

CDEST – A Cyber Defense Exercise Scoring Tool

John Franco (franco@ucmail.uc.edu)

Dept. Electrical Engineering and Computer Science
University of Cincinnati
Cincinnati, OH 45221-0030

January, 2021 – version 1.0

Table of Contents

CDEST – A Cyber Defense Exercise Scoring Tool.....	1
Overview.....	1
CDEST Details.....	1
Compromised Operating System.....	1
Contest Configuration Management.....	1
The CDX Control Panel.....	2
The Configurator.....	3
Scoreboard.....	4
Log File.....	5
Proxy Server.....	5
Running a Competition Without the GUI.....	6
Files.....	7
Files that are part of the Scorer package as distributed.....	7
Directories created for file distribution.....	12
Files made via Configurator commands and distributed to Players and others.....	12
OpenVPN server location.....	14
Players database.....	14
VPN Credentials.....	14
Transfer Files to Players.....	15
Scoring.....	15
Help Boxes.....	15
Accessibility.....	16
Acknowledgments.....	16
Appendix A – How an administrator sets up a contest.....	17
Collect Player information.....	17
Install the software and/or run it.....	17
Create a Player database, assign IP addresses, and save to file.....	17
Configure a contest.....	17
Create files to be sent to Players.....	18
Archive and send contest files to Players.....	18
Create the contest network.....	18
Start the contest and make checks.....	18
Appendix B – What A Player Does To Compete.....	20
Receive files from the Contest Administrator.....	20
Connect to the contest network.....	20
Join the competition.....	20
Appendix C – Create a Competition VPN with OpenVPN.....	21
Assumptions.....	21
Create the key-making environment.....	21
Get and install OpenSSL.....	21
Get and install LZO2.....	21
Get and install OpenVPN.....	21
Get and install EasyRSA.....	22
Create and distribute contest credentials and parameters.....	22
Start the openvpn server.....	27

Stop the openvpn server.....	27
Player's OS joins the VPN.....	27
Appendix D – How to Join the VPN Network.....	29
Assumptions.....	29
Overview.....	29
What the Player needs to do.....	29
Create an Ubuntu VM in Virtualbox.....	29
Configure the Ubuntu VM.....	30
Update and install software.....	31
Join the VPN.....	31
Disconnect from the VPN.....	32
Appendix E – Hard Coded Configuration Parameters.....	33
Appendix F – Sample Configurations and Skill Levels.....	34
Appendix G - Configurator Parameter Descriptions.....	35
Web Server.....	35
Database.....	35
Log.....	35
Contest Dates and Times.....	35
OpenVPN Key & Certificate Maker.....	36
Prepare Files.....	36
Controls.....	37
Appendix H - Structure of Files in Player Directories.....	38
Parms:.....	38
run.client:.....	38
run.vpn:.....	38
stop.client:.....	39
client.conf:.....	39
Other files in a Player's directory:.....	40
Appendix I - Files in Parameters and VPNServer directories.....	41
Parameters.txt:.....	41
server.conf:.....	41
ipp.txt:.....	42
clientXX:.....	42
run.server:.....	42
run.vpn:.....	43
stop.server:.....	43
sbin:.....	43
keys:.....	43
Appendix J - Files and subdirectories of contest directory.....	44
players.db:.....	44
vpnKeyIds.txt:.....	44
game-id.txt:.....	44
var, var1, var2:.....	44
openssl-easyrsa.cnf:.....	45
make-keys:.....	45
bin:.....	45
sbin:.....	45

keys:.....	45
examples:.....	45
client:.....	45
server:.....	45

Overview

CDEST is a team competition that is intended to enhance the Cyber Operations (CO) community by reducing time and cost of apprenticeship training and by improving the motivation and quality of the CO workforce.

Critical to improving quality and reducing time and cost of apprenticeship training is ensuring a greater depth of knowledge and utility of CO skills in personnel entering the workforce. CO specialists 1) protect data, networks, and net-centric capabilities; and 2) neutralize the digital capabilities of adversaries including their ability to communicate, initiate attacks, and control infrastructure. Critical CO skills therefore include low-level programming, operating system weaknesses and vulnerabilities, network protocols, encryption, authentication, integrity protection, reverse engineering, and forensic analysis of traffic and data. The I-Wars competition can exercise some or all of those skills.

CDEST supports a variety of Cyber Defense Exercises and consists of two major components: a modified operating system (OS) and scoring software (Scorer). The OS is distributed by a Contest Administrator (CA) to Teams some number of days, determined by the CA before a CDEST contest commences. Teams examine the OS for configuration errors, protocol weaknesses, and any vulnerabilities the OS may have and attempt to mitigate or fix such problems. At contest start the Teams put the OSes online to provide a collection of internet services that are specified by the CA in advance. Also at contest start the CA initiates the Scorer: at 1 minute intervals the Scorer checks to see if the services of a Team's OS are up. The Scorer adds 1 point to a team's cumulative score for each service that is deemed working when a check is made. A real-time scoreboard is maintained during the contest. The scoreboard is generally publicly accessible although it can be made private. At contest end the team with the highest cumulative score wins. More importantly, an assessment is made as to how well a Team was able to defend its OS.

There are several ways CDEST can be used. The supplied OS may be replaced by another at the discretion of the CA. The services checked may be changed by modifying the CheckServices.java file and recompiling the Scoring software. The time between checks may be changed in the same way. Teams may be allowed to attack the OSes of other Teams in a variety of ways as well as defend their OSes from attack. The CA may require Teams to defend only and enlist other Teams, having seen the OS in advance, to attack the OSes. Finally, the CA may ask Teams to choose their own OS and require that a collection of services must be running on particular ports.

Not included with CDEST are the many publicly available tools for analyzing, modifying, and controlling network traffic, for example firewalls. Teams should use those tools to anticipate and mitigate attacks. The CA will use those tools to analyze the performance of Teams after the contest is ended.

CDEST is best used at the end of a course on cyber defense. It helps if Team members have also taken a course in vulnerabilities analysis.

CDEST Details

CDEST has two components: the modified OS and the Scorer. Information about the supplied OS is given below. The CA is free to choose another one. The scorer not only checks OS services during the contest but also provides configuration management and a real-time scoreboard. Details of these functions are given below.

Compromised Operating System

Teams are given an operating system with many vulnerabilities including configuration, buffer overflow,

Contest Configuration Management

The CA has the following tasks to perform to prepare for a contest:

1. create a list of Players and files containing data that enables Players to join a competition and the Scorer to know where they are

2. set contest parameters such as scoreboard location, times of contest start and end, logging verbosity, whether to allow an account to be created remotely, whether to recover a database if the Scorer is restarted
3. establish a private network over which the contest is to be run
4. distribute all keys and contest information such as usernames, ip address, etc. to the Players so that they may have their OSe be seen by the Scorer during the contest.

This section provides details that are needed by the CA to configure a contest successfully.

The CDX Control Panel

A CA prepares for a competition using the CDX Control Panel which creates and distributes files needed by Players to join a contest network, and possibly the host of an OpenVPN server, to create a contest network. The CDX Control Panel is started by running the 'cdx-lig.sh script in Linux or 'cdx-wig.bat' script in windows. The CDX Control Panel UI is shown at startup in Figure 1. The Panel is divided into four sections. The large blank area on the right displays help, the results of configuration, and the status of all Players up to the current point in time. The area on the left contains buttons for activating commands and fields for setting parameters for commands. Some of the commands, such as 'Add Player' are used during configuration and some commands such as 'HTTP Query' are used by the CA while the contest is in progress. The left four buttons at the top are used to 'Start', 'Stop', 'Suspend', and 'Resume' a contest. The right three buttons at the top are used to 'Load' the player database file (players.db is the default name) into memory, 'List' the current player status (from memory) and 'Save' the Player status from memory to the player database file. A listing of Players and status is printed in the right text area when 'List' is clicked such as is shown in Figure 2 where the Os are points obtained so far by each player (this shot was taken before the start of the contest). The four buttons at the bottom of the UI on the right are 'Help' which displays a description of the commands invoked from clicking buttons in the Panel; 'Configure' which brings up the Configurator UI, outlined in the next section; 'Reset' which resets the status of all Players to what they are at the start of the contest; and 'Exit' which quits the CDX Control Panel. On the left is the 'Time to start:' field showing a contest has been set to start in 0 days, 7 hours, 18 minutes, and 22 seconds. This field changes to 'Time to end:' during a contest.

Figure 1: The CDX Control Panel at startup

CDX Control Panel

NG Fellows B	10.8.0.122	0
NG Fellows C	10.8.0.123	0
No Name Yet A	10.8.0.127	0
No Name Yet B	10.8.0.128	0
No Name Yet C	10.8.0.129	0
Sneed's Feed And Seed A	10.8.0.115	0
Sneed's Feed And Seed B	10.8.0.116	0
Sneed's Feed And Seed C	10.8.0.117	0
Team 3 A	10.8.0.124	0
Team 3 B	10.8.0.125	0
Team 3 C	10.8.0.126	0
The Boys A	10.8.0.112	0
The Boys B	10.8.0.113	0
The Boys C	10.8.0.114	0
The Pink Panther Squad A	10.8.0.100	0
The Pink Panther Squad B	10.8.0.101	0
The Pink Panther Squad C	10.8.0.102	0
Two Musketeers A	10.8.0.130	0
Two Musketeers B	10.8.0.131	0
Two Musketeers C	10.8.0.132	0
No Attack Pls A	10.8.0.133	0
No Attack Pls B	10.8.0.134	0
No Attack Pls C	10.8.0.135	0
franco	10.8.0.200	0

Time to start:

Figure 2: The Player 'franco' has been added to the Player database and the database has been loaded and listed

The Configurator

Click the 'Configure' button in the CDX Control Panel to bring up the Configurator. The Configurator allows the CA to customize settings for the parameters associated with the contest. Many settings are selected by drop down menus, however the scoreboard URL and scoreboard title must be edited in. An example Configurator window is shown in Figure 3. Descriptions of the parameters can be found in Appendix G as well as by clicking 'Show Help' and hovering the mouse over the menu associated with a parameter or button.

The Configurator UI is partitioned into sections, each of which represents some functionality that is needed for the contest to run smoothly. Each section is boxed with a title at the upper left of and above the box. The 'Web Server' section serves to configure the scoreboard so it can be seen by all participants and refreshed properly. The 'Web server directory' holds the place from which files are served to the web; the 'Scoreboard title' will appear at the top of the scoreboard; the 'Web server URL' is edited into the scoreboard header to make sure automatic refreshes show a correct update of the scoreboard page. The section labeled 'Database' has a menu 'Player DB state' which allows anyone to establish their own Client account remotely if 'Dynamic' is chosen by the CA or not if 'Static' is chosen. In the 'Log' section the verbosity may be selected (the name of the log file is fixed at 'cdx.log'). Contest dates and times may be set by choosing month, day, year, hour, and minute from the 'Start:' and 'End:' menus, then choosing the time zone from the 'timezone' menu, finally clicking the 'Set Dates' button to record the dates and times. This information is used by the CA and is distributed to the Players so everyone knows when the contest begins and when it ends. The recorded times automatically account for Daylight Savings Time.

The remaining three sections of the Configurator UI are used to prepare and, optionally send, files to the OpenVPN host, the Scorer host, and the Players¹. OpenVPN keys and certificates are made in the 'OpenVPN Key & Certificate Maker' section. Keys and certificates serve as credentials for admission to the contest VPN if one is used. A description of the contest location and contact must be filled in. Use the '#keys' menu to select the number of keys and certificates to make. Click the 'Make Keys' button to

1 The Windows version of the Configurator does not support management of an OpenVPN network.

make the keys. This does not have to be done for every contest – it is up to the CA to decide whether existing keys have become stale and should be replaced. Most UI features are disabled when keys and certificates are being made. Making keys takes a very long time. Key making can be interrupted by clicking the 'Stop Making Keys' button. Made keys are always saved. The 'Save' button saves only the contest location and contact information.

The 'Prepare Files' section has a button 'Prepare without OpenVPN keys' for saving all files to be distributed when OpenVPN is not being used and a button 'Prepare with OpenVPN Keys' for saving all files for distribution including those needed by a Player to connect to the VPN and those needed by the OpenVPN server to establish the VPN. Either way, the result is a 'Contestants' directory with subdirectories, named for each Player and containing a Player's files, a 'Parameters' directory containing a file Parameters.txt for the Scorer host, and, if OpenVPN is used, a subdirectory of contest named server containing all files needed by the OpenVPN server to establish a private network.

The 'Controls' section contains a button 'Send Files and Quit' which archives the contestant directories, sends them to Players, and, in case OpenVPN is being used, archives the directory containing OpenVPN server files and places the result in a directory that is created called 'VPNServer' (the CA will manually send the contents of this directory to the server host). There is also a button 'Quit, Do Not Send Files' which quits the Configurator without making any additional changes. The 'Help' button enables help tips to be displayed when the mouse pointer hovers over a menu or button in the Configurator. If the 'Cancel' button is clicked, the Configurator is exited with no changes.

The Configurator

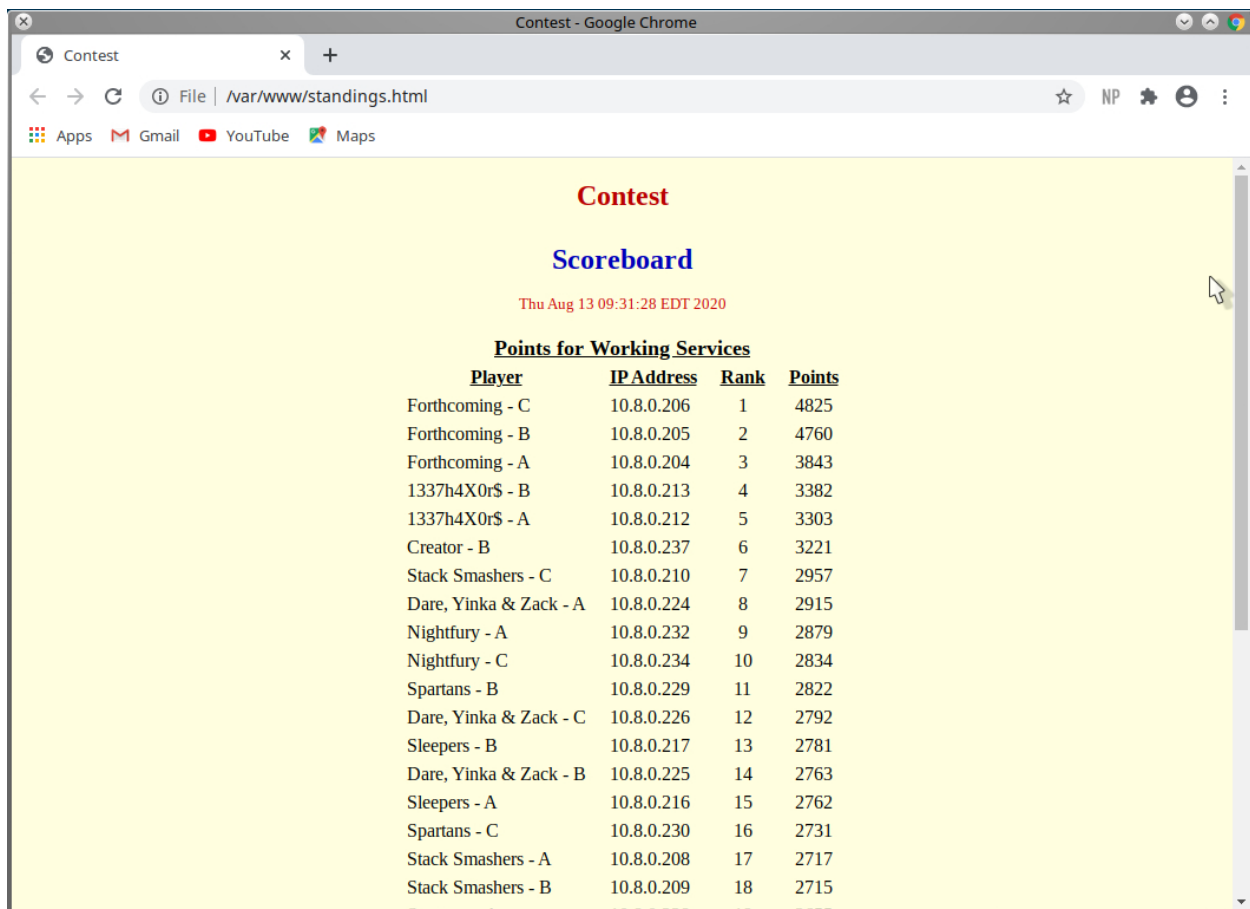
<p>Web Server</p> <table style="width: 100%;"> <tr> <td>Web server URL</td> <td>Scoreboard title</td> <td>Web server directory</td> </tr> <tr> <td><input type="text" value="file:///var/www/"/></td> <td><input type="text" value="Contest"/></td> <td><input type="text" value="/var/www/"/></td> </tr> </table>	Web server URL	Scoreboard title	Web server directory	<input type="text" value="file:///var/www/"/>	<input type="text" value="Contest"/>	<input type="text" value="/var/www/"/>	<p>Database</p> <table style="width: 100%;"> <tr> <td>Player DB state</td> <td>Recover database</td> </tr> <tr> <td><input type="text" value="Static"/></td> <td><input type="text" value="No"/></td> </tr> </table>	Player DB state	Recover database	<input type="text" value="Static"/>	<input type="text" value="No"/>	<p>Log</p> <table style="width: 100%;"> <tr> <td>Monitor log file</td> <td>Logging option</td> </tr> <tr> <td><input type="text" value="cdx.log"/></td> <td><input type="text" value="4"/></td> </tr> </table>	Monitor log file	Logging option	<input type="text" value="cdx.log"/>	<input type="text" value="4"/>																																																			
Web server URL	Scoreboard title	Web server directory																																																																	
<input type="text" value="file:///var/www/"/>	<input type="text" value="Contest"/>	<input type="text" value="/var/www/"/>																																																																	
Player DB state	Recover database																																																																		
<input type="text" value="Static"/>	<input type="text" value="No"/>																																																																		
Monitor log file	Logging option																																																																		
<input type="text" value="cdx.log"/>	<input type="text" value="4"/>																																																																		
<p>Contest Dates and Times</p> <table style="width: 100%;"> <tr> <td>Start:</td> <td><input type="text" value="January"/></td> <td><input type="text" value="17"/></td> <td><input type="text" value="2021"/></td> <td><input type="text" value="14"/></td> <td><input type="text" value="30"/></td> </tr> <tr> <td></td> <td>month</td> <td>day</td> <td>year</td> <td>hour</td> <td>minute</td> </tr> <tr> <td>End:</td> <td><input type="text" value="January"/></td> <td><input type="text" value="17"/></td> <td><input type="text" value="2021"/></td> <td><input type="text" value="14"/></td> <td><input type="text" value="30"/></td> </tr> <tr> <td></td> <td>month</td> <td>day</td> <td>year</td> <td>hour</td> <td>minute</td> </tr> <tr> <td></td> <td colspan="2"><input type="text" value="Eastern"/></td> <td colspan="3"><input type="button" value="Set Dates"/></td> </tr> <tr> <td></td> <td colspan="2">timezone</td> <td colspan="3"></td> </tr> </table>	Start:	<input type="text" value="January"/>	<input type="text" value="17"/>	<input type="text" value="2021"/>	<input type="text" value="14"/>	<input type="text" value="30"/>		month	day	year	hour	minute	End:	<input type="text" value="January"/>	<input type="text" value="17"/>	<input type="text" value="2021"/>	<input type="text" value="14"/>	<input type="text" value="30"/>		month	day	year	hour	minute		<input type="text" value="Eastern"/>		<input type="button" value="Set Dates"/>				timezone					<p>OpenVPN Key & Certificate Maker</p> <table style="width: 100%;"> <tr> <td><input type="text" value="US"/></td> <td><input type="text" value="OH"/></td> <td><input type="text" value="Cincinnati"/></td> </tr> <tr> <td>country</td> <td>state</td> <td>city (ex: Los Angeles)</td> </tr> <tr> <td colspan="3"><input type="text" value="University of Cincinnati"/></td> </tr> <tr> <td colspan="3">organization (ex: UCLA)</td> </tr> <tr> <td colspan="3"><input type="text" value="Dept. Electrical Eng. and Computer Sci."/></td> </tr> <tr> <td colspan="3">organizational unit (ex: Emergency Room)</td> </tr> <tr> <td colspan="3"><input type="text" value="franco@gauss.ececs.uc.edu"/></td> </tr> <tr> <td colspan="3">email</td> </tr> <tr> <td>#keys: <input type="text" value="150"/></td> <td><input type="button" value="Make Keys"/></td> <td><input type="button" value="Stop Making Keys"/></td> </tr> <tr> <td colspan="3"><input type="button" value="Save"/></td> </tr> </table>	<input type="text" value="US"/>	<input type="text" value="OH"/>	<input type="text" value="Cincinnati"/>	country	state	city (ex: Los Angeles)	<input type="text" value="University of Cincinnati"/>			organization (ex: UCLA)			<input type="text" value="Dept. Electrical Eng. and Computer Sci."/>			organizational unit (ex: Emergency Room)			<input type="text" value="franco@gauss.ececs.uc.edu"/>			email			#keys: <input type="text" value="150"/>	<input type="button" value="Make Keys"/>	<input type="button" value="Stop Making Keys"/>	<input type="button" value="Save"/>		
Start:	<input type="text" value="January"/>	<input type="text" value="17"/>	<input type="text" value="2021"/>	<input type="text" value="14"/>	<input type="text" value="30"/>																																																														
	month	day	year	hour	minute																																																														
End:	<input type="text" value="January"/>	<input type="text" value="17"/>	<input type="text" value="2021"/>	<input type="text" value="14"/>	<input type="text" value="30"/>																																																														
	month	day	year	hour	minute																																																														
	<input type="text" value="Eastern"/>		<input type="button" value="Set Dates"/>																																																																
	timezone																																																																		
<input type="text" value="US"/>	<input type="text" value="OH"/>	<input type="text" value="Cincinnati"/>																																																																	
country	state	city (ex: Los Angeles)																																																																	
<input type="text" value="University of Cincinnati"/>																																																																			
organization (ex: UCLA)																																																																			
<input type="text" value="Dept. Electrical Eng. and Computer Sci."/>																																																																			
organizational unit (ex: Emergency Room)																																																																			
<input type="text" value="franco@gauss.ececs.uc.edu"/>																																																																			
email																																																																			
#keys: <input type="text" value="150"/>	<input type="button" value="Make Keys"/>	<input type="button" value="Stop Making Keys"/>																																																																	
<input type="button" value="Save"/>																																																																			
<p>Prepare Files</p> <table style="width: 100%;"> <tr> <td><input type="button" value="Prepare with OpenVPN keys"/></td> </tr> <tr> <td><input type="button" value="Prepare without OpenVPN keys"/></td> </tr> </table>	<input type="button" value="Prepare with OpenVPN keys"/>	<input type="button" value="Prepare without OpenVPN keys"/>	<p>Controls</p> <table style="width: 100%;"> <tr> <td colspan="4"><input type="text" value="msgs:"/></td> </tr> <tr> <td><input type="button" value="Send Files and Quit"/></td> <td><input type="button" value="Quit, Do Not Send Files"/></td> <td><input type="button" value="Cancel"/></td> <td><input type="button" value="Show Help"/></td> </tr> </table>	<input type="text" value="msgs:"/>				<input type="button" value="Send Files and Quit"/>	<input type="button" value="Quit, Do Not Send Files"/>	<input type="button" value="Cancel"/>	<input type="button" value="Show Help"/>																																																								
<input type="button" value="Prepare with OpenVPN keys"/>																																																																			
<input type="button" value="Prepare without OpenVPN keys"/>																																																																			
<input type="text" value="msgs:"/>																																																																			
<input type="button" value="Send Files and Quit"/>	<input type="button" value="Quit, Do Not Send Files"/>	<input type="button" value="Cancel"/>	<input type="button" value="Show Help"/>																																																																

Figure 3: The Configurator

Scoreboard

The scoreboard location is set by the CA in the Configurator in the editable parameter fields called 'Web server URL' and 'Web server directory'. The 'Web server directory' default is /var/www and the 'Web server URL' default is http://example.edu. The default path to the scoreboard file will then be /var/www/scoreboard.html as the file that is served to the web containing the scoreboard is named scoreboard.html. The scoreboard.html file is updated directly in the Web server directory at 45 second intervals so permissions must be set to prevent permission denied errors. The reason the Web server URL is a parameter in the Configurator is

that the value in the Web server URL field is embedded in the scoreboard.html file and causes an automatic and periodic refresh to the scoreboard. A scoreboard example, representing the result of a short mock contest, is shown in Figure 4.



Contest			
Scoreboard			
Thu Aug 13 09:31:28 EDT 2020			
Points for Working Services			
Player	IP Address	Rank	Points
Forthcoming - C	10.8.0.206	1	4825
Forthcoming - B	10.8.0.205	2	4760
Forthcoming - A	10.8.0.204	3	3843
1337h4X0r\$ - B	10.8.0.213	4	3382
1337h4X0r\$ - A	10.8.0.212	5	3303
Creator - B	10.8.0.237	6	3221
Stack Smashers - C	10.8.0.210	7	2957
Dare, Yinka & Zack - A	10.8.0.224	8	2915
Nightfury - A	10.8.0.232	9	2879
Nightfury - C	10.8.0.234	10	2834
Spartans - B	10.8.0.229	11	2822
Dare, Yinka & Zack - C	10.8.0.226	12	2792
Sleepers - B	10.8.0.217	13	2781
Dare, Yinka & Zack - B	10.8.0.225	14	2763
Sleepers - A	10.8.0.216	15	2762
Spartans - C	10.8.0.230	16	2731
Stack Smashers - A	10.8.0.208	17	2717
Stack Smashers - B	10.8.0.209	18	2715

Figure 4: Example scoreboard during a contest

Log File

The Scorer generates a log file that contains all events and the times they occurred. The CA may choose to make the log file available to the participants of the contest. This will be especially useful in low level contests where participants lack familiarity with advanced forensic tools such as Wireshark. Figure 5 shows the beginning of a log file that was generated by a Scorer. The format of the log is date and time followed by an event, one event per line. Events are categorized as a) Directory and file creation, file reading; b) Configuration events plus contest commands and services; c) Checking service results plus other commands and results during a contest; d) Only the results of checking services. Events that appear in the log are determined by the CA who chooses a number from the 'Logging Option' menu in the Configurator before the contest begins: possibilities are 1) all events are logged; 2) events in categories b-d are logged; 3) events in categories c-d are logged; 4) only events in category d are logged. If the log file is made public a link should be set from the same directory containing the scoreboard to `cdx.log` so it may be served to the web.

Proxy Server

If OpenVPN is used to establish a contest network, the OpenVPN server is behind an organization's firewall, and some Players intend to enter the contest from outside the organization's perimeter then it is

likely that a proxy server is needed to channel outside connections to the OpenVPN server. If an ssh server is operating behind the firewall then this can be done as follows from the Player's Linux machine:

```
ssh -N -f -T -D 8080 visitor@helios.ececs.uc.edu
```

where it is assumed a ssh server is running on `helios.ececs.uc.edu` and an account named `visitor` has been established with reduced privileges to allow a connection to be established between the server and a Player's OS. If a proxy server is used by a Player then that Player must modify `client.conf` by uncommenting the line:

```
;socks-proxy 127.0.0.1 8080
```

This is done by removing the `';` from the beginning of the line.

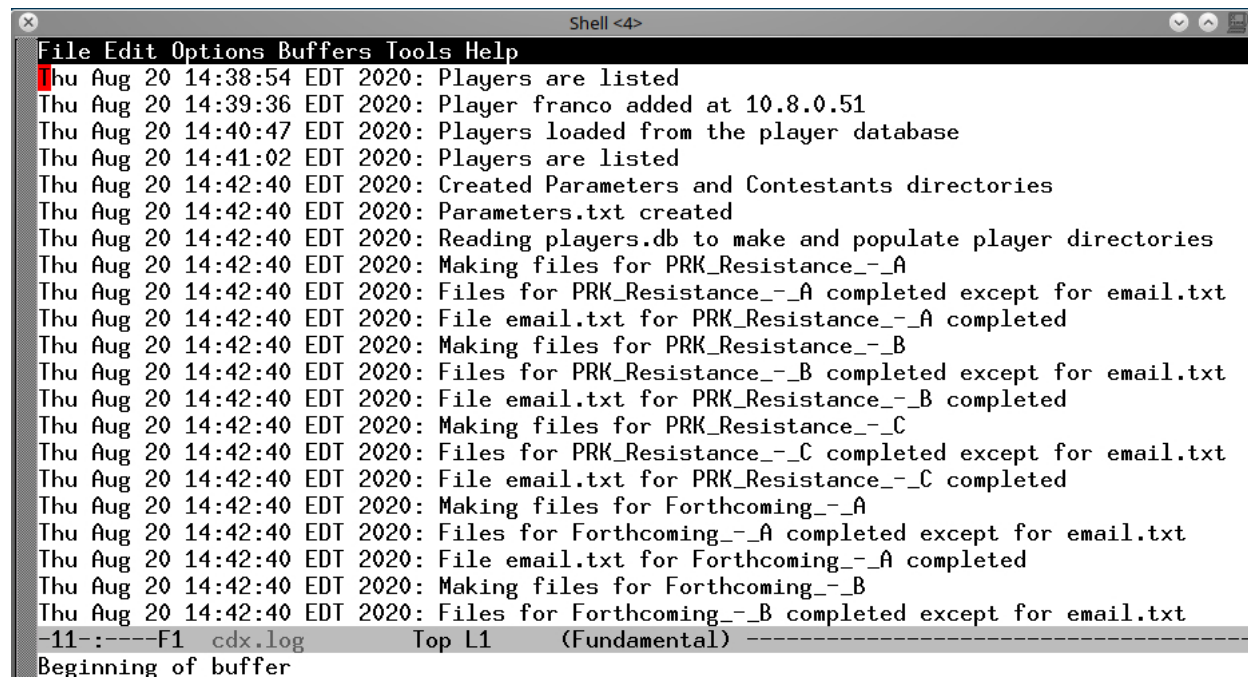


Figure 5: Sample beginning of a log at the beginning of a contest. Entries show time and date as well as an event

Running a Competition Without the GUI

Although a competition can be run from the CDX Control Panel discussed above, it may be much more convenient to run a competition from an application that is not graphical. This is because the CA likely needs to issue commands during a competition and because it is further likely that the Scorer will be run remotely with respect to the CA. Thus, the CA will usually start the Scorer as a remote process, which it detaches, and later reattaches to the Scorer, as needed, to issue commands. In Linux this is facilitated by an application called 'screen'². In Windows 10 'powershell' has commands to run detached remote processes and 'screen' can be used if the Scorer is run in the Ubuntu shell. But a detached process cannot be run graphically. For this reason there is a Scorer application that runs only with command line inputs. This Scorer does not have the CDX Control Panel – the buttons and argument text fields are replaced by commands with arguments. This Scorer also does not include the Configurator.

Use of the command line Scorer will be detailed in . Here, an example screenshot of the Scorer, at startup, is shown in Figure 6. The strings command> show the command prompt. The first Time command, invoked by the CA, shows 5 days, 2 hours, 52 minutes, 44 seconds to the end of the contest.

² There are other applications that do this as well.

Since the contest start time was before the execution of the Scorer, the player database was automatically loaded. The scores, shown as a result of invoking the List command, are all 0 because the Parameters.txt file indicated that all scores should be reset upon initial loading. Invoking the command Stop causes the contest to end immediately.

```
[franco@franco Scoreboard]$ cdx-lin.run
  Players loaded from 'players.db' - invoke LIST to see them
-----
command> time
  Time to end: 5 days, 2 hours, 52 minutes, 44 seconds
-----
command> list
  Listing players
-----
  franco1          10.8.0.200      0
  franco2          10.8.0.201      0
  franco3          10.8.0.202      0
  franco4          10.8.0.203      0
-----
command> stop
  Wait at least 10 seconds...
  Contest is stopped
-----
command> time
  Contest: Finished
-----
command> █
```

Figure 6: The command-line Scorer has been started with four players, and a running contest. The Time command shows how much time is left until the end of the contest. The Stop command terminates the contest immediately as the second call to Time shows.

Files

There are many files that need to be created, modified, and distributed by the Contest Administrator. This is made simple by commands 'Prepare with OpenVPN keys' and 'Prepare without OpenVPN keys' in the Configurator (see Figure 3) which make the files and the command 'Send Files and Quit' which distributes the files. There is also command 'Make Keys' in the Configurator which makes OpenVPN keys and certificates if OpenVPN is used. Command 'Make Keys' may be skipped if the contest being prepared has been preceded by another contest with which keys and certificates can be shared and keys and certificates have already been created for the preceding contest. In addition to the files that are made for distribution there are a number of other files that are permanently part of the Scorer package and exist to run the Scorer and create files for distribution. Below, the files and their locations are described. The contents of many of these files are in Appendix H, Appendix I, and Appendix J.

Files that are part of the Scorer package as distributed

Directory	File(s)	Description
contest/bin	tar tar.exe	Used to archive all files in a Player's directory as a single file which is sent to a Player. Archived files exist in directory 'Contestants'. This executable is statically compiled so runs independently of system libraries. tar is the linux command and tar.exe is the windows version.
	openssl	Used to create keys and certificates. This is called by the easysa bash script in directory contest. This is an ELF executable that is statically compiled. The Windows version of this software does not use openssl because there is no provision for using OpenVPN in Windows. However, the Linux version will work in the Ubuntu Shell in windows along with the Xming X server for Windows. Also a Linux VM in VMWare or Virtualbox may be used to run the Linux version of the software if OpenVPN is intended to be used.
	mutt	Statically compiled mailer. Called by bash script mailit. The Windows version of this software does not use a mailer – so mailing must be done manually, one Player at a time. Using the Linux version in Ubuntu Shell or a VM in a hypervisor allows the possibility of mailing in Windows but if the host is forbidden to email then all files (now archived as tar files) need to be sent manually
contest/client	run.client	Calls run.vpn to join an OpenVPN network. A copy is placed in each Player's directory if OpenVPN is used to establish a contest network. Available in Linux only.
	stop.client	Uses vpn.pid which was created by run.vpn to stop the running openvpn process that has made a connection to an OpenVPN network. A copy is placed in each Player's directory if OpenVPN is used to establish a contest network. Available in Linux only.
	run.vpn	Makes a connection to an existing OpenVPN network using statically compiled sbin/openvpn on the client.conf that is created specifically for a Player. Saves the process number of the openvpn process in vpn.pid. A copy is placed in each Player's directory if OpenVPN is used to establish a contest network. Only available in Linux.
	client.conf	A template of the file needed by openvpn to join an existing OpenVPN network. A customized client.conf is made for each Player by appending a Player's OpenVPN keys, certificates, and the location of the OpenVPN server to the template. This is accomplished in function 'appendToClientConfig' in Java class 'vpnFrame'. The custom client.conf is placed in the Player's directory if OpenVPN is used to establish a contest network. Available only in Linux.
	JAVA.txt	Contains information about the use of Java
	email.txt	Email address of the Player who will receive all relevant files for joining a contest.

	README.txt	Contains general information for a Player that may be useful when using the files from this directory
	instructions.pdf	Instructions for joining a contest if OpenVPN is used. A copy is placed in each Player's directory and included in the tar file sent to each player if OpenVPN is used. Available only in Linux.
contest/sbin	openvpn	Statically compiled executable for a Player to join an OpenVPN network. A copy is placed in a Player's sbn directory but only if OpenVPN is to be used. Called from a Player's run.vpn. Available only in Linux.
contest/keys	xxx.crt xxx.key ca.crt dh2048.pem	Created by the Configurator when preparing for a contest that is run over OpenVPN. These are the credentials that get distributed to Players and the OpenVPN server.
contest/examples	xxx.db xxx.example	Sample player database files and parameter files
contest/x509-types	xxxx	Files that could be edited to add values that every certificate should have and other things that are stated in the comments of each file – used by easysa
contest/doc	xxxx.md	Easysa documentation
contest/server	server.conf.tpl	A template of the server.conf file that is missing the name and location of server keys and the ip address of the server host. Used to construct server.conf for the OpenVPN server.
	run.server	Calls run.vpn to create an OpenVPN network. This script is intended for Linux.
	stop.server	Uses vpn.pid which was created by run.vpn to stop the running openvpn process that creates and sustains an OpenVPN network. Intended for Linux.
	run.vpn	Creates and sustains an OpenVPN network using statically compiled sbn/openvpn on the server.conf that is created specifically for the OpenVPN host. Saves the process number of the openvpn process in vpn.pid. Intended for Linux.
	server.conf	The completed OpenVPN server configuration file that is created from server.conf.tpl when the 'Prepare with OpenVPN keys' button in the Configurator is pressed.
	server.tar	Archive of OpenVPN files that is sent to the OpenVPN server if an OpenVPN network is to be used. This is created from directory contest/server when the 'Send Files and Quit' button is pressed in the Configurator.
	run.proxy	Shows an example of how to create a connection to a firewalled OpenVPN server via a socks proxy using ssh.
	README.txt	Contains general information for a Player that may be useful when using the files from this directory
	ipp.txt	File mapping Common Names to IP addresses. This file is created by the Configurator when OpenVPN is used and keys are made. Its purpose is to ensure a Player, given keys of prefix clientXX, XX a number,

		always have the same, given IP address.
contest/server/sbin	openvpn	Statically compiled executable for an OpenVPN host to create an OpenVPN network. A copy is placed in this directory when the 'Prepare with OpenVPN keys' button is pressed in the Configurator.
contest/server/ccd	client0, client1 ... client149	Files, one for each set of credentials created by the Configurator when making keys, that map credentials to IP addresses and provide a netmask. Used with ipp.txt to ensure that a Player always has the same IP address in an OpenVPN network. This directory is copied from contest/ccd when the 'Prepare with OpenVPN keys' button is pressed in the Configurator.
contest/server/keys	ca.crt, dh2048.pem, server.key, server.crt	Credentials for the OpenVPN server. This directory is created and populated when the 'Prepare with OpenVPN keys' button is pressed in the 'Prepare Files' section of the Configurator.
contest/server/allkeys	clientXX.crt, clientXX.key ca.crt dh2048.pem	Complete sets of credentials for as many key sets as made in the Configurator in the 'OpenVPN Key & Certificate Maker' section, also credentials for the OpenVPN server. Credentials are created when the 'Prepare with OpenVPN keys' button is pressed in the 'Prepare Files' section of the Configurator.
contest	easyrsa	Script for producing keys and certificates. Relies on bin/openssl. Available only for Linux.
	cmd1 - cmd9	Bash scripts for making OpenVPN keys and certificates. Makes use of the easyrsa script. Invoked from within the running Java jar file, method of the 'MakeKeys' class in directory src-lig. In addition, files that associate IP addresses with keys and certificates are produced and placed in directory contest/server/ccd and file contest/server/ipp.txt. See the next Section for more details on those files.
	vars1/vars2	Two halves of the vars file which are concatenated with contest information supplied in the 'OpenVPN Key & Certificate Maker' Section of the Configurator to produce the 'vars' file that easyrsa uses to make certificates.
	openssl-easyrsa.cnf	Configuration file for easyrsa.
	gpl-2.0.lic	Software license
	contest-setup.txt	Body of the message that is sent to Players along with files needed by the player to participate in the contest.
	workaround	Sets up an environment so easyrsa can generate a server certificate request and key. This is a kludge and probably can be eliminated by moving this command to another script such as make-keys where the environment must be set differently.
	vpnKeyIds.txt	List of names of directories that are created from Player names in the player database file. When a button in the 'Prepare Files' section of the Configurator is pressed, these directories are created to hold all the contest files that will be sent to the Players.
	README.txt	Contains general information for a Contest Administrator

src-lig (Linux) src-lin (Linux) src-wig (Windows) src-win (Windows)	xxxxx.java	Java source files that compile to class files that are archived as cdx-contest.jar in directory src-xxx. Available only to developers.
	run	Script that invokes java on cdx-contest.jar in the Linux source directories.
	run.bat	Script that invokes java on cdx-contest.jar in the Windows source directories.
	cdx-contest.jar	Executable java archive of the contest software
	compile.bat	Script that compiles the Java source files and archives the resulting class files as a Jar file. For Windows. Available only to developers.
	Makefile	Instructions used to compile the Java source files and archive the resulting class files as a Jar file. For Linux. Execute 'make' in one of the Linux source directories to do this. Developers only.
	Parameters.txt	A file containing information such as contest dates and times that is needed to run a competition. Created in the Configurator.
	players.db	A player database file (default name is shown) created by repeated invocations of the 'Add' command in the CDX Control Panel.
	nmap	Files to support nmap in Windows. In the Windows directories only.
doc	manual.pdf description.pdf scoreboard.pdf	Documentation in the form of a manual and in the form of a short description of the software.
HowToJoinVPN	instructions.pdf	File to be distributed to contestants to tell them what to do with the tar file they receive from the contest admin.
	what-to-do-OCR.pdf	Instructions for operating in a Cyber Range
.	cdx-lig.run cdx-lin.run cdx-wig.bat cdx-win.bat	Script that runs the Scorer in one of four ways – cdx-lig.run invokes the GUI which looks like Figure 2 and Figure 3. The GUI supports configuration plus manufacture and distribution of OpenVPN credentials. This is a Linux script that may be run in the Ubuntu shell of Windows 10 if the Xming X server is installed and running. The Windows batch file cdx-wig.bat is the counterpart of cdx-lig.run except that it does not bring up anything related to the OpenVPN credentials. Both scripts have the ability to start and stop contests, manually and automatically. cdx-lin.run opens a command-line only utility that can manage a contest but cannot configure one in Linux. The cdx-win.bat counterpart can do the same.

Table 1: Relevant files that are part of the contest package

Directories created for file distribution to competitors

Directory	Description
Contestants	Contains a subdirectory for each Player in the player database that is created after 'Send Files and Quit' command is activated in the Configurator. The name of each subdirectory is the name of the Player in the player database where blanks are replaced with underscore. Thus, if a Player's name is given as 'John the Farmer' then the name of the subdirectory is 'John_the_Farmer'. Below, '<Player>' is used to represent any Player's name. The contents of a Player's directory depends on whether OpenVPN is employed to establish a contest network. If not, the directory contains a file specifying a Player's contest ip address and start and end times. If so, additional files allow making a connection to the contest network via OpenVPN.
Parameters	Contains Parameters.txt for the CA – see Appendix I for contents
VPNServer	Contains server.tar for the OpenVPN server host – see Page 13 and Appendix I for contents

Table 2: Repositories for distribution

Files made via Configurator commands and distributed to Players and others

Directory	File	Description
Contestants/<player>	Parms	Information for a Player – contest start time, contestant end time, ip address for the contest.
	email.txt	The email address of the Player. This comes from the 'Add Player' command which requires an email address.
	run.client	Calls run.vpn to join an OpenVPN network. Exists only if OpenVPN is used to establish a contest network.
	stop.client	Kills an openvpn process that connects the Player to a contest network if OpenVPN is used.
	run.vpn	Makes a connection to an existing OpenVPN network using statically compiled/sbin/openvpn on the client.conf that is created specifically for a Player. Saves the process number of the openvpn process in vpn.pid. Exists only if OpenVPN is used.
	client.conf	A customized configuration file that/sbin/openvpn is applied to for connecting to a contest network established by OpenVPN. Does not exist unless OpenVPN is used.
	JAVA.txt	Notes on the use of Java. Exists only if OpenVPN is used.
	README.txt	General operating notes. Exists only if OpenVPN is used.
Contestants/<Player>/keys	ca.crt	Certificate of the OpenVPN server. This directory and its contents exists only if OpenVPN is used.
	clientXX.key	Player's key for a secure connection to the contest network if OpenVPN is used. XX is a

		number no greater than 255. The name <code>clientXX.key</code> matches the name stated in <code>client.conf</code> and this location is also part of the customization for a Player. The OpenVPN server uses <code>clientXX</code> as well in directory <code>ccd</code> to coordinate matching an ip address with a key.
	<code>clientXX.crt</code>	Player's OpenVPN certificate.
Contestants/<Player>/sbin	<code>openvpn</code>	Statically compiled version of <code>openvpn</code> that is applied to <code>client.conf</code> to establish a connection to an OpenVPN network if one is established.
Parameters	<code>Parameters.txt</code>	File intended for the Contest Administrator with information regarding the contest including start date and time, stop date and time, ip address of the Scorer, scoreboard URL, scoreboard location, log verbosity, database recovery mode, and whether Players can be added remotely.
VPNServer	<code>server.tar</code>	An archive of all files needed by an OpenVPN server. These include the following: <ul style="list-style-type: none"> - <code>allkeys</code> – a directory that contains all keys and certificates that were made when 'Make Keys' is clicked in the Configurator. - <code>keys</code> – a directory containing keys and certificates specifically for the server including <code>server.crt</code>, <code>server.key</code>, <code>ca.crt</code>, and <code>dh2048.pem</code>. - <code>ccd</code> – directory that contains a collection of files named '<code>clientXX</code>', <code>XX</code> a number, with contents '<code>ifconfig-push <ip-address> 255.255.255.0</code>' that maps a key to an ip address so that a Player getting a key/certificate pair is tied to a given ip address. This is done so the Scorer knows who it is scoring. - <code>sbin</code> – contains <code>openvpn</code> executable which allows for creating the OpenVPN network - files for starting and stopping the network including <code>run.server</code>, <code>stop.server</code>, <code>run.vpn</code>, and <code>server.conf</code>. - example files for starting and stopping a socks proxy including <code>run.proxy</code>, and <code>stop.proxy</code> - <code>ipp.txt</code> – a file whose lines map a key (common) name to an ip address – it seems both <code>ipp.txt</code> and the files in directory <code>ccd</code> are necessary for the mapping to work as expected (mapping is retained after restarts). - information files – <code>JAVA.txt</code> and <code>README.txt</code>

Table 3: Relevant files that are created for a Player with information needed to join a contest

The contest directory contains `openvpn`, `easy-rsa` files, some templates for vpn configuration, starting and stopping scripts, and Java source code for the CDX Control Panel and Configurator package. The `client` subdirectory contains the `openvpn` start and stop scripts which are to be distributed to Players for connecting their OSes to the contest private network in case OpenVPN is being used for that purpose. The supplied `run.client` script shows how to connect to an OpenVPN server. It also shows how to set up a connection to a proxy server that is inside an organization perimeter - those lines are commented in the script. The first commented line of `run.client` would cause all running `openvpn` processes to be

killed, if uncommented, before being connected to the VPN. This may not be desirable if more than one vpn address is needed on a host and, in that case, leave it commented but alert Players that they may need to kill running OpenVPN processes on their own before connecting to the VPN. The `client` subdirectory also contains a `readme.txt` file, which explains the use of the entire package that will be distributed to Players, and a template for `client.conf`, the configuration file for setting up a connection to a running openvpn server via `run.client`. Three lines need to be added to `client.conf` before distribution – these lines are unique to each Client and are explained below.

Other files include `game-id.txt` which contains certificate identification information for the X.509 certificates used in the contest; the directory `keys` which holds all the openvpn keys and certificates used for connecting to the VPN; and `vpnKeyIds.txt` which is a list of Player names that is used to create directories containing information that is distributed to Players.

Another subdirectory is `server` which contains the template for `server.conf`, `ipp.txt` and the `ccd` subdirectory: the latter two ensure a stable, predictable match between the keys and certificates to be distributed and VPN IP addresses assigned to Players.

Files in the `src-xxx` directory that are created by CDX Control Panel and Configurator operations include `Parameters.txt` and the player database, the default name of which is `players.db`. `Parameters.txt` is used by the CA to set up the competition. It contains contest start and end dates and times so that Scoring can be started automatically plus logging and player database options, and scoreboard setup information. The player database file, the default name of which is `players.db`, contains a list of names of Players, their IP addresses, their current scores, and email addresses.

OpenVPN server location

This is a text field in the CDX Control Panel that is filled in with the IP address or domain name of the host on which the OpenVPN server is to be run if OpenVPN is to be used. If OpenVPN is not to be used then this field may be left blank. Otherwise, the contents of this field become part of `server.conf` and each Player's `client.conf`. See Page 41 for the contents of `server.conf` and Page 39 for the contents of `client.conf`.

Players database

The default name for the player database is `players.db`. The name can be changed by editing the file `GameParameters.java` in `src-xxx` and recompiling using `make` in Linux and `compile.bat` in Windows. This file may be created manually or by means of the 'Add' command in the CDX Control Panel. The file may also be edited manually or by means of the 'Delete' or 'Bump' commands in the CDX Control Panel. Information in `players.db` consists of current score, an unused field, the IP address that a Player's OS takes (so that the Scorer knows who it is scoring), an email address of the Player, and the contest identity of the Player's OS. All of this information occupies one line of `players.db` for each Player. Table 4 shows a few sample lines from a `players.db` file.

VPN Credentials

The section of the Configurator called 'OpenVPN Key & Certificate Maker' sets up the files needed for an OpenVPN server to establish a network and for Players to connect to that network. There is no need to do anything with this section if OpenVPN is not used. Figure 7 shows this section. Information seen in this window comes from file `game-id.txt` a default version of which is supplied. The fields may be edited and changes will be stored when 'Save' is clicked. File `game-id.txt` is unchanged unless 'Save' is clicked. All fields must be populated if keys are to be made. Set the menu '#keys' to a number of keys to be made: default is 150. Click 'Make Keys' to make the keys. The keys and certificates for the server, certificate authority, and Players are made in subdirectory `keys`. Click 'Stop Making Keys' to interrupt the key making. Keys that are already made are not erased.

```

...
1957 0 10.8.0.-46 franco@localhost Stack Smashers - C
3303 0 10.8.0.-44 franco@localhost 1337h4X0r$ - A
2437 0 10.8.0.-54 franco@localhost PRK Resistance - C
3843 0 10.8.0.-52 franco@localhost Forthcoming - A
...

```

Table 4: A few lines from a `players.db` file. The fourth octet in the IP address in each case is a negative number – add that number to 256 to get the positive octet. For example, the IP address for Player Forthcoming – A is 10.8.0.204, for PRK Resistance – C is 10.8.0.202, and for Stack Smashers – C is 10.8.0.210.

OpenVPN Key & Certificate Maker

country: US state: OH city (ex: Los Angeles): Cincinnati

organization (ex: UCLA): University of Cincinnati

organizational unit (ex: Emergency Room): Dept. Electrical Eng. and Computer Sci.

email: franco@gauss.ececs.uc.edu

#keys: 150 ▼

Make Keys Stop Making Keys Save

Figure 7: Make and distribute keys and certificates for connecting to an OpenVPN network

Transfer Files to Players

If OpenVPN is to be used to establish a private network keys and certificates must first be made by selecting an appropriate number of keys to make and then clicking 'Make Keys' in the 'OpenVPN Key & Certificate Maker' section of the Configurator (see Figure 7). The keys are distributed to Player directories when 'Prepare with OpenVPN keys' is clicked in the 'Prepare Files' section of the Configurator (see Figure 3). Keys are distributed to recipients, whose email address is part of `players.db`, when 'Send Files and Quit' is clicked in the 'Controls' section of the Configurator. In the Windows version the Player files need to be distributed manually using the email addresses stated in the `email.txt` files.

Scoring

Scoring begins manually when the 'Start' button in the CDX Control Panel is clicked or automatically when 'Time to start:' becomes 0. Scoring ends manually when the 'Stop' button is clicked or automatically when 'Time to end:' becomes 0. Scoring may be suspended and resumed when those buttons are clicked. A real-time scoreboard is maintained by the Scorer. For details see the Scoreboard section above.

Help Boxes

In the Configurator hovering the mouse pointer over a button, menu, or text box will bring up an information box that explains what action the button is intended to perform or what the value of a text box means. To enable this feature click the 'Show Help' button in the bottom right section of the Configurator. An example is shown in Figure 8. Click 'Hide Help' to disable this function.

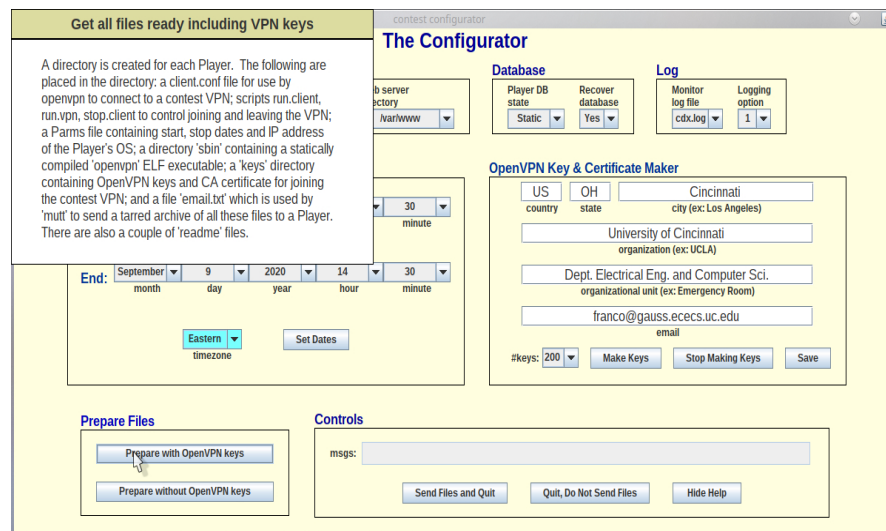


Figure 8: Example of a help box opened after hovering over the 'Prepare with OpenVPN keys' button

Accessibility

The following are accessibility features in the ready-made Client:

1. Little actual typing is necessary. The setup parameters are provided by the CA or other person in a file and the file populates most editable fields and all necessary fields in the GUI. New passwords are generated by one button click. A list of all Players is obtained by one button click – all commands, such as TRADE_REQUEST or GET_CERTIFICATE, that name a Player use the list: the Player merely clicks on the list entry to identify another Player.
2. Hovering over a button or field displays a popup that describes what the button or field is for. This 'help' feature can be turned on or off and is off by default.
3. Text to speech is supported. All transactions are text based and are printed to the console to the console to allow a text-to-speech translator to transform the text to speech if the 'Showing Messages' label on a Command Panel button is present. The text that is printed to the console does not contain all the words in the transactions, rather the console messages are designed to be understood with minimal dialog. Clicking the "Showing Messages" button disables this feature and changes the label to 'Not Showing Messages'. Clicking that button again enables the feature.

Acknowledgments

This project was influenced by the iWars project that was designed and written by several students including graduate students Jonathon Meeks, Hrishikesh Bhide, and Brad Kuhn plus undergraduate students Coleman Kane, Robert Sexton, and Greg Larson.

Appendix A – How an administrator sets up a contest

Collect Player information

Assume the CA is beginning from scratch without a player database. The CA collects the following information from people who will be players: their preferred contest name and their email address. If OpenVPN is to be used to support the contest network the CA needs to know the IP address of the host for the OpenVPN server.

Install the software and/or run it

The software is bundled in a file named `cdest.zip`. This unzips to a directory named `cdest`. Move `cdest.zip` to a desirable location in your directory structure and unzip it there. Change directory to `cdest`. In Linux run `cdx-lig.run`. In Windows run `cdx-wig.bat`. The CDX Control Panel appears (Figure 1).

Create a Player database, assign IP addresses, and save to file

Using information collected from Players, for each Player, in the line beginning with the 'Add' button, enter the Player's name (usually as requested by the Player), the Player's email address, and the IP address to be given to the Player. It is important that the Player sets its IP address to what is assigned or else the Scorer will not be able to probe that Player. If OpenVPN is used the IP address will be `10.8.0.XXX` where XXX is a number from 100 to 249 (depending on the credential sets that have been made and exist in directory `contest/keys`) that is chosen by the CA and should be unique with respect to all other Players, the OpenVPN server, and the Scorer. If OpenVPN is not used then the CA chooses IP addresses consistent with the requirements of the network the contest will be run on. After a Player's information is filled in, click the 'Add' button. At any time click the 'List' button to see what the player database looks like. Click the 'Save' button to copy the player database to a file with name specified in the source file `GameParameters.java` (`players.db` by default). The 'Save' button should be clicked at least once – when the contest Players have all been added. If some change to the player database must be made before the contest begins it is easiest to edit the player database file using a text editor. Otherwise, use the 'Delete' button in the Control Panel and then 'Add' the updated information for the Player. Use the 'Bump' button if a Player is to begin the contest with a non-zero number of points.

Configure a contest

The first and important thing to do if OpenVPN is going to be used to establish a contest network is type the IP address of the host for the OpenVPN server into the CDX Control Panel field named 'OpenVPN server location'. Then click the button named 'Configure' at the bottom of the Panel. This brings up the Configurator as shown in Figure 3. Edit the fields 'Web server URL', 'Scoreboard title', and 'Web server directory' as described in Section Contest Configuration Management on Page 1. Choose a DB state which is either Dynamic or Static. If Static, only the CA can edit the Player database using the 'Add' button in the CDX Control Panel, or by directly editing the player database file (likely `players.db`). If Dynamic, anyone can enter a Player in the database remotely. Details are in Appendix B. Choose whether restarting a contest should return state to what it had been when the contest was stopped. Choose how verbose the log is. The contest start and end times and days are set in the section 'Contest Dates and Times' – choose the dates and times and be sure to choose the correct time zone and then click the 'Set Dates' button. If OpenVPN is to be used the CA may fill in the fields in the 'OpenVPN Key & Certificate Maker' section, and click the 'Save' button. Choose 'Make Keys' to create new credentials. It is up to the discretion of the CA to make credentials before any particular contest. If credentials have to be re-distributed due to some failure, possibly a network failure, making new keys should be probably be avoided as that would change credentials for everyone surely leading to some problems connecting to the server for some or all Players.

Create files to be sent to Players

When satisfied with the configuration choices and after dates and times are set click the 'Prepare with OpenVPN keys' button if OpenVPN is to be used or the 'Prepare without OpenVPN keys' button. This action will create a directory called Contestants which contains a subdirectory for each Player in the player database with name the same as the Player's name and the contents of each Player subdirectory contains at least a file with the email address of the Player plus a file named Parm's with IP address and contest start and end times in unix and human readable format. If OpenVPN is used each Player subdirectory also contains OpenVPN credentials, a configuration file for openvpn, a statically compiled version of openvpn, and some scripts for starting and stopping the openvpn client. Directory Parameters which contains Parameters.txt, the configuration file to be used by the Scorer, is also created at this point. That file may be sent to the person who operates the Scorer during the contest in case 1) the Scorer is to be run on a machine other than the one used to configure the contest or 2) is on the same machine but run from a directory that is different from src-xxx (src-xxx has the Parameters.txt file as a result of this step).

Archive and send contest files to Players

Assuming no errors were encountered in creating the above directories click the 'Send Files and Quit' in Linux or 'Tar Files and Quit' in Windows. The result is each Player subdirectory of directory Contestants is archived as a tar file. In either Linux or Windows the CA may individually send those tar files to Players using the email address that is placed in email.txt in Players' directories. In the case of Linux, an attempt is made to automatically email the tar files using mutt. This will not work unless the machine used by the software is not blocked from sending email. In both Linux and Windows 10 Players can apply a tar command to unarchive the tar file they receive.

If an error occurs, it likely has something to do with OpenVPN. Check the player database file – particularly the IP addresses – and make sure keys and certificates have been created for all Players (there will be errors if too few credentials were created when making keys).

In case OpenVPN is used, a directory named VPNServer is created and a tar archive of all files that should be sent to the server host is placed in that directory. That tar file needs to be sent to the person who will maintain the OpenVPN server during the contest.

Create the contest network

The contest should be run on a private network. The CA must supervise the establishment of this network before the contest begins. If OpenVPN is to be used to create the network the file server.tar will be sent to the person responsible for maintaining the OpenVPN server. That person will untar the file received in a convenient location and must be able to use administrative privileges to run the script run.server as root. Doing so creates a network interface, most likely named tap0, that associates with the IP address 10.8.0.1. It may be necessary to additionally create a socks proxy in case the OpenVPN server operates from behind an organization's perimeter. This may be accomplished using an OpenSSH server and establishing an account, for example named visitor with a password to be distributed to Players that need to access the proxy. However, care must be taken to make sure that account will only allow access to the proxy and nothing else. It is recommended to put the OpenSSH server on a second machine behind the firewall to greatly limit the possibilities of an attacker to cause damage to organization machines. The proxy server could be started just before the contest and be terminated just after it ends for extra protection.

Start the contest and make checks

A contest may be started automatically or manually and may be controlled by the CDX Control Panel or by a command-line application. To start a contest manually from the CDX Control Panel just click he 'Start' button. Click the 'Stop' button to stop the contest or 'Suspend' then 'Resume' to suspend scoring then resume it. A stopped contest can be restarted only by exiting and re-running the Scorer software. When doing so care must be taken to make sure that the Recover option is set in the Parameters.txt

file that is loaded when the Scorer is re-run so that scores will be retained (it is safe for Recover to always be set because if it is desired to reset all scores to 0 on the re-run, this can be accomplished by clicking the 'Reset' button). If dates and times were set properly in the Configurator, they will occupy two lines in the Parameters.txt file which is read by the CDX Control Panel when the Scorer is run. Assuming the start time is in the future. Then there will be text at the bottom left of the Control Panel that says 'Time to start:' followed by a string formatted like this: dd:hh:mm:ss where dd is number of days, hh is number of hours, dd is number of days, and ss is number of seconds – this string counts down the time to the beginning of the contest. The Scorer does not probing during this countdown. Probing begins when the countdown reaches 0. At that moment the text changes to 'Time to end:' and a countdown to the scheduled end of the contest, with same format as above, begins. When that countdown reaches 0 probing ceases and the text changes to 'Contest: Finished'. The 'Start' button may be clicked to start the contest before the scheduled start time and the 'Stop' button may be clicked to stop the contest before the scheduled stop time.

The command-driven Scorer performs the same operations as the CDX Control Panel. It is ideal for scoring a contest, especially if the Scorer is on a remote machine. Both Windows and Linux allow a command-line application (free of any use of graphics) to be started remotely, then continue running after the connection to the remote machine is cut, then reconnected at a later time when it is desired to issue commands, in this case to observe or control the Scorer. One of the oldest such applications in Linux is called screen. One logs in remotely then runs screen which, after typing space twice, brings up a shell. The Scorer can be started in that shell. To disconnect yet keep the Scorer running type control-A then type d. You will see something like [detached from 66011.pts-0.gauss]. The number in that string is a process number used to reattach to the running process. You can log out then log in later and run the command screen -list which presents a message that looks something like this:

```
There is a screen on:
    66011.pts-0.gauss      (01/24/2021 02:55:57 PM)      (Detached)
  1 Socket in /run/screen/S-gauss.
```

To re-attach to the running process, for this example, run screen -r 66011.

An example of the use of the command-line Scorer is shown in Figure 6.

During the contest the CA should check that the scoreboard is available and being updated at short intervals. If the CA wants to make the log file publicly available, it should also make sure that file is reachable as well.

Appendix B – What A Player Does To Compete

Receive files from the Contest Administrator

Players receive a tar archive containing files that are important to joining the contest. A Player untars the archive in a convenient location. If OpenVPN is not used to establish a contest network then the only file in the archive is Pargs. See Appendix H for the contents of Pargs. With Pargs a Player will know what IP address it will be assigned, when the contest begins and when the contest ends. If OpenVPN is used additional files, as described in Appendix H, are used to join the contest.

Connect to the contest network

A Player needs to make sure its IP address is set to the value that is given in the Pargs file which is included in the archived set. This means DHCP (the usual default) is not used and a static IP address must be set instead. Doing this is straightforward with the tools that are available in Linux and Windows. If OpenVPN is used then the Player needs to connect to the OpenVPN server. To do this the Player must have administrative privileges. If the Player needs to connect to the network using a socks proxy the CA will have informed contestants what the account, password, and IP address of the socks proxy is. The Player will connect to that proxy in a manner described by the CA. If the socks proxy is created in Linux, say with the account name visitor on machine example.edu then the following line, followed by password when prompted, will open a proxy connection.

```
ssh -N -f -T -D 8080 visitor@example.edu
```

To use the proxy the Player must make sure the socks-proxy line in client.conf is uncommented (no semi-colon at the beginning of the line). To connect to the network invoke run.client. To quit the network invoke stop.client.

Join the competition

Normally, a competition is joined after the CA has started the Scorer. That happens at precisely the day and time given by the CA in the Pargs file. Before that time a Player should already have put its OS online at the specified IP address (set manually – not with DHCP) and started serving. The task of the Player is to ensure the specified services are up and running in its OS as often as possible and, possibly, to try to prevent an adversary's OS from having their services up and running.

Appendix C – Create a Competition VPN with OpenVPN

There are numerous details associated with creating a competition and getting all those details correct is a challenge. For this reason the configuration tool, discussed in detail in Section Contest Configuration Management, Page 1, was created. The configuration tool reduces the work in getting a competition set up to a few mouse clicks. However, in some cases, for example setting up a socks-proxy, some additional editing and/or distribution of files after using the tool will be necessary. This section presents what much of the tool does so as to enable a CA to work around any difficulties that are seen after the configuration tool is applied.

For OpenVPN to succeed it must cooperate with several other packages including OpenSSL, LZO, and EasyRSA, among others. But in our experience, one combination of versions of the above do not interact in the same way that another combination does rendering it difficult to create a lasting working environment for making OpenVPN credentials. Compounding this is that, at least for Ubuntu 20.04, the version of EasyRSA that is installed from repository is considerably out-of-date. Thus, installation of a specific, suitable collection of packages is detailed here before working with EasyRSA to create credentials is described. This will likely avoid many of the frustrations that we have experienced trying to get EasyRSA/OpenVPN to operate satisfactorily.

Assumptions

An OpenVPN server runs on a Linux host that is not inside an organization's firewall-protected perimeter
Player or Team OSes run on Linux machines, likely in VMs, that are outside the perimeter
The Linux host running the OpenVPN server is accessible via an OpenSSH server

Create the key-making environment

The instructions of this section, for the Linux operating system, are adapted from [the Anubiss github site](#)

Get and install OpenSSL

```
prompt> sudo mkdir /cdest // comment: choose any name you like
prompt> sudo chown user.user /cdest // user is the username of the person doing this
prompt> mkdir /cdest/contest
prompt> cd /cdest/contest
prompt> wget https://www.openssl.org/source/openssl-1.0.2j.tar.gz
prompt> tar -xvf openssl-1.0.2j.tar.gz && cd openssl-1.0.2j
prompt> ./Configure gcc -static -no-shared -prefix=/cdest/vpn
prompt> make
prompt> make install
```

check for the existence of /cdest/vpn/bin/openssl /cdest/vpn/lib/libssl.a

Get and install LZO2

```
prompt> cd /cdest/contest
prompt> wget http://www.oberhumer.com/opensource/lzo/download/lzo-2.09.tar.gz
prompt> tar -xvf lzo-2.09.tar.gz && cd lzo-2.09
prompt> ./configure --prefix=/cdest/vpn --enable-static --disable-debug
prompt> make
prompt> make install
```

check for the existence of /cdest/vpn/lib/liblzo2.a /cdest/vpn/lib/liblz02.la

Get and install OpenVPN

```
prompt> cd /cdest/contest
prompt> wget https://swupdate.openvpn.org/community/release/openvpn-2.3.12.tar.gz
prompt> tar -xvf openvpn-2.3.12.tar.gz && cd openvpn-2.3.12
prompt> ./configure --prefix=/cdest/vpn --enable-static --disable-shared \
--disable-debug --disable-plugins OPENSSL_SSL_LIBS="-L/cdest/vpn/lib -lssl" \
OPENSSL_SSL_CFLAGS="-I/cdest/vpn/include" \
OPENSSL_CRYPTO_LIBS="-L/cdest/vpn/lib -lcrypto" LZO_LIBS="-L/cdest/vpn/lib -llzo2" \
OPENSSL_CRYPTO_CFLAGS="-I/cdest/vpn/include" LZO_CFLAGS="-I/cdest/vpn/include"
prompt> make LIBS="-all-static"
```

```
prompt> make install
check for the existence of /cdest/vpn/sbin/openvpn
Move /cdest to a convenient, permanent location, for example /opt.
Prompt> sudo mv /cdest /opt
```

Get and install EasyRSA

Download EasyRSA-unix-v3.0.6.tgz from the Easy RSA github site

```
prompt> cd ~/Downloads
prompt> tar xf EasyRSA-unix-v3.0.6.tgz
prompt> mv EasyRSA-v3.0.6/* /opt/cdest/contest/
```

Note: it may be necessary to install bridge-utils (ex: sudo apt install bridge-utils)
you may as well do that to be on the safe side.

Note: consider disabling openvpn from automatic startup, if openvpn has been installed by a package manager, since a running openvpn may interfere with starting the server openvpn for the contest.

Create and distribute contest credentials and parameters

Assume the EasyRSA-v3.0.6 package has been moved to /opt/cdest/contest.

```
prompt> cd /opt/cdest/contest
prompt> cp vars.example vars
```

Edit the file vars:

```
#set_var EASYRSA_OPENSSL "openssl"           ← replace this
set_var EASYRSA_OPENSSL "../vpn/bin/openssl" ← with this
...
#set_var EASYRSA_DN "cn_only"                 ← change this
set_var EASYRSA_DN "org"                     ← with this
...
set_var EASY_REQ_COUNTRY "US"                 ← Choose country, city,
set_var EASY_REQ_PROVINCE "OH"                province, organization,
set_var EASY_REQ_CITY "Cincinnati"           organizational unit, and
set_var EASY_REQ_ORG "UC"                    email address that fits
set_var EASY_REQ_EMAIL "contestant@gmail.com" your site
set_var EASY_REQ_OU "EECS"
...
# In how many days should the root CA key expire?
#set_var EASYRSA_CA_EXPIRE 3650                ← 10 years default
set_var EASYRSA_CA_EXPIRE 365                 ← Suggest good for 1 year
...
# In how many days should certificates expire?
#set_var EASYRSA_CERT_EXPIRE 1080              ← almost 3 years default
set_var EASYRSA_CERT_EXPIRE 365               ← other certs good for 1 year
```

Make a Certification Authority certificate, server key, and server certificate from the command line

```
prompt> ./easyrsa --batch init-pki
prompt> ./easyrsa --batch build-ca nopass
prompt> EASYRSA_REQ_CN=server ./easyrsa --batch gen-req server nopass
prompt> ./easyrsa --batch sign-req server server
```

OpenVPN has a mechanism which maps a Player's common name (EASYRSA_REQ_CN) to an IP address. This entails making a file whose name is the Players common name and whose content is the IP address and netmask and adding an entry such as client0,10.8.0.50 in a file named ipp.txt. To prepare for this do the following:

```
prompt> mkdir server
prompt> mkdir server/ccd
prompt> mkdir server/keys
prompt> cp pki/ca.crt server/keys
```

```
prompt> cp pki/private/server.key server/keys
prompt> cp pki/issued/server.crt server/keys
```

Then, for each Player, make credentials that will be passed to the Player. The credentials consist of two certificates and one key. Naming format is <Common-Name>.key and <Common-Name>.crt. Let <Common-Name> be client0. One certificate, ca.crt, has already been made in a previous step. To make and place the remaining credentials of client0 do this:

```
prompt> EASYRSA_REQ_CN=client0 ./easyrsa --batch gen-req client0 nopass
prompt> ./easyrsa --batch sign-req client client0
prompt> echo "ifconfig-push 10.8.0.50 255.255.255.0" > server/ccd/client0
prompt> echo "client0,10.8.0.50" >> server/ipp.txt
```

Check directory pki/issued/ for client0.crt and pki/private for client0.key. Repeat for all Player Common Names (which do not have to match contest Player identities). When done, if, say, 50 client keys and certificates were made with Common Names from client0 to client49 then directory pki/issued should have client0.crt to client49.crt plus server.crt and directory pki/private should have ca.key, server.key and client0.key to client49.key. Finally, run

```
prompt> ../vpn/bin/openssl dhparam -out pki/dh2048.pem 2048
```

Check directory pki for dh2048.pem.

The OpenVPN server needs to have configuration files made. Enter the server directory.

```
prompt> cd server
```

current directory is /opt/cdest/contest/server

Create file server.conf with the following contents in directory /opt/cdest/contest/server :

```
# the address of the machine which hosts the openvpn server
local 10.52.10.254          - change this to match the IP address of the machine running
                           the openvpn server

# the port - 1194 is the usual
port 1194

# TCP or UDP server - I have run successful contests with tcp
proto tcp

# dev tap means ethernet frames, dev tun means tcp packets
dev tap

# server credentials
ca keys/ca.crt
cert keys/server.crt
key keys/server.key # This file should be kept secret
dh keys/dh2048.pem

# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 10.8.0.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file. If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist ipp.txt 0

# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific
# configuration files
client-config-dir ccd
```

```

route 10.8.0.0 255.255.255.0

# There should be one file in ccd for every key
# that has been made for a Client and the name
# of the file should be the Common Name given to
# that key. The format of the file in directory ccd
# is
#   ifconfig-push <ip-address-of-client> 10.8.0.1
#
# For example, for a Client key with Common Name client0
# a file client0 is created in ccd which has only the
# following line:
#   ifconfig-push 10.8.0.50 10.8.0.1
#
# where 10.8.0.50 is the IP address that has been
# assigned by the Contest Administrator to the
# Client who gets the key with Common Name client0.
# If X is the number of Client keys created there will
# be X files in directory ccd and each will
# have the one line format above. For this distribution
# Common Names will range from client0 to client49.

# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 10.8.0.0 255.255.255.0

# Allows different clients to see each other
client-to-client

# Ping-like messages are sent back and forth so each side
# knows when others go down. The following causes a ping
# every 10 seconds, the peer is considered down if there
# is no response in 120 seconds.
keepalive 10 120

# Choose cipher
cipher AES-128-CBC # AES

# Enable compression on the VPN link.
comp-lzo

# The maximum number of concurrently connected clients allowed
max-clients 200

# Reduce the OpenVPN daemon's privileges after initialization.
user nobody
group nogroup

# Avoid accessing resources on restart no longer be accessible due to privilege downgrade.
persist-key
persist-tun

# Show current connections, truncated and rewritten every minute.
status openvpn-status.log

# log file - new one on restart. Use log-append openvpn.log to append to existing log file
log openvpn.log

# verbosity 4 - reasonable for general usage
verb 4

```

Create server start script `run.server` in directory `/opt/cdest/contest/server` with the following contents:

```

#!/bin/bash
# first line is likely necessary - other openvpn processes
# may interfere with the one that is being started here
sudo killall openvpn

```

```
sleep 2
sudo ./run.vpn
```

and create run.vpn in the same directory

```
../../vpn/sbin/openvpn server.conf &
echo $! > vpn.pid
```

Create server stop script stop.server in directory /opt/cdest/contest/server:

```
#!/bin/bash
if [ -e vpn.pid ]; then
    sudo kill `cat vpn.pid`
    rm -f vpn.pid
fi
```

Note: once familiar with this package the user may attempt to use the OS's openvpn instead of the one built above. In that case, openvpn should be in the system path and /opt/cdest/vpn/sbin/openvpn in run.server can be replaced with openvpn.

Make all the scripts executable

```
chmod a+x run.server stop.server
```

Directory /opt/cdest/contest/server contains directory ccd with many files whose names are the Common Names given to Player credentials plus files ipp.txt, run.server, stop.server, server.conf. There is also a keys directory which now needs to be populated with the server's credentials as follows:

```
prompt> cp ../pki/dh2048.pem keys
prompt> cp ../pki/issued/server.crt keys
prompt> cp ../pki/private/server.key keys
prompt> cp ../pki/ca.crt keys
```

The server directory may now be archived and sent to the person that will maintain the OpenVPN server.

```
prompt> cd ..
prompt> tar cf server.tar server
```

For each Common Name a directory similar to that of server is to be created, populated, archived, and sent to the Player for whom the Common Name applies. This is done here for client0.

```
prompt> cd ..
prompt> mkdir client0
prompt> mkdir client0/keys
prompt> cd client0
```

current directory is /opt/cdest/contest/client0

Create file client.conf with the following contents in directory /opt/cdest/contest/client:

```
# Specify that this is a client
client

# Use the same setting as on the server - choose tap
dev tap

# Connect to a TCP server
proto tcp

# The hostname/IP and port of the server.
remote 10.52.10.254 1194      ← replace 10.52.10.254 with local address used in server.conf
                             unless a socks proxy is used (then use remote localhost 1194)

# Keep trying indefinitely to resolve the host name of the OpenVPN server.
resolv-retry infinite

# Most clients don't need to bind to a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
```

```

user nobody
group nogroup

# Try to preserve some state across restarts.
persist-key
persist-tun

# credentials
ca keys/ca.crt
cert keys/client0.crt          - replace client0 with Common Name of client
key keys/client0.key           - replace client0 with Common Name of client

remote-cert-eku "TLS Web Server Authentication"

# cipher same as for the server
cipher AES-128-CBC

# compression
comp-lzo

# log file verbosity.
verb 4

# Do not use socks proxy if Client is inside perimeter:
# otherwise uncomment by removing ';'
; socks-proxy 127.0.0.1 8080    - uncomment if using a socks proxy

```

Create Client start script `run.client` in directory `/opt/cdest/contest/client0` with the following contents:

```

#!/bin/bash
# consider uncommenting next line if Client is the
# only Client on host
# sudo killall openvpn
# uncomment the next 3 lines if a socks-proxy is to be used
# sleep 1
# ssh -N -f -T -D 8080 <login-name-of-proxy-host>@<IP-address-of-openvpn-server-host>
# sleep 1
sudo ./run.vpn

```

and create `run.vpn` in the same directory

```

#!/bin/bash
../../vpn/sbin/openvpn client.conf &
echo $! > vpn.pid

```

Note: `/opt/cdest/vpn/sbin/openvpn` can be replaced with `openvpn` if the host has `openvpn` installed from a repository and `openvpn` is visible to applications.

Create Client stop script `stop.client` in directory `/opt/cdest/contest/client0`:

```

#!/bin/bash
LINE=`pstree -paul | grep ssh | grep 8080 | grep <login-name-proxy-host>`
IFS=' ' read -ra N <<< $LINE
PID=${N[1]}
if [ -z "$PID" ]; then
    echo no proxy running
else
    kill $PID
    echo proxy with pid $PID killed
fi

if [ -e vpn.pid ]; then
    sudo kill `cat vpn.pid`
    rm -f vpn.pid
fi

```

The `stop.client` script contains code that kills a socks proxy that would have been activated if the commented portion of `run.client` was uncommented. There should not be side-effects if `stop.client` is run when no socks proxy exists.

Make all the scripts executable

```
chmod a+x run.client stop.client
```

Create the Parms file that is used to provide information to the Client that enables the Client to enter a competition. The following is an example.

```
# Start Time
1599516000          ← POSIX time that contest will start
07.09.2020 18:00:00 Eastern ← start time in human readable form

# End Time
1599775200          ← POSIX time that contest will end
10.09.2020 18:00:00 Eastern ← end time in human readable form

# Client Location
10.8.0.200          ← IP address of the Player's Servers
```

Directory /opt/cdest/contest/client0 contains scripts run.client, stop.client, and files Parms and client.conf. There is also a keys directory which now needs to be populated with the Player's credentials as follows:

```
prompt> cp ../pki/issued/client0.crt keys
prompt> cp ../pki/private/client0.key keys
prompt> cp ../pki/ca.crt keys
```

The client0 directory may now be archived and sent to the person that will operate the OS designated as client0.

```
prompt> cd ..
prompt> tar cf client0.tar client0
```

The above is repeated for all OSes in the contest.

Start the openvpn server

Whatever machine the server is operated from, it should have access to an openvpn binary that is in directory /opt/cdest/vpn/sbin where the openvpn executable built above resides (or else change the path to openvpn in run.server). To start the VPN server run the following:

```
prompt> run.server
```

Stop the openvpn server

To stop the VPN server run the following from the same directory that run.server was run from.

```
prompt> stop.server
```

Player's OS joins the VPN

Assume that /opt/cdest/vpn/sbin/openvpn exists (could be just a link to some installed openvpn). A Player receives <player-name>.tar from the CA. The Player untars the file.

```
tar xf <player-name>.tar
```

This results in directory clientX which contains run.client, stop.client, client.conf, Parms, and subdirectory keys which contains ca.crt, clientX.key, and clientX.crt where X is a number from 0 to 49 assuming the setup above was followed (otherwise the client key and certificate could be anything the CA chooses). To join the VPN the Player executes

```
prompt> run.client
```

This adds IP address 10.8.0.Y to the Client host's network interface.

Note: the server has file `clientX` in its `ccd` directory and the contents of `clientX` is
`ifconfig-push 10.8.0.Y 255.255.255.0`

Note: the server also has a line in `ipp.txt` that says
`clientX,10.8.0.Y`

Then the Player checks the ip address with the command:

```
/sbin/ifconfig
```

Before starting its OS, the Player makes use of the information in the `Parms` file to set up its OS – the IP address of the OS must be set as in the `Parms` file and the start time should be noted and the OS must be providing services by that time. Then the OS services can be started.

Appendix D – How to Join the VPN Network

Assumptions

The Player will enter the competition through a Virtualbox VM that is a Linux variant.

The instructions below are written specifically for Ubuntu 20.04 but similar procedures apply for others

The Ubuntu 20.04 desktop install iso has been downloaded from [the Ubuntu website](#).

The Player receives <player-name>.tar from the CA containing files in Appendix H.

The competition Monitor is run in a VPN which is behind some organization's firewall-protected perimeter

Overview

The competition is run over an IPv4 VPN network which is facilitated by the OpenVPN package. IP addresses given to Players are pre-assigned in the range 10.8.0.100 to 10.8.0.249. Since each Player may get more than one contest account, depending on the decision of the CA, each Player may be assigned more than one set of credentials and therefore more than one VPN IP address. Player (or Team) OSes are expected to be installed on separate VMs – one VM hosting one Player (or Team) OS. Instructions for setting up those VMs are given below assuming Virtualbox is used as a (type 2) hypervisor.

What the Player needs to do

Virtualbox may be downloaded from [the Virtualbox website](#). The extension needs to be obtained as well: click 'All supported platforms'. Installation for Windows or MacOS begins by clicking one of those links. To install in a Linux distribution click the 'Linux distributions' link and then scroll down until you reach instructions for your OS. To install the extension start Virtualbox (command line: virtualbox, menu: system). Open the 'File' menu and select 'preferences'. Click 'Extensions' to bring up the dialog box shown in Figure 9.

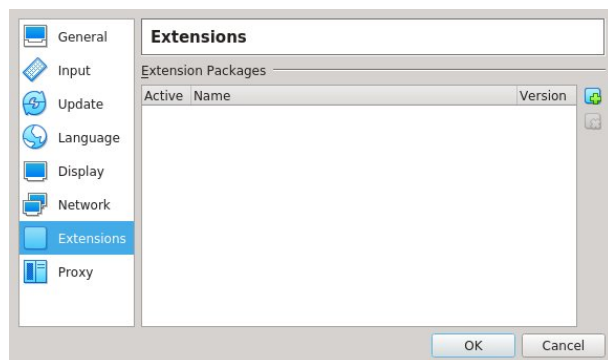


Figure 9: Click the blue-green square icon to load extensions

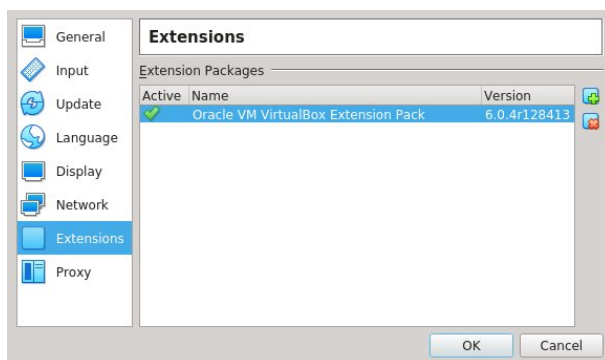


Figure 10: Extensions have been loaded

Click on the small blue-green square icon with a plus in the lower right corner to bring up a file dialog box. Select the downloaded extensions file and then click on install, accept, and so on. If done correctly the extensions dialog box will be as shown in Figure 10.

Create an Ubuntu VM in Virtualbox

The first step is to prepare an environment for the OS. Click the 'New' button shown in Figure 12 top and fill in the details as shown in Figure 12 middle except change /home/franco to the Player's home directory. Click 'Next' and choose a memory size as big as can be made (say 3GB if the host computer has 16GB of RAM). Click 'Next', then click 'Create', then click 'Next', click 'Next', choose, say 30GB, for the disk size (the disk actually uses much less storage - the 30GB is just a maximum size). Then click 'Create'. A new tag appears in the left margin of the Virtualbox screen as shown in Figure 12 bottom.

With the new tag selected click the 'Settings' icon as shown in Figure 11 top and select 'Storage' to get the screen in Figure 11 bottom. Click the small blue disk with a plus to the right of 'Controller: IDE' as seen in Figure 11 bottom. Click 'Choose disk' - select the downloaded Ubuntu iso image (which should be in the Downloads directory). Then select the new Ubuntu entry in the storage dialog, click 'OK', and click the green arrow facing right, shown in Figure 11 top. The Ubuntu install image will boot. Choose install - answer questions on the way - choose language, choose normal installation, choose 'Erase and install Ubuntu' and click 'Install Now'. Choose 'Continue' to write changes to disk, enter name, username, password, timezone etc. Reboot when a dialog box appears and says to do so.



Figure 12: Create an environment for the new VM

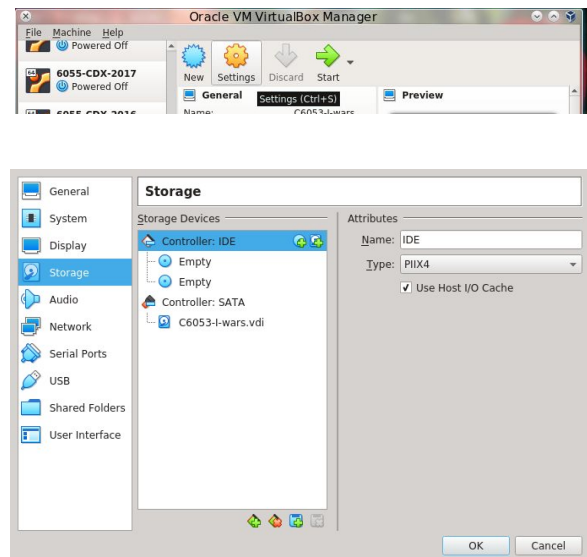


Figure 11: Ubuntu ISO as a disk drive

Configure the Ubuntu VM

With the VM powered down, configure the OS by selecting the VM tag on the left of the Virtualbox main dialog box and clicking 'Settings' as before. Then select the tags in the left side of the Settings box one by one and choose resources and settings. Most of the defaults are OK. Increase the number of cores dedicated to the VM, if possible. Changing the Graphics Controller to VBoxSVGA should provide increased screen area. The Network should be set to NAT as shown in Figure 13.

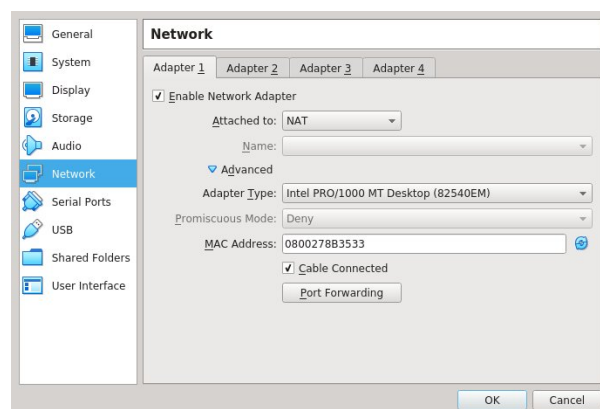


Figure 13: Network setting

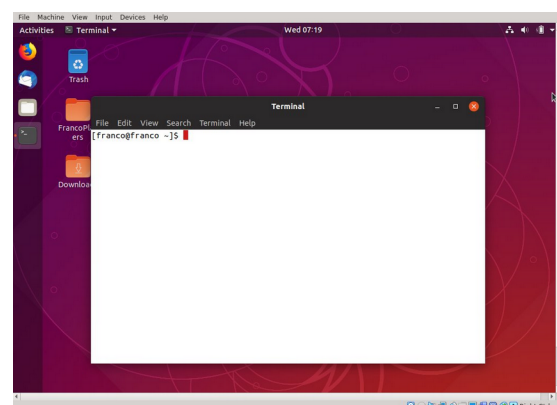


Figure 14: Desktop

Update and install software

Open Virtualbox, select the VM tag in the left margin, click the green arrow facing right to boot the OS. Once logged in, open the 'Activities' menu at the top left, search for 'terminal', and hit return. The desktop looks something like Figure 12. Update the OS using the commands below which are entered at the terminal prompt.

```
prompt> sudo apt update
prompt> sudo apt upgrade
```

The OS will authenticate by asking for the password specified during the OS install after the first sudo only. Next, install important software.

Make sure OpenVPN is installed with

```
prompt> locate openvpn | grep bin
```

If it is not installed it can be obtained with

```
prompt> sudo apt install openvpn
```

Also run

```
sudo apt install net-tools bridge-utils
```

Next, place files obtained from the CA and use credential info.

Each Player is given the following file (see Appendix I for the files it contains):

```
<player-name>.tar
```

The files are intended for a single VM. To get the files into the VM find out the IP address of the host that these files exist on. This is done in Linux with `/sbin/ifconfig`. If the host is Windows use `ipconfig` from powershell. Say the host IP address is 192.168.1.103. Also, determine the directory those files are in on the host. Say it's `~/Downloads`. From a terminal in the VM:

```
mkdir ~/Contest
cd ~/Contest
scp <host-username>@192.168.1.103:Downloads/<player-name>.tar .
```

Next untar the tar file like this:

```
tar xf <player-name>.tar
```

This results in a directory named `<player-name>` with subdirectory `keys` plus start and stop scripts and `client.conf`. The keys and certificates in the directory `keys` are unique to a single account and, among other things, they determine what the VPN IP address of the account will be. The `<player-name>` directory can be placed anywhere that can be accessed by a normal user, such as that user's home directory.

The next step is to connect to the VPN.

Join the VPN

Change directory to `<player-name>`. Look at `run.client`. Here are the contents with lines 2 to 5 uncommented:

```
#!/bin/bash
sudo killall openvpn
sleep 1
ssh -N -f -T -D 8080 visitor@example.edu
sleep 1
sudo openvpn client.conf
echo $! > client.pid
```

The `ssh` line establishes a socks5 proxy behind the organization's firewall to allow external communication to port 1194 of the openvpn server. For illustration only, suppose an account named `visitor` has been created on a machine named `example.edu` which is inside the organization's

(uc.edu) perimeter. Although the socks5 proxy is intended for external communication it should work just fine inside the organization's network so there is no need to change anything if the competition VPN is entered from outside or inside the organization's perimeter. Commenting out the ssh line is OK inside the organization's perimeter but then the last line in `client.conf` must be commented or removed as well. Run `run.client` like this:

```
prompt> ./run.client
```

The result is a long output which ends with something similar to this:

```
Wed Mar 20 09:56:29 2019 us=137912 do_ifconfig, tt->ipv6=0, tt->did_...
Wed Mar 20 09:56:29 2019 us=138002 /sbin/ip link set dev tap0 up mtu 1500
Wed Mar 20 09:56:29 2019 us=141321 /sbin/ip addr add dev tap0 10.8.0.104/24...
Wed Mar 20 09:56:29 2019 us=144110 GID set to nogroup
Wed Mar 20 09:56:29 2019 us=144175 UID set to nobody
Wed Mar 20 09:56:29 2019 us=144203 Initialization Sequence Completed
```

If Initialization Sequence Completed is not observed something is wrong. If so, the problem could be due to an already running instance of `openvpn` or `vpnagentd` that was not killed (most common problem) or the keys can not be found because their location does not match that stated in `client.conf`.

Here are some additional checks. Run `/sbin/ifconfig` to get something like this:

```
tap0  Link encap:Ethernet  HWaddr 4e:f3:3f:3d:f8:b5
      inet addr:10.8.0.101  Bcast:10.8.0.255  Mask:255.255.255.0
      inet6 addr: fe80::4cf3:3fff:fe3d:f8b5/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:50 errors:0 dropped:0 overruns:0 frame:0
      TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:2100 (2.1 KB)  TX bytes:6414 (6.4 KB)
```

No tap interface means there is no connection to the VPN. If the Scorer is running and its IP address is known to be, say, `10.8.0.100`, try this to make sure you can connect to it.

```
ping 10.8.0.100
PING 10.8.0.100 (10.8.0.100) 56(84) bytes of data.
64 bytes from 10.8.0.100: icmp_seq=1 ttl=64 time=77.1 ms
64 bytes from 10.8.0.100: icmp_seq=2 ttl=64 time=37.4 ms
64 bytes from 10.8.0.100: icmp_seq=3 ttl=64 time=35.2 ms

--- 10.8.0.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 35.258/49.958/77.126/19.232 ms
```

Passing the above tests means the Client software is connected to the VPN.

Disconnect from the VPN

To disconnect run

```
prompt> ./stop.client
```

Appendix E – Hard Coded Configuration Parameters

File	Line	Purpose
CheckServices.java	srvports[0] = "13/tcp";	Services to be monitored by the Scorer. These include, in order, daytime, ftp, http, printer, mysql
	srvports[1] = "21/tcp";	
	srvports[2] = "80/tcp";	
	srvports[3] = "631/tcp";	
	srvports[4] = "3306/tcp";	
ConfigFrame.java	fos = new FileOutputStream("../Parameters/Parameters.txt");	Fix "Parameters.txt" name
	fos = new FileOutputStream("Parameters.txt");	
	fis = new FileInputStream(GameParameters.PLAYER_DB_FILE);	Fix "players.db" name
	String ip="10.8.0."+ip_count++;	Set IP address 3 octets
	FileOutputStream fos = new FileOutputStream(contdir+"/Parms");	Fix "Parms" name for OpenVPN
	FileOutputStream fos = new FileOutputStream(contdir+"/email.txt");	Fix "email.txt" name
DynamicListener.java	socket = new ServerSocket(9180);	Entry port for Dynamic mode
GameParameters.java	public static String GAME_DIRECTORY = "./"	Game directory
	static final String PLAYER_DB_FILE = "players.db";	Fix "players.db" name
	public static int TIME_BETWEEN_PLAYER_PROBES = 10000;	Fix time between probes in milliseconds
Monitor.java	String logfile = "cdx.log";	Fix name of log file
	HTTPQuery q = new HTTPQuery(player, "wordpress/?p=4", 80, phrase, null);	Fix WordPress query
	HTTPQuery q = new HTTPQuery(player, "index.html", 80, "<head>", null);	Fix HTTP query

Appendix F – Sample Configurations and Skill Levels

Configuration	CA Decisions	Group/Machines
Basic	Ready made Clients are handed out to competitors Three VMs and three Clients per team No authentication, encryption, integrity checking Monitor source and binary is withheld Monitor log is made public	Middle School Monitor on desktop Clients on laptops Students do not code
Intermediate	Ready made Clients are handed out to competitors Ten VMs and Clients per team Authentication, encryption, integrity checking provided Monitor source code and binary are withheld Monitor log is made public	High School Monitor on desktop Clients on laptops Students choose protection params
Experienced	Teams build Clients using high level language Existing libraries may be used Twenty VMs and Clients per team Authentication, encryption, integrity checking provided Monitor source code is distributed Monitor log is made public	University Monitor on server Clients on student computers VPN networked
Advanced	Teams must build Clients using assembly language Existing networking libraries disallowed Hundreds of VMs and Clients per team Client binaries may or may not be distributed Authentication, encryption, integrity checking supported Monitor binary is made public, source withheld Monitor log is withheld	Advanced Monitor and Clients run on Cyber Range

Table 5: Sample configurations and target audience with expected supporting computing environment

CO Skill / Motivating	Configurations			
	Basic	Intermediate	Experienced	Advanced
Low-level coding	No	No	No	Yes
Operating System coding/analysis	No	No	No	Yes
Networking	No	No	Slight	Yes
Advanced analysis	No	No	Slight	Yes
Advanced tools	No	No	Yes	Yes
Elementary analysis	No	Slight	Yes	Yes
Defend	Slight	Yes	Yes	Yes
Attack	Yes	Yes	Yes	Yes
Engrossing	Yes	Yes	Yes	Yes

Table 6: Expected impact on CO skill development by sample configurations described in Table 5

Appendix G - Configurator Parameter Descriptions

Web Server

Web server URL:

The URL that a browser uses to access the scoreboard and log file. This is used in the scoreboard html file to make scoreboard refreshes point to the location of the scoreboard. The default is `http://example.edu` which obviously needs to be changed.

Scoreboard title:

The title the scoreboard takes. For example 'CDX Practice Contest' to indicate that a practice contest is in session. The default is just 'Contest' as shown in Figure 3.

Web server directory:

The place where the scoreboard.html file and cdx.log file should be placed so that they can be served to the web

Database

Player DB state:

Possibilities are STATIC and DYNAMIC. In the case of DYNAMIC a Player may create its own OS identities, as many as it would like. This state is most suitable for practice and development. A STATIC state is used for contests. A Player is assigned an identity as well as IP address by the CA and only by the CA.

Recover database:

If YES, the old player database file is retained after the Scorer is killed and is reinstated when the Scorer is restarted. If NO, the database file scores are cleared (become 0) when the Scorer is restarted.

Log

Monitor log file:

The name of the file which contains the contest log. The file is located in the same directory as the monitor executable. This name is fixed at `cdx.log`.

Logging option:

- 1: Events named below plus events that occur during file and direction creation, and deletion, and file reading
- 2: Events named below plus events that occur during configuration
- 3: Events named below plus other events that take place during a contest
- 4: Events concerned with checking that services are up

Contest Dates and Times

Start:

Select the time and day the contest will begin. Choose month, day, year, hour, and minute. This information is recorded in file `Parms`, a unique version of which is given to Players, in both Unix time and human readable time, to enable a Player to easily get ready for the contest either by developing a function that automatically starts its OS at the appropriate time or by joining a contest manually. `Parameters.txt` also gets this information. Times selected are in local time as indicated by the timezone menu (see below).

End:

Select the time and day the contest will end. Choose month, day, year, hour, and minute. This information is recorded in `Parms`, a unique version of which is given to Players, in both Unix time and human readable time to enable a Player to easily get ready for the contest end either by developing a function that automatically shuts its OS at the appropriate time or by joining a contest

manually. `Parameters.txt` also gets this information. Times selected are in local time as indicated by the timezone menu (see below).

timezone:

Select the official timezone for the contest. Daylight savings is automatically accounted for. As stated above the start and end times are given in Unix time and human readable time. The Unix time includes the timezone information.

Save Dates:

Click to record the dates in `Parms` files and `Parameters.txt`.

OpenVPN Key & Certificate Maker

country, state, city, organization, organizational unit:

The address and organization that is hosting the contest. This information becomes part of the OpenVPN credentials that are given to the Players. If OpenVPN is not used then these fields are irrelevant and may be left blank. Otherwise, no field is to be left blank. A default is provided and should be edited. It is OK for blank spaces to exist in any of the fields.

email:

Email address of the Contest Administrator that is taking care of the contest. This is needed only if OpenVPN is used. Otherwise, this field may be left blank. A default is provided.

#keys:

The number of key/certificate pairs (credentials) to be made. If OpenVPN is to be used, these credentials will be distributed to Players. The possibilities are 150, 100, and 50.

Make Keys:

Begin the process of making the OpenVPN key/certificate pairs, the number of which is given by the #keys menu. This takes a very long time, especially to make 150 credentials. When completed certificates `clientXX.crt` and `server.crt` appear in directory `contest/keys/issued`, `clientXX.key` and `server.key` appear in directory `contest/keys/private`, and `ca.crt` and `dh2048.pem` appear in directory `contest/keys`. The XX in those file names is a number from 1 to 255. Nothing is distributed at this point and no credentials will be distributed if OpenVPN is not used, but the credentials can be made regardless. Credentials do not have to be remade for each contest. Any pre-existing files in the directories named above are erased when this button is clicked.

Stop Making Keys:

May be clicked while credentials are being made to stop the process. All credentials made up until that time remain but some things are incomplete such as `dh2048.pem`.

Save:

Click this button to save the organizational and email above the button to file `game-id.txt`. When the Configurator is launched this file is read and its contents are shown in the organizational fields. The `game-id.txt` file is a simple text file that can be edited by a text editor.

Prepare Files

Prepare with OpenVPN keys:

Click this button to create directories for each Player and to include in those directories `Parms` and OpenVPN credentials and configuration files, plus `email.txt` which contains the email address of the Player who will receive the files. All Player directories appear in directory `Contestants`. See Appendix H for a description of the files and directory structure in Player directories. Directory `Parameters` is also created with its only contents as `Parameters.txt` which is contest information for the CA.

Prepare without OpenVPN keys:

Click this button to create directories for each Player containing only `Parms` and `email.txt`. These directories appear in directory `Contestants`. Directory `Parameters` is also created and contains file `Parameters.txt` for the CA.

Controls

Send Files and Quit:

Click this button to archive all the Player directories as tar files. All the Player tar files appear in directory Contestants. These files are sent to the email address given for the Players. In addition, if 'Prepare Files with OpenVPN' had been clicked, the directory VPNServer is created and contains an archive server.tar of all the information an OpenVPN server needs to set up a VPN for the contest. The CA must ensure that this archive is received by the OpenVPN server host.

Quit, Do Not Send Files:

Exit the Configurator without sending any files to anyone. The directories Contestants, Parameters, and VPNServer, if they exist, remain.

Show Help:

Click this button to see help windows for each of the menus and buttons displayed in the Configurator. Just move the mouse cursor over a button or menu and information about that widget appears as, for example, in Figure 8. Move the mouse cursor to another widget and the current Help window is replaced by a Help window for the widget the mouse is currently over. The 'Show Help' button becomes the 'Hide Help' button when it is clicked. Click the 'Hide Help' button to remove the currently displayed Help window and disable the Help function. This function has no effect on the CDX Control Panel.

Cancel:

Click this button to exit from the Configurator without any configuration changes being saved.

msgs:

Notifications are shown here

Appendix H - Structure of Files in Player Directories

Player directories are located in directory Contestants and have the form <player-name> where <player-name> is what is entered in the rightmost field of a line in the player database file except that blanks are replaced with underscore characters. The name of the player database file is determined from GameParameters.java and is players.db by default.

Parms:

This file is unique to all Players and exists regardless of whether OpenVPN is used. It contains contest start time, end time, and IP address assigned to the Player's OS by the CA. Here is a sample Parms file:

```
# Start Time
1599516000
07.09.2020 18:00:00 Eastern

# End Time
1599775200
10.09.2020 18:00:00 Eastern

# Client Location
10.8.0.228
```

The start and end times are translations to Unix time from the date and time selected and saved in Configurator (Figure 3). A human readable date and time is also displayed. The OS location comes from the third field of a line of the player database file (named players.db by default). The OS location, which is the IP address from which all the Player OS services are accessible, can be entered using the 'Add' command in the add player window as shown in Figure 2.

run.client:

This is a script in the package sent to Players and may be used to connect a Player's OS to an OpenVPN network. This script is included only if OpenVPN is used. Line 4 is where the socks-proxy is invoked, if needed. In the supplied run.client file this is commented, meaning no socks proxy is used. Uncomment Lines 4 and 5 if a socks-proxy is used and replace the address visitor@helios.ececs.uc.edu with the address of the correct competition socks-proxy server. Also uncomment the socks-proxy line in client.conf (see below). If Player Oses are to have one IP address per host the CA may decide to uncomment lines 2 and 3 to make sure no other openvpn processes are running when Line 6 is reached – interference with other openvpn processes will likely prevent a connection with the openvpn server. All edits are done for convenience before configuration so as not to have to change a file for each Player.

```
#!/bin/bash
# sudo killall openvpn
# sleep 1
# ssh -N -f -T -D 8080 visitor@helios.uc.edu
# sleep 1
sudo ./run.vpn
```

run.vpn:

This is called from run.client and is included only if OpenVPN is used. Its lines are separated from run.client so that stop.client can be used effectively. The script runs the statically compiled openvpn in subdirectory sbin on client.conf. The process number of openvpn is saved in file vpn.pid, to be used by stop.client later. Contents of run.vpn are:

```
#!/bin/sh
./sbin/openvpn client.conf &
echo $! > vpn.pid
```

stop.client:

A script in the package sent to Players which is executed by a Player's OS to kill the connection to the OpenVPN network if such a network is used. This script also terminates the connection to the proxy, if one is used. The Player will have to edit line 2 and replace 'visitor' with the username associated with the proxy, and uncomment the commented lines if a socks proxy is used. If the local port is different from 8080 that number needs to be changed here and in client.conf. This script is included only if OpenVPN is used.

```
#!/bin/bash
# LINE=`pstree -paul | grep ssh | grep 8080 | grep visitor`
# IFS=', ' read -ra N <<< $LINE
# PID=${N[1]}
# if [ -z "$PID" ]; then
#   echo no proxy running
# else
#   kill -9 $PID
#   echo proxy with pid $PID killed
# fi

if [ -e vpn.pid ]; then
    sudo kill -9 `cat vpn.pid`
    rm -f vpn.pid
fi
```

client.conf:

This is the OpenVPN configuration file that is sent to Players if OpenVPN is used. The text below is the uncommented contents of a typical configuration file. All Players will see the same uncommented contents except for the lines beginning with cert, and key. Keys and certificates will be custom created for each Player and the names of the key and certificate files for each Player must replace the names in those lines below. This is done automatically by the 'Make Keys' command of Figure 7 and Page 36 and 'Prepare with OpenVPN keys' on Page 36, and 'Send Files and Quit' on Page 37. The line beginning with remote shows an IP address which is set in the 'OpenVPN server location' field of the CDX Control Panel shown in Figure 2. If a socks-proxy is used, the semi-colon at the beginning of the line starting with socks-proxy must be removed (the semi-colon at the beginning of a line means the line is commented out). The CA should not have to edit this file.

```
client
dev tap
proto tcp
resolv-retry infinite
nobind
user nobody
group nogroup
persist-key
persist-tun
remote-cert-eku "TLS Web Server Authentication"
cipher AES-128-CBC
comp-lzo
verb 4
;socks-proxy 127.0.0.1 8080 # uncomment to use a socks proxy
ca keys/ca.crt
cert keys/client0.crt
key keys/client0.key
remote localhost 1194
```

Other files in a Player's directory:

- email.txt: has the email address of the recipient of the Player's tar file
- JAVA.txt: instructions for using Java
- README.txt: general usage information
- openvpn: executable for establishing a tap connection, located in subdirectory sbin
- ca.crt: OpenVPN server's certificate, located in subdirectory keys
- clientXX.crt: Player's OpenVPN certificate, located in subdirectory keys
- clientXX.key: Player's OpenVPN key, located in subdirectory keys

Appendix I - Files in Parameters and VPNServer directories

Parameters.txt:

This file is intended for the administrator of the contest and is the only file in directory Parameters. The directory and file are created when 'Prepare with OpenVPN keys' or 'Prepare without OpenVPN keys' is invoked in the Configurator. Contents are, by example, as follows:

```
//Database Parameters
PLAYER_DATABASE_STATE 0

//Recover Parameters
RECOVERY_STATE 1

//Logging Parameters
LOG_FILE cdx.log
LOGGING_OPTION 0

//Scorecard Parameters
SCORECARD_FILE standings.html
WEB_URL http://example.edu/
SCORECARD_TITLE Contest
WEB_DIRECTORY /var/www/

//Extra
START_TIME_UNIX 1599516000
START_TIME_CONV 07.09.2020 18:00:00 Eastern
END_TIME_UNIX 1599775200
END_IIME_CONV 10.09.2020 18:00:00 Eastern
```

The meaning of the parameters is given in Appendix G.

server.conf:

This is the configuration file for the OpenVPN server and is in `server.tar` in subdirectory `VPNServer`. The following shows the uncommented lines from `server.conf`. The `ca`, `cert`, and `key` lines act as similar lines do for `client.conf` except that in this case the key and certificate belong to the OpenVPN server. The line beginning with 'server' ensures an IP address exists for the server – in this case it is 10.8.0.1. The lines

```
ifconfig-pool-persist ipp.txt 0
and
client-config-dir ccd
```

assure that, for all keys that are distributed to Players, there is a match of OpenVPN credentials with an IP address that is stated in files of subdirectory `ccd` and lines of file `ipp.txt`. More on this is given in the sections below that describe `ccd` and `ipp.txt`. The line beginning with 'local' contains an address that comes from the 'OpenVPN server location' text field of the CDX Control Panel. This file is used like this:

```
./sbin/openvpn server.conf
from the subdirectory server. Here is a sample server.conf file:

port 1194
proto tcp
dev tap
ca keys/ca.crt
```

```

cert keys/server.crt
key keys/server.key # This file should be kept secret
dh keys/dh2048.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt 0
client-config-dir ccd
route 10.8.0.0 255.255.255.0
client-to-client
keepalive 10 120
cipher AES-128-CBC # AES
comp-lzo
max-clients 100
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
log openvpn.log
verb 4
local localhost

```

ipp.txt:

This file is in the `server` subdirectory and is referenced in `server.conf`. Each line of this file pairs a key/certificate surname matched with an IP address. This file is created when invoking 'Make Keys' in the Configurator. The first few lines of an example `ipp.txt` file follow:

```

client0,10.8.0.50
client1,10.8.0.51
client2,10.8.0.52
client3,10.8.0.53
client4,10.8.0.54
client5,10.8.0.55
client6,10.8.0.56
client7,10.8.0.57

```

...

```
client49,10.8.0.99
```

Thus, for this example, key and certificate named `client5.key` and `client5.crt` belong to the Client that will live on IP address `10.8.0.55` in the contest.

clientXX:

These files are placed in subdirectory `server/ccd`. The XX in each is a number from 0 up to 199. They enforce the matching between key and contest IP address. These are created when 'Make Keys' is invoked in the Configurator. An example for file `client40` is the following:

```
ifconfig-push 10.8.0.90 255.255.255.0
```

run.server:

Runs `run.vpn`. Uncomment the two commented lines to kill `openvpn` processes that may be running before `run.vpn` is invoked. Contents of this script is:

```

#!/bin/sh
#sudo killall openvpn
#sleep 2
sudo nohup ./run.vpn
sleep 2

```

run.vpn:

This is called from `run.server`. Its lines are separated from `run.server` so that `stop.server` can be used effectively. The script runs the statically compiled `openvpn` in subdirectory `sbin` on `server.conf`. The process number of `openvpn` is saved in file `vpn.pid`, to be used by `stop.server` later. Contents of `run.vpn` are:

```
#!/bin/sh
./sbin/openvpn server.conf &
echo $! > vpn.pid
```

stop.server:

Kills the connection to the OpenVPN network. This script also terminates the connection to the proxy, if one is used. The CA will have to edit line 2 and replace 'visitor' with the username associated with the proxy, and uncomment the commented lines. If the local port is different from 8080 that number needs to be changed and in `server.conf`. This script looks like this:

```
#!/bin/sh
if [ -e vpn.pid ]; then
    sudo kill -9 `cat vpn.pid`
    rm -f vpn.pid
fi

rm -f nohup.out
rm -f *.log
```

sbin:

A directory the contents of which is only the statically compiled `openvpn`.

keys:

A directory containing the following server credential files:

- `ca.crt`: the certification authority certificate
- `server.crt`: the server certificate
- `server.key`: the server key
- `dh2048.pem`: the Diffie-Hellman parameters

These are referenced in `server.conf`.

Appendix J - Files and subdirectories of contest directory

The following descriptions do not include files that are part of the easyrsa package which share this directory with files and subdirectories for creating archives that are distributed to Players, an OpenVPN host, and a Contest Administrator.

players.db:

Contains current Player OS information, one OS per line. The following is a sample. Columns, from left to right, are Current Score, unused, IP address (the negative number is just the way the unsigned character number that is actually used is displayed in a text editor – e.g. 10.8.0.-40 is actually 10.8.0.216), email address of the Player, Player or Team name.

```
3843 0 10.8.0.-52 forth@forth.gmail.com Forthcoming - A
2717 0 10.8.0.-48 smashers@smasher.gmail.com Stack Smashers - A
2762 0 10.8.0.-40 sleepers@sleeper.gmail.com Sleepers - A
```

vpnKeyIds.txt:

Contains a list of directory names, taken from the players properties list of , so that directories may be manually created for the Player and Monitor packages. Below is an example:

```
Forthcoming_-_A
Stack_Smashers_-_A
Sleepers_-_A
```

game-id.txt:

Contains information that is saved by and for the key maker as shown in Figure 7. An example is shown below.

```
US
CA
Los Angeles
UCLA
Cyber Game Room
player@gmail.com
```

var, var1, var2:

The contents of game-id.txt, with edits, is sandwiched between var1 and var2 to produce var which is used by easy-rsa to locate openssl and the openssl-easyrsa configuration file as well as set up parameters for certificates including expiration dates. Editable parameters include the following (defaults are preceded with #):

```
#set_var EASYRSA "${0%/*}"
set_var EASYRSA_OPENSSL "./bin/openssl"
set_var EASYRSA_PKI "$PWD/keys"
set_var EASYRSA_DN "org"
set_var EASY_REQ_COUNTRY "US"
set_var EASY_REQ_PROVINCE "OH"
set_var EASY_REQ_CITY "Cincinnati"
set_var EASY_REQ_ORG "University of Cincinnati"
set_var EASY_REQ_EMAIL "franco@gauss.eecs.uc.edu"
set_var EASY_REQ_OU "Dept. Electrical Eng. and Computer Sci."
set_var EASYRSA_ALGO rsa
#set_var EASYRSA_CURVE secp384r1
set_var EASYRSA_CA_EXPIRE 365
set_var EASYRSA_CERT_EXPIRE 365
#set_var EASYRSA_CERT_RENEW 30
```



```
#set_var EASYRSA_CRL_DAYS 180
set_var EASYRSA_NS_SUPPORT "no"
#set_var EASYRSA_SSL_CONF "$EASYRSA/openssl-easyrsa.cnf"
#set_var EASYRSA_DIGEST "sha256"
#set_var EASYRSA_EXT_DIR "$EASYRSA/x509-types"
```

openssl-easyrsa.cnf:

The configuration file for openssl that is used by easyrsa to establish certification authority locations, names, expiration dates etc., policy, request handling, Distinguished Name handling, and extension handling. This does not need to be edited.

make-keys:

Script that is invoked by 'Make Keys' in the Configurator to make and place OpenVPN credentials. The script easyrsa in the same directory is used to initialize the pki, make Certificate Authority key and certificate, make OpenVPN server key and certificate, and make keys and certificates for Players. The script workaround in the same directory is created and used to simplify a part of the latter operation.

bin:

A directory that contains statically compiled software for mailing archives, openssl, and archiving sets of files as follows:

- tar: archives files in subdirectory client for use by Players and subdirectory server for the OpenVPN server
- mutt: mails the archives – must be used on a machine that legitimately supports mail transfer
- openssl: for creating OpenVPN keys and certificates
- mailit: the script that assembles and executed the command to mail tar files
- cdir_no: the script that creates Player archives in case OpenVPN is not used
- cdir_vpn: the script that creates Player archives in case OpenVPN is used

sbin:

Contains only the openvpn executable.

keys:

The directory in which OpenVPN keys, certificates, revocations, requests, etc. are placed, in some cases for distribution. See Section OpenVPN Key & Certificate Maker for a description of the keys and certificates that are made by 'Make Keys' of the Configurator.

examples:

A directory that contains examples of some of the files that get distributed or are used to create files for distribution including players.db, Parameters.txt, vpnKeyIds.txt, game-id.txt, and Params.

client:

A directory that contains files and templates that are customized for Players and distributed to Players as a set of files that are archived. See Appendix H - Structure of Files in Player Directories for a description of these files and directories.

server:

A directory that contains files and directories that are customized for the OpenVPN server if OpenVPN is used. These files and directories are archived as tar files. See Appendix I - Files in Parameters and VPNServer directories for a description of those files and directories.