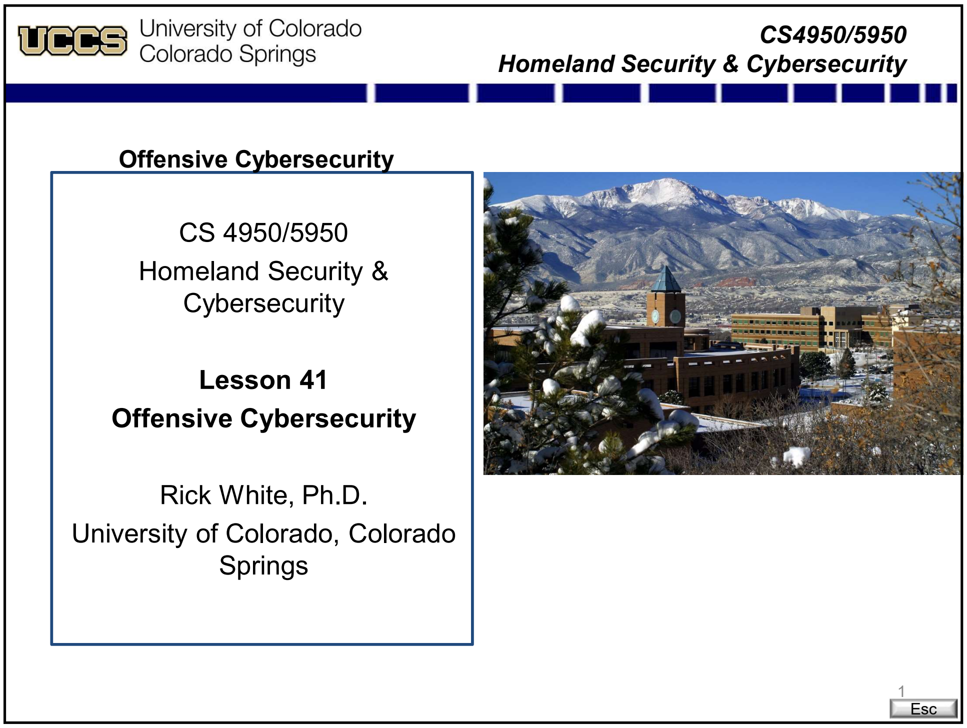


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Offensive Cybersecurity

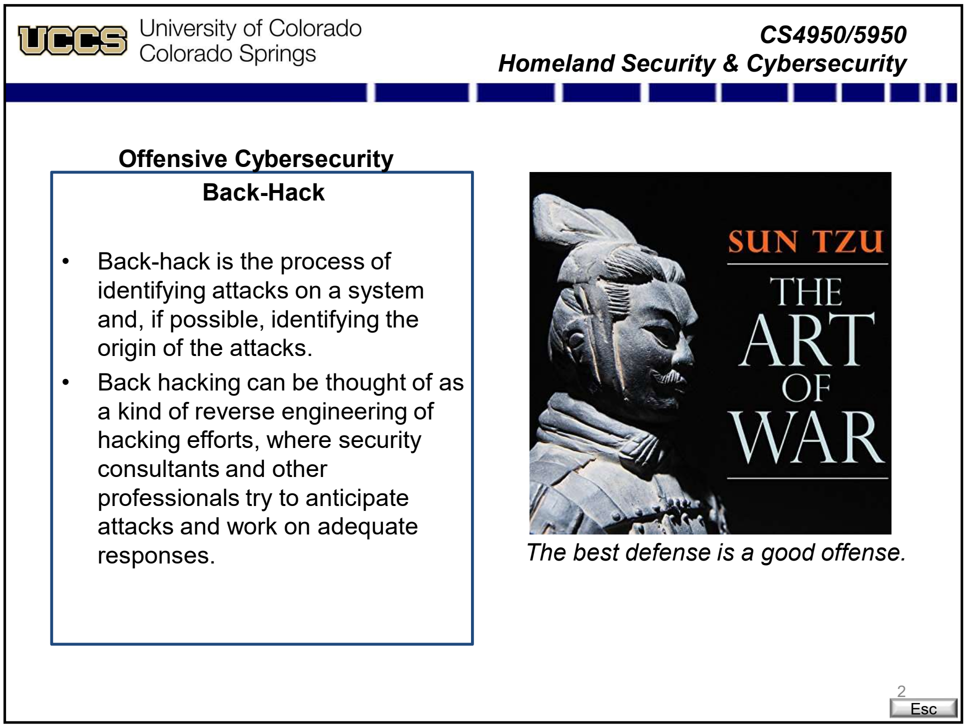
CS 4950/5950
Homeland Security & Cybersecurity

Lesson 41
Offensive Cybersecurity

Rick White, Ph.D.
University of Colorado, Colorado Springs

1
Esc

1



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Offensive Cybersecurity

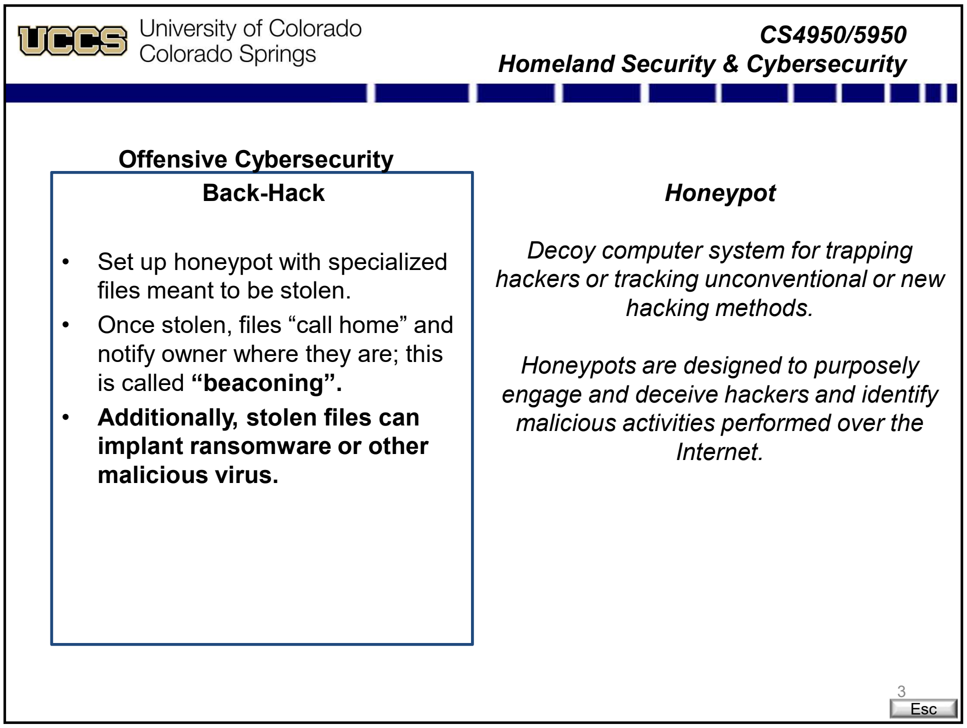
Back-Hack

- Back-hack is the process of identifying attacks on a system and, if possible, identifying the origin of the attacks.
- Back hacking can be thought of as a kind of reverse engineering of hacking efforts, where security consultants and other professionals try to anticipate attacks and work on adequate responses.

The best defense is a good offense.

2
Esc

2



UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Offensive Cybersecurity

Back-Hack

- Set up honeypot with specialized files meant to be stolen.
- Once stolen, files “call home” and notify owner where they are; this is called **“beaconing”.**
- **Additionally, stolen files can implant ransomware or other malicious virus.**

Honeypot

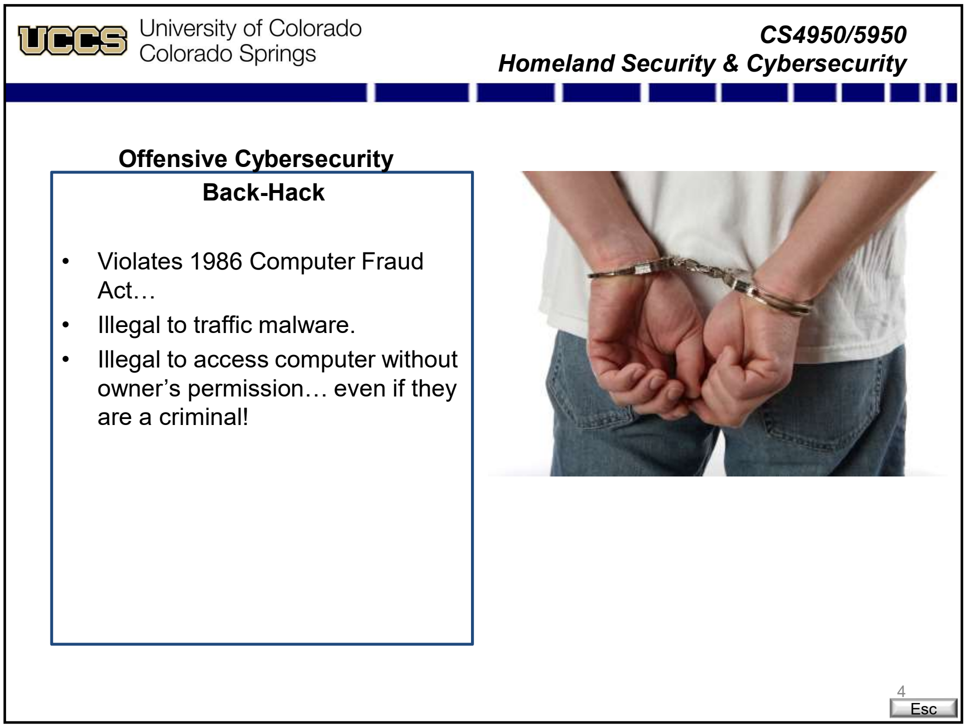
Decoy computer system for trapping hackers or tracking unconventional or new hacking methods.

Honeypots are designed to purposely engage and deceive hackers and identify malicious activities performed over the Internet.

3

Esc

3



UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Offensive Cybersecurity

Back-Hack

- Violates 1986 Computer Fraud Act…
- Illegal to traffic malware.
- Illegal to access computer without owner’s permission… even if they are a criminal!

4

Esc

4

Offensive Cybersecurity

Is this fair?

Offensive Cybersecurity

ACDC

- Active Cyber Defense Certainty (ACDC) Act
- Bipartisan bill introduced to Congress 13 Jun 19* by Reps. Tom Graves (R-GA) and Josh Gottheimer (D-NJ)
- **ACDC would exempt hacking victims from prosecution for mounting a back-hack defense.**

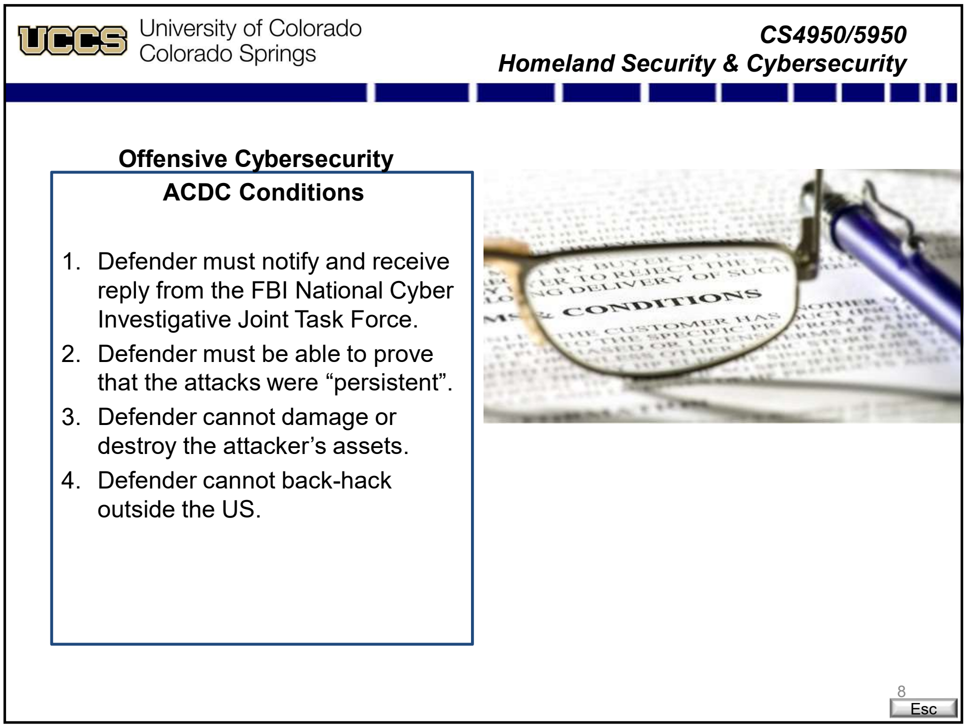
*Revised bill. Original bill introduced 13 Oct 17.

Offensive Cybersecurity

ACDC Provisions

1. Defender may access attacker's computer to establish attribution.
2. Defender may disrupt attack without damaging other computer.
3. Defender may retrieve and destroy stolen files.
4. Defender may even monitor attacker's behavior.
5. Defender can use beaconing technology.

7



Offensive Cybersecurity

ACDC Conditions

1. Defender must notify and receive reply from the FBI National Cyber Investigative Joint Task Force.
2. Defender must be able to prove that the attacks were "persistent".
3. Defender cannot damage or destroy the attacker's assets.
4. Defender cannot back-hack outside the US.

8

Offensive Cybersecurity

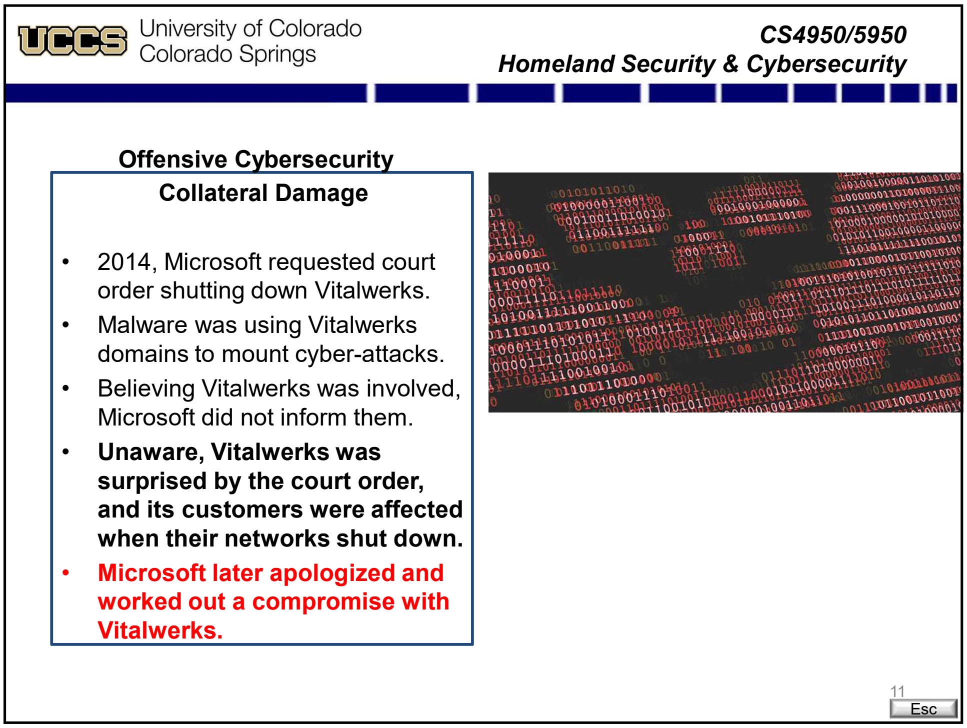
ACDC Advocates

1. Active-defense is effective.
2. Defenders already back-hacking.
3. ACDC unties hands of defenders.
4. ACDC will innovate cybersecurity.

Offensive Cybersecurity

ACDC Critics

1. Majority of hacks originate from outside the US, beyond ACDC.
2. Hard to prove “persistent” attack before conducting back-hack.
3. Deception could cause defender to back-hack innocent computers.
4. Successful back-hack could interfere with legal investigation.
5. Attackers could intentionally cause defenders to back-hack wrong computers, creating worse incident.



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Offensive Cybersecurity

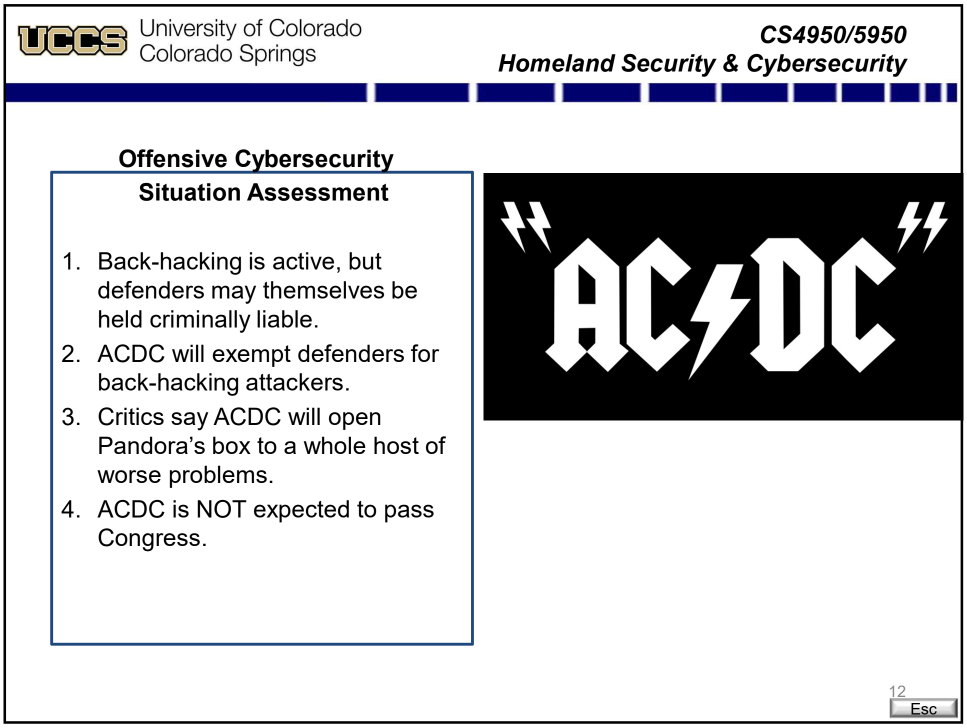
Collateral Damage

- 2014, Microsoft requested court order shutting down Vitalwerks.
- Malware was using Vitalwerks domains to mount cyber-attacks.
- Believing Vitalwerks was involved, Microsoft did not inform them.
- **Unaware, Vitalwerks was surprised by the court order, and its customers were affected when their networks shut down.**
- **Microsoft later apologized and worked out a compromise with Vitalwerks.**

11

Esc

11



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Offensive Cybersecurity

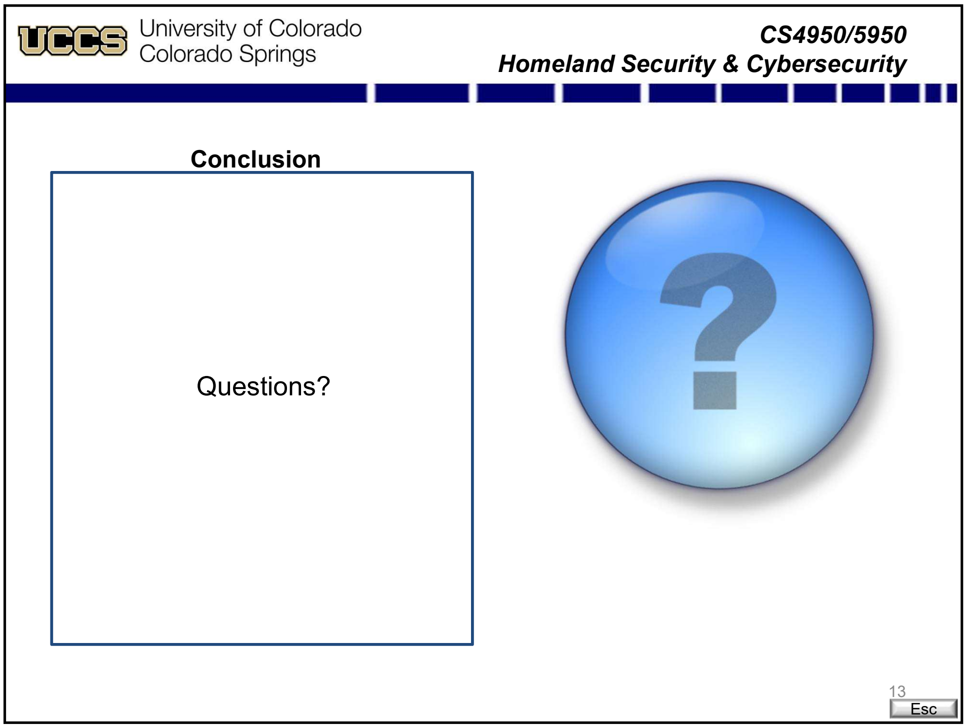
Situation Assessment

1. Back-hacking is active, but defenders may themselves be held criminally liable.
2. ACDC will exempt defenders for back-hacking attackers.
3. Critics say ACDC will open Pandora’s box to a whole host of worse problems.
4. ACDC is NOT expected to pass Congress.

12

Esc

12



UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?

13

13