SE 421: Project - Penetration Test

Due on December 5, 2018 at 12:00 PM (noon)

Instructor: Ben Holland

Student Name:

Problem 1

(10 points - Professionalism)

Your report will be graded on its professional quality. At a minimum your report should:

- Clearly document the names of each team member and their roles in the vulnerability assessment. Note that you should discuss with your team how to best balance the workload among all team members. Allowing team members to specialize on tasks that suit each team member's strengths may be one way to divide the workload, but is not required.
- Provide a table of contents
- Include page headers and page numbers
- Be single spaced with 1 inch margins
- Use an appropriate font (no Comic Sans)
- Be professionally typed (see Syllabus and Piazza clarifications for details)
- Use complete and grammatically correct sentences (run a spell checker)
- Include captions and identifiers for figures (Example: "Figure 2 - Shows XYZ")
- Include appropriate references and citations if needed
- Be complete in the sense that the report would enable a business executive to make an informed decision with the information contained in the report. To provide additional completeness you may wish to include citations to additional references.
- Be targeted at a professional audience. Present ideas clearly and succinctly. You may assume that your audience is vaguely familiar with the original project source code and with the basic concepts presented in this course (i.e. use the appropriate technical terminology, but also provide concise definitions of the concepts in laymen's terms). If you have difficulty writing, you may wish to seek advice from one of the Writing Media Centers on campus.

Problem 2

(10 points - Exploit Development)
For each identified vulnerability assess if the vulnerability is exploitable by developing an exploit for the vulnerability. Your exploit may be fully automatic or involve some manual steps. For each vulnerability in your vulnerability assessment report provide the following details:

1. Provide the vulnerability identifier listed in your Vulnerability Assessment report. If the vulnerability was previously unidentified by your Vulnerability Assessment report then indicate that is the case and assign a new vulnerability identifier.

2. Provide any steps necessary to execute the exploit of the vulnerability. Provide all necessary information for a third party to independently perform the attack. Include references to any attack scripts, code, or required tools. If the vulnerability is not exploitable then provide a rationale of why it is not exploitable.

Problem 3

(10 points - Penetration Test)
The attack phase of the final project will begin at noon on 11/26/2018 and end at noon on 11/30/2018. During this time you are allowed to attack any other team. You are not allowed to attack a team before the official engagement period. Your attacks must be professional. Do not post obscene materials. You may however engage in friendly taunts such as defacing a website to say something to the effect of "team 1 was here" or "hacked by SE421's l33t h4xerz".

During the engagement each team's web service will be available at (`teamN.vulnerablevideoservice.com`) by replacing `N` with the team number. For example team 1 will be available at (`team1.vulnerablevideoservice.com`).

For each exploit that you have developed in the Exploit Development section of this report attempt to use the exploit against each team. Your report should document the following:

1. Identify the vulnerability or exploit in the traceability system established in your report.
2. A list of teams that were vulnerable to the exploit. Provide evidence for each team and include a precise time of when the attack was performed.
3. A list of teams that were not vulnerable to the exploit. Provide evidence and a precise time when the attack was attempted. Also provide a speculation of what the team did to prevent the attack.

Problem 4

(10 points - Intrusion Detection & Response)
During the attack phase of the final project that will begin at noon on 11/26/2018 and end at noon on 11/30/2018 other teams will be allowed to attack you. During this time you should be monitoring for any malicious activity.

You may not actively block any IP addresses! For this section you are not being graded on how successful you were in preventing the attacks, you are being graded on your monitoring/detection and response to malicious activity. Being attacked by adversaries will make this section easier to write because you will have more findings to report.

Note that the TA's will be checking the uptime of your services periodically to compare their findings with your report findings. Note also that the attacks will be originating from both inside and outside of the course, which includes hacking teams throughout the US and India. For this reason you are not allowed to "attack back". You may only attack the designated targets (`teamN.vulnerablevideoservice.com`).

Your report should document the following information:

1. What malicious activity did you detect. Provide evidence to support your claims.
2. Were any attacks successful? If so what evidence do you have that the attack was successful?
3. Detail any steps that you have taken to respond to an attack.

Problem 5

(5 points - Debrief Slides) You will conclude the final project by giving a short (no more than 10 minutes) presentation as a group. You have already created this material in other sections of your report. Your job is to quickly and succinctly communicate the most important findings of your report to the rest of the class. For this problem you should include exactly 5 power point slides in addition to a title and closing slide. Note that while only 5 points are allocated for the creation of the slides, your presentation will be used by the graders in the overall grading of your project.

- Title Slide: Team Members + Date and Location of Presentation
- Slide 1: Overview Threat Model
- Slide 2: Overview Audit Strategy (Sales Pitch)
- Slide 3: Overview Audit Findings & Security Recommendations
- Slide 4: Overview Penetration Test Findings
- Slide 5: Overview Intrusion Detection & Response
- Closing Slide: Thank audience and ask for questions