Cyber Security

**2021**

**Rajkumar Jangid**

**SELF-DESIGNED**

21-Dec-21



***Cheptar-1(Introduction to Cyber Security)***

* **Strengthening** the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs.
* Cyber-attack is also known as a computer network attack (CNA).
* APT (Advanced Persistent Threat), which is kind of thread but not a brand new.
* **Tentative Definitions:** Cyber Security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.
* “**Cyber**-” is a prefix derived from the word “cybernetics” and has acquired the general meaning of “through the use of a computer”. The “cyber-” prefix is often used synonymously with “cyberspace”.
* **Indian Cyber Space**

• The National Informatics Centre (NIC) was set up as early as 1975 v with the goal of providing IT solutions to the government.

• Between 1986 and 1988, three N/Ws were set up:

**∞**INDONET, connecting the IBM mainframe installations that made up India’s computer infrastructure;

∞ NICNET (the NIC Network), being a nationwide very small aperture terminal (VSAT) N/W for public sector organizations as well as to connect the central government with the state governments and district administrations;

**∞** The Education and Research Network (ERNET), to serve the academic and research communities.

• Policies such as the New Internet Policy of 1998 paved the way for multiple Internet service providers (ISPs) and saw the Internet user base grow from 1.4 million in 1999 to over 15 million by 2003.

* **National e-Governance Plan (NeGP)**

Critical sectors such as Defence, Energy, Finance, Space, Telecommunications, Transport, Land Records, Public Essential Services and Utilities, Law Enforcement and Security all increasingly depend on N/Ws to relay data, for communication purposes and for commercial transactions.

* The National e-governance Program (Ne GP) is one of the most ambitious in the world and seeks to provide more than 1200 governmental services online. Schemes like ‘Rajiv Gandhi scheme for broadband to PRIs’ and National Optic Fiber Network (NOFN) mission is already dedicated to accelerate cyber connectivity in far reaching areas of country.

***CHAPTER–2(CYBER ADVERSARIES)***

* Commas adversaries that you could be pursuing during a hunt.
* **Malicious Insider**

An insider attack that is malicious in nature, and is typically perpetrated by disgruntled, troubled, or just greedy insiders. This is a targeted attack, motivated by financial gain or grievance.

Hackers are actively advertising for help from specific company’s employees to join the dark side. Desperate people can do desperate things. Good people can do bad things. In fact, this survey showed that 20% of employees would sell their corporate credentials, 44% of which would be willing to do it for less than $1,000, and some for as little as $100.

* **Inadvertent Insider**

Not all insider threats are malicious, sometime people just make mistakes, or fall victim to common social engineering tactics, such as phishing, vendor spoofing, or pretexting. People are typically the weakest link in security because human nature makes us vulnerable.

* **Hacker**

Hackers are opportunistic, and typically get a thrill from gaining access to secured systems. They are looking to prove themselves, and do it for bragging rights. There efforts don’t always have a malicious intent. Professional “white hat” hackers can be employed by companies to perform penetration tests to identify vulnerabilities and other weaknesses. Performing regular vulnerability assessments and penetration tests is an important part of your cyber security program and can help inform your cyber security strategy.

1. **White Hat**

White hat hackers are the persons who hack the system to find the security vulnerabilities of a system and notify to the organizations so that a preventive action can be taken to protect the system from outside hackers. White hat hackers may be paid employee of an organization who is employed to find the security loop-holes, or may be a freelancer who just wants to prove his mantle in this field. They are popular known as ethical hackers.

1. **Grey Hat**

Grey hat hackers find out the security vulnerabilities and report to the site administrators and offer the fix of the security bug for a consultancy fee.

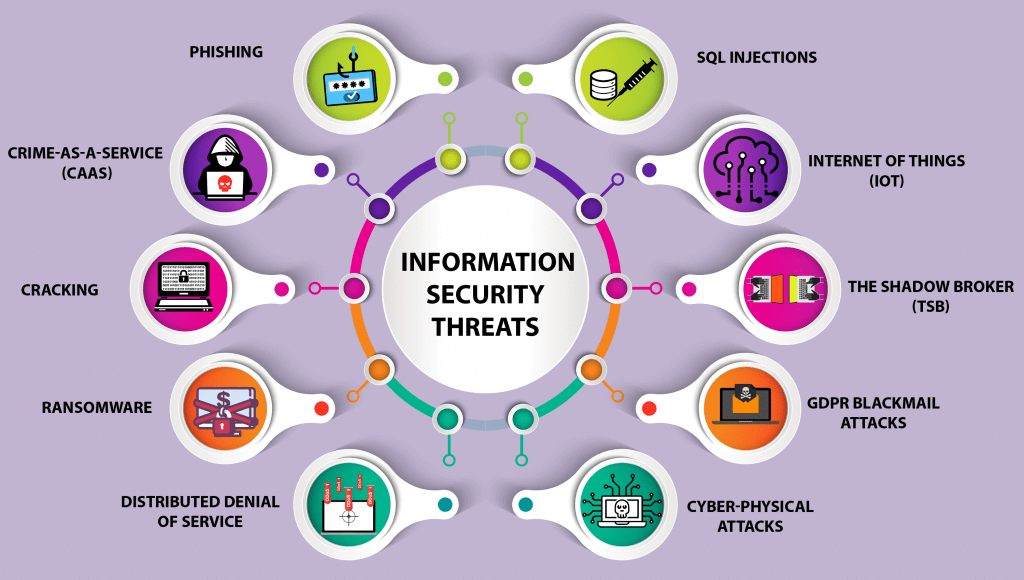
1. **Blue Hat**

A blue hat hacker is someone outside computer security consulting firms who is used to bugtest a system prior to its launch, looking for exploits so they can be closed.

* **Cyber** **Hacktivist**

Hacktivist attacks are targeted, and are often perpetrated to promote a political agenda or a social change. They are often looking to disrupt services and bring attention to a cause, such as free speech, human rights, or freedom of information. Anonymous is well-known for their hacktivist activities.

***Cyber Threats***



* **Malware**

Malware attacks are the most common type of cyberattack. Malware is defined as malicious software, including spyware, ransomware, viruses, and worms, which gets installed into the system when the user clicks a dangerous link or email. Once inside the system, malware can block access to critical components of the network, damage the system, and gather confidential information, among others.

**Below are the different kinds of malware:**

|  |  |  |
| --- | --- | --- |
| **Type** | **What It Does** | **Real-World Example** |
| Ransomware | disables victim's access to data until ransom is paid | RYUK |
| Fileless | Malware makes changes to files that are native to the OS | Astaroth |
| Adware | serves unwanted advertisements | Fireball |
| Trojans | disguises itself as desirable code | Emotet |
| Worms | spreads through a network by replicating itself | Stuxnet |
| Rootkits | gives hackers remote control of a victim's device | Zacinlo |
| Keyloggers | monitors users' keystrokes | Olympic Vision |
| Bots | launches a broad flood of attacks | Echobot |
| Mobile Malware | infects mobile devices | Triada |

**A. Ransomware**

Ransomware is software that uses encryption to disable a target’s access to its data until a ransom is paid. But there is no guarantee that payment will result in the necessary decryption key or that the decryption key provided will function properly.

**B. Fileless Malware**

Fileless malware doesn’t install anything initially, instead, it makes changes to files that are native to the operating system, such as PowerShell or WMI. Because the operating system recognizes the edited files as legitimate, a fileless attack is not caught by antivirus software — and because these attacks are stealthy, they are up to ten times more successful than traditional malware attacks.

**C. Spyware**

Spyware collects information about users’ activities without their knowledge or consent. This can include passwords, pins, payment information and unstructured messages.

The use of spyware is not limited to the desktop browser: it can also operate in a critical app or on a mobile phone.

e.g. Darkhotal.

**D. Adware**

Adware tracks a user’s surfing activity to determine which ads to serve them. Although adware is similar to spyware, it does not install any software on a user’s computer, nor does it capture keystrokes.

The danger in adware is the erosion of a user’s privacy — the data captured by adware is collated with data captured, overtly or covertly, about the user’s activity elsewhere on the internet and used to create a profile of that person which includes who their friends are, what they’ve purchased, where they’ve travelled, and more. That information can be shared or sold to advertisers without the user’s consent.

Adware **Example** Adware called Fireball infected 250 million computers and devices in 2017, hijacking browsers to change default search engines and track web activity.

**E. Trojan**

A Trojan disguise itself as desirable code or software. Once downloaded by unsuspecting users, the Trojan can take control of victims’ systems for malicious purposes. Trojans may hide in games, apps, or even software patches, or they may be embedded in attachments included in phishing emails.

Trojan Example: Emotet is a sophisticated banking trojan that has been around since 2014. It is hard to fight Emotet because it evades signature-based detection.

**F. Worms**

Worms target vulnerabilities in operating systems to install themselves into networks. They may gain access in several ways: through backdoors built into software, through unintentional software vulnerabilities, or through flash drives. Once in place, worms can be used by malicious actors to launch DDoS attacks, steal sensitive data, or conduct ransomware attacks.

Worm Example: Stuxnet was probably developed by the US and Israeli intelligence forces with the intent of setting back Iran’s nuclear program. It was introduced into Iran’s environment through a flash drive. Because the environment was air-gapped, its creators never thought Stuxnet would escape its target’s network — but it did.

DDoS attack (Distributed Denial for Services) generate traffic on a server by no. of system because a local user to be access server detail as application or website .

**G. Virus**

A virus is a piece of code that inserts itself into an application and executes when the app is run. Once inside a network, a virus may be used to steal sensitive data, launch DDoS attacks or conduct ransomware attacks.

***Differences between Viruses and Trojans***

|  |  |
| --- | --- |
| **Viruses** | **Trojans** |
| 1. A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data. | Trojan Horse is a form of malware that capture some important information about a computer system or a computer network. |
| 1. The main objective of virus is to modify the information. | The main objective of Trojan horse is to steal the information. |
| 1. It is more harmful. | It is less harmful as compared. |
| 1. Virus can’t be controlled by remote. | Trojan Horse can be controlled by remote. |
| 1. Viruses are executed via executable files. | Trojan horse is executed through a program and interprets as utility software. |
| 1. Resident and Non -resident viruses are two types of Viruses. | Back orifice, Rootkit and Beast Trojan are some of the common Trojan horses. |
| 1. Virus replicates itself. | Trojan Horse does not replicates itself. |

**H. Rootkits**

A rootkit is software that gives malicious actors remote control of a victim’s computer with full administrative privileges. Rootkits can be injected into applications, kernels, hypervisors, or firmware. They spread through phishing, malicious attachments, malicious downloads, and compromised shared drives.

**I. Keyloggers**

A keylogger is a type of spyware that monitors user activity. Keyloggers have legitimate uses; businesses can use them to monitor employee activity and families may use them to keep track of children’s online behaviors.

However, when installed for malicious purposes, keyloggers can be used to steal password data, banking information and other sensitive information. Keyloggers can be inserted into a system through phishing, social engineering or malicious downloads.

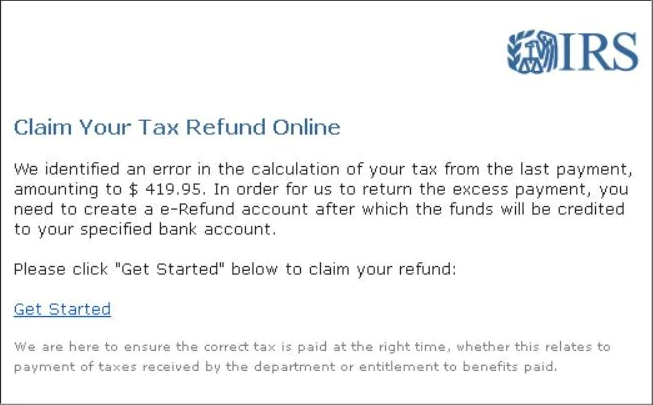
**Keylogger Example** A keylogger called Olympic Vision has been used to target US, Middle Eastern and Asian businessmen for business email compromise (BEC) attacks. Olympic Vision uses spearphishing and social engineering techniques to infect its targets’ systems in order to steal sensitive data and spy on business transactions. The keylogger is not sophisticated, but it’s available on the black market for $25 so it’s highly accessible to malicious actors.

***Different types of attacks***

1. **Phishing**

Phishing is fraudulent attempt, usually made through email, to steal your personal information. Phishing is the attempt to obtain sensitive information such as username, password and credit card details often for malicious reasons through an electronic communication (such as E-mail).

E.X.:-



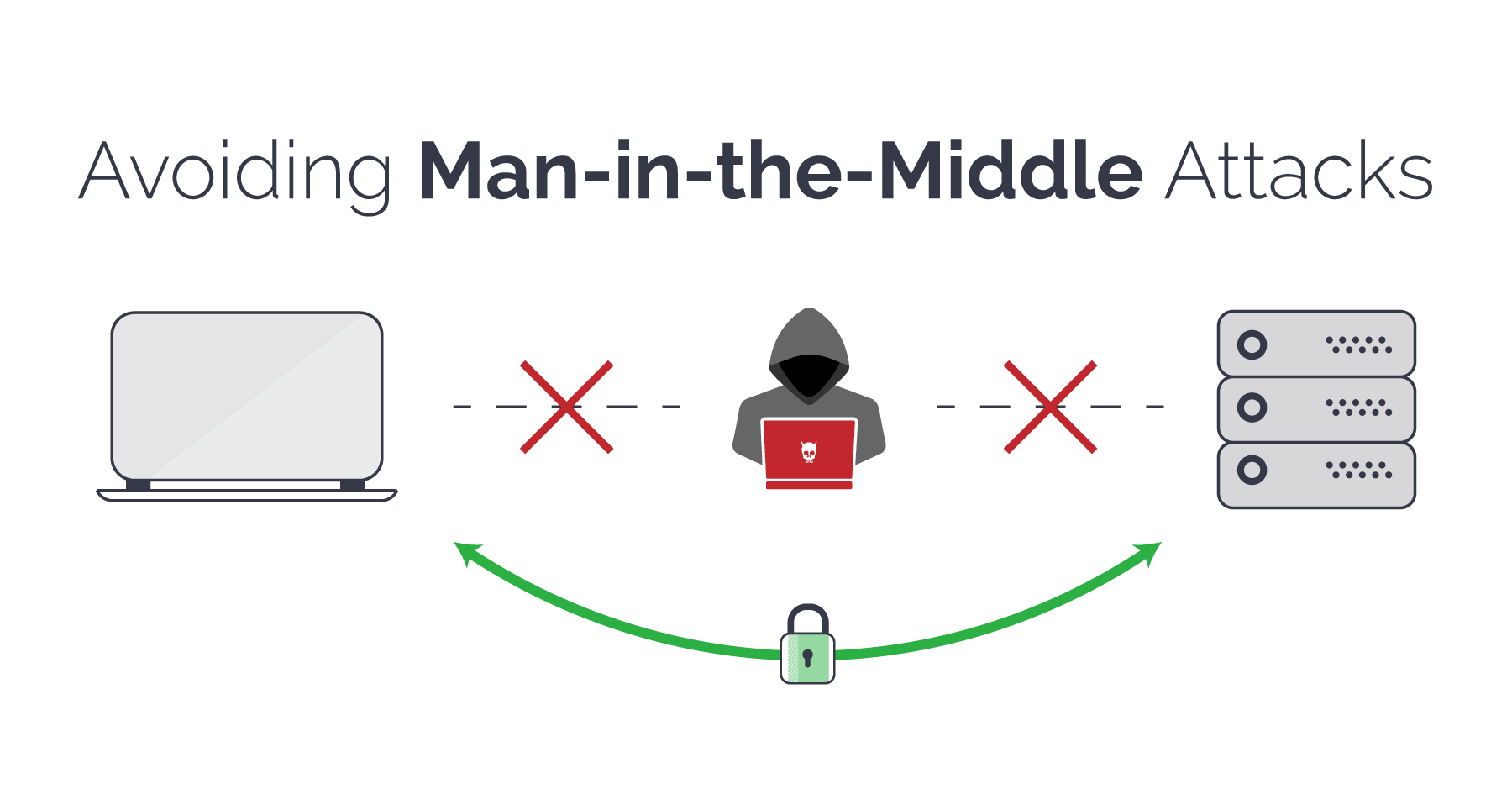
|  |  |
| --- | --- |
| **Spoofing** | **Phishing** |
| 1. Hacker tries to steal the identity to act as another individual. | Hacker tries to steal the sensitive information of the user. |
| 1. Needs to download some malicious software in victim computer. | No Such malicious software is needed. |
| 1. Spoofing is basically done to get a new identity. | Phishing is done to get secret information. |
| Types: IP Spoofing, Email Spoofing, URL Spoofing etc. | Types: Phone Phishing, Clone Phishing etc. |

1. **Man in the Middle Attack**

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

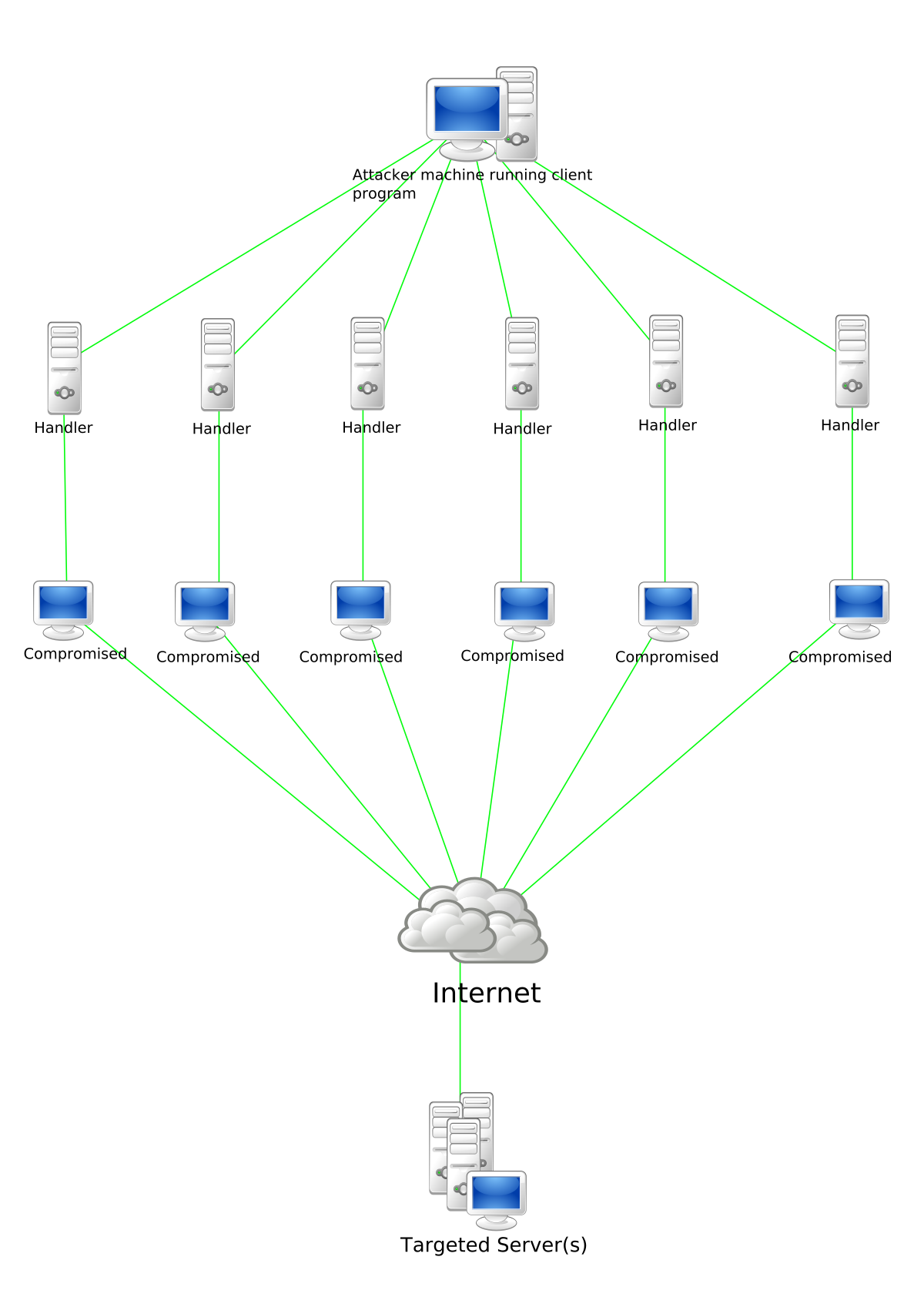
The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.

Additionally, it can be used to gain a foothold inside a secured perimeter during the infiltration stage of an advanced persistent threat (APT) assault.



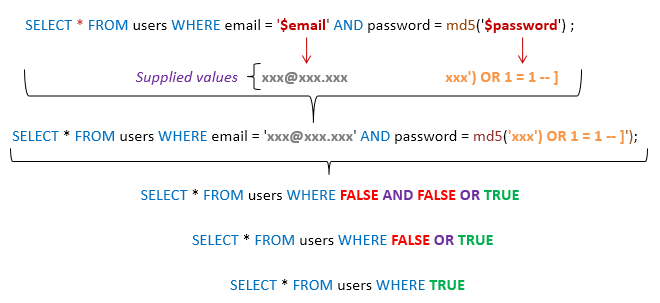
1. **Denial of Service Attack**

Denial of Service attacks aims at flooding systems, networks, or servers with massive traffic, thereby making the system unable to fulfil legitimate requests. Attacks can also use several infected devices to launch an attack on the target system. This is known as a Distributed Denial of Service (DDoS) attack.



1. **SQL Injection**

A Structured Query Language (SQL) injection attack occurs when cybercriminals attempt to access the database by uploading malicious SQL scripts. Once successful, the malicious actor can view, change, or delete data stored in the SQL database.



1. **Zero-day Exploit**

A zero-day exploit hits after network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. Zeroday vulnerability threat detection requires constant awareness.

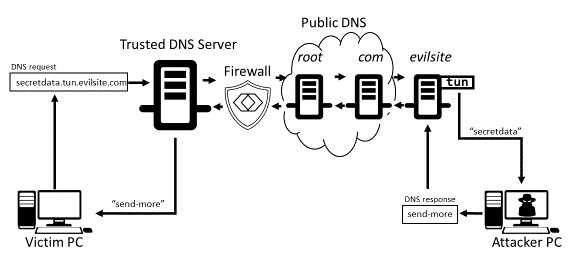
1. **Advanced Persistent Threats (APT)**

An advanced persistent threat occurs when a malicious actor gains unauthorized access to a system or network and remains undetected for an extended time.

45% of organizations feel that they are likely to be the target of an APT.

1. **DNS Attack**

A DNS attack is a cyber-attack in which cybercriminals exploit vulnerabilities in the Domain Name System (DNS). The attackers leverage the DNS vulnerabilities to divert site visitors to malicious pages (DNS Hijacking) and exfiltrate data from compromised systems (DNS Tunneling).



***CHAPTER–3***

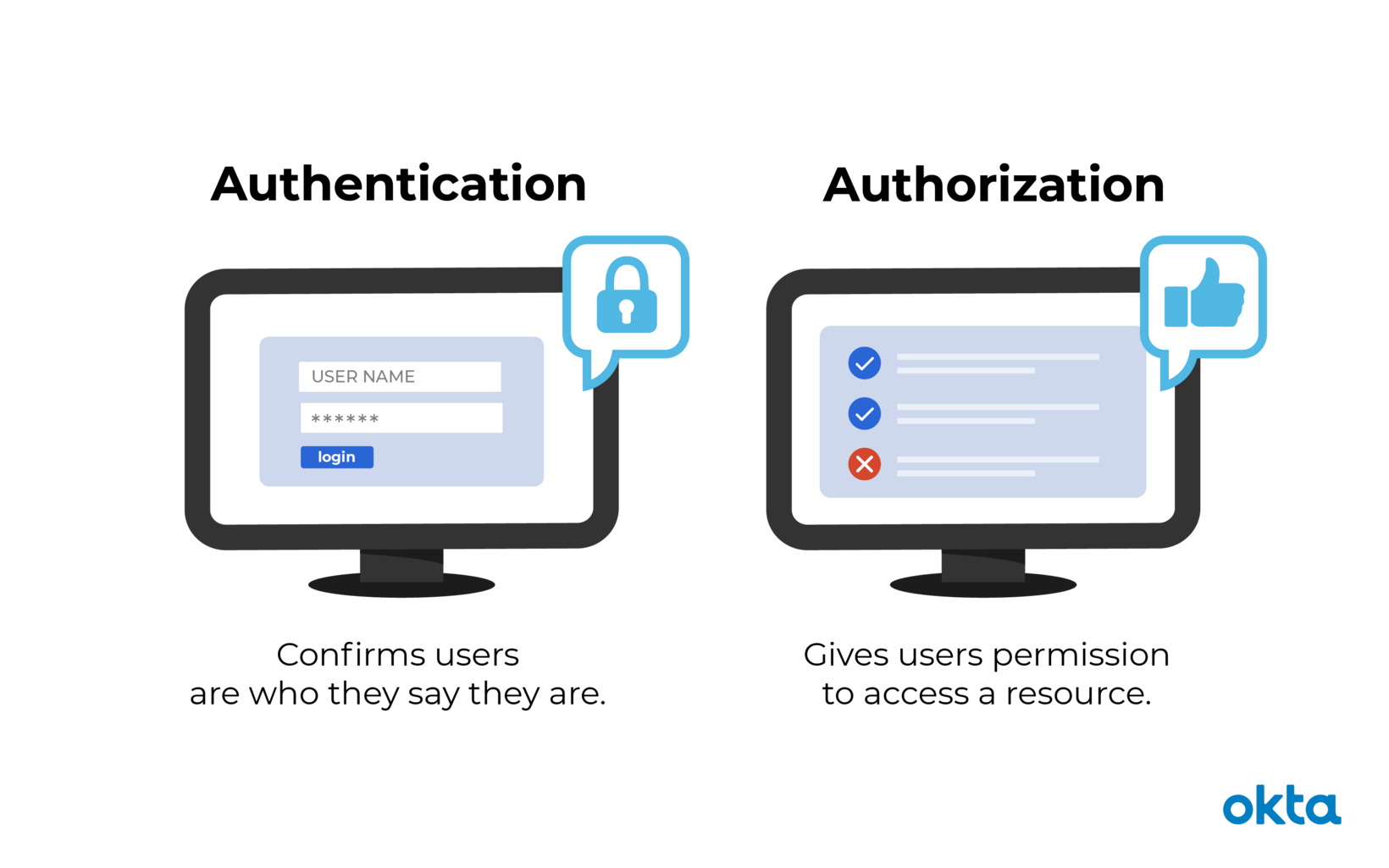
***CYBER*** ***SECURITY MEASURES & ITS TECHNIQUES***

**Cyber Security Techniques**

There are many cyber security techniques to combat the cyber security attacks. The next section discusses some of the popular techniques to counter the cyber-attacks.

**1. Authentication**

* It is a process of identifying an individual and ensuring that the individual is the same who he/she claims to be. A typical method for authentication over internet is via username and password.
* the organizations have made some additional arrangements for authentication like One Time Password (OTP), as the name suggest it is a password which can be used one time only and is sent to the user as an SMS or an email at the mobile number/email address that he have specified during the registration process.
* Some other popular techniques for two-way authentication are: biometric data, physical token, etc. which are used in conjunction with username and password.
* Some of the larger organizations also use VPN (Virtual Private Network), which is one of the methods to provide secure access via hybrid security authentication to the company network over internet.



**2. Encryption**

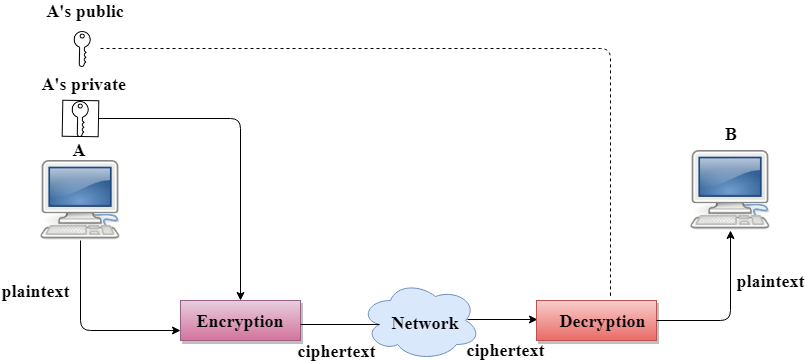
It is a technique to convert the data in unreadable form before transmitting it over the internet. Only the person who have the access to the key and convert it in the readable form and read it. Formally encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms.

The decoding of the complex code to original text using key is known as decryption.



**3. Digital** **Signatures**

* It is a technique for validation of data. Validation is a process of certifying the content of a document. The digital signatures not only validate the data but also used for authentication.
* The digital signature is created by encrypting the data with the private key of the sender. The encrypted data is attached along with the original message and sent over the internet to the destination.



**4. Antivirus**

There are verities of malicious programs like virus, worms, Trojan horse, etc. that are spread over internet to compromise the security of a computer either to destroy data stored into the computer or gain financial benefits by sniffing passwords etc. To prevent these malicious codes to enter to your system, a special program called an anti-virus is used which is designed to protect the system against virus. It not only prevents the malicious code to enter the system but also detects and destroys the malicious code that is already installed into the system. There are lots of new viruses coming every day. The antivirus program regularly updates its database and provides immunity to the system against these new viruses, worms, etc.



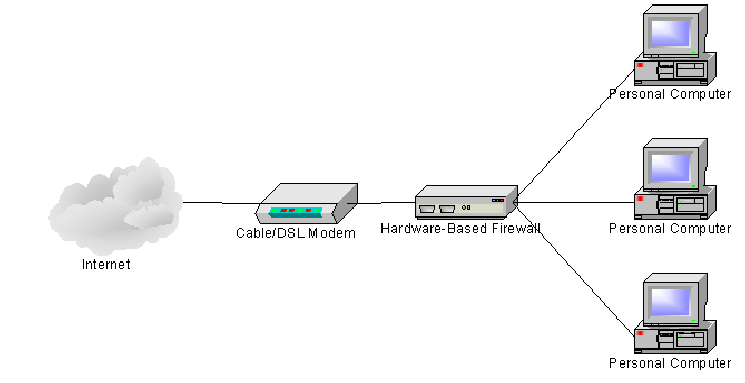
**5. Firewall**

* It is a hardware/software which acts as a shield between an organization’s network and the internet and protects it from the threats like virus, malware, hackers, etc.
* It can be used to limit the persons who can have access to your network and send information to you. There are two types of traffic in an organization viz. inbound traffic and outbound traffic.
* Using firewall, it is possible to configure and monitor the traffic of the ports. Only the packets from trusted source address can enter the organization’s network and the sources which are blacklisted and unauthorized address are denied access to the network.

A firewall can be implemented using hardware as well as software or the combination of both.

**5.1 Hardware Firewalls**

Example: of hardware firewalls are routers through which the network is connected to the network outside the organization i.e., Internet.



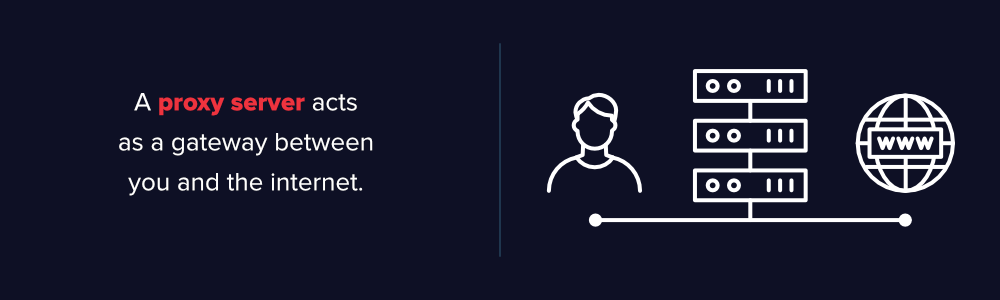
**5.2 Software Firewalls**

These firewalls are installed and installed on the server and client machines and it acts as a gateway to the organizations‟ network.



In the operating system like Windows 2003, Windows 2008 etc. it comes embedded with the operating system. The only thing a user need to do is to optimally configure the firewall according to their own requirement. The firewalls can be configured to follow “rules” and “policies” and based on these defined rules the firewalls can follow the following filtering mechanisms. :-

* **Proxy:** All the outbound traffic is routed through proxies for monitoring and controlling the packet that are routed out of the organization.



* **Packet Filtering:** Based on the rules defined in the policies each packet is filtered by their type, port information, and source & destination information. The example of such characteristics is IP address, Domain names, port numbers, protocols etc. Basic packet filtering can be performed by routers.

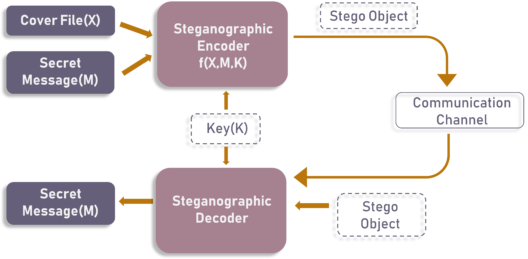


* **Stateful Inspection:** The firewalls are an essential component of the organizations‟ network. They not only protect the organization against the virus and other malicious code but also prevent the hackers to use your network infrastructure to launch DOS attacks.

**6. Steganography**

* It is a technique of hiding secret messages in a document file, image file, and program or protocol etc. such that the embedded message is invisible and can be retrieved using special software. Only the sender and the receiver know about the existence of the secret message in the image.
* The advantage of this technique is that these files are not easily suspected. There are many applications of steganography which includes sending secret messages without ringing the alarms, preventing secret files from unauthorized and accidental access and theft, digital watermarks for IPR issues, etc.

Let us take an example of an image file which is used as a cover medium. Each pixel of a high-resolution image is represented by 3 bytes (24 bits). If the 3 least significant bits of these 24 bits are altered and used for hiding the data. There are various free software’s available for Steganography. Some of the popular ones are: QuickStego, Xiao, Tucows, OpenStego, etc.



**Cyber Security Measures**

1. **Prediction of a Cyber-Attack:** Prediction is the easiest way to start securing data. Appraising data, identifying potential parties that would have interest in it, and anticipating events that may trigger attacks are all predictive measures. However, there are also more technical forms of prediction. These methods will be supported by the application of AI and other technologies to analyze surrounding activity instead of personal security. This may include analyzing dark data produced in a workplace to accurately gauge or identify malicious actors.
2. **Prevention from a Cyber-Attack:** Prevention is the most common form of cyber security, but is often inefficient or insufficient. This line of defines includes unique passwords with frequent changes, encryption of all data transmissions across any network, firewalls, securely developed applications, restricted access to data, limited authorizations, regular security testing and tightly secured stored data. Prevention also means establishing an information security policy and network security protocols that are strictly adhered to. An organization is only as safe as its least careful employee with access.
3. **Detection of a Cyber-Attack:** Detection is the most important aspect of protection. It is the 24/7 surveillance of vulnerable targets and gateways. Organizations should run “fire drills” of hacking frequently, weekly if not daily, to test their response systems. No software or network is fully patched or protected, so finding the gaps in protection is essential. Detection includes having a dedicated development security operation (DevSecOps) team, where security begins from day one of development. Gone are the days of creating a product or service and securing it from the outside, relying on a lengthy chain of communication. Having a one-stop unit that secures its products and detects future vulnerabilities means faster secure response time.
4. **Response to A Cyber-Attack:** Response is the last line of cyber security and the second most important. Even if a vulnerability is exploited, being able to respond quickly and effectively will save billions of dollars in the worst cases. However, this is some of the least funded areas of cyber security in many organizations. The response team should be comprised of IT professionals, members of a DevSecOps team with intricate knowledge of the entry point, and cyber security experts who can evict the intruder and shore up the protections. Response also includes client service teams that can reassure those affected and help handle the potential damages from consequences. Responding by ignoring the issue is the worst reaction.

***CHAPTER–4 DOMAINS IN CYBER SECURITY***

For this reason, many would-be attackers decided castles were not worth attacking at all. Modern-day defines in depth strategies revolve around this same concept of making an attacker go through multiple layers of defines, with one key difference: we’re applying that to our computer systems. Think about all the controls we have in place on our networks today: firewalls, authentication systems, intrusion detection and prevention systems (network- and host-based), router and switch security, operating system security, data encryption — the list goes on and on. Let’s be clear here, though: No system is unbreakable, so our goal with employing a defines in depth strategy is to put so many obstacles in the path that it’s now not worth the effort to attack. But with all those controls, how can we jam all the knowledge needed into just one single job? Oftentimes, we don’t. We keep them separated into multiple domains of cyber security:

**Domain 1: Security Management**

The first domain I’d like to discuss has more to do with people and processes than it does with computers. Security management is one of the most overlooked domains, which I think is a shame because almost nothing we do in the other domains means anything without it. Security management is made up of several tasks:

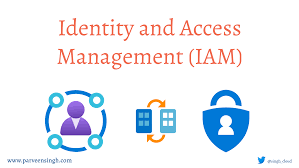
* Risk assessments, which is the process we use to identify risks to the organization and systemically identify methods to combat those risks, usually relying on input from experts in the below domains

* Overseeing the processes for other security functions to ensure those align with business/operations processes.
* Change management processes and procedures in place
* User security awareness training



**Domain 2: Identity and Access Management**

Usually referred to as IAM, this domain entails all the systems, processes, and procedures an organization uses to assign identities, handle authentication, and manage access control. Identity is the process of assigning each individual user and system their own unique name. Authentication is the process of establishing a method for users to prove their identity. Identity and authentication are usually carried out through the use of usernames and passwords, respectively. Access management is generally achieved using the principle of least privilege, meaning we assign the bare minimum rights or privileges to each individual that is necessary for them to carry out their job duties. To help simplify this, the individuals responsible for IAM should be included in conversations that have an impact on access change requirements on various resources.



**Domain 3: Security Engineering**

Security engineering usually refers to two key subdomains: network security and computer operations security. This domain is where your technical expertise is put to use in securing both the network and hosts from attacks. It’s in this domain that we lump the following:

• Firewalls

• Router/switch security

• Intrusion detection and prevention systems (IDS/IPS)

• Host-based security tools (such as antivirus and endpoint data loss prevention, DLP, tools)

• Email filtering

• Vulnerability scanning

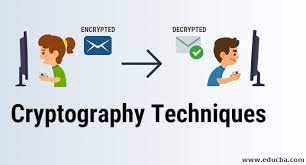
**Domain 4: Business Continuity**

This domain of cyber security focuses on restoring business operations after a catastrophic event, such as a natural disaster. This includes disaster recovery and business continuity plans and procedures. Of course, we should also make sure we’re periodically reviewing these plans as well as testing them. The business continuity domain revolves around understanding which functions of the organization are vital to the survival of that organization. Once we’ve identified these critical functions and associated systems, we should put in place procedures to ensure they are operable as soon as possible, with as little data loss as possible, in the event of catastrophic failures.



**Domain 5: Cryptography**

This is an amazing field that works in the analogy of a lock and key in the real world. In layman’s terms, a message is locked with a key (encrypted) and sent over the insecure network. The receiver then opens the lock (decrypts) to read the original message. In the meanwhile, if any eavesdropper tries to intercept the message, then he’d not get a sense of it as the original message is replaced with random characters. Cryptology deals with symmetric and asymmetric encryption where the key can be mutually decided by two communicating people or can be different. Cryptanalysis is another field where we have to analyze the algorithm used to encode the message.



**Domain 6: Physical Security**

A commonly overlooked domain, physical security refers to all the controls that should be applied to the physical hardware within our purview:

• Do we have fencing around our facility that forces individuals to enter and exit at the appropriately controlled point?

• Do we have security guards posted at every entrance to our organization?

• Are we securing the data Centre to only allow physical access to our servers to the authorized individuals?

• Do we have the proper HVAC (Heating ventilation and air-conditioning) system in place? Basically the means of HVAC is air gap between networks which is responsible for insert malware using command line in host system, so all procedure is harmful for host system(user).



**Domain 7: Security Operations**

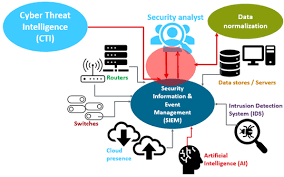
The Security Operations domain is where we monitor all of the tools, we discussed in the Security Engineering Domain in other words we can take remote from other system who is controlled by security organization. Most SOC (Security Operations Centre) positions are going to operate in this domain, as the name implies, but they need to have a good understanding of most of the other domains to be able to perform their job functions well. Some of the duties include:

• Threat hunting

• Incident Response

• Threat Intel

• Forensics



**FUTURE SCOPE**

• The Indian IT industry has in the past few years contributed significantly to the economic growth of the country. In a report released after the joint study of the PwC India and The DSCI or the Data Security Council of India, it was mentioned that the cybersecurity market in India would grow substantially and in 2022, would register USD 3.05 billion. The CAGR or the compound growth rate would be 15.6% This would be much higher than the global security market rate by 1.5 times.

• The cybersecurity incidents in India have risen considerably. As compared to other countries India and Asia are being subjected to successful attacks.

• According to data collected over the past 3 months, there has been a 39 % increase in ransomware attacks. According to this data, India ranks 2nd in the list of most affected countries. When the whole world was reeling under the COVID-19 attack, the cybercriminals were using this crisis as an opportunity for malicious attack. There is a prediction of attacks on the healthcare sector in India in the future.

**REFERENCES**

1. https://en.wikipedia.org/wiki/Computer\_security

2. https://www.ibm.com/topics/cybersecurity

3. https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-

common-types-of-cyber-security-attacks/

4. https://www.cybersecurityeducationguides.org/industries-and-domains/