

[TOOL] DetectCon Detects Hidden Ports

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-07/0008.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/06/05

To: list@securiteam.com

Date: 6 Jul 2005 13:59:22 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

DetectCon Detects Hidden Ports

SUMMARY

DETAILS

This is a little program is able to detect if a rootkit is hiding a certian port from being detected as a port that listens on connection. The program will only work when the rootkit uses a port based listening backdoor.

Tool source:

/*

+++++

+This is a little Disclaimer for if you havn't read the one on our site.

+

+The tools and tutorials KD-Team develops and publishes are only ment for

+

+educational purpose only.WE DO NOT encourage the use of this tools and

+

+tutorials for mailicious purpose.We learned a lot during the development of them +

+so we hope you also learn and don't just use it without any brains. +

+We take completly NO responsability for any damage caused by them nor

+

Securiteam: [TOOL] DetectCon Detects Hidden Ports

```
+are we or our isp responsible for what you do with them. +
+Greetz: KD-Team +
+http://www.kd-team.com +
+++++
*/
#include <windows.h>
#include <stdio.h>
#include <Iphlpapi.h>
#include <winsock2.h>

void BindPort();

void main(int argc,char *argv[])
{
if(argc > 1)
{
printf("\t\tDetect Hidden Connections\n");
printf("\t\tWritten By: Kd-Team\n");
printf("\t\tThis is just a POC to show\n");
printf("\t\tHowto detect hidden tcp ports\n");
printf("\t\tUsually rootkits hide them\n");
printf("\t\tThis DOES NOT WORK WHEN:\n");
printf("\t\t\"setsockopt(SO_REUSEADDR)\" is set\n");
printf("\t\tRead readme.txt for more info\n");
printf("\t\tUsage: %s\n",argv[0]);
printf("\t\tWhen this output's ports that netstat doesn't\n");
printf("\t\tthat would theoretically be a indication\n");
printf("\t\tthat the port is hidden\n");
}
else
{
BindPort();
}
}
void BindPort()
{
WSADATA wsa;
SOCKET hLstnSock;
struct sockaddr_in ServAddr;

if(WSAStartup(MAKEWORD(2,0),&wsa) != 0)
{
printf("WSAStartup() failed\n");
}

memset(&ServAddr,0,sizeof(ServAddr));
ServAddr.sin_family = AF_INET;
ServAddr.sin_addr.s_addr = htonl(INADDR_ANY);

for(int i=0;i<65536;i+)
{
```

Securiteam: [TOOL] DetectCon Detects Hidden Ports

```
ServAddr.sin_port = htons(i);

hLstnSock = WSASocket(AF_INET, SOCK_STREAM, IPPROTO_TCP,0,0,0);
if(hLstnSock == SOCKET_ERROR)
{
    printf("socket() %d failed\n",WSAGetLastError());
    WSACleanup();
}

if(bind(hLstnSock,(struct sockaddr *)&ServAddr,sizeof(ServAddr)) < 0)
{
    printf("port: %i bind() %d failed\n",i,WSAGetLastError());
    closesocket(hLstnSock);
}
else
{
    //printf("port %i succeeded\n",i); just uncomment this if you wanna
    know on what ports the bind succeeded.
    closesocket(hLstnSock);
}
}

WSACleanup();
}
```

ADDITIONAL INFORMATION

The information has been provided by kd team.
To keep updated with the tool visit the project's homepage at:
<<http://www.kd-team.com/>> <http://www.kd-team.com/>

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.