Western Regional Collegiate Cyber Defense Competition – 2019

Hosted by Coastline College in conjunction with:

Raytheon

workday. Disney

FIREEYE™

Bank of America

paloalto NETWORKS

ISACA Los Angeles Chapter

AIR FORCE CIVILIAN SERVICE

OWASP Open Web Application Security Project

Documentation for Competitors:

Welcome to the 2019 WRCCDC Finals! Congratulations of making it to this round and competing for a spot in the National CCDC to be held in April.

The following documentation is provided to you as a scenario for the purpose of selecting the very best team to move forward. Provided to you in this document you will find a topology of your environment, username and password information, phone system information, and additional hints, and tips.

Scenario:

Overdrive Dinosaur Systems (ODS for short) is a bioengineering startup company whose original focus was the restoration of long extinct animals in hopes of recovering extinct species for preservation and eventual restoration of these species. While originally founded as a preservation society there was great interest in the potential profitability of cloning. Following a scientific breakthrough in cloning technology, the company received an influx of funding and is now launching as majority stakeholder Triassic Land (park.ods.com), a wholly owned subsidiary. Since then, ODS has split the scientific research and business needs into separate holdings - HBC and ODS. The holding company is now focused on opening a park for customers to visit and pet the new dinosaurs. Moving forward, ODS is eyeing new ventures such as the Pleistocene Zone, an ice age themed park. You will be taking over from the system integration team "Black Team".

In more recent news, rival company Next Gen Dinos has purchased a nearby island and is planning on opening their own amusement park within the next 12 months. Given their newfound success, Triassic Land is concerned that some trade secrets, or worse, scientific research, has been stolen. Security experts have been called in to assist in securing the holding and all subsidiaries from further corporate espionage.

Location

Overdrive Dinosaur Systems Research Facility

Once a naval health research center located in Point Loma California - Today, ODS research facility houses thousands of contractors and employees in an approximately 100,000 sqft state of the art facility. Historically, the Naval Medical Research Center (NMRC) focused research funding on infectious diseases, military medicine, battlefield medicine, and bone marrow research. Due to unknown and classified reasons, the health research center was decommissioned and moved to unknown location. Overdrive Dinosaur Systems, after receiving an influx of funding and wanting to continue preservation efforts, seized the opportunity and requested occupancy of the research facility. Federal government approved the occupancy and construction began in late 1990s.

Bldg. KPg-KT, Ryne Rd

San Diego, CA 92152

Opens 7am - 5pm Mon - Fri

Closed Saturday and Sunday

Phone Number: 10*

Triassic Land

Archaeological evidence suggests that Mullet Island in SoCal has been occupied by humans for thousands of years. Not until recent scientific breakthroughs, there has been strong evidence to suggest a total eradication of life on the island due to an epidemic of rampant deformities, decomposition and decay, genetic mutations, and violent sub-human and primal animal aggressive behaviors due to an unknown microorganism strain. The island ultimately seized to house life and was left uninhabited for hundreds of years.

Once wasted and barren, the island started cultivating on it's own and vegetation was plentiful. As civilization thrived on the mainland, Mullet Island was left uninhabited, untouched, and perfect real estate for Overdrive's Dinosaur Systems's mission - Triassic Land. Surrounded by the Salton Sea, Warmed by the San Andreas fault line, and consistent weather patterns, Mullet Island was purchased by ODS where construction started soon after during the mid 2000s. Today, the island houses hundreds of species and is a thriving ecosystem of rare and exotic plants, organisms, protozoa, and other forms of life.

Island Coordinates

33.2253° N, 115.6080° W

Imminent Threat:

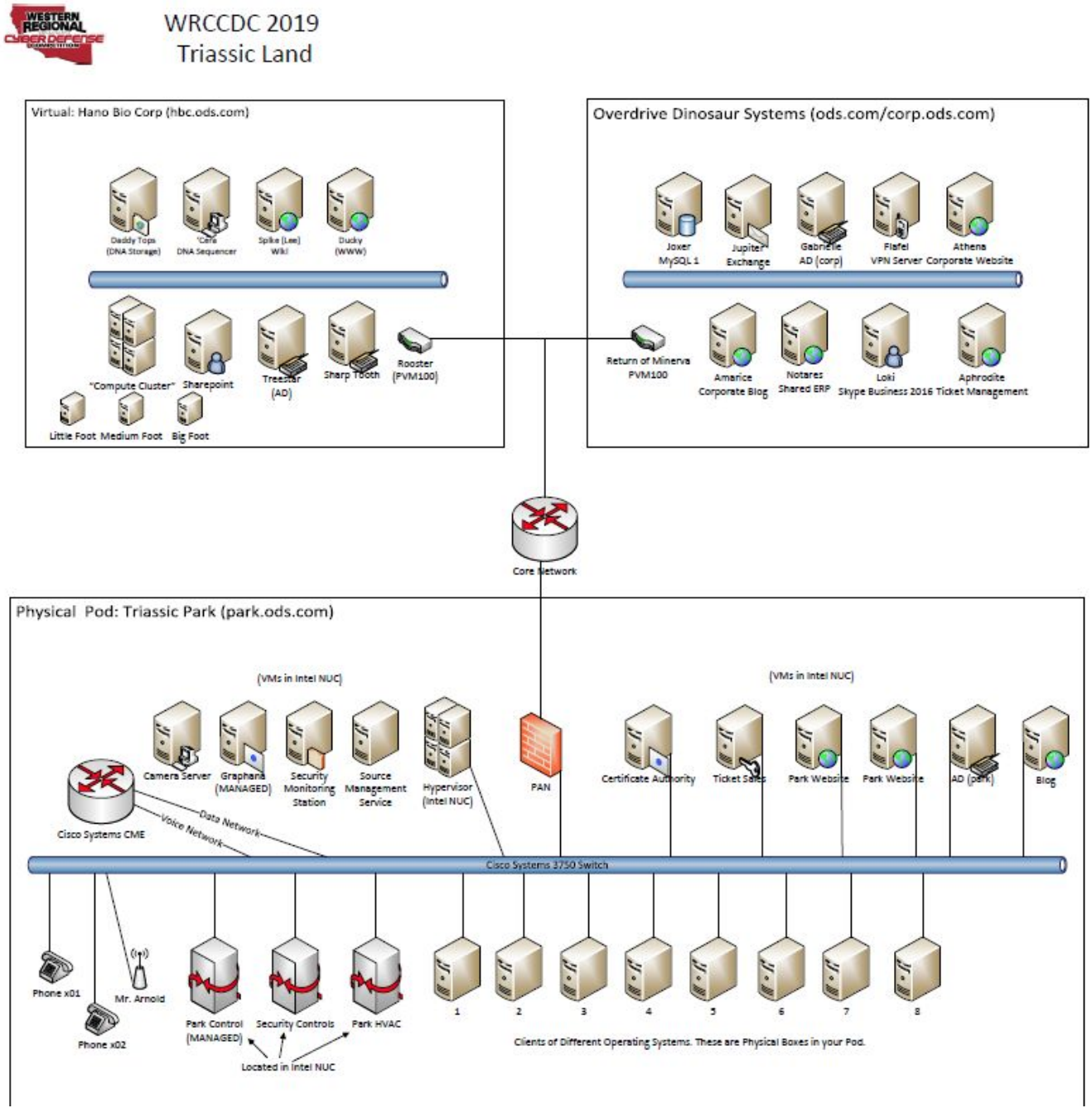
An organization calling itself REDPEACE (A.K.A. the RED TEAM) is an Environmental Terrorist Organization that is bent on disrupting operations of these organizations (Overdrive Dinosaur Systems, HBC, and Triassic Land) individually and as a whole. This opposing force (OPFOR) is an international environmental and animal rights organization that sees these groups as exploiting the animals they have created. Their ultimate goal is to find information that proves cruelty to the animals and in light, if none exists, plant it there for maximum hacktivist exposure to the media (Social and Mainstream!).

Additionally, we have recent intelligence that they may be at cause for the demise of your predecessors. This has come through the advent of recent

attacks on our control systems that have disabled fences, gates, and other vital equipment used for the operation of the park.

The integration team had their hands full bringing up a full amusement park so they setup required systems as quickly and cheaply as possible. They had their strengths but ultimately did not do a very good job at managing these complicated environments and thus may have paid the ultimate price for their lack of skill and knowledge especially in Cyber Security, and IT operations.

The general topology that we have garnered from their limited records is as follows:



Technical Info:

General users (superusers) are any one of the following unless otherwise noted:

root

admin

Administrator

Domain: triassicland.com

Administrator Password: WelcomeToTriassicLand
Administrator Password (with Complexity): WelcomeToTriassicLand1
Domain: triassicland.com
Public IP Range: 10.59.TEAM#.0/24
Private IP Range: 192.168.220.0/24

Infrastructure Equipment: (Cisco Switch, CME)
Telnet Password: cisco
Enable Password: cisco

We recently introduced a wireless router and camera. The IT staff was working on this when they met their unfortunate end. We are combing through our records to obtain those passwords.

Domain: hbc.com

Administrator Password: TheLandBeforeTime (Includes PAN)
Domain: hbc.com
Public IP Range: 10.58.TEAM#.0/24
Private IP Range: 172.20.0.0/24

Domain: corp.ods.com

Administrator Password: Ov3rDrive!
Domain: corp.ods.com
Public IP Range: 10.57.TEAM#.0/24
Private IP Range: 172.16.0.0/24

vCenter Username: Team0#@wrccdc.org (Team01, Team02, etc)

vCenter Password: WelcomeToHyperV + Team # (WelcometoHyperV01, WelcometoHyperV02, etc)

Orange Team

A Note on Corporate Staff (A.K.A. The Orange Team)

You will find, I am sure, many accounts and records pertaining to staff from all three organizations. These accounts must be maintained as they will be interacting with you throughout your tenure. These staff members range from simple park staff to corporate titans that sign your paycheck! (O.K. out of context, NO ONE IS GETTING PAID THIS WEEKEND!!!!)

(BACK IN CONTEXT)

You will be asked to support them and provide your expertise when needed. This may include but not be limited to documentation on the systems, consultation on its improvement, and interaction with staff in their support.

Staff may contact you via phone, email, or blog post so pay attention to them.

Control Systems:

We have a few systems that are incorporated into the park for monitoring key systems. These systems have dashboards and are located on the following systems:

10.57.TEAM#.36 and 10.57.TEAM#.46

Their passwords are: UnifiedSystems

They are maintained by Unified Systems Inc. for operational purposes, but you are in charge of their access and general security.

Please allow data.wrccdc.org, data2.wrccdc.org, and data3.wrccdc.org in and out of your firewall.

Competition Services

In your pod (company) you have functional email, corporate chat, ticket management, ERP solution(s), and other services that will be used by both Orange Team, Black Team, and possibly others. Your services are also configured to use these systems and you may be asked to configure other services to use resources.

If you have issues during competition please contact Black Team Via:

Please try to open tickets via https://tickets.wrccdc.org/

Username: teamXX
Password: EverybodyDoTheDinosaur

However if you have issues, please contact us at

Phone Numbers:

Each IT Team (Blue Team) will have two phones and a phone system in their room. Your phone numbers are:

X01 & X02

where X = your team number. So, Team 1 would be 101 and 102.

Teams can't call one another but 411 service does work as does its alternate 412. This will reach the Black Team.

The white team can be reached at 911

Other calls may come in from our staff. We do not have their phone numbers at this time.

It is critical that you keep your phone system up. If it goes down. There will be someone from security (White Team) co-located with you. They will have backup communications to reach operations and management (Black Team and White Team respectfully).

On a lighter note, we may want you to look at a voicemail solution since we do not have one in place at this time. But more on that later.

Welcome to Triassic Land!

J Hammond

Founder & CEO