

Lab-11

D.Lalitha
18bcn7025

Lab experiment – Creating secure and safe executable

1) C++ Code & building the Executable

```
#include <iostream>

int main(void)
{
    int authentication = 0;
    char cUsername[10];
    char cPassword[10];

    std::cout << "Username: ";
    std::cin >> cUsername;

    std::cout << "Pass: ";
    std::cin >> cPassword;

    if (std::strcmp(cUsername, "admin") == 0 &&
std::strcmp(cPassword, "adminpass") == 0)
    {
        authentication = 1;
    }
    if (authentication)
    {
        std::cout << "Access granted\n";
        std::cout << (char)authentication;
    }
    else
    {
        std::cout << "Wrong username and password\n";
    }

    return (0);
}
```

}

```
#include <iostream>

int main(void)
{
    int authentication = 0;
    char cUsername[10];
    char cPassword[10];
    std::cout << "Username: ";
    std::cin >> cUsername;
    std::cout << "Pass: ";
    std::cin >> cPassword;
    if (std::strcmp(cUsername, "admin") == 0 &&
        std::strcmp(cPassword, "adminpass") == 0)
    {
        authentication = 1;
    }
    if (authentication)
    {
        std::cout << "Access granted\n";
    }
    else
    {
        std::cout << "Access denied\n";
    }
}
```

Microsoft Visual Studio Debug Console

```
Username: admin
Pass: adminpass
Access granted
```

2) Verifying the DEP & ASLR status in Process Explorer

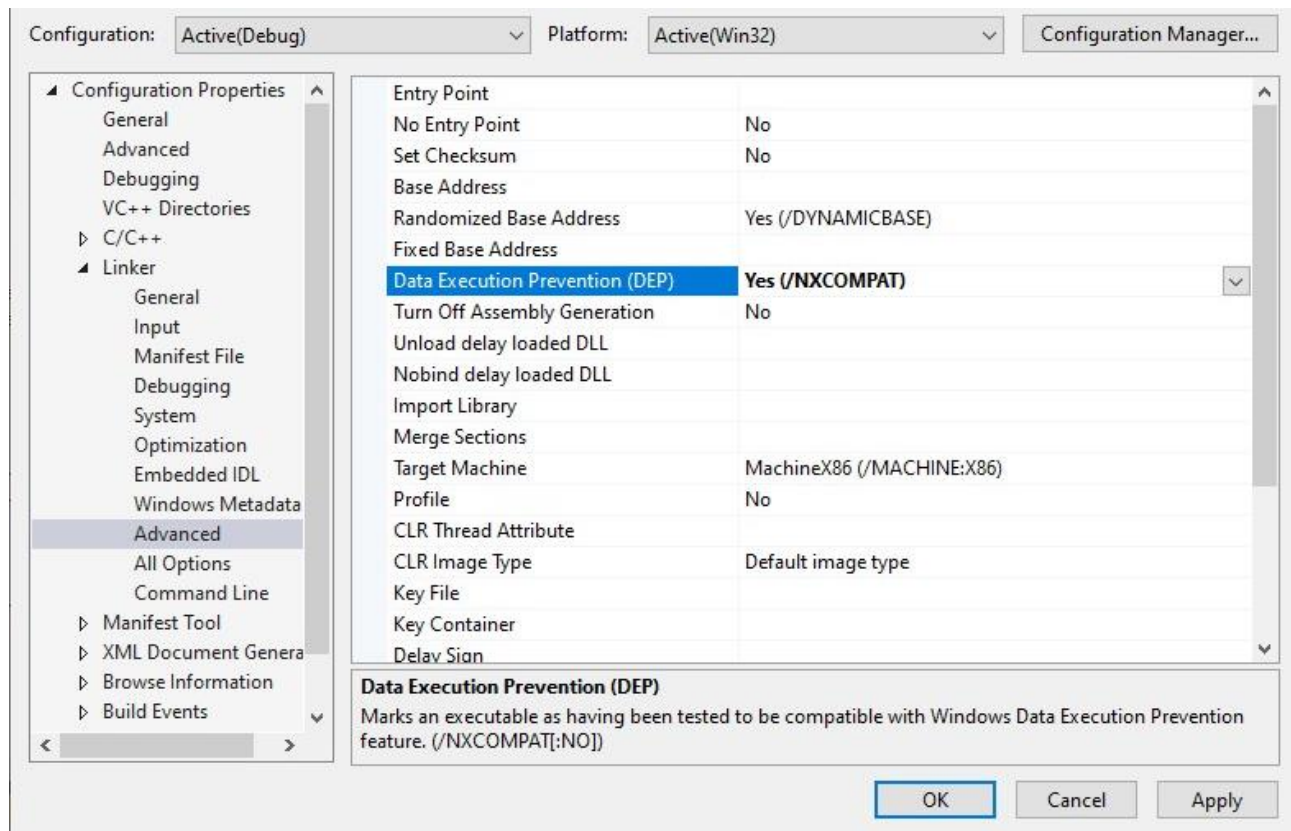
Microsoft Visual Studio Debug Console

```
Username: admin
Pass: adminpass
Access granted
```

vcpgkgsrv.exe	< 0.01	43,024 K	19,028 K	9988	Microsoft (R) Visual ...	Microsoft Corporation
MSBuild.exe		28,612 K	43,636 K	13444	MSBuild.exe	Microsoft Corporation
conhost.exe		6,492 K	11,060 K	20152	Console Window Host	Microsoft Corporation
VsDebugConsole.exe		1,236 K	6,136 K	5968	Visual Studio Debug...	Microsoft Corporation
conhost.exe		7,188 K	16,284 K	5072	Console Window Host	Microsoft Corporation
18BCN7130_secu...		780 K	4,496 K	19128		
msedge.exe	< 0.01	44,000 K	86,880 K	16884	Microsoft Edge	Microsoft Corporation
msedge.exe		6,504 K	7,484 K	17008	Microsoft Edge	Microsoft Corporation

You can see DEP disabled & No ASLR.

3) Rebuilding the same executable After enabling DEP & ASLR



As you can see, I have enabled DEP, ASLR, SEH above.

I have Rebuilt my project and run the same and we can verify the status of DEP, ASLR, SEH.

4) Verifying the DEP & ASLR status in Process Explorer after enabling

```
#include <iostream>

int main(void)
{
    int authentication = 0;
    char cUsername[10];
    char cPassword[10];
    std::cout << "Username: ";
    std::cin >> cUsername;
    std::cout << "Pass: ";
    std::cin >> cPassword;
    if (std::strcmp(cUsername, "admin") == 0 &&
        std::strcmp(cPassword, "adminpass") == 0)
    {
        authentication = 1;
    }
    if (authentication)
    {
        std::cout << "Access granted\n";
        std::cout << (char)authentication;
    }
    else
    {
    }
}
```