COMP 012 - Network Administration

Windows + Linux + Packet Tracer + Python Automation

SESSION 9: CYBERSECURITY FUNDAMENTALS

ACTIVITY 9.1: SECURITY PRINCIPLES AND THREAT LANDSCAPE

Topic: Understanding cybersecurity fundamentals

Description: Learn core security principles and common threats

INSTRUCTIONS:

Research and document security principles:

- CIA Triad: Confidentiality, Integrity, Availability
- AAA: Authentication, Authorization, Accounting
- Defense in Depth strategy
- Principle of Least Privilege
- Zero Trust model

Document common threats:

- Malware types (virus, worm, trojan, ransomware)
- Phishing and social engineering
- DDoS attacks
- Man-in-the-Middle attacks
- SQL injection, XSS
- Insider threats

For each threat document:

- How it works
- Real-world example
- Prevention/mitigation methods

Research recent security breaches (2024-2025)

Create threat matrix for your lab environment

Deliverables: Submit cybersecurity fundamentals document with threat analysis	**25 Points**

ACTIVITY 9.2: IDS/IPS CONCEPTS

Topic: Intrusion Detection and Prevention Systems

Description: Understand IDS/IPS technologies and deployment

INSTRUCTIONS:

Research IDS/IPS:

- IDS vs IPS - detection vs prevention
- Signature-based detection
- Anomaly-based detection

- Network-based (NIDS) vs Host-based (HIDS)

Popular IDS/IPS solutions:

- Snort (open source)
- Suricata
- OSSEC (host-based)
- Commercial: Cisco, Palo Alto, Fortinet

Deployment considerations:

- Inline vs passive mode
- Placement in network (before/after firewall)
- Performance impact
- False positives management

Optional hands-on:

- Install Snort on Linux VM
- Configure basic rules
- Generate alerts with test traffic

Document IDS/IPS best practices

Deliverables: Submit IDS/IPS research document (and Snort setup if done)	**30 Points**

ACTIVITY 9.3: VPN AND DMZ DESIGN

Topic: Secure remote access and network segmentation

Description: Design and understand VPN and DMZ architectures

INSTRUCTIONS:

VPN fundamentals:

- Site-to-Site VPN vs Remote Access VPN
- IPSec protocol suite (ESP, AH, IKE)
- SSL/TLS VPN
- VPN tunneling concepts

In Packet Tracer:

- Build Site-to-Site VPN between two routers
- Configure ISAKMP policy
- Configure IPSec transform set
- Create crypto ACL and crypto map
- Test encrypted communication

DMZ Design:

- What is DMZ? (Demilitarized Zone)
- Purpose: Isolate public-facing servers
- Three-legged firewall design
- Dual-firewall design (more secure)

Create DMZ network design:

- Inside zone: Internal LAN

- DMZ zone: Web server, Email server
- Outside zone: Internet
- Define traffic rules between zones

Deliverables: Submit VPN .pkt file and DMZ design document	**40 Points**

TOTAL POINTS: 95