Bônus

# Cibersegurança Ofensiva

## Automação de Segurança da Informação com Python

## 06– Black Hat Python

**LEONARDO LA ROSA**

Leonardo La Rosa

# Bio

# LEONARDO LA ROSA

**Mais de 25 Anos de Experiência nas áreas de TI e Cibersegurança, com atuação em diversos setores de mercado.**

Tecnólogo em Processamento de Dados pela UNIBAN
MBA em Gestão de Tecnologia da Informação pela FIAP

● C|EI ● SANS Foundations ● C|SCU ● N|SF ● C|ND ● C|EH MASTER ● C|SA ● E|CIH ● C|TIA ● CASE JAVA ● Lead Implementer ISO27701

- Cyber Security & Infrastructure Manager
- Docente na Pós Graduação de Cibersegurança
- Instrutor Certificado EC-Council
- Criador de conteúdo e Instrutor de treinamentos personalizados
- Speaker & Digital Influencer

POS | ACADI-TI

# Objetivo do módulo

| | |
|---|---|
| 1 | https://github.com/ytisf/PyExfil |
| 2 | https://nostarch.com/download/BHPCode.zip |
| 3 | https://github.com/dloss/python-pentest-tools |
| 4 | https://nostarch.com/download/ghpython_src.zip |
| 5 | https://github.com/proxyanon |
| 6 | https://github.com/PacktPublishing/Python-Penetration-Testing-Essentials-Second-Edition |
| 7 | https://github.com/PacktPublishing/Python-Penetration-Testing-Cookbook |
| 8 | https://github.com/PacktPublishing/Python-for-Offensive-PenTest |
| 9 | https://github.com/PacktPublishing/Hands-On-Penetration-Testing-with-Python |

600MB+ de scripts

# Black Hat Python

# Black Hat Python

Este módulo extra tem por objetivo agrupar as mais diversas ferramentas para Black Hat.

Utilize o conhecimento adquirido aqui com cuidado.

# Black Hat Python

- PyExfil é uma coletânea de ferramentas para exfiltração de dados, que abrange DNS, ICMP, HTTP, FTP, IMAP, NTP e muito mais

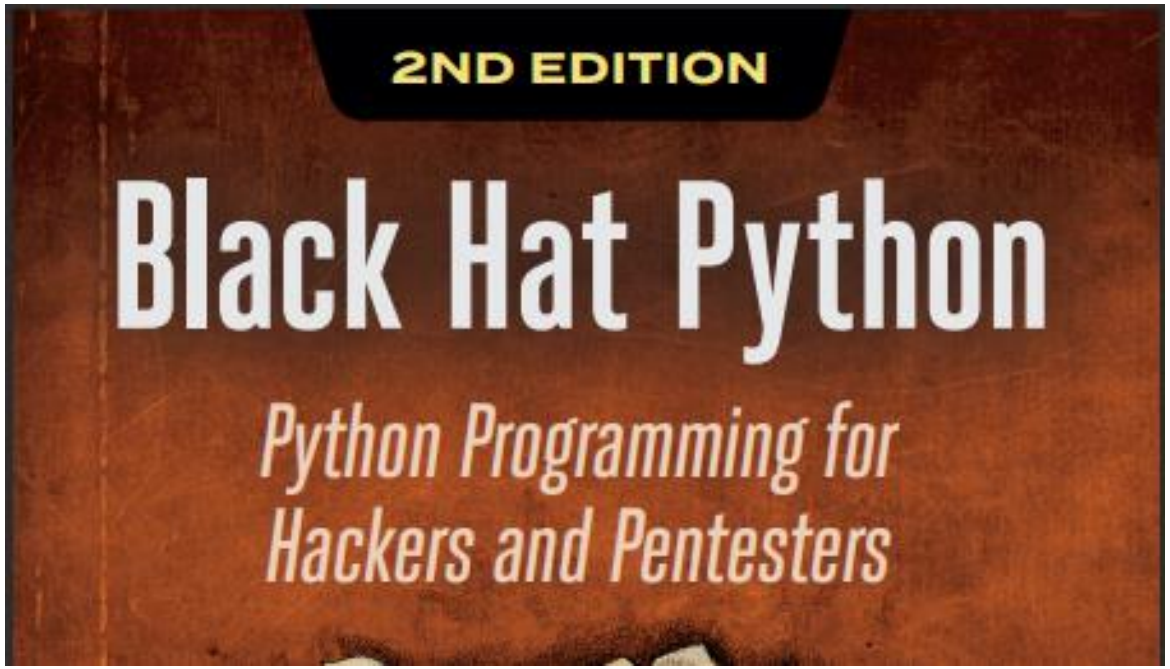

**Network**
**-** DNS query- HTTP Cookie- ICMP (8)- NTP Body- BGP Open- HTTPS Replace Certificate- QUIC - No Certificate- Slack Exfiltration- POP3 Authentication (as password)- FTP MKDIR - Idea thanks to Itzik Kotler- Source IP-based Exfiltration- HTTP Response- IMAP_Draft
**Communication**
- NTP Request- DropBox LSP (Broadcast or Unicast)- DNS over TLS- ARP Broadcast- JetDirect- GQUIC - Google Quick UDP Internet Connections (Client Hello)- MDNS Query - Can be used as broadcast.- AllJoyn. Name Service Protocol (IoT discovery) Version 0 ISAT.- PacketSize. Using size of packet rather than actual data.- UDP-Source-Port Using the source port in UDP as a transmission medium.- CertExchange Leveraging certificate exchange function for short bursts of communication.- DNSQ Leveraging DNS Queries for communication.
**Physical**
- Audio - No listener.- QR Codes- WiFi - On Payload
**Steganography**
- Binary Offset- Video Transcript to Dictionary- Braille Text Document- PNG Transparency- ZIPCeption

https://github.com/ytisf/PyExfil

# Black Hat Python

- Black Hat Python 2nd Edition é a versão mais nova deste best seller contendo várias ferramentas úteis para pentesters. A nova versão foi reescrita utilizando python 3.






**Chapter02**
-netcat.py-proxy.py-ssh_cmd.py-ssh_rcmd.py-ssh_server.py-tcp_client.py-tcp_server.py-udp_client.py
**Chapter03**
-scanner.py-sniffer.py-sniffer_ip_header_decode.py-sniffer_with_icmp.py
**Chapter04**
-arper.py-detector.py-mail_sniffer.py-mail_sniffer1.py-recapper.py
**Chapter05**
-bruter.py-mapper.py-wp_killer.py
**Chapter06**
-bhp_bing.py-bhp_fuzzer.py-bhp_wordlist.py
**Chapter07**
-config.json-dirlister.py-environment.py-github_trojan.py
**Chapter08**
-keylogger.py-sandbox_detect.py-screenshotter.py-shell_exec.py
**Chapter09**
-cryptor.py-email_exfil.py-exfil.py-paste_exfil.py-transmit_exfil.py
**Chapter10**
-file_monitor1.py-file_monitor2.py-process_monitor1.py-process_monitor2.py-bhservice.py-bhservice_task.vbs.txt
**Chapter11**
-aslrcheck.py

https://nostarch.com/download/BHPCode.zip

# Black Hat Python

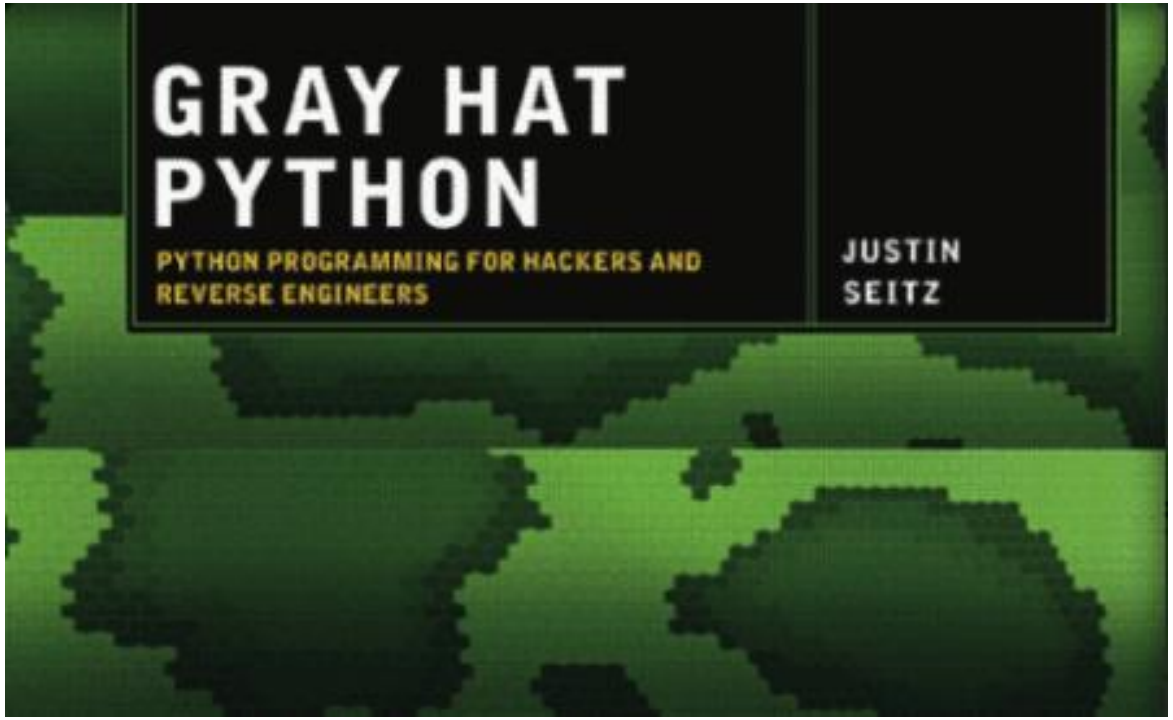
- A maioria das ferramentas listadas aqui são escritas em Python, outras são apenas vinculações Python para bibliotecas C existentes, ou seja, tornam essas bibliotecas facilmente utilizáveis a partir de programas Python. Todas sob a licença do MIT.

**Network**
-Knock Subdomain Scan-Spyse-SubBrute-Mallory-Pytbull-Spoodle-SMBMap-Habu
**Debugging and reverse engineering**
-Paimei-Immunity Debugger-mona.py-IDAPython-PyEMU-pefile-pydasm-PyDbgEng-uhooker-diStorm-Frida-python-ptrace-Androguard-Capstone-Keystone-PyBFDFuzzing-afl-python-Peach Fuzzing Platform -antiparser-untidy: general purpose XML fuzzer
**SMUDGE**
-Mistress-Fuzzbox: multi-codec media fuzzer-Forensic
**Fuzzing Tools**
-fuzzer.py (feliam)-FusilWeb-Ghost.py-spynner-python-spidermonkey-spidy
**Forensics**
-Volatility-pyew-pyClamAV-yara-python-phoneyc

https://github.com/dloss/python-pentest-tools

# Black Hat Python

- Apesar de conter muitos scripts na versão 2 de Python, os scripts de Gray Hat Python abrangem ferramentas Forenses, Fuzzing, Emuladores para sandbox em malware




-access_violation_handler.py-addnum.cpp-addnum.exe-addnum_function_call.py-backdoor.py-backdoor_shell.py-badchar.py-buffer_overflow.py-code_injector.py-cross_ref.py-dll_injector.py-file_fuzzer.py-file_hider.py-findinstruction.py-firefox_hook.py-func_coverage.py-ghp_inject.cpp-ghp_inject.dll-hippie_easy.py-injector.py-ioctl_dump.py-ioctl_fuzzer.py-my_debugger.py-my_debugger_defines.py-my_ioctl_fuzzer.py-my_test.py-printf_loop.py-printf_random.py-setup.py-stack_calc.py-sulley.zip-upx_unpacker.py

https://nostarch.com/download/ghpython_src.zip

# Black Hat Python

- Este é um repositório de um brasileiro com muitas ferramentas úteis para pentests desenvolvidas em Python



- admin_finder.py- batsploit.py- brouter.py- brute_any.py- crackpass.py- ddos_web.py- crack.py- keylogger.py- pdiscover.py- ransomware.py- socket_ddos_web.py- udp-flood.py- wd_generator.py- zCrack.py

https://github.com/proxyanon

# Black Hat Python

- Mai uma coletânea de um livro bem conhecido que está em sua segunda edição


connect_ex.pygetadd1.pyserver1.pyserver2.pyserver3.pyudp1.pyudptime1.pyudptime2.pyclient1.pyclient3.py.pyudp2.pycreatdicnew.pyips.pyiptcpscan.pyiptcpscan_t.pyiptcpscan_t_l.pynmap_python1.pyOS_detection.pyping_sweep.pyping_sweep_send_rec.pyping_sweep_th.pyping_sweep_th_l.pyport_scanner15.pyack.pyarpsp.pyarpspex.pyeth.pyfin.pyhalfopen.pynetdiss.pypingofd.pysniffer1.pysniffer_new.pysniffer_ttl.pystr1.pystruct1.pybanner.pydiv1.pyemail_finder.pyheader.pyinfo.pypar3.pyresult.txtwhois.pywhois5.pyDDOS_detect1.pymimp.pyparameter temp.py simp.py sisp.py

https://github.com/PacktPublishing/Python-Penetration-Testing-Essentials-Second-Edition

# Black Hat Python

- Mai uma coletânea de um livro bem conhecido que está em sua segunda edição




-download_image.py-download_image_p3.py-download_image_without_try_catch_p3 copy.py-download_image_without_try_catch_p3.py-html_table_parser.py-html_table_parser_p3.py-xml_parse.py-xml_parse_p3.py-item.py-middlewares.py-pipelines.py-settings.py-home.py-home2.py-ack-scanner.py-fin-scanner.py-network-scanner.py-port-scanner-default-ports-py3.py-port-scanner-default-ports.py-port-scanner-py3.py-port-scanner.py-syn-scanner.py-xmas-scanner.py-ack-scanner.py-basic-packet-sniffer-linux.py-basic-parse-packet-linux.py-pyshar_sample.py-pyshar_sniff.py-mitm-scapy.py-packet-layers.py-pcap-file-scapy.py-scapy-packet.py-scapy-sniffer.py-send-packet.py-sendp-packet.py-sr-packet.py-dictionary-attack-ssid.py-fake-access-point.py-sniff-hidden-ssid.py-sniff-ssid.py-ssidList.txt-wifi-sniff.py-arp-cache-poisoning.py-arp-monitor.py-arp-scanner.py-arp-spoofing-over-vlan.py-dhcp-starvation.py-mac-flooder.py-vlan-hopping.py-ip-spoof-ping.py-pass-sniffer.py-syn-flooding.py-exploit.py-exploit_bof.py

https://github.com/PacktPublishing/Python-Penetration-Testing-Cookbook

# Black Hat Python

- Outro livro recheado com diversos scripts desenvolvidos em python com foco em segurança ofensiva




DDNS Aware Shell.pyDirectory Navigation.pyLow Level Port Scanner.pyScreen Capturing.pySearching for Content.pyTweets Grabber.pyClipboard Hijacking.pyDNS_Poisoning.pyDumping Google Chrome Passwords .pyExercise -Firefox-Hooking.pyFirefox-Hooking.pyKeylogger.pyPhishing.zipSetup As Admin.pyHijacking IE - Shell Over IE.pyInteracting with Google Forms.pyInteracting with SourceForge.pyXOR Encryption.pyAre we Admin.pyBackdoor-ing Legitmate Windows Service.pyCreate a New Admin account.pyAES - Client - TCP Reverse Shell.pyAES - Server- TCP Reverse Shell.pyAES Stream.pyGenerate Keys.pyHybrid - Client - TCP Reverse Shell.pyHybrid - Server- TCP Reverse Shell.pyRSA - Client - TCP Reverse Shell.pyRSA - Server- TCP Reverse Shell.pyRSA ENC-DEC.py

https://github.com/PacktPublishing/Python-for-Offensive-PenTest

# Black Hat Python

- Outro livro recheado com diversos scripts desenvolvidos em python com foco em segurança ofensiva. São mais de 128MB com scripts.




Abstract.pyclass_methods.pycsv_parser.pyFile_access.pyiterators_pythonJoins_enumerate_terminate_processes.pyjson_parse.pyos_directories.pyProcess_demons.pypy.txtpython.txtThreads.pyThreads_join.py__init__.pyCj_detector.pyCsrf_automate.pyHSTS_detector.pyXss_automate.pyCj_detector.pyCsrf_automate.pyHSTS_detector.pysel.pyXss_automate.pyexploit.pyexploit_test.pyfuzz.pyexploit.pyexploit_test.pyexp_buf.pyfuzzer.pyfuzzer.pyfuzz_eip_jump.pyfuzz_exact_bytes.pyfuzz_exploit.pyfuzz_exploit_c.pyfuzz_exploit_final.pyfuzz_exploit_poc.pyfuzz_exploit_unix.pyfuzz_exploit_un_fuzz.pyfuzz_increased.pyfuzz_unique.pyexploit.pyfuzz.pyfuzzer.pyfuzz_eip_jump.pyfuzz_exact_bytes.pyfuzz_exploit.pyfuzz_exploit_c.pyfuzz_exploit_final.pyfuzz_exploit_poc.pyfuzz_exploit_unix.pyfuzz_exploit_un_fuzz.pyfuzz_increased.pyfuzz_unique.pytest.pyfuzzer.pyfuzz_eip_jump.pyfuzz_exact_bytes.pyfuzz_exploit.pyfuzz_exploit_c.pyfuzz_exploit_final.pyfuzz_exploit_poc.pyfuzz_exploit_unix.pyfuzz_exploit_un_fuzz.pyfuzz_increased.pyfuzz_unique.pyLFI_RFI.py

https://github.com/PacktPublishing/Hands-On-Penetration-Testing-with-Python

POS ACADI-TI

# OBRIGADO