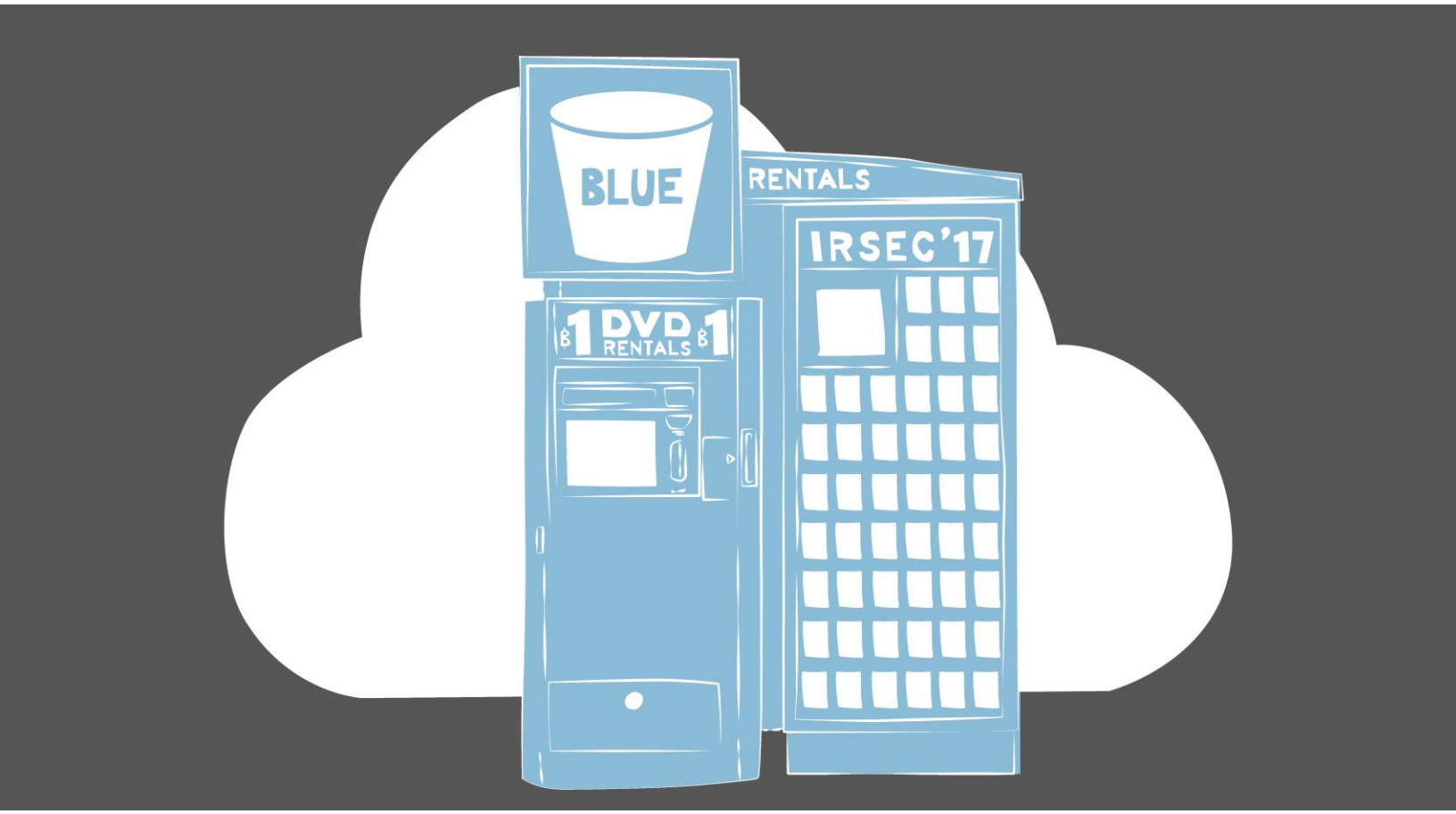
RIT COMPETITIVE CYBERSECURITY CLUB



Blue Team Packet 1.0

Dear Sponsors,

RIT Competitive Cybersecurity Club would like to extend our sincerest appreciation to you, without whom our events would not be possible.

We are extremely grateful for your support in making our annual 3rd^{h} Incident Response Security Competition possible!

Thank you,

Everyone at RC3

Ben Bornholm, President

Nick Piazza, Vice President

Sean Sun, Competition Architect

Brad Campbell, Technical Lead

Michael Milkovich, Treasurer

Ohan Fillbach, Website Administrator

Kristen Tumacder, Secretary

Platinum

Gold

Silver

Computer Science House

Bronze

qocreate

covermymeds®

R·I·T

B. Thomas Golisano College of Computing and Information Sciences

R·I·T

Computing Security

A Word from BlueBucket's CEO

Dear magical security unicorns,

BlueBucket passed many milestones in 2016; by year-end we had served more than 1.5 million customers, yielding 838% revenue growth to $147.8 million, and extended our market leadership despite aggressive competitive entry.

But this is Day 1 for cable cutters and, if we execute well, for BlueBucket.irsec. Today, online media rental saves customers money and precious time. Tomorrow, through personalization, online media rental will accelerate the very process of discovery.

BlueBucket.irsec uses the World Wide Web to create real value for its customers and, by doing so, hopes to create an enduring franchise, even in established and large markets.

It's All About the Long Term

We believe that a fundamental measure of our success will be the shareholder value we create over the long term. This value will be a direct result of our ability to extend and scale our current market leadership. We have invested and will continue to invest aggressively to expand and leverage our customer base, brand, and infrastructure as we move to establish an enduring franchise.

Because of our emphasis on the long term, we may make decisions and weight tradeoffs differently than some companies. We want to share with you our fundamental management and decision-making approach so that you, our newly hired security team, may work with us on making sure BlueBucket will last lifetimes.

- We will continue to focus relentlessly on our customers.
- We will continue to focus on the ability to scale and maintain stability.
- We will continue to make decisions only when all the information has been presented and analyzed.
- We have moved towards using new and exciting technologies like the cloud.
- We expect a constant communication with you to maintain transparency throughout departments.

May Ben be with you,

J-Money, CEO

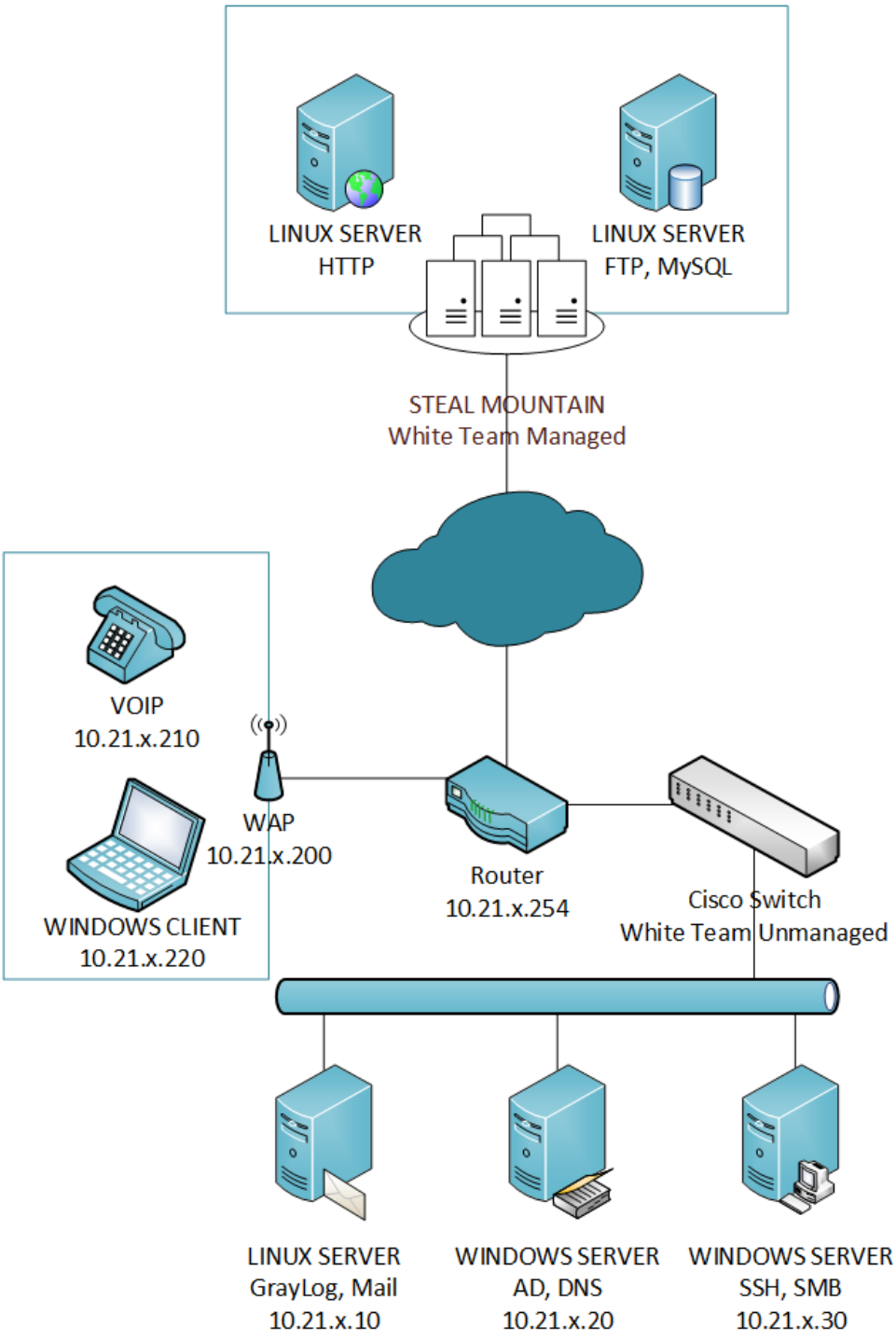
Company Policy

Please read and follow these rules when doing work for BlueBucket. We take this incredibly seriously, and failure to follow these rules will result in termination.

- This is a defense only competition. There will be **no** attacking by any blue team under any circumstance. The red team are the only ones who will be performing attacks.
- Attacking White Team infrastructure will result in a **severe** deduction in points **or elimination** from the competition.
- Attacking Blue Team infrastructure will result in **immediate elimination.**
- All devices should be pingable at all times. This means no disabling your NIC.
- You cannot block entire subnets or ranges of IP addresses, but you may block individual IP addresses. Expect severe point deductions if we find out you've been blocking subnets.
- Entering the Red Team room is prohibited.
- Food is to be eaten in the designated rooms only. No food will be allowed in the labs.
- You are allowed to use pre-staged scripts; however they must be downloaded from the internet, as external storage devices will **not** be allowed.
- You are allowed to use printed aids, and we encourage it.
- Do not log into personal accounts on any competition machine; you've been warned.
- Physical host machines (excluding laptops) are not in scope of attack for Red Team.
- You can trust Red Team members when you see them in person (ie when they come into the blue team area: sys lab). When communicating with Red Team members via phones or some other way, you should not assume they can be trusted.
- Learn something new.
- Have fun.

Lay of the Land

When BlueBucket was just a startup, there wasn't too much emphasis on documentation. This is the topology we have currently recorded.



Critical Services

BlueBucket's core functionality relies on the following services.

IMAP4

Host: 10.21.x.10
Employees must be able to log into their mailbox and be able to retrieve mail from our customers.

Active Directory (AD)

Host: 10.21.x.20
Employees must be able to authenticate to the domain from any client and server.

DNS

Hosts: 10.21.x.20
Our DNS servers must be able to resolve forward and reverse queries.

SMB

Host: 10.21.x.30
Employees should be able to access their files and back them up to the server.

SSH

Host: 10.21.x.30 / Cloud Service, unknown IP
Employees must be able to log in and access their local and cloud workspaces.

HTTP

Host: Cloud Service, unknown IP
Customers must be able to visit and use this site. It should be in working order so that they may order movie rentals.

FTP

Host: Cloud Service, unknown IP
Employees must be able to log in as well as upload and download a file.

MYSQL

Host: Cloud Service, unknown IP
A MySQL user should be able to log in remotely and select database entries. The webshop should be able to talk to the database and make changes as necessary.

Measuring Success

At BlueBucket, we are obsessed with metrics. To evaluate our ability to operate, we perform health checks and use a point system to measure our success.

Critical Service Uptime

Responsible for **60%** of your score. Maintaining 100% uptime is the key to success,

Injects

Responsible for **40%** of your score. These injects will be evaluated by our team to determine the amount of points for a given inject. All injects have a maximum amount of points attainable. However, for each inject you are able to attain less than the maximum number of points if the inject is attempted, but not done fully.

In addition, if your team chooses not to or are unable to complete an inject in the allotted time, your team is able to explain the inability or decision not to complete the inject in an email to the CEO. If this is done in a **professional** manner and sent **before** the allotted time is up, your CEO may be inclined to award you a small percentage of points for the inject. Also, it is possible to extend the due date of an inject (see Budget).

Point Deductions

SLA (Service Level Agreement) Violations - After 6 consecutive missed checks, a point deduction will happen. If there are more than 6 consecutive checks missed, each time the 6th consecutive check is missed, there will be a large point deduction.

Hacker activity - Upon successful breaches/attacks on our infrastructure, there will be some point deductions. However, prompt incident response reports can decrease the amount of the point deduction for any given attack up to 65%.

System Resets - If a laptop, router or other non-virtual device becomes completely unusable/unbootable for any reason other than hardware and/or white team failure, the only way for you to reset it back to its initial conditions is by paying for it with a point deduction; The deduction will be 5% of your score at the current time.

Incident Response Reports

We strongly encourage heavy monitoring of our systems. Please submit incident reports for each hacker incident you detect. Do **not** submit a report that covers numerous incidents and breaches; each report should focus on a specific, individual successful attack against your team.

Incident reports can be completed as needed throughout the competition and submitted to our inject/IR report submission portal. **All** incident reports must include your team name and number in it—without this info the report will **not** receive any recognition.

Incident reports must contain a description of what occurred, how the red team was able to get in, a discussion of what was affected, and a remediation plan. A thorough incident report that correctly identifies a successful attack may reduce the hacker penalty for that event by up to 65 percent. The more complete and accurate your report is, the better it will be scored, but there will be partial credit awarded if the report meets enough criteria. Submitting an incident report without all of the relevant data is better than not submitting a report at all, but if the report is missing too much information it will not receive any credit.

Screenshots may be submitted for evidence of the incident but are **not** required. Below are items you should strongly consider including to receive maximum credit for your reports:

- Attacker IP address(es)
- Timelines of activity
- Level of access obtained by attacker
- IP address and/or hostnames of affected machines
- How the attacker gain accessed
- Steps to remediate the incident
- Description of attacker activity (ie passwords cracked, files affected, services affected, data lost or defaced, etc.)

To aid your reports, we have set up GrayLog on one of the Linux servers to monitor events and the environment. Please use this to your advantage. Remember, while screenshots are suggested and not required, usage of easy to understand graphs and images will allow non-technical management to understand all the data presented to them and will aid in good decision making.

Budget

We have created a financial plan for our security team. We understand security, at times, can be a cost, so feel free to use the allocated daily budget of **10,000 coins** at your leisure. With a constant stream of revenue from our hit movies, we have also allocated some overflow from our profit for you. This should be good incentive to make sure our website never goes down. The currency we accept at BlueBucket is a popular cryptocurrency that we believe has long term stability and real intrinsic value.

You may only access this wallet on your client laptop, so please make sure it stays secure.

Approved Items

Below is a list of items approved for purchase. If you would like to purchase an item, simply transfer the number of coins needed to the white team wallet/account with the name or description of the item you'd like to buy in the comment/notes of the transfer.

Reset any server to initial company-approved snapshot

Cost: 5,000 coins
You may reset any VM to a snapshot of its initial state from the start of the competition. This can be purchased any number of times for any of the VMs so long you have enough money to purchase the reset.

Hire a consultant

Cost: 2,000 coins/10 minutes
Hire a company-approved consultant to offer advice on your issue at hand. Please include in the service and operating system you are having an issue with so we may find you the most fitting consultant. Please have specific questions ready, we can only book them for a maximum of a half hour at a time. They can also only be booked once an hour.

Extend time/due date of inject

Cost: 500 coins/10 minutes
Time is money. When we ask for an important task to be completed, we expect it by the due date, but we understand if there are other more pressing matters at hand. Since we use time as a measure of success and in calculating company value, you will

have to transfer part of your budget in order to compensate for the lack of on-time completion.

Consult the help of an auditor

Cost: 500 coins
Your choice of an auditor (from our pentesters or sponsors) can give suggestions and advice only but not actually put hands on keyboards. Auditor can only give help for one server, one service or one specific area per consultation. Red team will occasionally come out and tell a team that they have breached them and how they did it, but they won't offer any solutions to the problem. To receive advice may provide an actual solution, you can buy this.

Note

While that is our list of generally approved items of purchase, we understand that some other transactions will have to be made throughout your time working at BlueBucket as that is simply the nature of this field of work. Please do not feel reluctant to have to spend money if you have to.

Company Presence

As an up and coming institution, we are always under public scrutiny. In order to maintain a healthy company image, we have created a Twitter account to promote BlueBucket. We aim to reach 1mil followers by the end of the 4th quarter, and we aim to do this by keeping the feed as live as possible.

Please keep our social media clean and professional, or you will be brought under scrutiny by our board of directors.