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。

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。

基础环境

openssh-server gedit docker java8 java11 java17 java21 anaconda3 proxychains4

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) ➜  ~
```

codna的python环境常用的有两个为pwn和web，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
```

```
(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
```

```
(pwn) ➜  ~ p4 curl
[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  ...                  ...                  ...  OK
IP       :
地址     : 美国  美国

数据二   : 美国

数据三   : 美国加利福尼亚

URL      :
(pwn) ➜  ~
```

PWN环境

gcc g++ gdb pwndbg pwndgdb gef seccomp_tools one_gadget ROPgagdet ropper glibc-all-in-one patchelf pwnScript pwncli

pwntools

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 :

```
(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".
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 0.01ms using Python engine 3.12
gef➤
```

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) ➜  ~
```

WEB环境

fscan nmap sqlmap msfconsole jDumpSpider

具体使用如下：

fscan：

```
(web) ➜ ~ fscan --help

   ___                              _
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 1.8.4
Usage of /home/xaut/Tools/web_tools/fscan/fscan:
  -br int
        Brute threads (default 1)
  -c string
        exec command (ssh|wmiexec)
  -cookie string
        set poc cookie,-cookie rememberMe=login
  -debug int
        every time to LogErr (default 60)
  -dns
        using dnslog poc
  -domain string
        smb domain
  -full
        poc full scan,as: shiro 100 key
  -h string
        IP address of the host you want to scan,for example: 192.168.11.11 | 192.168.11.11-255 | 192.168.11.11,192.168.11.12
  -hash string
        hash
```

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 :

```
(base) ➜  Temp jdump_spider ./heapdump
=============================================
SpringDataSourceProperties
-------------
not found!

=============================================
WeblogicDataSourceConnectionPoolConfig
-------------
not found!

=============================================
MongoClient
-------------
not found!

=============================================
AliDruidDataSourceWrapper
-------------
not found!

=============================================
HikariDataSource
-------------
not found!

=============================================
RedisStandaloneConfiguration
-------------
not found!

=============================================
JedisClient
-------------
not found!

=============================================
CookieRememberMeManager(ShiroKey)
-------------
algMode = GCM, key = h3M6xnO9BPPO2NQjaNcx/A== algName = AES

=============================================
```

MISC环境

basecrack

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！！

作者：ckyan

日期：2024.08.02