快速安装

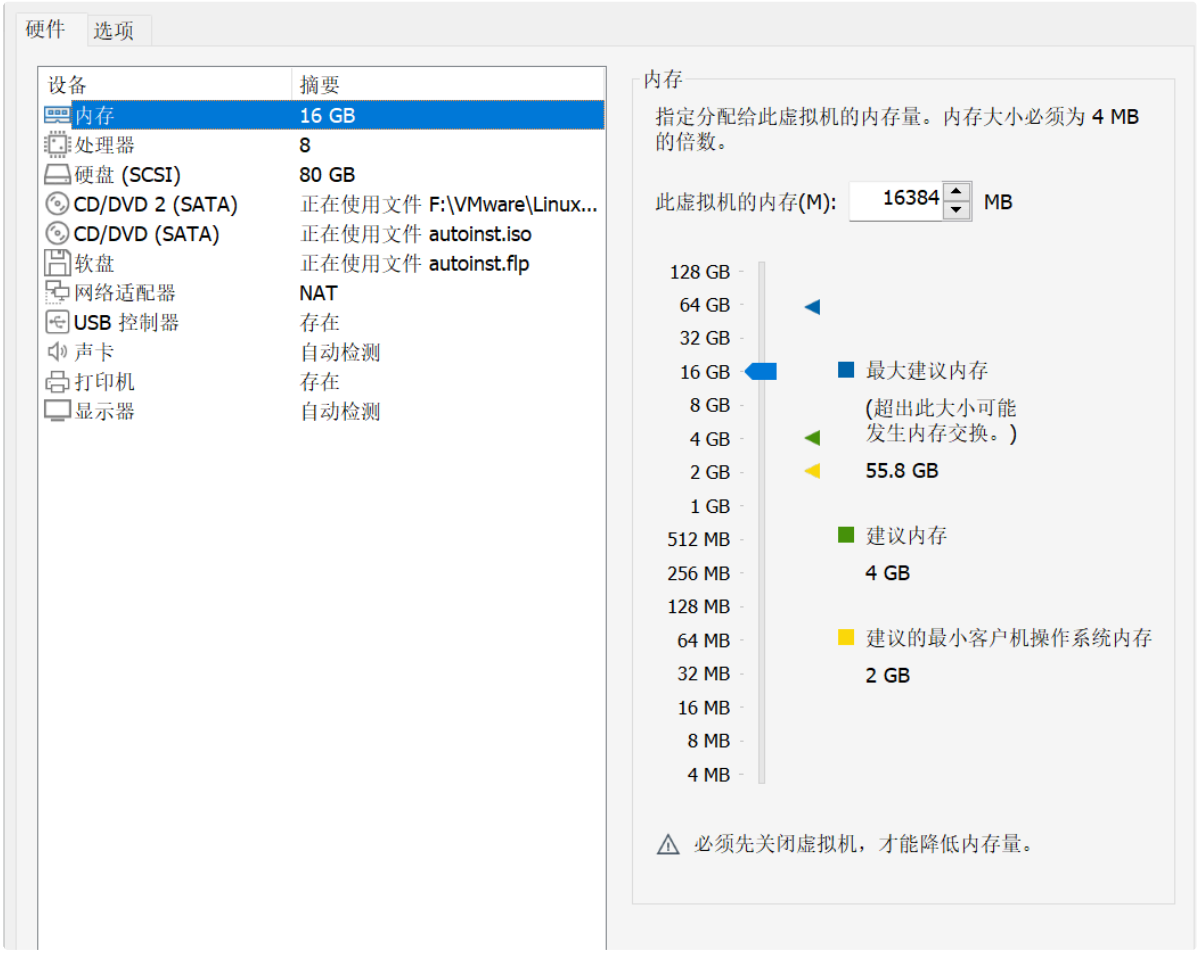
文件中分别有Ubuntu24.04_ovf.zip和Ubuntu24.04.zip文件，可以选择任意一个下载

Ubuntu24.04_ovf.zip文件解压后需要通过VMware导入ovf文件即可。 Ubuntu24.04.zip文件则解压通过VMware打开vmx文件即可。

其中iso文件夹中的iso文件，是Ubuntu24.04的系统镜像文件。

详细虚拟机教程可以自行查找学习。

注意：下载好虚拟机请自行修改CPU核心数和内存等，根据自己电脑配置修改即可。如遇到黑屏无法进入系统，可以关闭显示器设置里的加速3D图形



Github开源地址：

```
https://github.com/c0mentropy/CTF_Ubuntu24.04
```

下载链接：

```
通过百度网盘分享的文件：Ubuntu24.04_CTF
链接：https://pan.baidu.com/s/1OVxcDnNX6VmzNlku7m_tFQ?pwd=XAUT
提取码：XAUT
--来自百度网盘超级会员V3的分享
```

环境说明

这是一个基于Ubuntu24.04搭建的基础CTF环境，内置了web和pwn部分常用的工具，和LINUX基础工具等。**其中绝大部分工具都加载进了环境变量里，对新手使用非常友好。**

默认用户密码：

```
username: xaut
password: xaut
```

默认root密码：

```
username: root
password: XAUTCTF@
```

用户名密码大家可以自行修改。

特别说明：截止到我打包环境，我只想到了这些常用工具，后续有其他工具会再同步更新，或者大家也可以自行下载。而且为了避免环境太乱，所以只是大概测试了环境功能，如果有任何bug可以联系我，或自行修改。

工具列表速览

基础环境：

openssh-server gedit docker gcc g++ java8 java11 java17 java21 anaconda3 golang rust proxychains4 vscode tmux p7zip-full

PWN环境：

gdb pwndbg pwngdb gef seccomp_tools one_gadget ROPgagdet ropper glibc-all-in-one patchelf pwnScript pwncli pwntools alpha3 binwalk

WEB环境：

fscan nmap sqlmap msfconsole jDumpSpider fenjing impacket dirsearch john gobuster wfuzz faketime BloodHound searchsploit evil-winrm rogue_mysql_server ysoserial-all.jar kerbrute frp EarthWorm

MISC环境：

basecrack CyberChef wireshark stegosuite zsteg

CRYPTO环境：

gmpy2 pycryptodome pwntools sage

基础环境

openssh-server gedit docker gcc g++ java8 java11 java17 java21 anaconda3
golang rust proxychains4 vscode tmux 等

特殊说明：我在系统中加入了kali的源，方便使用apt下载一些kali上的工具

```
(base) ➜  ~ sudo apt update
[sudo] password for xaut:
Hit:1 http://downloads.metasploit.com/data/releases/metasploit-framework/apt lucid InRelease
Hit:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:3 http://http.kali.org/kali kali-rolling InRelease
Hit:4 https://debian.neo4j.com stable InRelease
Hit:5 http://mirrors.tuna.tsinghua.edu.cn/ubuntu noble InRelease
Hit:6 http://mirrors.tuna.tsinghua.edu.cn/ubuntu noble-updates InRelease
Hit:7 http://mirrors.tuna.tsinghua.edu.cn/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1062 packages can be upgraded. Run 'apt list --upgradable' to see them.
(base) ➜  ~
```

java：

java有常用的四个版本，可以切换需要的版本，也在bash里新增了对应四个版本的命令

```
(web) ➜  ~ java --version
openjdk 21.0.4 2024-07-16
OpenJDK Runtime Environment (build 21.0.4+7-Ubuntu-1ubuntu224.04)
OpenJDK 64-Bit Server VM (build 21.0.4+7-Ubuntu-1ubuntu224.04, mixed mode, sharing)
(web) ➜  ~ java8 -version
openjdk version "1.8.0_422"
OpenJDK Runtime Environment (build 1.8.0_422-8u422-b05-1~24.04-b05)
OpenJDK 64-Bit Server VM (build 25.422-b05, mixed mode)
(web) ➜  ~ java11 --version
openjdk 11.0.24 2024-07-16
OpenJDK Runtime Environment (build 11.0.24+8-post-Ubuntu-1ubuntu324.04.1)
OpenJDK 64-Bit Server VM (build 11.0.24+8-post-Ubuntu-1ubuntu324.04.1, mixed mode, sharing)
(web) ➜  ~ java17 --version
openjdk 17.0.12 2024-07-16
OpenJDK Runtime Environment (build 17.0.12+7-Ubuntu-1ubuntu224.04)
OpenJDK 64-Bit Server VM (build 17.0.12+7-Ubuntu-1ubuntu224.04, mixed mode, sharing)
(web) ➜  ~ java21 --version
openjdk 21.0.4 2024-07-16
OpenJDK Runtime Environment (build 21.0.4+7-Ubuntu-1ubuntu224.04)
OpenJDK 64-Bit Server VM (build 21.0.4+7-Ubuntu-1ubuntu224.04, mixed mode, sharing)
(web) ➜  ~
```

conda：

codna的python环境常用的有三个，分别为pwn、 web和crypto，其他环境为对应工具的**单独**环境，无需加载使用

```
codna activate web
codna activate pwn
codna activate crypto
```

```
(web) ➜  ~ conda activate pwn
(pwn) ➜  ~ conda env list
# conda environments:
#
alpha3                   /home/xaut/.conda/envs/alpha3
pwn                   *  /home/xaut/.conda/envs/pwn
web                      /home/xaut/.conda/envs/web
base                     /usr/local/anaconda3

(pwn) ➜  ~
```

proxychains4 :

proxychains4 的配置文件在 /etc/proxychains4.conf ， 可以直接使用 p4 接一个命令来走代理

```
p4 curl www.google.com
```

```
(base) ➜  ~ p4 curl [redacted]
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  [redacted]  ...  [redacted]  ...  OK
IP       : [redacted]
地址     : 日本  日本

数据二   : 日本

数据三   : 澳大利亚

URL      : [redacted]
(base) ➜  ~ ls -la /bin/p4
lrwxrwxrwx 1 root root 17 Aug 10 11:57 /bin/p4 -> /bin/proxychains4
(base) ➜  ~
```

language :

gcc & g++ & golang & rust :

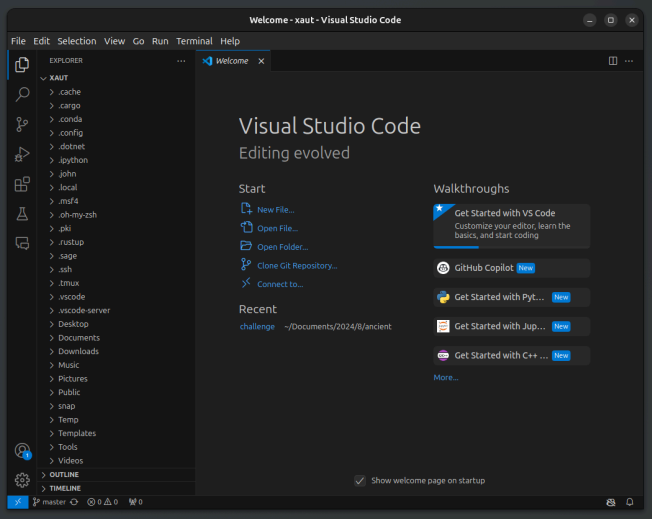
```
(base) ➜  ~ go version
go version go1.22.2 linux/amd64
(base) ➜  ~ rustc -V
rustc 1.80.1 (3f5fd8dd4 2024-08-06)
(base) ➜  ~
```

```
(base) ➜  ~ gcc -v                                                    11:48:25 [12/15]
Using built-in specs.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-linux-gnu/13/lto-wrapper
OFFLOAD_TARGET_NAMES=nvptx-none:amdgcn-amdhsa
OFFLOAD_TARGET_DEFAULT=1
Target: x86_64-linux-gnu
Configured with: ../src/configure -v --with-pkgversion='Ubuntu 13.2.0-23ubuntu4' --with-bugurl=file:///usr/share/doc/gcc-13/README.Bugs --enable-languages=c,ada,c++,go,d,fortran,objc,obj-c++,m2 --prefix=/usr --with-gcc-major-version-only --program-suffix=-13 --program-prefix=x86_64-linux-gnu- --enable-shared --enable-linker-build-id --libexecdir=/usr/libexec --without-included-gettext --enable-threads=posix --libdir=/usr/lib --enable-nls --enable-clocale=gnu --enable-libstdcxx-debug --enable-libstdcxx-time=yes --with-default-libstdcxx-abi=new --enable-libstdcxx-backtrace --enable-gnu-unique-object --disable-vtable-verify --enable-plugin --enable-default-pie --with-system-zlib --enable-libphobos-checking=release --with-target-system-zlib=auto --enable-objc-gc=auto --enable-multiarch --disable-werror --enable-cet --with-arch-32=i686 --wit
[0] 1:zsh*                                                  xaut-VMware-Virtual-Platform | Sat 2024
```

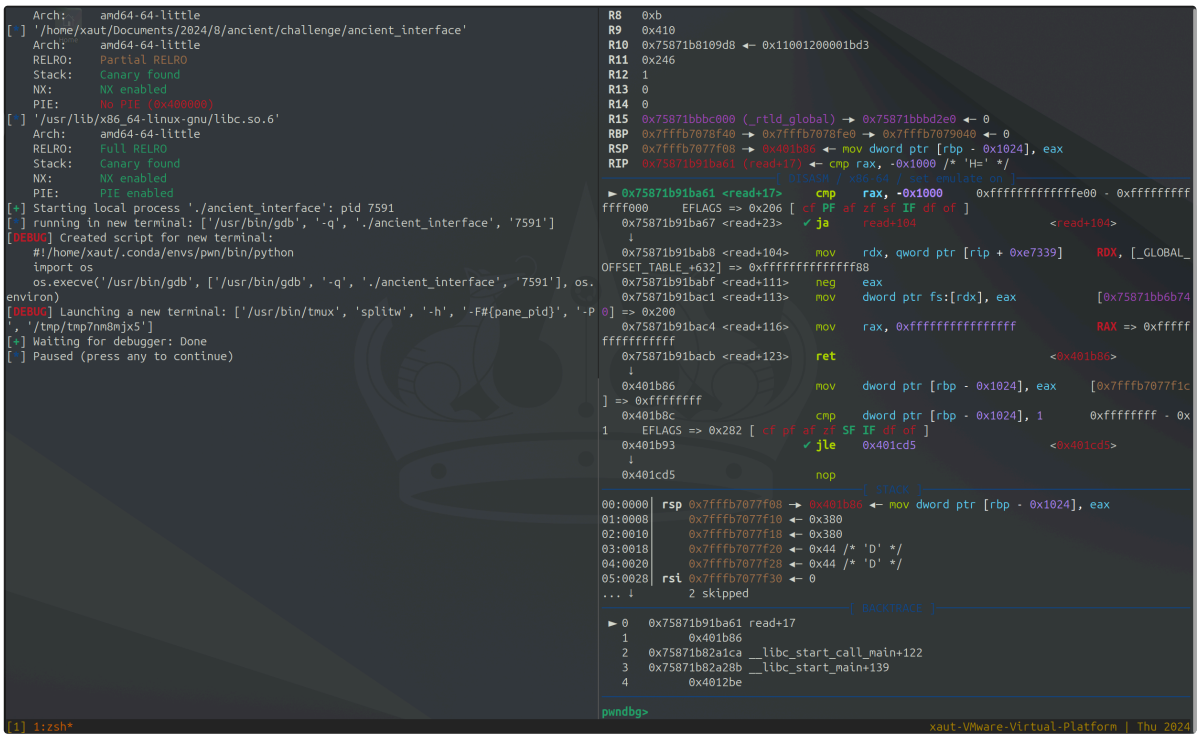
```
(base) ➜  ~ g++ -v                                                    11:48:34 [12/13]
Using built-in specs.
COLLECT_GCC=g++
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-linux-gnu/13/lto-wrapper
OFFLOAD_TARGET_NAMES=nvptx-none:amdgcn-amdhsa
OFFLOAD_TARGET_DEFAULT=1
Target: x86_64-linux-gnu
Configured with: ../src/configure -v --with-pkgversion='Ubuntu 13.2.0-23ubuntu4' --with-bugurl=file:///usr/share/doc/gcc-13/README.Bugs --enable-languages=c,ada,c++,go,d,fortran,objc,obj-c++,m2 --prefix=/usr --with-gcc-major-version-only --program-suffix=-13 --program-prefix=x86_64-linux-gnu- --enable-shared --enable-linker-build-id --libexecdir=/usr/libexec --without-included-gettext --enable-threads=posix --libdir=/usr/lib --enable-nls --enable-clocale=gnu --enable-libstdcxx-debug --enable-libstdcxx-time=yes --with-default-libstdcxx-abi=new --enable-libstdcxx-backtrace --enable-gnu-unique-object --disable-vtable-verify --enable-plugin --enable-default-pie --with-system-zlib --enable-libphobos-checking=release --with-target-system-zlib=auto --enable-objc-gc=auto --enable-multiarch --disable-werror --enable-cet --with-a$
```

vscode :

```
(pwn) ➜  ~ code .
(pwn) ➜  ~
```



tmux :



PWN环境

gdb pwndbg pwngdb gef seccomp_tools one_gadget ROPgagdet ropper glibc-all-in-one patchelf pwnScript pwncli pwntools alpha3 binwalk 等

conda activate pwn :

大部分工具均为python开发，所以使用pwn工具时建议进入pwn的python环境

```
conda activate pwn
```

gdb :

其中pwndbg和gef是**同一个功能**插件，如果需要切换，则需要修改~/.gdbinit文件里的注释即可。

```
(pwn) ➜  ~ cat ~/.gdbinit
#source ~/Tools/pwn_tools/gef/gef.py
source ~/Tools/pwn_tools/pwndbg/gdbinit.py
source ~/Tools/pwn_tools/Pwngdb/pwngdb.py
source ~/Tools/pwn_tools/Pwngdb/angelheap/gdbinit.py

define hook-run
python
import angelheap
angelheap.init_angelheap()
end
end
(pwn) ➜  ~
```

pwndbg

```
(pwn) ➜  ~ gdb
GNU gdb (Ubuntu 15.0.50.20240403-0ubuntu1) 15.0.50.20240403-git
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word".
pwndbg: loaded 163 pwndbg commands and 47 shell commands. Type pwndbg [--shell | --all] [filter] for a list.
pwndbg: created $rebase, $base, $bn_sym, $bn_var, $bn_eval, $ida GDB functions (can be used with print/break)
------- tip of the day (disable with set show-tips off) -------
Pwndbg sets the SIGLARM, SIGBUS, SIGPIPE and SIGSEGV signals so they are not passed to the app; see info signals for full GD
B signals configuration
pwndbg>
```

gef

这里将 pwndbg 写在 gef 前面可以同时加载两个工具，但我没这么试过，不知道会不会冲突。

```
(pwn) ➜  ~ gdb
GNU gdb (Ubuntu 15.0.50.20240403-0ubuntu1) 15.0.50.20240403-git
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word".
pwndbg: loaded 163 pwndbg commands and 47 shell commands. Type pwndbg [--shell | --all] [filter] for a list.
pwndbg: created $rebase, $base, $bn_sym, $bn_var, $bn_eval, $ida GDB functions (can be used with print/break)
GEF for linux ready, type `gef' to start, `gef config' to configure
93 commands loaded and 5 functions added for GDB 15.0.50.20240403-git in 0.00ms using Python engine 3.12
gef➤
```

ohterTools :

其他的就不一一展示了，使用如下：

```
(pwn) ➜  ~ seccomp-tools --version
SeccompTools Version 1.6.1
(pwn) ➜  ~ patchelf --version
patchelf 0.18.0
(pwn) ➜  ~ ROPgadget --version
Version:        ROPgadget v7.4
Author:         Jonathan Salwan
Author page:    https://twitter.com/JonathanSalwan
Project page:   http://shell-storm.org/project/ROPgadget/
(pwn) ➜  ~ ropper --version
Version: Ropper 1.13.8
Author: Sascha Schirra
Website: http://scoding.de/ropper

(pwn) ➜  ~ pwnScript --version
PwnScript: version 2.1.6
Author: Comentropy Ckyan
Email:  comentropy@foxmail.com
GitHub: https://github.com/c0mentropy/ckyan.pwnScript
(pwn) ➜  ~ pwncli --version
pwncli: version 1.6
author: roderick chan
github: https://github.com/RoderickChan/pwncli
(pwn) ➜  ~ one_gadget --version
OneGadget Version 1.9.0
(pwn) ➜  ~
```

alpha3 :

```
(pwn) ➜  challenge alpha3 --help
________________________________________________________________________________
      ,sSSs,,s,  ,sSSSs,    ALPHA3 - Alphanumeric shellcode encoder.
     dS"  Y$P"  YS"  ,SY    Version 1.0 alpha
    iS'   dY       ssS"     Copyright (C) 2003-2009 by SkyLined.
    YS,  dSb   SP,  ;SP     <berendjanwever@gmail.com>
    `"YSS'"S'  "YSSSY"      http://skypher.com/wiki/index.php/ALPHA3
________________________________________________________________________________

[Usage]
  ALPHA3.py  [ encoder settings | I/O settings | flags ]

[Encoder setting]
  architecture              Which processor architecture to target (x86,
                            x64).
  character encoding        Which character encoding to use (ascii, cp437,
                            latin-1, utf-16).
  casing                    Which character casing to use (uppercase,
                            mixedcase, lowercase).
  base address              How to determine the base address in the decoder
                            code (each encoder has its own set of valid
                            values).

[I/O Setting]
  --input="file"            Path to a file that contains the shellcode to be
                            encoded (Optional, default is to read input from
                            stdin).
  --output="file"           Path to a file that will receive the encoded
                            shellcode (Optional, default is to write output
                            to stdout).
```

binwalk :

```
(base) ➜  ~ binwalk --help

Binwalk v2.3.3+cddfede
Craig Heffner, ReFirmLabs
https://github.com/ReFirmLabs/binwalk

Usage: binwalk [OPTIONS] [FILE1] [FILE2] [FILE3] ...

Signature Scan Options:
    -B, --signature             Scan target file(s) for common file signatures
    -R, --raw=<str>             Scan target file(s) for the specified sequence of bytes
    -A, --opcodes               Scan target file(s) for common executable opcode signatures
    -m, --magic=<file>          Specify a custom magic file to use
    -b, --dumb                  Disable smart signature keywords
    -I, --invalid               Show results marked as invalid
    -x, --exclude=<str>         Exclude results that match <str>
    -y, --include=<str>         Only show results that match <str>

Extraction Options:
    -e, --extract               Automatically extract known file types
    -D, --dd=<type[:ext[:cmd]]>  Extract <type> signatures (regular expression), give the files an extens
ion of <ext>, and execute <cmd>
    -M, --matryoshka            Recursively scan extracted files
    -d, --depth=<int>           Limit matryoshka recursion depth (default: 8 levels deep)
    -C, --directory=<str>       Extract files/folders to a custom directory (default: current working di
rectory)
    -j, --size=<int>            Limit the size of each extracted file
    -n, --count=<int>           Limit the number of extracted files
    -0, --run-as=<str>          Execute external extraction utilities with the specified user's privileg
es
    -1, --preserve-symlinks     Do not sanitize extracted symlinks that point outside the extraction dir
```

WEB环境

fscan nmap sqlmap msfconsole jDumpSpider fenjing impacket dirsearch john gobuster wfuzz faketime BloodHound searchsploit evil-winrm rogue_mysql_server ysoserial-all.jar 等

具体使用如下：

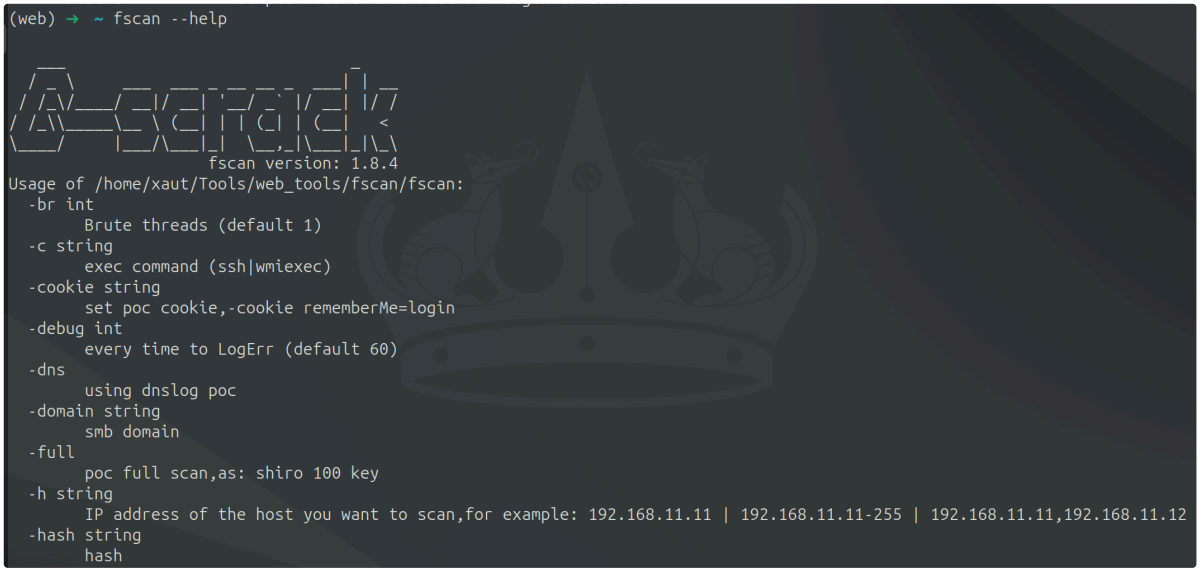
conda activate web :

大部分工具均为python开发，所以使用web工具时建议进入web的python环境

```
conda activate web
```

fscan :

（使用 fscan 的时候注意， fscan 会在使用目录生成一个result.txt）



nmap :

```
(web) ➜  ~ nmap --help
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```

sqlmap :

```
(web) ➜  ~ sqlmap --help
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.7.3#dev}
|_ -| . ["]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python sqlmap.py [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs
```

msfconsole :

```
(web) ➜  ~ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.21-dev-                         ]
+ -- --=[ 2440 exploits - 1256 auxiliary - 429 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

jDumpSpider :

使用注意名称jdumpspider

```
(web) ➜  Temp jdumpspider heapdump | grep "key = "
algMode = GCM, key = h3M6xnO9BPPO2NQjaNcx/A==, algName = AES
(web) ➜  Temp
```

fenjing :

```
(base) ➜  ~ fenjing --help
Usage: python -m fenjing [OPTIONS] COMMAND [ARGS]...

  click的命令组

Options:
  --help  Show this message and exit.

Commands:
  crack          攻击指定的表单
  crack-path     攻击指定的路径
  crack-request  从文本文件中读取请求并攻击目标，文本文件中用`PAYLOAD`标记payload插入位置
  scan           扫描指定的网站
  webui          启动webui
(base) ➜  ~
```

Impacket :

类型	脚本名	脚本介绍
远程执行	psexec.py	使用了RemComSvc的实现了PSEXEC功能的脚本。
远程执行	smbexec.py	类似PSECEX的执行方式，但未使用RemComSvc。这个脚本使用了一个本地SMB Server接收返回的结果，可以避免目标SMB没有可写的目录
远程执行	atexec.py	这个脚本通过MS-TSCH协议控制计划任务在目标机器上执行命令并获得回显
远程执行	wmiexec.py	通过WMI实现了半交互式的Shell，不需要在目标安装任何服务或软件。而且高度隐蔽的以管理员权限运行
远程执行	dcomexec.py	类似wmiexec.py的半交互式Shell，但是使用了DCOM接口，目前支持的接口有MMC20.Application、ShellWindows、ShellBrowserWindows
Kerberos协议	GetTGT.py	提供密码、hash或aeskey用来请求TGT并且保存为ccache格式
Kerberos协议	GetST.py	提供密码、hash、aeskey或ccache格式的TGT，可以请求服务票据并保存为ccache格式。如果提供的账户存在约束委派且支持协议转换，那么可以使用-impersonate选项模拟为其他用户请求票据
Kerberos协议	GetPac.py	这个脚本会为指定用户请求经过身份验证的PAC，通过使用MS-SFU协议的S4USelf和U2U的Kerberos认证实现
Kerberos协议	GetUserSPNs.py	这个脚本会找出和普通用户账户关联的SPN，输出格式与JtR和hashcat兼容
Kerberos协议	GetNPUsers.py	这个脚本会尝试获得并列出不需要Kerberos域认证(UF_DONT_REQUIRE_PREAUTH)的用户，输出和JtR兼容。
Kerberos协议	rbcd.py	这个脚本可以处理目标机器的msDS-AllowedToActOnBehalfOfOtherIdentity属性
Kerberos协议	ticketConverter.py	这个脚本可以在mimikatz常用的kirbi文件和Impacket常用的ccache文件之间进行转换
Kerberos协议	ticketer.py	这个脚本可以基于模板或自己创建金、银票据，并允许你自定义PAC_LOGON_INFO、groups、ExtraSids、duration等属性
Kerberos协议	raiseChild.py	这个脚本通过金票据和ExtraSids实现从子域到域森林的提权

类型	脚本名	脚本介绍
Windows 密码	secretsdump.py	提供各种技术以不运行任何程序远程dump密码。对SAM和LSA以及缓存的凭据，会尝试从目标注册表中读取并将hives保存在%SYSTEMROOT%\Temp目录，再将hives读取回来。对于DIT文件，会使用DL_DRSGetNCChanges函数来dump目标的NTLM hash、明文密码和Kerberos keys。也可以通过smbexec或wmiexec执行vssadmin得到NTDS.dit，并对其进行解密。这个脚本在服务不可用的情况下会打开对应的服务，例如远程注册表。在执行结束后，会将激活的服务还原。
Windows 密码	mimikatz.py	一个用来控制远程mimikatz RPC服务器的Shell，由@gentikiwi开发。

```
(web) ➜  ~ psexec.py --help
Impacket v0.12.0.dev1+20240807.21946.829239e3 - Copyright 2023 Fortra

usage: psexec.py [-h] [-c pathname] [-path PATH] [-file FILE] [-ts] [-debug] [-codec CODEC]
                 [-hashes LMHASH:NTHASH] [-no-pass] [-k] [-aesKey hex key] [-keytab KEYTAB]
                 [-dc-ip ip address] [-target-ip ip address] [-port [destination port]]
                 [-service-name service_name] [-remote-binary-name remote_binary_name]
                 target [command ...]

PSEXEC like functionality example using RemComSvc.

positional arguments:
  target                [[domain/]username[:password]@]<targetName or address>
  command               command (or arguments if -c is used) to execute at the target (w/o path) -
                        (default:cmd.exe)

options:
  -h, --help            show this help message and exit
  -c pathname           copy the filename for later execution, arguments are passed in the command
                        option
  -path PATH            path of the command to execute
  -file FILE            alternative RemCom binary (be sure it doesn't require CRT)
  -ts                   adds timestamp to every logging output
  -debug                Turn DEBUG output ON
  -codec CODEC          Sets encoding used (codec) from the target's output (default "utf-8"). If errors
                        are detected, run chcp.com at the target, map the result with
                        https://docs.python.org/3/library/codecs.html#standard-encodings and then
                        execute smbexec.py again with -codec and the corresponding codec
```

dirsearch :

```
(web) ➜  ~ dirsearch --help
/home/xaut/Tools/web_tools/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as a
n API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict
Usage: dirsearch.py [-u|--url] target [-e|--extensions] extensions [options]

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit

  Mandatory:
    -u URL, --url=URL   Target URL(s), can use multiple flags
    -l PATH, --urls-file=PATH
                        URL list file
    --stdin             Read URL(s) from STDIN
    --cidr=CIDR         Target CIDR
    --raw=PATH          Load raw HTTP request from file (use '--scheme' flag
                        to set the scheme)
    --nmap-report=PATH  Load targets from nmap report (Ensure the inclusion of
                        the -sV flag during nmap scan for comprehensive
                        results)
    -s SESSION_FILE, --session=SESSION_FILE
                        Session file
    --config=PATH       Path to configuration file (Default:
                        'DIRSEARCH_CONFIG' environment variable, otherwise
                        'config.ini')
```

john :

```
(web) ➜  web_tools john
John the Ripper password cracker, version 1.9.0
Copyright (c) 1996-2019 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single                  "single crack" mode
--wordlist=FILE --stdin   wordlist mode, read words from FILE or stdin
--rules                   enable word mangling rules for wordlist mode
--incremental[=MODE]      "incremental" mode [using section MODE]
--external=MODE           external mode or word filter
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
--status[=NAME]           print status of a session [called NAME]
--make-charset=FILE       make a charset, FILE will be overwritten
--show                    show cracked passwords
--test[=TIME]             run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..]      load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]    load users with[out] this (these) shell(s) only
--salts=[-]N              load salts with[out] at least N passwords only
--save-memory=LEVEL       enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL    this node's number range out of TOTAL count
```

gobuster :

```
(base) ➜  ~ gobuster --help
Usage:
  gobuster [command]

Available Commands:
  completion  Generate the autocompletion script for the specified shell
  dir         Uses directory/file enumeration mode
  dns         Uses DNS subdomain enumeration mode
  fuzz        Uses fuzzing mode. Replaces the keyword FUZZ in the URL, Headers and the request body
  gcs         Uses gcs bucket enumeration mode
  help        Help about any command
  s3          Uses aws bucket enumeration mode
  tftp        Uses TFTP enumeration mode
  version     shows the current version
  vhost       Uses VHOST enumeration mode (you most probably want to use the IP address as the URL paramet
er)

Flags:
      --debug                Enable debug output
      --delay duration       Time each thread waits between requests (e.g. 1500ms)
  -h, --help                 help for gobuster
      --no-color             Disable color output
      --no-error             Don't display errors
  -z, --no-progress          Don't display progress
  -o, --output string        Output file to write results to (defaults to stdout)
  -p, --pattern string       File containing replacement patterns
  -q, --quiet                Don't print the banner and other noise
  -t, --threads int          Number of concurrent threads (default 10)
  -v, --verbose              Verbose output (errors)
  -w, --wordlist string      Path to the wordlist. Set to - to use STDIN.
      --wordlist-offset int  Resume from a given position in the wordlist (defaults to 0)
```

wfuzz :

```
(wfuzz) ➜  Tools wfuzz -h
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
*                                                      *
* Version up to 1.4c coded by:                         *
* Christian Martorella (cmartorella@edge-security.com) *
* Carlos del ojo (deepbit@gmail.com)                   *
*                                                      *
* Version 1.4d to 3.1.0 coded by:                      *
* Xavier Mendez (xmendez@edge-security.com)            *
********************************************************

Usage:  wfuzz [options] -z payload,params <url>

        FUZZ, ..., FUZnZ  wherever you put these keywords wfuzz will replace them with the values of the s
pecified payload.
        FUZZ{baseline_value} FUZZ will be replaced by baseline_value. It will be the first request perform
ed and could be used as a base for filtering.


Options:
        -h                          : This help
        --help                      : Advanced help
        --version                   : Wfuzz version details
        -e <type>                   : List of available encoders/payloads/iterators/printers/scripts

        -c                          : Output with colors
        -v                          : Verbose information.
        --interact                  : (beta) If selected,all key presses are captured. This allows you to in
teract with the program.
```

faketime :

```
(base) ➜  ~ faketime --help

Usage: faketime [switches] <timestamp> <program with arguments>

This will run the specified 'program' with the given 'arguments'.
The program will be tricked into seeing the given 'timestamp' as its starting date and time.
The clock will continue to run from this timestamp. Please see the manpage (man faketime)
for advanced options, such as stopping the wall clock and make it run faster or slower.

The optional switches are:
  -m                 : Use the multi-threaded version of libfaketime
  -f                 : Use the advanced timestamp specification format (see manpage)
  --exclude-monotonic : Prevent monotonic clock from drifting (not the raw monotonic one)
  --disable-shm       : Disable use of shared memory by libfaketime.
  --date-prog PROG    : Use specified GNU-compatible implementation of 'date' program

Examples:
faketime 'last friday 5 pm' /bin/date
faketime '2008-12-24 08:15:42' /bin/date
faketime -f '+2,5y x10,0' /bin/bash -c 'date; while true; do echo $SECONDS ; sleep 1 ; done'
faketime -f '+2,5y x0,50' /bin/bash -c 'date; while true; do echo $SECONDS ; sleep 1 ; done'
faketime -f '+2,5y i2,0' /bin/bash -c 'date; while true; do date; sleep 1 ; done'
In this single case all spawned processes will use the same global clock
without restarting it at the start of each process.

(Please note that it depends on your locale settings whether . or , has to be used for fractions)

(base) ➜  ~
```

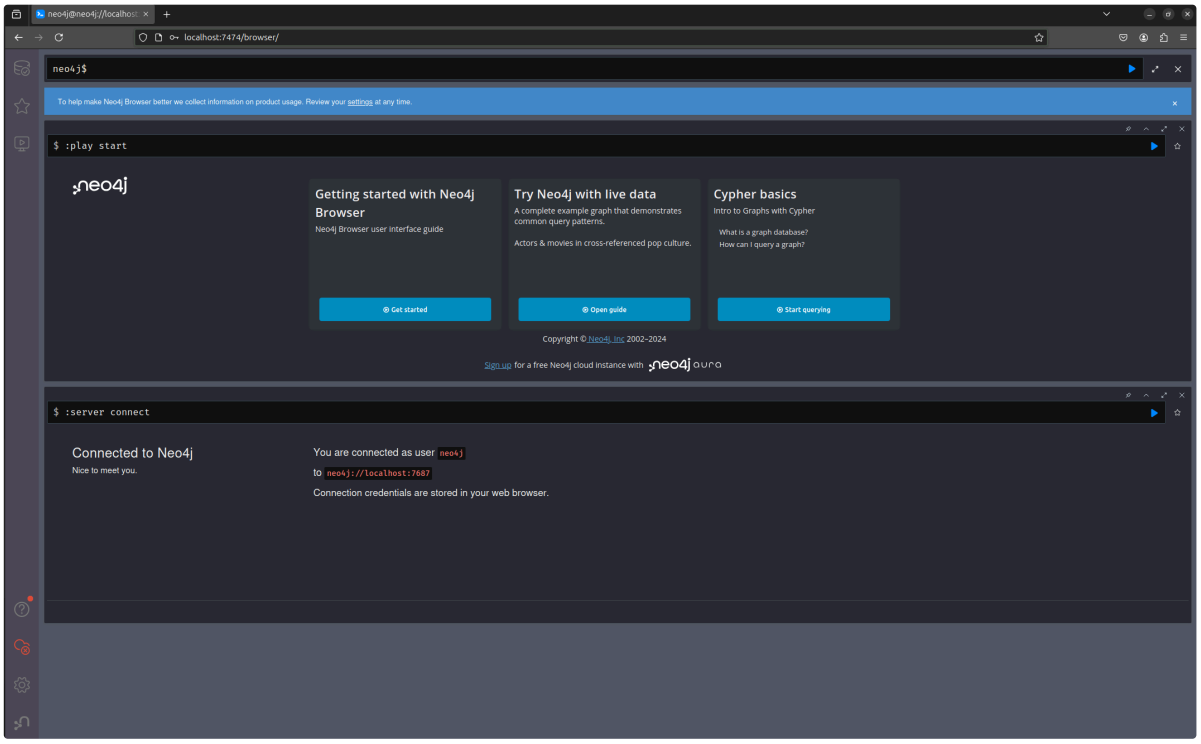
BloodHound :

neo4j

```
(base) ➜  ~ sudo neo4j console
Directories in use:
home:         /var/lib/neo4j
config:       /etc/neo4j
logs:         /var/log/neo4j
plugins:      /var/lib/neo4j/plugins
import:       /var/lib/neo4j/import
data:         /var/lib/neo4j/data
certificates: /var/lib/neo4j/certificates
licenses:     /var/lib/neo4j/licenses
run:          /var/lib/neo4j/run
Starting Neo4j.
2024-08-10 05:19:13.091+0000 INFO  Logging config in use: File '/etc/neo4j/user-logs.xml'
2024-08-10 05:19:13.126+0000 INFO  Starting...
2024-08-10 05:19:14.180+0000 INFO  This instance is ServerId{b4baea9d} (b4baea9d-8db3-4371-bccd-7b95462493
b4)
2024-08-10 05:19:15.612+0000 INFO  ======== Neo4j 5.22.0 ========
2024-08-10 05:19:17.949+0000 INFO  Anonymous Usage Data is being sent to Neo4j, see https://neo4j.com/docs
/usage-data/
2024-08-10 05:19:17.997+0000 INFO  Bolt enabled on localhost:7687.
2024-08-10 05:19:18.782+0000 INFO  HTTP enabled on localhost:7474.
2024-08-10 05:19:18.783+0000 INFO  Remote interface available at http://localhost:7474/
2024-08-10 05:19:18.786+0000 INFO  id: 2956E7988F8340747068728458AA2FC591A63CDC9FA46B5188F9811089CFD6CB
2024-08-10 05:19:18.786+0000 INFO  name: system
2024-08-10 05:19:18.787+0000 INFO  creationDate: 2024-08-10T05:19:16.71Z
2024-08-10 05:19:18.787+0000 INFO  Started.
```

访问网址：http://localhost:7474/browser/

用户名密码：neo4j/XAUTCTF@



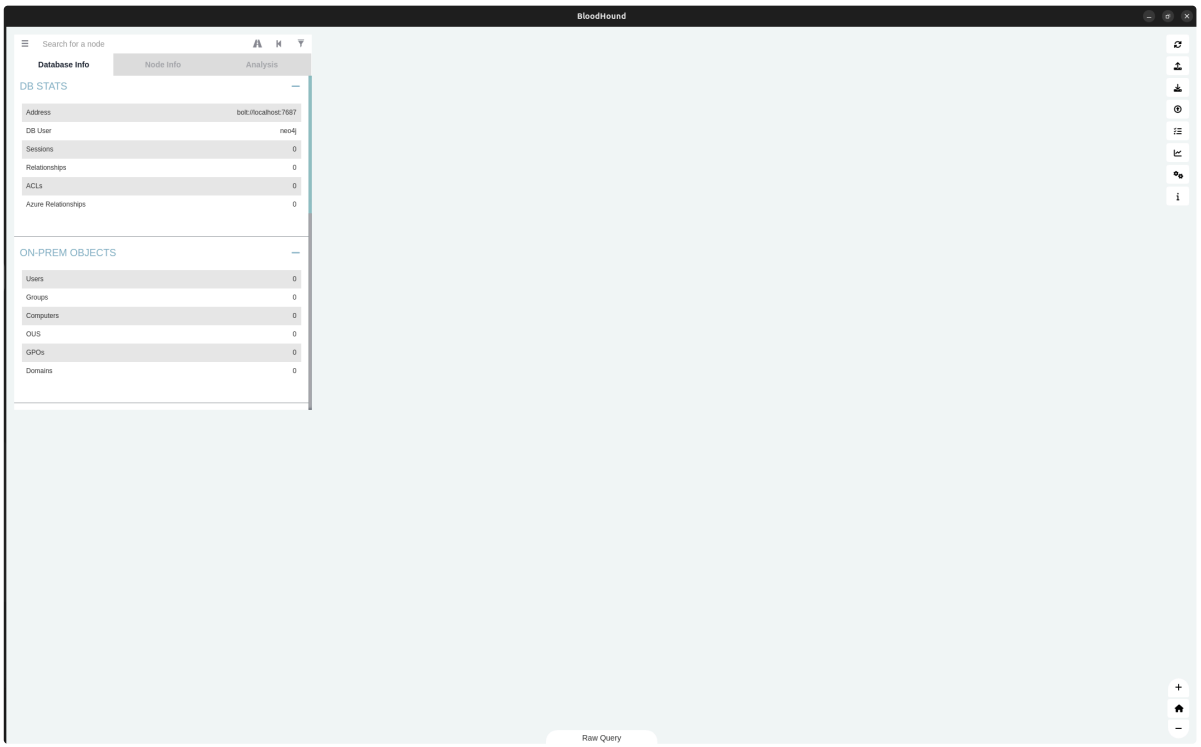
BloodHound

```
sudo neo4j start
```

```
(base) ➜  ~ sudo neo4j start
Directories in use:
home:         /var/lib/neo4j
config:       /etc/neo4j
logs:         /var/log/neo4j
plugins:      /var/lib/neo4j/plugins
import:       /var/lib/neo4j/import
data:         /var/lib/neo4j/data
certificates: /var/lib/neo4j/certificates
licenses:     /var/lib/neo4j/licenses
run:          /var/lib/neo4j/run
Starting Neo4j.
Started neo4j (pid:15462). It is available at http://localhost:7474
There may be a short delay until the server is ready.
(base) ➜  ~
```

```
bloodhound --no-sandbox
```

```
(base) ➜  ~ bloodhound --no-sandbox
(node:16006) electron: The default of contextIsolation is deprecated and will be changing from false to tr
ue in a future release of Electron.  See https://github.com/electron/electron/issues/23506 for more inform
ation
(node:16068) [DEP0005] DeprecationWarning: Buffer() is deprecated due to security and usability issues. Pl
ease use the Buffer.alloc(), Buffer.allocUnsafe(), or Buffer.from() methods instead.
```



bloodhound-python

```
(web) ➜  ~ bloodhound-python --help
usage: bloodhound-python [-h] [-c COLLECTIONMETHOD] [-d DOMAIN] [-v] [-u USERNAME] [-p PASSWORD] [-k]
                         [--hashes HASHES] [-no-pass] [-aesKey hex key]
                         [--auth-method {auto,ntlm,kerberos}] [-ns NAMESERVER] [--dns-tcp]
                         [--dns-timeout DNS_TIMEOUT] [-dc HOST] [-gc HOST] [-w WORKERS] [--exclude-dcs]
                         [--disable-pooling] [--disable-autogc] [--zip] [--computerfile COMPUTERFILE]
                         [--cachefile CACHEFILE] [--use-ldaps] [-op PREFIX_NAME]

Python based ingestor for BloodHound
For help or reporting issues, visit https://github.com/Fox-IT/BloodHound.py

options:
  -h, --help            show this help message and exit
  -c COLLECTIONMETHOD, --collectionmethod COLLECTIONMETHOD
                        Which information to collect. Supported: Group, LocalAdmin, Session, Trusts,
                        Default (all previous), DCOnly (no computer connections), DCOM, RDP,PSRemote,
                        LoggedOn, Container, ObjectProps, ACL, All (all except LoggedOn). You can
                        specify more than one by separating them with a comma. (default: Default)
  -d DOMAIN, --domain DOMAIN
                        Domain to query.
  -v                    Enable verbose output

authentication options:
  Specify one or more authentication options.
  By default Kerberos authentication is used and NTLM is used as fallback.
  Kerberos tickets are automatically requested if a password or hashes are specified.

  -u USERNAME, --username USERNAME
                        Username. Format: username[@domain]; If the domain is unspecified, the current
                        domain is used.
```

searchsploit :

```
(base) ➜  ~ searchsploit --help
  Usage: searchsploit [options] term1 [term2] ... [termN]

==========
 Examples
==========
  searchsploit afd windows local
  searchsploit -t oracle windows
  searchsploit -p 39446
  searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"
  searchsploit -s Apache Struts 2.0.0
  searchsploit linux reverse password
  searchsploit -j 55555 | jq
  searchsploit --cve 2021-44228

  For more examples, see the manual: https://www.exploit-db.com/searchsploit

=========
 Options
=========
## Search Terms
   -c, --case     [term]      Perform a case-sensitive search (Default is inSEnsITiVe)
   -e, --exact    [term]      Perform an EXACT & order match on exploit title (Default is an AND match on
 each term) [Implies "-t"]
                                e.g. "WordPress 4.1" would not be detect "WordPress Core 4.1")
   -s, --strict               Perform a strict search, so input values must exist, disabling fuzzy search
 for version range
                                e.g. "1.1" would not be detected in "1.0 < 1.3")
   -t, --title    [term]      Search JUST the exploit title (Default is title AND the file's path)
```

evil-winrm :

```
(base) ➜  Tools evil-winrm --help

Evil-WinRM shell v3.5

Usage: evil-winrm -i IP -u USER [-s SCRIPTS_PATH] [-e EXES_PATH] [-P PORT] [-p PASS] [-H HASH] [-U URL] [
-S] [-c PUBLIC_KEY_PATH ] [-k PRIVATE_KEY_PATH ] [-r REALM] [--spn SPN_PREFIX] [-l]
    -S, --ssl                        Enable ssl
    -c, --pub-key PUBLIC_KEY_PATH    Local path to public key certificate
    -k, --priv-key PRIVATE_KEY_PATH  Local path to private key certificate
    -r, --realm DOMAIN               Kerberos auth, it has to be set also in /etc/krb5.conf file using th
is format -> CONTOSO.COM = { kdc = fooserver.contoso.com }
    -s, --scripts PS_SCRIPTS_PATH    Powershell scripts local path
        --spn SPN_PREFIX             SPN prefix for Kerberos auth (default HTTP)
    -e, --executables EXES_PATH      C# executables local path
    -i, --ip IP                      Remote host IP or hostname. FQDN for Kerberos auth (required)
    -U, --url URL                    Remote url endpoint (default /wsman)
    -u, --user USER                  Username (required if not using kerberos)
    -p, --password PASS              Password
    -H, --hash HASH                  NTHash
    -P, --port PORT                  Remote host port (default 5985)
    -V, --version                    Show version
    -n, --no-colors                  Disable colors
    -N, --no-rpath-completion        Disable remote path completion
    -l, --log                        Log the WinRM session
    -h, --help                       Display this help message
(base) ➜  Tools
```

rogue_mysql_server :

```
(base) ➜  ~ rogue_mysql_server
INFO[2024-08-10 14:52:16] Server started at [0.0.0.0:3306]
INFO[2024-08-10 14:52:23] New client from addr [127.0.0.1:57430] logged in with username [root], database
 [mysql], ID [2]
INFO[2024-08-10 14:52:23] ==== ATTRS ====
INFO[2024-08-10 14:52:23] [_client_name]: [Go-MySQL-Driver]
INFO[2024-08-10 14:52:23] [_os]: [linux]
INFO[2024-08-10 14:52:23] [_platform]: [amd64]
INFO[2024-08-10 14:52:23] [_pid]: [24020]
INFO[2024-08-10 14:52:23] [_server_host]: [127.0.0.1]
INFO[2024-08-10 14:52:23] ===============
INFO[2024-08-10 14:52:23] Client from addr [127.0.0.1:57430], ID [2] try to query [SET NAMES utf8]
INFO[2024-08-10 14:52:23] Now try to read file [/etc/passwd] from addr [127.0.0.1:57430], ID [2]
INFO[2024-08-10 14:52:23] Read failed, file may not exist or empty in client
INFO[2024-08-10 14:52:23] Client leaved, Addr [127.0.0.1:57430], ID [2]
INFO[2024-08-10 14:52:23] New client from addr [127.0.0.1:57444] logged in with username [root], database
 [mysql], ID [3]
INFO[2024-08-10 14:52:23] ==== ATTRS ====
INFO[2024-08-10 14:52:23] [_client_name]: [Go-MySQL-Driver]
INFO[2024-08-10 14:52:23] [_os]: [linux]
INFO[2024-08-10 14:52:23] [_platform]: [amd64]
INFO[2024-08-10 14:52:23] [_pid]: [24020]
INFO[2024-08-10 14:52:23] [_server_host]: [127.0.0.1]
INFO[2024-08-10 14:52:23] ===============
INFO[2024-08-10 14:52:23] Client from addr [127.0.0.1:57444], ID [3] try to query [SET NAMES utf8]
INFO[2024-08-10 14:52:23] Now try to read file [/etc/passwd] from addr [127.0.0.1:57444], ID [3]
```

ysoserial-all.jar :

```
(base) ➜  ~ ysoserial
Y SO SERIAL?
Usage: java -jar ysoserial-[version]-all.jar [payload] '[command]'
  Available payload types:
Aug 10, 2024 3:08:25 PM org.reflections.Reflections scan
INFO: Reflections took 89 ms to scan 1 urls, producing 18 keys and 153 values
     Payload             Authors                               Dependencies

     -------             -------                               ------------

     AspectJWeaver       @Jang                                 aspectjweaver:1.9.2, commons-collections:
3.2.2
     BeanShell1          @pwntester, @cschneider4711           bsh:2.0b5

     C3P0                @mbechler                             c3p0:0.9.5.2, mchange-commons-java:0.2.11
```

kerbrute :

```
(base) ➜  ~ kerbrute --help

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 08/10/24 - Ronnie Flathers @ropnop

This tool is designed to assist in quickly bruteforcing valid Active Directory accounts through Kerberos
Pre-Authentication.
It is designed to be used on an internal Windows domain with access to one of the Domain Controllers.
Warning: failed Kerberos Pre-Auth counts as a failed login and WILL lock out accounts

Usage:
  kerbrute [command]

Available Commands:
  bruteforce    Bruteforce username:password combos, from a file or stdin
  bruteuser     Bruteforce a single user's password from a wordlist
  help          Help about any command
  passwordspray Test a single password against a list of users
  userenum      Enumerate valid domain usernames via Kerberos
  version       Display version info and quit

Flags:
      --dc string       The location of the Domain Controller (KDC) to target. If blank, will lookup via
DNS
      --delay int       Delay in millisecond between each attempt. Will always use single thread if set
  -d, --domain string   The full domain to use (e.g. contoso.com)
```

frp :

```
(base) ➜  frp_0.59.0_linux_amd64 ls -la
total 32008
drwxr-xr-x 2 xaut xaut     4096 Aug 10 16:02 .
drwxrwxr-x 3 xaut xaut     4096 Aug 10 15:58 ..
-rwxr-xr-x 1 xaut xaut 14483608 Jul  9 11:00 frpc
-rw-rw-r-- 1 xaut xaut      808 Aug 10 16:01 frpc.ini
-rw-r--r-- 1 xaut xaut      142 Jul  9 11:03 frpc.toml
-rwxr-xr-x 1 xaut xaut 18247832 Jul  9 11:00 frps
-rw-rw-r-- 1 xaut xaut      649 Aug 10 16:02 frps.ini
-rw-r--r-- 1 xaut xaut       16 Jul  9 11:03 frps.toml
-rw-r--r-- 1 xaut xaut    11358 Jul  9 11:03 LICENSE
(base) ➜  frp_0.59.0_linux_amd64 pwd
/home/xaut/Tools/web_tools/frp/frp_releases/frp_0.59.0_linux_amd64
(base) ➜  frp_0.59.0_linux_amd64
```

EarthWorm :

```
(base) ➜  ew git:(master) ✗ ls -la
total 540
drwxrwxr-x  3 xaut xaut   4096 Aug 10 16:04 .
drwxrwxr-x 22 xaut xaut   4096 Aug 10 16:04 ..
-rw-rw-r--  1 xaut xaut 200121 Aug 10 16:04 ew_for_Arm32
-rw-rw-r--  1 xaut xaut  32680 Aug 10 16:04 ew_for_Linux32
-rwxrwxr-x  1 xaut xaut  28080 Aug 10 16:04 ew_for_linux64
-rw-rw-r--  1 xaut xaut  34912 Aug 10 16:04 ew_for_MacOSX64
-rw-rw-r--  1 xaut xaut  56949 Aug 10 16:04 ew_for_Win.exe
-rw-rw-r--  1 xaut xaut 173604 Aug 10 16:04 ew_mipsel
drwxrwxr-x  8 xaut xaut   4096 Aug 10 16:04 .git
-rw-rw-r--  1 xaut xaut   6682 Aug 10 16:04 Readme.txt
(base) ➜  ew git:(master) ✗
```

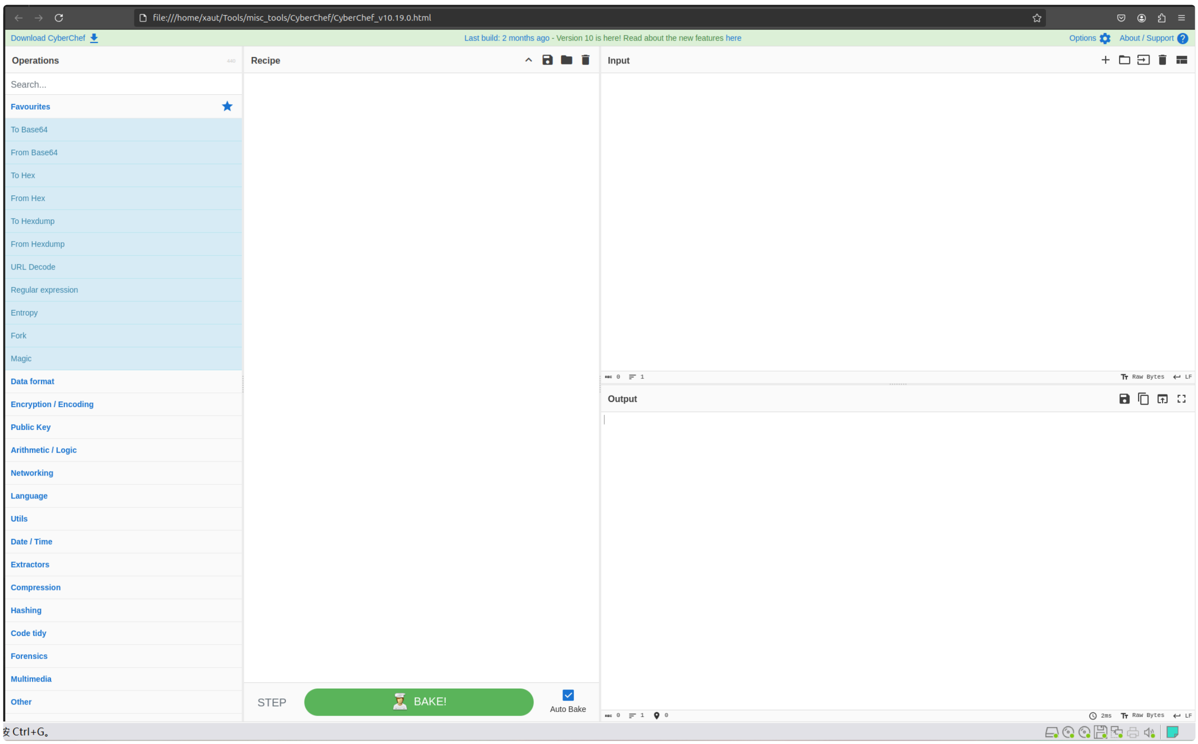
MISC环境

basecrack　CyberChef　wireshark　stegosuite　zsteg　等

basecrack：

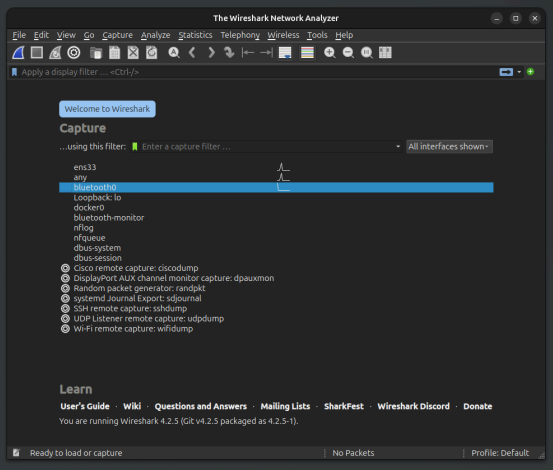
CyberChef：

```
file:///home/xaut/Tools/misc_tools/CyberChef/CyberChef_v10.19.0.html
```



wireshark :

```
(base) ➜  ~ sudo wireshark
 ** (wireshark:25720) 14:56:29.836112 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```



stegosuite :

```
(base) ➜  ~ stegosuite --help
Steganography tool to hide information in image files

Usage: stegosuite [-hV] [COMMAND]

Options:
  -h, --help      Show this help message and exit.
  -V, --version   Print version information and exit.

Commands:
  help      Displays help information about the specified command
  gui       Starts the GUI
  embed     Embeds data into image
  extract   Extracts data from image
  capacity  Shows the maximum amount of embeddable data

Example:
  stegosuite help embed            Displays help for stegosuite embed
(base) ➜  ~
```

zsteg :

```
(base) ➜  ~ zsteg --help
Usage: zsteg [options] filename.png [param_string]

    -a, --all                        try all known methods
    -E, --extract NAME               extract specified payload, NAME is like '1b,rgb,lsb'

Iteration/extraction params:
    -o, --order X                    pixel iteration order (default: 'auto')
                                     valid values: ALL,xy,yx,XY,YX,xY,Xy,bY,...
    -c, --channels X                 channels (R/G/B/A) or any combination, comma separated
                                     valid values: r,g,b,a,rg,bgr,rgba,r3g2b3,...
    -b, --bits N                     number of bits, single int value or '1,3,5' or range '1-8'
                                     advanced: specify individual bits like '00001110' or '0x88'
        --lsb                        least significant bit comes first
        --msb                        most significant bit comes first
    -P, --prime                      analyze/extract only prime bytes/pixels
        --shift N                    prepend N zero bits
        --invert                     invert bits (XOR 0xff)
        --pixel-align                pixel-align hidden data

Analysis params:
    -l, --limit N                    limit bytes checked, 0 = no limit (default: 256)

        --[no-]file                  use 'file' command to detect data type (default: YES)
        --no-strings                 disable ASCII strings finding (default: enabled)
    -s, --strings X                  ASCII strings find mode: first, all, longest, none
                                     (default: first)
    -n, --min-str-len X              minimum string length (default: 8)
```

CRYPTO环境

gmpy2 pycryptodome pwntools sage 等

conda activate crypto :

其中大部分python的包都在crypto这个环境里

```
1  conda activate crypto
```

```
(crypto) ➜  sage pip list | grep "gmpy2"
gmpy2                 2.2.1
(crypto) ➜  sage pip list | grep "pycryptodome"
pycryptodome          3.20.0
(crypto) ➜  sage pip list | grep "pwntools"
pwntools              4.12.0
(crypto) ➜  sage
```

sage :

sage是单独装在conda activate sage里的

```
(crypto) ➜  sage conda activate sage
(sage) ➜  sage sage
 ┌────────────────────────────────────────────────────────────────────┐
 │ SageMath version 10.3, Release Date: 2024-03-19                    │
 │ Using Python 3.12.4. Type "help()" for help.                       │
 └────────────────────────────────────────────────────────────────────┘
sage: help()
Welcome to Sage 10.3!

To view the Sage tutorial in your web browser, type "tutorial()", and
to view the (very detailed) Sage reference manual, type "manual()".
For help on any Sage function, for example "matrix_plot", type
"matrix_plot?" to see a help message, type "help(matrix_plot)" to see
a very similar message, type "browse_sage_doc(matrix_plot)" to view a
help message in a web browser, and type "matrix_plot??" to look at the
function's source code.

(When you type something like "matrix_plot?", "help(matrix_plot)", or
"matrix_plot??", Sage may start a paging program to display the
requested message. Type a space to scroll to the next page, type "h"
to get help on the paging program, and type "q" to quit it and return
to the "sage:" prompt.)
```

写在最后

我想说的是，在我第一次接触CTF的时候，配环境真的是很烦很痛苦的一个环节。以至于我差点放弃。所以我有了打包一个基础的LINUX环境，让各位可以先跳过这个环节，之后再一点一点慢慢学习。加油各位，希望可以在CTF这条路上陪大家走得更久！

对了，如果有**PWN方向**疑问可以和我一起讨论学习！！ （在Documents目录里给大家留了一道题，感兴趣可以自己做一下哦~）

作者：ckyan

创建日期：2024.08.02

更新日期：2024.08.10