TO:CIO

FROM: IT Staff

SUBJECT: Incident Report 1

Inject Number: 5

DATE: February 4, 2017

INCIDENT REPORT FOR THE 2017 REGIONAL CCDC COMPETION

Good [TOD]. Below is an incident report for a suspected malicious attack by the Red Team. Please review the following details:

Date/Time the attack was started (if known): 2/4/2017

Date/Time the attack was discovered: 2/4/2017 11:40am

Attacker’s source address: 10.0.0.110

Target system name / address: 172.20.241.11

Target port / service(s): NA

Type of attack (virus, hacking, DoS, etc.): remote login. Tried running commands

Result of the attack: Had to shut down website to prevent further damage.

Vulnerability that allowed the attack:

How attack was discovered: Watching logs.

How the attack was contained: Blocked IP

Remediation actions / controls:

Result of remediation: Attacker has been blocked.

Thank you,

IT Staff