Collection

In the collection phase, **attackers gather data of interest from within the compromised environment**. This phase is focused on harvesting valuable information such as databases, credentials, sensitive files, and communications. Common methods of collection include **database dumps, capturing audio, video, or screen activity, and accessing internal documentation, network shared drives, and internal traffic**.

1. Database Dumps

- Definition: Attackers may extract entire databases or specific tables from database servers. This data often includes sensitive information such as user credentials, personally identifiable information (PII), or financial records.
- Methods:
  - SQL Queries: Attackers with database access may use SQL queries to export data from key tables or perform full database dumps.
  - Automated Tools: Tools like **mysqldump for MySQL**, **pg_dump for PostgreSQL**, or custom scripts can facilitate large-scale data extraction.
- Security Implications: Database dumps can provide attackers with high-value, structured data that can be used for credential stuffing, identity theft, or extortion. Detecting unusual queries or large data exports can be a sign of unauthorized data collection.

2. Audio/Video/Screen Capture and Keylogging

- Audio/Video/Screen Capture:
  - Definition: Attackers may record audio or video from a device’s microphone or camera, or take screenshots to capture real-time activity, sensitive communications, or visual data.
  - Methods: Malware can activate microphones, cameras, or screen capture tools to record interactions. Some remote access tools (RATs) include built-in capture functionality.
- Keylogging:
  - Definition: Keyloggers record keystrokes on a compromised device, capturing usernames, passwords, messages, and other typed information.
  - Types: Keyloggers can be hardware-based (plugged into a keyboard) or software-based (installed malware).
- Security Implications: Audio, video, and screen captures can reveal sensitive conversations and activities, while keyloggers expose credentials and personal information. These techniques often **operate in the background, making them difficult to detect without dedicated security measures**.

3. Internal Documentation, Network Shared Drives, and Internal Traffic Interception

- **Internal Documentation**:
  - Definition: Attackers search for sensitive documents stored on the target’s system, network drives, or document management platforms. This may include internal procedures, financial records, employee details, and strategic plans.
  - Methods: Attackers may navigate through directories or search for specific document types, such as PDF, DOCX, or spreadsheets, to find valuable data.

- **Network Shared Drives**:
    - Definition: Shared network drives provide centralized file storage that multiple users within an organization can access. Attackers target these drives to collect shared files, including documents, presentations, and databases.
    - Security Implications: Shared drives often contain valuable information accessible by multiple departments, making them high-priority targets. They allow attackers to collect a broad array of data without needing to access individual devices.
- **Internal Traffic Interception**:
    - Definition: Attackers intercept and analyze internal network traffic to gather credentials, communications, and other transmitted data. This may involve capturing data packets or setting up a man-in-the-middle (MitM) attack.
    - Methods: Tools like **Wireshark** or **TCPDump** can capture and analyze network traffic, revealing sensitive data like login credentials and internal communications.
- Security Implications: Intercepted traffic can expose unencrypted data, allowing attackers to gather information without directly interacting with user accounts. Internal traffic interception often goes undetected, especially if attackers have compromised internal network points.

Summary

- Database Dumps allow attackers to quickly obtain structured and high-value data, including PII and credentials, from database servers.
- Audio/Video/Screen Capture and Keylogging give attackers insight into live communications, activities, and credentials, helping them gather sensitive information discreetly.
- Internal Documentation, Network Shared Drives, and Internal Traffic Interception provide attackers with access to valuable organizational information, shared resources, and communications, which can be used for further exploitation or data exfiltration.

By understanding these collection methods, organizations can take steps to **secure data, such as monitoring large database exports, securing network shares with access controls, and encrypting internal traffic to prevent interception**. Additionally, monitoring for unusual behavior on endpoints can help detect unauthorized access to resources like screen capture and keylogging tools.