Roles for individuals on the Coastline CCDC Team 2023

Windows

- Vinh
  - □ Identify the Domain Controller and create an administrative user account for yourself.
  - □ Identify any additional users on the domain and document their usernames.
  - □ Identify any additional computers on the domain and document their hostnames.
  - □ Identify any additional groups on the domain and document their names.
  - □ Identify any additional shares on the domain and document their names.
  - □ Identify any additional services on the domain and document their names.
  - □ Identify any additional Administrative User on the Domain and change their password.
    - □ Submit a change request form for any changes made to the domain.
  - □ Identify the hostname and IP addresses of the Domain Controller and document them.
- Alvin
  - □ Identify the Windows Clients and create an administrative user account for yourself.
  - □ Identify additional users on the Windows Clients and document their usernames.
  - □ Identify any additional Administrative User on the Windows Clients and change their password.
    - □ Submit a change request form for any changes made to the Windows Clients.
  - □ Identify any services running on the Windows Clients and document their names.
  - □ Identify the hostname and IP addresses of the Windows Clients and document them.

Linux

- Loren
  - □ Identify the Linux Servers and create an administrative user account for yourself.
  - □ Identify any additional users on the Linux Servers and document their usernames.
  - □ Identify any additional administrative users on the Linux Servers and change their password.
    - □ Submit a change request form for any changes made to the Linux Servers.
  - □ Identify any services running on the Linux Servers and document their names.
  - □ Identify the hostname and IP addresses of the Linux Servers and document them.
  - □ Setup Kibana and ElasticSearch on host machine?
    - □ Ask at meeting if we can install anything on jump boxes including Kibana and ElasticSearch
- Cameron
  - □ Identify the Linux Clients and create an administrative user account for yourself.
  - □ Identify any additional users on the Linux Clients and document their usernames.
  - □ Identify any additional administrative users on the Linux Clients and change their password.
    - □ Submit a change request form for any changes made to the Linux Clients.

  - ☐ Identify any services running on the Linux Clients and document their names.
  - ☐ Identify the hostname and IP addresses of the Linux Clients and document them.
  - ☐ Gather list of hostnames and IP addresses from Loren, Vinh, Alvin and create firewall rules to allow traffic between the hosts and disable all other traffic.

Business Injects

- Spencer

  - ☐ Track active business injects and document the Goal and Due Time for each (Add to whiteboard)
  - ☐ Prioritize business injects and assign to team members
  - ☐ Communicate all change requests to Ops Team on behalf of the team
  - ☐ Notify team of any changes to the competition environment communicated in Discords
  - ☐ Primary responsibility is managing the business injects and ensuring that they are completed on time

- Bryan

- ☐ Execute on business injects assigned by Spencer with assistance from the rest of the team
- ☐ Format information gathered from the rest of the team into a business inject report
- ☐ Deliver draft report to Spencer and Mike for final review (This is meant to be collaborative)
- ☐ Primary responsibility is completing assigned business injects by gathering required information from the rest of the team.

Incident Response / Threat Hunting

- Brent / Terrie

  - ☐ Begin monitoring the network for suspicious activity
    - ☐ Nmap scan of all hosts
    - ☐ Nessus or other vuln scanning tools
    - ☐ Work closely with Loren on the ability to monitor the Kibana logs. You should have access and know how to query the logs.
  - ☐ Respond to any alerts generated by the monitoring tools or other team members
    - ☐ Use draft incident response report to document the incident
  - ☐ Eternal Blue:
    - ☐ Wireshark signatures and search parameters to identify Cobalt Strike Beacons

- Mike

  - ☐ Manage the incident response process
    - ☐ Assign incident response tasks to team members
    - ☐ Review draft incident response reports and provide feedback
    - ☐ Review final incident response reports and provide feedback
    - ☐ Communicate incident response reports to Spencer for forwarding to Ops Team
  - ☐ Eternal Blue:
    - ☐ Bluespawn as a defense to Cobalt Strike. https://bluespawn.cloud/en/develop/

    - □ General team management

TODO

- □ Create a standard format for documenting the usernames, hostnames, IP addresses, and other information gathered by each team member.
- □ Modify and update Windows Hardening checklist
- □ Modify and update Linux Hardening checklist
- □ Develop standard format for submitting change requests
- □ Finalize format of business inject responses.
- □ Create ***cheatsheet*** for Kibana and Elastic