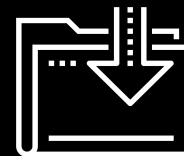




# Introduction to Intelligence Gathering




Cybersecurity Boot Camp  
Pentesting Day 1



# Class Objectives

---

By the end of class today, students will be able to:

-  Articulate the steps of the Penetration Testing Execution Standard.
-  Use Nmap to perform host discovery and port scan targets.
-  Use Nessus to perform vulnerability scans.

# Introduction to Intelligence Gathering

# Lesson Overview

---

Today, you'll be taking the first steps to becoming real hackers...

We'll cover:



The business purpose and goals of penetration testing



The Pentesting Execution Standard, a technical process for conducting a pentest



Information gathering



Vulnerability scanning



Exploitation with Metasploit



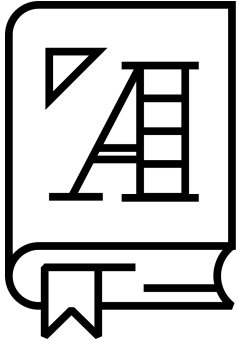
With these techniques, we will be able to break into networks and cause serious damage to network infrastructure.



## **Don't take this week's lessons lightly...**

Do not use the techniques and tools you'll be learning against any computer you do not own or have expressed, written permission to be interacting with.

# Business Goals of Penetration Testing



**Pentesting** is the systematic process of identifying an organization's vulnerabilities and providing recommendations on how to fix them.

# Goals of Penetration Testing

---

While breaking into machine is part of the pentesting process, the real **purpose** of an engagement is to **help the client improve their security**.

- A pentest is often referred to as an **engagement** by practitioners.
- Pentesters are hired to assess a company's security controls by finding flaws, helping companies understand them, and then providing recommendations of how to prioritize and fix vulnerabilities.
- It often takes an external perspective to identify misconfigurations and subtle security holes.



# Penetration Methods

---

## Black-Box Penetration

Most engagements are black-box.

Penetration testers are expected to attack the target network as an **outsider**.

They are paid to learn as much as they can about the network using only the same tools available to an attacker on the public Internet.

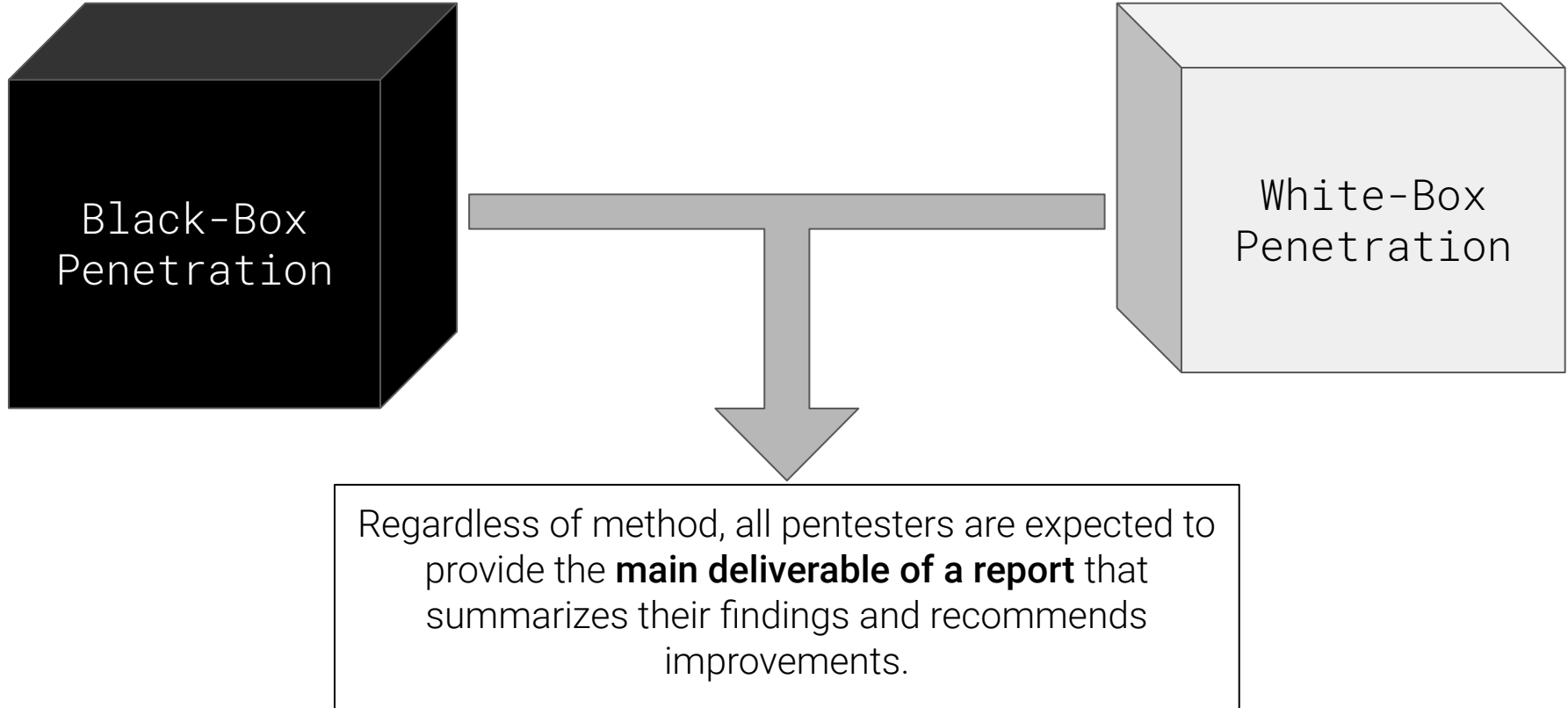
## White-Box Penetration

In **white-box** scenarios, pentesters have **full knowledge** of the network that is under scrutiny, allowing them to tear apart subtle security issues on behalf of their clients.

Most appropriate when the client wants a detailed analysis of all *potential* security flaws, rather than all exposed and visible vulnerabilities.

# Penetration Methods

---



# Pentesting Execution Standard (PTES)

---

Most penetration test are executed using an industry standard series of steps known as the **Penetration Testing Execution Standard**.

- ☐ Pre-Engagement Interaction
- ☐ Intelligence Gathering / Mapping
- ☐ Threat Modeling
- ☐ Vulnerability Assessment
- ☐ Exploitation
- ☐ Post-Exploitation

# Step 1: Pre-Engagement Interaction

---

## Determining scope and purpose

Businesses are primarily concerned with how an exploited vulnerability can have major consequences on the business reputation, operations, bottom-line, etc.

When meeting with clients for the first time, pentesters need to determine:

**Scope:** the range of networks and buildings that pentesters are allowed to assess.

**Purpose:** areas of concern for the client. For example: “Can you read sensitive data without authorization?”



## Step 2: Intelligence Gathering

---

Learning about a company's system

Passive reconnaissance	Active reconnaissance
<p>Passive reconnaissance is the process of using publicly available information to learn as much as possible about the target .</p> <p><i>Not interacting with the client's network directly.</i></p>	<p>Active reconnaissance is the process of learning about the client's networks by actively interacting with them.</p>
<p><b>For example:</b> Using Google to identify key figures in the organization; generating email lists; finding leaked documents exposed to search engines.</p>	<p><b>For example:</b> port scanning, in which you attempt to connect to every port on the targeted machine, eventually finding which services are running on exposed ports.</p>

## Step 3: Threat Modeling and Vulnerability Assessment

---

### Utilizing the the information gathered from Step 2

Using data obtained from intelligence gathering in order to determine:

- Where the system is likely to be most vulnerable?
- Which vulnerabilities are most severe?
- How to exploit the most critical vulnerability?

**For example:** After a pentester port-scans a network (Step 2: Intel Gathering), they will look at the list of exposed services and determine if any of the them are vulnerable by checking a database of vulnerabilities and exploits.

## Step 4: Exploitation

---

Leveraging a vulnerability to compromise security

- **Automated Exploitation:** Pentesters use tools like **Metasploit** to automatically exploit known vulnerabilities.
- **Use of Pre-existing Exploits:** Consultants manually download and deploy exploits developed by other security researchers.
- **Custom Exploits:** Pentesters write their own exploits, typically requiring considerable research into the vulnerabilities discovered in the intelligence gathering phase

**For example:** if you find an exposed SSH server during your vulnerability analysis, you might attempt to exploit it with a brute-force attack.

## Step 5: Post-Exploitation

---

Gaining administrative privileges or accessing sensitive data

**Privilege escalation:** Gaining administrative privileges, which usually implies unrestricted access to a system

- **Vertical escalation:** gaining higher privileges on the exploited machine.
- **Horizontal escalation:** moving between machines at the same privilege (using a user shell on Machine A to get a user shell on Machine B)

**Data exfiltration:** Stealing sensitive data, which can cause significant damage to a business if it fell into the wrong hands. Tactics include:

- Downloading files
- Running database queries
- Creating a user that allows access



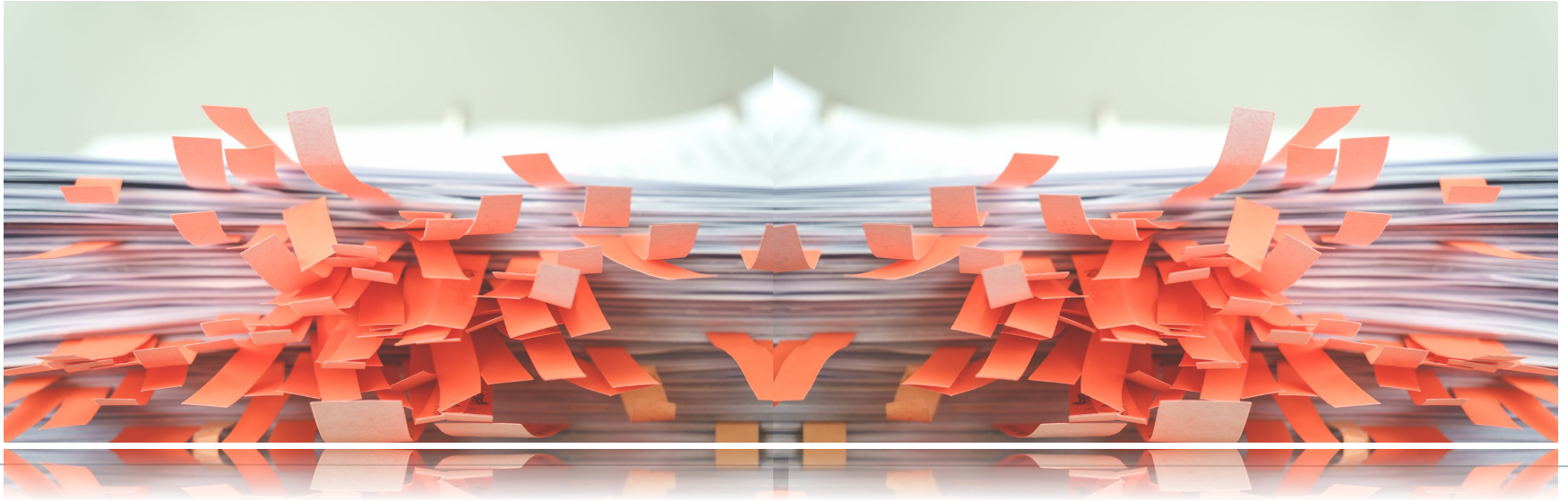
## Step 6: Finalizing Report

---

Reporting is not quite the last step...

**Pentesters should be documenting data every step of the process.**

The last step of a penetration test is finalizing the presentation of data, not collecting the data.



# Intelligence Gathering Tools

# Intelligence Gathering Tools

---

Pentesters commonly focus on two classes of vulnerabilities:

## **Network Vulnerabilities:**

Vulnerabilities due to improperly configured services or poorly patched machines on the client's network.

## **Social Vulnerabilities:**

Pentesters sometimes assess an organization's readiness for social engineering attacks by running phishing and other campaigns against their client's organization.

# Intelligence Gathering Tools

---

At a minimum, intelligence gathering usually entails:

**Mapping the Network:** Finding machines controlled by your client, and mapping their connections to one another.

**Fingerprinting Servers:** Determining which services and operating systems are running on which machines.

**Organizational Research:** If social engineering attacks are in-scope, intelligence gathering also entails finding the names, contact information, and even social media profiles of as many employees as possible

A good baseline goal for intelligence gathering involves:

- Enumerating all subdomains associated with the client's domain name.
- Port-scanning in-scope subdomains.
- Collecting as much email and social information as possible about the organization's employees.



## **Activity:** Scanning and Enumeration

In this exercise, you'll use ZenMap to scan and map a subnet.

Search for **Scanning and Enumeration Lab**

You will use the **Part 1 - Performing Initial Scans with Zenmap and Nmap** instructions inside the lab environment. Stop once you reach **Part 2 - Run a Vulnerability Scan with OpenVAS** instructions.

**Suggested Time:**  
35 minutes





# **Times Up!** Let's Review.

Scanning and Enumeration

# Take a Break!

---



# Nessus Set-up and Configuration



# Vulnerability Assessment

---

Vulnerability scanning is the next step after information gathering.

After enumerating hosts and services, you correlate those services with known vulnerabilities.

- In previous lessons, we have used **Nmap** to perform vulnerability scans. Today, they'll revisit nmap, with additional focus on:
  - Scan types
  - Saving output
  - Researching vulnerabilities

# Enumerating Services

---

Port scans determine which ports are exposed and which services are running on the target.

Nmap can scan both TCP and UDP ports.

- Most familiar services, such as HTTP, FTP, and SMTP, run over TCP.
- Notable services such as DNS (53), DHCP(67/68), and TFTP (69), run over UDP.

Begin by conducting a SYN scan of a target.

- SYN scan exchange SYN-SYN/ACK packets, but do not open a connection.

**Run a SYN Scan with:** `nmap -sS <Target IP Address>`

**Run a UDP scan against specific ports:** `nmap -sU -p53, 67,68,69 <Target IP Address>`

# Banner Grabbing and Version Detection

---

Demonstrate with `crackme.cenzic.com`:

In order to exploit an exposed port, you need to know which service it furnished.

Nmap can determine which services are running on which port via **banner grabbing**:

- Banner grabbing opens a connection to a port and prints out anything that the server sends within five seconds.
- Servers often send a string describing themselves, such as `220 FTP version 1.0\x0D\x0A`.

Nmap performs service and version detection with the `-sV` flag.

- `Nmap -sV crackme.cenzic.com`

Print full banners with `--script=banner`

- `Nmap -sV --script=banner crackme.cenzic.com`

# Vulnerability Scanning

---

Attackers can often penetrate machines by exploiting known vulnerabilities in old software.

Attackers will look up a service by version in a database of known vulnerabilities and use the results to guide their exploitation.

We can automatically look up known vulnerabilities for a given service with the `--script vulners` switch.

- Install vulners with: `curl -o /usr/share/nmap/scripts/vulners.nse https://raw.githubusercontent.com/vulnersCom/nmap-vulners/master/vulners.nse`

Run: `nmap -sV --script vulners crackme.cenzic.com`

Save the results of this scan to a file: `nmap -sV --script vulners crackme.cenzic.com -oN filename`

# Overview of Nessus

---

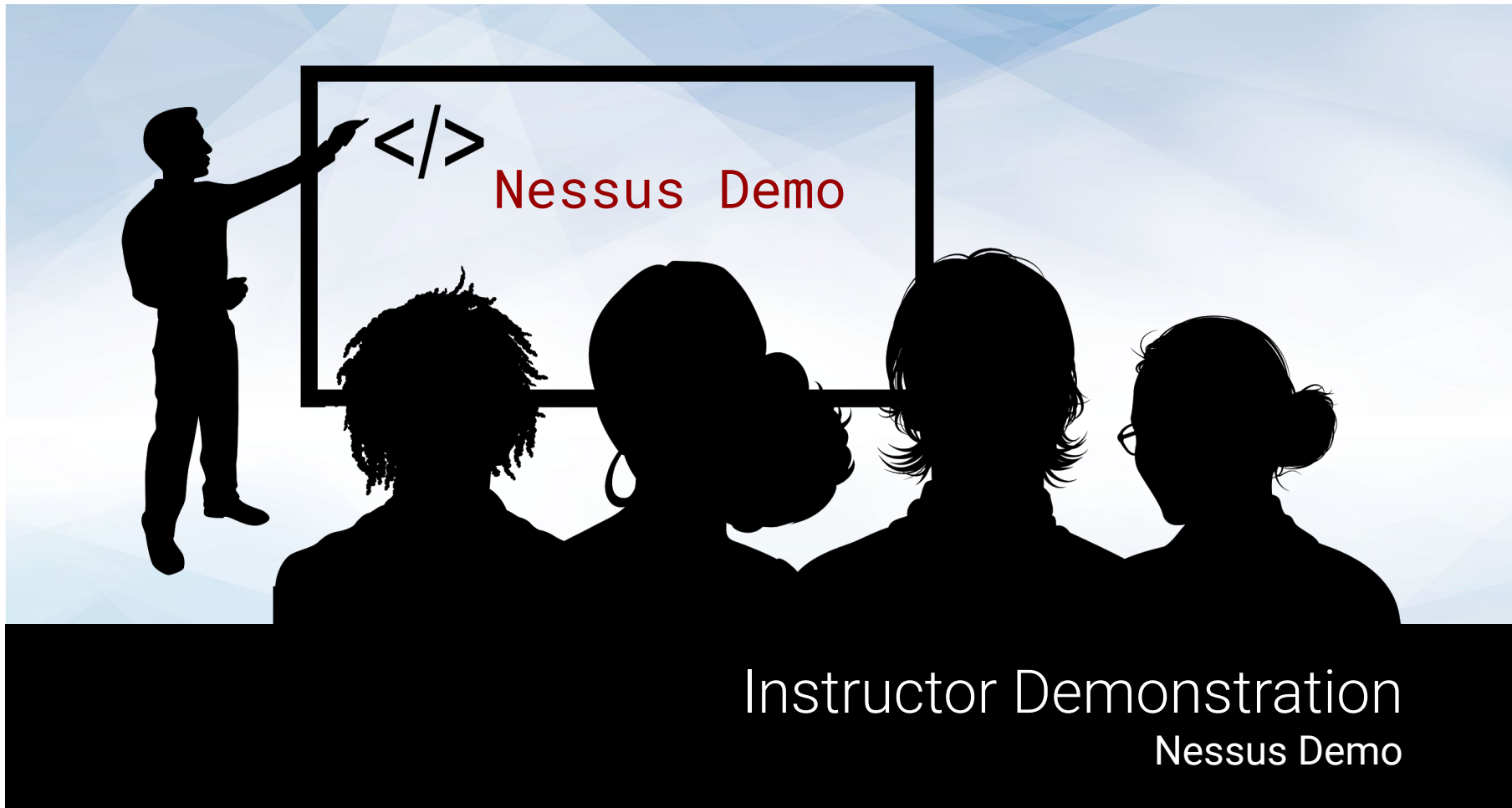
Vulners' output is sparse and difficult to parse.

**Nessus** provides a more powerful, graphical vulnerability scanning solution.

Nessus is used to:

- Port scan hosts
- Identify services
- Find vulnerabilities related to these services

Nessus allows you to save frequently used scan parameters, browse vulnerability in the web browser, and generate reports, and more.



Instructor Demonstration

Nessus Demo



## **Activity:** Nessus Scanning and Reporting

In this activity, you will use Nessus to perform a vulnerability scan.

Search for **Nessus Scanning and Reporting**.

Be sure to launch the lab and run the requisite scans yourself as soon as you start the lab

**Suggested Time:**  
40 minutes





**Times Up!** Let's Review.

Nessus Scanning and Review



# Nessus Scanning and Reporting Review

---

## **8. Notice the different types of “Discovery type”.**

i. How is this different/similar to NMAP?

# Nessus Scanning and Reporting Review

---

## 8. Notice the different types of “Discovery type”.

i. How is this different/similar to NMAP?

Nessus offers host enumeration, port scan (common ports), and port scan (all ports).

This is similar to Nmap in that it allows us to port scan a target, but different in that we have fewer options.

Nmap, for example, lets us select between TCP SYN and Connect scans, scan specific ports, etc.

# Nessus Scanning and Reporting Review

---

**11b. Notice the default for the SSL search is on “Known SSL ports.”**

i. List one known SSL port.

ii. Why would you want to search for SSL “on all ports”?

# Nessus Scanning and Reporting Review

---

**11b. Notice the default for the SSL search is on “Known SSL ports.”**

i. List one known SSL port.

443 (HTTPS), 995 (POP3-SSL), 993 (IMAP-SSL)

ii. Why would you want to search for SSL “on all ports”?

# Nessus Scanning and Reporting Review

---

## **11b. Notice the default for the SSL search is on “Known SSL ports.”**

i. List one known SSL port.

443 (HTTPS), 995 (POP3-SSL), 993 (IMAP-SSL)

ii. Why would you want to search for SSL “on all ports”?

Encrypted services can run on any port. There is no reason admins can't run SSL service on non-standard ports, such as running HTTPS on 8443.

# Nessus Scanning and Reporting Review

---

**12bii. Why would you want to add application/file white/blacklisting to your scan?**

# Nessus Scanning and Reporting Review

---

**12bii. Why would you want to add application/file white/blacklisting to your scan?**

These additions help you stay within the scope of your engagement and avoid sending traffic to delicate hosts.

# Nessus Scanning and Reporting Review

---

**19. Provide the OS running on each target.**



# Nessus Scanning and Reporting Review

---

## 19. Provide the OS running on each target.

192.168.0.20: Windows 7

192.168.0.221: Windows 8.1

192.168.0.112: Windows 7 Professional

192.168.0.125: Linux Kernel

The scan did not produce results for the other hosts.

# Nessus Scanning and Reporting Review

---

**26. What are three things that are different or similar between Nessus and Nmap?**

# Nessus Scanning and Reporting Review

---

## 26. What are three things that are different or similar between Nessus and Nmap?

- Nessus and Nmap both run port scans, but only Nessus is a specialized vulnerability scanner.
- Nmap provides more granular control over exactly how it scans targets.
- Nessus allows you to save profiles and generate reports, making it more useful than Nmap for generating artifacts for use in reports.

# Nessus Scanning and Reporting Review

---

**27. Provide an example of where/why you would use one over the other?**

**Is there an instance where you would not want to use either?**

# Nessus Scanning and Reporting Review

---

**27. Provide an example of where/why you would use one over the other?**

Nmap should be used for more granular port scanning.

- UDP scanning / banner grabbing on specific ports.

Nessus is useful for generating vulnerability reports.




**Is there an instance where you would not want to use either?**

No cases come to mind in which Nmap wouldn't be useful, but Nessus is heavy for light/early-stage reconnaissance.

# Class Objectives

---

By the end of class today, students will be able to:

-  Articulate the steps of the Penetration Testing Execution Standard.
-  Use Nmap to perform host discovery and port scan targets.
-  Use Nessus to perform vulnerability scans.