2016 RC3 IRSeC
Blue Team Packet

Gold Sponsors

Silver Sponsors

Bronze Sponsors

A word from Xanadu's CEO

Welcome Innovators!

Xanadu is a young, fast, synergistic e-commerce startup. Our amazing website is unparalleled in its awesomeness and collision of amazing ideas. Xanadu first emerged from an intense innovative thought tornado (a technique that I, Lord Reverend Kane, created), about a year ago, and has grown faster than anyone in the world could imagine. Because of our super fast growth we need a security team to make sure we don't invite any new "friends" into our systems, so you have been hired as our new security team to make sure that doesn't happen. Here at Xanadu we have a lot of things to protect (like Rosebud), and it's now your job to make sure they're protected. Our entire business hinges on our online reputation, so don't screw it up. Here at Xanadu we don't screw up, we *innovate*.

I've had the CIO create a topology of the nervous system of Xanadu, the network. We think it's pretty accurate but since Xanadu is so innovative and full of creative people, you never know!

Think big, be big, with Xanadu.
Lord Reverend Kane, CEO

Schedule - Saturday, April 30th

8:00 AM - 8:40 AM: Breakfast

- We will provide doughnuts, muffins, coffee and hot chocolate
- This will take place in the CIMS building room 2210
    - See picture below

8:40 AM - 9:00 AM: Competition rules

- Brief overview of the rules and schedule for the competition

9:00 AM -12:00 PM: Competition begins

- Hands on keyboards!
- This happens in the Systems Administration lab (Sys lab)

12:00 PM - 1:00 PM: Lunch and tech talk

- Hands off keyboards; no more competing during this time
- We will provide food and drinks for lunch
- Cyber Ark will give a tech talk during part of this time
- This will take place in the same area as breakfast: the CIMS building

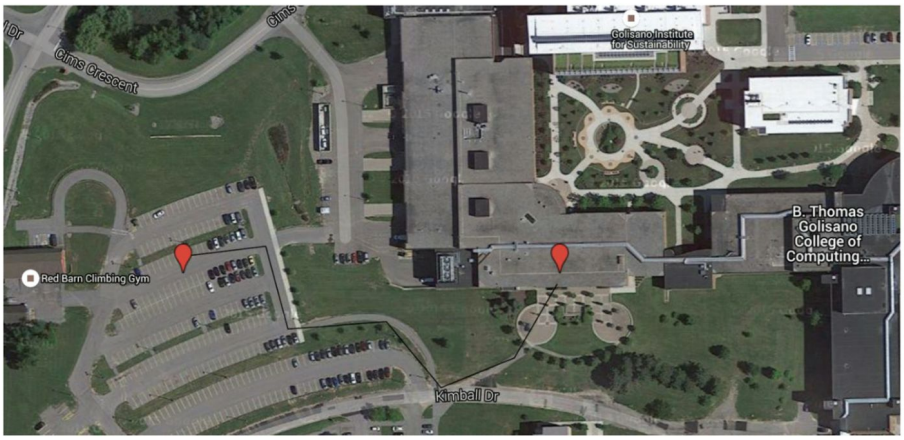
1:00 PM - 6 PM: Competition continues

- Hands back on keyboards!

6:00 PM - 7 PM: Dinner and closing remarks

- We will provide food and drinks for dinner
- There will be a red and white team debrief
- Winners and prizes will be announced
- This will take place in the same area as breakfast and lunch

Address: Please enter "RIT Red Barn" into Google Maps to be directed to this parking lot. RIT Address is 1 Lomb Memorial Dr, Rochester, NY 14623.



Rules

- 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.
- All devices should be pingable at all times. This means no disabling your NIC.
- 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.
- 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.
- *Innovate*.

Scoring

Service checks

Responsible for **60%** of a blue team's score. Services scored include: AD, DNS, HTTP, FTP, SSH, and Mail.

Injects

Responsible for **40%** of a blue team's score. There will be an inject submission portal for blue teams to submit their injects and other deliverables. These injects will be "graded" by white team to determine if a blue team will get 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 does not or cannot 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 the Kitten Coin section below.

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.

Red Team activity - When red team is able to successfully breach/attack a blue team, there will be some point deductions. However incident response reports from blue teams can decrease the amount of the point deduction for any given attack up to 50%.

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 a blue team to reset it back to its initial conditions is by paying for it with a point deduction; they may not use Kitten Coins to pay for the reset. The deduction will be 1% of the theoretical maximum achievable score for a blue team.

Insufficient Kitten Coin (see Kitten Coin section below) Balance - If there is a payment a blue team needs to make (ie. they are losing some of their coins, not purchasing something that benefits them), there will be a point deduction in the equivalent amount of points as converted from Kitten Coins.

Incident Response Reports

Teams are strongly encouraged to submit incident reports for each Red Team incident they 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 the White Team inject/IR report submission portal. **All** incident reports must include the team name and number in it—without this info the report will **not** receive any credit. 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 Red Team attack may reduce the Red Team penalty for that event by up to 50 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.)

VoIP

There will be a network of VoIP phones for blue teams as well as red and white team. However, VoIP is not a scored blue team service; it is maintained by white team.

Scoring Breakdown

Active Directory (AD)

Host: 10.10.x.10
A user must be able to authenticate to the domain.

DNS

Hosts: 10.10.x.10, 10.10.x.30
Your DNS servers must be able to resolve forward and reverse queries

HTTP

Host: 10.10.x.40
A user must be able to visit and use this site. It should remain the same throughout the competition. This check also relies on the database backend which is MySQL running on the Ubuntu/Debian server located at 10.10.x.30.

FTP

Host: 10.10.x.40
A user must be able to log in as well as upload and download a file.

SSH

Host: 10.10.x.30
A user must be able to log in and run commands.

SMTP

Host: 10.10.x.20
Mail must be able to be routed through this server.

IMAP4

Host: 10.10.x.20
A user must be able to log into their mailbox and be able to retrieve mail.

Webmail

Host: 10.10.x.20
A user must be able to log into their mailbox via a web browser and retrieve mail.

White Team Managed Services

Injects and Incident Response Reports

As stated earlier, injects will be posted on the inject portal throughout the competition. You will submit injects and incident response reports to this portal, which is located at **injects.whiteteam.irsec**.

- Your team will receive **one** set of login credentials for the portal. Do not lose your credentials.
- The portal is out of scope for Red Team, so you will not have to/be able to change your credentials.
- Injects must be submitted in pdf, doc, docx, txt, rtf, zip, tar, gz, png, jpg, jpeg, gif, csv, conf.
- Keep your inject submissions professional.
- **IR reports will also be submitted here.** There will be an open inject throughout the competition where you will submit your Incident Response reports for every incident you write up.
- If you submit more than one response to an inject, the **last** submission will be graded.
- If you believe there is an issue with the inject portal, contact white team. We have worked hard to test and make sure it works bug free, but we are not perfect..

Scoring Engine

Each team will be able to see the status of each of their scored services. Teams may go to **scoring.whiteteam.irsec** and log in with your team's credentials. This scoring engine is also where you manage the username and password combination that is used to score your services. If you change a username/password combination that is being used to score a certain service, you must update it in the scoring engine or the scoring checks using that information will fail.

DNS

White team has a core DNS server to which your network's DNS is preconfigured to forward queries

Kitten Coin

Kitten Coin is a currency that can be used to purchase helpful items (listed below). Your Kitten Coin wallets will be managed by White Team and should be considered secure. As part of this secure online wallet, your password will change once every hour, on the hour. We will use the SSH username and password given to the scoring engine to login and “drop off” this password (in plaintext) inside a file in that user’s home directory. So the SSH server is kind of important if you want to access your Kitten Coin wallet and be able to buy things. If the initial SSH connection fails, we will reattempt to drop off a new password periodically. You still start out with **10,000** coins.

Items for sale

Below are a list of items for sale. If you want to purchase an item, simply transfer the number of coins needed to the white team Kitten Coin wallet/account (called “whiteteam”) 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 snapshot

Cost: 1,000 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 kitten coins to purchase the reset.

Consult router/networking expert

Cost: 1,000 coins/10 minutes
Have a networking expert come in, give advice for your network and actually put hands on your keyboard for certain things. If expert helps for more than 10 minutes, then you will have to pay another 1,000 coins for another 10 minutes.

Regain access to company Twitter (see Twitter section below) account if lost

Cost: 1,000 coins
White team will have the emails for the twitter accounts so if a twitter account is compromised by red team or you forget the password, white team will reset the password if you pay for it. You can pay for this as many times as you want as long as you have the funds for it.

Extend time/due date of inject

Cost: 500 coins
You can extend an inject’s due date by up to 30 minutes. If you pay to extend the time there will not be any refunds even if you still do not submit the inject successfully. In your transfer comment, make sure you are very clear about which inject you want to extend.

Consult the help of an auditor

Cost: 500 coins
Your choice of an auditor (from red team or from 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 that provides an actual solution, you can buy this.

Possible Kitten Coin Expenses

If the items below happen, white team will charge your wallet the given fee. As stated in the Scoring section above, if you do not have enough Kitten Coins, we will deduct points from your team's score.

Credit Card Data Loss

Expense: 100 coins
If customer credit card data is lost in a data breach, you will have to pay the fees for that.

Inventory stolen

Expense: 100 coins
This corresponds with your IoT device. More information about this will be made available on the day of the competition.

No response to publicized compromise (Twitter)

Expense: up to 250 coins
If a red team tweets about a data breach or network compromise they successfully performed on you, you must respond in a professional way to ensure your customers that you take their security seriously and tell them anything to convince them of that. You don't need to respond to every single tweet that red team makes about your team, just every incident they tweet about. For example, they may tweet multiple times about the same compromise of your team; this would only need one response from your team's Twitter.

Twitter account posting unprofessional/offensive content

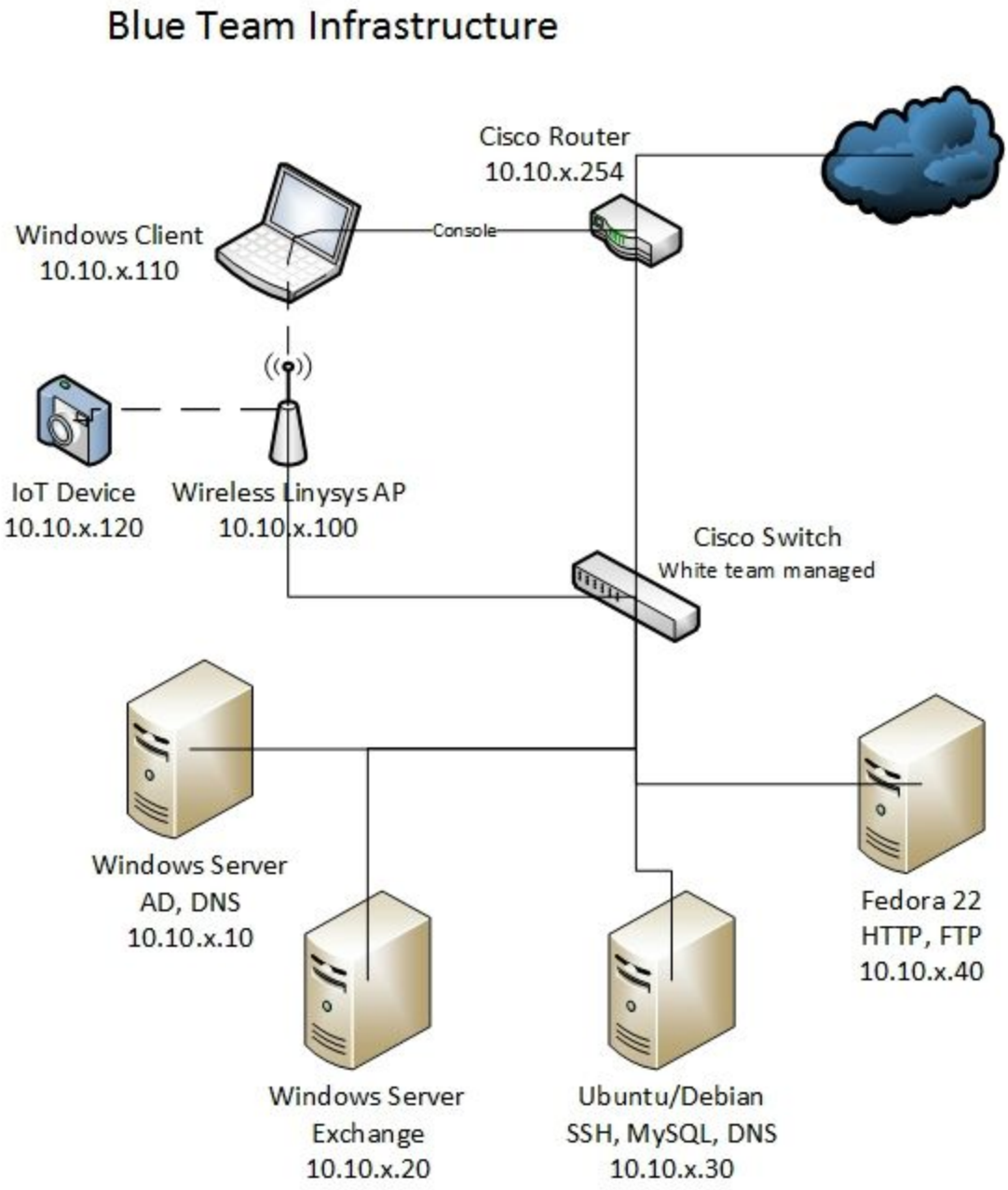
Expense: up to 100 coins
If your Twitter account posts obscene, offensive or unprofessional content that comes from your team accidentally or red team if they compromise it, you can be charged anywhere from 0 to 100 coins per hour.

Twitter

We have created Twitter accounts for each team, and they are @XanadutX, where the X at the end is your team number. You will receive credentials to this account on the day of the competition. You may promote your business in any way you see fit using this Twitter account, but you must keep content professional and not offensive or crude unless you want a charge to your Kitten Coin wallet (see Possible Kitten Coin Expenses above). These accounts must remain public.

Red team will post any breaches using the following hashtags: #OPXanadu2016 #IRSeC2016. Red team may also tweet at your company if you are involved in a breach. Make sure to respond in a timely manner to any tweets red team makes about them breaching you in order to avoid losing Kitten Coins (see Possible Kitten Coin Expenses above).

Topology


Blue Team Infrastructure
Cisco Router
10.10.x.254
Windows Client
10.10.x.110
Console
IoT Device
10.10.x.120
Wireless Linysys AP
10.10.x.100
Cisco Switch
White team managed
Windows Server
AD, DNS
10.10.x.10
Fedora 22
HTTP, FTP
10.10.x.40
Windows Server
Exchange
10.10.x.20
Ubuntu/Debian
SSH, MySQL, DNS
10.10.x.30