# Capstone Project: Phase 1: Perform Reconnaissance - Winton Fong

2-3 page description of all the tools and methods you’ll use to perform reconnaissance

Goal: Build a robust profile on the target (Artemis)

* The profile should include the target’s technology stack, email addresses, phone numbers, resumes, and so on
  + Tech stack:
    - Artemis’ RFQ/RFP web app doesn’t restrict or filter user uploads by file type. This is a vulnerability that could allow threat actors to connect remotely, execute arbitrary code, and then elevate their privileges within the app. In this instance, the threat actors would be able to view or download sensitive info regarding bids and even gain admin rights within the app.
    - Firewall:
      * Cisco, Fortinet, and Palo Alto
    - Load balancing
      * F5 (Big IP)
    - Secure Remote application access
      * Zscaler
    - Servers:
      * 50% in the cloud (AWS)
      * 50% on-prem
        + Houston
        + Paris
        + Cairo
        + Singapore
    - Network
      * In transition to SD-WAN
      * Still several MPLS links, especially at smaller remote locations
    - Considerations:
      * Switching to Fortigates’ firewall service to cut costs, instead of using Cisco gear
    - Network Diagram
      * Unable to supply; outdated
    - Software
      * Microsoft Active Directory
        + Single Sign-On (SSO) for authentication to other apps, namely SAP
      * SAP = company’s primary ERP system, runs on servers running Linux and Oracle 12c
      * Messaging:
        + Mix of Exchange Online (via Office 365 cloud tenant) and on-prem Microsoft Exchange Servers
    - Apps
      * PARS system
        + Allows engineers to submit technical info regarding potential patents
        + If submission passes legal and technical reviews, it’s forwarded to the Intellectual Property group for submission to either the US Patent Office, the National INstitute of Industrial Property (INPI) in France, or both
      * APOLLO system
        + Repository for trade secrets, primarily around manufacturing processes

Procedure:

* Detail the activities you plan to use to obtain as much publicly available info as possible
  + In this reconnaissance, there will be a mixture of OSINT tools and commercial tools since we are provided with the access and the permission of Artemis to professionally and ethically go through their systems and their profile overall.
  + The goal here is to first perform as much OSINT reconnaissance as possible to see what has already been made publicly available by Artemis to get a general understanding of the security posture before any active reconnaissance tools have been utilized.
  + Then, with the information provided by Artemis about their systems, software, and technology stack, we will perform an active reconnaissance using the tools listed below.
  + With the help of both OSINT resources and commercial tools, our cybersecurity consulting firm that specializes in penetration tests, vulnerability assessments, and regulatory compliance will be able to give the organization the best advice, support, and instruction on how to harden the security side of their organization and how to move forward so that they can be assured that their operations will continue to run as smoothly as possible.

Deliverable:

* Provide a minimum two-page description of all the tools and methods you will use to accomplish this task
* Deliverable should cover at least 15 tools/resources
  + [Beenverified](https://www.beenverified.com/)
    - Unlimited people, vehicle, property, and contact info
  + [Builtwith](https://builtwith.com/)
    - Find out what websites are built with
    - Used to scan sites, see what they have underneath for vulnerability scanning, see the tech stack
  + [Censys](https://censys.io/)
    - Attack surface management for the cloud
    - Reduces your internet attack surface by continually discovering unknown assets and helping remediate Internet facing risks
  + [Checkusernames](http://checkusernames.com)
    - Find the use of your brand or username on 160 social networks
  + [Dnsdumpster](http://dnsdumpster.com)
    - Type domain of your organization and you’ll find which dns servers you are using, which MX records you have, and TXT records
  + Duckduckgo
  + [Foca](https://www.elevenpaths.com/innovation-labs/technologies/foca)
    - Fingerprinting Organizations with Collected Archives
    - Tool used to find metadata and hidden info in documents
    - Might only run on windows workstation
  + Nessus
    - Vulnerability scanner
    - Remote scanning tool, scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network
    - Lowest false positive rate with six-sigma accuracy
  + [Nmap](https://nmap.org/)
    - Network mapper
    - a free and open-source network scanner created by Gordon Lyon
    - used to discover hosts and services on a computer network by sending packets and analyzing the responses
    - provides a number of features for probing computer networks, including host discovery and service and operating system detection
    - Perform port scans, ping scans, OS scans, version scans, etc.
  + [OSINT Framework](https://osintframework.com/)
    - Gathering info from free tools/resources to find free resources
    - Great place to start your OSINT journey
    - Comprehensive, has all sorts of different types of resources
  + [Recon-NG](https://tools.kali.org/information-gathering/recon-ng)
    - Used by all offsec professionals
    - Enumerate targets, intelligence and investigate targets
    - Powerhouse tool
    - Command-line tool
    - Stock with kali linux builds
  + Rocketreach.co
    - Access real-time verified personal/professional emails, phone numbers, social media links
  + [Shodan](https://www.shodan.io/)
    - Search engine for the internet of everything, for internet-connected devices
    - Crawls the internet and finds what’s at the end of the IP addresses
    - Find endpoint devices
    - Standard in the infosec industry
  + [Spyse](https://spyse.com/)
    - Records of the internet connected assets available for search and download
    - Allows (like Shodan/Zoomeye) to put in diff information that may have documented/recorded by the Spyse backend and you can pull info
    - Free to use (has a paid program too)
  + [theHarvester](https://tools.kali.org/information-gathering/theharvester)
    - Gather OSINT to determine a company’s external thread landscape on the internet
    - Find emails, names, subdomains, URLS, and IPs using multiple public data sources
    - Scrape info from Google or Bing
      * Find associated IP addresses
    - List of people from LinkedIn
      * Names and titles
    - DNS brute force
      * Find those unknown hosts; vpn, chat, mail partner, etc.