LOCKDOWN v0

TEAM PACKET

APRIL 9, 2016

201A CAPEN HALL

UNIVERSITY AT BUFFALO

University at Buffalo
The State University of New York

Sponsors

Supporter

University at Buffalo
The State University of New York

Making our planet more productive℠

Lunch

Competition Scenario

You and your team have been hired to take over the IT and Security operations for the Office of Blue Team Management (OBM), a federal government agency manages Blue Team hiring and granting clearances. Previously, the Office of Blue Team Management IT and Security Operations was managed by a team of 9 people - Malcolm, Zoe, Wash, Inara, Jayne, Kaylee, Simon, River, and Derrial. Recently the Director of OBM, Dave Murray, along with CIO Kevin Cleary, launched an investigation to figure out what the IT and Security Operations team were really doing. Upon inspection, the Director and CIO noticed that the team goofing off on Reddit and Facebook all day. As a result of these findings, the original IT and Security Operations team was fired - and in their place comes you and your team.

As the new IT and Security Operations team for the Office of Blue Team Management, you have been tasked with multiple objectives:

1. Follow IT and Information Security best practices to harden the company's IT infrastructure from potential threats.

2. Ensure the company's network services (described in this document) are running at all times.

3. Complete several tasks, or injects, assigned by the Director or CIO to get the company back on track.

4. Effectively manage your departmental budget to ensure the IT and Security Operations department helps meet the strategic goals of the company.

Letter from the CIO

From: Kevin Cleary, CIO
To: IT and Security Operations Team

Hi Team,

First of all, I want to welcome you and your team to the Office of Blue Team Management! I personally look forward to working with all of you tomorrow. As you probably heard, our previous IT and Security Operations Team neglected their duties, which resulted in a poorly setup and managed infrastructure. Apparently, they did not follow current best security practices either. To make matters worse, we heard rumors about one of the former employees giving out credentials. A few hours later we started seeing spikes of traffic from China, Russia, and North Korea, so I decided to shut down all the servers which you can deal with tomorrow.

I know it sounds like a headache, but don't worry! I'm confident that I hired the best team money can buy.

See you tomorrow,
Kevin Cleary
Chief Information Officer
Office of Blue Team Management

Letter from the Director

From: Dave Murray, Director
To: IT and Security Operations Team

Hello Team,

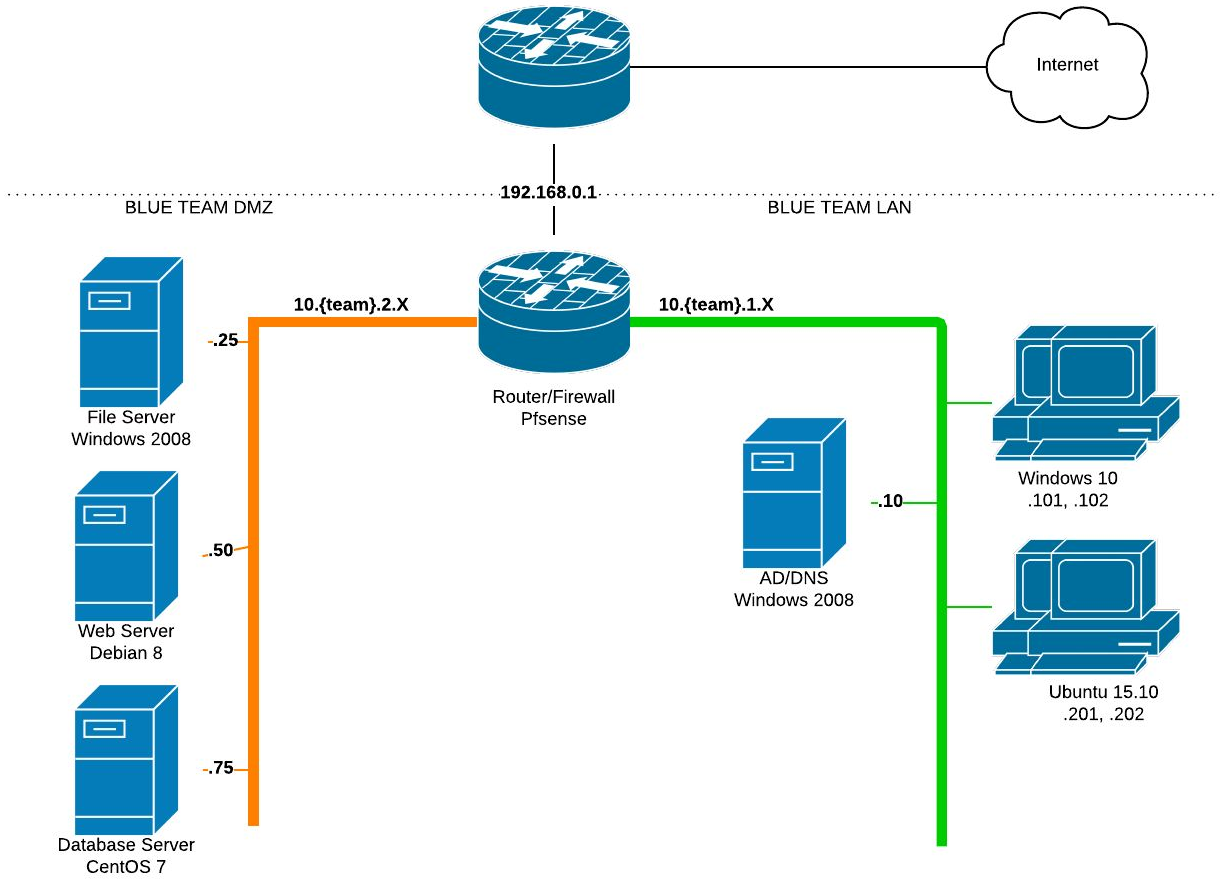
Welcome to the Office of Blue Team Management! I'm sure CIO Kevin has already sent you a welcome letter so I'm going to keep this communication brief and to the point. The management of your departmental budget and strategic expenditures of those funds are critical to the success of your team.

Of particular relevance, you should be aware that the previous IT and Security Operations Team entered into a long-term contract to lease the publicly accessible servers, and your team is responsible for paying $25,000 every hour. Unfortunately, if this amount is not paid, **the servers will be shutdown until you budget and pay for the hourly lease**. You will be able to pay for this through your departmental budget, which will continue to replenish as long as critical services remain online and accessible. Failure to keep those critical services online will decrease the budget you have available to spend on server leasing and other items.

I trust you will manage your departmental finances accordingly.

Dave Murray
Director
Office of Blue Team Management

Network Topology



Network Topology

Team Infrastructure

IP Address	Operating System	Purpose	Scored Services
10.X.{1,2}.1	pfSense	Router	
10.X.1.10	Windows 2008	Active Directory	AD, DNS
10.X.1.101	Windows 10	Client Machine	ICMP
10.X.1.102	Windows 10	Client Machine	ICMP
10.X.1.201	Ubuntu 15.10	Client Machine	ICMP
10.X.1.202	Ubuntu 15.10	Client Machine	ICMP
10.X.2.25	Windows 2008	File Server	FTP
10.X.2.50	Debian 8	Web Server	HTTP
10.X.2.75	CentOS 7	Database Server	MySQL

X = Your Team Number

White Team Infrastructure (Internal)

IP Address	DNS Name	Purpose
192.168.1.50	whiteteam.open	InjectEngine
192.168.1.51	bank.open	Bank Server
192.168.1.100	dns.whiteteam.open	Central DNS Server

White Team Infrastructure (External)

DNS Name	Purpose
bank.ubnetdef.org	Bank Server
scoring.ubnetdef.org	InjectEngine

Team Identification

Blue Team

This team refers to you and your coworkers. Your tasks include the objectives as outlined in the competition brief, or more simply – securing your network/computers, completing business tasks in a timely and professional fashion, and having fun! You must have a team captain who is directly accountable to the Director and acts in a leadership capacity within the team.

White Team

This team will be your direct points of contact between yourselves and the Director of the company. They will disseminate business tasks/injects to you at the Director's request, give you feedback on your work, answer any questions you have (to the best of their ability), and handle the overall competition scoring and organization.

Red Team

The red team is comprised of both professional and hobbyist penetration testers. They have volunteered their time to be your main adversary. Their goal is to assess and exploit the configuration of blue team networks, and also to capture specific data items and files on the targeted devices of each blue team. A main aim of the red team is to simulate situations which might be encountered "in the wild" to the best of their ability based on the limits of the competition environment.

Black Team

The black team is in charge of the underlying competition infrastructure. They setup all of the virtual machines used in the competition, documented the configuration settings, tuned the scoring engine, ensured the competition network was functioning properly, and tested the environment. They are in constant contact with the white team throughout the competition to coordinate with injects, answer blue team questions, and to promote overall stability of the competition environment.

Budget Information

Overview

You and your team will be responsible for maintaining your department's budget. Currently, **for every check you pass, your department will receive $100**. This amounts to a possible $600 every minute, and eventually $36,000 per hour. Your department will initially have a budget of **$80,000**.

Hourly Lease Information

Every hour, on the hour, your team is required to pay **$25,000** for your leased servers. Should you fail to pay this, all machines on your 10.X.2.0 network (DMZ) will be automatically powered down. To power on your machines, simply pay the power bill for the current hour. However, you will still be responsible for the next hour's power bill as well.

Possible Fines

You and your team can be assessed various fines throughout the competition.

- **$5,000**: Service Level Agreement (SLA) violation
  - ↳ Applied when a single machine is down for an entire half hour.
- **$5,000**: Insubordination
  - ↳ Applied every time 5 injects are not completed.
- **$7,500**: Cash Stolen Insurance Deductible
  - ↳ Applied when money is stolen from the your team's budget. Amount stolen, minus the deductible is returned.

Services Purchasable

You and your team can also purchase various services throughout the competition. A complete (and up to date) list will be found on the Bank Website.

- **$2,500**: KVM Console access to a server
- **$5,000**: White Team help on an inject
- **$7,500**: White Team assistance on fixing a VM
- **$10,000**: Revert a machine back to a pre-competition snapshot
- **$15,000**: Red Team advice on securing a box
- **$25,000**: Red Team immunity for 15 minutes

Competition Rules and Guidelines

Code of Conduct

1. All participants (competitors, organizers, volunteers) are expected to behave professionally at all times throughout the duration of the competition. This means to treat others with dignity and respect, and to foster an open and welcoming environment for all involved. Anyone found to be violating this stipulation will be penalized at the discretion of the competition organizers.

2. **All network traffic during the competition is being captured and logged. Do not enter any personal credentials unless you are comfortable with sharing it with the world.**

3. All university and local/state/federal government rules apply and ultimately supersede the regulations listed.

4. No alcohol or substance use will be tolerated, including smoking (the University at Buffalo is a smoke-free campus).

5. You are free to come and go from the competition room as you please so long as it is not for outside assistance regarding competition matters. What happens in the competition room stays in the competition room (until the event is over, then by all means talk about and review whatever you wish!)

Scoring

1. Service Uptime: **40%** of blue team scores will be determined by the uptime of various services within their network and configuration of new services and system, via inject request. These services include **HTTP, MySQL, DNS, FTP, Ping, and AD**. Teams will all have access to a scoreboard, which will show which services are currently “up” (meaning reachable and usable) and which are “down” (unreachable and/or unusable). Scoring engine checks occur in a synchronous fashion – each service will be checked once every 60 seconds. Misconfigurations and not following best practices will mostly likely result in loss of point. This is determined based on Red Team gaining access.

2. Injects: **40%** of blue team scores will be determined by the successful and quality completion of the tasks they are given by the white team throughout the competition. Completeness counts, as does quality. **It is expected that any injects that are written will be typed in a professional and report/documentation format.** Anything you submit inject-wise should be something that you would feel comfortable submitting to your boss at work.

3. Incident Reports: **20%** of blue team’s will be determined by the successful and quality reporting of any incidents that occurred during the competition. It is expected that any incident reports written will be typed in a professional and report/documentation format. The same rules apply that apply to Injects apply to Incident Reports .

Infrastructure

1. The University at Buffalo owns all infrastructure – this includes hardware, software, the hypervisor/VM's, etc. Treat it with respect and take due care to not cause any damage outside the scope of the competition.

2. You are not authorized to revert any VM's to a previous snapshot or template, or create your own snapshots or templates. Doing so will result in a significant team penalty. You may purchase this service from the white team during the competition, however. The white team purchase will inform you of any penalties to your budget at the time of the request.

3. **All software used by blue teams in the competition must be free and open source (FOSS) and publically available to anyone. No personal use or commercial trial software will be allowed.**

4. There is to be no "pre-staging" of scripts or software prior to the start of the competition (i.e. creating a .zip archive and hiding it on Dropbox). All scripts and software must be publically available and free for any competitor. The exceptions to this rule are scripts that are written during the competition inside of virtual machines and scripts written on paper.

5. You may not touch another team's infrastructure (either physical or virtual). Doing so will result in immediate disqualification for your team. If it isn't your team's –**don't touch it!**

6. There is no attacking in this competition, but certain injects may have you using tools such as nmap. You must only use these tools on your own team's network. Any activity that could be construed as reconnaissance or attacking against another team, the University, or an outside entity will result in immediate disqualification for your team.

7. You are allowed to collaborate with teams participating in the competition. Reason being, most industry professionals need to do this to be successful. Teams will still be individual scored even when a joint effort is made.

8. **You may NOT block entire subnet ranges in your Firewall Rules – you can only block specific IP addresses and you must have proof that they are malicious if you do so.**

Reference Material

1. You will have access to Internet on your host machines during the competition to use for looking up reference material. You may only use free and publically available resources (i.e. no paid support forums).

2. On the subject of Internet on your host machines – you may not use the host machine Internet for anything unrelated to the competition. This means no Facebook, Reddit, Twitter, etc. (unless specifically allowed by the white team for the purpose of an inject).

3. Any and all paper-based reference materials (cheat sheets, books, printed PDF's, etc.) are allowed and encouraged. You may also write scripts beforehand and print them on paper to bring with you.

4. No electronic media will be allowed in the competition, namely USB drives, external hard drives, CD's/DVD's/BD's etc.