Planprogrami për Cyber Security

Module 1: Introduction to Information Security Management

- *Introduction to Information Security Management*

This session introduces information security management, highlighting its importance in today's digital landscape and outlines the key principles and concepts of information security management. The session will also delve into the foundational knowledge of cybersecurity, emphasizing the impact of threats on organizations and individuals

- *Security Policies and Procedures*

Session three discusses the pivotal role of policies and procedures in effective security management. It emphasizes the development, implementation, and continuous monitoring of robust security policies and procedures.

- *Asset Management*

This session covers the significance of asset management in information security, as well as the importance of ensuring the security of those assets. It introduces asset management processes, such as identification, classification, control, and inventory management of software, hardware, and information assets.

- *Characteristics and Benefits of Cloud and Virtualization Technologies*

This session introduces the fundamental concepts of cloud and virtualization technologies, with a focus on their characteristics and benefits in the context of information security management. Students will understand how these technologies integrate into modern IT infrastructures, the potential security advantages they offer, and the need for adopting best practices when leveraging them.

- *Vulnerability and Patch Management*

Session five delves into the topic of vulnerabilities and their impact on security. It introduces the practice of patch management, providing strategies and best practices, vulnerability assessments, and highlights the necessity of regular system updates.

- *Identity and Access Management*

Session five delves into the topic of vulnerabilities and their impact on security. It introduces the practice of patch management, providing strategies and best practices, vulnerability assessments, and highlights the necessity of regular system updates.

- *Third-Party Management*

The seventh session addresses third-party management in information security. It discusses how to manage risks associated with third parties, third-party security assessments, audits, and the necessity of security agreements in third-party contracts. It also introduces the Secure Software Development Lifecycle (SDLC).

- *Security Operations and Monitoring*

Session eight provides an understanding of Security Operations Centers (SOCs), processes for incident detection, analysis, and response. It also introduces Security Information and Event Management (SIEM) and Intrusion Detection and Prevention Systems (IDS/IPS).

- *Risk Management and Compliance*

Session nine addresses understanding and managing risk in the context of information security, with an emphasis on risk assessment and mitigation strategies, regulatory compliance, and information security standards like ISO 27001.

- *Security Assessment and Testing*

Session ten discusses security assessment and testing methods, including penetration testing and vulnerability assessments. It covers the basic concepts of threat hunting and the execution of social engineering campaigns.

- *Incident Response*

The eleventh session discusses the fundamentals of incident response, including the step-by-step process of responding to security incidents and the role of an incident response team in ensuring rapid and effective recover

- *Disaster Recovery*

This session introduces students to the importance of business continuity planning and business impact analysis. It elaborates on disaster recovery strategies and procedures, emphasizing the critical role of backups and synchronization to ensure data integrity and availability..

- *Data Protection*

This session focuses on data protection, covering the data lifecycle, data protection strategies such as encryption and masking, understanding Data Loss Prevention (DLP) strategies, and responses to data breaches..

- *Legal and Ethical Considerations in Information Security*

Session fourteen discusses the legal and ethical considerations related to information security, including laws related to the field, ethical hacking guidelines, and the importance of professional ethics in information security practice.

- *Module Review and Group Discussions*

The fifteenth session allows students to review the module content, analyze sample examination questions, and participate in group discussions on current security challenges, fostering collaborative learning and examination preparation.

- *Review & Group Discussion*

The final session consists of an examination designed to assess students' comprehension of the module material and their ability to practically apply the knowledge gained throughout the module.

Module 2: Network Security

- *Introduction to networking*

This session offers a comprehensive overview of the fundamental principles and technologies of modern computer networks. We will delve into the basics of network architecture, protocols, data

transmission, and network topologies. Through this course, a foundational understanding of how data flows across interconnected devices and systems.

- *Introduction to network components*

This session provides an overview of the key building blocks that constitute computer networks. Participants will delve into the core components such as routers, switches, modems, access points, and cables. Through this course, students will acquire a foundational understanding of how these components work together to facilitate data communication and enable seamless connectivity.

- *Essentials of network devices*

This session introduces the fundamental aspects of network devices such as routers, switches, and access points. Participants will develop a basic understanding of how these devices facilitate data transmission, connectivity, and efficient network management. Through this, insights into the essential building blocks of modern network infrastructure will be provided

- *Introduction to initial device configuration*

This session is an essential introduction to the process of setting up and configuring network devices. Participants will learn the foundational steps required to initialize devices like routers, switches, and firewalls. Through this course, students will gain a basic understanding of how to establish device connectivity, assign essential settings, and ensure security measures are in place

- *Understanding of core networking concepts (TCP/IP, DNS, DHCP, HTTP/S, SSH) 1/3*

During this course, a comprehensive exploration of fundamental networking principles, including key protocols such as TCP/IP, DNS, DHCP, HTTP/S, and SSH will be provided. Participants will delve into the inner workings of these essential elements that underpin modern network communication.

- *Understanding of core networking concepts (TCP/IP, DNS, DHCP, HTTP/S, SSH) 2/3*

Follow up of the session, part two.

- *Understanding of core networking concepts (TCP/IP, DNS, DHCP, HTTP/S, SSH) 3/3*

Follow up of the session, part three.

- *Introduction to Network Security*

This session provides essential principles and methodologies for securing computer networks from potential cyber threats. Participants will have the opportunity to deep dive in significant subject areas, including encryption, authentication, firewalls, and intrusion detection systems cultivating a foundational comprehension of the tactics and technological solutions employed to shield network

- *Network Security Policy, Protocols and Controls*

This offers a concise exploration of crucial components in ensuring network security. Participants will delve into topics including security policies, protocols, and control mechanisms. Participants

will gain insights into establishing effective security guidelines, implementing protective protocols, and deploying control measures to safeguard networks from potential threats.

- *Implementation of Network Security Devices*

This course focuses on the practical implementation of network security devices. Participants will learn how to deploy and configure key security tools such as firewalls, intrusion detection systems, and VPNs. Through hands-on activities, students will gain experience in setting up these devices to enhance network protection.

- *Introduction to Zero Trust*

This provides an essential overview of the Zero Trust security model. Participants will explore the core principles and concepts behind this approach, which emphasizes continuous verification and strict access controls. Through this training, attendees will gain insights into implementing a security framework that treats all network activities as potentially risky, fostering heightened protection against modern cyber threats.

- *Network Traffic Monitoring and Analysis*

This session offers a comprehensive exploration of effectively observing and dissecting network data flow. Participants will be introduced to techniques for capturing, scrutinizing, and interpreting network traffic patterns. Participants will acquire the skills necessary to detect anomalies, identify potential security breaches, and optimize network performance.

- *Network addressing and network troubleshooting (tcpdump, wireshark)*

This session introduces the intricacies of IP addressing, subnetting, and network troubleshooting methodologies. Participants will gain practical hands-on experience in configuring network addresses and diagnosing common network issues. This session equips participants with the skills necessary to manage network addressing effectively and resolve connectivity challenges

- *Communication and Network Support*

This session offers a comprehensive exploration of effective communication practices and technical assistance within network environments. Participants will understand strategies for clear and efficient communication, both within technical teams and with non-technical stakeholders.

- *Review & Group Discussion*

This session allows students to review the module content, analyze sample examination questions, and participate in group discussions on current security challenges, fostering collaborative learning and examination preparation.

- *Module Review & Exam Preparation*

The final session consists of an examination designed to assess students' comprehension of the module material and their ability to practically apply the knowledge gained throughout the module.

Module 3: Vulnerability Assessment & Penetration Testing

- *Introduction to VAPT*

In this session we will explore the basics of vulnerability assessment and penetration testing, its significance, types, and methodologies. Definitions, the importance, the types, the methodologies, and the differences between them. Real-world case studies of successful VAPT.

- *Understanding Information Gathering*

In this session, we will discuss various types of information that can be collected and the potential use of each. Hands-on practice with some popular information gathering tools and techniques, such as Whois, nslookup, and the Harvester.

- *Scanning & Enumeration*

In this session, we will discuss various types of information that can be collected and the potential use of each. Hands-on practice with some popular information gathering tools and techniques, such as Whois, nslookup, and the Harvester.

- *Introduction to Hardening and SIEM Systems – 1/2*

In this session, we' will introduce system hardening and SIEM. Participants will understand the importance of these topics in preventing attacks and will get an overview of some SIEM tools

- *Introduction to Hardening and SIEM Systems – 2/2*

Continuing from the previous session, we'll delve deeper into system hardening techniques and effective use of SIEM systems. Participants will get hands-on practice

- *Understanding Social Engineering and Phishing – 1/2*

In this session, we will explore the concept of phishing, its techniques, and prevention methods. Hands-on exercises on how to identify phishing attempts will be conducted together with real life examples from the industry and highlights of the newest trends and attack vectors used.

- *Understanding Social Engineering and Phishing – 2/2*

Follow up of the previous session.

- *Introduction to Vulnerability Scanners*

In this session, we will explore the principles of vulnerability scanning, differences between various tools. Theoretical overview of how scanners work and the type of vulnerabilities they can detect

- *Using Open Source Scanners*

Practical session on popular open-source scanners like OpenVAS, Nessus Essentials, etc. Each participant will scan a test network and interpret the results.

- *Paid Vulnerability Scanners*

In this session, we will dive into the advanced features of paid scanners like Nexpose, Nessus Pro, etc. Demonstrations on a test network and discussion on when and why to use paid tools

- *Exploitation Basics*

In this session, we will discuss the principles of exploiting vulnerabilities. Introduction to manual and automated exploitation techniques with demonstrations.

- *Using Exploit Databases & Metasploit*

In this session, we will dive into the usage of Exploit DB and Metasploit. Participants will engage in hands-on activities to exploit identified vulnerabilities on a test network

- *Incident Response and Digital Forensics*

In this session, we will introduce and discuss the various phases of the Incident Response Lifecycle according to the National Institute of Standards and Technology (NIST) and SANS frameworks. Further concepts of digital forensics and its role in cyber incident investigations are explained together with real-world scenarios and best practices, as well as introduction to incident response and forensics tools with hands-on practice.

- *Report Writing & Communication*

This session will delve into the importance of clear and effective communication in VAPT. We'll host an interactive workshop on report writing, teaching you how to create professional and comprehensive reports

- *Ethics & Legal Considerations*

In this session, we will discuss the ethical and legal aspects of penetration testing. We'll explore case studies on breaches of ethics and their consequences and understand the importance of getting permission before conducting VAPT.

- *Review & Group Discussion*

Participants will perform a full VAPT on a test network, write a report on their findings, and present their results. Review of assessments, feedback, and wrap-up. Each session includes theoretical learning, hands-on exercises, discussions, and breaks.

- *Module review & examination*

The final session consists of an examination designed to assess students' comprehension of the module material and their ability to practically apply the knowledge gained throughout the module.

Module 4: Soft Skills

- *Analytical skills*
  - Understand analytical skills.
  - Understand analytical skills needed for Cyber Security.
  - Learn what to look for when analyzing ads.
- *Design skills,*
  - Basic design skills
- *Communication skills*
  - Basic email writing & communication with client skills.
  - Daily communication skills to have with clients.
  - Daily communication skills to have with clients II.

- *Presentations skills*
  - Importance of understanding the audience & types of presentations and how each one differs

- *Basics of time management*
  - Learn to utilize different time management apps
  - Leverage the benefits of time management apps

- *Various types of online outsourcing marketplaces that exist and their utilization in the context of Kosovo*
  - Various types of online outsourcing marketplaces that exist and their utilization in the Kosovo
  - Presenting main platforms for outsourcing skills & how to create & improve profiles (e.g.: Upwork, Fiverr, etc.)

- *How to approach and communicate with different types of clients & basics of project management (use of project management and communication software)*
  - How they can best approach communicate with clients
  - The importance of connecting with the client and understanding their needs & using tools to better manage the communication

- *Making a resume, project portfolio.*
  - Tips and Tricks on what a resume should contain & how to present your experience and education
- *Bidding, proposing and negotiating with clients*
  - The importance preparing a bid and negotiating with a client
  - How to best shape the presentations & how to use negotiating tactics to achieve their goals
- *Building long-term working relationships with online clients*
  - Tips on how to maintain the relationship with online clients/employer
- *Basics use of MS Office and Google Workspace*
  - How to use MS office and google docs most efficiently and appropriately