Erich J. Spengler
Midwest Collegiate
Cyber Defense Competition

2023 Erich J. Spengler Midwest Regional Collegiate Cyber Defense Competition Team Packet

BW Baldwin Wallace University

Davenport University

DePaul University

Drury University

Indiana Tech

Minneapolis Community & Technical College

Purdue University

University of Louisville

SIU Southern Illinois University Carbondale

University of Wisconsin Stout Wisconsin's Polytechnic University

March 17-18, 2023

Table of Contents

Contents

Midwest Regional CCDC Mission and Objectives

The 2023 Erich J. Spengler Midwest Regional Collegiate Cyber Defense Competition (CCDC) provides a competitive opportunity for collegiate teams who have proven themselves in 2023 Midwest State CCDC Qualification or Wildcard events. The Midwest Regional Collegiate Cyber Defense Competition 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 2023 Erich J. Spengler Midwest Regional CCDC is eligible to move on to the 2023 National CCDC on April 28-30, 2023. The second place team of the regional is eligible to compete in the National CCDC Wildcard competition on April 5, 2023. The winner of the National CCDC Wildcard is eligible to move on the 2023 National CCDC.

Overview

Midwest Collegiate Cyber Defence Competitions are managed by the 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.

After several years of concern over Covid, the 2023 Erich J. Spengler Midwest Regional CCDC will return as a hosted event, at Moraine Valley Community College, 9000 W. College Pkwy, Palos Hills, Illinois.

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.

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 ten teams competing in the 2023 Erich J. Spengler Regional CCDC comprising eight winners of respective state qualification CCDC plus two wildcard teams. Participating teams in the 2023 Erich J. Spengler Midwest CCDC are, in alphabetic order,

Baldwin Wallace University	Ohio
Davenport University	Michigan
DePaul University	Illinois
Drury University	Missouri
Indiana Institute of Technology	Indiana
Minneapolis College	Minnesota
Purdue University	Indiana
Southern Illinois University	Illinois
University of Louisville	Kentucky
University of Wisconsin-Stout	Wisconsin

Business Scenario

Your team is the infrastructure support group for Wichtige Firma LLC. The initial infrastructure which the company uses is the Hardware POD. The company has recently acquired the physical and virtual infrastructure components for a backup data center (ESXI POD), which consists of a VMWare platform and PF Sense.

The company is also in negotiations to acquire another related business, Kleinere Gesellschaft LLC, which has its own the infrastructure (Virtual POD). This acquisition has taken place, so the team will need to take on the support of this infrastructure and integrate all three PODs into a cohesive network of connectivity.

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)

Teams will gain access to all systems at the drop flag on Friday.

Midwest Regional 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 Midwest 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 register via Midwest CCDC Registration, and provide roster information to the Midwest CCDC Consortium.
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 consortium 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 minimum team size is four participants. 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 MWCCDC Consortium Competition Director or a MWCCDC Consortium Compliance Monitor present at the competition.

Further guidelines for Blue Team participation have been documented in respective 2023 Midwest State CCDC Team Packets.

  - National rules apply; www.nationalccdc.org
  - Further information is available at www.cssia.org/mwccdc, the main website for Midwest Collegiate Cyber Defense Competitions.

- **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/Black Team** – Representatives from industry who serve as competition judges (Black Team), remote site judges and remote judges (White Team), scoring management, room monitors and security enforcement in the various competition rooms. Judges will assess the competition team's ability to maintain their network and service availability based upon a business inject and a scoring instrument, delivering inject scenarios, scoring of injects, creating log entries, securing log files, issuing or controlling the timing of injects, etc. Each competing Blue Team may have a White Team member present in their room that will assist judges by observing teams, confirming proper inject completion as well as reported issues.

- **Chief Judge:**
  - Serves as the final authority on scoring decisions or issues relating to equity or fairness of events or activities
  - Cannot be from any institution that has a competing Blue team or have any interest in any team outcome
  - Ideally, should be a representative from industry or law enforcement
  - Final authority of all judging decisions, including assessment of final scores and winners of the competition

- **Gold Team** – Comprised of the MWCCDC Consortium Competition Director, as well as representatives from industry and academia who make up the administration team both in planning and during the exercises. Responsibilities include, but are not limited to,
  - Administration and staffing of the cyber defense competition
  - Works with industry partners to orchestrate the event
  - Along with Industry White Team approves the Chief Judge
  - Has the authority to dismiss any team, team member, or visitor for violation of competition rules, inappropriate or unprofessional conduct

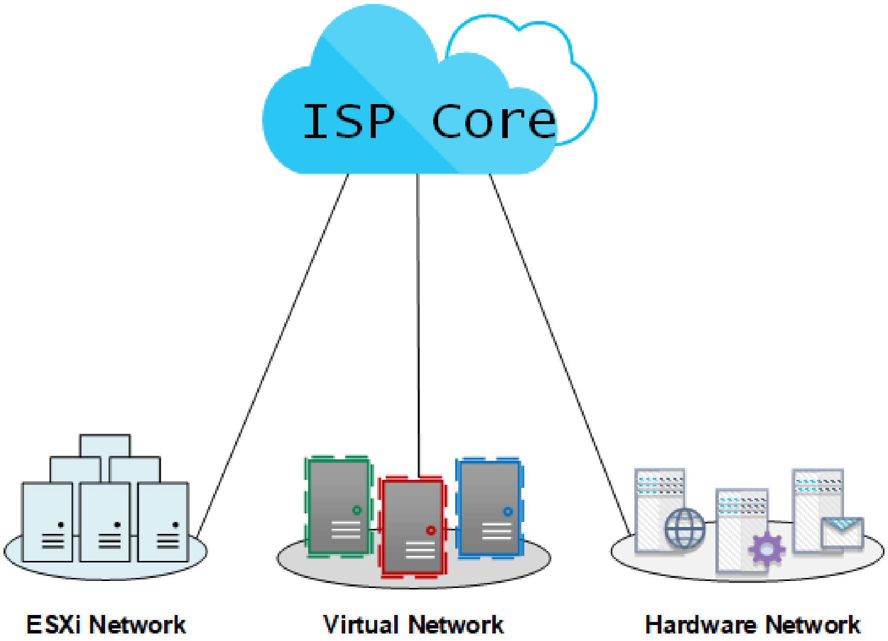
- **Orange Team** – Student workers and professionals who assist the competition by accessing team services. Orange team members act like typical users, and may come from extraneous IP addresses. The Orange Team is expected to keep track of the accessibility of services and report to the White Team their results. The white team will use results of Orange Team activity as a part of scoring.

- **Green Team** – Tech support – assists with any technical needs necessary to maintain the integrity of the competition.

Competition Topology

The competition topology for the 2023 Erich J. Spengler Midwest Regional CCDC comprises threefold network systems as follows:

Kleinere Gesellschaft LLC Virtual Network
Wichtige Firma LLC Hardware Network
Wichtige Firma 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 the topology used for the qualification CCDC.

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

ESXi Version: 7.0.2

ESXi server connections to the core are as follows:

Team	ESXi Server
1	172.31.21.6
2	172.31.22.6
3	172.31.23.6
4	172.31.24.6
5	172.31.25.6
6	172.31.26.6
7	172.31.27.6
8	172.31.28.6
9	172.31.29.6
10	172.31.30.6

Access to the ESXi server is,

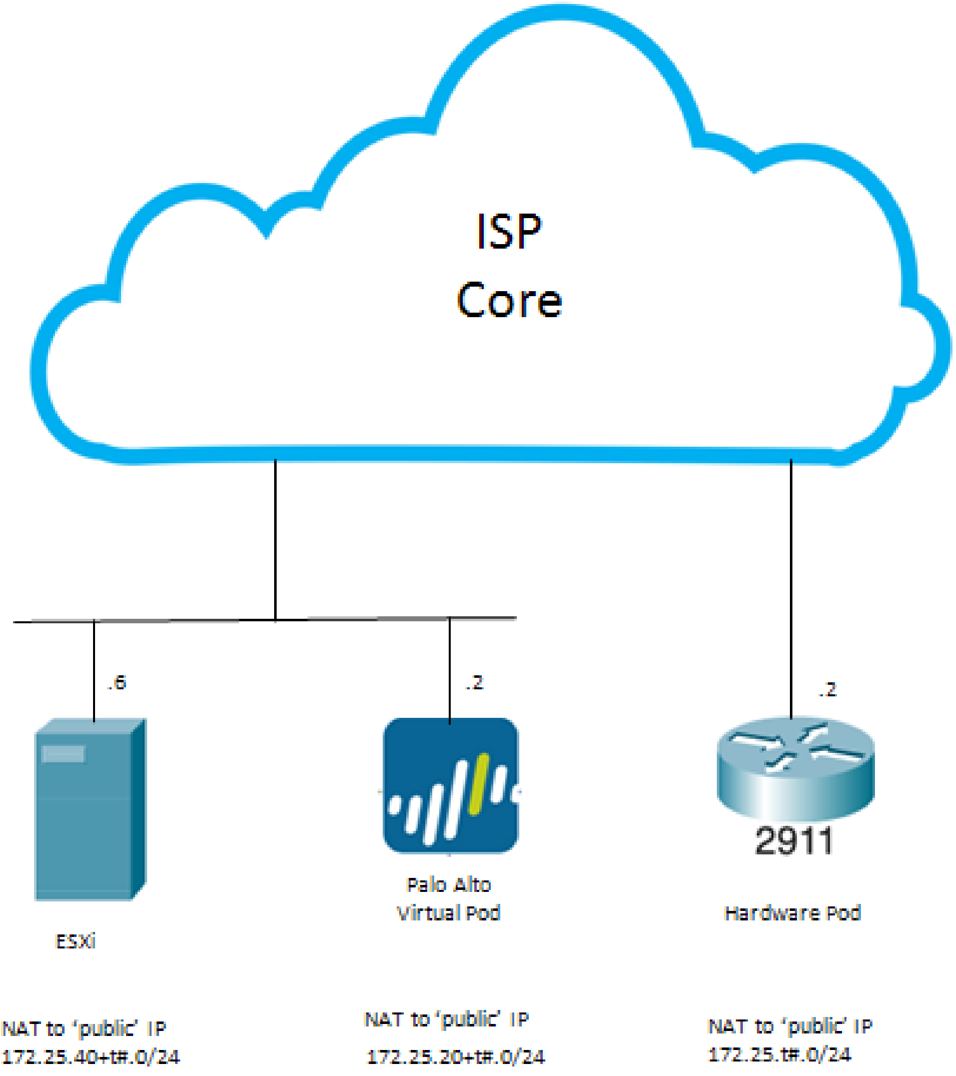
Account – root
Password - !Changeme123

There is communication between the threefold network systems.

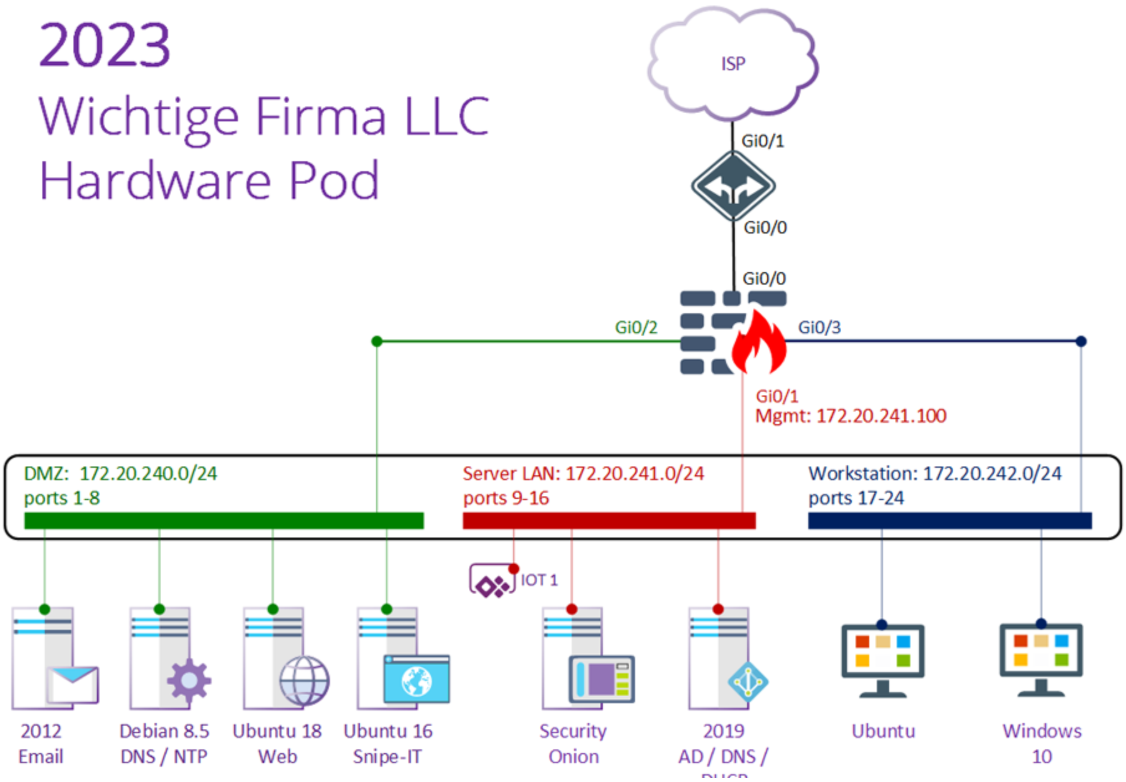
Summary of Core Connections & NAT

The ESXi server and the Virtual pod are on the same subnet. The Hardware pod is on a separate subnet which can communicate with the ESXi/Virtual pod subnet for each team.

In the diagram, t# = your team#.



Wichtige Firma 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-mz.150-2.SE4, Version 15.0(2)SE4

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
9	172.31.9.2/30	172.31.9.1	172.25.9.0/24
10	172.31.10.2/30	172.31.10.1	172.25.10.0/24

- The firewall is a Cisco Firepower FTDv10 VM running Smart Licensing/ Base License enabled. It provides the Malware, Threat Protection, and URL Filtering capabilities, and RA-VPN. It has Cisco Firepower Extensible Operating System (FX-OS) v2.10.1, and Threat Defense for VMware v7.04. The Cisco Firepower FW is configured with the following interface addresses:

Gi0/1	172.20.241.254
Gi0/2	172.20.240.254
Gi0/0	172.20.243.254
Gi0/3	172.20.242.254

The management IP is labeled on the topology: 172.20.241.100

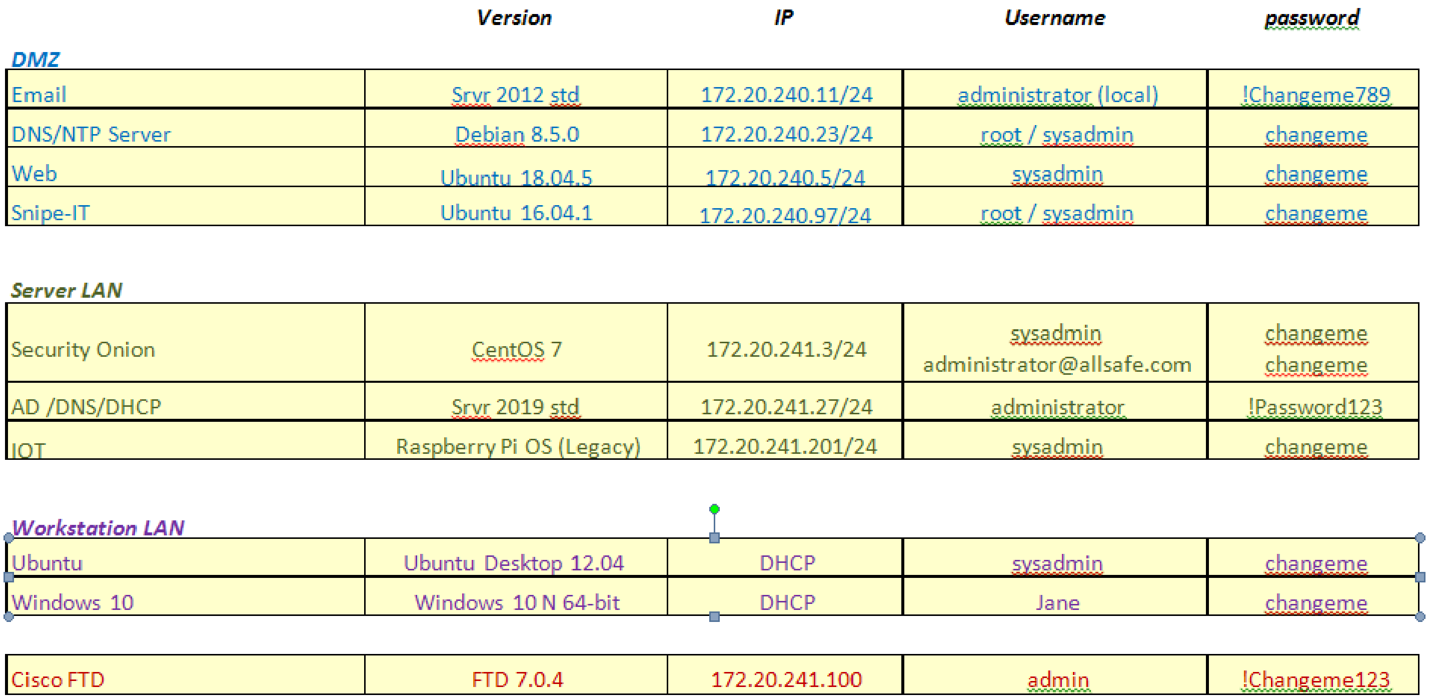
Access the Cisco Firepower FW via,

admin:!Changeme123

Switch port assignments within the topology are as follows:

VM Label	Switch Interface
2012 Email	f0/1
Debian 8.5	f0/2
Ubuntu 18	f0/3
Ubuntu 16	f0/4
Cisco Firepower Gi0/2	f0/8
Security Onion	f0/9
2019 AD	f0/10
IOT1	f0/14
Cisco Firepower Gi0/1	f0/16
Ubuntu WS	f0/17
Windows 10	f0/18
Cisco Firepower Gi0/3	f0/24

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



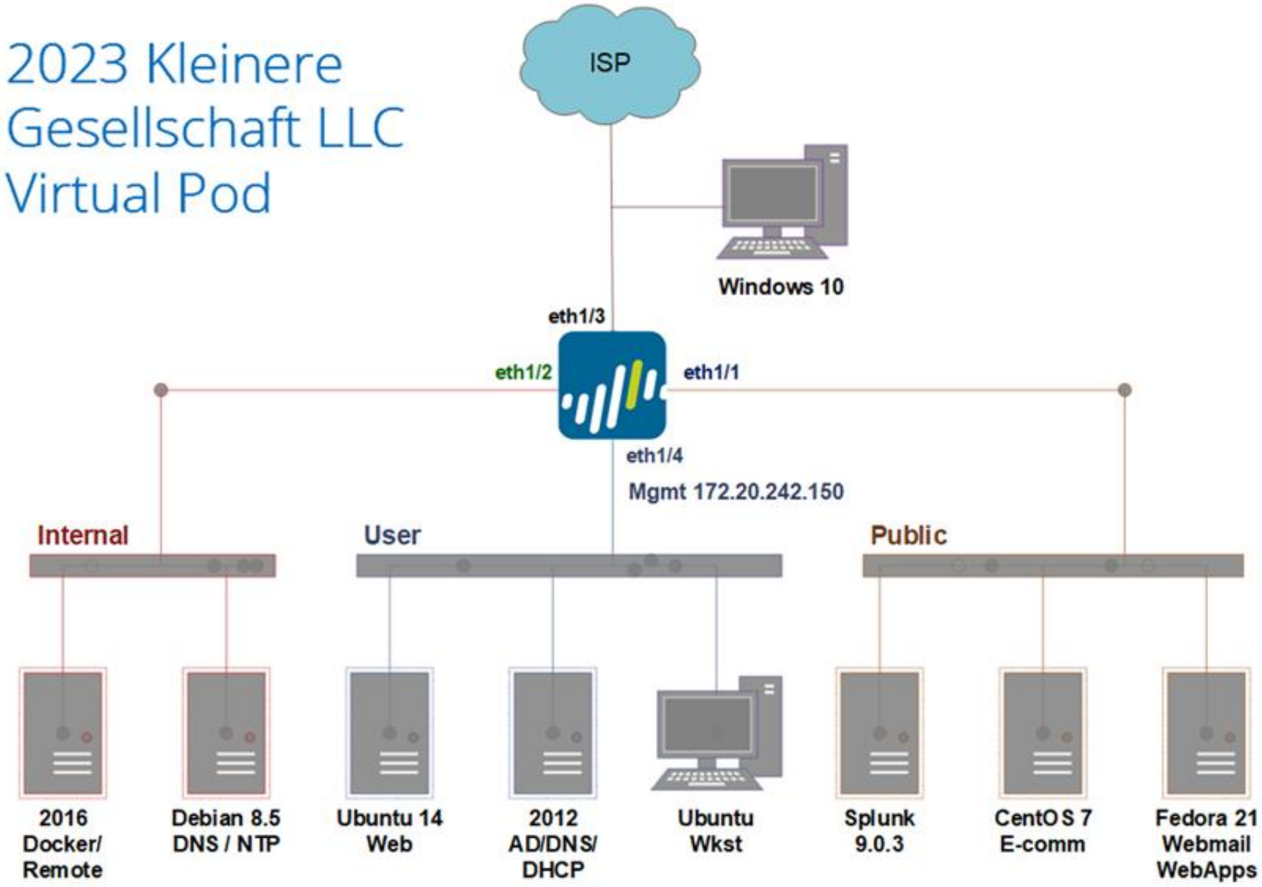
	Version	IP	Username	password
DMZ				
Email	Srvr 2012 std	172.20.240.11/24	administrator (local)	!Changeme789
DNS/NTP Server	Debian 8.5.0	172.20.240.23/24	root / sysadmin	changeme
Web	Ubuntu 18.04.5	172.20.240.5/24	sysadmin	changeme
Snipe-IT	Ubuntu 16.04.1	172.20.240.97/24	root / sysadmin	changeme
Server LAN				
Security Onion	CentOS 7	172.20.241.3/24	sysadmin administrator@allsafe.com	changeme changeme
AD /DNS/DHCP	Srvr 2019 std	172.20.241.27/24	administrator	!Password123
IOT	Raspberry Pi OS (Legacy)	172.20.241.201/24	sysadmin	changeme
Workstation LAN				
Ubuntu	Ubuntu Desktop 12.04	DHCP	sysadmin	changeme
Windows 10	Windows 10 N 64-bit	DHCP	Jane	changeme
Cisco FTD	FTD 7.0.4	172.20.241.100	admin	!Changeme123

‘Public’ IP are as follows:

VM	local IP	public' IP
2012 Email	172.20.240.11	172.25.team#.17
Debian 8.5	172.20.240.23	172.25.team#.9
Ubuntu 18	172.20.140.5	172.25.team#.34
Ubuntu 16	172.20.240.97	172.25.team#.29
Security Onion	172.20.241.3	172.25.team#.67
2019 AD	172.20.241.27	172.25.team#.83
IOT1	172.20.241.201	172.25.team#.97
Ubuntu		
Windows 10		

- IOT1, internet of things, is a physical device attached to the Hardware Network. IOT1 is a Raspberry Pi hardware appliance v1.2. Access the Raspberry Pi via ssh.
- 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.**
- Security Onion is v2.3 and takes considerable resources. Teams should monitor its performance so it does not become overloaded. It is configured to analyze incoming traffic continually. It also has the capability to analyze separate pcap traffic capture files. In the table, sysadmin:changeme is initial access to the VM. administrator@allsafe.com:changeme is the access via the browser on the Security Onion via url securityonion.allsafe.com, and associated feature access.

Kleinere Gesellschaft 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 10.0.0, which is licensed by Palo Alto, and includes Threat Defense.
- There is connectivity between your Hardware and Virtual networks.
- 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/Changeme123

- Each team has the following Palo Alto internal addresses:

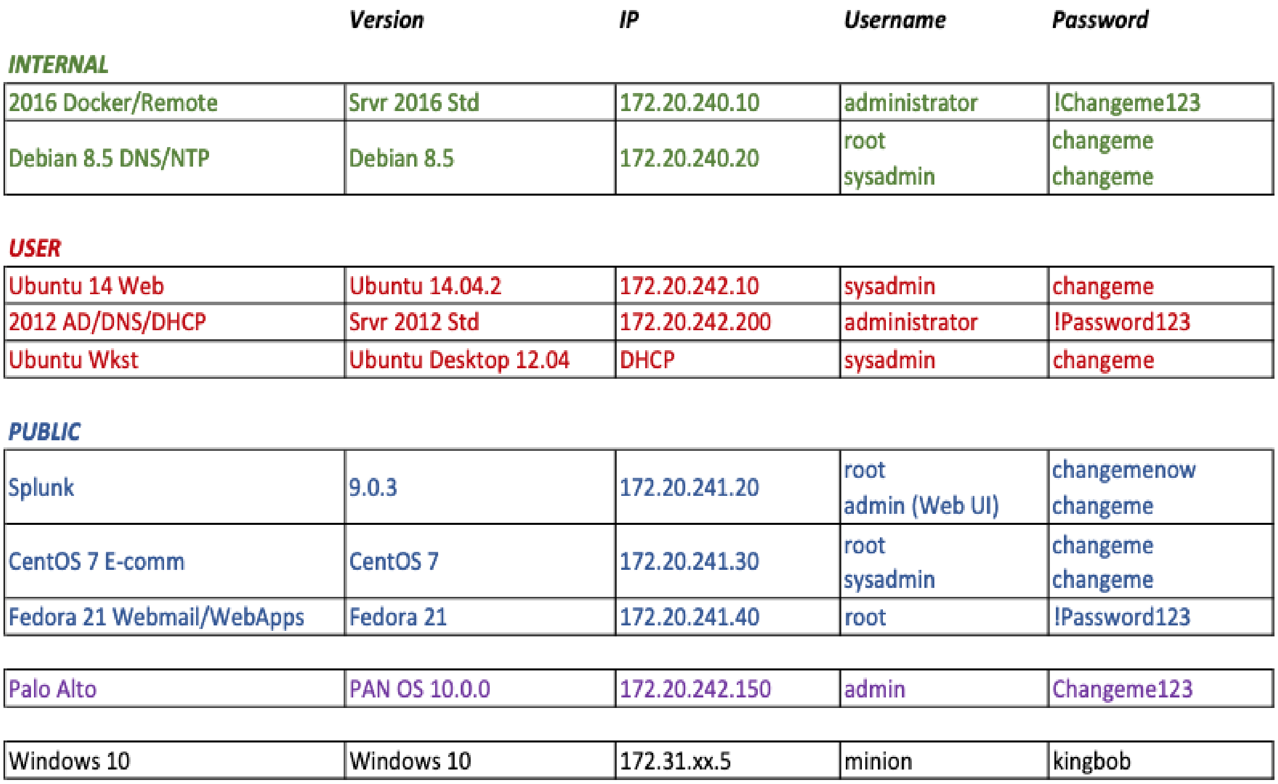
Internal, e1/2	172.20.240.254/24
User, e1/4	172.20.242.254/24
Public, e1/1	172.20.241.254/24

- 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
9	172.31.29.2/29	172.31.29.1	172.25.29.0/24

- VM data are as follows:

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

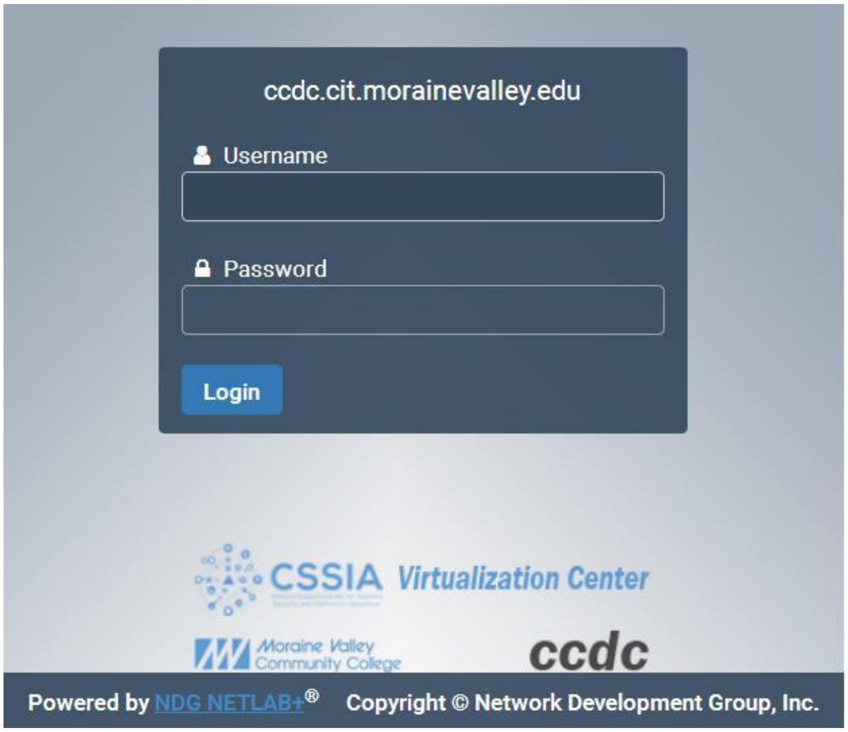


	Version	*IP*	*Username*	*Password*
INTERNAL				
2016 Docker/Remote	Srvr 2016 Std	172.20.240.10	administrator	!Changeme123
Debian 8.5 DNS/NTP	Debian 8.5	172.20.240.20	root sysadmin	changeme changeme
USER				
Ubuntu 14 Web	Ubuntu 14.04.2	172.20.242.10	sysadmin	changeme
2012 AD/DNS/DHCP	Srvr 2012 Std	172.20.242.200	administrator	!Password123
Ubuntu Wkst	Ubuntu Desktop 12.04	DHCP	sysadmin	changeme
PUBLIC				
Splunk	9.0.3	172.20.241.20	root admin (Web UI)	changemenow changeme
CentOS 7 E-comm	CentOS 7	172.20.241.30	root sysadmin	changeme changeme
Fedora 21 Webmail/WebApps	Fedora 21	172.20.241.40	root	!Password123
Palo Alto	PAN OS 10.0.0	172.20.242.150	admin	Changeme123
Windows 10	Windows 10	172.31.xx.5	minion	kingbob

Connecting to the Competition Network

- 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


ccdc.cit.morainevalley.edu

Username

Password

Powered by NDG NETLAB+® Copyright © Network Development Group, Inc.

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**, which become valid at the drop flag at the start of each day 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,

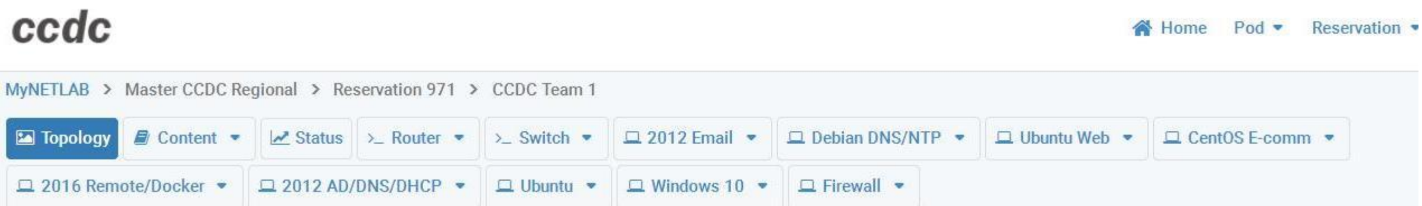
v1u1, v1u2,….,v1u8
v2u1,v2u2,…..

….
v10u1,…

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

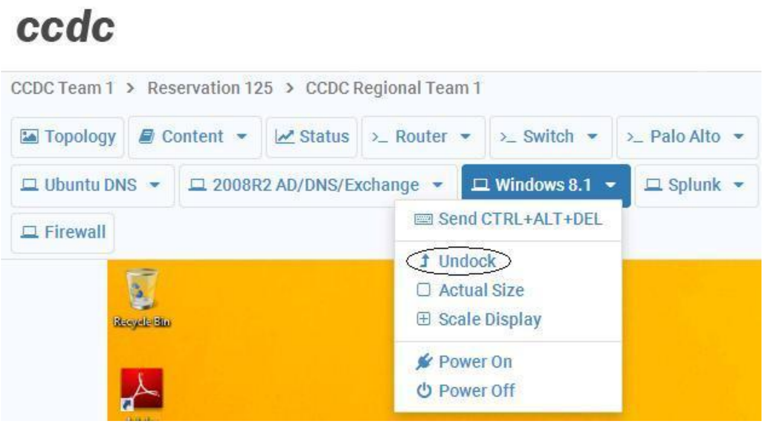
Note once again that each team will use two sets of eight accounts, eight ‘t’ accounts and eight ‘v’ accounts. Once logged in on either account, you will need to change your password. **Please remember or document your new password.** Password resets of t,v accounts will be via a Tech Support inject.

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:



Teams should be cautious with the Reservation drop-down where it’s possible to end your reservation. Your system will be restarted with services points retained, but your team will have start once again from the beginning.

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 provided workstations 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.

Accessing the Team Portal/ NISE – National Inject Scoring Engine

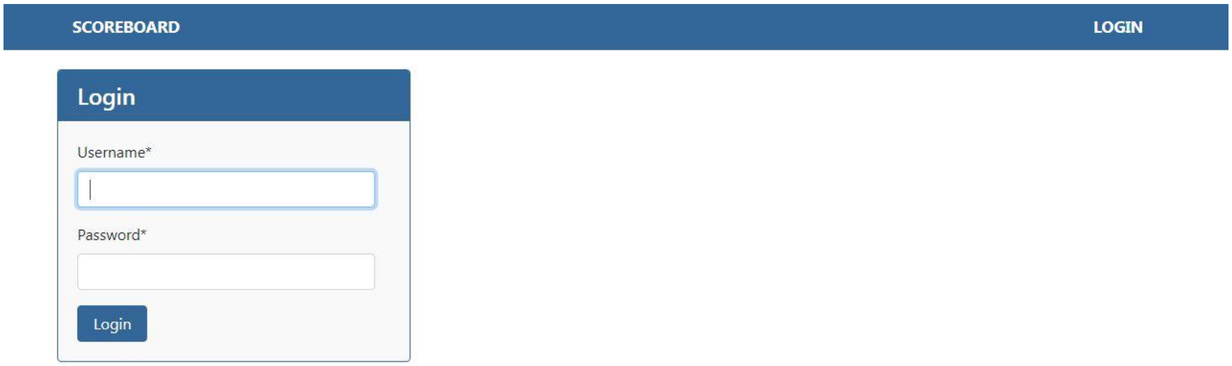
The Black/White and Red Teams and each respective Blue Team will communicate with each other via a Team Portal, a trouble ticket and response application (NISE – National Inject Scoring Engine) residing within the remote network at Moraine Valley Community College. This system is accessible via a browser with url,

ccdcadmin1.morainevalley.edu

Note that the MWCCDC Consortium supports an additional NISE/Team Portal,

ccdcadmin3.morainevalley.edu

Follow the instructions from your competition manager for the specific NISE/Team Portal that will be used for your CCDC competition.



Students should login to the NISE first. There are eight accounts per team that may be used to connect to the NISE where multiple logins using the same account is permissible. The accounts for team1 are,

team01a, team01b, team01c, …, team01h

For team2 the accounts are

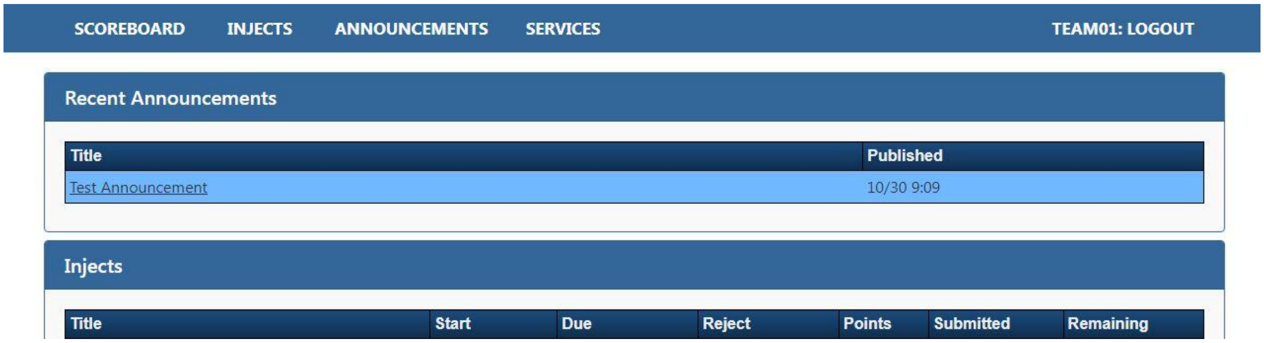
team02a, team02b, …, team02h

It's always two digits for the team number so team10 accounts are,

team10a, ….

Each team account has its own unique password which does not need to be changed.

After logging in the main (Inject) page is displayed.



Recent Announcements

Title	Published
Test Announcement	10/30 9:09

Injects

Title	Start	Due	Reject	Points	Submitted	Remaining

Using the NISE platform is straightforward and intuitive. Teams should explore the various features of the NISE during the event and be especially attentive to announcements and new inject tasks. **Times displayed on the NISE platform are set to CST.**

Responses to inject tasks must be in the form of an attached PDF file unless directed otherwise. It is possible to attach files with other formats, such as text files, but these cannot be read within the NISE platform. Such files must be downloaded and handled separately.

After an inject submission has been submitted, and while the inject task is still open, both teams and judges may mark a submission invalid allowing the team to resubmit. There is a limit to how many times a team may resubmit, depending on Black/Black/White Team policy.

Teams should be attentive to inject submission deadlines, and the NISE platform may need to be refreshed to keep information current. Teams might also take note a slight delay in the display of services compared with the Scoring Engine.

When first connecting to the NISE, a member of the team should check for an initial inject task, usually identified as “Welcome” or something similar. The task simply requests a response back to the competition judges, signaling that access to the NISE has been successful, and that the responding team is ready to compete.

Once the competition judges have verified that all teams are ready to compete, or have provided ample time to respond, the competition judges will release a notification indicating the drop flag has been issued and the competition has started.

- Teams should be attentive to monitor inject requests and notifications via the Team Portal/NISE.
- 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/NISE.

- **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 MWCCDC Consortium Director. This may include the use of additional NISE to split and manage service scoring. Only one NISE 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.

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.

FTP

Access to the FTP service either via authentication or anonymous will be made, and the presence of various files will be checked.

TFTP

Access to the tftp service will be made to pull down a small file with an integrity check.

Schedule – all times CST

Friday, March 17, 2023

12:00-1:00 pm	Check-in at Moraine Valley Community College, Technology Building Receive Competition Packets, Team and Room Assignment, NISE & NETLAB passwords Team captain signs off team packet
1:00 pm	Fogelson Auditorium David Durkee - Welcome & Introduction to the 2023 Regional CCDC Keynote Speaker: Dan Manson, Board Member of the NCL (National Cyber League) A Word from our Sponsors (5 minutes for each sponsor)
3:00 pm	**Student Networking Event/Mingle with the Sponsors**
4:30 pm	Students return to competition room/ login to NISE/ respond to Welcome inject
5:00 pm	Start of Competition; scoring begins
6:30 pm	Dinner – T100 Area – Food will be delivered to the team rooms so teams do not have to leave their rooms.
9:30 pm	Competition ends/Scoring ends for the day

Saturday, March 18, 2023

8:00-8:30am	Continental Breakfast Student Teams arrive at Moraine Valley Community College Go straight to the competition room
8:30am	Announcements via NISE
9:00am	Start of Competition; scoring begins
12:30pm	Lunch – T100 Area – teams filter through and return to their rooms
6:00pm	Competition ends/Scoring ends Dinner – T100 Area & Fogelson Foyer
7:00pm	Fogelson Theater - Presentations by Red & White Team representative(s) Announce final winners
7:30pm	Competition Director meets with First Place Team

Systems

1. Each team will start the competition with identically configured systems.
2. Teams will be provided all access credentials by the day 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.**
9. Teams must maintain “public” services as available from nominally all source IP addresses. Teams may block single IP addresses determined to be the source of malicious traffic. Teams should note that attempts to restrict or filter by IP source address may adversely affect scoring directly. Teams are prohibited from blocking access from entire IP subnets, or from placing a knife edge ACL at the ingress of their networks, attempting to allow only the scoring engine. Teams should be made aware that that controls are put in place and monitored by team based on traffic generation.
10. In the event of system lock or failure, teams will be able to request a complete restoration (scrub/snapshot) via a Tech Support inject released from the NISE. 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. Teams may not install additional software on the workstations used to access the competition network. Teams may use collaborative applications such as onenote, trello, slack, google docs, sharepoint, with the understanding it is for team collaboration, and these are newly created. You cannot use pre-build documents, that’s what your github site is for. Communication with anyone outside the team is prohibited.
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 Midwest CCDC. 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
2. Each team may have no more than two graduate students as team members.
3. 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 Site Administrator or a Gold Team member from MWCCDC Consortium 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. **Teams should not identify the school they represent to the White Team but communicate by team number.**
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 Black/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. Teams may freely access the list of Github team repository sites during the competition. These will be published during the competition.
6. An unbiased Red Team will probe, scan, and attempt to penetrate or disrupt each team's operations throughout the competition.
7. The Red Team is not granted access to the Cyber Stadium team networks outside of competition hours.
8. 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.
9. 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.
10. 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 Black/White Team via the password change request feature of the NISE. 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.
11. 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.
12. Each Blue Team will be provided with the same objectives and tasks.
13. Each Blue Team will be given the same inject scenario at the same time during the course of the competition.
14. Blue Teams may request information from the White 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 White Team. 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.

15. The White Team is responsible for implementing the scenario events, refereeing, team scoring and tabulation.
16. 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.
17. Scores for inject completion and incident reports will be maintained by the White 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.
18. 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, other than published Github repository sites.
5. Additional software or tools must be either free or open source within the limits of pre-determined internet accessibility. No software is permitted based on free trial.
6. Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition other than the published list of Github repositories.
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 White/Black 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 White 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 White Team. The White 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 White Team, in conjunction with the Red Team, will assess scores for incident report submission based on clarity, thoroughness, and accuracy. The White 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
10-30%	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 MWCCDC Consortium Director, the White/Black 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 MWCCDC Consortium, Gold, White, and Green Teams strive to make the Midwest CCDC 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/mwccdc. They are also forbidden from publishing, posting on the internet, or publicly communicating assessments of the Midwest CCDC, 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 Midwest CCDC, and may also enumerate participating teams and winners.

Sponsors:

Our Sponsors

Raytheon Technologies
Corporation
www.raytheon.com

Cisco Networking
Academy
www.netacad.com

Palo Alto Networks
www.paloaltonetworks.com

Crowdstrike, Inc.
www.crowdstrike.com

Battelle Memorial
Institute
www.battelle.org

Fortra, LLC
www.fortra.com

Secureworks, Inc.
www.secureworks.com

Center for Infrastructure
Assurance and Security
www.cias.utsa.edu

National Collegiate Cyber
Defense Competition
www.battelle.org

Midwest CCDC
www.cssia.org/mwccdc