

RE: Non-GUI intrusion

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-09/0231.html>

From: Vince Sola (sola-v@home.com)

Date: 09/26/01

From: "Vince Sola" <sola-v@home.com>
To: "'KK Mookhey'" <kkmookhey@yahoo.com>, <pen-test@securityfocus.com>
Subject: RE: Non-GUI intrusion
Date: Tue, 25 Sep 2001 23:54:56 -0400
Message-ID: <000001c1463f\$026d8360\$0e02a8c0@gambrills1.md.home.com>

Well It seems to me that you ought to be able to upload a tool like nbtDump.exe, wininfo.exe, or enum.exe on to one of the machines you have control of inside the dmz. From there run your remote command line to use those tools to enumerate the shares on the inside.

Once you've enumerated them; since you have the user names and passwords, you could use the command line to 'net use' one of the internal machines. At that point upload your access tool to the internal machine. Once it's there listening upload Fpipe to the machine on the DMZ and have it redirect to your tool on the internal machine. This way you can control the source port and dest port (depending on your tool) so you can try to make your traffic blend into routine traffic.

Anyway just my \$.02 I'm sure there will other ideas from the list.

Vince

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

From: KK Mookhey [<mailto:kkmookhey@yahoo.com>]
Sent: Tuesday, September 25, 2001 1:35 AM
To: pen-test@securityfocus.com
Subject: Non-GUI intrusion

Hi All,

This is the scenario. We are conducting a pen-test with the capture-flag as the source-code files of the client (a s/w firm).

We have managed to penetrate most of their servers in the DMZ (all Win NT/2K).

Using pwdump and L0phtcrack, we have the username/password of over 20 users in the admin group (this is a very large company).

These same users have admin rights on the intranet machines too.

We have a GUI remote control over the servers.

We also know that they have a Blue Team (or is it White Team) which is monitoring logs/traffic and our activities, to demonstrate to their bosses that they could detect an attack like ours.

RE: Non-GUI intrusion

SecurityFocus Penetration: RE: Non-GUI intrusion

We need to get to the inside machines, since thats where the source code is.
We could do it using the Net Neighb icon on the NT/2k machines thru the GUI we already have, using the password we have cracked.
But that would be like a bull in a china shop.
We already have remote command prompt access on the DMZ machines. We need to be able to query shares (enum?), and get source files from the inside, without raising any alarms.
So,
What we need is a command line utility, or a GUI utility which does not raise red flags at their ends.
Anyone any ideas?
Sorry for the slightly long mail.
TIA,
KKM

Do You Yahoo!?
Get your free @yahoo.com address at <http://mail.yahoo.com>

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/>

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:** [H D Moore: "IOWargames 2001 Slides – Making NT Bleed \(v2.0\)"](#)
- **In reply to:** [KK Mookhey: "Non-GUI intrusion"](#)
- **Next in thread:** [KK Mookhey: "Re: Non-GUI intrusion"](#)
- **Next in thread:** [m@rl206.org: "Re: Non-GUI intrusion"](#)
- **Reply:** [KK Mookhey: "Re: Non-GUI intrusion"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)