

# Lab-11

P.N.Ruthvika

18bce7340

## **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

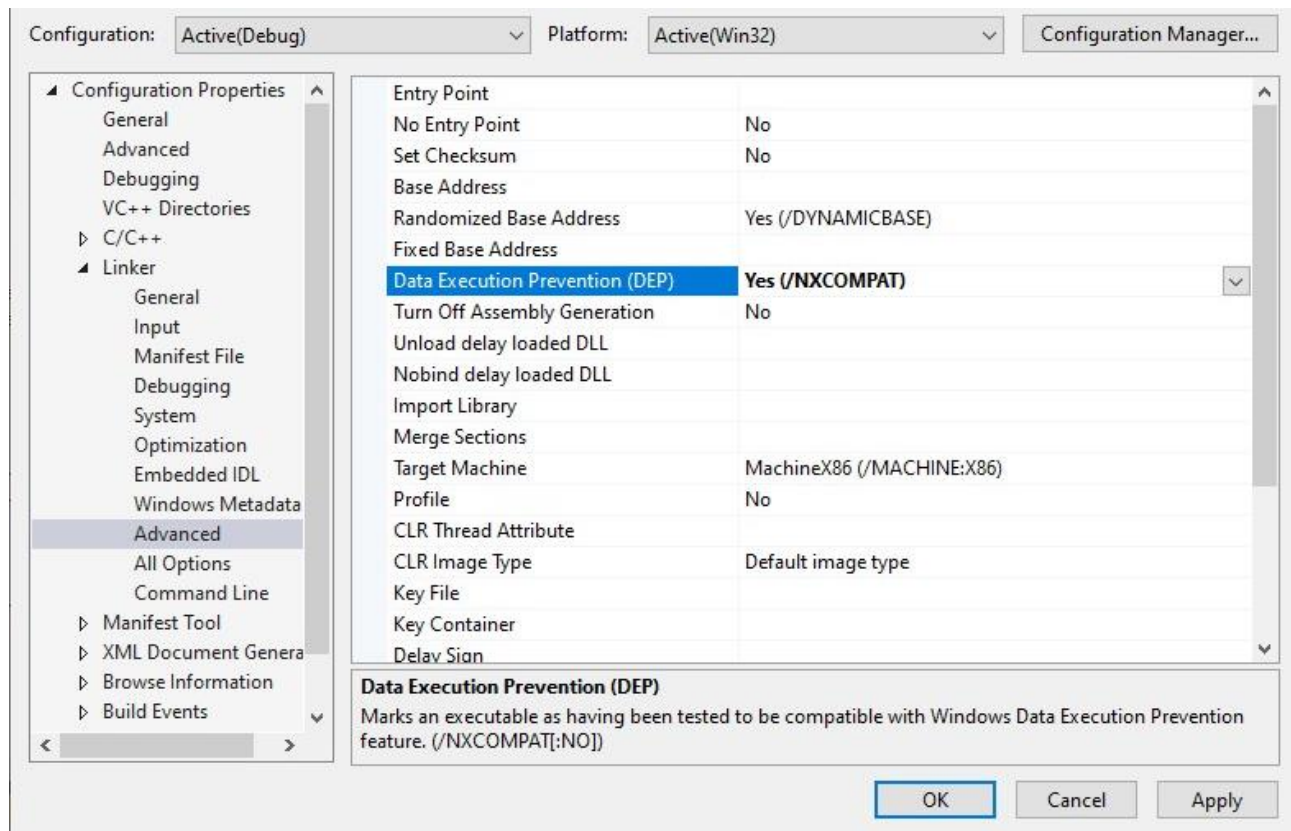
Microsoft Visual Studio Debug Console

```
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



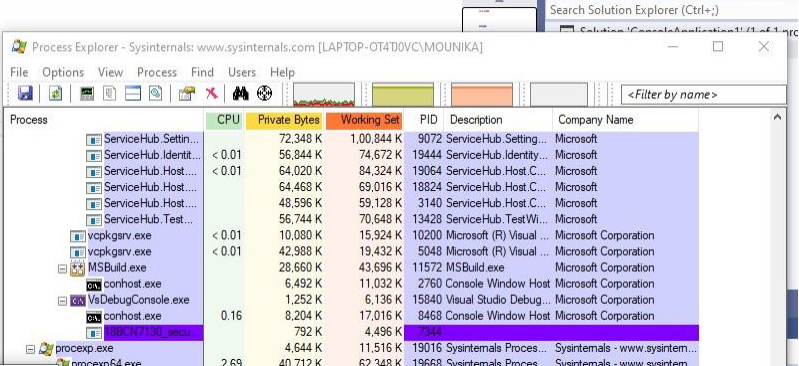
As you can see, I have enabled DEP, ASLR, SEH above.

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
    {
    }
}
```



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
ServiceHub.Setting...	72.348 K	1,00,844 K	9072	9072	ServiceHub.Setting...	Microsoft
ServiceHub.Identity...	< 0.01	56,844 K	74,672 K	19444	ServiceHub.Identity...	Microsoft
ServiceHub.Host...	< 0.01	64,020 K	84,324 K	19064	ServiceHub.Host...	Microsoft
ServiceHub.Host...		64,468 K	69,016 K	18824	ServiceHub.Host...	Microsoft
ServiceHub.Host...		48,596 K	59,128 K	3140	ServiceHub.Host...	Microsoft
ServiceHub.TestWi...		56,744 K	70,648 K	13428	ServiceHub.TestWi...	Microsoft
vcpkg.exe	< 0.01	10,080 K	15,924 K	10200	Microsoft (R) Visual ...	Microsoft Corporation
vcpkg.exe	< 0.01	42,988 K	19,432 K	5048	Microsoft (R) Visual ...	Microsoft Corporation
MSBuild.exe		28,660 K	43,696 K	11572	MSBuild.exe	Microsoft Corporation
conhost.exe		6,492 K	11,032 K	2760	Console Window Host	Microsoft Corporation
VisualStudioDebug.exe		1,252 K	6,136 K	15840	Visual Studio Debug...	Microsoft Corporation
conhost.exe	0.16	8,204 K	17,016 K	8468	Console Window Host	Microsoft Corporation
process explorer		792 K	4,496 K	7544		
process explorer		4,644 K	11,516 K	19016	Sysinternals Proces...	Sysinternals - www.sysintem...
process explorer	7.69	40,712 K	62,348 K	19668	Sysinternals Proces...	Sysinternals - www.sysintem...