WELCOME!

Please sign in through this link: http://tinyurl.com/campustech1907
or scan the QR code below.
AGENDA

• Organizational Updates
  • New Employees
  • IT Departments Office Change

• Vulnerability Management

• Patch Management Consolidation

• 2008 Server Upgrade

• Titan Digital Signage

• LinkedIn Learning

• Interdisciplinary Common Lab Area

• Important Key Dates
ORGANIZATIONAL UPDATES

BERHANU TADESSE
ORGANIZATIONAL UPDATES

• New Employees
  • Kenneth Bacos, Helpdesk
  • Hau Tao, SGC
  • Annalyn Mai, SGC
  • Walter Nirenberg, ERP Technical
  • Gaby Burns, PMO
  • Floris Coffey, PMO
  • Dan Carney, Administration
  • Carolina Rosells, EIP

• IT Departments Office Changes
INFORMATION SECURITY UPDATES

TONY MODIRI
RANSOMWARE ATTACKS CREATE DILEMMA FOR CITIES

Riviera City, Florida (June 18, 2019)
65 bitcoins, or $600,000 a week before Lake City attack. They paid to get the decryption key.

Lake City, Florida (June 25, 2019)
42 bitcoins or $460,000. They paid to get the decryption key. More than 100 years worth of municipal records digitized have been locked. The decision to fire the director of IT came after cyber attack. Also disabled city servers, phones, and email.

City of Baltimore (36 days before June 12, 2019)
13 bitcoins, or $75,000. They were advised NOT to pay, but it costed them $18,000,000. 95% of their systems came back online 36 days later.

Georgia Court System (July 4, 2019)
$51,000 demanded. They did not pay. Recovery costed $17,000,000.
RANSOMWARE ATTACKS CREATE DILEMMA FOR CITIES

Examples of other recent Ransomware attacks include:

- June 20, 2019: Riviera Beach, Florida, discloses ransomware attack and payment.
- May 7, 2019: City of Baltimore hit with ransomware attack.
- April 2019: Cleveland Hopkins International Airport suffered a ransomware attack.
- April 2019: Augusta, Maine, suffered a highly targeted malware attack that froze the city’s entire network and forced the city center to close.
- April 2019: Hackers stole roughly $498,000 from the city of Tallahassee.
- March 2019: Jackson County, Georgia officials paid cybercriminals $400,000 after a cyberattack shut down the county’s computer systems.
- March 2018: Atlanta, Georgia suffered a major ransomware attack.
- February 2018: Colorado Department of Transportation (CDOT) employee computers temporarily were shut down due to a SamSam ransomware virus cyberattack.
INFOSEC REPOSITORY

Dropbox Share:

• InfoSec Plan
• Incident Response
• OS Hardening
• BCP/BIA Template – Server New Image scenario vs. Restore
• Available software (Spirion, SecureWorks Red Cloak, EnCase, Qualys Cloud Agent)
INFOSEC REMINDER

• All Windows workstations/Laptops should have full disk encryption on using Bitlocker
• All MacOS workstation/Laptops should have full disk encryption on using FileVault
• L1 data-at-rest and transit encryption on all media, applications and databases
• No L1 data on mobile devices
• No Shadow IT
• Ability to rebuild your servers after a compromise
• Remediation of Level 4 & 5 Vulnerabilities within 30 days
• No unsupported Operating Systems
# VULNERABILITY MANAGEMENT

## Current External Vulnerabilities

### Summary of Vulnerabilities

<table>
<thead>
<tr>
<th>Vulnerabilities Total</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>by Severity</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td><strong>Confirmed</strong></td>
</tr>
<tr>
<td>5</td>
<td>11</td>
</tr>
<tr>
<td>4</td>
<td>43</td>
</tr>
</tbody>
</table>

### Vulnerabilities

Vulnerabilities are design flaws or mis-configurations that make your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Minimal</td>
<td>Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.</td>
</tr>
<tr>
<td></td>
<td>Serious</td>
<td>Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.</td>
</tr>
<tr>
<td></td>
<td>Critical</td>
<td>Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.</td>
</tr>
<tr>
<td></td>
<td>Urgent</td>
<td>Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.</td>
</tr>
</tbody>
</table>
QUALYS UPDATE

New Fullerton Qualys Portal
• User Management differences
• Qualys VM, 250 Licenses for Cloud Agent
  • Video on Qualys Cloud Agent

Web Application Scanning (WAS)
• Acunetix WAS not renewed, instead
• Qualys Web Application Scanning

Qualys Training & Certification
https://www.qualys.com/training/
Self-Paced Training or WebEX
QUALYS VM CLASS TOPICS

- Overview of the Vulnerability Management Lifecycle
- Vulnerabilities and the KnowledgeBase
- Asset Mapping and Discovery
- Asset Groups
- Asset Tagging
- Introduction to AssetView and Dynamic Dashboards
- Scanning Overview
- Scanning configuration
- Authenticated Scanning
- Reporting Overview and Templates
- User Roles
- Remediation Policies
- Certification Exam Preview

Upcoming Instructor-Led WebEX Classes:
Vulnerability Management (Sept 6 9AM-5PM UTC)
https://www.qualys.com/training/
QUALYS WAS CLASS TOPICS

• Web Application Scanning Overview
• The Qualys KnowledgeBase
• Basic Application Setup and Discovery
• Advanced Application Setup and Scanning
• Reporting
• Tags and Users - Tag Creation
• Burp and Malware Detection

Upcoming Instructor-Led WebEX Class:
WAS (July 30 10AM – 5PM UTC+5:30)
https://www.qualys.com/training/
Shodan is a search engine that allows you to look for devices connected to the internet using service banners.

When you connect to a server listening on a given port, the server (usually) responds with a service banner.

Service Banner: A block of text about the given service being performed.
SHODAN DATA COLLECTION

• Shodan uses a technique called “Banner Grabbing”
• Banner Grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports
• Indexes banners instead of web content
• Admins can use it to keep tabs on the services and systems on their networks
• Hackers can use it to expose potential targets
POTENTIAL TARGETS

• Routers
• Webcams
• SCADA systems
• Traffic Lights

• Note: Be careful what you try to access!
SHODAN LIVE DEMO
SERVER INFRASTRUCTURE UPDATES

BILL ELBETTAR
PATCH MANAGEMENT

Utilize the following tools for patch management:

• Mobiles Devices: JAMF, explore MS InTune in future
• Linux Servers: Explore RedHat Satellite and Ansible
• Desktops: Expand SCCM for campus use
• Windows and VM servers: Expand WSUS with SCCM for patching server OS, MS office products
• Third-Party Applications: Explore Cloud Management Suite software or use tailored code into SCCM
SCCM PATCHING UPDATE

• CSUF IT currently utilizes SCCM for patching over 3K endpoints (Windows Critical updates only) for both rollout and non-rollout computers

• No 3rd party patching at this time

• Please tell staff in your area to reboot their workstations at the end of the day to ensure a smooth patching process

• Most recently began patching a total of 19 campus servers for IT, AFIT and ASC

• We still need volunteers to help us test this new process for servers. Please reach out to JP Marquez at jpmarquez@fullerton.edu

• SCCM client can be found here:
  \adselect\shares1\Client Software\SCCM\Client
SCCM PATCHING UPDATE

Proposed server patching options for admins:

1. IT will push Security and Critical OS patches on a weekly basis and force servers to restart within a week of patch application.

2. IT will push Security and Critical OS patches on a weekly basis. Restart will be suppressed until tech in charge of server restarts manually.

3. IT will download Security and Critical OS patches on a weekly basis and make available through the SCCM Software Center. Patches will need to be manually applied by tech in charge of server.

4. IT will re-direct server to our WSUS server. Tech will need to run Windows Update manually to download and run updates. No SCCM client installation is required for this option.

5. Server admin will keep patching on their own using their own WSUS or other methods as long as they are passing the security scan administered by ISO.
### SCCM Software Center

**California State University Fullerton**

#### Applications

- **Sort by:** Application name A to Z

<table>
<thead>
<tr>
<th>Name</th>
<th>Publisher</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-08 Security Only Quality Update for Windows Server 2012 for x64-based Systems (KB4434396)</td>
<td>Microsoft</td>
<td>Requires restart</td>
</tr>
<tr>
<td>2018-09 Security Only Quality Update for Windows Server 2012 for x64-based Systems (KB44657140)</td>
<td>Microsoft</td>
<td>Requires restart</td>
</tr>
<tr>
<td>2018-10 Security Only Quality Update for Windows Server 2012 for x64-based Systems (KB4462931)</td>
<td>Microsoft</td>
<td>Requires restart</td>
</tr>
</tbody>
</table>

#### Updates

- **Operating Systems**
- **Installation status**
- **Device compliance**
- **Options**
2008 SERVER UPGRADE

• A list of Windows 2008, 2008 R2 servers and Windows 7 were created

• Notifications were sent to managers with the list of servers

Timeline of Events:

• **July 16** – Update the attachment with actions required and return to ISO@fullerton.edu

• **July 17** – Servers that do not need to be accessed from the Internet will be blocked

• **September 27** – Deadline for upgrading to latest supported OS

• **September 30** – All servers not upgraded will be retired and no longer available
TITAN DIGITAL SIGNAGE

ROMMEL HIDALGO

SEE TITAN DIGITAL SIGNAGE POWERPOINT
ACADEMIC TECHNOLOGY UPDATES

WILLIE PENG
LinkedIn Learning

• LinkedIn Learning, formerly Lynda.com, will go live on July 18, 2019
• Learning activity and history from Lynda.com will transfer to LinkedIn Learning
• Deep links need to be updated
• Users will receive an email invitation from LinkedIn Learning/Lynda.com
• [CSUF LinkedIn Learning Website](#)
INTERDISCIPLINARY COMMON LAB AREA

WELSON BADAL
INNOVATION/MAKERSPACE CENTER

Room Technology
- Dell Canvas
- High-end PC & Mac
- HTC Vive (Virtual Reality)
- Microsoft HoloLens
- Microsoft Surface Hub
- Raspberry Pi
- Ultimaker 3 Extended 3D Printer
- Wacom Cintiq 27" QHD, Creative Pen & Touch Display
DIGITAL VISUALIZATION CENTER

Room Technology

• 4 x 4 front video wall (46" display each)
• Four Epson Pro G 7500, 6500 Lumens Projectors
• HDMI Connection (up to 5 devices)
• Apple TV
• Audio/Video Conferencing Capability
• Blu-Ray Player
• Document Camera
• In Room PC with Three Outputs
• Lavaliere Wireless Microphone
• Pan/Tilt/Zoom Camera
• Wi-Fi Capability
CONCEPT DRAWING OF RENOVATION
CONCEPTUAL DESIGN (Not actual photo)
INTERDISCIPLINARY COMMON LAB AREA

College Collaborative Spaces

• 8 Clustered seating for each of the colleges
• 10 Workstations per cluster
• Workstations will have specialized software and/or hardware
# AREA TECHNOLOGY

## MAC Workstations
- College of the Arts
  - Cintiq graphic pen and tablet
- College of Communications

## PC Workstations
- College of Education
- College of Engineering and Computer Science
- College of Health and Human Development
- College of Humanities and Social Sciences
- College of Natural Sciences and Mathematics
- Mihaylo College of Business and Economics
CONCEPT LAYOUT
CONCEPT FURNITURE
IMPORTANT KEY DATES

• Jul 18 – LinkedIn Learning Go-Live
• Oct 15 – Password Change Month for All Users / Extended MFA Deadline
• Dec 31 – Old VCL Decommissioned
• Jan 14 – Windows Server 2008, 2008 R2 & Win7 EOL
SURVEY INSTRUCTIONS

• On your mobile device or laptop’s browser, type "http://srs.campuslabs.com" or just scan the QR Code here:

• Enter your First Name, Last Name. You can use “Tuffy Titan” as your first and last name.

• Enter the Connect ID (12244)

• Tap/Click on “Connect” button to join the session.

• Once a question appears, answer the question and tap/click “Submit.” You may have to scroll down to access “Submit” button.
QUESTIONS?

THANK YOU!

For more information, please visit the Information Technology Technical Architecture Committee (TAC) website.
REFERENCES

• Ransomware Attacks Create Dilemma For Cities: