



# Vulnerability Scanning

By: Chandos  
Carrow, CISSP

2015 COV IS Conference –  
Richmond, VA

---

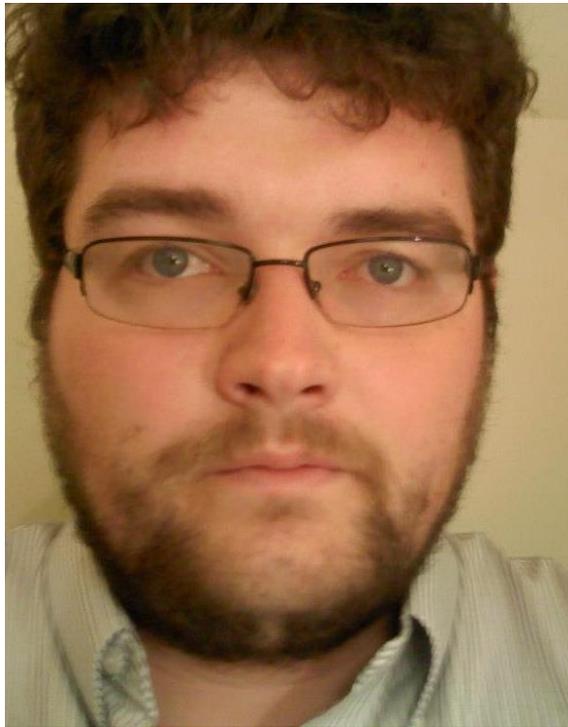
# Myself

- ~7 years experience with the state in information security
- ~2 years experience with the VCCCS as an Information Security Analyst
- BBA/IT, AAS IT, AAS IS, and working on MSIS
- CISSP, Network+, CBP

I am not John Popper



I am not Chewbacca



# VCCCS

- 23 community colleges across the Commonwealth
- 46 campus
- ~15,000 staff and faculty
- ~400,000 student headcount

# VCCCS Enterprise Systems

- 600 servers – 400 virtual and 200 physical
- Capability of holding 6 petabytes of data
- The largest single instance of PeopleSoft CampusSolutions
- The largest single instance of BlackBoard
- The largest single instance of BlackBoard Analytics (data warehouse)
- 15+ enterprise systems

# History of the VCCS and Vulnerability Scanning

- VCCS used to complete vulnerability scanning several years ago, but that process stopped
- VCCS decided to purchase Rapid 7
  - Leader in field – in the Gartner magic quadrant
  - Scalable
  - Created Metasploit
  - Price
  - Frequency of updates
  - When outsourced some vendors used this product

# Start of project

- Proof of concept completed October 2013
- Purchased December 2013
- Installation February 2014
  - SO, BRCC, SVCC, PDCCC
  - Started with 2,800 licenses

# Vulnerability scanning now at VCCS

- Became the standard for vulnerability scanning for the VCCS as of 2014-06-05
- Currently have ~17,000 licenses
- Ability to scan Class A networks (16,858,877 discoverable assets)
- 45 users
- 20 scan engines used
- 70 sites and 19 groups
- ½ of the colleges are using Nexpose

# Centralized process

- SO offers Nexpose as a service to the colleges
- Each college purchases the necessary licenses for the assets they are responsible for
- Scan engines are installed in strategic areas
- Scan engines connect back to the security console located at the SO
- College administrators have access to their sites and groups
- Only global administrators at the SO can see all assets at each college, each college can only see their own
- College administrators responsible for running their own scans and remediating the vulnerabilities found
- Goal: have full network scans completed on a quarterly basis and show a downward trend in vulnerabilities

# Scanning

- Majority of the scanning occurs at the scan engine at each college/location
  - Reduces strain on the security console
  - The colleges can run scans all at once and it will not impact the security console performance
  - Scanning can be completed during work hours even on production systems

# Reports

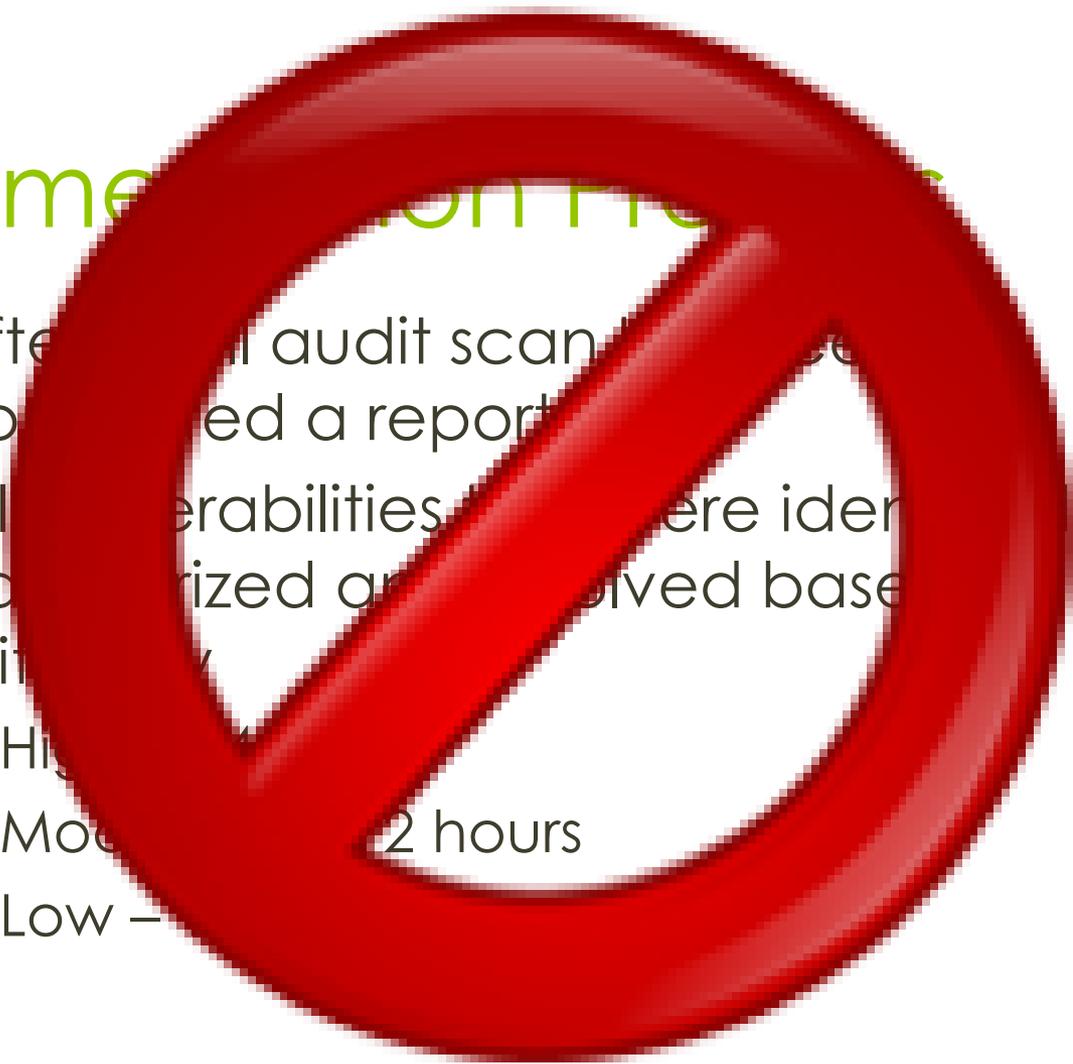
- Reports can be generated by anyone who has access to the sites/groups
- Several different reports templates available
  - PCI, SCADA, Top 10s, Top 25 Remediations
- Report templates can be created by anyone and used by anyone, but they can only see the reports ran against their own sites/groups

# Information Overload

- Raw information that comes from scans can be very overwhelming
  - If Java is behind one version you will get a vulnerability for each patch that has come out since it was last updated
- Reports solve some of the issues
  - Remediation reports seem to work best

# Remember on the ...

- After an audit scan, the ...  
completed a report
- All vulnerabilities were identified and are their  
categorized and assigned based on their  
criticality
- High - 4
- Moderate - 2 hours
- Low -



# Remediation Process

- As a whole the SRC, ASC, and ESC came together to review the Top 25 Vulnerabilities
- Determined that it would be better to resolve the vulnerabilities on machines related to non-COTS
  - Based on risk
- Access to the security console will be provided to those in ITS based on the application/system they are responsible for
- Vulnerabilities are analyzed based on their criticality, exploitability, access to the system from the outside, and the skill level needed by the attacker
- Colleges will complete their own scans and remediation process, but scans must be done on a quarterly basis
- After remediation is completed a scan is ran again to show that the vulnerability is fixed
- This is a work in progress and will change down the road

# Vulnerability Lifecycle



# Hypothetical Scenario

- A long time ago in a galaxy far far away...



# Discovery

- First step along the process
- Typically involves a scan of some sort
  - In house
  - Outsourced/Third Party
  - Internal/External
- Could be from a bug reported
- Also could come CVE (Common Vulnerabilities and Exposures) reports

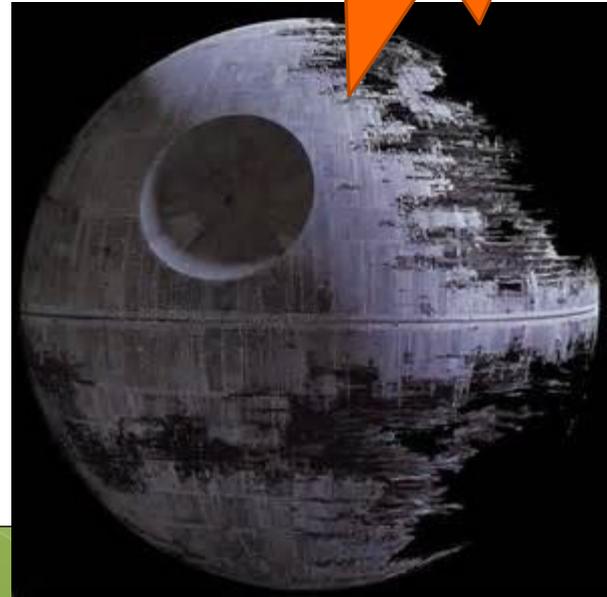
# Scenario



Risk  
Score  
10



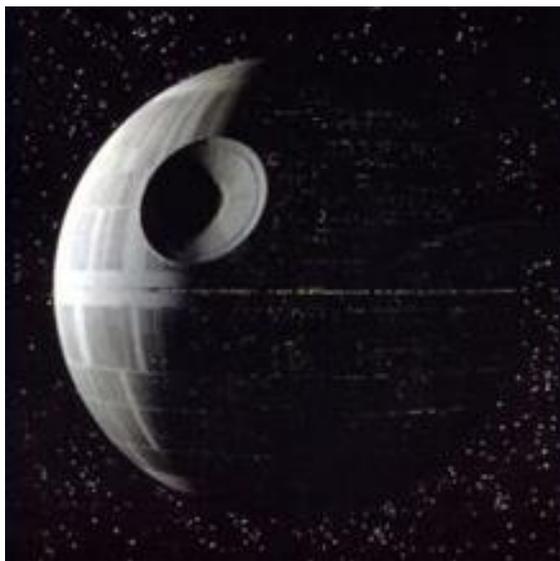
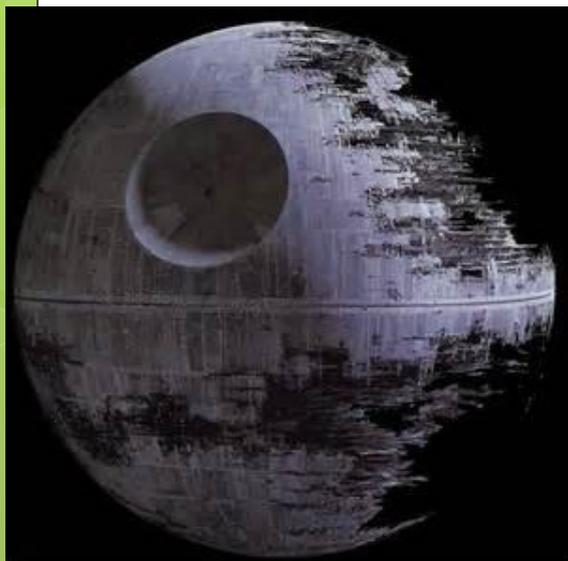
Warning  
CVE  
001100  
010010  
100001  
101101  
110011



# Prioritize Assets

- Most important part of the lifecycle
- Determine what assets are the most important to protect from vulnerabilities
- This is where risk assessments become part of the vulnerability lifecycle
  - What is the level of risk your organization is willing to accept?

# Scenario



# Assess

- Time to assess the vulnerabilities on the most risky assets
  - Who/what/when/how/why
  - Is there an exploit publically available?
  - Level of expertise needed to execute exploit

# Scenario

- Who/what/when/how/why
  - proton torpedo, shot precisely into a small exhaust port, could trigger a reaction that would destroy the Death Star
  - Exploit was released to the Rebels when the schematics were stolen
  - Expert skills in the force needed to make the impossible shot

# Report

- Create report of the assessment and the information you were able to research
- Provide and present the information to your vulnerability team and any additional stakeholders necessary

# Scenario



# Remediate

- Once the report has been analyzed its time to create a remediation plan
  - Identify the users/teams necessary to resolve the vulnerabilities
  - Create change management tickets and assigned those to the appropriate people
- Proceed through the remediation plan as indicated

# Scenario

- Once the Empire knew that the schematics for Death Star I were stolen by the Rebel forces their remediation plan went into effect
  - They sent Darth Vader to collect the schematics, he was not successful
  - The alternate plan was put in place, capture Princess Leia and blow up her home planet. Success...

# Verify

- The final step in the vulnerability lifecycle is to verify that the vulnerability has been resolved
- Most of the time this takes place when another scan is completed
  - Asset(s) that went through the remediation process
  - Full scan

# Scenario

- Unfortunately the Empire did not verify that their remediation for the vulnerability in Death Star I remediate the vulnerability
- The Rebels used the schematics to find the vulnerability, created a plan to save the princess, and sent an attack against the Death Star I to exploit the vulnerability
- But the Empire was not wrong in their vulnerability process because they assumed the risk on Death Star I because they had Death Star II waiting

Can you assume that risk though?



# Student Success and Vulnerability Scanning

- System/Network Uptime
  - If systems or the network go down due frequently to vulnerabilities or attacks from vulnerabilities then the student experience is affected
- Bad Publicity
  - If the systems are breached due to a vulnerability the students data can be lost and less students would be interested in coming to your college
- Students Systems
  - Since the students connect their systems to your network a vulnerability on your network could impact the students system by increasing its chance of being infected

# Things to take away

- Vulnerabilities are out there and can be potential vectors for hackers
- Resolve vulnerabilities based on the risk to your environment not solely on risk scores
- There is no I in team - The vulnerability lifecycle is not a one person job and there should be a team created
- Knowing is half the battle - Any progress in the remediation of vulnerabilities is better than not having any resolved

Questions?



Thank You



E-mail: [ccarrow@vccs.edu](mailto:ccarrow@vccs.edu)