

Identify OS?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-01/0064.html>

From: Nick Jacobsen (nick@ethicsdesign.com)

Date: 01/31/03

From: "Nick Jacobsen" <nick@ethicsdesign.com>
To: <pen-test@securityfocus.com>
Date: Thu, 30 Jan 2003 23:33:20 -0800

Hey All again,

Could any of you give me an idea of what type of machine the following might be, based on the ports open? it is sitting at xxx.xxx.xxx.001 on a network, so I am thinking it is some sort of gateway, but what OS/hardware? Below is the results of telnetting to port 23, and the results of an nmap scan (tried the identify OS option, didn't do sh*t)

Nick J.

Ethics Design

nick@ethicsdesign.com

<----- Telnet results ----->

Authorized uses only. All activity may be monitored and reported.

login: cisco

Password:

Login incorrect

<----- End Telnet Results ----->

<----- Nmap Scan Results ----->

21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
53/tcp open domain
111/tcp open sunrpc
161/tcp filtered snmp
162/tcp filtered snmptrap
389/tcp open ldap
512/tcp open exec
513/tcp open login
514/tcp open shell
1002/tcp open unknown
1169/tcp open unknown
1433/tcp filtered ms-sql-s
1720/tcp open H.323/Q.931
2410/tcp open unknown
2785/tcp open unknown
2786/tcp open unknown

Identify OS?

SecurityFocus Penetration: Identify OS?

6000/tcp open X11

6112/tcp open dtspc

7937/tcp open unknown

7938/tcp open unknown

32774/tcp open sometimes-rpc11

32775/tcp open sometimes-rpc13

32778/tcp open sometimes-rpc19

Too many fingerprints match this host for me to give an accurate OS guess

TCP/IP fingerprint:

SInfo(V=3.10ALPHA7%P=i686-pc-windows-windows%D=1/30%Time=3E394B34%O=21%C=1)

T1(Resp=N)

T2(Resp=N)

T3(Resp=N)

T4(Resp=N)

T5(Resp=N)

T6(Resp=N)

T7(Resp=N)

PU(Resp=N)

<----- End Nmap Scan Results ----->

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>