CYBR-2100 Cyber Ethics & Cyber Law

Week 2 – Cybercrime, Access & Legal Boundaries

Welcome to Week 2.

Last week, we focused on a foundational professional question: just because you can perform a cybersecurity action, should you?

This week adds another question:

Are you actually authorized to do it?

Many of the same tools and techniques used by penetration testers, security analysts, incident responders, and researchers can also be used for unauthorized access and computer misuse.

The difference is not necessarily the tool.

Authorization, scope, purpose, circumstances, and professional conduct matter.

This Week's Big Question

Where is the line between legitimate cybersecurity work and unauthorized activity?

You will examine that question through security testing, vulnerability research, cybercrime law, incident investigation, and digital evidence.

What You Will Learn

By the end of Week 2, you should be able to:

- Explain why authorization is fundamental to professional cybersecurity practice.
- Distinguish authorized security testing from potentially unauthorized activity.
- Recognize the importance of written scope and testing boundaries.
- Identify legal issues associated with unauthorized computer access and computer misuse.
- Explain foundational concepts associated with the Computer Fraud and Abuse Act.
- Evaluate the legal and professional boundaries of vulnerability research.
- Identify and evaluate relevant digital evidence.
- Explain why evidence integrity and documentation matter.
- Distinguish underlying evidence from analytical conclusions.
- Evaluate AI-assisted legal research and digital investigation.
- Determine when a cybersecurity professional should stop, escalate, or seek additional authority.
- Develop and defend a professionally responsible course of action.

- Develop and defend a professionally responsible course of action.

Course Objective Connection

This week's work primarily develops your ability to differentiate ethical, legal, regulatory, and policy considerations affecting cybersecurity and cybercrime.

You will also apply ethical reasoning and legal principles to authorized access, hacking, incident response, digital evidence, and professional conduct.

The case work will require you to identify stakeholders, legal obligations, ethical conflicts, privacy concerns, security risks, and appropriate courses of action.

Authorization Comes Before Testing

A cybersecurity tool does not know whether you have permission to use it.

A vulnerability scanner can be used during:

- an authorized penetration test;
- a cybersecurity lab;
- a CTF;
- a vulnerability disclosure program;
- a bug bounty program;
- an unauthorized scan of someone else's systems.

The technology may be identical.

The authorization is not.

Before performing security testing, professionals need to understand exactly what they have permission to do.

That may include:

- which systems are in scope;
- which systems are excluded;
- when testing may occur;
- which techniques are permitted;
- which techniques are prohibited;
- how discovered data should be handled;
- how findings should be reported;
- when testing must stop;
- who should be contacted if something unexpected happens.

When scope is unclear, the professional response is not to guess.

Clarify the authorization before proceeding.

Cybercrime and the Computer Fraud and Abuse Act

One of the federal laws you will encounter this week is the Computer Fraud and Abuse Act, commonly called the CFAA.

You do not need to memorize the entire statute.

Instead, we will focus on concepts that cybersecurity professionals need to recognize, particularly:

- access without authorization;
- exceeding authorized access;
- knowledge and intent;
- authorization boundaries.

Required Resource

U.S. Department of Justice – Computer Fraud and Abuse Act guidance

https://www.justice.gov/jm/jm-9-48000-computer-fraud (https://www.justice.gov/jm/jm-9-48000-computer-fraud)

When reading legal material, pay attention to the exact language being used.

Avoid turning complex legal concepts into oversimplified rules.

For example, do not assume that every violation of an employer policy, website rule, or terms-of-service agreement automatically establishes a federal computer crime.

Security Research and Vulnerability Disclosure

Finding a vulnerability creates another important professional question:

What are you authorized to do with it?

Discovering a vulnerability does not automatically authorize you to exploit it further.

Professional security researchers need to understand:

- vulnerability disclosure policies;
- authorized testing scope;
- prohibited activities;
- privacy requirements;
- data-handling expectations;
- reporting procedures;
- disclosure expectations;
- safe-harbor language.

CISA Resource

CISA Vulnerability Disclosure Policy Template

https://www.cisa.gov/vulnerability-disclosure-policy-template (https://www.cisa.gov/vulnerability-disclosure-

https://www.cisa.gov/vulnerability-disclosure-policy-template (https://www.cisa.gov/vulnerability-disclosure-policy-template)

We will use vulnerability disclosure guidance to examine how organizations can establish clearer expectations and authorization for security researchers.

Class Meeting 1

When Does Security Testing Become Unauthorized Access?

During the first class meeting, you will work through situations involving:

- vulnerability scanning;
- penetration testing;
- scope;
- unauthorized access;
- computer misuse;
- vulnerability disclosure;
- responsible security research;
- AI-assisted legal research.

You will begin with a scenario involving a cybersecurity student who discovers a vulnerable system belonging to a local business and decides to investigate further without first obtaining authorization.

The question will not simply be whether the student meant well.

You will determine where professional security research should stop when authorization does not exist.

Scope Challenge

You will work with a fictional penetration-testing authorization that defines:

- an authorized network range;
- testing times;
- prohibited techniques;
- excluded production systems.

During the assessment, your team discovers additional systems, cloud services, credentials, and third-party resources.

You will decide whether each discovery is:

- clearly in scope;
- clearly out of scope;
- unclear and requiring additional authorization.

The goal is to develop a habit that matters in professional cybersecurity:

When the scope is unclear, stop and clarify.

AI-Assisted Legal Research

AI can be useful when working with difficult legal material.

You may use ChatGPT Edu to:

- explain unfamiliar terminology;
- identify questions that require research;
- summarize a difficult passage after you have read it;
- identify competing interpretations;
- challenge your understanding;
- suggest authoritative sources to investigate.

AI is not the legal authority.

A confident answer does not make a legal claim accurate.

During Week 2, you will practice this workflow:

AI identifies a question → locate the authoritative source → verify the information → determine whether the source actually applies.

Between Class Meetings

DOJ Authorization Research

Review the DOJ CFAA guidance:

https://www.justice.gov/jm/jm-9-48000-computer-fraud (https://www.justice.gov/jm/jm-9-48000-computer-fraud)

Focus on the discussion of:

- access without authorization;
- exceeding authorized access.

Come to Class Meeting 2 prepared to discuss:

1. One important distinction between the two concepts.
2. One part of the DOJ guidance you found surprising or particularly important.
3. One implication for penetration testers or security researchers.
4. One question you still have.

Read the actual DOJ material.

You may use ChatGPT Edu afterward to help clarify difficult language, but compare any AI explanation with the original source.

Class Meeting 2

Digital Evidence, Investigation & Legal Decision-Making

Cybersecurity incidents create evidence.

That evidence may help an organization:

- understand what happened;
- determine the scope of an incident;
- contain an attack;
- recover systems;
- identify responsible accounts or devices;
- support disciplinary action;
- support insurance or regulatory requirements;
- support a legal investigation.

How evidence is identified, collected, preserved, analyzed, and documented matters.

Sources of Digital Evidence

Depending on the incident, evidence may include:

- authentication logs;
- endpoint logs;
- firewall logs;
- cloud audit records;
- email;
- browser artifacts;
- file metadata;
- network traffic;
- memory;
- mobile-device data;
- security alerts;
- photographs or screenshots;
- forensic images.

Not everything produced during an investigation is underlying evidence.

An analyst's summary is an interpretation.

An AI-generated incident report is an interpretation.

The original logs or other underlying data remain critical.

Digital Forensics Foundations

Digital Forensics Foundations

You will use selected concepts from:

NIST SP 800-86 – Guide to Integrating Forensic Techniques into Incident Response

https://csrc.nist.gov/pubs/sp/800/86/final (https://csrc.nist.gov/pubs/sp/800/86/final)

You will focus on four broad activities:

Identification

What evidence may exist, and where might it be located?

Collection

How can relevant information be acquired appropriately?

Examination

What useful information can be extracted?

Analysis

What does the information mean when considered with other evidence?

You are not becoming a digital-forensics examiner in one week.

The goal is to understand why professional cybersecurity investigations require systematic handling of evidence.

Evidence Integrity and Chain of Custody

When evidence may become important to an investigation, professionals need to document how it was handled.

Relevant information may include:

- what was collected;
- who collected it;
- when it was collected;
- where it came from;
- how it was collected;
- integrity information such as hashes;
- who subsequently handled it.

A technically interesting file is less useful if nobody can explain where it came from or whether it changed.

AI-Assisted Digital Investigation

AI can also assist cybersecurity investigations

AI can also assist cybersecurity investigations.

Potential uses include:

- summarizing logs;
- identifying patterns;
- developing investigative questions;
- organizing timelines;
- explaining unfamiliar events;
- correlating information;
- helping organize reports.

These capabilities also create risks.

AI may:

- invent events;
- misinterpret timestamps;
- overlook context;
- create false correlations;
- omit relevant evidence;
- expose confidential information;
- generate conclusions that cannot be reproduced.

If an AI-generated incident summary says that an employee exfiltrated data at 2:14 a.m., the professional response is not simply to copy that statement into the incident report.

Return to the underlying evidence and verify it.

Evidence vs. Analysis

Throughout this week, keep this distinction in mind:

Source evidence → analysis → conclusion

A security tool alert is not automatically proof.

An AI-generated summary is not automatically proof.

An analyst's theory is not automatically proof.

Professional investigators should be able to explain what evidence supports their conclusions.

Mock Legal/Ethical Decision Exercise

During Class Meeting 2, you will examine a suspected insider incident.

The organization believes an employee may have copied proprietary information.

The employee uses a company laptop but also has a personal cloud-storage account accessible through the browser.

browser.

The security team may technically be able to access the personal cloud account.

Management wants the team to check everything.

An AI incident-analysis tool also suggests that company files were probably transferred to the personal account.

You will determine:

- what evidence actually exists;
- what remains an assumption;
- what the security team is authorized to examine;
- what privacy concerns exist;
- what evidence should be preserved;
- whether additional authority is required;
- how much weight the AI-generated conclusion should receive;
- what the security team should do next.

Mock Hearing

You will also participate in a professional mock hearing.

Possible roles include:

- security team;
- organizational management;
- employee representative or privacy advocate;
- legal/compliance reviewer.

The purpose is not to win an argument.

The purpose is to defend a cybersecurity decision using:

- evidence;
- authorization;
- legal principles;
- ethical reasoning;
- professional judgment.

Expect your assumptions to be challenged.

Your Week 2 Graded Work

Cybercrime Case Analysis

Points: 40

Category: Case Studies, Simulations & Interactive Activities

You will analyze a cybersecurity case involving security testing, unauthorized access, scope, cybercrime law, digital evidence, and professional responsibility.

Your analysis will require you to:

- identify what happened;
- distinguish facts from assumptions;
- determine what authorization existed;
- identify relevant legal issues;
- examine testing scope or access boundaries;
- identify relevant digital evidence;
- consider stakeholders and ethical concerns;
- research authoritative sources;
- evaluate AI-assisted research;
- recommend an appropriate professional response.

You are not expected to provide legal advice.

You are expected to recognize legal issues and know how to research, evaluate, and appropriately escalate them.

Mock Legal/Ethical Decision Exercise

Points: 15

Category: Knowledge Checks & Applied Analysis

This is your Week 2 applied analysis instead of a traditional quiz.

You will receive a short scenario requiring you to make a professional decision involving:

- authorization;
- scope;
- evidence;
- legal boundaries;
- ethical responsibility;
- AI-generated information.

You will need to make and defend a decision.

There may be more than one defensible response.

Preparation & Professional Engagement

Points: 10

Category: Professionalism & Engagement

This week's professional engagement includes:

- DOJ reading preparation;
- security-testing discussions;
- scope challenge;
- legal-source verification;
- digital evidence mini-lab;
- AI investigation analysis;
- mock hearing;
- evidence-based professional discussion.

Week 2 Checklist

Before completing Week 2:

- Participate in Class Meeting 1.
- Complete the security-testing opening analysis.
- Participate in the Scope Challenge.
- Review the CISA vulnerability disclosure resource.
- Participate in the AI-assisted legal research exercise.
- Read the assigned DOJ CFAA guidance.
- Prepare the four DOJ discussion items for Class Meeting 2.
- Participate in the digital evidence mini-lab.
- Work with the selected NIST digital-forensics concepts.
- Participate in the AI-assisted investigation discussion.
- Participate in the mock legal/ethical decision activity.
- Participate in the mock hearing.
- Submit the Cybercrime Case Analysis.
- Submit the Mock Legal/Ethical Decision Exercise.
- Complete required professional engagement activities.

Before You Leave Week 2

You should be able to explain why these statements matter:

Good intentions do not create authorization.

Finding a vulnerability does not automatically authorize you to exploit it.

When scope is unclear, stop and clarify.

Technical access does not automatically establish legal authority.

An analytical conclusion is not the same thing as the evidence supporting it.

AI can help identify legal and investigative questions, but authoritative sources and underlying evidence must be verified.

What to Expect Next Week

Week 3 moves into privacy, surveillance, digital identity, data protection, and regulatory obligations.

The questions become increasingly personal.

Who gets to collect information about you?

Who gets to monitor you?

What happens to the data after it is collected?

How much surveillance is justified in the name of security?

What rights do individuals have when organizations, cybersecurity systems, and AI technologies collect, analyze, infer, and act upon their data?

You will examine these questions through privacy and surveillance cases, stakeholder analysis, regulatory requirements, policy decisions, and technologies that increasingly make it possible to identify, track, profile, and evaluate people.