## Assignment 10: Final Exam Preparation Quiz

This Unit’s homework assignment is a short quiz covering Chapters 1 – 15.

Multiple Choice questions are worth 1 point each.

True and False questions are worth 1 point each.

Fill in the Blank questions are worth 2 points each (1 point for each blank that must be answered).

1. **What two terms are closely associated with VPNs?**
2. Tunneling and Encapsulation
3. Bridging and Filtering
4. Path and Network Management
5. Encapsulation and Decapsulation
6. Port Forwarding and Port Blocking
7. **All of the following are mistakes in firewall security except:**
8. Managing security poorly
9. Deploying too many firewalls
10. Using firewalls to provide filtering for networks and hosts
11. Not writing a security policy
12. Failing to keep current with updates and patches
13. **Which of the following is not ensured or provided by a secured VPN?**
14. Confidentiality
15. Quality of Service
16. Integrity
17. Privacy
18. Authentication
19. **Which attack is based on the impersonation of a legitimate host?**
20. DoS
21. Replay
22. Fragmentation
23. Spoofing
24. Hijacking
25. **What is the essential purpose or function of authorization?**
26. Granting or denying access to resources
27. Checking policy compliance
28. Identifying entities
29. Monitoring levels of utilization
30. Detecting spoofed content
31. **Resetting the system configuration back to factory defaults is a potential hazard when installing patches or updates.**
32. True
33. False
34. **The biggest issue or problem with an IDS is false negatives.**
35. True
36. False
37. **Port forwarding supports caching, encryption endpoints and load balancing.**
38. True
39. False
40. **NMAP is a tool that can be used to test and probe whether a port is open or closed.**
41. True
42. False

1. **NETCONFIG is the command line utility used to display the IP configuration of a Windows computer.**
2. True
3. False
4. **\_**Two-Factor Authentication (2FA) or Token/Biometrics **and** \_ Multifactor authentication (MFA)\_\_ **are stronger authentication methods for client VPN over passwords alone.**
5. \_\_SSL\_ **and** \_IPSec\_\_ **are the two different protocols commonly used for remote access VPN.**
6. \_Troubleshooting Information\_\_ **and** \_ Troubleshooting Plan\_\_ **are two commonly used tools for troubleshooting firewalls.**
7. **The** \_Remote Desktop Protocol (RDP)\_\_ **Protocol is a proprietary protocol developed by Microsoft that provides a user with a graphical interface to another computer.**
8. \_IDS\_\_ and \_IPS\_\_ **are two types of devices that monitors network traffic and alerts during a potential attack.**

NAME: Natnael kebede