1. ข้อใดคือระบบที่ช่วยให้ Linux แชร์ไฟล์กับ Windows ได้

A) DNS

B) DHCP

C) Samba

D) Apache

2. ข้อใดไม่ใช่วิธีการแชร์ไฟล์ในระบบเครือข่าย

A) ใช้ Shared folder ใน Windows

B) ใช้ Samba บน Linux

C) ใช้การส่ง Email แนบไฟล์

D) ใช้ Cloud Storage (เช่น Google Drive)

3. ข้อใดคือการเข้าถึง Shared folder ใน Linux ผ่านprotocol SMB

A) smb://IP-Address/ชื่อแชร์

B) ftp://IP-Address/ชื่อแชร์

C) http://IP-Address/ชื่อแชร์

D) telnet://IP-Address/ชื่อแชร์

4. ข้อใดคือผลเสียถ้าเปิดแชร์โดยไม่กำหนดสิทธิ์

A) ไฟล์จะถูกเข้าถึงโดยไม่ได้รับอนุญาต

B) เครื่องพิมพ์จะพิมพ์ช้าลง

C) ไม่สามารถพิมพ์ได้

D) ไม่สามารถเข้าถึงเครือข่ายได้

5. ข้อใดคือประโยชน์หลักของการแชร์ทรัพยากรในเครือข่าย

A) ทำให้คอมพิวเตอร์เร็วขึ้น

B) ใช้ทรัพยากรร่วมกันได้สะดวก ประหยัดค่าใช้จ่าย

C) ทำให้ระบบปฏิบัติการใหม่ล่าสุด

D) ลดการใช้พลังงานไฟฟ้าโดยอัตโนมัติ

6. ข้อใดคือคำสั่งที่ใช้ตรวจสอบการเชื่อมต่อระหว่างคอมพิวเตอร์กับปลายทางในเครือข่าย

A) Tracert

B) Ping

C) Netstat

D) Nslookup

7. ข้อใดใช้สำหรับตรวจสอบเส้นทางการส่งข้อมูลจากเครื่องต้นทางไปยังเครื่องปลายทา

A) Ipconfig

B) Ping

C) Tracert

D) netstat

8. ข้อใดคือเครื่องมือที่ใช้ในการดักจับและวิเคราะห์ Packet ข้อมูล

A) Wireshark

B) Ping

C) Ipconfig

D) Netstat

9. ข้อใดเป็นคำสั่งที่ใช้ตรวจสอบรายละเอียดการตั้งค่า IP ของเครื่องใน Windows

A) Ifconfig

B) Ipconfig

C) Nslookup

D) Netstat

10. ข้อใดคือเครื่องมือใน Linux ที่ใช้ตรวจสอบการตั้งค่า IP Address

A) Ping

B) Ifconfig

C) Netstat

D) dig

11. ข้อใดคือประโยชน์ของการใช้เครื่องมือ ping

A) ตรวจสอบเส้นทางการส่งข้อมูล

B) ตรวจสอบความเร็ว CPU

C) ตรวจสอบการเชื่อมต่อกับ host

D) ตรวจสอบการเปิด Port

12. ข้อใดคือการทำงานหลักของคำสั่ง netstat

A) ตรวจสอบเส้นทางของข้อมูล

B) ตรวจสอบพอร์ตและการเชื่อมต่อที่ใช้งาน

C) ตรวจสอบการตั้งค่า DNS

D) ตรวจสอบความเร็วการ์ดจอ

13. ข้อใดคือคำสั่งที่ใช้ตรวจสอบการแปลงชื่อ domain ไปเป็น IP Address

A) Nslookup

B) Ping

C) Ipconfig

D) tracert

14. ข้อใดคือเครื่องมือที่นิยมใช้ในการตรวจสอบสถานการณ์ทำงานของระบบเครือข่ายทั้งองค์กร

A) Wireshark

B) PRTG

C) Ping

D) ifconfig

15. ข้อใดไม่ใช่เครื่องมือสำหรับวิเคราะห์เครือข่าย

A) Wireshark

B) Netstat

C) Photoshop

D) Tcpdump

16. ข้อใดคือข้อจำกัดของการใช้คำสั่ง ping

A) ไม่สามารถตรวจสอบเส้นทางได้

B) ไม่สามารถตรวจสอบการเชื่อมต่อได้

C) ใช้ได้เฉพาะใน Linux เท่านั้น

D) ใช้ได้เฉพาะใน Windows เท่านั้น

17. ข้อใดคือคำสั่งที่ใช้ใน Linux เพื่อดูการตั้งค่าเส้นทาง (Routing Table)

A) Route

B) Tracert

C) Ping

D) nslookup

18. ข้อใดคือประโยชน์ของการใช้เครื่องมือ Wireshark

A) ใช้ตรวจสอบการเชื่อมต่อเบื้องต้น

B) ใช้ดักจับและวิเคราะห์ Packet ข้อมูลในเครือข่าย

C) ใช้ตรวจสอบการตั้งค่า IP

D) ใช้ตรวจสอบการทำงานของ hard disk

19. ข้อใดคือการใช้งานคำสั่ง tracert อย่างถูกต้อง

A) tracert www.google.com

B) tracert -p 80

C) tracert 192.168.1.1/24

D) tracert config

20. ข้อใดไม่ถูกต้องเกี่ยวกับการใช้เครื่องมือวิเคราะห์เครือข่าย

A) ใช้ตรวจสอบการเชื่อมต่อ

B) ใช้ดักจับข้อมูลเครือข่าย

C) ใช้หาสาเหตุปัญหาเครือข่าย

D) ใช้เพิ่มความเร็ว CPU

21. ข้อใดเป็นองค์ประกอบหลักของความปลอดภัยเครือข่าย (CIA Triad)

A) Confidentiality, Integrity, Availability

B) Control, Information, Authentication

C) Communication, Integrity, Access

D) Connection, Isolation, Authority

22. ข้อใดเป็นภัยคุกคามเครือข่าย

A) การสำรองข้อมูล

B) การเข้ารหัสข้อมูล

C) การโจมตีแบบ DDoS

D) การตั้งรหัสผ่านที่รัดกุม

23. ข้อใดเป็นวิธีการรักษาความลับของข้อมูล (Confidentiality)

A) การสำรองข้อมูล

B) การเข้ารหัสข้อมูล

C) การติดตั้งสายแลนเพิ่ม

D) การใช้ Switch

24. ข้อใดหมายถึงความถูกต้องครบถ้วนของข้อมูล (Integrity)

A) ป้องกันไม่ให้ข้อมูลถูกแก้ไขโดยไม่ได้รับอนุญาต

B) ป้องกันไม่ให้บุคคลภายนอกเข้าถึงข้อมูล

C) ทำให้ระบบพร้อมใช้งานเสมอ

D) การสำรองไฟล์เก็บไว้

25. ข้อใดคืออุปกรณ์ที่ใช้ควบคุมการรับ–ส่งข้อมูลเพื่อความปลอดภัย

A) Switch

B) Firewall

C) Hub

D) Repeater

26. ข้อใดเป็นการป้องกันการโจมตีจาก Malware

A) ใช้รหัสผ่านอ่อน

B) ติดตั้ง Antivirus

C) แชร์ไฟล์โดยไม่กำหนดสิทธิ์

D) ปิด Firewall

27. ข้อใดคือการโจมตีที่ผู้ไม่หวังดีส่งข้อมูลจำนวนมากเพื่อทำให้ระบบไม่สามารถให้บริการได้

A) Phishing

B) Sniffing

C) DoS/DDoS

D) Spoofing

28. ข้อใดคือการดักจับข้อมูลที่ส่งผ่านเครือข่าย

A) Phishing

B) Sniffing

C) DoS

D) Spoofing

29. ข้อใดคือการปลอมแปลง Email หรือเว็บไซต์เพื่อหลอกผู้ใช้

A) DoS

B) Sniffing

C) Phishing

D) Firewall

30. ข้อใดเป็นการสื่อสารข้อมูลอย่างปลอดภัยผ่าน Internet

A) FTP

B) HTTP

C) HTTPS

D) Telnet