Hackathon In-Kind Sponsors

- AWS
- CONTAINERlab
- NANOG
Honorable Mentions

- docker
- CTFd
- Juniper Networks
- Arista
- NANOG
Theme

• CTF style!
• Resolve a variety of network problems
• Players were presented with a set of challenges
  • Challenges were to resolve a variety of network problems in order to capture a flag.
  • Each flag was equal to a certain amount of points. First to score most points wins.
Scenario - GraphQL

- A network topology was modeled in Nautobot with hardware roles, addressing, and interface connections.
Scenario - GraphQL

- Participants were challenged to craft GraphQL queries to retrieve specific information about the network.
Scenario - GraphQL

- At the final stage, participants generated a router configuration from GraphQL facts in NB.
Scenario: Network Modeling

- Participants were given a pre-seeded Nautobot instance.
- The first set of challenges led them through finding and entering network information in the Nautobot web interface.
- The second set of challenges involved performing similar activities programmatically using the API.
- Goal: learn and demonstrate the basics of modeling a network with a tool like Nautobot.
Scenario: Kubernetes

• Participants were guided through deploying a Kubernetes cluster
• Challenged to perform requested operations on cluster, report back results.
Scenario: Rain Cloud

- Participants given a clab topology where they are a hired consultant for a network here in KC.
- The network is having issues reaching their RPKI validator and web server behind AWS.
- The network connects to KCIX and it is assumed that something has gone wrong at the IX causing these issues. KCIX is willing to accept the consultant's help as well.
- Players were tasked with diagnosing and resolving these issues.
Scenario: Rain Cloud
Scenario: Rain Cloud

- First, find out why their web server is only intermittently reachable? It seems this may be contributed due to a flapping IX RS bgp session.

```
root@2_player_crpd> show bgp summary
Threading mode: BGP I/O
Default eBGP mode: advertise - accept, receive - accept
Groups: 1 Peers: 2 Down peers: 1
Table Tot Paths Act Paths Suppressed History Damp State Pending
inet.0 1 1 0 0 0
Peer AS InPkt OutPkt OutQ Flaps Last Up/Dwn State#Active/Received/Accepted/Damped...
192.168.100.33 16509 74 83 0 0 1:12 Establ
inet.0: 1/1/1/0
192.168.100.34 65002 0 0 0 0 3 12 Connect
```
Scenario: Rain Cloud

• After flapping is resolved the bgp session with the IX RS comes up, but now the web server and rpki validator are not reachable at all due to a new best-active route taken. The player's network is AS59209. This new path is originated by AS24342.
Scenario: Rain Cloud

- It is discovered that this new path is an rpki invalid route, the goal is to no longer take this route and capture a flag from the web server via the client behind the cRPD router.

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Max Length</th>
<th>ASN</th>
</tr>
</thead>
<tbody>
<tr>
<td>103.243.140.8/24</td>
<td>24</td>
<td>AS59209</td>
</tr>
</tbody>
</table>

At least one VRP Covers the Route Prefix, but no VRP ASN matches the route origin ASN
Scenario: Rain Cloud

- Multiple ways to accomplish that goal. Once the invalid route is no longer best-active, the player can retrieve the flag. The next steps are to find a contact from the router originating the rpki-invalid route and find out when they started announcing it.
Scenario: Rain Cloud

- Run whois AS24342 and find a contact. Use RIPEStat routing history to see when the route was first announced.
What We've Learned

• We had high engagement in the room.
• Had a wider range of smaller challenges this time, teams kept occupied
• Learned more about CTFd features, avoided glitches (flags were strings or md5sums generated by validation scripts)
• Looking forward to building on this!
Results

<table>
<thead>
<tr>
<th>Place</th>
<th>Team</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MajesticFalcon</td>
<td>41</td>
</tr>
<tr>
<td>2</td>
<td>Team FoCo</td>
<td>23</td>
</tr>
<tr>
<td>3</td>
<td>team octopi</td>
<td>11</td>
</tr>
<tr>
<td>4</td>
<td>Rocket</td>
<td>8</td>
</tr>
</tbody>
</table>
Next up…. Hackathon at NANOG 92 in Toronto

- We will continue the competition format
- A virtual kick-off in the week of 14 October
- Sunday, 20 October 2024 is Hybrid Competition Day
- Registration to open mid-July