eDynamicLearning

CAREER & ELECTIVE COURSES

INFORMATION TECHNOLOGY

Cybersecurity 1b

Defense Against Threats

Course Syllabus

Cybersecurity 1b:
Defense Against Threats

Course Code: EDL099

Course Description

Ever wonder what it's like to be a hacker? Or think about who is trying to steal your passwords while you're shopping online using the free Wi-Fi at your local coffee shop? Unmask the cybersecurity threats around you by understanding hackers and identifying weaknesses in your online behavior. Learn to avoid the various types of cyber attacks, including those to your social media accounts, and to predict the potential legal consequences of sharing or accessing information that you do not have rights to. Dig into these crimes in depth by taking a look at cyber forensics and other cybersecurity careers. In a world where such threats have no boundaries, cybersecurity will undoubtedly play an increasingly larger role in our personal and professional lives in the years to come.

Required Materials

- Slide-show presentation program
- Word processing program

Software:

Wireshark: https://www.wireshark.org/#download

In order to run Wireshark on your machine, you need:

- Hard disk: USB memory stick (Recommended to be at least 4 GB)
- Memory: 2+GB RAM
- Supported Operating System: Windows, Mac OS X

Software:

Virtual Box: https://www.virtualbox.org/wiki/downloads

In order to run VirtualBox on your machine, you need:

- CPU: Recent Intel or AMD processor
- Memory: 2+GB RAM
- Hard disk: About 4GB free hard disk space
- Supported Operating System: Windows, Mac OS X, Linux, Solaris and OpenSolaris

Other Materials

- USB memory stick (Recommended to be at least 4 GB)

Optional Materials

(The following materials will only be needed if student chooses to do some activities/labs by hand.)

- Printer
- Blank paper (a variety of sizes)
- Markers, crayons, pens, pencils

Note: Your state's standards for this Cybersecurity course may require students to purchase and to install security equipment. Check with your school's administration to determine if this is necessary for course completion. This course provides alternate activities that could address these standards.

Table of Contents

Unit 1: Cybersecurity Threats

Unit Summary

Even though it's a major part of modern life, the internet is still a pretty new invention. And, like any emerging innovation, it has drawbacks. Recognizing these vulnerabilities is important because they give us, as users, the power to see danger and predict problems in cyberspace. There must be a way to protect ourselves from online threats while still enjoying the endless benefits of the web, right? Yes—the answer is most definitely, yes. In fact, it is the main objective of any good cybersecurity effort. Once we are able to identify and respond to the shortcomings of the internet and step up our own defensive behavior as a result, we bring ourselves that much closer to improving, maintaining, and enjoying one of the most valuable technological resources in the world.

Learning Objectives

- Explain the motivations behind cyberattacks
- Understand the strategies of ethical and malicious hackers
- Identify the tools and strategies hackers use to gain access to computer systems
- Describe the impact of cyber breaches on individuals, society, and the world

Unit 2: Laws, Ethics, and Digital Boundaries

Unit Summary

Would you ever walk into a store and start breaking things just to see what happens? What about stealing something just to see if you get caught? The reasons you give for why you would or would not do such things are a part of your ethics, or sense of right and wrong. Similarly, whenever you log on to a computer, pick up your smartphone, or access a website, you must also use good judgment. When you're on the internet, it's supremely important to behave the same way you would in real life—with integrity, honesty, and a serious regard for the law. Because our online presence can feel anonymous on some level and less "observable" by others, it becomes easier to believe your digital boundaries don't impose any real limits—but they do. You may be surprised to learn just how many of your clicks, keystrokes, and online movements are tracked by outside entities looking to either enforce or breach security. As a result, it's important to fully understand how you can navigate and enjoy the internet while still keeping yourself—and your precious data—safe in every way.

Learning Objectives

- Identify key legislative acts that impact cybersecurity
- Define "netiquette" and how it applies to the field of information technology
- Understand consequences associated with unethical online practices, both personally and professionally
- Explain digital rights management and the importance of intellectual property

Unit 3: Black Hats

Unit Summary

While it may seem like just about everything can be found on the internet these days, the truth is Google itself has only indexed about 200 terabytes of data, which translates into a mere 0.004 percent of the total internet. This begs the question, what else is out there? The answer to this question would surprise most people, as it reveals there's a lot more happening on the internet than most of us can see or access. And understanding a bit more about this complicated online realm can also provide insight about the natural habitat of hackers and how they use it to cultivate their cyber threats. Once we grasp the many ways this larger environment can affect our own online security, it also becomes easier to protect all aspects of privacy.

Learning Objectives

- Understand the significance of the darknet
- Identify key issues related to online privacy
- Describe the various methodologies used by hackers
- Explain how malicious actors camouflage their communications

Unit 4: Cyber Safety

Unit Summary

As we know, the internet can be viewed as one giant analogy for our lives in the real world. The terminology, the construct, the vulnerabilities, the philosophies—they all relate back to what we, as humans, already know and understand about our surroundings. Since the dawn of humankind, we have been required to protect ourselves from predators, from enemies, from starvation, and cold weather. And, in the real world today, we still take endless precautions to protect ourselves from a host of new threats, including those found online. If we don't, we may likely suffer the digital equivalent of a tiger attack, otherwise known as an exploit. So, no matter what you read and learn throughout this cybersecurity course, the most important takeaway is remembering how to keep your data (and your physical self) safe in the digital world. Just as the hunters and gatherers of long ago knew how to read their landscape for danger, we too must observe our online surroundings with the same degree of caution and good judgment.

Learning Objectives

- Identify and understand different types of social engineering attacks
- Explain how social media affects cybersecurity and personal privacy
- Discover ways to prevent and stop cyberbullying
- Recognize the importance of security for email and web browsing

Midterm Exam

Learning Objectives

- Review information acquired and mastered from this course up to this point.
- Take a course exam based on material from the first four units in this course (Note: You will be able to open this exam only one time.)

Unit 5: Personal Cybersecurity Inventory

Unit Summary

Take it from the experts: there are a lot of threats out there in the digital world! And to truly protect your virtual self from malicious actors, you will need to learn more about the art of anticipating, detecting, and mitigating risk through your own best practices. This means listening to the advice of various authorities in the cybersecurity field and learning how to use their knowledge to forge a stronger and more effective personal protocol for the internet and beyond. Once you understand how to turn your security knowledge into practical protection efforts, the internet becomes a more welcoming and enjoyable place for everyone.

Learning Objectives

- Describe ways to safeguard yourself and your digital assets
- Identify national organizations that post bulletins and warnings about cyber risks
- Create a plan for how you will improve your cybersecurity
- Explain the importance of online identity management and monitoring

Unit 6: White Hat Hackers

Unit Summary

Considering recent cyberattacks, it's easy to assume the world has reached the absolute apex of digital chaos. After all, outside hacking forces have been accused of tampering with national elections, swaying popular sentiment through fake online news, and stealing big data from giant corporations and governments—how could it possibly get any crazier? At times, it can feel a bit like the black hats have taken over the virtual realm and robbed us all of our freedom to move about the internet with safety and confidence. Some hackers claim they can weaponize a commercial airliner by overwriting the flight controls, while others say shutting down the power grid of a whole city is entirely feasible. While some of this may be true, the digital war is far from lost. With the help of ethical hackers and cyber do-gooders, it is possible to actively assess the risks we face and successfully stamp out threats at every turn. Yes, it's a big job. And yes, it is only going to get bigger. So, the question is, are you ready to join the forces of good?

Learning Objectives

- List the four levels of risk assessment
- Explain the principles and practices behind ethical hacking
- Identify assessment tools and techniques to identify security risks
- Debate the appropriateness of both ethical and malicious hacking

Unit 7: Incident Response, Investigations, and Digital Forensics

Unit Summary

No one really thinks about a crisis until it happens. When our personal devices, privacy, and information are attacked, finding the best way to recover and move on is the only thing that matters. How we respond, investigate, and use science to accomplish these goals becomes valuable to our livelihood. By learning how to best handle a breach in security, we can begin to see more about our general vulnerabilities and how we—and the world of law enforcement—can continually work to improve our systems and our security.

Learning Objectives

- Identify common risks, alerts, and warning signs of a compromised system
- Explain the five steps in the digital forensics process
- Give examples of how computer forensics affects law enforcement and private citizens
- Recognize the types of information recovered through computer forensics

Unit 8: Cybersecurity Careers

Unit Summary

In the world of cybersecurity, the demand for talented and dedicated people never stops. Most experts agree this emerging field is not only an exciting and robust one, but it may just be the single most important industry to arise in our nation since the Industrial Revolution. Now that's a big deal! And with this assertion comes all sorts of new ideas about how to launch a cyber career. Not only are the positions plentiful, but they offer a large degree of financial security and the chance to make a real difference in the safety of the nation, its technology, and its people.

Learning Objectives

- Pinpoint the information technology skills required for career development
- Explain the important functions resumes and portfolios play in the workplace
- Identify various employment requirements and opportunities in the cybersecurity field
- Describe the value of positive work behaviors and how they affect professional success

Final Exam

Learning Objectives

- Review information acquired and mastered from this course up to this point.
- Take a course exam based on material from units five to eight in this course – the last four units. (Note: You will be able to open this exam only one time.)