



# 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:

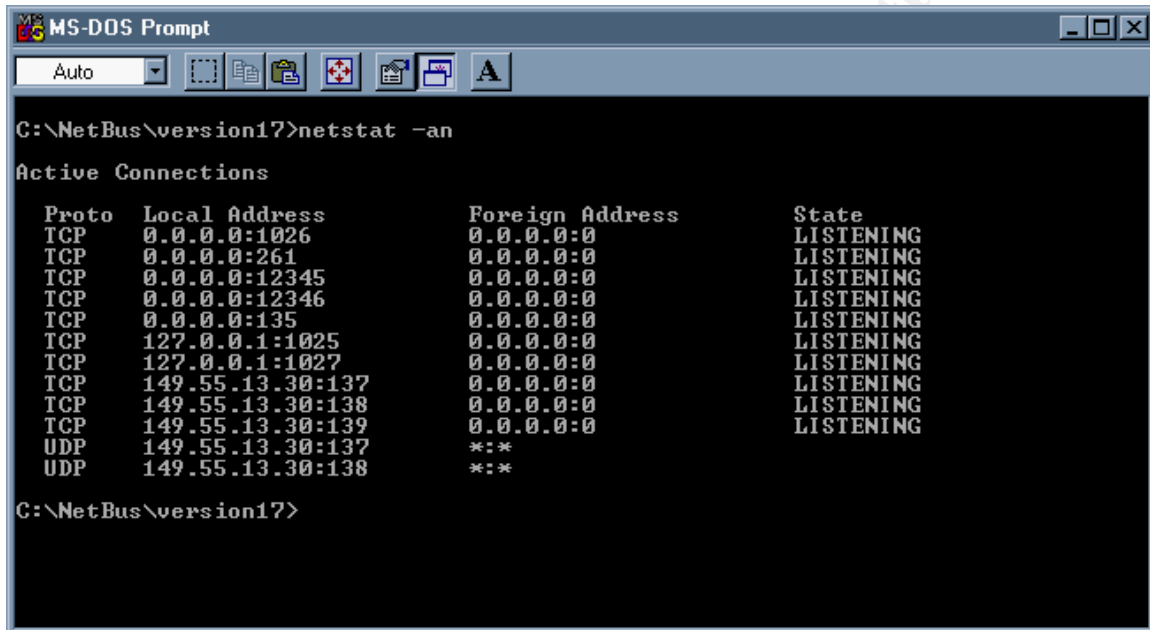
```
\\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\  
"PATCH"="C:\\WINDOWS\\PATCH.EXE /nomsg"
```

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       *:.*                     LISTENING
UDP   149.55.13.30:138       *:.*                     LISTENING

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 Miami 2019	Miami, FL	Jan 21, 2019 - Jan 26, 2019	Live Event
SANS Las Vegas 2019	Las Vegas, NV	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
Security East 2019 - SEC401: Security Essentials Bootcamp Style	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
SANS Northern VA Spring- Tysons 2019	Tysons, VA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Anaheim 2019	Anaheim, CA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Dallas 2019	Dallas, TX	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Secure Japan 2019	Tokyo, Japan	Feb 18, 2019 - Mar 02, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NV	Feb 25, 2019 - Mar 02, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VA	Feb 25, 2019 - Mar 03, 2019	Live Event
Mentor Session @Work - SEC401	Raleigh, NC	Feb 27, 2019 - Mar 06, 2019	Mentor
SANS Baltimore Spring 2019	Baltimore, MD	Mar 02, 2019 - Mar 09, 2019	Live Event
Baltimore Spring 2019 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Mar 04, 2019 - Mar 09, 2019	vLive
Community SANS Indianapolis SEC401	Indianapolis, IN	Mar 04, 2019 - Mar 09, 2019	Community SANS
SANS Secure India 2019	Bangalore, India	Mar 04, 2019 - Mar 09, 2019	Live Event
SANS Secure Singapore 2019	Singapore, Singapore	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS London March 2019	London, United Kingdom	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CA	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS St. Louis 2019	St. Louis, MO	Mar 11, 2019 - Mar 16, 2019	Live Event
Mentor Session - SEC401	Fredericksburg, VA	Mar 12, 2019 - May 14, 2019	Mentor
SANS Secure Canberra 2019	Canberra, Australia	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Norfolk 2019	Norfolk, VA	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Munich March 2019	Munich, Germany	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201903,	Mar 19, 2019 - Apr 25, 2019	vLive
SANS 2019	Orlando, FL	Apr 01, 2019 - Apr 08, 2019	Live Event
Community SANS Raleigh SEC401	Raleigh, NC	Apr 01, 2019 - Apr 06, 2019	Community SANS
SANS 2019 - SEC401: Security Essentials Bootcamp Style	Orlando, FL	Apr 01, 2019 - Apr 06, 2019	vLive
SANS London April 2019	London, United Kingdom	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KY	Apr 11, 2019 - Apr 18, 2019	Live Event