Name

Student Number

ITEC2210 Final Exam

11 December 2023

Exam overview:

This exam is divided into three parts worth 30 marks (multiple choice), 10 marks (short answer), and 15 marks (long answer), for a total of 55 marks.

1. The first section consists of multiple choice questions, each worth 1 mark. There are 30 questions worth 30 marks in total.

2. The second section consists of short answer questions, each worth 2 marks each. There are 5 questions worth 10 marks in total.

3. The last section consists of long answer questions, each worth 5 marks. There are three questions worth a total of 15 marks.

Name

Student Number

Section 1, multiple choice

Choose the single **most** correct answer for each of the following questions. Extra space is provided after each question if for some reason you wish to elaborate on your answer.

1. Which of the following is **not** a namespace?
(A) Ethernet addresses
(B) Account names
(C) Unix UIDs
(D) Local workstation passwords

2. Given a machine name *prod-ottawa-db01*, which kind of naming method is being used?
(A) Functional
(B) Thematic
(C) Hybrid
(D) Descriptive

3. What is a DNS resolver?
(A) One of the 13 root servers with a list of all top-level domains
(B) A system that queries other DNS servers
(C) One of a pair of DHCP servers that also handles DNS
(D) A DNS server that is setup using anycast routing

4. Which of the following is **not** a reason to restore a file or system?
(A) Accidental file deletion
(B) Disk failure
(C) Archival purposes
(D) RAID 1 disk failure

5. Which of the following is an **incorrect** way to backup a database?
(A) Copy the DBMS files to another disk or server
(B) Take a disk snapshot of the database and copy to another disk or server
(C) Perform a full dump of the database to another disk or server
(D) Copy a base backup along with binary logs to another disk or server

Name

Student Number

6. A level 2 incremental backup:
(A) Is a combination of level 1 and a differential backup
(B) Only contains changes since the last incremental backup
(C) Contains all previous incremental backups
(D) Is a snapshot of a filesystem in time

7. A DNS root hints file contains:
(A) Active Directory password hints for users
(B) A list of name servers used to initialize a DNS resolver
(C) IPV6 to IPv4 mappings of top-level domains like .com, .ca, .org etc.
(D) A complete list of Top Level Domains (TLDs)

8. Which of the following is a primitive cryptographic operation?
(A) Key exchange
(B) Hashing
(C) Transposition
(D) Distribution

9. Symmetric encryption:
(A) Only uses substitution for operations
(B) Relies on a public and private key and an initialization vector
(C) Can operate on blocks of data or a stream of bits
(D) Is weak because keyspaces are smaller than asymmetric encryption

10. A cryptographic hash function:
(A) Requires a public key and modulus exponent factor as part of its input
(B) Can easily be reversed to regenerate the input data
(C) Generates a digital signature to authenticate a user or system or file
(D) Maps an input of arbitrary length to a fixed length binary output

11. Diffie-Hellman is a method to:
(A) Build a web of trust between PGP users who do not know each other
(B) Establish a shared symmetric encryption key over an insecure channel
(C) Authenticate a TLS 1.2 session using a client supplied certificate
(D) Hash TLS certificate data to submit to third party Certificate Authorities

Name

Student Number

12. The RSA algorithm requires:
(A) Two prime numbers and an exponent
(B) A signature from a Certificate Authority (CA)
(C) Hashing a private key to produce a public key
(D) Keys equal to or larger than 1024 bits in length

13. Which of the following statements about historical monitoring systems is **false**?
(A) Monitoring data used for billing may need to be kept indefinitely
(B) Graphs are a good way to visualize monitoring data
(C) Capacity planning is easier with historical data
(D) Historical monitoring requires a pull architecture

14. What is a possible problem that can arise when acknowledging an alert?
(A) Someone else might acknowledge the alert at the same time as you
(B) Alerting will be off indefinitely for that check until it is un-acknowledged
(C) The service in question will be negatively affected
(D) Central monitoring systems will become overloaded until the issue is resolved

15. Which of the following is **false?** Configuration Management/IaC systems:
(A) Have steep learning curves
(B) Should have end to end CI/CD testing
(C) Will automate you out of a job
(D) Produce higher quality configuration results

16. Which of the following is **not** true regarding Configuration Management (CM) systems?
(A) Declarative CM systems describe what a system should look like
(B) Most CM tools will have modules for common databases and applications
(C) CM systems only have modules for the platform you run them on
(D) An idempotent CM system will only make changes if they are needed

17. In a CI/CD pipeline, what does Continuous Delivery (CD) mean?
(A) CD means code is continuously delivered to production
(B) CD means code is continuously available for delivery to production
(C) CD means compute infrastructure is continuously available for deployments
(D) CD means compute capacity is continuously delivered to a datacentre

Name

Student Number

18. Black-box monitoring means:
(A) Purchasing a proprietary Black-Box™ appliance to monitor infrastructure
(B) Using monitoring tools that only detect if something is up/down or broken
(C) Building instrumentation into application code and running health checks
(D) Collecting historical data to draw graphs of service availability

19. RAID 0 is:
(A) Faster than RAID 5 because it mirrors data across all drives
(B) Slower than RAID 1 because it has to write parity data to all drives
(C) Still reliable if a drive fails in an array
(D) Not a backup

20. RAID 1 is:
(A) Faster than RAID 5 because it stripes data across all drives
(B) Slower than RAID 0 because it has to write parity data to all drives
(C) Unreliable if a drive fails in an array
(D) Not a backup

21. Address Space Layout Randomization (ASLR) is used to:
(A) Prevent attackers from running compromised binaries on a system
(B) Scramble directory layouts to confuse attackers
(C) Block local users from running commands with sudo privileges
(D) Make it difficult to predict memory locations for stack and heap overflow attacks

22. Software Defined Networking (SDN) abstracts away:
(A) VLANs
(B) VPNs
(C) Network topologies
(D) Underlay networks

23. An Infrastructure as a Service provider will:
(A) Only allow you to run certain operating systems
(B) Provide you with CPU, memory, network, and storage
(C) Configure your application stack and scale it for you
(D) Come to your datacentre and build servers

Name

Student Number

24. A router's main task is to:
(A) Deliver packets directly to their intended recipients
(B) Bridge between VLANs in an internal network
(C) Send packets closer to their destinations
(D) Ensure redundant network links in a datacentre

25. In a TCP session, SYN packets are intended to:
(A) Synchronize sequence numbers for subsequent communication
(B) Send application data that requires explicit acknowledgement
(C) Stop a packet from being transmitted
(D) Request retransmission of a packet

26. The sudo command is intended for:
(A) Running Mattermost as a dedicated user
(B) Restarting services on a virtual machine
(C) Moving files between directories
(D) Executing a command as a different user

27. nginx is a:
(A) Chat platform that is an alternative to Slack
(B) TLS certificate authority that issues certificates
(C) Web server
(D) Application server

28. The chown command is used to:
(A) Change the working directory in a terminal session
(B) Alter ownership of files or directories
(C) Create a new system user
(D) Move a file from one directory to another

29. RFC 1149 **IPoAC** is designed to:
(A) Ensure IP packets are transmissible over 802.11A/C WiFi
(B) Allow datacenter air conditioners to be remotely controlled
(C) Link offices in a multi-star network topology
(D) Send data using birds

Name

Student Number

30. letsencrypt is a:
(A) Tool that encrypts files on a server
(B) Free service that issues TLS certificates
(C) Paid subscription service that checks encryption cipher suites
(D) Tool that generates nginx configurations with TLS certificates

Section 2 short answer.

For each question, define or explain using point form. Each question is worth 2 marks.

1. What is the difference between a **namespace** and a **nameservice**? 2 marks.

2. What are some problems that can arise with poorly chosen host or DNS names? 2 marks.

3. How does a **differential** backup work? 2 marks.

4. How do hashing algorithms/functions work and why are they useful? 2 marks.

5. What is symmetric encryption and how does it work? 2 marks.

Name

Student Number

Section 3 long answer

For each question, define or explain using point form. Each question is worth 5 marks.

1. Why are configuration management tools like Puppet and Ansible useful? What kind of tasks would you carry out using either tool? What are the advantages of configuring infrastructure as code?

2. How does TCP work? Explain the types of packets, how they are ordered during handshakes, and what they contain.

Name

Student Number

3. Explain how the TLS handshake works when you browse to **https://itec2210.ca** with a browser or command line client**.** Specifically, explain what happens **before** encrypted data is transmitted between the client and server.