Standard Operating Procedure

First 28 minutes, starts now.

Get credentials:

Receive credentials and share as necessary to all Gold team members.

Ensure smooth and secure login for all members. (SSH, RDP).

Initial Configurations:

Make sure all passwords are changed and most accounts disabled.

- **Create new admin accounts and disable and delete old ones.**
- **Search system for all user accounts. Including default, guest, idle and hidden accounts. If found disable and delete.**
- **Check critical files and user's permissions.**
- **Limit execution capabilities.**
- **Configuring and enforcing initial group policy.**
- **Enable event logging**

Limit Network access and turn on firewalls.

- **Enable firewalls and configure implicit deny rules.**
- **Disable unused remote administration.**
- **Reconfigure SSH, prevent root login. delete and regenerate SSH keys and enforce key only authentication.**
- **Check IP routing table, host file, ARP tables. Make note of current state and refresh all connections.**
- **Prevent traffic redirection.**
- **Check for network taps and other nodes connected to the network. (correlate IP addresses with provided network architecture)**

Access Systems and network states:

Run vulnerability scanner (OpenVAS, Nessus, Qualys, Burpsuite).

Baseline systems and network.

- **Make note of normal state and services running within the network.**
- **Network traffic collection and analysis.**
- **Enumerate services and network connections.**
- **Check all autorun locations (folders and registry keys). Remove all unwanted software.**
- **Nmap and Masscan assessment**

Backup systems.

Deploy IDS and IPS systems (snort, pfsense, security onion)

Initial Remediation:

Remediate all critical vulnerabilities identified during initial assessment.

- **Update systems, applications and remove unwanted services and close unused ports discovered during assessment.**
- **Deploy Antivirus ?**
- **Reevaluate IDS, IPS and Firewall rules**

Create firewall rules to optimize connections.