ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha

DIPLOMA IN CYBER SECURITY

DCS-04 APPLICATION CYBER SECURITY

BLOCK

2 SECURITY MANAGEMENT

EXPERT COMMITTEE

Dr.P.K.Behera (Chairman)
Reader in Computer Science
Utkal University
Bhubaneswar, Odisha

Dr.J.R.Mohanty (Member)
Professor and HOD
KIIT University
Bhubaneswar, Odisha

Sri Pabitrananda Pattnaik (Member)
Scientist-E, NIC
Bhubaneswar, Odisha

Sri Malaya Kumar Das(Member)
Scientist-E, NIC
Bhubaneswar, Odisha

Dr. Bhagirathi Nayak(Member)
Professor and Head (IT & System)
Sri Sri University
Bhubaneswar,Odisha

Dr.Manoranjan Pradhan (Member)
Professor and Head (IT & System)
G.I.T.A
Bhubaneswar, Odisha

Sri Chandrakant Mallick (Convener)
Consultant (Academic)
School of Computer and Information Science
Odisha State Open University
Sambalpur, Odisha

DIPLOMA IN CYBER SECURITY

Course Writers

Chandrakant Mallick
Odisha State Open University, Sambalpur, Odisha
Bijay Kumar Paikaray
Centurion University of Technology and Management, Odisha
Guru Prasad Dash
Ravenshaw University, Cuttack, Odisha

UNIT-1 DISASTER RECOVERY

Unit Structure

1.0 Introduction

Organizations cannot always avoid disasters, but with careful planning the effects of a disaster can be minimized. The objective of a disaster recovery plan is to minimize downtime and data loss. The primary objective is to protect the organization in the event that all or parts of its operations and/or computer services are rendered unusable. The plan minimizes the disruption of operations and ensures that some level of organizational stability and an orderly recovery after a disaster will prevail. Minimizing downtime and data loss is measured in terms of two concepts: the recovery time objective (RTO) and the recovery point objective (RPO). The recovery time objective is the time within which a business process must be restored, after a major incident (MI) has occurred, in order to avoid unacceptable consequences associated with a break in business continuity. The recovery point objective (RPO) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a MI. The RPO is expressed backwards in time (that is, into the past) starting from the instant at which the MI occurs, and can be specified in seconds, minutes, hours, or days. The recovery point objective (RPO) is thus the maximum acceptable amount of data loss measured in time. It is the age of the files or data in backup storage required to resume normal operations after the MI.

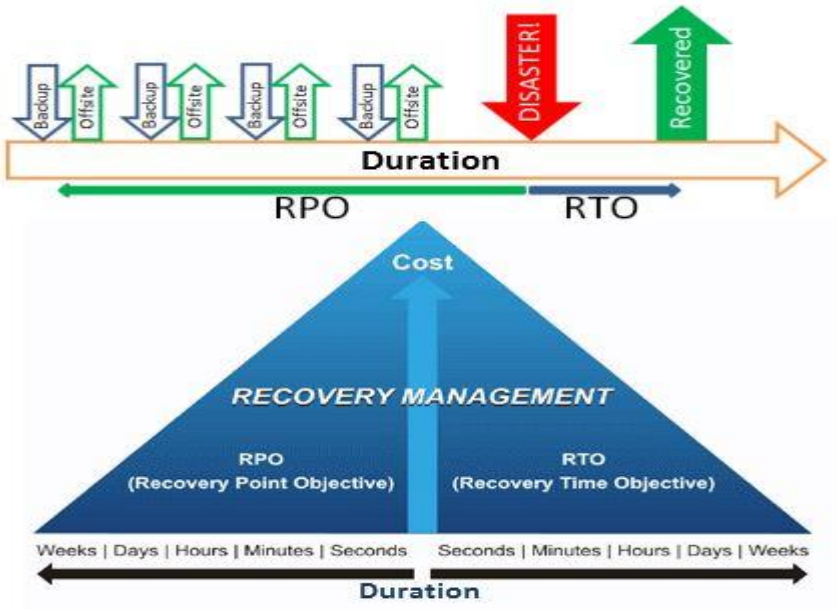

Fig: A DR plan illustrating the chronology of the RPO and the RTO

1.1 Learning Objectives

After going through this unit, you will able to:

- Know about disaster recovery plan (DRP)
- Know the benefits of DRP
- Understand the relationship of DRP with Business continuity plan
- Know, why DRP is important
- Know different types of Disasters
- Know different types of planning methodology
- Know DRP controversies

1.2 The Development of Disaster Recovery

Disaster recovery was developed in late 1970s because computer center managers started to recognize dependence of their organizations on their systems. Most systems at that time were batch-oriented mainframes that could be down for some days before significant damage could be done to organization. As the knowledge sensibility of potential business disruption which should follow the IT-related disaster, disaster recovery industry was developed in order to provide Sun Information Systems to the backup computer centers becoming the first major US commercial hot site vendor in 1978. (Sun Information Systems became later SunGard Availability Services). During 1980s and 1990s, customer's knowledge sensibility and this industry grew rapidly through an advent of real-time processing and open systems that increased the dependence of different organizations on their IT systems. With the rapid growth during 1990s and 2000s of the Internet, organizations in different sizes became dependent on continuous availability of their IT systems. This increasing dependence on the IT systems, besides the increased knowledge sensibility from large-scale disasters like tsunami, flood, earthquake, and volcanic eruption, could spawn disaster recovery-related services and products, ranging from the high-availability solutions to the hot-site facilities. The rise of the cloud computing technology in 2010 continues that trend and nowadays, it even matters less where computing services are served physically, just too long as network itself is reliable sufficiently. Recovery as a Service (RaaS) is now one of the security features of the cloud computing as it's promoted by Cloud Security Alliance.

1.3 What is Disaster Recovery Plan?

A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster. It is "a comprehensive statement of consistent actions to be taken before, during and after a disaster." The disaster could be natural, environmental or man-made. Man-made disasters could be intentional (for example, an act of a terrorist) or unintentional (that is, accidental, such as the breakage of a man-made dam). Given organizations' increasing dependency on information technology to run their operations, a disaster recovery plan, sometimes erroneously called a Continuity of Operations Plan (COOP), is increasingly associated with the recovery of information technology data, assets, and facilities.

1.4 Importance of Disaster Recovery Plan

As IT systems have become increasingly critical to the smooth operation of a company, and arguably the economy as a whole, the importance of ensuring the continued operation of those systems, and their rapid recovery, has increased. For example, of companies that had a major loss of business data, 43% never reopen and 29% close within two years. As a result, preparation for continuation or recovery of systems needs to be taken very seriously. This involves a significant investment of time and money with the aim of ensuring minimal losses in the event of a disruptive event.

1.5 Don't ignore it until it's too late!

Maybe software developers are naturally optimistic but in my experience they rarely consider system failure or disaster scenarios when designing software. Failures are varied and range from the likely (local disk failure) to the rare (tsunami) and from low impact to fatal (where fatal may be the death of people or bankruptcy of a business). Failure planning broadly fits into the following areas:

- Avoiding failure
- Failing safely
- Failure recovery
- Disaster Recovery

Avoiding failure is what a software architect is most likely to think about at design time. This may involve a number of High Availability (HA)

techniques and tools including; redundant servers, distributed databases or real time replication of data and state. This usually involves removing any single point of failure but you should be careful to not just consider the software and hardware that it immediately runs on - you should also remove any single dependency on infrastructure such as power (battery backup, generators or multiple power supplies) or telecoms (multiple wired connections, satellite or radio backups etc). Failing safely is a complex topic that I touched on recently and may not apply to your problem domain (although you should always consider if it does). Failure recovery usually goes hand-in-hand with High Availability and ensures that when single components are lost they can be re-created/started to join the system. There is no point in having redundancy if components cannot be recovered as you will eventually lose enough components for the system to fail!

1.6 Benefits of Disaster Recovery

Like every insurance plan, there are benefits that can be obtained from the drafting of a disaster recovery plan. Some of these benefits are:

1. Providing a sense of security
2. Minimizing risk of delays
3. Guaranteeing the reliability of standby systems
4. Providing a standard for testing the plan
5. Minimizing decision-making during a disaster
6. Reducing potential legal liabilities
7. Lowering unnecessarily stressful work environment

1.7 Classification of Disasters

Disasters can be classified into two broad categories:

1.7.1 Natural Disasters

The first is natural disasters. A **natural disaster** is a major adverse event resulting from **natural** processes of the Earth. The examples include floods, tsunamis, tornadoes, hurricanes/cyclones, volcanic eruptions, earthquakes, heat waves, and landslides. While preventing, a natural disaster is very difficult, risk management measures such as avoiding disaster-prone situations and good planning can help. A natural disaster is a major adverse event resulting from the earth's natural hazards. Other types of disasters include the more cosmic scenario of an asteroid hitting the Earth.

Fig: Natural Disaster

1.7.2 Man-Made Disasters

Man-made disasters are the consequence of technological or human hazards. Examples include stampedes, urban fires, industrial accidents, oil spills, nuclear explosions/nuclear radiation and acts of war. Other types of man-made disasters include the more cosmic scenarios of catastrophic global warming, nuclear war, and bioterrorism.

Fig: Man-made disaster

1.8 Relationship to the Business Continuity Plan

The Business Continuity Plan (BCP) is a comprehensive organizational plan that includes the disaster recovery plan. The Institute further states that a Business Continuity Plan (BCP) consists of the five component plans:

1. Business Resumption Plan
2. Occupant Emergency Plan
3. Continuity of Operations Plan
4. Incident Management Plan
5. Disaster Recovery Plan

The Institute states that the first three plans (Business Resumption, Occupant Emergency, and Continuity of Operations Plans) do not deal with the IT infrastructure. They further state that the Incident Management Plan (IMP) does deal with the IT infrastructure, but since it establishes structure and procedures to address cyber-attacks against an organization's IT systems, it generally does not represent an agent for activating the Disaster Recovery Plan, leaving The Disaster Recovery Plan as the only BCP component of interest to IT. Disaster Recovery Institute International states that disaster recovery is the area of business continuity that deals with technology recovery as opposed to the recovery of business operations.

1.9 It Disaster Recovery Control Measures

Control measures are steps or mechanisms that can reduce or eliminate various threats for organizations. Different types of measures can be included in disaster recovery plan (DRP). Disaster recovery planning is a subset of a larger process known as business continuity planning and includes planning for resumption of applications, data, hardware, electronic communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity.

IT disaster recovery control measures can be classified into the following three types:

1. **Preventive measures** - Controls aimed at preventing an event from occurring.
2. **Detective measures** - Controls aimed at detecting or discovering unwanted events.
3. **Corrective measures** - Controls aimed at correcting or restoring the system after a disaster or an event.

Good disaster recovery plan measures dictate that these three types of controls be documented and exercised regularly using so-called "DR tests".

1.10 Disaster Recovery Planning Methodology

According to Geoffrey H. Wold of the Disaster Recovery Journal, the entire process involved in developing a Disaster Recovery Plan consists of 10 steps:

1.10.1 Obtaining Top Management Commitment

For a disaster recovery plan to be successful, the central responsibility for the plan must reside on top management. Management is responsible for coordinating the disaster recovery plan and ensuring its effectiveness within the organization. It is also responsible for allocating adequate time and resources required in the development of an effective plan. Resources that management must allocate include both financial considerations and the effort of all personnel involved.

1.10.2 Establishing a Planning Committee

A planning committee is appointed to oversee the development and implementation of the plan. The planning committee includes representatives from all functional areas of the organization. Key committee members customarily include the operations manager and the data processing manager. The committee also defines the scope of the plan.

1.10.3 Performing a Risk Assessment

The planning committee prepares a risk analysis and a business impact analysis (BIA) that includes a range of possible disasters, including natural, technical and human threats. Each functional area of the organization is analyzed to determine the potential consequence and impact associated with several disaster scenarios. The risk assessment process also evaluates the safety of critical documents and vital records. Traditionally, fire has posed the greatest threat to an organization. Intentional human destruction, however, should also be considered. A thorough plan provides for the "worst case" situation: destruction of the main building. It is important to assess the impacts and consequences resulting from loss of information and services. The planning committee also analyzes the costs related to minimizing the potential exposures.

1.10.4 Establishing Priorities for Processing and Operations

At this point, the critical needs of each department within the organization are evaluated in order to prioritize them. Establishing priorities is important because no organization possesses infinite resources and criteria must be set as to where to allocate resources first. Some of the areas often reviewed during the prioritization process are functional operations, key personnel

and their functions, information flow, processing systems used, services provided, existing documentation, historical records, and the department's policies and procedures. Processing and operations are analyzed to determine the maximum amount of time that the department and organization can operate without each critical system. This will later get mapped into the Recovery Time Objective. A critical system is defined as that which is part of a system or procedure necessary to continue operations should a department, computer center, main facility or a combination of these be destroyed or become inaccessible. A method used to determine the critical needs of a department is to document all the functions performed by each department. Once the primary functions have been identified, the operations and processes are then ranked in order of priority: essential, important and non-essential.

1.10.5 Determining Recovery Strategies

During this phase, the most practical alternatives for processing in case of a disaster are researched and evaluated. All aspects of the organization are considered, including physical facilities, computer hardware and software, communications links, data files and databases, customer services provided, user operations, the overall management information systems (MIS) structure, end-user systems, and any other processing operations. Alternatives, dependent upon the evaluation of the computer function, may include: hot sites, warm sites, cold sites, reciprocal agreements, the provision of more than one data center, the installation and deployment of multiple computer system, duplication of service center, consortium arrangements, lease of equipment, and any combinations of the above. Written agreements for the specific recovery alternatives selected are prepared, specifying contract duration, termination conditions, system testing, cost, any special security procedures, procedure for the notification of system changes, hours of operation, the specific hardware and other equipment required for processing, personnel requirements, definition of the circumstances constituting an emergency, process to negotiate service extensions, guarantee of compatibility, availability, non-mainframe resource requirements, priorities, and other contractual issues.

1.10.6 Collecting Data

Among advised data gathering materials or documentation usually included are different lists such as (Critical telephone numbers list, master vendor list, employee backup position listing, master call list, notification checklist), inventories such as (Off-site storage location equipment,

documentation, communications equipment, microcomputer hardware and software, forms, insurance policies, office equipment, workgroup and data center computer hardware, office supply, telephones, etc.), distribution register, temporary location specifications, software and data files backup/retention schedules, and any other lists, materials, inventories and documentation. The pre-formatted forms are usually used in order to facilitate data gathering process.

1.10.7 Organizing and Documenting a Written Plan

Next, an outline of the plan's contents is prepared to guide the development of the detailed procedures. Top management reviews and approves the proposed plan. The outline can ultimately be used for the table of contents after final revision. Other four benefits of this approach are that

1. It helps to organize the detailed procedures,
2. Identifies all major steps before the actual writing process begins,
3. Identifies redundant procedures that only need to be written once, and
4. Provides a road map for developing the procedures.

It is often considered best practice to develop a standard format for the disaster recovery plan so as to facilitate the writing of detailed procedures and the documentation of other information to be included in the plan later. This helps ensure that the disaster plan follows a consistent format and allows for its ongoing future maintenance. Standardization is also important if more than one person is involved in writing the procedures. It is during this phase that the actual written plan is developed in its entirety, including all detailed procedures to be used before, during, and after a disaster. The procedures include methods for maintaining and updating the plan to reflect any significant internal, external or systems changes. The procedures allow for a regular review of the plan by key personnel within the organization. The disaster recovery plan is structured using a team approach. Specific responsibilities are assigned to the appropriate team for each functional area of the organization. Teams responsible for administrative functions, facilities, logistics, user support, computer backup, restoration and other important areas in the organization are identified. The structure of the contingency organization may not be the same as the existing organization chart. The contingency organization is usually structured with teams responsible for major functional areas such as administrative functions, facilities, logistics, user support, computer backup, restoration, and any other important area. The management team is especially important because it coordinates the recovery process. The team assesses the disaster, activates

the recovery plan, and contacts team managers. The management team also oversees, documents and monitors the recovery process. It is helpful when management team members are the final decision-makers in setting priorities, policies and procedures. Each team has specific responsibilities that are completed to ensure successful execution of the plan. The teams have an assigned manager and an alternate in case the team manager is not available. Other team members may also have specific assignments where possible.

1.10.8 Developing Testing Criteria and Procedures

Best practices dictate that DR plans be thoroughly tested and evaluated on a regular basis (at least annually). Thorough DR plans include documentation with the procedures for testing the plan. The tests will provide the organization with the assurance that all necessary steps are included in the plan. Other reasons for testing include:

- Determining the feasibility and compatibility of backup facilities and procedures.
- Identifying areas in the plan that needs modification.
- Providing training to the team managers and team members.
- Demonstrating the ability of the organization to recover.
- Providing motivation for maintaining and updating the disaster recovery plan.

1.10.9 Testing the Plan

After the testing procedures been completed, initial “dry run” plan is performed through conducting structured walk-through test. This test will provide an additional information towards any further changes in procedures which are not effective, steps which may need to be included, and other appropriate adjustments. Remember that these cannot become an evident unless actual dry-run test is performed. The plan is updated subsequently in order to correct any problems that are identified during the test. But initially, the testing of the plan will be done in sections and even after normal business hours in order to minimize disruptions to overall operations of organization and as plans are further polished, future tests also occur during the normal business hours.

Different types of tests include:

1. Checklist tests.
2. Full interruption tests.

3. Parallel tests.
4. Simulation tests.

1.10.10 Obtaining Plan Approval

Once the disaster recovery plan has been written and tested, the plan is then submitted to management for approval. It is top management's ultimate responsibility that the organization has a documented and tested plan. Management is responsible for:

1. Establishing the policies, procedures and responsibilities for comprehensive contingency planning, and
2. Reviewing and approving the contingency plan annually, documenting such reviews in writing.

Organizations that receive information processing from service bureaus will, in addition, also need to:

- Evaluate the adequacy of contingency plans for its service bureau, and
- Ensure that its contingency plan is compatible with its service bureau's plan.

1.11 Caveats/Controversies

Due to its high cost, disaster recovery plans are not without critics. Cormac Foster has identified five "common mistakes" organizations often make related to disaster recovery planning:

1.11.1 Lack of Buy-In

One factor is the perception by executive management that DR planning is "just another fake earthquake drill" or CEOs that fail to make DR planning and preparation a priority, are often significant contributors to the failure of a DR plan.

1.11.2 Incomplete RTOs and RPOs

Another critical point is failure to include each and every important business process or a block of data. "Every item in your DR plan requires a Recovery Time Objective (RTO) defining maximum process downtime or a Recovery Point Objective (RPO) noting an acceptable restore point. Anything less creates ripples that can extend the disaster's impact." As an example, "payroll, accounting and the weekly customer newsletter may not be mission-critical in the first 24 hours, but left alone for several days, they can become more important than any of your initial problems".

1.11.3 Systems Myopia

A third point of failure involves focusing only on DR without considering the larger business continuity needs: "Data and systems restoration after a disaster are essential, but every business process in your organization will need IT support, and that support requires planning and resources." As an

example, corporate office space lost to a disaster can result in an instant pool of teleworkers which, in turn, can overload a company's VPN overnight, overwork the IT support staff at the blink of an eye and cause serious bottlenecks and monopolies with the dial-in PBX system.

1.11.4 Lax Security

When there is a disaster, an organization's data and business processes become vulnerable. As such, security can be more important than the raw speed involved in a disaster recovery plan's RTO. The most critical consideration then becomes securing the new data pipelines: from new VPNs to the connection from offsite backup services. Another security concern includes documenting every step of the recovery process—something that is especially important in highly regulated industries, government agencies, or in disasters requiring post-mortem forensics. Locking down or remotely wiping lost handheld devices is also an area that may require addressing.

1.11.5 Outdated Plans

Another important aspect that is often overlooked involves the frequency with which DR Plans are updated. Yearly updates are recommended but some industries or organizations require more frequent updates because business processes evolve or because of quicker data growth. To stay relevant, disaster recovery plans should be an integral part of all business analysis processes, and should be revisited at every major corporate acquisition, at every new product launch and at every new system development milestone.

1.12 Let us Sum-up

A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Organizations cannot always avoid disasters, but with careful planning the effects of a disaster can be minimized. Minimizing downtime and data loss is measured in terms of two concepts: the recovery time objective (RTO) and the recovery point objective (RPO). The recovery time objective is the time within which a business process must be restored, after a major incident (MI) has occurred, in order to avoid unacceptable consequences associated with a break in business continuity. The recovery point objective (RPO) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a MI. As IT systems have become increasingly critical to the smooth operation of a company, and arguably the economy as a whole, the importance of ensuring the continued operation of those

systems, and their rapid recovery, has increased. Benefits include providing a sense of security, Minimizing risk of delays, Guaranteeing the reliability of standby systems, Providing a standard for testing the plan, Minimizing decision-making during a disaster, Reducing potential legal liabilities, Lowering unnecessarily stressful work environment. A natural disaster is a major adverse event resulting from the earth's natural hazards.Man-made disasters are the consequence of technological or human hazards. Disaster Recovery Institute International states that disaster recovery is the area of business continuity that deals with technology recovery as opposed to the recovery of business operations. Control measures are steps or mechanisms that can reduce or eliminate various threats for organizations. Different types of measures can be included in disaster recovery plan (DRP) like Preventive measures, Detective measures and Corrective measures. With the help of planning methodology the impact of disaster can be minimized and Business continuity may be achieved.

1.13 Self Assessment Questions

1. What is disaster recovery plan (DRP)?

……
……
……
……
……

2. Why DRP is important? Write its benefits.

……
……
……
……
……

3. What is Disaster recovery? What are its impacts on different organization?

……
……
……
……
……

4. Describe different types of Disasters with appropriate example.

……
……
……
……
……

5. What is the relationship between BCP and DRP?

……
……
……
……
……

6. What are different types of Disaster recovery control measures?

……
……
……
……
……

7. Write the steps of Disaster Recovery planning methodology.

……
……
……
……
……

1.14 References & Further Readings

1. Information Security Assurance: Framework, Standards & Industry Best Practices (PGDCS-05), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security
2. *Disaster recovery.* Computer Business Research
3. *Disaster Recovery and Business Continuity, version 2011.* IBM.
4. A Brief History of Disaster Recovery, safetynet247.co.uk .
5. https://www.google.co.in//Image

UNIT-2 DIGITAL SIGNATURES

Unit Structure

2.0 Introduction

Cryptography today involves more than encryption and decryption of messages. It also provides mechanisms for authenticating documents using a digital signature, which binds a document to the possessor of a particular key, while a digital time stamp binds a document to its creation at a particular time. These are important functions which must take the place of equivalent manual authentication procedures as we move into the digital age. Cryptography also plays an important part in the developing field of digital cash and electronic funds transfer.

The encryption techniques applied for the following purposes:

- To protect privacy and confidentiality.
- To transmit secure information (e.g. credit card details)
- To provide authentication of the sender of a message.
- To provide authentication of the time a message was sent.

2.1 Learning Objectives

After learning this unit, you should be able to

- Understand the concept of digital signature.
- Understand Mechanism of Digital signature
- Know the uses and Importance of Digital signature.

Know the mechanism and use of digital signature certificates (DSC)

2.2 What is a Digital Signature?

A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).

A digital signature is the electronic equivalent of a handwritten signature, verifying the authenticity of electronic documents. In fact, digital signatures provide even more security than their handwritten counterparts.

Some banks and package delivery companies use a system for electronically recording handwritten signatures. Some even go so far as to use biometric analysis to record the speed with which you write and even how hard you press down, ensuring the authenticity of the signature. However, this is not

what is usually meant by digital signatures — a great relief to those of us with limited budgets and resources.

More often than not a digital signature uses a system of public key encryption to verify that a document has not been altered.

2.3 Applications of Digital Signature

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

2.4 Mechanism of Digital Signatures

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash - along with other information, such as the hashing algorithm - is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.

The value of the hash is unique to the hashed data. Any change in the data, even changing or deleting a single character, results in a different value. This attribute enables others to validate the integrity of the data by using the signer's public key to decrypt the hash. If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed. If the two hashes don't match, the data has

either been tampered with in some way (integrity) or the signature was created with a private key that doesn't correspond to the public key presented by the signer (authentication). A digital signature can be used with any kind of message - whether it is encrypted or not -- simply so the receiver can be sure of the sender's identity and that the message arrived intact. Digital signatures make it difficult for the signer to deny having signed something (non-repudiation) - assuming their private key has not been compromised - as the digital signature is unique to both the document and the signer, and it binds them together. A digital certificate, an electronic document that contains the digital signature of the certificate-issuing authority, binds together a public key with an identity and can be used to verify a public key belongs to a particular person or entity.

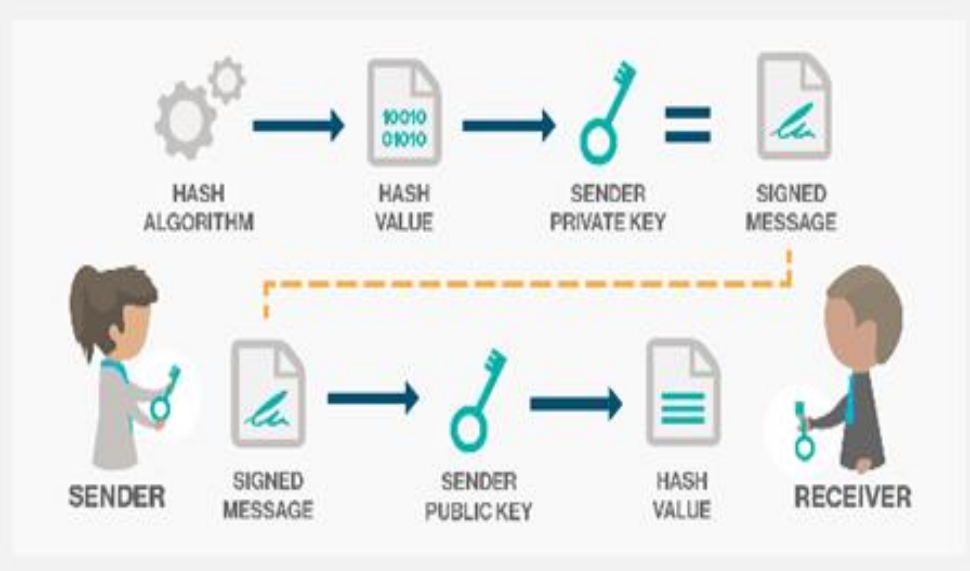

Fig: Digital Signature Process

Most modern email programs support the use of digital signatures and digital certificates, making it easy to sign any outgoing emails and validate digitally signed incoming messages. Digital signatures are also used extensively to provide proof of authenticity, data integrity and non-repudiation of communications and transactions conducted over the Internet.

2.5 What Is Public Key Encryption?

Public key encryption (PKE) is a cryptographic system that uses a system of two keys:

- a **private key**, which only you use (and of course protect with a **well-chosen, carefully protected passphrase**); and

- a **public key**, which other people use. Public keys are often stored on **public key servers**.

A document that is encrypted with one of these keys can be decrypted only with the other key in the pair.

For example, let's say that Alice wants to send a message to Bob using **PGP** (a popular public key encryption system). She encrypts the message with Bob's public key and sends it using her favorite email program. Once the message is encrypted with Bob's public key, only Bob can decrypt the message using his private key. Even major governments using supercomputers would have to work for a very long time to decrypt this message without the private key.

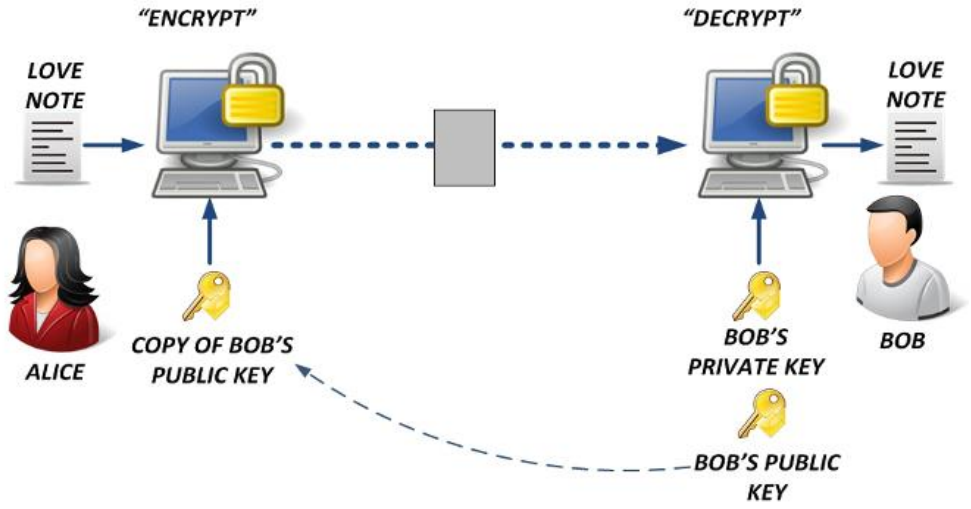

Fig: Public Key Encryption Process

2.6 What does PKE Have to do with Digital Signatures?

Digital signatures often use a public key encryption system. Consider Alice and Bob again: how can Bob be sure that it was really Alice who sent the message, and not the criminally-minded Eve pretending to be Alice?

This is where digital signatures come in. Before encrypting the message to Bob, Alice can sign the message using her private key; when Bob decrypts the message, he can verify the signature using her public key. Here's how it works:

1. Alice creates a digest of the message — a sort of digital fingerprint. If the message changes, so does the digest.

2. Alice then encrypts the digest with her private key. The encrypted digest is the digital signature.
3. The encrypted digest is sent to Bob along with the message.
4. When Bob receives the message, he decrypts the digest using Alice's public key.
5. Bob then creates a digest of the message using the same function that Alice used.
6. Bob compares the digest that he created with the one that Alice encrypted. If the digests match, then Bob can be confident that the signed message is indeed from Alice. If they don't match, then the message has been tampered with — or isn't from Alice at all.

If this sounds complicated, rest assured that the software makes it all very easy.

2.7 How to verify a signature from someone?

That's where digital certificates and certificate authorities come in. Let's start with how it works in PGP. Say that someone claiming to be Bob's acquaintance Carol sends a message to Alice. How does Alice know that Carol is who she claims to be? Carol signed the message with her own private key, which has been digitally signed by Bob (essentially saying, "I trust that this key is valid and hope that you will, too"). Because Alice knows and trusts Bob's key (and therefore his signature), Alice can trust that Carol's key is valid — so the person claiming to be Carol almost certainly really is Carol.

Furthermore, once Alice trusts Carol's key, she can sign it. Then someone who has and trusts Alice's key will be able to trust Carol's. This builds a web of trust among PGP users.

However, this informal web of trust may not be rigorous enough for business or government purposes. For these cases, third-party entities known as certificate authorities validate identities and issue certificates. These certificates, signed with the CAs' well-known and trusted keys, can be used to verify someone's identity.

2.8 How Digital Signatures are used?

Digital signatures can be used anywhere that a system for authenticating data is necessary, i.e. anywhere a handwritten signature could be used but can't or shouldn't for some reason — online banking or payroll

transactions, for example, or web registration for college courses. A system of digital signatures and encryption is used in e-commerce all the time, to protect confidential information.

2.9 Model of Digital Signature

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration.

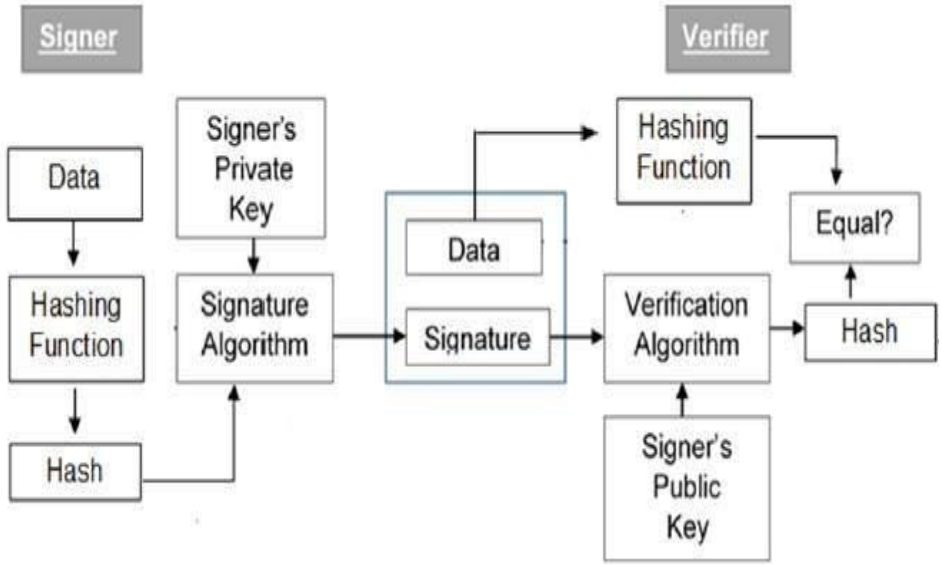

Fig: Digital Signature Process

The following points explain the entire process in detail −

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.

- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

Let us assume RSA is used as the signing algorithm. As discussed in public key encryption chapter, the encryption/signing process using RSA involves modular exponentiation.

Signing large data through modular exponentiation is computationally expensive and time consuming. The hash of the data is a relatively small digest of the data, hence signing a hash is more efficient than signing the entire data.

2.10 Importance of Digital Signature

Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.

Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature −

- **Message authentication** − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature

on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely − Privacy, Authentication, Integrity, and Non-repudiation.

2.11 Applications of digital signatures

As organizations move away from paper documents with ink signatures or authenticity stamps, digital signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. The United States Government Printing Office (GPO) publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures. Universities including Penn State, University of Chicago, and Stanford are publishing electronic student transcripts with digital signatures. Below are some common reasons for applying a digital signature to communications:

2.11.1 Authentication

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

2.11.2 Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a

valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

2.11.3 Non-repudiation

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Note that these authentications, non-repudiation etc. properties rely on the secret key not having been revoked prior to its usage. Public revocation of a key-pair is a required ability; else leaked secret keys would continue to implicate the claimed owner of the key-pair. Checking revocation status requires an "online" check, e.g. checking a "Certificate Revocation List" or via the "Online Certificate Status Protocol". Very roughly this is analogous to a vendor who receives credit-cards first checking online with the credit-card issuer to find if a given card has been reported lost or stolen. Of course, with stolen key pairs, the theft is often discovered only after the secret key's use, e.g., to sign a bogus certificate for espionage purpose.

2.12 Encryption with Digital Signature

In many digital communications, it is desirable to exchange an encrypted message than plaintext to achieve confidentiality. In public key encryption scheme, a public (encryption) key of sender is available in open domain, and hence anyone can spoof his identity and send any encrypted message to the receiver.

This makes it essential for users employing PKC for encryption to seek digital signatures along with encrypted data to be assured of message authentication and non-repudiation.

This can archive by combining digital signatures with encryption scheme. Let us briefly discuss how to achieve this requirement. There are **two possibilities, sign-then-encrypt** and **encrypt-then-sign**.

However, the crypto system based on sign-then-encrypt can be exploited by receiver to spoof identity of sender and sent that data to third party. Hence, this method is not preferred. The process of encrypt-then-sign is more reliable and widely adopted. This is depicted in the following illustration −

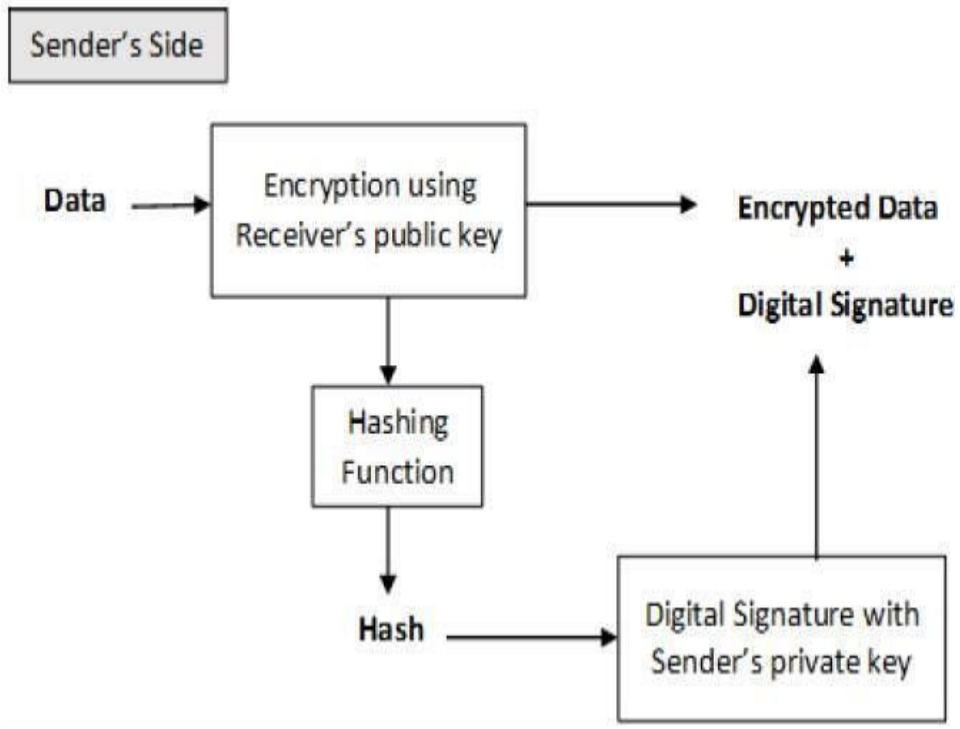

Fig: Encryption with Digital Signature

The receiver after receiving the encrypted data and signature on it, first verifies the signature using sender's public key. After ensuring the validity of the signature, he then retrieves the data through decryption using his private key.

2.13 Digital Signature to Electronic Signature

Digital Signature was the term defined in the old I.T. Act, 2000. Electronic Signature is the term defined by the amended act (I.T. Act, 2008). The concept of Electronic Signature is broader than Digital Signature. Section 3 of the Act delivers for the verification of Electronic Records by affixing Digital Signature.

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

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

- Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
- Those bases on the physical features of the user, i.e., biometrics.

- Those based on the possession of an object by the user, i.e., codes or other information stored on a magnetic card.
- Types of authentication and signature methods that, without falling under any of the above categories might also be used to indicate the originator of an electronic communication (Such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message).
- According to the UNCITRAL Model Law on Electronic Signatures, the following technologies are presently in use
- Digital Signature within a public key infrastructure (PKI)
- Biometric Device
- PINs
- Passwords
- Scanned handwritten signature
- Signature by Digital Pen
- Clickable "OK" or "I Accept" or "I Agree" click boxes

2.14 Digital Signatures Versus Ink on Paper Signatures

An ink signature could be replicated from one document to another by copying the image manually or digitally, but to have credible signature copies that can resist some scrutiny is a significant manual or technical skill, and to produce ink signature copies that resist professional scrutiny is very difficult. Digital signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document. Paper contracts sometimes have the ink signature block on the last page, and the previous pages may be replaced after a signature is applied. Digital signatures can be applied to an entire document, such that the digital signature on the last page will indicate tampering if any data on any of the pages have been altered, but this can also be achieved by signing with ink and numbering all pages of the contract.

2.14.1 Some Digital Signature Algorithms

- RSA-based signature schemes, such as RSA-PSS
- DSA and its elliptic curve variant ECDSA
- ElGamal signature scheme as the predecessor to DSA, and variants Schnorr signature and Point cheval–Stern signature algorithm
- Rabin signature algorithm
- Pairing-based schemes such as BLS
- Undeniable signatures

- Aggregate signature - a signature scheme that supports aggregation: Given n signatures on n messages from n users, it is possible to aggregate all these signatures into a single signature whose size is constant in the number of users. This single signature will convince the verifier that the n users did indeed sign the n original messages.
- Signatures with efficient protocols - are signature schemes that facilitate efficient cryptographic protocols such as zero-knowledge proofs or secure computation.

2.15 The Current State of Use- Legal and Practical

All digital signature schemes share the following basic prerequisites regardless of cryptographic theory or legal provision:

1. **Quality algorithms**: Some public-key algorithms are known to be insecure, practical attacks against them having been discovered.
2. **Quality implementations:** An implementation of a good algorithm (or protocol) with mistake(s) will not work.
3. **The private key must remain private:** If the private key becomes known to any other party, that party can produce perfect digital signatures of anything whatsoever.
4. The public key owner must be verifiable: A public key associated with Bob actually came from Bob. This is commonly done using a public key infrastructure (PKI) and the public key ↔ user association is attested by the operator of the PKI (called a certificate authority). For 'open' PKIs in which anyone can request such an attestation (universally embodied in a cryptographically protected identity certificate), the possibility of mistaken attestation is nontrivial. Commercial PKI operators have suffered several publicly known problems. Such mistakes could lead to falsely signed, and thus wrongly attributed, documents. 'Closed' PKI systems are more expensive, but less easily subverted in this way.
5. Users (and their software) must carry out the signature protocol properly.

   Only if all of these conditions are met will a digital signature actually be any evidence of who sent the message, and therefore of their assent to its contents.

2.16 Industry Standards

Some industries have established common interoperability standards for the use of digital signatures between members of the industry and with

regulators. These include the Automotive Network Exchange for the automobile industry and the SAFE-Bio Pharma Association for the healthcare industry.

2.16.1 Using Separate Key Pairs for Signing and Encryption

In several countries, a digital signature has a status somewhat like that of a traditional pen and paper signature, like in the EU digital signature legislation. Generally, these provisions mean that anything digitally signed legally binds the signer of the document to the terms therein. For that reason, it is often thought best to use separate key pairs for encrypting and signing. Using the encryption key pair, a person can engage in an encrypted conversation (e.g., regarding a real estate transaction), but the encryption does not legally sign every message he sends. Only when both parties come to an agreement do they sign a contract with their signing keys, and only then are they legally bound by the terms of a specific document. After signing, the document can be sent over the encrypted link. If a signing key is lost or compromised, it can be revoked to mitigate any future transactions. If an encryption key is lost, a backup or key escrow should be utilized to continue viewing encrypted content. Signing keys should never be backed up or escrowed unless the backup destination is securely encrypted.

2.17 Introduction to Digital Signature Certificates (DSC)

Digital Signature Certificate (DSC) is a secure **digital** key that certifies the identity of the holder, issued by a Certifying Authority (CA). A **digital certificate** is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web.

Digital Signature Certificates (DSC) are the digital equivalent (that is electronic format) of physical or paper certificates. Few Examples of physical certificates are drivers' licenses, passports or membership cards. Certificates serve as proof of identity of an individual for a certain purpose; for example, a driver's license identifies someone who can legally drive in a particular country. Likewise, a digital certificate can be presented electronically to prove one’s identity, to access information or services on the Internet or to sign certain documents digitally.

2.18 Digital Signature Certificates (DSC) Polices

A Digital Signature is a method of verifying the authenticity of an electronic document. Digital signatures are going to play an important role

in our lives with the gradual electronization of records and documents. The IT Act has given legal recognition to digital signature meaning, thereby, that legally it has the same value as handwritten or signed signatures affixed to a document for its verification. The Information Technology Act, 2000 provides the required legal sanctity to the digital signatures based on asymmetric cryptosystems. The digital signatures are now accepted at par with handwritten signatures and the electronic documents that have been digitally signed are treated at par with paper documents.

2.19 How does a Digital Signature Certificate Work?

A Digital Signature Certificate explicitly associates the identity of an individual/device with a pair of electronic keys - public and private keys - and this association is endorsed by the CA. The certificate contains information about a user's identity (for example, their name, pin code, country, email address, the date the certificate was issued and the name of the Certifying Authority that issued it).

These keys complement each other in that one does not function in the absence of the other. They are used by browsers and servers to encrypt and decrypt information regarding the identity of the certificate user during information exchange processes. The private key is stored on the user's computer hard disk or on an external device such as a token. The user retains control of the private key; it can only be used with the issued password. The public key is disseminated with the encrypted information. The authentication process fails if either one of these keys in not available or do not match. This means that the encrypted data cannot be decrypted and therefore, is inaccessible to unauthorized parties.

2.20 Use of Digital Certificates

Three uses are outlined here. Your digital certificate could be used to allow you to access membership-based web sites automatically without entering a user name and password. It can allow others to verify your "signed" e-mail or other electronic documents, assuring your intended reader(s) that you are the genuine author of the documents, and that the content has not been corrupted or tampered with in any way. Finally, digital certificates enable others to send private messages to you: anyone else who gets his/her hands on a message meant for you will not be able to read it.

2.20.1 Sending Digitally Signed Mail

You can use your Digital Certificate to digitally sign your emails sent through Outlook Express / MS-Outlook etc. Digitally signing the mail authenticates your identity and enables the receiver to ensure that the mail has come from you only. It also ensures that the content of the mail is not tampered in the transit and the mail received by the receiver is the same what you have sent.

2.21 Who Needs a Digital Signature Certificate?

MCA21 Mission Mode Project (MCA21) is the e-governance initiative from the Ministry of Corporate Affairs, Government of India. Under MCA21, Every person who is required to sign manual documents and returns filed with ROC is required to obtain a Digital Signature Certificate (DSC). Accordingly following have to obtain Digital Signature Certificate:

1. Directors
2. Auditors
3. Company Secretaries
4. Bank Officials - for Registration and Satisfaction of Charges
5. Other Authorized Signatories.

2.22 Types Of Digital Signature Certificate

There are 3 types of Digital Signature Certificates, having different security levels, namely:-

- Class-1
- Class-2
- Class-3

For filing documents under **MCA21**, a Class-**2** Digital Signature Certificate issued by a Licensed Registration Authority is required. We also offer Class 1 and 3 besides Class 2 certificates.

2.23 Let us Sum-up

The digital signature has become a significant tool in international commerce. Because a digital signature provides the legal elements of a traditional hand written signature (i.e., evidence, ceremony, approval, and efficiency) and enhanced security, integrity, and authenticity, additional businesses will likely use digital signatures in an increasing percentage of

their commercial transactions. Secure electronic commerce provides a "paperless" way of transacting business.

Currently, the PKI-digital signature is the best type of signature for electronic contracts. PKI-digital signature software is inexpensive and the technology is mathematically improbable to break. With future advances in technology, other types of electronic signatures may replace the PKI-digital signature. Regardless of the technology used, digital and electronic signatures are an increasingly significant part of commerce and will continue to evolve.

Self Assessment Questions

1. What is a Digital Signature? What is its purpose?
   ……
   ……
   ……
   ……
   ……
2. Explain the working of a Digital Signature.
   ……
   ……
   ……
   ……
   ……
3. Compare Digital Signatures with Ink-on paper signatures.
   ……
   ……
   ……
   ……
   ……
4. Write the uses of Digital Certificates.
   ……
   ……
   ……
   ……
   ……
5. Discuss the importance of Digital Signature in Information Security.
   ……
   ……
   ……

……
……

2.25 References & Further Readings

1. Digital Signature. (2016). Retrieved Jan. 09, 2016, from Wikipedia: https://en.wikipedia.org/wiki/Digital_signature available under the Creative Commons Attribution-Share Alike License
2. Course-I-Fundamentals of Information Security, Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e-Governance and Cyber Security
3. W. Everett Lupton, Comment, The Digital Signature: Your Identity by the Numbers, Volume VI, Issue 2, Fall 1999.
4. https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm
5. https://www.tutorialspoint.com/information_security_cyber_law/digital_and_electronic_signatures.htm

UNIT-3 ETHICAL HACKING AND PENETRATION TESTING

Unit Structure

3.0 Introduction

Computers have become mandatory to run a successful business. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and cybercrime. Cybercrime is using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data etc**. Cybercrimes cost many organizations millions of dollars every year**. Businesses need to protect themselves against such attacks.

Most people think hackers have extraordinary skill and knowledge that allow them to hack into computer systems and find valuable information. The term hacker conjures up images of a young computer whiz who types a few commands at a computer screen—and poof! The computer spits out passwords, account numbers, or other confidential data. In reality, a good hacker, or security professional acting as an ethical hacker, just has to understand how a computer system works and know what tools to employ in order to find a security weakness. In this unit we book will discuss different types of hacking, some techniques and software tools that many hackers use to gather valuable data and attack computer systems.

3.1 Learning Objectives

After going through this unit, you will be able to:

- Understand the meaning of hacking.
- Know the benefits of Penetration Testing and Ethical Hacking.
- Identify various types of penetration testing.
- Classify various types of Hackers.
- Analyze various phases involved in Penetration Testing.
- Know various hacking tools and techniques.

3.2 About Ethical Hacking and Penetration Testing

There are many definitions of hacking. In this unit, we will define **hacking as the process of identifying weakness in computer systems and/or networks and exploiting the weaknesses to gain access**. An example of hacking is using by passing the login algorithm to gain access to a system. A **hacker** is a person who finds and exploits weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

Vulnerability analysis and Penetration Testing, commonly known as Ethical Hacking is a branch wherein, hackers engage in sanctioned hacking—that is, hacking with permission from the system's owner. In the world of ethical hacking, most tend to use the term pen tester, which is short for penetration tester. Pen Testers penetrate systems like a hacker, but for "benign" purposes. As an ethical hacker and future test candidate you must become familiar with the jargons of the trade. Here are some of the terms you will encounter in pen testing.

Glossary

1. **Hack Value:** This term describes a target that may attract an above-average level of attention to an attacker. Presumably because this target is attractive, it has more value to an attacker because of what it may contain.
2. **Target of Evaluation (TOE):** A TOE is a system or resource that is being evaluated for vulnerabilities. A TOE would be specified in a contract with the client.
3. **Attack:** This is the act of targeting and actively engaging aTOE.
4. **Exploit:** This is a clearly defined way to breach the security of a system.
5. **Zero Day:** This describes a threat or vulnerability that is unknown to developers and has not been addressed. It is considered a serious problem in many cases.
6. **Security:** This is described as a state of well-being in an environment where only actions that are defined are allowed.
7. **Threat:** This is considered to be a potential violation of security.
8. **Vulnerability:** This is a weakness in a system that can be attacked and used as an entry point into an environment.
9. **Daisy Chaining:** This is the act of performing several hacking attacks in sequence with each building on or acting on the results of the previous action.

   As an ethical hacker, you will be expected to take on the role and use the mind-set and skills of an attacker to simulate a malicious attack. The idea is that ethical hackers understand both sides, the good and the bad, and use this knowledge to help their clients. By understanding both sides of the equation, you will be better prepared to defend yourself successfully.

Some things to remember about being an ethical hacker are:

- You must have explicit permission in writing from the company being tested prior to starting any activity. Legally, the person or persons that

must approve this activity or changes to the plan must be the owner of the company or their authorized representative. If the scope changes, update the contracts to reflect those changes before performing the new tasks.

- You will use the same tactics and strategies as malicious attackers.
- You have every potential to cause harm that a malicious attack will have and should always consider the effects of every action you carry out.
- You must have knowledge of the target and the weaknesses it possesses.
- You must have clearly defined rules of engagement prior to beginning your assigned job.
- You must never reveal any information pertaining to a client to anyone but the client. If the client asks you to stop a test, do so immediately.
- You must provide a report of your results and, if asked, a brief on any deficiencies found during a test.
- You may be asked to work with the client to fix any problems that you find.
- As an ethical hacker you must agree to the following code of ethics:
- Keep private and confidential information gained in your professional work (in particular as it pertains to client lists and client personal information). Do not collect, give, sell, or transfer any personal information (such as name, e-mail address, social security number, or other unique identifier) to a third party without prior client consent.
- Protect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator.
- Disclose to appropriate persons or authorities potential dangers to any e-commerce clients, the Internet community, or the public, that you reasonably believe to be associated with a particular set or type of electronic transactions or related software or hardware.
- Provide service in your areas of competence; be honest and forthright about any limitations of your experience and education. Ensure that you are qualified for any project on which you work or propose to work by an appropriate combination of education, training, and experience.
- Never knowingly use software or a process that is obtained or retained either illegally or unethically.

- Do not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.
- Use the property of a client or employer only in ways properly authorized, and with the owner's knowledge and consent.
- Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.
- Ensure good management for any project you lead, including effective procedures for promotion of quality and full disclosure of risk.
- Add to the knowledge of the e-commerce profession by constant study, share the lessons of your experience with fellow EC-Council members, and promote public awareness of the benefits of e-commerce.
- Conduct yourself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in your knowledge and integrity.
- Ensure ethical conduct and professional care at all times on all professional assignments without prejudice.
- Do not associate with malicious hackers or engage in any malicious activities.
- Do not purposefully compromise or allow the client organization's systems to be compromised in the course of your professional dealings.
- Ensure all pen testing activities are authorized and within legal limits.
- Do not take part in any black hat activity or be associated with any black hat community that serves to endanger networks.
- Do not take part in any underground hacking community for purposes of preaching and expanding black hat activities.
- Do not make inappropriate references to the certification or misleading use of certificates, marks or logos in publications, catalogs, documents, or speeches.
- Do not violate any law of the land or have any previous conviction.

Under the right circumstances and with proper planning and goals in mind, you can provide a wealth of valuable information to your target organization. Working with your client, you should analyze your results thoroughly and determine which areas need attention and which need none at all. Your client will determine the perfect balance of security versus convenience. If the problems you uncover necessitate action, the next challenge is to ensure that existing usability is not adversely affected if security controls are modified or if new ones are put in place. Security and

convenience often conflict: the more secure a system becomes, the less convenient it tends to be.

A pen test is the next logical step beyond ethical hacking. Although ethical hacking sometimes occurs without a formal set of rules of engagement, pen testing does require rules to be agreed on in advance in every case.

3.3 Types of Pen testing

When a pen test is performed it typically takes one of three forms: white box, gray box, or black box. The three forms of testing are important to differentiate between, as you may be asked to perform any one of them at some point during your career, so let's take a moment to describe each:

3.3.1 Black Box

A type of testing in which the pen tester has little or no knowledge of the target is said to be Black Box testing. This situation is designed to closely emulate the situation an actual attacker would encounter as they would presumably have an extremely low level of knowledge of the target going in.

3.3.2 Gray Box

It is a form of testing where the knowledge given to the testing party is limited. In this type of test, the tester acquires knowledge such as IP addresses, operating systems, and the network environment, but that information is limited. This type of test would closely emulate the type of knowledge that someone on the inside might have; such a person would have some knowledge of a target, but not always all of it.

3.3.3 White Box

White Box is a form of testing in which the information given to the tester is complete. This means that the pen tester is given all information about the target system. This type of test is typically done internally or by teams that perform internal audits of systems.

3.3.4 CIA Triad

An ethical hacker is trying to preserve what is known as the CIA triad: confidentiality, integrity, and availability. The following list describes these core concepts and what they mean. Keep these concepts in mind when performing the tasks and responsibilities of a pen tester:

a. **Confidentiality:** The core principle that refers to the safeguarding of information and keeping it away from those not authorized to possess it. Examples of controls that preserve confidentiality are permissions and encryption.
b. **Integrity:** Deals with keeping information in a format that is true and correct to its original purposes, meaning that the data that the receiver accesses is the data the creator intended them to have.
c. **Availability:** The final and possibly one of the most important items that you can perform. Availability deals with keeping information and resources available to those who need to use it. Information or resources, no matter how safe and sound, are only useful if they are available when called upon.

   CIA is possibly the most important set of goals to preserve when you are assessing and planning security for a system. An aggressor will attempt to break or disrupt these goals when targeting a system. As an ethical hacker your job is to find, assess, and remedy these issues whenever they are discovered to prevent an aggressor from doing harm. Another way of looking at this balance is to observe the other side of the triad and how the balance is lost. Any of the following break the CIA triad:

- **Disclosure** is the inadvertent, accidental, or malicious revealing or accessing of information or resources to an outside party. If you are not supposed to have access to an object, you should never have access to it.
- **Alteration** is the counter to integrity; it deals with the unauthorized or other forms of modifying information. This modification can be corruption, accidental access, or malicious in nature.
- **Disruption** (also known as loss) means that access to information or resources has been lost when it should not have. Information is useless if it is not there when it is needed. Although information or other resources can never be 100-percent available, some organizations spend the time and money to get 99.999-percent uptime, which averages about 6 minutes of downtime per year.

Think of these last three points as the anti-CIA triad or the inverse of the CIA triad. The CIA triad deals with preserving information and resources, whereas the anti-CIA triad deals with violating those points. You can also think of the anti-CIA as dealing more with the aggressor's perspective rather than the defender's.

An ethical hacker will be entrusted with ensuring that the CIA triad is preserved at all times and threats are dealt with in the most appropriate manner available (as required by the organization's own goals, legal requirements, and other needs). For example, consider what could happen if an investment firm or defense contractor suffered a disclosure incident at the hands of a malicious party. The results would be catastrophic.

In this unit you will encounter legal issues several times. You are responsible for checking the details of what laws apply to you, and you will need to get a lawyer to do that. You should be conscious of the law at all times and recognize when you may be crossing into a legal area that you need advice on. Both ethical hackers and hackers follow similar processes as the one outlined here though in less or stricter ways. Hackers are able to write their own rules and use the process however they want without concern or reasons except those that make sense to them. Ethical hackers follow the same type of process as seen here with little modification, but there is something that they have added that hackers do not have: Ethical hackers will not only have permission prior to starting the first phase, but they will also be generating a report that they will present at the end of the process. The ethical hacker will be expected to keep detailed notes about what is procured at each phase for later generation of that report.

When you decide to carry out this process, seek your client's guidance and ask the following questions along with any others that you think are relative. During this phase, your goal is to clearly determine why a pen test and its associated tasks are necessary.

- Why did the client request a pen test?
- What is the function or mission of the organization to be tested?
- What will be the constraints or rules of engagement for the test?
- What data and services will be included as part of the test?
- Who is the data owner?
- What results are expected at the conclusion of the test?
- What will be done with the results when presented?
- What is the budget?
- What are the expected costs?
- What resources will be made available?
- What actions will be allowed as part of the test?
- When will the tests be performed?
- Will insiders be notified?
- Will the test be performed as black or white box?

- What conditions will determine the success of the test?
- Who will be the emergency contacts?
- Pen testing can take several forms. You must decide, along with your client, which tests are appropriate and will yield the desired results. Tests that can be part of a pen test include the following:
- An insider attack is intended to mimic the actions that may be undertaken by internal employees or parties who have authorized access to a system.
- An outsider attack is intended to mimic those actions and attacks that would be undertaken by an outside party.
- A stolen equipment attack is a type of attack where an aggressor steals a piece of equipment and uses it to gain access or extracts the information desired from the equipment itself.
- A social engineering attack is a form of attack where the pen tester targets the users of a system seeking to extract the needed information.

The attack exploits the trust inherent in human nature. Once you discuss each test, determine the suitability of each, and evaluate the potential advantages and side effects, you can finalize the planning and contracts and begin testing.

3.4 Vulnerability Research and Tools

An important part of your toolkit as an ethical hacker will be the information gathered from vulnerability research. This process involves searching for and uncovering vulnerabilities in a system and determining their nature. Additionally, the research seeks to classify each vulnerability as high, medium, or low. You or other security personnel can use this research to keep up to date on the latest weaknesses involving software, hardware, and environments. The benefit of having this information is that an administrator or other personnel could use this information to position defenses. Additionally, the information may show where to place new resources or be used to plan monitoring. Vulnerability research is not the same as ethical hacking in that it passively uncovers security issues whereas the process of ethical hacking actively looks for the vulnerabilities.

3.5 Ethics and the Law

As an ethical hacker, you need to be aware of the law and how it affects what you will do. Ignorance or lack of an understanding of the law is not only a bad idea, but it can quickly put you out of business—or even in prison. In fact, under some situations the crime may be serious enough to

get you prosecuted in several jurisdictions in different states, counties, or even countries due to the highly distributed nature of the Internet. Of course, prosecution of a crime can also be difficult considering the web of various legal systems in play. A mix of common, military and civil laws exists, requiring knowledge of a given legal system to be successful in any move toward prosecution.

Depending on when and where you're testing takes place, it is even possible for you to break religious laws. Although you may never encounter this problem, it is something that you should be aware of—you never know what type of laws you may break.

Always ensure that you exercise the utmost care and concern to ensure that you observe proper safety and avoid legal issues. When your client has determined their goals along with your input, the contract must be put in place. Remember the following points when developing a contract and establishing guidelines:

Trust The client is placing trust in you to use the proper discretion when performing a test. If you break this trust, it can lead to the questioning of other details such as the results of the test. Legal Implications Breaking a limit placed on a test may be sufficient cause for your client to take legal action against you.

When we work in this area of specialization, it is paramount to know laws of various countries. Since most of the laws have their roots in US Laws, it is mandatory that we go through them.

3.6 Hacking

Hacking is any technical effort to manipulate the normal behavior of network connections and connected computers or systems. A hacker is any person engaged in hacking.

3.6.1 Culture of Hacking

To be accepted as hacker one should have the attitude, behave as though one have the attitude, and belief in that. Some of them can be listed as follows:

- Strong zeal to learn and obtain more knowledge
- Breaking law
- Anonymity

- Stealing confidential information.

3.6.2 Types of Hackers

Hackers can be classified in to the following types based on their depth of knowledge and activities.

a. **White Hats:** White hats are the good guys, the ethical hackers who use their hacking skills for defensive purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weaknesses and implement countermeasures.
b. **Black Hats:** Black hats are the bad guys: the malicious hackers or crackers who use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote systems, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and just cause problems for their targets. Black-hat hackers and crackers can easily be differentiated from white-hat hackers because their actions are malicious. This is the traditional definition of a hacker and what most people consider a hacker to be.
c. **Gray Hats:** Gray hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Grayhat hackers may just be interested in hacking tools and technologies and are not malicious black hats. Gray hats are self-proclaimed ethical hackers, who are interested in hacker tools.
d. **Suicide Hackers:** Individuals who will aim to bring down the critical infrastructure whatever the consequence may be.
e. **Script Kiddies:** In hacker culture a script kiddie or skiddie are unskilled individuals who use scripts or programs developed by others to attack computer systems and networks and deface websites. It is generally assumed that script kiddies are juveniles who lack the ability to write sophisticated hacking programs or exploits on their own, and that their objective is to try to impress their friends or gain credit in computer-enthusiast communities. The term is typically intended as an insult.
f. **Hacktivist:** Detects and sometimes reports or exploits security vulnerabilities as a form of social activitism. A hacktivist is a hacker who utilizes technology to announce a social ideological, religious or political message. In general most hacktivism involve defacement or denial of service attacks. Hacktivits are also known as Neo hackers

3.7 Phases of Penetration Testing

As brought out earlier that a Pen-tester uses the same methodology as a hacker does, we will be using this terminology interchangeably

3.7.1 Foot printing

Now let's circle back around to the first step in the process of ethical hacking i.e. Foot printing. Foot printing, or reconnaissance, is a method of observing and collecting information about a potential target with the intention of finding a way to attack the target. Foot printing looks for information and later analyzes it, looking for weaknesses or potential vulnerabilities. The end result should be a profile of the target that is a rough picture but one that gives enough data to plan the next phase of scanning. When you conduct foot printing- as with all phases and processes described in this unit—you must be quite methodical. A careless or haphazard process of collecting information can waste time when moving forward or, in a worst-case scenario, cause the attack to fail. The smart or careful attacker spends a good amount of time in this phase gathering and confirming information. Foot printing generally entails the following steps to ensure proper information retrieval:

1. Collect information that is publicly available about a target (for example, host and network information).
2. Ascertain the operating system(s) in use in the environment, including web server and web application data where possible.
3. Issue queries such as whois, DNS, network, and organizational queries.
4. Locate existing or potential vulnerabilities or exploits that exist in the current infrastructure that may be conducive to launching later attacks.

3.7.1.1 Why Perform Foot printing?

Foot printing is about gathering information and formulating a hacking strategy. With proper care you, as the attacking party, may be able to uncover the path of least resistance into an organization. Passively gathering information is by far the easiest and most effective method. If done by a skilled, inventive, and curious party (you!), the amount of information that can be passively gathered is staggering. Expect to obtain information such as:

- Information about an organization's security posture and where potential loopholes may exist. This information will allow for adjustments to the hacking process that make it more productive.
- A database that paints a detailed picture with the maximum amount of information possible about the target.
- A network map using tools such as the Tracert utility to construct a picture of a target's Internet presence or Internet connectivity. Think of the network map as a roadmap leading you to a building; the map gets you there, but you still have to determine the floor plan of the building.

3.7.1.2 Goals of the Foot Printing Process

Before you start doing foot printing and learn the techniques, you must set some expectations as to what you are looking for and what you should have in your hands at the end of the process. Keep in mind that the list of information here is not exhaustive, nor should you expect to be able to obtain all the items from every target. The idea is for you to get as much information in this phase as you possibly can, but take your time!

Here's what you should look for:

- Network information
- Operating system information
- Organization information, such as CEO and employee information, office information, and contact numbers and e-mail
- Network blocks
- Network services
- Application and web application data and configuration information
- System architecture
- Intrusion detection and prevention systems
- Employee names
- Work experience

3.7.1.3 Types of Reconnaissance

Process of Reconnaissance can be categorized as Passive and Active Reconnaissance.

3.7.1.3.1 Passive Reconnaissance

This involves gathering information about a potential target without the targeted individual‘s or company‘s knowledge. Passive reconnaissance can

be as simple as watching a building to identify what time employees enter the building and when they leave. However, most reconnaissance is done sitting in front of a computer. When hackers are looking for information on a potential target, they commonly run an Internet search on an individual or company to gain information. This process when used to gather information regarding a TOE is generally called information gathering. Social engineering and dumpster diving are also considered passive information-gathering methods. These two methods will be discussed Sniffing the network is another means of passive reconnaissance and can yield useful information such as IP address ranges, naming conventions, hidden servers or networks, and other available services on the system or network. Sniffing tools are simple and easy to use and yield a great deal of valuable information. These tools are which literally let you see all the data that is transmitted on the network. Many times this includes usernames and passwords and other sensitive data. Examples: Domain name lookup, Whois, NSlookup, Sam Spade. Information that can be gathered during this phase includes:

- IP address ranges
- Namespaces
- Employee information
- Phone numbers
- Facility information
- Job information

3.7.1.3.2 Active reconnaissance

This involves probing the network to discover individual hosts, IP addresses, and services on the network. This process involves more risk of detection than passive reconnaissance and is sometimes called rattling the doorknobs. Active reconnaissance can give a hacker an indication of security measures in place (is the front door locked?), but the process also increases the chance of being caught or at least raising suspicion. Many software tools that perform active reconnaissance can be traced back to the computer that is running the tools, thus increasing the chance of detection for the hacker. Both passive and active reconnaissance can lead to the discovery of useful information to use in an attack. For example, it‘s usually easy to find the type of web server and the operating system (OS) version number that a company is using. This information may enable a hacker to find vulnerability in that OS version and exploit the vulnerability to gain more access. Foot printing takes advantage of the information that is carelessly exposed or disposed of inadvertently.

3.7.2 Scanning

It focuses on an active engagement of the target with the intention of obtaining more information. Scanning the target network will ultimately locate active hosts that can then be targeted in a later phase. Foot printing helps identify potential targets, but not all may be viable or active hosts. Once scanning determines which hosts are active and what the network looks like, a more refined process can take place.

Scanning involves taking the information discovered during reconnaissance and using it to examine the network.

Scanning is of two types.

i. **Network Scanning**: Network scanning is a procedure for identifying active hosts on a network. Hosts are identified by their individual IP addresses. Network- scanning tools attempt to identify all the live or responding hosts on the network and their corresponding IP addresses.

ii. **Vulnerability Scanning:** Vulnerability scanning is the process of proactively identifying the vulnerabilities of computer systems on a network. Generally, a vulnerability scanner first identifies the operating system and version number, including service packs that may be installed. Then, the scanner identifies weaknesses or vulnerabilities in the operating system.

During this phase most commonly used tools are:

- Pings
- Ping sweeps
- Port scans
- Tracert

Hackers are seeking any information that can help them perpetrate an attack on a target, such as the following:

- IP addresses and open/closed ports on live hosts
- Information on the operating system(s) and the system architecture
- Services or processes running on hosts

Scanning is a set of procedures used to identify hosts, ports, and services on a target network. Scanning is considered part of the intelligence-gathering process an attacker uses to gain information about the targeted environment. Expect the information that is gathered during this phase to take a good amount of time to analyze, which will vary depending on how good you are at reading the resulting information. If you have performed your initial reconnaissance well, however, this process should not be complicated. Your

knowledge will help you not only target your initial scans better, but also better determine how to decipher certain parts of the results. To successfully negotiate the scanning phase, you need a good understanding of networks, protocols, and operating systems.

3.7.3 Enumeration

The last phase before you attempt to gain access to a system is the enumeration phase. Enumeration is the systematic probing of a target with the goal of obtaining user lists, routing tables, and protocols from the system. This phase represents a significant shift in your process; it is the initial transition from being on the outside looking in to moving to the inside of the system to gather data. Information such as shares, users, groups, applications, protocols, and banners all proved useful in getting to know your target, and this information is now carried forward into the attack phase.

Enumeration occurs after scanning and is the process of gathering and compiling usernames, machine names, network resources, shares, and services. It also refers to actively querying or connecting to a target system to acquire this information. Hackers need to be methodical in their approach to hacking. The following steps are an example of those a hacker might perform in preparation for hacking a target system:

- Extract usernames using enumeration
- Group information
- Passwords
- Hidden shares
- Device information
- Network layout
- Protocol information
- Server data
- Service information.
- Gather information about the host using null sessions.
- Perform Windows enumeration using the SuperScan tool.
- Acquire the user accounts using the tool GetAcct.
- Perform SNMP port scanning.

The objective of enumeration is to identify a user account or system account for potential use in hacking the target system. It isn‘t necessary to find a system administrator account, because most account privileges can be escalated to allow the account more access than was previously granted.

3.7.4 Gaining Access

Once you have completed the first three phases, you can move into the system-hacking phase. At this point, the process becomes much more complex: You can't complete the system hacking phase in a single pass. It involves using a methodical approach that includes cracking passwords, escalating privileges, executing applications, hiding files, covering tracks, concealing evidence, and then pushing into a more involved attack. Phase 3 is when the real hacking takes place. Vulnerabilities exposed during the reconnaissance and scanning phase are now exploited to gain access to the target system. The hacking attack can be delivered to the target system via a local area network (LAN), either wired or wireless; local access to a PC; the Internet; or offline. Examples include stack based buffer overflows, denial of service, and session hijacking. Gaining access is known in the hacker world as owning the system because once a system has been hacked, the hacker has control and can use that system as they wish. In order to gain access in a system, hacker's first attempt is to crack the password. In the enumeration phase, you collected a wealth of information, including usernames. These usernames are important now because they give you something on which to focus your attack more closely. You use password cracking to obtain the credentials of a given account with the intention of using the account to gain authorized access to the system under the guise of an authentic user.

3.7.4.1 Password Cracking Techniques

Popular culture would have us believe that cracking a password is as simple as running some software and tapping a few buttons. The reality is that special techniques are used to recover passwords. For the most part, you can break these techniques into five categories, which you will explore in depth later in this chapter; but let's take a high-level look at them now:

i. **Dictionary Attacks**: An attack of this type takes the form of a password-cracking application that has a dictionary file loaded into it. The dictionary file is a text file that contains a list of known words up to and including the entire dictionary. The application uses this list to test different words in an attempt to recover the password. Systems that use passphrases typically are not vulnerable to this type of attack.
ii. **Brute-force Attacks**: In this type of attack, every possible combination of characters is attempted until the correct one is uncovered. According to RSA Labs, "Exhaustive key search, or brute-force search, is the

basic technique for trying every possible key in turn until the correct key is identified".

iii. **Hybrid Attack**: This form of password attack builds on the dictionary attack, but with additional steps as part of the process. In most cases, this means passwords that are tried during a dictionary attack are modified with the addition and substitution of special characters and numbers, such as P@ssw0rd instead of Password.

iv. **Syllable Attack:** This type of attack is a combination of a brute-force and a dictionary attack. It is useful when the password a user has chosen is not a standard word or phrase.

v. **Rule-based Attack:** This could be considered an advanced attack. It assumes that the user has created a password using information the attacker has some knowledge of ahead of time, such as phrases and digits the user may have a tendency to use. In addition to these techniques, there are four types of attacks. Each offers a different, effective way of obtaining a password from a target:

vi. **Passive Online Attacks:** Attacks in this category are carried out simply by sitting back and listening—in this case, via technology, in the form of sniffing tools such as Wire shark, man-in-the-middle attacks, or replay attacks.

vii. **Active Online Attacks:** The attacks in this category are more aggressive than passive attacks because the process requires deeper engagement with the targets. Attackers using this approach are targeting a victim with the intention of breaking a password. In cases of weak or poor passwords, active attacks are very effective. Forms of this attack include password guessing, Trojan/spyware/key loggers, hash injection, and phishing.

viii. **Offline Attacks:** This type of attack is designed to prey on the weaknesses not of passwords, but of the way they are stored. Because passwords must be stored in some format, an attacker seeks to obtain them where they are stored by exploiting poor security or weaknesses inherent in a system. If these credentials happen to be stored in a plaintext or unencrypted format, the attacker will go after this file and gain the credentials. Forms of this attack include pre-computed hashes, distributed network attacks, and rainbow attacks.

ix. **Nontechnical Attacks**: Also known as non-electronic attacks, these move the process offline into the real world. A characteristic of this attack is that it does not require any technical knowledge and instead relies on theft, deception, and other means. Forms of this attack include shoulder surfing, social engineering, and dumpster diving.

3.7.5 Privilege Escalation

Escalating privileges basically means adding more rights or permissions to a user account. Simply said, escalating privileges makes a regular user account into an administrator account. Generally, administrator accounts have more stringent password requirements, and their passwords are more closely guarded. If it isn‘t possible to find a username and password of an account with administrator privileges, a hacker may choose to use an account with lower privileges. In this case, the hacker must then escalate that account‘s privileges. This is accomplished by first gaining access using a non-administrator user account— typically by gathering the username and password through one of the previously discussed methods—and then increasing the privileges on the account to the level of an administrator. When you obtain a password and gain access to an account, there is still more work to do: privilege escalation. The reality is that the account you're compromising may end up being a lower-privileged and less defended one. If this is the case, you must perform privilege escalation prior to carrying out the next phase. The goal should be to gain a level where fewer restrictions exist on the account and you have greater access to the system.

Every operating system ships with a number of user accounts and groups already present. In Windows, preconfigured users include the administrator and guest accounts. Because it is easy for an attacker to find information about the accounts that are included with an operating system, you should take care to ensure that such accounts are secured properly, even if they will never be used. An attacker who knows that these accounts exist on a system is more than likely to try to obtain their passwords.

There are two defined types of privilege escalation, each of which approaches the problem of obtaining greater privileges from a different angle:

- **Horizontal Privilege Escalation**: An attacker attempts to take over the rights and privileges of another user who has the same privileges as the current account.
- **Vertical Privilege Escalation**: The attacker gains access to an account and then tries to elevate the privileges of the account. It is also possible to carry out a vertical escalation by compromising an account and then trying to gain access to a higher-privileged account.

One way to escalate privileges is to identify an account that has the desired access and then change the password. Several tools that offer this ability, including the following:

- Active@ Password Changer
- Trinity Rescue Kit
- ERD Commander
- Windows Recovery Environment (WinRE)
- Password Resetter

Once you gain access to a system and obtain sufficient privileges, it's time to compromise the system and carry out the attack. Which applications are executed at this point is up to the attacker, but they can either be custom-built applications or off-the-shelf software. Once an attacker has gained access to a system and is executing applications on it, they are said to own the system. An attacker executes different applications on a system with specific goals in mind:

- **Backdoors:** Applications of this type are designed to compromise the system in such a way as to allow later access to take place. An attacker can use these backdoors later to attack the system. Backdoors can come in the form of rootkits, Trojans, and similar types. They can even include software in the form of remote access Trojans (RATs).
- **Crackers:** Any software that fits into this category is characterized by the ability to crack code or obtain passwords.
- **Keyloggers:** Keyloggers are hardware or software devices used to gain information entered via the keyboard.
- **Malware:** This is any type of software designed to capture information, alter, or compromise the system.

3.7.6 Pilfering

The objective is to gain access to trusted systems by information gathering. Once Administrator equivalent status has been obtained, attackers typically shift their attention to grabbing as much information as possible that can be leveraged for further system conquests.

3.7.7 Creating backdoors

The objective is to hide the fact of total ownership from the system administrators by erasing all tracks from logs. There are many ways to plant a backdoor on a system, but let's look at one provided via the PsTools suite. This suite includes a mixed bag of utilities designed to ease system administration. Among these tools is PsExec, which is designed to run commands interactively or non-interactively on a remote system. Initially, the tool may seem similar to Telnet or remote desktop, but it does not require installation on the local or remote system in order to work.

To work, PsExec need only be copied to a folder on the local system and run with the appropriate switches. Let's take a look at some of the commands you can use with:

- The following command launches an interactive command prompt on a system named \\dbserver: psexec \\dbserver cmd.
- This command executes ipconfig on the remote system with the /all switch, and displays the resulting output locally:psexec \\ dbserver ipconfig /all.
- This command copies the program rootkit.exe to the remote system and executes it interactively: psexec \\dbserver -c rootkit.exe.
- This command copies the program rootkit.exeto the remote system and executes it interactively using the administrator account on the remote system: psexec \\dbserver -u administrator -c rootkit.exe.

As these commands illustrate, it is possible for an attacker to run an application on a remote system quite easily. The next step is for the attacker to decide what to do or what to run on the remote system. Some of the common choices are Trojans, rootkits, and backdoors. Other utilities that may prove helpful in attaching to a system remotely are the following:

- **PDQ Deploy:** This utility is designed to assist with the deployment of software to a single system or to multiple systems across a network. The utility is designed to integrate with Active Directory as well as other software packages.
- **RemoteExec:** This utility is designed to work much like PsExec, but it also makes it easy to restart, reboot, and manipulate folders on the system.
- **DameWare:** This is a set of utilities used to remotely administer and control a system. Much like the other utilities on this list, it is readily available and may not be detected by antivirus utilities. DameWare also has the benefit of working across platforms such as Windows, OS X, and Linux

3.7.8 Covering Tracks

Once you have penetrated as system and installed software or run some scripts, then next step is cleaning up after yourself or covering your tracks. The purpose of this phase is to prevent your attack from being easily discovered by using various techniques to hide the red-flags and other signs. During this phase, you seek to eliminate error messages, log files, and other items that may have been altered during the attack process. The objective is to lay trap doors in various parts of the system so as to ensure easy

privileged access. Last on the intruders checklist is the creation of future opportunities to return to the compromised system, hopefully disguised from the purview of system administrators.

3.7.8.1 Disabling Auditing

One of the best ways to prevent you from being discovered is to leave no tracks at all. And one of the best ways to do that is to prevent any tracks from being created or at least minimize the amount of evidence. When you're trying not to leave tracks, a good starting point is altering the way events are logged on the targeted system. Disabling auditing on a system prevents certain events from appearing and therefore slows detection efforts. Remember that auditing is designed to allow for the detection and tracking of selected events on a system. Once auditing is disabled, you have effectively deprived the defender of a great source of information and forced them to seek other methods of detection. In the Windows environment, you can disable auditing with the audit poll command included. Using the NULL session technique you saw during your enumeration activities, you can attach to a system remotely and run the command as follows:

auditpol \\<ip address of target> /clear

You can also perform what amounts to the surgical removal of entries in the Windows Security Log, using tools such as the following:

- Dumpel
- Elsave
- WinZapper
- CCleaner
- Wipe
- MRU-Blaster
- Tracks Eraser Pro
- Clear My History

3.7.8.2 Data Hiding

There are other ways to hide evidence of an attack, including hiding the files placed on the system such as EXE files, scripts, and other data. Operating systems such as Windows provide many methods you can use to hide files, including file attributes and alternate data streams. File attributes are a feature of operating systems that allow files to be marked as having certain properties, including read-only and hidden. Files can be flagged as

hidden, which is a convenient way to hide data and prevent detection through simple means such as directory listings or browsing in Windows Explorer. Hiding files this way does not provide complete protection, however, because more advanced detective techniques can uncover files hidden in this manner.

3.7.8.3 Alternate Data Streams (ADS)

A very effective method of hiding data on a Windows system is also one of the lesser-known ones: Alternate Data Streams (ADS). This feature is part of the NTFS file system and has been since the 1990s, but since its introduction it has received little recognition; this makes it both useful for an attacker who is knowledgeable and dangerous for a defender who knows little about it. Originally, this feature was designed to ensure interoperability with the Macintosh Hierarchical File System (HFS), but it has since been used for other purposes. ADS provide the ability to fork or hide file data within existing files without altering the appearance or behavior of a file in any way. In fact, when you use ADS, you can hide a file from all traditional detection techniques as well as dir and Windows Explorer. In practice, the use of ADS is a major security issue because it is nearly a perfect mechanism for hiding data. Once a piece of data is embedded and hidden using ADS, it can lie in wait until the attacker decides to run it later.

The process of creating ADS is simple:

triforce.exe > smoke.doc:triforce.exe

Executing this command hides the file triforce.exe behind the file smoke.doc. At this point, the file is streamed. The next step is to delete the original file that you just hid, triforce.exe. As an attacker, retrieving the file is as simple as this:

Start smoke.doc:triforce.exe

This command has the effect of opening the hidden file and executing it. As a defender, this sounds like bad news, because files hidden this way are impossible to detect using most means. But by using some advanced methods, they can be detected. Some of the tools that can be used to do this include the following:

- SFind—A forensic tool for finding streamed files
- LNS—Used for finding ADS streamed files
- Tripwire—Used to detect changes in files; by nature can detect ADS

An AD is available only on NTFS volumes, although the version of NTFS does not matter. This feature does not work on other file systems.

3.7.9 Denial of Service (DoS)

The objective is to use the readily available exploit code to disable a target. Essentially, a DoS attack disrupts or completely denies service to legitimate users, networks, systems or other resources. The intent of any such attack is usually malicious in nature and often takes little skill because of the requisite tools are readily available.

3.8 Let us Sum-up

When becoming an ethical hacker, you must develop a rich and diverse skill set and mind-set. Through a robust and effective combination of technological, administrative, and physical measures, organizations have learned to address their given situation and head off major problems through detection and testing. Technology such as virtual private networks (VPNs), cryptographic protocols, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), access control lists (ACLs), biometrics, smart cards, and other devices have helped security become much stronger, but still have not eliminated the need for vigilance. Administrative countermeasures such as policies, procedures, and other rules have also been strengthened and implemented over the past decade. Physical measures include devices such as cable locks, device locks, alarm systems, and other similar devices. Your new role as an ethical hacker will deal with all of these items, plus many more. As an ethical hacker you must not only know the environment you will be working in, but also how to find weaknesses and address them as needed. You will also need to understand the laws and ethics involved, and you also must know the client's expectations. Understand the value of getting the proper contracts in place and not deviating from them. Hacking that is not performed under contract is considered illegal and is treated as such. By its very nature, hacking activities can easily cross state and national borders into multiple legal jurisdictions. Breaking outside the scope of a contract can expose you to legal harm and become a career-ending blunder.

3.9 Self-Assessment Questions

1. Explain the various components of CIA Triad. Explain each of them.

……...……...…….……
……..….

2. What are the various types of hackers? Explain each of them briefly?

……...……
……...…
……

3. Enumerate and explain various phases involved in penetration testing. Briefly explain each of them.

……...……
……

3.10 References & Further Readings

1. Study Material "Post-Graduate Diploma in Cyber Security Information System (PGDCS-06), Certificate in e-Governance and Cyber Security", Uttrakhand Open University, Haldwani, made available under a Creative Commons Attribution Share-Alike 4.0 Licence (International),
2. http://creativecommons.org/licenses/by-sa/4.0/
3. http://www.guru99.com/what-is-hacking-an-introduction.html
4. http://bedaone.blogspot.in/p/chapter-1-introduction-to-ethical.html

UNIT 4: COMPUTER FORENSIC

Unit Structure

4.0 Introduction

Computer forensics is the art of recovering and analyzing the contents found on Computer devices such as desktops, notebooks, tablets, smart phones, etc. It was little-known a few years ago. However, with the growing incidence of cyber-crime adoption of computer devices, this branch of forensics has gained momentum in the recent years, augmenting what was conventionally limited to the recovery and analysis of biological and chemical evidence during criminal investigations. This has been used an important technology used many investigating agencies for detection of cyber-criminal activities and evidences. In this unit we will discuss the evolution and of computer forensics technology, its benefits and applications.

4.1 Learning Objectives

After going through this unit, you will be able to:

- Define Computer Forensic
- Know the history and evolution of Computer forensics
- Describe various types of cyber crimes
- Understand benefits of computer forensics
- Know about forensics readiness
- Implement forensics readiness plan

4.2 Definition of Computer Forensics

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it. It is the use of specialized techniques for recovery, authentication and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, and authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel. Similar to all forms of forensic science, computer forensics is comprised of the application of the law to computer science. Computer forensics deals with the preservation, identification, extraction,and documentation of computer evidence. Like many other forensic sciences, computer forensics involves the use of sophisticated technological tools and procedures that must be followed to guarantee the

accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing. So Computer Forensic is the use of specialized techniques for recovery, authentication, and analysis of computer data, typically of data which may have been deleted or destroyed.

4.3 Cyber Crime

Computer crime or cybercrime is any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Dr.Debarati Halder and Dr. K. Jaishankar define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare.

Computer forensics is traditionally associated with criminal investigations and, as you would expect, most types of investigation center on some form of computer crime. This sort of crime can take two forms. (a) Computer based crime and (b) Computer facilitated crimes.

4.3.1 Computer Based Crime

This is criminal activity that is conducted purely on computers, for example cyber-bullying or spam. As well as crimes newly defined by the computing age it also includes traditional crime conducted purely on computers (for example, child pornography).

4.3.2 Computer Facilitated Crime

Crimes conducted in the "real world" but facilitated by the use of computers. A classic example of this sort of crime is fraud: computers are commonly used to communicate with other fraudsters, to record/plan activities or to create fraudulent documents.

Not all Computer forensics investigations focus on criminal behavior; sometimes the techniques are used in corporate (or private) settings to recover lost information or to rebuild the activities of employees.

4.4 Evolution of Computer Forensics

It is difficult to pinpoint the first "computer forensic" examination or the beginning of the field for that matter. But most experts agree that the field of computer forensics began to evolve more than 30 years ago. The field began in the United States, in large part, when law enforcement and military investigators started seeing criminals get technical. Government personnel charged with protecting important, confidential, and certainly secret information conducted forensic examinations in response to potential security breaches to not only investigate the particular breach, but to learn how to prevent future potential breaches. Ultimately, the fields of information security, which focuses on protecting information and assets, and computer forensics, which focuses on the response to hi-tech offenses, started to intertwine.

Over the next decades, and up to today, the field is evolving. Both Government and private organizations and corporations have followed suit – employing internal information security and computer forensic professionals or contracting such professionals or firms on an as- needed basis. Significantly, the private legal industry has more recently seen the need for computer forensic examinations in civil legal disputes, causing an explosion in the e- discovery field.

4.5 Stages of Computer Forensics Process

The overall computer forensics process is sometimes viewed as comprising four stages:

1. **Acquire**: Identifying and Preserving
2. **Analyze**: Technical Analysis
3. **Evaluate:** What the Lawyers Do
4. **Present:** Present Computer evidence in a manner that is legally acceptable in any legal proceedings.

4.6 Benefits of Computer Forensics

With the ever increasing rate of cyber-crimes, from phishing to hacking and stealing of personal information not only confined to a particular country but the globally at large, there is a need for forensic experts to be available in public and private organizations. To be able to handle this, it's vital for network administrator and security staff of networked organizations to have this course in practice making sure that they have the laws pertaining to this on their fingertips. This would ensure that should need for the service avail itself, then they would come in and rescue the situation.

The survival and integrity of any given network infrastructure of any company or organization strongly depends on the application of computer

forensics. They should be taken as the main element of computer and network security. It would be a great benefit for a company if it has knowledge of all the technical and legal aspects of this field. Should the company's network be under attack and the intruder caught in the act, then an understanding about computer forensics will be of help in provision of evidence and prosecution of the case in the court of law.

New laws aimed at the protection of customer's data are continuously being developed. Should they lose data, then naturally the liability goes to the company. Such cases, if they occur will automatically result in the company or organization being brought to the court of law for failure to protect personal data, this can turn out to be very expensive. But through the application of forensic science, huge chunks of money can be saved by the firms concerned. A lot of money is lately being spent on network and computer security. Software for vulnerability assessment and intrusion detection has passed the billion dollar mark, this is according to experts. It simply means that there is a necessity in investment in either employing an expert in computer forensic in the firms, or having part of their staff trained into this venture so as to help in detection of such cases should they arise.

4.7 Uses of Computer Forensics

There are few areas of crime or dispute where computer forensics cannot be applied. Law enforcement agencies have been among the earliest and heaviest users of computer forensics and consequently have often been at the forefront of developments in the field.

Computers may constitute a 'scene of a crime', for example with hacking or denial of service attacks or they may hold evidence in the form of emails, internet history, documents or other files relevant to crimes such as murder, kidnap, fraud and drug trafficking.

It is not just the content of emails, documents and other files which may be of interest to investigators but also the 'metadata' associated with those files. A computer forensic examination may reveal when a document first appeared on a computer, when it was last edited, when it was last saved or printed and which user carried out these actions.

More recently, commercial organizations have used computer forensics to their benefit in a variety of cases such as:

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Forgeries

- Bankruptcy investigations
- Inappropriate email and internet use in the work place
- Regulatory compliance

4.8 Objectives of Computer Forensics

We all will agree to the fact that we are depending more on more on Information & Communication Technology (ICT) tools and internet for digital services to an extent that today we talk online using chat application, we depend on email to communicate with relatives and office, we stay in touch with our friends and update status using social engineering platforms like Facebook, etc., we work online by staying connected to our office/ client using internet, we shop online, we teach online, we learn online, we submit our bill online today. Our dependency on Computer and Internet have increased so much that we are "online" most of the time. Therefore, there is an increased need of protecting our information from being misused by following Information security guidelines. However, if the security of our computer is compromised, computer forensics comes handy for post-incident investigation.

The objectives of Computer forensics are to provide guidelines for:

- Following the first responder procedure and access the victim's computer after incident.
- Designing procedures at a suspected crime scene to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication.
- Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Provide guidelines for analyzing digital media to preserve evidence, analyzing logs and deriving conclusions, investigate network traffics and logs to correlate events, investigate wireless and web attacks, tracking emails and investigate email crimes.
- Producing computer forensic report which provides complete report on computer forensic investigation process.
- Preserving the evidence by following the chain of custody.
- Employing the rigorous procedures necessary to have forensic results stand up to scrutiny in a court of law.
- Presenting Computer forensics results in a court of law as an expert witness.

4.9 Role of Forensics Investigator

Following are some of the important duties of a forensic investigator:

- Confirms or dispels whether a resource/network is compromised.
- Determine extent of damage due to intrusion.
- Answer the questions: Who, What, When, Where, How and Why.
- Gathering data in a forensically sound manner.
- Handle and analyze evidence.
- Prepare the report.
- Present admissible evidence in court.

4.10 Forensics Readiness

There are several reasons for this field's growth; the most significant being that computers are everywhere. You'd be hard pressed to find a household today without at least one computer. And it is not just computers that computer forensic examiners get involved with. Computer forensic examiners analyze all types of technical devices. Look around you while you walk down the street – people are on their cell phones, using iPods, PDAs, and text messaging. Computer forensic examiners analyze all of these electronic devices! Cyber forensics is a rapidly changing field. There are new technologies coming out daily that are becoming smaller, but storing more and more data. This leads to why cyber forensics is import. In computer related crimes, such identity fraud, it is becoming easier to hide data. With the proper analysis of digital evidence, better security can be made to protect computer users, but also catch those who are committing the crimes. Organizations have now realized the importance of being prepared to combat cyber criminals with their forensic readiness plan ready.

4.10.1 What is Forensics Readiness?

Forensic readiness is the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation. In a business context there is the opportunity to actively collect potential evidence in the form of log files, emails, back-up disks, portable computers, network traffic records, and telephone records, amongst others. This evidence may be collected in advance of a crime or dispute, and may be used to the benefit of the collecting organization if it becomes involved in a formal dispute or legal process.

4.10.2 Goals of Forensic Readiness

Some of the important goals of forensics readiness are:

- To gather admissible evidence legally and without interfering with business processes;

- To gather evidence targeting the potential crimes and disputes that may adversely impact an organization;
- To allow an investigation to proceed at a cost in proportion to the incident;
- To minimize interruption to the business from any investigation; and
- To ensure that evidence makes a positive impact on the outcome of any legal action.

4.10.3 Benefits of Forensic Readiness

Forensic readiness can offer an organization the following benefits:

- Evidence can be gathered to act in an organization's defense if subject to a lawsuit;
- Comprehensive evidence gathering can be used as a deterrent to the insider threat (throwing away potential evidence is simply helping to cover the tracks of a cyber- criminal);
- In the event of a major incident, an efficient and rapid investigation can be conducted and actions taken with minimal disruption to the business;
- A systematic approach to evidence storage can significantly reduce the costs and time of an internal investigation;
- A structured approach to evidence storage can reduce the costs of any court-ordered disclosure or regulatory or legal need to disclose data (e.g. in response to a request under data protection legislation);
- Forensic readiness can extend the scope of information security to the wider threat from cyber-crime, such as intellectual property protection, fraud, extortion etc.;
- It demonstrates due diligence and good corporate governance of the company's information assets;
- It can demonstrate that regulatory requirements have been met;
- It can improve and facilitate the interface to law enforcement if involved;
- It can improve the prospects for a successful legal action;
- It can provide evidence to resolve a commercial dispute;
- It can support employee sanctions based on digital evidence

4.10.4 Steps for Forensic Readiness Planning

The following ten steps describe the key activities in forensic readiness planning:

1. Define the business scenarios that require digital evidence;
2. Identify available sources and different types of potential evidence;
3. Determine the evidence collection requirement;

4. Establish a capability for securely gathering legally admissible evidence to meet the requirement;
5. Establish a policy for secure storage and handling of potential evidence;
6. Ensure monitoring is targeted to detect and deter major incidents;
7. Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched;
8. Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence;
9. Document an evidence-based case describing the incident and its impact.
10. Ensure legal review to facilitate action in response to the incident.

Let us now discuss in brief each of the ten steps.

1. Define the business scenarios that require digital evidence: The first step in forensic readiness is to define the purpose of an evidence collection capability. The rationale is to look at the risk and potential impact on the business from the various types of crimes and disputes. What is the threat to the business and what parts are vulnerable? This is, in effect, a risk assessment, and is performed at the business level.

The aim is to understand the business scenarios where digital evidence may be required and may benefit the organization the event that it is required. In general the areas where digital evidence can be applied include:

- Reducing the impact from computer-related crime;
- Dealing effectively with court orders to release data;
- Demonstrating compliance with regulatory or legal constraints;
- Producing evidence to support company disciplinary issues;
- Supporting contractual and commercial agreements; and
- Proving the impact of a crime or dispute.

In assessing these scenarios, this step provides an indication of the likely benefits of being able to use digital evidence. If the identified risks, and the potential benefits of forensic readiness, suggest a good return on investment is achievable, then an organization needs to consider what evidence to gather for the various risk scenarios.

2. Identify available sources and different types of potential evidence: The second step in forensic readiness is for an organization to know what sources of potential evidence are present on, or could be generated by, their systems and to determine what currently happens to the potential evidence data. Computer logs can originate from many sources. The purpose of this

step is to scope what evidence may be available from across the range of systems and applications in use. Some basic questions need to be asked about possible evidence sources to include.

- Where is data generated?
- What format is it in?
- How long is it stored for?
- How is it currently controlled, secured and managed?
- Who has access to the data?
- How much is produced?
- Is it archived? If so where and for how long?
- How much is reviewed?
- What additional evidence sources could be enabled?
- Who is responsible for this data?
- Who is the formal owner of the data?
- How could it be made available to an investigation?
- What business processes does it relate to?
- Does it contain personal information?

Email is an obvious example of a potential rich source of evidence that needs careful consideration in terms of storage, archiving & auditing and retrieval. But this is not the only means of communication used over the internet, there is also instant messaging, web-based email that bypasses corporate email servers, chat-rooms and newsgroups, even voice over the internet. Each of these may need preserving and archiving. The range of possible evidence sources includes:

- Equipment such as routers, firewalls, servers, clients, portables, embedded devices etc.
- Application software such as accounting packages etc for evidence of fraud, ERP packages for employee records and activities (e.g. in case of identity theft), system and management files etc;
- Monitoring software such as intrusion detection software, packet sniffers, keyboard loggers, content checkers, etc;
- General logs such as access logs, printer logs, web traffic, internal network logs, internet traffic, database transactions, commercial transactions etc;
- Other sources such as: CCTV, door access records, phone logs, pabx data etc;
- Back-ups and archives.

3. Determine the Evidence Collection Requirement: It is now possible to decide which of the possible evidence sources identified in step 2 can help

deal with the crimes and disputes identified in step 1 and whether further ways to gather evidence are required. This is the evidence collection requirement. The purpose of this step is to produce an evidence requirement statement so that those responsible for managing the business risk can communicate with those running and monitoring information systems through an agreed requirement for evidence. One of the key benefits of this step is the bringing together of IT with the needs of corporate security. IT audit logs have been traditionally configured by systems administrators independently of corporate policy and where such a policy exists there is often a significant gap between organizational security objectives and the 'bottom-up' auditing actually implemented. The evidence collection requirement is moderated by a cost benefit analysis of how much the required evidence will cost to collect and what benefit it provides (see above). The critical question for successful forensic readiness is what can be performed cost effectively. By considering these issues in advance and choosing storage options, auditing tools, investigation tools, and appropriate procedures it is possible for an organization to reduce the costs of future forensic investigations.

4. Establish a capability for securely gathering legally admissible evidence to meet the requirement: At this point the organization knows the totality of evidence available and has decided which of it can be collected to address the company risks and within a planned budget. With the evidence requirement understood, the next step is to ensure that it is collected from the relevant sources and that it is preserved as an authentic record. At this stage legal advice is required to ensure that the evidence canbe gathered legally and the evidence requirement can be met in the manner planned. For example, does it involve monitoring personal emails, the use of personal data, or 'fishing trips1' on employee activities? In some countries, some or all of these activities may be illegal. Relevant laws, in the areas of data protection, privacy and human rights, will inevitably constrain what can actually be gathered. Some of the guidelines are:

- Monitoring should be targeted at specific problems.
- It should only be gathered for defined purposes and nothing more;
- Staff should be told what monitoring is happening except in exceptional circumstances.

Physical security of data such as back-up files or on central log servers is important from the data protection point of view, and also for secure evidence storage. As well as preventative measures such as secure rooms and swipe card access it is also prudent to have records of who has access to the general location and who has access to the actual machines containing

evidence. Any evidence or paperwork associated with a specific investigation should be given added security by, for example, storing in a safe. Additional security of logs can also be achieved through the use of WORM storage media.

5. Establish a policy for secure storage and handling of potential evidence: The objective of this step is to secure the evidence for the longer term once it has been collected and to facilitate its retrieval if required. It concerns the long-term or off-line storage of information that might be required for evidence at a later date. A policy for secure storage and handling of potential evidence comprises security measures to ensure the authenticity of the data and also procedures to demonstrate that the evidence integrity is preserved whenever it is used, moved or combined with new evidence. In the parlance of investigators this is known as continuity of evidence (in the UK) and chain of custody (in the US). The continuity of evidence also includes records of who held, and who had access to, the evidence (for example from swipe control door logs). A significant contribution to the legal collection of evidence is given by the code of practice on the legal admissibility and weight of information stored electronically, published by the British Standards Institution. This document originated from a perceived need for evidence collection in the paperless office. The problem it addressed is if all paper documents are scanned, can the paper sources be thrown away without loss of evidential usability? The current edition broadens the scope to all information management systems, Ad hoc opportunistic searches, without justification, for potentially incriminating activities or communication such as those where information is transmitted over networks such as email systems for example. It points out that methods of storage, hardware reliability, operation and access control, and even the programs and source code, may be investigated in order to determine admissibility. A closely related international standard is being developed as ISO 15801. The required output of this step is a secure evidence policy. It should document the security measures, the legal advice and the procedural measures used to ensure the evidence requirement is met. Upon this document rests the likely admissibility and weight of any evidence gathered.

6. Ensure monitoring and auditing is targeted to detect and deter major incidents: In addition to gathering evidence for later use in court, evidence sources can be monitored to detect threatened incidents in a timely manner. This is directly analogous to Intrusion Detection Systems (IDS), extended beyond network attack to a wide range of behaviors that may have implications for the organization. It is all very well collecting the evidence.

This step is about making sure it can be used in the process of detection. By monitoring sources of evidence we can look for the triggers that mean something suspicious may be happening. The critical question in this step is when should an organization be suspicious? A suspicious event has to be related to business risk and not couched in technical terms. Thus the onus is on managers to explain to those monitoring the data what they want to prevent and thus the sort of behavior that IDS might be used to detect for example. This should be captured in a 'suspicion' policy that helps the various monitoring and auditing staff understand what triggers should provoke suspicion, who to report the suspicion to, whether heightened monitoring is required, and whether any additional security measures should be taken as a precaution. Each type of monitoring should produce a proportion of false positives. The sensitivity of triggers can be varied as long as the overall false positive rate does not become so high that suspicious events cannot be properly reviewed. Varying triggers also guards against the risk from someone who knows what the threshold on a particular event is and makes sure any events or transactions he wishes to hide are beneath it.

7. Specify circumstances when escalation to a full formal investigation (which may use digital evidence) is required: Some suspicious events can be system generated, such as by the rule-base of an IDS, or the keywords of a content checker, and some will be triggered by human watchfulness. Each suspicious event found in step 6 needs to be reviewed. Either an event will require escalation if it is clearly serious enough, or it will require enhanced monitoring or other precautionary measures, or it is a false positive. The purpose of this step is to decide how to react to the suspicious event. The decision as to whether to escalate the situation to management will depend on any indications that a major business impact is likely or that a full investigation may be required where digital evidence may be needed. The decision criteria should be captured in an escalation policy that makes it clear when a suspicious event becomes a confirmed incident. At this point an investigation should be launched and policy should indicate who the points of contact are (potentially available on a 24x7 basis) and who else needs to be involved. As with steps 3 and 6, the network and IT security managers and the non-IT managers need to understand each other's position. What level of certainty or level of risk is appropriate for an escalation? What strength of case is required to proceed? A preliminary business impact assessment should be made based on whether any of the following are present:

- Evidence of a reportable crime

- Evidence of internal fraud, theft, other loss
- Estimate of possible damages (a threshold may induce an escalation trigger)
- Potential for embarrassment, reputation loss
- Any immediate impact on customers, partners or profitability
- Recovery plans have been enacted or are required; and
- The incident is reportable under a compliance regime.

8. Train staff, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence: A wide range of staff may become involved in a computer security incident. The aim of this step is to ensure that appropriate training is developed to prepare staff for the various roles they may play before, during and after an incident. It is also necessary to ensure that staff is competent to perform any roles related to the handling and preservation of evidence. There will be some issues relevant to all staff if they become involved in an incident. The following groups will require more specialized awareness training for example:

- The investigating team;
- Corporate HR department;
- Corporate PR department (to manage any public information about the incident);
- 'owners' of business processes or data;
- Line management, profit center managers;
- Corporate security;
- System administrators;
- IT management;
- Legal advisers; and
- Senior management (potentially up to board level).

At all times those involved should act according to 'need to know' principles. They should be particularly aware whether any staff, such as 'whistle blowers' and investigators, need to be protected from possible retaliation by keeping their names and their involvement confidential. Training may also be required to understand the relationships and necessary communications with external organizations that may become involved.

9. Present an evidence-based case describing the incident and its impact: The aim of an investigation is not just to find a culprit or repair any damage. An investigation has to provide answers to questions and demonstrate why those answers are credible. The questions go along the lines of who, what, why, when, where and how. Credibility is provided by evidence and a logical argument. The purpose of this step is to produce a

policy that describes how an evidence-based case should be assembled. A case file may be required for a number of reasons:

- To provide a basis for interaction with legal advisers and law enforcement;
- To support a report to a regulatory body;
- To support an insurance claim;
- To justify disciplinary action;
- To provide feedback on how such an incident can be avoided in future;
- To provide a record in case of a similar event in the future (supports the corporate memory so that even if there are changes in personnel it will still be possible to understand what has happened);
- To provide further evidence if required in the future, for example if no action is deemed necessary at this point but further developments occur.

10. Ensure legal review to facilitate action in response to the incident: At certain points during the collating of the cyber-crime case file it will be necessary to review the case from a legal standpoint and get legal advice on any follow-up actions. Legal advisers should be able to advice on the strength of the case and suggest whether additional measures should be taken; for example, if the evidence is weak is it necessary to catch an internal suspect red handed by monitoring their activity and seizing their PC? Any progression to a formal action will need to be justified, cost-effective and assessed as likely to end in the company's favour. Although the actual decision of how to proceed will clearly be post-incident, considerable legal preparation is required in readiness. Legal advisors should be trained and experienced in the appropriate cyber laws and evidence admissibility issues. They need to be prepared to act on an incident, pursuant to the digital evidence that has been gathered and the case presented in step 9. Legal advice should also recognize that the legal issues may span legal jurisdictions e.g. states in the US, member states in the EU.
Advice from legal advisers will include:

- Any liabilities from the incident and how they can be managed;
- Finding and prosecuting/punishing (internal versus external culprits);
- Legal and regulatory constraints on what action can be taken;
- Reputation protection and PR issues;
- When/if to advice partners, customers and investors;
- How to deal with employees;
- Resolving commercial disputes; and
- Any additional measures required.

4.11 Issues Facing Computer Forensics

The issues facing computer forensics examiners can be broken down into three broad categories: technical, legal and administrative

4.11.1 Technical Issues

a. **Encryption –** Encrypted data can be impossible to view without the correct key or password. Examiners should consider that the key or password may be stored elsewhere on the computer or on another computer which the suspect has had access to. It could also reside in the volatile memory of a computer (known as RAM) which is usually lost on computer shut-down; another reason to consider using live acquisition techniques, as outlined above.

b. **Increasing storage space –** Storage media hold ever greater amounts of data, which for the examiner means that their analysis computers need to have sufficient processing power and available storage capacity to efficiently deal with searching and analyzing large amounts of data.

c. **New technologies –** Computing is a continually evolving field, with new hardware, software and operating systems emerging constantly. No single computer forensic examiner can be an expert on all areas, though they may frequently be expected to analyze something which they haven't previously encountered. In order to deal with this situation, the examiner should be prepared and able to test and experiment with the behavior of new technologies. Networking and sharing knowledge with other computer forensic examiners is very useful in this respect as it's likely someone else has already come across the same issue.

d. **Anti-forensics –** Anti-forensics is the practice of attempting to thwart computer forensic analysis. This may include encryption, the over-writing of data to make it unrecoverable, the modification of files' metadata and file obfuscation (disguising files). As with encryption, the evidence that such methods have been used may be stored elsewhere on the computer or on another computer which the suspect has had access to. In our experience, it is very rare to see anti-forensics tools used correctly and frequently enough to totally obscure either their presence or the presence of the evidence that they were used to hide.

4.11.2 Legal Issues

Legal issues may confuse or distract from a computer examiner's findings. An example here would be the 'Trojan Defense'. A Trojan is a piece of computer code disguised as something benign but which carries a hidden and malicious purpose. A lawyer may be able to argue that actions on a

computer were not carried out by a user but were automated by a Trojan without the user's knowledge; such a Trojan Defense has been successfully used even when no trace of a Trojan or other malicious code was found on the suspect's computer. In such cases, a competent opposing lawyer, supplied with evidence from a competent computer forensic analyst, should be able to dismiss such an argument. A good examiner will have identified and addressed possible arguments from the "opposition" while carrying out the analysis and in writing their report.

4.11.3 Administrative Issues

a. **Accepted standards –** There are a plethora of standards and guidelines in computer forensics, few of which appear to be universally accepted. The reasons for this include: standard-setting bodies being tied to particular legislations; standards being aimed either at law enforcement or commercial forensics but not at both; the authors of such standards not being accepted by their peers; or high joining fees for professional bodies dissuading practitioners from participating.
b. **Fit to practice –** In many jurisdictions there is no qualifying body to check the competence and integrity of computer forensics professionals. In such cases anyone may present themselves as a computer forensic expert, which may result in computer forensic examinations of questionable quality and a negative view of the profession as a whole.

4.12 Let us Sum-up

Computer forensics is the practice of collecting, analyzing and reporting on Computer data in a way that is legally admissible. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel. Computer crime, or cybercrime, is any crime that involves a computer and a network. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare.

The survival and integrity of any given network infrastructure of any company or organization strongly depends on the application of computer forensics. Forensic readiness is the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation.

Monitoring should be targeted at specific problems. Physical security of data such as back-up files or on central log servers is important from the data protection point of view, and also for secure evidence storage.

A policy for secure storage and handling of potential evidence comprises security measures to ensure the authenticity of the data and also procedures

to demonstrate that the evidence integrity is preserved whenever it is used, moved or combined with new evidence.

The aim of an forensic investigation is not just to find a culprit or repair any damage. An investigation has to provide answers to questions and demonstrate why those answers are credible. At certain points during the collating of the cyber-crime case file it will be necessary to review the case from a legal standpoint and get legal advice on any follow-up actions.

4.13 Self Assessment Questions

1. Name the four stages of computer forensic process.

……
……
……
……
……

2. Outline the uses of computer forensics.

……
……
……
……
……
……

3. Mention the objectives of computer forensics?

……
……
……
……
……

4. Write the role of a forensics investigator?

……
……
……
……
……

5. What are the benefits of forensic readiness?

……
……
……
……
……

6. Explain various steps involved in forensic readiness planning.

……
……
……
……
……

4.14 References & Further Readings

1. Digital Forensics, (PGDCS-07), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security,
2. Robert Rowlingson Ph.D , qinetiq Ltd., A Ten Step Process for Forensic Readiness, International Journal of Digital Evidence, Winter 2004, Volume 2, Issue 3.
3. ICT and Education, Fundamental of ICT in education, By Dr. T. Manichander.
4. http://einvestigations.com/computer-forensics/expert-witness/
5. http://searchsecurity.techtarget.com/definition/computer-forensics
6. https://www.linkedin.com/pulse/computer-forensic-egharevba-etinosa-aca-acfe-amscce-clrmp-ifrs-cert.
7. https://forensiccontrol.com/resources/beginners-guide-computer-forensics.

Answer to Self Assessment Questions (Unit-1)

1. **What is disaster recovery plan (DRP)?**
   A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster. It is "a comprehensive statement of consistent actions to be taken before, during and after a disaster."
2. **Why DRP is important? Write its benefits.**
   As IT systems have become increasingly critical to the smooth operation of a company, and the importance of ensuring the continued operation of those systems, and their rapid recovery, has increased.
   So preparation for continuation or recovery of systems needs to be taken very seriously. This involves a significant investment of time and money with the aim of ensuring minimal losses in the event of a disruptive event.
3. **What is Disaster recovery? What are its impacts on different organization?**
   Disaster recovery (DR) is an area of security planning that aims to protect an organization from the effects of significant negative events. DR allows an organization to maintain or quickly resume mission-critical functions following a disaster.
   As businesses have become more reliant on high availability, the tolerance for downtime has decreased.

A disaster can have a devastating effect on a business. Studies have shown that many businesses fail after experiencing a significant data loss, but DR can help.

Recovery point objective (RPO) and recovery time objective (RTO) are two important measurements in disaster recovery and downtime.

4. **Describe different types of Disasters with appropriate example.**

Disasters can be classified into two broad categories:

(i)Natural Disasters

The first is natural disasters. A **natural disaster** is a major adverse event resulting from **natural** processes of the Earth. The examples include floods, tsunamis, tornadoes, hurricanes/cyclones, volcanic eruptions, earthquakes, heat waves, and landslides. While preventing, a natural disaster is very difficult, risk management measures such as avoiding disaster-prone situations and good planning can help.

(ii) Man-Made Disasters

Man-made disasters are the consequence of technological or human hazards. Examples include stampedes, urban fires, industrial accidents, oil spills, nuclear explosions/nuclear radiation and acts of war. Other types of man-made disasters include the more cosmic scenarios of catastrophic global warming, nuclear war, and bioterrorism.

5. **What is the relationship between BCP and DRP?**

Disaster Recovery Plans (DRP) is comprehensive statement of actions to be taken before, during and after a disaster that causes loss of availability of Information Systems. Primary objective of DRP is to provide an alternate processing site and return to primary site within a minimal time frame when ever any disaster occurs in the information systems. Whereas the Business Continuity Plans (BCP) suggests a more comprehensive approach to deal with the restoration of computer systems with all attendant software and connections to full functionality under a variety of damaging or interfering external conditions that businesses face from time to time.

6. **What are different types of Disaster recovery control measures?**

IT disaster recovery control measures can be classified into the following three types:

a) **Preventive measures** - Controls aimed at preventing an event from occurring.

b) **Detective measures** - Controls aimed at detecting or discovering unwanted events.

c) **Corrective measures** - Controls aimed at correcting or restoring the system after a disaster or an event.

7. Write the steps of Disaster Recovery planning methodology.

According to Geoffrey H. Wold of the Disaster Recovery Journal, the entire process involved in developing a Disaster Recovery Plan consists of 10 steps:

1. Obtaining Top Management Commitment
2. Establishing a Planning Committee
3. Performing a Risk Assessment
4. Establishing Priorities for Processing and Operations
5. Determining Recovery Strategies
6. Collecting Data
7. Organizing and Documenting a Written Plan
8. Developing Testing Criteria and Procedures
9. Testing the Plan
10. Obtaining Plan Approval

Answer to Self-Assessment Questions (Unit-2)

1. What is a Digital Signature? What is its purpose?

A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity). In simple words a digital signature Digital signatures are the public-key primitives of message authentication.

2. Explain the working of a Digital Signature.

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash - along with other information, such as the hashing algorithm - is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.

3. **Compare Digital Signatures with Ink-on paper signatures.**

   A pen and ink signature is a biometric, not a secret. By careful examination of the physical paper, one can determine that a live person actually swished a pen over the paper, and thus that a live person with certain distinctive habits of writing made that mark. No secret is involved, but it is physically difficult for one living person to perfectly imitate another.

   But Digital signatures rely on a secret, either a secret passphrase, or, more commonly, a secret file. Anyone (without needing to know the secret) can check that two documents were signed by the same secret, and thus presumably by the same person, and that neither document has been changed since it was signed.

4. **Write the uses of Digital Certificates.**

   Your digital certificate could be used in the following ways:

   To allow you to access membership-based web sites automatically without entering a user name and password.

   It can allow others to verify your "signed" e-mail or other electronic documents, assuring your intended reader(s) that you are the genuine author of the documents, and that the content has not been corrupted or tampered with in any way.

   The digital certificates enable others to send private messages to someone. Anyone else who gets his/her hands on a message meant for you will not be able to read it.

5. **Discuss the importance of Digital Signature in Information Security.**

   Digital signatures enable the business organizations to manage their monetary subsidiary and cost of paper work. Also, these signatures help the companies in proving that they are utilizing the green policies and eco-friendly procedures by cutting back the use of pen and paper. This vast technology even reduces the time consumed in sending numerous emails and documents, since the entire work is entitled in few moments. The corporations prove their sharp time management skills through this technology. As organizations move away from paper documents with ink signatures or authenticity stamps, digital signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory.

Answer to Self-Assessment Questions (Unit-3)

1. **Explain the various components of CIA Triad. Explain each of them.**

   An ethical hacker is trying to preserve what is known as the CIA triad: confidentiality, integrity, and availability. The following list describes these core components:

a) **Confidentiality:** The core principle that refers to the safeguarding of information and keeping it away from those not authorized to possess it. Examples of controls that preserve confidentiality are permissions and encryption.

b) **Integrity:** Deals with keeping information in a format that is true and correct to its original purposes, meaning that the data that the receiver accesses is the data the creator intended them to have.

c) **Availability:** The final and possibly one of the most important items that you can perform. Availability deals with keeping information and resources available to those who need to use it. Information or resources, no matter how safe and sound, are only useful if they are available when called upon.

2. **What are the various types of hackers? Explain each of them briefly?**

   Hackers can be classified in to the following types based on their depth of knowledge and activities.

a) **White Hats:** White hats are the good guys, the ethical hackers who use their hacking skills for defensive purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weaknesses and implement countermeasures.

b) **Black Hats:** Black hats are the bad guys: the malicious hackers or crackers who use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote systems, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and just cause problems for their targets.

c) **Gray Hats:** Gray hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker.

d) **Suicide Hackers:** Individuals who will aim to bring down the critical infrastructure whatever the consequence may be.

e) **Script Kiddies:** In hacker culture a script kiddie or skiddie are unskilled individuals who use scripts or programs developed by others to attack computer systems and networks and deface websites.

f) **Hacktivist:** Detects and sometimes reports or exploits security vulnerabilities as a form of social activitism. A hacktivist is a hacker who utilizes technology to announce a social ideological, religious or political message.

3. Enumerate and explain various phases involved in penetration testing. Briefly explain each of them.

A Pen-tester uses the same methodology as a hacker does, we will be using this terminology interchangeably

a) Foot printing

Foot printing, is a method of observing and collecting information about a potential target with the intention of finding a way to attack the target. Foot printing looks for information and later analyzes it, looking for weaknesses or potential vulnerabilities.

Foot printing is about gathering information and formulating a hacking strategy.

b) Scanning

It focuses on an active engagement of the target with the intention of obtaining more information. Scanning the target network will ultimately locate active hosts that can then be targeted in a later phase. Foot printing helps identify potential targets, but not all may be viable or active hosts. Once scanning determines which hosts are active and what the network looks like, a more refined process can take place.

Scanning involves taking the information discovered during reconnaissance and using it to examine the network.

c) Enumeration

Enumeration is the systematic probing of a target with the goal of obtaining user lists, routing tables, and protocols from the system.

Enumeration occurs after scanning and is the process of gathering and compiling usernames, machine names, network resources, shares, and services. It also refers to actively querying or connecting to a target system to acquire this information.

Answer to Self-Assessment Questions (Unit-4)

1. Name the four stages of computer forensic process.

The overall computer forensics process is sometimes viewed as comprising four stages:

i. **Acquire**: Identifying and Preserving
ii. **Analyze**: Technical Analysis
iii. **Evaluate:** What the Lawyers Do
iv. **Present:** Present Computer evidence in a manner that is legally acceptable in any legal proceedings.

2. Outline the uses of computer forensics.

The computer forensics is used in variety of cases such as:

- Intellectual Property theft
- Employment disputes
- Fraud investigations
- Forgeries
- Bankruptcy investigations
- Inappropriate email and internet use in the work place
- Regulatory compliance

3. Mention the objectives of computer forensics?

The objectives of Computer forensics are to provide guidelines for:

- Following the first responder procedure and access the victim's computer after incident.
- Designing procedures at a suspected crime scene to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication.
- Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Provide guidelines for analyzing digital media to preserve evidence, analyzing logs and deriving conclusions, investigate network traffics and logs to correlate events, investigate wireless and web attacks, tracking emails and investigate email crimes.
- Producing computer forensic report which provides complete report on computer forensic investigation process.
- Preserving the evidence by following the chain of custody.
- Employing the rigorous procedures necessary to have forensic results stand up to scrutiny in a court of law.
- Presenting Computer forensics results in a court of law as an expert witness.

4. Write the role of a forensics investigator?

Following are some of the important duties and role of a forensic investigator:

- Confirms or dispels whether a resource/network is compromised.
- Determine extent of damage due to intrusion.
- Answer the questions: Who, What, When, Where, How and Why.
- Gathering data in a forensically sound manner.
- Handle and analyze evidence.
- Prepare the report.
- Present admissible evidence in court.

5. What are the benefits of forensic readiness?

Forensic readiness can offer an organization the following benefits:

- Evidence can be gathered to act in an organization's defense if subject to a lawsuit;
- Comprehensive evidence gathering can be used as a deterrent to the insider threat (throwing away potential evidence is simply helping to cover the tracks of a cyber- criminal);
- In the event of a major incident, an efficient and rapid investigation can be conducted and actions taken with minimal disruption to the business;
- A systematic approach to evidence storage can significantly reduce the costs and time of an internal investigation;
- A structured approach to evidence storage can reduce the costs of any court-ordered disclosure or regulatory or legal need to disclose data (e.g. in response to a request under data protection legislation);
- Forensic readiness can extend the scope of information security to the wider threat from cyber-crime, such as intellectual property protection, fraud, extortion etc.;
- It demonstrates due diligence and good corporate governance of the company's information assets;
- It can demonstrate that regulatory requirements have been met;
- It can improve and facilitate the interface to law enforcement if involved;
- It can improve the prospects for a successful legal action;
- It can provide evidence to resolve a commercial dispute;
- It can support employee sanctions based on digital evidence (for example to prove violation of an acceptable use policy)

6. Explain various steps involved in forensic readiness planning.

The following ten steps describe the key activities in forensic readiness planning:

1. Define the business scenarios that require digital evidence;
2. Identify available sources and different types of potential evidence;
3. Determine the evidence collection requirement;
4. Establish a capability for securely gathering legally admissible evidence to meet the requirement;
5. Establish a policy for secure storage and handling of potential evidence;
6. Ensure monitoring is targeted to detect and deter major incidents;
7. Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched;
8. Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence;
9. Document an evidence-based case describing the incident and its impact.
10. Ensure legal review to facilitate action in response to the incident.