Internet-based Network Security Assessment Report

For Matta Technologies Limited

27 March 2008

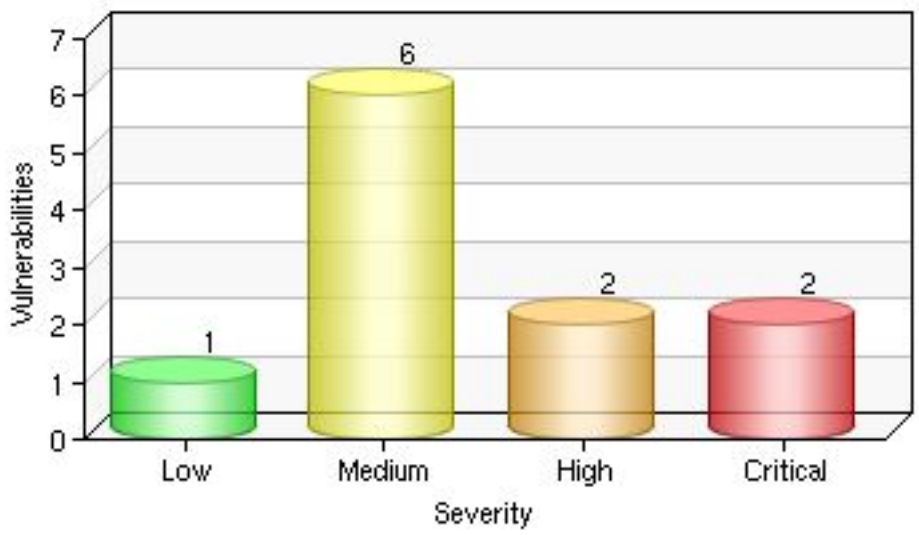
Matta Technologies Limited

Falstaff House
34 Bardolph Road
Richmond upon Thames
United Kingdom
+44 (0) 8700 77 11 00
www.trustmatta.com

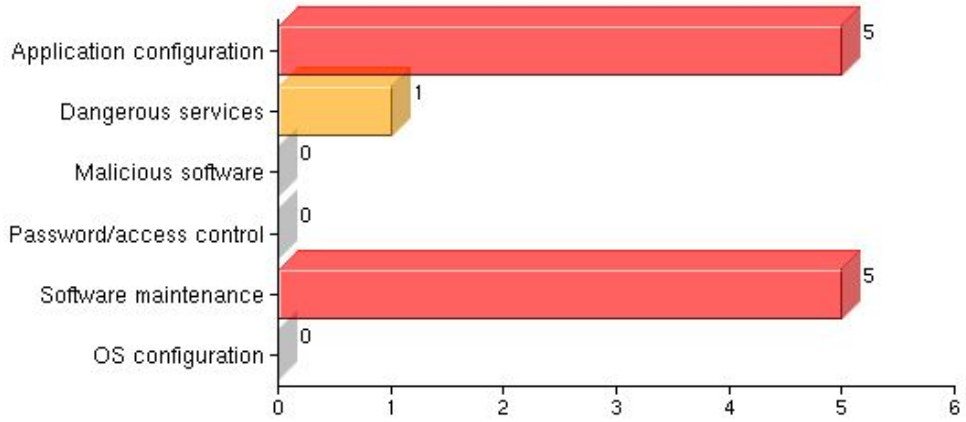
1. Executive Summary

1.1 Metrics

1.1.1 Total vulnerabilities found

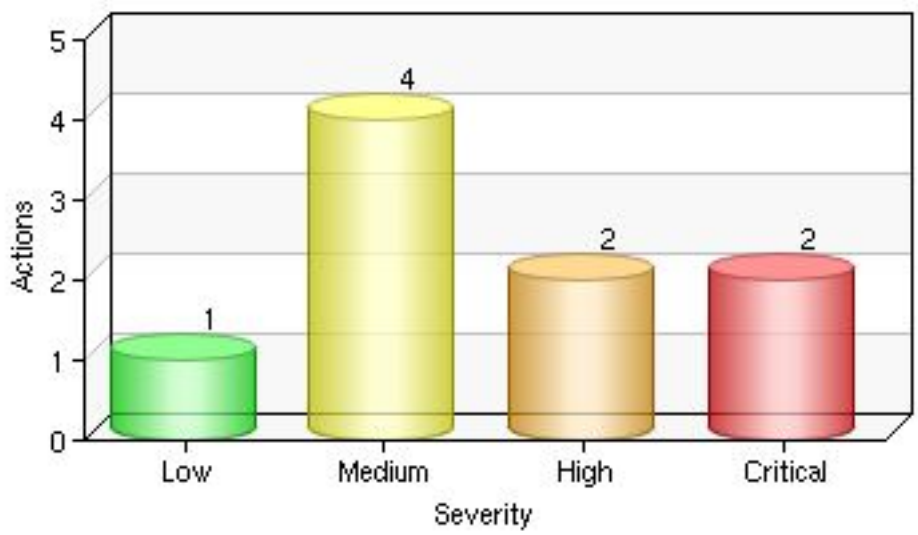


1.1.2 Vulnerabilities by class



1.1.3 Asset by Highest Risk

1.1.4 Number of Action Points



2. Test Scope and Approach Details

2.1 Scope

2.1.1 The scope of the exercise was to probe the following range of IP addresses:

- 83.142.224.20 - 83.142.224.30

2.1.2 Matta performed the following Internet-based tests against the accessible devices and servers:

- Open source reconnaissance (using DNS, WHOIS, Google, and Netcraft)
- ICMP network sweeping (issuing echo, timestamp, and address mask requests)
- TCP port scanning (performing half-open SYN scanning along with stealth scans)
- UDP port scanning (performing UDP data scanning and inverse UDP scanning)
- Fingerprinting of the accessible TCP and UDP network services
- Thorough active testing of the accessible TCP and UDP network services
- Cross-referencing of service versions with vulnerability lists (CVE, NVD, et all)
- Web application infrastructure assessment and server crawling

2.2 Tool Selection

2.2.1 Matta uses proprietary in-house software, known as Colossus, to perform bulk Internet-based scanning tasks. Colossus is capable of thoroughly assessing the following services and application components:

- Remote Information Services (DNS, Finger, identd, NTP, SNMP, LDAP, and RPC rusers)
- Web Services (Lotus Domino, Microsoft IIS, Apache, Jakarta Tomcat, IBM WebSphere, and Sun iPlanet)
- Web Applications (PHP, JSP, and ASP in particular)
- Remote Maintenance Services (SSH, Telnet, RSH, X Windows, Microsoft RDP, VNC, Symantec PcAnywhere, and Citrix services)
- FTP Services (Internal FTP services, WU-FTP, ProFTP, and Microsoft IIS FTP)
- Database Services (Microsoft SQL Server, MySQL, Postgres, and Oracle)
- Windows Networking Services (NetBIOS, CIFS, Microsoft RPC services, Samba)
- Email Services (Sendmail, Exchange, Postfix, Qmail, MAILsweeper, POP3, and IMAP)
- IPsec VPN Services (ISAKMP testing in particular, along with specific Check Point tests)
- Unix RPC Services (NFS services, OpenWindows / window manager services, and others)

2.2.2 Colossus is a thorough and broad network security assessment tool, which allows Matta to perform tests in a thorough and consistent manner. By using Colossus, along with manual qualification and deep testing of systems regarding vulnerabilities that are identified, Matta provides a high degree of testing quality and accuracy.

3. Internet-based Network Security Assessment

3.1 Objective

3.1.1 The objective of an external security assessment is to identify vulnerabilities in the Internet-based network infrastructure, its configuration, and security devices. An external attacker will target vulnerabilities that provide the quickest and best chance of successful exploitation without risk of detection. External security assessment emulates this approach of determined hackers and is concentrated upon the publicly accessible hosts and networks of the target organisation

3.2 Reconnaissance and Network Mapping

3.2.1 Searches of Internet-based sources (performing DNS, WHOIS, Google, and Netcraft sweeps in particular) were conducted to gather background information relating to the target networks and their users. Upon performing this public querying, ICMP, TCP, and UDP scanning was undertaken to identify accessible devices and systems within the target IP network blocks.

3.2.2 The following accessible Internet-based devices and systems were found:

IP Address	Primary Hostname	System Details
83.142.224.22	europa	Solaris 8 mail and FTP server
83.142.224.23	trustmat-webapp	Windows 2000 web server
83.142.224.30	Unknown	Cisco Systems device

3.2.3 The following IP addresses were comprehensively scanned by Colossus, but found to not be running any accessible network services:

IP Address	Primary Hostname
83.142.224.20	Unknown
83.142.224.21	Unknown
83.142.224.24	Unknown
83.142.224.25	Unknown
83.142.224.26	Unknown
83.142.224.27	Unknown
83.142.224.28	Unknown
83.142.224.29	Unknown

3.2.4 What follows are the findings of the security assessment of these Internet hosts, with vulnerabilities detailed and categorised by risk.

3.2.5 Vulnerability risk categories used in this report are high, medium, and low-risk. High-risk issues are significant issues that will easily lead to the loss of control over privileged information or critical business assets, and should be fixed or mitigated against immediately. Medium-risk issues are often exploited by extremely determined attackers to gain access to privileged systems and data, and so should also be fixed or mitigated against. Low-risk issues do not pose immediate risk to the business or privileged data, and should be addressed only when high and medium-risk flaws have been dealt with.

3.3 83.142.224.22 (europa)

3.3.1 TCP and UDP port scan results:

Port	Protocol	State	Service Details
21	TCP	open	Solaris 8 FTP service
25	TCP	open	Sun Sendmail 8.11.6 mail service (SMTP)

3.3.2 The issues identified are as follows:

Outdated Server Software	CRITICAL

Vulnerability

3.3.3 The following accessible network service packages are outdated and contain vulnerabilities:

- Sendmail 8.11.6

References

3.3.4 A number of these issues are listed in the MITRE CVE vulnerability list (http://cve.mitre.org), as follows:

- CVE-2006-4434, Sendmail 8.13.7 and prior denial of service (DoS) via a long email header
- CVE-2006-1173, Sendmail 8.13.6 and prior multipart MIME message denial of service (DoS) issue
- CVE-2002-1337, Sendmail 8.12.7 and prior crackaddr() overflow

Recommendations

3.3.5 It is imperative that software is maintained and patched up-to-date, to avoid process manipulation, information leak, and Denial of Service (DoS) attacks from being effective. Matta recommends that the following current releases of server software packages are installed:

- Sendmail 8.14.1 (http://www.sendmail.org/releases/8.14.1.php)

File Transfer Protocol - Outdated Server Software	HIGH

Vulnerability

3.3.6 The version of SunOS FTP server running on this host is outdated and vulnerable to arbitrary code execution through a heap overflow.

3.3.7 The SunOS FTP server version was obtained from the server banner upon connecting to TCP port :

```
$ ftp 83.142.224.22 21
Connected to 83.142.224.22.
220 europa FTP server (SunOS 5.8) ready.
```

References

3.3.8 A number of these issues and potential issues (that depend on the configuration) are listed in the MITRE CVE vulnerability list (http://cve.mitre.org), as follows:

- CVE-2001-0249, Glob heap overflow vulnerability in FTP daemon in Solaris 8

Recommendations

3.3.9 At the time of writing, Matta recommends that the software components are updated as follows:

- SunOS FTP 5.8 server patch: http://sunsolve.sun.com/search/document.do?assetkey=1-21-111606-06-1%38searchclause=ftp%2420SERVER5.8

3.4 83.142.224.23 (trustmat-webapp)

3.4.1 TCP and UDP port scan results:

Port	Protocol	State	Service Details
80	TCP	open	Microsoft IIS 5.0 web service (HTTP)
135	TCP	open	Microsoft RPC endpoint mapper service
139	TCP	open	NetBIOS session service (Windows 2000)
443	TCP	open	Unknown service
445	TCP	open	Microsoft CIFS service
1025	TCP	open	Microsoft RPC endpoint mapper service
1027	TCP	open	Microsoft RPC endpoint mapper service
1028	TCP	open	Microsoft RPC endpoint mapper service
1433	TCP	open	Unknown service
5800	TCP	open	RealVNC 4 web service (HTTP)
5900	TCP	open	VNC service

3.4.2 The issues identified are as follows:

Server Message Block (SMB) Anonymous Access	CRITICAL

Vulnerability

3.4.3 Anonymous null sessions are permitted to the SMB protocol, accessible through the following service ports:

- TCP 139 (NetBIOS session)

3.4.4 Upon connecting to, and authenticating with SMB through these vectors, attackers can enumerate users, groups, accessible shares, and named pipes. These components can be targeted and lead to a serious compromise.

3.4.5 Colossus was able to launch a brute-force password grinding attack, and compromise the following user account passwords:

- Administrator (blank password)

3.4.6 Other low-level data, such as accessible named pipes, and server details, including hostname, were also enumerated, but are not listed here for brevity.

Recommendations

3.4.7 Anonymous null session access to SMB should not be permitted. Please review the following documents that discuss SMB hardening and its effects:

- http://support.microsoft.com/kb/246261
- http://support.microsoft.com/kb/890161

3.4.8 Windows filesharing services (including NetBIOS and CIFS) should not be exposed to the public Internet, as they are complex and have a number of known weaknesses. Matta recommends that access to the following services is disabled, and offered only through a secure VPN or similar private network (such as PPTP):

- NetBIOS (UDP 137 and TCP 139)
- CIFS (TCP and UDP port 445)

Microsoft RPC Endpoints Exposed	HIGH

Vulnerability

3.4.9 The following ports are running Microsoft RPC endpoints:

- TCP 135

3.4.10 Through these endpoints, the following RPC services are accessible:

- RPC endpoint mapper
- DCOM WMI interface

3.4.11 These RPC services have a number of known vulnerabilities and weaknesses, including:

- RPC endpoint mapper Denial of Service (CVE-2002-1561)
- DCOM WMI interface, used for brute-force password grinding and information gathering

References

3.4.12 For more details relating to Microsoft RPC testing and security weaknesses, please review the following:

- http://www.blackhat.com/presentations/win-usa-04/bh-win-04-seki-up2.pdf
- http://www.blackhat.com/presentations/win-usa-01/Sabin/bh-win-01-sabin.ppt
- http://www.hsc.fr/ressources/presentations/null_sessions/index.html.en

Recommendations

3.4.13 Matta recommends that access to these Internet-accessible Microsoft RPC endpoints is filtered and tightly controlled. Ideally, access to core operating system components should be provided through more secure means, such as a private VPN.

3.4.14 Through disabling unnecessary services (such as the Messenger service), the number of RPC endpoints and interfaces is reduced. Matta recommends that unnnecessary services are stopped and disabled on the server.

3.4.15 HSC has some useful Microsoft RPC hardening recommendations, which are available for review at http://www.hsc.fr/ressources/presentations/null_sessions/img36.html)

Unnecessary Remote Maintenance Services	MEDIUM

Vulnerability

3.4.16 This is running unnecessary remote maintainence services, used to manage and maintain the server remotely. If an attacker is able to compromise valid credentials (through brute-force, network sniffing, man-in-the-middle, or other means), he can instantly compromise the server.

3.4.17 The unnecessary services running on this host are as follows:

- VNC service (TCP port 5900)

3.4.18 These services are susceptible to network sniffing and man-in-the-middle attacks to compromise valid credentials, along with brute-force password grinding. If an attacker is focused and determined enough, and logs are not regularly checked to identify abuse or authentication failures, it is possible that the server will be compromised.

Recommendations

3.4.19 Maintenance of such servers running critical Internet-facing services should be performed through a secure channel, such as a VPN. In particular, three sound VPN technologies are recommended:

- IPsec VPN
- SSL VPN
- SSH port forwarding / tunnelling

3.4.20 A VPN will provide protection against brute-force password grinding attack (minimising the surface of vulnerability), and will ensure that data (including credentials) is protected from network sniffing and man-in-the-middle attacks.

3.4.21 Upon ensuring these services are offered through a VPN, they should no longer be accessible through the public Internet in this manner.

HTTP Brute-Force	**MEDIUM**

Vulnerability

3.4.22 It is possible for an attacker to launch a brute-force password grinding attack against these authentication mechanisms and URLs to potentially compromise the server:

- http://83.142.224.23/localstart.asp
- http://83.142.224.23/printers/
- http://trustmat-webapp/localstart.asp
- http://trustmat-webapp/printers/

Recommendations

3.4.23 Matta recommends removing the http://83.142.224.23/localstart.asp file, http://83.142.224.23/printers/ directory, http://trustmat-webapp/localstart.asp file and http://trustmat-webapp/printers/ directory from the web root folder, as they are not necessary. This will increase simplicity thus improve security and minimise administration.

3.4.24 If authentication is indeed required for the web server, it is important that password strength is sufficient, and auditing processes identify brute-force attempts. Matta recommends that SSL is also used to protect from sniffing and man-in-the-middle attacks.

Unnecessary HTTP Methods Supported	**MEDIUM**

Vulnerability

3.4.25 The web server supports a handful of HTTP methods which can often be used to retrieve sensitive information about server configuration and underlying components:


```
OPTIONS / HTTP/1.1

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 27 Mar 2008 12:34:08 GMT
MS-Author-Via: MS-FP/4.0,DAV
Content-Length: 0
Accept-Ranges: none
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND,
PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
Cache-Control: private
```

3.4.26 The unnecessary methods are listed below:

- HTTP 1.1 (TRACE)
- WebDAV (COPY, PROPFIND, SEARCH, LOCK and UNLOCK)

3.4.27 The TRACE method can be used to perform cross-site tracing (XST) attacks, which can lead to attackers stealing cookie and session data. Papers discussing XST can be found at the following locations:

- http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
- http://www.securiteam.com/securityreviews/5YP0L1FHFC.html
- http://en.wikipedia.org/wiki/Cross-site_tracing

3.4.28 WebDAV methods are particularly dangerous, resulting in information disclosure, arbitrary code execution, and modification of content server-side upon authenticating.

3.4.29 The following CVE references relate to relevant WebDAV vulnerabilities within IIS 5.0:

- CVE-2003-0109, SEARCH overflow, resulting in arbitrary code execution (MS03-007)
- CVE-2002-0422, Information disclosure, including internal IP address, through PROPFIND, WRITE, and MKCOL methods (MS KB 218180)
- CVE-2000-0951, Index Server misconfiguration, resulting in SEARCH directory listing (MS KB 272079)

Recommendations

3.4.30 The unnecessary methods should be disabled to prevent information leaks and further compromises.

3.4.31 Matta strongly recommends that Microsoft URLScan is installed. In its default configuration, URLScan will filter access to these unnecessary components and improve security. URLScan is freely available from http://www.microsoft.com/technet/security/tools/urlscan.mspx

Unnecessary ISAPI Extensions Enabled	MEDIUM

Vulnerability

3.4.32 The web server has a number of unnecessary ISAPI extensions enabled. Vulnerabilities have been identified in most of these features, and they are disabled by default in IIS 6.0.

3.4.33 The following unnecessary ISAPI extensions were found to be enabled on the web server over TCP port 80:

- htw, ida, idq, printer

3.4.34 The following terminal dump shows the printer ISAPI extension being enabled:

```
GET /NULL.printer HTTP/1.0

HTTP/1.1 500 13
Server: Microsoft-IIS/5.0
Date: Thu, 27 Mar 2008 12:34:09 GMT
Connection: close
Content-Type: text/html

<b>Error in web printer install.</b>
```

References

3.4.35 Serious remote vulnerabilities have been previously identified in the htw, ida, idq, printer extensions. CVE references for these issues are as follows:

- CVE-2001-0500, Buffer overflow in ISAPI extension allows remote attackers to execute arbitrary commands via a long argument to IDA and IDQ files
- CVE-2001-0241, Buffer overflow in Internet Printing ISAPI extension in Windows 2000 allows remote attackers to gain root privileges via a long print request

3.4.36 These IIS features are not required by the software running on the server, and provide attackers with avenues in which to compromise the server in the event of a new vulnerability being disclosed which relates to any of these ISAPI extensions.

Recommendations

3.4.37 Matta strongly recommends that Microsoft URLScan is installed. In its default configuration, URLScan will filter access to these unnecessary components and improve security. URLScan is freely available from http://www.microsoft.com/technet/security/tools/urlscan.mspx

3.4.38 These extensions should also be manually removed, to ensure that a compromise is not possible, by clicking through the following options in the Internet Services Manager console:

- Click into the machine you want to configure under the ISM
- Right-click on the web service
- Select Properties
- Click the Home Directory tab
- Click Configuration
- Select the ISAPI extensions you wish to remove

IIS Local IP Disclosure	LOW

Vulnerability

3.4.39 The internal IP address of the IIS web server can be enumerated using the following methods:

- HTTP Location:
- HTTP PROPFIND response

3.4.40 The following terminal dump shows the IP address being obtained upon connecting to the web server and issuing GET requests:

```
GET /images HTTP/1.0

HTTP/1.1 302 Object Moved
Location: http://192.168.250.164/images/
Server: Microsoft-IIS/5.0
Content-Type: text/html
Content-Length: 153
```

References

3.4.41 The following sites provide useful references and information relating to this issue:

- http://support.microsoft.com/kb/218180
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0422
- http://www.securityfocus.com/bid/1499

Recommendations

3.4.42 The IIS web server should be configured to use and present a Fully Qualified Domain Names (FQDN). This configuration is outlined in Microsoft KB article #218180, and should be implemented to improve resilience.

3.4.43 Secondly, support for unnecessary HTTP methods (such as PROPFIND) should be disabled, and a mechanism such as Microsoft URLScan installed to improve security further.

3.5 83.142.224.30 (unknown)

3.5.1 TCP and UDP port scan results:

Port	Protocol	State	Service Details
21	TCP	open	Xlight 2.7 FTP service

3.5.2 No issues were identified on this host.