

SecurityFocus Penetration: Re: Scanning for blank admin passwords on a windows box

Re: Scanning for blank admin passwords on a windows box

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-07/0067.html>

From: Muhammad Faisal Rauf Danka (mfrd@attitudex.com)

Date: 07/15/02

Date: Sun, 14 Jul 2002 15:04:03 -0700 (PDT)
From: Muhammad Faisal Rauf Danka <mfrd@attitudex.com>
To: pen-test@securityfocus.com

LanGuard Scanner from www.languard.com produces a list of users enumerated through a NetBIOS NULL session and information obtained via SNMP queries scan for "interesting" ports, password brute force attack and information gathering, and ChkLock can be used to get the system-wide password policy information (intruder lockout, the depth of the password history, minimum password length requirements, the name of the PDC, and so forth) from Windows NT and Windows 2000 machines. Because it's RPC-based, like all the net functions, it can be executed remotely (providing the relevant ports are not blocked by an intermediate router or firewall), you can get it from packetstorm.

Regards,

Muhammad Faisal Rauf Danka

Chief Technology Officer
Gem Internet Services (Pvt) Ltd.
web: www.gem.net.pk

[ATTITUDEX.COM]
<http://www.attitudex.com/>

Promote your group and strengthen ties to your members with email@yourgroup.org by Everyone.net
<http://www.everyone.net/?btn=tag>

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/>

Re: Scanning for blank admin passwords on a windows box

- **Previous message:** [st0ff st0ff: "PenTesting a IPX/SPX Client"](#)
- **Maybe in reply to:** [Jason: "Scanning for blank admin passwords on a windows box"](#)
- **Next in thread:** [Erwin van der Zwan: "Re: Scanning for blank admin passwords on a windows box"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)