Byte by Byte Brute Force attack

version：*1.0*

Last update：*March 27, 2019*

1 与远程服务器通信代码

编译程序：

```
$ gcc -o exploit exploit.c
```

打开终端，进入当前目录，执行一下指令：

```
$ ./exploit -v 114.212.85.254
```

2 暴力破解 canary 攻击

修改 exploit 程序，暴力破解 Canary。

3 文章阅读

阅读文章列表 Stack Guard：Cowan et al. (1998), BruteForceAttack：Bittau et al. (2014),RAF:Marco-Gisbert and Ripoll (2013), DyanGuardPetsios et al. (2015), Polymorphic CanaryWang et al. (2018)。

参考文献

Bittau, Andrea, Adam Belay, Ali Mashtizadeh, David Mazières, and Dan Boneh, “Hacking blind,” in “2014 IEEE Symposium on Security and Privacy” IEEE 2014, pp. 227–242.

Cowan, Crispan, Calton Pu, Dave Maier, Jonathan Walpole, Peat Bakke, Steve Beattie, Aaron Grier, Perry Wagle, Qian Zhang, and Heather Hinton, “Stackguard: Automatic adaptive detection and prevention of buffer-overflow attacks.,” in “USENIX Security Symposium,” Vol. 98 San Antonio, TX 1998, pp. 63–78.

Marco-Gisbert, Hector and Ismael Ripoll, “Preventing brute force attacks against stack canary protection on networking servers,” in “2013 IEEE 12th International Symposium on Network Computing and Applications” IEEE 2013, pp. 243–250.

Petsios, Theofilos, Vasileios P Kemerlis, Michalis Polychronakis, and Angelos D Keromytis, “Dynaguard: Armoring canary-based protections against brute-force attacks,” in “Proceedings of the 31st Annual Computer Security Applications Conference” ACM 2015, pp. 351–360.

Wang, Z., X. Ding, C. Pang, J. Guo, J. Zhu, and B. Mao, “To Detect Stack Buffer Overflow with Polymorphic Canaries,” in “2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN),” Vol. 00 Jun 2018, pp. 243–254.