

Re: penetration test in a Windows 2000/NT network

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-05/0053.html>

From: Chris Beek (*c.beek_at_pinkroccade.com*)

Date: 05/14/03

To: <pen-test@securityfocus.com>

Date: Wed, 14 May 2003 21:22:42 +0200

As mentioned in the email from Mark Ng, L0phtcrack will be your tool. One of the scenario's you could try is to take a laptop, install l0phtcrack on it and put it with a valid ip-adress in the network (most of the networks do have dhcp, so that won't be the hardest).

Next you have to setup L0phtcrack in "listening/sniffing" mode. Also create a shared directory on this machine.

From your station you will send around an email which contains an URL (which will connect towards the share). Make the email attractive so people are triggered to click. When clicking to the URL, Windows will notice that it's a Share and sends the NTLM hashes.

If the network is switched, you have to use a combination of the tool Ettercap and later on L0phtcrack to decrypt the passwords. You can use Ettercap the spoof (be carefull) the switch, so all ports can be sniffed. Choose for storing the sniffed traffic towards a file. This file can later on be analyzed by L0phtcrack.

Kind regards,

Chris Beek

Security Consultant

Pinkroccade RISC Tiger Team

----- Original Message -----

From: "heron heron" <h.heron@firemail.de>

To: <pen-test@securityfocus.com>

Sent: Wednesday, May 14, 2003 3:29 PM

Subject: penetration test in a Windows 2000/NT network

> *Hi,*

>

> *I will accomplish a penetration test in a Windows 2000/NT network shortly.*

A

> *goal is to get confidential information (files) and if possible get admin*

> *rights. I will be with my computers in the LAN. A computer for normal uses*

(thus

> *no Admin access) is likewise put to me at the disposal.*

>

SecurityFocus Penetration: Re: penetration test in a Windows 2000/NT network

> *Is there a possibility on a Windows 2000 computers (physical access is possible)*
> *to attain admin rights without to overwrite the admin account. Background:*
I
> *would like try to crack the password of the local admin (e.g. by means of pwdump*
> *and John). There ist the possibility that all admin passwords (also for the*
> *domain) is alike.*
>
> *Is there a tool, with which I can crack NTLMv2 hashes. Background: I will try to*
> *sniff hashes during the registration at the DC (e.g. CAIN, ettercap) and to*
> *crack them. Unfortunately me is still no tool known in order to crack NTLMv2*
> *hashes.*
>
> *A further possibility at to come to information, would be the employment of a*
> *SMB Proxy. By ARP Spoofing it would be nevertheless theoretically possible to*
> *intercept the LM/NTLM(v1/v2) authentication . Then the attacker could itself*
> *instead announce at the server. Does it give there already such a Tool?*
>
> *Who has suggestions? For Tools please give always in the Web URL (if possible of*
> *the programmer).*
>
> *Greeting*
> *Heron*
>
>

> *Arcor-DSL Flatrate – jetzt kostenlos einsteigen und bis zu 76,18 Euro sparen!*
> *Arcor-DSL gibt es jetzt auch mit bis zu 1500 Mbit/s Downstream!*
> <http://www.angebot.arcor.net/cgi-bin/angebot.cgi?key=b13e92247022>
>
>
>

-
> **** Wireless LAN Policies for Security & Management - NEW White Paper ****
> *Just like wired networks, wireless LANs require network security policies*
> *that are enforced to protect WLANs from known vulnerabilities and threats.*
> *Learn to design, implement and enforce WLAN security policies to lockdown*
> *enterprise WLANs.*

SecurityFocus Penetration: Re: penetration test in a Windows 2000/NT network

>
> To get your FREE white paper visit us at:
> <http://www.securityfocus.com/AirDefense-pen-test>

> -----
--

*** Wireless LAN Policies for Security & Management - NEW White Paper ***
Just like wired networks, wireless LANs require network security policies
that are enforced to protect WLANs from known vulnerabilities and threats.
Learn to design, implement and enforce WLAN security policies to lockdown enterprise WLANs.
To get your FREE white paper visit us at:
<http://www.securityfocus.com/AirDefense-pen-test>
