

BO2k Port?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-09/0257.html>

From: PM Systems – Rick Woehler (RWoehler@PMSysCorp.com)

Date: 09/28/01

Message-ID: <ADA8D8680FDBD2119BE00060083993AF2321F3@dns1.pmsyscorp.com>
From: PM Systems – Rick Woehler <RWoehler@PMSysCorp.com>
To: pen-test@securityfocus.com
Subject: BO2k Port?
Date: Fri, 28 Sep 2001 09:52:50 -0400

Howdy List,

Doing an audit on a gov agency with a Raptor Firewall. I was shocked to see nmap repeatedly reporting 31335 and 31337 UDP open on the firewall. I'm told by my firewall guys that Raptors and VelociRaptors install with all ports closed and ports have to be specifically opened to allow traffic. I can't imagine the person that installed this firewall would allow those ports.

I haven't been able to connect with my BO2k console and am beginning to wonder if this is a false positive. I've seen Raptor Firewalls report open ports when they in fact are not and am wondering if anyone has advice on these high ports.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmap -sU -oN test.txt
xxx.xxx.xxx.xxx
Interesting ports on (xxx.xxx.xxx.xxx):
(The 1436 ports scanned but not shown below are in state: closed)
Port State Service
19/udp open chargen
53/udp open domain
111/udp open sunrpc
137/udp open netbios-ns
138/udp open netbios-dgm
161/udp open snmp
162/udp open snmptrap
426/udp open smartsdp
445/udp open microsoft-ds
500/udp open isakmp
31335/udp open Trinoo_Register
31337/udp open BackOrifice
```

```
# Nmap run completed at Fri Sep 28 09:31:34 2001 -- 1 IP address (1 host up)
```

```
scanned in 37 seconds
```

SecurityFocus Penetration: BO2k Port?

RW

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/>

- **Previous message:** Nasir Farhat Khan: "Re: Pen-testing Simatic Data Aquisition Periphery e.g. PLC S5 orS7"
- **Next in thread:** Daniel Roethlisberger: "Re: BO2k Port?"
- **Reply:** Daniel Roethlisberger: "Re: BO2k Port?"
- **Reply:** H D Moore: "Re: BO2k Port?"
- **Reply:** H D Moore: "Re: BO2k Port?"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]