# CPE515 COMPUTER SECURITY TECHNIQUES I

- **Nontechnical attacks.**
- **Password protection and its vulnerability.**
- **Worm propagation and countermeasures: Intrusion detection, access control, scanning and analysis tools, port scanners, operating system detection tools, access control devices, vulnerability scanners, packet sniffers, wireless security tools.**
- **Disaster recovery: Recovery requirements, policy, strategy, technical team. Execution of recovery plans. Documentation and backup system. Loss estimation.**

**1. Non-technical attacks.**

Computer attack is any attempt of gaining an unauthorized access into a system/computer or network, to steal or destroy unauthorized assets. Attack maybe technical or non-technical attack.

**Non-technical attack** is the type of attack that uses social pressure to induce computer users to reveal sensitive information or to go against the security of a network/system to which those individual have access. This is one of the dangerous attacks that happening these days.

a) **Social Engineering**- This is an art of obtaining vital information from the victim without making him aware that he is being manipulated. The worst part of this social engineering is that, it is difficult to detect and fight, as we cannot correct human factors on what can be done in hardware and software. A number of social engineering methods are listed below.

i) **Dumpster Diving**: – it is a practice where hackers with bad intent scroll through recycle bin in a system so to get hold of useful links. It also provides confidential business information such as telephone contacts, hardware disk, memos and source codes impressions.

ii) **Impersonation over the phone**: – this is the easiest and most common way to manipulate a person over the telephone calls as it is widely used worldwide.

iii) **Phishing**: –This has fundamentally evolved based on social engineering as well as a disruptive methodology in mobile network known as phreaking. How it works, is by sending an email with malicious code to the user and this designed code in a way will looks like legit. By getting sensitive information or data, such as usernames, passwords and credit card details or other sensitive details

**2a. Password protection and its vulnerability**

A password is a secret goes with an identity. This links two elements, something what we own (an ATM card, badge, telephone, and fingerprint) and what we know (password or code/PIN). Passwords are commonly used for computers, telephones and banking and the simplest form is the personal identification number which known as PIN, with four to six numbers. Our smartphones use two PIN codes, one to unlock the device, and another associated with the SIM card, to access the network. Passwords are also associated with Internet services, like e-mails, social networks, e-commerce, etc.

Password protection can be defined as the security measured that protects information accessible on computers/system that needs to be protected from unauthorized persons. Password theft is the main risk in using

passwords for protection, in which the associated identity is stolen. A password must be kept hidden and remains secret in preventing identity theft when incidents arise, such as the theft of G boy's usernames.

These are some of the methods that makes password vulnerable and what precautions to take.

**2b. Password protection vulnerability**

Password Vulnerability due to Phishing: This type of attack makes victims to think they are accessing genuine content, which usually e-mail or websites, while in fact they are accessing fake/cloned content which produced by the attackers/hackers. This is a method in which attackers used to collect victim login information and store it, before redirecting the victims to legitimate site. One can only avoid this, by double-checking the address and the link to make sure it belong to desired location.

2. Brute Force Attack: This also known as brute force cracking is a cyber-attack equivalent of trying every key on your key ring and finally find the right one. Although, Brute force attacks are simple and reliable, where attackers let a computer do the work by trying different combinations of usernames and passwords until they find one that works. This type of attack cannot really be prevented because its robotic software that perform the action, but it possible to reduce suck hacking by increase the security of the website and by creating more complex password

3. Dictionary or Wordlist Attack: The dictionary-based attack is also considered a brute-force attack. Here, the attacker uses files containing thousands or even millions of words of the most varied types, languages, and software that allows this list to be tested quickly until the victim's password is found or until the dictionary finishes. This can be prevented by using complex password that is even more than 12 characters

4. Social Engineering: This is somewhat similar to phishing attacks and is a common spying method aimed at gaining access to confidential data. To extract confidential information, scammers very often exploit good faith, helpfulness, but also the insecurity of people. Whether over the phone, pretending to be someone else or the Internet, they are ready to do anything to get access to personal data. This can be avoided by revealing as little personal information as possible; social networks are real mines of information. To be suspicious when someone is asking for much details.

5. Malware attack: This the most obvious and efficient method to steal passwords now. Unlike most powerful viruses, they are not so apparent because their goal is to steal your data without you knowing or introduce a remote access Trojan horse to steal your credentials. To prevent this from happening is to keep your antivirus up to date, scan frequently, and avoid suspicious sites that are full of pop-up ads.

**3a. Worm propagation and countermeasures**

The task of propagating malicious code is to locate new targets to attack in the system. Viruses hunt for files in a computer system to which to attach, whereas worms search for new targets to which to propagate themselves. Depending on their method of transmission, hackers have developed different tactics for finding new victims. Worms transmitted via email have had great success propagating themselves because they find their next targets either by raiding a user's email address book or by searching through the user's mailbox. Such addresses are almost certain to be valid, permitting the worm to hijack the user's social web and exploit trust relationships. In most cases, the worm will create its own message to send to the target, but some will wait for the user to send a message

and attach themselves to it. Network worms, those that attack network services, must determine their next victim's IP address.

**Table 1:** Trojan, Virus, and Worm Differential

| | **Trojan** | **Virus** | **Worm** |
|---|---|---|---|
| **Definition** | Malicious program used to control a victim's computer from a remote location | Self-replicating program that attaches itself to other programs and files | Illegitimate programs that replicate themselves usually over the network |
| **Purpose** | Steal sensitive data, spy on the victim's computer, etc. | Disrupt normal computer usage, corrupt user data, etc. | Install backdoors on victim's computer, slow down the user's network, etc. |

**3b. Countermeasures**

- Use of anti-virus software, and must be frequently updated
- Update patches for operating systems, downloading operating system updates can help reduce the infection and replication of worms.
- Security policy on usage of the internet and external storage media, etc.
- Regular backups of critical information must be made and stored, preferably read-only media such as CDs and DVDs.
- Worms can also be avoided by scanning, all email attachments before downloading them.

**Access control and Intrusion detection:** These are cohesive system, which permits user to control and monitor physical access to a certain areas. If access control chooses who is permitted to be in a certain place at a certain time doing certain things, then intrusion detection is the process of guaranteeing access violations do not occur. This Intrusion detection involves constant monitoring and automatic/real-time feedback in a system. Like with access control, this may occur in a software/digital or hardware/physical state. Intrusion detection typically falls into one of five categories

1. Physical Surveillance: Video surveillance software secures perimeters, while other tools such as remote desktop monitoring programs keep an eye on user activity.

2. Network Oversight: Network intrusion detection systems monitor inbound and outbound traffic on a server or network

3. Host Monitoring: By monitoring devices and machines themselves, host monitoring spots malicious behavior arising from internal system and from machines, which have been compromised by malware.

4. Anomaly Detection: Many different attack routes occur, but unusual behavior is often a common thread between them.

5. Signature-Based Detection: Since most attacks and access violations have occurred before, robust intrusion detection systems can identify signatures, patterns of behavior associated with attacks.

When combined both access control and intrusion detection together, the two security approaches create extensive security, which keeps a one's valuable assets safe. Here is how they work together.

1. Access control sets restrictions for authorized access and use, making intrusion detection possible.

Access control helps set the baseline of normal activity by establishing rules regarding access and behavior. When proper use and normal traffic flows is recognized, it becomes much easier to spot improper use or intruders.

2. Intrusion detection helps to identify and implement access control.

Sometimes, intrusion detection may help spot instances where authentic access is necessary outside the bounds of what is allowed. Repeated intrusion alerts may be the first sign that access control policies may need to evolve.

3. In combining intrusion detection and access control together, the effect is greater than the sum of their separate effects.

For individual or company to secure a network or a system, they must know what to secure.

a) scanners & analysis tools can find weaknesses in systems, and security holes in individual system components and unsecured area of the network (hosts, routers, firewalls)
b) scanning tools are used to collect information needed by an attacker to succeed. Preparation part is known as Footprinting (Example of tool used: Sam Spaden). While the next part is fingerprinting, which is systematic examination of all of the Internet addresses of the organization and proceed to next activity, i.e. Port scanners, vulnerability Scanners or Packet Sniffers
c) many scanners and analysis tools are developed by hacker community, and are 'freeware'
    - these same tools can also be used by network/system defenders to find potential vulnerabilities in the network/system

**Categories of hacking tools**

1) Port Scanners
2) Network Mappers
3) Operating System Detection Tools
4) Firewall Analysis Tools
5) Vulnerability Scanners
6) Packet Sniffers
7) Wireless Sniffers
8) Password Crackers

1. **Port scanning utilities**

- This is to first identify (or fingerprint) computers that are active on a network, as well as the ports and services active on those computers, the functions and roles the machines are fulfilling, and other useful information.
- A port is a network channel or connection point in a data communication system.
- In TCP/IP network protocol TCP and User Diagram Protocol (UDP) port numbers differentiate between multiple communication channels used to connect to network services being offered on the same network device.
- An Open port can be used to send commands to a computer, gain access to a server, and exert control over a networking device.

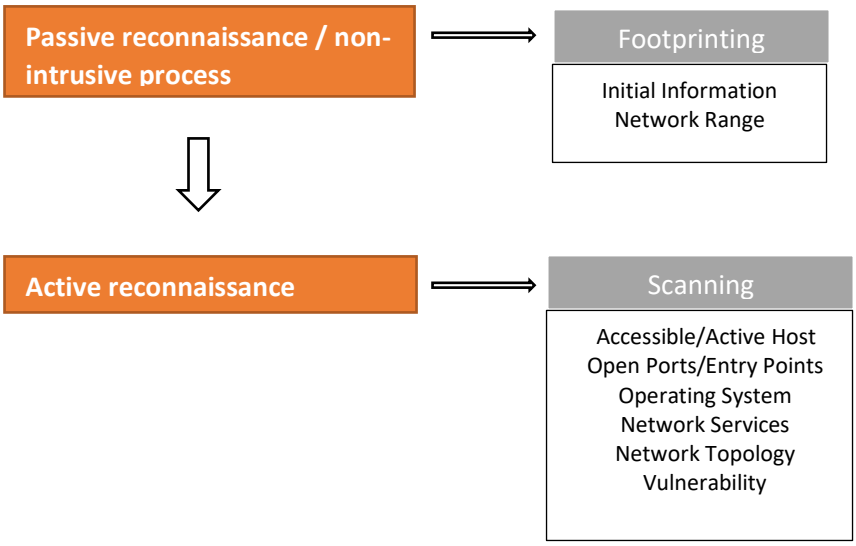



**Figure 1**: Information Generating Approach

**The output of port scan can be:**

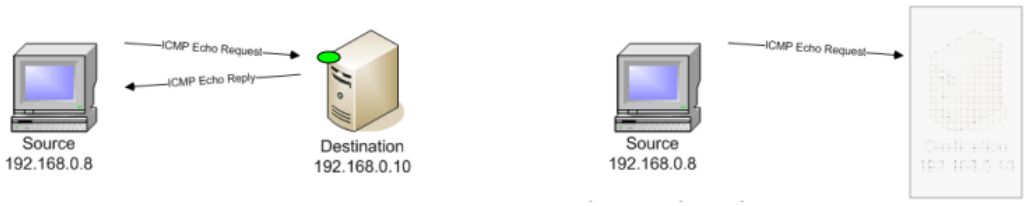
- open or accepted: host sends reply indicating that service is available on a port
- closed / denied / not listening: host sends reply indicating unavailable service on a port
- filtered / dropped / blocked: there is no reply

**Popular scanners:**

- Nmap (UNIX / Windows) – can rapidly sweep large networks, can bypass firewalls, IDSs (Intrusion Detection Systems) etc.
- SuperScan 4.0 (Windows) – GUI based with additional tools in one interface
- Advanced Port Scanner (Windows) – small, fast, straightforward GUI

**a. Port Scanner Techniques**

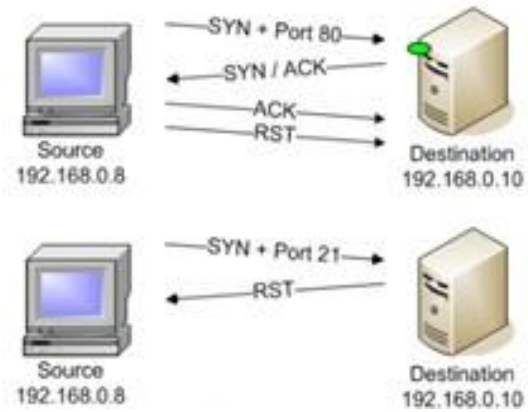
1) **ICMP (Internet Control Message Protocol) Ping Scan**: This is a Layer 3 protocol, but useful for probing of all active hosts in a network known as host scanning, this is not really port scanning. The scanner send single ICMP request to a destination; an ICMP response will not arrive back if the destination is not available or ICMP protocol is filtered. It is potentially faster than other footprinting technique, because it only sent one packet per machine. Though it does not provide lots of information




UDP to a closed port => ICMP unreachable arrives back

**Figure 2**: ICMP Ping scan to an open port and to closed port

2) **TCP (Transmission Control Protocol) connect() Scan**: This is most basic form of TCP scanning, which uses OS's connect() function is used to connect to a desired port. This technique is easy to implement; however, very slow and detected (loged) by most sites/firewalls




TCP to a closed port : (unless RST=1)

**Figure 3**: TCP connect() scan to an open and closed port

3) **TCP SYN Scan known as 'half-open' scanning**: Here, instead of using OS' network function, the scanner itself generates TCP-SYN packets; upon receiving a TCP-ACK, scanner immediately sends a RST to close the connection thus, handshake is never completed. This is most popular form of TCP scan, since most sites do not log half-open connections, which is much 'quieter' than connect() scan. This requires programming at OS level.


**Figure 4**: TCP SYN scan to an open and to a closed port

4) TCP FIN Scan (Stealth Scan): This is type of scan that sends a single frame to a TCP port without any TCP handshaking / additional packets. When TCP FIN scan sends a FIN packet, a closed port will reply with a

proper RST while an open port will ignore the packet “silence indicates an open port”. A UNIX system is vulnerable, but Microsoft is immune to this type of attack (RST sent regardless of the port state)


**Figure 5**: TCP FIN scan an open and to a closed port

5) **Xmas-Tree Scan (Stealth Scan):** This scanner sends a TCP frame with URG, PUSH and FIN flags set. In a Xmas packet, a few flags other than RST are set to 1, and when as in TCP FIN scan, silence indicates an open port.

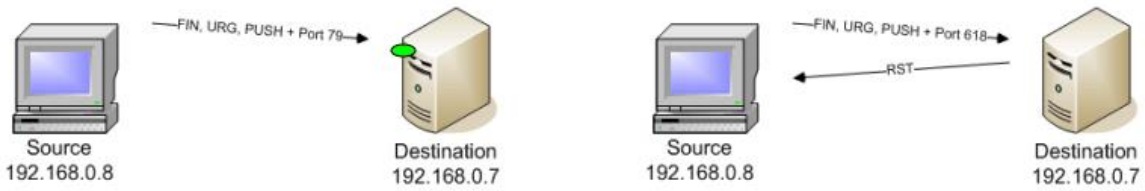



**Figure 6**: Xmas – Tree scan to an open and to a closed port

6) **UDP ICMP Scan**: The previous scans find TCP ports/services; but this scan looks for UDP ports/services. The scanner sends empty UDP datagrams and if port is listening, system sends back an error UDP message or nothing; but if port is closed, system sends an ‘ICMP Port Unreachable’ both UDP and ICMP are not guaranteed to arrive. However, many false positives possible and a rather slow scan, as some systems limit the ICMP error message rate.

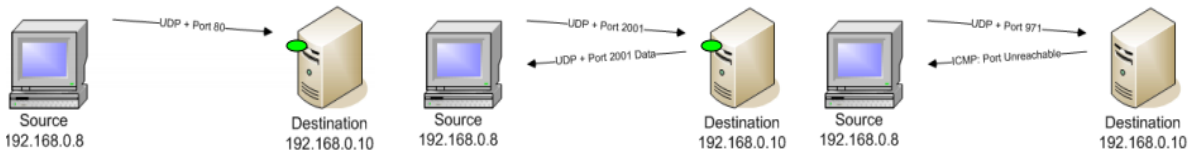



**Figure 7:** UDP ICPM scan to an open and to a closed port

**2. Operation System Detection Tools (OS Fingerprinting Tools)**

The aim is to detect target host’s OS. Knowing a host’s OS is a critical if one is to exploit the host’s vulnerabilities (e.g. known bugs of that OS).Fingerprinting maybe passive or active

- Passive fingerprinting – occurs without obvious querying of host machine (e.g. obtain information through sniffing)

- Active fingerprinting – directly query host machine; replies are matched against database on known responses.

Examples of OS detection tools are:

- ✓ Nmap: software tools that identify all systems connected to a network, using ICMP Ping
- ✓ Xprobe: These tools are heavily dependent upon the usage of the TCP protocol for remote active operating system fingerprinting.

I. **OS Detection techniques in active fingerprinting** (TCP/IP stack is pretty much a fixed standard, different OS vendors interpret the standard differently)

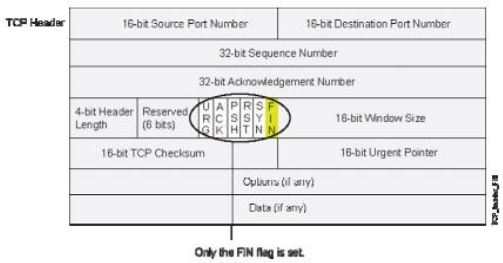
Active fingerprinting takes advantage of differences in TCP/IP implementation

a) a crafted packet is sent to a remote system to elicit a unique response from the TCP/IP stack of the underlying OS
b) the unique response is referred to as an OS fingerprint or signature
c) the attacker than carefully analyzes and compares the fingerprint to a database – comprising a wide range of known OS fingerprints …

**Nmap Fingerprint Methods**

1. TCP FIN Probing

a) TCP RFC requires that a system with an open port ignores (not respond to) a FIN packet if received at the start of a connect.
b) Microsoft Windows disregard this requirement and replies to the FIN packet with a RST packet



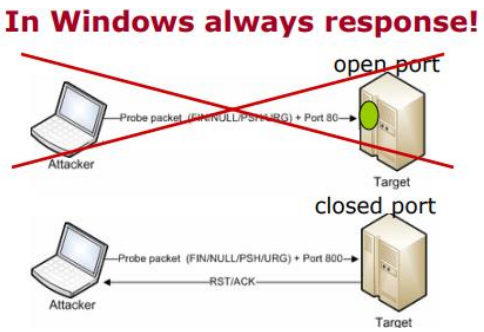




**Figure 8**: Probe a machine with a FIN packet on a port that is KNOW to be open, if you receive a response=> Windows OS

2. TCP Initial Sequence Number (ISN)

- when receiving a request to establish a connection, an OS must choose an ISN to respond and continue the 3-way handshake
- some OS choose ISN based on randomized values, while others (Windows) generate the ISN based on system's internal clock (ISN is incremented by 1 every 4 microseconds)

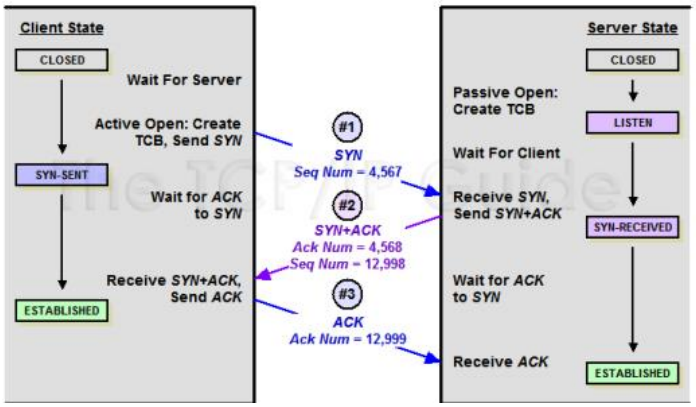



**Figure 9**: 3-way handshake/ TCP 3-way handshake

3. TCP Initial Window Size

- some OSs are known to use a unique Window size
- e.g. Linux 2.4 IWS=5840 bytes, Linux 2.2 IWS=32120 bytes

4. IP ID Sampling

- Windows OS usually use a predictable IP ID sequence numbers, such as increasing the number by 1 or 256 for each packet
- other OS, e.g. Linux, randomize IP ID numbers

5. ICMP Error Message Quoting

- according to ICMP RFC, OS must quote some parts of the original (ICMP) message - first 8 bytes - when generating an ICMP error message
- Linux and Solaris include much more information than required

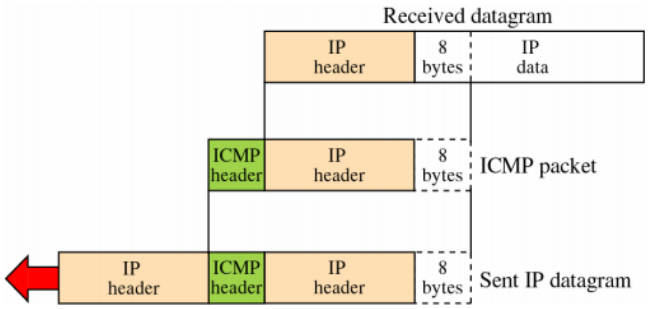



**Figure 10**: Example of UDP packet to a closed port

## II. OS Detection Techniques in Passive fingerprinting

This is less intrusive way to gather information about the OS of a remote host.

Instead of actively querying, attacker sniffs remote host's packets. It also generally less precise/effective than active fingerprinting because;

- have to accept whatever communication happens - there may not be much of it!
- has fewer header parameters/options to work with than active fingerprinting
- some of those parameters often get modified by firewall or proxy

On Nmaps 'avoided methods' list

a) Time-to-Live (TTL) in IP packets
- normally Linux sets TTL = 64, and Windows TTL = 128

b) Don't Fragment Bit in IP packet
- Most systems set it to 1; in OpenBSD set to 0

c) Type of Service (TOS)
- Normally set to 0; a few OS reported using different value. (Generally not reliable as the TOS value is often set by application.)

Example: Idle Scan by Nmap. Assume a sniffer/attacker has capture a packet with the following parameters and by traceroute, you observed 13:

Time-to-Live (TTL): 51
TCP Window Size: 57344
Don't Fragment Bit: 1
Type of Service (TOS): 0

How would you go about determining the host's OS?
**Solution** The original TTL is 51 + 13 = 64, therefore the host's OS should be Linux

**OS Detection Countermeasure**

To reduce chances of an OS being 'fingerprinted', OS's responses to various network requests/packets must be modify.

a) IP Personality – a patch for Linux kernel – allows changes to TCP/IP stack
- IP ID field, TCP Initial Window, TCP initial Sequence Number … values can be changed

b) Morph and IP Scrubber – operate in firewall manner
- any traffic traveling from local net. will be 'scrubbed' & any OS-related information will be removed

**3. Access Control Devices**

- Proximity Reader: Proximity Readers detect transmission from proximity cards and pass the credential data to be compared to the access control list.

  **Features**: a) Low Profile
  b) LED indicator for go/no-go verification.

**Benefits**: a) Doesn't require a card to be physically inserted in order to be verified

b) Easier to operate

- Keypad Reader: Keypad Readers provide a means for a user to enter a numeric code for additional verification.

  **Features**: a) 12-keys

  b) Requires code and/or credential to gain entry using dual factor authentication.

  **Benefits**: a) Requires credential AND special knowledge of a PIN

- Biometric Reader: Biometric Readers use physical credentials unique to further identify the user.

  **Features**: a) Touch-sensitive reading device

  b) Indicator for read/no-read and go/no-go

  **Benefits**: a) Prevents someone from using another's card for unauthorized entry.

- Multi-Technology Reader: Multi-technology Readers can accommodate more than one signal/technology.

  **Features**: a) Dual-frequency reader

  b) Read/write functionality between smart cards and reader

  **Benefits**: a) Supports both smart cards and proximity cards at the same time.

- Request to Exit-Motion: A Request to Exit (REX) - Motion is a device that uses motion technology to detect if a user leaving the access-controlled area.

  **Features**: a) Detects motion

  b) Passes signal to shunt the door contact

  **Benefits**: a) Authorizes egress, preventing door-forced alarms

  b) Improves Reporting

  c) Required by NFPA 101 Life Safety Code in many situations

- Mag-locks: A locking device that consists of an electromagnet that contacts an armature plate to lock when energized.

  **Features**: a) Electromagnetic locking device

  b) Works in conjunction with Request to Exit device or emergency egress button

  **Benefits**: a) Replaces standard key-locks, allowing for/aiding in use of an access control system

- Emergency Release Button: Used in conjunction with a Motion REX on doors in the path of egress.

  **Features**: a) Allows person to manually override the lock in an emergency

  b) Typically connected to the REX-Motion input to prevent false alarms

  **Benefits**: a) Prevents a person from being locked in if the system temporarily fails

- Mag Stripe Reader: A mag-stripe card can be swiped through the reader in both directions to identify the user, and the reader’s microprocessor automatically detects and rejects read errors.

**Features**: a) Swipe only or Swipe and PIN configurations

b) Various output modes

**Benefits**: a) Weatherproof design for either indoor or outdoor applications

b) Small size provides mullion mount, wall mount or single gang electrical box mounting plat

- Mag Stripe Card: A card with a programmable magnetic stripe used to identify a user by means of a Mag-Stripe reader

**Features**: a) Programmable Magnetic Stripe

**Benefits**: b) Ease-of-use, Low cost-of-entry

**4. Vulnerability Scanners**

Is a software tools that assess security vulnerabilities in networks & hosts to produce a set of scan results

i. functionality of port scanners and more!

- e.g. tell you not only which ports are open, but also the name and version of software running on the port, and its vulnerabilities
- Show open network shares
- Expose configuration problems

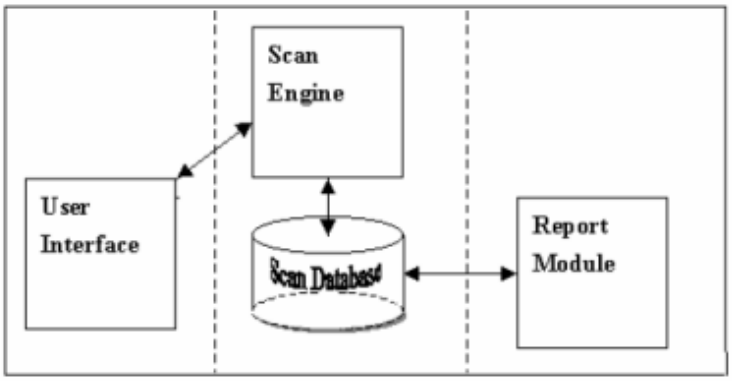



**Figure 11:** Components of a scanner

Example: Nessus

a) Leader in vulnerability scanners – used by over 75,000 companies.
b) Freeware
c) Can scan for vulnerabilities on either a local or a remote host.
d) Comes in different flavors for UNIX, Mac and Windows.
e) Able to detect:
    - open ports / available services
    - misconfigurations (e.g. missing patches)
    - default passwords

- presence of viruses and back-door programs, etc.

Employs client-server architecture:

- Nessus server includes a vulnerability database & a scanning engine.
- Nessus client includes a user configure tool and a report-generator tool.
- Client & server can run on same or different machines (e.g. in case of a slow link).

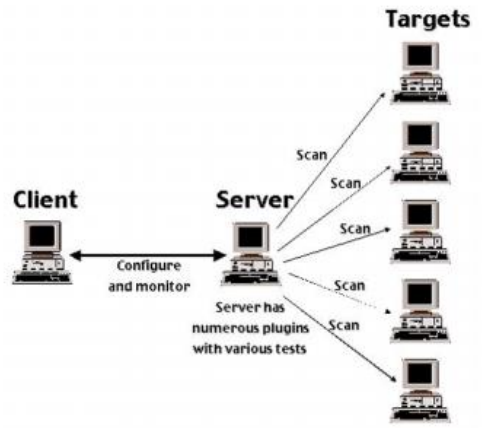



**Figure 12**: Client and Server Scanning

**5. Packet Sniffers also known as network protocol analyzers**: collect copies of packets from the network and analyses the contents

Common use:

- troubleshooting – e.g. diagnose protocol configuration mistakes and resolve network issues
- network traffic characterization – obtain a picture of type and make of network traffic to fine-tune/manage bandwidth
- security analysis – e.g. detect DoS attacks by observing a large number of specific type packets

Example: Ethereal () which allows administrator to examine data from both live network traffic and captured data

For a packet be able to 'sniff' all LAN packets packet sniffer should be put into unrestrained mode

a) to use a packet sniffer legally, one must:

- be under direct authorization of the owners of the network
- have knowledge and consent of the content creators

**6. Wireless Security Tools:** A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess level of privacy or confidentiality afforded on the wireless network. Any organization that spends its time securing wired network and leaves wireless networks to operate in any manner is opening itself up for security breach. Security professional must assess risk of wireless networks

**Wireless Sniffers** – software / hardware capable of capturing & decoding packets as they pass over airwaves

a) wireless sniffing is much easier than wired sniffing

- wireless medium is broadcast medium: everybody sees everything
- in a wired network, the attacker must find a way to install a sniffer on a host or in a target subnet

b) detection of wireless sniffing is extremely difficult – leaves no traceable evidence

c) name typically refers to WiFi (IEEE 802.11) sniffers

**1. Disaster Recovery** (DR): this is an area of security planning that intent to protect an organization's vital IT infrastructure to effectively recover from natural or human-induced disasters, and ensure business continuity.

Disaster recovery is generally a planning procedure and it produces a document, which ensures individual or an organization to solve critical events that affect their activities. Such events can be a natural disaster (earthquakes, flood, etc.), cyber–attack or hardware failure like servers or routers.

As such having a document in place, it will reduce the downtime of business process from the technology and infrastructure side. This document is generally combined with Business Continuity Plan which makes the analyses of all the processes and prioritizes them according to the importance of the businesses. In case of a massive disruption, it shows which process should be recovered first and what should be the downtime. It also minimizes the application service interruption. It helps us to recover data in the organized process and help the staff to have a clear view about what should be done in case of a disaster.

More specifically, a DRP needs to anticipate and delineate a plan of action in response to the loss of such mission-critical IT components and services as:

- Complete computer room environments
- Critical IT hardware including network infrastructure, servers, desktop or laptop computers, wireless devices, and peripherals
- Service provider connectivity
- Enterprise software applications
- Data storage devices or applications

**2. Requirements to Have a Disaster Recovery Plan**

Disaster recovery starts with an inventory of all assets like computers, network equipment, server, etc. and it is recommended to register by serial numbers too. We should make an inventory of all the software and prioritize them according to business importance.

You should prepare a list of all contacts of your partners and service providers, like ISP contact and data, license that you have purchased and where they are purchased. Documenting your entire Network that should include IP schemas, usernames and password of servers.

Table 2: Shown sample of Disaster recovery plan

| Systems | Down Time | Disaster type | Preventions | Solution strategy | Recover fully |
|---|---|---|---|---|---|
| Payroll system | 8 hours | Server damaged | We take backup daily | Restore the backups in the Backup Server | Fix the primary server and restore up to date data |

**3. Preventive steps to be taken for Disaster Recovery**

- The server room/system should have an authorized level. Either, only IT personnel should enter at any given point of time.
- In the server room, there should be a fire alarm, humidity sensor, flood sensor and a temperature sensor.
- At the server level, RAID systems should always be used and there should always be a spare Hard Disk in the server room.
- You should have backups in place; this is generally recommended for local and off-site backup.
- Backup should be done periodically.
- The connectivity to internet is another issue and it is recommended that the headquarters should have one or more internet lines. One primary and one secondary with a device that offers redundancy.
- If you are an enterprise, you should have a disaster recovery site, which generally is located out of the city of the main site. The main purpose is to be as a stand-by as in any case of a disaster, it replicates and backs up the data.

**4. Disaster Recovery Policy:** This is a document that outlines all the processes that must be carried out in the event of a disaster, such as data loss or a manmade error, to ensure that the business is able to perform normally within a short amount of time.

**5. Disaster Recovery Technical Team**: This is a group of individuals that responsible for establishing and maintaining business recovery procedures and coordinating the recovery of business processes and functions. It requires extensive efforts from different teams to come up with a plan, which may be complicated but should have a detailed systematic execution process.

**6. Execution of recovery plans:** It is predictable that every organization will experience an unexpected outage due to some form of disaster. Pandemic events or certain extreme weather conditions are predictable and may allow time to prepare for plan execution. Events like fire or electrical outage are truly unexpected and require immediate execution of the plan. These three phases required in the implementation of the disaster recovery plan (DRP):

- Plan activation phase
- Plan implementation phase
- Primary site restoration

Get the business up and running by executing the three phases of DRP implementation to minimize downtime, recover systems and restore normal operations.

**7. Loss estimation**

The first step for any organization is to look at their recovery time objective (RTO), the amount of time needed to restore applications and systems after a disaster interrupts the businesses. Estimates may costs ₦100, 000 per minute for network downtime, the enterprise then needs to identify its recovery point objective and the maximum acceptable amount of data loss measured in time. Ultimately, these issues boil down to how much data you can afford to lose, and for how long.

The points below should be considered, when establishing your data recovery plan

- **Initial costs**: What hardware or software will need to be purchased? What are the installation or software license costs? Will there be service upgrade fees?
- **Critical applications and services**: How will the business continue to meet security and compliance obligations? How long will it take to recover data about key customers or vendors? Will employees in all locations be able to access recovered data at the same time?
- **Data locations**: Consider that data may be on network servers, laptop computers, desktop computers, and wireless devices. What will be the total cost of recovering all the data, as well as costs for backing up hard copy records and information? What is the best way to extend the useful life of the data protection infrastructure?
- **Technology inventory**: Get a handle on your servers and storage systems, network diagrams, data-center blueprints, and key personnel. What third-party services are currently being used? Will they be able to support the organization in a disaster? How quickly?
- **Testing**: Who will test the solution? How often will such a test be performed? What is the cost of employee training for these tests? What about the training of outside partners? Testing is an important step and should not be ignored as costs may be higher down the road when critical errors are found.
- **Maintenance**: What will be the cost of maintaining the solution in the long term? Who will do this maintenance, and how often? Can technology advances be blended seamlessly into data protection storage?
- **Scalability**: Growing enterprises handle massive and growing amounts of data. The various kinds of data and varying accessibility to users can pose even more challenges when establishing a backup and recovery plan. Data recovery solutions must be able to scale with the business.

**Table 3: Estimation Table**

| **No of System in Use** | **20** |
|---|---|
| **No Of Server in Use** | **2** |
| Causes of Data Loss | Cost of Data Loss |
| Hardware Failure | 200, 000 |
| Human Error | 250, 000 |
| Software Corruption | 75, 000 |
| Computer Viruses | 105, 000 |

| | |
|---|---|
| Theft | 110, 000 |
| Hardware Destruction | 50, 000 |
| **Total** | **590, 000** |