EC-Council | Academia

N|DE™
Network Defense Essentials



Network Defense Essentials (NDE)

Lesson Plan

EC-Council | Academia

EC-Council Academia

Student Course Syllabus

Network Defense Essentials

Instructor Contact Information

Instructor Name:		**Office Location:**	
Email:		**Phone Contact:**	
Office Hours:			

I. Purpose of Class:

This class is designed to provide students to establish and govern minimum starndards for credentialing entry-level information security specialists in network security measures, inform the public that credentialed individuals meet or exceed the minimum standards, and reinforce network security as a unique and self-regulating profession.

II. Course Objectives:

Students who successfully complete this class will be able to:

1. Discuss fundamental concepts of network security, including Information Assurance (IA) principles, network defense challenges, defense approaches, security controls, and review essential network security protocols.
2. Discuss access control principles, terminologies, and models, and describe Identity and Access Management (IAM) concepts.
3. Examine various administrative network defense controls, including frameworks, laws, acts, and security policies.
4. Examine various physical network defense controls, including physical security controls, workplace security, and environmental controls.
5. Examine various technical network defense controls, including network segmentation, firewall, IDS/IPS, honeypot, proxy server, VPN, SIEM, UBA, and anti-malware.
6. Comprehend fundamental virtualization concepts, Virtualization Security Concerns, cloud computing, and suggest security best practices.
7. Explain wireless network fundamentals, different types of wireless encryption, and suggest security measures.

8. Discuss various mobile device connection methods, Mobile Device Management concepts, common mobile usage policies, examine different security risks, and review general security guidelines and best practices for mobile platforms.
9. Discuss working of IoT devices, application areas, communication models, IoT security principles, IoT framework security considerations, IoT device management, and identify IoT security best practices.
10. Discuss cryptography techniques, various cryptographic algorithms, and Public Key Infrastructure (PKI), and use various cryptography tools to protect information.
11. Discuss data security concepts, the importance of data encryption, data loss prevention, and compare different data backup concepts and technologies.
12. Discuss the need and advantages of network traffic monitoring, determine baseline traffic signatures for normal and suspicious network traffic, and perform network monitoring for suspicious traffic.

III. NDE Grading Policy:

The academic credit used by NDE is based off twelve-week courses that constitute 3 credits per course. All courses constitute approximately 100 hours of work per course (reading, Online Discussion Forum postings, assignments, papers and supplementary requirements).

Point-grade breakdown:

The NDE Course grading structure will follow the Academic Grading Symbols and Quality Points Earned.

Percentage	Points	Grade	Comments	Quality Points Earned
90 - 100%	360-400	A	Superior Attainment of Course Outcomes	4.0
80 - 89%	320-359	B	Good Attainment of Course Outcomes	3.0
70 - 79%	280-319	C	Acceptable Attainment of Course Outcomes	2.0
60 - 69%	240-279	D	Poor Attainment of Course Outcomes	1.0
0 - 59%	000-239	F	Non-Attainment of Course Outcomes	0.0

IV. NDE Grading Structure

S.No.	Assessment	Details	Points
1	**Course Discussion Threads**	There are 10 discussion threads (each is worth 4 pts.)	**40**
2	**Assignments from Readings**	There are 15 Readings (each question is worth 6 pts.)	**90**
3	**Lab Assignments**	There are 22 lab assignments (each assignment is worth 4 pts.)	**88**
4	**Course Quizzes**	There are 32 quiz questions (each question is worth 1 pt.)	**32**
5	**Research Project**	There is 1 Research Project (worth 50 pts.)	**50**
6	**Final Exam**	There is 1 Final Exam (worth 100 pts.)	**100**
		Total Points Possible:	**400**

NOTE: Each week you will have assessments that you must complete for class credit.

V. NDE PROGRAM OBJECTIVES:

1. Application of technical strategies, tools and techniques to secure data and information for a customer or client
2. Adherence to a high standard of ethical behavior
3. Use of research in both established venues and innovative applications to expand the body of knowledge in information assurance
4. Application of principles of critical thinking to creatively and systematically solve the problems and meet the challenges of the ever-changing environments of cyber security
5. Mastery of the skills necessary to move into leadership roles in companies, agencies, divisions, or departments

VI. LEARNING STANDARDS:

Four Standards of Performance:

Always use these standards of performance anytime you write a research paper, respond to a case study or answer discussion threads.

These 4 Standards of Performance, when used fully, will produce an excellent paper.

1. **Depth of Reflection**: Be sure to demonstrate a conscious and thorough understanding of the writing prompt and subject matter. Analyze the evidence from several perspectives, draw conclusions based on evidence, research and/or experience.
2. **Sequence your information:** Your work has a clear and appropriate beginning, development and conclusion. Most information is organized in a clear and logical way. There is a beginning and a conclusion. Paragraphing and transitions are adequate.

3. **Conclusions:** Draw conclusions based on evidence, research or experience. Use the context of your readings and the assumptions the author makes.
4. **Language Use**: Use sophisticated language that is precise and interesting. Sentence structure must be correct to the grammar of the language.

VII. ADDITIONAL NOTES AND EXPECTATIONS:

Attendance

Documenting Attendance in Distance Education Courses

Changes to federal regulations in recent years have highlighted the importance of accurate reporting on student attendance and participation in all courses, including distance education courses (online and hybrid/blended courses).

In order to comply, We provide the following procedural guidance to faculty when filling out your non-participation rosters. A student attends an online course (or the online portion of a hybrid/blended course) by participating in class or otherwise engaging in an academically related activity. Examples of such activity include but are not limited to:

1. Contributing to an online discussion or text chat session
2. Submitting an assignment or working draft; working through exercises
3. Taking a quiz or exams
4. Viewing and/or completing a tutorial
5. Initiating contact with a faculty member to ask a course-related question.

Such academically related activities are readily tracked and documented through the University learning management system, email system, and in some cases publisher websites. Documenting that a student has logged into an online class or website is not sufficient, by itself, to demonstrate academic attendance by the student. For example, if a student simply logs into an online course on September 15 and logs out, without any further activity, the student did not attend the online class on that day.

Late Assignments Late assignments are not in the student's best interest. In that regard, if you have a problem that will not allow you to complete the assignments in a timely manner, please send the instructor an immediate request and explanation. It is the instructor's option, decision, and discretion to accept or reject the student's request. Continued requests will not be accepted and the student may be dropped from the course at the instructor's request.

Writing Skills If your writing skills are not the best, there are some modules under "Student Orientation" in the LMS that can help you prepare for your writing process or you may want to purchase a basic writing skills book that will help you.

ACADEMIC HONESTY POLICY

Course Policies On Cheating and Plagiarism

As a model of the highest ethical standards and as an institution of higher learning, University expects its students to conduct themselves with an unquestionable level of honesty and integrity. University will not tolerate academic cheating or plagiarism in any form. Learning to think and work independently is not only a part of the educational process; it is the educational process. Cheating or plagiarism in any form is considered a serious violation of university policy, which each student agreed to when accepted into the program. Student academic beheviors that violate the university policy will result in disciplinary action, without exception.

Some examples of cheating and plagiarism include but are not limited to:

Cheating	Use of material, information, or study aids not permitted by the faculty
Plagiarism	Use of another's words or ideas without acknowledging the source of the information
Falsification or Fabrication	Changing or altering data, quotes, citations, grades or academic records
Unauthorized Collaboration	Intentional sharing of information when the faculty does not approve of such collaboration

University will take action in all cases of academic dishonesty. The first instance will result in a failing grade for the assignment. The second instance will result in a failing grade in the class. The third instance will result in dismissal from the university. A record of all instances of academic dishonesty for University, as well as a record of the action taken, will be kept in the individual student file and Dean's file.

1. Steps to be taken in the instance of academic dishonesty are: The faculty/staff will inform the student of the allegation and provide evidence, offering the student the opportunity to respond and/or rectify the issue depending on the nature of the dishonesty and the particular assignment.
2. Once the student has had a chance to respond, the faculty/staff will determine if academic dishonesty has occurred. If the faculty/staff concludes that academic dishonesty has occurred and has proof, they will report the student's name, the class and assignment, the nature of the academic dishonesty and the proof to the Dean. The type of disciplinary action to be taken will be determined by the student's record of instances identified above and will be applied by the faculty and/or the Dean.

Citing Sources

In academic communities, the ethics of research demand that writers be credited for their work and their writing. To not do so is to plagiarize- to intentionally or unintentionally appropriate the ideas, language, or work of another without sufficient acknowledgement that such material is not one's own. Whenever a student quotes, paraphrases, summarizes, or otherwise refers to the

work of another, the student must cite his or her source either by way of parenthetical citation or footnote. Unfortunately, this is the most common form of academic dishonesty, but regardless it will be responded to with failing grades or dismissal.

Original Content

Students are expected to create their discussion topics, assignments and essays using the majority of their own personal thoughts and ideas. All works must contain a minimum of 75% original work. Any work submitted that contains more than 25% unoriginal work regardless of whether the sources are cited properly may be considered a violation of the academic honesty policy, depending on the nature of the assignment, and consent of the assigned instructor.

Timeline

Discovery of violation of the Academic Honesty Policy can occur at any time. Issuance of a grade, or even degree, can be changed if it is discovered that an academic honesty violation occurred. *The bottom line is this; it's just not worth it.*

Student Identity Verification

- University takes measures to verify the identity of the students who are applying to the university, completing courses, and taking proctored exams.
- Students access their courses and reference materials through our secure online learning management system, where they are required to enter their username and password. Students are responsible for the safeguard of their individual credentials.
- University implements student identity verification in several ways to ensure proper ID.
    1. A Valid Government issued ID is required with admissions application.

Login credentials are required for the online LMS portal

VIII. REQUIRED TEXTS THROUGHOUT THIS COURSE:

The following texts will be required for this course:

- Network Defense Essentials (NDE) v1 Academia Series

These are embedded in the General Section of your course. The corresponding chapters for each week are embedded in your weekly readings.

IX. SCHEDULED OUTLINE OF COURSE TOPICS

WEEK ONE:

MODULES COVERED:

- Module 01 – Network Security Fundamentals
- Module 02 – Identification, Authentication, and Authorization

WEEK'S OBJECTIVES USED:

1. Discuss fundamental concepts of network security, including Information Assurance (IA) principles, network defense challenges, defense approaches, security controls, and review essential network security protocols.
2. Discuss access control principles, terminologies, and models, and describe Identity and Access Management (IAM) concepts.

WEEK 1 ASSESSMENTS:

These are found in the course under Week One.

- Discussion Threads: 1 discussion thread (4 pts.)
- Assignments from Readings: 1 Readings (each worth 6 pts.)
- Lab Assignment: 3 lab assignments (each assignment worth 4 pts.)
- Quizzes: 3 quiz questions (each question is worth 1 pt.)

DISCUSSION THREAD:

1. Discuss various network security protocols and access control models

ASSIGNMENTS FROM READINGS:

1. Examine various network defense approaches, network security controls, and types of authentication.

REQUIRED READINGS:

Read the following chapters from the book:

- Network Defense Essentials (NDE) v1 Academia Series – Module 01 Network Security Fundamentals
- Network Defense Essentials (NDE) v1 Academia Series – Module 02 Identification, Authentication, and Authorization

ADDITIONAL RESOURCES:

White Papers:

- Information Assurance/Information Security, https://csrc.nist.gov/csrc/media/events/csspab-june-2002-meeting/documents/lainhart-06-2002.pdf
- About RADIUS, https://www.patton.com/technotes/ras_about_radius.pdf
- Access Control Models: https://www.profsandhu.com/cs6393_s13/L2.pdf

Videos:

- What are the Different Types & Functions of Security Controls?, https://www.youtube.com/watch?v=SupdvOnkVi4
- How PGP Works, https://www.youtube.com/watch?v=dhFZAunAkLU
- Identity and Access Management: Technical Overview, https://www.youtube.com/watch?v=Tcvsefz5DmA

LAB ASSIGNMENTS:

Week 1 Lab Assignment 1: Implementing Access Controls in Windows Machine

Lab Scenario

Access control is a method of limiting the access of users to an organization's resources.

Lab Objectives

This lab demonstrates how to manage objects in Active Directory using different types of accounts and how to apply account policies using GPO (Group Policy Object) in a Windows machine.

Week 1 Lab Assignment 2: Managing Access Controls in Linux Machine

Lab Scenario

Access control assists in maintaining the integrity, confidentiality, and availability of the information and resources.

Lab Objectives

This lab demonstrates how to manage access control policies in a Linux machine. First, we will create local user accounts and groups on the system. Then, we will create directories and files where access control policies will be implemented. Further, we will configure the ownership to these directories and files.

Week 1 Lab Assignment 3: Implementing Role-Based Access Control in Windows Admin Center (WAC)

Lab Scenario

As a network defender, you should be aware of the various tools and tricks available to manage the servers and clients. WAC enables network defenders to perform administrative tasks on any client (except mobile devices). It uses role-based access control (RBAC) to control the activity of the users connected to the server. WAC allows management of system activity such as starting various services, adding and removing resources, and controlling applications.

Lab Objectives

This lab will demonstrate how to install WAC and configure RBAC in WAC to restrict user activities.

QUIZ:

1. Which of the following IA principles is crucial for identifying users/accounts and preventing unauthorized access to resources?
   a. Integrity
   b. Non-repudiation
   c. Authentication
   d. Availability
2. Which of the following protocol employs a client–server model and provides authentication, authorization, and accounting (AAA) for remote-access servers to communicate with a central server?
   a. SMTP
   b. RADIUS
   c. IPsec
   d. HTTPS
3. Which of the following authentication mechanisms provides cryptography-based authentication using a small computer chip that stores the user's personal information for identification?
   a. Single sign-on (SSO) authentication
   b. Password authentication
   c. Smart card authentication
   d. Two-factor authentication

WEEK TWO:

MODULES COVERED:

- Module 03 – Network Security Controls - Administrative Controls

WEEK'S OBJECTIVES USED:

3. Examine various administrative network defense controls, including frameworks, laws, acts, and security policies.

WEEK 2 ASSESSMENTS:

These are found in the course under Week Two.

- Discussion Threads: 1 discussion thread (4 pts.)
- Assignments from Readings: 2 Readings (each worth 6 pts.)
- Lab Assignment: 1 lab assignments (each assignment worth 4 pts.)
- Quizzes: 4 quiz questions (each question is worth 1 pt.)

DISCUSSION THREAD:

1. Discuss various types of information security policies.

ASSIGNMENTS FROM READINGS:

1. Examine various various regulatory frameworks, laws, and acts.
2. Describe key elements and contents of a security policy.

REQUIRED READINGS:

Read the following chapters from the book:

- Network Defense Essentials (NDE) v1 Academia Series – Module 03 Network Security Controls - Administrative Controls

ADDITIONAL RESOURCES:

White papers:

- White Paper on the Compliance function, https://www.asociacioncompliance.com/wp-content/uploads/2017/08/White-Paper-Compliance-ASCOM.pdf

- SOX Compliance White Paper, https://www.e-janco.com/samples/sarbanes%20oxley.pdf
- FEDERAL INFORMATION SECURITY MANAGEMENT ACT, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf

Videos:

- Regulatory Frameworks, https://www.youtube.com/watch?v=pmG8YS8ozp0
- GDPR: What Is It and How Might It Affect You?, https://www.youtube.com/watch?v=j6wwBqfSk-o
- Social Engineering Awareness: It's More Than Smiles, https://www.youtube.com/watch?v=guVBBTEKuK8

LAB ASSIGNMENTS:

Week 2 Lab Assignment 1: Implementing Password Policies using Windows Group Policy

Lab Scenario

Network defenders can use the GPMC to manage group policy in the Active Directory (AD) across the enterprise. It can be used to protect user accounts and implement domain password policy to enable the use of complex and lengthy passwords. This prevents attackers from cracking the user account passwords through brute-force attacks. The network defender needs to configure group policy settings (group policy object, or GPO) in the AD domain to implement common password requirements.

Lab Objectives

This lab demonstrates how to create a GPO from the GPMC; this group policy will implement a common password policy to enable the use of complex and lengthy passwords in the AD domain.

QUIZ:

1. Which of the following acts holds “Electronic Transactions and Code Set Standards”?
   a. **Health Insurance Portability and Accountability Act (HIPAA)**
   b. Digital Millennium Copyright Act (DMCA)
   c. Gramm-Leach-Bliley Act (GLBA)
   d. Federal Information Security Management Act (FISMA)
2. Identify the title of the Digital Millennium Copyright Act that implements the World Intellectual Property Organization (WIPO) treaties.
   a. Title II
   b. **Title I**

c. Title V

d. Title III

3. Which of the following acts is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information?

a. Gramm-Leach-Bliley Act (GLBA)

b. ISO/IEC 27001

c. ISO/IEC 27013

d. Health Insurance Portability and Accountability Act (HIPAA)

4. Identify the Internet access policy that enables only safe/necessary services individually, and nonessential services/procedures that cannot be made safe are not allowed.

a. Paranoid policy

b. Promiscuous policy

c. Prudent policy

d. Permissive policy

WEEK THREE:

MODULES COVERED:

- Module 04 – Network Security Controls - Physical Controls

WEEK'S OBJECTIVES USED:

4. Examine various physical network defense controls, including physical security controls, workplace security, and environmental controls.

WEEK 3 ASSESSMENTS:

These are found in the course under Week Three.

- Discussion Threads: 1 discussion thread (4 pts.)
- Assignments from Readings: 3 Readings (each worth 6 pts.)
- Quizzes: 3 quiz questions (each question is worth 1 pt.)

DISCUSSION THREAD:

1. Discuss various physical security attack vectors.

ASSIGNMENTS FROM READINGS:

1. Explain about different types of physical security controls.
2. Describe about workplace security.
3. Explain about various types of environmental controls.

REQUIRED READINGS:

Read the following chapters from the book:

- Network Defense Essentials (NDE) v1 Academia Series – Module 04 Network Security Controls - Physical Controls

ADDITIONAL RESOURCES:

White papers:

- Physical Security in Mission Critical Facilities, https://facilityexecutive.com/wp-content/uploads/SADE-5TNRPL_R2_EN1.pdf

- Future of Physical Security, https://www.accenture.com/_acnmedia/PDF-100/Accenture-Future-of-Physical-Security-Whitepaper.pdf.
- Physical Security Solutions for US Federal Government Applications, https://cdn2.hubspot.net/hubfs/359395/Physical%20Security%20Solutions%20for%20US%20Federal%20Government%20Applications%20-%20Fin....pdf

Videos:

- Security Awareness Training: Physical Security, https://www.youtube.com/watch?v=QvrpcSdRcL0
- Physical Security, Locks, Mantraps, and Video Surveillance, https://www.youtube.com/watch?v=0nPufMKOQRE
- Electromagnetic Interference Shielding, https://www.youtube.com/watch?v=xX0T2v81jog

QUIZ:

1. Which of the following layers in the OSI model cannot be protected by using traditional firewalls?
   a. Data link layer
   b. Physical layer
   c. Application layer
   d. Presentation layer
2. Which of the following fire suppression systems is used to suppress a fire at the initial stage using a suppressant agent but it cannot be used in case of a fire covering a large area?
   a. Standpipe system
   b. Sprinkler system
   c. Fire extinguisher
   d. Pre-piped water system
3. Which of the following physical security systems allows only one person inside and requests an identity; if the identity is invalid, the person is held inside until a security professional arrives?
   a. X-ray inspection systems
   b. Metal detectors
   c. Walkthrough detectors
   d. Mantrap systems

WEEK FOUR:

MODULES COVERED:

- Module 05 – Network Security Controls - Technical Controls

WEEK'S OBJECTIVES USED:

5. Examine various technical network defense controls, including network segmentation, firewall, IDS/IPS, honeypot, proxy server, VPN, SIEM, UBA, and anti-malware.

WEEK 4 ASSESSMENTS:

These are found in the course under Week Four.

- Discussion Threads: 1 discussion thread (4 pts.)
- Assignments from Readings: 1 Readings (each worth 6 pts.)
- Lab Assignment: 4 lab assignments (each assignment worth 4 pts.)
- Quizzes: 2 quiz questions (each question is worth 1 pt.)

DISCUSSION THREAD:

1. Discuss various types of network segmentation and various types of bastion hosts.

ASSIGNMENTS FROM READINGS:

1. Explain about various types of firewall technologies and IDS classification.

REQUIRED READINGS:

Read the following chapters from the book:

- Network Defense Essentials (NDE) v1 Academia Series – Module 05 Network Security Controls - Technical Controls

ADDITIONAL RESOURCES:

White papers:

- A Practical Guide to Network Segmentation, https://lp.tufin.com/rs/769-ICF-145/images/network-segmentation-white-paper.pdf?hsLang=de
- Network Security: A Simple Guide to Firewalls, http://www.uky.edu/~dsianita/390/firewall1.pdf

- Intrusion Prevention: A White Paper, http://www.cressidatechnology.com/pdfs/products/NitroGuard/whitepapers/NGDB.pdf

Videos:

- 5 Types of Firewalls, https://www.youtube.com/watch?v=uGaERP4Npys
- Types of Honeypot, https://www.youtube.com/watch?v=EDA3Cl_5Nsg
- What is a SIEM (Security Incident Event Management)?, https://www.youtube.com/watch?v=x5369tdNYdo

LAB ASSIGNMENTS:

Week 4 Lab Assignment 1: Implementing Host-Based Firewall Protection with iptables

Lab Scenario

As a network defender, you should know how to configure an iptables host-based firewall to allow or block traffic to or from a Linux system. Iptables allow network defenders to enter firewall rules into the existing tables using the command line.

Lab Objectives

This lab will demonstrate how to configure an iptables host-based firewall in an Ubuntu machine.

Week 4 Lab Assignment 2: Implementing Host-Based IDS Functionality using Wazuh HIDS

Lab Scenario

Intrusion Detection Systems (IDS) help monitor network activity. HIDS enables a network defender to monitor the network traffic for malicious activity or policy violations. Using Wazuh enables network defenders to perform continuous monitoring and respond to advanced threats.

Lab Objectives

This lab will demonstrate the use of Wazuh HIDS and agent to capture network traffic and show how to monitor the captured traffic for malicious activities. In this lab, you will learn:

- Installing and configuring Wazuh HIDS and Wazuh agent
- Monitoring network traffic for malicious activity using Sguil

Week 4 Lab Assignment 3: Detect Malicious Network Traffic using HoneyBOT

Lab Scenario

Network traffic is the amount of data packets passing through a network.

Lab Objectives

This lab demonstrates how to detect malicious network traffic using HoneyBot.

Week 4 Lab Assignment 4: Establishing Virtual Private Network Connection using SoftEther VPN

Lab Scenario

In an organization's network infrastructure, there are firewalls to isolate internal and external network traffic to ensure security. Organizations use firewalls, proxies, and Network Address Translators (NATs) not only to resolve security issues but also to share IP addresses with users in the office. These devices play a crucial role nowadays.

Lab Objectives

This lab will demonstrate how to establish a Virtual Private Network (VPN) connection using SoftEther VPN.

QUIZ:

1. Which of the following components of VPN is used to manage tunnels and encapsulate private data?
   a. Network access server
   b. Remote network
   c. VPN protocol
   d. VPN client
2. Identify the UBA tool that collects user activity details from multiple sources and uses artificial intelligence and machine learning algorithms to perform user behavior analysis to prevent and detect various threats before the fraud is perpetrated.
   a. Wireshark
   b. Dtex systems
   c. Nmap
   d. ClamWin

WEEK FIVE:

MODULES COVERED:

- Module 06 – Virtualization and Cloud Computing

WEEK'S OBJECTIVES USED:

6. Comprehend fundamental virtualization concepts, Virtualization Security Concerns, cloud computing, and suggest security best practices.

WEEK 5 ASSESSMENTS:

These are found in the course under Week Five.

- Discussion Threads: 1 discussion thread (4 pts.)
- Assignments from Readings: 1 Readings (each worth 6 pts.)
- Lab Assignment: 3 lab assignments (each assignment worth 4 pts.)
- Quizzes: 2 quiz questions (each question is worth 1 pt.)

DISCUSSION THREAD:

1. Discuss various types of cloud computing services.

ASSIGNMENTS FROM READINGS:

1. Describe OS virtualization security best practices and elements of cloud security.

REQUIRED READINGS:

Read the following chapters from the book:

- Network Defense Essentials (NDE) v1 Academia Series – Module 06 Virtualization and Cloud Computing

ADDITIONAL RESOURCES:

White papers:

- Virtualization Defined - Eight Different Ways, https://www.f5.com/pdf/white-papers/virtualization-defined-wp.pdf
- A Whitepaper on Containerization, https://www.veritis.com/wp-content/uploads/2019/09/whitepaper-container-technology-services-tools-veritis-overview-1.pdf

- Cloud Computing White Paper, https://www.legaltechnology.com/wp-content/uploads/2012/06/OSFT-WSPEC-R004-White-Paper-on-Cloud-Computing-1-071.pdf

Videos:

- Docker Container Networking, https://www.youtube.com/watch?v=NjVZjf53bkg
- Cloud Service and Deployment Models, https://www.youtube.com/watch?v=Dfkbd6VZSnE
- What is Cloud Security?, https://www.youtube.com/watch?v=jI8IKpjiCSM

LAB ASSIGNMENTS:

Week 5 Lab Assignment 1: Auditing Docker Host Security Using Docker-Bench-Security Tool

Lab Scenario

Docker has been used extensively by organizations that use containers for development or production. Therefore, Docker security plays a key role in safeguarding containers. Although Docker provides many security benefits, its default configuration during installation has some security issues that a network defender must fix.

Lab Objectives

This lab will demonstrate how to audit the security of a default Docker installation on an Ubuntu host using Docker-Bench-Security Tool and how to fix some of the identified security warnings. In this lab, you will learn how to do the following:

- Install Docker on Ubuntu OS
- Audit Docker Security using Docker-Bench-Security Tool

Week 5 Lab Assignment 2: Implementing AWS Identity and Access Management

Lab Scenario

AWS IAM enables network defenders to control access to AWS services and resources securely. It allows to establish access rules and permissions for specific users and applications. It controls who is authenticated (signed in) and authorized (has permissions) for resource access. This helps network defenders assign role-based access control for accessing critical information within the enterprise.

Lab Objectives

This lab will demonstrate how to create an IAM Group and IAM User, attach a policy to the user, and enable Multi-Factor Authentication (MFA) that enables adding two-factor authentication for individual users in order to ensure additional security for the user accounts in AWS.

In this lab, you will learn to do the following:

- Create IAM Group in AWS
- Create IAM User in AWS
- Assign permission policy to user
- Create custom IAM policy in AWS
- Enable MFA

Week 5 Lab Assignment 3: Securing Amazon Web Services Storage

Lab Scenario

In the cloud, data are stored on Internet-connected servers in data centers. It is important that network defenders understand and implement the data storage security features for data encryption and access management tools provided by service providers to secure the data stored in the data centers.

Lab Objectives

This lab will demonstrate how to restrict access to S3 resources by creating bucket policies, Access Control Lists (ACLs), and IAM policies to provide access to selected entities.

In this lab, you will learn to do the following:

- Assign Permissions to Amazon S3 Using ACL
- Assign Permissions to Amazon S3 Using Bucket Policy

QUIZ:

1. Which of the following components of a virtual machine is an application or firmware that enables multiple guest operating systems to share a host's hardware resources?
   a. Virtual storage
   b. Management server
   c. Management console
   d. Hypervisor
2. Which of the following cloud deployments is a dynamic heterogeneous environment that combines workloads across various cloud vendors and is managed via one proprietary interface to achieve long-term business goals?
   a. Community cloud
   b. Private cloud
   c. Multi cloud
   d. Public cloud

WEEK SIX:

MODULES COVERED:

- Module 07 - Wireless Network Security

WEEK'S OBJECTIVES USED:

7. Explain wireless network fundamentals, different types of wireless encryption, and suggest security measures.

WEEK 6 ASSESSMENTS:

These are found in the course under Week Six.

- Discussion Threads: 1 discussion thread (4 pts.)
- Assignments from Readings: 2 Readings (each worth 6 pts.)
- Lab Assignment: 1 lab Assignments (4 pts.)
- Quizzes: 4 quiz questions (each question is worth 1 pt.)

DISCUSSION THREAD:

1. Discuss various types of wireless network encryption mechanisms.

ASSIGNMENTS FROM READINGS:

1. Explain about components and classification of wireless networks.
2. Describe how to detect rogue access points.

REQUIRED READINGS:

Read the following chapters from the book:

- Network Defense Essentials (NDE) v1 Academia Series – Module 07 Wireless Network Security

ADDITIONAL RESOURCES:

White papers:

- White Paper on Wireless, https://www.pwdatagroup.co.uk/wp-content/uploads/2017/02/Wireless-Networks-Intro-PDF.pdf

- WPA3 and Enhanced Open: Next Generation Wi-Fi Security, https://www.arubanetworks.com/assets/wp/WP_WPA3-Enhanced-Open.pdf
- Security in Broadband Wireless Networks, https://rdlcom.com/wp-content/uploads/Redline-White-Paper-Networks-Security.pdf

Videos:

- Wireless Standards - 802.11a and More, https://www.youtube.com/watch?v=-9EVi6krIfU
- WiFi (Wireless) Password Security - WEP, WPA, WPA2, WPA3, WPS Explained, https://www.youtube.com/watch?v=WZaIfyvERcA
- 7. Authentication methods----Wireless Networks Security, https://www.youtube.com/watch?v=eD1Dx3Re1H4

LAB ASSIGNMENTS:

Week 6 Lab Assignment 1: Configuring Security on a Wireless Router

Lab Scenario

Organizations allow wireless devices to connect to their network in today's environment (Bring Your Own Device or BYOD). However, the security of the network infrastructure is a major challenge for organizations while adopting wireless devices. A wireless router/access point is the main entry for attackers. Attackers compromise wireless access points to gain access to the organization's network. Organizations should ensure that their wireless access points are configured securely. As a network defender, you should be able to configure the wireless router securely by applying all possible hardening techniques.

Lab Objectives

This lab will demonstrate the various hardening techniques on a wireless router.

QUIZ:

1. Identify the IEEE standard that defines Bluetooth, which is mainly used for exchanging data between fixed and mobile devices over short distances.
   a. **802.15.1**
   b. 802.15.4
   c. 802.15.5
   d. 802.11ad
2. Which of the following wireless technologies influences the spectral efficiency of 4G and 5G wireless communication services, reduces interference, and increases the channel robustness?

a. OFDM

b. FHSS

c. MIMO-OFDM

d. DSSS

3. Which of the following components of a wireless network is used to connect systems to a wireless network and access the Internet directly with the help of an ISP?

a. Wireless bridge

b. Wireless repeater

c. Wireless modem

d. Wireless NIC

4. Which of the following encryption algorithms is used in Wi-Fi Protected Access 2 (WPA2) encryption for securing the wireless network?

a. RC4, TKIP

b. AES-CCMP

c. AES-GCMP 256

d. RC4

WEEK SEVEN:

MODULES COVERED:

- Module 08 – Mobile Device Security

WEEK'S OBJECTIVES USED:

8. Discuss various mobile device connection methods, Mobile Device Management concepts, common mobile usage policies, examine different security risks, and review general security guidelines and best practices for mobile platforms.

WEEK 7 ASSESSMENTS:

These are found in the course under Week Seven.

- Discussion Threads: 1 discussion thread (4 pts.)
- Assignments from Readings: 2 Readings (each worth 6 pts.)
- Lab Assignment: 1 lab Assignments (4 pts.)
- Quizzes: 3 quiz questions (each question is worth 1 pt.)

DISCUSSION THREAD:

1. Discuss the common mobile usage policies in enterprises.

ASSIGNMENTS FROM READINGS:

1. Discuss various mobile device connection methods.
2. Describe various aspects of mobile device management.

REQUIRED READINGS:

Read the following chapters from the book:

- Network Defense Essentials (NDE) v1 Academia Series – Module 08 Mobile Device Security

ADDITIONAL RESOURCES:

White papers:

- The Do's and Don'ts of Mobile Application Management, https://www.ciosummits.com/Tangoe_WhitePaper_-_The_Dos_and_Donts_of_Mobile_Application_Management.pdf

- BRING YOUR OWN DEVICE (BYOD) POLICY, https://knowledge.spok.com/@api/deki/files/26359/Best_Practices_-_Example_BYOD_Policy.pdf?revision=1
- Security technologies for mobile and BYOD, https://media.kaspersky.com/pdf/kaspersky-mobile-byod-security-technologies-whitepaper.pdf

Videos:

- What is MDM (Mobile Device Management)?, https://www.youtube.com/watch?v=ug5KUH_jdA4
- What is EMM? -An Introduction to Enterprise Mobility Management Software, https://www.youtube.com/watch?v=4LjNAISsv88
- BYOD vs CYOD vs COBO vs COPE, https://www.youtube.com/watch?v=Q5oarIoUzaE

LAB ASSIGNMENTS:

Week 7 Lab Assignment 1: Implementing Enterprise Mobile Security using Miradore MDM Solution

Lab Scenario

Network defenders must use mobile device management (MDM) solutions to control and secure mobile devices. The growing variety of mobile devices such as smartphones, laptops, and tablets has made it difficult for enterprises to formulate policies for the secure management of these devices. MDM solutions help network defenders to handle the devices carefully while reducing support costs and business discontinuity and mitigating security risks.

Lab Objectives

The objective of this lab is to demonstrate how to implement the MDM solution. In this lab, you will learn to:

- Install Miradore online cloud-based MDM solution
- Install Miradore Online Client on Android device
- Enroll device to Miradore account as a User device
- Lock a lost device

QUIZ:

1. Which of the following technologies is referred to as a wireless sensor protocol that enables communication between sensors and their controllers?

   a. ANT

   b. GPS

c. USB

d. Satcom

2. Steve, a security professional, was instructed to provide secure access to corporate data on mobile devices across the organizational networks without compromising on access speed. In this process, Steve deployed a security solution that involves encrypting important information and allowing accessing, transmitting, or storing important information on only authorized apps using strong password protection policies.

   Identify the mobile security management solution employed by Steve in the above scenario.

   a. Vaultize

   b. Metasploit

   c. zANTI

   d. Tor's Hammer

3. Which of the following guidelines must be followed to protect a mobile device from malicious attackers?

   a. Do not share information within GPS-enabled apps unless necessary

   b. Never install applications from trusted stores

   c. Always load too many applications and auto-upload photos to social networks

   d. Always connect to two separate networks such as Wi-Fi and Bluetooth, simultaneously

WEEK EIGHT:

MODULES COVERED:

- Module 09 – IoT Device Security
- Module 10 – Cryptography and PKI

WEEK'S OBJECTIVES USED:

9. Discuss working of IoT devices, application areas, communication models, IoT security principles, IoT framework security considerations, IoT device management, and identify IoT security best practices.
10. Discuss cryptography techniques, various cryptographic algorithms, and Public Key Infrastructure (PKI), and use various cryptography tools to protect information.

WEEK 8 ASSESSMENTS:

These are found in the course under Week Eight.

- Discussion Threads: 1 discussion thread (4 pts.)
- Assignments from Readings: 1 Readings (each worth 6 pts.)
- Lab Assignment: 3 lab Assignments (4 pts.)
- Quizzes: 5 quiz questions (each question is worth 1 pt.)

DISCUSSION THREAD:

1. Discuss stack-wise IoT security principles and various types of ciphers.

ASSIGNMENTS FROM READINGS:

1. Explain about various IoT communication models and give a brief description on PKI.

REQUIRED READINGS:

Read the following chapters from the book:

- Network Defense Essentials (NDE) v1 Academia Series – Module 09 IoT Device Security
- Network Defense Essentials (NDE) v1 Academia Series – Module 10 Cryptography and PKI

ADDITIONAL RESOURCES:

White papers:

- Security in Internet of Things, https://www.thinxtream.com/whitepapers/thinxtream-iot-security-wp-005.pdf
- AES Encryption, https://townsendsecurity.com/sites/default/files/AES_Introduction.pdf
- Managed Public Key Infrastructure, https://adgrafics.net/docs/symantec/MPKI_Managed_Public_Key_Infrastructure_White_Paper.pdf

Videos:

- Device Management for IOT, https://www.youtube.com/watch?v=flolzimRdfU
- Government Access to Keys GAK, https://www.youtube.com/watch?v=hsfKGZYlxdI
- What is Public Key Infrastructure (PKI) by Securemetric, https://www.youtube.com/watch?v=i-rtxrEz_E8

LAB ASSIGNMENT:

Week 8 Lab Assignment 1: Securing IoT Device Communication using TLS/SSL

Lab Scenario

Network defenders must encrypt IoT device communication to prevent unauthorized users from viewing sensitive information.

Lab Objectives

The objective of this lab is to demonstrate how to secure Internet of things (IoT) device communication using the Bevywise message queuing telemetry transport (MQTT) Broker and Simulator. This tool demonstrates the use of IoT devices over the virtual network. In this lab, you will learn to:

- Install and configure the Bevywise MQTT Broker.
- Implement transport layer security (TLS)/secure sockets layer (SSL) to secure IoT communication.

Week 8 Lab Assignment 2: Calculate One-way Hashes using HashCalc

Lab Scenario

Message digests are also called one-way hash functions because they cannot be reversed.

Lab Objectives

This lab demonstrates how to calculate one-way hashes using HashCalc for checking the integrity of a file by comparing hash values.

Week 8 Lab Assignment 3: Create a Self-signed Certificate

Lab Scenario

Self-signed certificates are widely used for testing servers.

Lab Objectives

As a network defender, you must know how to create this certificate as it validates the public key contained within the certificate belonging to the person, company, server, or other entity mentioned. The labs in this exercise demonstrate the creation of a self-signed certificate.

QUIZ:

1. Which of the following layers in the IoT architecture allows businesses to make a decision based on the information derived from policies and procedures of IoT computing?
   a. Device layer
   b. Communication layer
   c. Cloud platform layer
   d. Process layer
2. Which of the following tiers of an IoT-enabled IT environment focuses on data computation to deliver insights and thereby generate business value?
   a. Cloud tier
   b. Control tier
   c. Gateway tier
   d. Device tier
3. An organization has deployed an extensible software-as-a-service (SaaS) platform that simplifies the setup of IoT solutions and features connecting, monitoring, and managing of IoT assets at scale. Additionally, using this solution, they can update the IoT firmware from remote locations.

   Identify the solution employed by the organization in the above scenario.
   a. Cain and Abel
   b. Medusa
   c. John the Ripper
   d. Predix
4. Which of the following applications with port number “23” must be disabled to prevent connecting with a remote host?

a. HTTPS

b. Telnet

c. SSL

d. FTP

5. Which of the following objectives of cryptography defines the trustworthiness of data or resources to prevent improper and unauthorized changes?

a. Confidentiality

b. Integrity

c. Nonrepudiation

d. Authentication

WEEK NINE:

MODULES COVERED:

- Module 11 – Data Security

WEEK'S OBJECTIVES USED:

11. Discuss data security concepts, the importance of data encryption, data loss prevention, and compare different data backup concepts and technologies.

WEEK 9 ASSESSMENTS:

These are found in the course under Week Nine.

- Discussion Threads: 1 discussion thread (4 pts.)
- Assignments from Readings: 1 Readings (each worth 6 pts.)
- Lab Assignment: 3 lab Assignments (4 pts.)
- Quizzes: 3 quiz questions (each question is worth 1 pt.)

DISCUSSION THREAD:

1. Discuss anout the RAID Technology and RAID levels.

ASSIGNMENTS FROM READINGS:

1. Explain how to select an appropriate backup method and how to choose the backup location.

REQUIRED READINGS:

Read the following chapters from the book:

- Network Defense Essentials (NDE) v1 Academia Series – Module 11 Data Security

ADDITIONAL RESOURCES:

White papers:

- Encrypting Data at Rest, https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

- Disk Encryption Overview Version 1.3, https://www.ibm.com/support/pages/system/files/inline-files/White_Paper_-_TS7700_Disk_Encryption_V1.3.pdf
- RAID Technology White Paper, https://www.lacie.com/files/lacie-content/whitepaper/WP_RAID_EN.pdf

Videos:

- Data States - Data-at-rest, in-transit and in-use, https://www.youtube.com/watch?v=yRxsQP740LM
- Data Backup: Types, Methods, & the Rule of Three, https://www.youtube.com/watch?v=q-oGCKihzg0
- What is DLP? Data Loss Prevention for Critical Business Information, https://www.youtube.com/watch?v=z1l18RYpbn4

LAB ASSIGNMENTS:

Week 9 Lab Assignment 1: Perform Disk Encryption using VeraCrypt

Lab Scenario

Network defenders should know how to encrypt a volume/disk to safeguard an organization's data.

Lab Objectives

The objective of this lab is to demonstrate how to encrypt a volume using the VerCrypt tool. It is prevalent to encrypt data as it prevents the data from unauthorized access. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space and metadata).

Week 9 Lab Assignment 2: File Recovery using EaseUS Data Recovery Wizard

Lab Scenario

Network defenders should know how to recover deleted files and partitions, which have been deleted accidentally by users or due to a natural disaster. They can use recovery techniques or proprietary applications to obtain critical information.

Lab Objectives

The objective of this lab is to demonstrate how to use EaseUS Data Recovery Wizard, by intentionally deleting a few files and, subsequently, recovering them.

Week 9 Lab Assignment 3: Backing Up and Restoring Data in Windows

Lab Scenario

Network defenders should know how to recover files and folders, that were deleted accidentally by users or lost because of a natural disaster. They can use recovery techniques or proprietary applications to recover sensitive and confidential information.

Lab Objectives

Data loss in an organization can affect its finances, customer relationship, and company data. Data loss in personal computers may lead to the loss of personal files, images, and other important documents saved in the system. Data can be lost because of various reasons such as: hard drive failure, accidental deletion of data or data corruption.

The objective of this lab is to demonstrate how to backup crucial data in a Windows Server machine and use remote servers to store backup data which helps an organization in restoring data in case of a hard-drive failure on the main server.

QUIZ:

1. Which of the following techniques is a built-in encryption system for Windows to protect private information from unauthorized users who have physical access to a computer?

   a. EFS

   b. DES

   c. AES

   d. RSA

2. Which of the following RAID levels is referred to as “stripe of mirrors” that includes disk striping and mirroring in a nested hybrid RAID level?

   a. RAID Level 5

   b. RAID Level 50

   c. RAID Level 10

   d. RAID Level 3

3. Stephen, a security auditor, was hired to check whether the organization’s data is plagiarism free and meets the organization’s needs and compliances. In this process, Stephen implemented a security policy that defines a set of rules for storing and maintaining the data for operational and regulatory purposes.

   Which of the following security policies has Stephen implemented in the above scenario?

   a. Internet usage policy

   b. Acceptable use policy

   c. Data retention policy

d. Data backup policy

WEEK TEN:

MODULES COVERED:

- Module 12 – Network Traffic Monitoring

WEEK'S OBJECTIVES USED:

12. Discuss the need and advantages of network traffic monitoring, determine baseline traffic signatures for normal and suspicious network traffic, and perform network monitoring for suspicious traffic.

WEEK 10 ASSESSMENTS:

These are found in the course under Week Ten.

- Discussion Threads: 1 discussion thread (4 pts.)
- Assignments from Readings: 1 Readings (each worth 6 pts.)
- Lab Assignment: 3 lab Assignments (4 pts.)
- Quizzes: 3 quiz questions (each question is worth 1 pt.)

DISCUSSION THREAD:

1. Discuss baselining normal traffic signatures and categories of suspicious traffic signatures.

ASSIGNMENTS FROM READINGS:

1. Explain about various attack signature analysis techniques.

REQUIRED READINGS:

Read the following chapters from the book:

- Network Defense Essentials (NDE) v1 Academia Series – Module 12 Network Traffic Monitoring

ADDITIONAL RESOURCES:

White papers:

- Network Monitoring and Technology Challenges, https://www.dialogic.com/-/media/products/docs/whitepapers/11961-monitoring-wp.pdf

- Network Monitoring White Paper, https://www.telogic.com.sg/PDF/Monitoring_White_Paper.pdf
- Best Practices for Security Monitoring, https://support.ixiacom.com/sites/default/files/resources/network-visibility-whitepapers/best_practices_for_security_monitoring.pdf

Videos:

- 27 Examining Normal Network Traffic Signatures, https://www.youtube.com/watch?v=K6gAkR9J53o
- Network Traffic Analysis using Wireshark, https://www.youtube.com/watch?v=HARQmykuteQ
- Network Monitoring and Analysis For Early Threat Detection, https://www.youtube.com/watch?v=hpkccQOvA90

LAB ASSIGNMENTS:

Week 10 Lab Assignment 1: Capturing Network Traffic using Wireshark

Lab Scenario

The traffic flowing through a network contains various kinds of data. Understanding the packets of data flowing through the network using command line applications is a tedious task, and it is difficult to sort out the required traffic from the live traffic that flows through the network. Hence, it is necessary to have an application with a graphical user interface that can capture the entire traffic in a network and help filter the traffic. As a network defender, you should have Wireshark installed to monitor and capture network traffic.

Lab Objectives

This lab will demonstrate how to capture network traffic.

Week 10 Lab Assignment 2: Applying Various Filters in Wireshark

Lab Scenario

Wireshark filters traffic flowing through the entire network. This traffic contains various kinds of data packets associated with various protocols flowing between the source and destination. Therefore, searching for a specific packet, port, or an IP address manually is extremely difficult. In such cases, applying Wireshark filters helps a network defender track down a huge amount of traffic and discover the intended packets. As a network defender, it is essential to have a good knowledge of various Wireshark filters that help you narrow down the traffic and obtain the desired result.

Lab Objectives

This lab will help you become familiar with various Wireshark filters.

Week 10 Lab Assignment 3: Analyzing and Examining Various Network Packet Headers in Linux using tcpdump

Lab Scenario

Each packet in a network contains control information and user data, known as the payload. The control information contains data for delivering the payload, which includes, for example, source and destination IP and MAC addresses and sequencing information. The header part of the packet stores this control information. Hence, the network administrator needs to know how to examine the packet headers while examining the data packets.

Lab Objectives

The objective of this lab is to help students learn how to inspect TCP/IP and other packet header fields of different network packets.

QUIZ:

1. Which of the following suspicious traffic signatures exposes malicious attempts such as ping sweep, port scan, and DNS querying?
   a. **Reconnaissance**
   b. Unauthorized access
   c. Denial-of-service (DoS)
   d. Informational
2. Which of the following filters in Wireshark displays only the traffic in a LAN (192.168.x.x) between workstations and servers with no Internet?
   a. ip.src != xxx.xxx.xxx.xxx && ip.dst != xxx.xxx.xxx.xxx && sip
   b. ip.addr==192.168.1.100 machine
   c. **ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16**
   d. ip.addr==192.168.1.100 && tcp.port==23
3. Which of the following display filters in Wireshark is used to perform filtering by multiple IP addresses?
   a. ip.addr==192.168.1.100 && tcp.port=23
   b. **ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5**
   c. tcp.analysis. retransmission
   d. ip.src != xxx.xxx.xxx.xxx && ip.dst != xxx.xxx.xxx.xxx && sip

WEEK ELEVEN:

WEEK'S OBJECTIVES USED:

1. Discuss fundamental concepts of network security, including Information Assurance (IA) principles, network defense challenges, defense approaches, security controls, and review essential network security protocols.
2. Discuss access control principles, terminologies, and models, and describe Identity and Access Management (IAM) concepts.
3. Examine various administrative network defense controls, including frameworks, laws, acts, and security policies.
4. Examine various physical network defense controls, including physical security controls, workplace security, and environmental controls.
5. Examine various technical network defense controls, including network segmentation, firewall, IDS/IPS, honeypot, proxy server, VPN, SIEM, UBA, and anti-malware.
6. Comprehend fundamental virtualization concepts, Virtualization Security Concerns, cloud computing, and suggest security best practices.
7. Explain wireless network fundamentals, different types of wireless encryption, and suggest security measures.
8. Discuss various mobile device connection methods, Mobile Device Management concepts, common mobile usage policies, examine different security risks, and review general security guidelines and best practices for mobile platforms.
9. Discuss working of IoT devices, application areas, communication models, IoT security principles, IoT framework security considerations, IoT device management, and identify IoT security best practices.
10. Discuss cryptography techniques, various cryptographic algorithms, and Public Key Infrastructure (PKI), and use various cryptography tools to protect information.
11. Discuss data security concepts, the importance of data encryption, data loss prevention, and compare different data backup concepts and technologies.
12. Discuss the need and advantages of network traffic monitoring, determine baseline traffic signatures for normal and suspicious network traffic, and perform network monitoring for suspicious traffic.

WEEK 11 ASSESSMENTS:

Summative Assessment Research Project: 50 pts.

Directions on Project:

Your instructor will provide information about project topics, scope of work, and submission requirements. Review scoring rubric for project to aid in the construction and organization of the project. Listed below are potential guidelines your instructor **MAY** follow.

Guidelines on Graduate Project

Following are the guidelines for a graduate project. Apart from these guidelines, your instructor may also suggest guidelines and instructions as required during the course of the graduate project.

Selecting a Topic

- Choose a project on a topic of your interest related to your subject of study. The idea for a project may come from your own curiosity, from your coursework, interactions with colleagues, faculty members, and general observation.
- Explore the idea; examine its significance and feasibility. Go through the existing projects on similar topics. Conduct a preliminary research on the idea. Review the relevant literature. Examine the gap areas in research and identify issues you want to address. The idea should be new or must add significant value to the existing projects.
- Prepare a rough outline of project proposal you would like to submit. Discuss the topic and draft project proposal with your project coordinator, exchange ideas and incorporate suggestions.
- Conduct further research on the topic. Make a detailed proposal. In the project proposal you should:
    a. Introduce the topic
    b. Explain your rationale for selecting the project
    c. Describe significance of the project
    d. State the objective of the project and project outline
    e. Describe the methodology to be adopted
    f. State the timeline for the project completion
    g. Include references
- Finalize the proposal with your instructor by week five (specific instructors may vary that date)

Working on the Project

- On approval of the project, you should start working on your project. It is recommended you do this prior to the 5th week of the course, but speak with your instructor to clarify dates. Limit your research to the approved proposal.

- You have to complete your project within the stipulated deadlines. Plan your project accordingly
- While meeting the executives of a company in relation to your project, make sure you have appropriate approvals and request letters from the concerned university department.
- Make sure your instructor approves questionnaires designed for any survey in relation to the project.
- You must use any data collected in course of the research, only for the approved project. You must not share collected information with other candidates.
- Make notes of key points during the course of research. It would save lot of time in preparation of project report.
- Make sure all relevant journals, magazines, papers and books are available in the university library. Please check with the library information desk for information on resources, currently not available with the library.
- Analysis is the most critical part of the project and forms basis for all findings. Make sure you make use of appropriate statistical tools in analysis. Take guidance of your project coordinator during the analysis. Do validate your findings with your project coordinator.

Writing a Project Report

- Review the style guidelines for project report
- The project report should not exceed 7,000 words
- Abstract should be between 150-250 words
- Select A4 size; page orientation should be portrait. Specify "1" margin on all sides.
- Number all pages consecutively. Start every chapter on a new page.
- Provide double spacing
- You should use Times New Roman Font- "12" for text and "10" for footnotes. Use a larger font size for section headings.
- A project report must contain:

Content	Section
a. Title Page	Preliminaries
b. Table of Contents	
c. Abstract	
d. Introduction and background	Body of the report
e. Problem statement	
f. Objectives of the project	

g. Literature review	
h. Methodology adopted	
i. Results - project findings	
j. Recommendations	
k. Conclusion	
l. Bibliography	References
m. Appendix	
n. List of figures and tables	
o. Index words (if required)	

- Be clear and precise. Express your ideas in a logical way.
- Abstract should reflect the essence of the project
- The introduction should provide the overview of the topic and highlight its significance
- Clearly indicate the objectives of your project.
- Describe all the methods used such as interviews, questionnaires in the methodology section.
- Ensure that literature review is in your own words. Analyze other person's contribution to the topic. Identify the gaps in the literature. Emphasize on the likely contribution of your project to the existing literature on the topic.
- Describe your findings from analysis in the results section. As this is the most critical part of the project, ensure that there are no errors in analysis. Make proper inferences from analysis and findings.
- The conclusion section should summarize your objectives, findings and learning's from the project. Provide useful supplementary information in the Appendix.
- Avoid plagiarism. The project report should reflect your understanding of the topic. The majority of the paper should be in your own words and reflect your own ideas.
- Give credit for all referenced work. Provide appropriate citation and references for all quotations.
- Ensure that papers referenced are relevant and not outdated.
- Your paper should be reader friendly. Use footnotes to explain difficult terms.
- Don't use text from Wikipedia in footnotes
- All tables and figures must be suitably numbered and titled. Give appropriate credit.
- On completion, go through the entire project. Ensure there are no proofing errors and you have adhered to all guidelines related to the project.

- Submit spiral bound copies of the project to your project coordinator and the project review committee. If suggested, create a soft copy of the project in PDF format and submit it relevant authorities.

WEEK TWELVE:

WEEK'S OBJECTIVES USED:

1. Discuss fundamental concepts of network security, including Information Assurance (IA) principles, network defense challenges, defense approaches, security controls, and review essential network security protocols.
2. Discuss access control principles, terminologies, and models, and describe Identity and Access Management (IAM) concepts.
3. Examine various administrative network defense controls, including frameworks, laws, acts, and security policies.
4. Examine various physical network defense controls, including physical security controls, workplace security, and environmental controls.
5. Examine various technical network defense controls, including network segmentation, firewall, IDS/IPS, honeypot, proxy server, VPN, SIEM, UBA, and anti-malware.
6. Comprehend fundamental virtualization concepts, Virtualization Security Concerns, cloud computing, and suggest security best practices.
7. Explain wireless network fundamentals, different types of wireless encryption, and suggest security measures.
8. Discuss various mobile device connection methods, Mobile Device Management concepts, common mobile usage policies, examine different security risks, and review general security guidelines and best practices for mobile platforms.
9. Discuss working of IoT devices, application areas, communication models, IoT security principles, IoT framework security considerations, IoT device management, and identify IoT security best practices.
10. Discuss cryptography techniques, various cryptographic algorithms, and Public Key Infrastructure (PKI), and use various cryptography tools to protect information.
11. Discuss data security concepts, the importance of data encryption, data loss prevention, and compare different data backup concepts and technologies.
12. Discuss the need and advantages of network traffic monitoring, determine baseline traffic signatures for normal and suspicious network traffic, and perform network monitoring for suspicious traffic.

WEEK 12 ASSESSMENTS:

Summative Assessment Final Exam: 100 pts.

During week twelve you will be required to complete a final exam that incorporates several areas of critical thinking and decision-making. The exam will include multiple choice, short answer, and essay questions covering all learning outcomes of the course. Contact your instructor for specific question related to this assessment.