2016

Collegiate Cyber Defense Competition

Team Name

Minnesota State University, Mankato

Playbook

# Event Information

## Event Scoring

## Incident Response

## Business Injects

Document template, memo form.

# Team Information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Full Name | Role | Backup Role | Cell Number | Email |
| Zach | Ubuntu DNS | Captain |  |  |
| Myles Landais | Palo Alto Firewall | Windows 2012 | (651) 707-7464 | Landais.myles@gmail.com |
| Dan | Win Server 2008 | AD and DNS |  |  |
| Jesse Aland | Windows 7 |  |  |  |
| Bradley | Win 2012 Server | Web Apps |  |  |
| Joshua | CENTOS/Ecommerce |  |  |  |
| Erica | Debian Email |  |  |  |
| Sarah Day | Tech Writer |  | 907-957-0624 | [Sarahday07@gmail.com](mailto:Sarahday07@gmail.com) |
| Ola | Tech Writer | Backup |  |  |
| Ed | Firewall | Backup |  |  |
| Michael | Debian Email | Backup |  |  |

Web browser of choice?

# Network Administration

## Network Topology Chart

|  |  |  |  |
| --- | --- | --- | --- |
| Dark Red | Palo Alto Firewall | 172.20.241.254 | Next Generation Firewall |
| Red | Debian | 172.20.241.39 | Mail Server; Roundcube |
| Orange | Ubuntu | 172.20.240.23 | DNS; Bind? |
| Yellow | CentOs | 172.20.240.11 | E-Commerce; apache,nginx,etc? |
| Light Green | Windows 2003 | 172.20.241.9 | FTP; WarFTP |
| Green | Windows 2008 | 172.20.241.27 |  |
| Blue | Windows 2012 | 172.20.241.3 | Active Directory, (internal) dns |
| Dark Blue | windows 7 | 172.31.x.3 | External |

## Network Firewall Policy

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Priority** | **Name** | **from** | **to** | **Application/Service** | **Description** |
| x01 |  |  |  |  |  |
| x02 | from-wins- |  |  |  |  |
| x03 |  |  |  |  |  |
| x04 |  |  | **[windows group]** | Windows-updates |  |
| x05 |  |  |  |  |  |
| x06 |  |  |  |  |  |
| x07 |  |  |  |  |  |
| x08 | from-any-to-2003 | any | win2003 | ftp | Mission Critical |
| x09 | from-fire-to-2003 | Palo Alto | win2003 | Ssh, panos-web | Firewall Management |
| x10 | from-fire-to-2012 | Palo Alto | win2012 | Ssh, panos-web | Firewall Management |
| x11 | from-2003-to-fire | win2003 | Palo Alto | Ssh, panos-web | Firewall Management |
| x12 | from-2012-to-fire | win2012 | Palo Alto | Ssh, panos-web | Firewall Management |
| x13 |  |  |  |  |  |
| x14 |  |  |  |  |  |
| x15 |  |  |  |  |  |
| x16 |  |  |  |  |  |
| x17 |  |  |  |  |  |
| x18 |  |  |  |  |  |
| x19 |  |  |  |  |  |
| x20 | from-any-to-any | Any | any |  | log and deny |

## Palo Alto Command Line Reference

Maintenance Mode

$ debug system maintenance-mode

# Linux Administration

## General Checklist

* Secure Linux Kernel (4.4.x)
* Remove unwanted local users

# Windows Administration

## Windows 2003 Checklist

* + Patch Service Application (WarFTP)
  + Remove Local Users
  + Recommended Windows Updates
    - Service Pack 2
    - Service Pack 3
  + Install recommended programs
    - Enhanced Mitigation Experience Toolkit
      * Requires dot net
    - Web Browser

# Link Directory

# Physical Security Checklist

* Check Network Cables, user services, passwords
  + Every user is accounted for, no shared accounts
  + Create admin account for the specific team member and escalate privileges as needed, watch root/admin
* Check for tape on mouses
* Check for GSM bugs, keyloggers, wifi access points
* Create a list of all hardware: device name, type, serial number, location, service tag

# More sections & content

Putty, an ssh client for windows