Stewart Technical Consulting's
IP Network Scan

IP Network Scan provided by Stewart Technical Consulting involves a series of security tests conducted on customer networks. An important aspect of **IP Network Scan** is the inclusion of manual tests and verification, giving the final security report a high level of accuracy.

Security scanning is a critical factor in secure and successful network operations. Newly established Internet connections often have several security flaws that need to be found and rectified. Existing Internet connections that have altered network layouts or added new Internet services need to be proven secure. Established Internet connections that consider security a high priority need an impartial view of their network from an external perspective to bring out security issues that might have been over looked.

Stewart Technical Consulting treats the issue of network security most seriously and will handle your case with complete confidentiality. Our staff will visit you to discuss any concerns you may have, and provide a quotation for an **IP Network Scan** on your network. After vigorous security scans and tests have been completed, a staff member will visit you with the resulting report and go over any major security issues that might be uncovered within your network. Complimentary phone and email support for report related queries is also allocated for **IP Network Scan** customers.

The final security report is concise and readable, and gives a view of your network and it's vulnerabilities from an Internet perspective. This gives you a clear picture of what potential hackers 'see' when they probe your network. Where possible the report will include a threat identifier for issues shown on the report, so those specific problems can be further explained by our online security database. Our online security database contains a set of documents from differing sources on many security issues current in today's Internet systems.

The table of contents is indexed by IP address, enabling reports even covering large networks to be followed easily.

Contents

In order to keep your network secure, the report includes a section on commonly overlooked areas of Internet security and some suggestions for maintaining a workable and realistic IT security policy.

The following examples further demonstrate the reports’ value added content.

```
192.168.100.65
  Host Summary:
    Operating System       : Linux 2.2.0-pre1 - 2.2.2
    Vulnerability Warnings : 8
    Obvious Services       :
        Port         Protocol     Warnings     Service
        21           tcp          2            ftp
        22           tcp          1            ssh
        25           tcp          2            smtp
        80           tcp          1            http
        139          tcp          1            netbios-ssn
        515          tcp          1            printer
```

The above example shows an Internet visible system with exposed ports. Each port has been tested, and the number of detected security issues for each port is shown here. A sub-section for each port would follow, detailing the specific issues.

```
  [21/tcp]
    Service Name : ftp
    Data Provided : 220 example.stewart.com.au FTP server [Version
      wu-2.4.2-VR17[1] Mon Apr 19 09:21:53 EDT 1999] ready.
    Service Analysis :
      This FTP server allows anonymous logins.
      Severity : Low
      This is an old version of wu-ftp, there are multiple known exploits, an
      upgrade is strongly recommended.[1003]
      Severity : High
```

In the above example the warning identifier ‘[1003]’ can be looked up on our online database, which will retrieve the “CERT® Advisory CA-99-13 Multiple vulnerabilities in WU-FTPD” document.

```
  [80/tcp]
    Service Name : http
    Data Provided : Alibaba/2.0
    Service Analysis :
      This web server seems to allow anyone to view any file on the server,
      simply by requesting ../../../file.txt the file will be returned.[1046]
      Severity : High
      This web server seems to allow anyone to execute arbitrary commands on
      the server by requesting /cgi-bin/program command .[1046]
      Severity : High
```

In the above example the identifier ‘[1046]’ would refer to a Bugtraq@securityfocus.com mailing list posting exposing some security exploits.

```
[80/tcp]
  Service Name     : http
  Data Provided    : Microsoft-IIS/3.0
  Service Analysis :
    This is an old version of Microsoft’s Internet Information Server, an
    upgrade is recommended.[1033]
    Severity : Moderate
```

The above example demonstrates a Microsoft IIS server that is out of date and has known security flaws.

```
[25/tcp]
  Service Name : smtp
  Data Provided : example1.stewart.com.au ESMTP Sendmail 8.9.3/8.8.7
    Fri, 10 Mar 2000 10:05:25 +1100
  Service Analysis :
    This SMTP server could be vulnerable to a redirection attack. It may be
    used to route a mail message through your firewall to internal mail
    servers, or by spammers, and could result in bandwidth or host loading
    and performance degradation.
    Severity : Moderate
    This SMTP server allows open mail relaying. It may be used by spammers,
    and could result in bandwidth or host loading and performance
    degradation.
    Severity : Moderate
    This version of Sendmail is current.
```

The above shows a mail server open for misuse by email spam.

Stewart Technical Consulting
P.O. Box 2784
Cheltenham, VIC 3192

Phone : +61 (0)417 305 719

Website: http://www.stewart.com.au/

Email : info@stewart.com.au