MOOC COMPLETION REPORT

Name	**Saurabh Bisht**
Registration No.	**PV-23010336**
University Roll Number	**2301336**
Program	**Master of Computer Applications (MCA)**
Semester	**IV**
Academic Year	**2023–2025**

MOOC COURSE DETAILS

Field	Information
Course Title	Introduction to Cybersecurity Tools & Cyberattacks
Platform	Coursera
Offering Institution	IBM
Course Duration	6 weeks
Instructor(s)	IBM Skills Network Team, Dee Dee Collette
Certificate ID / URL	https://coursera.org/verify/GIX34SM3ZEI3

Table of Contents

1. Introduction

Cybersecurity is a critical field that protects digital assets, personal privacy, and organizational data. The "Introduction to Cybersecurity Tools & Cyber Attacks" course by IBM on Coursera provides a thorough foundation for understanding the current landscape of cyber threats and the tools used to defend against them. This document summarizes the course content week by week, offering detailed explanations, examples, and practical applications.

2. Week 1: History of Cybersecurity & Critical Thinking

2.1 The Evolution of Cybersecurity

Cybersecurity has evolved dramatically since the early days of computing. Initially, security was not a major concern because computers were rare and isolated. However, as networks grew and the internet became widespread, so did the risks.

Key Milestones:

- 1970s-1980s: The first computer viruses and worms appeared, such as the "Creeper" virus and the "Morris Worm."
- 1990s: The rise of the internet brought new threats, including email viruses and early hacking incidents.
- 2000s: Major breaches and the spread of malware like "ILOVEYOU" and "Code Red" highlighted vulnerabilities.
- 2010s-present: Cybersecurity became a global concern, with high-profile attacks on governments, corporations, and individuals. Events like the WannaCry ransomware attack and the Equifax data breach demonstrated the scale of modern cyber threats.

2.2 Importance of Critical Thinking

Critical thinking is essential in cybersecurity. It involves analyzing information objectively, questioning assumptions, and making informed decisions.

Five Elements of Critical Thinking:

1. Questioning: Always ask why and how.
2. Gathering Evidence: Collect relevant data before making decisions.
3. Analyzing: Break down complex problems into manageable parts.
4. Synthesizing: Combine information from different sources.
5. Evaluating: Assess the reliability and relevance of information.

2.3 Real-World Example

During the 2017 WannaCry ransomware attack, organizations that practiced critical thinking—such as regularly backing up data and questioning suspicious emails—were better prepared to respond and recover.

3. Week 2: Cybersecurity Threats & Attackers

3.1 Types of Threat Actors

Cyber threats come from various sources, each with unique motivations and tactics.

Main Threat Actors:

- Hackers: Individuals or groups seeking unauthorized access for profit, challenge, or activism.
- Insiders: Employees or contractors who misuse their access.
- Nation-States: Governments conducting espionage or sabotage.
- Cybercriminals: Organized groups focused on financial gain.
- Hacktivists: Individuals or groups promoting political or social causes.

3.2 Common Cyber Threats

- Malware: Software designed to harm or exploit systems. Includes viruses, worms, Trojans, ransomware, and spyware.
- Ransomware: Encrypts files and demands payment for their release.
- Phishing: Fraudulent emails or messages tricking users into revealing information.
- Social Engineering: Manipulating people into breaking security protocols.

3.3 Case Study: Phishing Attack

A major bank experienced a phishing attack where employees received emails that appeared to be from their IT department. The emails requested password resets, leading to a data breach. This highlights the importance of employee training and awareness.

3.4 Defending Against Threats

11. Antivirus Software: Detects and removes malware.

12. Firewalls: Blocks unauthorized access.
13. Employee Training: Teaches staff to recognize suspicious activity.
14. Incident Response Plans: Outlines steps to take during an attack.

4. Week 3: Internet Security Threats & Controls

4.1 Network-Based Attacks

- Network Mapping: Attackers scan networks to find vulnerable devices.
- Packet Sniffing: Intercepting data as it travels across a network.
- IP Spoofing: Pretending to be another device by falsifying IP addresses.
- Denial-of-Service (DoS): Flooding a system with traffic to make it unavailable.

4.2 Application-Level Attacks

- SQL Injection: Inserting malicious code into database queries.
- Cross-Site Scripting (XSS): Injecting scripts into web pages viewed by others.

4.3 Security Controls

Types of Controls:

- Preventive: Firewalls, encryption, access controls.
- Detective: Intrusion detection systems, security logs.
- Corrective: Backup and recovery processes.

4.4 Vulnerability Management

Regularly scanning systems for vulnerabilities and applying patches is essential. Tools like Nessus or OpenVAS can automate this process.

4.5 Incident Response

A well-prepared incident response plan includes:

- Detection: Identifying the breach.
- Containment: Limiting the spread.
- Eradication: Removing the threat.
- Recovery: Restoring systems.
- Lessons Learned: Reviewing the incident for future improvement.

4.6 Digital Forensics

Digital forensics involves collecting and analyzing digital evidence after a security incident. This helps determine the cause, impact, and perpetrator of the attack.

5. Week 4: Identity and Access Management (IAM)

5.1 Principles of IAM

IAM ensures that only authorized individuals can access specific resources.

Four Categories of IAM:

1. Identification: Recognizing a user.
2. Authentication: Verifying the user's identity.
3. Authorization: Granting permissions.
4. Accountability: Tracking user actions.

5.2 Authentication Methods

- Passwords: Most common, but vulnerable to attacks.
- Biometrics: Uses fingerprints, facial recognition, or voice.
- Tokens: Physical or digital devices generating codes.
- Multifactor Authentication (MFA): Combines two or more methods for enhanced security.

5.3 Authorization Models

- Role-Based Access Control (RBAC): Permissions based on user roles.
- Attribute-Based Access Control (ABAC): Permissions based on attributes like location, time, or

device.

5.4 Single Sign-On (SSO) and Passkeys

- SSO: Allows users to access multiple applications with one login.
- Passkeys: Passwordless authentication using biometrics or devices.

5.5 Practical Application

Enabling MFA on email and banking accounts significantly reduces the risk of unauthorized access.

6. Week 5: Physical Security and Threats

6.1 Importance of Physical Security

Physical security protects hardware, data, and personnel from physical actions and events that could cause loss or damage.

6.2 Types of Physical Threats

- Unauthorized Access: Intruders gaining entry to secure areas.
- Theft: Stealing devices or sensitive documents.
- Natural Disasters: Fires, floods, earthquakes.
- Environmental Hazards: Power surges, temperature extremes.

6.3 Physical Security Controls

- Locks and Access Cards: Restrict entry to authorized personnel.
- Surveillance Cameras: Monitor activities.
- Security Guards: Provide on-site protection.
- Alarms: Alert to breaches or hazards.

6.4 Integrating Physical and Cybersecurity

For example, a data center may use biometric access controls and CCTV to protect servers, while also employing firewalls and intrusion detection systems for digital security.

7. Week 6: Final Project and Course Wrap-Up

7.1 Final Project

The final project involves designing and implementing a secure access system using multifactor authentication. This demonstrates the practical application of IAM principles.

Steps:

1. Assess Risks: Identify potential threats.
2. Select Controls: Choose appropriate authentication methods.
3. Implement System: Set up MFA for a sample application.
4. Test Security: Attempt to bypass controls and document results.

7.2 Course Review

The course wraps up by reviewing key concepts and encouraging further learning. Topics include:

- The evolving threat landscape.
- The importance of continuous education.
- Career paths in cybersecurity

8. Reflections and Learning Outcomes

8.1 Personal Reflections

Throughout this course, I gained a deeper understanding of both the technical and human aspects of cybersecurity. Real-world case studies and hands-on exercises reinforced the importance of proactive defense and continuous learning.

8.2 Key Takeaways

- Cybersecurity is a constantly evolving field requiring vigilance and adaptability.
- Both technical controls and human awareness are vital for effective defense.
- Practical skills, such as configuring MFA and responding to incidents, are essential for any cybersecurity professional.

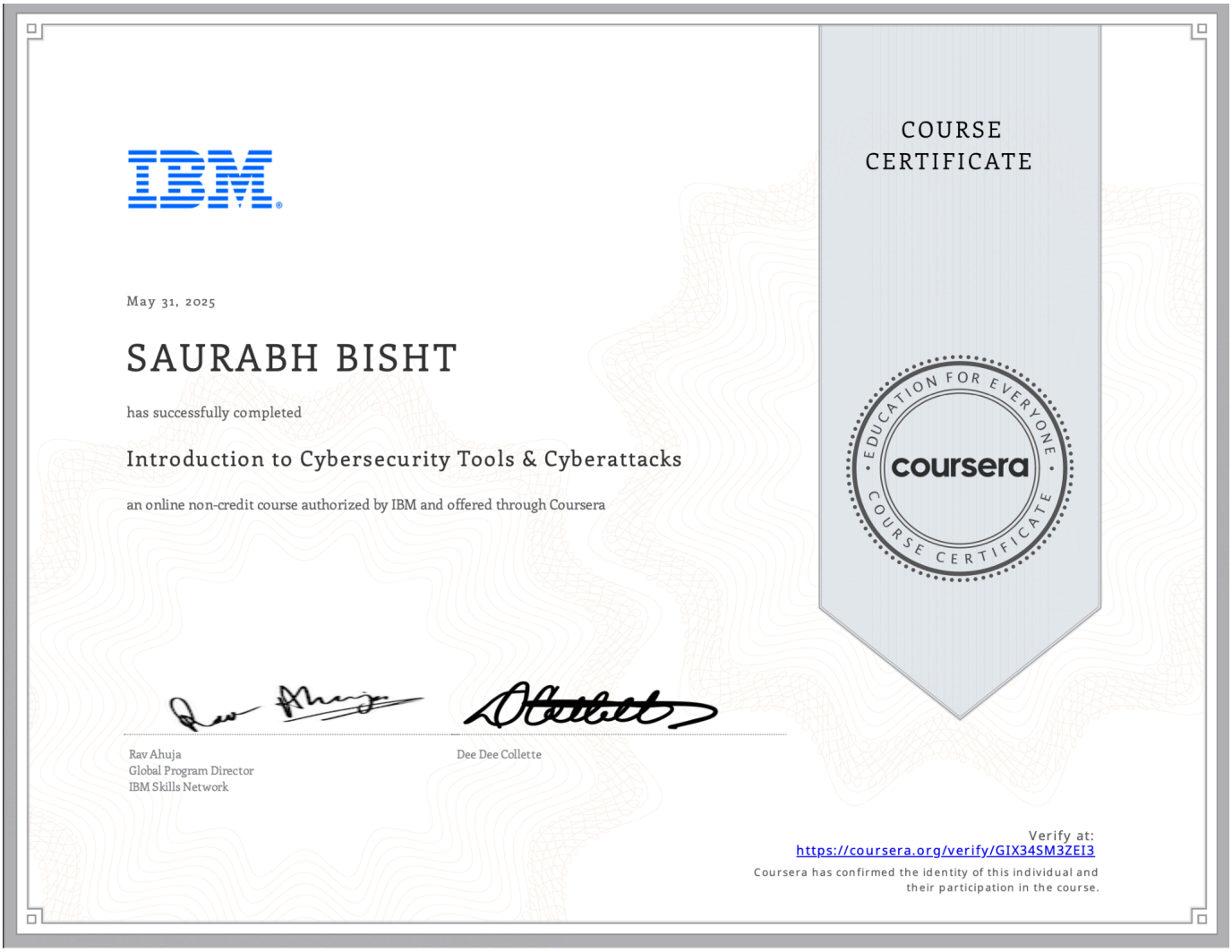
9. Skill Gained

- Antivirus: Software that detects and removes malware.
- Authentication: Verifying the identity of a user or device.
- Firewall: A system that controls incoming and outgoing network traffic.
- Malware: Malicious software designed to harm systems.
- Phishing: Fraudulent attempts to obtain sensitive information.
- Ransomware: Malware that encrypts files and demands payment.
- Vulnerability: A weakness that can be exploited by attackers.

10. References

- IBM Skills Network. (2024). Introduction to Cybersecurity Tools & Cyber Attacks. Coursera.
- IBM Security X-Force Threat Intelligence Index.
- National Institute of Standards and Technology (NIST) Cybersecurity Framework.
- Additional readings and resources from course materials.

CERTIFICATE



IBM

COURSE CERTIFICATE

May 31, 2025

SAURABH BISHT

has successfully completed

Introduction to Cybersecurity Tools & Cyberattacks

an online non-credit course authorized by IBM and offered through Coursera

EDUCATION FOR EVERYONE · coursera · COURSE CERTIFICATE

Rav Ahuja
Global Program Director
IBM Skills Network

Dee Dee Collette

Verify at:
https://coursera.org/verify/GIX34SM3ZEI3

Coursera has confirmed the identity of this individual and their participation in the course.

DECLARATION

I hereby declare that the above MOOC course was completed by me independently, and all information provided is accurate.

Signature: Saurabh Bisht

Date: 31/05/2025