

White Hat Security Guide "How To Hack With Telnet"

White Hat Security Guide "How To Hack With Telnet"

This is a White Hat computer security training guide. To use this guide you must have your own TCP/IP network. This can be as simple as two computers connected over a single wire connection or as complex as a network with thousands of routers. Casual readers are advised that if you use these procedures on any network, such as the networks connected to the Internet, without the permission of the owner that it could be a violation of national or international law. If you are responsible for the security of one or more Internet networks this guide can significantly enhance your understanding of how exploitation of networks is accomplished using the very simple hacker Telnet protocol.

Telnet is an Internet Network Virtual Terminal (NVT) protocol that is easier to use than to explain. The Telnet protocol is used by other Internet applications, such as the Control Connection in FTP, so knowledge of Telnet is useful within multiple applications. This general applicability of Telnet within the Internet enables a hacker to reap lots of information and potentially exert control over many applications. By using Telnet, a human hacker can emulate any number of Internet applications disguising the human as just another Internet computer.

Within the Internet, each application (Well Known Port) is assigned a number in accordance with Internet Standard 002. A few of these numbers are enumerated below:

Internet Application Numbers

WWW	80	FTP	21	Telnet	23	SMTP	25
-----	----	-----	----	--------	----	------	----

WWW Example - Use of Telnet to emulate a WWW client for information gathering. telnet 192.168.1.1
 80 Telnet to server application port 80 note: the server will not provide an automatic
 response... GET / HTTP 1.1

Instruct the WWW server to return
data using HTTP 1.1 format

```
HTTP/1.1 200 OK
Date: Mon, 05 Nov 2007 14:55:33 GMT
Server: Apache/2.2.3 (FreeBSD) DAV/2
PHP/5.1.6 with Suhosin-Patch mod_ssl/2.2.3 OpenSSL/0.9.7e-p1
Last-Modified: Mon, 08 Oct 2007 00:41:47 GMT
ETag: "1c8216-2562-847088c0"
Accept-Ranges: bytes
Content-Length: 9570
Connection: close
! Content-Type: text/html
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  web server is running on a FreeBSD Unix server.
  The WWW server is Apache version 2.2.3.
  The server is also running PHP version
  5.1.6 and SSL version 0.9.7.
```

Lots of information is returned. We see that the

SMTP (email) Spoofing Example - Use of Telnet
to hack (forge) email telnet 192.168.1.1 25 Telnet to the email application
Trying 192.168.1.105...
Connected to host.
Escape character is '^]'.
220 192.168.1.105 ESMTP Sendmail 8.13.8/8.13.8; Mon, 5 Nov 2007 10:42:59 -0500 (EST) Server
response. HELO SANTA.ANY-REAL.ADDRESS Make up a hostname...or pick a real
hostname
from DNS The remote server returns 250 192.168.1.105 Hello [192.168.1.100],
pleased to meet you MAIL FROM: <SantaClaus@localhost> Type any address
you like Server accepts address 250 2.1.0 <USER@ANYREAL.ADDRESS>
... Sender ok RCPT TO:<someone@anyreal.address> This should be a
username used within this domain...
Server checks its usernames then replies Recipient ok DATA Server replies 354
Enter mail, end with "."

on a line by itself

Type your message followed by a line with just a period.

```
.                Server replies 250 2.0.0 IA5FgxM4000833 Message accepted for delivery      quit
Server replies 221 2.0.0 192.168.1.105 closing connection
Connection closed by foreign host.
```

Resulting Message...

```
From SantaClause@localhost.com Tue Nov 6 12:04:30 2007
Date: Tue, 6 Nov 2007 12:01:19 -0500 (EST)
From: SantaClause@localhost.com
Subject: Email Forgery
To: undisclosed-recipients;
```

This email was forged using the Telnet protocol.

Summary

Telnet is a simple protocol designed to provide compatible terminal services across TCP/IP networks. The simple character mode design of the Internet Protocols like Telnet make them great tools for hackers looking for information about your hardware and software infrastructure. Telnet provides you with an excellent White Hat tool to familiarize yourself with this level of network interactions. The knowledge will prove itself invaluable as you configure routers, switches, and other devices on your network.

{mosypn}

Peach ePublishing, LLC Disclaimer: THE INFORMATION AND MATERIAL CONTAINED IN THIS SITE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY CONCERNING THE ACCURACY, ADEQUACY, OR COMPLETENESS OF SUCH INFORMATION OR MATERIAL OR THE RESULTS TO BE OBTAINED FROM USING SUCH INFORMATION OR MATERIAL. THE AUTHOR SHALL NOT BE RESPONSIBLE FOR ANY CLAIMS ATTRIBUTABLE TO ERRORS, OMISSIONS, OR OTHER INACCURACIES IN THE INFORMATION OR MATERIAL CONTAINED IN THIS SITE, AND IN NO EVENT SHALL THE AUTHOR OR THE PUBLISHER BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF SUCH INFORMATION OR MATERIAL.