**RMCCDC 2018 Coaches Packet**

**Scenario**

Regis Hotel Systems (RHS, Inc.) is the provider of hotel rooms at its main complex in Denver Colorado. It supports its own reservation services as well as enterprise networking environment. Although a rather small company as it is configured, it does have the goal of expanding its reach as it grows to support additional hotels in Thornton, Colorado and Greenwich Village, CO. During these events, problems can occur and they have. The company’s IT controls, governance, documentation, security policies and procedures are immature. However, in an attempt to correct some of the issues, the company has contracted with a Threat Intelligence organization which will provides realtime threat information to the organization. The infrastructure/networking/security team has never fully determined the presence of suspected bad actors on the network however they have noted abnormalities in the system which seems to be creating problems in the system. The RSH, Inc. CEO is asking you to focus your attention on three tasks:

* Determine if an adversary has compromised the system and gained a foothold in the system.
* Remove any compromise from the system without degrading system operations.
* Report findings to shared threat intelligence website.

Your team (here after referred to as the Blue team) has been engaged to secure the internal systems, answer questions posed to you by your CEO, and ensure the response and integration to the threat analysis information which is coming into the organization. The bottom line? You are responsible for defending the computer systems and network infrastructure while maintaining internal/external business services.

**Core Business**

RHS, Inc. has a reputation for good customer service, reliable and reputable processing of customer data, and accountability to management, stakeholders and customers. The internal and customers, administrative staff, as well as employees, require constant and reliable access to all system services. The corporation has standardized on Palo Alto routers, firewalls and switches but this doesn’t mean that others don’t exist in your environment. Of course, there are always surprises in ad hoc legacy networks.

**Core Services**

* + HTTP
  + HTTPS
  + FTP
  + DNS
  + SMTP & POP3
  + SSH
  + RDP
  + Video and sound
  + Internet Connectivity
  + Remote connectivity for systems administration
  + Firewalls, switches and routers
  + Printing
  + Wireless not certain how many networks?
  + Company employee email
  + Customer support/helpdesk

**Network Details**

At the start of the competition each team will be assigned a network environment with identical hardware, software and system configuration. Blue teams will be allowed to alter their network/operating system/application configuration as they see fit, provided they maintain the required core services at all times on the same public IP addresses. **DO NOT REMOVE OR CHANGE THE PASSWORDS FOR BLUE TEAM COMPETITION PACKET ACCOUNTS HIGHLIGHTED IN RED.** Throughout the competitions Blue teams may be asked to bring up additional services by the RHS, Inc. management. Each team should have those services listed above running at all times. Failure to provide these public services will result in a loss of points. An example of the companies’ network diagram is provided in figure 1- Network Diagram. Realize, however, that this example may be incomplete as prior to your arrival in the organization, there was poor recordkeeping.

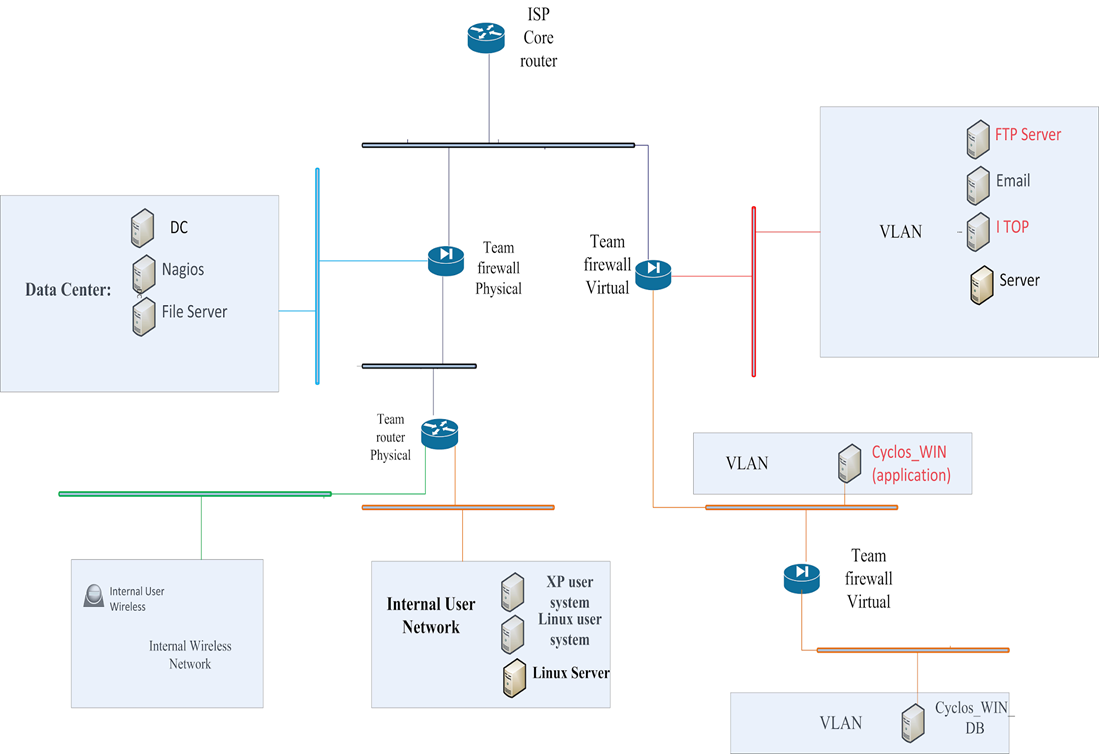


Figure 1 - Network Diagram

Blue teams will have control of their infrastructure, firewall, systems and devices. All communications (injects, announcements, updates and team response) will be communicated through a separate system in their room identified as known as RMCCDC portal. This team portal is not part of the RHS, Inc. systems and not the responsibility of the Blue team to control, modify or protect. Blue teams will have remote network access to the switches and routers via secure shell (SSH). Blue teams will have remote desktop access via RDP and Putty to all servers and hosts.

SSL and SSH sessions will be blocked. No access to Blue team repositories except for the RMCCDC provided Citrix Share File accounts will be allowed because only publicly available information can be used during the competition. Access information will be provided on the first competition day. Blue teams will have Internet access to research topics and up-date operating systems. **No social engineering may be conducted by Blue teams nor will any social engineering be conducted by RMCCDC support teams. Only three RMCCDC officials may interact with your team to clarify situations and ask questions about your environment. These officials can be recognized by the gray polo shirts which they will be wearing on the first day of the competition. You can feel free to discuss your individual team situations with them. No other individuals will be authorized to come into your rooms and talk to you about the competition.** VIPs and camera crews will be escorted by competition officials. Blue teams must grant access to team rooms by competition officials.

There will be a Chief Executive Officer (CEO) for the RHS, Inc. system who will reside in the CEO office. The CEO will be your point of contact for questions during the competition. The only way that a Blue team will communicate to the competition officials will be through the CEO office. *However, the CEO is known for being business-like and it is possible that he will be upset if he is disturbed needlessly*. He can (and will) deduct funds from your bonus if he feels you are needlessly asking questions which he does not need to answer.

You will use provided accounts to share documents across team members and store documents. The Black team will be monitoring all inbound and outbound network traffic.

**Team Roles**

Throughout the competition, there will be several teams, each responsible for different aspects of the competition. The roles of the different teams are outlined in Table 1: Team Responsibilities.

|  |  |
| --- | --- |
| **Color** | **Purpose** |
| White | Observers. A White team member will remain in each competition room to observe activities and ensure RMCCDC rules are being followed. |
| Gold | The Gold team will focus on scoring injects which are given to the teams throughout the event. There will be no Blue team initiated interaction with the Gold team however the Gold team may contact the Blue team for clarification of injects as needed. |
| Black | Operations. The Black Team will monitor network traffic, service availability, and system availability. There will be no Blue team initiated interaction with the Black team however the Black team may notify Blue teams of unavailability of system or system services. |
| Green | The Green team will be providing your threat intelligence to your teams. All interaction between you and this team will be via the Threat Intelligence delivery system. There should be no Green team interaction initiated by the Blue team |
| Blue | Student competitors. The Blue teams are the competition teams. |
| Red | Adversaries. The Red team will be working to attack the systems being protected by Blue teams. There will be no Red team interaction initiated by the Blue team. |

Table 1: Team Responsibilities

**Expectations**

Blue teams must be familiar with regional and national CCDC rules.

<http://rmccdc.regis.edu> and <http://nccdc.org/> . Please review these before the day of the competition. YOU ARE RESPONSIBLE FOR UNDERSTANDING THESE RULES PRIOR TO THE START OF THE COMPETITION.

Scoring will be based on keeping required services up, controlling/preventing un-authorized access, responding to valid threat intelligence and completing business tasks that will be provided throughout the competition. Teams accumulate points by successfully completing injects, maintaining services and responding to business tasks. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by the Red Team as well as by not completing business tasks. *Be aware that providing pre-made business policies and procedures in response to business tasks which do not reflect the environment in which you are working can, in fact, reduce points from your teams score.*

Any team action that interrupts the scoring system is exclusively the responsibility of that team and will result in a lower score. Any team member that modifies a competition system or system component in order to mislead the scoring engine into assessing a system or service as operational, when in fact it is not, may be disqualified and/or the team assessed penalties. Should any question arise about scoring, the scoring engine, or how scoring functions, the Team Captain should immediately contact the competition officials to address the issue.

NOTE: Unlike previous years and this year’s preliminary competition, teams will not be scored based on their recognition of an attack by the red team and then reporting that attack. This doesn’t limit your SLA requirements nor your need to respond to relevant threat intelligence reports. Scoring will be based on your ability to recognize and respond to relevant attacks to your system.

**Emergency Contact**

Emergency Contact dial 6124 from your room phone

6380 South Fiddlers Green Circle, Suite 200  
Greenwood Village, CO 80111

Please be at the competition location by 0800. Registration will be on the second floor of the Regis DTC campus.  Enter via the front door to the building and go up the stairs and you’ll see the table. Make sure to bring all necessary laptops/equipment.