

Re: FW: RE Modem identification

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-09/0202.html>

From: Bikar Dude (bika@nuclear.biodome.org)

Date: 09/23/01

Date: Sat, 22 Sep 2001 18:17:53 -0400 (EDT)
From: Bikar Dude <bika@nuclear.biodome.org>
To: Stephan Barnes <stephan.barnes@foundstone.com>
Subject: Re: FW: RE Modem identification
Message-ID: <Pine.LNX.4.33.0109221740450.7078-100000@nuclear.biodome.org>

> *Regardless of TeleSweep or PhoneSweep it is an ASCII text
> banner match issue. In our tests the jury is still out but
> I would tend to agree with Nate that PhoneSweep might be
> doing a better job of classifying the modems that were found
> than TeleSweep as of late; most recent release against most
> recent release. Run your own drag race and see.*

Would be curious to see results of this, too.

I looked @ wardialers about a month back went with TeleSweep. Be sure to check out compatible & suggested modem lists from a product before choosing. I went with a suggested 6 modem internal PCI card – physical footprint and wiring logistics for 6 modems didn't sound fun nor did messing with a PRI & Ascend Max. 6 lines @ 50 seconds/call ~ = 450 call/hr or 10k in 3 evenings. Performance junkies: larger weapons available at: <http://www.empirix.com/empirix/voice+network+test/products/telephony+performance+test.html>

Some bad points about Telesweep:

Missed an AS/400. Someone else said this was 3270/3278 emulation which Telesweep doesn't have a signature for (?).

It dropped a few numbers in a simple 1000 number range (always check your results!)

Some good points for Telesweep:

Pretty inexpensive – \$1k software + \$700 hardware. I can't imagine most of us needing a distributed, enterprise enabled, ODBC backed, client server _war dialer_.

```
/** ObHacker: Pick any 6 unix utilities and write a complete war-dialer.  
ObHacker++: Try to reduce the total number of letters in the 6 commands to  
less than 20. */
```

Re: FW: RE Modem identification

SecurityFocus Penetration: Re: FW: RE Modem identification

Simple (good) reports. HTML tables were handy for some things but I mostly just used the .CSV which is generated at scan time. Also very handy were the transaction logs – ASCII & hex dump of all modem calls. In a few cases just by reading this I was able to identify systems pretty easily without actually dialing them again.

–b

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:* Craig Holmes: "binary switching, no killing"
- *In reply to:* Stephan Barnes: "FW: RE Modem identification"
- *Next in thread:* Stephan Barnes: "RE: FW: RE Modem identification"
- *Messages sorted by:* [date] [thread] [subject] [author] [attachment]