Critical Knowledge Content Library

Unit 1: Networking Foundations

NETWORK FUNDAMENTALS
- OSI & TCP/IP Models
- Data Encapsulation
- Network Topologies
- Networking Devices

DATA TRANSMISSION PROTOCOLS
- MAC & ARP
- IPv4, IPv6, ICMP
- TCP & UDP
- TCP & UDP Ports

APPLICATION PROTOCOLS
- Web Communications
- DHCP Overview
- NTP Overview
- Email Communication Protocols
- Remote Access Protocols

Unit 2: Attack Types

ATTACK LIFECYCLE
- Overview
- Reconnaissance
- Resource Dev.
- Initial Access
- Execution
- Privilege Escala.
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Ctrl.
- Exfiltration
- Impact

AUTHENTICATION ATTACKS
- Social Engineering
- Session Hijacking
- Password Cracking Techniques

DoS/DDoS ATTACKS
- SYN Flood Attacks
- DDoS Attacks
- Amplification

INJECTION ATTACKS
- Buffer Overflow Attacks
- Cross-site Scripting (XSS) Attacks
- SQL & LDAP Injection Attacks

MALWARE ATTACKS
- Malware by Propagation Types
- Malware by Actions on Victims
- Malware by Detection Avoidance Methods

LAYER 1 & 2 ATTACKS
- Wireless Recon & Sniffing
- Wireless Access Points & Association Attacks
- Bluetooth Attacks
- Physical Attacks

Unit 3: Network Security

SECURITY COMPONENTS
- Firewalls
- Load Balancers
- Intrusion Detection & Prevention Systems
- Proxy Servers
- SIEM & UTM Devices

NETWORK SECURITY
- Network Segmentation
- VLANs
- IPSec
- Secure Network Protocols

Unit 4: Security Engineering

ENCRYPTION
- Symmetric vs. Asymmetric Encryption
- Hashing
- Public Key Infrastructure
- Certificate Infrastructure

IDENTITY & ACCESS MGMT
- I-AAA
- Multi-Factor Authentication
- Access Control Models
- Single Sign On
- Windows Authentication

SECURE CODING
- Insecure Coding
- Secure Software Dev. Lifecycle
- Secure Coding Best Practices
- Application Testing

Unit 5: Governance, Risk, & Compliance

RISK MANAGEMENT
- Defining Risk
- Risk Assessment
- Risk Response
- Control Types

COMPLIANCE & GOVERNANCE
- Security Frameworks
- Privacy
- Auditing Process & Reports
- Third Party Management
- Laws & Regulations
- Business Continuity Planning & Disaster Recovery

Unit 6: Security Operations

SECURITY OPERATIONS
- Critical Assets, Inventorying, & Inventory Management
- Attack Surface Management
- Logging & Monitoring
- Proactive Security Operations

INCIDENT RESPONSE
- Incident Response Models in Use
- Prepare
- Defect & Identify
- Contain & Eradicate
- Recover
- Lessons Learned
- Integrating Threat Intelligence

CLOUD SECURITY
- Cloud Technologies Overview
- Cloud Architecture & Dev.
- Cloud Considerations & Tools
- Common Cloud Vulns. & Threats
- Critical APIs for Security

VIDEOS QUIZ LAB NOTES