Syllabus - The Advanced Program Cyber Defense Incident Responder

Course Outline:

I. FORENSICS

Topic Covered:

- Computer Memory Forensics, Memory Dump Analysis
- FTK Imager, Autopsy, Redline and RAM capturing
- Digital Evidence Acquisition Methodologies
- Registry Forensics
- Windows Timeline Analysis and Data Recovery
- Network Forensics, Anti-Forensics and Steganography

TOOLS: Volatility Framework, FTK Imager, Autopsy, NetworkMiner, Wireshark, OpenStego, ShellBags Explorer, winmd5free, Magent RAM Capture, Redline, HxD

II. MALWARE ANALYSIS

Topic Covered:

- Dynamic Malware Analysis, Reverse Engineering and Malware Obfuscation
- Fileless Malware Analysis
- Containment, Eradication and Recovery Malware Stages
- Android APK Analysis

TOOLS: HashCalc, Exeinfo PE, PDF Stream Dumper, FileAlyzer, HxD, Yaazhini Vulnerability Scanner, APK Tool, Ghidra, HashCompare, UPX Easy GUI, Wireshark

III. ETHICAL HACKING AND INCIDENT RESPONSE

Topic Covered:

- Ethical Hacking Processes and Methodologies
- Network Hacking, Reconnaissance, Google Hacking and Locating Attack Vectors
- Exploitation Techniques

- Web Application Hacking, OWASP Top 10 – XSS, SQL Injection, Manual and Automated Attacks
- Post Incident Activity

TOOLS: Metasploit, SQLMap, Nmap

Here's are the of component needed in hosting cybersecurity learning platform via Cloud Services.

1. **Server Infrastructure:**
    - Webservers: Apache Nginx for hosting the platform
    - Database Servers: MySQL, PostgreSQL, MongoDB for storing user data, courses, and progress.
2. **Networking Equipment:**
    - Routers switched and firewalls to manage network security.
    - Load balancers for distributing incoming traffic across multiple servers.
3. **Security Software:**
    - Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS) to monitor and protect against cyber threats.
    - Anti-malware and antivirus software to scan for and remove malicious software.
    - Security information and event management (SIEM) software for aggregating and analyzing security logs.
4. **Authentication and Authorization Systems:**
    - Single Sign-On (SSO) solutions for seamless login across multiple services.
    - Role-based access control (RBAC) for managing user permissions within the platform.
5. **Encryption Tools:**
    - SSL/TLS certificates for encrypting data transmitted between servers and clients.
    - Encryption protocols (e.g., AUS) for securing stored data.
6. **Monitoring and Logging Tools:**
    - Monitoring tools for tracking system performance, uptime, and resource usage.
    - Logging tools for recording user activity system events, and security incidents.
7. **Content Delivery Systems:**
    - Content Delivery Network (CDNs) for delivering course materials and multimedia content quickly and reliably.

8. **Virtualization and Containerization Platforms:**
    - Virtual machines (VMs) or containers for isolating and running application services.
    - Orchestration tools like Kubernetes or Dockers Swarm for managing containerized applications.
9. **Backup and Disaster Recovery Solutions:**
    - Regular backups of data to prevent data loss in case of system failure or cyber-attacks.
    - Disaster recovery plans and procedures to restore services quickly in the event of a major outage.
10. **Development and testing Environments:**
    - Development frameworks and tools for building and testing new features.
    - Continuous Integration/Continuous Deployment (CI/DC) pipelines for automating software deployment.
11. **User Interface and Experience Tools:**
    - Fronted frameworks like React.js or Angular for building responsive and interactive user interfaces.
    - Design tools for creating visually appealing and intuitive user experiences.
12. **Compliance and Regulatory Tools:**
    - Tools for ensuring compliance with data protection regulations (e.g., GDPR, HIPAA).
    - Vulnerability scanning tools for identifying and addressing security weaknesses.
13. **Customer Support and Communication Tools:**
    - Helpdesk software for managing user inquiries and support tickets.
    - Communication tools like email, chat, and collaboration.
14. **Education Content Creation Tools:**
    - Authoring tools for creating and editing educational materials, such as videos, presentations, and quizzes.
    - Learning management system (LMS) for organizing and delivering course content to users.

15. **User Analytics and Feedback Systems:**
    - Analytics tools for tracking user engagement, course completion rates, and other key metrics.
    - Feedback mechanics for collecting user opinions and suggestions for improving the platform.
16. **Legal and Compliance Support:**
    - Legal consultation for ensuring compliance with intellectual property laws, terms of service, and privacy policies.
    - Cyber insurance to protect against potential legal liabilities and financial losses from security incidents.
17. **Training and Support for Staff:**
    - Training programs for platform administrators, instructors, and support staff on cybersecurity best practices and platform usage.
    - Technical support for troubleshooting issues and resolving user concerns.
18. **Internet Bandwidth:**
    - The required amount will depend on factors such as the numbers of users accessing the platform simultaneously, the type of content being served (e.g., test, images, videos), and any streaming of interactive features.