

# Hi Tech Crime Solutions

## Am I Hacker Proof Security Audit



**Audit completed on: December 2, 2011 11:10 AM**

# Table of Contents

- [Introduction](#)
- [Personal Information](#)
- [Rating Score](#)
- [Scan Information](#)
- [Fingerprint](#)
- [Traceroute](#)
- [Scan Tasks](#)
- [Vulnerability Information](#)
- [Website Vulnerabilites](#)
- [Word Press Vulnerabilites](#)
- [Glossary](#)

# Quick Scan Report

## Introduction

---

This report represents a security audit performed by Am I Hacker Proof from Hi Tech Crime Solutions. It contains confidential information about the state of your network.

## Personal Information

---

Here is some personal information about you.

Name: Test Run  
Address: 1234 Test Way  
New York, NY 20123  
E-Mail Address: test@test.com  
IP Address: 1.2.3.4

## Rating Score

---

Our Am I Hacker Proof Rating Score is based on several factors, open ports, responses to pings, and also if a firewall was detected.

Only can get an A+ if they do not accpet pings and they have 0 vulnerabilities

Subtract the points for:

-1 vulnerabilites

# Scan Information

---

Here is some basic information about the Am I Hacker Proof Scan we collected.

Start Date: December 2, 2011 11:05 AM

End Date: December 2, 2011 11:10 AM

Computer Type:

Browser Version:

Number of open ports: 17

# Fingerprint

---

## Description

Fingerprinting is ascertaining the operating system of a remote computer on the Internet.

## Actual Fingerprint

```
OS:SCAN(V=5.00%D=12/2%OT=21%CT=1%CU=34347%PV=N%DS=10%G=N%TM=4ED8F86D%P=x86_
OS:64-unknown-linux-gnu)SEQ(SP=CC%GCD=1%ISR=D3%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M
OS:5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%
OS:O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%
OS:DF=Y%T=3C%W=16D0%O=M5B4NNSNW7%CC=N%Q=)T1(R=Y%DF=Y%T=3C%S=O%A=S+%F=AS%R
OS:0%Q=)T2(R=N)T3(R=Y%DF=Y%T=3C%W=16A0%S=O%A=S+%F=AS%O=M5B4ST11NW7%RD=0%Q=)
OS:T4(R=Y%DF=Y%T=3C%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=3C%W=0%S=Z%A
OS:+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=3C%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%D
OS:Y%T=3C%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=3C%IPL=164%UN=0%RIPL=C
OS:%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=3C%CD=S)
```

## Operating System Guess

general purpose Linux 100% Accuracy

# Traceroute

---

## Description

Traceroute is an operation of sending trace packets for determining information; traces the route of UDP packets for the local host to a remote host. Normally traceroute displays the time and location of the route taken to reach its destination computer.

## Traceroute results

| Hop | IP Address      | Host                                |
|-----|-----------------|-------------------------------------|
| 1   | 50.56.35.8      |                                     |
| 2   | 184.106.126.49  | core1-aggr701a-2.ord1.rackspace.net |
| 3   | 184.106.126.188 | corea.ord1.rackspace.net            |
| 4   | 184.106.126.137 | edge2.ord1.rackspace.net            |
| 5   | 65.116.208.161  | chx-edge-03.inet.qwest.net          |
| 6   | 205.171.93.142  | chp-brdr-03.inet.qwest.net          |
| 7   | 77.67.79.121    | xe-4-3-0.chi12.ip4.tinet.net        |
| 8   | 89.149.184.26   | xe-0-0-0.den11.ip4.tinet.net        |
| 9   | 77.67.73.6      | fdc-servers.ip4.tinet.net           |
| 11  | 1.2.3.4         |                                     |

# Scan Task Begin

---

## Times at which the scan started

Parallel DNS resolution of 1 host. started at December 2, 2011 11:06 AM  
SYN Stealth Scan started at December 2, 2011 11:06 AM  
Service scan started at December 2, 2011 11:07 AM  
Traceroute started at December 2, 2011 11:09 AM  
Parallel DNS resolution of 10 hosts. started at December 2, 2011 11:09 AM  
NSE started at December 2, 2011 11:09 AM

# Scan Task End

---

## Times at which the scan ended

Parallel DNS resolution of 1 host. ended at December 2, 2011 11:06 AM  
SYN Stealth Scan ended at December 2, 2011 11:07 AM  
Service scan ended at December 2, 2011 11:09 AM

Traceroute ended at December 2, 2011 11:09 AM

Parallel DNS resolution of 10 hosts. ended at December 2, 2011 11:09 AM

NSE ended at December 2, 2011 11:10 AM

# Firewall/Router Vulnerabilities

---

## Description

Here is a list of all of the open ports that we discovered on your network.

## Vulnerability Information results

| #  | Service   | Protocol | Port Number | Status |
|----|-----------|----------|-------------|--------|
| 1  | ftp       | TCP      | 21          | open   |
| 2  | ssh       | TCP      | 22          | open   |
| 3  | smtp      | TCP      | 25          | open   |
| 4  | domain    | TCP      | 53          | open   |
| 5  | http      | TCP      | 80          | open   |
| 6  | pop3pw    | TCP      | 106         | open   |
| 7  | pop3      | TCP      | 110         | open   |
| 8  | rpcbind   | TCP      | 111         | open   |
| 9  | imap      | TCP      | 143         | open   |
| 10 | http      | TCP      | 443         | open   |
| 11 | smtp      | TCP      | 465         | open   |
| 12 | rpcbind   | TCP      | 817         | open   |
| 13 | imap      | TCP      | 993         | open   |
| 14 | pop3      | TCP      | 995         | open   |
| 15 | mysql     | TCP      | 3306        | open   |
| 16 | https-alt | TCP      | 8443        | open   |
| 17 | unknown   | TCP      | 8880        | open   |

# Level 1: Web Site Vulnerabilites ( 15 total)

---

**Item ID:** 999986

**OSVDB Link:** No Link Available

**Description:** Retrieved x-powered-by header: PleskLin

**URI:** /t0G6kOvb.save

**Name Link:** <http://test.com:80/t0G6kOvb.save>

---

**Item ID:** 999996

**OSVDB Link:** No Link Available

**Description:** robots.txt retrieved but it does not contain any 'disallow' entries (which is odd).

**URI:** /robots.txt

**Name Link:** <http://test.com:80/robots.txt>

---

**Item ID:** 740000

**OSVDB Link:** No Link Available

**Description:** Multiple index files found: default.asp, index.jhtml, index.htm, index.pl, default.htm, index.aspx, default.aspx, index.asp, index.do, index.php3, index.cfm, index.cgi, index.html, index.shtml,

**URI:** /

**Name Link:** <http://test.com:80/>

---

**Item ID:** 999972

**OSVDB Link:** No Link Available

**Description:** DEBUG HTTP verb may show server debugging information. See <http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx> for details.

**URI:** /

**Name Link:** <http://test.com:80/>

---

**Item ID:** 000266

**OSVDB Link:** [Click here](#)

**Description:** /?mod=some\_thing&op=browse: Sage 1.0b3 reveals system paths with invalid module names.

**URI:** /?mod=some\_thing&op=browse

**Name Link:** http://test.com:80/?mod=some\_thing&op=browse

---

**Item ID:** 000687

**OSVDB Link:** [Click here](#)

**Description:** /userinfo.php?uid=1;: Xoops portal gives detailed error messages including SQL syntax and may allow an exploit.

**URI:** /userinfo.php?uid=1;

**Name Link:** http://test.com:80/userinfo.php?uid=1;

---

**Item ID:** 001384

**OSVDB Link:** [Click here](#)

**Description:** /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

**URI:** /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000

**Name Link:** http://test.com:80/index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000

---

**Item ID:** 001386

**OSVDB Link:** [Click here](#)

**Description:** /some.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

**URI:** /some.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42

**Name Link:** http://test.com:80/some.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42

---

**Item ID:** 001387

**OSVDB Link:** [Click here](#)

**Description:** /some.php?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

**URI:** /some.php?=PHPE9568F35-D428-11d2-A769-00AA001ACF42

**Name Link:** http://test.com:80/some.php?=PHPE9568F35-D428-11d2-A769-00AA001ACF42

---

**Item ID:** 750000

**OSVDB Link:** [Click here](#)

**Description:** /icons/: Directory indexing found.

**URI:** /icons/

**Name Link:** http://test.com:80/icons/

---

**Item ID:** 003575

**OSVDB Link:** [Click here](#)

**Description:** /xmlrpc.php: xmlrpc.php was found.

**URI:** /xmlrpc.php

**Name Link:** http://test.com:80/xmlrpc.php

---

**Item ID:** 003584

**OSVDB Link:** [Click here](#)

**Description:** /icons/README: Apache default file found.

**URI:** /icons/README

**Name Link:** http://test.com:80/icons/README

---

**Item ID:** 006181

**OSVDB Link:** No Link Available

**Description:** /wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version usually matches the WordPress version

**URI:** /wp-content/plugins/akismet/readme.txt

**Name Link:** http://test.com:80/wp-content/plugins/akismet/readme.txt

---

**Item ID:** 006183

**OSVDB Link:** No Link Available

**Description:** /readme.html: This WordPress file reveals the installed version.

**URI:** /readme.html

**Name Link:** http://test.com:80/readme.html

---

**Item ID:** 006186

**OSVDB Link:** [Click here](#)

**Description:** /license.txt: License file found may identify site software.

**URI:** /license.txt

**Name Link:** http://test.com:80/license.txt

---

## Level 2: Word Press Vulnerabilites ( 4 total)

---

**Description:** The Wordpress theme in use is called platformpro

**Vulnerability URL:** N/A

---

**Description:** The WordPress http://test.com/readme.html file exists.

**Vulnerability URL:** N/A

---

**Description:** Wordpress version 3.1.4 identified from meta generator.

**Vulnerability URL:** N/A

---

**Description:** XSS Vulnerability in NextGEN Gallery Wordpress Plugin

**Vulnerability URL:** <http://www.exploit-db.com/exploits/12098/>

---

# Glossary

---

## Glossary

Below are several technical terms that will help you understand your report.

- Closed
  - "Closed Port", which is set to deny all packets with that port number. A port is registered as closed when there is no process running that listens to connections to that port.
- Filtered
  - A port reported as filtered when a firewall blocks packets and (typically) drops them ( -j DROP). Then no response comes back. Note that a filtered port is unknown to you whether it is open or closed.
- Fingerprinting
  - When exploring a network for security auditing or inventory/administration, you usually want to know more than the bare IP addresses of identified machines. Your reaction to discovering a printer may be very different than to finding a router, wireless access point, telephone PBX, game console, Windows desktop, or Unix server. Finer grained detection (such as distinguishing Mac OS X 10.4 from 10.3) is useful for determining vulnerability to specific flaws and for tailoring effective exploits for those vulnerabilities.
- Firewall
  - A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting outward communication.
- IP Address
  - An Internet Protocol (IP) address is a numerical identification (logical address) that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes. It is like having a telephone number to your computer. Static IP addresses are manually assigned to a computer by an administrator. The exact procedure varies according to platform. This contrasts with dynamic IP addresses, which are assigned either by the computer interface or host software itself, as in Zeroconf, or assigned by a server using Dynamic Host Configuration Protocol (DHCP). Even though IP addresses assigned using DHCP may stay the same for long periods of time, they can generally change. In some cases, a network administrator may implement dynamically assigned static IP addresses.
- Open Port
  - Open port is a TCP/IP port number that is configured to accept packets. Open is a port when it will accept() connections, therefore a process must be running and listening to that port. And yes, to see a port as open, the firewall must allow access to it.
- OS
  - Operating system of your computer. Example, Windows, Linux, Mac .....
- Ping
  - 'Ping' is a computer network tool used to test whether a particular host is reachable across an IP network. If you cannot ping the IP, that means you can't scan it.
- Port scanner
  - a piece of software designed to search a network host for open ports.
- Router
  - a networking device whose software and hardware are usually tailored to the tasks of routing and forwarding information. For example, on the Internet, information is directed to various paths by routers.

- Who is
  - widely used for querying an official database in order to determine the owner of a domain name, an IP address, or an autonomous system number on the Internet.
- Traceroute
  - An operation of sending trace packets for determining information; traces the route of UDP packets for the local host to a remote host. Normally traceroute displays the time and location of the route taken to reach its destination computer.
- Web Results
  - This section will show various vulnerabilities about the web site that was scanned.
- Cross Site Scripting (XSS)
  - a code injection vulnerability sometimes found in web applications that can be used by malicious hackers to e.g. hijack a legitimate user's session with the website. XSS vulnerabilities are caused because of improper validation of URL parameters or user input by the Server side program and then sending this invalidated input back to the user in some exploitable form. Forms of common vulnerabilities/attacks include HTML &/or JavaScript injection and SQL injection.
- SSH (Secure SHell)
  - A program and protocol for securely logging in to and running programs on remote machines across a network, with encryption to protect the transferred information and authentication to ensure that the remote machine is the one desired; To use ssh to connect to a remote computer
- HTTP (Hyper Text Transfet Protocol)
  - The standard way of transferring information across the World Wide Web. It supports a variety of media and file formats across a variety of platforms.