

# How to Hack Like a Pornstar

*Master the secrets of hacking through real-life hacking scenarios*

*通过现实生活中的黑客场景掌握黑客攻击的秘密*

**Copyright © 2017 Sparc FLOW**

**本书籍由0penSec内部翻译，在不侵害原版权商和原作者的前提下，进行翻译仅供内部学习使用，其他方式的复制、分发传播请遵守原版权商的约定。**

**译者：两块（0penSec）**

版权所有。未经出版商事先书面许可，不得以任何形式或方式（包括影印，录制或其他电子或机械方法）复制、分发或传播本出版物的任何部分，除非有简短的引用。在严格审查和版权法允许的某些其他非商业用途。

**ISBN** 978-1-5204-7851-7

# 前言

这不是一本关于信息安全的书，当然也不是关于IT方面的书籍。这是一本关于黑客攻击的书，具体来说，如何渗透进入某一公司的网络，找到他们最关键的数据，并在不触发公司浪费预算而购置的任何亮眼的新安全措施(工具)的情况下窃取数据。

无论你是一个崇尚道德的黑客，还是一个因过时的书籍和虚假媒体报道而感到沮丧被挫败的爱好者，这本书绝对适合你。

我们将设置一个虚假但足够现实的目标，并详细介绍渗透入公司的主要步骤：构建网络钓鱼恶意软件，查找漏洞，扎根Windows域，获取大型机权限等。

我几乎记录了本书中使用的所有工具和自定义脚本。我强烈建议您在您可控制和自己拥有的环境中测试并掌握它们的功能（和限制）。考虑到这本书的性质，期望它涵盖所有可以想象的每一种黑客技术是荒谬的，尽管我会尽力提供尽可能多的例子，同时坚持本书的既定目的。

我将通过简要解释它们如何工作以及它们在黑客场景中的含义来简述一些像IPSEC，TOR和NTLM这样的概念。如果您想要深入了解，我强烈建议您按照我在每个项目附近提供的链接，探索每种技术和工具背后的黑暗、有趣的概念。

***Note:*** *本书中记录的自定义脚本和特殊命令可以在[www.hacklikeapornstar.com](http://www.hacklikeapornstar.com)上公开获得。*

# 重要免责声明

本书中的例子完全是虚构的。提供的工具和技术是开源的，因此可供所有人使用。Pentesters经常在测试工作任务中使用它们，但攻击者也是如此。如果您最近遭受了攻击，并找到了本书中所示的技术或工具，那么这绝不会导致本书的作者入罪，也不会暗示作者与犯罪者之间存在任何联系。

与本书中包含的内容相关的任何行动和或活动完全由您自己负责。滥用本书中的信息可能会导致对相关人员提起刑事指控。如果对任何滥用本书信息的人违反法律规定提起任何刑事指控，作者将不承担任何责任。

本书不会促进黑客攻击，软件破解或盗版。本书中提供的所有信息仅用于教育目的。它将帮助公司保护其网络免受所提出的攻击，并将帮助调查人员评估在事件期间收集的证据。

**未经计算机系统所有者书面许可授权，执行任何黑客攻击或测试都是非法的。**

# 安全第一

*“I am a blank slate – therefore I can create anything I want.”*

***Tobey Maguire***

如果有一个部分是大多数黑客书籍和博客文章目前忽视的话，那就是关于黑客攻击的“保持安全”部分。换句话说，他们没有详细说明典型黑客可以用来保证一定程度的匿名性和安全性的方案和技术。你可能是世界上最好的黑客，但是如果你无法控制你在互联网上的足迹并正确地擦除你的踪迹，你就会崩溃和被烧伤。

因此，在尝试新技术之前，我们将详细介绍如何堆叠安全层以确保最大程度的保护。如果您想立即开始黑客攻击，请随意跳转到第3节，但请确保您以后有时间再阅读此部分。

## 白板

最有效的黑客安全规则可以用七个词来概括：“每次都从头开始”。通过“从头开始”，我的意思是为每次攻击获得一台新计算机、新热点、新IP地址和新服务器。调查人员将寻找攻击之间的共同模式。他们会尝试将小证据拼凑在一起，以获得更大更清晰的画面：“我们是否在另一次攻击中看到了这个IP？ 当时使用哪种浏览器[[1]](#bookmark1)？它访问了哪个Gmail/Yahoo/Microsoft/Facebook帐户？”

# Getting in

*“There is a crack in everything, that’s how the light gets in.”*

***Leonard Cohen***

# North of the (fire)wall

*“Why is it that when one man builds a wall, the next man immediately needs to know what's on the other side?”*

***Georges R.R. Martin***

# Hacking the unthinkable

*“Nothing and everything is possimpible”*

***Barney Stinson***

# Summary

我希望你喜欢站在黑客的立场上，以及其所带来的所有情感：沮丧、快乐和兴奋。当然，这是在我的实验室中设置的一个虚拟的例子，用于模仿真实公司的网络，但它非常准确地突出了我们在现实生活中可以发现和利用的许多缺陷。传统上这样的黑客攻击或者需要几天或几周完成，但是我们加快了这个过程，主要关注我们在开始时建立的目标。

如果您不熟悉道德黑客攻击，我建议您阅读本书中引用的文章。 不要犹豫，执行提供的多个脚本和命令。和他们一起玩，扭曲他们的论点，掌握他们的局限性。

Have fun p0wning[[93]](#bookmark93) the world!

# 参考链接

1. Your browser has a unique fingerprint: OS version, plugins installed, patch level, etc. It is used by many social networks to identify users even if they change IP addresses.
2. http://www.imdb.com/title/tt4044364/ and https://www.theguardian.com/us-news/the-nsa-files
3. https://www.torproject.org/
4. A layer of security used over HTTP to encrypt web content (HTTPs)
5. Use Bitcoin or other cryptocurrencies to pay anonymously
6. https://www.bitcoin.com/
7. http://cryto.net/~joepie91/bitcoinvps.html
8. https://www.kali.org/
9. http://www.linuxliveusb.com/ for a bootable USB Linux.
10. https://www.whonix.org/
11. https://tails.boum.org/
12. https://blog.barkly.com/phishing-statistics-2016
13. Using an anonymous email service, of course: protonmail.com, yopmail.com, etc.
14. https://github.com/laramies/theHarvester
15. https://getgophish.com/
16. Although some hackers try to hide the file by adding a dummy extension: e.g., “image.jpg.exe”.
17. https://www.metasploit.com/
18. http://www.freevbcode.com/ShowCode.asp?ID=3353
19. https://www.peerlyst.com/posts/resource-infosec-powershell-tools- resources-and-authors
20. http://www.labofapenetrationtester.com/2015/05/week-of-powershell- shells-day-1.html
21. http://www.shellntel.com/blog/2016/9/13/luckystrike-a-database-backed- evil-macro-generator
22. https://www.powershellempire.com/
23. http://www.powershellempire.com/?page\_id=110
24. https://github.com/Veil-Framework/Veil-Evasion
25. http://www.consulting-bolte.de/index.php/9-ms-office-and-visual-basic-for- applications-vba/154-determine-architecture-64-or-32-bit-in-vba
26. The above scenario will work on any Windows computer, provided that the user opens the document and activates its macros. Some hackers go a step further and exploit a vulnerability either on Word/Excel or on the browser (especially the plugins installed such as flash, adobe reader, etc.) in order to execute code on the computer and automatically elevate their privileges. Such vulnerabilities that are not yet patched by the editor are called zero-days, and can easily be worth thousands of dollars, especially for Microsoft products.
27. Check out this repository for inspiration on PowerShell obfuscation https://github.com/danielbohannon/Invoke-Obfuscation
28. https://github.com/darkoperator/dnsrecon
29. https://github.com/rbsec/dnscan
30. Another approach would be to directly query private databases for IP segments registered by SPH or its regular registrars, but many online tools request payment to perform such precise requests.
31. I put a private range to avoid any potential legal issues when publishing the book
32. How to configure Burp Suite: https://portswigger.net/burp/help/suite\_gettingstarted.html
33. The ping command on Windows sends a packet with 32 bytes of data.
34. More one-liners can be found here http://pentestmonkey.net/cheat- sheet/shells/reverse-shell-cheat-sheet
35. Check out the HTTP headers using ZAP or BURP to know which language the website is using.
36. Check out fuzzdb for basic webshells in multiple languages https://github.com/tennc/webshell/tree/master/fuzzdb-webshell
37. A helpful browser extension to get is ‘Wappalyzer’. It automatically fingerprints every component on the website.
38. ‘+’ is URL encoded in the address bar to %2B
39. Complete book about SQL injections: https://www.amazon.com/SQL-Injection-Attacks-Defense-Second/dp/1597499633
40. https://github.com/sqlmapproject/sqlmap
41. If you want to manually practice SQL injections, check out the following website http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection- cheat-sheet
42. https://www.drupal.org/project/drupal/releases/8.0.0
43. https://crackstation.net/
44. http://www.netmux.com/blog/how-to-build-a-password-cracking-rig
45. https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys--2
46. https://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Execution-Privesc-CVE-2016-6662.html
47. RDP for Remote Desktop Protocol is a Windows protocol used to remotely control a machine. The service usually runs on port 3389.
48. https://nmap.org/
49. www.shodan.io
50. Interestingly, while editing this book, it became apparent that thousands of MongoDBs are currently being trapped by malicious users who encrypt data and demand a ransom. The scary thing is that the same ‘vulnerability’ affects Cassandra, ElasticSearch, and Redis databases.
51. We can create efficient custom rules for John. Here are a few examples: http://contest-2010.korelogic.com/rules.html
52. https://github.com/lanjelot/patator, https://github.com/vanhauser-thc/thc- hydra, https://github.com/galkan/crowbar
53. We will stick with a compromised Linux server to show some nice pivoting techniques later on, otherwise it would be simple if we landed directly on Windows from the start.
54. For Windows: http://tim3warri0r.blogspot.fr/2012/09/windows-post- exploitation-command-list.html. For Linux: https://github.com/mubix/post- exploitation/wiki/Linux-Post-Exploitation-Command-List.
55. There is always the MongoDB server we got earlier, but I want to show you how to attack one from the “inside”.
56. https://raw.githubusercontent.com/mfontanini/Programs-Scripts/master/socks5/socks5.cpp
57. The firewall blocks every port other than 80 and 443, which are already used by the website.
58. http://proxychains.sourceforge.net/
59. I would never run an out of the box meterpreter file on a Windows machine. However, given that admins are so reluctant to equip Linux with an antivirus solution, we can be indulgent.
60. Check out explot-db.com for publicly available exploit code.
61. https://www.youtube.com/watch?v=\_8xJaaQlpBo
62. https://www.youtube.com/watch?v=-IMrNGPZTl0
63. Remote Procedure Calls is a protocol used by Windows to interact remotely with a machine. A call is made to port 135, which instructs the client to contact a random port (between 49152 and 65335) to issue its commands.
64. https://github.com/clymb3r/PowerShell/tree/master/Invoke-Mimikatz
65. Each domain can be further broken down into Organization Units.
66. There are several other ways to achieve total control over a domain: write privilege on GPO, administrative delegation, etc.
67. A term I just invented.
68. This statement only applies to local users. As previously explained, a domain user authenticates to the domain controller. The lockout count is then held by the DC and does not take into account the targeted machine. E.g., if lockout = 5 and we fail authentication on 5 different machines, a domain account is effectively locked, whereas a local account is not.
69. Admin may sometimes set up the LocalAccountTokenFilterPolicy registry key which effectively disables remote UAC.
70. We will show later on how to target users who did not click on the malicious payload.
71. https://github.com/FuzzySecurity/PowerShell-Suite/blob/master/Invoke-MS16-032.ps1
72. For this maneuver to work, we obviously need to set up a persistence scheme, using the run key for instance as detailed previously.
73. First method of extracting NTDS:https://www.trustwave.com/Resources/SpiderLabs-Blog/Tutorial-for-NTDS- goodness-(VSSADMIN,-WMIS,-NTDS-dit,-SYSTEM)/Second method: https://www.cyberis.co.uk/2014/02/obtaining-ntdsdit-using- in-built.html
74. https://github.com/samratashok/nishang/blob/master/Utility/Do-Exfiltration.ps1
75. https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon
76. We covered this part in the previous section: 5.6.2 Strategic files.
77. Outlook client works well. Otherwise there are plenty that can be found on Google that do the job just fine.
78. I cannot think of a greater book for cryptology than Bruce Schneier’s Applied Cryptography.
79. If RDP port was not available, we could have gone with GPO like before, or WMI calls, which we will demonstrate later.
80. http://www.blackhillsinfosec.com/?p=5296
81. Thanks in great part to researchers like Soldier of Fortran, BigEndianSmalls and Singe.
82. Job Control Language, a « scripting » language used on mainframes to execute programs
83. http://x3270.bgp.nu/download.html
84. The proper way to do it would be to download a second socks proxy and run it on 10.10.20.118. Then, instruct proxychains to go through two proxies: one in the DMZ, then this second one. Since I already detailed how to put this in place, I would rather focus entirely on the Mainframe.
85. We have to wait until users disconnect from the mainframe before using their credentials.
86. https://github.com/ayoul3/Privesc/blob/master/ELV.APF
87. https://github.com/magnumripper/JohnTheRipper
88. For a talk about the actual hacking of a mainframe in Sweeden: https://www.youtube.com/watch?v=SjtyifWTqmc
89. https://github.com/ayoul3/Rexx\_scripts/blob/master/REXX.GETUSERS
90. We run a second socks proxy on the 10.10.20.118 machine. That way our probes can avoid the DMZ firewall. We alter proxychain’s configuration file to take it into account.
91. There are some amazing nmap scripts to brute force user accounts as well as passwords. I encourage you to check out Soldier of Fortran’s work on the subject.
92. https://github.com/zedsec390/NMAP
93. Legally, of course.