C++ DYNAMIC ALLOCATED ARRAY

#include<iostream>

using namespace std;

int main() {

int x, n;

cout << "Enter the number of items:" << "\n";

cin >>n;

int \*arr = new int(n);

cout << "Enter " << n << " items" << endl;

for (x = 0; x < n; x++) {

cin >> arr[x];

}

cout << "You entered: ";

for (x = 0; x < n; x++) {

cout << arr[x] << " ";

}

return 0;

}

**Why would you want to use SSH from a Windows PC?**

SSH (TCP port 22) is a secure connection used on many different systems and dedicated appliances. Routers, switches, SFTP servers and unsecure programs being tunneled through this port all can be used to help harden a connection against eavesdropping. Despite the fact that most times when you hear about somebody “SSHing” into a box it involves Linux, the SSH protocol itself is actually implemented on a wide variety of systems — though not by default on most Windows systems. Programs like PuTTY, Filezilla and others have Windows ports available, which allow Windows users the same ease-of-use connectivity to these devices as do Linux users.

**what’s the difference between symmetric and asymmetric encryption?**

symmetric encryption uses the same key to encrypt and decrypt, while asymmetric uses different keys for encryption and decryption.

**DATA LEAKAGE :**The separation or departing of IP from its intended place of storage is known as data leakage. The factors that are responsible for data leakage can be

Copy of the IP to a less secure system or their personal computer

Human error

Technology mishaps

System misconfiguration

A system breach from a hacker

A home-grown application developed to interface to the public

Inadequate security control for shared documents or drives

Corrupt hard-drive

Back up are stored in an insecure place

**List out the steps to successful data loss prevention controls?**

Create an information risk profile

Create an impact severity and response chart

Based on severity and channel determine incident response

Create an incident workflow diagram

Assign roles and responsibilities to the technical administrator, incident analyst, auditor and forensic investigator

Develop the technical framework

Expand the coverage of DLP controls

Append the DLP controls into the rest of the organization

Monitor the results of risk reduction

Free online ctf – subject areas , open source intelligence resource

Hak the box

Security tube

Podcasts- pauls security weekly , darknet diaries

Vulnerable virtual machine

Aws container security , ec2 s3buckets

Books to possiblyt reead – the alchemist palo quelo , character and leadership development

Brandon sarah – infosec

Interview 2 corporate apps:

Ashleigh – managment

Phillip – tech – apache camel framework (components), red hat fuse osdi app , looking to convert to spring boot / get out of fuse. Kafkfa event streaming. Openshift , maben – build tool. Intelijay , eclipse , springboot.