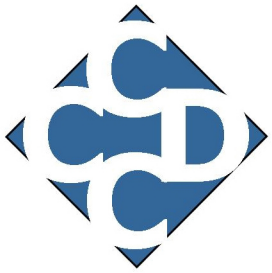

2019 At-Large
Collegiate Cyber
Defense
Competition

2019 ALCCDC



Collegiate Cyber Defense Competition

Team Packet

March 9-10, 2019

Table of Contents

Competition Schedule

Please note all times are in Central Time. Please also note that Daylight Saving time for the Central time zone begins at 2 AM on Mar 10th.

Saturday, Mar 9th

1:00 – 1:30 PM	Pre-competition briefing
1:30 – 8:00 PM	Competition Day 1

Sunday, Mar 10th

1:00 – 1:15 PM	Pre-competition briefing
1:15 – 8:00 PM	Competition Day 2

There are no competition activities outside of competition hours. Competitor access to the environment will be terminated at the end of each competition day.

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 manage and protect the IT infrastructure at a retail and online pharmacy chain. The teams are expected to manage the computer network, keep it operational, and control/prevent any unauthorized access. Each team will be expected to maintain and provide public services: 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:

- Gold Team/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 competition teams' systems.
- Black Team - competition support members that provide technical support, pick-up and deliver communications, and provide overall administrative support to the competition.
- Blue Team/Competition Team - the institution 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.
- 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 - 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) **Competitor Eligibility**
    a. Competitors in CCDC events must be full-time students of the institution they are representing.
        i. Team members must qualify as full-time students as defined by the institution they are attending.
        ii. Individual competitors may participate in CCDC events for a maximum of five seasons. A CCDC season is defined as the period between the start of the first state event and the completion of the National CCDC event. Participation on a team in any CCDC event during a given season counts as participation for that entire season.
        iii. A competitor in their final semester prior to graduation is exempt from the full-time student requirement and may compete in CCDC events as a part-time student provided the competitor has a demonstrated record of full-time attendance for the previous semester or quarter.
        iv. If a team member competes in a qualifying, state, or regional CCDC event and graduates before the next CCDC event in the same season, that team member will be allowed to continue to compete at CCDC events during the same season should their team win and advance to the next round of competition.
    b. Competitors may only be a member of one team per CCDC season.
    c. A team member may not participate in any role at CCDC events held outside the region in which their team competes during the same CCDC season.
    d. Individuals who have participated in previous CCDC events in any role other than as a competitor must obtain eligibility approval from the director of the region in which their team competes prior to being added to the team roster. Once a candidate's eligibility has been approved they will remain eligible for all CCDC events during the same season.

2) **Team Composition**
    a. Each team must submit a roster of up to 12 competitors to the competition director of the first CCDC event they participate in during a given CCDC competition season. Rosters must be submitted at least two weeks prior to the start of that event. All competitors on the roster must meet all stated eligibility requirements. No changes to the team roster will be permitted after the team competes in their first CCDC event. The competition team must be chosen from the submitted roster. A competition team is defined as the group of individuals competing in a CCDC event.
    b. Each competition team may consist of up to eight (8) members chosen from the submitted roster.
    c. Each competition team may have no more than two (2) graduate students as team members.
    d. If the member of a competition team advancing to a qualifying, state, regional, or national competition is unable to attend that competition, that team may substitute another student from the roster in their place prior to the start of that competition.

e. Once a CCDC event has begun, a team must complete the competition with the team that started the competition. Substitutions, additions, or removals of team members are prohibited except for extreme circumstances.

    i. Team Representatives must petition the Competition Director in writing for the right to perform a change to the competition team.
    ii. The Competition Director must approve any substitutions or additions prior to those actions occurring.

f. Teams or team members arriving after an event's official start time, for reasons beyond their control, may be allowed to join the competition provided a substitution has not already been made. Event coordinators will review the reason for tardiness and make the final determination.
g. 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. In the event of the Team Captain's absence, teams must have an identified team liaison serving as the captain in the competition space during competition hours.
h. An institution is only allowed to compete one team in any CCDC event or season.
i. A CCDC team may only compete in one region during any given CCDC season.
j. Exhibition teams are not eligible to win any CCDC event and will not be considered for placement rankings in any CCDC event.

3) **Team Representatives**

a. Each team must have at least one representative present at every CCDC event. The representative must be a faculty or staff member of the institution the team is representing.
b. Once a CCDC event has started, representatives may not coach, assist, or advise their team until the completion of that event (including overnight hours for multi-day competitions).
c. Representatives may not enter their team's competition space during any CCDC event.
d. Representatives must not interfere with any other competing team.
e. The representative, or any non-team member, must not discuss any aspect of the competition event, specifically event injections, configurations, operations, team performance or red team functions, with their team during CCDC competition hours and must not attempt to influence their team's performance in any way.
f. Team representatives/coaches may not participate on the Red Team, Gold Team, Operations Team, Black Team, White Team, or Orange Team at any CCDC event.

4) **Competition Conduct**
   a. Throughout the competition, Operations and White Team members will occasionally need access to a team's system(s) for scoring, troubleshooting, etc. Teams must immediately allow Operations and White Team members' access when requested.
   b. Teams must not connect any devices or peripherals to the competition network unless specifically authorized to do so by Operations or White Team members.
   c. Teams may not modify the hardware configurations of competition systems. Teams must not open the case of any server, printer, PC, monitor, KVM, router, switch, firewall, or any other piece of equipment used during the competition. All hardware related questions and issues should be referred to the White Team.
   d. Teams may not remove **any** item from the competition area unless specifically authorized to do so by Operations or White Team members including items brought into the team areas at the start of the competition.
   e. Team members are forbidden from entering or attempting to enter another team's competition workspace or room during CCDC events.
   f. Teams must compete without "outside assistance" from non-team members including team representatives from the start of the competition to the end of the competition (including overnight hours for multi-day events). All private communications (calls, emails, chat, texting, directed emails, forum postings, conversations, requests for assistance, etc) with non-team members including team representatives that would help the team gain an unfair advantage are not allowed and are grounds for disqualification and/or a penalty assigned to the appropriate team.
   g. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.
   h. Team representatives, sponsors, and observers are not competitors and are prohibited from directly assisting any competitor through direct advice, "suggestions", or hands-on assistance. Any team sponsor or observers found assisting a team will be asked to leave the competition area for the duration of the competition and/or a penalty will be assigned to the appropriate team.
   i. Team members will not initiate any contact with members of the Red Team during the hours of live competition. Team members are free to talk to Red Team members during official competition events such as breakfasts, dinners, mixers, and receptions that occur outside of live competition hours.
   j. Teams are free to examine their own systems but no offensive activity against any system outside the team's assigned network(s), including those of other CCDC teams, will be tolerated. Any team performing offensive activity against any system outside the team's assigned network(s) will be immediately disqualified from the competition. If there are any questions or concerns during the competition about whether specific actions can be considered offensive in nature contact the Operations Team before performing those actions.

k. Teams can 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.
l. All team members will wear badges identifying team affiliation during competition hours.
m. Only Operations Team/White Team members will be allowed in competition areas outside of competition hours.

5) **Internet Usage**
   a. Internet resources such as FAQs, how-to's, existing forums and responses, and company websites, are completely valid for competition use provided there is no fee required to access those resources and access to those resources has not been granted based on a previous membership, purchase, or fee. Only resources that could reasonably be available to all teams are permitted. For example, accessing Cisco resources through a CCO account would not be permitted but searching a public Cisco support forum would be permitted. Public sites such as Security Focus or Packetstorm are acceptable. Only public resources that every team could access if they chose to are permitted.
   b. Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition. Teams are not allowed to access private Internet-accessible libraries, FTP sites, web sites, network storage, email accounts, or shared drives during the competition. All Internet resources used during the competition must be freely available to all other teams. The use of external collaboration and storage environments such as Google Docs/Drive is prohibited unless the environment was provided by and is administered by competition officials. Accessing private staging areas or email accounts is grounds for disqualification and/or a penalty assigned to the appropriate team.
   c. No peer to peer or distributed file sharing clients or servers are permitted on competition networks unless specifically authorized by the competition officials.
   d. Internet activity, where allowed, will be monitored and any team member caught viewing inappropriate or unauthorized content will be subject to disqualification and/or a penalty assigned to the appropriate team. This includes direct contact with outside sources through AIM/chat/email or any other public or non-public services including sites such as Facebook. For the purposes of this competition inappropriate content includes pornography or explicit materials, pirated media files, sites containing key generators and pirated software, etc. If there are any questions or concerns during the competition about whether specific materials are unauthorized contact the White Team immediately.
   e. All network activity that takes place on the competition network may be logged and subject to release. Competition officials are not responsible for the security of any information, including login credentials, which competitors place on the competition network.

6) **Permitted Materials**

a. No memory sticks, flash drives, removable drives, CDROMs, electronic media, or other similar electronic devices are allowed in the room during the competition unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.
b. Teams may not bring any type of computer, laptop, tablet, PDA, cell phone, smart phone, or wireless device into the competition area unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.
c. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition as specified by the competition officials.

7) **Professional Conduct**
   a. All participants, including competitors, coaches, White Team, Red Team, Ops Team, and Gold Team members, are expected to behave professionally during all CCDC events including preparation meetings, receptions, mixers, banquets, competitions and so on.
   b. In addition to published CCDC rules, Host Site policies and rules apply throughout the competition and must be respected by all CCDC participants.
   c. All CCDC events are alcohol free events. No drinking is permitted at any time during competition hours.
   d. Activities such as swearing, consumption of alcohol or illegal drugs, disrespectful or unruly behavior, sexual harassment, improper physical contact, becoming argumentative, willful violence, or willful physical damage have no place at the competition and will not be tolerated.
   e. Violations of the rules can be deemed unprofessional conduct if determined to be intentional or malicious by competition officials.
   f. Competitors behaving in an unprofessional manner may receive a warning from the White Team, Gold Team, or Operations Team for their first offense. For egregious actions or for subsequent violations following a warning, competitors may have a penalty assessed against their team, be disqualified, and/or expelled from the competition site. Competitors expelled for unprofessional conduct will be banned from future CCDC competitions for a period of no less than 12 months from the date of their expulsion.
   g. Individual(s), other than competitors, behaving in an unprofessional manner may be warned against such behavior by the White Team or asked to leave the competition entirely by the Competition Director, the Operations Team, or Gold Team.

8) **Questions, Disputes, and Disclosures**
   a. PRIOR TO THE COMPETITION: Team captains are encouraged to work with the Competition Director and their staff to resolve any questions regarding the rules of the competition or scoring methods before the competition begins.
   b. DURING THE COMPETITION: Protests by any team must be presented in writing by the Team Captain to the White Team as soon as possible. The

competition officials will be the final arbitrators for any protests or questions arising before, during, or after the competition. Rulings by the competition officials are final. All competition results are official and final as of the Closing Ceremony.

c. In the event of an individual disqualification, that team member must leave the competition area immediately upon notification of disqualification and must not re-enter the competition area at any time. Disqualified individuals are also ineligible for individual or team awards.
d. In the event of a team disqualification, the entire team must leave the competition area immediately upon notice of disqualification and is ineligible for any individual or team award.
e. All competition materials including injects, scoring sheets, and team-generated reports and documents must remain in the competition area. Only materials brought into the competition area by the student teams may be removed after the competition concludes.

9) **Scoring**

a. Scoring will be based on keeping required services up, controlling/preventing un-authorized access, and completing business tasks that will be provided throughout the competition. Teams accumulate points by successfully completing injects and maintaining services. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by the Red Team.
b. Scores will be maintained by the competition officials and may be shared at the end of the competition. There will be no running totals provided during the competition. Team rankings may be provided at the beginning of each competition day.
c. Any team action that interrupts the scoring system is exclusively the responsibility of that team and will result in a lower score. Any team member that modifies a competition system or system component, with or without intent, to mislead the scoring engine into assessing a system or service as operational, when in fact it is not, may be disqualified and/or the team assessed penalties. Should any question arise about scoring, the scoring engine, or how scoring functions, the Team Captain should immediately contact the competition officials to address the issue.
d. Teams are strongly encouraged to provide incident reports for each Red Team incident they detect. Incident reports can be completed as needed throughout the competition and presented to the White Team for collection. Incident reports must contain a description of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, access obtained, damage done, etc), a discussion of what was affected, and a remediation plan. A thorough incident report that correctly identifies and addresses a successful Red Team attack may reduce the Red Team penalty for that event – no partial points will be given for incomplete or vague incident reports.

10) **Remote/ Team Site Judging and Compliance**

With the advent of viable remote access technologies and virtualization, teams will have

the ability to participate in CCDC events from their respective institutions. This section addresses policy for proper engagement in CCDC events for remote teams.

a. Remote teams are required to compete from a location with controlled access, i.e., a separate room or a portion of a room that is dedicated for use during the CCDC event. Workstations and internet access must comply with published requirements.
b. One or more Remote Site Judge(s) must be assigned to the team site. At least one Remote Site Judge must be present at the remote site for the duration of the event in order to facilitate the execution of the CCDC. The qualifications of Remote Site Judge are the same as Event Judge. Subject to the specifications of the remote competition, the responsibilities of the Remote Site Judge may include the following:
    i. Be present with the participating team to assure compliance with all event rules
    ii. Provide direction and clarification to the team as to rules and requirements
    iii. Establish communication with all Event Judges and provide status when requested
    iv. Provide technical assistance to remote teams regarding use of the remote system
    v. Review all equipment to be used *(SECCDC: before and)* during the remote competition for compliance with all event rules
    vi. Assure that the Team Captain has communicated to the Event Judges approval of initial system integrity and remote system functionality
    vii. Assist Event Judges in the resolution of grievances and disciplinary action, including possible disqualification, where needed
    viii. Report excessive misconduct to local security or police
    ix. Assess completion of various injects based on timeliness and quality when requested by Event Judges
    x. Act as a liaison to site personnel responsible for core networking and internet connectivity
    xi. Provide direct technical assistance to teams when requested by Event Judges
    xii. Provide feedback to students subsequent to the completion of the CCDC event
c. A recommendation for Remote Site Judge(s) is expected to be given from a Team representative of the participating institution to the CCDC Event Manager. Remote Site Judge(s) must not be currently employed, a student of, or otherwise affiliated with the participating institution, other than membership on an advisory board. CCDC Event Managers should also be apprised of a contact from the participating institution responsible for core networking and internet connectivity that will be available during the CCDC event.

11) **Local Competition Rules**

a. Incident reports must be complete to receive any consideration for points. You may create your own form, 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.

b. No unapproved operating system or application changes are permitted on Day One of the competition (servers or workstations). You may patch, apply service packs, and update but you must defend what you are given for the first day.
c. You many not containerize any platform or service without authorization.
d. You may not migrate or replicate any critical services to a different platform or system without authorization.
e. 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.
f. 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@kwikiepills.com and send email to tina@kwikiepills.com.
g. 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.
h. All inject responses and deliverables must be typed and delivered electronically via officially approved mechanisms.
i. 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.
j. Password changes to user accounts for critical services must be provided to the Operations team in electronic format. For more details refer to the discussion in your team packet.
k. If you configure SPOP, you must inform the Operations Team prior to making the change and you must run SPOP on TCP port 995.

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@kwikiepills.com must be able to send mail to tina@kwikiepills.com.

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 10 service checks, the team will be assessed a 20-point penalty. After a service is down for 10 consecutive checks, **each additional 10 consecutive checks** where the service is down will result in an additional 20-point penalty.

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.

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). If the inject does not require a deliverable (report, memo, note, etc.) then you do not need to submit an inject response.

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, POP3, and FTP) 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:

user, password
user2, password2

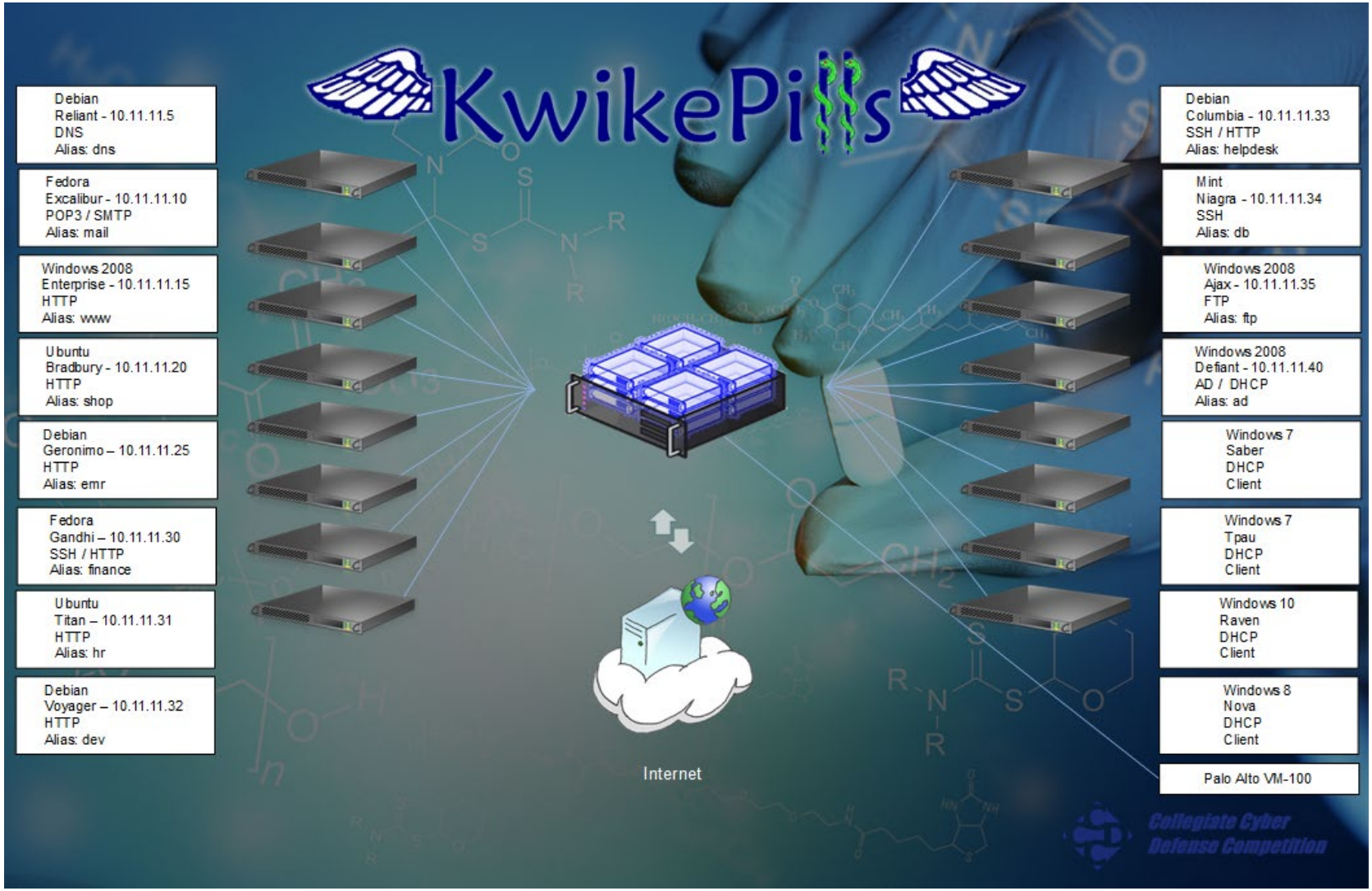
The only information inside the file should be the users and passwords – **do not** include headers or any other additional information inside the file. You must provide 1 file for EACH service that requires password changes – **do not** include multiple services in the same file. Name the file "TeamXX_SERVICE_PWD" 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.** You must upload password changes via officially provided channels and you must inform the Operations Team when you have uploaded a new password file. 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: . @ # $ % & ! ? : * ^ _ - + = < > ~

Competition Network Information

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

10.120.0.5 – Team portal
10.120.0.10 – NTP server for official competition time
10.120.0.20 – Inject server
10.11.11.1 – Default route for your team's core network

Team Network Diagram



Letter from the CEO

From: Tom Malik
To: New Cyber Security and IT Gurus
Subject: Welcome

Welcome to Kwikepills! We are thrilled to have you on board. As you know from your hiring briefings, we are a chain of retail and online pharmacies. Our previous administrative staff is no longer with us. The network and services seem to be "working", but I would not take anything for granted. I have my suspicions our network was hacked into recently and I'm sure the previous admins would not have detected it.

You are now responsible for managing and maintaining this network. Patch and repair as you see fit, but before making any big changes like replacing applications or operating systems come see 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. 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. Make sure you can quickly roll back any changes that affect critical services. And make sure you backup our critical data!

Thank you and welcome aboard,

Tom

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 an identical network which is NAT'd based on your team number. Your internal network addresses will all be 10.11.11.X. When you log into your ESXi server you will see all the local VMs have a 10.11.11.X address. Critical services must be maintained on their assigned IP address to be scored properly. For example, the static website is visible to the outside on a 10.X.X.15 address but must be reachable at 10.11.11.15 inside your team network at all times.

> **NOTE**: **The .1 and .254 addresses belong to the operations network and are your default gateways for these networks. Do not attempt to use the .1 or .254 address inside your team network. Do not scan, ping, probe, or interfere with .1 and .254. Do not change the IP address of your team's ESXi server.**

Externally, each team has an assigned subnet as follows:

Team 1 – 10.10.10.X
Team 2 – 10.20.20.X
Team 3 – 10.30.30.X
Team 4 – 10.40.40.X
Team 5 – 10.50.50.X
Team 6 – 10.60.60.X
Team 7 – 10.70.70.X
Team 8 – 10.80.80.X

The scoring engine will be checking your services on those external IP addresses. You will also be able to reach the external addresses for your team's systems from your VPN connection – so you can "see" exactly what the scoring engine "sees". Your team has no control over the 10.X.X.X to 10.11.11.X NAT mappings and those will not change during the competition.

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 10.11.11.15 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) and the ability to login to those services 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/SSH to any server.

Company Directory:
A company directory is available in our corporate HRM system.

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.

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 (ie 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 Kwikepills admins should be able to login to those SSH services.

- DNS: You must maintain the DNS service on 10.11.11.5
- POP3: You must maintain the POP3 service on 10.11.11.10
- SMTP: You must maintain the SMTP service on 10.11.11.10
- WWW: You must maintain the HTTP service on 10.11.11.15
- SHOP: You must maintain the HTTP service on 10.11.11.20
- EMR: You must maintain the HTTP service on 10.11.11.25
- SSH1: You must maintain the SSH service on 10.11.11.30
- HRM: You must maintain the HTTP service on 10.11.11.31

- SSH2: You must maintain the SSH service on 10.11.11.33
- SSH3: You must maintain the SSH service on 10.11.11.34
- FTP: You must maintain the FTP service on 10.11.11.35

NOTE: All critical services operate under an SLA agreement. A penalty will be assessed **every time** an SLA violation occurs. An SLA violation is defined as the failure of 10 consecutive checks.

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, 10.111.0.0/16, and 192.168.251.0/24 to reach **all** systems in each of your networks. Your systems must respond to ICMP traffic from the subnets listed above.

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 server first (10.X.X.5) and a public DNS (such as 1.1.1.1 or 8.8.4.4) second.

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" must remain user workstations and cannot be re-tasked, reloaded, or otherwise altered unless you receive an inject instructing you to do so.