# PIP-104: PROFESSIONAL PRACTICE-II (INTERNSHIP)

## Viva-Voce Presentation

## Red Team Assessment on Ather Networks

Submitted to the Presidency University, Bengaluru in partial fulfillment of the requirements for the PIP-104: PROFESSIONAL PRACTICE-II (INTERNSHIP)

By

Batch No:

| Student Details | |
|---|---|
| **Name** | AKASH K |
| **Roll No** | 20201COM0008 |
| **Section** | 7COM3 |
| **Batch No** | |

Under the supervision of

**Ms. Shilpa C N**

Assistant Professor Grade - 1
Department of Computer Science & Engineering

January , 2024

# Introduction and About Company or Organization

**CyberSmithSECURE** stands as a beacon of excellence in the realm of cybersecurity, setting the standard for cutting-edge and comprehensive solutions that fortify businesses and organizations against the relentless onslaught of ever-evolving cyber threats.

With a commitment to excellence and a passion for staying ahead of the technological curve, our organization has become synonymous with trust, innovation, and resilience in the face of an increasingly complex digital landscape.

At the core of CyberSmithSECURE's success is our dedicated team of highly skilled professionals. These individuals are not just employees; they are cybersecurity experts armed with the latest advancements in technology. We understand that the key to effective cybersecurity lies in staying ahead of the curve, and our team is equipped with the knowledge and skills needed to tackle the challenges posed by an ever-changing threat landscape.

# Introduction and About Company or Organization

Our primary mission revolves around safeguarding our clients' digital assets. In an era where data breaches and cyber-attacks are becoming more sophisticated, we recognize the critical importance of upholding the security and privacy of our clients at all times.

**CyberSmithSECURE** takes a proactive approach to cybersecurity, implementing robust measures to ensure that our clients can operate in a secure digital environment without compromising their sensitive information.

One of our standout services is Red Teaming, where CyberSmithSECURE has established itself as a pioneering force in the field. Our Red Teaming services go beyond conventional cybersecurity approaches, focusing on simulating realistic cyber-attacks to test the vulnerabilities of our clients' systems.

# Introduction and About Company or Organization

By adopting the mindset of potential adversaries, we provide invaluable insights that allow organizations to enhance their security measures and fortify weaknesses before they can be exploited by real threats.

In the ever-evolving landscape of cyber threats, CyberSmithSECURE remains committed to being at the forefront of innovation and excellence. We continually invest in research and development to stay abreast of emerging technologies and tactics employed by cyber adversaries.

Red Teaming Pioneering in the field, we stand out as premier providers of Red Teaming services, and specialize in simulating realistic cyber-attacks

# About your team and reporting Manager

As a pivotal member of **Project Heimdall**, the esteemed red team operating within our cybersecurity department, I find myself at the forefront of a dynamic and highly specialized team. Within this collaborative framework, I engage with a cohort of proficient and diverse professionals, each bringing their unique skills and insights to the table.

Project Heimdall's structure is meticulously designed to cover a broad array of offensive security domains, and my responsibilities within this esteemed group encompass various facets such as network penetration testing, web application security, social engineering, and beyond. This strategic segmentation ensures that our team is not only well-rounded but also adept at delving into the intricacies of diverse security challenges.

# About your team and Reporting Manager

In the collaborative ethos of Project Heimdall, I work closely with a highly skilled and diverse team of professionals. This collective expertise allows us to orchestrate comprehensive and realistic red teaming exercises, wherein each team member's contribution is integral to the success of our assessments.

Our collaborative efforts are not only focused on identifying vulnerabilities but also on providing actionable insights that contribute significantly to the organization's overall security objectives.

Under the direct oversight of Mr. Smith, a seasoned leader in the cybersecurity domain, I report my findings and insights derived from our targeted red teaming exercises.

# About your team and reporting Manager

Furthermore, being part of Project Heimdall provides the flexibility and agility necessary to adapt to the ever-evolving landscape of cyber threats and challenges. The proactive nature of our red teaming exercises allows us to stay ahead of emerging threats, providing the organization with a proactive defense strategy. This adaptability is crucial in an environment where cyber threats constantly evolve, and our commitment to maintaining this agility is reflected in our team's ability to swiftly respond to emerging challenges.

The collaboration within our team, combined with the strategic alignment with organizational objectives, ensures that our efforts go beyond identification of vulnerabilities to provide tangible and actionable insights that fortify the organization's cybersecurity posture.

# About the Project

In a recent cybersecurity assessment conducted at Ather Energy, my role as a meticulous cybersecurity analyst unveiled a critical SQL injection vulnerability within a targeted website.

The success of this endeavor lay not only in the identification of the vulnerability but in the strategic exploitation that followed. Through a rigorous process of analysis and testing, I discerned that this SQL injection vulnerability could serve as a gateway for remote code execution, employing a sophisticated Time-based blind SQL injection technique.

The culmination of these efforts allowed me to breach the system's defenses and gain unauthorized access to the underlying systems. Once inside, I discovered that I had ascended to the privileges of a domain user. This marked a pivotal point in the assessment, providing the groundwork for further escalation of privileges within the network.

# About the Project

A strategic move ensued, as I executed a Kerberoasting attack targeting the MySQL service account. This attack method involved exploiting vulnerabilities inherent in the Kerberos authentication system. The success of this endeavor was evident as I successfully acquired credentials associated with a domain admin account.

This pivotal moment granted me elevated privileges, significantly amplifying the scope of my Infiltration.

Subsequently, armed with the obtained domain admin credentials, I meticulously orchestrated a strategic impersonation, positioning myself to operate with the highest level of administrative privileges within the network. This intricate process involved the extraction of sensitive information through an NTDS.DIT File (Active Directory database) dump.

# About the Project

This strategic move not only provided insights into the network's structure but also granted a comprehensive understanding of user accounts, laying bare the intricacies of the organization's digital landscape.

The accomplishment of successfully navigating and exploiting the identified vulnerabilities during the cybersecurity assessment at Ather Energy serves as a compelling illustration of my adeptness in the realm of offensive security. Beyond being a testament to my proficiency in identifying and capitalizing on weaknesses, this achievement underscores the indispensable value of comprehensive penetration testing in contemporary cybersecurity strategies.

The seamless progression from uncovering a critical SQL injection vulnerability to attaining domain admin credentials and extracting sensitive information reflects the profound depth of my expertise in offensive security practices.

# About the Project

This multifaceted approach doesn't merely stop at identifying and patching vulnerabilities but extends to the strategic exploitation of these weaknesses, mirroring the tactics employed by real-world cyber adversaries.

This experience not only emphasizes the critical role of a vigilant and proactive cybersecurity stance but also highlights the imperative need for organizations to fortify their defenses against increasingly sophisticated cyber threats.

It serves as a poignant reminder that cybersecurity is not a static state but an ever-evolving landscape that demands continuous monitoring, proactive measures, and strategic foresight to stay ahead of malicious actors.

Furthermore, the successful cybersecurity assessment at Ather Energy stands as a tangible contribution to enhancing their overall cybersecurity posture.

# About the Project

By exposing vulnerabilities, infiltrating systems, and acquiring sensitive information, the assessment provided invaluable insights that can be leveraged to reinforce the organization's digital resilience.

This proactive approach not only mitigates immediate risks but also contributes to a robust and adaptive cybersecurity strategy capable of withstanding the unpredictable nature of emerging digital threats.

It demonstrates a dedication to not only identifying vulnerabilities but also actively contributing to the development of robust security measures that align with the specific needs and nuances of the organization.

# Objectives of the work

**Realistic Simulation of Adversarial Tactics**

**Purpose:** Red teaming aims to replicate the methodologies used by genuine threat actors, offering a more realistic and immersive testing environment. This approach enables organizations to understand how well their defenses withstand sophisticated and targeted attacks.

**Usage:** Red teaming involves the deployment of advanced tactics such as social engineering, phishing, and exploiting zero-day vulnerabilities. By simulating real-world attack scenarios, organizations gain valuable insights into their susceptibility to complex and evolving cyber threats.

# Objectives of the work

## Continuous Improvement

**Purpose:** Regular red teaming, guided by a structured roadmap, facilitates a cycle of continuous improvement. It ensures that security measures evolve alongside emerging threats, fostering adaptability and resilience.

**Usage:** Insights gained from each red teaming engagement inform future security strategies. This iterative process allows organizations to refine their security measures, update policies, and enhance incident response capabilities based on real-world scenarios.

# Objectives of the work

**Customized and Contextual Assessments**

**Purpose:** Red teaming allows for customized and contextual assessments tailored to the specific needs and nuances of an organization. This approach ensures that assessments align with the organization's unique threat landscape.

**Usage:** Red teaming engagements are designed based on the organization's industry, infrastructure, and operational environment. This customization ensures that assessments are relevant, providing insights that directly contribute to securing the organization effectively.

# About the Working domain and the technology

- "In my role as a cybersecurity analyst, my primary domain of expertise is in offensive security, commonly known as **Red Teaming**.
- Red teaming involves simulating cyber-attacks to evaluate the effectiveness of an organization's security posture. Within this domain, I specialize in assessing and identifying vulnerabilities in various technological environments
- Technologically, my work spans a broad spectrum of areas, including but not limited to network security, web application security, cloud security, and endpoint security. I leverage a diverse set of tools and methodologies to mimic real-world cyber threats, allowing organizations to proactively identify and remediate potential weaknesses in their defenses
- Additionally, my proficiency extends to understanding and exploiting common security weaknesses in both traditional and modern IT infrastructures. This includes expertise in penetration testing frameworks, social engineering tactics, and the manipulation of various security controls to assess an organization's resilience to cyber threats.

# Methodology and Phases

The process begins with a thorough examination of the organization's security landscape to identify potential vulnerabilities and weaknesses that adversaries could exploit. This involves continuous monitoring, threat intelligence analysis, and staying informed about the latest attack vectors

Once potential issues are identified, the next step is to formulate a problem statement. This involves clearly defining the security challenge or risk in a concise and specific manner. The problem statement serves as a foundation for designing effective red teaming exercises that simulate real-world threats

A problem statement could revolve around assessing the resilience of a critical web application to sophisticated **SQL** injection attacks.

The formulation involves specifying the scope, objectives, and success criteria for the red teaming engagement, ensuring alignment with broader organizational goals

# Project Work Flow

Assessment Planning - Detailed planning involves scoping the engagement, defining objectives, and identifying the specific techniques and tactics to be employed during the red teaming exercise.

Execution - This phase involves the active execution of red teaming activities, simulating real-world cyber threats to identify vulnerabilities and weaknesses in the organization's defenses.

Analysis and Reporting - Following the engagement, a thorough analysis of findings is conducted. A comprehensive report is then generated, detailing identified risks, recommended mitigations, and lessons learned.

# Project Work Flow

Identification of Weaknesses - The structured approach allows for the systematic identification of weaknesses and vulnerabilities within the organization's security infrastructure

Strategic Insights - A roadmap provides strategic insights into potential risks and gaps, enabling the organization to prioritize and address critical security issues

Continuous Improvement - Regular red teaming, guided by a roadmap, facilitates a cycle of continuous improvement. The insights gained from each engagement inform future security strategies and measures

# Results and Discussion

## Proactive Security Measures

In the contemporary landscape of cybersecurity, proactive measures are indispensable in safeguarding an organization against an array of evolving threats. The adoption of a strategic roadmap plays a pivotal role in facilitating proactive security measures. By adhering to this structured approach, the organization gains the capability to identify and address potential security issues before they become exploitable by real adversaries.

Proactivity in this context involves a forward-thinking mindset that anticipates and mitigates risks before they manifest into tangible threats. The roadmap serves as a guide, steering the organization through a systematic process of assessment, planning, execution, and analysis.

This proactive approach, underpinned by the strategic guidance of the roadmap, positions the organization as a proactive force against the ever-evolving threat landscape.

# Results and Discussion

**Strategic Resource Allocation**

Effective cybersecurity requires judicious resource allocation, ensuring that efforts are directed towards areas with the highest potential impact on overall security. The strategic roadmap emerges as an invaluable tool in this regard, facilitating a meticulous and data-driven approach to resource allocation.

The roadmap guides the organization in scoping engagements, defining objectives, and identifying specific techniques to be employed during red teaming exercises.

This clarity in planning allows for the prioritization of resources based on the severity and criticality of potential threats.

# Results and Discussion

**Enhanced Incident Response**

The insights derived from red teaming activities play a pivotal role in enhancing incident response capabilities. As part of the roadmap, the execution phase involves simulating real-world cyber threats to identify vulnerabilities and weaknesses.

The subsequent analysis and reporting phase provide a wealth of information that contributes to refining incident response plans and strengthening overall resilience against cyber threats.

Red teaming activities not only highlight potential weaknesses but also shed light on the effectiveness of existing incident response mechanisms. By subjecting the organization to simulated attacks, cybersecurity teams gain firsthand experience in dealing with various threat scenarios.

# Results and Discussion

Moreover, the comprehensive report generated after red teaming exercises provides a detailed breakdown of identified risks and recommended mitigations.

This information becomes a foundational resource for improving incident response protocols.

It allows organizations to prioritize actions, addressing critical vulnerabilities and bolstering defenses where they are most needed.

In essence, the roadmap ensures that the insights gained from red teaming activities are not isolated occurrences but integral components of a holistic cybersecurity strategy.

This continuous feedback loop, driven by the roadmap, contributes to an organization's ability to adapt, learn, and enhance its incident response capabilities over time.

# Challenges Faced in Internship

Securing an internship can be a highly competitive and demanding process, presenting aspiring interns with various challenges. From the initial application phase to adapting to the workplace environment, interns often encounter obstacles that require resilience and adaptability.

# Challenges Faced in Internship

**Competitive Selection Process**

Landing an internship often involves facing a highly competitive selection process. Companies receive numerous applications for limited positions, making it challenging to stand out among the pool of candidates.

Crafting a standout resume and cover letter, highlighting relevant skills and experiences, is crucial. Additionally, preparing for interviews with thorough research about the company and showcasing a genuine passion for the industry can enhance one's chances.

# Challenges Faced in Internship

## Cracking the Interview

The interview phase can be particularly daunting, as it requires effectively communicating one's qualifications, skills, and enthusiasm for the role. Navigating behavioral and technical questions poses an additional challenge.

Preparing thoroughly for potential interview questions, practicing responses, and participating in mock interviews can help build confidence. Demonstrating a proactive and positive attitude during the interview is equally important.

# Challenges Faced in Internship

**Adjusting to the Team and Company Culture**

Once selected, interns face the task of acclimating to the team dynamics and the overall company culture. Understanding expectations and fitting into an established work environment can be both exciting and challenging.

Actively engaging with team members, seeking mentorship, and observing the company culture can aid in a smooth transition. Flexibility and openness to learning from experienced colleagues contribute to successful integration into the workplace.

# Challenges Faced in Internship

### Overcoming Imposter Syndrome

Interns may experience imposter syndrome, feeling like they don't belong or questioning their capabilities. This psychological challenge can impact confidence and hinder performance.

Acknowledging that it's normal to feel a bit overwhelmed initially and seeking constructive feedback from mentors and colleagues can help combat imposter syndrome. Focusing on accomplishments and continuous learning reinforces confidence.

# Challenges Faced in Internship

**Balancing Responsibilities and Learning Objectives**

Striking the right balance between fulfilling assigned tasks and achieving personal learning objectives can be a challenge. Interns may find themselves caught between meeting immediate demands and pursuing long-term growth.

Open communication with supervisors regarding learning goals, seeking opportunities to take on diverse tasks, and maintaining a proactive approach to professional development can help interns navigate this challenge effectively.

# Challenges Faced in Internship

**Networking and Building Professional Relationships**

Establishing meaningful connections within the organization and industry is essential for future career prospects. However, interns may find it challenging to network effectively.

Attend company events, connect with professionals on platforms like LinkedIn, and express genuine interest in learning from colleagues. Building relationships gradually by actively participating in team activities can foster a supportive network.

# Challenges Faced in Internship

**Demonstrating Initiative**

Interns may struggle with finding opportunities to showcase their initiative and take on additional responsibilities, especially in a structured environment.

Proactively seeking feedback, volunteering for projects, and demonstrating a genuine interest in contributing beyond assigned tasks can highlight an intern's initiative.

# Q&A

# Thank you !!