Leveling Up Cyber Skills: Mapping Bandit Labs to the NICE Framework

Allison Youngblood, Sam White
Mentors: Zachary Werle and Dr. James Crabb

INTRODUCTION

- Our goal over this semester was to use the Bandit wargame from OverTheWire to acquaint ourselves with Linux commands and to relate what we were doing and learning to the NICE Framework.

- Project Goal **-**
  - Explore and complete the *Bandit* wargame from OverTheWire.

- Learning Focus **-**
  - Gain hands-on experience with essential Linux commands and terminal navigation.

- Framework Alignment **-**
  - Connect practical exercises to relevant categories and tasks in the NICE Cybersecurity Workforce Framework.

- Outcome **-**
  - Develop foundational skills in cybersecurity operations and command-line environments.

Figure 1: The seven categories of cybersecurity work roles in the NICE Framework.

OVERTHEWIRE BANDIT

- What is OverTheWire? **-**
  - A collection of cybersecurity wargames designed as educational tools.
- Purpose:
  - Help users learn and practice cybersecurity concepts through interactive, game-based challenges.
- Focuses on Bandit Wargame:
  - Tailored for beginners.
  - Introduces foundational Linux commands and basic cybersecurity skills.
  - Prepares users to tackle more advanced wargames in the OverTheWire series.

NICE FRAMEWORK

- What is the NICE Framework? **-**
  - A national resource that helps employers develop and manage their cybersecurity workforce.
- Purpose:
  - Provides a common language to describe cybersecurity work and workers across all sectors (public, private, and academic).
- Applicability:
  - Designed to be universal and adaptable to various work environments.
- Key Components:
  - Work Role Categories:
    - Broad groups of related cybersecurity functions.
  - Work Roles:
    - Specific groupings of responsibilities (not equivalent to job titles).
  - TKS Statements:
    - Tasks, Knowledge, and Skills required to perform specific roles.
  - Competency Areas:
    - Clusters of knowledge and skills linked to performance in the domain.

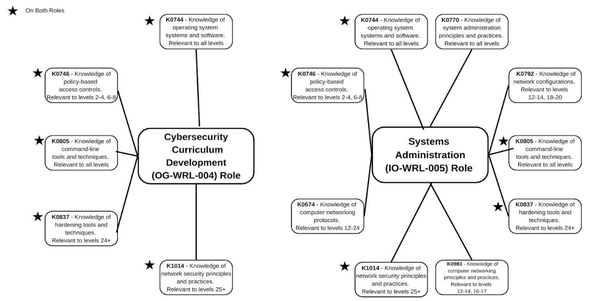

Figure 2: Links NICE Framework knowledge areas to two cybersecurity roles, Curriculum Developer and Systems Administrator, using skills reinforced by OverTheWire's Bandit labs.

HOW THE NICE FRAMEWORK RELATES TO THE OVERTHEWIRE BANDIT LABS

- The OverTheWire Bandit game supports skill development for both Cybersecurity Curriculum Development and Systems Administration roles the NICE Framework.
- Bandit has foundational exercises aligned with introductory cybersecurity courses.
- For Cybersecurity Curriculum Developers:
  - Activities include navigating the command line, analyzing file permissions, and identifying basic security misconfigurations.
  - These exercises build hands-on competencies aligned with NICE standards.
  - Developers can integrate Bandit into training programs to ensure learned again cybersecurity skills.
- For System Administrators:
  - Exercises cover managing file systems, understanding user privileges, and during secure remote access tools like SSH.
  - And tasks like locating files, interpreting logs and maintaining secure configurations.
- The Unix-like environment in Bandit simulates task encountered in operational tech roles.
- Bandit is a great tool for learning essential cybersecurity skills and preparing individuals for technical operational roles

TACTICS

- **The Use of Command Line (CLI) -** We heavily relied on basic Linux command-line tools like ls, cat, find, grep and ssh. We experimented directly in the terminal to understand how different commands worked. We were trying out various options and observing the results we developed as better grasp of file navigation, permission changes and command line behavior. It helped us understand the use of the command line and made us more comfortable with working in a Linux environment.
- **Note-Taking and Level Mapping -** As we were going through the levels, we kept notes that mapped each bandit level to the specific concept or challenge that it covered (file permissions, symbolic links). This helped us track our progress and connect what we learned to real world cybersecurity tasks and relate them to the NICE Framework.
- **Trial and Error with Critical Thinking** - We were learning by doing, and for each challenge we read the description carefully, planned and then tested different commands. If something didn't work, we reflected on the error messages or output, then chose a different approach. This helped with our problem-solving skills and helped with working through complex technical issues.

ACKNOWLEGEMENTS

This work is supported by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by The Office of the Undersecretary of Defense for Research and Engineering, in collaboration with the Air Force Research Laboratory and Griffiss Institute.