CYB 301 – Rules of Engagement

The following are rules of engagement (ROEs) for students enrolled in CYB 301, Hacker Tools and Techniques. All students **must** follow ROEs when performing any type of cyber-related tasks pertaining to Oregon Tech's cybersecurity curriculum, in and out of assignment environments. Violations of any or all ROEs may result in failure of assignments and potential drop from the course.

1) You **shall not** scan nor exploit any systems at any time.
    a. You must receive explicit permission from your instructor for any type of active exploits.
2) You **shall not** take advantage of or publicize any vulnerabilities found during passive footprinting. If vulnerabilities are found, alert your instructor for guidance.
3) You **shall not** disclose any sensitive information pertaining to businesses.
    a. This includes, but not limited to, business operations, business information systems, employees, owners, and customers.
    b. Sensitive information includes, but not limited to, full names, phone numbers, addresses, age, marital status, family members (immediate / extended), criminal backgrounds, financial information.
    c. You will prepare this information in a document required for lab assignment submission.
4) You **shall not** perform any type of active footprinting.
    a. Active footprinting includes, but is not limited to, social engineering of any type, live interaction with current or former employees, visitation of any business with a purpose other than normal business interaction, and any active electronic interaction.
5) Scanning, enumeration, sniffing, or exploitation tools and techniques may **only be performed on approved information systems** explicitly assigned to you by your instructor.
    a. Any type of activity related to active penetration testing, or ethical hacking, **will result in failure** of current assignments, and possible failure of the course.
6) Any communications related to your findings will be diectly with your instructor, or, through documents submitted via the Learning Management System, e.g., Canvas.
    a. **Do not** use your @oit.edu nor any personal e-mail addresses to communicate findings.
        i. This includes your alter ego e-mail account(s).
7) If compromised systems are found, **do not** take any action on that system.
    a. Alter your instructor of your findings and for additional guidance.
8) It is **highly-recommended** to use virtual machines for all cyber-related tasks.
9) It is **recommended** you create an alter ego for accounts requiring login information. This includes an e-mail account, social media accounts, and possibly job website user accounts.
    a. Alter ego accounts are for *your* protection. We never perform reconnaissance using anything related to ourselves.
10) You **may** collect as much information as possible using the tools and techniques discussed in this course via publicly accessible channels, e.g., the Internet.

CYB 301 – Rules of Engagement

11) Creativity is a key factor to success.
   a. To get the information you are seeking, you will need to think outside of the box. There is no 'perfect' or 'prescribed' way of doing business in cybersecurity. Do what you can to collect information **legally** and **ethically**.

The bottom line: treat all information as if it were your own. You are the security professional and must operate with the **highest level of ethics at all times**. Not doing so puts you, your customer, innocent civilians, and Oregon Tech at risk.