

Module 8: Assignment

8-1: DDoS Mitigation

- How do organizations attempt to mitigate a sudden DDoS attack directed at their web servers?

Use the Internet to research DDoS mitigation techniques, technologies, and third-party entities that provide mitigation services.

Write a one-page paper on your research.

8-2: DNS Services

Many organizations offer a free domain name resolution service that resolves DNS requests through a worldwide network of redundant DNS servers. The claim is that this is faster and more reliable than using the DNS servers provided by Internet service providers (ISPs). These DNS servers are supposed to improve security by maintaining a real-time blacklist of harmful websites and warning users when they attempt to access a site containing potentially threatening content. The providers also say that using their services can reduce exposure to types of DNS poisoning attacks.

- Research free DNS services.
- Identify at least three providers and create a table comparing their features. Are the claims of providing improved security valid?
- How do they compare with your ISP's DNS service?

Write a one-page paper on your research.

8-3: DNS-over-HTTPS (DoH)

To protect DNS, some providers are using DNS-over-HTTPS, also called DoH. As its name implies, DoH uses HTTPS instead of HTTP to send DNS queries via an encrypted HTTPS connection (Port 443) rather than sending them in clear text (Port 53). The encrypted DoH query is sent to a special DoH resolving server that aggregates all user's DoH queries and then translates them into regular unencrypted DNS queries for processing by DNS servers.

- However, DoH has become controversial. Why?
- What are the advantages of DoH?
- What are its disadvantages?
- How does it compare with DNS-over-TLS (DoT)?

Write a one-page paper on your research.

8-4: CCTV Technologies

Research new technologies for CCTV, including motion recognition and object detection.

- How accurate are the technologies?
- What are the advantages?
- What are the disadvantages?

Write a one-page paper on your research.

8-5: Robot Sentries

Research the Internet regarding robot sentries.

- Where are they being used?
- What is the purpose of a robot sentry?
- What are the risks?
- What is your projection on the future of robot sentries?

Write a one-page paper on your research.

Module 9: Assignment

9-1: Data Loss Prevention Comparison

Research at least four different data loss prevention (DLP) products from four different vendors.

- *Create a table that compares at least six different functions and options.*

Based on your research:

- Which would you choose?
- What features make this product the optimum? and why?

Write a short paragraph that summarizes your research.

9-2: Cloud-Based Honeypots

Research cloud-based honeypots.

- What are their advantages?
- What are their disadvantages?
- When should they not be used?
- How could one be set up?

Create a one-page paper of your research.

9-3: Hardening a Jump Box

How should a jump box be configured?

- *Create a list of configurations that you would use to set up a jump box that had the fewest risks.*

9-4: Researching Network Access control

Use the Internet to research the network access control products from Microsoft and Cisco.

- How are they different?
- How are they similar?
- What are some of the options for each product?
- Which would you choose, and why?

Write a one-page paper on your research.

9-5: UTM Comparison

Create a table of four UTM devices available today.

- *Include the vendor name, pricing, a list of features, the type of protection it provides, etc.*

Based on your research, assign a value of 1–5 (from lowest to highest ranking) that you would give that UTM.

- *Include a short explanation of why you gave it that ranking.*

9-6: Zero Trust

Use the Internet to research Zero Trusts.

- What is it?
- What are its advantages?
- What are its disadvantages?
- What technologies does it require?
- Is it a long-term security solution?
- Is it widely accepted?
- What do you think about it?

Write a one-page paper on your research.

9-7: Network Firewall Comparison

Use the Internet to identify three network firewalls and create a chart that compares their features. Note if they are rule-based or policy-based, perform stateless or state-full packet filtering, what additional features they include (IDS, content filtering, etc.), their costs, etc.

- *Which would you recommend? Why?*

Module 10: Assignment

10-1: Trustworthy email Protocols and Standards

In addition to S/MIME, several protocols and standards protect email. These include STARTTLS, DNS-Based Authentication of Named Entities (DANE), Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC).

- Use the Internet to research each of these.
- Create a summary of each along with the respective strengths and weaknesses.

Which would you recommend? Why?

10-2: Secrets Management Systems

Cloud computing providers typically offer their own proprietary secrets management systems, and there are several third-party systems available.

- Identify two proprietary secret management systems from cloud providers and two third-party systems.

Research each and then create a document outlining how they are used, their strengths, and their weaknesses.

10-3: Comparing MSSPs

Identify three MSSPs and research the services that they provide.

- Create a document that outlines the services provided by each MSSP.
- Would you support contracting with an MSSP for part of an organization's security functions?
- Would you support using an MSSP for all security functions?

Write a one-page paper arguing both the pros and cons of using MSSPs.

10-4: Create a Cloud Conceptual Model

Use the Internet to research different cloud conceptual models and identify at least three.

- Then create your own model.
- Draw the different layers and label each along with how each layer would function.

10-5: IPv6

Use the Internet to research the security enhancements of IPv6.

- *Write a one-page paper on how IPv6 is more secure than IPv4.*

Module 11: Assignment

11-1: Comparisons of Contactless Payment Systems

Three of the most popular contactless payment systems are Apple Pay, Google Pay, and Samsung Pay. Each has advantages and disadvantages.

- Using the Internet, research these three different systems.
- Create a table that lists each system and its features, strengths, and weaknesses, ease of use, security, etc.
- Which of them would you recommend?
- In your opinion, what can be done to make these more popular?

Write a one-paragraph summary to accompany your table.

11-2: Bluetooth Range Estimator

The range at which a Bluetooth device can transmit depends on several factors. Understanding the ranges helps you be aware of whether a Bluetooth-enabled device could be the victim of a blue-jacking or bluesnarfing attack.

Go to www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/range/ to explore the Bluetooth Range Estimator tool.

- First, watch the video and then read the details of each of the key factors.
- Then use the range estimator tool, changing the different parameters (receiver sensitivity, path loss, transmit power, transmitter antenna gain, and receiver antenna gain) to determine the estimated range.
 - What does this tell you about Bluetooth ranges?
 - How could this tool be used?

Write a one-page paper on what you have learned.

11-3: EAP

Use the Internet to research information on the EAP protocols that are supported in WPA2 Enterprise (see Table 11-5 on page 335 from the textbook).

- Write a brief description of each, and indicate the relative strength of its security.

Write a one-page paper on your research.

11-4: WPA3 Features

Use the Internet to research WPA3 features, particularly SAE and OWE.

- What are the primary advantages and disadvantages of each of these features?
- How do they enhance Wi-Fi security?

Write a one-page paper on your research.

11-5: Antennas

To many users, antennas are just one of life's great mysteries. They know from experience that any antenna is better than having no antenna and that the higher the antenna is located, the better the reception will be. Yet the antenna is arguably one of the most important parts of a wireless network. Antennas play a vital role in both sending and receiving signals, and a properly positioned and functioning antenna can make all the difference between a WLAN operating at peak efficiency or a network that nobody can use.

- Use the Internet to research antennas for APs.
- What different types of antennas are used?
- What are their strengths?
- What are their weaknesses?
- Which types would be used to concentrate a signal to a more confined area?

Write a one-page paper on what you find.

11-6: Your Personal Wireless Security

Is the wireless network you own as secure as it should be?

- Examine your wireless network or that of a friend or neighbor, and determine which security model it uses.
- Next, outline the steps it would take to move it to the next highest level.
- Estimate how much it would cost and how much time it would take to increase the level.
- Finally, estimate how long it would take you to replace all the data on your computer and what you might lose if the data were corrupted by an attacker.
- Would this be motivation to increase your current wireless security model?

Write a one-page paper on your work.