

Re: Non-GUI intrusion

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-09/0239.html>

From: Mike Brentlinger (mdbrentlinger@hotmail.com)

Date: 09/26/01

From: "Mike Brentlinger" <mdbrentlinger@hotmail.com>
To: kkmookhey@yahoo.com, pen-test@securityfocus.com
Subject: Re: Non-GUI intrusion
Date: Tue, 25 Sep 2001 22:02:22 -0400
Message-ID: <F210U5zxLol1S7TWiHV00008389@hotmail.com>

whats wrong with things like...

```
c:\>net view
c:\>net view /d:domain
c:\>net use z: \\pcname\share password /u:domain_name\user_name
c:\>dir z:\*/*/s > index.txt
etc etc...
```

-mdb

-----Original Message Follows-----

From: "KK Mookhey" <kkmookhey@yahoo.com>
To: <pen-test@securityfocus.com>
Subject: Non-GUI intrusion
Date: Tue, 25 Sep 2001 11:05:19 +0530

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.

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.

Re: Non-GUI intrusion

SecurityFocus Penetration: Re: Non-GUI intrusion

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/>

Get your FREE download of MSN Explorer at <http://explorer.msn.com/intl.asp>

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:*** [Todd Ransom: "Re: Non-GUI intrusion"](#)
- ***Maybe in reply to:*** [KK Mookhey: "Non-GUI intrusion"](#)
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)