# Week 4 Hands On

Eric Vara

The University of Arizona Global Campus

CYB 300

Instructor Bipin Bhatt

12, December 2022

## Part One

### Module 08: Security Technology: Access Controls, Firewalls, and VPNs Review Questions

1. What is the typical relationship among the untrusted network, the firewall, and the trusted network?
   * Answer:
2. What are the two primary types of network data packets? Describe their packet structures.
   * Answer:
3. List some authentication technologies for biometrics.
   * Answer:
4. How is static filtering different from dynamic filtering of packets? Which is perceived to offer improved security?
   * Answer:
5. What is stateful-packet inspection? How is state information maintained during a network connection or transaction?
   * Answer:
6. Explain the conceptual approach that should guide the creation of firewall rule sets.
   * Answer:
7. List some common architectural models for access control.
   * Answer:
8. What is the main difference between discretionary and nondiscretionary access controls?
   * Answer:
9. What is a hybrid firewall?
   * Answer:
10. Describe Unified Threat Management (UTM). How does UTM differ from Next Generation Firewalls?
    * Answer:
11. What is a Next Generation Firewall (NextGen or NGFW)?
    * Answer:
12. What is the primary value of a firewall?
    * Answer:
13. What is Port Address Translation (PAT), and how does it work?
    * Answer:
14. What are the main differences between a password and a passphrase?
    * Answer:
15. What is a sacrificial host? What is a bastion host?
    * Answer:
16. What is a DMZ?
    * Answer:
17. What questions must be addressed when selecting a firewall for a specific organization?
    * Answer:
18. What is RADIUS?
    * Answer:
19. What is a content filter? Where is it placed in the network to gain the best result for the organization?
    * Answer:
20. What is a VPN? Why is it becoming more widely used?
    * Answer:

### Module 09: Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools Review Questions

1. What common security system is an IDPS most like? In what ways are these systems similar?
   * Answer:
2. How does a false positive alarm differ from a false negative alarm? From a security perspective, which is less desirable?
   * Answer:
3. How does a network-based IDPS differ from a host-based IDPS?
   * Answer:
4. How does a signature-based IDPS differ from a behavior-based IDPS?
   * Answer:
5. What is a monitoring (or SPAN) port? What is it used for?
   * Answer:
6. List and describe the three control strategies proposed for IDPSs.
   * Answer:
7. What is a honeypot? How is it different from a honeynet?
   * Answer:
8. How does a padded cell system differ from a honeypot?
   * Answer:
9. What is network footprinting?
   * Answer:
10. What is network fingerprinting?
    * Answer:
11. How are network footprinting and network fingerprinting related?
    * Answer:
12. Why do many organizations ban port scanning activities or the use of hacker tools on their internal networks?
    * Answer:
13. Why would ISPs ban outbound port scanning by their customers?
    * Answer:
14. What is an open port? Why is it important to limit the number of open ports to those that are absolutely essential?
    * Answer:
15. What is a system’s attack surface? Why should it be minimized when possible?
    * Answer:
16. What is a vulnerability scanner? How is it used to improve security?
    * Answer:
17. What is the difference between active and passive vulnerability scanners?
    * Answer:
18. What is Metasploit Framework? Why is it considered riskier to use than other vulnerability scanning tools?
    * Answer:
19. What kind of data and information can be found using a packet sniffer?
    * Answer:
20. What capabilities should a wireless security toolkit include??
    * Answer:

### Module 10: Cryptography Review Questions

1. What are cryptography and cryptanalysis?
   * Answer:
2. What was the earliest reason for the use of cryptography?
   * Answer:
3. What is a cryptographic key, and what is it used for? What is a more formal name for a cryptographic key?
   * Answer:
4. What are the cryptographic tools discussed in this module, and what does each accomplish?
   * Answer:
5. What is a hash function, and what can it be used for?
   * Answer:
6. What does it mean to be “out of band”? Why is it important to exchange keys out of band in symmetric encryption?
   * Answer:
7. What is the fundamental difference between symmetric and asymmetric encryption?
   * Answer:
8. How does public key infrastructure add value to an organization seeking to use cryptography to protect information assets?
   * Answer:
9. What are the components of PKI?
   * Answer:
10. What is the difference between a digital signature and a digital certificate?
    * Answer:
11. What critical issue in symmetric and asymmetric encryption is resolved by using a hybrid method like Diffie–Hellman?
    * Answer:
12. What is steganography, and what can it be used for?
    * Answer:
13. Which security protocols are predominantly used in web-based electronic commerce?
    * Answer:
14. Which security protocols are used to protect e-mail?
    * Answer:
15. IPSec can be implemented using two modes of operation. What are they?
    * Answer:
16. Which kind of attack on cryptosystems involves sequential guessing of all possible key combinations?
    * Answer:
17. Consider the earlier module discussion about encryption key power and key strength, and then review Table 10-5. If you were setting up an encryption-based network, what key size would you choose and why?
    * Answer:
18. What are the strongest key sizes used in encryption systems today?
    * Answer:
19. What encryption standard is currently recommended by NIST?
    * Answer:
20. What are the most popular protocols used to secure Internet communication?
    * Answer:

## Part Two

### Hands-On Project: Log Management

Complete the Hands-On Project: Log Management

After completing the hands-on project, answer the following prompts

### Self-Reflection and Response

What are some of the reasons you would need to look at the Windows System Log?

|  |
| --- |
|  |

Breifly describe how you might manage the growth in the size of system log files. Why would you need to keep copies of log files?

|  |
| --- |
|  |

How long do you think system logs shold be retained?

|  |
| --- |
|  |

### Hands-On Project: Footprinting

Complete the Hands-On Project: Footprinting

After completing the hands-on project, answer the following prompts

### Self-Reflection and Response

Some of the activties in this lab were flagged as being considered potentially hostile unless you have permission to do them. Why would a company want to keep network users from using thse tpye of tools?

|  |
| --- |
|  |

Can you think of reasons why you would need to be able to determine who controls a web address or web site?

|  |
| --- |
|  |

What are some reasons you may want to use nmap on your own network?

|  |
| --- |
|  |