Unit 4

1. What Operating System does the website utilise?
2. What web server software is it running?
3. Is it running a CMS (Wordpress, Drupal, etc?)
4. What protection does it have (CDN, Proxy, Firewall?)
5. Where is it hosted?
6. Does it have any open ports? Which did you expect to be open?
7. Does the site have any known vulnerabilities?
8. What versions of software is it using? Are these patched so that they are up to date?

1. Scan whatweb: Apache, Bootstrap (USA)

2. Scan whatweb: HTTPServer: Apache, imunify360-webshield/1.18

3. Scan cmseek: CMS Detection Failed

   Result: No found CMS

4. Firewall scan NMAP:
   Starting Nmap 7.93 (https://nmap.org) at 2023-02-28 05:45 EST
   Nmap scan report for 68.66.247.187.static.a2webhosting.com (68.66.247.187)
   Host is up (0.000030s latency).
   All 1000 scanned ports on 68.66.247.187.static.a2webhosting.com (68.66.247.187) are in ignored states.
   Not shown: 1000 unfiltered tcp ports (reset)

   Result: No firewall

5. scan whois:
   NetName: INTERNET-BLK-A2HOS-13
   NetHandle: NET-68-66-212-0-1
   Parent: NET68 (NET-68-0-0-0-0)
   NetType: Direct Allocation
   OriginAS: AS55293
   Organization: A2 Hosting, Inc. (A2HOS)
   RegDate: 2009-09-01
   Updated: 2020-01-07

   Result: A2 Hosting, Inc.

6. SYN scan NMAP:
   PORT STATE SERVICE
   21/tcp open ftp
   24/tcp filtered priv-mail
   25/tcp open smtp
   53/tcp open domain
   80/tcp open http
   110/tcp open pop3
   143/tcp open imap
   443/tcp open https
   465/tcp open smtps

587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
2525/tcp open ms-v-worlds
3306/tcp open mysql
3389/tcp filtered ms-wbt-server
5432/tcp open postgresql

Result: 14 open ports, 2 filtered

7. Cusory scan ZAPROXY (manual):
   CSRF token missing
   HTTP unencrypted
   Cookies expired

8. scan whatweb: JQuery[1.12.4] uncommon headers: cf-edge-cache; unpatched

Reflection:

1. Did you have any issues or challenges with the scans?
   No challenges; was able to do well. VPN brought the connection to bookacheckup back
2. How did you overcome them?
   Used a VPN, all's good.
3. How will they affect your final report?
   This will add nuance to the mitigations involved.