RC3

RIT COMPETITIVE CYBERSECURITY CLUB

BENRON

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 4th annual Incident Response Security Competition possible!

Thank you,
Everyone at RC3
Sean Sun, President
Ohan Fillbach, Vice President
Kristen Kate Tumacder, Competition Architect
Shannon McHale, Treasurer
Susan Lunn, Operations Lead
Bryson McIver, Web Admin
Joel Margolis, Tech Lead
Sean Newman, Secretary
Zach Jorgensen, Junior Operations Lead
Simon Buchheit, Junior Tech Lead

PLATINUM

GRIMM INGRESSIVE IOMAXIS

GOLD

facebook hackerone Wegmans

EDUCATIONAL SUPPORTERS

Malshare Trello

TOP SECRET INFORMATION AHEAD
FOR BLUE TEAM MEMBERS ONLY

To: The aBENgers

From: Ben Jamin

THE

aBENGERS

YOUR SECRET MISSION

Hello Security Superheroes.

My name is Ben Jamin, the CEO of Benron Corporation. My company creates perfect sandwiches, from PB&J to BLT. It is with great pride for me to say that my company has the best roast beef sandwich in the entire world. I have tasted other hot roast beef sandwiches across the globe and have spent years perfecting the recipe. Finally, a few years ago, I put it on the menu as Ben's Favorite, and it became an instant hit: everyone, from children to elders, loves my sandwich.

As my company rose in fame, we needed to hire more people to make sandwiches and to protect the ways of sandwich-making.

As I was coming to work this morning (yes, I work on Saturdays), the staff who arrived before me immediately told me that the safe and database that hold the secret recipes have been opened and the recipes have been stolen! I believe that this is the work of Bad-Ron, my arch nemesis. I have hired you, security superheroes from the company The aBENgers to help me with this breach. Your task is to find evidence of the breach, protect my company and kick them out of our systems.

May the beef be with you,
Ben Jamin, CEO

COMPANY POLICY

Please read and follow these rules when doing work for Benron. 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 (Air Gap) 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 SysLab or NetLab). When communicating with Red Team members via phones or some other way, you should not assume they can be trusted.
- Have fun!
- Learn something new!

SCHEDULE - SATURDAY, APRIL 21, 2018

Time **Details**

8 a.m. - 8:40 a.m. **Breakfast**

- Location: Gosnell 3305 (tentative)
- RC3 will provide doughnuts, muffins, coffee, and hot chocolate to sponsors and competition participants. Please arrive as early as possible to set up your table and mingle with participants.

8:40 a.m. - 9 a.m. **Rules and Guidelines Explained**

- Location: Gosnell 3305 (tentative)
- Quickly review how the competition will progress throughout the day and review Blue Team rules of engagement.

9 a.m. - 12 p.m. **Competition Time**

- Location: Golisano Sys Lab and Net Lab
- Competition begins at 9 a.m. and pauses at 12 p.m. for lunch

12 p.m. - 1 p.m. **Lunch**

- Location: Gosnell 3305 (tentative)
- The competition is paused and all Red Team activities stop. RC3 will provide lunch and various drinks.

1 p.m. - 6 p.m. **Competition Resumes**

- Location: Golisano Sys Lab and Net Lab
- The competition resumes again and Red Team shenanigans continue.

5 p.m. - 6 p.m. **Hour of IR**

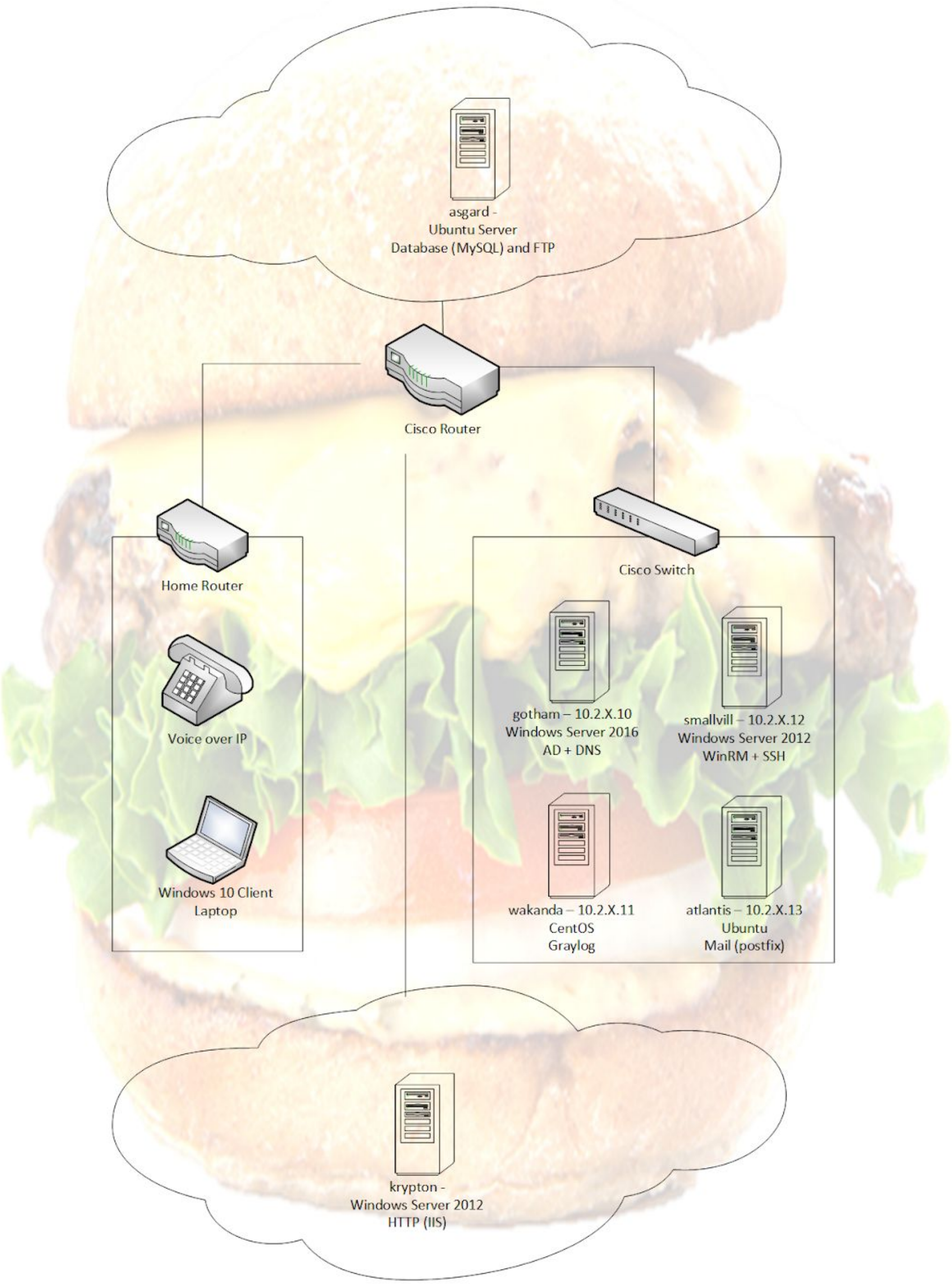
During the last hour, Red Team will stop attacking and will inform blue teams about their attacks so that teams can submit IR reports.

6 p.m. - 8 p.m. **Dinner and Closing Ceremony**

- Location: Golisano Auditorium
- The competition ends and points are finalized. The RC3 President and Competition Architect will make a quick speech about the event and the Red Team captain will give a debrief. Bryson Bort, the CEO of GRIMM, will give a keynote speech. The winning teams will receive their prizes.

Sandwich World

As a sandwich company, we are focused on sandwiches, not IT. Therefore, this topology is subject to change or may not be correct.



Critical Services

Caution: These services and IPs may not be accurate because my staff is focused on sandwiches, not IT and security.

Mail (postfix)
Host: 10.2.X.13
Employees must be able to log into their mailbox and be able to retrieve mail from our customers.

Active Directory (AD)
Host: 10.2.X.10
Employees must be able to authenticate to the domain from any client and server.

DNS
Host: 10.2.X.10
Our DNS servers must be able to resolve forward and reverse queries.

SMB
Host: 10.2.X.12
Employees should be able to access their files and back them up to the server.

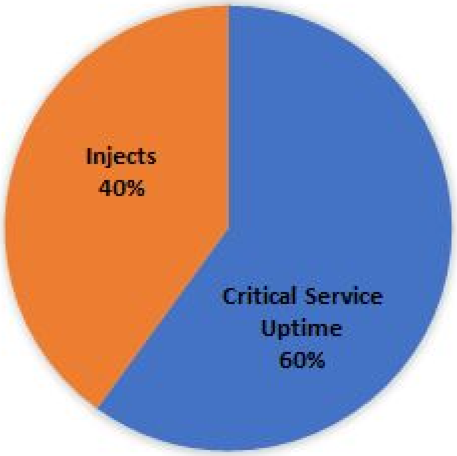
SSH
Host: 10.2.X.12
Employees must be able to log in and access their local and cloud workspaces.

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

MySQL
Host: Cloud Service, IP to be determined
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.

TRACKING PROGRESS AND SUCCESS



Critical Service Uptime - 60%
Although a service is up and listening, it must be functional. For example, for SSH, a white team account should be able to login and run a simple command. Check your team's service uptime frequently, so that you earn points and kudos from CEO Ben and all the customers!

Injects - 40%
These injects will be graded based on a rubric by veteran sandwich makers (aka white team). All injects list the maximum amount of points attabinable; however, if the inject is incomplete, appropriate number of points will still be given.

In addition, if your team chooses not to or is unable to complete an inject in the allotted time, your team MUST send an email to CEO Ben explaining this decision. If your explanation is approved, you will be given a small percentage of points for the inject.

INCIDENT RESPONSE (IR) REPORTS

If your team has noticed incidents caused by Bad-Ron, please submit an incident response report. Please include your team number - without it you won't get any points and sandwich kudos. See the CCDC IR template in the Resource page for reference.

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 provided and set up GrayLog on one of the Linux servers to monitor events and the environment. In addition, we have set up all clients to forward logs to the GrayLog server. 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 (TENTATIVE)

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 delicious sandwiches, 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 Benron 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.

<u>Approved Items</u>

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.

<u>Reset any server to initial company-approved snapshot</u> - 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.

<u>Hire a consultant</u> - 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.

<u>Extend time/due date of inject</u> - 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 Red Team 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 Benron 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 a sandwich company, it is important that we keep on rising to the top, just as our freshly-baked bread does every morning. Please keep our Twitter account active and post frequently (be professional or else no sandwiches for you). Credentials will be given out on the day of the competition.

RESOURCES/SOURCES

Ben Jamin's Graylog Hitchhiker's Guide to the Galaxy
https://tinyurl.com/ybb2krj9

Ben Jamin's Windows Event Viewer - Graylog
https://tinyurl.com/ybb7utsf

IRSeC 2017 Blue Team Packet
https://tinyurl.com/yb72x3ko

IRSeC 2016 Blue Team Packet
https://tinyurl.com/ycztxtlm

IRSeC 2015 Blue Team Packet
https://tinyurl.com/y9yu8p9h

Russ' Presentation on Windows Offense / Red Team (RC3 Week 8)
https://tinyurl.com/y9x34lff

Russ and Brandon's Presentation on Windows Defense / Blue Team (RC3 Week 9)
https://tinyurl.com/ycvktnd3

Micah's Presentation on Linux Offense / Red Team (RC3 Week 10)
https://tinyurl.com/yacfvfmq

Kyle's Presentation on Linux Defense / Blue Team (RC3 Week 11)
https://tinyurl.com/y8ma3hta

Ben Jamin's Windows Defense and Sysinternals Presentations
https://tinyurl.com/yb5drv84 (Fall 2016 - Week 7)
https://tinyurl.com/ycf6xa8g (Spring 2017 - Week 5)

CCDC's IR Template
https://tinyurl.com/y98ftv4n