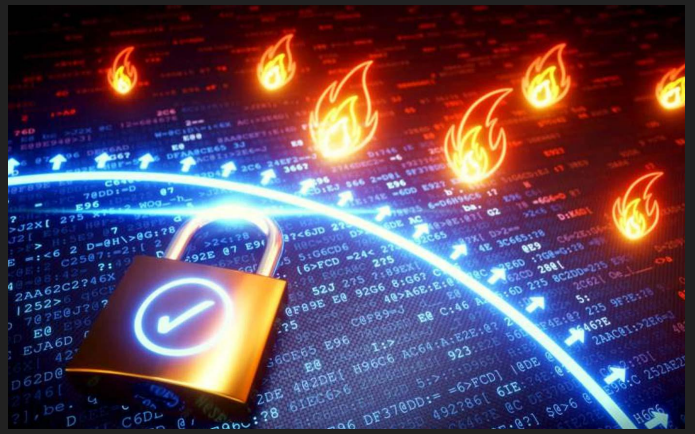
Operation Diamondhouse

Mission

- FOB Diamond has been established along the border of a near-peer nation. It protects a satellite ground terminal that provides internet to the nearby region.
- However, numerous weaknesses in the defense have been identified, both physical and digital.
- Your team has been deployed to boost physical security around the two ECPs, and configure the firewalls on two sensitive devices within the FOB’s network.



Mission

- Two machines on FOB Diamond's network need security improvements to their firewalls.
- One firewall can be configured directly on the device. The other, you must login via SSH to configure. Both use the iptables firewall.
- Intel states that three ports are considered highly vulnerable and must drop traffic to:
  - HTTP (Port 80) - Unencrypted web traffic
  - POP3 (Port 110) - Unencrypted mail traffic
  - Telnet (Port 23) - Unencrypted version of SSH

local

$ ssh


iptables -A INPUT -i lo -j DROP
iptables -A INPUT -i lo -j ACCEPT
imgflip.com

Rules of Engagement

- FOB Bravo has pre-established challenge/response phrases
  - **Challenge:** Wire
  - **Normal Response:** Chip
  - **Duress Response:** Port

- Check your fire. Friendly forces (military AND civilian) on foot or in vehicles may be moving in and out of the FOB.

- Maintain OPSEC at all times, including with all friendly personnel. Only your team is authorized to work with cyber defense assets.