Cybersecurity

BootCon Presentation Guide

Contents

What Is BootCon?

BootCon is a mock cybersecurity conference. It takes place during class, and you will have an opportunity to showcase the skills that you've learned throughout the course with a presentation to the class. This "conference" occurs on the last day of the course and will also count as the final project.

What Is a BootCon Presentation?

Cybersecurity professionals commonly present the following to their peers:

- Security research that they're conducting
- Newly discovered security vulnerabilities of products, devices, software, or hardware
- Demonstrations of the "hacks" that will exploit these vulnerabilities
- Mitigations to protect against these vulnerabilities

These presentations often occur at security conferences, trade shows, and other industry events.

All students of the Cybersecurity boot camp have a similar opportunity to showcase the skills they learned during the boot camp with a bootCon presentation.

Most cybersecurity professionals present at conferences when they've found a new vulnerability. However, for bootCon presentations, it is acceptable and recommended that you recreate a finding that has already been discovered.

Guidelines for BootCon Presentations

- A bootCon presentation is **NOT** a research paper.
- While research will be required, all presentations must be tangible and demonstrable.
- A demonstration can either be conducted in person or in a prerecorded video that accompanies the presentation if a live demonstration isn't practicable.

All bootCon presentations should fall into one of the following three categories:

1. Exploiting a vulnerability of an **IoT device**.
    a. *For example, hacking your personal Blu-ray player.*
2. Developing **code or program** that can complete a cybersecurity task.
    a. *For example, developing a Python script that can automate an Nmap scan.*
3. Demonstrating how a **cybersecurity tool** that was not covered in class can accomplish a specific goal.
    a. *For example, demonstrating using Mimikatz to dump passwords from a Kerberos ticket.*

Rules & Requirements

1. You must submit a project summary to your instructor for approval before proceeding with your project. The project summary should include:
    a. The title and topic of your presentation
    b. The end goal or vulnerability being exploited
    c. The devices and/or technologies that will be used to accomplish the goal
    d. A summary of how the devices and/or technologies will be used to accomplish the goal

2. IMPORTANT! UNDER NO CIRCUMSTANCE MAY ANY ASPECT OF YOUR PRESENTATION BE UNETHICAL OR ILLEGAL.

a. You must perform all hacks and tests in simulated environments.
b. You must complete any network connections in your home and/or controlled environment.
c. You may only perform IoT hacks on devices you own.

3. Presentations must have a **goal** whose achievement you can **demonstrate**.
    a. For example:
        i. **Goal:** Cracking WEP wireless traffic from your home router.
        ii. **Demonstration:** Demonstrating how you captured and cracked your wireless traffic.
    b. You can either conduct your demonstration live or record it and present it while you walk through what took place.

4. You must submit your presentation in the form of a Google Slides deck that, at a minimum, includes the following:
    a. **Cover slide:** Presentation title and team member(s) presenting
    b. **Technical background:**
        i. Explanation of why you selected the topic
        ii. Networking, cryptographic, or security concepts applied
        iii. Research steps taken
    c. **Demonstration preview:** A preview of the steps that you'll take in the upcoming demonstration.
    d. **Demonstration:** A live or recorded demonstration is conducted here.
    e. **Demonstration summary:** A summary of the demonstration that you just conducted and any impact it may have.
    f. **Mitigation:** Recommendations for mitigating against the attack that you just conducted. If your presentation isn't about an attack, this is not required.

5. Your total presentation time should be between 7 and 10 minutes.

Sample Guide to Completing a bootCon Presentation

Sample Topic: Intercept and Crack Traffic from a WEP Wireless Router

- **Goal:** Cracking WEP wireless traffic from our home router.
- **Demonstration:** Demonstrating how we captured and cracked our wireless traffic.

Part 1 – Research

First, we researched wireless security issues. We learned the differences between the wireless encryption used with WEP, WPA, and WPA2.

Through our research, we determined that wireless routers that have WEP encryption are susceptible to their encrypted traffic being decrypted.

We watched many videos and read “how to” guides on wireless hacking.

We determined that in order to capture wireless traffic on our computer, we needed a network card that could capture traffic in “monitor mode.”

Our laptop didn’t offer this capability, but we discovered that there was a wireless USB device that could capture this traffic. It was available for $10, so we purchased one.

We researched how to configure the device to capture wireless traffic in monitor mode.

We learned that once the traffic was captured, the Kali Linux tool Aircrack-ng could easily crack WEP traffic with a single command.

Part 2 – Installation and Configuration

We confirmed that our current wireless router has the ability to change its settings to WEP encryption, so that we could conduct an at-home test. We configured the router to briefly use WEP encryption.

We configured the wireless USB device to intercept wireless traffic in monitor mode.

We set up Wireshark to pull in the intercepted traffic captured from the USB device.

We ran tests to make sure that the USB device was able to pull “802.11” wireless traffic into Wireshark for analysis.

Part 3 – Testing the Vulnerability

We used Gruyere.com as an unencrypted test website to illustrate how captured website traffic can pose a security risk.

We turned on Wireshark to start capturing the wireless traffic, and we logged into the Gruyere website with a sample login. We created the unique login name “MrHacker” so that we would be able to confirm that the hack had worked successfully.

After the wireless traffic was captured, we used the Kali Linux tool Aircrack-ng to figure out the decryption key of the traffic.

Aircrack-ng quickly figured out the key, and we used that key to decrypt the wireless traffic.

We confirmed that in Wireshark we were able to view the decrypted HTTP traffic where we’d logged in as MrHacker, and that the password was exposed.

Part 4 – Project Preparation

It wasn't feasible to bring our wireless router to class. So, we decided to record a video showing how we captured the wireless traffic and then demonstrate in person how to crack the wireless traffic using Aircrack-ng.

We practiced this procedure several times to confirm that the presentation would run smoothly when we ran it live.

We put together a slide deck with images and videos illustrating:

- What our project is, why we chose it, and what its end goal is
- Our research into wireless vulnerabilities
- The WEP encryption vulnerabilities that we found
- The devices that we used to conduct this demonstration
- Our demonstration of capturing the wireless traffic
- Our demonstration of cracking the wireless key
- A summary of mitigations and how WPA and WPA2 address WEP's vulnerabilities

Resources for Presentation Ideas

Presentation Example

- DHCP Starvation Attack with Yersinia

List of Kali Linux Tools

- Kali Linux Tool List

List of IoT Hacks

- Wonder How To Main Website
- Wonder How To: Mr Robot Hacks
- Wonder How To: IoT Hacks
- Curated List of IoT Hacks
- IoT Security Wiki

For Inspiration: Videos of Hacks Presented at Security Conferences

- Black Hat video: Hacking a Drone
- DEFCON Conference video: Hacking an Elevator
- DEFCON Conference video: Hacking Web Apps
- Black Hat video: Exploiting Network Surveillance Cameras

- CBS Mornings video: Meet a 12-year-old Hacker