Cybersecurity

BootCon Project - Interview and Resume Guidance

Congratulations on completing your final project!

- When networking and talking to potential employers, you can reference the work that you did on this project to answer specific interview questions or demonstrate your skills within a specific domain.
- This guide will assist you in adding your project to your resume, discussing your project, and answering potential interview questions regarding your project's activities.
- Since everyone selected a different presentation topic, this guide will provide an example of resume guidance for the sample presentation that was shown on Day 1: **DHCP Attacks with Yersinia.**

Resume Guidance

Many IT and cybersecurity professionals showcase their projects by adding them to their resume. Add your project to your resume by doing the following:

- List your project under the "work experience" or "accomplishments" section of your resume. Include the name of the project, the technologies that you used, and what you accomplished or achieved with your project. Consider the following example:

  BootCon Project:: **DHCP Attacks with Yersinia**

  Technologies Used: Kali Linux, Wireshark, Yersinia

  - Presented a simulated DHCP starvation attack using the offensive security tool Yersinia.
  - Analyzed the raw traffic of the DHCP starvation attack to provide recommended mitigations.

Interview Guidance

As a reminder, good interview responses do the following:

1. Restate the problem.
2. Provide a concrete example scenario.
3. Explain the solution requirements.
4. Explain the solution details.
5. Identify advantages and disadvantages of the solution.

Including each of these components will help demonstrate both competency in the subject matter and critical thinking.

Interview Questions

1. **Describe your project and findings.**

   Within my closed environment, I simulated a DHCP starvation attack using the Kali Linux tool Yersinia. With Wireshark, I analyzed how Yersinia was able to make thousands of DHCP requests to starve the DHCP server of available IP addresses. I also recognized how Yersinia changed the mac address for each request.

2. **What were your project requirements?**

   Our requirements included:

   - *Demonstrating a security tool or security attack.*
   - *Analyzing the findings and providing recommendations for mitigations.*
   - *Presenting our findings to the class with a live presentation.*

3. **What future mitigations would you recommend based on your findings?**

   Based on my findings, I would recommend that organizations use rate limiting to prevent attackers from launching a similar attack.