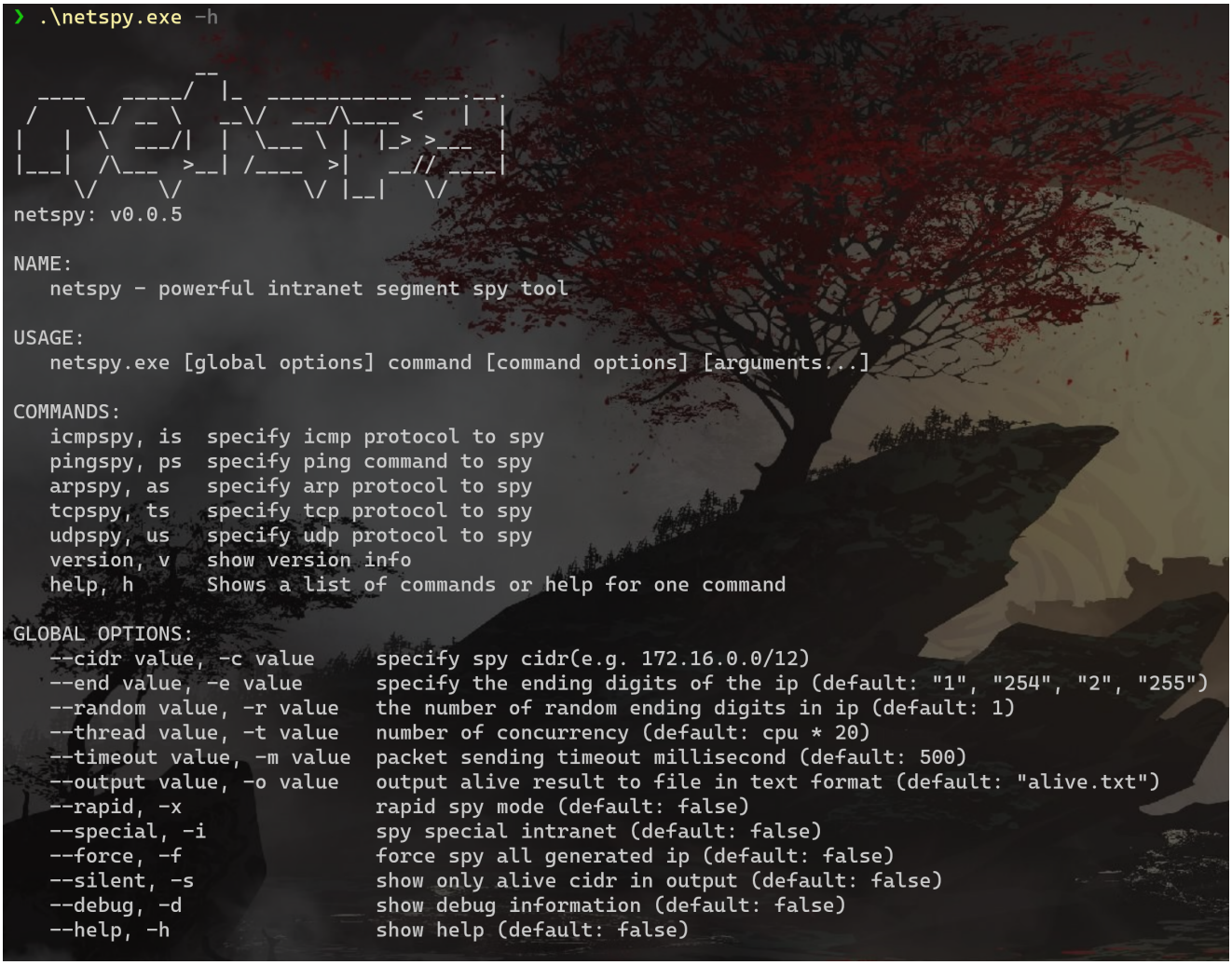
GitHub - shmilylty/netspy: netspy是一款快速探测内网可达网段工具（深信服深蓝实验室天威战队强力驱动）

github.com/shmilylty/netspy

shmilylty

✨ 项目简介

🦄 netspy是一款快速探测内网可达网段工具（深信服深蓝实验室天威战队强力驱动）



当我们进入内网后想要扩大战果，那我们可能首先想知道当前主机能通哪些内网段。

netspy正是一款应用而生的小工具，体积较小，速度极快，支持跨平台，支持多种协议探测，希望能帮到你！

🚀 快速使用

1. 查看帮助信息

```
netspy -h
```

2. 使用icmpspy模块进行探测

   使用icmpspy模块进行自动探测，自动探测网段为："192.168.0.0/16", "172.16.0.0/12", "10.0.0.0/8"。

```
netspy is
```

   注：当没有权限发送icmp包时可以尝试使用pingspy模块。

3. 使用arpspy模块进行探测

   指定使用eth0网络接口进行arp协议探测，探测网段为192.168.0.0/16和59.192.0.0/10。

```
netspy -c 192.168.0.0/16 -c 59.192.0.0/10 as -i eth0
```

4. 使用tcpspy模块进行探测

```
netspy ts -p 22 -p 3389
```

   注：如果不指定-p参数，netspy默认探测21, 22, 23, 80, 135, 139, 443, 445, 3389, 8080端口。

5. 使用udpspy模块进行探测

```
netspy us -p 53 -p 137
```

   注：如果不指定-p参数，netspy默认探测53, 123, 137, 161, 520, 523, 1645, 1701, 1900, 5353端口。

6. 使用icmpspy模块强制进行段内所有IP存活探测

```
netspy -c 192.168.91.0/24 -r 255 -f is
```

7. 使用icmpspy模块急速探测模式

```
 netspy -x is
```

   注：急速模式协程数量为cpu核数*40，只探测段内网关。

😸 帮助信息

```
                __
  ____   _____/  |_  ____________ ___.__.
 /    \_/ __ \   __\/  ___/\____ <   |  |
|   |  \  ___/|  |  \___ \ |  |_> >___  |
|___|  /\___  >__| /____  >|   __// ____|
     \/     \/          \/ |__|   \/
netspy: v0.0.5

NAME:
   netspy - powerful intranet segment spy tool

USAGE:
   netspy.exe  [global options] command [command options] [arguments...]

COMMANDS:
   icmpspy, is   使用icmp协议探测
   pingspy, ps   使用ping命令探测
   arpspy,  as   使用arp协议探测
   tcpspy,  ts   使用tcp协议探测
   udpspy,  us   使用udp协议探测
   version, v    显示版本信息
   help, h       显示帮助信息

GLOBAL OPTIONS:
   --cidr value, -c value     指定探测CIDR(例如: 172.16.0.0/12)
   --end value, -e value      指定IP末尾数字(默认: 1, 254, 2, 255)
   --random value, -r value   IP随机末尾数字的个数(默认: 1)
   --thread value, -t value   并发数量(默认: cpu * 20)
   --timeout value, -m value  发包超时毫秒(默认: 100)
   --output value, -o value   存活网段结果保存路径(默认: "alive.txt")
   --rapid, -x                急速探测模式(默认: false)
   --special, -i              是否探测特殊内网(默认: false)
   --force value, -f value    强制探测所有生成的IP(默认: false)
   --silent, -s               只显示存活网段(默认: false)
   --debug, -d                显示调试信息(默认: false)
   --help, -h                 显示帮助信息(默认: false)
```

🏄 计划功能

- 支持多种协议探测
- 支持自定义网段探测
- 支持探测特殊内网
- 支持探测段内所有主机
- 支持探测进度显示

欢迎反馈贴近实战的建议！

🐱 鸣谢

感谢网上开源的相关项目！

📜 免责声明

本工具仅能在取得足够合法授权的企业安全建设中使用，在使用本工具过程中，您应确保自己所有行为符合当地的法律法规。 如您在使用本工具的过程中存在任何非法行为，您将自行承担所有后果，本工具所有开发者和所有贡献者不承担任何法律及连带责任。 除非您已充分阅读、完全理解并接受本协议所有条款，否则，请您不要安装并使用本工具。 您的使用行为或者您以其他任何明示或者默示方式表示接受本协议的，即视为您已阅读并同意本协议的约束。

💞Star趋势