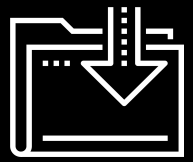
Introduction to Pen Testing and OSINT

Cybersecurity

Lesson 16.1



Class Objectives

By the end of today's class, you will be able to:

Understand the role of a pen tester in assessing a business's security.

Collect domain information using OSINT techniques and tools like Google dorking, Shodan, and certificate transparency.

Use Shodan and Recon-ng to discover domain server information.

Introduction to Penetration Testing

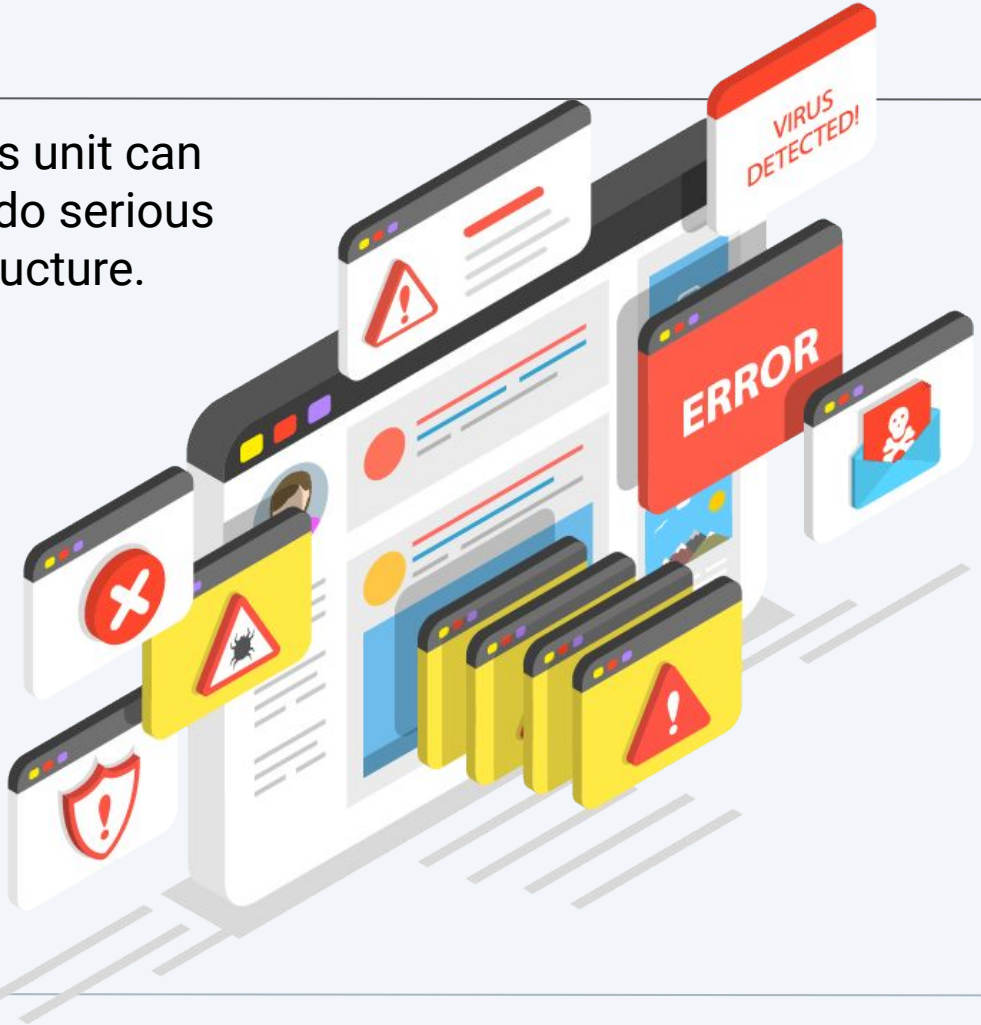
Introduction to Penetration Testing

Today we will cover the following:

Important!

The techniques that we'll learn in this unit can be used to break into networks and do serious damage to an organization's infrastructure.

- **This is illegal when done without permission.**
- The tools and techniques we'll discuss are serious, and misusing them has serious consequences.
- **Do not practice these techniques against computers that you do not own or have clear written permission to interact with.**



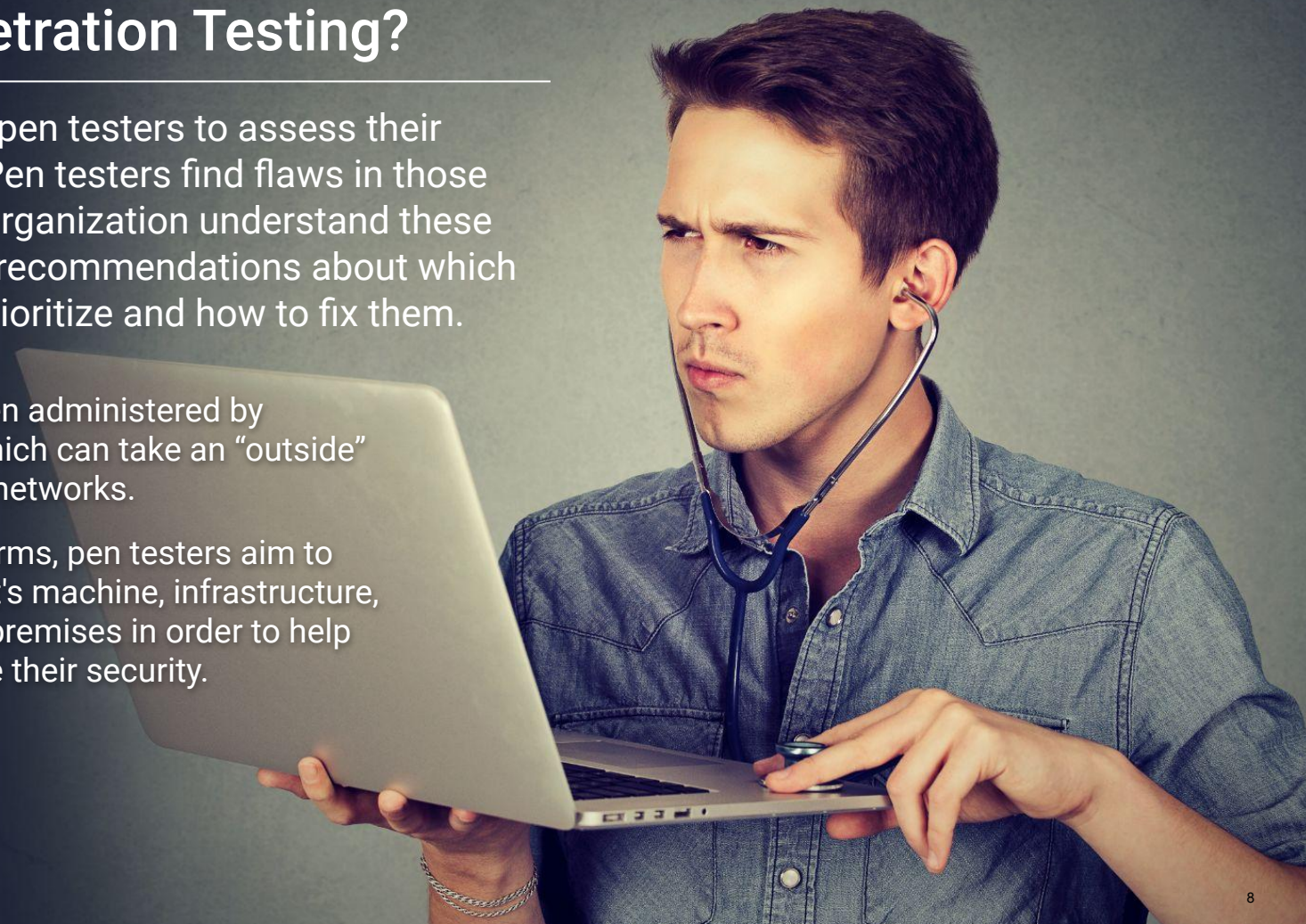
What Is Penetration Testing?

Penetration testing, often referred to as **pen testing** or **ethical hacking**, is the offensive security practice of attacking a network using the same techniques that a malicious hacker would use, in an effort to identify security holes and raise awareness within an organization.

What Is Penetration Testing?

Organizations hire pen testers to assess their security controls. Pen testers find flaws in those controls, help the organization understand these flaws, and provide recommendations about which vulnerabilities to prioritize and how to fix them.

- Pen tests are often administered by consultancies, which can take an “outside” view of a client’s networks.
- In the simplest terms, pen testers aim to break into a client's machine, infrastructure, or even physical premises in order to help the client improve their security.



A penetration test is often referred to as an engagement by practitioners.

What Is Penetration Testing?

Unlike malicious hackers, pen testers only begin an engagement after receiving permission from the security owner.

What Is Penetration Testing?

Penetration testers use a combination of automated and manual tools to research vulnerabilities, craft phishing emails, manually exploit hosts, and write shell code. Pen testers use these tools creatively, just as criminal hackers do.

Unit Overview and Penetration Testing Phases

This Week's Scenario

This week, you will play the role of consultants at GoodCorp who have been hired to conduct a penetration test against MegaCorpOne.

MegaCorpOne is an organization that specializes in disruptive innovation in the nanotechnology industry and has hired GoodCorp to run a penetration test.

You will be tasked with completing a penetration testing engagement to assess MegaCorpOne's security.

You will conclude your test with a report of your findings. **Keep notes of all your results as you proceed through the penetration testing activities.**

Penetration testers follow a methodology during an engagement that is designed to mimic that of an actual attack.

This helps network defenders understand how effective their organization's defenses are.

Reporting

Post exploitation

Exploitation

Scanning

Planning and reconnaissance

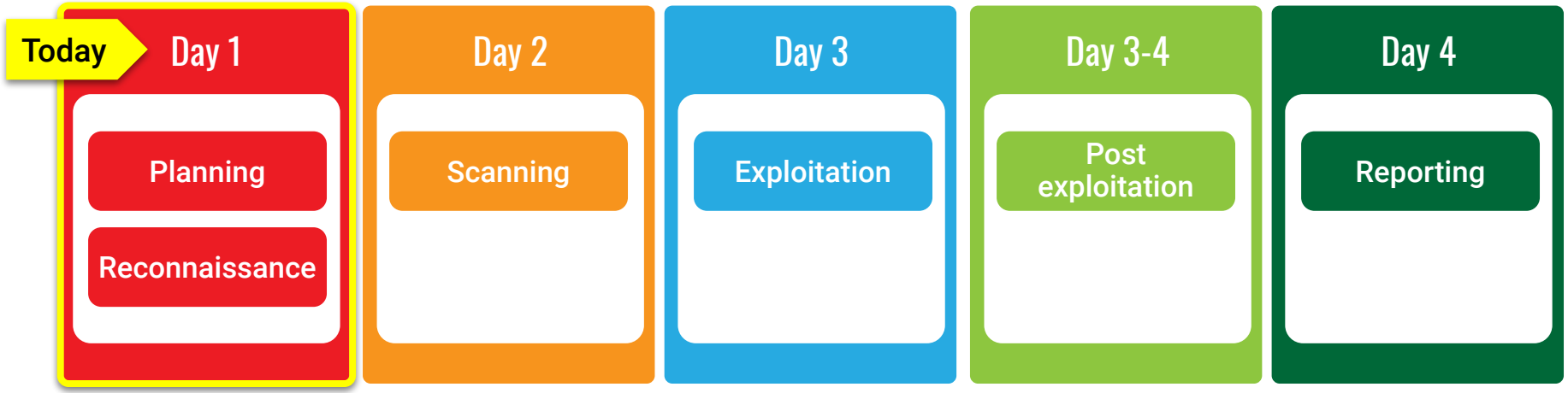
Pen Testing Phases

An engagement consists of five phases:

01A	**Planning**	Define the purpose and scope of the test, and sign all legal contracts.
01B	**Reconnaissance**	Obtain publicly available information about your target.
02	**Scanning**	Use tools to run a scan against your target to gather information, such as open ports, and run services to determine potential vulnerabilities.
03	**Exploitation**	Attack the vulnerabilities discovered in the previous steps in order to gain access to the target.
04	**Post exploitation**	Gather valuable information from the compromised systems.
05	**Reporting**	Report on the previous five steps to provide a summary of actions taken, findings, and recommended mitigations.

Unit Progression

Over the four classes in this unit, we will proceed through these five phases as we conduct a penetration test against MegaCorpOne.



Be sure to keep your findings from each activity. You will use them on the fourth day when you create your penetration test report.

While we've shown these phases sequentially, there are times when steps are skipped or repeated or when their order is switched, as in a real attack.

Phase 1:
Planning

Phase 1: Planning

The planning step is an interaction between the organization and the pen testing team. It helps the pen testers thoroughly understand the client's needs before beginning the test.

Most businesses' primary interest is not how attackers might gain access to their networks.

Instead, their main concern is the major consequences that an exploited vulnerability may have for their reputation, operations, or bottom line.

Purpose and Scope

Planning usually begins with a kick-off meeting, during which clients work with pen testers to determine the purpose and scope of the project.

Phase 1: Planning

The primary deliverable from this stage is a document summarizing:

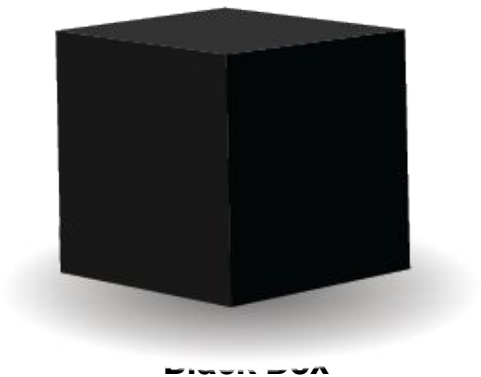
- The engagement’s purpose
- The scope
- Associated details such as timeframe and emergency contacts

Types of Penetration Testing

Types of Penetration Testing

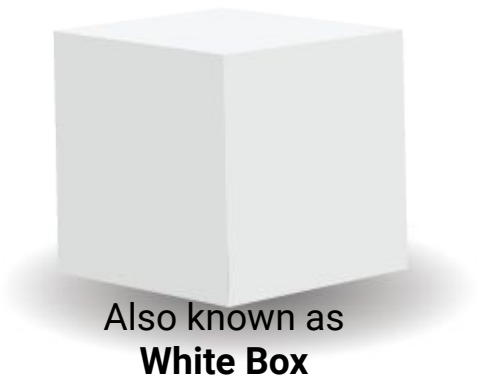
There are three types of penetration tests:

No View



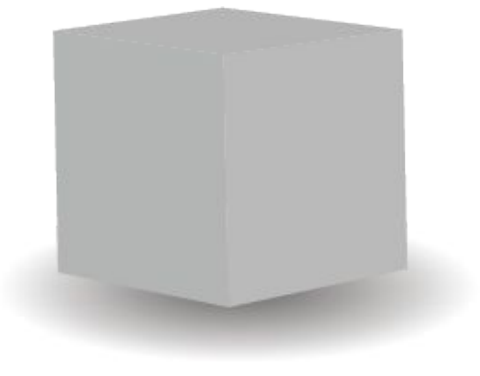
Also known as
Black Box

Full View



Also known as
White Box

Partial View

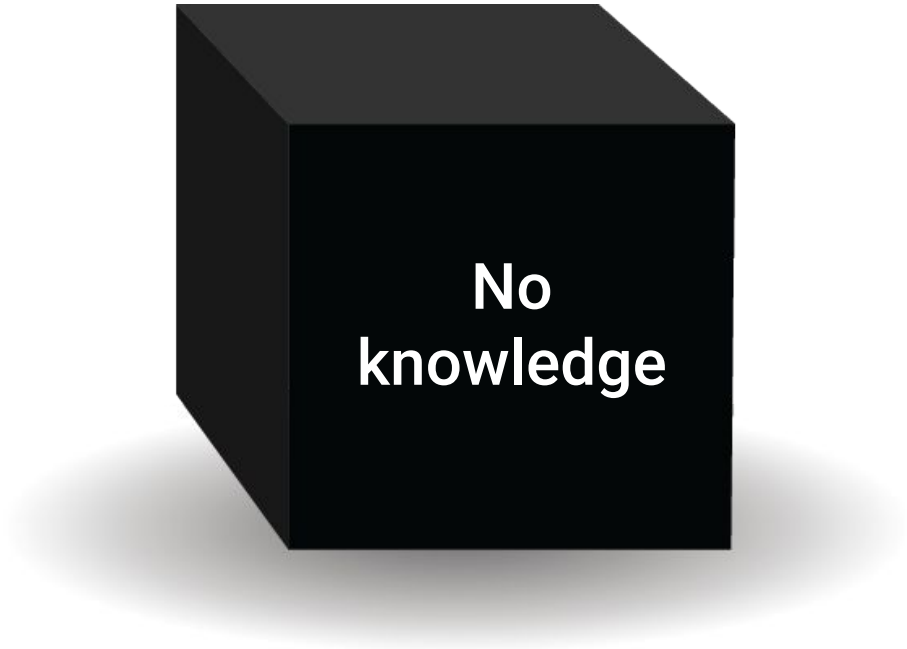


Also known as
Gray Box

No-View Pen Testing

In no-view testing, the pen tester simulates a malicious hacker who has no prior knowledge of the target system and network.

- The pen tester is paid to learn and exploit as much as they can about the network using only the tools publicly available to an attacker on the internet.
- For example, they may know only the company name and have to find various key resources, like IP ranges and access credentials.



Full-View Pen Testing

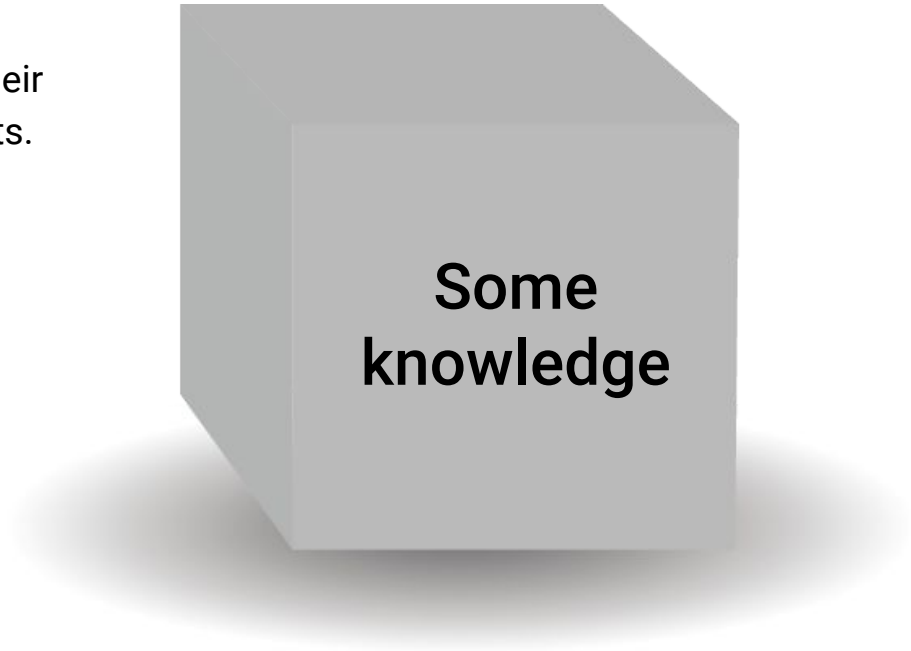
In full-view testing, the pen tester is given full knowledge of the system or network.

- This knowledge allows them to tear apart subtle security issues on behalf of their clients.
- Full-view pen testing is most appropriate when the client wants a detailed analysis of all potential security flaws, rather than exposed and visible vulnerabilities.
- Full-view testers are given network diagrams, access credentials to the networks, system names, usernames, emails, and phone numbers.

Partial-View Pen Testing

Partial-view pen testing is performed by the in-house system or network admin.

Regardless of the scenario, the main deliverable for any pen tester is a report that summarizes their findings and recommendations for improvements.



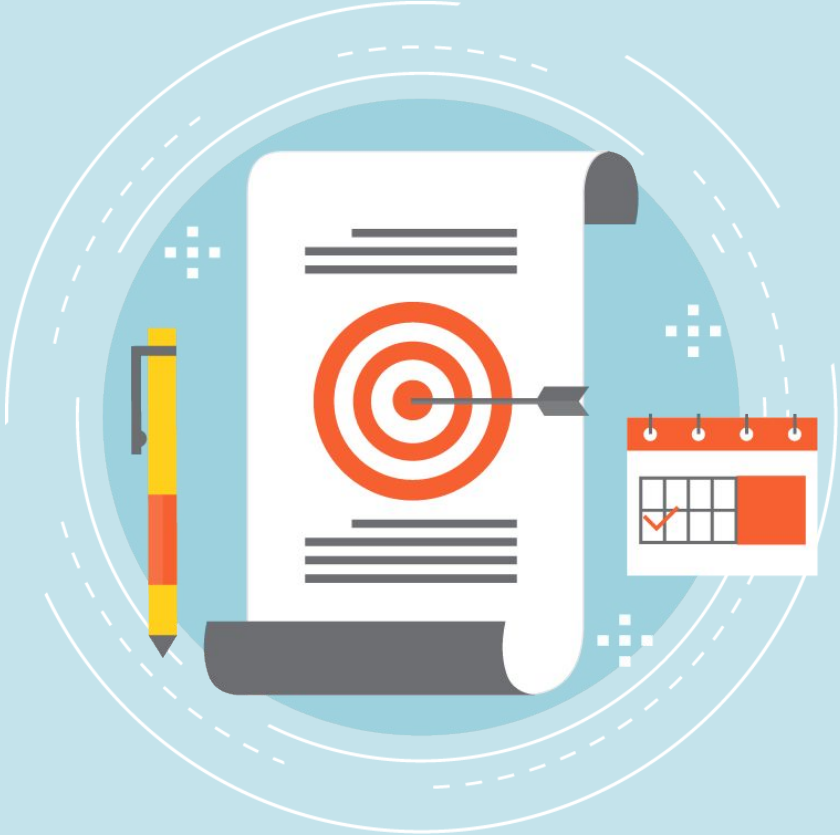
Statements of Work & Legal Indemnification

Statements of Work & Legal Indemnification

Before beginning a security assessment, several legal steps must be completed.

Since penetration testing is hacking, the entity being hacked must consent to the test.

To protect the assessors from legal ramifications, a **statement of work (SoW)** must be agreed upon and signed by both parties.



A **statement of work (SOW)** outlines the scope of the test, the timeline, the points of contact, and how the test will be conducted.

Penetration testing without a contractual agreement is **illegal** unless it is conducted on your own network or devices.

Scenario 1:

A financial institution asks you to perform a penetration test on their private network.

They will give you access to all the credentials and architecture diagrams that you may need.

You will also meet with them beforehand to sign a contract clearly illustrating the scope and purpose of the test.

Scenario 1:

A financial institution asks you to perform a penetration test on their private network.

They will give you access to all the credentials and architecture diagrams you may need.

You will also meet with them beforehand to sign a contract clearly illustrating the scope and purpose of the test.

This is a **legal** full-view penetration test, because you have signed a contract before you begin your assessment.

Scenario 2:

A friend has verbally asked you to perform a penetration test on a social media website they just joined as they want to make sure their information is safe.

Scenario 2:

A friend has verbally asked you to perform a penetration test on a social media website they just joined as they want to make sure their information is safe.

This is an **illegal** no-view test, because neither the friend nor you own the social media website network or devices, and the social media website has not granted permission or signed a contract authorizing this test.

Summary

Penetration testing, often referred to as **pen testing** or **ethical hacking**, is the offensive security practice of attacking a network using the same techniques that a malicious hacker would use, in an effort to identify security holes and raise awareness within an organization.

The five phases of a pen testing engagement are **planning and reconnaissance**, **scanning**, **exploitation**, **post exploitation**, and **reporting**.

During the planning phase, the engagement's **scope** and **purpose** are defined.

The scope includes the type of penetration test that will be run. Types include **no view**, **full view**, and **partial view**.

A **statement of work (SoW)** is also completed during the planning phase. It outlines the scope of the test, the timeline, the points of contact, and how the test will be conducted.

Questions?

Activity: Types of Penetration Testing

In this activity, you will evaluate pen testing scenarios and determine the type and legality of each.

Suggested Time:

15 Minutes

Time's Up! Let's Review.

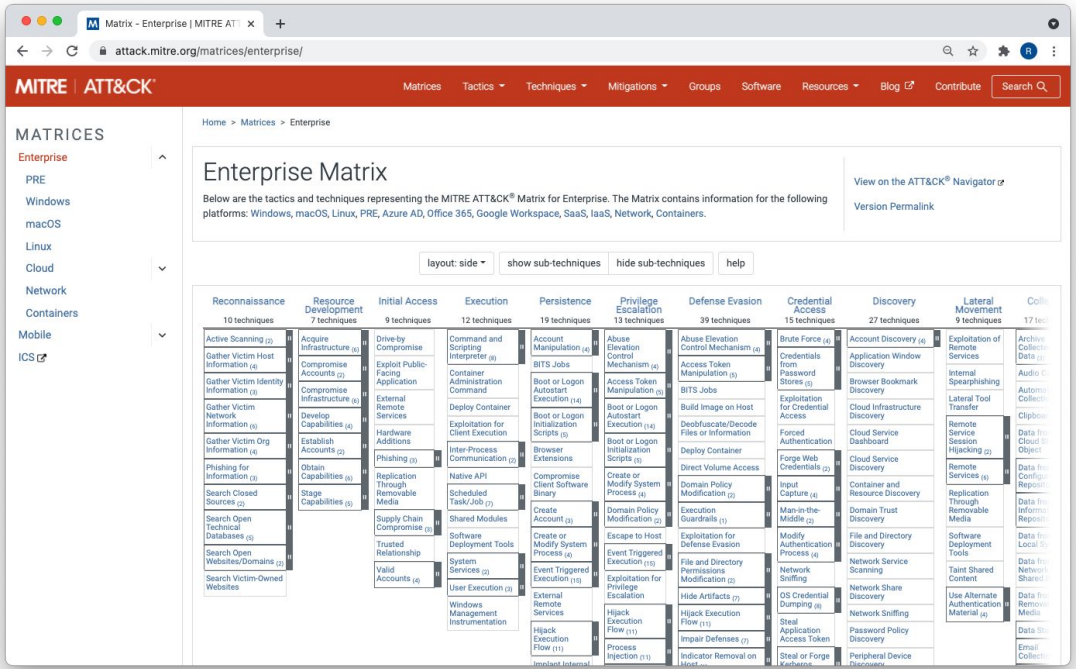
Questions?

Intro to MITRE ATT&CK

MITRE ATT&CK

The company **MITRE** developed the **MITRE ATT&CK matrix** to provide a visual representation of all the **techniques, tactics, and procedures (TTPs)** that may be performed throughout an assessment.

We will use this matrix as a reference for the TTPs that we will conduct throughout the next two weeks of class.



MITRE ATT&CK

The MITRE ATT&CK matrix consists of the following:

Tactics / Headers

- Each header represents a **tactic**.
- For example, the first tactic listed is **reconnaissance**.
- It's listed first because attackers conduct reconnaissance on a target before actually performing any exploitation.

Techniques / Rows

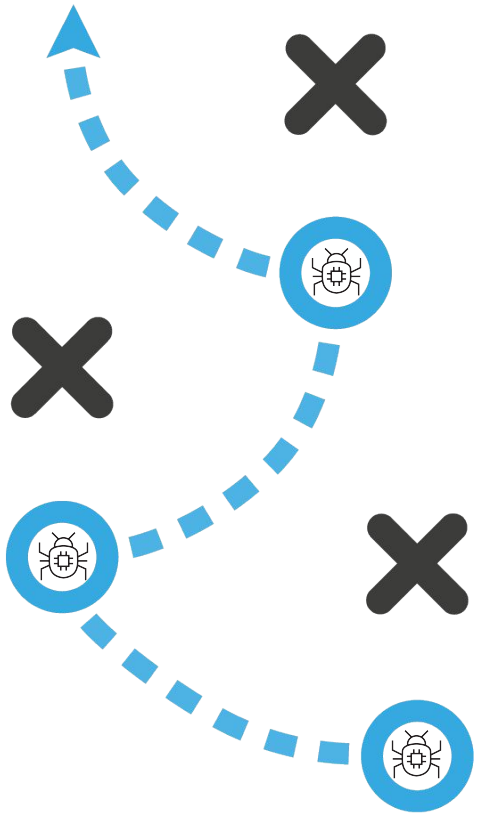
- Each row under the header is a **technique**.
- For each tactic, there are multiple techniques.
- For example, during reconnaissance, an attacker may use **active scanning** to gather information about a target, or they may **search open technical databases** to gather similar information.

MITRE ATT&CK

MITRE ATT&CK is a “hacker’s playbook.”

The matrix is comprehensive, meaning that virtually every potential attack falls under a tactic and maps to a specific technique.

As a penetration tester, it’s beneficial to map out the techniques that you performed in an assessment so that the customer can learn which TTPs were successful and what needs to be addressed.



MITRE

MITRE is a powerful matrix to follow and reference for several reasons:

- It is comprehensive and includes almost every possible tactic or technique that an attacker could perform during a hack.
- In your final report, it provides a way to refer to tactics and techniques that an attacker would use in a manner that less-technical staff can understand.
- It helps create a more comprehensive report by categorizing specific security deficiencies.

  For example: If a red team successfully demonstrates several techniques under the **lateral movement** tactic, it highlights that tactic as a security hole in the organization.

MITRE

This week's unit will follow the MITRE ATT&CK matrix tactics from left to right. We won't cover every tactic due to time constraints, but we'll begin by learning about reconnaissance today.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques

Reconnaissance with OSINT and Google Dorking

Reconnaissance, or **recon**, means gathering information about your target.

Reconnaissance

Reconnaissance is divided into two types:

01 Passive Recon

Often refers to **open source intelligence (OSINT)**, which leverages information about the target that is publicly available on the internet.

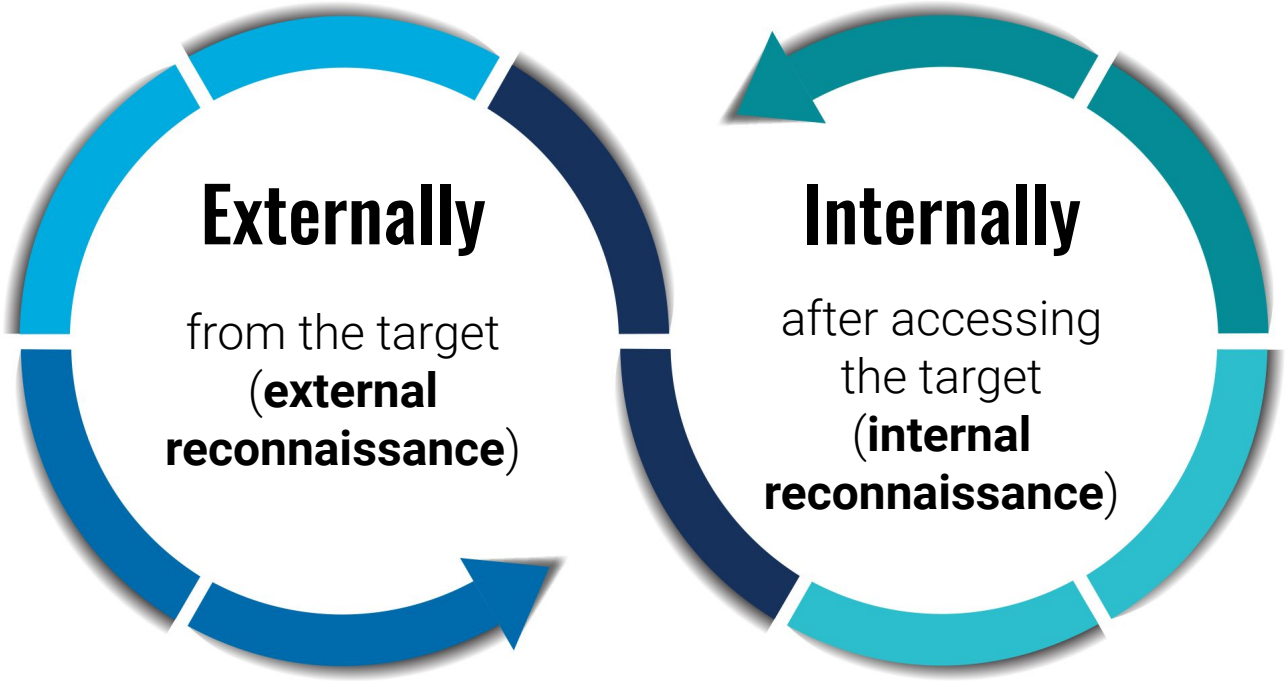
This includes all domains and hosts belonging to a target that are publicly viewable.

02 Active Recon

Also refers to gathering information about the target, but it involves directly interacting with the target.

Reconnaissance

Reconnaissance can be conducted:



Google Dorking

Enables us to manipulate Google searches to narrow down our queries in order to acquire actionable intel.

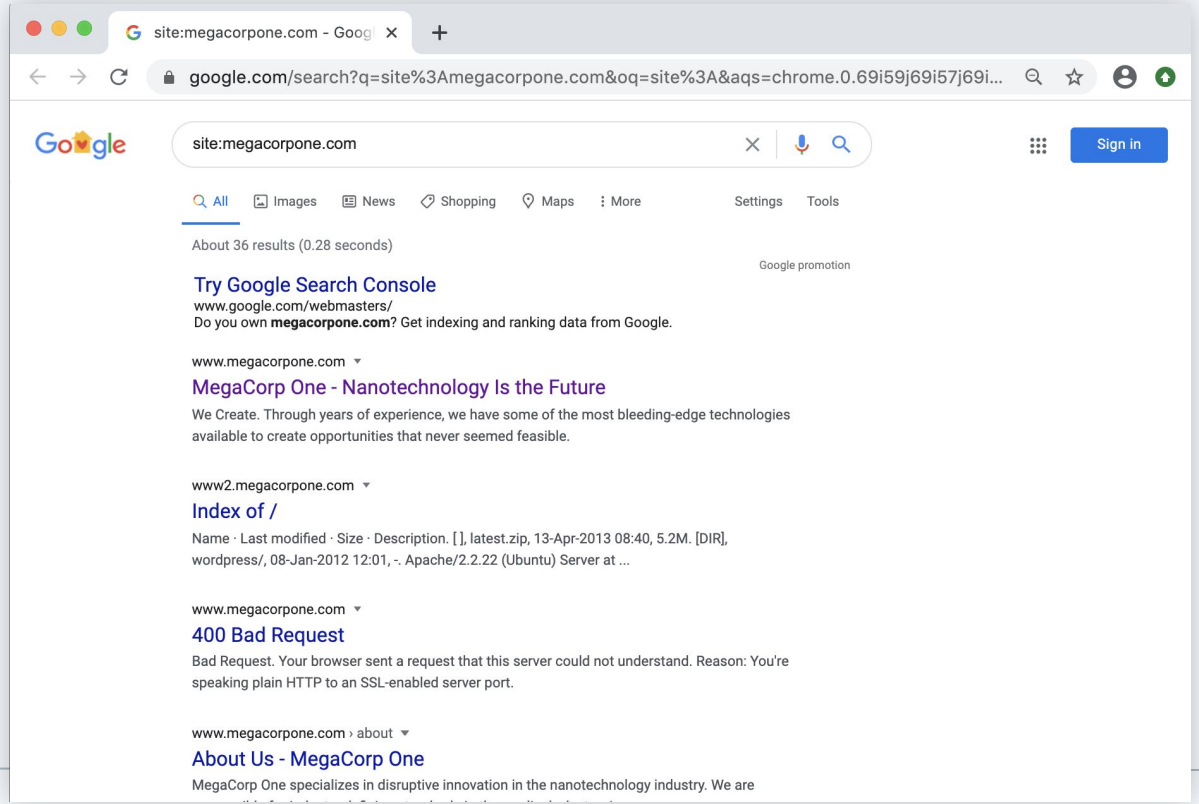
Google Dorking

Falls under the technique

Search Open Websites/Domains: Search Engines, ID T1593-002.

Google Dorking Demo

In this demonstration, we'll use Google search techniques to target sans.org.



Instructor Demonstration

Google Dorking

Summary

We've covered the following concepts:

Reconnaissance	Gathering information about your target. It's part of the **planning and reconnaissance** phase.
Passive recon	Leveraging information about the target that is publicly available on the internet. Often refers to **open source intelligence (OSINT)**.
Active recon	Directly interacting with the target to obtain information.
External reconnaissance	Reconnaissance that is conducted externally from the target.
Internal reconnaissance	Reconnaissance that is conducted internally after accessing the target.
Google dorking	A reconnaissance **Technique** that enables us to manipulate Google searches to narrow down our queries in order to acquire actionable intel.

Activity: Google Dorking

In this activity, you will use Google dorking techniques to find information about MegaCorpOne.

Don’t forget to keep your findings for the final report!

Suggested Time:

15 Minutes

Time's Up! Let's Review.

Questions?


Break

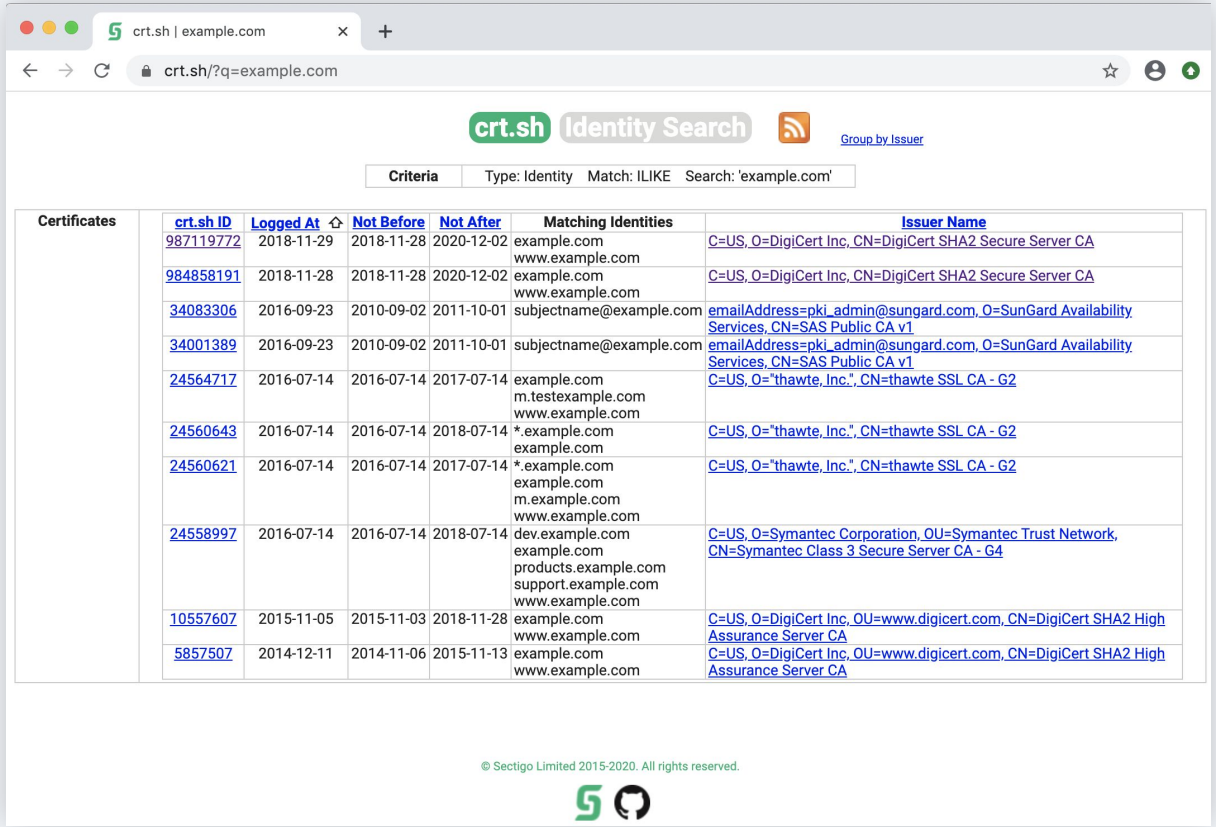
Certificate Transparency

Certificate Transparency

Certificate issuers publish logs of SSL/TLS certificates that they issue to organizations.

This is known as **certificate transparency**. Attackers can exploit it to search for subdomains.

This falls under the **Search Open Technical Databases: Digital Certificates** MITRE technique, **ID T1596.003**.



Instructor Demonstration

Certificate Transparency

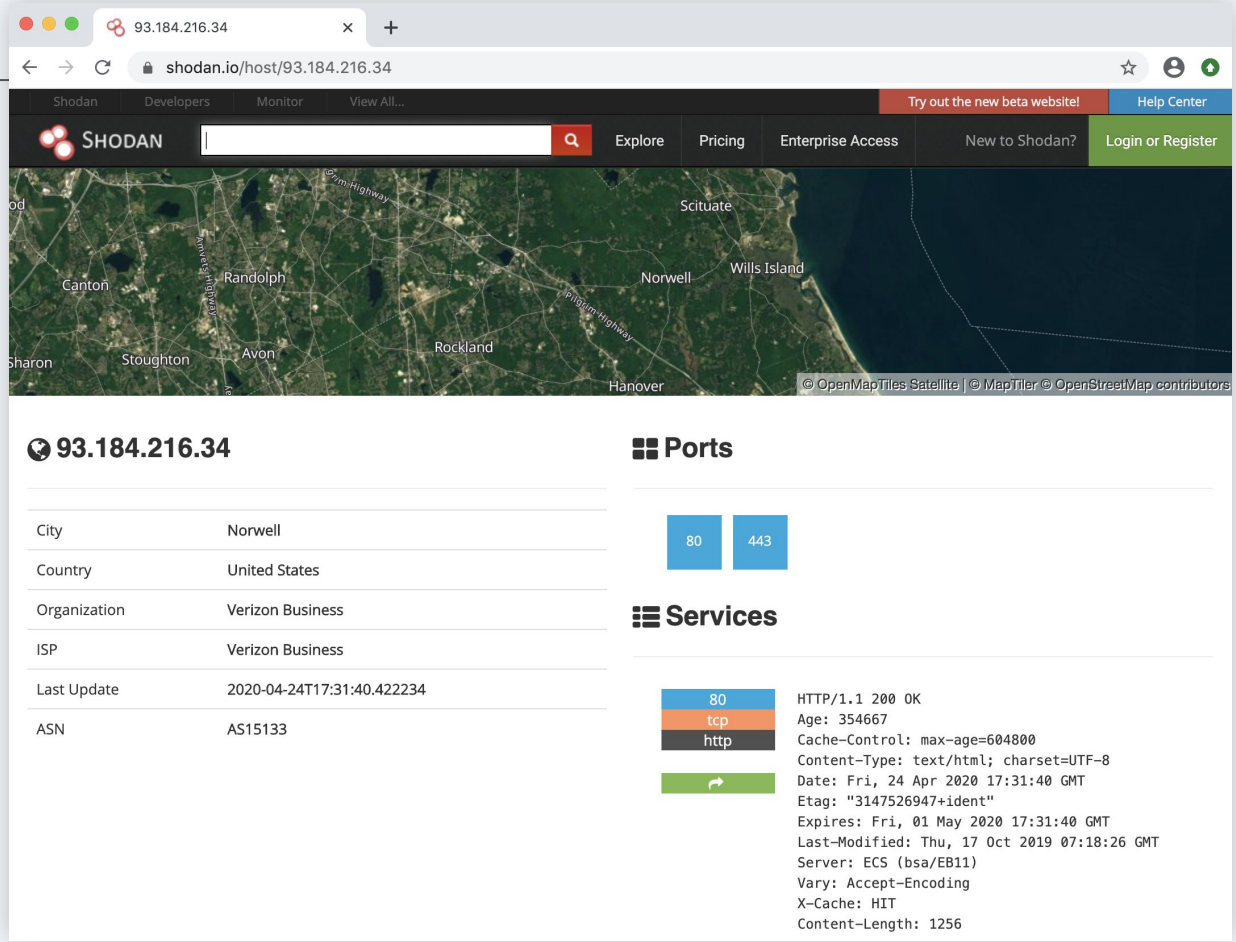
Shodan

Shodan.io

Shodan.io conducts port scanning across the entire internet and catalogs the results for quick searching.

This saves us the time we would spend conducting a port scan. Not conducting the scan also allows us to keep our originating IP address hidden.

This falls under the MITRE technique **Search Open Technical Databases: Scan Databases, ID T1596.005**.



Instructor Demonstration

Shodan.io

Summary

We've covered the following concepts:

Certificate transparency

A reconnaissance tactic where a penetration tester can gather information from certificate issuers, which publish logs of the SSL/TLS certificates that they issue to organizations.

- Attackers can exploit certificate transparency to search for subdomains.

Shodan.io

A reconnaissance website that conducts port scanning across the entire internet and catalogs the results for quick searching.

Activity: Shodan.io

In this activity, you will use Shodan.io to examine previously completed port scans on several targets.

Don’t forget to keep your findings for the final report!

Suggested Time:

15 Minutes

Time's Up! Let's Review.

Questions?

Recon-ng

Recon-ng is a web reconnaissance framework written in Python.

Recon-ng

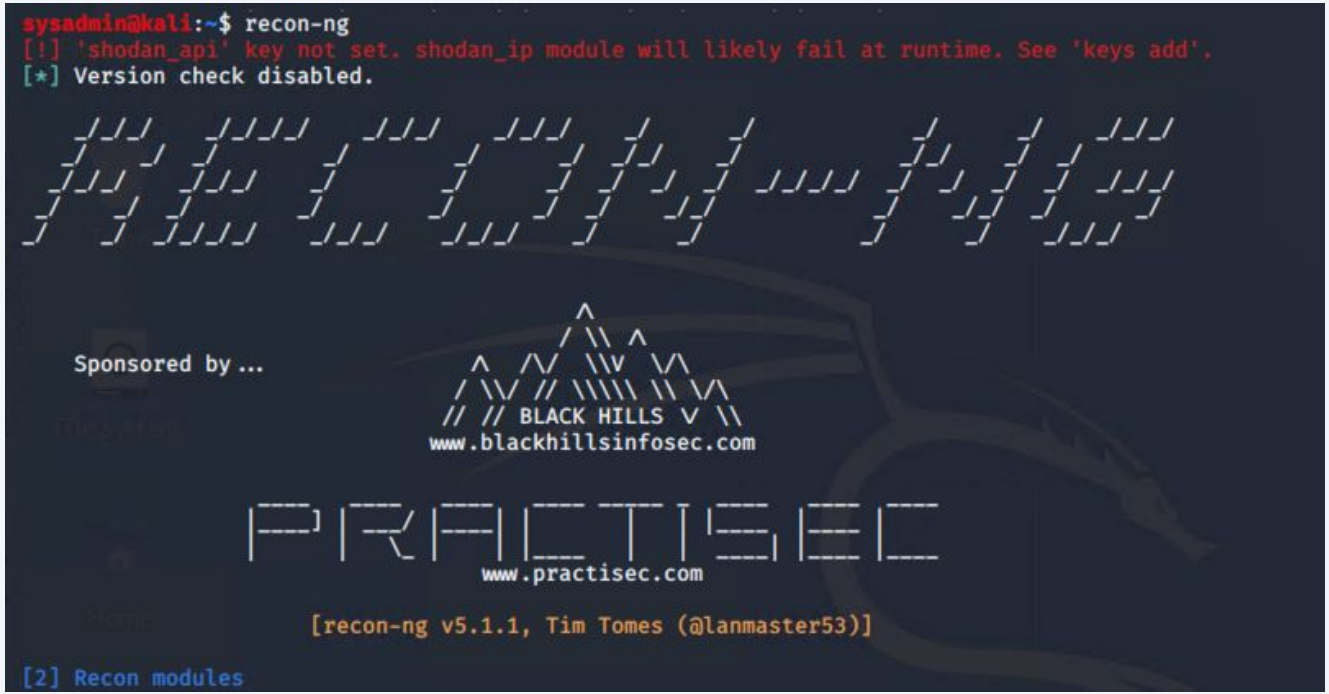
Recon-ng provides a powerful, open source, web-based framework for conducting reconnaissance quickly and thoroughly.

It includes the following features:

- Independent modules
- Database interaction
- Built-in convenience functions
- Interactive help
- Command completion

Recon-ng

The Recon-ng framework ingests many popular OSINT modules, allowing the results of multiple tools to be combined into a single report.



Instructor Demonstration

Recon-ng

Activity: Recon-ng

In this activity, you will use Shodan and Recon-ng to determine whether MegaCorpOne's domain server info is accessible using OSINT tools.

Don't forget to keep your findings for the final report!

Suggested Time:

15 Minutes

Time’s Up! Let’s Review.

Questions?


The End