Security Aduit for waldock.ca

Meredith Waldock WEB109 2022-04-10

Section 1

Definitions:

DNS: Domain Name System: translating IP addresses into human languages for readability

DNS Server is the server protocol that matches the hostname to the IP address

IP: internet protocol address

Domain Registrar: a business that reserves domain names and assigns IP addresses to those domain names

Ports: in networking, ports are the end point for information communication, with the in the operating system. Port 80 and 443 are open as end points for communication to http https. They act as the gates to sending info to a website/server

NMAP: network mapper is an open-source tool of cyber security to find and analyze services and communications on computer networks and among other features checks for vulnerabilities of programs and libraries

IMAP: Internet Message Access protocol: an internet protocol for emails to be retrieved from a mail server. IMAP communicates on TCP

FTP: Files Transfer Protocol also using TCP is a protocol as the name suggests sends files between computers. FTP Server is the server side of the transfer, sending between FTP client and server

TCP: Transmission Control Protocol: used in conjunction with IP for the reliable transmission of 'packets' (information) over the network between server and client

SSL Certification: Secure Socket Layer: the standard security technology by created an encrypted link between two systems. This makes sure information is encrypted when its sent between client and server. SSL should include all domains attached to an IP for correct security.

Kali Linux: an open-source distribution used for testing cyber security, also known as penetration testing

Dmitry: Deepmagic Information Gathering Tool, is a tool included in Kali Linux used to find public information from the target host. If host is secured, emails names addresses will not be public otherwise Dmitry with find it

Vulnerabilities: areas of insecurity in open -source code, libraries, programs and internet protocols

Known Vulnerabilities: vulnerabilities that were tested and found or made aware (got hacked). Open-Source community finds them to update and fix or provide secure solutions.

SSLScan: another Kali Linux tool for outputting SSL services and the information attached to the certificate

SearchSploit :A command line search tool for Exploit-DB that allows for an offline copy of Exploit Database. SearchSploit gives you the power to perform detailed off-line searches through locally checked-out copy of the repository.

RSA: RSA is a public-key cryptosystem that is widely used for secure data transmission. RSA uses a public and private key; the key strength relates to the encryption strength in 'bits'.

Section 2

Domain and DNS Services Audit

The first section of the audit focuses on the website domain, IP, and registrar. This allows for a first glimpse into the security of the website.
Using NMAP it was determined *Waldock.ca* had :
103 ports open including:

143 imap: Internet Message Protocol	20 ftp-data: File Transfer Protocol
993 imaps: Internet Message Protocol	21 ftp: File Transfer Protocol
80 http: Web Traffic	110 pop3: Post Office Protocol
443 https: Web traffic	

Ports work as gates or doorways to the website, when they're open to the web anyone can walk in. *Waldock.ca* is at very high risk if it already hasn't been hacked.
There are secured open ports such as 443 HTTPS and 80 HTTP that require encryption or 'key' to enter the doorways of the website
Next in testing the domain and IP to see if any personal information was attached and made public using dmitry in Kali Linux. *Waldock.ca* did protect the personal information such emails, addresses, names, and phone numbers.
Now for testing the SSL certificate - *Waldock.ca* is networked correctly to it's IP address 216.187.109.203 The certificate does include the alternative names: cpanel.waldock.ca, cpcalendars.waldock.ca, webmail.waldock.ca, www.waldock.ca. The certificate is not expired, and the RSA Key Strength is 2048.
SSLSCAN

Section 3

Application Audit

The second section is assessing the application. *Waldock.ca* no longer has many applications live However we can analyze the applications that were on the domain until February 2018 including WordPress- WordPress 4.4 as the CMS. For best security it is always critical to keep with the latest updated versions of applications and WordPress themes as known vulnerabilities get fixed with updates.

Some Known Vulnerabilities in WordPress 4.4:
WordPress <= 4.4.2 - Script Compression Option CSRF
WordPress <= 4.4.2 - Reflected XSS in Network Settings
WordPress <= 4.4.2 - SSRF Bypass using Octal & Hexedecimal IP addresses
WordPress 3.7-4.4.1 - Open Redirect
WordPress 3.7-4.4.1 - Local URIs Server Side Request Forgery (SSRF)
WordPress 3.7-4.4 - Authenticated Cross-Site Scripting (XSS)

When *Waldock.ca* ran these applications, they were on a LAMP stack (Linux, Apache, MySQL, PHP). As with WordPress there are known vulnerabilities with different versions. Keeping these updated can aid in securing the website. Vulnerabilities are found and listed with CVE Details:
https://www.cvedetails.com/vulnerability-list/vendor_id-74/product_id-128/opdos-1/PHP-PHP.html

https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/Apache-Http-Server.html
Some Known Vulnerabilities in PHP 7:

PHP 5.x - 7.x <= - ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.

PHP 5.x - 7.1.24 <= - ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.

Some Known Vulnerabilities in Apache2 2.2.x (No longer supported):

Apache2 2.2.x - 2.4.6 <= Use-after-free when using <Limit > with an unrecognized method in .htaccess ("OptionsBleed") (CVE-2017-9798)
Apache2 2.2.x - 2.4.6 <= ap_get_basic_auth_pw() Authentication Bypass (CVE-2017-3167)
Apache2 2.2.x - 2.4.6 <= mod_ssl Null Pointer Dereference (CVE-2017-3169)
Apache2 2.2.x - 2.4.6 <= ap_find_token() Buffer Overread (CVE-2017-7668)
Apache2 2.2.x - 2.4.6 <= mod_mime Buffer Overread (CVE-2017-7679)

Some Known Vulnerabilities in nginx 1.18 1.20 1.21:
1-byte memory overwrite in resolver. Severity: medium. Advisory CVE-2021-23017
Not vulnerable: 1.21.0+, 1.20.1+ Vulnerable: 0.6.18-1.20.0

Section 4

Server Audit

Web applications run on servers. Servers carry the underlying hardware to accepts requests via HTTP/HTTPS. Insecurities in the servers allows for attacks on applications. Using NMAP it was found that *Waldock.ca* is running Linux 3.10 kernel and has known vulnerabilities.

Some Known Vulnerabilities in Linux Kernel 3.10:
Linux Kernel 3.10.1 -3.10.6 <= CVE-2013-4254 The validate_event function in arch/arm/kernel/perf_event.c in the Linux kernel prior to 3.10.8 on the ARM platform allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) by adding a hardware event to an event group led by a software event.

Linux Kernel 3.10.1 -3.17.3 <= CVE-2014-8884 Stack-based buffer overflow in the ttusbdecfe_dvbs_diseqc_send_master_cmd function in drivers/media/usb/ttusb-dec/ttusbdecfe.c in the Linux kernel prior to 3.17.4 allows local users to cause a denial of service (system crash) or possibly gain privileges via a large message length in an ioctl call.

RECOMMADATIONS

In conclusion, Waldock.ca needs a lot of help to be secure again. Update all applications, libraries, and dependencies. Contact the web hosting and close nearly all the ports that are open.