



Lab 1.3.4 Vulnerabilities and Exploits

Objective

In this lab, the students will complete the following tasks:

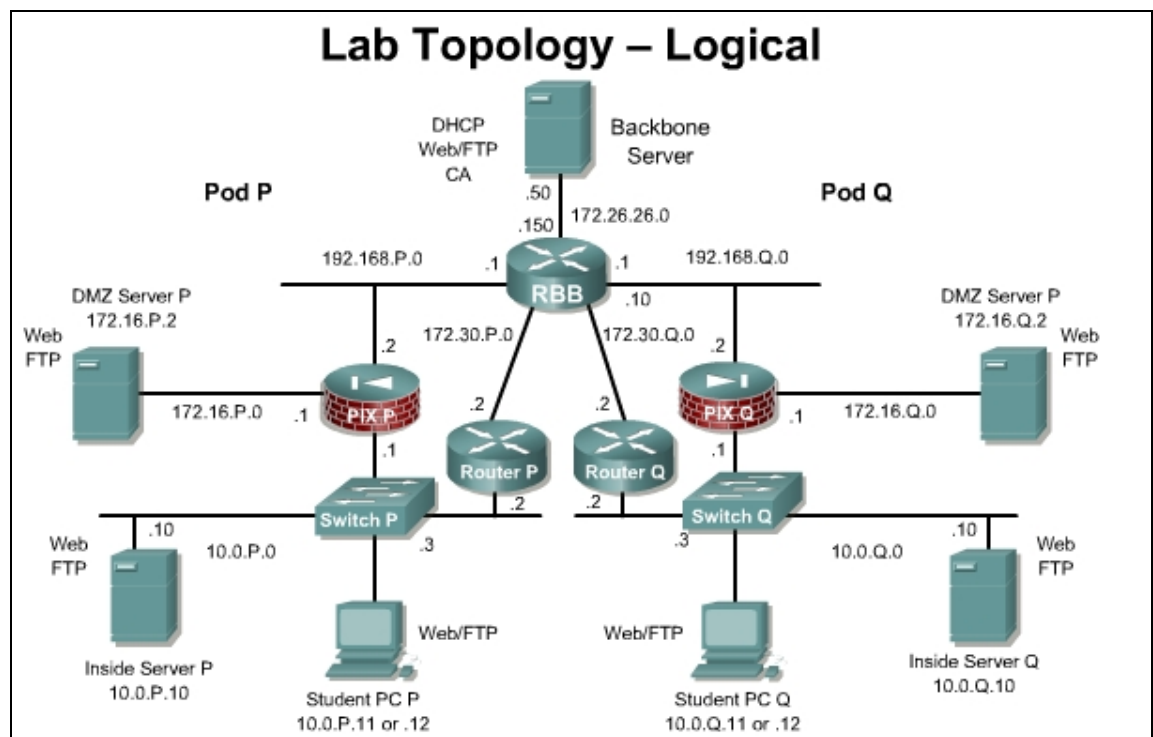
- The use of common network mapping tools, hacking programs, and scripts on a LAN and across a WAN.
- Where vulnerabilities are discovered, propose a fix or solution to the problem.

Scenario

A small company is using the topology discussed in the following topic. Assume that minimal security measures have been implemented. Discover vulnerability in any of the devices or software used in the network. This includes routers, switches, workstations, printers, servers, hubs, and wiring. The students will demonstrate this solution in the lab environment for observation by peers and the instructor.

Topology

This figure illustrates the network environment that will be used in this lab.



Preparation

Use the standard lab topology and startup router configuration for the Pod router. Configure the additional devices with the appropriate network address, gateway, and subnet mask if required.

Part I: Students or small groups will be stepped through the process of using a bootable Linux Security CD on the Student PC. Programs such as Nessus and Ethereal will be used to scan for vulnerabilities on the Pod router, Inside server, or other select targets on the lab topology. This lab is written to use the Local Area Security Linux CD.(200MB)

Part II: Students or small groups will conduct a search for one known vulnerability or exploit, or utilize one of the many tools on the Linux security CD. This lab can be repeated to allow students to experience each type of tool. Some of the common tools used are listed in the following:

- Reconnaissance
 - Network/packet sniffers or port scanners
 - Key loggers
 - Simple Network Management Protocol (SNMP) or other network management/configuration tools
- Access
 - Java, ActiveX or cgi scripts
 - Self executing software
 - Robots and control daemons
 - SNMP or other network management/configuration tools
 - Password tools such as brute force, dictionary, and so on
- Denial of service
 - Ping of death
 - SYN flood, User Datagram Protocol (UDP) bomb, and so on

Commands

Command	Description
<code>ifconfig</code>	Display the IP address settings for a Linux device
<code>ping</code>	Verify Layer 3 connectivity to another device.
<code>sudo bash</code>	Change to the root user in linux
<code>telnet</code>	Initiate a telnet connection with a remote device.

For this lab students can use any host PC or server for demonstration or implementation.

Tools and resources

To complete this lab, students should have access to the following equipment:

- Standard lab topology setup
- Bootable Linux security CD (Local Area Security Linux or equivalent)
 - There are numerous bootable Linux CDs available such as Local Area Security Linux, Knoppix STD, F.I.R.E., Auditor security collection, and many others. They range in size from 50MB to 750MB.
 - A bootable Linux Security CD allows a student to access many tools without the installation issues on Windows platforms.
 - The images run in RAM and typically do not affect the operating system on the PC.

Additional materials

The curriculum lists several excellent Web links that will help the student understand the material presented in these labs.

Other resources include these websites:

- <http://www.2600.com/>
- <http://www.cert.org>
- *Hacking Exposed: Network Security Secrets & Solutions*, Fourth Edition by [Stuart McClure](#), [Joel Scambray](#), [George Kurtz](#)
- <http://www.localareasecurity.com/>
- <http://www.moser-informatik.ch>
- <http://www.nessus.org>
- <http://www.ethereal.com/>

Safety

Students and instructors must be careful not to violate any local, state, or federal laws as well as school or university network security policies. Using a bootable Linux security CD provides the tools with minimal risk and configuration requirements. However, it may be necessary to re-image or reload a workstation, device, or server operating system (OS) in order to completely eliminate any malicious code, virus, Trojan horse, or control daemon encountered in this lab.

Part I:

Step 1 Boot the Student PC (laptop) with the Linux CD

The Student PC will receive an address from the pod router DHCP server. Make sure the starting configuration is loaded on the Pod device, which has the DHCP server running.

- On the powered down Student PC or laptop, insert the LAN Security CD into the CD ROM drive.
- Power the Student PC or laptop
- Assure the laptop boots into the Linux environment. This procedure will vary depending on the PC and laptop brand and current BIOS configuration. The Linux distribution may not support all hardware properly. If some of the PC hardware components are not detected, load the Linux distribution on another PC or laptop.
- Open a Linux shell. **Apps>Shells>Bash** and verify the PC has an IP address in the 10.0.P.0/24 network range.

```
root@0 [root] $ ifconfig
```

Step 2 Execute Nessus via GUI or CLI

GUI menu steps

- Right click on the desktop, and navigate to **Apps>I.a.s>nessus**
- Left click on the **nessus** application

CLI menu steps

- Open a Linux shell. **Apps>Shells>Bash** Become root in your terminal if not already root.

```
root@0 [root] $ sudo bash
root@0 [root] #
```

- First, start the nessus daemon and put the process in the background.

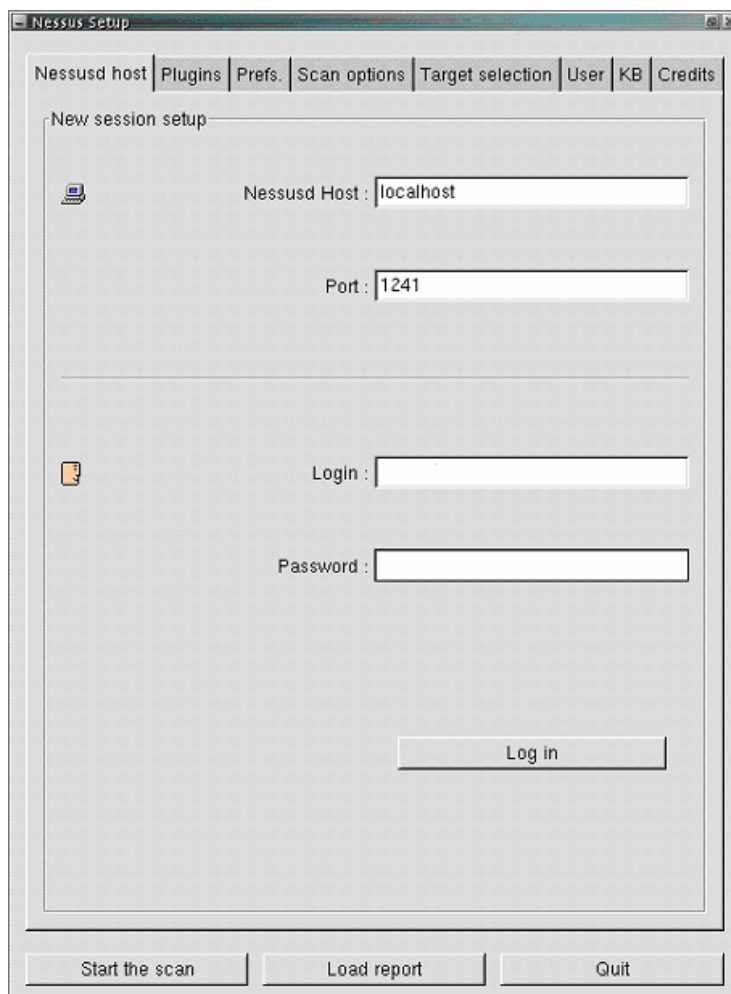
```
root@0 [root] # nessusd&
```

- Launch the nessus client.

```
root@0 [root] # nessus&
```

Step 3 Log into the Nessus client

- a. Login with the username **root** and password **root**
- b. Click the **Log in** button



- c. Click the **OK** button after reading the Warning message.

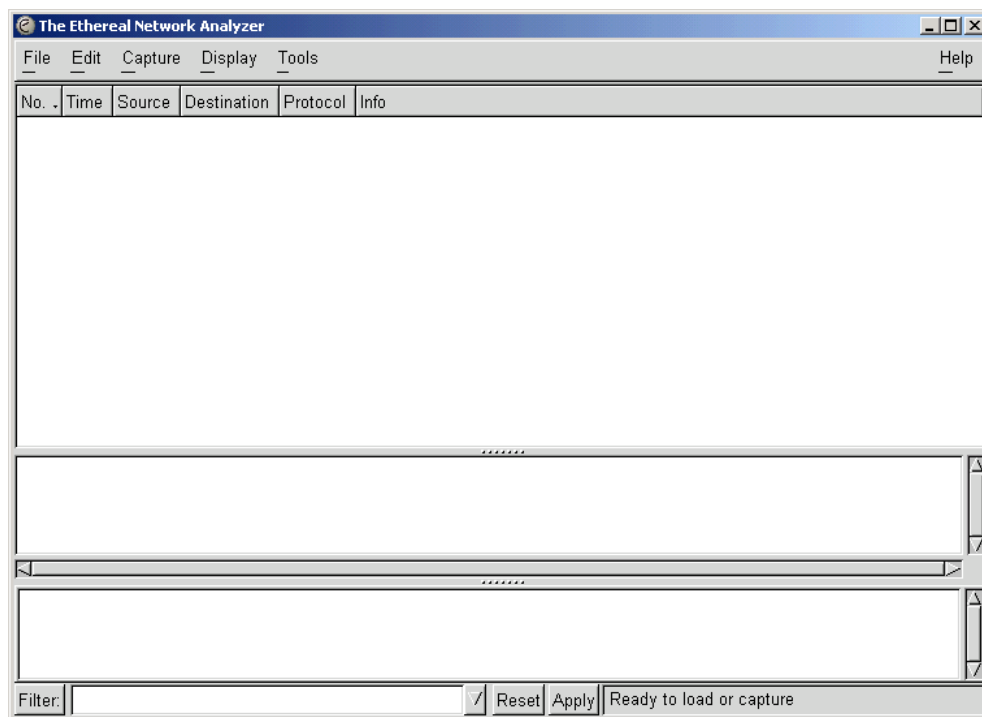
Step 4 Modify the Nessus Scan Options

- a. Select the **Plugins** tab. Include all attacks, by clicking on the **Enable All** button. This should enable the dangerous plugins as well.
- b. Select the **Prefs** tab. This tab displays the scanning options. Some of these options are options, such as scanning speed and scan type, are meant to be used with Nmap, and other options are passed to different Nessus modules. A few of the options on this page can be changed to speed up the scans.
 - i. Change the ping type from TCP to ICMP.
 - ii. Next, change the port selections to choose the **Fast scan (nmap-services)** instead of user specified ports.
- c. Select the **Scan Options** tab. Some of these options are passed to NMAP, and other options affect the amount of information that is gathered. Make the following changes:
 - i. Change the number of hosts to test to 5
 - ii. Disable the LaBrea tarpit scan, if it is not already disabled.

- d. Now choose the **Target Selection** tab. In the targets field, enter the network address of 10.0.P.2, 10.0.P.10, or another select host. The following options can be used to define the targets:
- i. A single IP address: For example, the IP address of the Pod device's inside interface.
 - ii. A range of IP addresses: 10.0.1.1-254
 - iii. Another range of IP addresses: 10.0.1.1-10.0.1.254
 - iv. Again a range of IP addresses in CIDR notation: 10.0.1.1/24
 - v. A hostname in Full Qualified Domain Name notation: Router1.cisco.com
 - vi. A hostname (as long as it is resolvable on the server). Router1
 - vii. Any combination of the aforementioned forms separated by a comma: 10.0.1.2, 10.0.1.10, 10.0.1.1

Step 5 Start the Scan and Monitor the packets using Ethereal

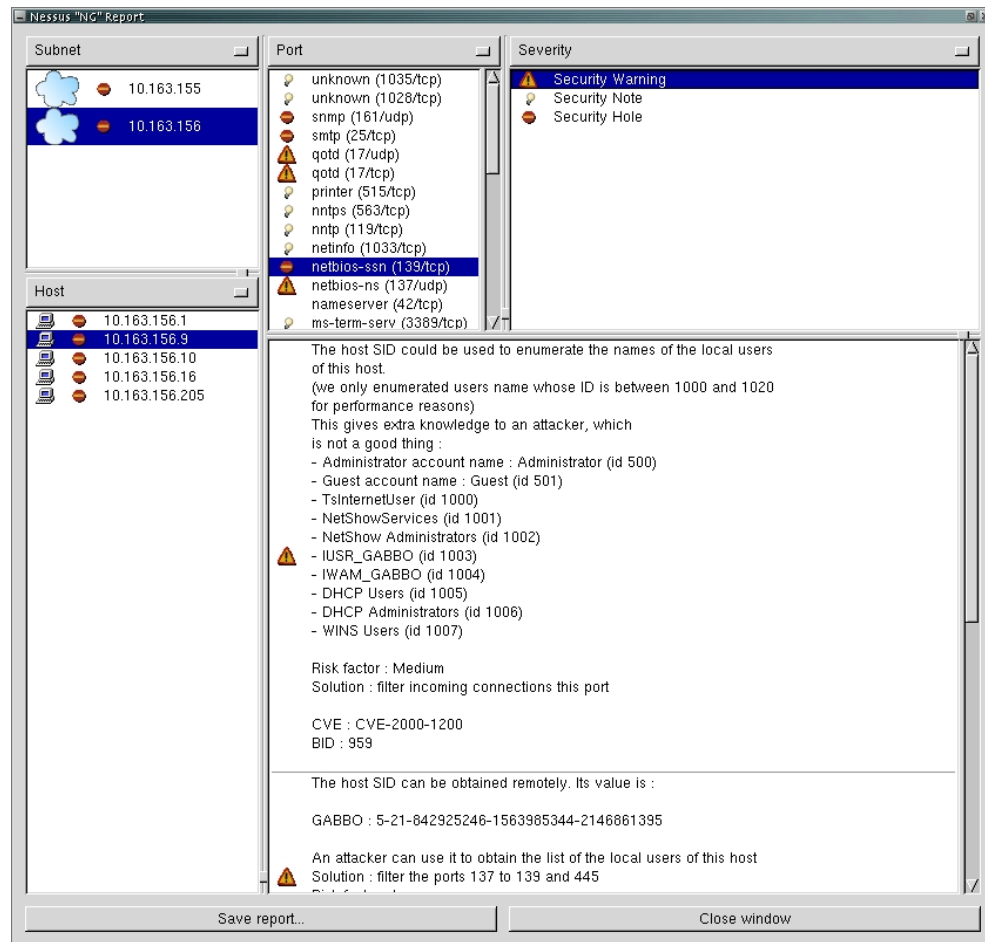
- a. Click **Start the Scan**.
- b. While the Scan is running, go to **Apps>I.a.s>Ethereal**



- c. Start a capture. **Capture>Start**.
- d. Click the **OK** button.
- e. Allow Ethereal to capture about 100 packets, then stop the capture.
- f. View the packets and notice the various types of IP traffic (TCP, ICMP, HTTP) which is part of the scan.

Step 6 View the vulnerabilities

- a. Let the scans complete, and then check the results displayed in the Nessus window.



- b. Four boxes of results will be displayed after the scan. Check through the results and see what vulnerabilities were identified.
- c. If you have a question about the vulnerabilities you identified, you can perform a quick Internet search using Google or another search engine.
- d. When you are finished using Linux on your PC or laptop, enter the `halt` command at the Bash prompt to exit Linux and then restart your computer after removing the Linux CD.

Part II:

Step 1 Research an exploit or vulnerability

- a. Research on the Internet one known exploit, script, or software tool of your choice. Or, use another tool available on the Linux security CD.
 1. What is the filename, program name, and exploit name?

- b. Obtain instructor approval, and then install the file. Make sure that instructor approval has been obtained before downloading or executing.
 1. What is the filename of the executable that has been downloaded?

 2. How long did it take to find the desired exploit, script, and software tool?

 3. What was the source of the file, exploit, or vulnerability?

 4. Describe the target device in terms of its name, model, OS, and function in the network.

 5. What source device or operating system is required to implement this exploit or vulnerability?

 6. Is this a known exploit? Who posted the advisory? Did the vendor acknowledge the problem? What are the recommended countermeasures?

 7. Are there any additional tools or knowledge required to implement this exploit or vulnerability?

 8. What is the projected cost to implement this exploit or vulnerability?

9. How difficult is it to implement this exploit or vulnerability?

10. What is the projected damage or cost to a victim's network if this exploit is used against it? Which devices are most impacted?

Step 2 Install, configure, and execute software tool

a. Install, configure, and execute one of the software tools.

1. How long did it take to install and configure this tool?

2. What were the results? Did the tool perform as anticipated? Why or why not?

3. If the target device was unaffected, what measures were taken to prevent the exploit?

Step 3 Fix the problem caused by the exploit

a. Fix the problem or damage caused by the exploit.

1. Is the damage easily reversed or remedied?

2. What is the time required to perform the repair or fix?

Step 4 Find a solution to the exploit

a. Find or propose a solution to this exploit or vulnerability.

1. Describe the proposed permanent solution or prevention.

2. With the approval of the instructor, implement the solution. How long did it take to implement the solution?

3. How difficult was it to implement or apply the solution or patch? What obstacles were encountered?

4. If a corporation has hundreds or thousands of the same target devices that are subject to the same exploit, how could a solution be implemented?

Step 5 Verify that the fix solved the problem

- a. It is easy to go through the motions of installing a patch or fix without verifying that it actually solved the problem. Return to Step 2 and repeat the steps.
 1. Did the solution prevent the exploit or vulnerability?

Step 6 Demonstrate the exploit

- a. Demonstrate the exploit or vulnerability to other students and the instructor.
 1. Did it function as planned?

Step 7 Reset all lab devices

- a. Reset all lab devices and re-image the computers or devices if necessary or directed by the instructor.