Windows Security Topics

1. Windows Registry and Group Policy

- **Windows Registry**
  - **A hierarchical database storing low-level settings for the operating system, applications, and services**.
  - Common Forensic Uses
    - Track user activities: Timestamps, installed programs, USB connections.
    - Configuration changes: Startup programs (HKLM\Software\Microsoft\Windows\CurrentVersion\Run).
- **Group Policy**
  - A centralized management system for configuring and enforcing policies across Windows systems.
  - Key Features
    - User and computer settings.
    - Control over security options (e.g., password policies, software restrictions).
  - Common Applications
    - Enforcing compliance standards.
    - Locking down sensitive configurations (e.g., disabling USB ports).

2. Active Directory (AD)

- What It Is
  - **A directory service used in Windows networks for centralized authentication, authorization, and directory management**.
  - Components
    - **Domain Controllers (DCs)**: **Servers hosting the AD database**.
    - **Objects**: Users, groups, devices, and policies.
    - **Authentication Protocols**: Kerberos, NTLM.
  - **BloodHound Tool**
    - A tool for mapping and analyzing AD environments to identify attack paths.
    - Features:
      - Visualizes relationships between users, groups, and computers.
      - Identifies misconfigurations, such as over-permissioned users or groups.
    - Typical Use Cases
      - Penetration testing to identify privilege escalation paths.
      - Blue team activities to harden AD environments.
  - Kerberos Authentication with AD
    - How It Works
      - Kerberos uses tickets issued by a Key Distribution Center (KDC) to authenticate users.
      - Components
        - TGT (Ticket Granting Ticket): Issued to authenticate users within the domain.
        - Service Tickets: Granted for specific resource access.

        - Attack Techniques
            - Golden Ticket
                - Forged TGTs using the KRBTGT account hash.
            - Silver Ticket
                - Forged service tickets to access specific resources.
            - Pass-the-Ticket
                - Reusing stolen Kerberos tickets.

3. Windows SMB (Server Message Block)

- What It Is
    - **A protocol for sharing files, printers, and network resources**.
    - Common Uses
        - File sharing between Windows systems.
        - Remote access to shared resources.
- Security Concerns
    - EternalBlue Exploit
        - Exploited vulnerabilities in SMBv1 (e.g., WannaCry ransomware).
    - SMB Relay Attacks
        - Intercepting and relaying SMB authentication to gain unauthorized access.
- Best Practices
    - Disable SMBv1.
    - Enable SMB signing.
    - Use firewalls to restrict SMB traffic.

4. Samba (with SMB)

- What It Is
    - **An open-source implementation of the SMB protocol for non-Windows systems (e.g., Linux, macOS)**.
    - Common Uses
        - File and printer sharing in mixed OS environments.
        - Integrating Linux servers into Windows domains.
    - Security Considerations
        - Ensure Samba is properly configured to prevent unauthorized access.
        - Use encryption for sensitive SMB traffic.

5. Buffer Overflows

- Overview
    - Occurs when a program writes data beyond the bounds of a buffer, overwriting adjacent memory.
    - Exploitation
        - Overwriting return addresses to redirect execution to malicious code.
- Defense Mechanisms:
    - **DEP (Data Execution Prevention)**
        - Prevents execution of code in non-executable memory regions.
    - **ASLR (Address Space Layout Randomization)**

        - Randomizes memory layout to make buffer overflow attacks more difficult.

6. Return-Oriented Programming (ROP)

- What It Is
    - **An advanced exploitation technique used to bypass defenses like DEP**.
    - How It Works
        - Instead of injecting code, **attackers chain together existing instructions ("gadgets") in memory**.
        - Each gadget ends with a RET instruction, which controls the flow of execution.
- Example Workflow
    1. Overwrite the return address to point to a sequence of gadgets.
    2. Chain gadgets together to perform malicious actions.
    3. Execute the payload without injecting new code.
- Defense Mechanisms
    - **Control Flow Integrity (CFI)**
        - Ensures program execution follows legitimate control flow paths.
    - **Shadow Stack**
        - Maintains a separate stack to verify return addresses.

Summary

Topic	Key Details
Windows Registry	Stores system and application settings; valuable for forensic analysis.
Group Policy	Centralized management of Windows security and configurations.
Active Directory	Centralized authentication and resource management; Kerberos is the default protocol.
BloodHound Tool	Maps AD environments to identify privilege escalation paths.
Kerberos Attacks	Golden Ticket, Silver Ticket, Pass-the-Ticket exploits in AD environments.
Windows SMB	Protocol for file sharing; vulnerabilities include EternalBlue and SMB relay attacks.
Samba	SMB implementation for Linux; integrates with Windows domains.
Buffer Overflows	Exploits memory overflows to execute malicious code; mitigated with DEP and ASLR.
ROP (Return-Oriented Programming)	Bypasses defenses like DEP by chaining existing memory instructions; mitigated with CFI and shadow stacks.

Understanding these core Windows topics, including Active Directory, SMB, and exploitation techniques like buffer overflows and ROP, is critical for securing systems and conducting effective forensic investigations. Leveraging tools like BloodHound and implementing robust defenses such as ASLR, DEP, and Control Flow Integrity can help mitigate risks and enhance system resilience.