



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

NetBus

Chris A. Hayden

December 17, 2000

Introduction

NetBus is a “Trojan Horse” that is similar to another well known program Back Orifice. It is promoted as a remote administration tool by its author Carl-Fredrik Neikter however there have been special hacking versions of “NetBus 2.0” developed by various individuals. The first official version was published in March 1998 and since many versions have been written including versions 1.60, 1.70, and 2.xPro which are discussed in this paper.

NetBus utilizes a client-server architecture in which the server program is installed on the target machine(s) and a client piece is used to connect to these servers. The intent of this paper is to provide methods for detecting and preventing infection by these server programs.

Overview

NetBus is a remote control utility for Windows 9x and Windows NT. Some of the most important features are as follows:

Version 1.6

- Start optional application – start any application on the server
- Get a screendump
- Download and deletion of any file from the target
- Open/close the CD-ROM once or in intervals
- Go to an optional URL within the default web-browser
- Send keystrokes to the active application on the target computer
- Listen for keystrokes and send them back to the client
- Show, kill, and focus windows on the system
- Record sounds that the microphone catch

Version 1.7

- All features from version 1.6
- Ultra-fast Port scanner
- Port Redirect – redirects data to another host and port
- Server setup – configures the server-exe with some options, like TCP-port and mail notification
- Application Redirect – redirects I/O from console applications to a specified TCP-port

Version 2.x

- All features of previous versions
- Complete rewrite of software with more robust and efficient algorithms and a newer more professional looking GUI (Version 2 is promoted as commercial software)
- Registry manager - list keys, fields and values, create keys and delete keys, change values among others
- Telnet support
- Window manager – full control over all windows
- Plugin manager – run Plugins that extend the capabilities of NetBus
- File manager – explorer, upload and download files, delete files and folders, create folders and share folders
- Host scheduler, predefine time to run scripts at hosts
- Command broadcaster, broadcasts commands to multiple hosts

In versions 1.6 and 1.7 the NetBus server defaults to ports TCP/UDP 12345 and 12346. This is configurable in version 1.7 and above. In version 2.x this has been changed to TCP/UDP 20034. Once a system has been infected the server program opens up the default/configured port for communications and waits for a connection from a client.

Installation

NetBus can be configured to run “visibly” or “invisibly” on the system running the server. When configured “invisibly” the server program attempts to hide itself from the Windows 9x task list.

In version 1.6 and 1.7 of the software the installation is accomplished by simply running the executable on the target machine. The executable can be named anything however it is normally named Sysedit.exe or patch.exe. The default installation causes the server to be installed in the \windows directory and started at windows startup. The automatic startup is accomplished through a registry key, for example, on a computer running Windows 95 I installed the version 1.7 executable named patch.exe and it created the following registry key:

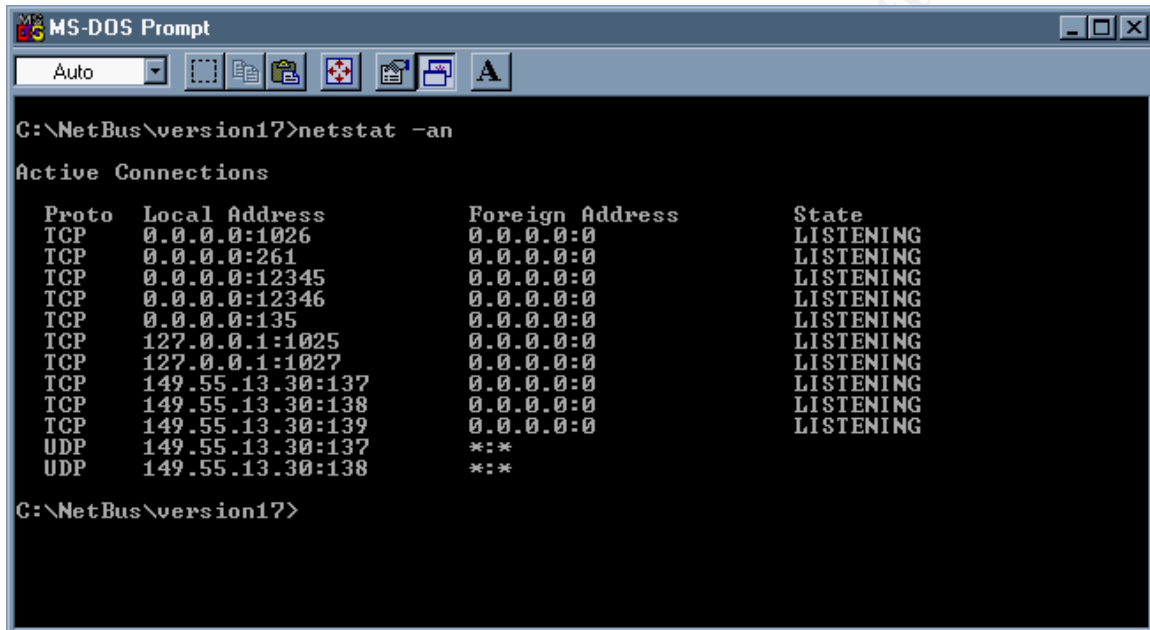
```
\\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\  
"PATCH"="C:\\WINDOWS\\PATCH.EXE /nomsg"
```

If this key is removed the server will not start at Windows startup. The server may also be removed by running the executable with the /remove option. This will delete the registry key as well.

Since version 2.x is promoted as a commercial version of NetBus, it comes with an “Installation Wizard”. The default installs the server to run in “visible” mode and manual startup mode however it may be configured to start automatically and to hide itself from the task list.

Detection

NetBus may be detected by good antiviral software with current updates however this may be changing, "Both Symantec and Panda Software have given in to pressure and have removed Netbus Pro from their respective Anti-Virus products." Since antiviral software is only as good as its database, it is a good idea for one to familiarize oneself with the services that typically run on the system in question. If one knows which ports are typically open on a particular system the netstat command can be used to determine if any suspect ports are opened on that system.



```
MS-DOS Prompt
Auto
C:\NetBus\version17>netstat -an

Active Connections

Proto  Local Address           Foreign Address         State
TCP    0.0.0.0:1026             0.0.0.0:0               LISTENING
TCP    0.0.0.0:261             0.0.0.0:0               LISTENING
TCP    0.0.0.0:12345           0.0.0.0:0               LISTENING
TCP    0.0.0.0:12346           0.0.0.0:0               LISTENING
TCP    0.0.0.0:135             0.0.0.0:0               LISTENING
TCP    127.0.0.1:1025          0.0.0.0:0               LISTENING
TCP    127.0.0.1:1027          0.0.0.0:0               LISTENING
TCP    149.55.13.30:137        0.0.0.0:0               LISTENING
TCP    149.55.13.30:138        0.0.0.0:0               LISTENING
TCP    149.55.13.30:139        0.0.0.0:0               LISTENING
UDP    149.55.13.30:137        *:                        *:
UDP    149.55.13.30:138        *:                        *:

C:\NetBus\version17>
```

The above example is of a system with version 1.7 of NetBus running with the default configuration. One can see that ports TCP 12345 and 12346 are listening for connections.

It is also a good idea to examine the registry for services being started at Windows startup. Most services are started in the following section of the registry on Windows 9x:

\\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run\

Prevention

It is always a good idea to install antiviral software on each client machine in an organization. Since the software can only look for viruses it has signatures for, make sure to keep the database up to date. Many antiviral software packages have schedulers or auto-updaters for users who are connected to a network, which may relieve the administrative burden and requires less intervention on the end-user's part.

If one is in an environment that is connected to the Internet it is a good idea to protect the private network from the Internet with a good firewall product. If no unsolicited connections were allowed inside the network from the Internet, only certain services were allowed from the clients to the Internet, and the firewall's rulebase was reflective of this policy then it would be difficult for an intruder to connect to a system on the internal network without being inside the firewall.

User education is one of the best ways to protect against infection. If a user is aware of the risks, he/she is less likely to run attachments or download programs from an unknown or unreliable source.

Conclusion

NetBus is a legitimate remote administration tool. It has very powerful features, which can also be very dangerous when used with malicious intent. By protecting a network with the methods discussed and educating users on all potential security risks, one may maintain a more secure environment.

References

1. Neikter, Carl-Fredrik. "NetBus v.1.60." 1998. URL: <http://home.t-online.de/home/TschiTschi/nbv16.htm>
2. Neikter, Carl-Fredrik. "NetBus v.1.70." 1998. URL: <http://home.t-online.de/home/TschiTschi/nbv17.htm>
3. RenderMan. "NetBus Freed." 5 September 2000. URL: <http://www.antiav.com/Netbusfreed.html>
4. ISS X-Force. "Windows Backdoors Update II: NetBus 2.0 Pro, Caligula, and Picture.exe." 19 February 1999. URL: <http://xforce.iss.net/alerts/advis020.php>
5. Symantec. "Backdoor.NetBus.svr." Symantec Virus Encyclopedia. URL: <http://www.symantec.com/avcenter/cgi-bin/virauto.cgi?vid=7662>

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event