DATE: / / PAGE: STAG

Assignment 2

Que 1

1] What does 'secure' means ?

Ans

A secure network is any home business, school or another network that has security measures in place that help protect it from outside attackers. Once the computer or other device on same network connects to the internet, it immediately becomes vulnerable to attacks.

2] Give features of windows 2003 server

Ans

1] XML web services

2] Directory services

3] Remote access

4] Internet firewall

5] update management

6] File services

3] what is public key encryption service

Ans

Public key encryption is an cryptography system that uses two keys.

- A public key known to everyone

DATE: / /

PAGE:

- A private or secret key known only to recipie of the message.

4] What are the security goals

Ans The primary goal of network security are confidentiality, integrity and availability.

Confidentiality - is sometimes called secrecy or privacy.

Integrity - modification includes writing, changing, deleting & creating

Availability - assets are accessible to authorized parti at appropriate time.

5] State different limitations of firewall

Ans

1] Inside intrusion

2] Direct internet traffic

3] Virus attack.

Qu 2

1] How Amateures are different from career criminals.

Ans

Amatures have committed most of the computer crimes reported to data. Most of them are not career criminals but rather are normal people who observe a weakness in security system that allows them to access cash or other valuables. ~~Amm~~ Amatures does not have skills & they are not a proffesionals.

On the other hand career criminals understands the targets of computer crime. Criminals seldom change fields from arson, murder or auto theft to computing more often criminals begin as computer professionals who engage in computer crime, finding the prospects & payoff good career criminals has predefined target & they have motive to attack.

2) State reasons behind network vulnerability

Ans

1] Anonymity

- An attackers access the web while blocking and tracking or tracking of their identity on the internet.
- An attacker can mount an attack from thousand

of miles away & never come into direct contact with the system.
- The attacks can be passed through many other hosts in an efforts to disguise the attack's origin.

2] Many points of attack with target & origin

- A simple computing system is self contained unit.
- Access controls on one machine preserve the confidentiality of data on that processor
- An attack can come from any host to any host, so that a large network offers many points of vulnerability.

3] Sharing

- Because network enables resource & workload sharing, more user have potential to access networked system than on single computer.

4] Complexity of system

- An OS is a complicated piece of software.
- Large, complex system increase probability of flaws & unintented access points.

3) Give impacts of installing unauthorized software / hardware.

Ans

1] Unauthorized s/w increases the risk of outsiders gaining access to sensitive data.

2] Without having knowledge of agency s/w, IT managers cannot fully protect their data & information.

3] This creates a backdoor into network and an enviroment all other security mechanism.

4] User account always be sure where the s/w originally came from & what may be hidden inside.

Que 3

1) List any 3 kinds of damage a company could suffer when the integrity of program or company data is comprised.

Ans

a) Can damage their public image :-

→

1. The possibility of crime is bad enough.
2. But worse yet, in the event of a crime, some organization neither investigate nor prosecute for fear that the revelation will damage their public image.

b) Serious damage to hardware involve :-
→

1. Hardware is more visible than s/w, largely because it is composed of physical objects.
2. Because we can see what devices are hooked to the system, it is rather simple to attack by adding devices, changing them, removing them intercepting traffic to them or flooding them with traffic until they can no longer function.

c) Data modification / interception :-
→

1. S/w can be replaced or changed or destroyed maliciously or it can be modified, deleted or misplaced accidently.
2. Sometimes, the attacks are serious as when the s/w no longer run.

2) List feature of Window NT domain.

Ans

1. With multi-boot capability, windows NT can co-exist with other OS.

2. It implements pre-emptive multi tasking & multi threading operations.

3. It supports multiple CPU systems with SMP (Symmetric multiprocessing technology).

4. It spf supports a variety of hardware platforms such CISI and RISC.

5. Its security meets the US department of Defense's C2 standards.

6. The NT system is a popular network OS because of its low price, strong application service capability, high performance and rich s/w.

7. The disadvantage is that the file service funct^n is not as powerful Netware, which occupies more service resources.

5) Describe IDS with its types.

Ans

1] IDS (Intrusion Detection System) is a device, typically another seperate computer, the monitors activity to identify malicious or suspicious events.

2] An IDS is a sensor like smoke detector, that raise alarm if specific things occur

3] Variety of functions :-

(a) monitoring users and system activity
(b) auditing system configuration for vulnerabilities & mis configuration.

(c) Correct system configuration error
(d) recognizing know.

Types of IDS:

1] Signature - Based IDS

→

A simple signature for a know attack type might describe a series of TCP SYN packets sent to many different ports in succession & at time close to on another as would be the case for port scan.

2] Heuristic IDS

→

The original work in this area focused on individual trying to find characteristics of that person that might be helpful in understanding normal & abnormal behaviour.

Que 4

1) What is Dumpster Diving & How to protect against dumpster diving?

Ans

Dumpster diving is looking for treasure in someone's else trash. Dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network.

DATE: / /

PAGE:

Solution against dumpster diving :

1) Company should establish policy where all paper including print-out are shredded in a cross cut shredder before being recycled.

2) All storage media are erased.

3) All staff are educated about the danger of untracked trash.

2) Describe different terms used for good network design

Ans

Application :-

1) A good place to start with a network design is to list and understand the application that will run on the network

2) Most network have both common application and department and user-specific application.

Users :-

1) Estimating total user will likely be easier because the company should already have a business plan for from which you can derive these estimates.

DATE: / /

PAGE:

Network Services :-

1) Network services can vary widely in different companies.

2) A very basic network might need only file and print services, plus perhaps Internet connectivity.

Security and safety

1) Security and safety concern the companys need to keep information on secure both inside and outside an organization and to keep the company's data safe from loss.

3) Describe the role of people in security

Ans :

1] Set & implement user access controls & identify and access management systems.

2] Moniter network & application performance to identify and irregular activity.

3] Perform regular audits to ensure security practices are compliant.

4] Deploy endpoint detection & prevention tools the thwart malicious hacks.

5] Set up patch management system to update application automatically.

6] Implement comprehensive vulnerability management systems across all assets on premises an in the cloud.

Que 5

i] (1) How packet filtering firewall is different from application proxy firewall?

Ans

1) Packet filtering firewall looks only at headers of packet not at data inside the packet.

2) Therefore, a packet filter would pass anything to port 25 assuming its screening rules allow inbound connections to that port.

3) But application are complex & sometimes contain errors.

4) Worse, appⁿ often act on behalf of all users, so they require privileges all users.

5) A flawed appⁿ running with all users privileges can cause much damage.

i) (ii) Why guard firewall is mostly used in universities ? Give reason.

Ans

1) A guard is sophisticated firewall

2) Like a proxy firewall, it receives protocols data unit interprets them, & passes through same or different protocol data unit that achieve either the same result or modified result.

3) The guard decides what services to perform on users behalf in accordance with its available knowledge.

4) The degree of control a guard can provide its limited only by what is computable.

ii) Give steps for creating user account in windows 2003 server & which options required for deleting user account.

Ans

1) Click start button, the Run

2) The type "lusrmgs.msc" without quotes

3) In the window that open right click in right pannel & click new user.

4) In new user dialog type your preference for new user name & password. Uncheck user must change password. & check password never expires.

5) Now click create, & the click close.

For deleting.

1) Disable a user ad account immediately.

2) Set a user account to disable at end of specified date.

Qu 6

1) Illustration Active Directory services in brief.

Ans

1) A microsoft active directory in simple terms, is like a giant telephone book. that organized within it all of the computers & people that have been entered into it.

2) Administrator use an active directory to apply policies to object put people into security group & to better keep track of things in group.

Features :-

1] Security
→ Having only one domain means better security through a single policy & single set of administration.

2] Single platform
→ A single platform service means form for all other directory were service including monitoring and messaging.

3] Single group policy container (SGPC)
→ With a SGPC management policy need to be defined only once and can be used throughout the entire enterprise without need to manually export & import GPOs

4] Backup & recovery
→ Having only a single domain means better resiliency because every location has a fully backup.

2) Write the steps required for the installation of a Network printer in windows 2003 server environment. Also give steps test this installation from another PC.

Ans

1) Go to start and select printer & faxes.

2) Click on add printer.

3) A dialog box opens click next on it.

4) Click on the radio button named as 'local printer attached to this computer'

5) Click next

6) In next dialog box choose 'create a new port' select type 'standard TCP/IP port' click next.

7) Again click next

8) Again a new dialog box appear in that enter the printer name or IP address and click next.

9) Choose device type standard and the click next.

10) Now finish the process by clicking on Finish button.

11) Now select your printer from the list ~~again~~ given on screen if not then click on 'Windows updates' rather click next.

DATE: / /

PAGE:

12) Again click next enter printer name in next dialog box.

13) Click next until it gets finished.