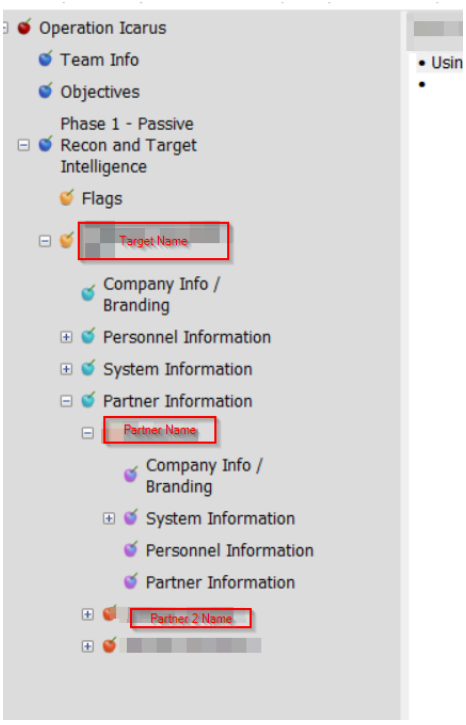
So this is a walkthrough I put together for what I did in Phase 1. Remember, this is a walkthrough from someone with several years of Sysadmin and Helpdesk experience, but has never done any sort of CTF, or engagement anything close to this. Just going through things I think are important. I don't claim this to be the best way (not by a longshot) and I'm sure there are several things I miss and gloss over, while having other things I look in to for way too much detail.

Anyhow, I wanted to post this to give an idea on the way I approached this operation, not only to help myself with any welcomed feedback, but to help others in any spots they may have gotten stuck, or some unconventional lines of thought they may not have had.

Sorry, but this is a short novel :)

Day 0, setup ahead of time:

1. Organization of information is key. If you gather information but can't find it later, you may as well not have gathered it at all. Because of this, it was important for me to think about how to do this ahead of time.
    a. For me, a hierarchical note-taking app that can support images and linking to other sections was important. As such, I settled on CherryTree, a free, open-source program, available on windows, linux, and mac that is updated regularly. (https://www.giuspen.com/cherrytree/)
    b. I then put together a summary page of the mission objectives, my teammates info, and mapped out sections for info on the operation. As the op ensued, I added sections in this hierarchical format. This makes it super easy to dig down to a specific piece of information for the company, and within the notes, link back to the other sections when mentioned.

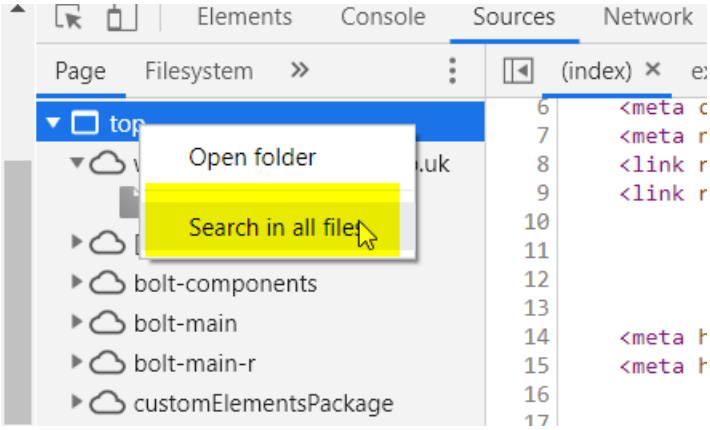
c. 

d. With this foundation set, I can then move on to the actual information collection.

Day 1:

1. The first thing I did after this operation went live and I read through the assignment was navigate directly to the target website, using the domain name in the given email address.
    a. From here I gathered all the obvious relevant info:
        i. Services, CEO info, contact info, address, partners, etc.
        ii. I also have the "Wappalyzer" plugin, this gives us more info about what services the site is running. Document all of this
2. I then navigated around going to all available links and doing the same from each page
    a. My first "discovery" was the ToDo/Admin link at the bottom of the page
        i. Take a screenshot of this page, as it's possible it could be patched at any moment and become no longer available. This information could prove to be very useful later.
            1. Just an aside, I use greenshot (https://getgreenshot.org/) for screenshots. It is free. It basically takes over your printscreen button, and lets you select a place to screenshot, then gives you tons of options in the editor including obfuscation and highlighting which are obviously very useful when using these screenshots for sharing sensitive and important info.
        ii. We find some decent info here, a new service coming up, a new partner, the fact that they are likely moving from Wix to WordPress, and the name and alias of the web admin.
    b. Home, Services, About, and Partners all link to the same page, just pops you around to different sections, nothing to see here
    c. Partner sections take us to their respective sites – will visit this later

    d. Twitter link as well – again will visit this later
3. Ok, obvious info on the target site has been gathered. Now let's take a brief look at the source code for anything glaring.
    a. Simple way to do this, at least in Chrome on Windows – hit F12
    b. From here let's see if anything sticks out. Search all the code for some things that might stick out – keywords here, 'password', 'username', 'admin', and because of the 'hint' document to start us off, indicating that there are flags available with a specific string, 'found flag'.
        i. In chrome, searching all is easy, right click the "top" element on the "sources" tab and select "Search in all files"



        ii. Nothing really sticks out to me at this point, but I don't know much HTML. Since nothing obvious I'll return to this later after discussing with my teammates.
4. Last thing to check on initial pass of the website, any other pages available.
    a. Google fu "site:philmansecurityinc.co.uk" – shows us just the home and /admin, nothing else sticking out.
5. Moving on, let's go to the company Twitter
    a. From here, check out the bio, users followed, users following, likes, and of course tweets.
        i. We find that they are following one of their employees -- the web admin we discovered earlier, so we'll check him out after we finish up here.
        ii. Their tweets give us a little bit of info, a new partner will be launched (which we learned about already), and that the CEO will be doing an interview released next week. Time to set a reminder to check that out
    b. OK, moving on to this web admin
        i. Bio confirms he's the web admin for target, and his location
        ii. Tweet states that he's going to be moving to AWS and away from Wix, corroborating info we found earlier, and giving a new piece of info.
        iii. His following and followers are a bit more scattered, but this info is definitely useful – we know some hobbies and possible ways in if we want to try social engineering later.
6. Partner Site 1 – blackarch
    a. Same as with the target, gather the obvious – services, contacts, partners, other links, etc.
        i. We confirm the partnership with the target, and what the partnership is for

    b. Check source code, again nothing glaring sticking out at this time.
    c. Google fu – shows us the home page and privacy policy. – check privacy policy page, again nothing worthy of keeping shows up currently.
7. Partner Site 2 – Dickson
    a. Site is down, but we have a contact email and a date that they will be back up.
    b. Check source code – good discovery here, and it's obvious, our first flag finding!
    c. Nothing else around, google fu doesn't even find this website

OK – so in my opinion that wraps up the "obvious" stuff. Not to throw shade or make you feel down for not finding any of these pieces, but this is everything I feel was right in front of our faces by just clicking around. Now, let's get a little deeper.

8. WhoIs lookups on each of the sites:
    a. We get registrar, location, registered dates, expiry dates, and nameservers for each site.
9. DNS Lookups
    a. The first tool I used didn't get me all of the info, so I'll just mention the last tool I used, which got me the most information -- https://hackertarget.com/dns-lookup/
    b. We get the IP address, A-records, AAAA-records, Name servers, SOA, MX records, and TXT records – this leads us to our next flag finding!
        i. Other DNS lookup tools I used didn't display the TXT records, so while I had the other info at first, I didn't find the flag until revisiting this info on a later date.

Day 2:

1. Let's try to gather some more info by reaching out to our contact information
    a. Email all current available email addresses, just a blank email to see if any autoresponders are up
        i. Ping – we get another employee name and find an autoresponder for our target
        ii. This autoresponder also has a ".onmicrosoft.com" address, indicating O365 is the system they are using.
    b. Let's also call any available phone numbers
        i. Nothing found here, they aren't real for the op, but I feel this could be important as you find out if there's an answering service, a directory listing, direct to a receptionist, etc.
2. Recheck all sites, twitter for any obvious updates
3. Let's try and look up anything on the secret service from our target "BlackFall"
    a. No other mentions in the source code
    b. A google search also returns nothing relevant
4. Let's try and lookup the new partner "Zar"
    a. Again no other mentions, no new findings here.
5. OK – I feel like I'm hitting a wall today. After some more google searches and other social media searches I'm not finding anything.

Day 3:

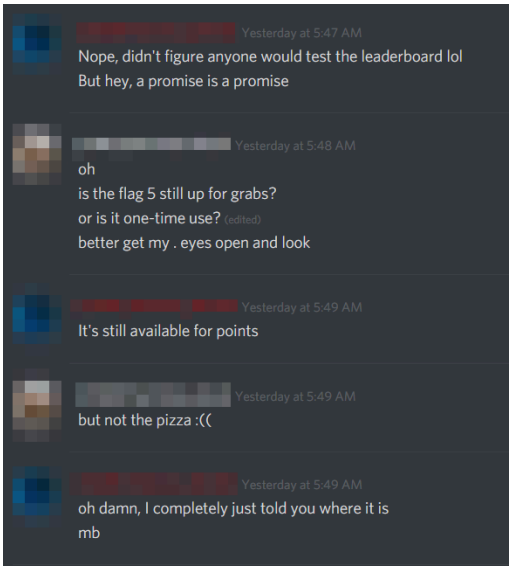
1. New Day – New info!
    a. After checking twitter we find out about a new employee, and get her blog post this could be juicy!

2. Check the blog and anywhere it leads us
    a. Yep – we weren't wrong, this is juicy! Scouring all of the blog posts and blogger profile we find several pieces of info:
        i. We get new employees company email, and as such the naming scheme the company is likely using for all employee emails, so now we have the CEO, web admin, and support person emails as well through inference
        ii. We get some info about the employee herself, where she went to university, her major, and title
        iii. We find out that "Zach" and "Dave" are mentoring her, likely meaning these are two more employees at our target.
        iv. We find a github for this employee, which leads us to our next flag finding! (woohoo)
3. Let's check everything again for updates (website, partner sites, twitter)
    a. Nothing else new glaring out at us
4. At this point I met with my team and we shared a few findings. Oh man, I was missing an obvious technique, how can I be so dumb! I hadn't tried googling any people yet!
    a. Form here we find a linkedIn profile for the CEO. This profile had been removed, but we at least get a location from the google blurb. I can't seem to find anything more from here, but have a feeling there's more info to be had
        i. I check wayback machine but not finding anything.

This felt like a productive day, feeling good so far!

Day 4:

1. After my initial checks for updates I'm not finding anything new. Let's fire up burpsuite and see if there's anything out there.
    a. Disclaimer: the only experience I have with burpsuite is about 1 hour of watching videos on it in the last week or so, so I know this likely isn't the most "efficient" or "thorough" way to use it.
    b. Anyhow, let's put it up and navigate to the target and partner sites. Check out the "http history" tab after doing so, and start parsing through the responses to see if anything good pops up.
        i. As I'm not even sure what to look for here, I'm not finding anything.
        ii. A-Ha a discord chat slip-up (or hint) from our assignee! Let's go over to the leaderboard

1. 

iii. A response message in burp when visiting the leaderboard gives us another flag! Excellent.

This is all I found today, but a good find nonetheless. I also want to mention at this point, knowing we had a CTF style thing going on and we were in the public domain, in my search for flags (as I'm not sure how many are out there at this point, but have found 1, 2, 3, and 5, so I know there is a 4) I decide to do a little google-fu and do a Google search for "found flag" and limit the scope to a time period about a week before the start of the operation. I did find flag 5 a second time using this method, but nothing new. I just want to point this out, because if you have other information (like you know something happened within the last week) you can target your search a bit better. It feels like a cheesy way to find this flag, but hey, whatever works to get you the intel you need, right?

As I didn't continue this walkthrough while the operation was ongoing and it's been a few weeks since the end of it, I'm going to finish the walkthrough by just going through the rest of the items that I have found, and list what I did to find them.

The Flags:

- Flag 1 – Hint = DNS – Found via DNS TXT record for dicksonunited.co.uk, using https://hackertarget.com/dnslookup
- Flag 2 – Hint = Code – Located on Sammie Woods' GitHub page in her code for "Disrupt0r" – link was on Sammie's blog
- Flag 3 – Hint = HTML – located in source code for home page of dicksonunited.co.uk
- Flag 4 – Hint = Social Media – Located in the bio for @hexgroup12 twitter account. Code was written in hex, so needed to be decoded
- Flag 5 – Hint = No one will find this – Found using burp suite visiting the Operation Icarus leaderboard page. Navigating to the page while capturing the responses via burp showed the flag. Alternative way was using a google search for the text "found flag" with a targeted time stamp of the time the operation was going on.
- Flag 6 – Hint = Accounts – Did not find
- Flag 7 – Hint = Leak – When Hexgroup announced their breach, they had a pastebin page posted. At first this only included the credentials leaked, however checking back closer toward the end of the operation the pastebin was modified and contained the flag in the post.
- Flag 8 – Hint = Investigation – Did not find

Info on Philman Security Inc.

Company Info / Branding

• Services:
◇ Internal Pen Tests (target website)
◇ External Pen Tests (target website)
◇ Incident Response (target website)
◇ BlackFall -- new unidentified service (target website /admin page)

• Known Emails:
◇ contact@philmansecurityinc.co.uk (target website)
◇ support@philmansecurityinc.co.uk (given in assignment)
◇ sammiewoods@philmansecurityinc.co.uk (sammie woods blog)
◇ johnfiddler@philmansecurityinc.co.uk (inferred from naming convention on sammie's email)
◇ jackflemming@philmansecurityinc.co.uk (inferred from naming convention on sammie's email)
◇ carolspears@philmansecurityinc.co.uk (inferred from naming convention on sammie's email)
◇ BenjaminGoddard@PhilmanSecurityInc.co.uk | @Th3StrongF0xOnionP4rade! // (DICKSON UNITED breach, pastebin)

• Address:
◇ 100 Fake St, London, UK (target website)

• Number of Employees - 6 (target website)

• Social Media Presence
◇ Twitter - @philmanSecurity (target website)

• Partners
◇ BlackArch
▪ BlackArch provides Incident Response resources for philman (target website)
◇ Dickson United
▪ Dickson provides hardware for philman (target website)

• Notes
◇ acquiring Zarath Industries (was on /admin page of target website, later announced via twitter)
▪ digital forensics services (twitter announcement)
◇ Founded in 2018 – (CEO Interview)
◇ Looking to hire more people soon, growing team (twitter)

Personnel Information

- 6 Total employees (target website)
- Jack Flemming – CEO (target website)

    - Email – jackflemming@philmansecurityinc.co.uk (inferred from other email formats)
    - Located in Exeter, UK (google search > linkedIn blurb)
    - 41 years old (interview)
    - Believes hexgroup12 is led by former disgruntled employee (interview)
- John Fiddler – Web admin (twitter bio, posts, /admin page of target website)
    - johnfiddler@philmansecurityinc.co.uk (inferred from email format)
    - UK based (twitter bio)
    - Moving website from WIX to AWS, likely to use wordpress (target website /admin page, twitter post)
    - Interested in gaming (twitter follows and posts)
- Carol Spears – Support & Relations (auto-reply from support@philmansecurityinc.co.uk)
    - carolspears@philmansecurityinc.co.uk (inferred from email format)
- Sammie Woods – Junior Pen Tester (target twitter, blog post)
    - sammiewoods@philmansecuritying.co.uk (sammie's blog)
    - Blogs at https://sammiewoodsec.blogspot.com (target twitter)
    - Github repo https://github.com/sammiewoodsec (sammie's blog)
    - Attended Plymouth University, degree in cyber security and forensics (sammie's blog)
- Zach ? – Unknown (mentioned as mentor in sammie's blog)
- Dave ? – Unknown (mentioned as mentor in sammie's blog)
- Benjamin Goddard (hexgroup12 breach)
    - benjamingoddard@philmansecurityinc.co.uk / @Th3StrongF0xOnionP4rade! (pastebin from hexgroup12)

System Information

- Uses MySQL internally (CEO interview)
- Website
    - Moving from Wix to AWS for main site (web admin twitter)
    - Moving to self hosted wordpress (note in /admin page of target site)
    - JavaScript Framework (wappalyzer)
    - IP 23.236.62.147 (lookup)

DNS Info:
philmansecurityinc.co.uk. 3599 IN A 23.236.62.147
philmansecurityinc.co.uk. 21599 IN NS ns12.wixdns.net.
philmansecurityinc.co.uk. 21599 IN NS ns13.wixdns.net.
philmansecurityinc.co.uk. 3599 IN SOA ns12.wixdns.net. support.wix.com. 2019062410 10800 3600 604800 3600
philmansecurityinc.co.uk. 3599 IN MX 0 philmansecurityinc-co-uk.mail.protection.outlook.com.

WhoIS Lookup:
Domain name:
philmansecurityinc.co.uk

Data validation:
Nominet was able to match the registrant's name and address against a 3rd party data source on 30-May-2019

Registrar:
GoDaddy.com, LLP. [Tag = GODADDY]
URL: http://uk.godaddy.com

Relevant dates:
Registered on: 30-May-2019
Expiry date: 30-May-2020
Last updated: 24-Jun-2019

Registration status:
Registered until expiry date.

Name servers:
ns12.wixdns.net
ns13.wixdns.net

WHOIS lookup made at 16:12:27 01-Jul-2019

-
- Philman Certificate CA: Portswigger CA - Page info - certificate details philmansecurityinc.co.uk
- Philman Certificate Signature Algorithm: PKCS #1 SHA-256 with RSA Encryption - Page info - certificate details philmansecurityinc.co.uk
- Philman Public Key Algorithm - PKCS #1 RSA Encryption - Page info - certificate details philmansecurityinc.co.uk

- Email Server
  - Using O365 (auto response from an @onmicrosoft.com domain name)

Partner Information

BlackArch

Company Info / Branding

- Services:
  - Network Security (partner website)
  - IT Support (partner website)
  - Incident Response (partner website)
- Known Emails:
  - enquiries@basolutions.com (partner website)
  - clientsupport@basolutions.com (partner website)
- Phone – 206-134-5678 (partner website)
- Hours of Operation
  - M-F 9AM – 5PM, closed Sat/Sun (partner website)
- Partners with Philman, providing Incident Response services (partner website)

System Information

- Blackarchsolutions.com (target website)
- Website powered by GoDaddy (bottom of website)
  - IP – 198.71.232.3 (lookup)

DNS Info:
blackarchsolutions.com. 599 IN A 198.71.232.3
blackarchsolutions.com. 3599 IN NS ns39.domaincontrol.com.
blackarchsolutions.com. 3599 IN NS ns40.domaincontrol.com.
blackarchsolutions.com. 3599 IN SOA ns39.domaincontrol.com. dns.jomax.net. 2019070101 28800 7200 604800 600

▸ WhoIs Lookup:

Domain Name: BLACKARCHSOLUTIONS.COM
Registry Domain ID: 2398296408_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-06-03T18:32:32Z
Creation Date: 2019-06-03T18:32:31Z
Registry Expiry Date: 2020-06-03T18:32:31Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS39.DOMAINCONTROL.COM
Name Server: NS40.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2019-07-04T02:06:23Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

  - NOTICE: The expiration date displayed in this record is the date the
  - Blackarch Certificate CA: Portswigger CA - Page info - certificate details blackarchsolutions.com
  - Blackarch Certificate Signature Algorithm: PKCS #1 SHA-256 with RSA Encryption - Page info - certificate details blackarchsolutions.com

- Blackarch Public Key Algorithm - PKCS #1 RSA Encryption - Page info - certificate details blackarchsolutions.com

Dickson United

Company Info / Branding

- Provides Hardware Solutions (philman website)
- Known Emails
  - Inquiry@dicksonunited.co.uk (from Dickson website)
  - Security@dicksonunited.co.uk (Dickson website)
  - From Breach:

  - Located in London, England (twitter bio)
  - Social Media:
    - Twitter Handle @dicksonunited (website, philman twitter)
  - Partners with Philman, providing hardware support (philman website)

System Information

- Website hosted on AWS (shown on website error pages)
- IP – 52.95.150.11 (lookup)

DNS Info:

```
dicksonunited.co.uk.   4   IN A   52.95.148.39
dicksonunited.co.uk.   21599   IN NS ns-1144.awsdns-15.org.
dicksonunited.co.uk.   21599   IN NS ns-1930.awsdns-49.co.uk.
dicksonunited.co.uk.   21599   IN NS ns-346.awsdns-43.com.
dicksonunited.co.uk.   21599   IN NS ns-993.awsdns-60.net.
dicksonunited.co.uk.   899   IN SOA   ns-1930.awsdns-49.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
dicksonunited.co.uk.   299   IN TXT   "You've Found Flag One! PGQGFJCNALVLA"
```

- WhoIs lookup:

  Domain name:
  dicksonunited.co.uk

  Data validation:
  Nominet was able to match the registrant's name and address against a 3rd party data source on 30-May-2019

  Registrar:
  GoDaddy.com, LLP. [Tag = GODADDY]
  URL: http://uk.godaddy.com

  Relevant dates:
  Registered on: 03-Jun-2019
  Expiry date: 03-Jun-2020
  Last updated: 27-Jun-2019

  Registration status:
  Registered until expiry date.

  Name servers:
  ns-1144.awsdns-15.org
  ns-1930.awsdns-49.co.uk 205.251.199.138
  ns-346.awsdns-43.com
  ns-993.awsdns-60.net

  WHOIS lookup made at 03:04:50 04-Jul-2019

-

Other Notes

- Data breach occurred, affecting internal servers containing contract details, email addresses, and remote support credentials (Dickson twitter 7/6)
- Acknowledges Hexgroup12 pastebin data is real and accurate, forced users to reset passwords (twitter, 7/9)
- States investigation concluded and backdoor was closed. Breach started by a phish (twitter)

Zarath Industries

Company Info / Branding

- Services – Digital Forensics (philman twitter)
- Acquired by Philman (philman twitter)

Other Info

HexGroup12

- Twitter handle @hexgroup12 (found via twitter search related to philman)
- Claims responsibility for dicksonunited breach, claims have all databases and demand bitcoin (twitter)
- Threatens philman, implying ‘they know why’ (twitter)
- https://pastebin.com/fu0grFxW
- Leader – Jack Williams (philman ceo interview/twitter)
    - Former employee of Philman (philman ceo interview)
    - Fired for negligence and misconduct (philman ceo interview)
- Members arrested for breaking laws including Computer Misuse Act and Data protection act (philman twitter)