Exam Cram Notes: Asset Management

1. Overview

Asset management in cybersecurity refers to the **identification, tracking, protection, and maintenance** of an organization's IT assets, including hardware, software, data, and cloud resources. Effective asset management helps organizations **reduce security risks, maintain compliance, and enhance operational efficiency**.

---

2. Types of Assets

A. Hardware Assets

✅ **Servers, Workstations, Laptops, Mobile Devices –** Require security controls like encryption, endpoint protection, and patch management.
✅ **Networking Devices (Routers, Switches, Firewalls) –** Need firmware updates, access control, and logging.
✅ **IoT & Embedded Systems –** Require strict security policies to prevent unauthorized access.

B. Software Assets

✅ **Operating Systems (Windows, Linux, macOS) –** Must be updated and secured against vulnerabilities.
✅ **Applications & Licenses –** Should be inventoried and monitored for outdated or unauthorized software.
✅ **Firmware & Middleware –** Must be patched regularly to prevent exploits.

C. Data Assets

✅ **Customer & Employee Data –** Must be encrypted and protected from breaches.
✅ **Intellectual Property & Business Records –** Require backups and access control.
✅ **Logs & Security Data –** Need proper retention policies for forensic analysis.

D. Cloud & Virtual Assets

✅ **Virtual Machines & Containers –** Must be monitored for unauthorized changes.
✅ **Cloud Services & APIs –** Require access controls and encryption.
✅ **Shadow IT (Unauthorized Cloud Usage) –** Needs monitoring to prevent security gaps.

---

3. Asset Management Lifecycle

1️⃣ **Identification & Discovery –** Track all IT assets (hardware, software, cloud).
2️⃣ **Classification –** Categorize assets based on **sensitivity, value, and risk**.

3️⃣ **Tracking & Inventory –** Maintain an **updated asset database** for compliance.
4️⃣ **Security Controls –** Apply **encryption, access control, and patching**.
5️⃣ **Monitoring & Auditing –** Use **SIEM, log analysis, and asset tracking tools**.
6️⃣ **Disposal & Decommissioning –** Securely wipe or destroy assets before disposal.

---

4. Asset Inventory & Tracking

A. Asset Inventory Tools

✅ **CMDB (Configuration Management Database) –** Centralized tracking of all IT assets.
✅ **Automated Discovery Tools –** Scan networks for new or unauthorized devices.
✅ **Barcode & RFID Tagging –** Physical asset tracking using unique identifiers.

B. Asset Labeling & Classification

✅ Assign **classification levels** (e.g., Public, Internal, Confidential, Restricted).
✅ Use **data tagging** to control access and prevent unauthorized sharing.

C. Asset Ownership & Responsibilities

✅ Clearly define who is responsible for **asset maintenance and security**.
✅ Assign roles to manage **hardware, software, and data assets**.

---

5. Security Measures for Asset Management

A. Access Control & Authentication

✅ **RBAC (Role-Based Access Control) –** Limit access based on user roles.
✅ **MFA (Multi-Factor Authentication) –** Prevent unauthorized asset usage.
✅ **Least Privilege Principle –** Restrict access to only what is necessary.

B. Patch Management & Vulnerability Scanning

✅ Regular **security updates** for OS, applications, and firmware.
✅ Conduct **vulnerability scans** to detect outdated software and misconfigurations.

C. Secure Configuration & Hardening

✅ **Remove default credentials** and unnecessary services on assets.
✅ Apply **baseline security configurations** to all devices and software.

D. Endpoint Protection

✅ Deploy **antivirus, EDR (Endpoint Detection & Response), and host firewalls**.
✅ Monitor endpoint devices for **malicious activity**.

E. Encryption & Data Protection

✅ Encrypt **data at rest, in transit, and in use**.
✅ Use **BitLocker, TLS/SSL, and full-disk encryption**.

---

6. Asset Decommissioning & Disposal

✅ **Secure Data Wiping –** Use tools like DBAN to erase sensitive data.
✅ **Physical Destruction –** Shred or degauss hard drives before disposal.
✅ **Asset Recycling –** Ensure proper disposal to prevent data leakage.

---

7. Key Exam Takeaways

✅ Maintain an **updated asset inventory** (hardware, software, cloud).
✅ Use **automated tools** to track and manage assets.
✅ Implement **access controls, encryption, and endpoint protection**.
✅ Regularly **patch and scan** assets for vulnerabilities.
✅ **Securely dispose of decommissioned assets** to prevent data leaks.