**FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA**
**SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY**
**DEPARTMENT OF INFORMATION AND MEDIA TECHNOLOGY**

**Time Allowed: 2 Hours** **Credit Unit: 3 Units** **Course Lecturer: Dr. S.O. Ganiyu**

**INSTRUCTION: Answer Question ONE (1) and Any Other THREE (3) Questions**

**Question 1 (24 marks) Compulsory**

(a) What are the five (5) processes you will adopt when creating a security policy? (**2½ marks**)
(b) Describe Smurf attack. (**3½ marks**)
(c) Briefly describe three (3) of the characteristics of denial of service (DOS) attack. (**3 marks**)
(d) Write three (3) of the disadvantages of honeypots. (**3 marks**)
(e) Briefly describe Demilitarized Zone (DMZ) (**2 marks**)
(f) You are attempting to back hack an intruder who secured his/her control system with username and password. For simplicity, suppose the intruder carelessly revealed his identity after entering a trap-and-trace security countermeasure.
i. What software will you utilise to gain access into the intruder's system? (**1 mark**)
ii. Give at least three (3) specific examples of the software you mentioned in question **f(i)** above. (**3 marks**)
(g) Explain the underlisted cryptography concepts and terminologies.
i. Cryptovariable (**2 marks**)
ii. Post quantum cryptography (**2 marks**)
iii. Link encryption (**2 marks**)

**Question 2 (12 marks)**

(a) XProbe is essentially one of the viable tools for detecting the operating systems of remote hosts in a computer network. Explain how you can use it for ethical hacking. (**4 marks**)
(b) Explain the two default policy settings for a firewall. (**4 marks**)
(c) Briefly discuss the copy routine of a typical computer virus. (**4 marks**)

**Question 3 (12 marks)**

(a) Briefly describe network-based intrusion detection and prevention system. (**3 marks**)
(b) Explain computer worm. (**5 marks**)
(c) How do worms spread in a network? (**2 marks**)
(d) Describe the biggest danger of computer worm. (**2 marks**)

**Question 4 (12 marks)**

(a) Explain **personnel** and **operations** as components of security. (**3 marks**)
(b) List the six (6) common types of firewalls. (**3 marks**)
(c) Explain security Plan (RFC 2196). (**6 marks**)

**Question 5 (12 marks)**

(a) Discuss synchronisation attack. (**6 marks**)
(b) No doubt, setting up security rules for a firewall can become complex and tedious for network security expert. Explain with six (6) valid points, how a firewall can be configured in such a way that it will not have negative impacts on business interest. (**6 marks**)

**Question 6 (12 marks)**

(a) Summarise how will you ensure the security of an organisation's web as a security professional. (**3 marks**)
(b) Discuss the Prevention component of an Intrusion Detection and Prevention System (IDPS) for network and host IDPS. (**4 marks**)
(c) Explain the following attacks:
i. USB password stealer. (**2 marks**) ii. Brute force. (**3 marks**)