Day 16-20: Security Policies and Compliance

Information security policies and standards

Regulatory compliance (e.g., GDPR, HIPAA, PCI DSS)

Risk management and assessment

Day 21-25: Incident Response and Forensics

Incident response planning and procedures

Digital forensics techniques

Evidence collection and preservation

Day 26-30: Vulnerability Management

Vulnerability scanning and assessment

Patch management and software updates

Vulnerability remediation strategies

Days 31-60: Vulnerability Assessment and Penetration Testing (VAPT)

Day 31-35: Introduction to VAPT

Understanding the VAPT process

Ethical hacking principles and methodologies

Legal and ethical considerations

Day 36-40: Network Reconnaissance and Scanning

Network mapping and discovery

Port scanning and service enumeration

Vulnerability identification

Day 41-45: Web Application Security

Common web application vulnerabilities (e.g., SQL injection, XSS)

Web application penetration testing techniques

Exploiting web application vulnerabilities

Day 46-50: System Hacking and Exploitation

Privilege escalation and lateral movement

Windows and Linux system hacking

Exploiting system vulnerabilities

Day 51-55: Wireless and Mobile Security

Wireless network security protocols and attacks

Mobile device security vulnerabilities

Penetration testing for wireless and mobile systems

Day 56-60: Reporting and Remediation

Documenting VAPT findings and recommendations

Presenting VAPT results to stakeholders

Remediation strategies and validation

Days 61-90: Malware Analysis and Incident Response

Day 61-65: Introduction to Malware

Types of malware (viruses, worms, trojans, etc.)

Malware infection vectors and distribution methods

Malware detection and prevention techniques

Day 66-70: Static Malware Analysis

Analyzing malware samples using static analysis tools

Identifying malware characteristics and behaviors

Reverse engineering malware code

Day 71-75: Dynamic Malware Analysis

Setting up a malware analysis sandbox environment

Executing and monitoring malware behavior

Extracting and analyzing malware artifacts

Day 76-80: Incident Response Planning

Incident response framework and best practices

Incident response team roles and responsibilities

Incident response plan development

Day 81-85: Incident Detection and Triage

Security monitoring and log analysis

Indicators of compromise (IoCs) and threat intelligence

Incident classification and prioritization

Day 86-90: Incident Containment and Eradication

Containment strategies and techniques

Malware removal and system remediation

Incident documentation and reporting

Days 91-120: Cloud Security

Day 91-95: Cloud Computing Fundamentals

Cloud service models (IaaS, PaaS, SaaS)

Cloud deployment models (public, private, hybrid)

Cloud infrastructure components and services

Day 96-100: Cloud Security Architecture

Cloud security shared responsibility model

Identity and access management in the cloud

Network security in cloud environments

Day 101-105: Cloud Data Security

Data encryption and key management

Cloud storage security best practices

Data backup and disaster recovery in the cloud

Day 106-110: Cloud Threat Modeling and Risk Assessment

Cloud-specific threat modeling

Cloud risk assessment and mitigation strategies

Compliance and regulatory requirements in the cloud

Day 111-115: Cloud Monitoring and Incident Response

Cloud security monitoring and logging

Incident response in cloud environments

Forensics and investigations in the cloud

Day 116-120: Cloud Security Automation and DevSecOps

Infrastructure as code (IaC) and security as code

Continuous integration and continuous deployment (CI/CD)

Cloud security automation tools and techniques

This roadmap provides a structured approach to developing your cybersecurity skills, from the fundamentals to more specialized areas like VAPT, malware analysis, and cloud security. Remember to adapt this roadmap based on your prior knowledge, learning pace, and specific career goals within the cybersecurity field.

Related

what are some beginner-level resources to learn about vapt

what are some intermediate-level resources to learn about malware

what are some beginner-level resources to learn about cloud security