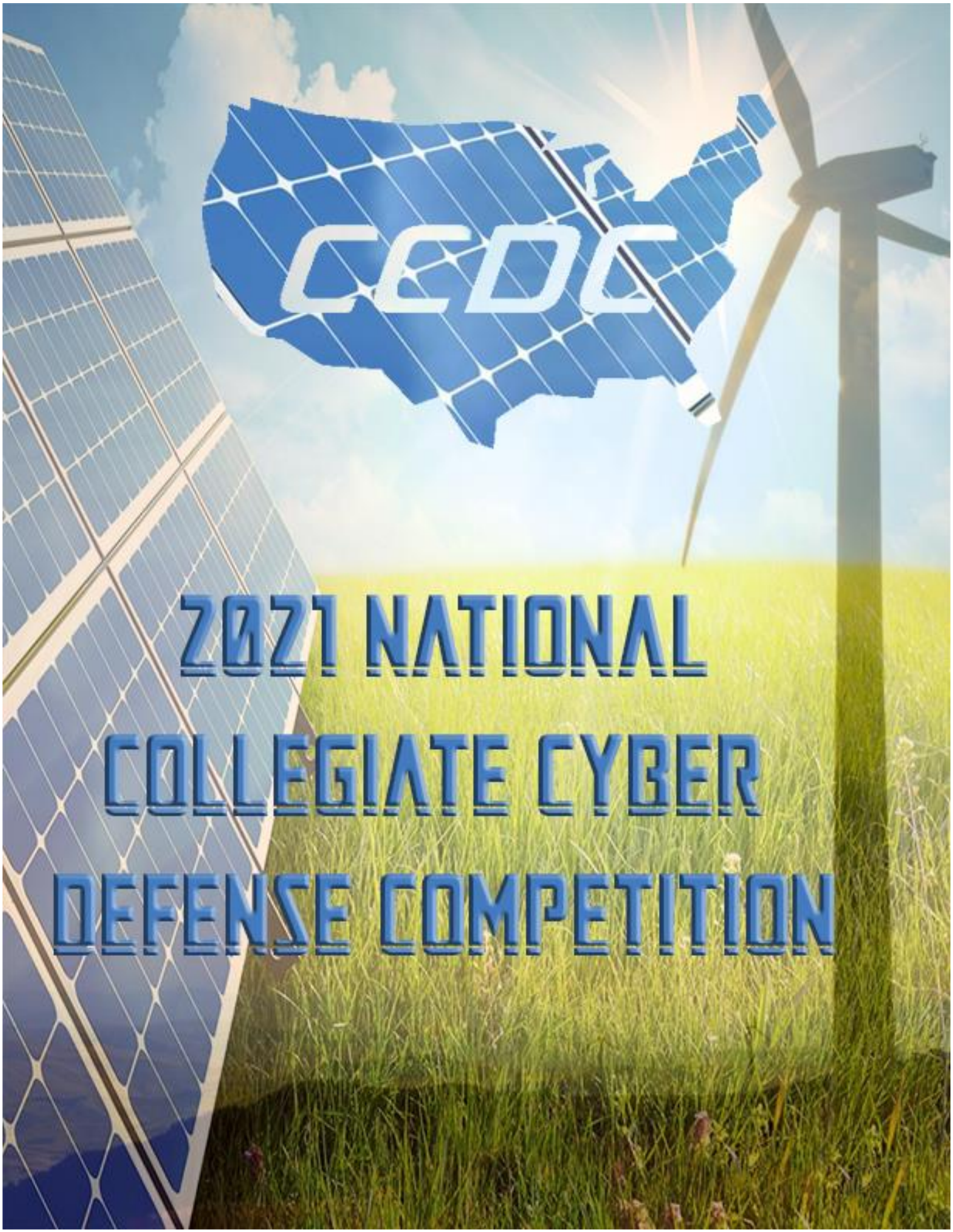

CCDC
2021 NATIONAL
COLLEGIATE CYBER
DEFENSE COMPETITION

2021 NCCDC

Team Packet

April 23-24, 2021

Table of Contents

Competition Schedule

Please note all times are in Central Time.

Friday, Apr 23rd

11:00 AM – 12:00 PM	Opening Ceremonies
12:00 PM – 8:15 PM	Competition Day 1

Saturday, Apr 24th

11:00 AM – 12:00 PM	Pre-competition briefing
12:00 PM – 8:15 PM	Competition Day 2

Sunday, Apr 25th

4:30 PM	Awards Pre-show
5:00 PM	Awards Ceremony

There are no competition activities outside of competition hours. Competitor access to the environment will be terminated at the end of each competition day. Scoring will stop when competition hours end. Please leave VMs running overnight. Please note these times may change – your coach and team captain will be notified of any schedule changes.

Sponsors

Competition Rules

Overview

The competition is designed to test each team's ability to secure and administer networked computer systems while maintaining standard business functionality. The scenario involves team members simulating a group of new employees brought in to integrate, manage and protect a fictional small business. Teams are expected to manage the computer network, keep it operational, address vulnerabilities/misconfigurations, and control/prevent any unauthorized access. Each team will be expected to maintain and provide a set of public services such as: a website, an email server, a database server, an application server, and workstations used by simulated sales, marketing, and research staff. Each team will start the competition with a set of identically configured systems.

The objective of the competition is to measure each 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. A technical success that impacts the business operation will result in a lower score, as will a business success which results in security weaknesses.

Throughout these rules, the following terms are used:

- Operations Team - competition officials that organize, run, and manage the competition.
- White Team - competition officials that observe team performance in their competition area and evaluate team performance and rule compliance.
- Red Team - penetration testing professionals simulating external hackers attempting to gain unauthorized access to Blue Team systems.
- Blue Team/Competition Team - the competitive teams consisting of students competing in a CCDC event.
- Team Captain - a student member of the Blue Team identified as the primary liaison between the Blue Team and the White Team or Operations Team.
- Team Co-Captain - a student member of the Blue Team identified as the secondary or backup liaison between the Blue Team and the White Team, should the Team Captain be unavailable (i.e., not in the competition room).
- Team representatives/Coach - a faculty or staff representative of the Blue Team's host institution responsible for serving as a liaison between competition officials and the Blue Team's institution.

1) **The NCCDC will be governed by the National CCDC ruleset posted here: http://www.nccdc.org/index.php/competition/competitors/rules.**
    a. Rule 10 has been suspended. Teams are NOT to gather together and there is no requirement for an onsite judge to be present at individual competitor locations

2) **Local Competition Rules – in additional to the National CCDC rules, the following rules will also be enforced during this event**
    a. Incident reports must be complete to receive any consideration for points. You may create your own form or use the form provided for you on the inject portal, but all incident reports must have team number, date, source IP, destination IP, date/time of activity, description of activity, and remediation/mitigation plans. Only incident reports that correspond to actual Red Team activity where your team lost points will be considered for point recovery. "I got port scanned" is not a valid incident response report (please don't waste your time with those type of incident reports).
    b. Teams must ensure all ESXi servers continue to forward syslog information to 10.120.0.201. Failure to do so will result in severe point penalties and may be grounds for disqualification.
    c. No unapproved operating system or application changes are permitted on Day One of the competition (servers or workstations) unless allowed via inject. You may patch, apply service packs, and update but you must defend what you are given for the first day. For example, you may upgrade from Debian 9.1 to 9.3, but not to Debian 10. You may upgrade from Apache 2.4.6 to Apache 2.4.9 but you may not migrate to Nginx.
    d. You may not containerize any scored platform or service unless instructed to do so in an inject. You may use containers for non-scored systems and services your team creates for their own use such as an IPS, sniffer, or team file server.
    e. You may not migrate or replicate any critical services to a different platform or system without authorization.
    f. You may setup a DMZ or NAT critical services provided the critical service is always reachable on the "public" IP address and fully qualified domain name it was initially assigned.
    g. You must configure all SMTP servers to allow the scoring engine to connect to and send mail from a valid user at your organization to another valid user at the same organization. For example, the scoring engine must be able to connect as bob@malachor.net and send email to tina@malachor.net.
    h. Teams must not intentionally disconnect competition systems from the network. All systems must remain connected to the network, be powered up, and be operational in their assigned role. This includes user workstations. Failure to do so will result in point deductions and may be grounds for disqualification.
    i. All inject responses and deliverables must be typed and delivered electronically via the inject portal.

j. You must maintain both the functionality and content of all critical services. For example, a website that serves dynamic content must continue to serve up dynamic content. An FTP service that allows anonymous access must continue to allow anonymous access.
k. Password changes to user accounts for critical services must be provided to the Operations team in electronic format via the inject portal. For more details refer to the discussion later in this team packet.
l. If you configure SPOP, you must inform the Operations Team **prior** to making the change and you must run SPOP on TCP port 995.
m. Injects will be delivered via the inject portal. Teams are responsible for monitoring the inject portal for injects and announcements.
n. VMs are monitored via the "CCSClient" service running on the VM. The CCSClient service must be able to communicate with 10.120.0.111 on TCP ports 80 and 443 at all times. If you reinstall or upgrade an operating system you must reinstall the CCS client. See the software portal for copies of the CCSClient.
o. Resetting or reverting provided VMs back to any snapshot will incur point penalties per the following schedule. Reversions counts are cumulative for all VMs over **both** days of competition (i.e., the total number of VM reversions your team performs during the entire competition). Reversions to VMs your team created for internal use are not included in the reversion total.
    i. 12 or fewer reversions: no penalty
    ii. 13 or more reversions: 50 points **per** reversion

Scoring

The winner will be determined by the highest cumulative score at the end of the competition. Accumulated point values are broken down as follows (some variance in points may occur due to the timing and randomization of scoring engine checks):

- Critical services account for roughly half the possible points (based on a random polling interval of core services)
- Successful completion of business tasks account for roughly half the possible points (awarded points will vary by task, but will be part of a cumulative total)

Successful Red Team actions will result in point deductions from a team's total score based on the level of access obtained, the sensitivity of information retrieved, critical services affected, and so on.

Functional Services

Certain services are always expected to be operational 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 semi-random intervals, certain services will be tested for functionality and content where appropriate. Each successfully served request will gain the team the specified number of points. Unresponsive services are always marked as failures.

HTTP/HTTPS

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 using an MD5 sum of the returned page and key words/phrases on the page. The returned content must match the expected content 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. SMTP services must always be able to support unauthenticated sessions. The scoring engine must be able to connect to your SMTP and be able to send mail from one valid user to another valid user. For example, bob@malachor.net must be able to send mail to tina@malachor.net.

POP3
A simulated user connection will be made using a valid userid and password to check for mail. POP services must accept logins as described in the critical service description. POP services must support logins with a simple userid and password (such as "bevans" with a password of "afk$tmgh"). SPOP, APOP, and plaintext are the only supported authentication methods. Changes in POP3 authentication must be coordinated with the Operations Team prior to implementation.

SSH
An SSH session will be initiated to the system using a valid user account and password. The user will attempt to execute a specific command within that session. If the login and command are successful, points are awarded.

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

FTP
Connections will be made to the FTP server (either as anonymous or as a valid user depending on what is detailed in the critical service description) to check for the presence and availability of specific files (both file presence and integrity are checked). Failed logins, missing files, or modified/corrupt files will cause the check to fail.

Each of the critical services operates under a Service Level Agreement (SLA) and teams will be assessed penalties for extended critical service outages. If any critical service is continuously down for 6 service checks, the team will be assessed a penalty. After a service is down for 6 consecutive checks, **each additional 6 consecutive checks** where the service is down will result in an additional penalty. For the first 2 hours of competition time on Day 1, SLA penalties cost the team 50 points per SLA penalty. After the first two hours of competition, SLA penalties cost the team 20 points per SLA penalty. SLA are calculated and assessed on a per service basis.

NOTE: If you modify the configuration of any critical service, such as adding a userid/password where none existed before, modifying a user level password, or changing authentication methods

you MUST coordinate with the Operations Team desk prior to making that change. In some cases, these changes may not be allowed if they interfere with business operations or competition scoring. Unapproved changes to the functionality of a scored service will result in point losses.

Business Tasks (Injects)
Each team will be presented with identical business tasks at various points during the competition. Points will be awarded based upon successful completion of each business tasking or part of a tasking. Tasks will vary in nature and points and will be weighted based upon the difficulty, importance, and time sensitivity of the tasking. Tasks may contain multiple parts with point values assigned to each specific part of the tasking.

Some examples:

- Opening an FTP service for 2 hours given a specific user name and password: 200 points
- Closing the FTP after the 2 hours is up: 50 points
- Creating/enabling new user accounts: 100 points
- Installing new software package on CEO's desktop within 30 minutes: 100 points

Every team must try to complete each task. Failure to attempt completion of any tasking will result in a team penalty and can result in a "firing" of team members. You MUST provide a response to ALL injects that require a written deliverable or report (even if your "deliverable" just says you didn't complete the inject). Please submit a response to all injects even if it is a simple acknowledgement of the inject or a message indicating your team did not complete the inject.

Red Team Actions
Successful Red Team actions will result in penalties that reduce the affected team's score. Red Team actions include the following (penalties and point values may be different than listed below):

- Obtaining root/administrator level access to a team system: -100 points
- Obtaining user level access to a team system (shell access or equivalent): -25 points
- Recovery of userids and passwords from a team system (encrypted or unencrypted): -50 points
- Recovery of one or more sensitive files or pieces of information from a team system (configuration files, corporate data, etc.): -25 points
- Recovery of customer credit card numbers: -50 points
- Recovery of personally identifiable customer information (name, address, and credit card number): -200 points
- Recovery of encrypted customer data or an encrypted database: -25 points

Red Team actions are cumulative. For example, a successful attack that yields root level access and allows the downloading of userids and passwords will result in a -150-point penalty. Red Team actions are scored on a **per system** and **per method** basis – a buffer overflow attack that allows the Red Team to penetrate a team's system will only be scored once for that system; however, a different attack that allows the Red Team to penetrate the same system will also be scored. Only the highest level of account access will be scored per attack – for example, if the Red Team compromises a single user account and obtains root access in the same attack the

penalty will be -100 points for root level access and not -125 points for root and user level access. Please note the point values described above are examples – actual penalty points may be adjusted to match competition environment.

Red Teams can also execute additional malicious action based on their access. Attacks such as defacing websites, disabling or stopping services, adding/removing users, and removing or modifying files are permitted and may occur.

Password Changes

If your team changes user level passwords for **scored** services that require a password (such as SSH or POP3) you must provide a comma separated text file containing your password changes to the Operations Team (in electronic format). The file should contain comma separated values with one user per line like this (no space after comma):

user,password
user2,password2

The only information inside the file should be the users and passwords – **do not** include headers or any other additional information inside the file. You must provide one file for EACH service that requires password changes – **do not** include multiple services in the same file. Name the file "TeamXX_SERVICE_PWD" and replace XX with your team number and SERVICE with the critical service these password changes apply to. For example, a password file for the SSH1 service must be named "TeamXX_ SSH1_PWD". An improperly named file will be rejected. Accepted files will be loaded into the scoring engine as is. You must allow 10 to 15 minutes for password changes to take effect. **You DO NOT need to provide us with password changes to "root" or "administrator" accounts – only user accounts.** Passwords can be up to 24 characters long and may consist of any combination of upper case letters, lower case letters, numbers, and the following special characters: . @ # $ % & ! ? : * ^ _ - + = < > ~

Password change files must be uploaded to the Inject Portal under the "Password Changes" inject. You must message competitions officials in the "#password_changes" channel on the competition Discord server each time you upload a password change file. Please remember you only need to submit password files for **scored** services that use passwords.

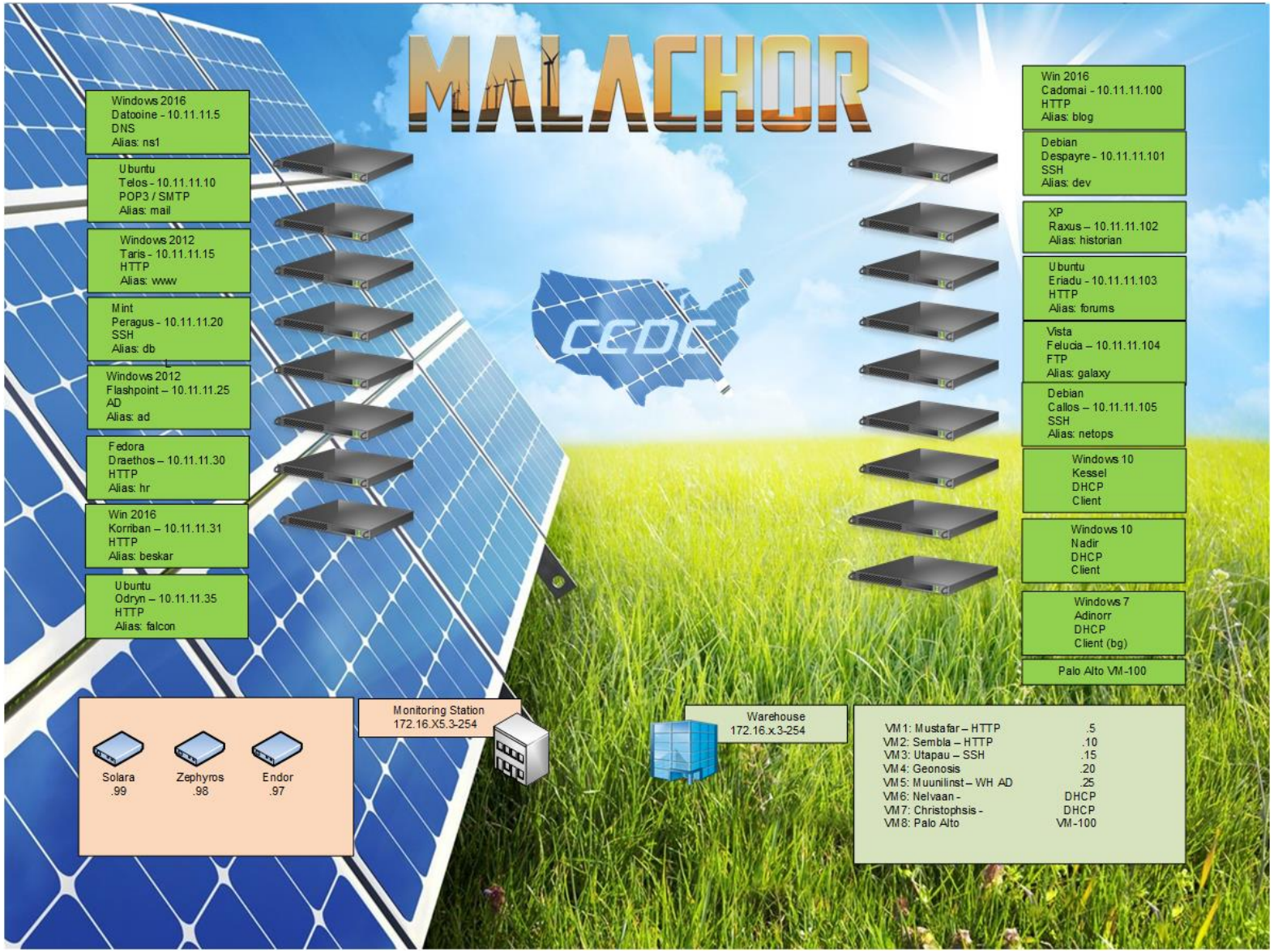
Competition Network Information

Here are some network addresses you will want to take note of:

10.120.0.9 – Internal Patch Server
10.120.0.10 – NTP server for official competition time (you can user pool.ntp.org as well)
10.120.0.20 – Inject Portal
X.X.X.1 – Gateway for your team networks will always be the .1 address of that network
10.X.X.3 – the IP address for your team's core ESXi server (where X is the external subnet for your team – team 4 is 10.40.40.3, team 7 is 10.70.70.3 and so on)
172.16.X.3 – the IP address for your team's warehouse ESXi server (where X is the external subnet for your team – team 4 is 172.16.40.3, team 7 is 172.16.70.3 and so on)
172.16.X5.3 – the IP address for your team's demo ESXi server (where X is the external subnet for your team – team 4 is 172.16.45.3, team 7 is 172.16.75.3, and so on)
255.255.255.0 – the subnet mask for all team networks (/24)

The internal patch server and the inject portal are "trusted assets" – any materials you download from them can be considered trusted as the Red Team does not have access to post materials on those systems. You may use any software you find on the internal patch server in this event.

Team Network Diagram



Letter from the CEO

From: Fenn Rau
To: New Cyber Security and IT Gurus
Subject: Welcome

Welcome to Malachor! We are thrilled to have you on board. As you know from your hiring briefings, we are a company that specializes in the sales, service, and installation of renewable energy systems such as wind turbines and solar panels. We recently had to replace a group of system administrators and security personnel. And they were not happy about being replaced. While everything "seems" to be working (at least on the surface) I'm quite sure we've got some major issues that need to be addressed on our network – and we're counting on you to do that for us. I can't guarantee documentation like this network map is completely accurate or up to date but it's the best we have at the moment. There are a few documents, like an outdated corporate directory, on the company's internal file server as well. I know it doesn't make "security" sense to have some of these services visible to the Internet, but we still have the majority of our office working from home. If our employees can't reach these systems they can't work. So, we have to find a way to keep these systems running and accessible to our staff. It's not an ideal situation, but let's make the best of it.

You are now responsible for managing and maintaining this entire network. Patch and repair as you see fit, but before making any big changes like replacing applications or operating systems contact me for approval. We're not making any big changes right away so plan on fixing what's here first and then we'll talk about changes later. Be careful when you upgrade/patch, as some of the systems are precisely configured to support current operations. Some of these applications might be sensitive to changes in patch level, passwords, and registry settings. You'll notice a few systems running rather old OSes – that's because they are running government recommended software packages related to our industry and those applications don't seem to work at all with modern OSes.

Make sure you can quickly roll back any changes that affect critical services. And make sure you backup our critical data! I'm not sure how long it's been…

Thank you and welcome aboard,

Fenn

Network Information from the Director of IT

The outline below details what little documentation was provided by the former administrative team on the inner workings of our infrastructure. While the executive staff recognizes this information is spotty at best, it should provide your team with enough details to get you started.

Overall Network Architecture:

Network Details:

Each team has its own ESXi server at the.3 address on **each** of your team networks (the password will be provided to your team captain). Critical services must be maintained on their assigned IP address to be scored properly. For example, the website visible to the "public" on 10.X.X.15 must be reachable at 10.X.X.15 at all times.

> **NOTE**: **The .1 address belongs to the operations network and are your default gateways for these networks. Do not attempt to use the .1 address of your team network. Do not scan, ping, probe, or interfere with .1. Do not change the IP address of your team's ESXi server.**

Externally, each team has assigned subnets as follows:

Team 1 – 10.10.10.X, 172.16.10.X, 172.16.15.X
Team 2 – 10.20.20.X, 172.16.20.X, 172.16.25.X
Team 3 – 10.30.30.X, 172.16.30.X, 172.16.35.X
Team 4 – 10.40.40.X, 172.16.40.X, 172.16.45.X
Team 5 – 10.50.50.X, 172.16.50.X, 172.16.55.X
Team 6 – 10.60.60.X, 172.16.60.X, 172.16.65.X
Team 7 – 10.70.70.X, 172.16.70.X, 172.16.75.X
Team 8 – 10.80.80.X, 172.16.80.X, 172.16.85.X
Team 9 – 10.90.90.X, 172.16.90.X, 172.16.95.X
Team 10 – 10.100.100.X, 172.16.100.X, 172.16.105.X

Do not attempt to connect to, probe, or reach any other team's network.

Networks available for additional internal NAT:
You may use any valid, private network for internal NAT if your team chooses to do so. If you choose to NAT your systems you must still provide "public" access to all critical services on their original IP addresses. For example, the static website must be reachable at its public IP address of 10.X.X.15 at all times.

Users:
Valid user accounts must remain active on all systems where they appear. You may not delete or disable valid user accounts. Accounts identified as administrators must have direct access to all critical services (RDP, SSH, FTP, and so on) on all servers and the ability to login to those services on all servers using their own accounts. For example, a user with administrative level permissions should be able to SSH to any of the scored SSH services and RDP or SSH to any server.

Company Directory:
A company directory is available in our corporate HRM system and will be available in the announcements section of the inject portal.

Passwords:

A password sheet with known administrator/root passwords will be distributed to your team.

DHCP:
Your corporate network must maintain the DHCP service on your corporate Active Directory server(s).

Critical Services:

For our business to function properly, the following services must always be available and open to **any** external IP address. Please note the names of the critical services – these are the names you must use when submitting password changes (i.e., use POP3 as the service name). The critical service **must** remain accessible on the IP address specified and must provide the content and functionality from its original configuration (unless you are directed to or required to make modifications by an inject). For example, an FTP service that supports anonymous read access must always support anonymous read access and a static website must provide all the original content throughout the competition. For SSH services all Malachor admins should be able to login to those SSH services using their own accounts.

- BLOG: You must maintain the HTTP service on 10.X.X.100
- DEMO: You must maintain the HTTP service on 172.16.X5.97
- DNS: You must maintain the DNS service on 10.X.X.5
- Dolibar: You must maintain the HTTP service on 10.X.X.31
- FTP_104: You must maintain the FTP service on 10.X.X.104. The FTP service must maintain anonymous read access at all times as it supports external customers.
- Forums: You must maintain the HTTP service on 10.X.X.103

- HRM: You must maintain the HTTP server on 10.X.X.30
- INVENTORY: You must maintain the HTTPS service running on TCP port 8443 on 172.16.X.5
- OTRS: You must maintain the HTTP server on 10.X.X.35
- POP3: You must maintain the POP3 service on 10.X.X.10
- SMTP: You must maintain the SMTP service on 10.X.X.10
- SOL: You must maintain the HTTP service running on TCP port 81 on 172.16.X5.99
- SSH_15: You must maintain the SSH service on 172.16.X.15
- SSH_20: You must maintain the SSH service on 10.X.X.20
- SSH_97: You must maintain the SSH service on 172.16.X5.97
- SSH_101: You must maintain the SSH service on 10.X.X.101
- SSH_105: You must maintain the SSH service on 10.X.X.105
- WH_TICKET: You must maintain the HTTP service on 172.16.X.10
- WWW: You must maintain the HTTP service on 10.X.X.15
- ZEP: You must maintain the HTTP service running on TCP port 81 on 172.16.X5.98

SSH, POP3, and SMTP services use userid/password lists in their service checks. If you change passwords associated with these services you must submit a password change file for all changed passwords. HTTP/HTTPS services do not use passwords lists.

NOTE: All critical services operate under an SLA agreement. A penalty of 20 points will be assessed **every time** an SLA violation occurs (50 points in the first two hours). An SLA violation is defined as the failure of 6 consecutive checks. All service checks are worth 1 point each. Service checks are run at random intervals (every 2 to 3 minutes).

Additional network services:

In addition to the critical services you are scored on, your team must also abide by the following directives concerning network traffic.

ICMP – You must always allow ICMP traffic from 10.120.0.0/16 to reach **all** systems in each of your networks. Your systems must respond to ICMP traffic from the

subnets listed above.

SSH – All Malachor admins should be able to SSH into servers running a scored SSH service from outside the organization.

RDP – All Malachor admins should be able to RDP into all Windows servers from outside the organization.

Internally you will also need to maintain:

File Servers
Client Workstations
Active Directory
Access to critical services
Internet Access for workstations

Outbound Services:

Your user base will need outbound access to common protocols such as HTTP, HTTPS, SSH, FTP, SFTP, POP3, DNS, and update services. All systems should be configured to use your team's DNS servers first (10.X.X.5) and 10.120.0.53 as the secondary DNS. You may need to adjust a system's DNS settings to reach the Internet.

As our business needs change, so might the preceding list of critical and outbound services shown above. The list provided is merely a snapshot in time of current critical services. Failure to provide any of these services for a prolonged amount time costs our company money and may ultimately cost you your job.

Please note that systems identified as a "Client" on the network map must remain user workstations and cannot be re-tasked, reloaded, or otherwise altered unless you receive an inject instructing you to do so.

Your systems inside the competition environment can only reach the Internet through a transparent proxy. While this should be fairly "transparent" for you, you will want to install the proxy certificates on your team VMs to remove the "invalid certificate" warnings from HTTPS sites. You may download the proxy certificates from the patch server (http://10.120.0.9/Proxy_Certificates/). You can also manually configure your VMs to use the proxy located at 10.120.0.200 TCP port 8080 (but that isn't really necessary – they're automatically routed through the proxy). If you are having issues reaching local HTTP/HTTPS services inside the competition environment on your competition VMs, configure your browser to bypass the proxy for those local systems. This includes some update sites that require HTTPS connections to retrieve files. NOTE: This only applies to the competition VMs – the Internet-bound traffic from your home system does not go through the VPN and is not affected by the proxy. You do not need to install the proxy certificates on your home system.