

**Lab 1: *Websites, Breaches & Games***

**Overview:**

This lab introduces you to a number of resources that can be used for daily updates, some provide education material, and others dates for local gatherings of IT Security professionals. You also get an opportunity to analyze some data breaches posted on the Internet. What you will do is try to break the stories into component parts so you can see what happened, what was lost etc.

At the end of the lab you have the opportunity to play a simple cyber security game. While it is simple, it does introduce some basic IT Security concepts.

**Objective:**

1. Investigate and assess online resources
2. Analyze breaches that have been in the press
3. Defend a company with cyber security techniques
4. Play a game to enhance your knowledge
5. Submit properly formatted professional looking report of your findings

**The Lab Activities**

**Resources**

This part is all about getting to know some of the resources available to you as an IT Security professional in training. Take your time and look at the resources below.

From the “News and Blogs” section, identify what you consider to be the top 3 general sites and top 3 specialized sites, in ranked order i.e. list then as 1, 2, 3, with 1 being what you consider the best site.

**In your lab report:**

1. **List the top 3 general sites with an explanation of why you picked those sites and why you ranked them in that order.**
2. Wired
   * Focuses on business security and new technology base on AI technology, automation devices and robot
3. ZD Net
   * New technology website just released focus on business technology, education, agriculture, software and mobile security
   * They give product reviews and client can be able to download the specific security software from company website.
4. The Register

* Focus on business security, software and hardware part.
* Release a newspaper article periodically

1. **List the top 3 specialized sites with an explanation of why you picked those sites and why you ranked them in that order.**

* **Naked Security**
  + Provide antivirus software for free to client to protect endpoint devices
  + Provide wide-range of security to million clients all over the world with specific technology.
* **The hacker News**
  + High rating newspaper platform in IT security field
    - More than 8 million subscribers from all over the world
    - Latest update technology from the Internet
    - Leading the future with new technology
* **Threatpost**
  + Good information about business security and
  + Great company team for making the great contend as video and report about security and IT field

1. **Provide a description of each of the security conferences and local groups. What is their focus? Who is their audience? What is interesting about each? Find interesting videos of some talks at these conferences. Describe them.**

* [DEF CON](https://www.defcon.org/)
  + Started in 1993
  + One of the largest hacker convention and attendees include:
    - Computer security professionals
    - Journalists
    - Lawyers
    - Federal government employees
    - Students
    - Hackers
  + The event consists of several tracks of speakers about computer- and hacking-related subjects, as well as cyber-security challenges and competitions
  + Known for its “capture the flag” contests
    - A hacking competition where teams of hackers attempt to attack and defend computers and networks
* [black hat](https://www.blackhat.com/)
  + Security consulting, training, and briefings to hackers, corporations, and government agencies around the world.
  + Brings in people who are interested in information security ranging from non-technical individuals, executives, hackers
  + 2 sections in black hat:
    - Briefing:
      * Composed of tracks, covering various topics including reverse engineering, identity and privacy, and hacking. The briefings also contain keynote speeches from leading voices in the information security field
    - Training:
      * Training is offered by various computer security vendors and individual security professionals.
* [SECTOR](http://sector.ca/)
  + IT Security professionals gather to learn from and network with the world’s most innovative, intellectual, exciting and entertaining security professionals.
  + Built a reputation of bringing together experts from around the world to share their latest research and techniques.
  + Sheds light on the underground threats and mischief that threaten corporate and personal IT systems. Through identifying, discussing, dissecting and debating these digital threats, the strongest defences can be mounted.
* [BSides (Toronto)](http://www.bsidesto.ca/)
  + Bring the Toronto InfoSec community together for a conference about the excitement, joy, and surprise of Information/Cyber Security.
  + Goal is to expand the spectrum of conversation beyond the traditional confines of space and time.  It creates opportunities for individuals to both present and participate in an intimate atmosphere that encourages collaboration. It is an intense event with discussions, demos, and interaction from participants. It is where conversations for the next-big-thing are happening.
* [BSides (Las Vegas)](http://www.bsidesto.ca/)
  + an Information / Security conference that’s different. We’re a volunteer organized event, put on by and for the community, and we truly strive to keep information free.
  + the original and largest Security BSides Conference, it is only one of many in a global movement that aims to increase InfoSec awareness, provide low-to-no-cost education, initiate conversations, and foster community and collaboration.
  + over 300 events, in 100 cities in 26 countries on 6 continents
* Hackfest
  + largest hacking event in Canada and brings together more than 900 computer security enthusiasts
  + takes place over two days of technical conferences about security and hacking and is preceded by 3 days of training.
    - measure their security and hacking skills in a unique CTF (Capture The Flag). The whole evening is accompanied by a lockpicking contest, DJ atmosphere, workshops, evening conferences, live podcast recording and more.
  + The three (3) days before the event we offer international quality training on various topics of hacking and security
* CanSecWest
  + the world's most advanced conference focusing on applied digital security, is about bringing the industry luminaries together in a relaxed environment which promotes collaboration and social networking.
  + lasts for three days and features a single track of thought provoking presentations, each prepared by an experienced professional and talented educator who is at the cutting edge of his or her field.
    - one hour presentations over the duration beginning at 9:00 a.m.
* [TASK](file:///C:\C:\Temp\task.to)
  + Forum for experts to encourage discussion and share expertise in understanding the latest trends and security threats facing computer networks, system and data
  + informal get-together of Information Security professionals (and those who want to be professional) that is held monthly in the Greater Toronto area.
  + Discuss about:
    - New technologies and products that impact information security
    - Emerging threats, and the vulnerabilities being exploited
    - Managing security
    - New laws and regulations
  + encourage discussion and share expertise in understanding the latest trends and security threats facing computer networks, systems and data.
    - non-biased forum to discuss issues
  + Membership is free and encourage full and active participation
* [OWASP (Toronto)](https://www.owasp.org/index.php/Toronto)
  + Open Web Application Security Project (OWASP) is a worldwide not-for-profit charitable organization focused on improving the security of software
  + mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.
* DEFCON416
  + free an open community for anyone interested in information security & computer hacking.
  + All skill levels and background experiences are welcome.
  + increase the awareness of ethical hacking and develop a community that will participate in active monthly hacker events
  + Meetup every month
  + Discuss about web applications, reverse engineering, mobile hacking, IOT, automobile hacking.

**News & Blogs**

Security news is widely available today. Nearly all the major general news sites have a section on “technology”. Computing news sites usually have a section on IT Security and there are specialist IT Security sites.

*General*

* [Wired](https://www.wired.com/)
* [Tech News World](http://www.technewsworld.com/)
* [Computer Weekly](http://www.computerweekly.com/)
* [The Register](http://www.theregister.co.uk/)
* [Computer World](http://www.computerworld.com/)
* [SC Magazine](http://www.scmagazine.com/)
* [ZD Net](http://www.zdnet.com/)
* [PC Magazine](http://www.pcmag.com/reviews/security-software)

*Specialized*

* [Krebs on Security](http://krebsonsecurity.com/)
* [The Hacker News](http://thehackernews.com/)
* [Dark Reading](http://www.darkreading.com/)
* [Threat Post](https://threatpost.com/)
* [Security Weekly](http://securityweekly.com/)
* [Security Affairs](http://securityaffairs.co/wordpress/)
* [Naked Security](https://nakedsecurity.sophos.com/)

**Conferences**

Conferences are great to attend. The local conference, SECTOR, offers a limited number of student tickets. Many of these conferences provide their presentations online after the conference.

* [DEF CON](https://www.defcon.org/)
* [black hat](https://www.blackhat.com/)
* [SECTOR](http://sector.ca/)
* [BSides (Toronto)](http://www.bsidesto.ca/)
* [BSides (Las Vegas)](http://www.bsidesto.ca/)
* Hackfest
* CanSecWest

**Local Groups**

There are also free local special interest groups that you can attend. They provide an opportunity for students to network within the industry.

* [TASK](file:///C:\C:\Temp\task.to)
* [OWASP (Toronto)](https://www.owasp.org/index.php/Toronto)
* DEFCON416

**Part 2: Breaches**

The purpose of this part of the lab is to analyze some of the privacy breaches that have been in the press. Doing so will allow you to create a comprehensive picture of these breaches and their implications for the companies and their customers.

1. Search the Internet and identify 1 breach e.g. Home Depot. Try to find several references for the breach, as this will give you more information about what happened and the outcomes.
2. Identify for the breach the following data:

|  |  |
| --- | --- |
| **Data** | **Description** |
| Company: | Company attacked |
| Method: | Method of breach i.e. how was it done |
| Data Lost (volume) | Amount of data lost |
| Data Lost (types) | Types of data lost e.g. names, addresses, credit card details etc. |
| Company Impact | Known or likely impact on the company e.g. will the company lose $$$, customers? |
| Customer Impact | Known or likely impact on those parties who have had their data lost |
| Remedial Action (data loss) | Steps taken to address the data loss i.e. are they doing anything for their customers? |
| Remedial Action (breach) | Steps taken to stop the breach happening again |

NB: You may not be able to get all the information above about a breach.

1. In your lab report write up your breach covering the topics above. The write-up should be in the format given in the lab assignment template.

**Part 3: Do one of the following 2 options**

**Option 1 (not challenging): Cyber Attack**

In this section of the lab you get to play a cyber security game using the PBS NovaLab Cybersecurity website: ‘http://www.pbs.org/wgbh/nova/labs/lab/cyber/’ . It provides an enjoyable introduction to cyber-attacks, cyber defense and cyber budgets.

Through the lab you’ll receive a basic introduction to cyber-attacks including password cracking and social engineering. Your goal will be to complete all 3 levels of the Cybersecurity Lab.

1. Navigate to the website: ‘http://www.pbs.org/wgbh/nova/labs/lab/cyber/’
2. Click on ‘PLAY GAME’
3. Sign into that game as a ‘Guest’
4. Successfully complete all three (3) levels of challenges.
5. Take a screen shot of the Level 3 page showing all challenges complete and save it as <<MySenecaUsername>>\_CLG\_L<<X>>.jpg
6. Insert the screenshot into your report under the heading: “Part 3: Cyber Security Game”

**Option 2 on next page**

**Option 2 (challenging): War Game**

In this section of the lab you get to play a type of computer war game known as Capture the Flag (CTF). There are many CTF games available on the Internet and at security conferences. The one we will start with is named Bandit, available at ‘<http://overthewire.org/wargames/>’. The wargames offered by the OverTheWire community can help you to learn and practice security concepts in the form of fun-filled games.

1. Navigate to the website: ‘http://overthewire.org/wargames/’
2. Click on the link named ‘Bandit’ in the left hand column
3. Read the instructions and start playing the game
4. Successfully complete as many levels as you can before the due date. Document the steps you took to achieve success on each level. Include this documentation in your report.
5. Take a screen shot (with personally identifiable information) of the final login challenges complete and save it as <<MySenecaUsername>>\_CTF<<X>>.jpg
6. **Insert the screenshot into your report under the heading: “Part 3: CTF”**

**Part 4: Report Submission**

Now that you have filled out the Lab report, you need to submit it. This is done through the submission link given with Lab 1 on Blackboard.

**Deliverable**

Submit your Lab report as a PDF“.pdf” format through the course’s web site with the following name:

* <<MySenecaUsername>>\_L1.pdf

For example, if my MySeneca username was “john.doe”, then the file should be “john.doe\_L1.pdf”. The angle brackets “<<” and “>>” show where information should be changed/customized, and they should not be included in the filename.

Note:

* Submissions deadlines are given through the lab submission link.
* You must cite your sources. Failure to do so will be considered plagiarism.