THE OPEN UNIVERSITY OF KENYA

DESIGN PLAN

The Design Plan presented below reflects the CUE suggested Plan but goes beyond that to specify how each outcome will be handled. All modules are based on this Design Plan.
Note: The principle of constructive alignment informs this Design Plan.

Programme title	Bachelor of Science in Cybersecurity and Digital Forensics
Course title	Operating Systems
Learning Module number	01
Learning module title	Security in Operating Systems
Module Developer	Elisha Abade
Module duration in hours	
Instructional Hour Equivalent (Divide duration by 2)	
Reviewed by	
Vision	The innovative university for inclusive prosperity
Audience description	Learners of Cyber Security in first semester of second year
Instructions to learners ⓘ	In this course we shall be learning about the concepts of security in Operating System. We'll begin by watching videos on Operating systems. You are encouraged to ensure that you have access to a reliable Internet and that your devices (computer, tablet or phone) have properly working multimedia systems. This module also presents a number of interactive and non-interactive activities. You will be required to complete all the activities.
Learning module description	This module aims to facilitate learners to have an understanding of the fundamental requirements of security including the CIA triad and non-repudiation, Operating system security artifacts of logging and auditing as well as syslog utility in Operating Systems .
Module objectives:	This module aims at facilitating learners to acquire knowledge about: 1. The basic concepts of security in Operating Systems 2. Security threats, vulnerabilities and attack vectors in Operating Systems 3. Operating Security models

	4. Advanced Operating System security concepts of auditing and syslog
Module learning outcomes:	By the end of the module, you should be able to: 1. Explain the concept of security in Operating Systems 2. Describe security threats, vulnerabilities and attack vectors in Operating Systems 3. Compare and contrast Operating Security models 4. Analyze syslog data for security details
Planned Learning Resources	
ACTIVITY 1: INTRODUCTION VIDEO 1: Pre-recorded lecture on topic emphasizing LEARNING OUTCOME 1: Factual knowledge. 	**Video 1 : Overview of Operating System Security (5 minutes)** In this session we shall begin by looking at what constitutes security in computer systems including Operating Systems. In computing, security is looked from multiple facets in what constitutes, the fundamental tents of security requirements. These include: • Confidentiality: This is a requirement in which data (or even its existence) should protected from disclosure to unauthorized entities. • Integrity: A requirement that data should not be modified by unauthorized entities. • Availability: A requirement that data should be available to authorized entities • Authenticity: A requirement that all entities should be identified, so that all operations are attributable. • Non-repudiation: A requirement that no entity should be able to deny doing any action that it did do. Attacks Many attacks on computer systems are not so easy to detect. For example, traffic analysis may reveal critical information and data aggregation may extract sensitive information from several apparently innocent sources but can be hard to notice. Since today's computer systems are used in processing sensitive and safety critical data, it is important that mechanisms are put in place to protect them from attacks and other forms of misuse. The protection usually takes place in many different forms and also applied at different points in the computing ecosystem. In this course we shall be focusing on the security within the confines of Operating Systems. Protection Different degrees and granularities of protection can be provided, with increasing difficulty, by operating systems including: • No protection: This is a very rare situation and can only be advised in instance when the system is going to be used in isolation with no interaction with other devices whatsoever. This is rarely the case in modern day computing.

	• Isolation of tasks: This approach is applicable where different tasks have separate address spaces, filespaces, etc., with no communication. Also a near impossible situation in modern computer systems. • Public/private: allow object owners to make them public (accessible to other processes) or private. • Sharing via access lists: In this approach, the Operating System enforces user-specified access restrictions given in Access Control Lists (ACLs) • Via capabilities: or with dynamically created access capabilities • Limit uses: constrain detailed use: printing, viewing, copying etc. Some of the techniques used in protection of data in computer systems include: • User identification • Passwords • Biometrics • OS facilities • Encryption • Authenticity and non-repudiation • Cryptographic signing **Video 2: Security Vulnerabilities and attack vectors (8 minutes)** In this second session of this module, we shall be looking at the weaknesses or vulnerabilities that make it possible to attack computer systems. These weaknesses are referred to as vulnerabilities. These vulnerabilities are exploited by active agents that make it possible to perpetrate the attacks. These agents are referred to as attack vectors. Malicious software are some of the most common attack vectors. **Malicious Software** Most of the security problems faced by Operating Systems come from malicious software. There are two main entry routes for malicious software in Operating Systems, namely: i. Exploiting bugs in system software, e.g. buffer overflow attacks ii. Exploiting users, e.g. most email viruses. Malicious software include worms, viruses, logic bombs, trojan horses, trap doors. Prevention of these malicious software can be achieved through: i. Rigorous access control on need-to-know basis ii. Reviews of potentially exploitable code

iii. User education

On the other hand, they can be detected through:

i. Signature scanning
ii. Sandboxed execution
iii. Performance and system behaviour analysis

Cracking and counter-cracking

The ultimate desideratum of a cracker is complete privileged access to a system. Attacks may involve several levels of indirection, including:

i. Break directly into a privileged network server, suborn an operator, etc.
ii. Break a user account, then exploit weakness in OS to get root
iii. Break into a trusted but more vulnerable machine, use as relay

Cracking user accounts

Nowadays, by far the easiest way is by tricking the user into opening an executable attachment or running a download. With foolishly designed mail systems, you may not even need to trick the user. Counter-measures, in increasing order of severity:

i. Educate users
ii. Scan mail for known viruses
iii. Modify local mail programs etc. to stop them executing attachments
iv. Prohibit (by modifying OS if necessary) execution of any program
v. Not digitally signed or otherwise known to be trusted

Video 3: Integrity Protection Strategies (8 minutes)

Strategies used in protection of Operating System files and data can broadly be categorized in three main classes, namely:

i. Prevention strategies
ii. Detection strategies
iii. Recovery strategies

Prevention Strategies

These can further be classified into three main classes of controls including:

a) Software Controls: These include file permissions, directory permissions and restrictions on root access
b) Low-level operating system controls: These are mainly immutability (only change in single-user mode) and append controls (only add to file, except single-user mode).

c) Hardware controls: These can be implemented in form of read-only file systems (CD ROM, WORM) and write-protect options.

Detection Strategies

There are a number of strategies that are deployed to detect malicious activities and attacks in computer systems. These include:

a) Comparison copies. This is usually done to check if there are unlawful alterations to files and data. It can be applied on read-only media, standard media, remote storage. They may require large space, and can be slow and expensive.
b) Metadata: This involves checking data about data such as stored list of files, path to files and modification times. The downside of this is that these approaches are easy to fool.
c) Digital Signature. This is a cryptographic approach to file and data security. It usually involves encryption with private key of modifier. It is usually fast and hard to fool but requires extra work.

Recovery Strategies

- Restore from backup - Rollback (Data Loss)
- If data problem, may be able to replay changes - Selective Rollback (some data loss)
- If redundant file system, vote file versions - Masking
- If specific changes found - correct - Roll forward
- In general -- the more detection and prevention, the easier the recovery

Video 4: Advanced Operating System Security concepts (8 minutes)

Auditing

- Installing security protection is only a beginning
- Need to monitor systems
- Monitoring methods: Audits and Logs
  - Audit - active scanning of current state of system
  - Log - record of actions taken in operation of system
- Audits often use logs, and do more

Log File Vulnerabilities

- Alteration
  - Append mode
  - Non-rewritable media (print)
- Deletion
  - Non-rewritable media
  - Move to restricted log host
  - PC linked by serial line
- Flooding
  - Ensure large storage
  - Reduce before logging (look for repeating patterns)

Syslog

- General purpose logging utility

	• Any program can generate syslog messages – Socket connect to syslogd process TCP port • Messages to files, devices or computers – Dependent on severity and service • Messages marked with authentication level – kern, user, mail, lpr, auth, demon, news, uucp, local0...local7, mark • Messages marked with priority – emerg, alert, crit, err, warning, notice, info, debug, none
ACTIVITY 2: READING READING MATERIAL 1 	You are required to undertake further reading on Operating System security from the following resources: a. Security Management Andrew S Tanenbaum. (2016). Modern Operating Systems Paperback. Pearson. pp 595 - 624 https://www.amazon.com/Modern-Operating-Systems-Andrew-Tanenbaum/dp/9332575770#detailBullets_feature_div
ACTIVITY 3: Comprehension questions: 	Use as much details as possible to answer the following questions: 1) Confidentiality, integrity, and availability are three components of security. Describe an application that integrity and availability but not confidentiality, an application that requires confidentiality and integrity but not (high) availability, and an application that requires confidentiality, integrity, and availability 2) In a full access-control matrix, the rows are for domains and the columns are for objects. What happens if some object is needed in two domains? 3) Give a simple example of a mathematical function that to a first approximation will do as a one-way function. **4)** After getting your degree, you apply for a job as director of a large university computer center that has just put its ancient mainframe system out to pasture and switched over to a

	large LAN server running UNIX. You get the job. Fifteen minutes after you start work, your assistant bursts into your office screaming: ‘‘Some students have discovered the algorithm we use for encrypting passwords and posted it on the Internet.’’ What should you do? 5) Suppose a system uses ACLs to maintain its protection matrix. Write a set of management functions to manage the ACLs when a. a new object is created; b. an object is deleted; c. a new domain is created; d. a domain is deleted; e. new access rights (a combination of r, w, x) are granted to a domain to access an object; f. existing access rights of a domain to access an object are revoked; g. new access rights are granted to all domains to access an object; h. access rights to access an object are revoked from all domains.
LEARNING OUTCOME 2: Conceptual knowledge ACTIVITY 4: Video to be used.	Learner is required to use factual knowledge acquired to answer question “Why”? The Case Method, (E-Case or written case) role play or any other visual aid to be used. An E-Case of a situation for the learner to solve possible problems using facts acquired. Learners will engage in online discussion either live or on forum to answer ‘Why’ questions.
CASE 1:  	Describe case here.
ACTIVITY 5: READING MATERIAL 	You have been provided with the following online sources that will enable you to learn more about auditing and logging in Operating Systems. Go through them keenly and use them to write a blog as you will be directed in the next section. 1) Operating Systems security auditing • https://nxlog.co/whitepapers/operating-systems-security-auditing/ 2) Auditing and logging in Windows • https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-security-audit-policies

	3) Auditing and logging in LINUX • https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-understanding_audit_log_files • https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/chap-system_auditing 4) Auditing and logging in UNIX • https://docs.freebsd.org/en/books/handbook/audit/ • Having gone through the resources above, you are required to write a blog in the LMS focusing on how different Operating Systems perform logging and auditing so as to ensure that their users are accountable for their actions while using the Operating System.
ACTIVITY 6: ONLINE DISCUSSION 	Your course instructor will create a discussion forum in the LMS to facilitate online group discussions. You are required to read the discussion topic and give comments. You are also encouraged to comment on contributions from at least three members of your group. You can use the LMS platform to send questions to your instructor on the discussion topics that he/she has posted on the LMS.
LEARNING OUTCOME 3: PRACTICAL SKILLS VIDEO 3: 	Watch the videos below in order for you to get more insights into the mechanisms provided by the Operating Systems to offer security. 1) Operating System Security features 5:56minutes 2) Protection and System Security (12:57 minutes) 3) Implementation of the Access Matrix (7:39 minutes) 4) Operating System Security models (13:55 minutes)
ACTIVITY 7: Learner practice sessions	In this session, you are required to do a “lightning talk” focusing on “Operating System Security Model”. In the “lightning talk”, use your smartphone or any other video camera to record yourself in not more than “30 seconds” while explaining the “***Bell La Padula Model***”. Note: 1. Upload your video with the captions <*fname_lname_talk10*>. where “*fname*” is your first name and “*lname*” is your last name (or surname). The video must not be more than 30 seconds long.

ASSESSMENT OF PRACTICAL SKILL:	In the above activity, you uploaded your video, <***fname_lname_talk10***>. It will be assessed by the instructor by looking at among others: a) Accuracy of the assertions you have made (5 Marks) b) Degree of completeness of your response to the task (3 Marks) c) Adherence to the requirements with regards to topic and length of the video. (2 Marks)
LEARNING OUTCOME 4: KEY/TRANSFERABLE SKILLS	In this section, you are provided with links to external resources where you can learn of how security implantation mechanism in various Operating Systems. Read them carefully to help you in writing your blog as required in the activity that follows. 1) Windows System Security a) https://learn.microsoft.com/en-us/windows/security/operating-system b) https://t4tutorials.com/windows-operating-systems-security/ 2) UNIX System security a) https://www.cs.ait.ac.th/~on/O/oreilly/tcpip/puis/ch01_04.htm b) https://www.ibm.com/docs/en/zos/2.2.0?topic=planning-establishing-unix-security c) https://commons.lbl.gov/display/cpp/Securing+Unix+Systems 3) Android Security a) https://source.android.com/docs/security/features#:~:text=Android%20uses%20the%20concept%20of,device%20and%20perform%20other%20tasks. b) https://resources.infosecinstitute.com/topic/android-security-c/ 4) iOS Security a) https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf
ACTIVITY 8	In this module, you have learnt about several concepts in Operating Systems Security. You are required to write a two page essay focusing on access control in UNIX, Windows, IOS and Android. Your instructor will create an activity in the LMS that will allow you to submit this essay for assessment. The essay will be marked out of 15 Marks. Some of the guidelines to success in this activity include:

	a) Originality (avoid copying from the Internet and other sources) (5 Marks) b) Level of accuracy of the essay content (5 Marks) c) Completeness of content (3 Marks) d) Sticking to length (number of pages) requirements (1 Mark) e) Keeping to the theme (1 Mark)
QUIZZ: 	1. _____ refers to identifying each user of the system and associating the executing programs with those users. A. One Time passwords B. Authentication C. Program Threats D. Security 2. In how many ways, Operating Systems generally identifies/authenticates users using ? A. 2 B. 3 C. 4 D. 5 3. _____ is a situation when a program misbehaves only when certain conditions met otherwise it works as a genuine program. A. Trojan Horse B. Trap Door C. Logic bomb D. Virus 4. Which of the following program threat, "Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources." A. Trojan Horse B. Trap Door C. Logic bomb D. Virus 5. How many Computer Security Classifications are there? A. 2 B. 3 C. 4 D. 5 6. Which of the following type is at Lowest level?

A. Type A
B. Type B
C. Type C
D. Type D

7. Which of the following type provides protection and user accountability using audit capabilities?

A. Type A
B. Type B
C. Type C
D. Type D

8. Which of the following is not a stream cipher?

A. TBONE
B. RC5
C. RC4
D. Two fish

9. How do viruses avoid basic pattern match of antivirus?

A. They are encrypted
B. They modify themselves
C. They act with special permissions
D. None of the above

10. What are the major components of the intrusion detection system?

A. Analysis Engine
B. Event provider
C. Alert Database
D. All of the above

Answers

1. B. Authentication
2. B. 3
3. C. Logic bomb
4. A. Trojan Horse
5. C. 4
6. D. Type D
7. C. Type C
8. A. TBONE
9. B. They modify themselves
10. D. All of the above

TAKE HOME MESSAGE	Your course instructor will create a feedback section in the LMS to facilitate provision of your take home message. You are required to give a brief description of what you have learnt in this module in not more than half a page (typed) in the feedback section provided.
Reference list	1. Andrew S Tanenbaum. (2016). *Modern Operating Systems Paperback, 5th Edition*. Pearson. 2. Silberschatz A., Galvin P. B. and Gagne G. (2008). *Operating System Concepts*, 8th Edition. Wiley. ISBN: 9780470128725 3. Meyers, M. (2016). *CompTIA A+ Certification Guide*. McGraw-Hill Education