Mission 1: Undermining and Protecting Shueworld's Elections

Shueworld, a distant planet near the star Rigel (the right foot of the star constellation Orion), has a planet-wide government. Every 3 years, the citizens of Shueworld vote on who will be the Sneaker of the House, which is the most powerful position in the government. Naturally, multiple factions vie for this honor and hope that their chosen representative will be selected Sneaker by the populace.

For arcane reasons, the Sneaker's election is broken up into individual precincts, called "laces." After doing some sole-searching, each citizen votes at a local lace. The laces then tabulate their votes and determine who won the lace. The candidate with the most laces wins. In the event the laces result in a tie, the two candidates both serve in a united government, known as a "knot." Unfortunately, most knots either unravel or become extremely difficult to untie for future elections.

In previous years, the citizens of Shueworld voted at their local lace by making a shoe print in a column of mud associated with their chosen candidate. Due to logistical considerations (particularly, rainy days and the growing fashion trend of oversized clown shoes) and privacy concerns, the citizens will now vote using computers available at each lace and some may choose to vote using their phones through the lace's wireless network. The lace computers are naturally connected to each other, the local lace tabulator system, the tabulators at other laces, and to the greater Shueworld wide web (SWW).

While most citizens have embraced the move to computerized elections (with the notable exception of the Galosh faction, which embraced mud-related voting), many are concerned about the security of the election and making sure the results are correct. In particular, they do not want the wrong Sneaker candidate to get the Boot, which is malodorous footwear that the loser must wear until the next election to signify de-feet.

Reconnaissance Phase

Students must determine the security goals of each part of an election. For each election component, the students must 1) determine the consequences of the security goal not being met, 2) propose ways that an attacker could undermine each security goal, and 3) propose countermeasures that would minimize the risk that a goal would not be met. Students should ensure they have identified at least one network-based attack vector for use in the next two phases.

Since the Shueworld government did not specify the details of how the computerized system would work, students may make reasonable assumptions about these details or consider a range of options. Students may wish to examine the infrastructure used in computerized elections on Earth as a potential model for how Shueworld may end up creating their infrastructure.

In the reconnaissance phase, students should consider a broad range of attackers, motives, and strategies. The attackers may have the desire to ensure a given Sneaker is elected, to cause chaos, or to undermine the populace's faith in the election outcome. After all, a Sneaker that stinks is as bad as no Sneaker at all.

Infrastructure Building Phase

Using the virtual machines on the isolated computer network in the Zoo lab, the students should construct the relevant portion of the election infrastructure and a system from which the adversary will launch his or her attack. Students should focus on assembling only the minimal election infrastructure needed to demonstrate the attack and its vulnerabilities. For example, if the system in which a person casts a ballot is needed, a simple HTML ballot with a few choices and a minimal backend form processor may suffice. An elaborately built system is unlikely to be necessary and this may divert student time from efforts that offer a more significant learning (and grading) impact.

Attack Phase

Students should select at least one network-based attack from the reconnaissance phase and consider how to implement it. The attack must have a significant impact on the election. For logistical reasons surrounding

shared infrastructure, the chosen attack must not be a resource exhaustion attack (e.g., anything that saturates the network, memory, or computational resources of the involved systems).

Students should avoid trivial attacks that exploit application vulnerabilities that the students themselves introduce. For example, both a "vote stuffing" attack in which the voting system does not attempt to prevent duplicate votes or an SQL injection attack in which the students create a application vulnerable to SQL injection are considered trivial. Part of the scoring for the attack phase is realism, ambition, and degree of learning.

Students must provide the necessary details of the configuration setup, the attack itself, and results needed for a reviewer to know the attack is real, to replicate the experiment, and to validate the results in the Mission Debriefing Report. The attack should have measurable, quantifiable outcomes and an indication of the resources needed to launch the attack. Consider the Mission Debriefing Report the team's only opportunity to convince the current Sneaker of the House that there is a legitimate concern in the election with evidence that allows the Sneaker to hire consultants to verify the team's work.

Defense Phase

After completing the attack phase, the students must create a proposed defense against the attack. The defense should be effective and realistic for the Shueworld government to deploy. For example, while DNA testing may be useful for ensuring a voter's identity, it is probably unrealistic; it would likely yield significant backlash from the populace and would be too expensive for the government to implement. The description of any defense should include a discussion on feasibility and costs: what will the government have to do, what resources are required, and why is it reasonable to assume those resources are available?

Students should demonstrate that the defense successfully mitigates the attack. They must provide all details of the defense, including any tools and configuration changes, along with log evidence demonstrating the attack was blocked. The defense should allow the team to demonstrate significant learning of new knowledge and/or ingenuity. A correct, but trivial, defense may not earn many points according to the grading rubric.

Mission Debriefing Report

The Mission Debriefing Report is the team's opportunity to explain the identified security goals and attack vectors in the election infrastructure to the government of Shueworld, including all the results from the reconnaissance phase. The report should then focus on a single network-based attack and demonstrate the negative consequences of not addressing the vulnerability the attack exploits. The report should then provide a feasible solution to defend the infrastructure.

The Mission Debriefing Report should be comprehensive and provide conclusive supporting evidence. It is likely that such a report will be at least five pages of write-up and any figures, followed by an appendix of supporting evidence (e.g., screenshots, output of terminal windows, log file output). In addition to the write-up, the debriefing report should include additional supporting files, such as source code or configuration files. For the report to be scientifically valid, enough detail must be provided that would enable the grader or another member of the class to create and run the experiment without the need to ask questions.

Mission Rubric

The mission score can be broken down into five components, each of which are scored independently. The total score is out of 25 points. The following are the components:

1. Reconnaissance: 4 points
2. Infrastructure Building: 5 points
3. Attack: 5 points
4. Defense: 5 points
5. Mission Debriefing: 6 points

We now describe each of the criteria and how they are graded.

Reconnaissance: 4 points

Rubric:

- 4 points: The team has identified a comprehensive set of security goals for the targeted system. Each security goal is described in detail and the impact of not achieving the security goal is clearly stated. The description includes at least one realistic attack vector for each security goal. The countermeasures for each attack vector are likely to be effective and realistic to deploy.
- 3 points: The reconnaissance phase is generally good, but a key security goal may be missing. Alternatively, one or more security goals is not described in sufficient detail or the attack vectors or countermeasures are not fully developed or are unrealistic. This score reflects solid work with relatively minor deficiencies.
- 2 point: The reconnaissance phase omits two or more key security goals. Alternatively, multiple security goals lack detail or attack vectors or countermeasures are poorly formulated or unrealistic. This score reflects work with moderate deficiencies.
- 0 points or 1 point: The reconnaissance phase has significant limitations. The work does not demonstrate a comprehensive review of the problem or the analysis is severely flawed.

Infrastructure Building: 5 points

Rubric:

- 5 points: The infrastructure is realistic and appropriate for the scenario evaluated. The details of the design are obvious with clear configuration files and step-by-step instruction on how the team built the infrastructure. An independent party would clearly be able to follow these instructions to quickly replicate the experimental setup. There is clear evidence that the team learned how to use the provided infrastructure and gave serious consideration into the best configuration that would enable a clear demonstration of the attack and its defense.
- 4 points: The infrastructure setup is generally good, but some details may be missing or some steps in the instructions may have minor errors. With some problem-solving efforts and additional time, an independent party would likely be able to replicate a close approximation of the experimental setup. The team used the provided infrastructure and designed a configuration that adequately enables a demonstration of an attack and defense.

- 3 points: The infrastructure setup has flaws or significant omissions in its instructions or design documentation. An independent party would have trouble recreating the experimental setup. The team used the provided infrastructure, but the configuration limits the effectiveness of an attack or defense demonstration.
- 2 points: The infrastructure setup is flawed and/or is inadequately described to allow replication. The team deviated from the provided infrastructure or the application of the infrastructure has the potential to undermine the validity of the attack or defense experiments.
- 0 points or 1 point: The infrastructure setup has severe flaws that greatly undermine its utility.

Attack: 5 points

Rubric:

- 5 points: The team identifies a realistic, high-impact attack vector. The attack is implemented flawlessly and the description of the attack and its supporting documentation allows an independent party to replicate the attack. The documentation provides evidence that conclusively shows that the team mounted the attack and that the attack was successful. To earn this score, the attack and/or the implementation of the attack must demonstrate significant independent learning or creative thinking by the team. The attack must be sufficiently complex that the students needed to invent or configure existing tools to effectively launch it.
- 4 points: The team identifies a realistic attack vector. The attack is implemented well and the supporting documentation is solid, but may be missing minor details that are needed to replicate the attack. The supporting documentation generally shows the attack was implemented and was likely successful. The attack showed that the students learned about a new way to launch an attack, but the team may have used an obvious or straightforward methodology to launch the attack.
- 3 points: The team identifies an attack vector, but it may be low impact or may be less realistic. The attack implementation or its supporting documentation may have small flaws. The supporting evidence suggests the attack was implemented and may have been effective, but the support is not conclusive. The attack itself may not have been sophisticated or provided significant learning opportunities for students.
- 2 points: The students identified an attack vector, but it may be low impact or unrealistic. The supporting documentation or evidence of the attack is lacking. The attack itself is trivial and there is little evidence the students learned much from the exercise.
- 0 points or 1 point: The attack has severe flaws that greatly undermine its utility.

Defense: 5 points

Rubric:

- 5 points: The team identifies a realistic, high-impact defense. The defense is implemented flawlessly and the description of the defense and its supporting documentation allows an independent party to replicate the defense. The documentation provides evidence that conclusively shows that the team mounted an effective attack and that the defense prevented the attack from being successful. To earn this score, the defensive approach and/or the implementation of the defense must demonstrate significant independent learning or creative thinking by the team. The defense must be sufficiently complex that the students needed to invent or configure existing tools to effectively deploy it.
- 4 points: The team identifies a realistic defensive strategy. The defense is implemented well and the supporting documentation is solid, but may be missing minor details that are needed to replicate the defense. The supporting documentation generally shows the defense was implemented and was likely

successful. The defense showed that the students learned about a new way to protect a system, but the team may have used an obvious or straightforward methodology to deploy the defense.

- 3 points: The team identifies a defensive strategy, but it may be low impact or may be less realistic. The defense implementation or its supporting documentation may have small flaws. The supporting evidence suggests the defense was implemented and may have been effective, but the support is not conclusive. The defense itself may not have been sophisticated or provided significant learning opportunities for students.
- 2 points: The students identified a defensive strategy, but it may be low impact or unrealistic. The supporting documentation or evidence of the defense is lacking. The defense itself is trivial and there is little evidence the students learned much from the exercise.
- 0 points or 1 point: The defense has severe flaws that greatly undermine its utility.

Mission Debriefing Document: 6 points

The mission debriefing document includes the write-up associated with the reconnaissance, attack, and defense. The primary grading of those sections are described above. The mission debriefing document includes overall communication strategy, organization of the information, and interpretation of the data. It also includes supporting appendices and related files.

Rubric:

- 6 points: The report has an introduction and a conclusion section that clearly explain the scenario being evaluated, its importance, the key components that require evaluation, and the results of the specific attack and defense the team evaluated. The report makes use of figures or tables where appropriate to succinctly inform the reader of results. Key supporting information is placed in an easy to read appendix to the report. Additional files are clearly labeled and easy to understand. A README file is provided describing each of the supporting files. All tools are described and the mechanism to obtain the tools (e.g., URLs, relevant repository names) are provided. Where necessary, appropriate academic or technical sources are referenced and cited. The document is compelling, accurate, and leaves little doubt about the attack, defense, and recommendations.
- 5 points: The report has an adequate introduction and conclusion that describe the scenario, its importance, key components, and results. The report is understandable and makes the appropriate points, but the presentation may be suboptimal. The appendix contains supporting information but may have only basic explanation or description of the information. All the supporting files and evidence are included, but it may take extra time to locate. The tools are described, but information on how to obtain them may be missing in some cases. Some academic and technical sources are cited, but there may be instances in which additional citations would be useful. The document is accurate and descriptive, but the document may not be as convincing due to writing limitations or insufficient evidence.
- 4 point: The report has some flaws or omits some of the important points described above. The report may be unclear or unconvincing in places and supporting evidence may be missing, hard to find, or inconclusive. The report is generally accurate, but with apparent flaws or omissions.
- 0-3 points: The report has deficiencies that hinder understanding, omits important data, or provides inadequate support. One of the report sections may be missing or incomplete.