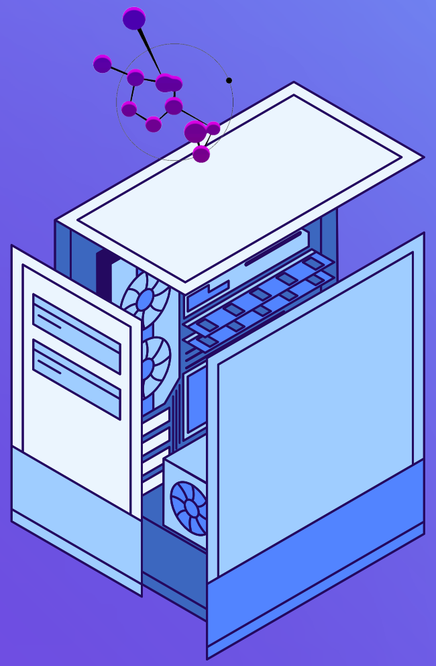
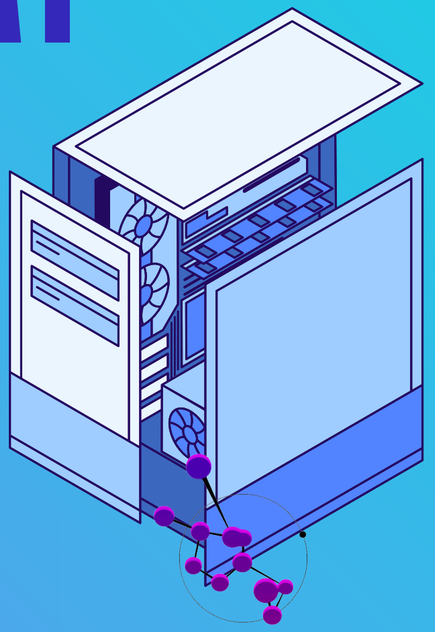
WINDOWS BYPASS KIT

Made by: Sara, Alaa, Nermeen

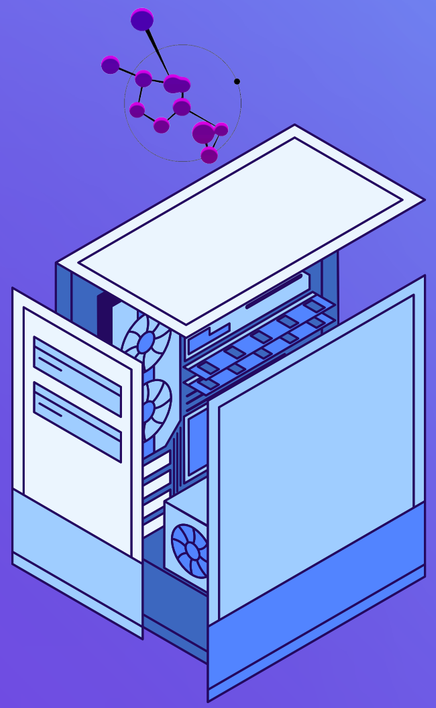
WHAT WE WILL DISCUSS TODAY

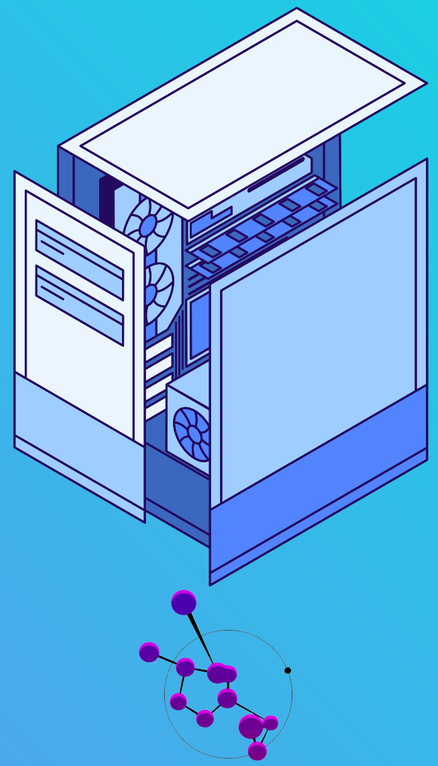




- Windows Authentication
- Bypassing Windows UAC Authentication
- What are kits and how to use them
- Recent and old windows vulnerabilities

WHAT IS WINDOWS AUTHENTICATION?





- Process of verifying the user’s identity.
- User provides credentials (password/PIN/biometric).
- Windows checks these credentials against SAM or Active Directory.
- If valid → an Access Token is created to define the user’s permissions.

Component	Function
Winlogon	Handles logon screen → collects credentials → user enters credentials
Credential Providers	Gathers user input (password/PIN/biometric) → used by Winlogon
LSASS	Core security component → validates credentials → receives credentials from Winlogon
Authentication Packages	Kerberos / NTLM → loaded by LSASS to check account
SAM / Active Directory	Stores user accounts → checked by Auth Package
Access Token	Created if credentials are valid → defines user permissions
Session Start	Winlogon launches user session using the token

WHY LAYERED ARCHITECTURE?

- Separation of responsibilities
- Strong security boundaries
- Easier to extend (PIN, biometrics, Smart Cards)
- Defense-in-depth: compromise of one layer doesn’t compromise the whole system

BYPASS

interrupting or replacing something in the chain:

1. Credential collection
2. Credential validation (LSASS)
3. Token generation
4. Session creation

BYPASS

- Post-Authentication privileges
- Boatloader

KIT

- **Definition**: a ready-made package of tools that attackers use to perform or automate an attack.
- **Types of Kits**
  - Exploit Kits – deliver exploits for browsers or OS vulnerabilities.
  - Phishing Kits – create fake login pages to steal credentials.
  - Malware Kits – build or customize malware like ransomware or RATs.
  - Bypass/Authentication Kits – bypass login, MFA, or security controls.

EVOLUTION OF WINDOWS LOGIN VULNERABILITY

Early Windows Era (Pre-Windows 10)

➤Sticky Keys (sethc.exe) replacement

➤Offline SAM extraction

Windows 8/10 Era

➤Windows Hello spoofing attacks

Modern Windows (10/11)

➤HiveNightmare (CVE-2021-36934)

➤Privilege Escalation (CVE-2024-43583)

➤Sticky Keys (sethc.exe) replacement

- **Affected**: Windows XP → Windows 8.1
- **Technique:** Attackers replaced sethc.exe (Sticky Keys) with cmd.exe using a bootable disk. Then pressing SHIFT ×5 on the login screen launched a SYSTEM command prompt.
- **Impact**: Full admin takeover without password.
- **Patched**: Mitigations started in Windows 8.1 → fully restricted by Windows 10 Secure Boot (2015).

➤Windows Hello spoofing attacks

- **Affected**: Windows 10
- **2015–2017**: Weak IR detection → bypassed with printed photos or IR images.
- **2017–2019**: Spoofed with → 3D masks
- **CVE-2021-34466 (2021)**:
  - Attackers created a fake USB IR camera to inject fake infrared images.
  - Windows Hello trusted the device and unlocked the PC without the real person present.
- **Patched:** August 2021

➤Offline SAM extraction

- **Affected**: Windows XP → Windows 8
- **Technique**: By booting into WinPE/Linux, attackers copied:
  - C:\Windows\System32\config\SAM
  - SYSTEM hive
  - Then cracked NTLM hashes offline.
- **Impact**: Attackers could recover or crack all local passwords/escalate to admin.
- **Patched**: Harder with Windows 10 (2015+)

➤HiveNightmare (CVE-2021-36934)

- **Affected**: Windows 10 & early Windows 11
- Windows allowed normal users to read VSS of critical system files:
  - SAM (contains password hashes)
  - SYSTEM (BootKey used to decrypt the SAM file)
  - SECURITY (LSA secrets, cached credentials)
- **Impact**:
  - Attacker with low-privilege account can copy SAM, SYSTEM, SECURITY
- **Fix**: Microsoft corrected the file permissions

➤Privilege Escalation (CVE-2024-43583)

- **Technique**:
  - Winlogon runs some tasks with more privileges than it should.
  - A normal user can trigger these tasks and make Windows run their code with SYSTEM permissions.
  - So the attacker “rides” Winlogon’s extra privileges to become admin.
- **Impact**:
  - Full privilege escalation to SYSTEM
  - Complete control over the machine
  - Ability to install programs, read/modify data

THANK YOU