# CHAPTER 1: GENERAL INFORMATION TO COMPUTER SECURITY

## INTRODUCTION

## PURPOSE OF COMPUTER SECURITY

## SOME IMPORTANT TERMINOLOGIES

## CASUAL FACTORS OF COOPERATIVE SECURITY ISSUES

## PRINCIPLES/SERVICES OF SECURITY

## SECURITY POLICY

# CHAPTER 2: NETWORK SECURITY

## INTRODUCTION

## GENERAL PRINCIPLES

## SECURITY TOOLS

## ACCESS CONTROL

# CHAPTER 3: OPERATING SYSTEM SECURITY

## INTRODUCTION

## OVERVIEW OF OS SECURITY

## NOTION OF CHECKLISTG

## THREATS OF THE HOST

## OS SECURITY BEST PRACTICES

## SECURITY ON WINDOWS

## SECURITY ON LINUX

# CHAPTER 4: VULNERABILITY AND ATTACK TECHNIQUES

## INTRODUCTION

## DEFINITION

## SECURITY PROTOCOLS

## VULNERABILITIES

## ATTACK STRATEGIES

# PROJECT

## PRACTICAL TOOLS WITHIN PARROT TO PERFORM PENETRATION TESTING

## SMALL KEY WORDS

### SECURITY

### IT

### NETWORK

### ATTACKS AND COUNTER MEASURES

CHAPTER 1: GENERAL INFORMATION TO COMPUTER SECURITY

**REQUIREMENTS**

Student should have knowledge in network, network protocols, manipulated computer devices and network devices and understand Linux OS

**GENERAL OBJECTIVES**

The main objective of this course is to raise student awareness on computer security, threats, teach them best practices to protect their computers and data to provide a deep understanding of the real-world security tools and techniques.

**SPECIFIC OBJECTIVES**

* Understand common security threats and how they can affect computer data.
* Know how to protect a computer from viruses, malwares and threats.
* Understand the basics of cryptography and how it is used to protect data privacy
* Know how to secure and internet connection and browse safely

**RISK ASSESSMENTS**

* Understanding certain threats associated with social networks and minimize them
* Understanding the importance of security update and how to apply them

## **INTRODUCTION**

Computer data often travels from one computer to another often leaving the safety of its protected physical surrounding. Once the data is out of your hands people with bad intentions can access, modify and/or damage it. While cryptography seeks to transform the data into a format that unauthorised parties can’t recognise it. This is done using complex mathematical and cryptographical algorithms.

Computer security refers to a generic name given to a collection of tools and resources designed to protect computers, routers, switches, hubs and all manners of network devices (endpoint devices or nodes) from malicious actors.

We have data security, network security and internet security

Data security: This refers to the methods used to assure data privacy including data integrity and data availability

Network security: This refers to all the measures put in place to protect data during its transmission as it travels from source to destination.

Internet security: These are all the methods and techniques used to protect data as it moves across networks (into a large geographical area).

CYBERSECURITY

This is the security which consolidates or condenses data security, computer security, network security and internet security. The cyber space represents an encapsulation of the real world where data is used to represent everything. We have endpoint devices connected to each other and data is the only currency of exchange. In a nutshell, cybersecurity seeks to understand the methods through which we can keep the cyber space safe. While no one user can guarantee cybersecurity because of its scale it becomes a collective effort.

## **DEFINITIONS**

DEFINITION OF KEY TERMS

1. Vulnerability: This is a weakness which allows a hacker to reduce an information system assurance. Vulnerability is the intersection of 3 elements; a flaw, knowledge of the flaw and ability to exploit the flaw

KNOW

ABILITY

FLAW

To exploit a vulnerability the attacker must have one applicable tool or techniques that connects directly to the vulnerability. In this frame, vulnerability is also known as **attack surface.**

Vulnerability is a cyclic path made up of Identifying, classifying, remediating and mitigating

1. Backdoor: A backdoor in a computer system is method of bypassing simple authentication securing remote access to the computer. E.g. Obtaining access to a plaintext with attempts to be undetected. A backdoor may take an install program It has the ability to display fake info about its disk and usage
2. Denial of Service Attack (DOS): Unlike other exploits, DOS are not used to gain unauthorised access or control access, they instead designed to make the system unusable. Attackers can deny services to individual victims such as…………… by deliberately entering the wrong passwords consecutively to cause the account of the victim to be locked or they may be overloading the capability of machine or network thereby blocking all its users at once. This type of attack is very hard to prevent because the whole network needs to be analysed not just the small piece of code.
3. Distributed Denial of Service Attack (DDOS): DDOS are always very common. In this type of attack, a very large number of computers (Zombie computers) used as part of botnets use worms, trojan horse and backdoors to control them are used to flood the target system thus attempting to render it unusable through resources
4. Eaves dropping: This is the act of surreptitiously listening to a private conversation typically between host on a network. For instance, programs like camivore and Narusinsight have been used by the FBI and NSA to eaves drop on a system of internet service providers.
5. Spoofing: Spoofing of user identity describe a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.
6. Tampering: It describes an international modification of the product in a way that will make them harmful to the user.
7. Repudiation: It describes a situation where the authenticity of a signature is being changed.
8. Information disclosure (privacy bridge or data leak): It describes a situation where information thought as secured is released in an untrusted environment.
9. Elevation Of Privilege (Privilege escalation): It describes a situation where a person or program wants to gain elevated privileges or access which is normally restricted to him (privilege escalate).
10. Exploit: It is a piece of software, a chunk of data or sequence of commands that takes advantage of a software “bug”, “glitch” or vulnerability in order to cause intended or unanticipated behaviour to occur on software, hardware or something electronic (usually computerized). This usually includes such things as gain control of a computer system or allowing privilege escalation or denial of service attack. The term exploit generally refers to small programs to take advantage of a software that has been discovered either remote or local. The code from the exploit program ID frequently reused in trojan horses and computer viruses
11. Attack: An attack is a method used to exploit the vulnerability. There are generally 2 types of attacks.

* Passive attack: They are difficult to detect because they usually pose no clear activity that can be monitored or detected. Example of passive attack will be packet sniffing or packet analysis. These types of attacks are designed to record and monitor traffic on the network. They are often used to gather information which could be later used to perform other attacks. These attacks are extremely difficult to protect against as they do not need or involve the modification of data. However, it is very possible to prevent them
* Active attacks: These are attacks that involve some modifications of the data stream or the creation of the flaw stream. Active attacks could be classified into 4 categories

1. Masquerade: one entity pretends to be another
2. Replay: This involves passive usage of data unit and its subsequent transmission to produce an authorized effect.
3. Modification of message: some portions of the message are alternated or deleted or recorded to produce an unauthorised effect.
4. DoS: since the kind of attack inhibit the normal use or management of communication facilities, as a result of flooding or damage of the devices. It is quite difficult to prevent active attack because to do so, you need to protect all the devices in the communications facilities. Hence the objective is rather to detect them and or mitigate them.

Attacks in the nature passive or active are largely classified into 4 general categories.

1. Interception: an unauthorized party gains access to an asset. This is a direct attack on confidentiality. The unauthorized party could be a person, a program or a computer, Wired tapping, illicit copying of files.
2. Interruption: an asset or a system is destroyed or is made temporally or permanently unavailable or unusable. This is a direct attack on availability. E.g. destruction of a piece of hardware, cutting of the communication line.
3. Modification: an unauthorized party not only gain access to an asset but tampers with the asset. This is a direct attack on integrity. E.g. changing value in a data file, altering a program, modifying the content of the message.
4. Fabrication: an unauthorized party inserts counterfeit objects or material into the system. This is a direct attack on authenticity. E.g. inserting a spurious message in a network or addition of records into a file.

**THE PILLARS OF SECURITY**

There are 5 main pillars of security, and they could be gotten from the acronym CIANA. These pillars could also be called principles or services.

* Confidentiality: this is a principle of security that stipulates that unauthorized parties should not be able to gain access to the content of the message or transmission i.e. only authorized parties are granted access to the content of the message. This service could be provided using CRYPTOGRAPHIC ALGORITHM (encryption and decryption). In this process, the message to be sent is encrypted with a key and upon reception of the message, the authorized should be able to decrypt the message with the right key.
* Integrity: it is the principal pillar of security that stipulates that the content of a message, data or IT resources should not be modified unless by the authorized parties i.e. only authorized parties are supposed to be able to modify a message in transition. Attacks of the nature that violates integrity fall under the category of modification. The service of integrity could be provided by some cryptographic algorithm such as hashing.
* Hashing: it is a one-way cryptographic function that provide a blueprint of digital data. This further consider a finger print. Some hash algorithms include MD5, SHA (128), SHA (256).
* Availability: in this service of security, data is supposed to be make accessible to authorized parties whenever they need it and however they need it. This pillar also serves for computer resources (modem, router, RAM, storage) e.g. of this attack could be flooding a server with more request that it can handle forcing the server to crack either temporally or permanently unavailable. A very popular way to mitigate this kind of attack is to use system that can automatically scale up e.g. the cloud, backup or mirroring.

Note: IDS means Intrusion Detection System and IPS means Intrusion Prevention System

* Non-repudiation: this is a pillar of security that stipulates that an individual can’t deny the action it performs within an information system. In this scenario, all users should be accountable for their actions. This service could be provided using logging. A log is a manifested that contains all actions performed by users of the system. Some applications that provide such services include SURICATA, SNORT, elastic search.
* Authentication: this is the last main pillar of security and stipulates that the origin of a communication must be known i.e. they must be who they are claiming to be. This comes about multiple factors of authentication (what you know, what you have, and who you are).

What you know

This refers to a construct that is supposed to exist solely in the user’s knowledge base (brain). NB you should never write it down e.g. the username and password belong to this category.

What you have

In this method, the user should possess some materials or asset that can vouch for its identity. In this method, if the object is found in the wrong hand, it could compromise the system e.g. credit card, access card, badges, phones.

Who you are

In this factor of authentication, the user possesses something that can’t be separated from their person i.e. it is a part and parcel of who they are. For this means, you can’t separate these properties from the user. E.g. include facial recognition, finger print, voice and eye recognition. Examples in this category are usually called Biometrics.

**ACCESS CONTROL**

It is a security that regulates who or what can view or use resources in a computer environment. It is the fundamental concept in security that minimises risks in a business or organization. There are 2 types of access control i.e. physical and logical.

Physical access control limit access to campuses, rooms and physical IT assets. Logical access control limits connection to computer network, system files and data. To secure a facility, organisations use electronic access control systems that rely on user criteria, access scan reader, auditing, and report to track employee access to restricted business locations and proprietary areas such as data centres. Some of these systems incorporate access control panels to restrict entries to rooms and buildings as well as alarms and lockdown capabilities to prevent unauthorized access or operations.

Logical access control systems perform identification, authentication and authorization of users or entities by evaluation required login criteria that can include passwords, personal identification numbers, biometrics scans, security tokens or other authentication factors. Multi-factor authentication (MFA) which requires 2 or more authentication factors, is often an important part of a layered defence to protect access control systems.

The goal of access control is to minimise the security risks of unauthorized access to physical and logical access. Access control is a fundamental component of security compliance programs that ensures security technologies and access control policies are in place to protect confidential information such as customer data. Most organisations have infrastructures and procedures that limit access to network, computer systems, applications, files and sensitive data such as personal identifiable information and intellectual property.

Access control systems are complex and can be challenging to manage in IT.

Environment that involves on-premises systems and cloud services. After high profile breaches, technology vendors have shifted away from single sign-on system to unify access management which offer access control for on-premises and cloud environment.

**HOW ACCESS CONTROL WORKS**

Access control identifies an individual or entity, verifies the person or application who is or what it claims to be, and authorizes the access level and set of actions associated to the username or IP address. Directory services and protocols including lightweight directory access protocol and security assertion markup language provide access control for authenticating and authorizing users or entities and enable them to connect to computer resources such as distributed application and web servers.

Organisations use different access control systems depending on their compliance and the security level of IT they are trying to protect.

**Types of access control**

**Mandatory access control (MAC):** This is a security model in which access rights are regulated by a central authority based on multiple levels of security. Often use in government and military environment, in this access control classification are assigned to all resources in the OS, or security kernels. MAC grants or denies access to system based on information security of the user or design.

For example: The MAC is very expensive to implement and very rigid

**Discretionary Access Control (DAC):** This an access control method in which owners or administrators of the protected system, data or resources set the politics defining who or what is to access the resources. Many of this system enables the administrators to limit the propagation of access right. A common criticism of that system is the lack of centralized control.

**Access control list**

The access control list is a list that shows all the users interacting with a resource and to what extend they can interact or use a resource

**Example 1:**

* User A has the ability to read file1 to execute and write on file2 and to write on file3
* User B has the ability to write on file1, he owns file 2 and he can only write on file 3
* User C can own file3, can read, write, execute on file2 and can only write on file1

Determine the access control matrix of the system

Solution:

|  |  |  |  |
| --- | --- | --- | --- |
| ACM | File1 | File2 | File3 |
| User A | r | x, w | w |
| User B | w | o {r, x, w} | w |
| User C | w | r, x, w | o {r, w, x} |

Access Control Matrix

|  |
| --- |
| User B |
| w |
|  |

|  |
| --- |
| User C |
| w |
|  |

|  |
| --- |
| User A |
| r |
|  |

F1

|  |
| --- |
| User B |
| o |
| r |
| w |
| x |
|  |

|  |
| --- |
| User C |
| r |
| w |
| x |
|  |

|  |
| --- |
| User A |
| x |
| w |
|  |

F2

|  |
| --- |
| User B |
| w |
|  |

|  |
| --- |
| User C |
| o |
| r |
| w |
| x |
|  |

|  |
| --- |
| User A |
| r |
|  |

F3

Access Control List

|  |
| --- |
| File 1 |
| r |
|  |

|  |
| --- |
| File 2 |
| w |
| x |
|  |

|  |
| --- |
| File 3 |
| w |
|  |

UserA

|  |
| --- |
| File 1 |
| w |
|  |

|  |
| --- |
| File 2 |
| o |
| r |
| w |
| x |
|  |

|  |
| --- |
| File 3 |
| w |
|  |

UserB

|  |
| --- |
| File 1 |
| w |
|  |

|  |
| --- |
| File 2 |
| r |
| w |
| x |
|  |

|  |
| --- |
| File 3 |
| o |
| r |
| w |
| x |
|  |

UserC

Compatibility list

Compatibility List: It shows the list of resources a user can interact with and at what extend he can use these resources

**Differences between Compatibility list and Access Control List**

* The CL shows the list of resources a user can interact with and at what extend he can use these resources while the ACL shows the list of users that interact with a given resource and at what extend he can these resources
* The ACL is obtained from the vertical columns o f the ACM while the CL is gotten from the horizontal row

**Role Base Access Control (RBAC):** This is a widely used access control mechanism that restrict access to computer resources based on individuals or groups with defined business functions i.e. executive level, engineering level, administrative level. Rather than the identity of individual users, the role-based security model relies in a complex structure of role assignment, role authorisation and role permissions developed using role engineering to regulate employee access to the system. RBAC systems can be used to enforce MAC and DAC.

**Rule Base Access Control (RuBAC): This** a security model in which the system administrator defines the rules that governs access to the resource or objects. This rule is often based on conditions such as time of the day or location. It is not uncommon to use the conjunction of rule base access control and RBAC to enforce access policies and procedures.

**Attribute Based Access Control (ABAC):** This is a methodology that manages access rights by evaluating a set of rules, policies and relationships using the different attributes of a user, including system and environmental conditions

Exercise:

UserA= file1(r, w), file2(w, x), file3(o without x), file 4(r, w, x)

UserB= file1(x), File2(o without r), File3(r), File4(r, x)

UserC= File1(w), File2(r), File3(x), File4(o without w)

Activity: Generate the

1. ACM
2. ACL
3. CL

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ACM | File1 | File2 | File3 | File 4 |
| User A | r, w | x, w | o {r, w} | r, w, x |
| User B | x | o {w, x} | r | r, x |
| User C | w | r | x | o {r, x} |

ACM

ACL

|  |
| --- |
| User B |
| x |
|  |

|  |
| --- |
| User C |
| w |
|  |

|  |
| --- |
| User A |
| r |
| w |
|  |

F1

|  |
| --- |
| User B |
| o |
| w |
| x |
|  |

|  |
| --- |
| User C |
| r |
|  |

|  |
| --- |
| User A |
| x |
| w |
|  |

F2

|  |
| --- |
| User C |
| x |
|  |

|  |
| --- |
| User A |
| o |
| r |
| w |
|  |

|  |
| --- |
| User B |
| r |
|  |

F3

|  |
| --- |
| User A |
| r |
| w |
| x |
|  |

|  |
| --- |
| User B |
| r |
| x |
|  |

|  |
| --- |
| User C |
| o |
| r |
| x |
|  |

F4

CL

|  |
| --- |
| File1 |
| r |
| w |
|  |
|  |

|  |
| --- |
| File2 |
| w |
| x |
|  |

|  |
| --- |
| File3 |
| o |
| r |
| w |
|  |

|  |
| --- |
| File4 |
| r |
| w |
| x |
|  |

UserA

|  |
| --- |
| File1 |
| x |
|  |

|  |
| --- |
| File4 |
| r |
| x |
|  |

|  |
| --- |
| File3 |
| r |
|  |

|  |
| --- |
| File2 |
| o |
| w |
| x |
|  |

UserB

|  |
| --- |
| File1 |
| w |
|  |

|  |
| --- |
| File2 |
| r |
|  |

|  |
| --- |
| File3 |
| x |
|  |

|  |
| --- |
| File4 |
| o |
| r |
| x |
|  |

UserC

**SECURITY TRINITY**

The 3 legs of security trinity are prevent, detect and respond. It should be the foundation of all security policies and measures that an organisation develops and employs

Prevention

Response

Detection

Security

1. Prevention: The foundation of the security trinity is prevention. To provide some level of security it is necessary to place measures to prevent the exploitation of the level of vulnerability. In developing network security skills, organisation should emphasize preventive measures over detection and response. It is easier, more efficient and much more cost effective to prevent a security breach than to detect or respond to one. Remember that it is impossible to devise a security scheme that will prevent all vulnerabilities from been exploited but companies should ensure that their preventive measures are strong enough to discourage potential criminals.
2. Detection: Once preventive measures are implemented, procedures need to be put in place to detect potential problems or security bridges in case preventive measures fails. It is very important that problems be detected immediately. The sooner the problem is detected the easier is to correct and clean up.
3. Response: Organisation needs to develop a plan that identifies the appropriate response to a security breach. The plan should be written and should identify who is responsible for what action and varying responses and level of appreciation. The difficult part is developing a security plan that fits the organisation business operation and getting people to comply with plan.

INFORMATION SECURITY

Network security concerns the security of companies assets. It often loose sight of the fact that it is the information and our ability to access that information that we are really trying to protect and not the computer and networks. A simple definition of information security is Confidentiality + Integrity+ Availability + Authentication. There can be no information security without confidentiality this ensures that unauthorized users do not intercept, copy or replicate information. At the same time integrity is necessary so that organisation have enough confidence in the accuracy on the information to act upon. Security measures are worthless, if organisation cannot get access to the vital information they need at any time. Information security also ensures adequate physical security;

Hiring proper personnel, developing and adhering to procedures and policies to procedures and policies ………………………………………………………………………………………………

It is important to remember that information security is not about protecting access from outside hackers. In many cases, threats are internal to an organisation; “we have found the enemy and it is us”.Information is also about procedures and policies that protect information from accident, incompetent and natural assets

Such policies need to address the following: backup,configuration controls and media controls, disaster recovery and confidency planning, data integrity. It is important to remember that network security is not absolute.

RISK ASSESTMENT

The concept of risk assestments are crucial to developing proportionate defenses.To perform risk analysis, organisations needs to understand possible threats and vulnerabilities. Risk is the probability that a vulnerability will be exploited. The following are risk assessments steps.

* Identifying and Priorizing Assets (Resources)
* Identifying vulnerabilities.
* Identifying counter measures.
* Developing a cost benefit analysis.
* Developing security policies and procedures

CHAPTER 2: NETWORK SECURITY MODEL

They 3 basic approaches used in developing a security model. Usually, organisations use some combination of the 3 approaches to achieve security. The 3 approaches are open access to network security, restrictive access to network security model and the closed access to network security model.

2.1 Open access security model: An open access security model is the easiest to implement.

Few securities are implemented in this design. Administrators configure existing hardware and softwares, basic security capabilities, firewalls and virtual private networks(VPN), intrusion detection system and other measures that inqure additional cost are typically not implemented. Simple passwords and server security becomes a foundation of this model. If encryption is used, it is implemented by individual users or on servers. This model assumes that the protected assets are minimal, users are trusted and threats are minimal. However, this does not exclude the need for data backup system. LANs that are not connected to the internet or public ones are more likely to implement this can of model. This type of network design give users free access to all areas. When security breaches occur, there are likely to result in break damage and loss. Network administrators are usually not held responsible for network breaches or abuse.

2.2 Restrictive access network: A restrictive security model is difficult to implement. Many security measures are implemented in this design. Administrators configure existing hardware and software for security capabilities in addition of deploying more costly hardware and software solutions such as firewalls, VPN, IPS, IDS and identity servers. Firewalls and identity servers became the foundations of this model. This model assume that the protected assets are substantial, some users are not trust-worthy and threats are likely. LANs that are connected to the internet or public WANs are more likely to implement this type of models. Ease of use for users diminishes as security titles.

2.3 Closed Access Network Security: A closed security model is more difficult to implement. All available security measures are implemented. Administrators configure existing hardware and software for maximum security capabilities. In adding for putting in place of most costly hardware or software solution such as firewalls, VPN, IDS and identity servers. Here the protected assets are premium, brief, all users are not trust-worthy and that threats are frequent. Users’ access is difficult and cumbersome. Network administrators require greater skills and more time to administer the network. Furthermore, companies require a higher number of and more efficient network administrators to maintain this tight security. In many organisations, these administrations are likely to be unpopular while implementing and maintaining this security. The network security departments must clarify that they only implement the policy which is designed, written and approved by the cooperation or organisation. Policies under the closed security model can be monumental. In the event of a security breach or network abuse, the network administrators might be held more accountable for problems.

Chapter 3 VULNERABILITIES THREATS AND ATTACKS

3.1 Vulnerability

Vulnerability is an inherent weakness in a designed configuration or implementation of a network or a system that renders it liable to a threat. Most vulnerabilities can be traced back to one of the following sources:

1. Poor design: Hardware and software designs flows that can be experimented, in effect, almost all systems are created with security holes.
2. Poor Implementation: The system that is incorrectly configured is very vulnerable to attacks. This type of vulnerability usually through experience, insufficient training or sloppy An example of this type of vulnerability will be a system that doesn’t have access to a restricted file thereby allowing rights to be altered by an unauthorized user
3. Poor management: This is an inadequate procedure and insufficient checks and balances. Security measures cannot operate in a vacuum. They need to be documented and monitored. Even something as simple as the daily backup of a system needs to be verified. There is need for definition of responsibility of some dual custody for others, in this manner, an organisation can ensure that operations are been followed and they are no other form of control. While they are 3 sources of vulnerability, they can manifest themselves in many ways.
4. Physical security:

Central hosts and server should be kept in secured room that can only be entered by some authorized personnel. Outers and communication equipment should be kept with restricted access in addition, critical removable media such as backups should be stored in the secure in which only authorized personnel have access. As part of this process, organization needs to keeps into consideration the natural and physical environment in which the operates. They should take into consideration the probability of earthquakes, flies flood and other natural disaster in order to plan accordingly.

Proper planning of physical facilities of physical activities can mitigate many other effect of natural disasters for instance, organizations in an earthquake zone needs to build their equipment’s to building structural standard, so that they do not bounce off the walls out of the window during the bigquake. Organization located in fluid plan zone should not placed rooms in their building basement

1. Media Vulnerabilitie:

Disk tapes and other medias can be stolen , lost or damage. Information copied and removed from an organization locally without detection. Accordingly, companies needs to ensures the safety of all needs that contains or saves vital information assets.

1. Transmission and Emanations Vulnerabilities:

Signal emission from electrical equipment can be remotely intercepted and monitored using sophisticated devices in a process called the VEN\_ECK. Monitoring organisations Also needs to be concerned about the interception of most forms of communication . Communication is the sharing of information in a medium and as it is inherently vulnerable to interception monitoring, forgery, alternation and interruption. Every medium used for the transmission of information can be tapped. Network sniffers, or packet sniffers have common hacker tools that can read traffic as it passes on a network.

1. Human vulnerability, human stupidity, carelessness, laziness and anger represents the greatest threats to network and systems and do more damage than the rest of the others combined. Moreover, human vulnerabilities and the risk associated with them are the most difficult to defend against. It is important to note that a totally secured network or system doesn’t exist

THREATS

A threat is anything that can disrupt the operation, the functioning, the integrity or availability if a network or system. There are different categories of threats: The natural threats occurances such as floods, earthquakes, storms. There are also unintentional threat that are accidental and stupidity result.

1. Unstructured Threats: This consists mostly inexperienced individuals using easily available hacking tools. Even unstructured threats that are only executable with the intention of testing and challenging the hacker’s skill can still be serious damage to the company. e.g. If an external company’s website is hacked the integrity of the company is damaged even if the external website is separated from the internal information that sits behind a protected firewall the public does not know that. All that the public knows is that the site isn’t a safe environment to conduct business.
2. Structured Threats: This comes from hackers that are highly motivated and technically competent. These people know system vulnerability and can understand and develop expert codes and scripts. They use sophisticated hacking tools on suspecting businesses. These groups are often involved in the major frauds and theft cases reported to the law enforcement agencies.
3. External threats: It can arise from individuals or organisations working outside of the company. They do not have unauthorised access to the computer systems or networks. They get in the network mainly through the internet or the dial-up access servers.
4. Internal threats: The internal threats occurs when someone has authorised access to the network with either an account on the server or physical access to the network. According to FBI, internal access and misuse of network accounts to 60% to 80% of reported incidents

**ATTACKS**

An attack is a specific technique used to exploit vulnerability e.g. **an attack can be a denial of service.** There are two general categories of attacks i.e. **passive and active.**

Passive attacks are very difficult to detect because there is no clear activity that can be monitored or detected. Examples of passive attacks could be **packet sniffing or traffic analysis**. These types of attacks are designed to record and monitor traffic on the network. They are often used for information gendering than can be used latter in active attacks.

Active attacks as the name implies uses more open actions on the network or systems. As a result, they can be easier to detect but at the same time can be much more devastating to the network e.g. **a denial of service attack or active probing in to the systems or network**

*CHAPTER IV: BASIC TYPES OF ATTACKS*

There exist four primary classes of attacks:

* + 1. **Reconnaissance attacks**

It is the unrecognised discovery and marking of systems, services or vulnerabilities. It is also known as information gendering and in most cases it precedes an actual access and denier of service attack. It is somewhat analogous to a thief casing a neighbourhood for vulnerable homes to break into; such as an unoccupied residence easy to pen doors or open windows. Reconnaissance attack can consist of the follow:

* **Packet sniffing**
* **Port scans**
* **Ping weeps**
* **Internet information queries**

A Malicious intruder usually pings sweeps the target network to determine which IP address are alive. After this, the intruder uses a port scanner to determine what network services or port are active on the life IP addresses. From this information, the intruders query the ports to determine the application type and version and also the type of the OS running on the targeted host. Based on this information, the intruder can determine whether a possible vulnerability exist that can be exploited.

Using for example the “**NSlookup**”and “**Whois**” software utilities, an attacker can easily determine the IP address space assigned to a give cooperation or entity. The ping command tell the attacker what IP address are live.

* + 1. **Access attack**

It is the ability for an intruder to get access to a device for which he doesn’t have an account or password. Entering or accessing systems to which one does not have authority usually involves rooming a hacked scripts or tools that exploit a non-vulnerability of the system. Access attack exploit non-vulnerabilities in authentication services, FTP services and web services to gain entry to web accounts, confidential databases and other sensitive information.

Access attacks can consist of the following:

* **Password attacks**
* **Trust exploitation**
* **Port redirection**
* **Man in the middle attack**
* **Social engineering**
* **Phishing etc.**

1. **Password attack**

It can be implemented using several methods including **brute force attack, Trojans horse program, IP spoofing and packet sniffing.** Password attack usually refers to repeated attempt to identify a user account, password or both. These repeated attempt are called **brute force attack.**

1. **Trust exploitation**

although it is more of a technique than a hack itself, trust exploitation refers to an attack in which an individual gains advantage of a trust relationship with a network. A classic example is a perimeter network connection from a cooperation.

These network segments often house domain name systems (DNS, SNTP and ATTP servers). Because all these servers reside on the same segments, the compromise of one system can lead to the compromise of the other because these systems usually trust others.

1. **Port redirection**

These are types of ports exploitations that uses a compromised host to traffic through a fire wall. Consider a fire world with three interfaces and a host on each interface. The host on the outside can reach the host on the public services segment but not the host on the private segment. These publicly assessable segment is commonly referred to as a **demilitarised zone (DNZ).** The host on the public services segment can reach the host on both the outside and the private segment. If hackers where able to compromise the public services segment host, they could install software to redirect traffic from the outside host directly to the private host.

1. **Man in the middle attack**

It requires that the hacker should have access to the network packet that came across a network. An example can be someone who is working for an internet service provider (**ISP**) and has access to all network packets transferred between the ISP network and any other network.

1. **Social engineering**

The easiest hack involves no computer skill at all. If an intruder can trick a member of an organisation into given over valuable information such as **location of files, servers and passwords,** the process of hacking is made immeasurably easier. Users of internet systems usually receive messages that request password or credit card information to set up their accounts or reactivate settings. Users of these systems must be worn early and frequently not to reveal sensitive information password or otherwise, to people claiming to be administrators. In reality, administrators of computer systems do not need to know user’s password to perform administrative stack.

1. **Phishing**

It is a type of social engineering attack that involves the use of emails and other types of messages in an attempt to treat others into providing sensitive information. The phisher masquerades as a trusted party that has seemingly legitimate need for a sensitive information. Frequent phishing scams involves sending out spam email that appear to be from common online banking or auction site.

* + 1. **Denial of service attack (DOS)**

It implies that an attacker disables or corrupt network systems or services with the intension to deny services to internet users. It involves either crashing the system or slowing it down to the point that it is unusable. It can also be as simple as deleting or corrupting information. In most cases, performing the attacks simple involves running a hack or scrip. It takes many forms, prevents authorised person from using the service by occupying system resources.

The following are some common examples of denial of service treats:

* **Pink of death:** this attack modifies the IP portion of the header, indicating that there is more data in the packet than there actually is; causing the receiving system to crash.
* **E-mail bombs**: programs can send bulk emails to individuals, list or domains monopolising email services.
* **CPU hogging:** this attacks constitutes programs such as trojan horse, viruses that ties up CPU cycles, memory and other resources
  + 1. **Warm viruses and Trojans horse attack**

A malicious software is inserted in a host to damage a system, corrupt a system, replicate or deny services or access to network. They can also allow information system to be copied or echoed to other systems. The nature of all these treats is changing from the relatively simple virus of 1980s to the more complex and damaging viruses in recent years. Today, the hacking tools are powerful and highly spread with the new danger self-spreading blending worm such as **slammer and blaster.**

The old base of attacks that take days or weeks to spread are over. Treats now spread worldwide in a matter of minutes. The next generations of attacks are expected to spread in just seconds.

**WORM**

**A** worm is a self-contained and independent program that is usually designed to propagate or spin itself on infected systems and to seek other systems via available networks. One of the first and perhaps the most famous worms was the internet worm created and released by **Robert Morris in 1986.**

**Morris** wrote worm his program and released it on to the internet. The worm functioning was relatively **benign** and the spreading was very rapid in such a way that it didn’t take long for the worm to consume all the CPU and memory resources until the systems crashed. The costs to clean up the internet worm was estimated to be in the **tenths of millions of dollars. Morris** was arrested, persecuted and convicted for his vandalism

**VIRUSES**

A virus is a parasitic program than cannot function independently. It is called a virus because **like its biological counter parts, it requires a host to function.** In case of computer virus, a host is some other program to which the virus attaches itself. A virus is usually spread by executing an infected program or by sending an infected file to someone else usual in the form of an email attachment. There are several virus scanning programs available on the market, most are effective against most viruses. Unfortunately, however, they incapable of recognising and adapting to new viruses. In general, virus scanning programs rely on recognising the signature of known viruses, turning to a database of known virus signatures that they use to compare against scanned results.

**TROJAN HORSE**

It is a program or code fragment that hides inside a program and performs a disguise function. This can be accomplished by modifying the existing program or by simply replacing the existing program with a new one. An example can be a password **grabber program.**

**THE TRACK DOORS/ THE BACK DOORS**

It is an undocumented way of gaining access to a system that is built into the system by its designer. It can also be a program that has been altered to allow someone to get privilege access to a system or process.

*CHAPTER V: POLICIES AND PROCEDURES*

**Introduction**

For most organisations, network and system security policies and procedures save the purpose of ensuring information security. They achieve this by defining what constitute information security, why it is important and hoe to maintain it. In addition, the policies and procedures define the acceptable level of information security. Before doing so, one must first but in place a process that determines what is an adequate level of security for any given organisation. We should recall from chapter one that: **the elements of information security include: confidentiality, integrity, availability, authentication and access control.**

**A**ll these fives elements need to be addressed whatever policies and procedures are implemented in the information security. In general terms, security policies are a set of rules and procedures that regulates how and organisation manages, uses, protect and distributes all information that directly or indirectly patterns or belongs to that organisation.

1. **Policies versus procedures**

Policies should always be developed before procedures, it should be concerned with what assets should be protected and why they should be protected. Procedures on the other hand must be much more precise and detailed. It must be concern with the specific measures necessary to protect the organisation assets.

1. **Information security policy objectives**

There are various reasons for an organisation to develop network and system security policies and procedures. Some reasons concern the direct benefits that an organization gains from having policies and procedures such as preventing and detecting fraud or hackers. Other benefits are indirect in that the policies protect the organization from potential liabilities or safe it from possible embarrassment.

Below is the list of some objectives generally associated with network security policies?

1. **Managing risk:** the primary goal of any policy concerning network and system security is to manage risk. It is almost impossible to completely secure an organisation’s information assets; as a result, an organisation needs to identify the risk that it faces and develop measures to minimise the impact of those risks.
2. **Insuring business continuity:** organizational policies and procedures should insure business resumption by outlining the appropriate actions necessary in the response of an incidence or disaster.
3. **Defining responsibilities, expectation and acceptable behaviours:** for any policy or procedure to be effective, those individuals subject to the policy or procedure must understand what is requires of them to comply. In addition, employees need to understand their responsibilities and how they may vary depending on the circumstances.
4. **Protecting the organisation from liability:** the policies and procedures developed by an organisationare often required to protect it from legal responsibility. In some cases, the existence of the policies and procedures are essential to demonstrate that an organisation did not approved by an end user action or that an employee was not acting with the authorisation of the organisation.
5. **Ensuring information integrity and confidentiality**

Ensuring the integrity and confidentiality of an organisation’s information is fundamental. Without information integrity, an organisation cannot make sound business decisions. Without information confidentiality, an organisation will lose its competitive edge through the loss of proprietary information regarding products, customers and even partners.

**5.3 Developing security policies**

For an organization’s information security policies and procedures, to achieve the stated objectives, it is essential that certain elements be included in the policies and procedures. These element can be thought of as key measures for the success of an organisation’s policy and procedures. The elements are the stepping stones in the development process. They are listed as follows:

* Identifying the organization’s assets
* Defining the risk
* Defining how information assets are to be managed
* Defining how information assets are to be accessed and what process will be used for authentication
* Defining clearly and in detail what does and does not constitute appropriate use of company owned electronic media and services.
* Clearly defining what kind of information may be accessed and distributed and by what means
* Defining what controls are to be put in place
* Notifying users of monitoring and auditing procedures, information disclosure and consequences for non-compliance
* Identifying those responsible for security enforcement and how policies and procedures will be enforced
* Developing steps to be taken in the event of non-compliance with policy, a security breach or a disaster

The first step is to determine responsibility for information security policy development. Too often the IT unit is given sole responsibility for this task, however, if the policies and procedures are to be comprehensive. It will require the active participation of all business units. Development of information security policies must be a collaborative effort between the IT units and the other business unit within an organization. Any policy or procedure implanted without the active participation of other business units faces an uphill battle.

The most critical factor in the success or failure of any information security policy is the support from senior management. The policy developers must be empowered by senior managers to implement the measures necessary to protect the organization’s information assets. Without the support of the senior management, any policies or procedures implemented are doomed to fail.

To go through the risk assessment process to determine what you want to protect, why you want to protect it and from what you need to protect it. As described in chapter one, the steps associated with risk assessment includes the following:

* The identification and prioritization of assets
* Identification of vulnerabilities
* Identification of threats and their probabilities
* Identification of counter measures

If you make a process too annoying, people will ignore it. If you make password too hard to remember, people will write them down. If you make the process of access to a room too difficult, people will probe open the door? All security measures whenever possible should complement the operational and business needs of an organization.

**Policies and procedure manners**

For a security policy to be practical, it must be documented. The plan must also be made available as a reference to all those subject to the policy. The policy and procedure manuals need to be kept current and updated with any necessary changes. Modifications to systems personnel, business priorities and other environmental factors must be reflected in a plan.

**Policy awareness and education**

A policy is of no value if no one knows what it states, end users and personnel must understand management expectations and their responsibilities in regard to complying with the organization’s policies. End users and employees must also understand the consequences of noncompliance. This aspect is very important for protecting the organization if litigation results from noncompliance.

**Policy Enforcement**

The only way to ensure compliance is monitoring and auditing. Those responsible for enforcing the IT security policies must have a support

**Security policy suggestions**

Remember that the major emphasis of all policies and procedures is to prevent bad things from happening. It doesn’t matter whether the bad thing is a mistake, a disaster or just being misled. Where design policies and procedures are flexible enough to address most probable threats, that is why a risk analysis is such an important part of the process

**The use of company owned electronic media and services**

With the advent of new technologies, organizations are finding themselves relying increasingly on electronic modes of communication and information storage. Most employees in an organization have access to one or more forms of electronic media or service. They include the following:

* Computers
* Email
* Telephones and voicemail
* Fax machines
* LANs
* Intranet
* The web

**Physical security**

Physical access to IT facilities should be restricted to only those authorized to perform their job functions. A policy should define who the appropriate individuals are and what policies and procedures are enacted. The type of issues addressed should include computer room or network centre, fire suppression systems and environmental controls e.g. if the computer room is not monitored constantly, is there any automated system in place that alerts someone in the event that the fire suppression system is triggered or the environmental control failed.

**CRISIS MANAGEMENT**

**Introduction**

This chapter describes the planning process that every organization should go through to prepare for an event that threatens the operation or viability of the organization. Disaster recovery and computer security incident response planning can be thought of as two sides of a coin. The two topics are closely related and share some common methodologies and goals. Both are concerned with ensuring the availability and integrity of an organization’s networks and systems.

**Disaster recovery planning**

From time to time, many businesses face a catastrophic event that can threaten the viability of the organization. Accordingly, every organization should formulate a set of procedures that details actions to be taken in anticipation of a catastrophic action. The procedures should be designed as if the catastrophic event is inevitable and is going to take place tomorrow. This type of plan is referred to as disaster recovery plan. In some organizations, it is called contingency planning or business resumption planning.

Some organizations believe that having hot site recovery services (**This is a Commercial disaster recovery service that allows business to continue computer and network operations in the event of a computer or event disaster**) is the same as having a disaster recovery plan. A hot site is a facility that is designed to be activated in the event that the organization’s computers are rendered inoperable. A hot side is preconfigured with the power, environmental controls, telecommunications and computers necessary for an organization to resume operations with a minimal disruption in service.

The requirements for a disaster recovery plan vary for each organization. However, for most organizations, the minimum objectives of a disaster recovery plan is to provide the information and procedures necessary to do the following:

1. A response to the occurrence of a disaster
2. Notify the necessary personnel
3. Assemble disaster recovery teams
4. Recover data that may have been lost as a result of the occurrence
5. Resume processing as quickly as possible to ensure minimal disruption of operations
6. Comply with any regulatory requirements that dictate the existence of a disaster recovery plan for the organization

Every organization that uses electronic media and services should have a policy that clearly defines the acceptable use of these media and services as company properties. The policies should not only exist to protect the organization but also to protect the employees of the organization.

One of the key factors in the success of the business resumption plan is proper planning for the IT group. Most organizations today rely mostly in computers, networks, telecommunications and IT in general, as a result IT plays a key role in most organization’s disaster recovery planning

**What level of preparation**

The extent to which an organization is willing to invest resources into IT disaster recovery planning should be directly related to the business of the organization. Different organizations have different recovery needs with regard to IT. As a result, the plan developed by different organizations should reflect their need e.g. a non-profit organization that relies on fund raising for income could probably survive several days, if not weeks of downtime. A bank on the other hand could find itself out of business if its systems were down for that period. Most banks could accept a few hours or a day or downtime as a result of a catastrophic occurrence while a stock exchange like NASDAG could find itself in financial ruin if its system was down for a few hours in it was unable to trade.

**What to restore first**

Just as different organizations have different recovery needs, different functions within an organization have different levels of priority for recovery. Any IT disaster recovery plan should assign levels of importance to each system to ascertain which systems will be given priority when restoring services. Critical functions need to be identified prior to the occurrence of a disaster so that when a disaster does occur. IT does not waste time installing unnecessary systems instead of those that are truly required. One approach is to gather these information through an assessment team headed by the IT group but with the participation of management and staff knowledgeable in the functioning of the organization and familiar with the various systems and applications.

**Review and test**

From a cost analysis perspective, successful disaster recovery preparation is proportionate to the potential lost.

From an operational perspective. A successful disaster recovery plan is responsive to the business needs of the organization.

From a general management perspective, a disaster recovery plan must be updated with any necessary changes. Modifications to systems, personnel, business priorities and other environmental factors must be reflected in the plan

**Computer security incident response plan**

Another incidence of crisis management planning is computer and network security incidence and response planning (CSIRP). This plan outlines actions that the company must take when there is fraud or misuse of company owned electronic media or services. A theft or destruction of company information, a penetration or attack on company owned systems and networks. The plan should address such things as what constitute a security incident. Identifying key personnel, communication and notification access as well as installation process,

Since security incidence occur with more frequency than disasters, organizations are finding that security incidence resource planning in some respect is more important than disaster recovery planning. In general, organisations experience few real disasters but deal with many security incidence. Denial of service attacks and virus outbreaks are becoming common

**OPERATING SYSTEMS SECURITY**

Network security begins at the individual system level. As the saying goes, a chain is only as strong as its weakest link and a network is nothing more than a change of systems. As a result, for a network to have a high level of security, all of the systems on the network must be properly administered and monitored.

Very few organizations adequately administer and monitor systems that reside on the internal network. This defence in-depth approach requires more of commitment to security than most organizations are willing to make. Instead most organizations choose to employ a perimeter defence. This approach relies on hardened border systems usually firewalls and routers that are designed to monitor and control graphic between and internal trusted network and an internal untrusted network. The assumption is that the perimeter or bother systems will secure the external systems. There are a number of problems with the perimeter defence. First, if an organizations border systems are every compromised and penetrated, the entire internal network will be open to attack. Hardening the internal systems can help to decrease the amount of damage from the breach of the perimeter system. At the very least. Adequate monitoring of the internal systems may at least detect a breach from the outside.

In addition, every organization that uses computers faces the threat of hacking from individuals within the organization. Employees with malicious intent who want to obtain information such as employee salaries or view other employees files are a threat to an organizations computer and networks

Critical systems should be constructed to monitor logins, failed logins and all network activities. Most network operating systems have utilities for monitoring this kind of activities. Unix in particular can be configured to record all sorts of activities that can be reviewed for security purposes e.g. almost all versions of UNIX allows you to monitor logins through the WTMP files. One simple security measure an organization can employ for UNIX system is to review the fail login log file on the daily basis. When reviewing the fail login log file. If there are multiple entries for a single account. It may be an indication that something is wrong and should be investigated. If there are unfamiliar IP addresses attempting to connect to the system, then this should also be investigated. Both of these activities could be indication that someone is probing the system.

Since these logs reside on the system’s local disk drive, it is possible for someone to alter the files, it is required that hard copy points of the logs should be generated and stored. The log file should also be cleared daily or weekly. There are a couple of reasons for doing this. First it reduces the risk of the files being altered, second, in the event of the system is ever compromised. It is necessary to refer to the hard copy printed to help determine exactly when the system was first compromised. The process of printing and clearing the files can be automated.

All the methods described above comprise a first step to securing and monitoring a system. These elementary steps can help to identify when a system is being probed. Even if a system sits on a secure or trusted network or behind a firewall. It is necessary to secure and monitor the system. Note that a network is only as secured as the information systems on that network.

**Passwords**

The measure of a system’s security is how effective it is in authenticating and identifying its users. There are 3 basic schemes for identification and authentication:

* Something you know
* Something you have
* Something you are

The most commonly employed scheme is something you know and the most widely implemented variation of this scheme is the use of passwords. Passwords are used by most systems or network as the first and usually only means of identification and authentication. Even though passwords are the most widely deployed scheme of authentication, they are perhaps the weakest link in any system security scheme. However, there are a number of measures and organization can take to lessen the risk associated with the use of passwords. Obviously, passwords should never be shared between end users or employees. Accordingly, every organization should have a policy that clearly states the users responsibility to maintain password secrecy, and the consequences for failing to do so.

People often use passwords that are to short and/or too easy to guest or deceiver or they simply never change them. There are programs known as crackers that are easily obtained from the internet and can be run in most systems to decipher the password file. Even if a password is encrypted for transmission between a client and server. It can be captured and transmitted at a later time as part of replay attack. The counter measures for the replay attacks include the one time passwords or the use of Kerberos. There are four general types of attacks on systems password.

1. **Brute force attack.**

It tries every combination of keys or algorithms to break a cipher. Doing so can require tremendous resources. Usually this type of attack require computer assistance. If the algorithm is simple or the key is small then the resources required could be provided by a simple pc. If the algorithm is sophisticated or the key is large then advanced computing power might be required.

1. **Dictionary based attack**

They are much more effective than the brute force attack. Many operating systems maintain a password file. This password file is a database of usernames and passwords. The passwords are almost always stored in the password file in an encrypted format. Dictionary based attacks actually utilize programs that compare the encrypted passwords in the password file to the encrypted word in the dictionary file. When a match is found, the password is decrypted. Obviously, the dictionary based methods is most effective against passwords that are common or known words, names or terms. Some systems try to get around this problem by not having the password file or not storing the password. Windows NT for instance does not store passwords in a password file.

1. **Password sniffing**

As stated in chapter 2, network sniffing or packet sniffing is a process of monitoring a network to gather information that can be used in an attack. One of the things that can be observed through network sniffing is passwords. With the proper tools, a hacker can monitor a network packet to obtain passwords or IP addresses. Password sniffing is particular a threat for users who log into a system over a network using telnet, rlogin, FTP or terminal emulator. These programs do not encrypt passwords. As a result, when a user enters his or her password, it is transmitted in clear meaning that anyone monitoring the network with the sniffer can read the network. There are several different sniffer programs available. Some are commercial products and others are freeware

**For example: the sniffer pro is a commercial software product**