

[WP-007]

Whitepaper: Login Warning Banners

A Discussion about Login/Warning Banners, Their Emplacements and Their Uses

Version 040517

May 2004

Author: Bob Radvanovsky, rsradvan@unixworks.com

(A special thanks goes to those listed for being my “sounding board” on this project.)

Copyright © 2004 Bob Radvanovsky. All rights reserved.



Limited Liability Statement

In no event shall the author(s) be liable for any found errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained within this document may be subject to change without any notice. No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this whitepaper.

Documentation pertaining to any security-related technical or proprietary information, its data and all information provided and contained within this document is considered proprietary in nature and subject to copyright protection and is intended solely for use by its owner. Additionally, this documentation is solely for the purpose of discussing a possible, and/or proposed IT security issue, and is not dependent upon any specified infrastructure, architectural condition or its issue(s).

All other product names mentioned herein are trademarks or registered trademarks of their respective owners. NOTE: Any names not outlined or mentioned above are fictional in nature; as such, any relation to any name or trademark (if any) is purely coincidental.

Introduction

With everything becoming more and more interconnected via the Internet as an unsecured communication medium, there raises several questions/issues regarding legalities. One of these issues is the issuance of the word “welcome” in the login banner and headings for any given system, server or network appliance. Many discussions have ensued (and still continue today, though not as intensely as several years ago) pertaining to the simple, but powerful, word “welcome”.

The prosecution of an individual in a criminal case must show that the individual’s actions were intentional in nature. It would be extremely difficult for anyone to argue that an individual’s intrusion attempts (or actions) were by accident or inadvertent insofar as to go past such without encountering any type of warning or disclaimer on the target system or throughout the network. It may still be possible (though highly unlikely) that an individual that attempted an unauthorized and/or illegal intrusion attempt admit that their actions were intentional. However, upon their sentence, they may argue that they were ignorant to any specified law or that they were unaware that their actions were unauthorized, thereby inducing the court to mitigate whatever penalty may be imposed. If the example warning is issued, it will be extremely difficult for an individual to present such arguments.



Use of the warning or login banners (shown on subsequent pages) for all systems and networking appliances that are supported, as well as access points into the network (remote access, modem pool, file transfer, VPN, etc.), is strongly recommended. This provides a definitive warning to any possible intruders that may want to access your system that certain types of activity are illegal, but at the same time, it also advises the authorized and legitimate users of their obligations relating to acceptable use of the computerized or networked environment(s).

The warning is deliberately general in nature as it has not yet been established what type of (if any) crime has been committed. Subsequent prosecution may be performed under either (or both) federal or state law, or handled by local institution disciplinary procedures (such as the local university or school). The recommendation is that any login banner or system initial message should not imply consent to use the computer services (e.g., words such as "greeting" or "welcome"), unless it is the expressed intention that any user is free to use the system or networking environment, and whether they are authorized to use it or not.

Usually, it is up to the discretion of the site administrator(s) and management to decide if they are concerned with identification of the site and/or hostname. If the hostname doesn't show or demonstrate the functionality of the environment, it may be applicable to display the hostname (e.g.; "svr101" instead of "bkup_svr"). Some organizations may not anything representative of the server, network device or appliance to indicate the site, location, functionality, etc; however, in a court of law, if an individual is being prosecuted for an unauthorized access, intrusion or penetration attempt, they may stipulate that the warning message was not on the server as it does not identify the server in question, and that the warning may have been pulled from a server that was disclaimed rather than the target server in question. Showing (at least) the hostname alleviates (if not dismisses) this argument.

Though displaying or prompting with warning or login banners may not cover all ways to connect to a server, networking device or appliance, it does serve as one point of warning for a number of cases. Warnings such as this are a positive step towards providing adequate notice as to the obligations and responsibilities relating to the use of the server and networking environments. If a person is known to have seen the warnings, they cannot subsequently claim ignorance of their responsibilities.

As a precautionary step, legal advisors and attorneys recommend utilizing some form of "boilerplate" stating legal ramifications of unauthorized or illegal use of the corporate or government environments (networks and/or servers) and their resources. One of the philosophies that surround these warning banners is that the privacy of an individuals' right to retain their privacy and/or prevent system environments from properly identifying these users, whether legitimate or otherwise, is invalidated as that individual, whether authorized or otherwise, is utilizing that organization's resources (networks, servers, applications, etc).



Recommended uses that would require warning banner may include: (1) interactive access points and methods to/from the Internet (console login: telnet, web, FTP, SSH [secure shell]); and (2) non-interactive access points that provide or require human-readable responses (finger, email, etc.). Banners are displayed (usually) prior to access to any system resource, and is recommended that the user acknowledge some form of compliance prior to accessing those resources. In the event that a system or appliance does not support or have pre-login capabilities, the system or appliance should display the banner immediately following authorization. Lastly, in the event that no banners are capable of being displayed by the system or appliance, displaying a printed banner (along with any state or federal statute pertaining to the industry, such as healthcare or financial industries) should be clearly visible in common areas where public users may access the system and its environments.

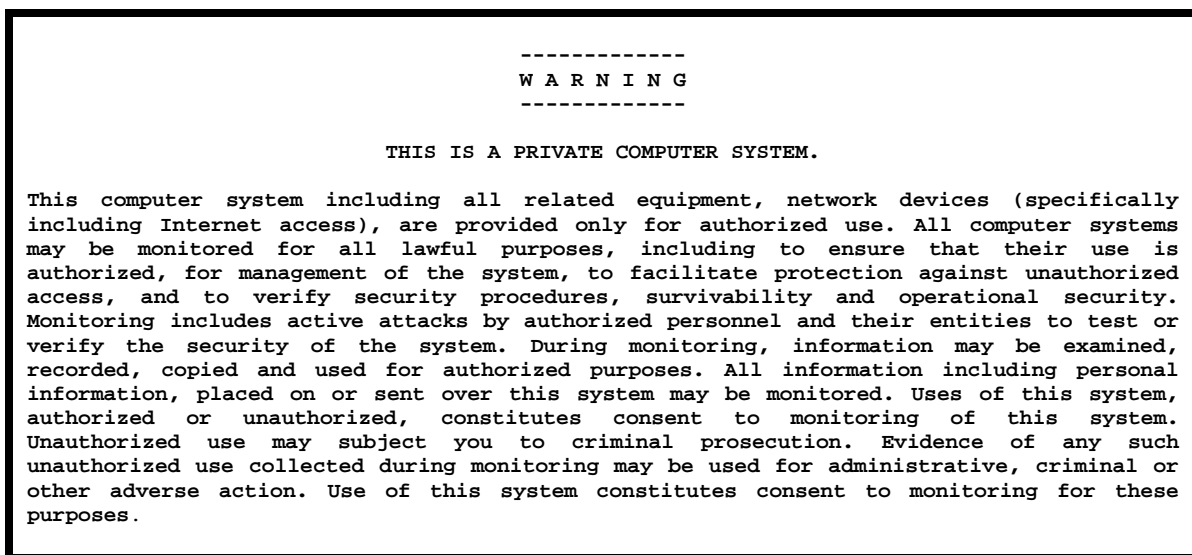
For any organization that may have publicly accessible or available workstations, terminals or kiosks, emplacement of a banner should be posted, either electronically and/or in printed form. Having a banner displayed in public indicates that any user utilizing the organization's resources should have no expectation of privacy whatsoever while using the server and network environments of that organization.

Types of Banners

For the interactive/login banner, one such banner, which was found to be instrumental, can be found on any federal government installation. The banner shown below was modified from the publicly accessible Great Lakes Naval Medical Center web site banner at the Great Lakes Naval Base in Glenview, IL.

Interactive Banner: Pre-Login

For interactive warning/login banners, the banner (shown below) is one possible pre-login banner that may be used.



Interactive Banner: Post-Login

For interactive warning banners, reinforce that everything is monitored and logged.

```
WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your
actions may be monitored if unauthorized usage is suspected.
```

Non-Interactive Banner: Electronic Mail

For email, the user of a disclosure banner indemnifies the organization against unsolicited and/or unauthorized electronic correspondence from that organization.

```
>>> CONFIDENTIALITY NOTICE <<<
This electronic mail message, including any and/or all attachments, is for the sole use
of the intended recipient(s), and may contain confidential and/or privileged information,
pertaining to business conducted under the direction and supervision of the sending
organization. All electronic mail messages, which may have been established as expressed
views and/or opinions (stated either within the electronic mail message or any of its
attachments), are left to the sole responsibility of that of the sender, and are not
necessarily attributed to the sending organization. Unauthorized interception, review,
use, disclosure or distribution of any such information contained within this electronic
mail message and/or its attachment(s), is(are) strictly prohibited. If you are not the
intended recipient, please contact the sender by replying to this electronic mail
message, along with the destruction all copies of the original electronic mail message
(along with any attachments).
```

Alternatively, the following email disclosure banner may be used in lieu of the more verbose version from above. This statement is more of a liability or limited liability statement indemnifying the author of any wrongful acts based upon their electronic mailing.

```
This document was prepared as an account of work sponsored by said organization. Neither
the organization listed nor any of its employees, assume any warranty, express or
implied, or any legal liability or responsibility for the accuracy, completeness, or
usefulness of the information, apparatus, product, or process disclosed, or represents
that its use would not infringe privately owned rights. Reference herein to any specific
commercial products, process, or service by trade name, trademark, manufacturer, or
otherwise, does not necessarily constitute or imply its endorsement, recommendation or
favoring by said organization nor their constituents. The views and opinions of the
authors expressed herein do not necessarily state nor reflect those of said organization
nor their constituents, and shall not be used for advertising or product endorsement
purposes whatsoever.
```



Banner Emplacement

The Microsoft Windows operating systems allows login access with a username and password before the system can be used. The following method displays a dialog box with a warning banner, prompting the user for an acknowledgement by pressing the “Ok” button to be displayed before the system displays the login dialog box within the Windows 95/98/ME environments, and (usually) after pressing “*Ctrl-Alt-Del*” within the Windows NT/2000/XP/2003 environments.

To create a login banner within the Windows environments, there will need to be two registry keys added to the Windows registry; there are two ways to edit the Windows registry. One is to edit it directly using the “*regedit*” application; the second is to create a “.reg” file containing the required modifications, followed with the execution of “*regedit*”.

WARNING: *This is VERY dangerous to use if unfamiliar with the “regedit” application, which may cause system instability requiring a reload/re-image of the operating system environment.*

Windows 2000 and Higher

Confirm the following registry key and its value sets for the local login banner. The caption text is what is displayed at the top of the window, with the caption body text displayed within the window.

```
Key:
    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon

Values:
    LegalNoticeCaption = "The caption text."
    LegalNoticeText = "The body of the banner."
```

Starting with Windows 2000 environments (and higher), there is a second registry key and value set associated with the local login banners. These keys are set through/with Microsoft’s Active Directory (ADS) service (Microsoft’s equivalence to LDAP). If these active directory local policy value sets are defined, they take precedence over the local settings in the WinLogon key above.

```
Key:
    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Values:
    LegalNoticeCaption = "The local policy caption text."
    LegalNoticeText = "The local policy body of the banner."
```



Pre-Windows 2000

For Windows 95/98/ME environments, substitute the word “*Windows*” in lieu of the word “*Windows NT*” in the registry keys below. For Windows NT 3.51, shorten the original banner slightly by changing the words “*United States*” in the first line of the banner to the abbreviation “*U. S.*” If you are using Microsoft’s Active Directory service, set the banner value sets there instead of setting them locally.

Follow the steps similar to what was outlined for Windows 2000 (or higher) environments.

Key:

```
...\Microsoft\Windows NT\CurrentVersion\WinLogon\LegalNoticeCaption
```

Values:

- ❖ Using “*regedit*”, scroll down to the WinLogon key.
- ❖ With the WinLogon key selected choose the Edit->New->String Value command.
- ❖ Type the name of the new string value as “*LegalNoticeCaption*”, then press <ENTER>.
- ❖ With the new string value selected, choose the Edit->Modify command.
- ❖ In the dialog box that is displayed, type “*NOTICE TO USERS*”, then press <ENTER>.

Key:

```
...\Microsoft\Windows NT\CurrentVersion\WinLogon\LegalNoticeText
```

Values:

- ❖ Using “*regedit*”, scroll down to the WinLogon key.
- ❖ With the WinLogon key selected choose the Edit->New->String Value command.
- ❖ Type the name of the new string value as “*LegalNoticeText*”, then press <ENTER>.
- ❖ With the new string value selected, choose the Edit->Modify command.
- ❖ In the dialog box that is displayed, type the body of the legal notice or banner, then press <ENTER>
Note that the notice appears as a single paragraph, as the “*regedit*” key editor does not recognize carriage returns.

After editing the Windows registry key with the RegEdit application, the entries are saved as a “.*reg*” file. To create the file, select the two keys created and choose the Registry->Export->Registry File command, give the file a name and click Save->Edit the “.*reg*” file with a text editor and remove all the keys but “*LegalNoticeCaption*” and “*LegalNoticeText*”. To copy the “.*reg*” file to other machines and simply double clicking on the filename makes the same edits to the registries of the other machines.

If the file was created using a Windows NT/2000/X/2003 “.*reg*” file, it may be converted to a Windows 95/98/ME “.*reg*” file by editing it with a text editor and changing “*Windows NT*” in the two keys to “*Windows*”, then saving the file under a different name. When converting from a Windows NT 4.0 release banner to a pre-4.0 Windows NT release banner, this may be performed by shortening the banner text slightly. Replace the words “*United States*” within the first line of the banner text to “*U. S.*” and save the “.*reg*” file with a different name.



UNIX and Linux

The banners for commercial-grade versions of UNIX (HP-UX, AIX, Solaris, etc.) depend largely upon the particular vendor and service provided. For more recent versions of the UNIX environment, creating the file `"/etc/issue"` containing the banner text will display a login banner prior to the familiar `"login:"` prompt (this is often inclusive to services such as: telnet, ftp, SSH [secure shell], rsh [restricted shell] and rlogin [remote login]). Some version may require parameters settings (such as HP-UX) in which a `"-f"` followed by the absolute filename path of the `"issue"` file is located.

The LINUX environments have two pre-login banner methods: one for the console login, the other one for remote login (via telnet, ssh, etc.). For the console login, the file is under `"/etc/issue"`; for the remote login, the file is under `"/etc/issue.net"`. As some SSH clients (such as the one provided by SSH, Inc.) may have difficulty displaying all of the text, some partial editing may be necessary; therefore, a third `"issue"` file may be necessary. Edit the `"/etc/ssh/sshd_config"` (SSH Version 1) or `"/etc/ssh2/sshd2_config"` (SSH Version 2) file and look for the entry:

```
BannerMessageFile      /etc/issue.bnr
```

As a suggestion, edit the `"/etc/issue.net"` file to however the file needs to be addressed, save it, then reset the `"sshd"` daemon. Upon resetting, at login time, the banner will be displayed prior to the login dialog (much to the same manner/method that Windows displays their login dialogs).

For UNIX/Linux environments that do not recognize the `"/etc/issue"` file, place the banner text within the file `"/etc/motd"`; those environments that do recognize the `"/etc/issue"` file, reiterate the legal statement after login within the `"/etc/motd"` file.

Some versions of the FTP service (such as ProFTP, NCFTP or WU-FTP) allow the display of login banners prior to and following login. Please refer to the application developers of these applications for specific questions regarding emplacement of pre/post-login banners via the FTP process.



TCP Wrappers

UNIX users may apply banners to services such telnet, FTP, ssh [secure shell] etc. using the TCP Wrappers application. TCP Wrappers is an application used for controlling who can/cannot connect to the various services on any given server or workstation. Additionally, by controlling access to the server/workstation, the TCP Wrappers application has the ability to display a banner to the connecting client whenever a connection to a service is requested. Care must be taken as to which services banners are added to, as many protocols are not meant to be read by humans and do not support text banners. Note also that this works only for those services that are controlled by the TCP Wrappers application.

The TCP Wrappers program must first be downloaded and installed on your system. The source code for “*tcpwrappers*” is available from:

ftp://ftp.cert.org/pub/tools/tcp_wrappers/

To add banners to the specified TCPwrappers program, the application must be recompiled with the `-DPROCESS_OPTIONS` flag. This options flag, which is a language extension, is NOT enabled by default. Within the “*/etc/hosts.allow*” file, add a text entry, “*: banners /banner/path*” after the list of clients that the banner will be displayed to. The string, “*/banner/path*” is the path to a directory that contains the banner files. The banner files have the same names as the daemons/processes they will apply to. That is, the banner for the “*in.ftpd*” daemon is in a file named “*in.ftpd*” (or in this case, if the “*/banner/path*” is used, it would be “*/banner/path/in.ftpd*”). It is possible to have a different banner for each rule listed within the “*/etc/hosts.allow*” file (as desired).

Apache

To display a warning banner for general site access using the Apache web server, edit the “*/etc/httpd/conf/httpd.conf*” (or wherever the “*httpd.conf*” file may be located), and look for the “*<Directory /usr/local/apache/htdocs>*” directive set.

```
<Directory "/usr/local/apache/htdocs">
  AuthType Basic
  AuthName "This is a private computer system. Only authorized
  users are permitted access to this web site. All access attempts
  onto this system are closely monitored and logged. Any attempt to
  circumvent security on this systems may result in legal action(s)."
```

```
  AuthUserFile /usr/local/apache/htdocs/.htpasswd
  AuthGroupFile /usr/local/apache/htdocs/.htgroup
  Require group apache
  Order allow,deny
  Allow from all
</Directory>
```

If different warning banners or disclaimers are to be shown for virtual web sites, alter the directory location based upon the actual directory location for the virtual web site. Please note the “*AuthGroupFile*” directive is NOT necessary.



Mueslix – Sample Banners throughout the Internet

Some sample warning/login banners currently in use throughout the Internet community. Their locations, along with the URL, are shown (and if the banner is short enough, is also displayed).

University of Chicago Networking and Information Services: NSC Sample Banners
http://security.uchicago.edu/docs/login_banners.shtml

Restricted Server Warning Banner:

Unauthorized access to this machine is prohibited. Use of this system is limited to authorized individuals only. All activity is monitored.

Login Server Warning Banner:

Unauthorized use of this machine is prohibited. This is a University machine intended for University purposes. The University reserves the right to monitor its use as necessary to ensure its stability, availability, and security.

University College London: Sample Login Banners
<http://www.ucl.ac.uk/privacy/login-banners.htm>

JANET-CERT Sample Banners
<http://www.ja.net/CERT/JANET-CERT/regulation/banners.html>

University of Oklahoma Health Services Center: Login Banner Policy (very lengthy and rather informative of course of action that will be taken if violations/unauthorized access is suspected; their verbiage is similar to the example for this document)
<http://www.ouhsc.edu/it/security/policy/login-banner.asp>

laidback.org Funny Quotes throughout the Internet (includes sample USAF banner; plain, simple and quite effective for a military installation)
<http://www.laidback.org/issue.shtml>

IRIX System V.4 (tornado.army.mil)

Access to this computer system is restricted to personnel of the White Plains USAF base. All connections are logged. By attempting connection without permission, you are in violation of federal law.

United States Department of Justice Keystroke Monitoring and Login Policy
<http://doe-is.llnl.gov/Orders/dojkeymn.pdf>

