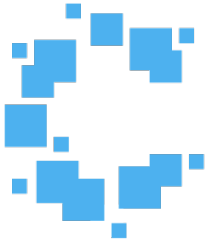
RC3 IRSEC 2015

Incident Response Security Competition

May 9th 2015

GOLD SPONSORS



cigital

facebook

PARSONS

0x07DF CYBER

SILVER SPONSORS

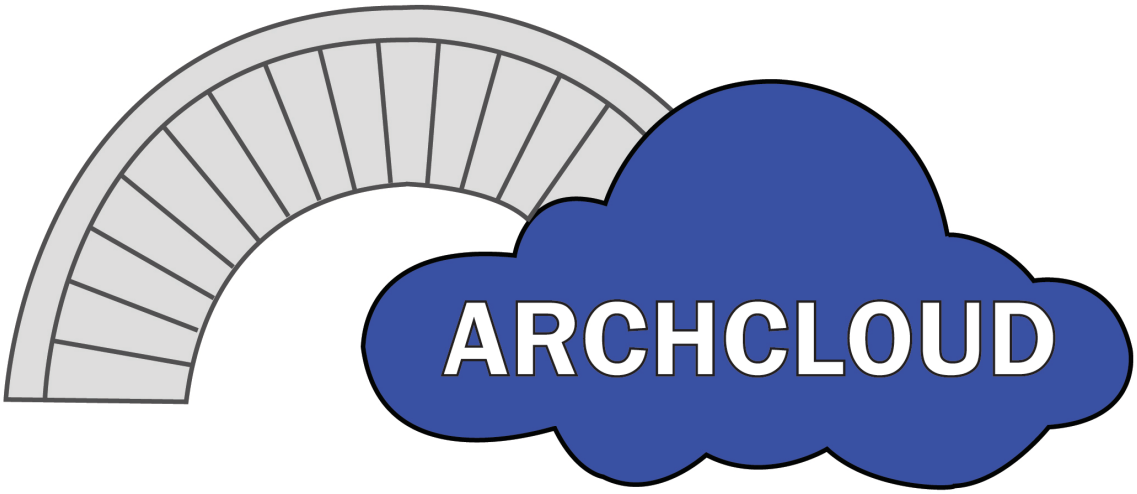
indeed

BRONZE SPONSORS

covermymeds

Malshare

B. THOMAS GOLISANO
COLLEGE OF COMPUTING
& INFORMATION SCIENCES



Congratulations! Your team is the most recent addition to ArchCloud. When building ArchCloud only one thing was kept in mind, usability. It has been brought to our attention that we have neglected security in the process. We have been seeing a lot of companies in the news recently about security breaches where customer data and other information is stolen and we don't want ArchCloud to be the next target. That's where you come in! We have this great infrastructure in place but we're a little concerned that there are too many "holes" built in.

We like to think we run a pretty tight ship here. It is going to be your team's job to secure our network, keep our services online, and make improvements where you see fit. We were told you guys are the best; don't make us regret hiring you guys.

Best of luck,
Scott Vincent
CIO ArchCloud
Bringing the future to you yesterday

Message from the CEO

Hey Gang,

CEO here, I'm super exited to have a bunch of you young RIT kids come in and defend our infrastructure. Since we're a cloud based hosting company, it's pretty darn important I can access my files. I may come around and try to do that from time to time. Gotta look at those selfies ya know. Also, we're getting ready to IPO soon, so we might have a few more policies and "formal business" plans to attend to. Don't worry, I'm sure you'll figure it out. I'll be wandering around from time to time, so lets get ready to have fun!

Jared Stroud
CEO ArchCloud
Bringing the future to you yesterday

Schedule of Events

Saturday May 9th 2015

0800-0845: Breakfast
Where: 70-3435

- Coffee and donuts/bagels will be provided
- T-shirts will also be given out to the team captains at this point.

0845-0900: Make way to Blue Team room and get set up and last minute remarks.

- Hands off keyboards until competition starts.

0900-1300: Competition
Where: Sys Lab 2320

1300-1330: Break for lunch.
Where: 70-3435

- Pizza and drinks will be provided

1330-1800: Competition.
Where: Sys Lab 2320

1800-1900: Talks from our **Gold Tier Sponsors**
Where: 70-3435

1900-2000: Closing remarks
Where: 70-3435

***Closing remarks will feature presentations from the red team by red team captain Michael Salsone and the white team by Scott Vincent while final scores are tallied up. After the final scores are in, the top three teams will be announced and prizes will be given out.

Scoring

Service Uptime – 35%

Services: DNS, FTP, SMTP, IMAP, Web Mail, HTTP, SSH

Uptime Checks

The scoring engine will automatically check scored services for uptime. A successful check will result in points while a failed check will result in no points. How the scoring engine scores varies on each service.

User Credentials

Teams will be able to change the passwords that service checks use. This must be done **in writing** and must be delivered to a **white team member.** Password changes are not automatic so a check or two might be missed during this time.

Losing Points

Points will be deducted from Blue Teams for three reasons:

SLA Violations – After six consecutive missed checks, a predetermined amount of points will be deducted. Every 6 checks, this deduction will occur.

Red Team Activity – Teams will have points deducted when the red team is able to breach blue teams infrastructure and conduct malicious activity.

System Resets – If your system becomes completely unrecoverable, a system reset back to a base image from the start of the competition may be requested. This will result in a 5% deduction from your final overall score.

Injects – 35%

Injects will be handed out periodically throughout the competition. Injects will have deadlines and an inject submission will have to be submitted to receive full credit. If an inject requires a check, a white team member will come by to see if the inject was completed successfully. Partial credit may be received so it is strongly recommended that teams make an attempt.

Incident Response – 30%

Teams may receive points back from the deductions caused by red team in the form of an incident response. Incident responses must be detailed to receive full credit. Important information to include on an incident response is IP addresses, summary of the event, and mediation techniques.

How Services Are Scored

DNS

Host: 10.122.x.1
Your DNS server must be able to resolve forward and reverse queries.

FTP

Host: 10.122.x.18
A user must be able to log in and upload/download a file. Any user from the domain will be chosen for this task.

SSH

Host: 10.122.x.88
A user must be able to log in and run commands. Any user from the domain will be chosen for this task.

HTTP

Host: 10.122.x.88
The webpage must be available and the backend must be working. The layout of the webpage should be the same throughout the competition.

SMTP

Host: 10.122.x.25
E-mail server must be able to route mail.

IMAP

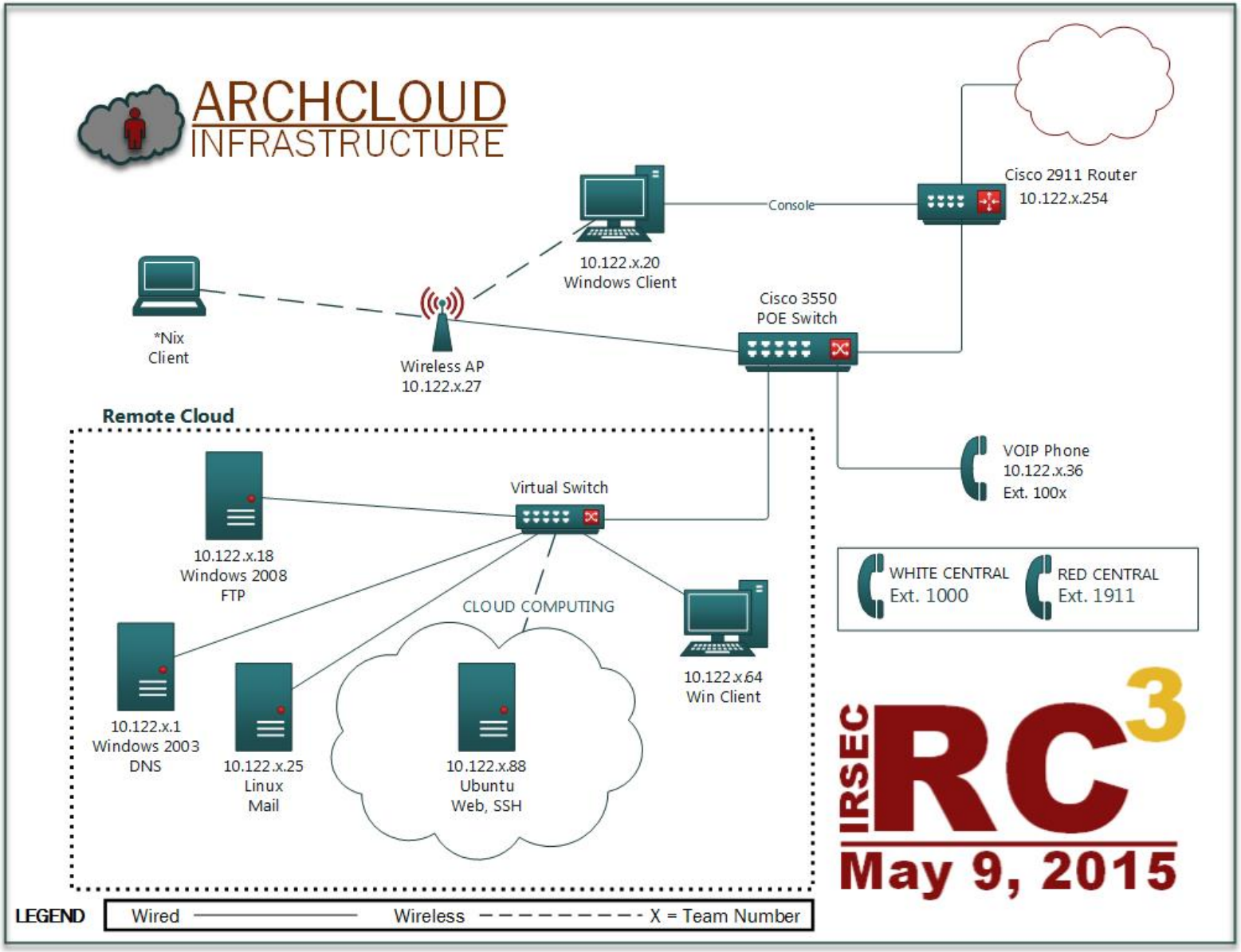
Host: 10.122.x.25
E-mail server must be able to route mail to the correct users inbox.

Webmail

Host: 10.122.x.25
Any user from the domain must be able to log in and send/receive mail from the webmail application.

Rules

- This is a defense only competition. There will be **no** attacking any other teams infrastructure except by Red Team.
- Attacking White Team infrastructure will result in **severe** deduction in points.
- All devices should be pingable at all times.
- 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.
- Host machines will not be allowed to access during the competition however, laptops may be brought in and used
    - Note: Minimal room may be available.
- Do not log into personal accounts on any competition machine.
- Learn something new.
- Have fun.


ARCHCLOUD
INFRASTRUCTURE
Cisco 2911 Router
10.122.x.254
Console
10.122.x.20
Windows Client
*Nix
Client
Wireless AP
10.122.x.27
Cisco 3550
POE Switch
Remote Cloud
VOIP Phone
10.122.x.36
Ext. 100x
Virtual Switch
10.122.x.18
Windows 2008
FTP
WHITE CENTRAL
Ext. 1000
RED CENTRAL
Ext. 1911
CLOUD COMPUTING
10.122.x.64
Win Client
10.122.x.1
Windows 2003
DNS
10.122.x.25
Linux
Mail
10.122.x.88
Ubuntu
Web, SSH
IRSEC
RC3
May 9, 2015
LEGEND
Wired
Wireless
X = Team Number