Phase 1: OSINT Reconnaissance

Social Media

Find a corporate web presence for the target, then see what employees are being tagged in their posts. Alternatively or in addition, search on Facebook, Instagram, Twitter, etc. for individual employees. If they have public profiles, there is likely a lot of information that can be gleaned from them, such as answers to security questions like pet names, birthdays, parents' given names, or elementary school names. This type of information could also be used for targeted spearphishing campaigns.

Search Engines

Search engines are particularly useful for performing reconnaissance on a target. There are specialized search engines, such as Shodan, which allows you to search through all Internet-exposed devices, such as security webcams and IoT devices. Internet-accessible security cameras are a boon to a reconnaissance operation, in varying ways depending on what the end goal is, especially because they often are protected with default credentials that are easy to look up, or even no credentials at all. As an example, a camera facing towards the door of the building will show employees and visitors coming and going, so after a few days of surveillance you could figure out when the building is empty or when it's expected for maintenance staff to be coming and going. A camera within the workplace might show the screens and keyboard of office employees, so you could watch someone typing in their password to log in every morning, and if the camera is high quality or physically close enough, you may be able to determine what letters they are typing and therefore what their password is. The Google search engine allows you to find similar information as Shodan, as well as other information, by using Google Dorks, searches with specialized syntax to hone a search to locate difficult-to-find information on the Internet. For instance, if you know a certain employee attended some conference the previous year, you could search for that conference and hone results to PowerPoint presentation files to find that person's published slide deck for the talk they gave. More often than not, these presentations will contain contact information for the speaker, frequently an email address,

which can then be used for spearphishing emails or other social engineering attacks, or use it as a username in an account compromise attack.

Job Boards

Go onto job boards such as LinkedIn or Indeed to look at tech job postings at the company and see which technologies they're looking for. For example, if the software developer postings are looking for .NET fluency, there is a good chance the company's servers are either self-hosted or Azure-based. Additionally, job postings often have the name and contact information, such as email address, for the hiring manager, which can be used for a spearphishing attack or tried out as a username in an account compromise attempt.

Company Research

For company research, the goal is ultimately to find out as much as possible about the specific company, its structure, its organization, etc. to enable you to draw informed conclusions about the best avenue of exploitation. The OSINT Framework is a good starting point, and sites like ZoomInfo will enable you to find out company details such as number of employees, number and location of offices, and so on. Google Maps satellite and street views can be used to determine the physical locations of the buildings and see which buildings look like office buildings, warehouses, etc. The company's website itself will be invaluable for this as well, as they often list the location of their headquarters office building for contact purposes.

Domain and IP Research

Websites and tools such as nslookup, whois.net or other whois services, traceroute, and ping can give you a lot of information about the company's servers, domain registration, and so on. Although less obvious, search engines like Google (using Google Dorks) and Shodan may also be useful for this. IBM X-Force can help you identify the Internet Service Provider (ISP) being used, from which you can significantly narrow down what hardware devices they have on premises (such as which router they use). Once you know the router type, it is easy to use a search engine like Google to find the default credentials for that router. Many users never change the default credentials when they set up a new router, perhaps unaware that these credentials are universal for their router type, so there is a decent chance that these credentials will work.

Pastebins

Pastebins, such as GitHub, JSFiddle, PrivateBin, ControlC, Hackology's pastebin, or the original PasteBin, sometimes have sets of previously compromised user credentials that haven't been changed. Even if the passwords have been changed, usernames generally are never changed, so you could use those in a password spraying attack.