Welcome To The 2020 MIAMI National Collegiate Cyber Defense Competition

NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

Presented by

Raytheon Technologies

2020 National Championship

May 22 – 23, 2020

Team Packet

Conducted by the Center for Infrastructure Assurance and Security

CIAS
CENTER FOR INFRASTRUCTURE ASSURANCE AND SECURITY
UTSA

Table of Contents

On behalf of the Center for Infrastructure Assurance and Security (CIAS) and The University of Texas at San Antonio (UTSA), I'd like to welcome each of you to the National Collegiate Cyber Defense Competition. You have already won your regional competition and have demonstrated your operational skills and information security capabilities. We hope you will find this national competition a challenging learning experience which enhances and expands your skill set. We apologize for not being able to provide you with the full "in person" NCCDC experience and appreciate your flexibility and willingness to participate under the current circumstances.

The CIAS and UTSA are excited to host the NCCDC, and we are very thankful to Raytheon, our sponsors, and our industry partners. Our staff, volunteers, and sponsors work hard to make this an interesting, exciting, and challenging competition. As most of you know, this event has grown from modest beginnings to a significant positive impact on security programs around the nation. The competition is receiving increased attention from government and industry, and we expect this attention to continue to grow. As competitors, your input is valuable - the entire CCDC program has been shaped and refined based on feedback from past competitors. Please provide comments and feedback to help us improve the NCCDC and other future events. We wish you and your team the very best of luck!

Gregory B. White, Ph.D.
Director
Center for Infrastructure Assurance and Security

2020 NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

Presented by

Raytheon Technologies

PLATINUM SPONSORS

Walmart InfoSec

UBER

PROGRAM SPONSORS

SAIC
Redefining Ingenuity

paloalto Cybersecurity Academy

RSM

GOLD SPONSORS

information security

abs Global Trading Limited

SILVER SPONSORS

DIRECTORATE OF CYBERSECURITY

Randori

FORCEPOINT

SPONSORS

Women in Cybersecurity WiCyS

KPMG

NDG

Carnegie Mellon University Information Networking Institute

COBALT STRIKE

AIR FORCE CIVILIAN SERVICE
Forces. Joined.

UNIVERSITY of WASHINGTON | BOTHELL
CYBER SECURITY ENGINEERING

Competition Schedule

Please note that due to the nature of the competition, schedule changes may occur. Please note all times listed are Central time.

Thursday, May 21st

4 PM – 7 PM	Virtual Career Fair

Friday, May 22nd

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

Saturday, May 23rd

11:30 AM – 12:00 PM	Morning Announcements
12:00 – 8:15 PM	Competition Hours – Day 2

Sunday, May 24th

5:30 PM	Pre-awards ceremony remarks
6:00 PM	Awards Ceremony

Please note competitor VPN access will be terminated at the end of Day 1 and will remain unavailable until start time on Day 2. Accessing the environment outside of competition hours in any way is prohibited.

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 small aerospace and defense Contractor. 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) **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 – the following rules will be enforced during the NCCDC**

    a. Incident reports must be complete to receive any consideration for points. You must create your own form and 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. Incident reports must be turned in on the day the activity occurred to receive credit.
    b. Teams must ensure all of their ESXi servers continue to forward syslog information to 10.120.0.201 at all times. 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). 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 asked 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@hylian.net and send email to pat@hylian.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. Teams must ensure the CCS client installed on competition VMs is active, running, and reporting to the CCS server. Point penalties will be assessed for CCS outages.

j. All inject responses and deliverables must be typed and delivered electronically via the inject portal.
k. 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.
l. 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 later in this team packet.
m. If you configure SPOP, you must inform the Operations Team prior to making the change and you must run SPOP on TCP port 995.
n. Resetting or reverting **scored** VMs back to any snapshot will incur point penalties per the following schedule:
    i. Reset/reversion 1 through 3: no penalty
    ii. Reset/reversion 4 through 7: 25 points per reversion
    iii. Reset/reversions 8 and up: 50 points per reversion
    iv. There are no penalties for resetting/reverting VMs a team creates for their own use such as an IPS, sniffer, or internal team file server.
    v. Reversions are calculated on a per VM basis - reverting a single VM 4 times would result in a penalty, reverting 10 VMs 2 times each would not result in any penalties
o. GitHub projects written by team members or affiliates must have existed and have been publicly available for at least 3 months prior to the NCCDC. All requests for access to GitHub or other Internet resources will be reviewed and may be denied if deemed inappropriate for competition use.
p. Teams may not use cloud services such as AWS or Azure outside the competition environment. Teams may not export data outside the competition environment to any cloud services. Teams may take screenshots and notes on their home systems to facilitate inject creation and competition operations.
q. Teams may not install VMWare Tools on any competition VM and are prohibited from mounting USB drives or external devices to any competition VMs. Teams must download software and files directly to competition VMs from approved sites (those already in the proxy) or from the internal competition patch server. Teams may transfer files between competition VMs at any time.
r. Teams may not use any unapproved method of transferring data into the competition environment. This includes but is not limited to "cut and paste" workaround sites, file servers, forum posting with the intent to download, and so on.

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@hylian.net must be able to send mail to tina@hylian.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. Throughout the competition, if any critical service is continuously down for 6 consecutive checks, the team will be assessed an SLA penalty for that service. 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.

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, modifying routing tables, 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 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.** 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: . @ # $ % & ! ? : * ^ _ - + = < > ~

Do not use any special characters in passwords other than those in the approved list above.

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. For clarity, please append a number to the name of your password change file every time you upload a new password file for that service – for example TeamXX_ SSH1_PWD_2 for the second password change file for SSH1, TeamXX_ SSH1_PWD_3 for the third, and so on.

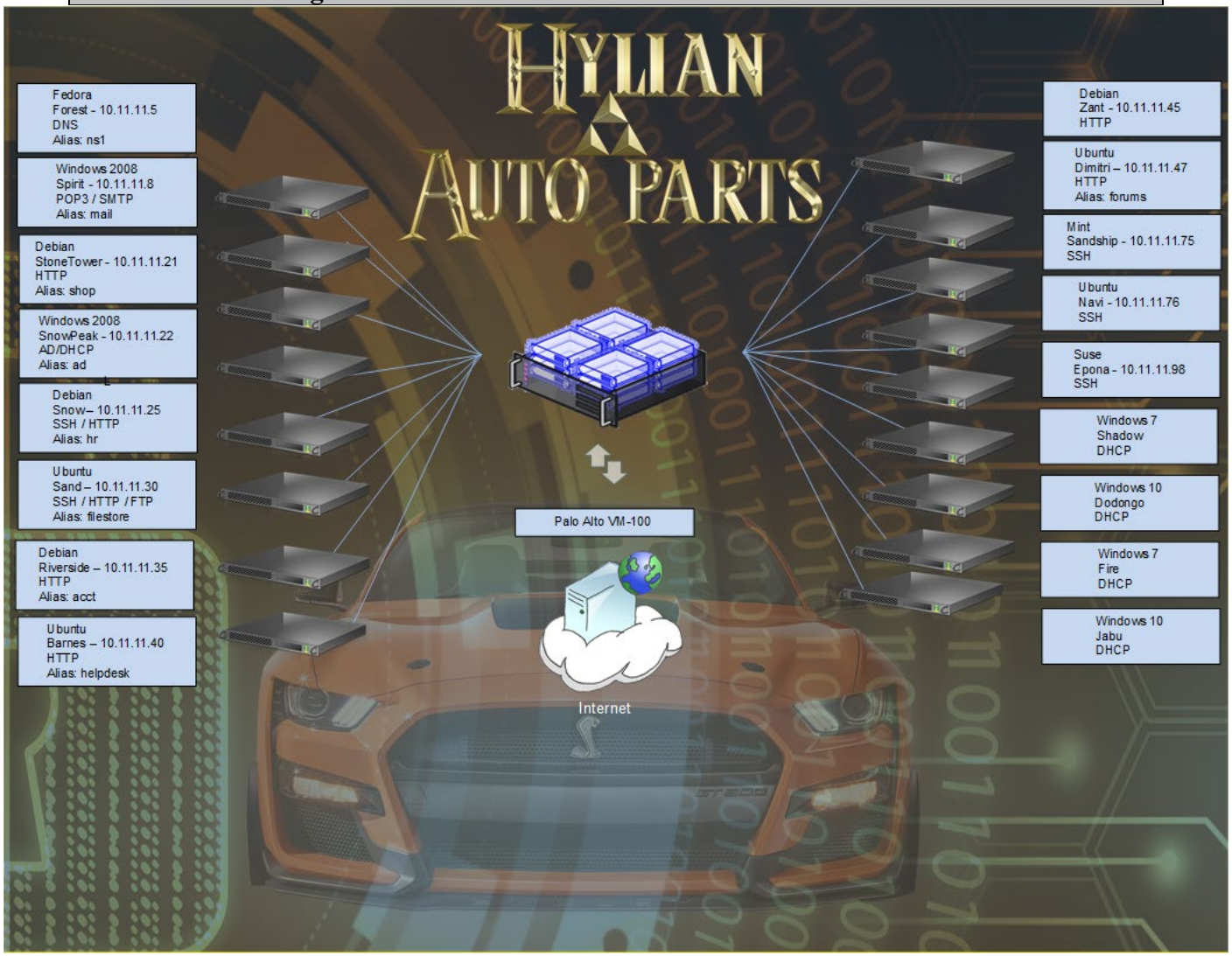
Competition Network Information

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
10.120.0.20 – Inject Portal
10.120.0.111 – CCS server (you must allow your competition VMs to reach TCP ports 80 and 443 on this server)
10.120.0.201 – Syslog server (you must allow your ESXi systems to send syslog messages here)
10.11.11.1 – Default route for your team's Main network inside your Main ESXi server
10.X.X.3 – the IP address for your team's Main 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 primary Cloud 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.X.4 - the IP address for your team's secondary Cloud ESXi server (where X is the external subnet for your team – team 4 is 172.16.40.4, team 7 is 172.16.70.4 and so on)

The internal patch server and the inject portal are "protected 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: Link
To: New Cyber Security and IT Gurus
Subject: Welcome

Welcome to Hylian! We are thrilled to have you on board. As you know from your hiring briefings, we are an auto parts retailer. Some our previous administrative staff are no longer with us and those that are still with us don't seem always do the right thing. 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 neither the previous or current admins would 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 or our CIO 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!

Our network has two major sections. Our "main" headquarters office and a cloud presence I'll tell you about later on your first day. Administrators should be able to reach remote systems using RDP or SSH as appropriate (RDP for Windows systems, SSH for non-Windows typically). You are responsible for securing and operating both network environments. For security reasons, the cloud systems are connected to the main network with a direct link and are only accessible from the main systems.

Thank you,

Link

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:

Teams are assigned IP blocks as listed below (Main – 10.X.X.X, Cloud – 172.16.X.X):

Team 1 10.10.10.0, 172.16.10.0
Team 2 10.20.20.0, 172.16.20.0
Team 3 10.30.30.0, 172.16.30.0
Team 4 10.40.40.0, 172.16.40.0
Team 5 10.50.50.0, 172.16.50.0
Team 6 10.60.60.0, 172.16.60.0
Team 7 10.70.70.0, 172.16.70.0
Team 8 10.80.80.0, 172.16.80.0
Team 9 10.90.90.0, 172.16.90.0
Team 10 10.100.100.0, 172.16.100.0

Subnet mask: 255.255.255.0
Default gateway: Always the .1 address of the network.

NOTE: **The .1 addresses on the above subnets belong to the operations network and are your default gateways for these networks. Do not attempt to use the .1 address inside your team network. Do not scan, ping, probe, or interfere with .1.**

Additional information regarding the Cloud network will not be disclosed before the start of the competition.

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, SMB, 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 remote system using their own account.

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

Passwords:

A password sheet with known administrator/root passwords will be supplied to your team captain prior to competition start.

Internet Proxy:
All Internet bound traffic from the competition VMs will pass through a transparent proxy. Connection attempts to sites not allowed in the proxy will be denied. You may submit written requests to add sites to the proxy via Discord in the #proxy_requests channel. Sites will be reviewed and may or may not be added at the discretion of competition officials.

SSL Certificates for the proxy can be found on the software portal in a directory called "Proxy Certificates". Installing these certificates on your systems will help address any issues you might have with certificate errors. Please install the certificate as a "Trusted Root Certification Authority" and not as a personal certificate.

DHCP:
Your corporate network must maintain a DHCP service with an address pool from 10.X.X.101 to 10.X.X.150 (where X is your team network, Team 1=10, Team 2=20, and so on).

Critical Services:

For our business to function properly, the following services must always be available and open to **any** external IP address (except the SMB services as described below). 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.

- DNS1: You must maintain the DNS service on 10.X.X.5
- FINANCE: You must maintain the HTTP service on 10.X.X.35
- FORUM: You must maintain the HTTP service on 10.X.X.47
- FTP: You must maintain the FTP service on 10.X.X.30
- HDESK: You must maintain the HTTP service on 10.X.X.40
- HR: You must maintain the HTTP service on 10.X.X.25
- INV: You must maintain the HTTP service on 10.X.X.45
- POP3: You must maintain the POP3 service on 10.X.X.8
- SMTP: You must maintain the SMTP service on 10.X.X.8
- SHOP: You must maintain the HTTP service on 10.X.X.21
- SSH1: You must maintain the SSH service on 10.X.X.25
- SSH2: You must maintain the SSH service on 10.X.X.30
- SSH3: You must maintain the SSH service on 10.X.X.75
- SSH4: You must maintain the SSH service on 10.X.X.98
- SSH5: You must maintain the SSH service on 10.X.X.76

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 6 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 to reach **all** systems in your Main and Cloud networks.

Internally you will also need to maintain:

- File Servers
- Client Workstations
- Active Directory
- Access to critical services
- Network Printing to competition printers
- 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. Internet bound traffic should be passing through the transparent proxy. All systems should be configured to use your team's DNS server first (10.X.X.5) and 10.120.0.53 second. DNS queries to any other name server will be rejected.

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

CCS Service:

On many of your team systems you may notice a service called "CCSClient". This is a scoring process used by competition officials. You must leave this process in place and running on any Windows, Debian, Fedora, or Ubuntu system inside your Main and Cloud networks. If the VM has a CCS client on it at the beginning of the competition, you must keep the CCSClient running on that system at all times. You must allow this process to communicate with the 10.120.0.0/16 network on ports 80 and 443 at all times. Do not modify any files in C:\CCS on Windows systems or /opt/CCS on Linux systems. The CCSClient is already installed on competition VMs, but if you perform a clean install of any Windows, Debian, or Ubuntu system you must place the CCSClient onto that system after the installation. Installation files for the CCS Client are available on the internal software portal (10.120.0.9). The CCSClient is a scoring process and is not used by the Red Team for any purpose. Penalties are assessed on a per VM basis for each 5 minute block your CCSClient is unable to connect to the server.