Assignment-2

Course: Cybersecurity Fundamentals

Semester-1 2019

University of Adelaide

Name: Karan Sethi

Student ID: a1745936

**Answer 1:**

The only file found matching the google search parameters in the question was at -

[www.asx.com.au/asxpdf/20121127/pdf/42bhg7c4937l1m.pdf](http://www.asx.com.au/asxpdf/20121127/pdf/42bhg7c4937l1m.pdf)

* Command used to find sha256 hash

|  |
| --- |
| # sha256sum 42bhg7c4937l1m.pdf |

* Commands used to find author and the creation software of the file

|  |
| --- |
| # sudo apt-get install exiftool # exiftool 42bhg7c4937l1m.pdf |

|  |  |
| --- | --- |
| **Question** | **Answer** |
| Google Search Syntax | site:asx.com.au filetype:pdf intitle:magnetic -drill -rare |
| SHA256 Hash of PDF file | 8e5c7b0837e36e3d28b249633e825658180df0d39657d6162049efe5b4b4d34a |
| PDF author according to metadata | rthomson |
| PDF creation software according to metadata | PDFCreator Version 1.4.1 |

**Answer 2:**

* Commands used to find required info -

|  |
| --- |
| # dig @8.8.8.8 dunstan.org.au any  # dig axfr @ns.adelaide.edu.au dunstan.org.au # whois 129.147.149.1  # dig @8.8.8.8 online-media.adelaide.edu.au any  # dig @8.8.8.8 adelaide.edu.au any  # dig axfr @ns.adelaide.edu.au adelaide.edu.au |

* Websites used -

<https://whois.domaintools.com/129.127.149.1>

<https://hackertarget.com/reverse-ip-lookup/>

<https://ipinfo.io/AS1851>

|  |  |
| --- | --- |
| **dunstan.org.au** resolves to: | 129.127.149.1 |
| Other domain names that resolve to the same address | acvt.com.au  adelaide.edu  adelaide.edu.au  adelaide.university  agbureau.com.au  agsb.adelaide.edu.au  agwine.adelaide.edu.au  ameb.adelaide.edu.au  arch.adelaide.edu.au  architecture.adelaide.edu.au  arcpoh.adelaide.edu.au  arts.adelaide.edu.au  arts-faculty.adelaide.edu.au  asp.adelaide.edu.au  biological.adelaide.edu.au  business.adelaide.edu.au  cats.adelaide.edu.au  chemeng.adelaide.edu.au  commerce.adelaide.edu.au  confucius.adelaide.edu.au  cs.adelaide.edu.au  csermoocs.adelaide.edu.au  dentistry.adelaide.edu.au  dunstan.org.au  ecic.adelaide.edu.au  ecms.adelaide.edu.au  economics.adelaide.edu.au  education.adelaide.edu.au  ees.adelaide.edu.au  elderhall.adelaide.edu.au  eleceng.adelaide.edu.au  emu.adelaide.edu.au  energystorageknowledge.com  gisca.adelaide.edu.au  gsm.adelaide.edu.au  health.adelaide.edu.au  hss.adelaide.edu.au  iibel.adelaide.edu.au  international.adelaide.edu.au  law.adelaide.edu.au  mbs.adelaide.edu.au  mecheng.adelaide.edu.au  media.adelaide.edu.au  molecular-biosciences.adelaide.edu.au  molecularbiosciences.adelaide.edu.au  music.adelaide.edu.au  mycology.adelaide.edu.au  nationalwinecentre.biz  nationalwinecentre.com  nationalwinecentre.com.au  nationalwinecentre.info  nationalwinecentre.net  nationalwinecentre.org  nursing.adelaide.edu.au  online-media.adelaide.edu.au  physiology.adelaide.edu.au  physsci.adelaide.edu.au  plantaccelerator.com  plantaccelerator.net  plantaccelerator.org  plantaccelerator.org.au  psychiatry.adelaide.edu.au  public-health.adelaide.edu.au  publichealth.adelaide.edu.au  science.adelaide.edu.au  sciences.adelaide.edu.au  seek-light.com  seek-light.net  seek-light.org  student.adelaide.edu.au  surgery.adelaide.edu.au  trc.adelaide.edu.au  ua.edu.au  union.adelaide.edu.au  unispace.adelaide.edu.au  usc.adelaide.edu.au  waite.adelaide.edu.au  waite.edu.au  waite-research-precinct.org  water.adelaide.edu.au  wireless.adelaide.edu.au  www.agbureau.com.au  www.plantaccelerator.org.au |
| Owner of the IP address | The University of Adelaide |
| The IP address range which the IP address belongs | 129.127.0.0 - 129.127.255.255 |
| The "AS" number of the same IP range | AS1851 |
| Other netblocks registered under the same ASN | IPv4 Ranges -  **Netblock, Description, Num IPs**[103.37.128.0/22](https://ipinfo.io/AS1851/103.37.128.0/22) The University of Adelaide 1,024  [129.127.0.0/16](https://ipinfo.io/AS1851/129.127.0.0/16) University of Adelaide 65,536  [192.160.71.0/24](https://ipinfo.io/AS1851/192.160.71.0/24) imported inetnum object for UNIVER-31 256  [192.43.227.0/24](https://ipinfo.io/AS1851/192.43.227.0/24) imported inetnum object for UNIVER-31 256  [192.43.228.0/24](https://ipinfo.io/AS1851/192.43.228.0/24) imported inetnum object for UNIVER-31 256  [203.9.156.0/24](https://ipinfo.io/AS1851/203.9.156.0/24) Open Learning Technology Corporation Ltd 256  [43.241.200.0/22](https://ipinfo.io/AS1851/43.241.200.0/22) The University of Adelaide 1,024  IPv6 Ranges -  **Netblock, Description**  [2403:7900::/32](https://ipinfo.io/AS1851/2403:7900::/32) imported inetnum object for UNIVER-31 |

**Answer 3:**

* Lookup search terms in Shodan.io -

asx.com.au

org:"Australian Stock Exchange Limited"

* Lookup search term in exploit-db.com and cve.mitre.org -

CrushFTP

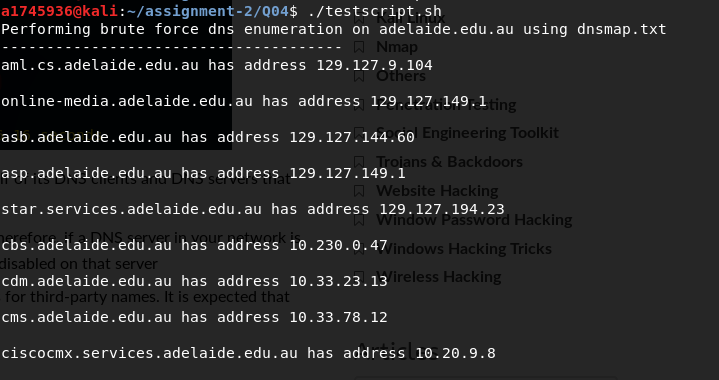
|  |  |
| --- | --- |
| ASN of ASX | AS18361 |
| THere are two IIS7.0 servers running (according to Shodan). What are the IP addresses and common names (CN)? | IP Addresses: 203.15.147.77, 203.15.147.71  Common Name: connect.asxonline.com, rlm.connect.asxonline.com (respectively for IP addresses) |
| There are two SFTP servers running on port 22 according to Shodan. What are the hostnames and name of the FTP server product? | Hostnames:ftp.asx.com.au, ftptest.asx.com.au  Product name: SSH-2.0-CrushFTPSSHD |
| Lookup the product in exploit-db.com. Are there known vulnerabilities for that product?  (copy the title of the one exploit listed) | CrushFTP 7.2.0 - Multiple Vulnerabilities |
| Lookup the product name at <https://cve.mitre.org>. What are some known vulnerabilities for the product (List 3 example CVEs and a short description) | **Name, Description**  CVE-2017-14038 -CrushFTP before 7.8.0 and 8.x before 8.2.0 has a redirect vulnerability.  CVE-2017-14037 - CrushFTP before 7.8.0 and 8.x before 8.2.0 has an HTTP header vulnerability.  CVE-2017-14036 - CrushFTP before 7.8.0 and 8.x before 8.2.0 has XSS. |

**Answer 4:**

The script that was used to enumerate hostnames under a given with an input dictionary -

|  |
| --- |
| #!/bin/bash #This is a script to enumerate hostnames under a given domain along with input dictionary and prints them all into a new file  domain="adelaide.edu.au" map="dnsmap.txt" output="domains.txt" truncate -s 0 $output #empty the file for storing a new DNS enumeration  echo "Performing brute force dns enumeration on $domain using $map" echo "--------------------------------------" cat $map | **while** read word #open dictionary and loop over words to brute-force **do**  #check if output of host command with domain has an address  **if** host $word.$domain | grep "has address"  **then**   ipinfo=$(getent hosts $word.$domain | awk '{ print $1 }')  #print the original domain into a text output file  echo "$word.$domain at address $ipinfo" >> $output  echo  **fi** **done** |
|  |

Some of the output on the terminal was -

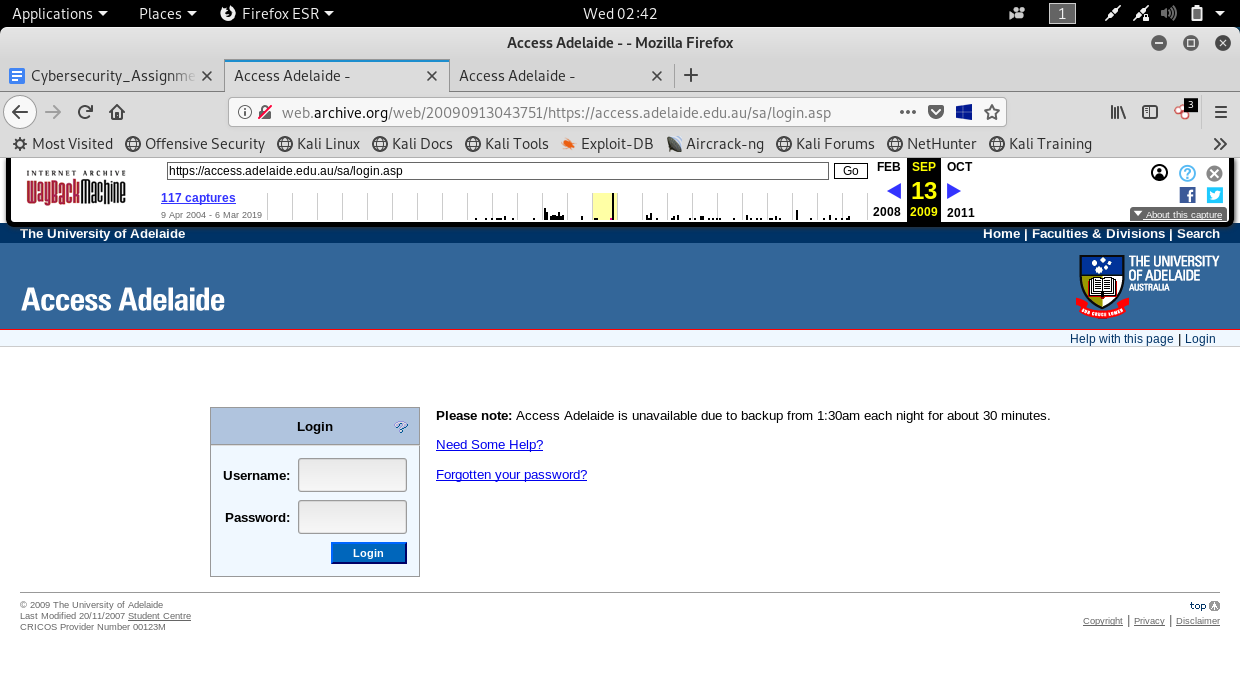


Output in the output file of the script - domains.txt (containing original brute force terms against adelaide.edu.au)

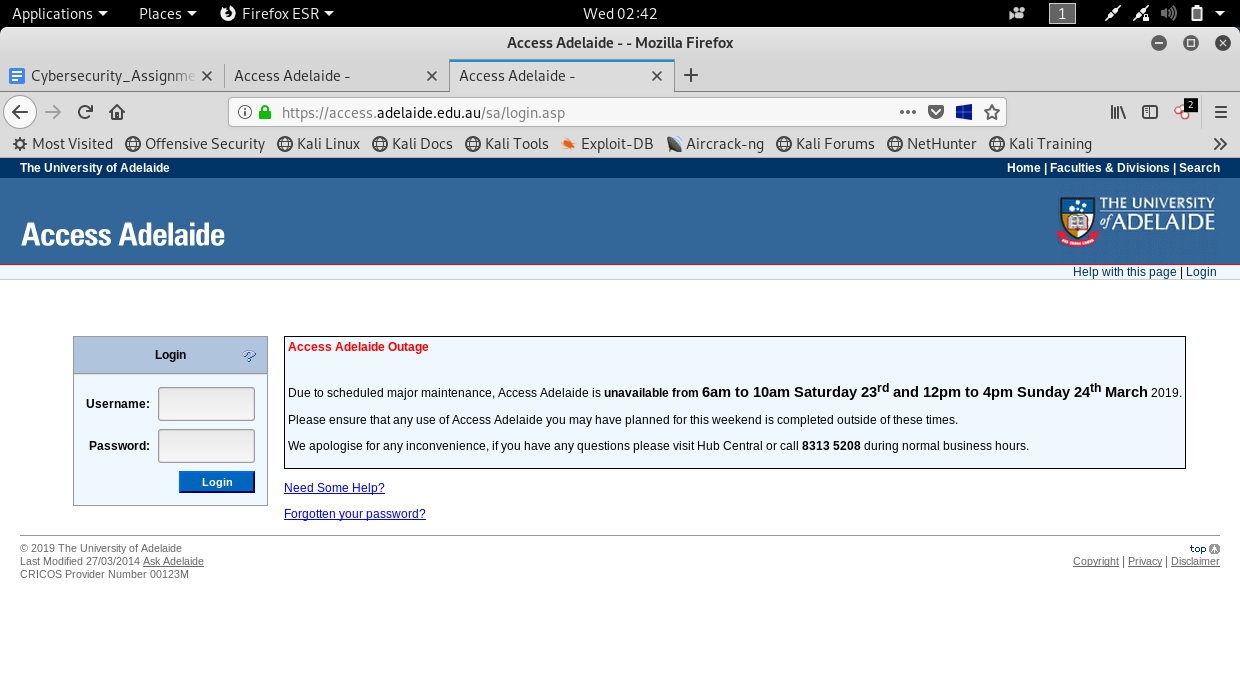
|  |
| --- |
| aml.adelaide.edu.au at address 129.127.9.104 apr.adelaide.edu.au at address 129.127.149.1 asb.adelaide.edu.au at address 129.127.144.60 asp.adelaide.edu.au at address 129.127.149.1 bsl.adelaide.edu.au at address 129.127.194.23 cbs.adelaide.edu.au at address 10.230.0.47 cdm.adelaide.edu.au at address 10.33.23.13 cms.adelaide.edu.au at address 10.33.78.12 cmx.adelaide.edu.au at address 10.20.9.8 cwa.adelaide.edu.au at address 129.127.44.182 edm.adelaide.edu.au at address 54.183.0.47 13.52.43.40 eeg.adelaide.edu.au at address 129.127.149.1 ees.adelaide.edu.au at address 129.127.149.1 eft.adelaide.edu.au at address 129.127.125.210 emu.adelaide.edu.au at address 129.127.149.1 eng.adelaide.edu.au at address 192.43.228.130 era.adelaide.edu.au at address 129.127.149.109 eso.adelaide.edu.au at address 192.43.228.152 faq.adelaide.edu.au at address 129.127.144.9 fcs.adelaide.edu.au at address 129.127.194.26 fin.adelaide.edu.au at address 10.230.0.20 ftp.adelaide.edu.au at address 192.43.228.177 fww.adelaide.edu.au at address 10.30.0.170 git.adelaide.edu.au at address 129.127.43.94 gpo.adelaide.edu.au at address 129.127.40.3 gsm.adelaide.edu.au at address 129.127.149.1 hcm.adelaide.edu.au at address 10.130.4.27 hdb.adelaide.edu.au at address 129.127.43.6 hss.adelaide.edu.au at address 129.127.149.1 iga.adelaide.edu.au at address 129.127.5.159 iit.adelaide.edu.au at address 129.127.149.1 law.adelaide.edu.au at address 129.127.149.1 lib.adelaide.edu.au at address 13.238.150.128 13.237.238.199 52.62.110.129 map.adelaide.edu.au at address 129.127.149.1 mbs.adelaide.edu.au at address 129.127.149.1 mdm.adelaide.edu.au at address 129.127.149.130 ncs.adelaide.edu.au at address 10.33.12.40 nic.adelaide.edu.au at address 129.127.40.3 noc.adelaide.edu.au at address 129.127.43.22 nsm.adelaide.edu.au at address 129.127.239.65 ntp.adelaide.edu.au at address 129.127.40.3 oid.adelaide.edu.au at address 10.33.121.8 omd.adelaide.edu.au at address 10.23.42.30 osb.adelaide.edu.au at address 10.230.0.4 owa.adelaide.edu.au at address 129.127.149.85 pce.adelaide.edu.au at address 129.127.149.94 prm.adelaide.edu.au at address 129.127.149.50 res.adelaide.edu.au at address 129.127.149.109 rqf.adelaide.edu.au at address 192.43.228.199 sch.adelaide.edu.au at address 129.127.149.109 sfc.adelaide.edu.au at address 10.33.76.11 sid.adelaide.edu.au at address 10.33.76.12 sip.adelaide.edu.au at address 129.127.95.143 smc.adelaide.edu.au at address 10.33.76.10 sso.adelaide.edu.au at address 129.127.149.59 svn.adelaide.edu.au at address 10.33.24.15 trc.adelaide.edu.au at address 129.127.149.1 upk.adelaide.edu.au at address 129.127.41.67 urn.adelaide.edu.au at address 10.32.14.4 usc.adelaide.edu.au at address 129.127.149.1 vpn.adelaide.edu.au at address 129.127.45.49 wcs.adelaide.edu.au at address 10.33.12.40 wta.adelaide.edu.au at address 129.127.44.231 www.adelaide.edu.au at address 129.127.149.1 xxx.adelaide.edu.au at address 129.127.102.4 |

**Answer 5:**

Using Wayback machine <http://web.archive.org> for seeing Access Adelaide on September 13 2009 -



Current Access Adelaide -



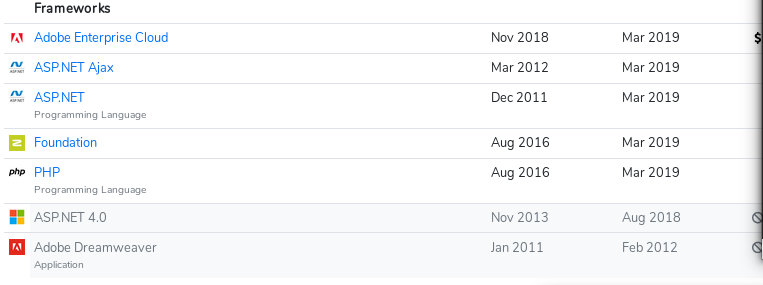
The login pages look almost the same except for some small link differences and page information. As we can see the current access adelaide has a major maintenance outage notice aside the login component.

**Answer 6:**

* Website used -

<https://builtwith.com/detailed/aph.gov.au>

The server-side technologies mainly being used are ASP.NET, ASP.NET Ajax, ZURB Foundation and PHP.



* Browser addon used -

Wappalyzer

