Evil Corp
Securing The Present & Future

Securing Servers & Desktop Workstations
- Contain Physical Access
- Key Card elevators
- Man-Trips
- Disabling un-needed devices & ports
- CD/DVD Drives, USB Ports, etc.
- Monitoring Software (SIEM)
- **Employee Training** on security aspects (phishing emails, social-engineering, etc.)

Securing Internet-Based Attacks
- Developing secure Web Applications
- Secure authentication & authorization for all logins
  - Dual-factor authentication *
- Honeypots/Honeynets/Honey-docs
- Security Audits
  - In-House:
    - Vulnerability Assessments
    - Port Scanning
- Outside Cyber Security company to perform “red team vs. blue team” exercise
- Find company’s weak points in:
  - Physical security
  - Internal network
  - External network
  - Employees

Securing Internal Routing Table Attacks
- Internal Gateway Protocols
- Routing protocol authentication & verification
- Disable ICMP Redirects
- ICMP Packet Filtering
- Anti-Spoofing Protections
  - Port Security
  - IP Source Guard
  - Dynamic ARP Inspection (DAI)
  - Anti-Spoofing ACLs

Legend

<table>
<thead>
<tr>
<th>VLAN Color Codes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SALES</strong> (data)</td>
<td>VLAN 18</td>
</tr>
<tr>
<td><strong>VOICE</strong></td>
<td>VLAN 28</td>
</tr>
<tr>
<td><strong>ADMINISTRATION</strong> (data)</td>
<td>VLAN 48</td>
</tr>
<tr>
<td><strong>MANAGEMENT</strong></td>
<td>VLAN 99</td>
</tr>
<tr>
<td><strong>SERVERS</strong></td>
<td>VLAN 115</td>
</tr>
</tbody>
</table>

Student: Michael Cyrus
Sponsor: Mike Harsh