Unit 1:

Unit code: Foundation of Cyber Security & Information Security Management

Level 7:

Credit value:

Guided learning hours: 20

Module designer: Dr. Shadi Zarrabi

Unit aim

This module aims to built a general understanding of cyber/information security in a way that students can apply the fundamental concepts and practices of cyber/info security on real case scenarios.

Unit introduction

This module introduces students to the foundations of cyber security, and professional context of information security management according to COMPTIA Security ++. Students learn the goals (principles of CIA triad) and concepts of cyber security and basics of cyber security on origin/definitions of cybersecurity/infosec. At the end of the module, they should be able to identify different types of cyber threats, risks and vulnerabilities and to distinguish goals and actions of attackers. Then they should be able to build fundamental skills of cyber security strategy to protect cyber spaces against risks and threats. They should be able to also understand the ethics, legal/regulatory landscape of cyber security and cyber space and demonstrate knowledge and basic skills of compliance procedures.

Learning outcomes and assessment criteria

In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

On completion of this unit a learner should:

Learning outcomes	Assessment criteria
1 to understand basic concept of COMPTIA Security+ Domain 1	1.1 Explain principles of CIA triad 1.2 Distinguish different types of cybercrimes and review their impacts on organisations 1.3 Distinguish different types of threat actors/threat landscape/threat harms
2 to understand ethics, legal/regulatory landscape of cyber security/infosec according to CompTIA CySA Domain 4	2.1 Explain the court systems in the UK and relevant courts to cybercrimes and technology 2.2 Explain privacy and data protection and analyse the impact of personal data breach 2.3 Explain Standards 2.4 Explain Computer Misuse Act and apply it to cyber crimes 2.5 Explain Code of Ethics and apply it on computing applications
3 Be able to apply methods and strategies for cyber security according to CompTIA Security + Domains 2,3 and CompTIA CySA + Domain 4	3.1 Explain cyber kill chain 3.2 Explain appropriate confidentiality/Integrity/availability methods 3.3 Explain appropriate authentication/authorization methods 3.4 Explain appropriate non-repudiation methods 3.5 Explain security by design 3.6 Explain appropriate privacy methods 3.7 Explain Business Continuity 3.8 Apply defense in depth 3.9 Apply security controls including physical security 3.10 Develop security policies

4 be able to conduct information security and privacy risk management according to CompTIA Security + Domain1 and CompTIA CySA + Domain4	4.1 Identify cyber/information security vulnerabilities 4.2 Use information security risk management frameworks 4.3 Use DPIA 4.4 Use appropriate security controls to treat risks

Unit content

---

1. **to understand concept of cybersecurity/infosec**

Basic concepts of COMPTIA Security +: definition of cyber security, CIA triad, , type of threats (internal, external, Malware & Social Engineering, spoofing, Dos v DDoS, Man-in-the-Middle, Password attacks, DNS attacks, etc), Threat Actors and vectors, Types of Harm, Threat Landscape.

2. **to understand ethics, legal/regulatory landscape of cyber security/infosec**

UK court systems, data protection, GDPR, NIST Privacy Framework, Computer Misuse Act, Tort of Negligence, Computer ethics principles and their impacts on cyber security methods, Institute for Certification of IT Professionals (ICCP) Code of Ethics.

3. **Be able to apply methods and strategies for cyber security**

Cyber security strategies: security services such as authentication (Kerberos, etc), authorisation, confidentiality (Encryption basics, Access Control, etc.), Integrity (Hashing, Digital Signature, etc), availability (SPOF, Disk Redundancy, etc.), non-reputation, privacy, Cyber Kill Chain, defence in deep (Layered Security), physical security, security controls, incident response, basic of security tools (anti-malware, antivirus, routine audits, event logs, firewall, etc), Business Continuity (BCP, BIA, etc), Control Implementation Methods, security policies (personnel policies, account management, data policies, etc).

4. **Be able to conduct information security risk management**

threat assessment, Information security risk management: Risk Management concepts and their types such as vulnerability (lack of update, default configuration, etc), basic of checking for vulnerabilities (Identifying IP address, open ports, penetration testing, etc), likelihood, impact, risk assessment matrix, risk avoidance, transfer, acceptance, etc, quantitative and qualitative risk assessment, Risk Treatment, ISO27001 and NIST frameworks, DPIA

Essential Guidance for tutors:

Delivery:
The module is delivered weekly with 2 hours sessions including 1 hour lecturing and 1 hour seminar. These include weekly lectures and seminars to encourage debate and discussion. Lectures will be used to introduce the main topics. In seminars, students will work on quizzes, practices and case studies to develop and reinforce the theory covered in the lectures.

The syllabus is divided into a number of related topics. Lecture notes in format of PowerPoint slides and pdf with reference to additional materials are provided for each topic. students are expected to consult independently with additional references to get themselves more familiar with the topics. To gain full advantage of this module students are expected to hone their skills and understand by working through progressive exercises. A seminar sheet is produced for each topic. Also, the practical demonstrations of the technologies will be discussed during the seminar sessions. In seminars students receive feedback on their progress and engage in discussions on issues arising from the exercises.

Learning and teaching activity hours for the module:

Lecture	: 10 hours
Seminar	: 10 hours
Assessment	: 2 hours
Total	: 22 hours

For learning outcome 1: it is important that learners understand the fundamental concepts of cyber and cyber security. Tutors must start by introducing the CIA triad of cyber security and to follow it by explaining how each of these elements of CIA can be targeted by internal and external attacks and different types of attacks such as espionage, trojan horse, SQL attack, brute force, identity theft, phishing, DOS and etc. Students should understand the meaning of threat and its difference from vulnerability and risk and also know different types of threats if they are caused by natural or human factors. Type of attackers from hackers to individuals or organized threat actors, their characteristics and types of harms they cause from modification to interception and other must be taught.

For learning outcome 2: students should learn about principle of ethics in general and in computing. They should be able to apply these principles to activities done by cyber professionals such as penetration testing or reverse engineering. For example, they should know the ethic consideration of penetrating into a client or suspected agent's computer system or what ethic principles need to be taken when reverse engineering an application. They should get familiar with common code of ethics for IT professionals such as ICCP and also to know how to comply with ICCP or any organizational code of ethics. Tutors must introduce the main legal topics and laws relevant to cyber security and privacy such as GDPR and Computer Misuse Act, also tort of negligence. They can give examples of when each applies. They will also get familiar with known standards and frameworks in cyber security such as ISO 27001 and NIST.

For learning outcome 3: student should be able to understand different types of security services, and methods such as confidentiality, availability, integrity,

authentication, authorisation, non-repudiation and privacy. They must get familiar with different tools and methods for each of these services and to be able to distinguish between them. Tutors must explain in brief cyber security strategies such as cyber kill chain, defense in depth, security by design, anonymization, consent, data minimization, security policy and physical security. Tutors must pay more emphasis on the seminar sessions and practical exercises for these topics and practice different case studies with them.

For learning outcome 4: Tutors must explain in details information security risks assessment elements (vulnerability, likelihood, impact and risk) and how to identify and assess them in quantitative and qualitative risk assessment matrixes. They should give examples of different risk scenarios from daily life to cyber security in a way students understand these concepts and learn how each risk is assessed and how different risk treatment strategies are taken for different risk levels. In specific they should examine two main frameworks in information security risk management as ISO27001 and NIST. They must teach different stages of these framework from scope and criteria identification, to asset inventory, categorization, risk identification and assessment to risk treatment strategies and examine them in seminars with some case studies.

Outline learning plan

The outline learning plan has been included in this unit as guidance and can be used in conjunction with the program of suggested assignments.

The outline learning plan demonstrates one way in planning the delivery and assessment of this unit.

Topic and suggested assignments/activities and/assessment
Introduction to unit and program of learning
Tutor-led discussion on definitions of cyber security, CIA, threat and attacker types –learner group work and exercises including individual quizzes on main topic of cyber security and group working on real-world examples of cyber threats and involved cyber security concepts
Tutor lectures on legal and ethical topics of cyber security and then learner practice on real world scenarios of cyber security practices to identify the ethical and legal matters involved and what are their solution
Tutor input on theoretical models and concepts of cyber security methods and strategies and learners individually work on quizzes and cases for confidentiality, integrity, availability, authentication, authorisation and non-reputation. Students will also work in groups to identify and place some relevant mitigation technique against the stage in the kill chain and implement a defense in depth strategy in a scenario of organisation
Tutor to discuss UK court systems, GDPR, Computer Misuse act and Tort of Negligence. Learner research on their local courts in general and in cyber security, and will practice article fast reading. Students will read articles and blogs on legal maters of cyber security in groups and discuss them
Tutor to teach and present stages of ISO 27001, DPIA and NIST and discuss the main elements of risk assessment. Students to participate in a mock test to practice the final exam

Formal Assessment (individual): Exam including 30 optional answer questions
In-formal assignment (seminar session): Students will work in groups on case scenarios to identify the security and privacy risks, create asset inventory and fill risk assessment checklist or DPIA forms
Review of unit and program of assignments

Assessment

For AC1.1: students will have an online exam including 30 questions with optional answers. All questions and answers are from the materials taught in this module. However, to test the level of understanding the answers may include examples or scenarios from external resources. Students will be marked automatically and feedbacks will be provided to them after exam. This assessment weight 100% of their final mark.

Additional Resources

Caravelli, J. and Jones, N., 2019. *Cyber security: Threats and responses for government and business*. ABC-CLIO.

Dulaney, E. and Easttom, C., 2017. *CompTIA Security+ Study Guide: Exam SY0-501*. John Wiley & Sons.

Unit 2: Network Security

Unit code:

Level 7:

Credit value: 10

Guided learning hours: 30

Unit aim

This segment furnishes the learner with an intricate comprehension and practical competence to effectively operate in real-world scenarios concerning network protection. They will acquire the necessary technical proficiency to formulate a secure organizational network and serve as a network administrator proficient in network security technologies, achieving a comprehensive Defense-in-Depth approach.

Unit introduction

This module provides candidates with a foundational comprehension of authentic data transfer structures, network and software technologies. This knowledge equips them to grasp the functioning of networks and learn how to safeguard against, identify, and counteract network assaults. The curriculum includes practical exercises using commonly employed network security utilities. The module readies network administrators to adeptly handle network security technologies and procedures, ensuring comprehensive readiness for safeguarding networks. It encompasses a strategy of protection, identification, and response to ensure network security.

Learning outcomes and assessment criteria

In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

On completion of this unit a learner should:

Learning outcomes	Assessment criteria
1 Understand fundamental networking concepts, analyse protocols and implement established standards according to CompTIA Security + Domain 7, 8 and CompTIA CySA Domain 2	1.1 Distinguish various types of computer networks including WAN, LAN, MAN, Intranet, Extranet and Internet 1.2 Distinguish OSI and TCP/IP models and the various protocols of TCP/IP 1.3 Setting different types of network topologies 1.4 Run and set network components e.g. switch, router, firewall, etc. 1.5 set IP addressing 1.6 Recognise Computer Network Common threats and vulnerabilities e.g. spoofing, firewall by-pass, DDOS, etc.
2 understand and implement secure network architecture concepts according to CompTIA Security + and CompTIA CySA Domain 1 and 4	2.1 Design secure network using various network zones such as DMZ, VLAN, segmentation, etc. 2.2 Design secure Wireless using secure infrastructure modes such as wireless access point, SSID, BSSID, ESSID, WEP, WPA, WPS, wireless hardening, etc. 2.3 Recognise wireless vulnerabilities and attacks such as wireless sniffing, Rogue access point, etc.
3 understand and configure network security features according to CompTIA Security + and CompTIA CySA + Domain 1	3.1 Set network access control methods and protocols such as agent-based an agent-less, SSL, TLS, etc. 3.2 Recognise and use different types of firewalls and set policies and rules such as ACL, Permit/Allow/Deny/Implicit Deny 3.3 Recognise Honeypots and

	Honeynets and their rule in network security 3.4 Recognise and use different types of proxies and their rule in network security 3.5 Recognise and use different types of IDS and their different detection methods (behavior/anomaly, signature-based, rule-based, heuristic) and set up in-bound or out-of-bound modes 3.6 Recognise and use network security protocols and ports such as HTTPS, SSH, FT/SSH, FTPS, SFTP, SCP, TFT, etc.
4 Understand Network Physical Security controls and methods according to CompTIA Security +	4.1 Recognise and establish different physical and host security controls 4.2 Recognise and use deterrence preventive and caballing systems controls

Unit content

---

1 Understand fundamental networking concepts, analyse protocols and implement established standards according to CompTIA Security + Domain 7, 8 and CompTIA CySA Domain 2

Network types: LAN, WAN, MAN, Intranet, Extranet, Internet

Network models: ISO and TCP/IP models

Network topologies: Bus, Star, tree and hybrid topologies, hubs, switch and routers,

Network protocols: TCP and UTP

IP addressing: IPV4 and IPV6 addressing scheme, classes, subnetting and configuration

Network threats and vulnerabilities: MAC address spoofing, DNS flooding and spoofing, firewall by-passing, DOS, DDOS, HTTP flood SSL, password sniffing, eavesdropping, phishing, wireless attacks, missing firmware updates, DNS issues

2 understand and implement secure network architecture concepts according to CompTIA Security + and CompTIA CySA Domain

Network Zones: Network segmentation, layered network design, VLAN, DMZ, wireless network, guest network, virtualization and airgap, 802.11, 802.11i

Wireless Security: wireless access point, SSID, BSSID, ESSID, WEP, WPA, WPS, wireless hardening, wireless vulnerabilities and attacks

3 understand and configure network security features according to CompTIA Security + and CompTIA CySA + Domain 1

network access control: models including agent-based, agentless, in-bound, out-of-band, VPN, wireless access, remote access and protocols including PPP, PAP, CHAP, EAP and EAP methods, layer 2 tunneling, SSL, TLS, Open VPN

firewall types and concepts: packet filtering, stateful, stateless, NGFWs, Application-based firewalls, etc. configure firewall and its rules and policies (ACL, Permit/Allow/Deny/Implicit Deny), firewall logs analysis, Honeypots

different types of proxies: Load balancer, etc.

Network Intrusion Detection systems: NIDS and NIPS, their differences and detection methods (behavior/anomaly, signature-based, rule-based, heuristic), fine-tuning, port mirroring and network taps, out-of-band and in-band set up, DDoS mitigator

Network security protocols: HTTPS, SSH, FT/SSH, FTPS, SFTP, SCP, TFTP, NETbios, DNSSEC, SSL/TLS SMTP, DHCP, SNMP, LDAP, RDP, TLS

4 Be able to plan the development of leadership skills

Detection controls: lighting, signage, security guards for server rooms, alarms, log files

Deterrence controls: access control authentication, workplace security, host security, virtualization security, fences, barricades, air gaps, lockdowns, locked cabinets, faraday cages, key management systems, screen filters for network admins.

Essential guidance for tutors

Delivery

Tutors will need to use a wide range of teaching and learning methods so that learners meet the learning outcomes in this unit. Methods include lectures, seminars, workshops, project work and individual and group assessments.

Some formal delivery will be necessary, but work can be increasingly learner-centred to develop independent learning. Learners need to adopt an investigative, analytical and participative approach to achieve the learning outcomes and reflect on their own experiences and roles to enhance the learning experience.

Sufficient time needs to be built into the delivery schedule to allow learners to undertake the practices needed to help them meet the learning outcomes and be responsible for their own learning.

For learning outcome 1, it is important that learners review the fundamentals of computer network, even if this is a recap of their current knowledge. In order to understand network security requirements in organisations, learners need to explore the fundamentals of the concept of networking, including network types, models and topologies. Tutors must provide complete input on the key elements of IP addressing using practical examples to set up different types of using IP classes and subnetting procedure, as well as evaluating different types of network attacks and vulnerabilities. The development of network admin tasks versus recruiting lab sessions are needed.

When covering learning outcome 2 and 3, it is important to focus on different types of network architectural elements and security features which help to protect security of network. For most of the learning outcome, it is preferable for time to be spent on consolidating and actively learning and considering the application of the security architectural models in practical scenarios, rather than learning many different theories and models using a tutor-led approach. It is important to have lab sessions for security feature configurations and small-group working to enable learners to use case studies to investigate application of them in different scenarios. They could then produce a short presentation assessing the likely future leadership requirements for the different situations, identifying the challenges faced. Examples include case studies from different types of organisation, a local charity, a new business start-up or a public sector organisation and design security models for them to safeguard against a general situation or a specific type of security threat. Learners would apply network zones or firewalls rules on above scenarios. It can also be in shake of a network structure and asking students to re-design it in a secure model.

For learning outcome 4, it is important that tutors highlight the differences types of physical security controls in network and the usage and application of each – tutorial sessions can be used to examine them in real world scenarios similar to previous sections.

Outline learning plan

The outline learning plan has been included in this unit as guidance and can be used in conjunction with the program of suggested assignments.

The outline learning plan demonstrates one way in planning the delivery and assessment of this unit.

Topic and suggested assignments/activities and/assessment
Introduction to unit and program of learning
Tutor-led discussion on definitions of computer network concepts –learner group work and exercises on IP addressing and network vulnerabilities and threats
Tutor input on network secure architectures
Learner group work on adapting designing secure network architectures in different situations contributing into **Assignment 1: Secure Network Design**
Tutor input on network security features followed by learner activities on their configuration in practical labs. Learners to also work in groups to apply security features in case scenarios contributing to **Assignment 1: Secure Network Design** in the follow up of the scenario in previous section
Tutor input on network physical security controls
Learner activity on a case study on recruiting physical controls in the previous section case study contributing to **Assignment 1: Secure Network Design**
Review of unit and program of assignments

Assessment

Learners can use their own workplaces as a base for the first assessment for this unit which weights 20% of their total mark. However, they should initially use their lab sessions to work in groups on the given case scenario for this assessment.

For AC2.1 to AC4.2 learners need case study provided to them to implement their learning and knowledge in network security architecture, features and controls in designing a secure network for the orenisation's network in the scenario. However, the assignment should be split into 3 parts, each to be used in practical labs of each relevant weekly sessions. But students do not have to hand each part's answer at the end of each weekly session and must submit the whole assignment report at the end of module program.

For AC1.1 to AC4.2, learners will also have a final exam of questions similar to CompTIA exam at the end of module program, weighting 80% of tehir final mark.

Programme of suggested assignments

The table below shows a programme of suggested assignments that cover the criteria in the assessment grid. This is for guidance only and it is recommended that centres either write their own assignments or adapt Pearson assignments to meet local needs and resources.

Assessment criteria covered	Assignment title	Scenario	Assessment method
AC 1.1 to AC 4.2	Final exam	N/A	Optional questions
AC 2.1 to AC4.2	Secure Network Design	A case study of a typical organisation's network, which needs security measures to safeguard it against a general or specific attack scenario	Case study Assignment

Essential resources

There are no essential resources required for this unit.

Indicative resource materials

Textbooks

CompTIA Security+ 2008 In Depth
Mark Ciampa
ASIN: 1598638130
Publisher: Delmar; 1st edition (20 Dec. 2008)
Language: English
Paperback: 464 pages
ISBN-10: 9781598638134
ISBN-13: 978-1598638134

Websites

https://www.comptia.org/ https://www.comptia.org/training/resources/practice-tests	CompTIA resources and free mock tests
https://www.ncsc.gov.uk/	Latest cyber security guidelines and reports from NCSC
https://www.helpnetsecurity.com/	Technical reports on latest network security attacks and measures
https://www.infosecinstitute.com/resource-center/	Education and training site for cyber secuerity

Unit 3:

Unit code: Incidence Response & digital Forensic

Level 7:

Credit value:

Guided learning hours: 30

Unit aim

In this module, students will learn about the tools and techniques of incident response and digital forensic and will study the formal procedure of SOC centers for incident tracking, investigation and reporting according to investigation laws, policies and standards.

Unit introduction

Incident response is the process of detecting occurred attacks and incidents against computer systems, stopping effects of such incidents which are followed by digital forensic to extract evidences to present them to legal authorities and courts. Regarding the rise of computer systems and consequence hacking activities, there are advancement in alarming and detecting different types of events and in particular incidents using network and software tools. In this module trainees learn how to act as a SOC analyst to monitor systems, track alerts, distinguish false positive and true positive alarms from each other, analyse different types of advanced attacks, and report them to relevant departments for follow up procedures. At the end trainees also exercise some main functions of digital forensic investigation such to collect data from systems and analyse them as admittable evidences for legal procedures. In this module, we aim to prepare trainees for cyber security certification schemes such as COMPTIA Security +, CySA and also SOC analysis.

Learning outcomes and assessment criteria

In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

On completion of this unit a learner should:

Learning outcomes	Assessment criteria
1 examine various phases in incident response and the process of chain of custody according to COMPTIA CySA+ Domain 3: Cyber Incident Response and NCSC Guidance for Cyber Security Response and Recovery	1.1 Gain skills of different stages of the incident response process for various types of incidents (NIST SP 800-61) 1.2 Establish a SOC laboratory (toolkits) and team for investigation (CSIRT) 1.3 Maintain a proper chain of custody 1.4 Develop Incident Response program and Policy along with logging policy 1.5 Understand and gain skills on Threat Intelligence and Threat Hunting in incident Response 1.6 Understand and gain skill on The cyber Killchain and Mitre Attack framework in incident Response
2 recognize the significance of incident detection, and recovery (according to COMPTIA CySA + Domain 3 and COMPTIA Security ++ Domain10	2.1 Examine roles of SOC officers (alert, logs & incident monitoring & analysing, incident ticketing & management, reporting, etc.) 2.2 Examine methods for incident detecting (systems monitoring, recognition between event and incident, recognise true positive, false positive, false negative, false positive alarms, etc.) 2.3 Analyse network events and detect network attacks such as DNS, DDOS, Host Discovery, Port Scanning, ARP poisoning using tracking tools and logs such as firewalls, IDS, SIEM, EDR 2.4 Analyse incidents such as SQL injection, malware, Brute Force, Phishing, Zero day, web application, etc.

	2.5 Be able to classify Incidents and priorities them for response 2.6 Examine methods to stop the spread of the incident or losing evidences intentionally or by accident 2.7 Examine the methods and strategies for data recovery 2.8 Be able to comply with GDPR incident Response rules
3 recognize and examine the methods of digital forensics according to CompTIA CySA + Domain 3	3.1 Examine process of digital forensic and its aims and methods 3.2 perform live and statistic data acquisition using tools such as FTK/Encase 3.3 recognise and examine methods to analyse windows and Linux host and server registry and log 3.4 Recognise ACPO and apply its rules in digital forensic for various applications (mobile, network, desktop, IOT and cloud investigation)
4 Understand and practice digital forensic reporting tasks and post forensic tasks	4.1 perform Post-incident Activities such as lesson learned, log recording etc.

Unit content

1- examine various phases in incidentresponse and the process of chain of custody according to COMPTIA CySA+ Domain 3: Cyber Incident Response and NCSC Guidance for Cyber Security Response and Recovery

phases involved in incident response process as preparation, detection, analysis, recovery and post-incident activities, chain of custody, roles and responsibilities of first incident response, elements of incident response policy, building cyber defense planning and strategy, building SOC lab, Preparation toolkit, response kits and train personnel.

2- recognize the significance of incident detection, and recovery (according to COMPTIA CySA + Domain 3 and COMPTIA Security ++ Domain10

roles and responsibilities of SOC analyst including 24/7 monitoring, continues alert watching, creating/monitoring dashboards, raising incident tickets, incident follow up, Service level agreement, reporting, working with different stakeholders, knowledge transfer, Kali Linux Box, incident and alert analysis using network tools and indicators such as IDS/IPS, SIEM, EDR Anti-virus, or other software alerts, Event indicators, logs collected from network and security devices (operating systems, services, applications, network devices, and network flow), publicly available info, people, staff report, log management, monitor network traffic, real time analysis of incidents (including Brute Force, Malware, phishing emails, SQL injection, DDOS, Suspicious IP in network traffic, etc.), documentation, stop spreading and recovery strategies and methods, GDPR Incident Response Process.

3- recognize and examine the methods of digital forensics

forensic toolkits and workstation, live and static data acquisition methods and the metrics to select each, data acquisition steps, data acquisition tools, data collection priorities, filesystem analysis and file carving, imaging and data duplication, set up FTK/Encase and data analysis, Hashing and validation, Password cracking/recovery, Windows Registry analysis, Windows log files analysis, Linux log analysis, Memory analysis.

5 **Understand and practice digital forensic reporting tasks and post forensic tasks**

Types of report, reporting different stages of forensic investigation, characteristics of a good report, event reconstruction, lesson learned, evidence retention, Communication and info sharing.

Essential Guidance for tutors:

Delivery:

The module is delivered weekly with 2 hours sessions including 1 hour lecturing and 1hour practical lab/tutors. These include weekly lectures and labs to encourage debate and discussion. Lectures will be used to introduce the main topics. In labs, students will work on practices and questions to develop and reinforce the notes covered in the lectures. Lab practices are designed to practice technical exercises of real work scenarios and exams to prepare trainees for COMPTIA certification exams.

The syllabus is divided into a number of related topics. Lecture notes in format of PowerPoint slides and pdf with reference to additional materials are provided for each topic. Trainees are expected to consult independently with additional references to get themselves more familiar with the topics. To gain full advantage of this module trainees are expected to hone their skills and understand by working through progressive exercises. A lab/tutor exercise is produced for each topic. Also, the practical demonstrations of the technologies will be discussed during the lab sessions.

Learning and teaching activity hours for the module:

Lecture	: 12 hours
Lab	: 12 hours
Assessment	: 6 hours (100% assignment (case study,))
Total	: 30 hours

For learning outcome 1: trainees should learn about incident response processes including preparation, attack detection, recovery, data acquisition, analysis and reporting and managing the case from start to end of the process. They should be able to apply these stages to activities in simulated real attacks scenarios in the labs. They should get familiar with procedure of chain of custody and practice it with the case scenario. The requirements (criteria, tools and techniques) of building a forensic lab must be discussed.

For learning outcome 2: it is important that learners understand the role of SOC analyst and how they can detect different types of cyber-attacks and incidents. Tutors must start by introducing the SOC role and activities and continue with the methods SOC use to monitor events, detect incidents from events, reporting and stopping spread of attacks and to recover data. Trainees should understand different methods of incident detection from system alarms, system logs, network traffic monitoring and how to configure systems for alarming, to non-technical alarming methods such as information shared by colleagues, other organisations, news or learned from previous incidents. Students should also understand system recovery methods such as back up, network configuration and reset, etc. This must be exercised in labs by simulating attacks such as DDOS, email phishing, malware, etc. Classification of cyber-attacks and how they should be prioratised to be addressed in first incident response procedure should be discussed. Different

phases of attacks will be learned and simulated using Kali Linux Box. Some legal aspects of incident response will be examined by using GDPR Incident Response framework. This module outcome may take more than 1 and up to 3 lectures and labs to cover all the contents.

For learning outcome 3: Trainees should be able to understand and exercise the process of digital forensic and its aims, and different methods for digital forensic such as data acquisition and imaging by FTK or Encase tools and file carving, password recovery, hashing disks, data analysis through Windows registry, log files and file system analysis. This module outcome may take more than 1 and up to 2 lectures and labs to cover all the materials and practices.

For learning outcome 4: Tutors must explain in details different types of report writing for incident response and digital forensic investigation including formal and technical reports. Trainees must learn how to report for different stages of these processes. Other post investigation tasks such as lesson learning and how it might be logged for future investigation shall be explained to students too.

Unit 4: Essential Skills for Ethical Hacking

Unit code:

Level 7:

Credit value: **10**

Guided learning hours: 30

Unit aim

This segment furnishes the learner with an intricate comprehension and practical competence to effectively operate in real-world scenarios concerning ethical hacking. They will acquire the necessary technical proficiency to set an ethical hacking lab and serve as a penetration tester proficient, achieving a comprehensive ethical hacking approach.

Unit introduction

This module provides candidates with a foundational comprehension of concepts on ethical hacking, its process and legal aspects. This knowledge equips them to grasp the functioning of different stages of ethical hacking and learn how ethically and legally penetrate to a client's cyber system in order to identify their system's vulnerabilities, and safeguard their systems against future attacks. The curriculum includes practical exercises using commonly employed pen testing and vulnerability scans. The module readies cyber security professionals to adeptly handle vulnerability scanning and system penetration technologies and procedures, ensuring comprehensive readiness for safeguarding cyber spaces. It encompasses a strategy of planning, data collection, scanning, attacking and reporting.

Learning outcomes and assessment criteria

In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

On completion of this unit a learner should:

Learning outcomes	Assessment criteria
1 Understand fundamental concepts of ethical hacking according to CompTIA PenTest +	1.1 Recognise ethical hacking concepts Recognise Pen testing methodologies (Red and Blue team, Black/White/Gray Box, etc.) assessment types, testing strategies and Threat Actors 1.2 Recognise regulatory compliance necessary for ethical hacking and professionalism (GDPR, Ethical Code for Hackers,etc.) 1.3 Apply stages of pen testing, enumeration, attack and exploitation, reporting, communication
2 understand stages of planning and scoping according to ComTIA PenTest + Domain 1	2.1 Apply client engagement strategies in pen testing 2.2 plan elements of pen testing (methodology, strategy and target selection) 2.3 scoping, identifying restrictions, risks and customer requirements 2.4 Apply legal aspects of contracting (NDA, MSA, etc.) 2.5 Build a virtual lab
3 understand reconnaissance stage according to CompTIA PenTest + Domain 2	3.1 Examine Information gathering & identify vulnerability of target systems (opensource search, social engineering, Whois, Ping, etc.) 3.2 Examine passive and active reconnaissance and their techniques and tools

4 Understand scanning stage according to CompTIA PenTest + Domain 2	4.1 Examine scanning process and its types (host, network, code static and dynamic analysis, etc.) 4.2 Examine enumeration and its types 4.3 Examine fingerprinting and its methods 4.4 Examine Cryptographic Inspection and Certificate Inspection 4.5 Examine Eavesdropping methods and its types 4.6 Examine methods for Decompiling and Debugging 4.7 Examine methods and types of vulnerability scanning 4.8 Examine Analysing vulnerability scans 4.9 Examine the techniques to leverage information for exploit
5 understanding methods and types of attacks according to CompTIA PenTest Domain 3	5.1 Recognise common attacks techniques 5.2 Identify weakness in specialized systems 5.3 Identify motivation factors for attacks 5.4 Identify network-based vulnerabilities 5.5 Identify wireless vulnerabilities and attacks 5.6 Identify application-based vulnerabilities and attacks 5.7 Identify local host vulnerabilities and attacks 5.8 Recognise and use techniques to cover hacking tracks
6 understand reporting and communication in pen testing according to Domain 5	6.1 Understand and analyse 5 phases of real time attacking using Kali Linux Box 6.2 Examine report writing skills and methods 6.3 Examine post-report delivery activities 6.4 Examine communication methods and skills

7 practice and get familiar with pen testing tools and code analysis according to Domain 4	7.1 Use Nmap to conduct information gathering 7.2 Compare and contrast various tools credential testing tools, Debuggers, OSINT, social engineering tools, remote access tools, networking tools , programming tools 7.3 Analyse tools output

Unit content

---

1 Understand fundamental concepts of ethical hacking according to CompTIA PenTest +

pen tester, risk, vulnerability, threat, NIST, Adversary Emulation, MITRE ATT&CK Framework, OWASP, Red-team, supply chain, premerger, compliance-based, Black Box, Gray Box, White Box, APT, Hacktivist, Insider Threat, Script Kiddies, planning and scoping, reconnaissance, scanning, port scan, network mapper, ping vulnerabilities scan, password cracking, DOS, session hijacking, buffer overflow, compliance to GDPR, Ethical Code for Hackers, etc.

2 understand stages of planning and scoping according to ComTIA PenTest + Domain 1

rules of engagement, timelines, locations, transparency, written authorisation, MSA, NDA, contract, written permission, SOW, MSA, SLA, NDA, Confidentiality,

3 understand reconnaissance stage according to CompTIA PenTest + Domain 2

conducting information gathering methods such as open-source search, social engineering, ping, Whois, etc.

4 Understand scanning stage according to CompTIA PenTest + Domain 2

scanning Hosts, systems, networks, computers, enumerating hosts, networks, domains, Banner Grabbing, Packet Crafting, Packet Inspection, automated tools SSLyze, eavesdropping, sniffing network traffic, packet capture, reverse engineering, code static analysis and dynamic analysis, Credentialed and non-credentialed scans, discovery scan, full scan, static and dynamic, containers, asset categorization, adjudication, prioritise, common Themes, map vulnerabilities to exploit, prioritise efforts for Pentest

5 understanding methods and types of attacks according to CompTIA PenTest Domain

cross-compiling code, exploit modification and chaining, proof-of-concept development, social engineering, physical security attacks, authority, urgency, social proof, mobile devices, IOT, Embedded devices, vulnerabilities in NETBIOS Name Service, LLMNR, SMB, SNMP, FTP, Replay, Man-in-the-Middle, ARP spoofing, DOS, Evil Twin, de-authentication attacks, credential harvesting, Bluejacking, injection, authentication, XSS, file inclusion, unsecure code practices, Windows, Linux, Android OS vulnerabilities, erase, modify, or disable evidences, clear log files, hiding files and folders

6 understand reporting and communication in pen testing according to Domain 5

data normalization, writing report of findings, handling disposals, mitigation strategies, post-engagement cleanup, attestation, client acceptance, follow up actions, lesson learned, communication path, communication reasons, triggers,

7 practice and get familiar with pen testing tools and code analysis according to Domain 4

port scan, SYN scan, TCP connect scan, Nmap Demo, scanning tools: Nmap, Nessus, SQLmap, OpenVAS, Hashcat, Hydra, Patator, W3AF, Debuggers (Ollydbg, IDA, GDB, etc.), OSINT (Whois, Foca, Shodan, SET, BeEFSSH, Netcat, Wireshark, Hping, Bash, Powershell, password cracking, pass the hash, injection

Essential guidance for tutors

Delivery

Tutors will need to use a wide range of teaching and learning methods so that learners meet the learning outcomes in this unit. Methods include lectures, seminars, lab sessions, project work and individual and group assessments.

Some formal delivery will be necessary, but work can be increasingly learner-centred to develop independent learning. Learners need to adopt an investigative, analytical and participative approach to achieve the learning outcomes and reflect on their own experiences and roles to enhance the learning experience.

Sufficient time needs to be built into the delivery schedule to allow learners to undertake the practical activities needed to help them meet the learning outcomes and beresponsible for their own learning. Client engagement, identifying their requirements for project, scoping and contracting, specially the legal and ethical aspects of contracting are very important to be discussed further too.

For learning outcome 1, it is important that learners understand the fundamental concepts necessary for pen testing such as risk, attack and vulnerability. In order to understand requirements and skills of an ethical hacker in organisations, learners need to explore the fundamentals of the concept of around the topic. Tutors could provide input on the key elements of ethical hacking methodologies, strategies and framework. Learners need to appreciate the importance of using a strategic approach to examine the activities involved in ethical hacking practices. The legal and ethical aspects of ethical hacking is an issue which could involve much group discussion. Different stages of pen testing must be explained in a way that makes essential foundations for next sessions.

For learning outcome 2, It should be first a tutor lead teaching of methods and strategies for planning stage. All famous methods and strategies should be discussed in details. Students to practice the learning in Q&A tutorial session after

the lecture, also to have some case scenarios to practice best methods and strategies.

When covering learning outcome 3, it is important to focus on current methods and tools used to collect enough initial information for pen testing. For most of the learning outcome, it is preferable for time to be spent on lab sessions to practice and get familiar with information gathering tools and techniques rather than using a tutor-led approach. When learning about thecompetences for strategic leadership and styles of successful leaders, learners canuse their own experiences and relate them to current theories and models.

For learning outcomes 4 and 5, it is important that tutors highlight the differences types of system vulnerabilities and attacks, as well as the tools to be used to scan systems and discover vulnerabilities. Small-group working can enable learners to practice different vulnerability investigation tools in practical lab sessions. They could then produce a short presentation assessing the vulnerabilities found in specific short scenarios and challenges they faced. Examples include short case studies from CompTIA textbooks or using local organisations or internet sources. Learners could present their findings to the rest of the class and discuss the typical challenges that they faced during their investigation.

For learning outcome 6, it should be again a tutor -based teaching session on different methods and best approaches for ethical hacking reporting. Tutorial-based Q&A can be used later to examine students' learning.

For learning outcome 7, it should be more lab session focused. Students to practice Nmap in the lab session, guided and leaded by their tutors. Other tools mostly to be overviewed by their objectives and goals and shown in the lab sessions. Students should recognise when to use each of these tools, and at least practice one or two of them in lab sessions.

Outline learning plan

The outline learning plan has been included in this unit as guidance and can be used in conjunction with the programme of suggested assignments.

The outline learning plan demonstrates one way in planning the delivery and assessment of this unit.

Topic and suggested assignments/activities and/assessment
Introduction to unit and programme of learning
Tutor-led discussion on definitions of ethical hacking, its methods and strategies and different stages –learner individual and group work and exercises
Tutor input on planning stage, client engagement and contracting, also legal point of view. Learner individual and group work and exercises
Tutor input on methods and tools for information gathering and vulnerabilities identification a
Learner group work on a case study to gather information for an ethical hacking case contributing to **Assignment 1: Ethical Hacking**
Tutor input on methods and tools for system scanning

Learner activity on the case study to scan the relevant systems contributing to **Assignment 1: Ethical Hacking**
Tutor input on different types of system vulnerabilities and attacks
Learner activity – using the knowledge gained to exploit into the systems in the case study, contributing to **Assignment 1: Ethical Hacking** In case of not availability of tools for a real attack, students can only report on the strategies and tools to use to attack the system
Review of unit and program of assignments

Assessment

Learners can use lab sessions and their own workplaces as a base for much of the assessment for this unit. However, if they are not a part of a suitable organisation, other strategiesmay have to be used, for example a work placement, a detailed investigation of anorganisation or the use of suitable case study material.

For AC1.1, learners need to use a case study selected by themselves according to their organisation context or open-source cases (must be approved by the tutor) or the case study chose by the tutor. Learners need to use the example to explain the actions needs for an ethical hacking procedure on the case study systems. They must work in groups based on the weekly lab practices to examine their weekly session learnings on the case study. learners need to apply ethical hacking methods and strategies to specific situations and create a realistic ethical hacking strategy. They need to review a range of tools, with the emphasis on scanning the case's vulnerabilities. Learners donot have to perform a real attack on the systems, but to simulate their attack strategy in a written report.

For AC1.2, learners to sit on exam of optional answer questions. Questions to be chosen from CompTIA PenTest + exams.

Programme of suggested assignments

The table below shows a programme of suggested assignments that cover the criteria in the assessment grid. This is for guidance only and it is recommended that centres either write their own assignments or adapt Pearson assignments to meet local needs and resources.

Assessment criteria covered	Assignment title	Scenario	Assessment method
AC 1.1	Ethical hacking methods and strategies, scanning tools, attack and report	Learners to perfom ethical hacking on a case including all stages of EH.	Report
AC 1.2	Ethical hacking methods and strategies, scanning tools, attack and report		Exam

Essential resources

There are no essential resources required for this unit.

Indicative resource materials

Textbooks

CompTIA PenTest+ Study Guide: Exam PT0-002
by David Seidl (Author), Mike Chapple (Author)
ISBN-10: 1119823811
ISBN-13: 978-1119823810

Websites

https://www.comptia.org/faq/pentest/what-is-on-the-comptia-pentest-exam	CompTIA guidance on exam for pen test +
https://www.udemy.com	Mock tests
https://www.bulletproof.co.uk/blog	UK blog for professional pen testers
https://www.ncsc.gov.uk/guidance/penetration-testing	NCSC professional advices for pen testers