Assignments Document

Click on the Links to Navigate the Document

Contents

Assignment Instructions

The assessment rubric follows these instructions. Assure you meet the grading rubric requirements.

Use of existing solutions to any MindTap questions/security scripts/code/configurations will result in an automatic zero (0) on the entire assignment. Additionally, copying word for word and/or paraphrasing from the textbook, Internet, or any other previous work will not result in credit. We want to know what you learned. Therefore, only original and/or student authored answers, code, scripts, and/or configurations will be considered for credit. **This means you need to explain answers with your own understanding and words.**

Late assignments and/or assignments not submitted to D2L and/or answers that do not include the student's screenshots with a visible operating system date/timestamp will not be given credit.

Please submit one (1) and only one Microsoft Word Document for EACH assignment (e.g. Assignment 1 should have one document, Assignment 2 should have one document). The word document should have your answers to each question and screenshots in the instructions that follow in this document. Where permissions, configs, rules, code, SQL, diagrams, models, or other application-based activities exist, **you must submit a screenshot** of your completed configs/diagram/code/SQL/models/etc within the IDE/VM and with an operating system date/timestamp. The screenshot must show the results of actions like open ports, scans, identified vulnerabilities, firewall rules, and the actions taken to address these such as the associated configs/code/scripts/permission changes/firewall rules, etc. **Include all screenshots in-text under the associated question/exercise in your MS Word document submitted to D2L.**

Grading Rubric

Novice	Competent	Proficient	Pts
0 to 32 points	33 to 48 points	49 to 55 points	
Less than 70% of the assignment requirements are met and/or less than 70% of the solutions, including code/configs/rules, align with industry best practices and are the most efficient and effective solutions to the problems and/or less than 70% of the proper screenshots of all code/configs/rules are included with an OS date/time OR existing solutions were used resulting in a zero.	Less than 90% of the assignment requirements are met and/or less than 90% of the solutions, including code/configs/rules, align with industry best practices and are the most efficient and effective solutions to the problems and/or less than 90% of the proper screenshots of all code/configs/rules are included with an OS date/time.	Over 90% of the assignment requirements are met and over 90% of the solutions, including code/configs/rules, align with industry best practices and are the most efficient and effective solutions to the problems. Proper screenshots of all code/configs/rules are included with an OS date/time.	55
0 to 3 points	4 points	5 points	
Less than 70% of the assignment is well organized, uses correct spelling, uses proper grammar, and uses proper APA in-text and ending citations OR existing solutions were used resulting in a zero.	Less than 90% of the assignment is well organized, uses correct spelling, uses proper grammar, and uses proper APA in-text and ending citations.	Over 90% of the assignment is well organized, uses correct spelling, uses proper grammar, and uses proper APA in-text and ending citations.	5
Total			60

Assignment 1 Instructions

Cengage MindTap Modules 1-3 **Read & Reflect**. Following the assignments instructions, submit one (1) Microsoft Word document to D2L under the associated assignment submission link. Answer the following questions.

1. Why is data the most important asset an organization possesses? What other assets in the organization require protection?

2. Why are employees one of the greatest threats to information security?

3. What is the difference between a skilled hacker and an unskilled hacker, other than skill levels? How does the protection against each differ?

4. What are the various types of malware? How do worms differ from viruses? Do Trojan horses carry viruses or worms?

5. Why does polymorphism cause greater concern than traditional malware? How does it affect detection?

6. What is the most common violation of intellectual property? How does an organization protect against it? What agencies fight it?

7. Does the intellectual property owned by an organization usually have value? If so, how can attackers threaten that value?

8. What are the types of password attacks? What can a systems administrator do to protect against them?

9. What is the difference between a denial-of-service attack and a distributed denial-of-service attack? Which is more dangerous? Why?

10. For a sniffer attack to succeed, what must the attacker do? How can an attacker gain access to a network to use the sniffer system?

11. What is a buffer overflow, and how is it used against a Web server?

12. The chapter discussed many threats and vulnerabilities to information security. Using the Web, find at least two other reputable sources of information about threats and vulnerabilities. Explain each organization and their reputation in cybersecurity. Then, at each source/website, briefly explain the top two (2) most recent threats or vulnerabilities today. A total of four (4) threats or vulnerabilities should be explained.

13. What is the difference between law and ethics?

14. Which law amended the Computer Fraud and Abuse Act of 1986, and what did it change? The National Information Infrastructure Protection Act of 1996 amended the Computer Fraud and Abuse Act of 1986. It modified several sections of the CFA Act and increased the penalties for selected crimes.

15. What is PCI DSS and why is it important for information security?

16. What is intellectual property (IP)? Is it afforded the same protection in every country of the world? What laws currently protect IP in the United States and Europe?

17. How does the Sarbanes-Oxley Act of 2002 affect information security managers?

18. What is a policy? How is it different from a law?

19. What are the three general categories of unethical and illegal behavior?

20. What is the best method for preventing an illegal or unethical activity?

21. Using the resources in your library, identify and briefly describe the most recent five (5) laws passed in the state of Minnesota to prosecute computer crime.

Assignment 2 Instructions

Cengage MindTap Modules 4-5 **Read & Reflect**. Following the assignments instructions, submit one (1) Microsoft Word document to D2L under the associated assignment submission link. Answer the following questions.

1. Using a graphics program, design one security awareness poster on the following themes and include the acceptable use policy (added policy) at the bottom: updating antivirus signatures, protecting sensitive information, watching out for e-mail viruses, prohibiting the personal use of company equipment, changing and protecting passwords, avoiding social engineering, and protecting software copyrights. What other themes can you imagine?

2. Using the data classification scheme in Module / Chapter four (4), identify and classify the information in your personal computer or cellphone. Based on the potential for misuse or embarrassment, what information would be confidential, sensitive but unclassified, or for public release on this device?

3. Suppose Maverick Software Company (was XYZ company) has a new application development project with projected revenues of $1.5 million (Changed from 1.2 million). Using the following table, calculate the ARO and ALE for each threat category the company faces for this project.

4. Threat Category	**Cost per Incident (SLE)**	**Frequency of Occurrence**
Programmer mistakes	$5,000	1 per week
Loss of intellectual property	$75,000	1 per year
Software piracy	$500	1 per week
Theft of information (hacker)	$2,500	1 per quarter
Theft of information (employee)	$5,000	1 per 6 months
Web defacement	$500	1 per month
Theft of equipment	$5,000	1 per year
Viruses, worms, Trojan horses	$1,500	1 per week
Denial-of-service attacks	$2,500	1 per quarter
Viruses, worms, Trojan horses	$5,000	1 per week
Denial-of-service attacks	$7,000	1 per quarter
Earthquake	$250,000	1 per 20 years
Flood	$250,000	1 per 10 years

Fire	$500,000	1 per 10 years

5. Identify the top five (5) security frameworks from the assigned reading and explain them each in your own words using one or two sentences.

6. What is the ISO 27000 series of standards? Which individual standards make up the series?

7. What documents are available from the NIST Computer Security Resource Center, and how can they support the development of a security framework?

8. What are the differences between a policy, a standard, and a practice? What are the three types of security policies? Where would each be used?

9. What is contingency planning? How is it different from routine management planning? What are the components of contingency planning?

10. When is the IR plan used?

11. When is the DR plan used?

12. When is the BC plan used? How do you determine when to use the IR, DR, and BC plans?

13. What are the elements of a business impact analysis? Describe these each briefly.

14. What are Pipkin's three categories of incident indicators?

15. List and describe the six site and data contingency strategies identified in the text for disaster recovery (e.g. offsite facility types to store backups).

Assignment 3 Instructions

Cengage MindTap Module 6, NIST 800-34 pages 5-31 **Read & Reflect**. Following the assignments instructions, submit one (1) Microsoft Word document to D2L under the associated assignment submission link.

1. Use Table 1 in this question taken from NIST Special Publication (SP) 800-53. Generate a few PowerPoint slides and post them below that explain the contents of Table 1 to new users that have never seen this information. Assure each aspect of the table is defined and explained in an understandable way.

   Table 1. SP 800-43 Security Controls

Special Publication 800-53 Revision 4 — Security and Privacy Controls for Federal Information Systems and Organizations

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	P2	CM-10	CM-10	CM-10
CM-11	User-Installed Software	P1	CM-11	CM-11	CM-11
Contingency Planning					
CP-1	Contingency Planning Policy and Procedures	P1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	P1	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Contingency Training	P2	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	P2	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-5	**Withdrawn**	---	---	---	---

2. Use NIST Special Publication (SP) 800-34 and NIST Special Publication (SP) 800-53 for the Risk Assessment framework. NIST SP 800-34 outlines in Chapter 3 Table 3-6 ISCP TT&E Activities. Here is the table:

Table 3-6: ISCP TT&E Activities

TT&E Event	Sample Activity	FIPS 199 Availability Security Objective
ISCP Training (CP-3)	A seminar and/or briefing used to familiarize personnel with the overall ISCP purpose, phases, activities, and roles and responsibilities.	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Instruction (CP-3)	Instruction of contingency personnel on their roles and responsibilities within the ISCP and includes refresher training. (For a high-impact system, incorporate simulated events.)	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Contingency Plan Test / Exercise (CP-4)	Test and/or exercise the contingency plan to determine effectiveness and the organization's readiness. This could include planned and unplanned maintenance activities	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Tabletop Exercise (CP-4)	Discussion-based simulation of an emergency situation in an informal, stress-free environment; designed to elicit constructive scenario-based discussions for an examination of the existing ISCP and individual state of preparedness.	Low Impact = Yes

Using the same table with three columns (3), briefly research an organization you work at or are affiliated with like MNSU. Detail realistic TT&E events at the organization in column one, explain the sample activity in column two, and place the impact level using FIPS 199 in the last column. Add at least four (4) rows of TT&E events.

3. What is the typical relationship among the untrusted network, the firewall, and the trusted network?

4. What is the relationship between a TCP packet and UDP packet? Will any specific transaction usually involve both types of packets? What is the importance of a TCP and UDP port and is this important for a firewall configuration? Explain.

5. Research how to find listening TCP and UDP ports on your computer or the class VM. For example, the netstat command in Linux works well for this purpose. List the ports that are listening on your computer or the class VM. Take a screenshot of the command and the results with your operating system date and timestamp in the screenshot that shows listening TCP and UDP ports. Finally, briefly explain if any of these open ports are a concern to you.

6. How is static filtering different from dynamic filtering of packets? Which is perceived to offer improved security?

7. What is stateful inspection? How is state information maintained during a network connection or transaction?

8. Explain the conceptual approach that should guide the creation of firewall rule sets.

9. What special function does a cache server perform? Why is this useful for larger organizations?

10. Describe how the various types of firewalls interact with network traffic at various levels of the OSI model.

11. What is a Next Generation Firewall (NextGen or NGFW)?

12. What is the primary value of a firewall? Using screenshots from your computer, outline the active or inactive firewall running on your personal computer. If it is disabled or inactive, should it be activated?

13. What is Port Address Translation (PAT) and how does it work?

14. How do screened host architectures for firewalls differ from screened subnet firewall architectures? Which offers more security for the information assets that remain on the trusted network?

15. What is a DMZ? Why is it important in the scope of the rest of a computer network?

16. What questions must be addressed when selecting a firewall for a specific organization?

17. What is a content filter? Where is it placed in the network to gain the best result for the organization?

18. What is a VPN? Why is it becoming more widely used?

Assignment 4 Instructions

The goal of this assignment is to secure several applications for a business application server. Use the class lab virtual machine (VM). Either VM can be used for the assignments, both are used for the class projects.

1. Install the latest version of Oracle Virtualbox
    a. https://www.virtualbox.org/
2. Search the Internet for the Virtualbox documentation that associates with your installation version of the software
    a. Search "Importing an Existing Virtual Machine into VirtualBox"
    b. https://docs.oracle.com/cd/E26217_01/E26796/html/qs-import-vm.html
    c. Import the Bitnami Wordpress .ova file and the Prestashop .ova file from the links below
    d. In Virtualbox go to system settings of the VMs once they are imported
        i. In the system settings increase the RAM to 2GBs
        ii. In the system settings increase the CPU to 2 cores to make the VMs run faster
        iii. Take regular VM snapshots so that you can restore a working snapshot in case you break something in the VM during the assignments
3. The WordPress Server – A university website that uses WordPress for blogs and content management systems (CMS)
    a. WordPress must be run on a virtual machine
    b. Bitnami makes a pre-built VM you can install
        i. https://bitnami.com/stack/wordpress/virtual-machine
4. The Prestashop Server – The ecommerce bookstore service for purchasing merchandise
    a. The college e-commerce bookstore site must be run on a virtual machine
    b. Bitnami makes a pre-built VM you can install
        i. https://bitnami.com/stack/prestashop/virtual-machine

Assume this virtual machine is a server for a company. As a server, it serves and gives employees access to business applications. For example, it may host the email services for the organization. Employees connect to the server with their email client to receive and send email as a result. Employees need access via their phones, workstations, and tablets to several of the applications running on the server.

Note, if you cannot run virtual machines or run into problems, you should still attempt the labs and exercises on your own computer to the best of your ability to receive some amount of credit based upon best effort.

Begin by identifying:

- Applications running on the server
- User and group accounts on the server associated with applications

- User and file permissions of the associated running applications on the server
- Application vulnerabilities that need to be properly addressed

Choose a minimum of two (2) running applications to secure that are the most vulnerable/critical given a basic risk assessment and network scan using the Nmap command or another related application. Secure these applications while retaining service level agreements (SLAs) with the end users. In other words, the business applications must still be accessible to clients accessing the server.

In the Word Document that will be submitted to D2L include:

1. A description of each running application, the vulnerabilities found, and the strategies used to patch/address these vulnerabilities
2. The associated commands, configurations, and strategies used to find the vulnerabilities and secure the applications
3. Screenshots that prove before and after that the applications were secured, for example:
    a. Improved user, file, and application level permissions
    b. Updated/patched application version
    c. Stronger password requirements and associated enforcement policy on the VM
    d. Etcetera

Assignment 5 Instructions

The goal of this assignment is to design, implement, and test a legitimate firewall for a business application server. Use the class lab virtual machines (VMs). Once you design the firewall, implement it using iptables and test it by using nmap to scan **ONLY** the IP address of the virtual machine.

Assume this virtual machine is a server for a company. As a server, it serves or gives employees access to business applications. For example, it may host the email services for the organization. Employees would connect to the server with their email client to receive and send email as a result. Employees need access via their phones, workstations, and tablets to the server.

Note, if you cannot run virtual machines or run into problems, you should still attempt the labs and exercises on your own computer to the best of your ability to receive some amount of credit based upon best effort.

To be successful, the firewall must meet these two primary objectives:

1. Allow a business IP address range to access a minimum of five (5) working applications/services
    - **a.** Working services could be a file share, email service, SSH, DNS, etc
    - **b.** While not all IP addresses need to access the services, a range of business IP addresses defined by you must be able to access the services
2. Deny IP addresses foreign to the business from accessing five (5) working services and log any malicious attempts to access these services
    - **a.** These can be the same services that are accessible or different services
    - **b.** Log alerts in an existing log file and/or create a new log file

Once the firewall is designed and implemented, use a scan tool like nmap to determine if the firewall is working. If you do not know how to use a scanning tool skip this step. Do NOT under any circumstance scan any host/computer other than the virtual machine. **The instructor takes no responsibility for students that violate the campus and/or other policies by scanning computers other than their own virtual machine.**

In the Word Document that will be submitted to D2L include:

1. A description of each running application, their business uses, and the firewall strategy
2. The iptables firewall rules/script
3. Recent log entries from the new alert log file
4. Screenshots that prove before and after that the applications were secured, for example:
    a. A scan before the new firewall rules were applied and after the new rules are in operation