

Roles for individuals on the Coastline CCDC Team 2023

Windows

- Cameron
 - ☐ 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.
- Joseph
 - ☐ 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

- Jennifer
 - ☐ 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.
 - ☐ Identify kubernetes host machine using kubectl
 - ☐ Identify running containers with hostnames and IP addresses
 - ☐ Identify services hosted on Docker
- Thomas
 - ☐ 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.

Networking / Firewall

Aaron

- ☐ Change default password ASAP.
- ☐ Create new admin user and disable original "admin" user.
- ☐ Disable SSH access to Firewall.
- ☐ Allow access to pfSense web interface from only 1 IP Address (your jumpbox).
- ☐ Work on establishing firewall rules given hostnames and IP addresses from team, time permitting.

Business Injects

- Seon
 - ☐ Track active business injects and document the Goal and Due Time for each (Add to whiteboard).
 - ☐ Prioritize business injects and assign to appropriate 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 Mantis Ticketing system.
 - ☐ Primary responsibility is managing the business injects and ensuring that they are completed on time.
 - ☐ Format information gathered from the rest of the team into a business inject report

Incident Response / Threat Hunting

- Brent
 - ☐ Scan environment for all hostnames/IP addresses.
 - ☐ 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