Lab 11

Regularly Monitor and Test Networks

Regularly monitor, evaluate and test security systems and processes

Summary:

New vulnerabilities are regularly found and exploited, so it is essential that system components, processes and custom software are regularly tested. Documented processes must be implemented to detect and identify all unauthorized wireless access points on a quarterly basis. Internal and external network vulnerability scans must be performed by qualified personnel at least quarterly and after any significant change in the network (e.g. new system component installations, changes in network topology, firewall rule modifications and product upgrades). Intrusion detection/prevention techniques should be used to identify and/or prevent unauthorized network activity, and a change detection mechanism should be employed to perform weekly critical file comparisons, and to alert personnel to unauthorized system modifications.

Contents:

Summary: 1

Contents: 1

Lab Setup: 2

PCI_DSS Mapping: 2

Audit: 2

Policy option we need to confirm: 2

Audit HowTo: 3

ToDo: 7

References: 8

Lab Setup:

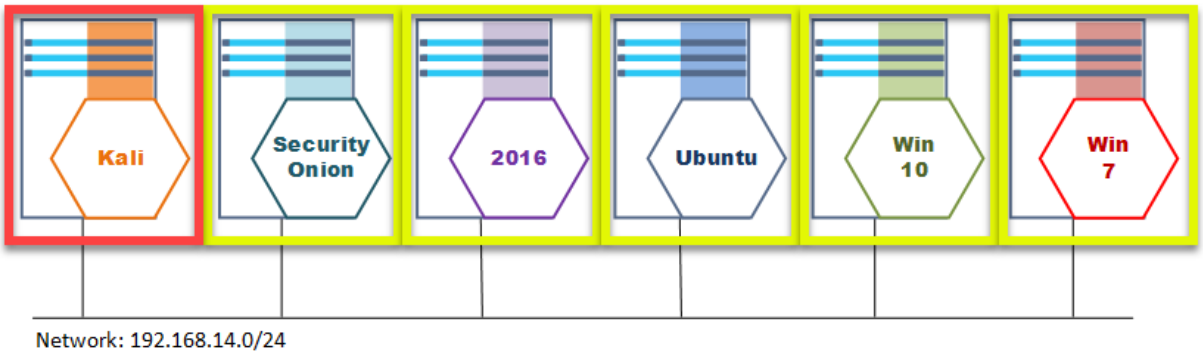
PCI_DSS Mapping:

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.
For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor

1. Verifies the most recent scan result was a passing scan
2. The entity has documented policies and procedures requiring quarterly scanning
3. Vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s).

For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.

11.2.1 Perform quarterly internal vulnerability scans and rescans as needed until all "high risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.



Audit:

Policy option we need to confirm:

In this lab we will be running our quarterly vulnerability scan to confirm that known high risk

vulnerabilities have been patched or otherwise mitigated.

Audit HowTo:

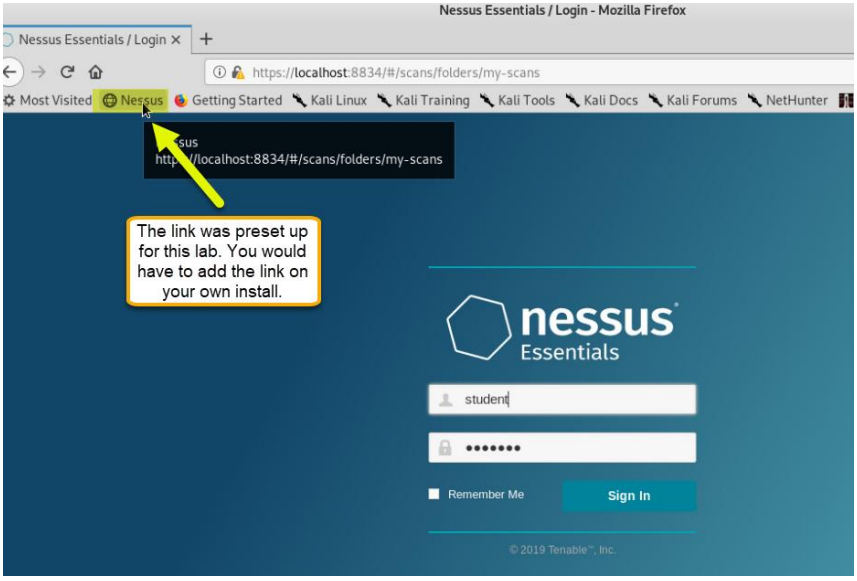
We will be using the Nessus vulnerability scanner to accomplish this task.

Step 1) On the Kali VM open up a browser and open Nessus.

In the toolbar select the browser:

Launch Nessus:

- Username: student
- Password : student

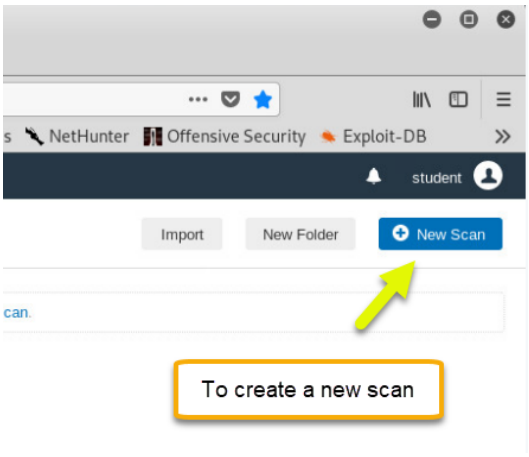


Step 2) Create a new scan.

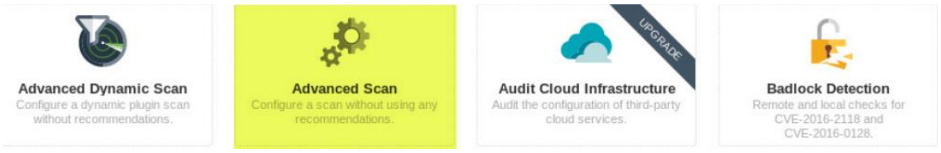
Nessus lets us organize resources into scans. For this lab we will be doing a vulnerability scan of the full 192.168.14.0/24 subnet (all machines).

Note: We are using the free version of Nessus and as such will be using the “Advanced Scan” plugin. You may have noticed when you created a new scan that there is an “Internal PCI Network Scan” plugin that comes with the full licensed version of Nessus. As the scan setup is exactly the same we can learn what we need to use the free version and apply it to the full version easily.

1. New Scan (Upper righthand corner)

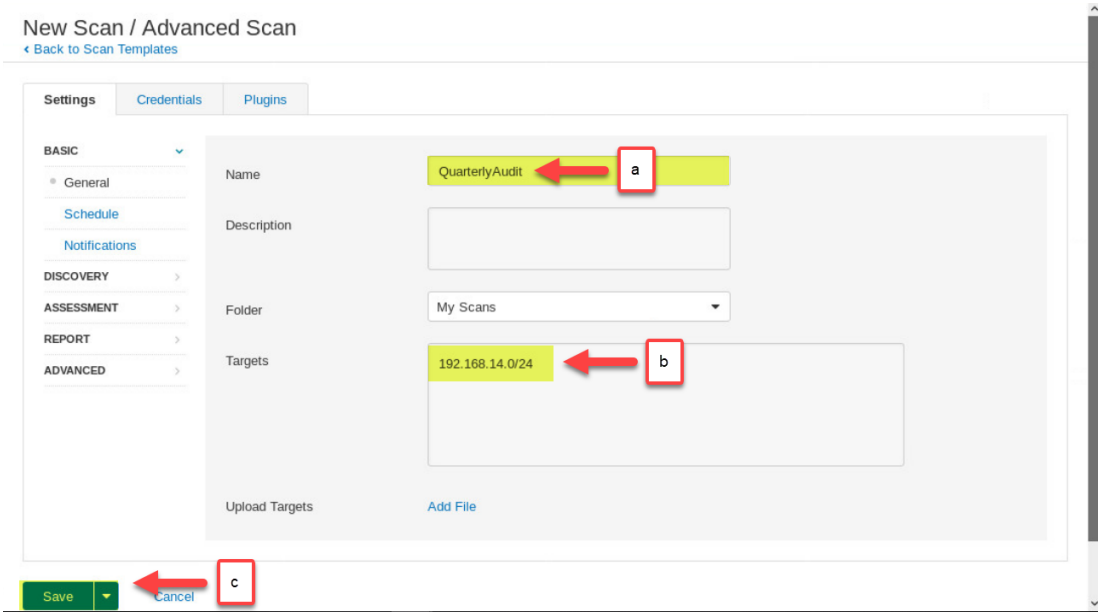


2. Select “Advanced Scan”



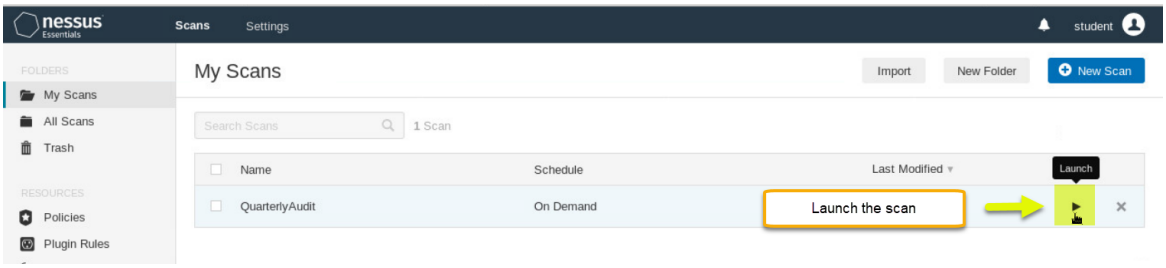
3. We need to define some information about our scan.

    a. We need to name our scan
        - QuarterlyAudit
    b. We need to set the IP address range of the target machines
        - 192.168.14.0/24
    c. We need to save the scan.

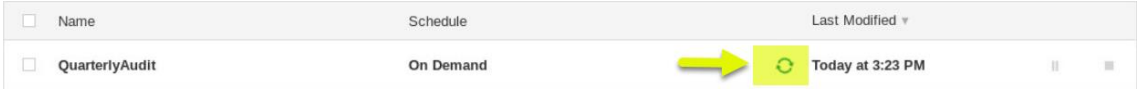


Step 3) Run the scan against the target.

1. Select “Launch”

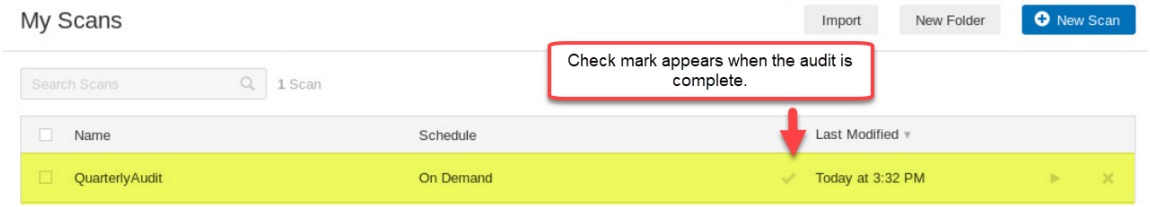


2. Wait for the scan to complete. Note: This will take a while, The circle with the two arrows will be spinning as it continues to run.



Step 4) Review the audit results.

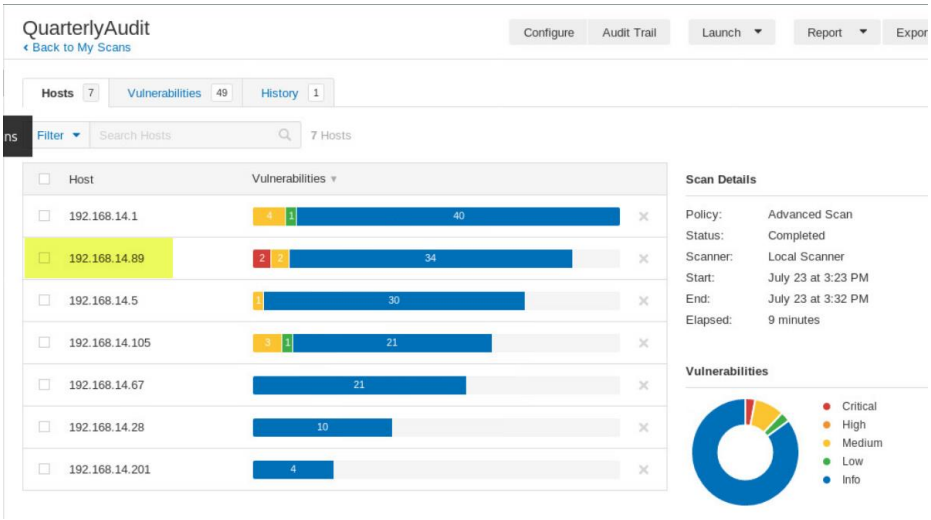
1. Click the line of the audit you want to see the report for (Note: In this case we only have one).



2. For each of the hosts in the network we get a vulnerability report. The vulnerability score for an address is computed by adding up the number of vulnerabilities at each severity level and multiplying it with the organization's severity score.

   The default severity scores at each level are:
   - Info - 0
   - Low – 1
   - Medium – 3
   - High – 10
   - Critical – 40

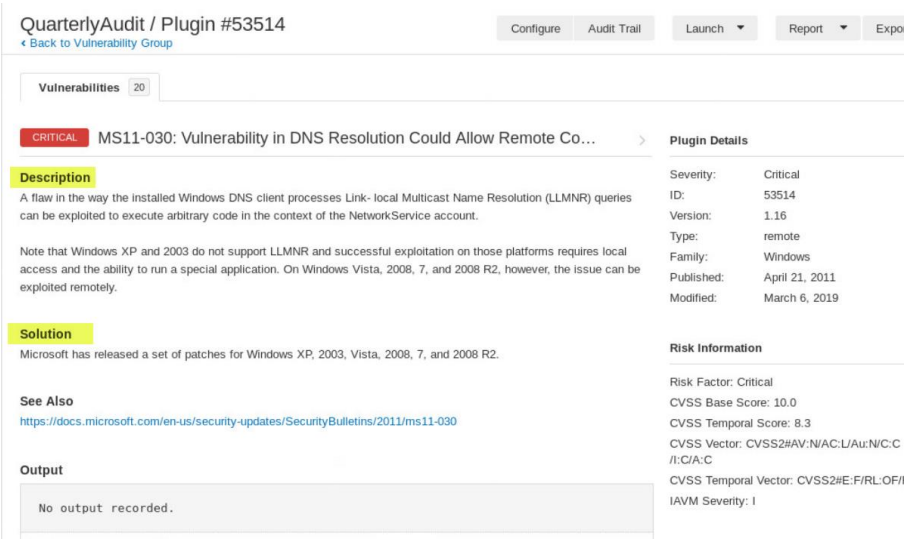
   Let's take a look at the 2 "Critical" vulnerabilities found on "192.168.14.89"



3. We need to select the “Mixed” box at the top as there were multiple issues found using the “Microsoft Windows” Plugin.

4. Read the “CRITICAL” lines of the report.

5. In each of the report lines there is a description of the vulnerabilities and a recommended solution to the issue.



ToDo:

We want to fix as many vulnerabilities as possible to reduce risk. Issues that are simple configuration mistakes can be corrected with no additional cost to the client.

Look at the report results for “192.168.14.105” and make recommendations on how to fix the “Medium” vulnerabilities.

1. SSL Certificate Cannot Be Trusted.
   Solution: _____

2. SSL Medium Strength Cipher Suites Supported (SWEET32).
   Solution: _____

3. SSL Self-Signed Certificate.
   Solution: _____

References:

https://www.tenable.com/solutions/pci