**Ali Hassen**

**03/31/2024**

**Cyber Security Boot Camp Experience at Michigan State University 2023**

During my Cyber Security Boot Camp at Michigan State University, I gained valuable hands-on experience and developed essential skills. Here are the highlights of my journey:

**Comprehensive Tools and Platforms:**

**I had the opportunity to work with a variety of tools, including:**

**Virtual Machines**: Used for testing and simulating different environments.

**Azure Lab**: Explored cloud-based security solutions and configurations.

**Linux Command Line and Bash**: Leveraged for scripting, automation, and system administration.

**Monitoring Tools**: Learned to monitor network traffic, detect anomalies, and respond to incidents.

**Intensive Learning Environment**:

Both inside and outside the classroom, I dedicated significant hours to mastering cybersecurity concepts.

Collaborated with instructors and classmates, exchanging knowledge, and troubleshooting challenges.

**Cybersecurity Fundamentals**:

Explored topics such as network security, cryptography, risk management, and ethical hacking.

Gained insights into threat detection, incident response, and vulnerability assessment.

**Projects Highlights**:

Participated in hands-on projects that reinforced theoretical knowledge.

Developed secure configurations, conducted penetration testing, and analyzed vulnerabilities.

**Achievement**:

Successfully completed the boot camp with a remarkable grade of 97.07%.

Overall, this intensive six-month program equipped me with practical skills, exposed me to real-world scenarios, and solidified my understanding of cybersecurity fundamentals. I am eager to apply these skills in a professional setting.

**Confirmation of Challenge Submissions for Cyber Security Boot Camp**

Throughout the Cyber Security Boot Camp, I diligently completed each module’s challenges and submitted my work. I have attached the links to my challenge submissions, which serve as evidence of the skills and knowledge I acquired during the program.

**Class learning curriculum:**

1. **Cyber Security Landscape**

<https://docs.google.com/document/d/1coq6pIiTfwA3TpHuu2w3Vbz8hwdY2YPsWDdWtngDc5c/edit?usp=sharing>

1. **Cyber Security Framework**
2. **Linux System Administration**

<https://docs.google.com/document/d/1ujr6HibrGHBWzLGXDrI6jhnILf2s1z_Opw3OgoXOq28/edit?usp=sharing>

1. **Archiving and Logging Data & Tar**

<https://docs.google.com/document/d/1TlSAJXnayvGcDUpUyq6qXHoev8lsuImjRfZVS5YRCeE/edit?usp=sharing>

1. **Advance Bash & Owning System**

<https://docs.google.com/document/d/1pojJ4u-SI-zEsNIsRVrymgEqqbgn_HMa2ufXmChcT-Y/edit?usp=sharing>

1. **PowerShell:**

<https://docs.google.com/document/d/1Q5Dj4EXqehQRSA6pXOoORfIca06xrzdNV0tMdVmSo14/edit?usp=sharing>

1. **Network Fundamentals:** Network challenge submission.

<https://docs.google.com/document/d/1vsqJEATrHYp-w35XkFMRG_Az9cLWFrS5-1iNJTaLubc/edit?usp=sharing>

1. **Cryptography Challenge: Ransomware Riddles**: Cryptography Challenge: Ransomware Riddles

<https://docs.google.com/document/d/1HnK6lxzQn6PwdU71PjclyCiX4RwPKJbAUyJVmIqD4jY/edit?usp=sharing>

1. **Network Security**: We were able to demonstrate investigative skills within the scope of the networking tasks. reviewing the security and intrusion questions.

<https://docs.google.com/document/d/1FzTpovwE2ARPlWTWDNtp2OvcoOaKh55m2KV8yQX2DhA/edit?usp=sharing>

**Cyber kill chain**: listing the steps and summaries.

**Snort Rules**: summaries for each section were excellent.

**Drop Zone lab:**

Run the command that removes any running instance of UFW. Keyword is “removed”

IDS vs IPS

1. Policies, procedures, and awareness
2. Physical security
3. Perimeter defense
4. Internal network security
5. Host security
6. Application security
7. Data security
8. **Windows administration and Hardening:** We’ve demonstrated PowerShell and sysadmin skills!
9. **Bash Scripting and Programming**: We’ve demonstrated the hacking skills, remotely accessed a victim’s machine, maintained access via a backdoor and cracked sensitive passwords!
10. **Web Development:**

<https://docs.google.com/document/d/10OP6rVtW66k1FvczatHMenEkh5sS7NIuQhWC8Np1dls/edit?usp=sharing>

1. HTTP Requests and Responses
2. Using curl
3. Sessions and Cookies
4. Example HTTP Requests and Responses
5. Monoliths and Microservices
6. Deploy and Test a Container Set
7. Databases

**Project 1 - Cloud Security:** Creating my own (Cloud Diagram) <https://drive.google.com/file/d/1YfUanAe5ygBBXs1cRu254n-pFFjj7WKf/view?usp=sharing>

**Project 2- Creating your own website application**: Build, Secure, and Protect a Web Application. Using Azure free domain application. I was able to create my own website. In addition to that I was able to answer all of the Web Development Questions.

<https://docs.google.com/document/d/1X0OpRR3zyCoZR9Qw2Zo7HzSacZauZadMEwHf5btEABM/edit?usp=sharing>

( [**https://alisecurityblog.azurewebsites.net/**](https://alisecurityblog.azurewebsites.net/)**)**

1. **Testing Web Application for Vulnerabilities:** Access the payloads using dot-dot-slash method. Using Burp Suite to find the correct match of username and password. Finally, setting the hook on DVWA website using BeEF exploits. For more information and screenshots kindly visit my docs.google.com the link below.

https://docs.google.com/document/d/1QMhRxWdxSgWnOpqGIq6hsutMb2ACafOX2GIjlpMu-so/edit?usp=sharing

1. **Penetration Test for Mega company & writing Penetration test report.**

<https://docs.google.com/document/d/1qXocVXLbMTrQRwkrWuFz5DZ1qLzFg3XJ_e0O2cqM8Ec/edit?usp=sharing>

1. report starts out strong with a creative company name, contact details, and a document revision history!
2. identify a weakness and a strength for Megacompanies company.
3. Find and exfiltrate any sensitive information within the domain.
4. Escalate privileges to domain administrator.
5. Compromise at least two machines.

**Project 3 -**

**Exploit Vulnerabilities in Rekall Corporation's Web Application, Linux Servers, and Windows Servers**

1. Find and exfiltrate any sensitive information within the domain.
2. Escalate privileges.
3. Compromise several machines.

For more details information and screenshot picture kindly visit my Docs. Google with link blew.

**https://docs.google.com/document/d/1aY4r9YA1Dk9\_a3O6fQIf3yfqNKfu7xnIqcjMBndyVIY/edit?usp=sharing**

1. **Monitoring tools Splunk & Autopsy**

Go Splunk : My reports included a comprehensive screenshot using Splunk’s table command to display the following statistics: • \_time • IP\_ADDRESS • DOWNLOAD MEGABITS • UPLOAD MEGABITS • ratio. You can check the find and the report with screenshot while visiting my file at:

https://docs.google.com/document/d/1jZ1tUKXn885nEwtGkPF0gIx21T7tUUJgURDVbV5tXLI/edit?usp=sharing

1. **Digital forensic**: in the homework assignment! My demonstration of digital forensic skills in searching, organizing, and presenting data as legal evidence is truly noteworthy.
2. A concise overview of the case.
3. A brief summary detailing the tools and equipment.
4. Unique specifics about the device under scrutiny.
5. Contact information and succinct conclusions regarding the subjects.
6. Key evidence pertaining to the theft conspiracy.
7. A plotted timeline.
8. Deductions drawn from the evidence.
9. Evidence sourced from email and SMS correspondences.
10. Evidence extracted from location services like GPS.

By visiting the below link. You will be able to review the case with detailed information.

<https://docs.google.com/document/d/1SJebsRYH-AxWhj07IqoS7bEPmHGmc8iaIPjGx93QXYQ/edit?usp=sharing>