**IT357 Tools and Techniques in Defensive Security**
**Assignment 4 – Vulnerability Scanning**
**14 answers – 50 pts**

---

**Objective**: To learn to use a vulnerability scanner to find weaknesses in systems and use the results to determine how to patch those weaknesses.

**Preparation**:

For this assignment, you will only use the Ubuntu-LAN, LAMP-D, and Win10-LAN VMs.

Turn off Win10-LAN firewall for all interfaces (Domain, Private, Public).

**Part 1: Scanning**
This section will use Nessus Essentials, a limited functionality free version of the popular vulnerability scanner Nessus.

1. Explain in your own words one scenario in which you would deploy a vulnerability scanner. Be detailed in your answer, a good answer will require a short paragraph.

Q1) Answer (3 pts): Once I was surfing on internet to download a game, at that time I visited couple of websites and finally I found what I was looking for and I started to download that game. After downloading I opened the zip folder and saw into it. I ran the setup file and things started getting worse and the system started rebooting itself while the software froze. At that time, I launched scanning and detected software vulnerabilities and erroneous configurations in in the game. Finally, after completing scan the scanner automatically deleted file.

2. Note down the IP addresses of the LAMP-D and Win10-LAN VMs:

IP address of LAMP-D: 127.16.1.21

IP address of Win10-LAN: 192.168.1.105

3. You will first need to register for an activation code for Nessus Essentials on the Tenable website using the following link:

   https://www.tenable.com/tenable-for-education/nessus-essentials?edu=true

   Use your real name, your *ilstu.edu* email address, and "Illinois State University" as the Company Name.

The activation code for Nessus Essentials will be sent to the email address you submitted.

Note: Be sure to check your junk mail folder. If you still have not received the activation code after several minutes, you can simply repeat the registration process using the link above.

4. Log in to Ubuntu-LAN and open a terminal window and run the following command to apply your activation code.

   - `sudo /opt/nessus/sbin/nessuscli fetch --register` *`xxxx-xxxx-xxxx-xxxx`*

   The *"xxxx-xxxx-xxxx-xxxx"* in this case will be the activation code that was sent to your email. Executing this command will both activate your instance of Nessus Essentials and download the latest updates. Once this has completed, run the following command to restart the Nessus service:

   - `sudo systemctl restart nessusd`

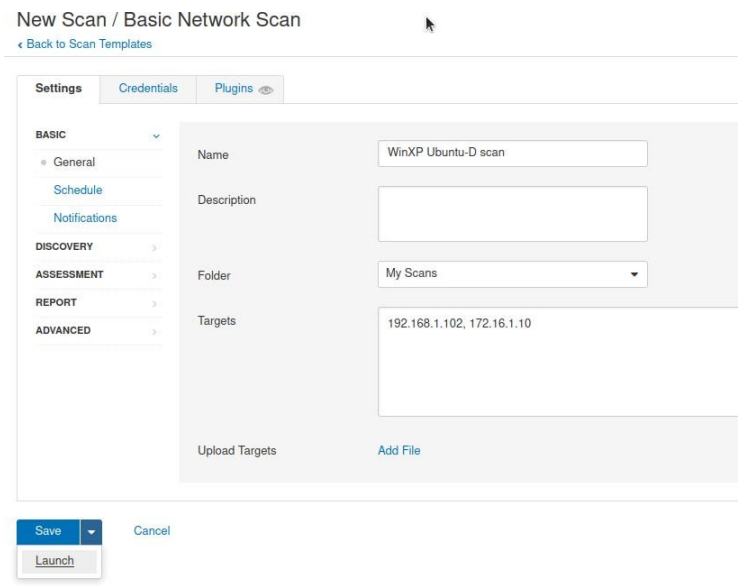
   Use Firefox and browse to **https://localhost:8834**. Then, login to the web interface for Nessus with the credentials provided.

   **Note: Be patient as Nessus may take about 10 or 12 mins to initialize the newly downloaded updates after restarting the service. So get up, stretch, grab a beverage or whatever it is you do when you're not staring at a computer screen.**

   a. Click the "New Scan" button in the upper right-hand corner of the My Scans page (you may need to scroll the browser window to the right).

   b. Click the "Basic Network Scan" button (you may need to scroll back to the left). Give your scan a meaningful name and enter the IP addresses of your LAMP-D and Win10-LAN VMs with a comma in between, (e.g., *a.b.c.d, w.x.y.z*) into the Targets box.

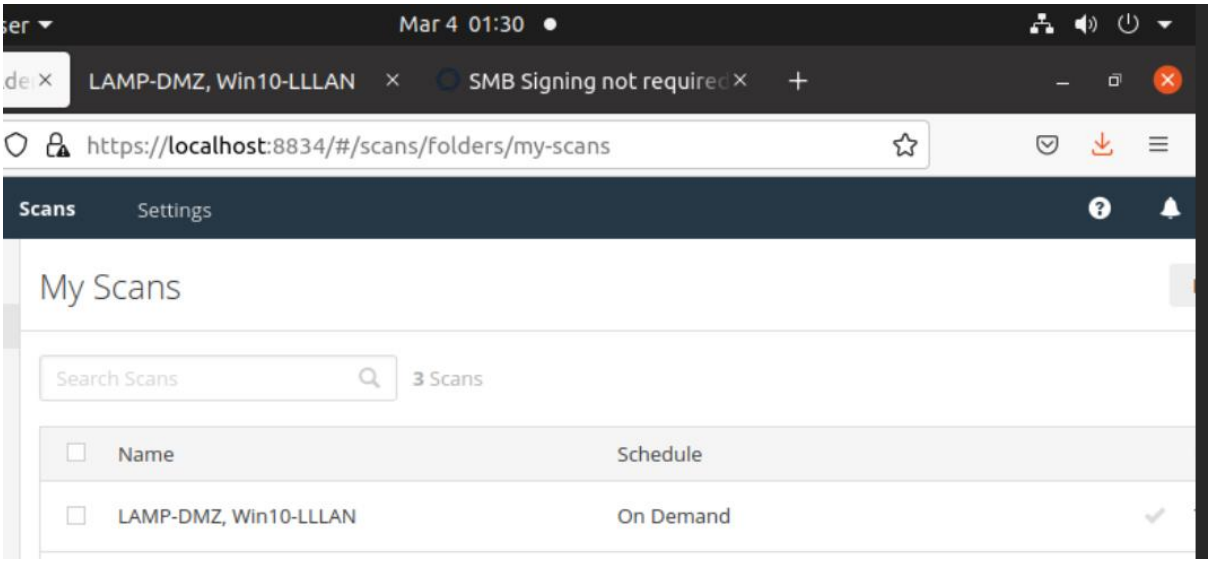
   c. Click the down arrow next to the Save button and click Launch




d. Take a screenshot of the next screen, showing that the task was created/running. (Note: Use the Windows Snipping tool to snip out the relevant portion of the screen shot so that it is easily viewable).

Q2) Take a screenshot of the task running. (3 pts)

[Insert Screenshot here]

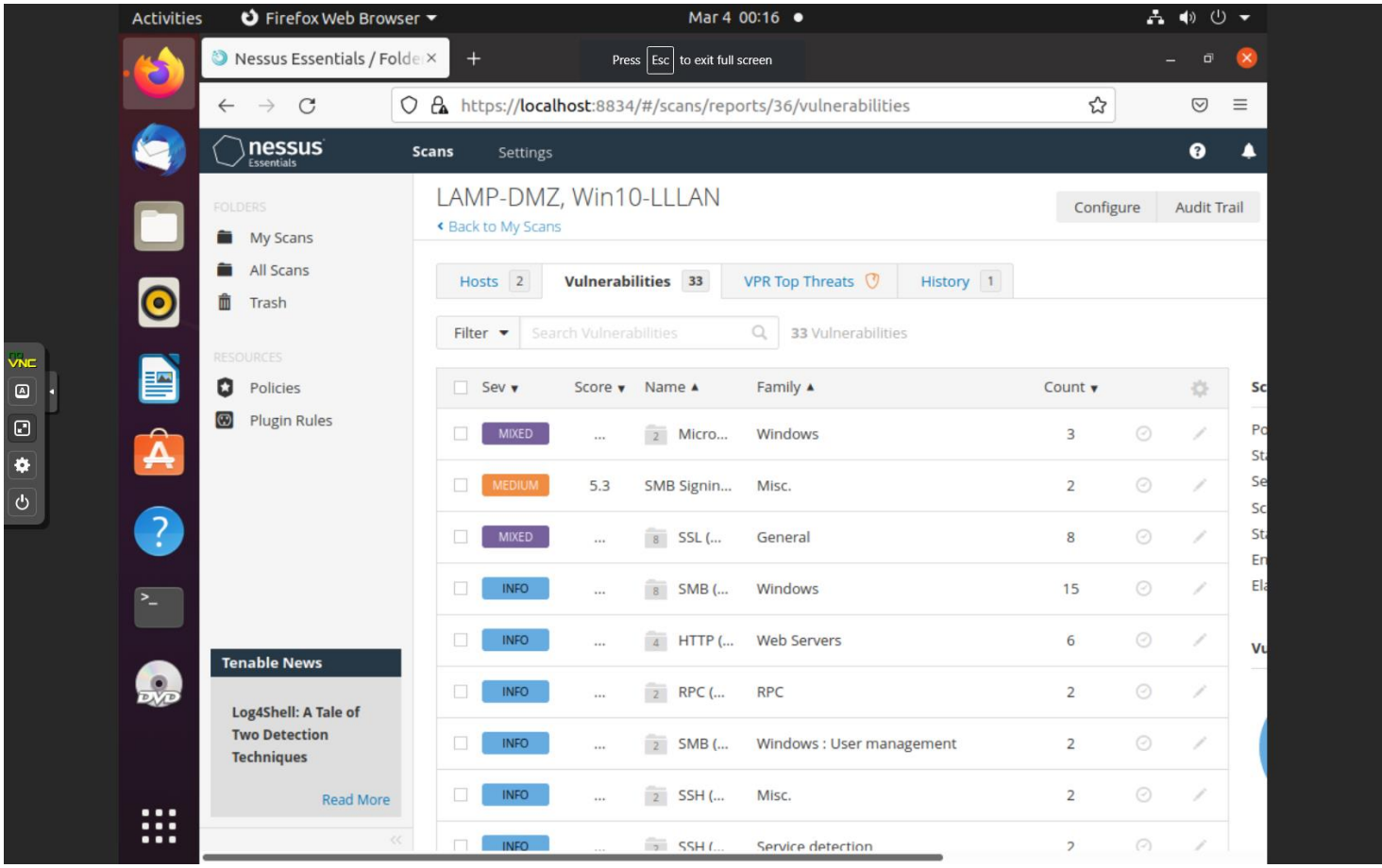


**The scan will take a few minutes to run, so go back to doing whatever you were doing while waiting for Nessus to initialize.**

e. Once the scan is done a greyed out check mark will appear near the Last Modified date. Click on the scan name to view the scan results.

f. Click on the Vulnerabilities tab of the scan results.

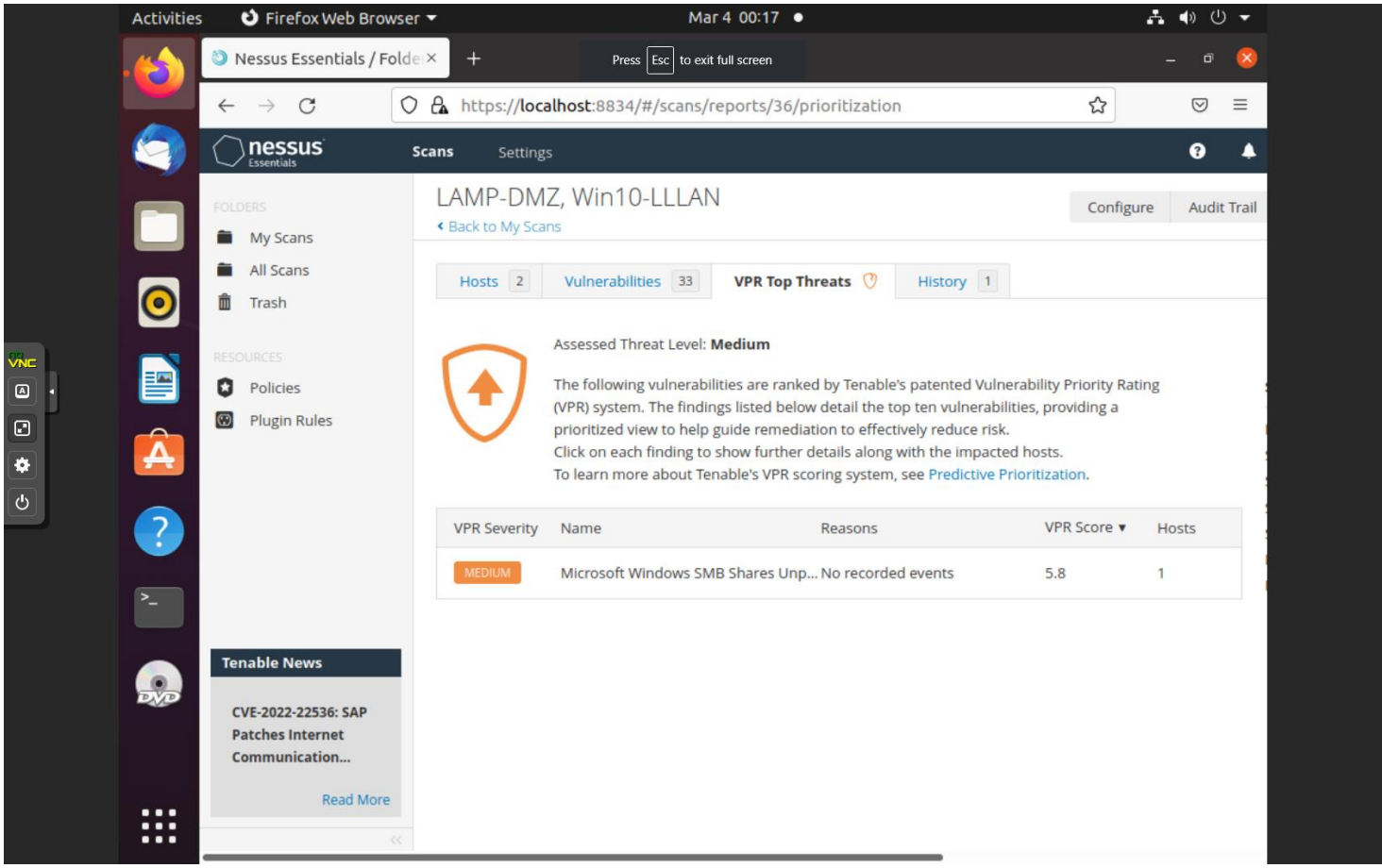
Q3) Take a screenshot of the identified list of vulnerabilities. (3 pts)



[Insert Screenshot here]

g. Click on the VPR Top Threats tab of the scan results.

Q4) Take a screenshot of the identified list of top threats. (3 pts)



5. Click on the “Report” dropdown at the top right and choose HTML. On the Generate HTML Report window that opens, choose Custom from the dropdown. Keep all the default options that are selected and click the Generate Report button. Save the file, email it to yourself, and attach it to your ReggieNET submission, along with this document. Please DO NOT zip the two files, attach them separately.

   Q5) Did you email it to yourself and did you attach it to this ReggieNET submission? (3 pts)

   **Yes**

6. Discuss two specific vulnerabilities found on the Win10-LAN scan, and two found on the LAMP-D scan. Be sure to name the vulnerability, provide a CVE number if applicable, discuss the severity, and a possible solution to the problem.

   a. (3 pts) Q6) Win10-LAN Answer 1: Microsoft windows SMB shares Unprivileged Access -medium vulnerability.

      The remote has one or more windows share that can be accessed through the network with the given credentials depending on the share rights it may allow an attacker to read/write credentials data

b. (3 pts) Q7) Win10-LAN Answer 2:
   Signing not required medium type of vulnerability .
   - Signing not required on the remote SMB server. An unauthorized, remote attacker can exploit this to conduct man in the middle attacks against the SMB server

c. (3 pts) Q8) LAMP-D Answer 1:
   There are couple of mix vulnerabilities which is medium and Info medium is SSl certificate cannot be trusted , Info is SSL certificate commanName mismatch

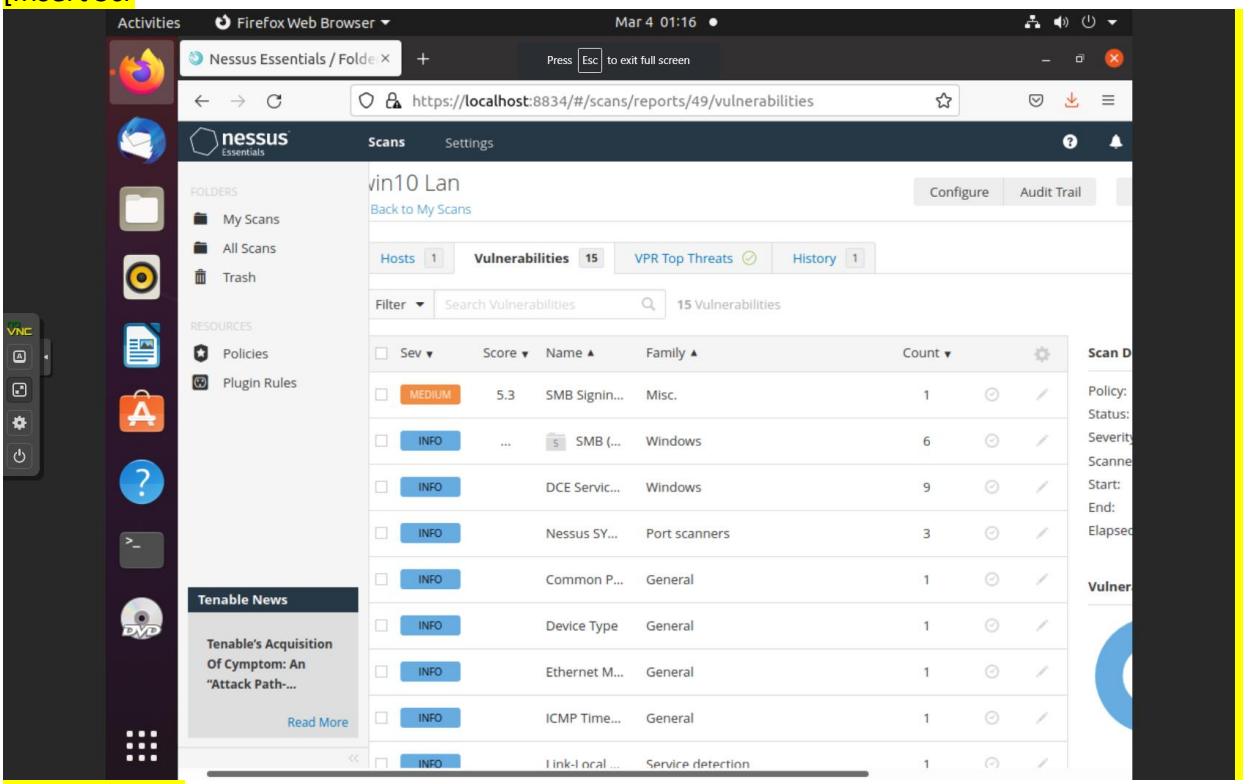
d. (3 pts) Q9) LAMP-D Answer 2:
   SBM signing not required which is medium type of vulnerabilities reason for man in middle attack

7. Patch the Win10-LAN VM and bring it up to the most secure possible configuration.
   **Hint:** You'll want to see if there are any available OS updates.

8. Once updated, use the My Scans page in Nessus to create a new scan, this time ONLY scanning the updated Win10-LAN VM, and compare these results with the initial scan.

a. Q10) Take a screenshot of the Vulnerabilities tab of the new report. (3 pts)

[Insert Scr




eenshot here]

b. In your own words, explain:

i. (3 pts) Q11) What specific vulnerabilities were fixed? Be sure to review only the Win10-LAN vulnerabilities from the first report.

-Enforce message singing in the host configuration on windows which is the policy setting

ii. (3 pts) Q12) Are there any remaining vulnerabilities? List them briefly.

- Win 10 lan have total 15 vulnerabilities left before this it has 18 total vulnerabilities

iii. (3 pts) Q13) How would you fix the remaining vulnerabilities?

-Update the system and check again and run vulnerability scanner.

9. Discuss specific steps you could take on the LAMP-D VM to bring it to its most secure state. These may include patching or other actions. You **DO NOT** need to perform the actions, just explain specific things that could be done.

Q14) Answer: (3 pts)
Vulnerabilities scanner, update system, run patching, run firewall and scan network time to time. Disable unnecessary functionality, Protect the guest operating system, Consider UEFI secure boot
.

Submit **BOTH** this PDF and the HTML Nessus report on ReggieNET.

**SAVE THIS AS A PDF, SUBMIT THE DOCUMENT ON REGGIENET**