

Forum:[Hack Forums](#)

Thread: [very simple security Console | C++](#)

Kali Shadow - June 25, 2018, 4:03 pm

Hello HF community .. I'm Sharing with you my very simple security console source code .

the idea is the console starts up when windows starts

[put the console in startup folder manually]

Once started it will kill explorer.exe process.

the PC will look like nothing but black screen with the console on it [desktop background may appear sometimes too]

it will ask you to Enter you password , And if it was correct it will start explorer.exe else will shut down the PC.

hope u like the idea.

I'd love to hear ur feedback about this .

```
Code #include<iostream>
#include<stdlib.h>
#include<fstream>
#include<string>
```

```
using namespace std;
```

```
static string password;
ofstream savaData;
ifstream getData;
string userPass;
void line();void header();void taskKiller();void taskStarter();
void passwordSetter(string);bool passwordChecker(string);
void dash();bool passStatus();
```

```
//Section of Main //
```

```
void main (){
    header();
    if(passStatus()){
        cout<<"\tEnter The Password inorder to Gain Access To the system : \n\t";
        cin >> userPass;
        if (passwordChecker(userPass)){
            cout<<"\tPassword Matched successfully !\n\t";
            taskStarter();
        }else{
            system("color 0c");
            cout<<"\n\tWrong Information , Security Console Will now shutdown your system...";
            system("shutdown /s -t 05 /f");
        }
    }else{
        cout<<"\tPassword Has not been set yet , Set your New Password Here : \n\t";
        cin >> userPass;
        passwordSetter(userPass);
    }
}
```

```

        taskStarter();
    }
    system("pause");
}
//<header Functions>..

```

```

void dash(char x){
cout<<"\n\t#";
    for(int i=0;i<=62;i++)
        cout<<x;
    cout<<"#";
}

```

```

void line(){
for(int i=0;i<=20;i++)
    cout<<"#";
}

```

```

void header(){
    taskKiller();
    system("title Security Console");
    system("color 0a");
    cout<<"\t \n"<<endl;
    system("cls");
    cout<<"\t";
    line();
    cout<<" Security Console 18.1 ";
    line();
    dash(' ');
    cout<<"\n\t#\t Written By : #Kali #### Shadow |HFC| # First Version \t#";
    dash(' ');
    dash('#');
    cout<<endl<<endl;
}

```

```

//</header Functions>..

```

```

void passwordSetter(string pass){
    savaData.open("setting.dat");
    savaData << pass;
    savaData.close();
}

```

```

bool passStatus()
{ bool res = false;
    getData.open("setting.dat");
    getData >> password;
    getData.close();
    if (password.compare("") == 0){
        res = false;
    }else{
        res = true;
    }
}

```

```

    return res;
}

bool passwordChecker(string x){
    bool res = false;
    if (password.compare(x) == 0){
        res = true;
    }else{
        res = false;
    }
    return res;
}

void taskKiller()
{
    system("taskkill /IM explorer.exe /f");
}

void taskStarter()
{
    system("start explorer.exe");
}

```

aeiro - June 25, 2018, 5:08 pm

(Jun 25, 2018 04:03 PM)Kali_Shadow Wrote: [\[CITE\]](#) Hello HF community .. I'm Sharing with you my very simple

security console source code .

the idea is the console starts up when windows starts

[put the console in startup folder manually]

Once started it will kill explorer.exe process.

the PC will look like nothing but black screen with the console on it [desktop background may appear sometimes too]

it will ask you to Enter you password , And if it was correct it will start explorer.exe else will shut down the PC.

hope u like the idea.

I'd love to hear ur feedback about this .

```

Code #include<iostream>
#include<stdlib.h>
#include<fstream>
#include<string>

```

```

using namespace std;

```

```

static string password;
ofstream savaData;
ifstream getData;
string userPass;
void line();void header();void taskKiller();void taskStarter();
void passwordSetter(string);bool passwordChecker(string);
void dash();bool passStatus();

```

```

//Section of Main //

```

```

void main (){
    header();
    if(passStatus()){
        cout<<"\tEnter The Password inorder to Gain Access To the system : \n\t";
        cin >> userPass;
        if (passwordChecker(userPass)){
            cout<<"\tPassword Matched successfully !\n\t";
            taskStarter();
        }else{
            system("color 0c");
            cout<<"\n\tWrong Information , Security Console Will now shutdown your system...";
            system("shutdown /s -t 05 /f");
        }
    }else{
        cout<<"\tPassword Has not been set yet , Set your New Password Here :\n\t";
        cin >> userPass;
        passwordSetter(userPass);
        taskStarter();
    }
    system("pause");
}
//<header Functions>..

```

```

void dash(char x){
    cout<<"\n\t#";
    for(int i=0;i<=62;i++)
        cout<<x;
    cout<<"#";
}

```

```

void line(){
    for(int i=0;i<=20;i++)
        cout<<"#";
}

```

```

void header(){
    taskKiller();
    system("title Security Console");
    system("color 0a");
    cout<<"\t \n"<<endl;
    system("cls");
    cout<<"\t";
    line();
    cout<<" Security Console 18.1 ";
    line();
    dash(' ');
    cout<<"\n\t#\t Written By : #Kali #### Shadow |HFC| # First Version \t#";
    dash(' ');
    dash('#');
    cout<<endl<<endl;
}

```

```

//</header Functions>..

```

```
void passwordSetter(string pass){
    savaData.open("setting.dat");
    savaData << pass;
    savaData.close();
}
```

```
bool passStatus()
{ bool res = false;
  getData.open("setting.dat");
  getData >> password;
  getData.close();
  if (password.compare("") == 0){
    res = false;
  }else{
    res = true;
  }
  return res;
}
```

```
bool passwordChecker(string x){
    bool res = false;
    if (password.compare(x) == 0){
        res = true;
    }else{
        res = false;
    }
    return res;
}
```

```
void taskKiller()
{
    system("taskkill /IM explorer.exe /f");
}
```

```
void taskStarter()
{
    system("start explorer.exe");
}
```

you should never use system() function. try another method.

Kali_Shadow - June 25, 2018, 5:11 pm

(Jun 25, 2018 05:08 PM)aeiro Wrote: [\[CITE\]](#) you should never use system() function. try another method.

Hey aeiro thanks for ur advice , may I know why ?
and if you know another function to replace I would like to know .

aeiro - June 25, 2018, 5:15 pm

(Jun 25, 2018 05:11 PM)Kali_Shadow Wrote: [\[CITE\]](#) Hey aeiro thanks for ur advice , may I know why ?

and if you know another function to replace I would like to know .
i've always thought that it'd be easy to hook. but if you google it you may find different results but theyre always negative.

Its also not about a single function. Look into terminating an application from another.

ps.. sorry for all the edits. trying to play WWII

.Grim - June 26, 2018, 8:20 am

interesting, thanks for the source.

hunter24957 - June 26, 2018, 11:04 am

An abstract idea, however, it's flawed.

I can simply start Task Manager with the keyboard shortcut and then run explorer.exe from there, thus eliminating any protection this has.

Also why would a user need this? Windows provides the ability to add a password to an account, what makes this a better alternative?

My suggestion is don't limit yourself to user-mode non-administrative programs, If you want to provide security for a user (like an anti-virus for instance) you should look into elevated processes, this will give your program more control over the system thus granting you the ability to do more then simply killing a process, such as loading a kernel driver. A kernel driver will grant you more or less full control over a system, this is what most modern-day anti-viruses use, from there to possibilities are endless. Just a suggestion, what you have here is good but just not secure enough to be considered a security based program. Good luck! ?

Kali_Shadow - June 26, 2018, 11:25 am

(Jun 26, 2018 11:04 AM)hunter24957 Wrote: [\[CITE\]](#) An abstract idea, however, it's flawed.

I can simply start Task Manager with the keyboard shortcut and then run explorer.exe from there, thus eliminating any protection this has.

Also why would a user need this? Windows provides the ability to add a password to an account, what makes this a better alternative?

My suggestion is don't limit yourself to user-mode non-administrative programs, If you want to provide security for a user (like an anti-virus for instance) you should look into elevated processes, this will give your program more control over the system thus granting you the ability to do more then simply killing a process, such as loading a kernel driver. A kernel driver will grant you more or less full control over a system, this is what most modern-day anti-viruses use, from there to possibilities are endless. Just a suggestion, what you have here is good but just not secure enough to be considered a security based program. Good luck! ?thanks a lot for your feedback bro , that meant a lot to me

hunter24957 - June 26, 2018, 11:36 am

(Jun 26, 2018 11:25 AM)Kali_Shadow Wrote: [\[CITE\]](#) thanks a lot for your feedback bro , that meant a lot to me

No problem man, C++ is a great language to use for this stuff, keep at it! ?

stdio - June 28, 2018, 1:47 am

I could just enter few hundred characters for buffer overflow causing your program to shutdown and give me access to explorer.exe ;)

Kali_Shadow - June 28, 2018, 6:29 am

(Jun 28, 2018 01:47 AM)Homi Wrote: [\[CITE\]](#) I could just enter few hundred characters for buffer

overflow causing your program to shutdown and give me access to explorer.exe ;) that will cause the program to shutdown without running the line where explorer.exe start .. you will have a blank screen , And you would have to restart ur pc

but the hole of Ctrl + alt + Del is true problem..

aeiro - June 28, 2018, 11:59 am

(Jun 28, 2018 06:29 AM)Kali_Shadow Wrote: [\[CITE\]](#) that will cause the program to shutdown without running the line where explorer.exe start .. you will have a blank screen , And you would have to restart ur pc

but the hole of Ctrl + alt + Del is true problem..

how is this a problem?

Hook into the keyboard and catch this combination and all other possible shortcuts.

stdio - June 28, 2018, 12:00 pm

(Jun 28, 2018 06:29 AM)Kali_Shadow Wrote: [\[CITE\]](#) that will cause the program to shutdown without running the line where explorer.exe start .. you will have a blank screen , And you would have to restart ur pc

but the hole of Ctrl + alt + Del is true problem..

you can always start explorer.exe, what is stopping after app is closed?

aeiro - June 28, 2018, 12:03 pm

(Jun 28, 2018 12:00 PM)Homi Wrote: [\[CITE\]](#) you can always start explorer.exe, what is stopping after app is closed?

isnt there a warning saying something about explorer.exe has stopped. restart the process?

hunter24957 - June 28, 2018, 12:17 pm

(Jun 28, 2018 11:59 AM)aeiro Wrote: [\[CITE\]](#) how is this a problem?

Hook into the keyboard and catch this combination and all other possible shortcuts.

If you don't mind me asking, how would he achieve this?

From the way I see it, Ctrl+Alt+Del generates a Window's interrupt, it's handled by the CPU on Kernel level.

How would a simple User-mode non-privileged program stop this from happening?

aeiro - June 28, 2018, 12:34 pm

(Jun 28, 2018 12:17 PM)hunter24957 Wrote: [\[CITE\]](#) If you don't mind me asking, how would he achieve this?

From the way I see it, Ctrl+Alt+Del generates a Window's interrupt, it's handled by the CPU on Kernel level.

How would a simple User-mode non-privileged program stop this from happening?

Didn't think about that one.Yeah now we're damn near talking about driver dev here.

constptr - June 29, 2018, 12:57 pm

(Jun 26, 2018 11:36 AM)hunter24957 Wrote: [\[CITE\]](#) No problem man, C++ is a great language to use for this stuff, keep at it! ?

I'm sorry but how is c++ used here?

C/asm yeah sure

But I don't see any use of STL, lambdas.. Etc in malware development

0xDEAD10CC - June 29, 2018, 4:56 pm

(Jun 29, 2018 12:57 PM)constptr Wrote: [\[CITE\]](#) I'm sorry but how is c++ used here?

C/asm yeah sure

But I don't see any use of STL, lambdas.. Etc in malware development

You don't see any use of the STL or C++ lol... Maybe you just don't know what the STL is or can't read? Maybe for the low level stuff too if you're speaking in general, C or ASM because it's closer to machine level and allows you to have an easier time with injection (smaller codesize, etc...), but after that, what is stopping someone from using C++? Also, if you've ever tried to compare C to C++ you would see that C++ can add a slight layer of obfuscation to reverse engineering attempts. Also - who said a "security console" was malware? You've only just assumed that the single and only topic here was malware.

hunter24957 - June 29, 2018, 6:27 pm

(Jun 29, 2018 12:57 PM)constptr Wrote: [\[CITE\]](#) I'm sorry but how is c++ used here?

C/asm yeah sure

But I don't see any use of STL, lambdas.. Etc in malware development

Really? I find myself using C++ quite a bit for security based projects since I like my code object orientated, although I do find that sometimes I may as well be programming in C since I'm not taking full advantage of the Visual C++ compiler, so I can see your point. In some ways it's all about preference, any language can be used for malware development, it just needs to be used in the right way. Hell, I know people who are using .NET to develop hacks, it can be done, the question is do you have the right knowledge to do so? ?

sqsgkrldwg - June 30, 2018, 12:29 am

(Jun 28, 2018 12:34 PM)aeiro Wrote: [\[CITE\]](#) Didn't think about that one.Yeah now we're damn near talking about driver dev here.

No.

He's talking about pure logic.

If you set up this kind of protection it means you are protecting against someone that may have physical access to your computer.

So there is million ways to bypass your program ...

Kali_Shadow - July 2, 2018, 5:55 am

(Jun 30, 2018 12:29 AM)sqsgkrldwg Wrote: [\[CITE\]](#) No.

He's talking about pure logic.

If you set up this kind of protection it means you are protecting against someone that may have physical access to your computer.

So there is million ways to bypass your program ...

Yes , Exactly this was I meant .. But its not perfect at all , Shared it for new Ideas and modifications

.