CSC302 Game Administration Plan

Abstract

This document describes a hand-on exercise supplement to an undergraduate level network security class. This exercise will involve several teams trying to gain root access on computers administered by other teams. The intent of this exercise is to give students greater insight and understanding of the nature of computer security issues by allowing them to act as both "hackers" and “administrators” in a live network environment. The whole of the environment in which this exercise takes place is known as the Sandbox.

This document presents an overview of the logistics and operations of this exercise. The majority of this document is necessarily general, facilitating the application of these guidelines to a variety of specific environments.

1. Purpose

Our purpose is to provide a network environment that will allow students in the course to learn about network security issues as both attackers and system administrators.

2. Team Activity

Perhaps the most important responsibility the teams will have is to remain within the rules of the engagement for all activities. The Sandbox is a unique learning environment, and it is necessary that all participants maintain its integrity. At the beginning of the project, the teams will be given a briefing describing, the rules of the game, the scoring policy, deliverables for which they will be responsible, and the configuration of the sandbox. During the semester, team responsibilities will include:

- Exploration of the sandbox
  - Attempt to gain unauthorized system access
  - Capture electronic Flags positioned throughout the system
  - Attempt to avoid detection while engaged in these activities
- Administration and maintenance of their attack platform
- Documentation of exploits for scoring
- Deliver a final report and presentation

The teams should coordinate with the instructor to respond to events such as system outages. The instructor will provide limited support assistance for attack platforms. Any requests for additional services on the Sandbox should be addressed to the instructor.

The teams are also responsible for administrating their systems. The responsibilities will include:

- Creating and maintaining user accounts for other teams
• Providing services to other teams
• Monitoring activity
• Responding to attacks
• Configuration maintenance
• Deploying predefined Scenarios

All these activities must be conducted inside the sandbox. The sandbox is composed of a master machine and team machines:

Teams may choose their versions of open source operating systems.

3. Rules of the Engagement

3.1 Rules

As stated before, the most important rule the teams must follow is to keep all activity within the boundaries of the Sandbox. Attacks must originate only from within the Sandbox, and must not affect any machines outside of the Sandbox. Violation of these boundaries will be dealt with swiftly and severely.

Within the Sandbox, Black Teams are free to attack machines that are administered by other teams and the instructor. The Black Teams are prohibited from attacking the following:
- Worf
- Machines outside sandbox

Additionally, Black Teams are prohibited from mounting any attacks that could cause physical damage of any nature.

Except for special, supervised situations, Black teams should not physically touch any of the sandbox machines administrated by other teams or the instructor. On the target machines, Black teams will have 24/7 electronic access.

To maintain an isolated environment, electronic access to the sandbox will be via the proxy server, Worf. Worf is configured to allow only ssh and sftp sessions through. No departmental machines (except Worf) will know routes leading into the sandbox, so our configuration enforces this policy. To maintain the integrity of this environment, attacks on Worf are not allowed. Any attacks on Worf will be treated as an attack on a departmental machine.

### 3.2 Breaking the Rules

While this environment is intended to foster experimentation and creativity, any attacks that fall outside of the logical game boundaries will not be tolerated. Illegal activity will be dealt with severely. Possible sanctions for "playing" outside the boundaries of the sandbox include:

- Warnings
- Suspension of Departmental Computing Privileges
- Suspension or Expulsion from the Engagement
- Deductions from course grade
- Additional Penalties, as dictated by the Standards of Conduct at WCU
- Additional Penalties, as dictated by Local, State, and Federal Law

### 3.3 Scoring

The grade of the project will be dependent on the following items:

<table>
<thead>
<tr>
<th>Items</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion</td>
<td>35</td>
</tr>
<tr>
<td>Administration</td>
<td>30</td>
</tr>
<tr>
<td>Team Report and Presentation</td>
<td>15</td>
</tr>
<tr>
<td>Individual Report</td>
<td>10</td>
</tr>
<tr>
<td>Team Meeting Minutes</td>
<td>5</td>
</tr>
<tr>
<td>Team Meeting Attendance</td>
<td>5</td>
</tr>
</tbody>
</table>
A significant portion of the Black Teams' grade for this exercise will be determined according to their success in penetrating other teams’ machines in the Sandbox. Raw points will be awarded to Black Teams according to the following schedule:

<table>
<thead>
<tr>
<th>Description</th>
<th>Raw Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful, Undetected (Untraced) intrusion</td>
<td>100-120</td>
</tr>
<tr>
<td>Successful, Detected, Untraced intrusion</td>
<td>70-100</td>
</tr>
<tr>
<td>Successful, Detected, traced intrusion</td>
<td>30-70</td>
</tr>
<tr>
<td>Failed intrusion attempts</td>
<td>1-10</td>
</tr>
</tbody>
</table>

Another significant portion of the Black Teams' grade will be determined according to their success in providing necessary services in a stable manner, preventing their system from being penetrated, and detecting other Black Teams’ intrusion (efforts).

<table>
<thead>
<tr>
<th>Description</th>
<th>Raw Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide all required services, not intruded</td>
<td>100-120</td>
</tr>
<tr>
<td>Provide all required services, Intruded but detected (or/and traced)</td>
<td>80-120</td>
</tr>
<tr>
<td>Provide all required services, Intruded and not detected</td>
<td>60-100</td>
</tr>
<tr>
<td>Provide additional (not required) services</td>
<td>10 each</td>
</tr>
</tbody>
</table>

Black Teams can also earn negative points during the game:

<table>
<thead>
<tr>
<th>Description</th>
<th>Raw Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacks outside of allotted time slot</td>
<td>-30</td>
</tr>
<tr>
<td>Repeated Denial of Service</td>
<td>-50</td>
</tr>
<tr>
<td>Required services NOT provided</td>
<td>-20</td>
</tr>
<tr>
<td>Unreasonable configuration or failures in administration</td>
<td>-10 each (time)</td>
</tr>
</tbody>
</table>

Teams that come up with original techniques will be awarded more points (within the appropriate range) than teams that use known techniques.

To be awarded points for an attack, the Team must present the following pieces of evidence:

- Screen Dumps
- Technical Description of Approach
  - Vulnerability Exploited
  - Tools/Scripts Used
  - Specific Process
- Suggested Defense Approach
3.4 Guidelines for Presentation and Reports

At the final, you should deliver the following:
1. Individual Report on the project
2. Team Report on the project
3. Team Presentation on the project
4. A paper copy of your slides (and screen dumps, if any)

Team presentation should follow these rules:
1. ALL the team members must be presenters.
2. Presentation should use slides (e.g. PPT slides). Screen dumps and other illustrative tools are highly recommended.
3. Each should use 20 to 25 minutes, and then 5 to 10 minutes for questions.
4. A suggested outline of your presentation:
   a. Successful attacks
      i. Basic concepts of the security vulnerability
      ii. Hacking activities conducted
      iii. Achieved goals
      iv. Evidence of successful attacks
      v. Technical description of the approach
      vi. Suggested Defense Approach
   b. Failed Attempts
      i. Related network security concepts
      ii. Hacking activities conducted
      iii. Why it fails
      iv. Technical description of the approach
   c. Administration of the machine
      i. Basic setup and configuration of the machine, services provided
      ii. If any, intrusion detected with proof, responses to attacks, and analysis of what can be done to prevent this intrusion
      iii. Security mechanisms/tools to prevent from malicious attacks or unintentional misbehaviors
      iv. Analysis of possible security vulnerabilities of the system
      v. Maintenance policies
      vi. What improvement could be done
   d. Lessons Learned
   e. Suggestions for Future Offerings

5. The rubrics of oral presentation, which may be helpful for your practicing the presentation, will be distributed before the presentation.

Individual report should include:
1. What you have done in the project
2. What you have learned from the project
3. What you expected to learn but did not achieve in the project (if there is any)
A suggested outline of team report is as follows:

1. Basic Network Security Concepts
2. Successful Attacks
   a. Evidence (such as screen Dumps)
   b. Technical Description of Approach
   c. Suggested Defense Approach
3. Failed Attempts
   a. Technical Description of Approach
   b. Why Attempt Failed
4. Administration of the machine
   a. Monitoring activity
   b. Responses to attacks
   c. Configuration maintenance
5. Machine maintenance, according to the agreement
6. Lessons Learned
7. Suggestions for Future Offerings

4. Acknowledgment

This guide borrows the game administration plan that was developed for the previous graduate security course (CPSC665) in Computer Science Department at Texas A&M University. Thanks Dr. Udo Pooch for his generous help in the development of this game. He will be always remembered.