Training Title: Cloud Security 101

Syllabus:

Day 1:

1. Introduction to Cloud pen testing

    - Definition and purpose of Cloud pen testing
    - Differences between traditional pen testing and Cloud pen testing
    - Key considerations for Cloud pen testing (such as scope, permissions, and legal implications)

2. Overview of AWS and Azure

    - Introduction to the two major Cloud providers: AWS and Azure
    - Overview of the different services and offerings provided by each provider

3. Identifying and enumerating Cloud resources

    - Techniques for discovering and mapping out Cloud resources, such as:
        - Scanning for open ports and services
        - Enumerating Cloud metadata and APIs
        - Using open-source intelligence (OSINT) techniques
        - IAM misconfiguration
        - Service misconfiguration
            - S3
            - EC2
            - Lambada Function
    - Tools and techniques for automating resource discovery and enumeration

4. Testing for vulnerabilities in Cloud infrastructure and applications

    - Overview of common vulnerabilities and attack vectors in Cloud environments
    - Techniques for testing for vulnerabilities, such as:

        - Performing network and port scans
        - Using tools and frameworks for testing Cloud security

5. Automating Vulnerability Assessment testing using AWS CLI and Python

---

Day 2:

1. Exploiting vulnerabilities and gaining access to Cloud resources

    - Techniques for exploiting vulnerabilities and gaining unauthorized access to Cloud resources, such as:
        - Using known vulnerabilities and exploits
        - Brute forcing passwords and keys
        - exploiting misconfiguration on services
    - Techniques for maintaining access and establishing persistence in Cloud environments
        - Disabling security controls and monitoring mechanisms
        - Creating backdoors or other means of re-entry in case their initial access is detected and blocked

        - Installing persistent malware or rootkits
        - Modifying system or configuration files to ensure that their access remains even after a restart
        - Creating scheduled tasks or cron jobs to run their malicious code on a regular basis
    - The importance of proper clean-up and post-exploitation activities
        - Remove all traces of the attack
        - Monitor for future attacks

2. Best practices for securing Cloud environments

    - Overview of best practices for secure Cloud deployment and operation
    - Strategies for implementing least privilege, network segmentation, and other security controls in Cloud environments
    - Techniques for monitoring and detecting security threats in Cloud environments

3. Advanced Cloud pen testing techniques

    - Attacking hybrid Cloud environments
    - Attacking Cloud-based applications
    - Attacking Cloud-based storage
    - Attacking Cloud-based networking

4. Conclusion and next steps for learning more about Cloud pen testing

    - Summary of key takeaways from the workshop
    - Recommendations for further learning and resources for staying up to date on Cloud pen testing best practices and techniques

---

Training Abstract:

The Tools watch Academy is pleased to announce a 2-day training on Cloud Penetration Testing for Amazon Web Services (AWS) and Microsoft Azure, including a Capture the Flag (CTF) event to give attendees the opportunity to practice their skills on their own. This course is suitable for beginners and professionals alike and aims to provide attendees with the confidence and skills to conduct cloud penetration testing on their own.

The training covers a range of topics, including vulnerability assessment, misconfiguration identification, and exploitation techniques. Attendees will learn about cloud security best practices and will have the opportunity to practice identifying and exploiting vulnerabilities in cloud environments. The CTF event will allow attendees to apply their knowledge and skills in a hands-on setting, giving them valuable experience in cloud penetration testing. By the end of the course, attendees will be able to conduct comprehensive cloud penetration tests and provide recommendations for improving the security of cloud-based systems.

Key takeaways from the training include an understanding of cloud security best practices, the ability to identify and exploit vulnerabilities in cloud environments, and the skills to implement secure configurations in the cloud. Don't miss this opportunity to enhance your cloud security skills and join the Tools watch Academy for this exciting training, including the CTF event.

Key takeaway for Attendees:

- Understanding of the purpose and importance of Cloud pen testing: Attendees will learn why it is important to test the security of Cloud environments and how Cloud pen testing differs from traditional pen testing.

- Knowledge of key concepts and best practices in Cloud security: Attendees will learn about key security concepts and best practices for securing Cloud environments, such as least privilege, network segmentation, and monitoring.
- Familiarity with the major Cloud providers (AWS and Azure) and their security models: Attendees will learn about the security models and offerings of the two major Cloud providers, AWS and Azure, and how to identify and enumerate resources in these environments.
- Ability to identify and enumerate Cloud resources: Attendees will learn techniques for discovering and mapping out Cloud resources, such as using scanning tools and open-source intelligence (OSINT) techniques.
- Skills in testing for vulnerabilities in Cloud infrastructure and applications: Attendees will learn how to test for vulnerabilities in Cloud environments, including how to perform security assessments, penetration tests, and use tools and frameworks for testing Cloud security.
- Techniques for exploiting vulnerabilities and gaining unauthorized access to Cloud resources: Attendees will learn how to exploit vulnerabilities and gain unauthorized access to Cloud resources, including using known vulnerabilities and exploits, brute forcing passwords and keys, and using social engineering techniques.
- Best practices for securing Cloud environments: Attendees will learn about best practices for secure Cloud deployment and operation, including strategies for implementing security controls and monitoring for threats.
- Understanding of advanced Cloud pen testing techniques: Attendees will learn about advanced techniques for attacking Cloud environments, such as attacking hybrid Cloud environments, Cloud-based applications, and Cloud-based storage.
- Recommendations for further learning and resources: Attendees will receive recommendations for additional learning resources and ways to stay up to date on Cloud pen testing best practices and techniques.

Author Bio:

Animesh Roy

Animesh Roy is an experienced cyber security professional who has served clients including governments, businesses, schools and universities, the military, and the community. He runs a community called "Arishti Live" to help those interested in working in the field and performs freelance consulting work for other vendors. He is known for his strong consulting and training skills and uses real-world case studies in his training sessions. He is also a partner in cybersecurity training with "TÜV SÜD" and has given talks on the subject at various locations, including Kolkata, OWASP Kolkata, SCRB, and Gangtok NIC. These talks can be found on his YouTube channel through the following links:

- https://www.youtube.com/watch?v=4gc6DfwJZWc
- https://www.youtube.com/watch?v=ma_xqtY0EMo
- https://www.youtube.com/watch?v=f0ZwYHRO2Ug
- https://youtube.com/playlist?list=PLI7QWMwOhNkQjcU5gOtOQ8DkjRjw4nxw

Namrata

Namrata is an active contributor in the Indian security community. She was one of the Null Ahmedabad chapter's co-leaders. She was also in charge of the Gujarat chapter of InfosecGirls. She is enthusiastic about hardware security, network security, cloud security, OSINT, and social engineering. She is quite well for her cloud security knowledge and skills, which include identifying cloud security threats, developing new features to meet security goals, and establishing. She is intimately familiar with the cloud security architect because she is knowledgeable about the organization's cloud-based security solutions and systems, as well as their technical direction, configuration, and deployment. She is currently working on vehicle safety and security. She is very extremely enthusiastic about her Lock-Picking abilities. She recently delivered workshop called Unlocking the Secret - Lock Picking in Bsides Delhi 2022. She also demonstrated card cloning as low-frequency exploitation

using the Proxmark3 in a local community chapter. She has also made contributions to the study of GSM network security. Namrata has trained over 1500 police officers from six different Indian states and three union territories, drawing on her background as a cyber lawyer and her expertise in cybercrime investigation. Also, a cyber lawyer with experience dealing with cybercrime. She'd already demonstrated her lock-picking prowess in a few local InfoSec communities.