**BTN710: Assignment #1 Guidelines (20%)**

**Group Research Topic**

**Assignment Overview**

The goal of this assignment is to work in teams and for the teams to show either an ‘exploit in action’ or an ‘exploit in code’.

The assignment must be “applied” research including programming, not merely a “research” paper.

Any project/topic is permitted, though instructor approval of the topic is required. The completed work will need to be:

1. Written up in a report
2. Presented in a video presentation
3. Hosted on a secure, password protected website i.e. your report and video need to be hosted on the website

The project has several deliverables:

1. Team and team role selection
2. Topic selection and approval
3. Report – a write up of your teams’ applied research
4. Video presentation of work done
5. A secure project website that hosts:

* Report
* A link to the video presentation

1. Sign-off document

**Goals**

There are a number of goals this assignment.

1. To give you an opportunity to work in teams.
2. To allow you to explore and research a topic "beyond the classroom" related to IT security and hopefully have some fun in doing so.
3. Get practical experience preparing a report and professional video presentation (6-10 minutes).  Many of you will have already have noticed that a good number of organizations have informational videos on YouTube rather than formal documents available on their websites. Often, you find a combination of both. This will put you in a good position to do both if so called upon.
4. Ensure you can produce materials on your topic of choice that are relevant, accurate, and logically organized, and of a standard that you would share with a future employer.

**Deliverable #1: Team and Team Role Selection**

This assignment should be done in a team of either 3 or 4 students. Where possible, there should be an even balance of work across all team members, with all members participating in conducting the research, preparing the report and preparing the video presentation etc. Each team must appoint members to the following roles:

*Team Leader:*

* Responsible for chairing meetings
* Ensuring material is completed on time
* Communicating with the instructor as required – all communications must cc’ the other team members
* Responsible for working out any problems within the group
* Submission of all deliverables

*Leads:*

* *Web Master:* Responsible for creation of the secure web site and posting the required items
* *Report:* Responsible for the creation of the report
* *Video Presentation:* Responsible for the creation of the video presentation

**NB:** Every team member must do a role and only one student can be assigned a role. In teams of less than 4 students, a student may do two roles**.**

***Team Problems***

This course is late in the BSD program, it is expected that you are well experienced in working in teams and dealing with team issues. **Given this, the instructor does not expect to be told of team problems at the last minute (i.e. 1 week before the end of the project) as this usually shows that a team has left things to the last minute and the issues often arise from poor planning.** If the team cannot resolve the problem a Problem Report can be filled and submitted to the instructor through e-mail, cc’ing all team members. In the absence of a Problem Report, all team members will get the same grade.

***Deliverable:***

Team Role assignment uploaded to Blackboard (see timetable at end of document).

**Deliverable #2: Topic Selection**

There are two topic options:

1. **Exploit in Action**

Document a particular vulnerability or exploit of a host system. Describe the method used to attack the vulnerability/exploit, and explain the security policy process that would be used to deal with such an attack. You may need to set up a testing lab to demonstrate your exploit. It does not matter whether the exploit was successful; if your exploit failed, you need to document why (you may need to surmise what prevented the attack from working)

1. **Exploit in Code**

Analyze a previous web-based program you wrote from a security perceptive. Critically access your source code and use the Fortify Source Code Analysis Tool, or other testing tools, to find threats. Demonstrate how the existing code can be exploited by an attacker. Identify what changes would you make, and rewrite the code to improve program security and demonstrate that it is now secure.

NB: If your code has minor or no security threats, select a different program.

***Deliverable:***

Your proposed topic must be sent to the instructor by e-mail, with all team members being cc’ed (see timetable at end of document).

**Deliverable #3: Report**

The assignment report must meet the guidelines and section criteria (see below) and be hosted on the web (see Deliverable #4).

**Guidelines:**

* Title Page: Title, Assignment, Team Number, Team member names, Course Code.
* Table of Contents
* Report Body: <10 pages in length
  + Introduction
  + Section 1:The Exploit – Summary
  + Section 2: The Attack
  + Section 3: Security Policy
  + Conclusion
* Bibliography Page(s): this is a separate page(s) for your references and citations.

The Report Body and Bibliography:

* Each page should be:
  + Single-spaced line
  + 12 point font (Calibri) – this is non-header text
  + 2 cm margins
  + Header: Team Name & Course Code
  + Footer: Assignment No. & Page Number
* Each section should start on a new page

**Section 1: The Exploit – Summary**

This section provides a high level overview/summary of the work you did. Be certain to include each stage of an attack: reconnaissance, scanning, exploiting the system, system remediation, and retesting, ***as appropriate to your topic***.

* ***Brief Description***

A short description of what the exploit does/how it works (a detailed explanation will be given in Part 2).

* ***Operating System (OS)***

List the OS (s) affected, including specific version numbers/patch levels, if appropriate.

* ***Protocols/Services/Applications***

List the protocol, service, or application affected, including version numbers/patch levels, if appropriate.

* ***Variants***

The name(s) of different variants of the exploit, if any, include a brief description of the differences between any variants and the exploits you have selected.

* ***References***

Include a minimum of **four** URLs for information on the exploit. At least one link should be to a description of the vulnerability and/or exploit (i.e., vendor, CERT, or other security bulletins; links to listserv or other archives).

At least one link should be to the exploit itself (source code, tool).

**Section 2: The Attack**

In section the team will describe how the exploit was used to attack the host system or web application.

* ***Description and diagram of network***

Include a description of the network (or the relevant parts of the network) where the incident occurred. Outline the network configuration that would provide maximum efficacy.

* ***Protocol\Service Description***

In most cases, in order to understand the exploit, you need to understand how the protocol or service that is being exploited works and what its weaknesses are. Provide a brief description of the protocol, service, or application that the exploit uses.

* ***How the exploit works***

Provide a detailed description of how the exploit works and why it is able to exploit the particular vulnerability in the protocol, service, or application. What is it about the protocol/service/etc. that is being exploited that makes it vulnerable? You must provide a step-by-step analysis of the actions the exploit takes in this section. You must include relevant sections of source code to illustrate and explain what the exploit is doing. If any programs exist to exploit this vulnerability, explain how to use the program(s). In addition to the program description, discuss how you could manually run the exploit against a system if an automated program did not exist.

* Also, outline each stage of an attack, including reconnaissance, scanning, exploiting the system (gaining access, elevating access, application level access and/or denial of service). For each stage, provide details of the steps you performed, the commands that you typed, the tools that you used, and why each step was performed. Use as many screen shots as possible to document the process. Your documentation should be so clear that someone could take your report and reproduce the attack.
* ***Description and diagram of the attack***

Explain how the attack was carried out. Include a diagram to illustrate how the exploit would typically work. This section should also include sample output (screen captures, packet captures, etc. as appropriate) from running the exploit on a test network.

* ***Signature of the attack***

What traces of the attack are left on the system affected? Does the attack have a "signature" that could be used to detect or block it? If no, explain why no signature exists. If yes, describe the signature and include sniffer output, intrusion detection rules, log files, or other output (such as messages/syslog etc.) as appropriate and provide a description of what the output means.

* ***How to protect against it***

Describe what can be done to protect against the exploit and/or fix the vulnerability. This section should be covered in two parts. First, what can someone who is running the vulnerable software do so their system can not be compromised? Second, what could or should the vendor do to fix the vulnerability? Be sure to include applicable links to the relevant patches or workarounds and examples of required changes to systems to protect against the vulnerability.

* ***Remediated System Test***

If appropriate, describe the retesting of your system once remediation has been made to it, to demonstrate the system has been secured

**Section 3 – Security Policy**

Outline what parts of a security policy should be implemented to prevent this attack from occurring and how should the incidence reporting be handled.

***Deliverable:***

This report should be submitted through Blackboard (see timetable at end of document).

**Deliverable #4: Secure Website**

The team needs to create a website/page to host the report and the video presentation. Ensure your website is “password protected”. The password is to be ‘**btn710@G#**’. You need to ensure that the source code is properly encoded\encrypted to prevent reverse engineering the password).

***Deliverable:***

A website (page) that in a secure manner host the report and video presentation.

**Deliverable #5: Video Presentation**

As part of this assignment you will be required to put together a video presentation. The video will be used to present some or all of the material in your report i.e. you should use the report as the basis for your script. It can be made up of demonstrations, screen captures, animated PowerPoint, video clips, videos of group members speaking, and more.

* It should be between 6-10 minutes in length, though **should not exceed 10 minutes**.
* Each group member should speak, though does not need to be shown, in the video at some point.
* The video should have a clear introduction and closing and your topic should be well organized.

You may use any software, apps, hardware you have at your disposal to create your video.

To start the video making process, you should make a script or storyboard, using the information you have researched for your report, to determine what will be said and what information will be presented during each stage of your video. Screen casts, demonstrations, animations, PowerPoint and talking heads should be combined in your video. It is important to mix up the type of video clips you use in your video to make it interesting and entertaining.A good plan will help you achieve your goal.

Note: As you can imagine a simple video with PowerPoint slides and a voice over will be marked a good deal lower than one with a mix of video clips, slides and animations.

Once your video is complete:

* It must be uploaded to YouTube – the video format is up to you, as long as it is accepted by YouTube
* All copyrighted video, music, pictures, text, etc. must be cited at the end of the video in the credits
* Only the Team Leader needs to upload the video

***Deliverables:***

A video presentation

**Deliverable #6: Team Submission Sign-off**

* **All team members need to “sign off” on the project work, report, website/pave and video presentation.**
* **Sign off must be done before the team video presentation is due.**

***Deliverables:***

A team-sign off document submitted through Blackboard

**Deliverables**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Del.** | **What** | **Details** | **Submission** | **%** | **Date** |
| 1 | Team Members & Role Assignments | A document that lists the assignment of team members to roles.  **Must be uploaded to Blackboard**. | Blackboard | 1% | 11pm, Sunday, October 1st |
| 2 | Topic Selection | An e-mail that gives the topic and a 3-4 sentence description of the topic.  **Must be** **emailed to the course instructor** | Email | 2% |
| 3 | Report | Project report.  **Must be posted on Blackboard.** | Blackboard | 6% | 11pm, Sunday December 17th |
| 4 | Video presentation | Video presentation link placed on website (see Deliverable #4).  **Link to video presentation** submitted by **e-mail to course instructor.** | Link  Email | 6% | 11pm, Sunday December 17th |
| 5 | Website | Project website with specified security in place and hosting the report and link to the video presentation.  **Link to website submitted** by **e-mail to course instructor.** | Email | 5% | 11pm, Sunday December 17th |
| 6 | Team Submission Approval | A document with the signatures of all group members giving approval for the project website, project report and project video presentation (see project documents).  **Must be posted on Blackboard**  **Note: If this is not provided, the assignment will not be marked.** | Blackboard | 0% | 11pm, Sunday, December 17th |

Note:

Each group must complete **all** deliverables in order for the project website, report and presentation to be marked.

Specific grading criteria will be given at a later time.

NOTE**: It is unethical and criminal to access a network without the explicit written authorization from the owner and operators of a computer network or system. You should never attempt to penetrate a system or adversely affect a system's operation. Such actions are a violation of Seneca AUP and, in some cases, violations of Canadian Criminal Code. Likewise, you should refrain from writing computer viruses, worms, self-reproducing code, or other kinds of potentially damaging software for this course unless you have explicit, written approval for the specific type of software that you wish to create. These kinds of programs are notoriously difficult to control and their release (intentional or otherwise) can result in substantial civil and criminal penalties.**