CySA+

Cybersecurity Analyst

CCI
Post Office Box 9627
Mississippi State, MS 39762

CySA+

Part 2

Vulnerability Management

Vulnerability Scanning

Chapter 6

Outline

- Execute Scanning
- Remediation
- Analyze Reports from a Vulnerability Scan
- Validate Results and Correlate Other Data Points

Execute Scanning

- **Modern scanners**
  - **Cannot find vulnerabilities**
  - **The most common vulnerability scanners have massed huge libraries of vulnerabilities**
  - **The three preferred scanners are**
    - **Nessus, OpenVAS, and Nikto**
- **Authentication scans**
  - **Method 1**
    - **Local agents are put on the endpoints to provide analysis during scans**
  - **Method 2**
    - **Administrative credentials are provided to the scanner and will be utilized as needed during scans**

[1]

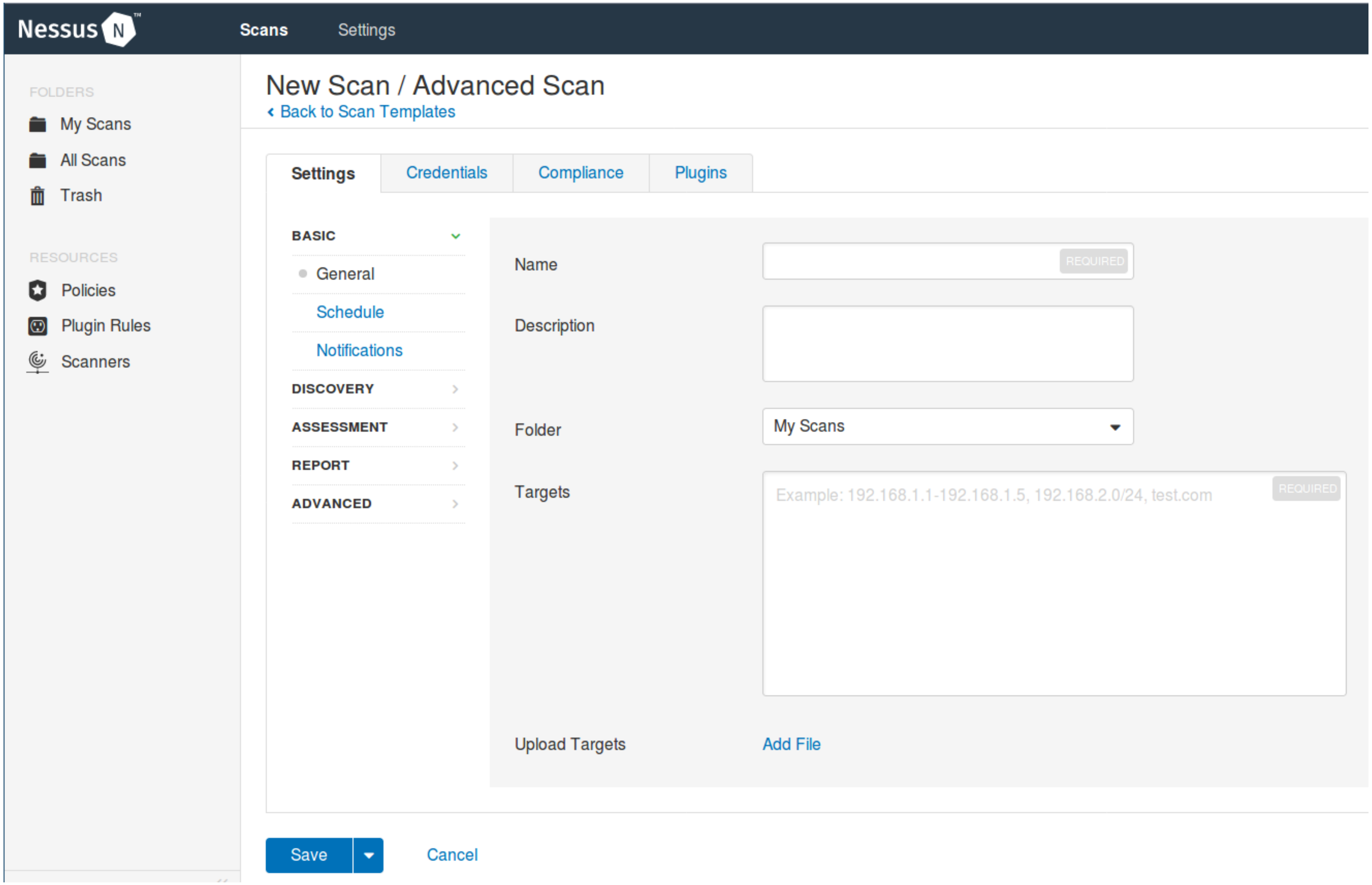
Execute Scanning

nessus

- Is a powerful scanner, which started out as an open source and free utility
- Can oversee scans across multiple networks that users can schedule and assign custom policies.
- Includes more than 80,000 plug-ins
- Other functions
  - Basic port scanning tools, Vulnerability identification, Misconfiguration detection, Default password usage, Compliance determination
- Default Features
  - Has the ability to generate reports, coordinate the vulnerability scan, and controls the vulnerability management
  - Has the ability to use the Nessus web client from anywhere on the network, or the machine that it was originally installed upon
  - The client was created to function from any browser that supports HTML5 a
  - Provides the user manipulate scan settings from the web's interface

[1,2]

Nessus



New Scan / Advanced Scan

‹ Back to Scan Templates

Name: REQUIRED

Description:

Folder: My Scans

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com REQUIRED

Upload Targets: Add File

[1,3]

Execute Scanning

- Open Vulnerability Assessment System (OpenVAS)
  - Is a free framework that consist of several analysis tools for both vulnerability identification and management
  - Originated from the Nessus framework
  - Supports browser-based access to its OpenVas manager
- OpenVAS Manager
  - Uses the OpenVAS Scanner to conduct assessment based on a collection of over 47,000 network vulnerability tests (NVTs)
  - Results of the NVTs are then sent back to the manager for storage

[1]

Execute Scanning

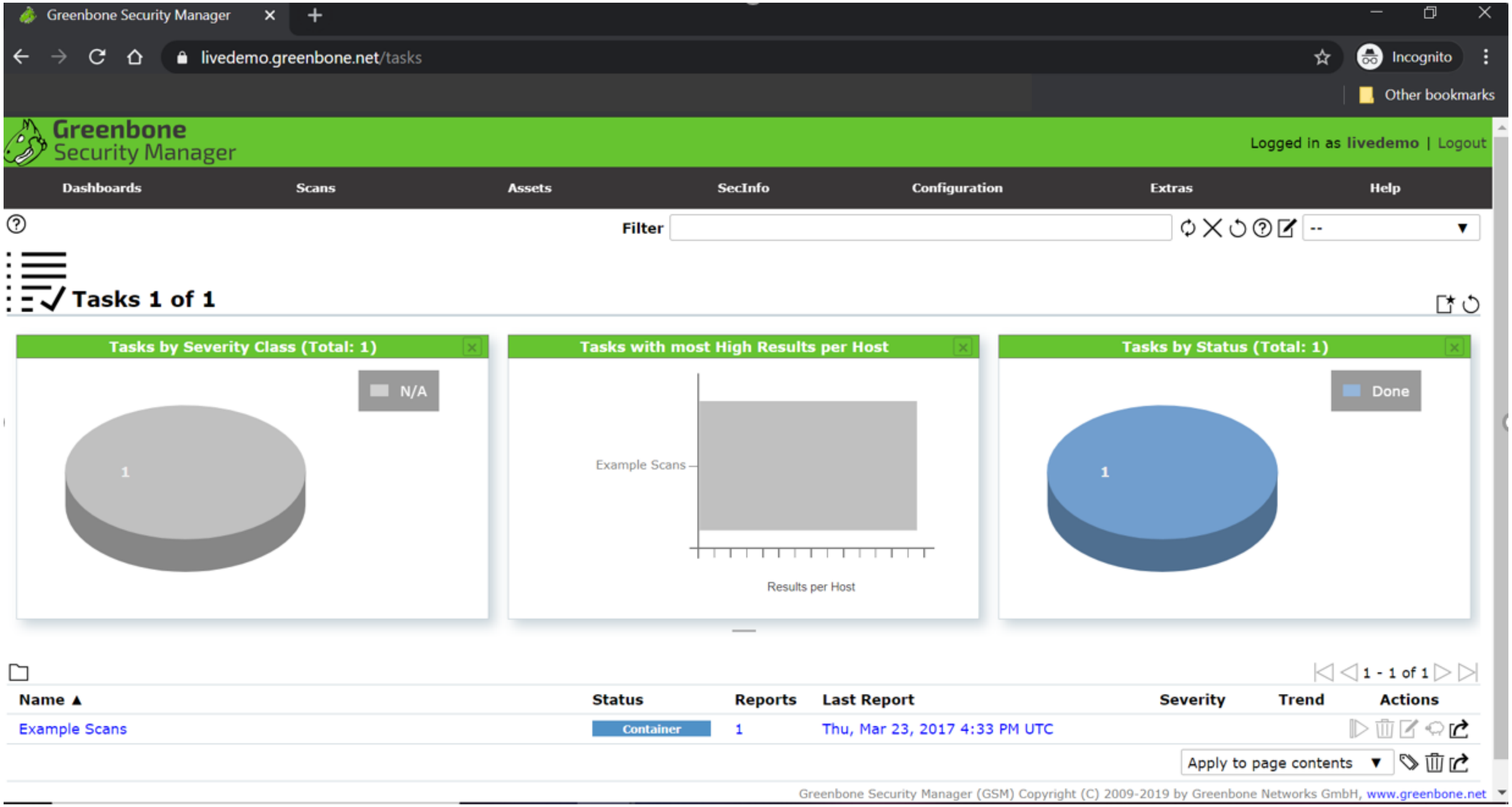
- **OpenVAS Operations**
  - **Admin can access OpenVAS's web user interface**
  - **Welcome screen appears, and the admin can access all setting for both OpenVAS manager and Scanner**
  - **Can be used to launch quick scans**
  - **Admin can see the status of each of the tests and get details on the test itself**
  - **A vulnerability score is given, and a level of confidence is assigned to the discovery method**

OpenVAS

Open Vulnerability Assessment Scanner

[1,4]

OpenVAS



Greenbone Security Manager
livedemo.greenbone.net/tasks
Incognito
Other bookmarks
Greenbone Security Manager
Logged in as livedemo | Logout
Dashboards
Scans
Assets
SecInfo
Configuration
Extras
Help
Filter
--
Tasks by Severity Class (Total: 1)
N/A
1
Tasks with most High Results per Host
Example Scans
Results per Host
Tasks by Status (Total: 1)
Done
1
1 - 1 of 1
Apply to page contents

Tasks 1 of 1

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Example Scans	Container	1	Thu, Mar 23, 2017 4:33 PM UTC			

Greenbone Security Manager (GSM) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbone.net

[1]

Execute Scanning

- **Nikto**
  - **Is a web server vulnerability scanner**
  - **Originated from Kali Linux distribution**
  - **Strengths**
    - **Finding vulnerabilities such as SQL, improper server configuration, cross-site scripting(XSS), and command injection susceptibility**
    - **Able to perform thousands of tests quickly and provide information on the nature of the weaknesses.**
  - **Weakness**
    - **Lacks a graphical interface as a command line executed utility**

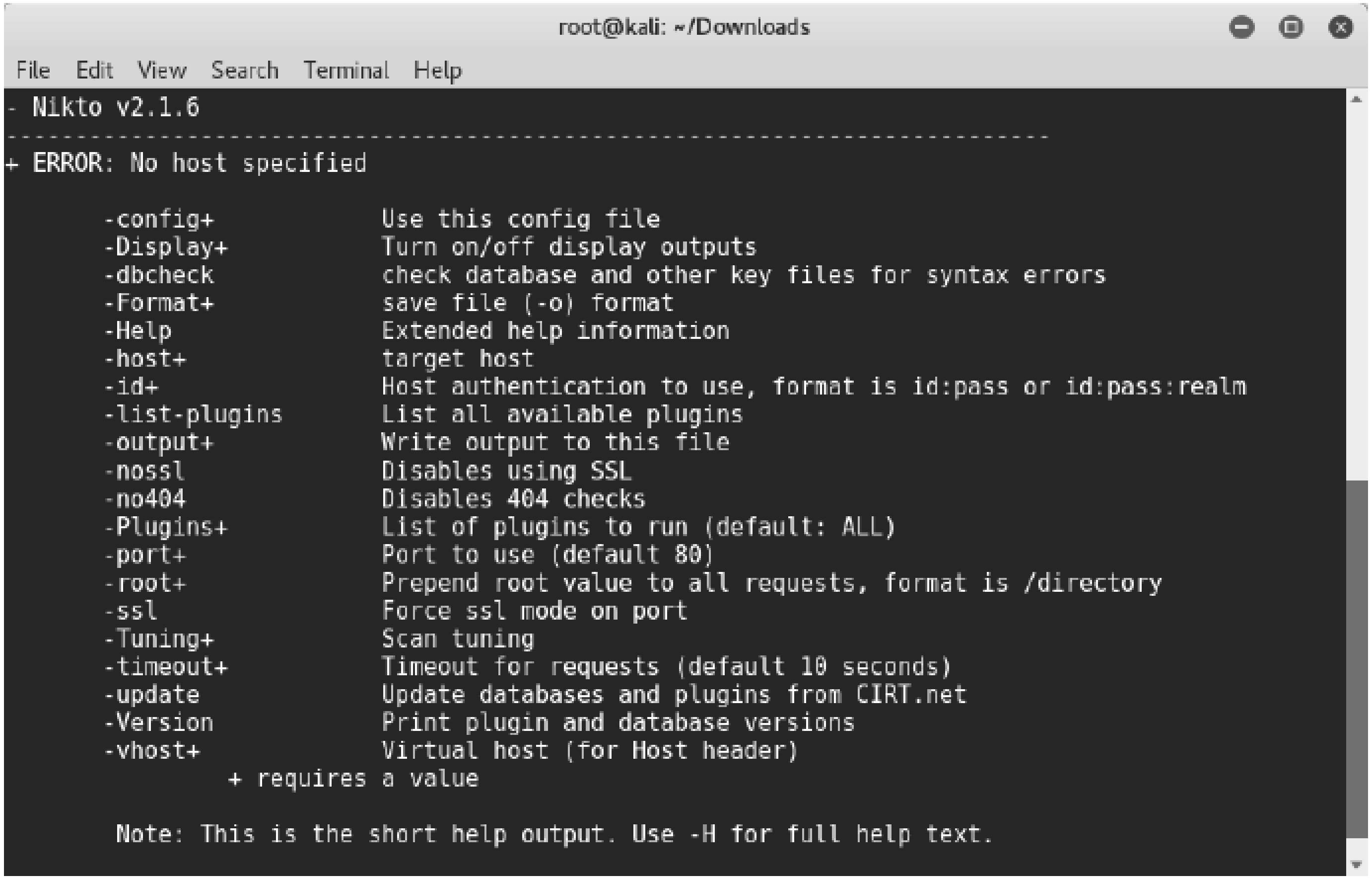
[1,5]

Execute Scanning

- **Nikto Operations**
  - **To conduct a scan against a web server you, must assign an IP with the host option enabled**
  - **By default results of the scan will be outputted in the same window**
    - **Not practical if you need a detailed analysis and is only should be used to confirm the status of the host**
  - **You can export the results to output files for a follow-on evaluation, by using other options in the command line**
- **Nikto Output**
  - **The output file includes the type of vulnerability, a short description, and any reference information about the vulnerability**

[1]

Nikto



```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: No host specified

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
                + requires a value

        Note: This is the short help output. Use -H for full help text.
```

[1]

Generate Reports

- Report Generation
  - Is critical for both vulnerability management and incident response process
  - All vulnerability scanners perform a reporting type of function of some kind, but some lack customizable options
    - For example, Nessus provides utilizes formats of PDF, HTML, CSV, and its own format to report
- Administrators
  - Should always consider the types of reporting their utility is capable of and how the reporting process could be automated
  - Sending and receiving important information in a timely manner is necessary for efficiently addressing those vulnerability scans

[1]

Generate Reports

- **Automated vs. Manual Distribution**
  - **Creating reporting templates**
    - **Allows you to rapidly create customized reports based on vulnerability scan results**
    - **Can be forwarded to needed points of contact**
  - **Best Practice**
    - **Automate the report delivery process**
      - **Prevents the primary admin from being required to manually manage every report**
      - **By giving administrators relevant reports to their role it will increase their efficiency**

[1]

Remediation

- OpenVAS's scanner
  - Show a summary of the vulnerability, location of concern, vulnerability's impact, how it was discovered, and any solutions/workarounds
- Remediation of network vulnerabilities
  - Must be implemented efficiently and as fast as possible without worsening the vulnerability
  - Effective Remediation
    - Continuous examination for vulnerabilities combined with a process to correct issues to keep the organizations resources accessible and confidential

[1]

Remediation

- The Simplest mechanism for verifying remediation
  - Is to compare consecutive scans to determine if the vulnerabilities were corrected via upgrade or patch.
- Patch Management
  - Utilizing a compensating control, users can provide feedback into vulnerability management system by adding a note to the report or override the alter
  - Helps document actions used to address the problem incase the user is unable to apply an update
  - Vendors offer this solution, as a way of managing the entire process of patching

[1]

Remediation

- Prioritizing
  - Prioritization of the vulnerabilities and correct remediation steps can help
    - System administrator from being overwhelmed with the results of the vulnerability scan
  - Discussions
    - How to prioritize the response include the capabilities of the technical staff and overall business goal of the organization
    - Include key stakeholders
      - Making them aware of your beliefs may create a buy-in for a future policy changes

[1]

Remediation

- Economics are used to drive the decisions of responding to vulnerabilities
  - Limited money, time, or personnel that could be utilized
- Nessus and OpenVAS
  - Provides visual references for overall severity of a discovered vulnerability on its results pages
  - OpenVAS Color-codes results and the options of sorting makes it easier to focus on the most important issues/ efficiency
- Common Vulnerability Scoring System (CVSS)
  - A framework designed to standardize the severity ratings for vulnerabilities
  - Provides accurate quantitative measurements so that users understand the dangers of the vulnerabilities
  - Members of academia, governments, and industries can collaborate using CVSS standard scoring system

[1,6]

Remediation

- Challenges in Remediation
  - Significant delays due to technical problems or costs
    - Continue working to complete the security requirement using alternative control
  - Include the nontechnical team members during the implementation process
    - This will encourage the adoption of the new alternate plan

[1]

Remediation

- **Communication/Change Control**
  - **Once the vulnerability scan results are received**
    - **Planning**
      - **You can not implement every recommendation. This only looks good on the surface and will cause problems if done all at once.**
      - **Must use a systematic approach**
    - **Systematic Approach**
      - **Establishes a formal communication and selects managing procedures.**
        - **Procedures are required so that service remain available, resources are used efficiently throughout changes, and ensures that the right changes are made.**
- **Change Advisory Board (CAB)**
  - **Approves major changes to company policies**
  - **Assist monitoring and assessment of change**
  - **Members often include entities that could be affected by a given change**

[1]

Remediation

- **Sandboxing/Testing**
  - **Sandbox**
    - **Can be used to test patches on multiple devices in a safe environment**
  - **Example**
    - **OpenSSL Project**
      - **Used to manage open source implementation of SSL and TLS protocols**
      - **September of 2016, released a security patch during it’s routinely updates**
        - » **The patch contained unsafe code, that was given a severity rating of “low” and could lead to a denial of service**
    - **The patch**
      - **Allowed for an attacker to execute arbitrary code**
      - **If the patch was tested in a sandbox before deploying across the enterprise**
        - » **It would have would have decreased the attack surface**
        - » **Prevented down time due to multiple patches**

[1,7]

Remediation

- **Inhibitors to Remediation**
  - **No matter the position or if a stakeholder of the organization has a plan for remediation, there will still be some obstacles**
  - **Challenges**
    - **Some challenges are from processes that depend heavily on IT systems**
    - **Other challenges could be due to an old policy that fails to correctly address the changes of technological landscape**
    - **There are also other common obstacles**
      - **Memorandum of Understanding**
      - **Service Level Agreement**
      - **Organizational Governance**
      - **Business Process Interruption**
      - **Degrading Functionality**

[1]

Remediation

- Memorandum of understanding (MOU)
  - Forms, duties, and expectations of all concerned parties
  - Vulnerability scan needs a clearly defined margin, and appropriate rules of engagement (ROE)
  - Reason
    - To control what can be done in the event of a vulnerability discovery and during the assessment.
  - Example
    - Using an informal MOU will cause ambiguity.
      - Imagine there is a vulnerability on your network with problems that intertwine onto another network that you're not able to control
        - » An MOU could cover these conditions so that the misconfiguration will not have a direct impact on services

[1]

Remediation

- **Service Level Agreement (SLA)**
  - **Is a contract from an outside provider, that can exist with a company or with an organization**
    - **It outlines the limits of services the outside provider can perform and their roles/responsibility**
  - **Many IT service provider offers their services based upon an SLA between them and the recipient**
    - **Example**
      - **If remedial action is not part of the providers agreement, providers cannot be compelled to perform them**

[1]

Remediation

- Organizational Governance
  - Corporate Governance
    - The system of processes and rules an organization uses to direct and control its operations
  - Objective would be to create a balance between the priorities of company stakeholders
    - Example
      - Has the authority to stop remedial actions if they negatively affect other business areas.
  - Communicating your actions are necessary
    - Allows leadership to factor the effects of your remedial actions with the others business issues to decide
    - Strong communication helps with timely decision-making

[1]

Remediation

- **Business Process Interruption**
  - **There is never a perfect time to apply a patch or take other remedial action**
  - **Production IT systems are used by many highly efficient businesses and industrial processes**
    - **Offers increased efficiency and reduced process times**
    - **Must be optimized to the business or process**
    - **Drawback**
      - **Systems have a higher chance of disruptions due to the optimized states**
    - **The fear of instability in the overall process causes leadership to avoid them or delay major updates**

[1]

Remediation

- **Degrading Functionality**
  - **Always try to avoid degrading production systems**
    - **E.g. Leadership might not accept quarantining key systems due to critical vulnerabilities**
  - **Leadership should have a plan for how much risk will be taking in order to remediate the vulnerability**
    - **If a remedial action breaks a critical application in a test environment**
      - **Instead of avoiding patching, you should focus on mitigating controls directed at the vulnerability**
      - **Must be done until a patch can be developed**

[1]

Ongoing Scanning and Continuous Monitoring

- Users should schedule automated vulnerability scanning to be performed daily
  - The number of scans performed daily is depended on the types of networks you operate, and your security polices.
  - Scanning tools should always be updated
- If critical vulnerabilities are found, they should be remediated within 48 hours
  - Some companies have started to offer web-based scanning due to the workload of maintaining software, reports, and libraries
  - Qualys and Tenable
    - Are both cloud enabled web application security scanners that provides increased scalability and speed for the network based on the subscription tier

[1,2,8]

Analyze Reports from a Vulnerability Scan

- Due to the large scale of modern networks, understanding a vulnerability scan output may be difficult
  - Tools such as Nessus utilize comprehensive reports that have visual tools and details of each vulnerability found
  - The tool produces a graph that uses color to rank the severity of the vulnerability and the distribution of the severity
- Review and Interpret Scan Results
  - Analysts should always review and comprehend the scan results before releasing them
    - Automated vulnerability reports are not perfectly accurate
  - Most importantly they should all identify false positive and exceptions to polices
    - After the process is complete, they must focus on prioritizing responses

[1]

Analyze Reports from a Vulnerability Scan

- **Identify False Positives**
  - **False positives are reporting a problem when there is not a problem**
    - **Vulnerability scanners often have false positives, which use time and resources to remediate**
    - **A 2% false positive rate would not be too bad for a small organization, but in a larger organization this would cause major problems**
    - **The problem could have been remediated but the notification was not successfully disabled**
  - **The Vulnerability scanner**
    - **Could be receiving the false positive from logical fault checks, NVT or other plug-ins**
    - **Scans are performed with certain assumptions**
      - **It might be difficult or impossible to write logic that applies perfectly to every system**

[1]

Analyze Reports from a Vulnerability Scan

- **Identify exceptions**
  - **There are always hidden exceptions**
    - **Due to the authors not being able to know the details of the user's networks**
    - **Their response is to create a rule that could be a false positive**
  - **Best Practice**
    - **Users should create their own test once a false positive is discovered**
- **Prioritize Response Actions**
  - **Networks should have accurate information**
    - **Allows for the technical team and company leadership to have confidence in their decisions**
    - **Helps with the efficiency with the appropriate course of action developed**
    - **Must have open lines of communication and vulnerability identified**
  - **After**
    - **The network can focus on prioritizing response actions, that will minimize the impact throughout the company**

[1]

Validate Results and Correlate Other Data Points

- Nessus
  - Receives feedback from the vulnerability scan reports
  - Provides a description of the weakness and multiple solutions are automated for the user to decide
- Compare to Best Practices or Compliance
  - Benchmarks that are available to improve network’s security
    - Industry, Academia, and Government
    - Ex. Most military networks standards are developed from Defense Information Systems Agency (DISA)
      - The Security Technical Implementation Guides(STIGs) are combined with National Security Agency(NSA) guides
      - These are the configuration standard used for the DoD information systems
      - All the guides provide steps required to strengthen software, endpoints, and network devices
      - There are many (STIGs) that are available to the public, but others require a DoD PKI certificate

[1]

Validate Results and Correlate Other Data Points

- **Reconcile Results**
  - **Taking notes explaining how you found and corrected a vulnerability will aid in the future**
    - **May be required depending on the industry you operate.**
  - **E.g. Should include steps required to configure a device, validate its configuration, verify its operation and test vulnerabilities**
  - **If your network activity is examined in an investigation, both Nessus and OpenVAS provide ways to track the actions performed on network devices**

[1]

Review Related Logs and/or Other Data Sources

- Event logs and network data are vital when reviewing reports
  - Offer the ability to compare listening ports, running services, and open connections with those that are authorized
- Historical network and service data
  - Are used with the vulnerability scan outputs and will provide you with a few benefits
- Benefits
  - It verifies the logging mechanism is capturing the activities related to the vulnerability scans
  - If there are patches or changes you have made, you can see the history of those changes on the network
  - Logs may show if the found vulnerabilities have been corrected
- Security Information and event management (SIEM) tools
  - Are utilized when beginning the process of reviewing
  - Can visualize all scanning activities, which provides a large resource for validating data

[1]

Determine Trends

- Trending gives users the ability to track the progress of vulnerabilities in the network that have changed
  - Using is either SIEM or other software
- Benefits
  - Improves the efficiency of the security teams, by allowing them to customize their threat reducing strategies
  - Can be used to detect if corrections are established and are effective
- Trouble ticket software
  - Allows users to track the completion of problems

[1]

Quiz

Chapter 6

Question #1

- **Which of the following is an open source vulnerability scanner that lacks a graphical user interface?**
  A. Open VAS
  B. NASL
  C. Nessus
  D. Nikto

[1]

Answer #1

- D
  - Nikto is a web server vulnerability scanner with only a command-line interface.
  - NASL is not a vulnerability scanner but rather the Nessus Attack Scripting Language.

[1]

Question #2

- **When prioritizing the remediation of newly discovered vulnerabilities, you should consider all the following except which?**
  A. Criticality
  B. SCAP score
  C. Difficulty of implementation
  D. CVSS

[1]

Answer #2

- B
  - The Security Content Automation Protocol (SCAP) defines the manner in which security software (such as a vulnerability scanner) communicates information about flaws and security configurations.
  - It plays no role in the prioritization of remediation.
  - The Common Vulnerability Scoring System (CVSS), on the other hand, can be used to determine the criticality of vulnerabilities.

[1]

Question #3

- **All the following might be inhibitors to the remediation of vulnerabilities except which?**
  1. **SLAs**
  2. **TLAs**
  3. **Governance**
  4. **Business processes interruption**

[1]

Answer #3

- B
  - Memorandums of understanding (MOUs), service level agreements (SLAs), organizational governance, business process interruptions, and degradation of functionality are all important factors that could delay remediation.

[1]

Question #4

- Which of the following statements is true about false positives?
  A. False positives are not generally a problem, but true negatives might be.
  B. False positives are indicative of human error in an automated scanning process.
  C. False positives are more problematic for smaller organizations than larger ones.
  D. False positives waste organizational resources.

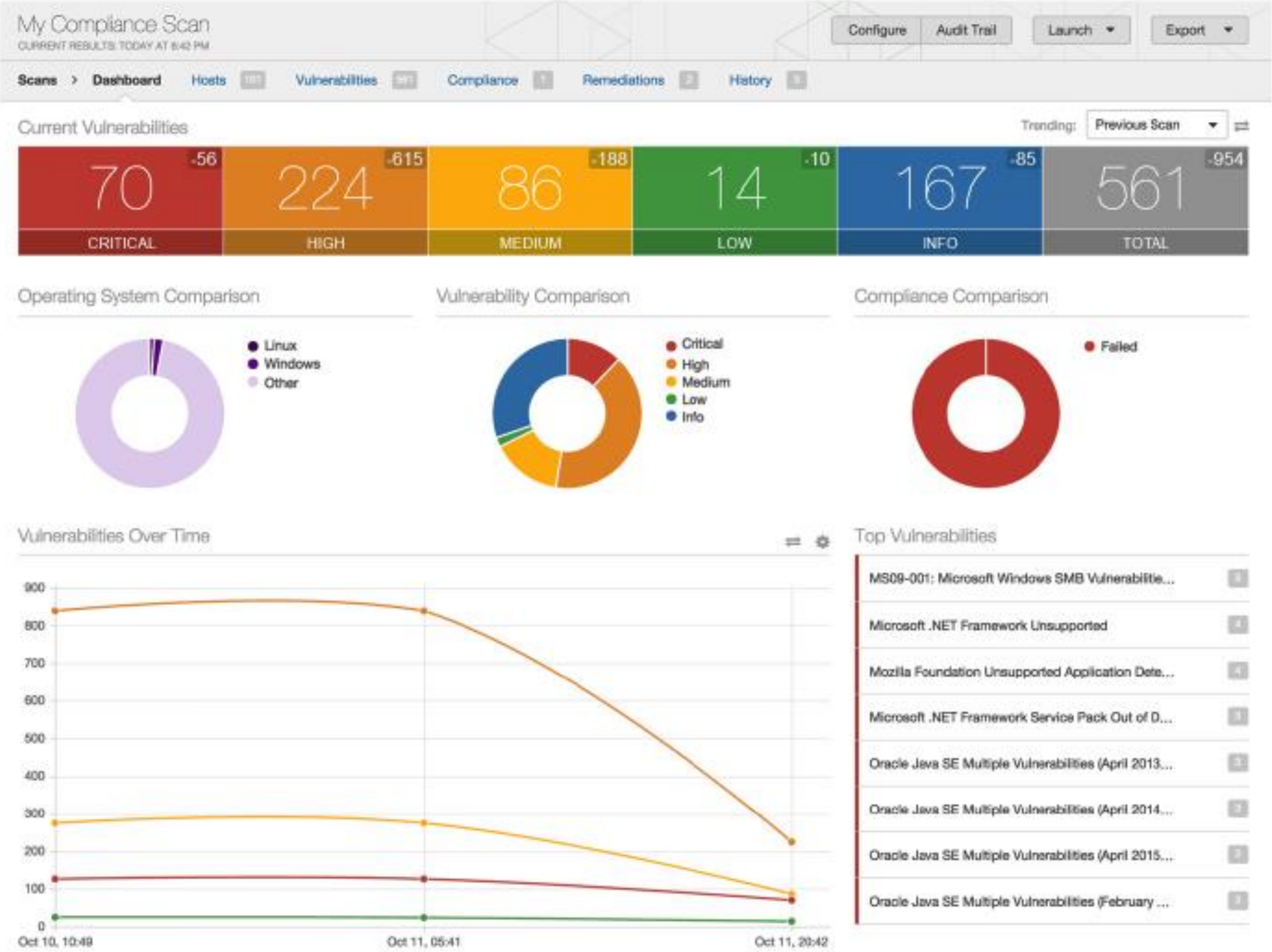
[1]

Answer #4

- D
  - False positives typically result in wasted resources because they have to be manually investigated to ensure they are not real issues.

[1]

Use Image for Questions 5 - 8



My Compliance Scan

CURRENT RESULTS TODAY AT 8:42 PM

Current Vulnerabilities

CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL
70	224	86	14	167	561
-56	-615	-188	-10	-85	-954

Top Vulnerabilities

- MS09-001: Microsoft Windows SMB Vulnerabilitie...
- Microsoft .NET Framework Unsupported
- Mozilla Foundation Unsupported Application Dete...
- Microsoft .NET Framework Service Pack Out of D...
- Oracle Java SE Multiple Vulnerabilities (April 2013...
- Oracle Java SE Multiple Vulnerabilities (April 2014...
- Oracle Java SE Multiple Vulnerabilities (April 2015...
- Oracle Java SE Multiple Vulnerabilities (February ...

[1]

Question #5

- **All the following might be account for the sudden drop in vulnerabilities on October 11 except which?**
  A. **The team decided to prioritize remediation by difficulty of implementation.**
  B. **The tool was tuned to reduce the number of false positives.**
  C. **A malfunctioning software update server was repaired on the morning of October 11.**
  D. **The team decided to prioritize remediation by criticality.**

[1]

Answer #5

- D
  - The drop in critical vulnerabilities between the last two scans was only 56 (for a 44% improvement), compared to a drop of 615 (or 73%) in high vulnerabilities and 188 (or 67%) in medium vulnerabilities.
  - The greater drops in less-critical vulnerabilities make it less likely that focus was on criticality.

[1]

Question #6

- **If your performance was measured strictly in terms of the total number of vulnerabilities, what might you do on October 12?**
  - **A. Prioritize remediation by criticality.**
  - **B. Focus on “high” vulnerabilities.**
  - **C. Prioritize remediation by difficulty of implementation.**
  - **D. Suspend change management protocols.**

[1]

Answer #6

- C
  - The fastest way to reduce the total count of vulnerabilities is to go after the easier ones to fix first.
  - It is important to note, however, that this may not be the most effective way to reduce the overall risk to the organization, because the easier fixes might not be the ones that mitigate the greater risks.

[1]

Question #7

- **What should be the likeliest impediment to correcting the 70 remaining "critical" vulnerabilities?**
  A. **The organization lacks governance processes related to vulnerability management.**
  B. **The vulnerabilities exist in servers that are needed for mission-critical business processes.**
  C. **All pertinent MOUs have expired or been rescinded.**
  D. **The organization has no SLAs in place.**

[1]

Answer #7

- B
  - Mission-critical business processes often pose challenges to remediation because of the fixes need to take place after business hours and typically require extensive testing and rollback planning.
  - The lack of governance, MOUs, or SLAs would likely expedite rather than hinder remediation.

[1]

Question #8

- **What could most likely lead to an increase in the number of vulnerabilities detected during a scan on October 12?**
  A. **Software security patches**
  B. **Further tuning of the vulnerability scanner**
  C. **Vulnerability scanner updates/ plug-ins**
  D. **Network device configuration improvements**

[1]

Answer #8

- C
  - Vulnerability scanners are periodically updated to respond to newly discovered vulnerabilities.
  - These tools can also be calibrated or tuned to change the rate of false positives, though this process can sometimes blind the scanner to real vulnerabilities.

[1]

Scenario for Questions 9-12

- You are asked to start performing vulnerability scans as part of a broader vulnerability management process. You have been running scans every 48 hours for the last couple of weeks and have noticed a high rate of false positives on your end-user workstations. More concerning to you is the fact that several critical vulnerabilities exist in both the primary and backup database servers used by the accounting department. With the end of the fiscal year approaching, you are pretty sure that the business impact will be considered too high to allow for remediation.

[1]

Question #9

- **How might you best be able to reduce the high rate of false positive results?**
  - A. Validating the logic of the checks against your IT environment
  - B. Using a different vendor’s scanner to double check your results
  - C. Limiting your vulnerability scans to the critical hosts on your network
  - D. Prioritizing your response actions

[1]

Answer #9

- A
  - Sometimes the logic that a check or plug-in uses is flawed or makes bad assumptions about your environment.
  - It is sometimes helpful to examine the checks that yield the highest false-positive rates and look for opportunities to tune them.
  - Adding a second scanner will probably increase the total number of false positives, while the last two responses do nothing to reduce that number.

[1]

Question #10

- **Apart from reducing the rate of false positives, how else might you deal with them?**
  A. **Correlate them to other data points.**
  B. **Compare them to best practices.**
  C. **Prioritize your response actions.**
  D. **Review related logs.**

[1]

Answer #10

- C
  - If you are unable to reduce false-positive rates, one option is simply to prioritize other results higher in terms of taking action.
  - Over time, analysts become adept at identifying the likely false positives and could just move them to the bottom of the queue.
  - The risk in doing this is that, unless you are certain that the result is unimportant, you risk deferring a real issue indefinitely.

[1]

Question #11

- **Which of the following actions is least likely to help you get permission to remediate the critical vulnerabilities found on the database servers?**
  1. **Scheduling the remediation on a weekend**
  2. **Implementing an SLA for your organization**
  3. **Using a sandbox to test the remediation process**
  4. **Presenting a rollback plan in case the remediation fails**

[1]

Answer #11

- B
  - Service level agreements (SLAs) almost always exist between an organization and an external service provider, so one wouldn’t help you get permission.
  - The other three actions, particularly if they are taken together, can present a compelling case to senior management.

[1]

Question #12

- What should you do with your growing library of vulnerability scan reports?
  A. Ensure you keep the last two sets of results.
  B. Present them to your change advisory board.
  C. Keep them for regulatory compliance.
  D. Track how vulnerabilities in the network have changed over time.

[1]

Answer #12

- D
  - Trend analysis improve context and allows your security response team to tailor its threat mitigation strategies to its efforts more efficiently.
  - Depending on your specific organization’s regulatory environment, you may be required to keep some of these reports.
  - However, because this is not universally true, keeping the reports for regulatory compliance is not the best answers.

[1]

References

1. Maymí Fernando, and Brent Chapman. CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). McGraw-Hill Education, 2018.
2. Tenable, 2020.
3. Koromicha. How to Scan a Remote Host using Nessus Vulnerability Scanner. Kifarunix, 2018.
4. New OpenVAS logo. Greenbone (2019).
5. Rai, Subhashini. How To Find Web Server Vulnerabilities With Nikto Scanner. Hackers Online Club, 2019.

References

6. Albeniz, Ziyahan. CVSS: Characterizing and Scoring Vulnerabilities. Netsparker, 2019.
7. Sandbox, 2020.
8. Miller, Kim. Qualys training now available. UW-Madison Information Technology, 2020.