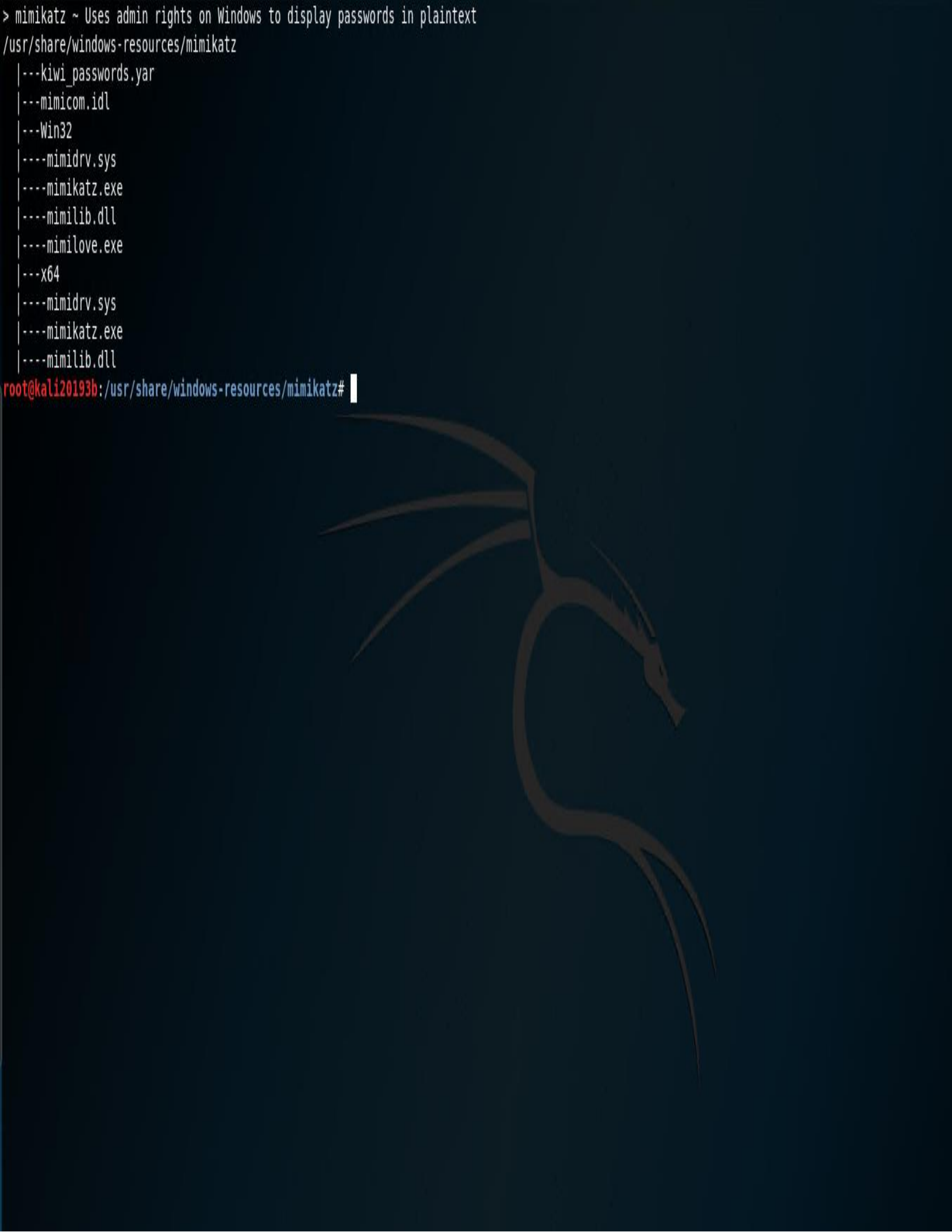

[*] exe2hex v1.5.1
Encodes an executable binary file into ASCII text format
Restore using DEBUG.exe (BATch - x86) or PowerShell (PoSh - x86/x64)
Quick Guide:
+ Input binary file with -s or -x
+ Output with -b and/or -p
Example:
$ /usr/bin/exe2hex -x /usr/share/windows-binaries/sbd.exe
$ /usr/bin/exe2hex -x /usr/share/windows-binaries/nc.exe -b /var/www/html/nc.txt -cc
$ cat /usr/share/windows-binaries/whoami.exe | /usr/bin/exe2hex -s -b debug.bat -p ps.cmd
Usage: exe2hex [options]
Options:
-h, --help show this help message and exit
-x EXE The EXE binary file to convert
-s Read from STDIN
-b BAT BAT output file (DEBUG.exe method - x86)
-p POSH PoSh output file (PowerShell method - x86/x64)
-e URL encode the output
-r TEXT pRefix - text to add before the command on each line
-f TEXT suFfix - text to add after the command on each line
-l INT Maximum HEX values per line
-c Clones and compress the file before converting (-cc for higher compression)
-t Create a Expect file, to automate to a Telnet session.
-w Create a Expect file, to automate to a WinEXE session.
-v Enable verbose mode
root@kali20193b:~#
POST EXPLOIT

```
> mimikatz ~ Uses admin rights on Windows to display passwords in plaintext
/usr/share/windows-resources/mimikatz
  |---kiwi_passwords.yar
  |---mimicom.idl
  |---Win32
  |----mimidrv.sys
  |----mimikatz.exe
  |----mimilib.dll
  |----mimilove.exe
  |---x64
  |----mimidrv.sys
  |----mimikatz.exe
  |----mimilib.dll
root@kali20193b:/usr/share/windows-resources/mimikatz#
```



```
> powersploit ~ PowerShell Post-Exploitation Framework
/usr/share/windows-resources/powersploit
  |---AntivirusBypass
  |---CodeExecution
  |---Exfiltration
  |---Mayhem
  |---Persistence
  |---PowerSploit.psd1
  |---PowerSploit.psm1
  |---Privesc
  |---README.md
  |---Recon
  |---ScriptModification
  |---Tests
root@kali20193b:/usr/share/windows-resources/powersploit#
```

- Download the latest source (version 3.1)
- ProxyChains HowTo (README)
- Public Forum
- ProxyChains project page at SourceForge
- Ezine articles about proxy servers (kind of humor)
- Proxy server search (try 1080 or 8080)

About proxychains tool:

* It's a proxifier.
* Latest version: 3.1
* Dedicated OS: Linux and other Unices.
* Allows TCP and DNS tunneling through proxies.
* Supports HTTP, SOCKS4 and SOCKS5 proxy servers.
* Different proxy types can be mixed in the same chain.
* Proxy chain: user-defined list of proxies chained together.

Usability :

* Run any program through proxy server.
* Access the Internet from behind a restrictive firewall.
* Hide your IP
* Run SSH, telnet, wget, ftp, apt, vnc, nmap through proxy servers.
* Access Intranets (192.168.*.*/10.*.*.*) from outside through reverse proxy.