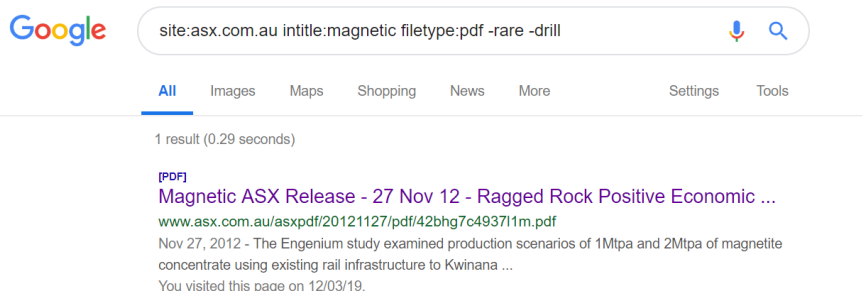


Cybersecurity Fundamentals (CS3308/7308)

Assignment 2 Example Answers

Question 1 (2points)

What is the Google search syntax for finding the PDF file(s) hosted on the Australian Stock Exchange (ASX) website containing the word "**magnetic**" in the title, but without the keywords "drill" or "rare" in the body? Download the file, and find out (a) the author and (b) software used to create the PDF. The tool "exiftool" is a useful tool for extracting file metadata.



```
root@kali:~/Downloads# ls *.pdf
42bhg7c49371m.pdf
root@kali:~/Downloads# sha256sum 42bhg7c49371m.pdf
8e5c7b0837e36e3d28b249633e825658180df0d39657d6162049efe5b4b4d34a 42bhg7c49371m.pdf
root@kali:~/Downloads#
```

- apt install exiftool to install exiftool, as it is not installed by default in Kali

```
root@kali:~/Downloads# exiftool 42bhg7c49371m.pdf
ExifTool Version Number      : 11.16
File Name                    : 42bhg7c49371m.pdf
Directory                   : .
File Size                    : 1292 kB
File Modification Date/Time  : 2019:03:29 07:46:08+04:00
File Access Date/Time       : 2019:03:29 07:46:30+04:00
File Inode Change Date/Time  : 2019:03:29 07:46:08+04:00
File Permissions             : rw-r--r--
File Type                   : PDF
File Type Extension         : pdf
MIME Type                   : application/pdf
PDF Version                 : 1.5
Linearized                  : Yes
Encryption                  : Standard V1.2 (40-bit)
User Access                 : Print, Fill forms, Extract, Asse
Author                     : rthomson
Create Date                 : 2012:11:27 18:14:48+11:00
Modify Date                 : 2012:11:27 18:14:48+11:00
Subject                     :
XMP Toolkit                 : 3.1-701
Producer                   : GPL Ghostscript 9.05
Keywords                    :
Creator Tool                 : PDFCreator Version 1.4.1
Title                      : Magnetic ASX Release - 27 Nov 12
Economic Result             :
Creator                    : rthomson
Description                 :
Page Layout                 : SinglePage
Page Mode                   : UseNone
Page Count                  : 3
```

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

Question 2 (2 points)

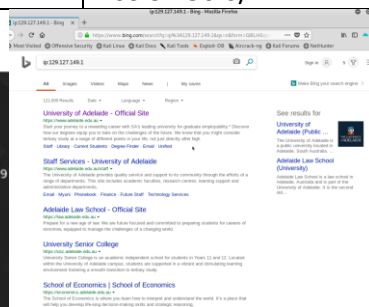
"Revers DNS lookup" usually refers to the PTR record on a DNS server. However, multiple host names (domain names) can resolve to a single IP address. This is typical in a shared hosting site. "Reverse IP lookup" relies on database of crawled websites to identify multiple hosts that resolve to the same address. For example, the Bing "ip:" search modifier can list domain names that resolve to the same address and there are other online services that can do the same.

Question	Answer
unstan.org.au resolves to:	129.127.149.1
Other domain names that resolve to the same address	law.adelaide.edu.au usc.adelaide.edu.au arts.adelaide.edu.au etc
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 (or 129.127.0.0/16)
The "AS" number of the same IP range	ASN1851
Other netblocks registered under the same ASN	43.241.200.0/22 103.37.128.0/22 129.127.0.0/16 192.43.227.0/24 192.43.228.0/24 192.160.71.0/24 203.9.156.0/24

```

root@kali:~# dig dunstan.org.au a
<>> Dig 9.11.5-P1-1-Debian <>> dunstan.org.au a
;; global options: +cmd
;; Got answer:
;;->HEADER<-- opcode: QUERY, status: NOERROR, id: 45273
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dunstan.org.au.                IN      A
;; ANSWER SECTION:
dunstan.org.au.                78291   IN      A      129.127.149.1

```



```

% [whois.apnic.net]
% Whois data copyright terms http://www.apnic.net/db/dbcopyright
% Information related to '129.127.0.0 - 129.127.255.255'
% Abuse contact for '129.127.0.0 - 129.127.255.255' is 'abuse@adelaide.edu.au'

inetnum:        129.127.0.0 - 129.127.255.255
netname:        ADELAIDE
descr:          University of Adelaide
country:        AU
org:             ORG-TU0A1-AP
admin-c:        UN21-AP
tech-c:         UN21-AP
status:         ALLOCATED PORTABLE
remarks:        This object was transferred from ARIN database
                on 11 December 2002
mnt-by:         APNIC-HM
mnt-lower:      MAINT-AU-UOFA
mnt-irt:        IRT-UOFANET-AP-AU
last-modified:  2017-10-30T13:01:55Z
source:         APNIC

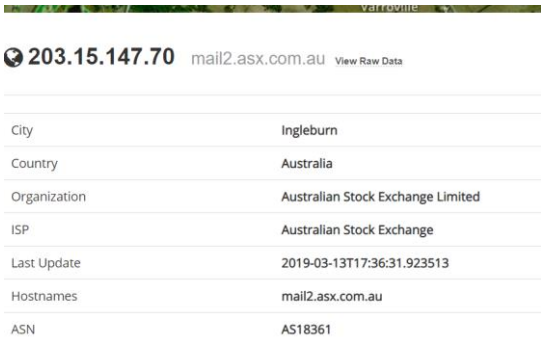
```

ASN	AS Name	CCIR Range
1851	The University of Adelaide	43.241.200.0/22
1851	The University of Adelaide	103.37.128.0/22
1851	The University of Adelaide	129.127.0.0/16
1851	The University of Adelaide	192.43.227.0/24
1851	The University of Adelaide	192.43.228.0/24
1851	The University of Adelaide	192.160.71.0/24
1851	The University of Adelaide	203.9.156.0/24

Question 3

Create a free account on shodan.io (<https://shodan.io> (Links to an external site.))Links to an external site.). You will be entitled to an academic upgrade if you register using your @student.adelaide.edu.au or @adelaide.edu.au account. Learn a bit about the Shodan search modifiers, similar to the Google ones (e.g., see here (Links to an external site.))Links to an external site.). Search for information on

hosts under "Australian Stock Exchange" and answer the following questions. Start with the "org:" modifier.

Question	Answer														
What is the ASN of ASX?	<p>Search by org:"Australian Stock Exchange" then click on any IP AS18361</p>  <p>203.15.147.70 mail2.asx.com.au View Raw Data</p> <table border="1"> <tr><td>City</td><td>Ingleburn</td></tr> <tr><td>Country</td><td>Australia</td></tr> <tr><td>Organization</td><td>Australian Stock Exchange Limited</td></tr> <tr><td>ISP</td><td>Australian Stock Exchange</td></tr> <tr><td>Last Update</td><td>2019-03-13T17:36:31.923513</td></tr> <tr><td>Hostnames</td><td>mail2.asx.com.au</td></tr> <tr><td>ASN</td><td>AS18361</td></tr> </table>	City	Ingleburn	Country	Australia	Organization	Australian Stock Exchange Limited	ISP	Australian Stock Exchange	Last Update	2019-03-13T17:36:31.923513	Hostnames	mail2.asx.com.au	ASN	AS18361
City	Ingleburn														
Country	Australia														
Organization	Australian Stock Exchange Limited														
ISP	Australian Stock Exchange														
Last Update	2019-03-13T17:36:31.923513														
Hostnames	mail2.asx.com.au														
ASN	AS18361														
There is an IIS7.0 server running. What is the IP address and the common name (CN)?	203.15.147.77 (or 203.15.147.71) connect.asxonline.com														
There is an SFTP server running on port 22. What is the hostname and the name of the FTP server product?	SSH-2.0-CrushFTPSSHD 203.15.145.110 ftp.asx.com.au														
Lookup the product in exploit-db.com. Are there known vulnerabilities for that product?	CrushFTP 7.2.0 - Multiple Vulnerabilities https://www.exploit-db.com/exploits/36126 Some XSS on the web interface														
Similarly, lookup the product name at https://cve.mitre.org What are some of the known vulnerabilities for this product?	<p>Search Results</p> <p>There are 5 CVE entries that match your search.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>CVE-2017-14038</td> <td>CrushFTP before 7.8.0 and 8.x before 8.2.0 has a redirect vulnerability.</td> </tr> <tr> <td>CVE-2017-14037</td> <td>CrushFTP before 7.8.0 and 8.x before 8.2.0 has an HTTP header vulnerability.</td> </tr> <tr> <td>CVE-2017-14036</td> <td>CrushFTP before 7.8.0 and 8.x before 8.2.0 has XSS.</td> </tr> <tr> <td>CVE-2017-14035</td> <td>CrushFTP 8.x before 8.2.0 has a serialization vulnerability.</td> </tr> <tr> <td>CVE-2001-0582</td> <td>Ben Spink CrushFTP FTP Server 2.1.6 and earlier allows a local attacker to access arbitrary files via</td> </tr> </tbody> </table>	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.	CVE-2017-14035	CrushFTP 8.x before 8.2.0 has a serialization vulnerability.	CVE-2001-0582	Ben Spink CrushFTP FTP Server 2.1.6 and earlier allows a local attacker to access arbitrary files via		
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.														
CVE-2017-14035	CrushFTP 8.x before 8.2.0 has a serialization vulnerability.														
CVE-2001-0582	Ben Spink CrushFTP FTP Server 2.1.6 and earlier allows a local attacker to access arbitrary files via														

Question 3

Write a simple DNS brute-force script in your language of choice to enumerate hostnames under a given domain and an input dictionary. Run the code against adelaide.edu.au using the dictionary file located at /usr/share/wordlists/dnsmap.txt in Kali (this file contains the entire 3-character permutations). Running the whole list will take a long time, so you can stop after a few minutes. Paste some preliminary results.

Example Script

```
#!/usr/bin/env python3
import socket, sys
socket.setdefaulttimeout(0.1)
```

```
f = open(sys.argv[2], "r")
for word in f:
    host = word.strip() + "." + sys.argv[1].strip()
    try:
        ip = socket.gethostbyname(host)
        print(host + " (" + ip + ")")
    except:
        pass
```

```
root@kali:~# python3 dns_brut.py adelaide.edu.au /usr/share/wordlists/dnsmap.txt
aml.adelaide.edu.au (129.127.9.104)
apr.adelaide.edu.au (129.127.149.1)
asb.adelaide.edu.au (129.127.144.60)
asp.adelaide.edu.au (129.127.149.1)
bsl.adelaide.edu.au (129.127.194.23)
cas.adelaide.edu.au (10.130.4.81)
cbs.adelaide.edu.au (10.230.0.47)
cdm.adelaide.edu.au (10.33.23.13)
```

Example Script 2

```
#!/bin/bash
domain="adelaide.edu.au"
wordlist="/usr/share/wordlists/dnsmap.txt"
cat $wordlist | while read prefix; do
    host=${prefix}.${domain}
    getent hosts $host
done
```

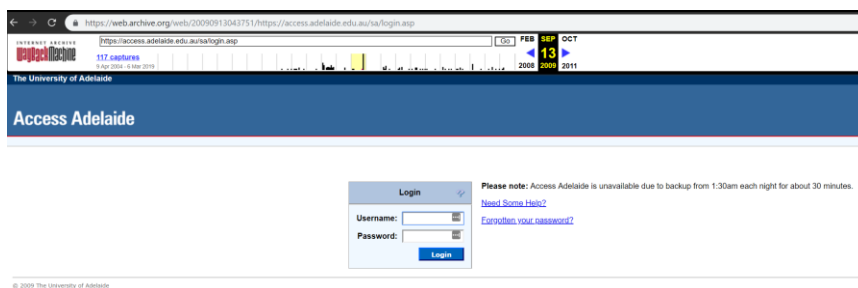
Example Script 3

```
#!/bin/bash
domain="adelaide.edu.au"
wordlist="/usr/share/wordlists/dnsmap.txt"
cat $wordlist | while read prefix; do
    host=${prefix}.${domain}
    dig +short $host
done
```

Question 4

Use the Wayback Machine to find out how Access Adelaide (access.adelaide.edu.au) looked like 10 years ago, in 2009. How does it look compared to the current Access Adelaide?

Access Adelaide has not changed in the last 10 years.



Question 5

What is the server-side technology (Node.js, Apache Tomcat, Cold Fusion, etc) used on the website of the Australian Parliament House (www.aph.gov.au)?

Using Wapplyzer, the Australian Parliament House website appears to be running IIS + ASP.NET.

