - Shodan.io

37

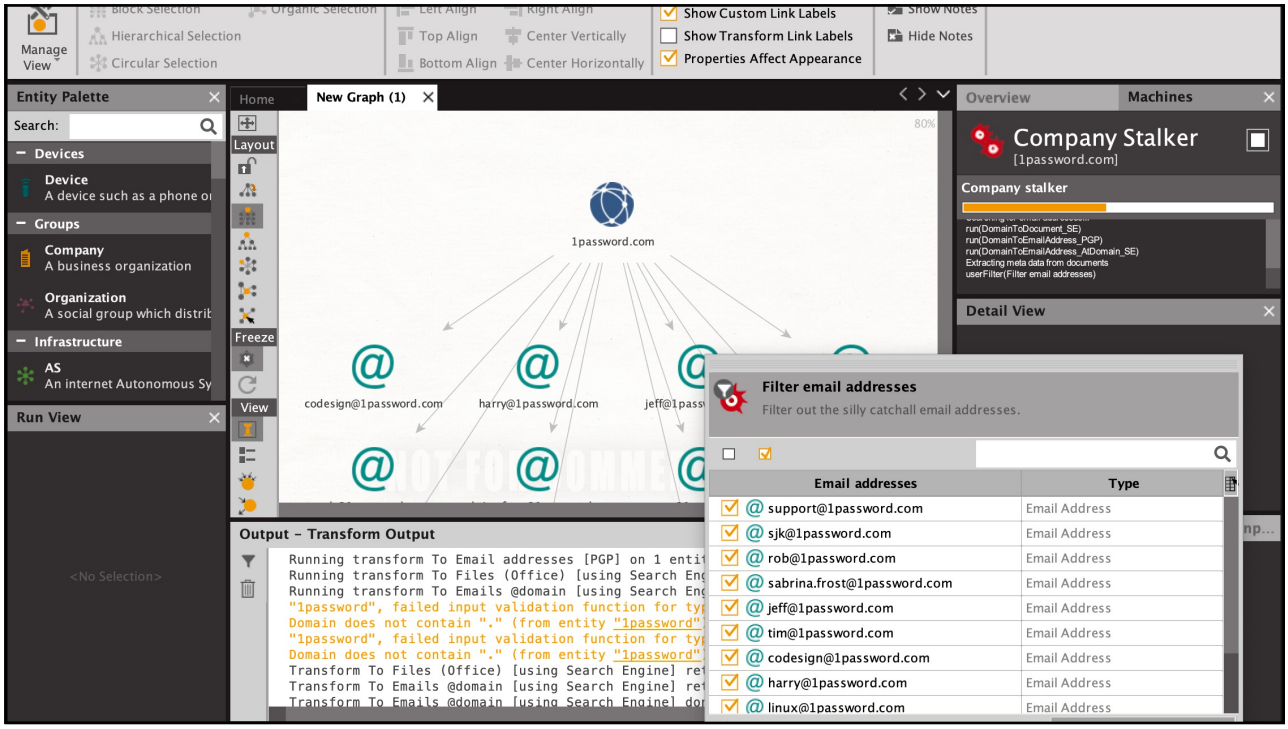
37

Example: Maltego

- **Maltego** is an open source intelligence and graphical link analysis tool for gathering and connecting information for investigative tasks. https://www.maltego.com/
- Tested on 1Password (leading password management tool, https://bugcrowd.com/agilebits)

Bugcrowd.com is a platform to manage "bug bounty" for many organisations

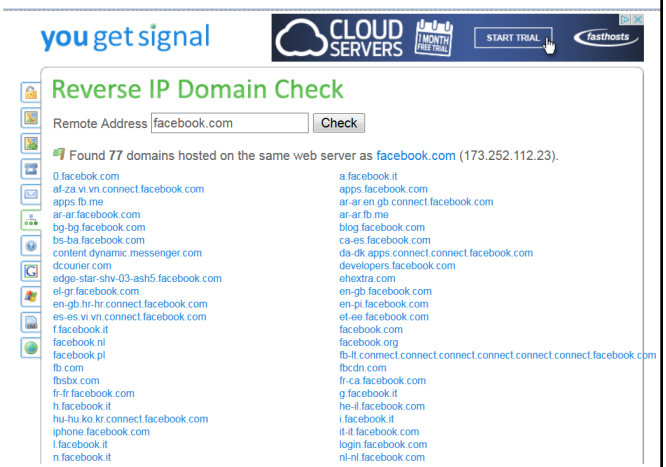
38



39

Example 1: Yougetsignal.com

- *Yougetsignal.com* allows you to perform a reverse IP lookup on a webserver to detect all other websites present on the same server. All you need to do is enter the domain.



40

Example 2: Tracing the Location

- **Traceroute** is a very popular utility available in both Windows and Linux.
- It is used for network orientation, to figure out how the network topology, firewalls, load balancers, and control points, etc. are implemented on the network.

41

41

Protection against reconnaissance

- Reconnaissance is an essential phase for attackers

  it allows them to potentially get a list of IP addresses, emails, URLs, and to find information relevant for planning the attack

  However, it doesn't provide information about '*what is actually attackable*'
- Defence is mainly focused on training, setting policies and configuration, but also on getting to know what the attacker can obtain using available tools.
- Protection against reconnaissance is about limiting amount of information the organization/ employees make public

  Train employees on security awareness (e.g., about social media security settings)

  Enforce policy on what can and cannot be posted on social media

42

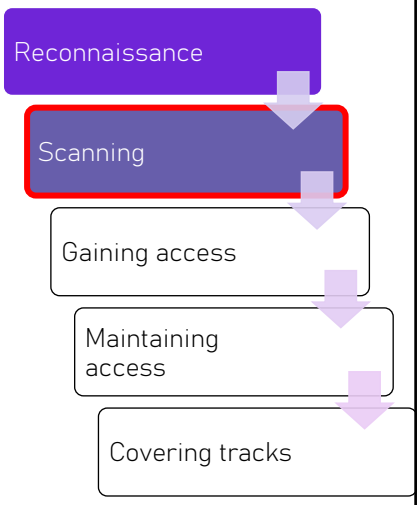
Scanning

- Scanning is about actively probing a system to find '*what is attackable*' → i.e., find entry points to a network / specific target

  In some ways there is a fuzzy line between active reconnaissance & scanning

- Goal: *Obtain a network map and find vulnerabilities*
- If you detect and block scanning activities, you stop the next phase – the actual attack

  If we cut off information at this point a hacker is likely to go elsewhere



43

43

What can be obtained via scanning ?

Scanning provide info such as :

- if a system is alive
- Open TCP/UDP ports
- Protocols used
- Services running
- Operating Systems/version installed
- Deployed defences
- Resources or shares on the network
- Usernames or groups assigned on the network
- Last time user logged on
- Known vulnerabilities

Scanning techniques

- Ping / Ping sweep
- Banner Grabbing
- Web-based directory enumeration
- Firewall enumeration & fingerprinting
- DNS enumeration
- Others

44

44

Ping / Ping Sweep

- Ping will tell you whether **one specific** host is live on the network and accepting traffic, whereas ping sweep is a basic network scanning technique used to identify live hosts within a network range (computers or network devices)
- Ping Sweep also allows to:
  - Detect rogue devices connected to the network
  - Ensure the IP addresses on the network match the documentation
- **Defence**:
  - ping sweep can be detected by protocol loggers
  - block's ICMP traffic from non-authorised users
  - IDS

45

45

Firewall enumeration & fingerprinting

- **Firewall**: hardware/software device that filters the traffic into and out of the network
- Firewall enumeration

  Used to enumerate firewall rules (what is allowed and what is denied)

  E.g., identifying a firewall remote management port open may allow firewall fingerprinting used to determine firewall type (manufacturer, model)
  - an attacker can then look for the default configuration and for known vulnerabilities affecting this specific firewall type

46

46

Firewall enumeration & fingerprinting

Defence:

Firewalk

- It is a network-auditing tool
- It scans the firewall rules to detect misconfigurations

Some firewall manufacturers allow **changing the default management port**

Network Intrusion Detection (NIDS)

- Used to detect scans for particular firewall ports

47

47

Nmap and Zenmap

- Network mapper (Nmap) runs at command line
- Zenmap is the graphical user interface to Nmap
- Originally intended as a network mapping utility
- Port scanning and host detection features
  - Identify access points to a network
  - Identify holes in access controls
- Highly configurable
- Open source

48

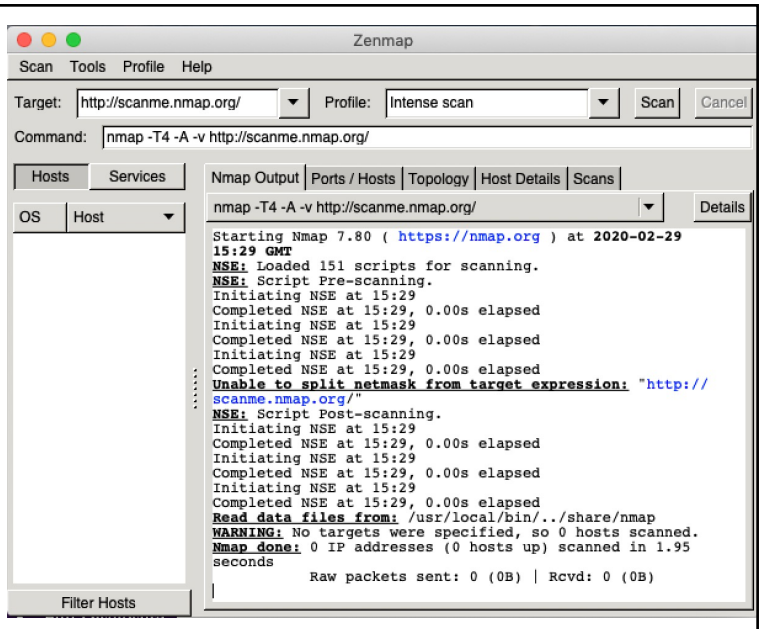
Nessus

- Commercial security scanner developed by Tenable Network Security
- UNIX based
- Network-centric with Web-based consoles and a central server
- Offers a comprehensive set of tools
- Useful tool for larger networks
- Reports indicate which ports are open on which hosts and any security threats to those ports

49

Zenmap: Nmap Output Tab

Tested on: scanme.nmap.com



50

Port Scanning

Mechanics	Uses

▪ TCP or UDP packets are sent to ports on a system
▪ Scanning performed on single IP address or IP address range
▪ Open ports can verify:
  ▪ Presence of a system and services
	Useful to both hackers and security professionals
	▪ Hackers determine existence of hosts and services
	▪ Security Professionals
	  ▪ Determine the existence of rogue hosts
	  ▪ Determine existence of rogue servers
	  ▪ Part of a vulnerability scan

51

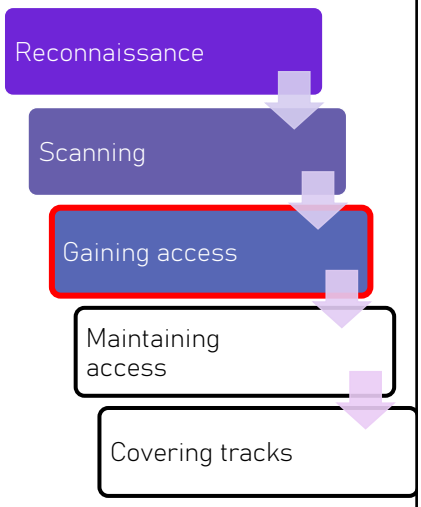
Gaining access

- Gaining access involves exploiting one or more vulnerabilities = The attack

  The previous phase aimed at finding out '*what is attackable*', i.e., entry points to a network / specific target

  This phase is about actually launching an attack

- Goal: *Reach a target for some sort of gain* (e.g., £££, affect reputation, revenge, espionage, raise attention)



52

52

Sources of security vulnerability

- **Incorrectly implemented** or malfunctioning controls
- **Control** being used **incorrectly**
- Assets used in a way, or for a purpose, **not intended** when the asset was purchased or made
- Software – design, implementation
- Hardware – design, manufacturing
- Network – design, operation
- Humans/personnel/3rd parties
- Physical environment
- Organisation – procedures, policies

53

Attack Surface

- Vulnerabilities may happen in any component that a user can interact with in some way → this potential exposure is known as attack surface
- Examples:

a. The Attack Surface of a network includes:
   - Published services and applications,
   - Authentication systems,
   - Management interfaces,
   - Remote-access services such as VPN, FTP, Telnet, SSH services.

b. The Attack Surface of a web application includes:
   - The input fields,
   - Query string parameters,
   - HTTP Protocol components.

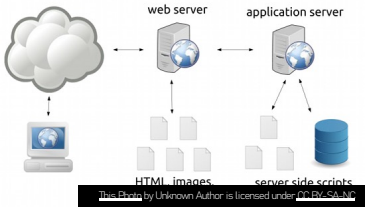
54

54

Example: externally-faced network

Typical externally-faced services may involve:

- Web Servers
- Router Administrative Interfaces
- SMTP Mail Servers
- Web Mail
- VPN/SSL Systems



55

Access Vector

There are two main possibilities about how a vulnerability is exploited :

1. Local: The attacker has physical access to the target or access to a command prompt/shell

2. Remote: The attacker exploits the target box without first gaining access to a command shell
   - E.g., by taking advantage of client-server message exchange via Remote Procedure Call protocol

56

56

Types of activities involved in gaining access

- Having identified the attack surface, the hacker will decide which vulnerability is easiest to exploit and more likely to remain undetected
- Getting ready for an attack involves developing exploits, purchasing them in the black market and/or using tools like Metasploit to 'select' appropriate off-the-shelf exploit software
- The exploit that is then used will depend upon the vulnerability and the operating system of the target

57

57

Types of activities involved in gaining access

- The execution of an exploit typically results in
  - The ability to execute unauthorized code
  - The ability to escalate privilege
  - The ability to bypass protection mechanisms (e.g., disable antivirus sw)
  - The ability to cause denial of service
- This is useful for
  - Infiltrating the LAN from the Internet
  - Acquiring knowledge about internal details
  - Moving from one host to another within the LAN

58

58

Types of activities involved in gaining access

- An activity often required to launch an attack is password cracking
  - Attackers use password cracking techniques to gain unauthorized access to a system (which not necessarily is vulnerable!), to escalate privileges and/or to run and install software
  - e.g., for authenticating to a user OS account, to an application or to a service running on the system

59

59

Privilege Escalation

1. Take advantage of **programming errors** or **design flaws** to grant the attacker elevated access to the network and its associated data and applications.
2. Not every system hack will initially provide an unauthorized user with full access to the targeted system. There are two kinds of privilege escalation: vertical and horizontal

   Vertical privilege escalation, also known as *privilege elevation*, where a lower privilege user or application gains the ability to access functions or content reserved for higher privilege users or applications

   Horizontal privilege escalation, where a normal user gains the ability to access functions or content reserved for other normal users

60

60

How to prevent privilege escalation ?

- Keep systems patched.
- Run services and applications without administrative privileges as much as possible.
- Run Host-based IDS on key servers
- Take steps to mitigate the consequences of a privilege escalation if it does occur to keep the damage to a minimum.
- Maintain as strict a separation between privilege areas as possible, e.g., maintain access to admin account separate from user account.

http://www.techrepublic.com/blog/it-security/mitigating-the-privilege-escalation-threat/

61

61

Installing and executing unauthorized code

- Executing unauthorized code (i.e., malware) is a crucial step in attacks
- It is sometimes called "**owning**" the system
- Examples of malware types:-

Spyware
Adware
Keylogger
Ransomware
Trojan Horse
Virus & Worm

Helps in the next step

62

62

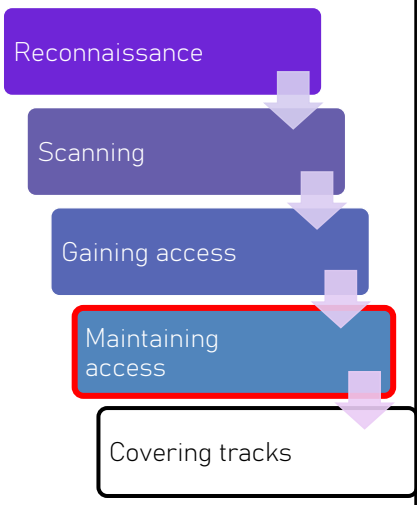
Maintaining access

- Maintaining access is about the ability of attackers to return to a target and/or to install & run malware to harvest something

  This phase involves the setup of a 'way' for attackers to connect to the target at any time (backdoor)

- Goal: Maintain long term access to systems and networks

  If you detect and close this open channel, there is a great chance that the attack will be discontinued



63

63

What covering tracks entails

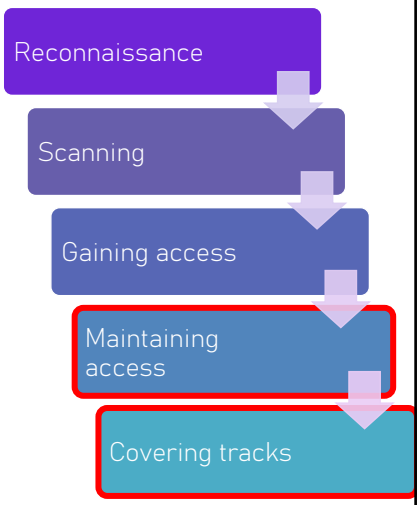
- Covering tracks is about erasing or disguising artefacts related to an attack

  It involves activities such as:

  - Clearing logs
  - Hiding/disguising files, processes & activities

    E.g., in the Target data breach, attackers used malware 'svchosts.exe' which resembles Windows service host process 'svchost.exe'
  - embedding malware to the OS kernel or to the BIOS

- Goal: Avoid detection



64

64

Ways to maintain access and/or covering tracks

- The main three techniques:
  - Backdoors
    - OS backdoors
    - Web backdoors
  - Rootkits

65

1

Outlines

- Part 1:
  - Cyber Security Safeguards- Overview,
  - Access control, Audit, Authentication, Biometrics. Cybercrime and
- Part 2:
  - The Indian IT Act- Challenges, Amendments, Challenges to Indian Law and cybercrime
  - Scenario in India, Indian IT Act and Digital Signatures.
  - Other legal and ethical considerations

2

What is access control?

- Access control is the formalization of those rules for **allowing or denying access**.
- Access controls define the allowable interactions between subjects and objects.
- It is based on the **granting of rights**, or privileges, to a subject with respect to an object

4

4

Access control systems

A well-defined access control system consists of three elements

- **Policies** – clear statement of the business requirements regarding access to resources
- **Procedures** – non-technical methods used to enforce policies
- **Tools** – Technical methods used to enforce policies

Example:

a company has strict **policies** to determine who has access to personnel records (sensitive and confidential data). To enforce the policy, the company has procedures that state that a record can be given only to employees with proper credentials (authentication), who fill out a form stating their specific need for the information contained in the record they request. When the request is approved, the employees may be given a username and passwordto access the employee records intranet website (authorization process)

5

5

Privileges

The right to execute a certain operations

Are associated with OS functions and relate to activities

- System administration
- Backup
- Mail access
- Network access

8

Security Models for Access Control

- Bell-LaPadula model
- Biba model
- Chinese wall model
- Clark-Wilson model
- Harrison-Ruzzo-Ullman model
- Information flow model
- Execution monitors

9

Bell-LaPadula model

- 4 access rights:

  Execute

  Read

  Append

  Write

	Execute	Append	Read	Write
observe			X	X
alter		X		X

10

Access control for data

Data at Rest	Data in motion	Object-Level Security
• Stored data • Some storage places are at very high risk, e.g web server. • Possible physical theft for portable devices such as smartphone, tablets, flash memory devices .	• Data at any time it travels from one place to another • Vulnerable as it travels over the network (improper disclosure and theft)	• An object is an item or a distinct group of information in a data storage system • e.g. relational data bases • By grouping information as an object, access control can be more sufficient.

13

13

Securing data

- Securing DAR
  - Encryption
  - Backup
  - Access policy (and accountability)
- Securing DIM
  - Encryption (e.g. email signature)
  - Secured communication (SSL, VPN)

14

Access control for file systems

- Access control List (ACL)
  - ACL is a list of security policies associated with an object
  - Collection of access control entities (ACEs)
  - Types of ACE: access denied, access allowed, system audit
- Discretionary access control List (DACL)
  - DACL controls access to an object, handles what access is allowed or denied
  - When an object is accessed all the ACEs contained in the DACL are checked
- System Access Control List (SACL)
  - System created access ACL that handles the information assurance aspect of access controls
  - System generated list based on the auditing rules set by the system admin
  - Doesn't allow or deny access, it only records the accees attempts and the success or failure of that attempt

15

15

Best practice for access control for information systems

Access controls for information systems are only as good as the policies and procedures that dictate their use, there are few general bets practices that you should follow to ensure reasonably secure access controls on information systems:

- Create a baseline for access
- Segregate users' right by their role
- Automate user creation
- Tie access controls to the environment
- Have a clear standard for decommissioning data storage devices

  Have a standard method to guarantee that data is removed from the device before disposal

16

16

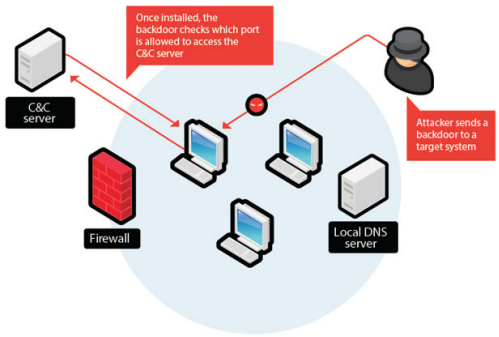
Access control threats

- Password cracking

  Guessing or deciphering password
- Heightened access

  The ability of an attacker to log into a system under one level of access and exploit a vulnerability to gain a higher level of access
- Social engineering

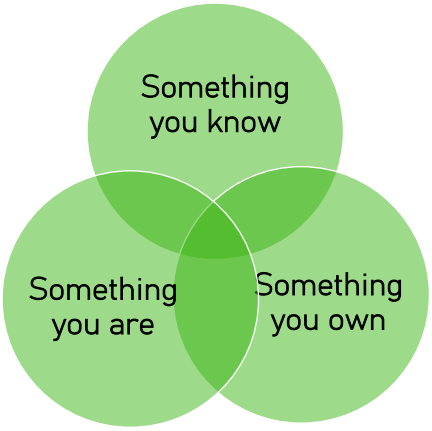
  The use of manipulation or trickery to convince authorised users to perform actions or divulge sensitive information to the attacker



17

17

What is authentication about?



- Verifying identity (prove possession of a secret)
  Assess identity of users
  By using credentials
- Mutual authentication
- Key distribution (secret for secure communication)

- Authorization
  Determining if users have the right to perform requested action (e.g. write a file, query a database etc.)

18

Memory cards

- Can store but do not process data
- The most common in the magnetic stripe card
- Can include an internal electronic memory
- Can be used alone for physical access
  Hotel room, underground ticket
- Provides significantly greater security when used combined with a password or PIN
- Issues/drawbacks:
  - Requires a special reader
  - Loos of the token
  - User dissatisfaction

21

Smart card

- Physical characteristics
  - Include an embedded microprocessor
  - A smart token (e.g. bank card)
  - Different form with calculator for example
  - Contact or contactless smart cards
- Interface
  - Manual interfaces include a keypad and display for interaction
  - Electronic interfaces communicate with compatible reader/writer
- Three categories of authentication protocols
  - Static
  - dynamic password generator
  - Challenge response

22

Authentication servers

When a user tries to access a remote service, three processes has to be applied:

Authentication: verify the identity of entity.

Authorization: determine whether requesting user is allowed access to a resource.

Accounting: process of gathering and sending user information on resource usage for the purpose of capacity planning, auditing, billing or cost allocation.

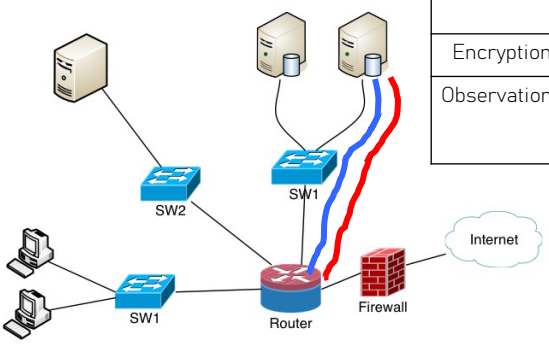
Two AAA protocols:

- Remote Authentication Dial-in User Service (RADIUS)
- Terminal Access Controller Access Control System Plus (TACACS+)
- Kerberos

23

23

Centralized management control



	RADIUS	TACACS
Transport protocol	UDP 1645 or 1812: authentication 1646 or 1813: accounting	TCP (Port 49)
Encryption	Encrypts the password only	Encrypts all the payload
Observations	**Open standards**,robust accounting features, less granular authorisation control	Proprietary to Cisco, granular control of authorization, AAA separated

25

25

Scenario: Which protocol ?

- RADIUS authenticates end users before allowing them access to the networks
- TACACS+ for authenticating and authorizing administrators
- Can we use both? YES

26

26

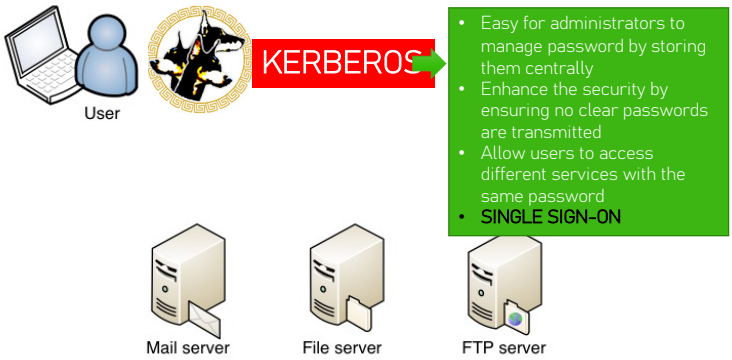
KERBEROS

- In Greek mythology, a many headed dog, the guardian of the entrance of Hades

27

27

What are we trying to secure with KERBEROS

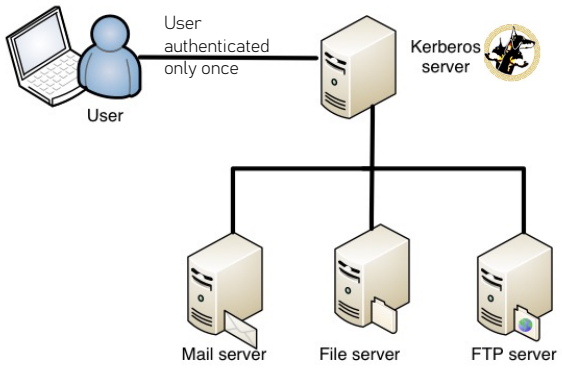


- Easy for administrators to manage password by storing them centrally
- Enhance the security by ensuring no clear passwords are transmitted
- Allow users to access different services with the same password
- SINGLE SIGN-ON

32

32

Single sign-on



33

33

References

1. Miller S., Neumann B., Schiller J. and Saltzer J. "Kerberos authentication and authorization System", Project Athena Technical Plan, MIT Project Athena (December 1987)
2. http://web.mit.edu/kerberos/
3. William Stallings "Network security essentials – Applications and standards" 5th edition, Pearson.
4. PFLEEGER C. P., PFLEEGER S. L. " Analyzing computer security – Athreat/vulnerability/ countermeasure approach". Pearson edition 2011.
5. Bhaiji, Fahim Hussain Yusuf: **"Network security technologies and solutions".** CCIE Professional Development series, Pearson Education, 2008.
6. Omar Santos: "**End-to-end Network Security**". CISCO Press 2008.

34

34

What is a firewall

An integrated collection of security measures that are designed to prevent unauthorized access to a networked computer system.

White G., (2003)

http://it.fotolia.com/Content/Comp/72187968

35

What a firewall can and cannot do ?

Can do:

- Security gateway
- Traffic control device
- Packet Filtering device
- Enforce a security policy
- Secure the network from external attacks

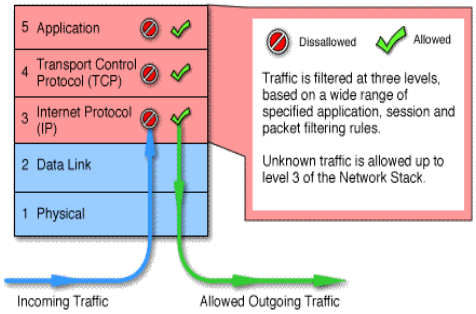
Cannot do:

- Firewall is only one piece of the large complex puzzle of network security
- Not an authentication server
- Not a Remote Access Server
- Cannot see the content of encrypted packets (Position is important)
- Cannot see all the traffic if not positioned properly
- Not a malicious code scanner
- Not an IDS

36

Firewall methods: Stateful Multilayer Packet Inspection

- Combines other 3 types (except no proxy's)
- Algorithms used to recognise application layer data
- Examines entire packet. Headers and data. Blurring the line between firewall and IDS



39

Firewalls Risks and Disadvantages

- **Central point for attack**, once it's down... the whole network is down.
- Packet filtering by a software firewall can degrade your system's performance.
- They may restrict legitimate users from accessing valuable services.
- Firewalls do not provide data **integrity and confidentiality**

40

Placement of the firewall

1. The structure of your network (Sections, subnets, DMZ)
2. The traffic patterns
3. Protect all internet access point and gateways
4. Remote access
5. Special needs of your infrastructure

Following all these points may not be practical and cost effective, so a risk assessment must be conducted to determine where a firewall is needed.

41

Firewall rules management

Deny by default, allow by exception

- Rules=filters
- Pre-configured firewalls are not good practice, you should:

  Do an inventory of essential business applications & communications

  Determine protocols/ports/IP @ of valid traffic

  Write the rules and test them in lab environment

  Obtain approval for the rules sets

  Document the rules into a security policy

42

DMZ design fundamentals

- DMZ designs generally consist of Firewalls and segments that are protected from each other by:
  - ✓firewall rules and routing as well as the use of RFC 1918 addressing on the internal network.
- Design of the DMZ is critically important to the overall protection of the internal network.
- Access control lists (ACLs)
  - ✓Determine who is allowed access to an item in a network and how that item can be used.

RFC1918 (Address Allocation for Private Internets) document specifies an Internet Best Current Practices for the Internet Community

45

Legal and ethical considerations

46

Cyber security challenges in India

- Lack of trained and **qualified manpower** to implement the counter measures
  But also to implement, design and harden network security
- No e-mail account policy especially for critical agencies (the defense forces and police)
- Promotion of Research & Development in ICTs is not up to the mark.
- Security forces and Law enforcement personnel are not equipped to address high-tech crimes.
- Present protocols are not self sufficient, which identifies the investigative responsibility for crimes that stretch internationally.
- Budgets for security purpose by the government especially for the training of law enforcement, security personnel's and investigators in ICT are less as compared to other crimes.

Other worldwide challenges

- Lack of awareness and **cyber security culture**,
- Cyber attacks can come from entities of political motivations (**cyber terrorism**)
- The speed of cyber technology changes always beats the progress of govt. sector so that they are not able to identify the origin of these cyber-crimes.

Source: https://philarchive.org/archive/BHAIAC

47

Action to reduce Cyber crime

- Technological actions
  - Use of Anti malware software and scanning tools to prevent attacks on first steps
  - Use of internet safety tools, appropriate time and as per machine requirement.
  - Restrict access (create clear authentication and access control policies)
  - **Adopt network and software hardening (Security by design).**
- Awareness actions
- Legal actions

48

Action to reduce Cyber crime

- Technological actions
- Awareness actions
  - Creating appropriate security policies and enforcing them (e.g. Password policy).
  - Create specific security trainings for different group of users.
  - Reduction in use critical internet services in public networks.
  - Rise Cyber security Awareness (gov or organization level, hacking competition and challenges, education and schools)
- Legal actions

49

Action to reduce Cyber crime

- Technological actions
- Awareness actions
- Legal actions
  - Indian IT Act,
  - Communications Act of 1934 updated 1996
  - Computer Fraud and Abuse Act of 1984.
  - Computer Security Act of 1996.
  - Economic Espionage Act of 1996.
  - Health Insurance Portability and Accountability Act of 1996.
  - Personal Data Privacy and Security Act of 2007.
  - Data Accountability and Trust Act.

50

Hacking in Indian law

- Cybercrimes are covered under Information Technology Act (IT Act) and the Indian Penal Code.
- The IT Act, 2000, deals with cybercrime and electronic commerce. The IT Act was later amended in the year 2008. The Act defines cyber crimes and punishments.
- Amendments to the Indian Penal Code, 1860, The Reserve Bank of India Act were also done under this IT Act. The purpose of this Act is to safeguard e-governance, e-banking, and e-commerce transactions.

- Why is there a need for New IT Law?
  - **India Entering into Digital Age**
  - **Majority of Cybercrimes in India are Bailable Offense:** A historical mistake was made when the **IT (Amendment) Act, 2008,** made almost all cybercrimes, barring a couple, bailable offences.
  - The IT Act **does not cover most crimes committed through mobiles.** This needs to be rectified.

51

India IT act amendments

- On June 6, 2022, the Ministry of Electronics and Information Technology released the draft amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021) for public feedback.
- The IT Rules were notified on February 25, 2021, under the Information Technology Act, 2000 (IT Act).
- The goals of these rules are to ensure an Open, Safe & Trusted and Accountable Internet for all Indian Internet Users. These rules have succeeded in creating a new sense of accountability amongst Intermediaries to their users especially within Big Tech platforms.
- As a part of pre-legislative consultation process, a copy of the aforesaid draft amendment to the IT Rules 2021 has been uploaded on the website of the Ministry of Electronics and Information Technology (www.meity.gov.in) for public feedback and inputs.

Source: https://prsindia.org/theprsblog/explained-draft-amendments-to-the-it-rules-2021

https://www.meity.gov.in/writereaddata/files/Gazette%20notification_IT%20Rules%20Amendment%202022_28Oct2022.pdf

52

India IT act key amendments

- The Internet should be Open, Safe & Trusted and Accountable for ALL Indians using the Internet – our Digital Nagriks. ·
- That ALL online intermediaries providing services in India shall never contravene the Indian constitution, Laws and Rules, and follow them in letter and spirit. The 2021 Rules require the intermediary to "publish" rules and regulations, privacy policy and user agreement for access or usage of its services.
- Unlawful and harmful information violative of their own terms and conditions shall be quickly removed when reported by users, while also providing the users a reasonable opportunity to respond in case of significant social media platforms. ·
- The IT Rules, 2021 provide for a robust grievance redressal mechanism. However, there have been many instances that grievance officers of intermediaries either do not address the grievances satisfactorily and/or fairly. In such a scenario, the need for an appellate forum has been proposed to protect the rights and interests of users,
- **Expeditious removal of prohibited content:** The 2021 Rules require intermediaries to acknowledge complaints regarding violation of Rules within 24 hours, and dispose of complaints within 15 days. Also, the complaints concerning the removal of prohibited content must be addressed within 72 hours.

Source - https://www.meity.gov.in/writereaddata/files/Press%20Note%20dated%206%20June%2022%20and%20Proposed%20draft%20amendment%20to%20IT%20Rules%202021.pdf

53

Examples of cyber crimes in India

India among top five victims of cybercrime: FBI crime report 2021

Among the complaints received in 2021, ransomware, business e-mail compromise (BEC) schemes, and the criminal use of cryptocurrency were among the top incidents reported

- UIDAI Aadhaar software hacked
  - UIDAI released the official notification about this **data breach** and mentioned that around 210 **Indian Government websites** were **hacked**. This data breach included Aadhar, PAN, bank account IFSC codes, and other personal information of the users and anonymous sellers were selling Aadhaar information for Rs. 500 over Whatsapp.
- Mobikwik data breach (2021)
  - The data breach affected 3.5 million customers, revealing addresses, phone numbers, Aadhaar cards, and PAN cards, ...etc. Only until the regulator, the Reserve Bank of India (RBI), instructed Mobikwik to immediately perform a forensic audit by a CERT-IN empanelled auditor and submit the findings did the business begin engaging with the appropriate authorities.
- Overall

More than half (52%) of Indian companies experienced fraud or economic crime in the last 24 months, A Trellix study published in September 2022 also noted that over two thirds of cybersecurity professionals in India work with more than ten different security tools or solutions across their organisation, making the setup extremely 'disconnected' and increasing chances of cyber-attacks.

Good news, in an earlier report, PwC noted that eight (82%) out of 10 business executives in India foresee an increase in cybersecurity budgets in 2023.

Sources:

https://www.thehindu.com/sci-tech/technology/cyber-attacks-intensity-increase-mail-servers-satellites-key-targets-2023-kaspersky-report/article66147340.ece

https://www.techcircle.in/2022/11/16/footballer-cristiano-ronaldo-launches-nft-collection-on-binance

54

Ethics

- https://www.dictionary.com/browse/ethics

1. (*used with a singular or plural verb*) a system of moral principles:
   the ethics of a culture.
2. (*used with a plural verb*) the rules of conduct recognized in respect to a particular class of human actions or a particular group, culture, etc.:
   medical ethics;
   Christian ethics.
3. (*used with a plural verb*) moral principles, as of an individual:
   His ethics forbade betrayal of a confidence.
4. (*used with a singular verb*) that branch of philosophy dealing with values relating to human conduct, with respect to the rightness and wrongness of certain actions and to the goodness and badness of the motives and ends of such actions.: Compare axiological ethics, deontological ethics.

55

Ethics

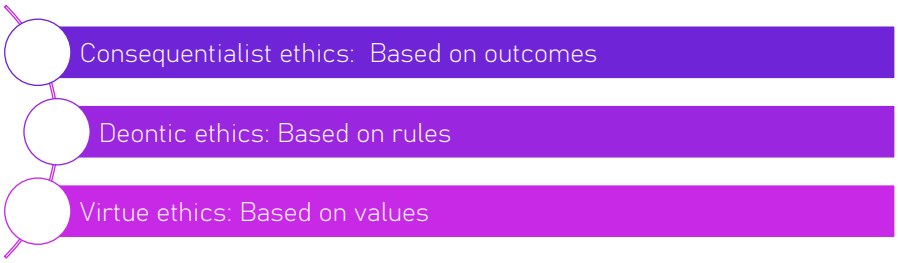
How do you decide whether something is good?

Not, what is good, but how do you decide?

59

Normative Ethics

- How do you decide whether an action is good?



- Useful to be able to reason using all of them
  - understand & respond to others' ethical reasoning
  - see sides of a problem you might have missed

60

Professional codes

- BCS (UK)
  - https://www.bcs.org/upload/pdf/conduct.pdf
- ACM (US)
  - https://www.acm.org/binaries/content/assets/about/acm-code-of-ethics-and-professional-conduct.pdf
- East Asia Academies of Engineering (China, Japan, Korea)
  - http://ethics.iit.edu/ecodes/node/5076
- EU ethics guidelines for Trustworthy AI
  - https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

61

Some values in professional codes

- In all three professional codes:
  - Public wellbeing, health and safety
  - Honesty, transparency
  - Non-discrimination/equality, inclusion
  - Accountability
  - Environmental sustainability
- In both the Computer Science codes:
  - Privacy, confidentiality
- EU AI guidelines: also Human agency & oversight

62

Uber's Greyball

- Identified local police & regulation officers
  - via e.g location, credit card info
- Showed them fake interface so they couldn't catch any Ubers
- Uber's legal team approved the program,
- https://www.theguardian.com/technology/2017/mar/03/uber-secret-program-greyball-resignation-ed-baker

63

Greyball Stakeholders?

- Uber drivers
- Police, regulation officers
- Uber customers
- Uber shareholders
- Other road users
- Other taxi drivers
- Local taxpayers
- Everyone (e.g. effect on climate change)
- (more?)

64

Greyball: was it OK?

Why / why not?

- outcomes, rules, values

65

What is a professional code of conduct/ethics?

"The Code is designed to inspire and guide the ethical conduct of all computing professionals, including current and aspiring practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way."

https://ethics.acm.org/

66

What is a professional code of conduct/ethics?

- A professional association, such as IEEE, ACM and BCS, is entitled to set entrance requirements that govern minimum levels of experience and qualifications for new members.
- However, in return for membership of a professional association, **the individual accepts a duty to meet certain standards of conduct and behavior**.

The standards of conduct and behavior expected by the association are described within a code of conduct that also sets out a number of the association's principles.

67

Who are IEEE and ACM?

- IEEE Institute of Electrical and Electronics Engineers

  The world's largest professional society with engineers and professionals from different backgrounds with a lot of strong volunteers around the world.

  https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/ieee_code_of_conduct.pdf

- ACM Association of computing Machinery

  is another professional society more focused towards computing and CS related fields like Data Analytics, Programming, Data Mining, Web and Software.

  https://ethics.acm.org/code-of-ethics/

68

ACM code of Ethics and Professional Conduct

A full explanation of each of these is found here: https://www.acm.org/code-of-ethics

1. GENERAL ETHICAL PRINCIPLES

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

1.2 Avoid harm.

1.3 Be honest and trustworthy.

1.4 Be fair and take action not to discriminate.

1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.

1.6 Respect privacy.

1.7 Honor confidentiality.

69

ACM code of Ethics and Professional Conduct

2. PROFESSIONAL RESPONSIBILITIES

2.1 Strive to achieve high quality in both the processes and products of professional work.

2.2 Maintain high standards of professional competence, conduct, and ethical practice.

2.3 Know and respect existing rules pertaining to professional work.

2.4 Accept and provide appropriate professional review.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

2.6 Perform work only in areas of competence.

2.7 Foster public awareness and understanding of computing, related technologies, and their consequences.

2.8 Access computing and communication resources only when authorized or when compelled by the public good.

2.9 Design and implement systems that are robustly and usably secure.

70

ACM code of Ethics and Professional Conduct

3. PROFESSIONAL LEADERSHIP PRINCIPLES

3.1 Ensure that the public good is the central concern during all professional computing work.

3.2 Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.

3.3 Manage personnel and resources to enhance the quality of working life.

3.4 Articulate, apply, and support policies and processes that reflect the principles of the Code.

3.5 Create opportunities for members of the organization or group to grow as professionals.

3.6 Use care when modifying or retiring systems.

3.7 Recognize and take special care of systems that become integrated into the infrastructure of society.

71

ACM code of Ethics and Professional Conduct

4. COMPLIANCE WITH THE CODE

4.1 Uphold, promote, and respect the principles of the Code.

4.2 Treat violations of the Code as inconsistent with membership in the ACM.

72

1

Outlines

- Part 1:
  - Email and web security
  - actors
  - Servers security
  - Application security
  - Security measures
- Part 2:
  - Machine learning in Information security
  - Challenges and application
  - Demo

2

Is email secured ?

- Email is a top **threat vector (tool and target)**
  - Emails are critical data, targeted by cyber attackers
  - Emails can also be used to launch cyber attacks
- An email travels between networks and servers, some vulnerable and unsecured, before landing in an inbox. Even though an individual's computer may be secure from an attacker, the network or server the email has to travel through may have been compromised.

3

Type of email attacks

- Phishing/spam
  - A phishing attack targets users by sending them a text, direct message, or email. The attacker pretends to be a trusted individual or institution and then uses their relationship with the target to steal sensitive data like account numbers, credit card details, or login information.
- Spoofing
  - Spoofing is a dangerous email threat because it involves fooling the recipient into thinking the email is coming from someone other than the apparent sender. This makes spoofing an effective business email compromise (BEC) tool.
  - The email platform cannot tell a faked email from a real one because it merely reads the **metadata**—the same data the attacker has changed.

4

Email security best Practices

Spam filter: A spam filter can detect spam and keep it from either hitting your inbox or file it as junk mail.

Email encryption: Email encryption can disguise corporate email by changing communications into a garbled arrangement of letters, numbers, and symbols that someone who intercepts it cannot read.

Antivirus protection: Antivirus protection screens emails and attachments for viruses, providing the user with warnings if anything suspicious is detected.

Secure email gateway (SEG): An SEG filters out potentially dangerous emails according to the settings of an IT administrator.

Multi-factor authentication (MFA): MFA is a key data loss protection and anti-hacking tool because it requires a user to provide more than one authentication factor to prove they should be granted access to a system.

Employee education: Employees can be educated to recognize social engineering, phishing, and other types of attacks that are typically executed using email.

5

Web and mail Security

- Both are now widely used by business, government, individuals
- but Internet & Web are vulnerable
- Challenges
  - integrity
  - confidentiality
  - Availability (denial of service)
  - authentication
- need added security mechanisms

6

6

Web security question

Question: User wants to use internet banking and email, wants to be able to check balance and emails anywhere in the world, wants to be able to transfer money and make payments or send received emails,
what kind of security safeguards need to be in place?

- Prevent interception by using encryption
  PKI is expensive (computationally) try to use symmetric key encryption
- If the client is to use/access resources, Authenticate Client
- Prove integrity of data by using hash algorithms
- Give user appropriate access by using an access control mechanism

7

7

The Web/mail Server

- Entry point for clients
  - To a variety of services
  - Customized for clients (e.g., via cookies)
  - Supported by complex backend applications (e.g.,databases)
- Target of attackers
  - Servers use common protocol
  - Servers support a wide range of user inputs
  - Running with high privilege
- Web servers need to be usable by the public and therefore accessible to the masses, but at the same time to be secure (which can be in conflict with the former goal)
- Q: How does this impact?
  - Vulnerabilities, Threats, Risks

8

8

Risks affecting Web/mail Servers

1. **Defects and misconfiguration risks**

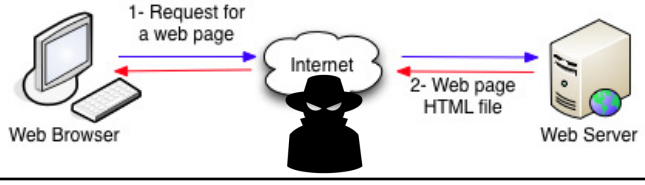
   Steal information from the server, run scripts or executable remotely, enumerate servers, and carry out a denial of service (DoS)

2. **Browser- and network-based risks**

   Risks in this type include an Attacker capturing network traffic between the client (web Browser) and the server

3. **Browser or client-side risks**

   Risks that affect the user's system directly, such as crashing the browser, stealing information, infecting the system, or having some impact on the system.



9

Vulnerabilities of Web Servers

- Same vulnerabilities as any other server + vulnerabilities associated with hosting content
- Can be the only face of the company that have no traditional location (e.g. amazon and Ebay)

1. Improper or poor Web design

   Can sometimes observe sensitive items by viewing the source code of the page

10

Source Code Example

```
<form method="post" action="../../cgi-bin/formMail.pl">

<!--Regular FormMail options---->

<input type=hidden name="recipient" value="someone@someplace.com">
<input type=hidden name="subject" value="Message from website visitor">
<input type=hidden name="required" value="Name,Email,Address1,City,State,Zip,Phone1">
<input type=hidden name="redirect" value="http://www.someplace.com/received.htm">
<input type=hidden name="servername" value="https://payments.someplace.com">
<input type=hidden name="env_report" value="REMOTE_HOST, HTTP_USER_AGENT">
<input type=hidden name="title" value="Form Results">
<input type=hidden name="return_link_url" value="http://www.someplace.com/main.html">
<input type=hidden name="return_link_title" value="Back to Main Page">
<input type=hidden name="missing_fields_redirect" value="http://www.someplace.com/
error.html">
<input type=hidden name="orderconfirmation" value="orders@someplace.com">
<input type=hidden name="cc" value="j.halak@someplace.com">
<input type=hidden name="bcc" value="c.price@someplace.com">

<!--Courtesy Reply Options-->
```

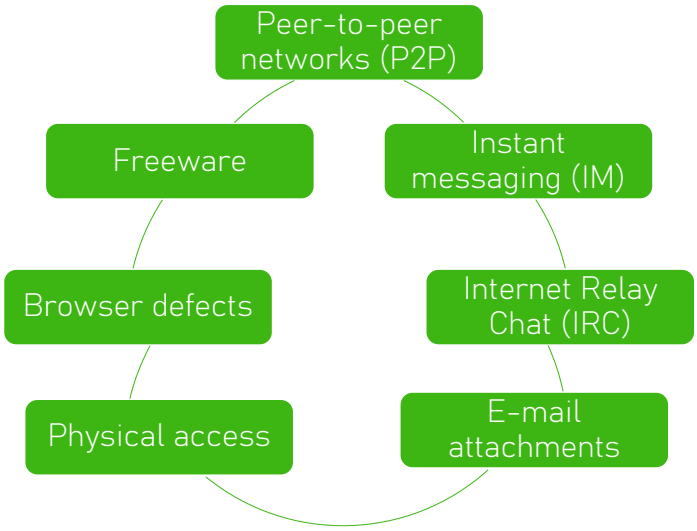
11

Web/mail Server Vulnerabilities

2. Denial of service (DoS) attack
3. Distributed denial of service (DDoS) attack
4. Structured Query Language (SQL) injections
5. Buffer overflow
6. Banner information
7. Permissions
8. Error messages
9. Unnecessary features
10. User accounts

12

Spyware Methods of Infection



13

Web application : mail apps

- Designed to be accessed from a web browser or similar client application that uses HTTP protocol to exchange information between client and server
- More and more popular, E.g. Sharepoint, moodle, GoogleDoc…etc

14

14

Web Application Vulnerabilities

- Insecure logon systems
- Scripting errors
- Session management issues
  - Long-lived sessions
  - Logout features
  - Insecure or weak session identifiers
  - Granting session IDs to unauthorized users
  - Absent or inadequate password change controls
  - Inclusion of unprotected information in cookies
- Encryption weaknesses: Weak ciphers and vulnerable software

15

Simple Mail Transfer Protocol (SMTP, RFC 822)

- SMTP Limitations – Can not transmit, or has a problem with:
  - executable files, or other binary files (jpeg image)
  - "national language" characters (non-ASCII)
  - messages over a certain size
  - ASCII to EBCDIC translation problems
  - lines longer than a certain length (72 to 254 characters)

16

Security measures

17

17

Clear-Text Vs Encrypted Protocols

- Clear-text Protocols
  - Are human readable
  - FTP, Telnet, Simple Mail Transfer Protocol (SMTP), HTTP, Post Office Protocol 3 (POP3), Internet Message Access Protocol (IMAPv4), Network Basic Input/Output System (NetBIOS), Simple Network Management Protocol (SNMP)
- Encrypted Protocols
  - Are not human readable
  - Secure Shell (SSH), SSH File Transfer Protocol (SFTP), HTTP Secure (HTTPS), Simple Mail Transfer Protocol Secure (SMTPS)

18

Encryption in Modern Computing Systems

- Uses of encryption for security:
  - Over the wire: Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Internet Protocol security (IPsec), Virtual Private Network (VPN)
  - E-mail via Pretty Good Privacy (PGP)/GNU Privacy Guard (GPG) and Secure/Multipurpose Internet Mail Extensions (S/MIME)

19

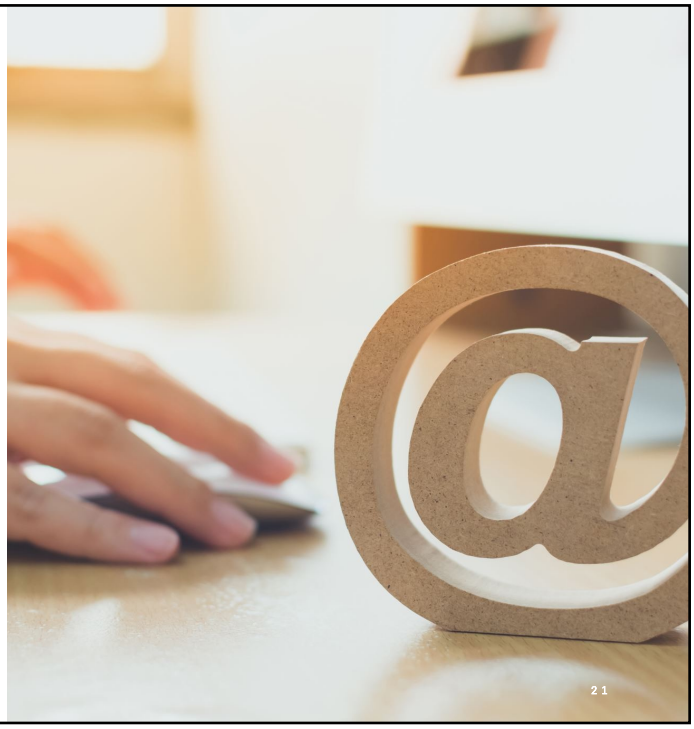
Cryptanalysis Tools

- Pretty Good Privacy (PGP)
  - It's an original accessible, secure encryption tool used in most environments.
  - It uses public or private key pairs, with users exchanging public keys.
  - It provides message authentication and integrity checking.
  - PGP trust is based on a "web of trust", with others signing keys.

20

S/MIME

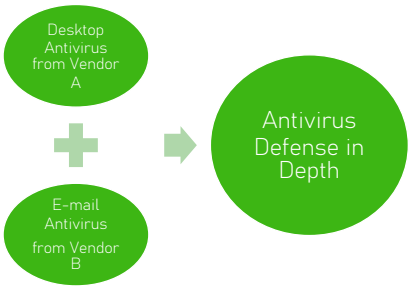
- Secure/Multipurpose Internet Mail Extension
- S/MIME emerging as the industry standard.
- PGP for personal e-mail security
- Functions:
  - **Enveloped Data**
  - **Signed Data**
  - **Clear-Signed Data:**
  - **Signed and Enveloped Data**



21

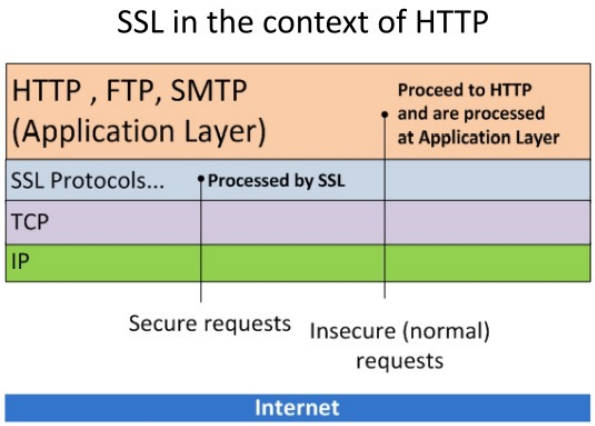
Building Upon Layered Security

- Layered only provides breadth
- Depth=overlapping countermeasures at each layer
- Can be from multiple vendors
  If one is good two must be better
  Different AV patterns=higher chance for detection



22

HTTPS (1/2)



23

23

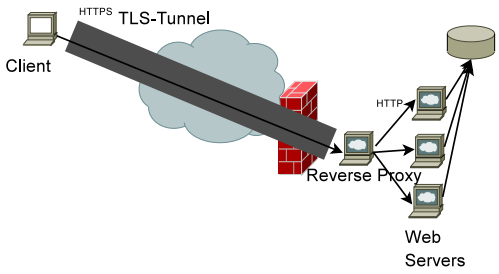
HTTPS (2/2)

- HTTPS (HTTP over SSL)

  combination of HTTP & SSL/TLS to secure communications between browser & server
  - documented in RFC2818
  - no fundamental change using either SSL or TLS
- use https:// URL rather than http://

  and port 443 rather than 80
- encrypts

  URL, document contents, form data, cookies, HTTP headers



24

24

SSL - Secure Socket Layer

Goal

Secure exchange of data over the Internet (TCP / IP network) between a client and a server.

Functionalities

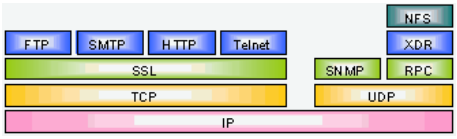
- Authentication of the server (and the client)
- Data encryption
- Non-repudiation
- Data integrity
- Data confidentiality

25

25

What is SSL ? (2/3)

- *Secure Socket Layer*: developed by Netscape (Elgamal is considered as the inventor of SSL)
- Cryptography protocol to secure connection between applications
- In every SSL session, the server MUST authenticate itself to the client
- SSL is a means for the server to prove its identity to the client
- Authentication performed with **public-key cryptography**,
- Data confidentiality and integrity ensured with **symmetric-key cryptography**.



26

26

SSL/TLS applications

- Secure e-commerce
- Secure emails
- Secure electronic banking

27

27

Recommended Web Sites

- PGP home page: www.pgp.com
- MIT distribution site for PGP
- S/MIME Charter
- S/MIME Central: RSA Inc.'s Web Site

28

Machine learning in Information security

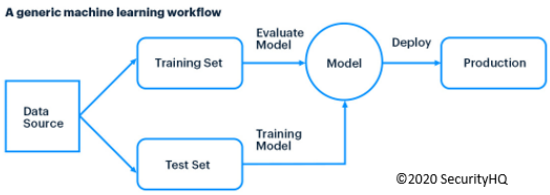
- In the Cambridge Dictionary ML is referred to as

  'The process of computers changing the way they carry out tasks by learning from new data, without a human being needing to give instructions in the form of a program'.

- Generally speaking, ML relies on mathematical models which are built by analysing patterns in datasets. These patterns are then used to make predictions on new input data.

29

Classes of machine Learning



- Supervised learning
  - The machine learns from training data, and maps out inputs and outputs, based on rules provided in said training data, and from inferred functions.
  - the dataset is labelled, wherein there is a target variable. The value of which the ML model learns to predict, using different algorithms. For instance, it may do this based on IP address location, frequency of web requests and so on. From this, an ML model can then predict if the IP was part of say a Distributed Denial-of-service (DDoS) attack, and more.
- Unsupervised learning

30

Classes of machine Learning

- Supervised learning
- Unsupervised learning
  - There is no labelled data, thereby, no prediction of a target variable.
  - Tries to find interesting associations, or patterns, within a dataset. For instance, clustering can be applied in user analytics where application users can be grouped together. By doing this, it is possible to see what data should belong to a specific group, or not.

31

Applications of ML in cyber security

- Task automation
  - Referred to as AutoML. AutoML signifies when repetitive tasks involved in development are automated to specifically aid the productivity of the analysts, data scientists and developers.
- Threat detection and classification
  - Machine learning algorithms are used in applications to detect and respond to attacks.
  - achieved by analysing data sets of security events and identifying patterns of malicious activities. ML works so that when similar events are detected, they are **automatically dealt with by the trained ML model**.
- Phishing analysis and detection
- Network risk analysis
  - ML can be used to analyse previous cyber-attack datasets and determine which areas of networks were mostly involved in particular attacks. This score can help quantify the likelihood, and impact of an attack, with respect to a given network area

32

Other applications of ML in cybersecurity

- Complete analysis of threat incidents and investigation.
- Threat forecasting
- Retrieve the affected systems, examine the root causes of the attack, and improving the security system.
- Monitoring of security

33

Signature-based IDS using ML algorithms

- Signature-based IDS using ML algorithms which includes Decision Trees (DT), Random Forest(RF), Hidden Markov Models (HMMs), Naive Bayes(NB) and Support Vectors Machine (SVM).
- The Snort is an open source framework to prevent suspicious behaviour. It applies rules that help to identify malicious activity in networks and alarm users to take actions.
- Although the snort framework was slow by matching features (rules), decision trees were employed to reduce this limitation by modifying the snort's detection engine with decision trees classifiers by Kruegel and Toth research. The research of Kruegel and Toth had started with clustering to decrease the number of comparisons (matching). After that, a decision tree was performed to select most features relative to rules to obtain better performance quickly.

Kruegel, C., Toth, T. (2003). Using Decision Trees to Improve Signature-Based Intrusion Detection. In: Vigna, G., Kruegel, C., Jonsson, E. (eds) Recent Advances in Intrusion Detection. RAID 2003. Lecture Notes in Computer Science, vol 2820. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-45248-5_10

34

Anomaly-based IDS using ML algorithms

- Ahmim et al. used several classifiers that depend on decision tree and rules-based by combining different algorithms to classify network traffic into either attack or normal and then combined the results as inputs toward the Forest PA algorithm
- In addition, a data normalization process was applied on the CIC-IDS2017 dataset, and preprocessing data were executed, which includes removing redundant rows, null or infinity values.
- The CIC-IDS2017 dataset contains 2,830,743 rows distributed across eight files with six categories, which are: DOS, PortScan, Bot, Brute-Force, Web Attack, and Infiltration, with seventy-nine features.
- The experimental results computed accuracy, detection rate, false alarm rate and time, where the values were better than Jrip, J48, Naive Bayes, and Random Forest algorithms according to the CIC-IDS2017 categories.

A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour and H. Janicke, "A Novel Hierarchical Intrusion Detection System Based on Decision Tree and Rules-Based Models," 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2019, pp. 228-233, doi: 10.1109/DCOSS.2019.00059.

35

Datasets used in IDS

- KDD CUP 99
  - Constructed by Darp'98, 7 weeks of network traffic, 5million records, 24 attack types, has many issues (redundant data and no official split)
- NSL KDD CUP
  - New version derived from KDD CUP99, solves the issues of KDD CUP 99. by the Canadian Institute for Cybersecurity (CIC) https://www.unb.ca/cic/
- CIC-IDS2017
  - One of the most used dataset, it was created using two separate networks; the Victim network and the attack network

36

IDS and IPS

IDS: Intrusion Detection System
- IDS functions
- Detection approaches

IPS: Intrusion Prevention System

37

What is an intrusion ?

Intrusion: A set of actions aimed to compromise the security goals: **Integrity**, **confidentiality**, or **availability**, of a computing and networking resource

Intrusion detection: The process of **identifying** and **responding** to intrusion activities

Intrusion prevention: Extension of IDS with exercises of access control to **protect** computers from exploitation

38

Intrusion detection system

IDS or IPS applications monitor system behaviour to watch for anomalies.

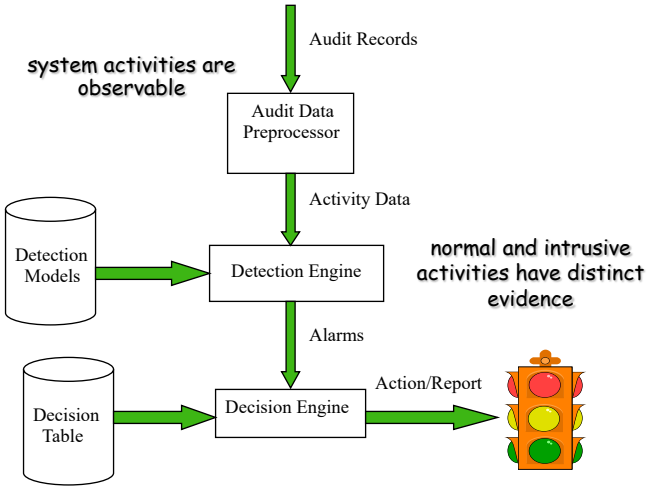
Activity is suspicious if it:

1. Matches a pattern for known malicious activity:
   Attacks such as overwriting many files, contacting all ports at a given network address, or transferring many files out of the local network.

2. Differs significantly from previous patterns of use:
   Can signal a different person controlling a computer, or mark a shift in computer needs.

39

Components of Intrusion Detection System



40

IDS functions

1. **Monitoring** users and system activity
2. **Auditing** system configuration for vulnerabilities and misconfigurations
3. **Assessing** the integrity of critical system and data files
4. **Recognizing** known attack patterns in systems activity
5. **Identifying** abnormal activity through statistical analysis
6. **Managing** audit trails and highlighting user violation of policy or normal activity
7. **Correcting** system configuration errors
8. **Installing** and operating traps to record information about intruders

41

Level of Monitoring

- Which types of events to monitor?
  - OS system calls
  - Command line
  - Network data (e.g., from routers and firewalls)
  - Keystrokes
  - File and device accesses
  - Memory accesses
- Auditing / monitoring should be scalable

42

Types of IDS

Analysis approach

- Misuse detection (a.k.a. signature-based)
- Anomaly detection (a.k.a. statistical-based)

Deployment approach

- Network based IDS

  IDSes that monitor network links and backbones looking for attack signatures are called *network-based IDSes*.

- Host based IDS

  IDS that operate on hosts and defend and monitor the operating and file systems for signs of intrusion and are called *host based IDSes*.

- *Distributed IDS*

  Groups of IDSes functioning as remote sensors and reporting to a central management station are known as distributed IDSes (DIDSes).

- A *gateway IDS*

  It is *a* network IDS deployed at the gateway between your network and another network, whereas **Application IDS** understand and parse application specific traffic and underlying protocol

43

Intrusion prevention system

IPS response is not just an alarm, it could be:

- Cutting a user access
- Reject traffic from certain addresses
- Stopping access to a file or program
- Block the attack by redirecting traffic to a monitoring host (**honeypot**), discarding the traffic or terminating the session
- …

44

Demo

- CIC dataset

47

ICS UNIT 5
Cybersecurity Techniques, Tools and Laws

Introduction, Proxy servers and Anonymizers, Phishing, Password Cracking tools, Key-loggers and Spywares, DoS and DDoS, Viruses, Worms, Trapdoors, Salami attack, Man-in-the- middle attacks, Covert channels, SQL injection, Cyber Security Safeguards- Overview, Access control, Audit, Authentication, Biometrics. Cybercrime and Legal perspectives, Cyber laws Indian context, The Indian IT Act- Challenges, Amendments, Challenges to Indian Law and cybercrime Scenario in India, Indian IT Act and Digital Signatures.

Stages of an attack on network

1. **Initial covering:** two stages
    1. Reconnaissance- social networking websites
    2. Uncovers information on company's IP
2. **Network probe:**
    1. Ping sweep- seek out potential targets
    2. Port scanning
3. **Crossing the line toward electronic crime:**
    1. Commits computer crime by exploiting possible holes on the target system

Stages of an attack on network

4**. Capturing the network:**

- attackers attempts to own the network
- uses tools to remove any evidence of the attack
- trojan horses, backdoors

5**. Grab the data:**

- attacker has captured the network
- steal confidential data, customer CC information, deface webpages…

6. Covering the attack:

- extend misuse of the attack without being detected.
- start a fresh reconnaissance to a related target system
- continue use of resources
- remove evidence of hacking

Various tools used for the attack

- Proxy severs and Anonymizers
- Phishing
- Password cracking
- Keyloggers and spywares
- Virus and Worms
- Trojan horses and Backdoors
- Steganography
- SQL injection
- DoS and DDoS attack tools
- Buffer overflow

1. Proxy severs and Anonymizers

- A **proxy server** is a dedicated computer or a software system running on a computer that acts as an intermediary between an endpoint device, such as a computer, and another **server** from which a user or client is requesting a service.
- A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.

Purpose of a proxy server

- **Improve Performance:**
- **Filter Requests**
- **Keep system behind the curtain**
- **Used as IP address multiplexer**
- **Its Cache memory can serve all users**

Attack on this: the attacker first connects to a proxy server- establishes connection with the target through existing connection with the proxy.

An Anonymizer

- An **anonymizer** or an **anonymous proxy** is a tool that attempts to make activity on the Internet untraceable.
- It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet.
- It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information.
- For example, large news outlets such as CNN target the viewers according to region and give different information to different populations

2. Phishing

- Stealing personal and financial data
- Also can infect systems with viruses
- A method of online ID theft

How Phishing works?

1. Planning : use mass mailing and address collection techniques- spammers
2. Setup : E-Mail / webpage to collect data about the target
3. Attack : send a phony message to the target
4. Collection: record the information obtained
5. Identity theft and fraud: use information to commit fraud or illegal purchases

3. Password Cracking

- **password cracking** is the process of recovering passwords from data that have been stored in or transmitted by a computer system.
- A common approach (brute-force attack) is to try guesses repeatedly for the password and check them against an available cryptographic hash of the password.

The purpose of password cracking

- help a user recover a forgotten password
- to gain unauthorized access to a system,
- or as a preventive measure by System Administrators to check for easily crackable passwords

Manual Password Cracking Algorithm

- Find a valid user
  - •Create a list of possible passwords
  - •Rank the passwords from high probability to low
  - •Key in each password
  - •If the system allows you in - Success
  - •Else try till success

examples of guessable passwords

- Blank
- Words like “passcode” ,”password”, “admin”
- Series of letters “QWERTY”
- User’ s name or login name
- Name of the user’s friend/relative/pet
- User’s birth place, DOB
- Vehicle number, office number ..
- Name of celebrity
- Simple modification of one of the precedings, suffixing 1 …

Categories of password cracking attacks:

- Online attacks
- Offline attacks
- Non-electronic attacks
  - Social engineering
  - Shoulder surfing
  - Dumpster diving

Online attacks

- An attacker may create a script- automated program- to try each password
- Most popular online attack;- man-in-the-middle attack or bucket-brigade attack
- Used to obtain passwords for E-mail accounts on public websites like gmail, yahoomail
- Also to get passwords for financial websites

Offline attacks

- Are performed from a location other than the target where these passwords reside or are used
- Require physical access to the computer and copying the password

Types of Password Attacks

- Password Guessing
  - Attackers can guess passwords locally or remotely using either a manual or automated approach
- Dictionary attacks
  - work on the assumption that most passwords consist of whole words, dates, or numbers taken from a dictionary.
- Hybrid password
  - assume that network administrators push users to make their passwords at least slightly different from a word that appears in a dictionary.

Weak passwords

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "<Company Name>", "sanjose", "sanfran" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1,1secret

Strong Passwords

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, @#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line.
- Try to create passwords that can be easily remembered.
- One way to do this is create a password based on a song title, affirmation, or other phrase.
- For example, the phrase might be: "This May Be One Way To Remember"
- and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

4. keyloggers

- **Keystroke logging**, often referred to as **keylogging** or **keyboard capturing**, is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.
- It has uses in the study of human–computer interaction.
- There are numerous keylogging methods, ranging from hardware and software-based approaches to acoustic analysis.

Software-based keyloggers

- Software-based keyloggers use the target computer's operating system in various ways, including: imitating a virtual machine, acting as the keyboard driver (kernel-based), using the application programming interface to watch keyboard strokes (API-based), recording information submitted on web-based forms (Form Grabber based) or capturing network traffic associated with HTTP POST events to steal passwords (Packet analyzers).
- Usually consists of two files DLL and EXE

Hardware keyloggers

- installing a hardware circuit between the keyboard and the computer that logs keyboard stroke activity (keyboard hardware).
- Target- ATMs

Acoustic keylogging

- Acoustic keylogging monitors the sound created by each individual keystroke and uses the subtly different acoustic signature that each key emits to analyze and determine what the target computer’s user is typing.

AntiKeylogger

- An **anti-keylogger** (or **anti–keystroke logger**) is a type of software specifically designed for the detection of keystroke logger software; often, such software will also incorporate the ability to delete or at least immobilize hidden keystroke logger software on your computer.

Benefits of Antikeyloggers

- **Keylogger removal** – It removes keyloggers that are running or being launched in your computer or mobile.

- **Security** – It ensures us that confidential information would not be stolen from our hard drives or computer units, and, prevents us from being a victim of cyber crimes and thefts. Financial institutions are usually targets of keyloggers. Anti-loggers perform regular scans in any computer.

- **Keylogger detector** – Apart from the "disabling" feature, the anti-keylogger provides a warning whenever a key logging activity is being launched in your unit.

- **Protects privacy** – As stated in reviews, it prevents your data or activities from being revealed through these keyloggers. Your messages, calls, videos, downloaded files, emails, website visits and other online transactions remain private unless you would reveal them yourself.

- **User friendly and reliable** – The anti-keylogger is easy to use and highly reliable

Spywares

- **Spyware** is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge

5. Virus and Worms

- A computer virus is a **malware** program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "**infected**".

Some typical virus actions

- Display a message to prompt an action
- Delete files in the system
- Scramble data on a hard disk
- Cause erratic screen behavior
- Halt the system
- Replicate themselves to propagate further harm

Virus spread through

- The internet
- A stand alone PC
- Local networks

Difference between virus and worm

	Computer Virus	Computer Worm
How does it infect a computer system?	It inserts itself into a file or executable program.	It exploits a weakness in an application or operating system by replicating itself.
How can it spread?	It has to rely on users transferring infected files/programs to other computer systems.	It can use a network to replicate itself to other computer systems without user intervention.
Does it infect files?	Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.	Usually not. Worms usually only monopolize the CPU and memory.
whose speed is more?	virus is slower than worm.	worm is faster than virus. E.g.The code red worm affected 3 lack PCs in just 14 Hrs.
Definition	The virus is the program code that attaches itself to application program and when application program run it runs along with it.	The worm is code that replicate itself in order to consume resources to bring it down.

Types of viruses

- Boot sector viruses
- Program viruses
- Multipartite viruses
- Stealth viruses
- Polymorphic viruses
- Macroviruses
- Active X and Java contrl

Boot sector viruses

- A boot sector virus is a computer virus that infects a storage device's master boot record (MBR).
- It is not mandatory that a boot sector virus successfully boot the victim's PC to infect it.
- As a result, even non-bootable media can trigger the spread of boot sector viruses.
- These viruses copy their infected code either to the floppy disk's boot sector or to the hard disk's partition table. During start-up, the virus gets loaded to the computer's memory. As soon as the virus is saved to the memory, it infects the non-infected disks used by the system.
- The propagation of boot sector viruses has become very rare since the decline of floppy disks. Also, present-day operating systems include boot-sector safeguards that make it difficult for boot sector viruses to infect them.

Program viruses

- A program virus becomes active when the program file (usually with extensions .BIN, .COM, .EXE, .OVL, .DRV) carrying the virus is opened.
- Once active, the virus will make copies of itself and will infect other programs on the computer.

Multipartite viruses

- A multipartite virus is a fast-moving virus that uses file infectors or boot infectors to attack the boot sector and executable files simultaneously.
- Most viruses either affect the boot sector, the system or the program files.
- The multipartite virus can affect both the boot sector and the program files at the same time, thus causing more damage than any other kind of virus.
- When the boot sector is infected, simply turning on the computer will trigger a boot sector virus because it latches on to the hard drive that contains the data that is needed to start the computer. Once the virus has been triggered, destructive payloads are launched throughout the program files.
- A multipartite virus infects computer systems multiple times and at different times. In order for it to be eradicated, the entire virus must be removed from the system.
- A multipartite virus is also known as a hybrid virus.

Stealth viruses

- A stealth virus is a hidden computer virus that attacks operating system processes and averts typical anti-virus or anti-malware scans. Stealth viruses hide in files, partitions and boot sectors and are adept at deliberately avoiding detection.

  Stealth virus eradication requires advanced anti-virus software or a clean system reboot.

Polymorphic viruses

- A polymorphic virus is a complicated computer virus that affects data types and functions.
- It is a self-encrypted virus designed to avoid detection by a scanner.
- Upon infection, the polymorphic virus duplicates itself by creating usable, albeit slightly modified, copies of itself.

- Polymorphism, in computing terms, means that a single definition can be used with varying amounts of data. In order for scanners to detect this type of virus, brute-force programs must be written to combat and detect the polymorphic virus with novel variant configurations.

Macroviruses

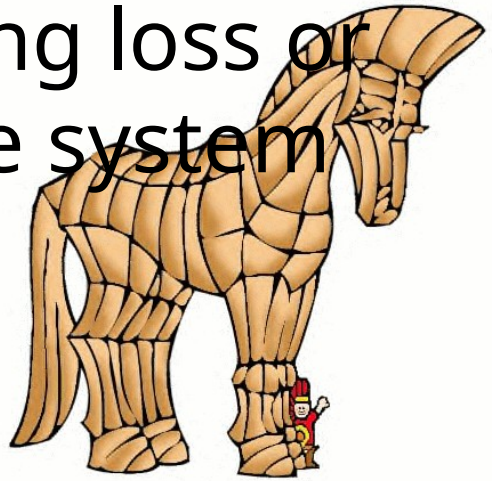
- **A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it.**

Active X and Java contrl

- ActiveX and Java were created for web page designers to incorporate a wide array of impressive effects on web pages, giving movement and added dimension to the previously "flat" web pages.
- To operate properly, these ActiveX controls and Java applets need to gain access to your hard disk. Insufficient memory and bandwidth problems necessitate this approach. Although this desktop access provides a wealth of beneficial applications of these controls and applets, malicious code developers have the same access. They are now using it to read and delete or corrupt files, access RAM, and even access files on computers attached via a LAN.

6. Trojan horses and Backdoors

- A **Trojan horse**, or **Trojan**, in computing is generally a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm



Examples of threats by trojans

- Erase, overwrite or corrupt data on a computer
- Help to spread other malware such as viruses- dropper trojan
- Deactivate or interface with antivirus and firewall programs
- Allow remote access to your computer- remote access trojan
- Upload and download files
- Gather E-mail address and use for spam
- Log keystrokes to steal information – pwds, CC numbers
- Copy fake links to false websites
- slowdown, restart or shutdown the system
- Disable task manager
- Disable the control panel

Backdoors

- A **backdoor** in a computer system is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected.
- Also called a *trapdoor*. An undocumented way of gaining access to a program, online service or an entire computer system.
- The backdoor is written by the programmer who creates the code for the program. It is often only known by the programmer. A backdoor is a potential security risk.

Functions of backdoors

Allows an attacker to

- create, delete, rename, copy or edit any file
- Execute commands to change system settings
- Alter the windows registry
- Run, control and terminate applications
- Install arbitrary software and parasites
- Control computer hardware devices,
- Shutdown or restart computer

Functions of backdoors

- Steals sensitive personal information, valuable documents, passwords, login name...
- Records keystrokes, captures screenshots
- Sends gathered data to predefined E-mail addresses
- Infects files, corrupts installed apps, damages entire system
- Distributes infected files to remote computers
- Installs hidden FTP server
- Degrades internet connection and overall system performance
- Decreases system security
- Provides no uninstall feature, hides processes, files and other objects

Examples of Backdoor trojans

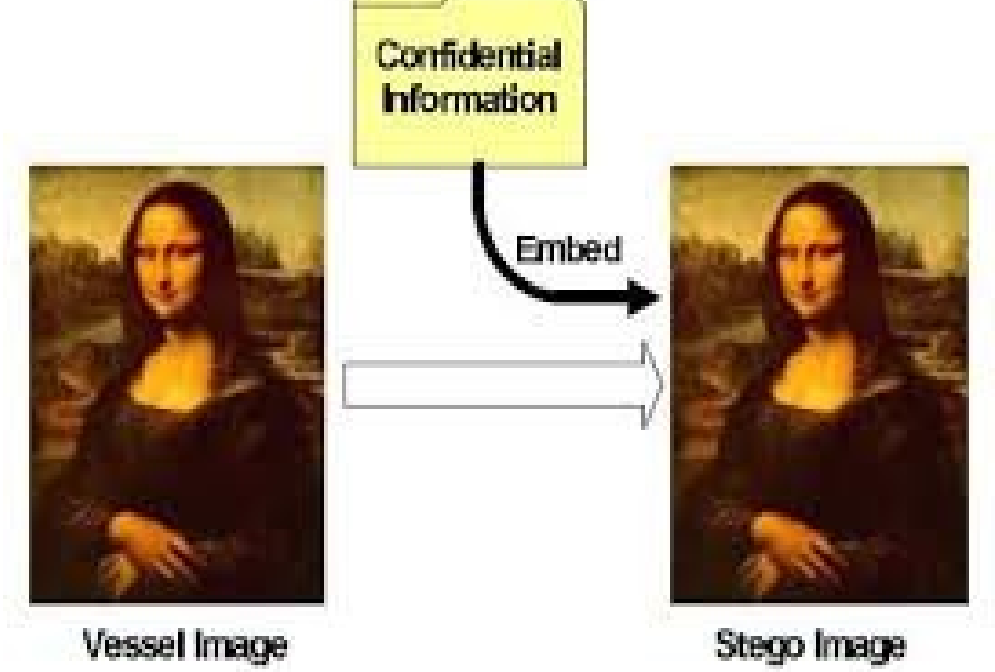
- **Back Orifice** : for remote system administration
- **Bifrost** : can infect Win95 through Vista, execute arbitrary code
- **SAP backdoors** : infects SAP business objects
- **Onapsis Bizploit:** Onapsis Bizploit is an SAP penetration testing framework to assist security professionals in the discovery, exploration, vulnerability assessment and exploitation phases of specialized SAP security assessment

How to protect from Trojan Horses and backdoors

- Stay away from suspect websites/ links
- Surf on the web cautiously : avoid P2P networks
- Install antivirus/ Trojan remover software

7. Steganography

- Steganography (from Greek steganos, or "covered," and graphie, or "writing") is the hiding of a secret message within an ordinary message and the extraction of it at its destination.
- Steganography takes cryptography a step farther by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data.
- Other names: data hiding, information hiding, digital watermarking


Confidential Information
Embed
Vessel Image
Stego Image


ORIGINAL IMAGE
IMAGE WITH HIDDEN DATA
R202 G212 B75
R198 G99 B59
R209 G124 B65
R215 G135 B70
R214 G129 B72
R223 G152 B64
R227 G168 B78
R227 G171 B86
R207 G120 B70
R203 G113 B75
R198 G98 B58
R208 G126 B67
R215 G134 B70
R215 G129 B75
R223 G153 B67
R226 G168 B81
R226 G170 B88
R206 G120 B71

digital watermarking

- Digital watermarking is the act of hiding a message (trademark) related to a digital signal (i.e. an image, song, video) within the signal itself.
- It is a concept closely related to steganography, in that they both hide a message inside a digital signal.
- However, what separates them is their goal.
- Watermarking tries to hide a message related to the actual content of the digital signal,
- while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.

Difference between steganography and ***cryptography***

- Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists.
- In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world.
- Due to this, Steganography removes the unwanted attention coming to the hidden message.
- Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content.
- By combining Steganography and Cryptography one can achieve better security.

Steganalysis

- **Steganalysis** is the study of detecting messages hidden using steganography;
- The goal of steganalysis is to identify suspected packages, determine whether or not they have a payload encoded into them, and, if possible, recover that payload.

8.DoS and DDoS attacks

- In computing, a **denial-of-service** (**DoS**) or distributed **denial-of-service** (**DDoS**) **attack** is an attempt to make a machine or network resource unavailable to its intended users.
- A **DoS attack** generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Symptoms of DoS attacks

- Slow network performance
- Unavailability of a particular website
- Inability to access any website
- Dramatic increase in number of Spam E-mails received

A DoS attack may do the following

- Flood the traffic, thereby preventing network traffic
- Disrupt connections between two systems- preventing access to service
- Prevent a particular individual from accessing a service
- Disrupt service to a specific system or person

Classification of DoS

- Bandwidth attacks
- Logic attacks
- Protocol attacks
- Unintentional DoS attack

Bandwidth attacks

- The most common DoS attacks
- target the computer's network bandwidth or connectivity.
- Bandwidth attacks flood the network with such a high volume of traffic, that all available network resources are consumed and legitimate user requests can not get through.

Logic attacks

- An attacker sends more requests to a server than it can handle, usually in a relentless manner, until the server buckles and gives in to the attacker. Once this type of attack ends, the server can return to normal operation.
- Generally, a logic attack requires your server to have a discoverable weakness that the attacker can locate and then use against it.
- Because of this prerequisite, it is usually easy to prevent by keeping your server software and hardware up-to-date with the latest security patches and firmware respectively

Protocol attacks

- Denial of service attacks may take advantage of certain standard protocol features.
- Several attacks capitalize on the fact that IP source addresses can be spoofed.
- In addition, connection depletion attacks take advantage of the fact that many connection-oriented protocols require servers to maintain state information after a connection request is made but before the connection is fully established.
- The most common connection depletion attack is SYN flooding

Unintentional DoS attack

- This describes a situation where a website ends up denied, not due to a deliberate attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity.
- This can happen when an extremely popular website posts a prominent link to a second, less well-prepared site, for example, as part of a news story.

Types or levels of DoS attacks

- Flood attack
- Ping of death attack
- SYN attack
- Teardrop attack
- Smurf attack
- nuke

Flood attack

- Flooding is a Denial of Service (DoS) attack that is designed to bring a network or service down by flooding it with large amounts of traffic.
- Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests.
- By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the hosts memory buffer. Once this buffer is full no further connections can be made, and the result is a Denial of Service.

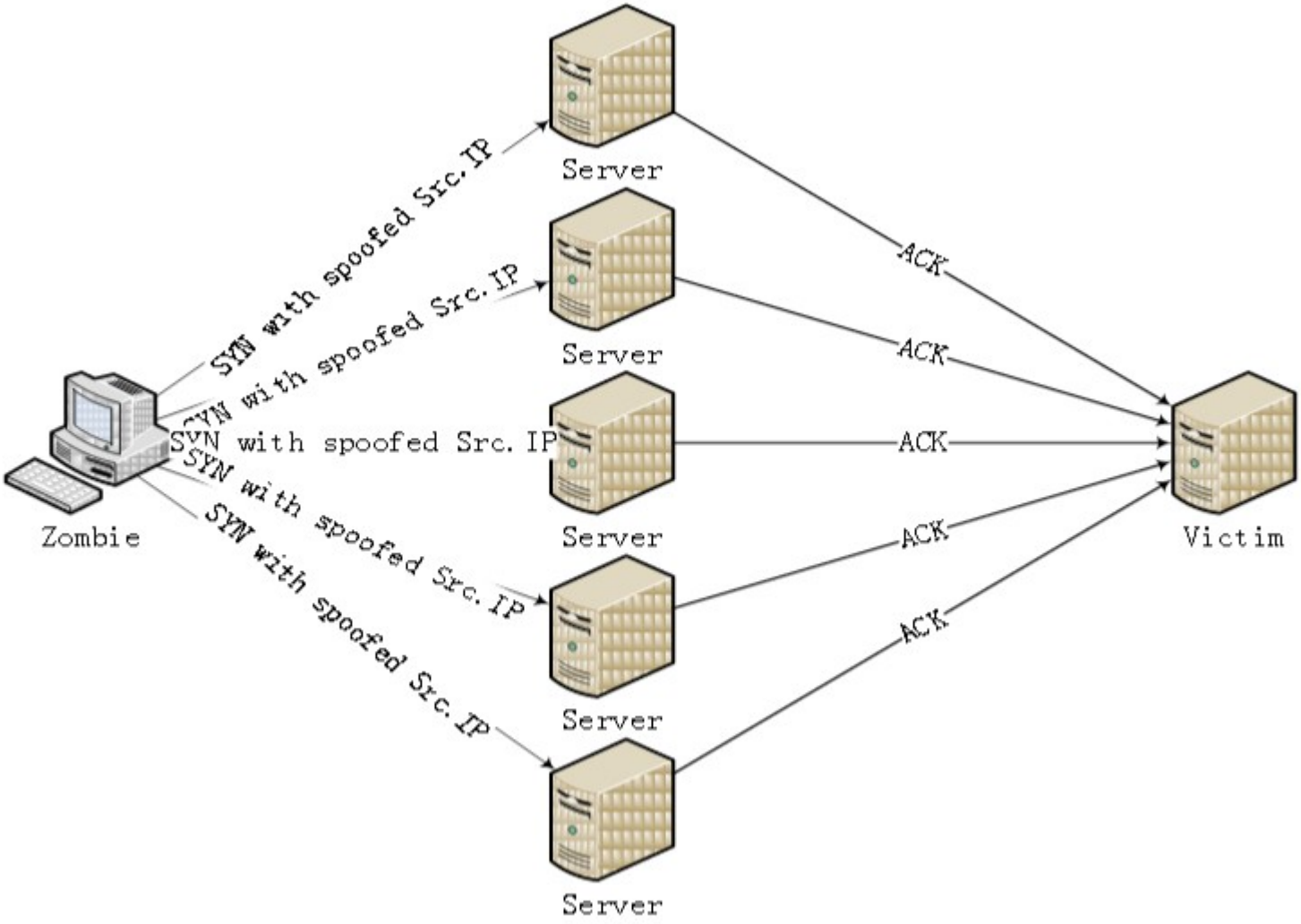
ping of death attack

- ping of death is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol.

SYN attack

- A SYN flood occurs when a host sends a flood of TCP/SYN packets, often with a forged sender address.
- Each of these packets are handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet (Acknowledge), and waiting for a packet in response from the sender address (response to the ACK Packet).
- However, because the sender address is forged, the response never comes. These half-open connections saturate the number of available connections the server can make, keeping it from responding to legitimate requests until after the attack ends

SYN attack


Server
Server
Server
Server
Server
SYN with spoofed Src. IP
SYN with spoofed Src. IP
SYN with spoofed Src. IP
SYN with spoofed Src. IP
SYN with spoofed Src. IP
ACK
ACK
ACK
ACK
ACK
Zombie
Victim

Teardrop attack

- A teardrop attack is a denial of service (DoS) attack conducted by targeting TCP/IP fragmentation reassembly codes.
- This attack causes fragmented packets to overlap one another on the host receipt;
- the host attempts to reconstruct them during the process but fails.
- Gigantic payloads are sent to the machine that is being targeted, causing system crashes.

Smurf attack

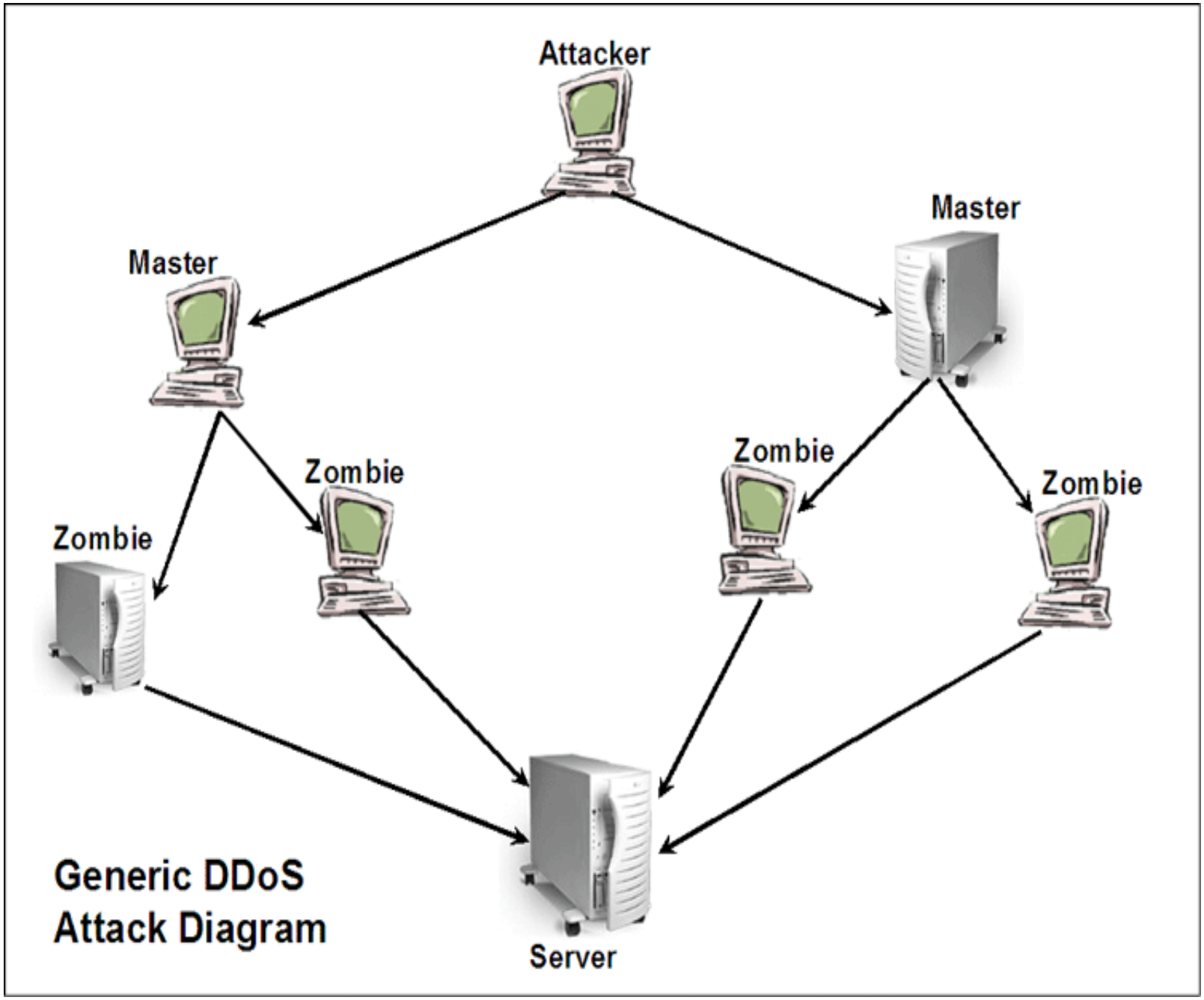
- A smurf attack is a type of denial of service attack in which a system is flooded with spoofed ping messages.
- This creates high computer network traffic on the victim’s network, which often renders it unresponsive.

Nuke

- A Nuke is an old denial-of-service attack against computer networks consisting of fragmented or otherwise invalid ICMP packets sent to the target, achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop.

DDoS attack

- A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
- They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.


Attacker
Master
Master
Zombie
Zombie
Zombie
Zombie
Zombie
Server
Generic DDoS
Attack Diagram

how to prevent dos/ddos attacks

- **Filtering:** Routers at the edge of the network can be trained to spot and drop DDOS connections, preventing them from slowing the network or the server.
- **Moving:** If the attack is pointed at a specific IP address, the site's IP can be changed.
- **Blackholing:** A host may simply "blackhole" a site that is being DDOSed, directing all traffic to it to an address that doesn't exist. This is normally a last resort.

9. SQL Injection

- **SQL injection** is a code **injection** technique, used to attack data-driven applications, in which malicious **SQL** statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- It is the type of attack that takes advantage of improper coding of your web applications that allows hacker to inject SQL commands into say a login form to allow them to gain access to the data held within your database.

What an attacker can do?

* ByPassing Logins : by obtaining username and passwords

* Accessing secret data : reconnaissance

* Adding new data or Modifying contents of website: INSERT/UPDATE

* Shutting down the My SQL server

steps for SQL Injection attack

- **Step 1: Finding Vulnerable Website:**
  - find the Vulnerable websites(hackable websites) using Google Dork list.
  - google dork is searching for vulnerable websites using the google searching tricks
  - use “inurl:” command for finding the vulnerable websites.
- Some Examples:
  inurl:index.php?id=
  inurl:gallery.php?id=
  inurl:article.php?id=
  inurl:pageid=
- **How to use?**
  copy one of the above command and paste in the google search engine box.
  Hit enter.
  You can get list of web sites.
  We have to visit the websites one by one for checking the vulnerability.

- **Step 2: Checking the Vulnerability:**
  - Now we should check the vulnerability of websites.
  - In order to check the vulnerability ,add the single quotes(‘) at the end of the url and hit enter.
- For eg:

  http://www.victimsite.com/index.php?id=2'
  - If the page remains in same page or showing that page not found or showing some other webpages. Then it is not vulnerable.
  - If it showing any errors which is related to sql query, then it is vulnerable.

- **Step 3: Finding Number of columns:**
  - Now we have found the website is vulnerable.
  - Next step is to find the number of columns in the table.
    For that replace the single quotes(') with "order by n" statement
  - Change the n from 1,2,3,4,,5,6,...n. Until you get the error like "unknown column ".
- For eg:

- http://www.victimsite.com/index.php?id=2 order by 1
  http://www.victimsite.com/index.php?id=2 order by 2
  http://www.victimsite.com/index.php?id=2 order by 3
  http://www.victimsite.com/index.php?id=2 order by 4
  .....
  http://www.victimsite.com/index.php?id=2 order by 8(error)

so now x=8 , The number of column is x-1 i.e, 7.

- **Step 4: Displaying the Vulnerable columns:**
  - Using “union select columns_sequence” we can find the vulnerable part of the table. Replace the “order by n” with this statement.
  - And change the id value to negative
  - Replace the columns_sequence with the no from 1 to x-1(number of columns) separated with commas(,).
- For eg:
  if the number of columns is 7 ,then the query is as follow:

- http://www.victimsite.com/index.php?id=-2 union select 1,2,3,4,5,6,7—

Blind SQL injection

- Blind SQL Injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker.
- The page with the vulnerability may not be one that displays data but will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page.
- This type of attack can become time-intensive because a new statement must be crafted for each bit recovered.
- There are several tools that can automate these attacks once the location of the vulnerability and the target information has been established

How to prevent SQL Injection attacks

- Input validation
  - Replace all single quotes to two single quotes
  - Sanitize the input: clean characters like ;, --, select, etc
  - Numeric values should be checked while accepting a query string value
  - Keep all text boxes and form fields short
- Modify error reports
  - SQL errors should not be displayed to the outside world
- Other preventions
  - Never use default system accounts for SQL server 2000
  - Isolate database server and webserver: different machines
  - Extended stored procedures, user defined functions should be moved to an isolated server.

10. Buffer overflow

- In computer security and programming, a **buffer overflow**, or **buffer** overrun, is an anomaly where a program, while writing data to a **buffer**, overruns the **buffer's** boundary and overwrites adjacent memory. This is a special case of violation of memory safety.
- This may result in erratic program behavior
- Buffer overflows are not easy to discover and even when one is discovered, it is generally extremely difficult to exploit.

- In a classic buffer overflow exploit, the attacker sends data to a program, which it stores in an undersized stack buffer. The result is that information on the call stack is overwritten, including the function's return pointer.
- The data sets the value of the return pointer so that when the function returns, it transfers control to malicious code contained in the attacker's data.
- At the code level, buffer overflow vulnerabilities usually involve the violation of a programmer's assumptions.
- Many memory manipulation functions in C and C++ do not perform bounds checking and can easily overwrite the allocated bounds of the buffers they operate upon.
- Even bounded functions, such as strncpy(), can cause vulnerabilities when used incorrectly.
- The combination of memory manipulation and mistaken assumptions about the size or makeup of a piece of data is the root cause of most buffer overflows.

example

- The code in this example also relies on user input to control its behavior, but it adds a level of indirection with the use of the bounded memory copy function memcpy().
- This function accepts a destination buffer, a source buffer, and the number of bytes to copy. The input buffer is filled by a bounded call to read(), but the user specifies the number of bytes that memcpy() copies.

```
... char buf[64], in[MAX_SIZE];
 printf("Enter buffer contents:\n");
read(0, in, MAX_SIZE-1);
printf("Bytes to copy:\n");
scanf("%d", &bytes);
memcpy(buf, in, bytes); ...
```

- **Note:** This type of buffer overflow vulnerability (where a program reads data and then trusts a value from the data in subsequent memory operations on the remaining data) has turned up with some frequency in image, audio, and other file processing libraries.

Types of buffer overflow

- stack-based buffer overflow
- Heap buffer overflow
- NOPs

stack-based buffer overflow

- A stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack
- Attack may exploit this to manipulate the program by
  - Changing the local variable
  - Changing the return address
  - Changing the function pointer or exception handler

heap buffer overflow

- A **heap overflow** is a type of buffer overflow that occurs in the heap data area.
- Heap overflows are exploitable in a different manner to that of stack-based overflows.
- Memory on the heap is dynamically allocated by the application at run-time and typically contains program data.
- Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers.
- The canonical heap overflow technique overwrites dynamic memory allocation linkage (such as malloc meta data) and uses the resulting pointer exchange to overwrite a program function pointer.

NOP-sled

- A NOP-sled is the oldest and most widely known technique for successfully exploiting a stack buffer overflow.
- It solves the problem of finding the exact address of the buffer by effectively increasing the size of the target area.
- To do this, much larger sections of the stack are corrupted with the no-op machine instruction. At the end of the attacker-supplied data, after the no-op instructions, the attacker places an instruction to perform a relative jump to the top of the buffer where the shellcode is located.
- This collection of no-ops is referred to as the "NOP-sled" because if the return address is overwritten with any address within the no-op region of the buffer it will "slide" down the no-ops until it is redirected to the actual malicious code by the jump at the end.

How to minimize buffer overflow

- Assessment of secure code manually
- Disable stack execution
- Compiler tools
- Dynamic run-time checks
- Various tools are used to detect/ defend buffer overflow
  - stackGaurd
  - Propolice
  - LibSafe

IT Act 2000

Amendments in 2008

Information Technology Act 2000

- The Government of India enacted The Information Technology Act with some major objectives which are as follows -

  - To deliver lawful recognition for transactions through electronic data interchange (EDI) and other means of electronic communication, commonly referred to as **electronic commerce** or E-Commerce.
  - The aim was to use replacements of paper-based methods of communication and storage of information.

  - To facilitate electronic filing of documents with the Government agencies and further to amend
    - the Indian Penal Code,
    - the Indian Evidence Act, 1872,

Information Technology Act 2000

- The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000.
- The I. T. Act got the President's assent on June 9, 2000 and it was made effective from October 17, 2000.
- By adopting this Cyber Legislation, India became the 12th nation in the world to adopt a Cyber Law regime.
- It is based on the *United Nations Model Law on Electronic Commerce 1996* (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997

Salient Features of I.T Act 2000

- Digital signature has been replaced with electronic signature to make it a more technology neutral act.
- It elaborates on offenses, penalties, and breaches.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- It defines in a new section that *cyber café is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public*.
- It provides for the constitution of the Cyber Regulations Advisory Committee.
- It is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.

Scheme of I.T Act 2000

- The following points define the scheme of the I.T. Act -
  - The I.T. Act contains **13 chapters** and **90 sections**.
  - The last four sections namely sections 91 to 94 in the I.T. Act 2000 deals with the amendments to the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934 were deleted.

Chapters in the Act

No.	Title	Description
1.	Preliminary	Definitions of terms used in the rest of the document
2.	Digital Signature	Very brief authorization for use of digital signatures for electronic records
3.	Electronic Governance	Provides for the legal recognition of electronic records – especially by Govt. agencies
4.	Attribution, Acknowledgement, and Despatch of Electronic Records	Discusses when an electronic message shall be considered to be “sent” and when it will be considered to be “received”
5.	Secure Electronic Records and Secure Digital Signatures	Discusses (a bit vaguely) what is considered as “secure” electronic records and digital signatures
6.	Regulation of Certifying Authorities	Discusses who can be appointed as a CA, and what their responsibilities and authorities are

Chapters in the Act

No.	Title	Description
7.	Digital Signature Certificates	Who can issue Digital Certificates, and what they should contain and rules for revocation
8.	Duties of Subscribers	Generation or acceptance of the key pair, and reasonable care for securely using it
9.	Penalties and Adjudication	Penalties for damage to computer systems – Rs. 1 crore Failure to furnish information – Rs. 1,50,000 Failure to maintain records – Rs. 10,000 per day Residuary penalty – Rs. 25,000
10.	Cyber Regulations Appellate Tribunal	Establishment, composition and powers of a Cyber Appellate Tribunal to adjudicate in matters related to this Act.

Chapters in the Act

No.	Title	Description
11.	Offences	Tampering with computer source documents – 3 years imprisonment, or fine of Rs. 2 lakhs or both Hacking with computer system – as above Publishing of obscene information – as above
12.	Network Service Providers not to be Liable in Certain Cases	If offence committed without his knowledge or due diligence was exercised.
13.	Miscellaneous	Power of police officer Offences by companies Power of Central and State Governments

- Chapter I – Preliminary
  - 1. Short title, extent, commencement and application. –
  - 2. Definitions. –
- Chapter II Digital Signature
  - 3. Authentication of electronic records. –
- Chapter III – Electronic Governance
  - 4. Legal recognition of electronic records –
  - 5. Legal recognition of digital signatures. –
  - 6. Use of electronic records and digital signatures in Government and its agencies. – (1) Where any law provides for-
  - 7. Retention of electronic records.-
  - 8. Publication of rule, regulation, etc., in Electronic Gazette.-
  - 9. Section 6, 7 and 8 not to confer right to insist document should be accepted in electronic form.-
  - 10. Power to make rules by Central Government in respect of digital signature.-

- Chapter IV – Attribution, Acknowledgement and Despatch of Electronic records
  - 11. Attribution of electronic records.-
  - 12. Acknowledge of receipt.-
  - 13. Time and place of desptach and receipt of electronic record. –
- Chapter V – Secure Electronic records and secure digital signatures
  - 14. Secure electronic record.-
  - 15. Secure digital signature.-
  - 16. Security procedure.-

- Chapter VI – Regulation of Certifying Authorities
  - 17. Appointment of Controller and other officers. –
  - 18. Functions of Controller. –
  - 19. Recognition of foreign Certifying Authorities. –
  - 20. Controller to act as repository. –
  - 21. Licence tissue Digital Signature Certificates. –
  - 22. Application for licence. –
  - 23. Renewal of licence –
  - 24. Procedure for grant or rejection of licence.-
  - 25. Suspension of licence. –
  - 26. Notice of suspension revocation of licence.-
  - 27. Power to delegate –
  - 28. Power to investigate contraventions. –
  - 29. Access to computers and data. –
  - 30. Certifying Authority to follow certain procedures.-
  - 31. Certifying Authority to ensure compliance of the Act, etc.-
  - 32. Display of licence.-
  - 33. Surrender of licence. –
  - 34. Disclosure. –

- Chapter VII – Digital Signature Certificates
  - 35. Certifying authority to issue Digital Signature Certificate. –
  - 36. Representations upon issuance Digital Signature Certificate. –
  - 37. Suspension of Digital Signature Certificate. –
  - 38. Revocation of Digital Signature Certificate. –
  - 39. Notice of suspension or revocation. –
- Chapter VIII – Duties of Subscribers
  - 40. Generating key pair.-
  - 41. Acceptance of Digital Signature Certificate. –
  - 42. Control of private key. –
- Chapter IX – Penalties and Adjudication
  - 43. Penalty for damage to computer, computer system, etc.-
  - 44. Penalty for failure to furnish information, return, etc.-
  - 45. Residuary penalty.-
  - 46. Power to adjudicate. –
  - 47. Factors to be taken into account by the adjudicating officer. –

- Chapter X – The Cyber Regulations Appellate Tribunal
  - 48. Establishment of Cyber Appellate Tribunal. –
  - 49. Composition of Cyber Appellate Tribunal.-
  - 50. Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal. –
  - 51. Term of office. –
  - 52. Salary , allowance and other terms conditions of service of Presiding Officer.-
  - 53. Filling up of vacancies. –
  - 54. Resignation and removal. –
  - 55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings. –
  - 56. Staff of the Cyber Appellate Tribunal. –
  - 57. Appeal to Cyber Regulations Appellate Tribunal. –
  - 58. Procedure and powers of the Cyber Appellate Tribunal. –
  - 59. Right to legal representation. –
  - 60. Limitation. –
  - 61. Civil court not to have jurisdiction. –
  - 62. Appeal to High Court. –
  - 63. Compounding of contraventions. –
  - 64. Recovery of penalty. –

- Chapter XI – Offences
  - 65. Tampering with computer source documents. –
  - 66. Hacking with Computer System. –
  - [66 A Punishment for sending offensive messages through communication service, etc.
  - [66 B Punishment for dishonestly receiving stolen computer resource or communication device (Inserted Vide ITA 2008)
  - [66C Punishment for identity theft. (Inserted Vide ITA 2008)
  - [66D Punishment for cheating by personation by using computer resource (Inserted Vide ITA 2008)
  - 66 E. Punishment for violation of privacy. (Inserted Vide ITA 2008)
  - 67. Publishing of information which is obscene in electronic form.
  - 68. Power of the Controller to give directions. –
  - 69. Directions of Controller to a subscriber to extend facilities to decrypt information. –
  - 70. Protected system.-
  - 71. Penalty for misrepresentation.-
  - 72. Breach of confidentiality and privacy.-
  - 73. Penalty for publishing Digital Signature Certificate false in certain particulars. –
  - 74. Publication for fraudulent purpose. –
  - 75. Act to apply for offence or contravention committed outside India. –
  - 76. Confiscation. –
  - 77. Penalties and confiscation not to interfere with other punishments. –
  - 78. Power to investigate offence. –

- Chapter XII – Network service providers not to be liable in certain cases
  - 79. Network service providers not to be liable in certain cases. –
- Chapter XIII – Miscellaneous
  - 80. Power of police officer and other officers to enter, search, etc. –
  - 81. Act to have overriding effect. –
  - 82. Controller, Deputy Controller and Assistant Controllers to be public servants. –
  - 83. Power to give directions.-
  - 84. Protection of action taken in good faith. –
  - 85. Offences by companies. –
  - 86. Removal of difficulties. –
  - 87. Power of Central Government to make rules. –
  - 88. Constitution of Advisory Committee. –
  - 89. Power of Controller to make regulations. –
  - 90. Power of State Government to make rules. –

Schedules in the Act / Amendments

- The First Schedule – Amendments to the Indian Penal Code
  - Primarily related to changes of the word “document” to “document and electronic record”/ electronic documents
- The Second Schedule – Amendment to the Indian Evidence Act
  - *inclusion of electronic document in the definition of evidence*
- The Third Schedule – Amendment to the Banker’s Book Evidence Act
  - Definition of “banker’s books” expanded to include electronic records
  - Legitimacy of print outs
  - This amendment brings about change in the definition of "Banker's-book". It includes printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device.
- The Fourth Schedule – Amendment to the RBI Act
  - Regulation of fund transfer through electronic means

Amendments – 2008 (IT Act 2008)

- Declare a system as a protected system and define security procedures for it
- Allow central government(CG) to intercept, monitor and decrypt any system or network, and for service providers to comply
- CG in consultation with private bodies may prescribe security practices and procedures
- Phishing, password and online identity theft, MMS type scandals, are all covered
- Child Pornography is explicitly covered allowing for heritage and religious material
- Section 43A and Section 72A which specify that they are measures towards "Data Protection"
- Cyber terrorism is extensively dealt with
- Invasion of privacy is still not dealt with – common citizen will find it difficult to prosecute for loss of personal information

Highlights of the Amended Act

- The newly amended act came with following highlights -
  - It stresses on privacy issues and highlights information security.
  - It elaborates Digital Signature.
  - It clarifies rational security practices for corporate.
  - It focuses on the role of Intermediaries.
  - New faces of Cyber Crime were added.

Intermediary Liability

- *Intermediary, dealing with any specific electronic records, is a person who on behalf of another person accepts, stores or transmits that record or provides any service with respect to that record*.
- According to the above mentioned definition, it includes the following -
  - Telecom service providers
  - Network service providers
  - Internet service providers
  - Web-hosting service providers
  - Search engines
  - Online payment sites
  - Online auction sites
  - Online market places and cyber cafes

Excluded from the purview of the IT Act

- Following are the documents or transactions to which the Act shall not apply -
  - **Negotiable Instrument** (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
  - A **power-of-attorney** as defined in section 1A of the Powers-of-Attorney Act, 1882;
  - A **trust** as defined in section 3 of the Indian Trusts Act, 1882;
  - A **will** as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;
  - Any **contract** for the sale or conveyance of immovable property or any interest in such property;
  - Any such class of documents or transactions as may be notified by the Central Government.

Digital Signatures

- If a message should be readable but not modifiable, a digital signature is used to authenticate the sender

Parameter	Paper	Electronic
Authenticity	May be forged	Cannot be copied
Integrity	Signature independent of the document	Signature depends on the contents of the document
Non-repudiation	a.Handwriting expert needed b.Error prone	a.Any computer user b.Error free

Digital Signature

- A digital signature is a technique to validate the legitimacy of a digital message or a document.
- A valid digital signature provides the surety to the recipient that the message was generated by a known sender, such that the sender cannot deny having sent the message.
- Digital signatures are mostly used for software distribution, financial transactions, and in other cases where there is a risk of forgery.

Electronic Signature

- An electronic signature or e-signature, indicates either that a person who demands to have created a message is the one who created it.

- A signature can be defined as a schematic script related with a person.

- A signature on a document is a sign that the person accepts the purposes recorded in the document.
- In many engineering companies digital seals are also required for another layer of authentication and security. Digital seals and signatures are same as handwritten signatures and stamped seals.

Digital Signature to Electronic Signature

- **Digital Signature** was the term defined in the old I.T. Act, 2000.
- **Electronic Signature** is the term defined by the amended act (I.T. Act, 2008).
- The concept of Electronic Signature is broader than Digital Signature.

- Section 3 of the Act delivers for the verification of Electronic Records by affixing Digital Signature.

- As per the amendment, verification of electronic record by electronic signature or electronic authentication technique shall be considered reliable.

Digital Signature to Electronic Signature

- According to the **United Nations Commission on International Trade Law (UNCITRAL),** electronic authentication and signature methods may be classified into the following categories -

- Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
- Those bases on the physical features of the user, i.e., biometrics.
- Those based on the possession of an object by the user, i.e., codes or other information stored on a magnetic card.
- Types of authentication and signature methods that, without falling under any of the above categories might also be used to indicate the originator of an electronic communication (Such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message).

Digital Signature to Electronic Signature

- According to the UNCITRAL MODEL LAW on Electronic Signatures, the following technologies are presently in use -

  - Digital Signature within a public key infrastructure (PKI)
  - Biometric Device
  - PINs
  - Passwords
  - Scanned handwritten signature
  - Signature by Digital Pen
  - Clickable “OK” or “I Accept” or “I Agree” click boxes

Civil Offences under the IT Act 2000

- Unauthorized copying, extracting and downloading of any data, database
- Unauthorized access to computer, computer system or computer network
- Introduction of virus
- Damage to computer System and Computer Network
- Disruption of Computer, computer network

Civil Offences under the IT Act 2000 (contd..)

- Denial of access to authorized person to computer
- Providing assistance to any person to facilitate unauthorized access to a computer
- Charging the service availed by a person to an account of another person by tampering and manipulation of other computer