

**2021 Rocky Mountain Regional Collegiate Cyber Defense Competition**

**Team Packet**

**March 26-27, 2021**

**Table of Contents**

Contents

[Rocky Mountain CCDC Mission and Objectives 3](#_Toc67397998)

[Overview 3](#_Toc67397999)

[Business Scenario 4](#_Toc67398000)

[RMCCDC Competition Goals 5](#_Toc67398001)

[Institutional Requirements for Participation 5](#_Toc67398002)

[Competition Team Identification](#_Toc67398003) 5

[COVID-19 & Competing Remotely 6](#_Toc67398004)

[Competition Topology](#_Toc67398005) 7

[Colligere LLC Hardware Network Topology](#_Toc67398006) 9

[Colligere LLC Virtual Topology 1](#_Toc67398007)2

[NDG NETLAB+™ VE System Access 1](#_Toc67398008)4

[Functional Services 1](#_Toc67398009)7

[Schedule – all times MST 1](#_Toc67398010)8

[Systems 1](#_Toc67398011)8

[Competition Rules: Acknowledgement & Agreement](#_Toc67398012) 19

[Competition Rules: Student Teams](#_Toc67398013) 19

[Competition Rules: Professional Conduct](#_Toc67398014) 20

[Competition Rules: Competition Play](#_Toc67398015) 20

[Competition Rules: Internet Usage 2](#_Toc67398016)2

[Competition Rules: Scoring 2](#_Toc67398017)2

[Business Tasks 2](#_Toc67398018)3

[Questions and Disputes 2](#_Toc67398019)4

[Aftermath 2](#_Toc67398020)4

[Sponsors: 2](#_Toc67398021)5

|  |
| --- |
| Rocky Mountain CCDC Mission and Objectives |

The Rocky Mountain Collegiate Cyber Defense Competition (RMCCDC) provides a competitive opportunity for collegiate teams who have proven themselves in 2021 RMCCDC Qualification or Wildcard events. The RMCCDC is designed to provide a controlled competitive environment that will permit each participating institution to assess their students’ depth of understanding and operational competency in managing the challenges inherent in protecting an enterprise network infrastructure and business information systems. The winner of the 2021 RMCCDC is eligible to move on to the 2021 National CCDC on April 23-25, 2021, a completely remote event. The regional 2nd place team is eligible to compete in the National CCDC Wildcard on April 7, 2021, a virtual four hour event without a red team. The winner of the National CCDC Wildcard will be eligible to participate in the National CCDC.

|  |
| --- |
| Overview |

This year the RMCCDC environment is managed by the Mid West Collegiate Cyber Defense Competition (MWCCDC) Consortium, an LLC independent from Moraine Valley Community College. The competition is designed to test each student team’s ability to secure a networked computer system while maintaining standard business functionality.

Because of lingering COVID concerns, the 2021 RMCCDC will be a completely remote event.

The teams are expected to manage the computer network, keep it operational, and prevent unauthorized access. Teams will also be expected to design and configure an ESXi server per requirements. Each team will be expected to maintain and provide public services per company policy and mission. Each team will start the competition with a set of identically configured systems.

The objective of the competition is to measure a team’s ability to maintain secure computer network operations in a simulated business environment. This is not just a technical competition, but also one built upon the foundation of business operations, policy, and procedures. A technical success that adversely impacts the business operation will result in a lower score as will a business success which results in security weaknesses.

Student teams will be scored on the basis of their ability to detect and respond to outside threats, including cyber-attack while maintaining availability of existing network services such as mail and web servers, respond to business requests such as the addition or removal of additional services, and balance security against varying business needs.

There are eight teams competing in the 2021 RMCCDC. They are:

Brigham Young University (BYU)

Colorado School of Mines

Ensign College

Red Rocks Community College

Regis University

Southern Utah University

University of Colorado Boulder

University of Colorado Denver

|  |
| --- |
| Business Scenario |

You have been hired as part of an IT infrastructure team to build out and operate an information processing platform for a new company, Colligere LLC. The organization’s purpose is to gather investor’s resources to expand existing services either by adding to infrastructure or purchase existing companies in order to leverage their expertise, intellectual property and markets that will make them more profitable together than they would be individually.

Therefore, part of the goals for the IT management group would be to support any acquisitions so that their individual networks can be efficiently and securely interconnected into a logical enterprise network infrastructure.

Initially Colligere LLC will expand its services via an ESXi server build and deploy. The marketing and sales arm of Colligere LLC has already secured customer contracts, so it’s essential that the infrastructure expansion be completed in a timely manner.

Colligere management is negotiating a business acquisition where final contract and transference of ownership are imminent. Colligere management hopes that the infrastructure expansion project will be completed prior to the final acquisition.

In order ensure the organization is considering the key IT security concerns, they are adopting

the Cyber Security Framework, which is an adaptation of elements from:

• NIST 800-53 and its DoD derivative NIST 800-171

• NIST Cybersecurity Framework

• ISO 27001/27002

• CIS Critical Security Controls (CSC)

• Cybersecurity Maturity Model Certification (CMMC)

The competition will unfold in two fundamental phases.

Phase 1 - Beginning Friday morning each team will have access to the competition environment representing the Colligere core. This will be similar to the environment used for qualification CCDC. Teams will also have access to an EXSI platform with which to build the topology for this organization. The number and choice of servers (I.e. Windows vs Linux) is yours. On which servers to house the required services is part of each team’s choice as long as they answer on the correct IP address for the Scoring Engine. Keep in mind the EXSI platform only has hardware capacity for 3 to 4 virtual servers. The scoring engine will be looking for these publicly facing services from the start of the competition, so teams that have these running early will benefit.

Phase 2 - Starting mid-day on Friday, a second competition network will be made accessible representing the acquisition Colligere has made. All three network areas, initial competition environment, ESXi server, and the acquisition should interconnect and be able to communicate with each other.

|  |
| --- |
| RMCCDC Competition Goals |

1. To promote fair and equitable standards for cyber defense and technology based competitions that can be recognized by industry
2. To evaluate the defensive and responsive skills of each team under exact hardware, software application, and operating system configurations using a joint academic and industry rating scale
3. To demonstrate the effectiveness of each participating institution’s academic security program
4. To be executed by a preponderance of industry professionals
5. To have industry recognition, participation and acceptance of each competition
6. To rate the effectiveness of each competition against a predefined standard of competition rules
7. To provide a cooperative and competitive atmosphere among industry partners and academia in the area of cyber defense education
8. To provide recognition for participating teams
9. To increase public awareness of academic and industry efforts in the area of cyber defense education
10. To select educational teams to represent the Rocky Mountain Region at the National CCDC and National Wildcard CCDC.

|  |
| --- |
| Institutional Requirements for Participation |

In order to compete at the regional, teams must satisfy the following requirements:

1. Register for the CCDC via the National CCDC registration, or submit paperwork from their institution authorizing their team to participate in the regional as an official school event. This authorization, for teams not registered with the NCCDC, must include an explicit list of all student participants, and be signed by a school administrator. Schools should use their own authorization forms. This may also be an authorization letter on school letterhead.
2. All student participants must have submitted a resume in electronic form. These are now collected via National CCDC Registration. Teams that have not registered with the NCCDC must send resumes to the competition director and administrator.

|  |
| --- |
| Competition Team Identification |

* **Blue Team** - student team representing a specific academic institution competing in this competition; Each team consists of up to 12 competitors, declare via National CCDC Registration, or submitted to the competition director as part of their authorization letter. Each competition team may consist of up to eight (8) members chosen from the submitted roster. The remainder of the roster is for substitution in the event a member of the active competition team cannot compete. Each competitor is expected to be a full time student at the school from which they compete. An exception is a part time student that expects to graduate in the current term. Such a student may compete if they were a full time student during the previous term. Substitution in the competition team requires approval from the RMCCDC Director. The RMCCDC follows the National CCDC rules.
  + National rules apply; [www.nationalccdc.org](about:blank)
* **Red Team** – Professional network penetration testers from industry approved by the competition director and industry representatives
  + Scan and map the network of each competition team
  + Attempt to penetrate the defensive capabilities of each Blue Team network and modify any acquired environment
  + Assess the security of each Blue Team network
  + Attempt to capture specific files on targeted devices of each Blue Team network
  + Attempt to leave specific files on targeted devices of each Blue Team network
  + Follow rules of engagement for the competition
* **White Team** – Competition officials that observe team performance in their competition area and evaluate team performance and rule compliance.
* **Gold Team** – Competition officials that release business injects and scores the competition.
* **Green Team** – Tech support – assists with any technical needs necessary to maintain the integrity of the competition.

|  |
| --- |
| COVID-19 & Competing Remotely |

Since many states, still have health mandates in place, it is necessary that the RMCCDC have all teams compete from remote locations. Ideally, a competing team will do so from a competition room at their institution. Some schools will not permit this, so in such a case teams may compete from their respective homes. Certain teams might also have a hybrid situation with some students on campus, and some from their homes.

White Teams must be in place to observe the event for each team. Such observers have been solicited via separate communications. White Team members are expected to join the competition Zoom meetings for both Friday and Saturday. Team members at their institution do not need to join the Zoom or Discord meeting and have a webcam or a computer with a camera so remote White Team members can observe the Blue Team competition rooms.

White team members with all Blue Team members competing from home are expected to join the team Zoom or Discord meeting where they will be competing.

All team members may join the Zoom meeting for the conclusion of the event after scoring has ended, to engage debrief and announce winners. Team coaches may also join the Zoom meeting after scoring has ended.

Teams competing at their institutions are urged to have speakers and headset for the debrief, as the consortium account has a limit of 100 people for Zoom.

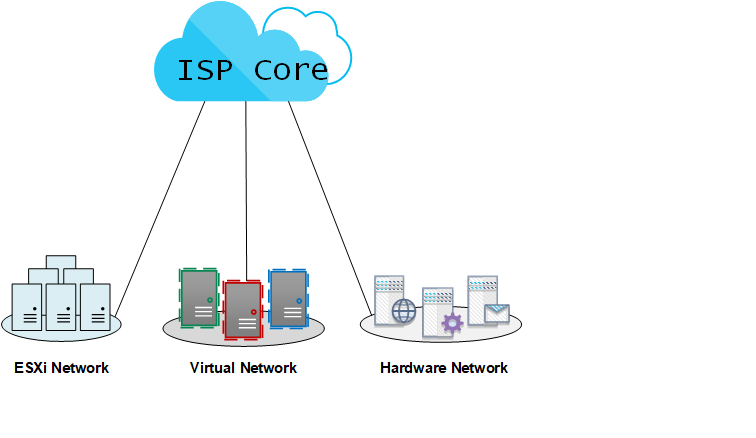
|  |
| --- |
| Competition Topology |

The competition topology for the 2021 RMCCDC comprises threefold network systems as follows:

Colligere LLC Virtual Network

Colligere LLC Hardware Network (acquisition to be added)

Colligere LLC ESXi Network



The Hardware Network is a separate team pod powered by NETLAB. It contains both hardware and virtual elements, but is named Hardware Network to differentiate from the Virtual Network.

The Virtual Network is all virtual, also a separate team pod powered by NETLAB. Teams will recognize the Virtual Network as similar to the topology used for the qualification RMCCDC.

Note that access to respective Hardware/ Virtual Networks is via different accounts, thus different browser sessions. See the section entitled, NDG NETLAB+™ VE System Access.

The ESXi Network is a single ESXi server loaded onto its own PC for each team. They are based on

ESXi Version: 6.7.0

ESXi server connections to the core are as follows:

|  |  |  |
| --- | --- | --- |
| Team | ESXi Server | ESXi Network Egress |
| 1 | 172.31.21.6 | 172.31.21.4/29 |
| 2 | 172.31.22.6 | 172.31.22.4/29 |
| 3 | 172.31.23.6 | 172.31.23.4/29 |
| 4 | 172.31.24.6 | 172.31.25.4/29 |
| 5 | 172.31.25.6 | 172.31.26.4/29 |
| 6 | 172.31.26.6 | 172.31.27.4/29 |
| 7 | 172.31.27.6 | 172.31.28.4/29 |
| 8 | 172.31.28.6 | 172.31.29.4/29 |

Access the ESXi server from a browser from within the Virtual Network at the ESXi server address.

Access to the ESXi server is,

Account – root

Password - !Changeme123

The ESXi Network egress IP is the ‘wan’ IP address of your ESXi Network gateway and is on the same core IP subnet as the ESXi server and Virtual Network. Care should be taken so that your ESXi Network configuration doesn’t overlap directly over the ESXi server itself. This will break your access to the ESXi server and necessitate a lengthy tech support process.

There is communication between the threefold network systems, ESXi, Hardware, and Virtual.

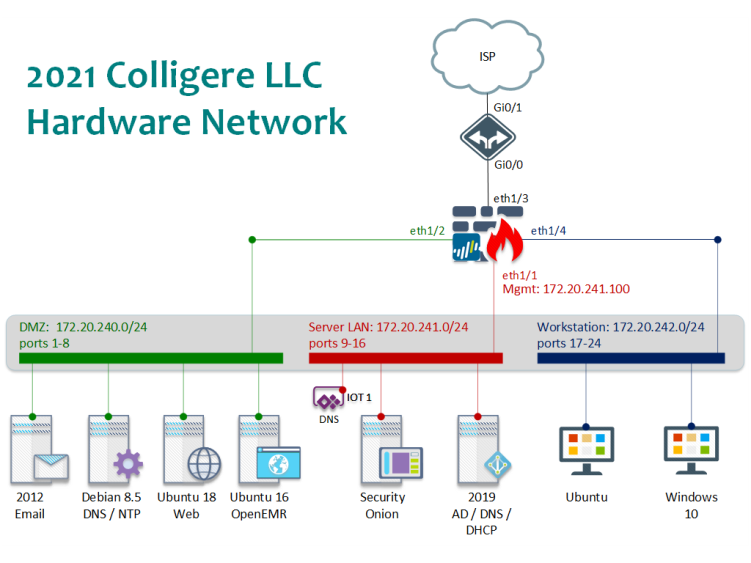
The ESXi server has local resources preloaded on the system, to be used for your first task of building a network. Local resources include Windows VMs, 2019 Servers and Win 10 workstation.

The 2019 Windows Server VMs have password,

!Password123

The Windows 10 workstation has no password. See the notes within local resources on the ESXi server.

|  |
| --- |
| Colligere LLC Hardware Network Topology |



* The router, and switch shown in the topology are hardware devices as follows:

Cisco 2911 Router with IOS c2900-universalk9-mz.SPA.154-3.M5, Version 15.4(3)M5

Cisco 2960 Switch with C2960-LANBASEK9-M, Version 15.0(2)SE5

You have direct access initially to the Cisco devices without login or privileged mode password.

On the Cisco devices, do not issue the following command:

(config)#no password recovery

All servers and workstations are virtual machines under the management of NETLAB+™.

* Each team has the following router internal address:

Router

g0/0 172.20.243.253

* Core IP addresses are the following:

|  |  |  |  |
| --- | --- | --- | --- |
| Team | Router g0/1 | Core Connection  To Router g0/1 | “Public” IP Pool |
| 1 | 172.31.1.2/30 | 172.31.1.1 | 172.25.1.0/24 |
| 2 | 172.31.2.2/30 | 172.31.2.1 | 172.25.2.0/24 |
| 3 | 172.31.3.2/30 | 172.31.3.1 | 172.25.3.0/24 |
| 4 | 172.31.4.2/30 | 172.31.4.1 | 172.25.4.0/24 |
| 5 | 172.31.5.2/30 | 172.31.5.1 | 172.25.5.0/24 |
| 6 | 172.31.6.2/30 | 172.31.6.1 | 172.25.6.0/24 |
| 7 | 172.31.7.2/30 | 172.31.7.1 | 172.25.7.0/24 |
| 8 | 172.31.8.2/30 | 172.31.8.1 | 172.25.8.0/24 |

* The firewall is a Palo Alto firewall hardware device model 3050 running version 9.1.0 with the following addresses:

ethernet1/1 172.20.241.254

ethernet1/2 172.20.240.254

ethernet1/3 172.20.243.254

ehternet1/4 172.20.242.254

The management IP is labeled on the topology:

172.20.241.100

Switch port assignments within the topology are as follows:



The delineation of local IP, major service, and administrative access credentials per VM are as follows:

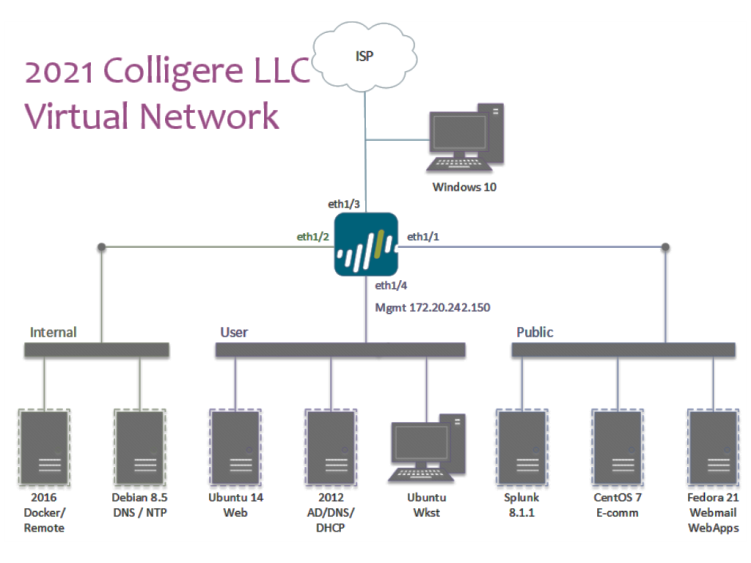


‘Public’ IP are as follows:



* IOT1, internet of things, is a physical device attached to the Hardware Network. IOT1 is a Raspberry Pi hardware appliance. Access the Raspberry Pi via ssh or the application from http. The IOT1 device is part of services offered to customers in the public for scrubbing ads on YouTube via DNS. Customers must be able to access your IOT1 device for DNS.
* Systems are loaded with various user accounts.  Teams are responsible to know which accounts are used for services. **Root, Administrator, Admin or Sysadmin will never be used for scoring.**

|  |
| --- |
| Colligere LLC Virtual Topology |



* Teams have access to 10 VMs – 7 servers, 2 workstations, and the Palo Alto firewall.
* All servers, workstations, and Palo Alto firewall are virtual machines under the management of NETLAB+™ VE.
* Teams do not have access to the underlying layer 2 switch for the Virtual Network.
* The firewall shown in the topology is a Palo Alto VM, version 8.0.0, which is licensed by Palo Alto.
* There is connectivity between your Hardware and Virtual networks, that is, once the acquisition of the Hardware network is complete.

You can access the Palo Alto VM either directly, which yields a command window, or via a browser 172.20.242.150 from any of the User LAN VMs. The PA user/password are,

admin/changeme

* Each team has the following Palo Alto internal addresses:

Internal, e1/2 172.20.240.254/24

User, e1/4 172.20.242.254/24

Public, e1/1 172.20.241.254/24

* Core IP addresses are the following:

|  |  |  |  |
| --- | --- | --- | --- |
| Team | Palo Alto e1/3  Outbound to Core | Core Connection to Palo Alto | “Public” IP Pool |
| 1 | 172.31.21.2/29 | 172.31.21.1 | 172.25.21.0/24 |
| 2 | 172.31.22.2/29 | 172.31.22.1 | 172.25.22.0/24 |
| 3 | 172.31.23.2/29 | 172.31.23.1 | 172.25.23.0/24 |
| 4 | 172.31.24.2/29 | 172.31.24.1 | 172.25.24.0/24 |
| 5 | 172.31.25.2/29 | 172.31.25.1 | 172.25.25.0/24 |
| 6 | 172.31.26.2/29 | 172.31.26.1 | 172.25.26.0/24 |
| 7 | 172.31.27.2/29 | 172.31.27.1 | 172.25.27.0/24 |
| 8 | 172.31.28.2/29 | 172.31.28.1 | 172.25.28.0/24 |

The delineation of local IP, major service, and administrative access credentials per VM are as follows:



This table is accessible on the topology tab of NETLAB+™ VE, via the “Content” upper left.

Specific NAT translations are as follows:

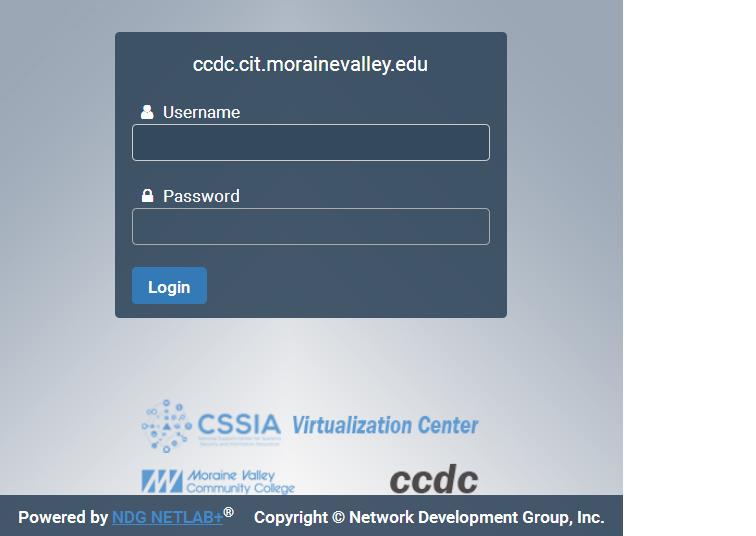


* Teams should be attentive to monitor inject requests and notifications via the Team Portal/ISE.
* Red Team activity will be active throughout the event. At no time will the Red Team have access outside the Cyber Stadium perimeter. Neither will the Red Team be given direct access to any Team network directly via the NDG NETLAB+™ VE system.
* Each Blue Team network will be monitored by a scoring system operating within the remote network. An indication of services, as viewed by the indigenous scoring engine, will be made available to each Blue Team via the Team Portal/ISE.
* **While every effort is made to provide a stable and well-defined competition topology, it is subject to change and /or modification as decided by the CCDC Competition Director.**

|  |
| --- |
| NDG NETLAB+™ VE System Access |

* The Hardware Network and Virtual Network will be hosted via the Cyber Stadium located at Moraine Valley Community College. Both of these networks will be located remotely from any competition room and will be logically isolated from all other competing Blue Teams. Access the NDG NETLAB+™ VE system at,

ccdc.cit.morainevalley.edu

****

The NDG NETLAB+™ VE is accessible via a web browser. The Hardware Network and Virtual Network will be **accessed by separate accounts where the initial password for each set of accounts will be the same**, released at the drop flag at the start of the competition.

Accounts to access the Hardware Network will be,

t1u1, t1u2,….,t1u8

t2u1,t2u2,…..

….

t10u1,…

These accounts are of the form t{team#}u1-t{team#}u8.

Accounts to access the Virtual Network will be,

v1u1, v1u2,….,v1u8

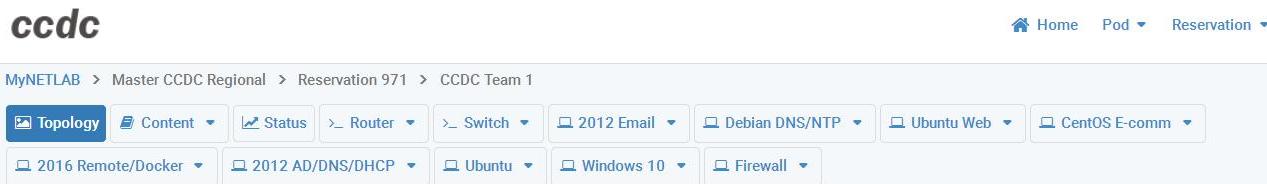
v2u1,v2u2,…..

….

v10u1,…

These accounts are of the form v{team#}u1-v{team#}u8.

Teams should see a lab reservation with each respective set of accounts. When entering the topology, the top menu should look similar to the following:



Note that NDG has fixed the annoying WE’RE DONE button, which would end a team reservation, thankfully no longer appears on the topology page. However, a team may still end their reservation via the Reservation drop down, so teams are advised to avoid this during the competition.

Users can still access VMs by clicking on the topology diagram, but they can also click on the appropriate button at the top of the screen shown in the image. The VM access will then replace the topology image instead of a separate window as with a PE system. Users might wish to work on a VM in a separate window which they can do by the ‘Undock’ feature.



* Teams are responsible to have workstations or laptops that adhere to NDG guidelines. See, https://www.netdevgroup.com/products/requirements/#client/
* Each competition network will be physically and logically isolated from the network used to access the system.
* The White Team and each respective Blue Team will communicate with each other via a Team Portal, a trouble ticket and response application (ISE – Inject Scoring Engine) residing within the remote network at Moraine Valley Community College. This system is accessible via a browser where the system is located at,

[ccdcadmin3.morainevalley.edu](about:blank)

* Team accounts to the ISE are,

team1, team2,…, team8

**Teams should login to the Team Portal/ISE first, using the team# account and password provided. Answer the Welcome inject signaling your readiness to compete. The drop flag is issued next, providing the initial password for all team accounts to the competition network at,**

**ccdc.cit.morainevalley.edu**

* Teams should be attentive to monitor inject requests and notifications via the Team Portal/ISE. A Welcome Inject will be issued ahead of the start of scoring. Response to this initial inject confirms team communication with the White Team. A Cyber Access inject will subsequently be issued containing the team password needed for initial access to the competition stadium.
* Red Team activity may be either externally or internally sourced with respect to the remote competition network. At no time will the Red Team have access outside the remote network perimeter. Neither will the Red Team be given direct access to any Team network directly via the NDG NETLAB+™ VE system.
* Each Blue Team network will be monitored by a scoring system operating within the remote network. An indication of services, as viewed by the indigenous scoring engine, will be made available to each Blue Team via the Team Portal/ISE.
* SLA will be in effect for all scored services, meaning that a penalty will accrue if services are down too long.
* **While every effort is made to provide a stable and well defined competition topology, it is subject to change and /or modification as decided by the RMCCDC Competition Director. This may include the use of additional ISE to split and manage service scoring. Only one ISE will be used for inject tasks.**

|  |
| --- |
| Functional Services |

Certain services are expected to be operational at all times or as specified throughout the competition. In addition to being up and accepting connections, the services must be functional and serve the intended business purpose. At random intervals, certain services will be tested for function and content where appropriate.

**HTTP**

A request for a specific web page will be made.  Once the request is made, the result will be stored in a file and compared to the expected result. The returned page must match the expected content for points to be awarded.

**HTTPS**

A request for a page over SSL will be made.  Again, the request will be made, the result stored in a file, and the result compared to the expected result. The returned page needs to match the expected file for points to be awarded.

**SMTP**

Email will be sent and received through a valid email account via SMTP.  This will simulate an employee in the field using their email.  Each successful test of email functionality will be awarded points.

**DNS**

DNS lookups will be performed against the DNS server.  Each successfully served request will be awarded points.

**SSH**

SSH connections will be performed against the system using credentials and usernames from Active Directory.  Once connected a series of commands will be run and the output examined.  Correct responses will be awarded points.

**POP3**

POP3 connections will be performed against the system using usernames from Active Directory.  Once connected a series of commands will be run and the output examined.  Correct responses will be awarded points.

|  |
| --- |
| Schedule – all times MST |

**Friday, March 26, 2021**

7am Teams arrive at their competition rooms; join Zoom meeting

Welcome Inject Released; teams login to the ISE

8am Drop Flag – competition virtual network stadium access inject released

8am-6pm Active Scoring

**Saturday, March 27, 2021**

7am Teams arrive at their competition rooms; join Zoom meeting

teams login to the ISE

8am Drop Flag – competition stadium access inject released

8am-5pm Active Scoring

5-6pm Debrief, Announce Winners, Closing Dialogue & Wrap-up

|  |
| --- |
| Systems |

1. Each team will start the competition with identically configured systems.
2. Teams will be provided all access credentials by the morning of the competition.
3. Teams should not assume any competition system is properly functioning or secure.
4. Throughout the competition, Green, Orange, and White Team members will occasionally need access to a team’s systems for scoring, troubleshooting, etc. Teams should not be alarmed if ‘status’ shows access to team VMs is being made by those managing the event. Such access will never have a negative impact to teams, and no red team member will have such access.
5. Network traffic generators may be used throughout the competition to generate traffic on each team’s network. Traffic generators may generate typical user traffic as well as suspicious or potentially malicious traffic from random source IP addresses throughout the competition.
6. Teams must maintain specific services on the “public” IP addresses assigned to their team. Moving services from one public IP to another is not permitted unless directed to do so by an inject. Likewise, teams are not permitted to change the internal addressing or VLAN scheme of the competition network unless directed to do so by an inject.
7. Teams are not permitted to alter the system names or IP address of their assigned systems unless directed by an inject; this may affect the results of the scoring mechanism.
8. **Teams are permitted to move services to another platform, provided that the same “public” IP address and DNS naming convention is maintained, along with other requirements of the service. Teams must also notify the White Team if services are moved to another platform, with a rationale for the change.**
9. Teams must maintain “public” services as available from all source IP addresses. Attempts to restrict or filter by IP source address may adversely affect scoring directly, and may also incur a penalty when detected.
10. In the event of system lock or failure, teams will be able to request a complete restoration (scrub/snapshot) via an inject released from the ISE. This will reset any system to its initial starting configuration. The number of system restorations will be tracked and negatively impact scores at the discretion of the White Team. Teams should also consider that system restoration will take time.
11. Systems designated as user workstations within the competition network are to be treated as user workstations and may not be re-tasked for any other purpose by teams.
12. Teams may not modify the hardware configurations of workstations used to access the competition network.
13. Servers and networking equipment may be re-tasked or reconfigured as needed. Teams may avail themselves of the ESXi server to add additional VMs and tools not specifically requested via an inject.

|  |
| --- |
| Competition Rules: Acknowledgement & Agreement |

Competition rules are applicable to all participants of the RMCCDC. They provide structure for the makeup of student teams, permitted actions during competition play, guidelines for scoring, and contingencies for handling disputes. They also document expectations for appropriate conduct during the entire time participants are guests at the host site. Team response to the Welcome inject is tacit acknowledgement of competition rules and their commitment to abide by them.

Team advisers and team captains are responsible for deploying the competition rules to the remaining members of their team. Host sites reserve the right to stipulate additional rules conforming to local policies and guidelines.

|  |
| --- |
| Competition Rules: Student Teams |

1. Each team will consist of up to no more than eight members. All team advisers have been informed of and will adhere to all national rules. See [www.nationalccdc.org](about:blank)
2. Each team may have no more than two graduate students as team members.
3. Each team must have one at least one White team present during the entire competition. Team advisers and faculty representatives may not assist or advise the team during the competition. Team advisers and faculty representatives may not be involved in any scoring or decisions that involve a participating institution or Blue Team.
4. Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and the teams before and during the competition. Team Captains should identify themselves to the White Team by team number, and not by institution.

|  |
| --- |
| Competition Rules: Professional Conduct |

1. All participants are expected to behave professionally at all times they are visiting the host site, and at all preparation meetings.
2. Host site/ local site policies and rules apply throughout the competition.
3. All Midwest Cyber Defense Competitions are alcohol free events. No drinking is permitted at any time during the competition.
4. Activities such as swearing, consumption of alcohol or illegal drugs, disrespect, unruly behavior, sexual harassment, improper physical contact, becoming argumentative, or willful physical damage have no place at the competition.
5. In the event of unprofessional conduct, student team members and their adviser will meet with Gold Team members upon request. The consequence of unprofessional conduct will be determined by the Site Administrator with the recommendation of the Gold Team. This may be a warning, point penalty, disqualification, or expulsion from the campus.
6. The Director of the RMCCDC reserves the right to disqualify an offender from participation in future competitions.

|  |
| --- |
| Competition Rules: Competition Play |

1. All requests for items such as software, service checks, system resets, and service requests must be submitted to the White Team. Requests must clearly show the requesting team by number, action or item requested, and date/time requested. **Teams should not identify the school they represent to the White Team.**
2. Teams must compete without outside assistance from non-team members which includes team advisers and sponsors. All private communications (calls, emails, chat, directed emails, forum postings, conversations, requests for assistance, etc.) with non-team members are forbidden and are grounds for disqualification.
3. No PDAs, memory sticks, CD-ROMs, electronic media, or other similar electronic devices, are allowed in the competition unless specifically authorized by the White Team in advance.
4. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.
5. An unbiased Red Team will probe, scan, and attempt to penetrate or disrupt each team’s operations throughout the competition.
6. The Red Team is not granted access to the Cyber Stadium team networks outside of competition hours.
7. Teams are permitted to replace applications and services provided they continue to provide the same content, data, and functionality of the original service. For example, one mail service may be replaced with another provided the new service still supports standard SMTP commands, supports the same user set, and preserves any pre-existing messages users may have stored in the original service. Failure to preserve pre-existing data during a service migration will result in a point penalty as deemed appropriate by the White Team for each user and service affected.
8. Teams are free to examine their own systems but no offensive activity against other teams, the White Team, or the Red Team is permitted. This includes port scans, unauthorized connection attempts, vulnerability scans, etc. Any team performing offensive activity against other teams, the White Team, the Red Team, or any global asset will be immediately disqualified from the competition. If there are any questions or concerns during the competition about whether or not specific actions can be considered offensive in nature contact the White Team before performing those actions.
9. Blue Team members may not change usernames within their respective environment, unless directed to do so by the White Team. Blue Team members may change passwords for administrator and user level accounts. **Changes to passwords affecting scored services must be communicated to the White Team via the password change request feature of the ISE. Look for a password change policy to be issued during the competition. Changes to administrator and root account passwords may be changed without notification, since these are not used for scoring services**. Competitors have the responsibility to determine how accounts relate to services.
10. Teams are allowed to use active response mechanisms such as TCP resets when responding to suspicious/malicious activity. Any active mechanisms that interfere with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams. Any firewall rule, IDS, IPS, or defensive action that interferes with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams.
11. Each Blue Team will be provided with the same objectives and tasks.
12. Each Blue Team will be given the same inject scenario at the same time during the course of the competition.
13. Blue Teams may request information from the Gold Team and Scoring Manager as to why a particular service is not scoring properly. Disclosure of information regarding non-scoring of services is at the discretion of the GoldTeam. Nevertheless, if core system or scoring system faults are discovered, every effort will be made towards corrective action together with modification of scores to maintain equity and fairness.
14. The Gold Team is responsible for implementing the scenario events, refereeing, team scoring and tabulation.
15. Scoring will be based on keeping required services up, controlling/preventing un-authorized access, and completing business tasks in a timely manner that will be provided throughout the competition.
16. Scores for inject completion and incident reports will be maintained by the Gold Team, and will not be shared with Blue Team members. Running totals will not be provided during the competition. Some debriefing of a general nature is likely at the end of the competition.
17. If a scenario or event arises that may negatively impact the integrity or fairness of any aspect of the competition that was not previously anticipated, it is the final decision and discretion of the Chief Judge to make adjustments in scores, or deploy new policies.

|  |
| --- |
| Competition Rules: Internet Usage |

1. Competition systems will have controlled access to the Internet for the purposes of research and downloading patches. **All internet access from the competition network will be through a web proxy.**
2. The web proxy will permit a predetermined set of common web sites including several used for software repositories. Per National CCDC practice, the complete list of accessible sites will not be published.
3. Internet activity will be monitored throughout the competition to assure compliance with competition rules.
4. No peer to peer, distributed file sharing clients or servers are permitted on competition networks.
5. Additional software or tools must be either free or open source within the limits of pre-determined internet accessibility.
6. Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition.
7. All network activity that takes place on the competition network may be logged and is subject to release. **Competition officials are not responsible for the security of any personal information, including login credentials that competitors place on the competition network.**

|  |
| --- |
| Competition Rules: Scoring |

1. Scoring will be based on keeping required services up, controlling/preventing un-authorized access, mitigating vulnerabilities, and completing business tasks that will be provided throughout the competition. Teams accumulate points by successfully completing injects, maintaining services, and by submitting incident reports. Teams lose points by violating service level agreements after services have been unavailable, usage of recovery services, and successful penetrations by the Red Team.
2. Scores will be maintained by the Gold Team. Individual tracking of services will be available to respective teams during the competition. Blue Team members should use available service reports and internal testing to assess the integrity of their network. Blue Team members should refrain from making direct requests to the Gold Team for routine service verification.
3. Any team action that interrupts the scoring system is exclusively the fault of that team and will result in a lower score. Should any question arise about specific scripts or how they are functioning, the Team Captain should immediately contact the competition officials to address the issue.
4. Any team that tampers with or interferes with the scoring or operations of another team’s systems will be disqualified.
5. Teams are required to provide incident reports for each Red Team incident they detect. Incident reports can generally be completed as needed throughout the competition and submitted to the Gold Team. The Gold Team reserves the right to stipulate the times and manner in which incident reports may be submitted. Incident reports must contain a description of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, etc), a discussion of what was affected, and a remediation plan. The Gold Team, in conjunction with the Red Team, will assess scores for incident report submission based on clarity, thoroughness, and accuracy. The Gold Team may also, at their discretion, assess negative scores for frivolous, unnecessary, or excessive communication.
6. The winner will be based on the highest score obtained during the competition. Point values are broken down as follows:

|  |  |
| --- | --- |
| **35-50%** | Functional services uptime as measured by scoring engine |
| **35-50%** | Successful completion of inject scenarios will result in varying points, depending upon the importance or complexity of the inject scenario |
| **10-20%** | Incident Response and Red Team Assessment |

Precise percentage breakdown will be determined by the White Team.

|  |
| --- |
| Business Tasks |

Throughout the competition, each team will be presented with identical business tasks. Points will be awarded based upon successful completion of each business task. Tasks will vary in nature and points will be weighted based upon the difficulty and time sensitivity of the assignment. Tasks may contain multiple parts with point values assigned to each specific part of the tasking. Each business task may have an indication of relative importance or value assigned and a specific time period in which the assignment must be completed. Business tasks may involve modification or addition of services.

|  |
| --- |
| Questions and Disputes |

1. Team captains are encouraged to work with the Director, the White Team, and contest staff to resolve any questions or disputes regarding the rules of the competition or scoring methods before the competition begins. Protests by any team will be presented by the Team Captain to the competition officials as soon as possible. Competition Gold Team officials will be the final arbitrators for any protests or questions arising before, during, or after the competition and rulings by the competition officials are final.
2. In the event of an individual disqualification, that team member must leave the competition immediately upon notification of disqualification and must not re-enter the competition area at any time. Disqualified individuals are also ineligible for individual awards or team trophies.
3. In the event of a team disqualification, the entire team will be blocked from the competition environment immediately upon notice of disqualification and is ineligible for any individual or team award.

|  |
| --- |
| Aftermath |

Members of Gold, White, and Red Teams strive to make the RMCCDC enriching experiences. All management and administrative teams are open to feedback and suggestions for improvement after the completion of the competition. This may include areas of concern or dissatisfaction.

Whether feedback is positive or negative, participants are forbidden from publishing, posting on the internet, or publicly communicating details of the competition other than what is available at www. cssia.org/ccdc. They are also forbidden from publishing, posting on the internet, or publicly communicating assessments of the RMCCDC, nor assessments of the performance of any team, nor speculations concerning different possible outcomes. Institutions that fail to adhere to this rule may be refused participation in future competitions.

Institutions may publish, post on the internet, or publicly communicate news stories of a general nature about the RMCCDC, and may also enumerate participating teams and winners.

|  |
| --- |
| Sponsors: |

|  |  |
| --- | --- |
|  | Raytheon Intelligence & Space  https://www.raytheonintelligenceandspace.com/ |
|  | Palo Alto Networks  [https://www.paloaltonetworks.com/](about:blank) |
|  | ISACA Denver Chapter  https://engage.isaca.org/denverchapter/home |
|  | HelpSystems, LLC  https://www.cobaltstrike.com |