NECCDC 2021 Regional Finals

An Overview

Raytheon Intelligence & Space

RIT | Global Cybersecurity

Agenda

- Meet the Competition Staff
- Black Team Brief
- White Team Reminders
- Operations and Logistics
- Schedule Reminder
- Q&A

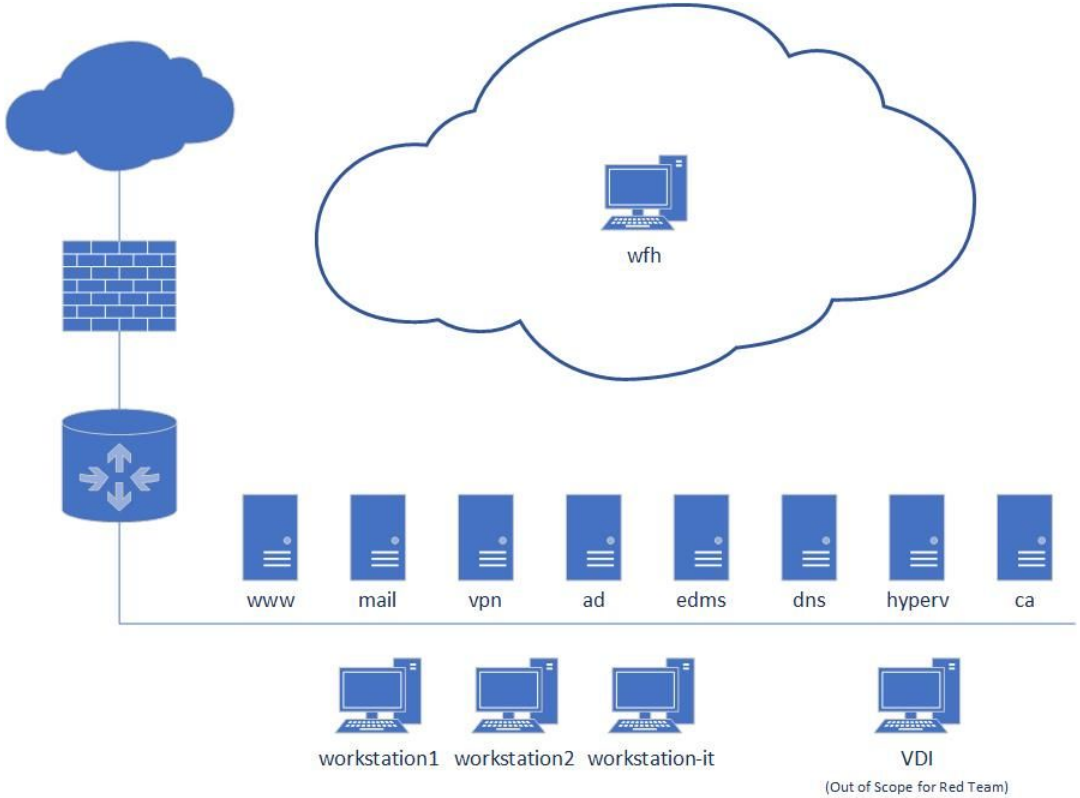
Competition Staff

- NECCDC 2021 Director: Justin Pelletier
- White Team Co-Captains: Yin Pan & Sumita Mishra
- Black Team Captain: Rob Olson
- Red Team Co-Captains: Daryl Johnson & Dan Becker
- Operations: Brock Wagehoft
- League Representatives: Devin Paden, Joe Eastman & Damira Pon

Black Team Brief

- Theme: Mobility
  - People / Systems / Data can all move
  - User functionality is not limited by user location
- Scenario: 24 / 7 Global News Bureau
  - COVID-19 exists in scenario
  - Employees need to work from home, news bureau employees naturally work from many locations
    - Cloud, cloud, cloud!
  - News agencies have been the target of advanced persistent threat actors
    - Zero trust, particularly for remote employees
  - Governments may be interested in data that your news agency has
- Red Team Focus Shift
  - CCDC has been traditionally focused on availability
  - News agencies need to focus on confidentiality (sources!) and data integrity (fake news!)

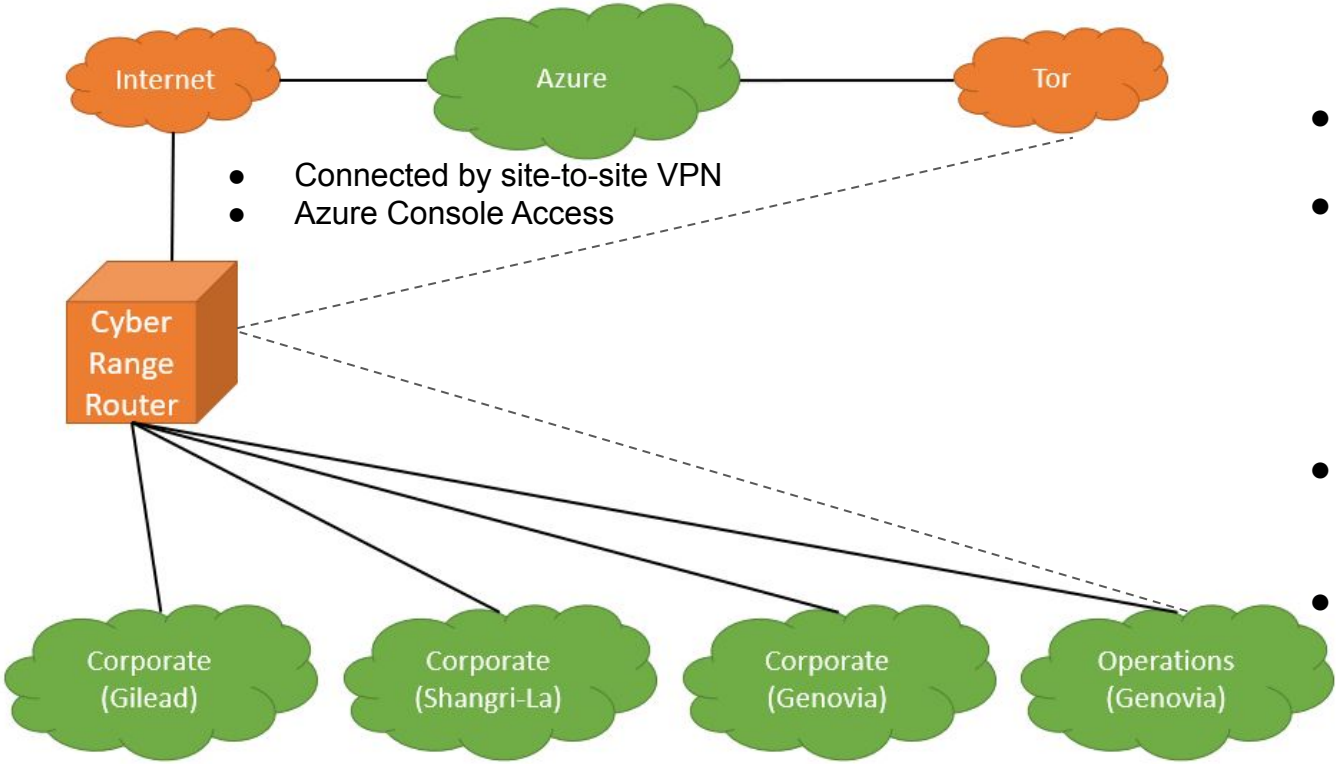
Black Team Brief - Quals Outbrief



Black Team Observations

- Work-from-home in a environment focused on host-based security was challenging
- Security tools need to be configured before use
- Remember essentials
  - Per Red Team: time-to-password-change was higher than normal

Regionals Network Map



- Still NO network security appliance
- 22 to 26 Hosts
- Many returning systems/services from quals
  - Not Hyper-V
  - Corporate networks will seem *very* familiar
- Corporate networks will be very similar
- Some services scored over Tor - think like a news agency!

More on Azure….

- Azure is expected come into play through a series of injects:
  - Newscrier will looking to migrate on-premise Active Directory to a system that lives in Azure and syncs with Azure AD to facilitate remote employee access
  - Suggestions: Research Azure AD, Azure AD Connect, Windows Virtual Desktop, MFA
  - Azure ADDS (Active Directory Domain Services) is not *needed*.
  - Azure may be used for other tasks as needed you will be responsible for staying within your limit of free Azure credits
- There will be non-Azure injects too!
- Azure Resources:
  - https://signup.microsoft.com/signup?OfferId=91335633-c285-41a9-adf6-4969361779e5&ali=1
  - https://docs.microsoft.com/en-us/learn/modules/manage-users-and-groups-in-aad/
  - https://docs.microsoft.com/en-us/learn/modules/secure-aad-users-with-mfa/

Other Black Team Notes

- Newscrier will be concerned with protecting privacy of whistleblowers
  - May want to research systems used by journalists
- There will a new scoring engine - Score Stack
  - Reasons:
    - “Pwnbus” scoring engine hasn’t been actively maintained
    - System architecture limits ability to develop some new kinds of scoring checks that involve irregular timing
    - Doesn’t scale well, even w/ significant resources (Quals: ~160 vCPUs / 250 GB memory)
  - https://github.com/scorestack/scorestack
- We’re working with IBM to make QRadar available (but not mandatory)

White Team Reminders - Rules

- Rules & FAQ
  - Ensure you know the National CCDC rules: http://nationalccdc.org/index.php/competition/competitors/rules
  - For Questions related to the rules - prior to competition (communicate via coach) & during competition (communicate via moderator)
  - See FAQ for Q&A and NECCDC specific rules at: https://docs.google.com/document/d/1mEbhetYhofhBnCe-0DrDkC1uLVOas3dJqjFLDPx5X3Q/edit (includes public repos & incident response template)
- Read Carefully
  - Feedback from NECCDC Qualifiers
  - Every inject has different requirements - sometimes people answer a question not being asked ;)

White Team Reminders - Inject Responses

- Follow Formatting / Submission Instructions
  - Naming format for inject submissions: **Team##Inject## in .pdf, .docx or .rtf**
  - Only send ONE file - can add separation in file if needed, e.g., “email” followed by report - no other attachments
  - If inject requests specific format, e.g., formal report, ensure it is that format
  - Submit on time! Note: Google Classroom time may be different than system time
- Provide Evidence
  - Access to environment post-competition not available and/or changes could have occurred
  - Include screenshots that demonstrate you accomplished what you did
  - Ensure screenshots indicate appropriate systems (keep in mind IP addresses can change)
- Be Professional
  - Use salutation / closing in communications (especially to executive management)
  - References should be acknowledged either as footnotes or citations

Operations and Logistics

- Zoom Webinar will be used for opening & closing ceremonies
- Discord will be main communication line for competition activities
  - My name is Brock (Ops) or bwageoft#0108
  - https://discord.gg/Z2rtZwq2Gy
  - Include alternates (will be removed from team room prior to competition)
- Labels, tags, nicknames have all changed
- NOT required to fill out form
  - Moderators will walk through IPv4 Friday Mar 19
- Ticketing System being reworked to streamline requests
- Please reach out to your network for moderators
  - https://forms.gle/sSJdmuhG5yS4F3BY8
- Symposium Presentation Applications are still open - please submit & share
  - https://forms.gle/JCrJGFcKMtQgzYfV9

Schedule Reminder

- Friday 19th
  - 1800: Opening Ceremony
  - 1830: Authentication Check-In
  - 1900-2100: Environment Open
- Saturday 20th
  - 0830: Reauth Check-In
  - 0900-1630: Environment Open
  - 1630: End of Day Closing
- Sunday 21st
  - 1230-1530: Job Fair
  - 1530-1700: Debrief and Awards

Questions?


RIT
NECCDL


Raytheon
Intelligence & Space


RIT
Global
Cybersecu
Institute


NECCDL


paloalto
NETWORKS


cobaltstrike
by HelpSystems


IBM


RSM


no starch
press


Arete


SRA
SECURITY RISK ADVISORS


cloudcover