KEVIN MITNICK

WILLIAM L. SIMON

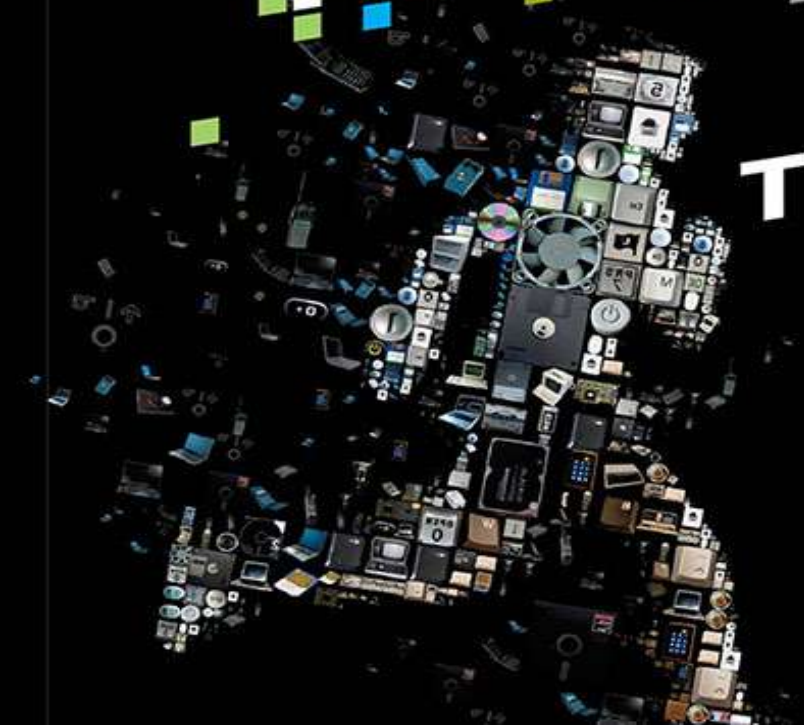
Trần Thanh Hương và LeVN *dịch*

GHOST IN THE WIRES

NGUYÊN SỐ AN TOÀN THÔNG TIN TRONG KỶ

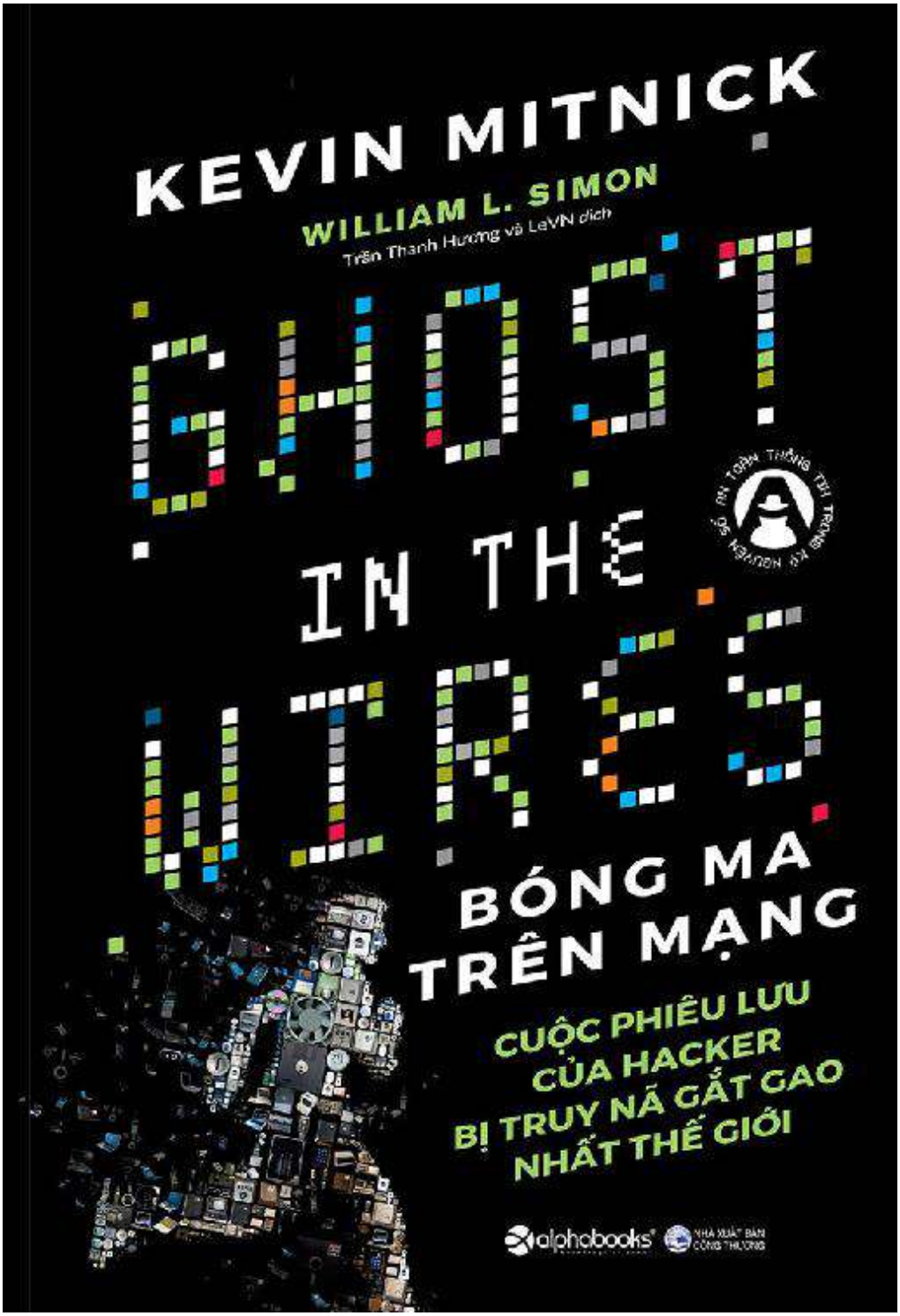
BÓNG MA TRÊN MẠNG

CUỘC PHIÊU LƯU CỦA HACKER BỊ TRUY NÃ GẮT GAO NHẤT THẾ GIỚI



alphabooks knowledge is power

NHÀ XUẤT BẢN CÔNG THƯƠNG



https://thuviensach.vn

Mục lục

1. An toàn thông tin trong kỷ nguyên số
2. Lời giới thiệu
3. Lời tựa
4. Lời nói đầu
5. PHẦN MỘT: SỰ RA ĐỜI CỦA MỘT HACKER
6. 01. Khởi đầu chông gai
7. 02. Chỉ là ghé thăm
8. 03. Tội lỗi đầu tiên
9. 04. Nghệ sĩ trốn chạy
10. 05. Tất cả đường dây điện thoại của các anh đều thuộc về tôi
11. 06. Hack vì yêu
12. 07. Kết hôn vội vã
13. 08. Lex Luthor
14. 09. Gói cước giảm giá kiểu Kevin Mitnick
15. 10. Hacker bí ẩn
16. PHẦN HAI: ERIC
17. 11. Mờ ám
18. 12. Không thể giấu giếm
19. 13. Kẻ nghe lén
20. 14. Anh nghe lén tôi, tôi nghe lén anh
21. 15. “Làm thế quái nào các cậu có được nó?”
22. 16. Khách không mời mà tới
23. 17. Phân tích lưu lượng

https://thuviensach.vn

24. 18. Sáng tỏ
25. 19. Vén màn
26. 20. Cắn ngược
27. 21. Mèo và chuột
28. 22. Công việc thám tử
29. 23. Bị vây bắt
30. 24. Hô biến
31. PHẦN BA: TRỐN CHẠY
32. 25. Harry Houdini
33. 26. Thám tử tư
34. 27. Mặt trời lên
35. 28. Săn lùng chiến tích
36. 29. Rời đi
37. 30. Đánh lén
38. 31. Vây bắt từ trên cao
39. 32. Đêm trắng ở Seattle
40. PHẦN BỐN: KẾT THÚC VÀ KHỞI ĐẦU
41. 33. Hack gã samurai
42. 34. Lánh về phương Nam
43. 35. Trò chơi kết thúc
44. 36. Ngày lễ tình yêu của FBI
45. 37. Thoát nạn vật tế thần
46. 38. Hồi kết: Vận mệnh đổi chiều
47. Lời cảm ơn
48. Đôi điều về tác giả

https://thuviensach.vn

AN TOÀN THÔNG TIN TRONG KỶ NGUYÊN SỐ

Trong kỷ nguyên số, vấn đề bảo mật và an toàn trên không gian mạng ngày càng trở nên quan trọng, không chỉ đối với các doanh nghiệp, tổ chức, chính phủ, mà còn đối với từng cá nhân. Việt Nam có 58 triệu tài khoản Facebook (tính đến hết quý 1/2018); 127 triệu thẻ ngân hàng với 66,6 triệu tài khoản thanh toán cá nhân; cùng hàng tỷ các giao dịch mua bán, trao đổi trên mạng diễn ra mỗi ngày. Chính vì vậy, an ninh mạng trong kỷ nguyên số đang trở thành một chủ đề ngày càng nóng.

Chỉ rất gần đây, nhiều tài khoản Facebook cũng như email cá nhân đã bị hacker tấn công và chiếm đoạt. Thủ đoạn của hacker khá đơn giản khi tận dụng các sơ hở của người dùng cũng như các lỗi bảo mật của hệ thống, nhưng chúng đã gây ra những thiệt hại rất lớn cả về vật chất và tinh thần cho người dùng – rất nhiều thông tin cá nhân bị lộ và bị mất, và điều đó cũng đang xảy ra với rất nhiều tổ chức, công ty, cả tư nhân lẫn nhà nước.

Ngay đầu tháng 11/2018, một số nguồn tin lan truyền trên mạng cho rằng hệ thống công nghệ của Thế giới Di động bị hacker tấn công và thông tin của khách hàng bị tiết lộ. Các tài khoản thẻ ngân hàng cũng như email và số điện thoại cá nhân bị kẻ xấu công khai trên mạng dù cho nghi vấn lộ dữ liệu khách hàng vẫn đang tiếp tụcđược điều tra, xác minh.

Ngược về quá khứ, tháng 4/2018, website của ngân hàng Vietcombank bị tấn công. Sự cố xảy ra với trang con của website Vietcombank khi người dùng đăng ký email liên kết với tài khoản ngân hàng. Khi được chia sẻ qua Facebook, ảnh bìa của trang con này hiển thị dòng chữ “Đại học Quốc gia Hà Nội”. Hacker còn để lại hai câu thơ “Trăm năm Kiều vẫn là Kiều/ Sinh viên thi lại là điều tất nhiên”.

https://thuviensach.vn

Năm 2016, hệ thống các sân bay lớn tại Việt Nam như Sân bay Quốc tế Tân Sơn Nhất, Sân bay Quốc tế Nội Bài, Sân bay Quốc tế Đà Nẵng, Sân bay Phú Quốc đều bị hacker tấn công và để lại nhiều nội dung xúc phạm, xuyên tạc.

Cuối năm 2014, hệ thống các website của VCCorp cũng bị tấn công, làm tê liệt hoạt động truy cập vào toàn bộ hệ thống website báo chí đối tác của VCCorp và gây thiệt hại trực tiếp tới hoạt động của các trang này, đồng thời ảnh hưởng tới hàng triệu độc giả và người tiêu dùng sử dụng các dịch vụ trực tuyến của họ. Theo VCCorp, ước tính sơ bộ sau hai ngày bị tấn công, số tiền VCCorp bị thiệt hại vào khoảng 5 tỷ đồng, bao gồm tất cả các loại doanh thu như quảng cáo, thương mại điện tử…

Trên thực tế, không ít những vụ tấn công mạng đã xảy ra liên tiếp tại Việt Nam trong thời gian gần đây và để lại những hậu quả không hề nhỏ. Những vụ việc như thế này đang gióng lên một hồi chuông cảnh báo đối với các cá nhân cũng như doanh nghiệp trong thời đại số. Với xu thế phát triển mạnh mẽ của cuộc cách mạng công nghiệp 4.0 trên toàn thế giới, trong đó có Việt Nam, sự bùng nổ của các thiết bị IoT sẽ mang lại nhiều nguy cơ tiềm ẩn về các cuộc tấn công trên không gian mạng hoặc bị kẻ xấu lợi dụng để tấn công vào các hạ tầng.

Chuyên gia an toàn thông tin, vấn đề bảo mật không có tính tuyệt đối. Ngay cả các cường quốc trong ngành công nghệ thông tin-bảo mật như Anh, Pháp, Đức, Mỹ, Trung Quốc... cũng đều bị hacker tấn công. Vậy các doanh nghiệp và người dùng Việt Nam phải làm gì để vừa có thể tận dụng được những lợi thế của nền công nghiệp IoT mà vẫn đảm bảo an toàn thông tin trên mạng?

Nhằm mang tới cho độc giả và các doanh nghiệp, tổ chức những kiến thức cơ bản về bảo mật dữ liệu, cảnh báo người đọc về vấn đề quyền riêng tư và nâng cao ý thức bảo mật thông tin, Apha Books trân trọng giới thiệu bộ sách “An toàn thông tin trong kỷ nguyên số” gồm 4 cuốn: The Cuckoo’s Egg (Gián điệp mạng), Ghost in the Wires (Bóng ma trên mạng), The Art of Invisibility (Nghệ thuật ẩn mình) và Hackers lược sử. Thông qua các câu

https://thuviensach.vn

chuyện ly kỳ hấp dẫn về những cuộc truy bắt hacker, những chiến công của các hacker mũ trắng – những kẻ mê máy tính thông minh và lập dị, dám mạo hiểm, bẻ cong các quy tắc và đẩy thế giới vào một hướng đi hoàn toàn mới, độc giả sẽ có được cái nhìn toàn diện về hacker, về đạo đức nghề nghiệp cũng như tương lai của ngành công nghệ để có được cái nhìn rõ ràng hơn về an ninh mạng, chủ đề chưa bao giờ hết nóng hổi của các tín đồ mạng.

Bộ trưởng TT&TT Nguyễn Mạnh Hùng đã nhấn mạnh: “An toàn, an ninh mạng được coi là điều kiện để thúc đẩy chính phủ điện tử, chính phủ số và nền công nghiệp nội dung số. Vì vậy, Việt Nam phải trở thành cường quốc về an ninh mạng”. Đồng hành với những vấn đề thời sự nhức nhối hiện nay, với bộ sách này, Apha Books và các đối tác – những nhà cung cấp các giải pháp bảo mật & an ninh mạng như CMC, Netnam, Securitybox, CyRadar... mong muốn đóng góp một phần tri thức cho xã hội, giúp nền kinh tế số Việt Nam phát triển lành mạnh, bền vững.

Trân trọng giới thiệu!

Tháng 11/2018

Công ty Cổ phần Sách Alpha

https://thuviensach.vn

LỜI GIỚI THIỆU

Hôm nay, khi tôi đang suy nghĩ về lời giới thiệu cho cuốn sách tuyệt vời này, hệ thống thu thập thông tin của SecurityBox thông báo cho tôi hai tin tức rất quan trọng. Một là hệ thống thương mại điện tử của một tập đoàn trong nước bị tấn công, hacker đã lấy cắp và công bố số lượng lớn dữ liệu người dùng. Hai là 59 học viên của trường Học viện Kỹ thuật Mật mã sắp tổ chức lễ tốt nghiệp và trở thành những chuyên gia an ninh mạng được đào tạo bài bản. Những sự kiện đối lập giữa "tấn công" và "phòng thủ" như thế này vô tình lại rất liên quan đến nội dung của cuốn sách, hồi ký về cuộc đời và sự nghiệp kỳ lạ của Kevin Mitnick, người từng được coi là hacker bị truy nã gắt gao nhất thế giới.

Kevin Mitnick luôn có tên trong mọi bảng xếp hạng những hacker nguy hiểm nhất mọi thời đại. Ông nổi tiếng với khả năng tấn công mọi hệ thống phức tạp bằng phương pháp tấn công phi kỹ thuật (social engineering). Phương pháp này nhắm thẳng đến người dùng đang tham gia vào hệ thống, Kevin sẽ giao tiếp trực tiếp hoặc gián tiếp với những người này, đặt họ vào tình huống khiến họ vô tình cung cấp thông tin quan trọng cho phép ông có thể dễ dàng chiếm quyền điều khiển hệ thống.

Ngày nay, kỹ thuật tấn công này vẫn rất phổ biến, điển hình là trên mạng xã hội Facebook, khi hacker giả danh người thân, người nổi tiếng hoặc công ty nổi tiếng để lừa đảo các nạn nhân, khiến họ tin tưởng và tự động thực hiện những hành vi do hacker đề xuất. Tuy nhiên, khi đọc cuốn sách này, tôi nhận ra Kevin Mitnick còn là một kỹ sư công nghệ xuất chúng, chính sự kết hợp hoàn hảo giữa tấn công bằng kỹ thuật và phi kỹ thuật mới là điều làm nên tên tuổi của ông.

Chi tiết quan trọng nhất trong cuộc đời của Kevin chính là việc ông bị bắt giam vì tấn công vào hệ thống tối mật của chính phủ Mỹ. Việc không bao

https://thuviensach.vn

giờ thực hiện các hành vi phá hoại là điều đáng ngưỡng mộ của hacker này. Điều này lý giải vì sao sau khi ra tù, các công ty từng bị Kevin tấn công đã thuê ông tư vấn về giải pháp đảm bảo an ninh mạng.

Ngay tại SecurityBox, chúng tôi cũng có các chuyên gia và công nghệ cho phép tìm ra những điểm yếu có thể bị tấn công trong hệ thống mạng của khách hàng. Chúng tôi hiểu rằng việc có trong tay công cụ để kiểm soát một hệ thống lớn, cũng giống như khi nhìn thấy một lượng tiền lớn còn bỏ ngỏ, chúng ta sẽ khó tránh khỏi lòng tham. Vấn đề nằm ở khái niệm "đạo đức", chúng tôi phải giữ được đạo đức làm nghề và đào tạo kỹ sư của mình cũng phải như vậy.

Bóng ma trên mạng thể hiện ham muốn kiểm soát, tấn công mọi hệ thống mạng, sự ám ảnh đối đầu với chính quyền và bản lĩnh của một hacker tài năng. Việc Kevin từng trải qua cuộc cách mạng máy tính và Internet với tư cách là một hacker kiêm chuyên gia an ninh mạng đã góp phần khiến cuốn sách này trở thành tư liệu quý báu dành cho các chuyên giao bảo mật, kỹ sư an ninh mạng hoặc thậm chí là các hacker. Tôi tin rằng, cuốn sách này sẽ rất thú vị không chỉ đối với những người trong nghề mà còn hữu ích cho bất kỳ ai đang sống trong kỷ nguyên số hiện nay nhằm nâng cao hiểu biết và ý thức bảo vệ các "tài sản số" của chính mình.

Bùi Quang Minh

CEO SecurityBox

Bùi Quang Minh đã có 15 năm kinh nghiệm làm việc trong lĩnh vực bảo mật với tư cách là hacker mũ trắng kiêm chuyên gia về an ninh mạng. Năm 2010, ông đã phát hiện và công bố lỗ hổng phần mềm của các hãng công nghệ nổi tiếng thế giới như Google, Microsoft. Năm 2011, ông công bố lỗ hổng nghiêm trọng trong mạng 3G của ba nhà mạng Mobifone, Vinaphone và Viettel. Ngoài ra, ông cũng là đồng tác giả của một số phát hiện bảo mật nghiêm trọng từng được công bố trong và ngoài nước.

https://thuviensach.vn

LỜI TỰA

Tôi gặp Kevin Mitnick lần đầu tiên vào năm 2001 trong đợt quay bộ phim tài liệu *The History of Hacking* (tạm dịch: *Lịch sử hacking*) của kênh Discovery Channel và chúng tôi giữ liên lạc từ đó. Hai năm sau, tôi bay tới Pittsburgh để gặp anh trong buổi diễn thuyết của anh ở Đại học Carnegie Mellon. Tại đây, tôi đã chết lặng khi nghe anh nói về lịch sử hacking của mình. Anh đã đột nhập vào hệ thống máy tính của các công ty nhưng không hủy dữ liệu, cũng không hề dùng hay bán các thông tin thẻ tín dụng mà mình có trong tay. Anh lấy trộm phần mềm nhưng chưa từng bán chúng. Anh hack cho vui, và vì tính thử thách trong đó.

Trong buổi diễn thuyết, Kevin kể chi tiết câu chuyện khó tin về việc anh đã quấy phá cuộc truy lùng của Cục Điều tra Liên bang (FBI) đối với mình ra sao. Kevin đã thâm nhập vào toàn bộ quá trình điều tra, phát hiện ra một "người bạn" hacker mới hóa ra lại là kẻ chỉ điểm của FBI, biết tên và địa chỉ của toàn bộ tổ FBI phụ trách vụ này, thậm chí còn nghe lỏm được các cuộc gọi và tin nhắn thoại của những người đang cố thu thập bằng chứng chống lại mình. Anh còn thiết lập cả một hệ thống cảnh báo riêng để biết được khi nào FBI chuẩn bị chiến dịch vây bắt.

Khi các nhà sản xuất của chương trình truyền hình Screen Savers (tạm dịch: Bảo vệ màn hình) mời Kevin và tôi cùng dẫn một tập, họ đề nghị tôi nói về một thiết bị điện tử mới xuất hiện trên thị trường tiêu dùng dạo đó: Hệ thống định vị toàn cầu (GPS). Tôi được yêu cầu lái xe lòng vòng trong khi họ theo dõi xe tôi qua thiết bị định vị. Khi chương trình lên sóng, các nhà sản xuất yêu cầu tôi lái theo lộ trình tưởng chừng như rất ngẫu nhiên. Thế rồi, một thông điệp hiện ra:

FREE KEVIN

https://thuviensach.vn

(tạm dịch: Hãy trả tự do cho Kevin)

Chúng tôi lại cùng xuất hiện trong một chương trình khác vào năm 2006, khi Kevin là người dẫn chương trình tạm thời cho buổi trò chuyện Coast to Coast AM (tạm dịch: Từ bờ đông sang bờ tây) của Art Bell và mời tôi cùng tham gia với tư cách khách mời. Trước đó, tôi thường ở vị trí là người lắng nghe các câu chuyện về anh; còn buổi tối hôm đó, anh là người phỏng vấn tôi và chúng tôi đã vô cùng vui vẻ, hệt như mỗi lần gặp gỡ trước đó.

Kevin đã làm thay đổi cuộc sống của tôi. Một ngày nọ, tôi phát hiện ra anh thường gọi cho tôi từ những nơi rất xa: Anh ở Nga để diễn thuyết, ở Tây Ban Nha để giúp một công ty giải quyết các vấn đề an ninh, ở Chile để tư vấn cho một ngân hàng đã bị xâm nhập máy tính. Nghe thật tuyệt! Tôi đã không đụng tới hộ chiếu của mình suốt 10 năm cho tới khi những cuộc gọi này khiến tôi ngứa ngáy. Kevin giới thiệu tôi với một đại diện chuyên đặt lịch cho các buổi diễn thuyết của anh. Cô ấy nói với tôi: “Tôi có thể đặt các buổi nói chuyện cho anh luôn.” Vậy là nhờ Kevin, tôi đã trở thành kẻ dịch chuyển khắp năm châu như anh.

Kevin trở thành một trong những người bạn tốt nhất của tôi. Tôi thích ở gần anh để được nghe về các trải nghiệm khai phá và mạo hiểm. Anh đã sống một cuộc đời đầy say mê và hấp dẫn hệt như những bộ phim về tội phạm hay nhất.

Giờ đây, bạn cũng có thể biết đến tất cả những câu chuyện mà tôi đã lần lượt được nghe trong suốt những năm qua. Ở khía cạnh nào đó, tôi thấy ghen tị với những trải nghiệm trong hành trình mà bạn sắp bắt đầu. Bạn sẽ thấy say mê câu chuyện khó tin, gần như là không tưởng về cuộc đời và những kỳ tích mà Kevin Mitnick đã tạo ra.

— Steve Wozniak, đồng sáng lập công ty Apple

https://thuviensach.vn

LỜI NÓI ĐẦU

"Cuộc đột nhập thực tế": lẻn vào tòa nhà của công ty mục tiêu. Tôi không bao giờ thích làm việc này. Quá nguy hiểm. Chỉ viết về nó thôi cũng khiến tôi vã mồ hôi rồi.

Nhưng tôi đã ở đó, núp trong bãi đỗ xe tối đen của một công ty trị giá hàng tỷ đô-la trong buổi tối mùa xuân ấm áp để tìm cơ hội. Một tuần trước, tôi đã ghé thăm tòa nhà này vào ban ngày, lấy cớ chuyển một bức thư cho nhân viên tại đây. Lý do thực sự là để tôi có thể nhìn kỹ thẻ ID của họ. Công ty này đặt ảnh nhân viên ở góc trái phía trên, tên ngay bên dưới, họ ở trước, in hoa. Tên công ty ở phía dưới thẻ, màu đỏ, cũng in hoa.

Tôi từng đến Kinko's và xem qua trang web của công ty, do đó, tôi có thể tải về và sao chép hình ảnh logo công ty. Có ảnh này và bản scan ảnh của chính mình, tôi chỉ mất chừng 20 phút dùng Photoshop để thiết kế và in ra một tấm thẻ nhân viên công ty khá chuẩn, rồi nhét nó vào một dây đeo thẻ rẻ tiền mua ở một cửa tiệm bách hóa. Tôi chế thêm một thẻ ID giả nữa cho bạn mình, người đã đồng ý đi cùng trong trường hợp tôi cần giúp đỡ.

Bất ngờ thay, những tấm thẻ này thậm chí còn không cần phải trông giống hàng thật. 99% là người ta sẽ chỉ liếc mắt nhìn nó lấy lệ. Miễn sao những chi tiết chính yếu ở đúng vị trí và trông có vẻ giống thẻ thật, bạn sẽ dễ dàng vượt qua cửa kiểm soát… đương nhiên là trừ khi có một gã bảo vệ quá hăng hái hoặc một nhân viên nào đó khoái trò kiểm tra an ninh khăng khăng muốn nhìn thật kỹ. Đây là mối nguy hiểm bạn buộc phải chấp nhận nếu sống một cuộc đời như tôi.

Trong bãi đỗ xe, tôi nấp vào chỗ kín đáo, theo dõi từng đốm sáng lóe lên từ những điếu thuốc của dòng người bước ra ngoài nghỉ giải lao. Cuối cùng, tôi phát hiện ra một nhóm nhỏ chừng 5-6 người chuẩn bị quay trở lại tòa nhà.

https://thuviensach.vn

Cửa hậu là một trong những cánh cửa chỉ mở khóa khi nhân viên đặt thẻ ra vào của mình lên máy đọc thẻ. Khi cả tốp xếp thành hàng đi qua cửa, tôi nhảy ngay vào cuối hàng. Gã ở phía trước với tay lên cửa và để ý thấy còn ai đó đứng ngay sau, đưa mắt để đảm bảo tôi có đeo thẻ nhân viên của công ty, rồi giữ cửa giúp. Tôi gật nhẹ cảm ơn.

Kỹ thật này gọi là "tailgating" – theo đuôi.

Vào tới trong, thứ đầu tiên đập vào mắt tôi là tấm áp phích chình ình trước mắt. Nó là một tấm áp phích an ninh, cảnh báo bạn không được giữ cửa cho người khác và yêu cầu mỗi người đều phải qua cửa bằng cách đặt thẻ của mình vào máy đọc thẻ. Có điều, thói lịch thiệp xã giao, phép lịch sự đối với "đồng nghiệp" đồng nghĩa với việc lời cảnh báo trên tấm áp phích an ninh này thường xuyên bị tảng lờ.

Khi đã yên vị ở trong tòa nhà, tôi bắt đầu bước qua từng dãy hành lang đầy những người đang rảo bước trên đường thực hiện nhiệm vụ quan trọng nào đó. Trên thực tế, tôi đang trong hành trình khám phá, cố tìm cho ra Phòng Công nghệ Thông tin (IT). Sau khoảng 10 phút, tôi tìm thấy nó ở khu phía tây của tòa nhà. Tôi đã chuẩn bị kỹ càng trước đó và biết tên của một trong những kỹ sư mạng ở đây; tôi đoán là anh ta có toàn quyền quản trị hệ thống máy tính của cả công ty.

Chết tiệt! Nơi anh ta ngồi không phải là một ô làm việc dễ dàng thâm nhập, mà là một văn phòng riêng … đằng sau cánh cửa đã bị khóa kín. Nhưng tôi đã có cách. Trần nhà được làm từ những tấm vật liệu vuông, trắng, cách âm vẫn thường được dùng để tạo ra lớp trần thấp có khoảng trống ở giữa có thể bò qua, nơi chứa các đường ống, đường dây điện, thông khí…

Tôi gọi điện cho chiến hữu để yêu cầu trợ giúp và quay trở lại cửa hậu để mở cửa cho anh vào. Với dáng người cao lêu nghêu và gầy, hy vọng anh ấy có thể làm được việc mà tôi không thể. Quay trở lại phòng IT, anh ấy trèo lên một chiếc bàn. Tôi ôm chặt hai chân anh, đẩy anh lên cao đủ để có thể

https://thuviensach.vn

nâng một tấm trần vuông lên và trượt nó sang một bên. Trong lúc tôi căng sức để nâng cao hơn nữa, thì anh ấy cũng cũng xoay xở để có thể túm chặt lấy một đường ống và đu lên. Vài phút sau, tôi nghe thấy tiếng anh nhảy vào văn phòng khóa kín. Nắm cửa xoay mở và anh đứng đó, người đầy bụi, miệng cười nhăn nhở.

Tôi bước vào phòng và nhẹ nhàng đóng cửa. Chúng tôi đã an toàn, ít có khả năng bị phát hiện. Căn phòng tối đen. Bật đèn có thể gây nguy hiểm mà cũng không cần thiết – ánh sáng phát ra từ chiếc máy tính của gã kỹ sư đủ để tôi nhìn thấy mọi thứ mình cần, giảm thiểu được khối rủi ro. Tôi nhìn lướt trên bàn, kiểm tra ngăn kéo trên cùng và dưới bàn phím xem liệu gã có ghi lại mật khẩu máy tính ở đâu đó không. Tiếc là không. Nhưng đó không phải là vấn đề.

Từ túi đeo hông, tôi rút ra một chiếc đĩa CD với phiên bản có thể khởi động máy tính của hệ điều hành Linux, chứa bộ công cụ dành cho hacker và thả vào ổ CD của gã, sau đó khởi động lại máy. Một trong những công cụ này cho phép tôi thay đổi mật khẩu quản trị trên máy tính; sau khi đổi xong, tôi có thể đăng nhập bình thường. Tôi bỏ chiếc đĩa CD ra khỏi ổ và khởi động lại máy tính một lần nữa, lần này là để đăng nhập vào tài khoản quản trị.

Thao tác nhanh nhất có thể, tôi cài đặt một phần mềm gián điệp cho phép truy cập từ xa (remote access Trojan), phần mềm mã độc giúp tôi có toàn quyền đăng nhập vào hệ thống, nhờ vậy tôi có thể ghi lại thao tác bàn phím, lấy được chuỗi mã băm[1] mật khẩu và thậm chí, điều khiển webcam chụp hình người đang sử dụng máy tính. Loại Trojan mà tôi cài đặt sẽ khởi động kết nối mạng Internet tới một hệ thống khác dưới quyền kiểm soát của tôi sau mỗi vài phút, cho phép tôi toàn quyền kiểm soát máy tính của nạn nhân.

[1] Mã băm (hash): Chuỗi ký tự có độ dài cố định do các thuật toán mã hóa thông tin tạo ra, được dùng phổ biến trong việc kiểm tra chữ ký điện tử, tập tin… (BTV)

https://thuviensach.vn

Gần xong việc, ở bước cuối cùng, tôi vào phần lưu thông tin cấu hình hoạt động của máy tính và đặt mục "tài khoản đăng nhập lần cuối" (last logged-in user) sang tài khoản của gã kia, như vậy tôi sẽ không để lại bất kỳ dấu vết nào cho lần đăng nhập này bằng tài khoản quản trị. Sáng hôm sau, gã kỹ sư có thể phát hiện ra mình đã thoát khỏi máy. Không thành vấn đề: miễn sao khi đăng nhập, mọi thứ trông vẫn hệt như cũ là được.

Tôi đã sẵn sàng rời đi. Lúc này, chiến hữu của tôi đã đặt tấm lát trần vào chỗ cũ. Trên đường ra, tôi khóa phòng lại như cũ.

Sáng hôm sau, gã kỹ sư bật máy vào khoảng 8 giờ 30 phút, và phần mềm gián điệp đã khởi động kết nối tới máy tính xách tay của tôi. Bởi Trojan đang chạy trên tài khoản của gã còn tôi nắm toàn quyền quản trị miền, nên chỉ mất vài giây để xác định được bộ điều khiển miền[2] chứa toàn bộ mật khẩu tài khoản của cả công ty. Một công cụ hacker có tên "fgdump" cho phép tôi trích xuất các chuỗi mã băm mật khẩu của tất cả người dùng.

[2] Bộ điều khiển miền (domain controller): Máy chủ có chức năng phản hồi các yêu cầu xác nhận an ninh (như đăng nhập, kiểm tra quyền, v.v…). (BTV)

Chỉ sau vài giờ, tôi đã quét toàn bộ chuỗi mã băm này qua một "bảng danh sách cầu vồng" (rainbow table) – một cơ sở dữ liệu khổng lồ chứa các chuỗi mã băm mật khẩu có sẵn – nhằm khôi phục mật khẩu của hầu hết nhân viên trong công ty. Tôi còn tìm được một trong những máy chủ back-end[3] xử lý các giao dịch khách hàng, nhưng mã số thẻ tín dụng đều bị mã hóa. Không thành vấn đề: Tôi phát hiện ra chìa khóa để mã hóa số thẻ được giấu trong một đoạn mã chương trình lưu bên trong cơ sở dữ liệu của máy tính được gọi là "máy chủ SQL", có khả năng tiếp cận bất kỳ quản trị cơ sở dữ liệu nào.

[3] Back-end: Thuật ngữ chỉ giai đoạn kết thúc của một quá trình xử lý, khái niệm này thường được sử dụng trong lĩnh vực phát triển phần mềm, ám chỉ

https://thuviensach.vn

việc tương tác với hệ quản trị dữ liệu. (BTV)

Hàng triệu triệu số thẻ tín dụng. Tôi có thể mua sắm cả ngày bằng cách mỗi lần sử dụng một thẻ khác nhau mà không bao giờ cạn thẻ.

Nhưng tôi không làm vậy. Câu chuyện thực này không phải tái hiện cảnh hacking đã đẩy tôi vào bước đường cùng. Ngược lại, đó là công việc tôi được thuê làm.

Đây là thứ chúng tôi gọi là “pen test” (đánh giá bảo mật), viết tắt của cụm từ “penentration test” (phép thử đột nhập) và nó chiếm phần lớn những gì đang diễn ra trong cuộc sống của tôi. Tôi đã tấn công vào những công ty lớn nhất trên hành tinh và đột nhập vào những hệ thống máy tính tốt nhất từng có – chính các công ty đã thuê tôi để giúp họ hàn gắn các kẽ hở và phát triển hệ thống an ninh, nhờ đó họ không trở thành nạn nhân kế tiếp của trò hack. Phần lớn kiến thức tôi có được là nhờ tự học với nhiều năm nghiên cứu phương pháp, chiến thuật, chiến lược để phá vỡ an ninh máy tính, và để học hỏi thêm nhiều điều về cơ chế hoạt động của các hệ thống máy tính cùng hệ thống viễn thông.

Đam mê của tôi dành cho công nghệ và sự mê hoặc của nó đã đẩy tôi vào một hành trình gập ghềnh. Hành vi hack liều lĩnh đã khiến tôi phải trả giá bằng 5 năm bóc lịch trong tù và khiến những người tôi yêu thương tổn thương.

Đây là câu chuyện của tôi, từng chi tiết đều chính xác theo những gì tôi nhớ, các ghi chép cá nhân, biên bản phiên tòa công khai, các tài liệu có được thông qua Luật Tự do Thông tin, bản ghi âm các cuộc nghe lén FBI, nhiều giờ phỏng vấn và cả các cuộc thảo luận cùng hai kẻ chỉ điểm của chính phủ.

Đây là câu chuyện kể về hành trình trở thành hacker máy tính bị truy nã gắt gao nhất thế giới của tôi.

https://thuviensach.vn

Phần một

SỰ RA ĐỜI CỦA MỘT HACKER

https://thuviensach.vn

01

KHỞI ĐẦU CHÔNG GAI

Yjcv ku vjg pcog qh vjg uauvgo wugf da jco qrgtcvqtu vq ocmg htgg rjqpg ecnnu?

Bản năng tìm cách tránh né rào cản và chốt chặn của tôi bắt đầu từ rất sớm. Hồi một tuổi rưỡi, tôi đã tìm ra cách để trèo khỏi cũi, bò tới thanh chắn an toàn ở cửa và tìm được cách mở nó. Đối với mẹ tôi, đây là dấu hiệu cảnh báo đầu tiên cho những gì sau này.

Tôi là con một trong nhà. Sau khi cha bỏ đi lúc tôi lên ba, mẹ tôi, tên là Shelly, và tôi đã sống trong những căn hộ đẹp với mức giá trung bình thuộc các khu dân cư an toàn ở Thung lũng San Fernando, chỉ cách thành phố Los Angeles một ngọn đồi. Chúng tôi sống nhờ công việc chạy bàn của mẹ tại một trong những nhà hàng nằm trên Đại lộ Ventura, chạy theo hướng đông-tây suốt chiều dài thung lũng. Cha tôi sống ở một bang khác và dù có quan tâm đến tôi, nhưng nhìn chung, ông chỉ tới thăm tôi vài lần cho tới khi ông chuyển đến Los Angeles năm tôi 13 tuổi.

Mẹ con tôi chuyển nhà nhiều đến mức tôi không có cơ hội kết bạn như những đứa trẻ khác. Tôi dành thời thơ ấu cho các thú vui đơn độc, phần lớn là những hoạt động không phải di chuyển. Khi tôi còn đi học, các thầy cô thường nói với mẹ rằng tôi thuộc nhóm 1% đứng đầu về toán và đánh vần, vượt xa so với các bạn cùng tuổi. Nhưng do bản tính hiếu động, nên thật khó để tôi có thể ngồi yên một chỗ.

Trong suốt quá trình trưởng thành của tôi, mẹ đã lấy thêm ba người chồng và có vài người bạn trai. Một kẻ hành hung tôi, một gã khác – tay này làm trong lực lượng chấp pháp – đã quấy rối tôi. Không giống như các bà mẹ mà

https://thuviensach.vn

tôi từng biết, mẹ chưa bao giờ làm ngơ. Ngay khi bà phát hiện ra tôi bị đối xử tệ hại – hoặc thậm chí chỉ là bị nặng lời – gã đàn ông đó sẽ phải ra khỏi nhà ngay lập tức. Tôi không định kiếm cớ bao biện, nhưng tôi thường tự hỏi không biết những gã đàn ông ưa bạo lực kia có góp phần làm nên tư tưởng chống đối lực lượng chức năng của tôi hay không.

Mùa hè là khoảng thời gian tuyệt vời nhất, đặc biệt là khi mẹ làm theo ca và được nghỉ vào giữa ngày. Tôi sung sướng được mẹ cho đi bơi ở bãi biển Santa Monica tuyệt vời. Mẹ nằm trên cát, tắm nắng và thư giãn, nhìn tôi chơi đùa cùng những con sóng, bị sóng đánh ngã rồi lại nhổm lên cười. Ngoài ra, tôi còn tập luyện mấy kiểu bơi được học ở trại hè YMCA mà tôi đã tham gia được vài kỳ (tôi luôn ghét chúng trừ những lúc được dẫn ra biển).

Khi còn bé, tôi khá giỏi thể thao và cảm thấy thích thú khi được chơi tại Giải Bóng chày Thiếu niên (Little League). Tôi nghiêm túc với việc này tới mức dành hết thời gian rảnh rỗi để tập đánh bóng. Nhưng niềm đam mê dẫn tới hành trình trọn đời của tôi bắt đầu từ năm tôi lên 10. Người hàng xóm sống trong căn hộ đối diện có cô con gái trạc tuổi mà tôi rất có cảm tình. Ở tuổi đó, điều tôi thấy hứng thú hơn cả lại là thứ mà cha cô bé mang tới: ảo thuật.

Ông là một nhà ảo thuật có tài với những màn ảo thuật bằng lá bài, đồng xu và những hiệu ứng hoành tráng đầy mê hoặc. Nhưng quan trọng hơn, tôi nhìn thấy niềm hân hoan trên gương mặt các khán giả của ông khi bị qua mặt, dù đó là một người, ba người, hay cả căn phòng. Dù chưa từng thực sự suy ngẫm về điều này, nhưng việc phát hiện ra rằng con người thích bị lừa đã ảnh hưởng rất lớn đến đường đời của tôi.

Cửa hàng bán đồ ảo thuật chỉ cách nhà một cuốc xe đạp ngắn trở thành chốn bí mật yêu thích của tôi trong thời gian rảnh rỗi. Ảo thuật là cánh cửa đầu tiên đưa tôi đến với nghệ thuật qua mặt con người.

https://thuviensach.vn

Đôi khi thay vì đạp xe, tôi sẽ nhảy lên xe buýt. Vào một ngày nọ, vài năm sau, Bob Arkow, một tài xế xe buýt, người để ý thấy tôi mặc chiếc áo phông có ghi "CBers Do It on the Air" (tạm dịch: Dân chơi mạng làm việc như trên mây), đã nói rằng anh ta vừa kiếm được một thiết bị cầm tay Motorola vốn là chiếc bộ đàm của cảnh sát. Tôi nghĩ có thể gã đã bắt được tần số của cảnh sát, nếu thế thì thật tuyệt. Hóa ra, gã bịp tôi chuyện đó, nhưng Bob là một gã cuồng chơi vô tuyến điện nghiệp dư[4] (ham radio), và sự nhiệt tình của gã với thú vui đó đã khơi lên mối quan tâm trong tôi. Gã cho tôi thấy cách thực hiện một cuộc gọi miễn phí thông qua sóng vô tuyến điện, nhờ một tính năng có tên là miếng vá tự động[5] trên một số vô tuyến điện nghiệp dư. Gọi điện thoại miễn phí! Điều này khiến tôi ấn tượng không tài nào kể xiết. Tôi nghiện trò này luôn.

[4] Vô tuyến điện nghiệp dư (ham radio hay còn gọi là amatuer radio): Thiết bị sử dụng các dải tần số vô tuyến cho mục đích phi thương mại như giải trí, trao đổi tin nhắn… (ND)

[5] Miếng vá tự động (auto patch): Một tính năng của ham radio, được dùng để thực hiện cuộc gọi đi trên điện thoại. Người dùng có bộ thu phát có thể tạo ra tín hiệu điện thoại quay ở trạng thái âm kép đa tần để thực hiện các cuộc gọi bị giới hạn trong mô-đun của miếng vá tự động đến các số điện thoại cố định, như cuộc gọi nội hạt hoặc các số điện thoại không mất phí. (BTV)

Sau vài tuần tham dự lớp học buổi tối, tôi đã nắm được mạch liên lạc vô tuyến và các quy định về ham radio để qua bài thi viết, và cũng đã đủ thành thạo về mã Morse để lấy được chứng chỉ. Chẳng bao lâu sau, tôi nhận được một phong bì từ Ủy ban Truyền thông Liên bang (FCC) đựng giấy phép ham radio của tôi, mà không nhiều đứa trẻ mười mấy tuổi có được. Tôi tự hào ghê gớm.

Lừa gạt mọi người bằng ảo thuật cũng thú vị. Nhưng học cách vận hành hệ thống điện thoại mới mê hoặc. Tôi muốn biết mọi thứ liên quan tới công ty

https://thuviensach.vn

điện thoại. Tôi muốn thông thạo cách thức vận hành bên trong đó. Tôi luôn đạt điểm cao hồi cấp 1 và cấp 2, nhưng đến năm lớp 8 hay lớp 9, tôi bắt đầu trốn học và lảng vảng ở Henry Radio, một cửa hàng ham radio phía Tây Los Angeles, để đọc sách về lý thuyết vô tuyến điện hàng giờ liền. Đối với tôi, điều đó tuyệt như một chuyến đi đến Disneyland vậy. Ham radio cũng đem đến một số cơ hội để tôi có thể giúp đỡ cộng đồng. Có dạo tôi hoạt động tình nguyện vào các dịp cuối tuần nhằm cung cấp dịch vụ hỗ trợ thông tin liên lạc cho hội Chữ thập Đỏ địa phương. Có mùa hè tôi cũng làm việc tương tự cả tuần cho kỳ Thế vận hội dành cho người khuyết tật.

Đối với tôi, những chuyến xe buýt hệt như một kỳ nghỉ – tận hưởng khung cảnh thành phố, ngay cả ở những nơi quen thuộc. Thời tiết ở Nam California luôn hoàn hảo, trừ những lúc có sương mù. Vé xe tốn 25 xu, thêm 10 xu để đổi chuyến. Vào kỳ nghỉ hè khi mẹ đi làm, có khi tôi ngồi xe buýt cả ngày. Đến năm 12 tuổi, đầu óc tôi đã nảy ra những ý tưởng khác người. Một ngày tôi phát hiện ra, nếu có thể tự bấm vé chuyển chuyến, mình sẽ chẳng tốn xu nào.

Cha và chú bác tôi đều là những người bán hàng khéo miệng. Tôi đoán mình thừa hưởng gen đó nên ngay từ nhỏ, tôi đã có tài thuyết phục mọi người làm điều gì đó cho mình. Tôi lên xe buýt qua cửa trước và ngồi gần ghế lái. Khi tài xế dừng đèn đỏ, tôi nói: “Cháu đang thực hiện một bài tập ở trường và cần bấm lỗ tạo hình thù hay ho lên mấy miếng bìa các-tông. Cháu thấy cái máy bác dùng để bấm lỗ lượt chuyển chuyến tuyệt quá. Cháu có thể mua nó ở đâu ạ?”

Tôi không nghĩ người tài xế sẽ tin tôi vì điều này nghe thật ngu ngốc. Hẳn ông ấy không ngờ một thằng nhóc ở độ tuổi tôi lại đang cố lợi dụng mình. Ông ấy cho tôi biết tên cửa hiệu, và khi tôi gọi đến đó, họ nói chiếc máy bấm lỗ có giá 15 đô-la. Khi bạn 12 tuổi, bạn có thể nghĩ kế để xin mẹ 15 đô-la không? Tôi làm chuyện đó ngon ơ. Ngay ngày hôm sau, tôi đã có mặt ở cửa hàng để mua máy bấm lỗ. Nhưng đó mới chỉ là Bước 1. Làm thế nào để có được cả một xấp vé chuyển chuyến còn trống?

https://thuviensach.vn

Hừm, người ta rửa xe buýt ở đâu nhỉ? Tôi đi bộ đến một trạm xe gần đó, thấy một thùng rác lớn ở trạm nơi các xe được dọn rửa, đu lên trên đó và nhìn ngó.

Trúng lớn rồi!

Tôi nhét đầy túi những tập vé chưa dùng hết – lần đầu tiên trong vô vàn lần "Lục-thùng-rác" sau này.

Tôi có trí nhớ khá tốt và đã cố gắng nhớ lịch xe buýt của gần như toàn bộ Thung lũng San Fernando. Tôi bắt đầu đi khắp nơi có hệ thống xe buýt – Quận Los Angeles, Quận Riverside, Quận San Bernandino. Tôi vui sướng nhìn ngắm tất cả các địa danh khác nhau đó và thu nhận thế giới xung quanh.

Trong quá trình rong ruổi, tôi kết bạn với Richard Williams, người cũng làm trò tương tự nhưng có chút khác biệt. Thứ nhất, Richard là con trai của một tài xế xe buýt, nên việc cậu ta được đi lại miễn phí bằng xe buýt là điều đương nhiên. Thứ hai (ít nhất lúc đầu là vậy) là cân nặng: Richard mập ú và thường dừng ở Jack in the Box[6] để gọi một phần bánh Taco cỡ lớn 5-6 lần một ngày. Tôi học theo lối ăn uống của cậu ta gần như ngay lập tức và bắt đầu phát tướng phần bụng.

[6] Jack in the Box: Thương hiệu đồ ăn nhanh ở Mỹ. (ND)

Chẳng bao lâu sau, một cô bé với mái tóc vàng tết đuôi sam đi cùng chuyến xe buýt đến trường bảo tôi: "Trông cậu cũng dễ thương đấy, nhưng hơi béo. Cậu phải giảm cân đi."

Liệu tôi có tiếp nhận lời khuyên tuy khó nghe nhưng đúng đắn đó không? Không.

Liệu tôi có gặp rắc rối vì đã lục-thùng-rác để có vé chuyển chuyến và đi xe miễn phí không? Cũng không. Mẹ nghĩ tôi thật thông minh, còn cha nghĩ tôi

https://thuviensach.vn

thật sáng tạo, và những tài xế biết tôi tự bấm vé chuyển chuyến nghĩ đó là một trò vui lớn. Cứ như thể, tất cả những người biết tôi đều đang khuyến khích tôi làm vậy.

Trên thực tế, tôi không cần lời khen ngợi từ mọi người để những trò quỷ đẩy tôi vào rắc rối. Ai ngờ rằng một lần mua sắm nhỏ lại có thể dạy cho tôi một bài học sẽ làm thay đổi cuộc đời tôi sau này… theo một hướng không may?

https://thuviensach.vn

02
CHỈ LÀ GHÉ THĂM

Wbth lal voe htat oy voe wxbirtn vfzbqt wagye C poh aeovsn vojgav?

Rất nhiều gia đình Do Thái dù không mộ đạo vẫn muốn tổ chức lễ trưởng thành Bar mitzvah cho con trai họ và tôi nằm trong số đó. Buổi lễ bao gồm việc đứng trước đám đông và đọc một đoạn trong Kinh Torah – bằng tiếng Hebrew. Dĩ nhiên, tiếng Hebrew sử dụng một bảng chữ cái hoàn toàn khác biệt với các ký tự kiểu שׁ, ך, ב, do đó, người đọc phải mất vài tháng mới có thể thành thạo một đoạn Kinh Torah.

Tôi đăng ký vào một trường Hebrew ở Sherman Oaks nhưng bị đuổi vì tội lười biếng. Mẹ tìm được một vị chỉ huy ban thánh ca để kèm riêng cho tôi, vì vậy tôi không thể né tránh bằng cách lén đọc sách công nghệ dưới gầm bàn nữa. Tôi xoay xở học vừa đủ để hoàn thành nhiệm vụ trong buổi lễ và đọc to đoạn Kinh Torah của mình trước cả giáo đường mà không vấp váp quá nhiều cũng như tự làm xấu mặt bản thân.

Sau buổi lễ, tôi bị cha mẹ mắng vì đã bắt chước giọng đọc và điệu bộ của rabbi[7]. Nhưng đó chỉ là vô thức. Sau này, tôi mới nhận ra đây là một kỹ thuật vô cùng hiệu quả vì con người thường bị cuốn hút bởi những người có nét giống họ. Vậy là ngay từ khi còn rất nhỏ, dù chưa nhận thức rõ nhưng tôi đã luyện tập cái được gọi là "tấn công bằng kỹ thuật xã hội"[8] – một phương thức thao túng người khác, dù vô tình hay cố ý, nhằm tác động đến họ và khiến họ thực hiện những điều thông thường không làm, trong đó bao gồm cả việc thuyết phục mà không khiến họ mảy may nghi ngờ.

[7] Rabbi: Thầy giảng đạo người Do Thái. (BTV)

https://thuviensach.vn

[8] Tấn công bằng kỹ thuật xã hội (social engineering): Phương pháp phi kỹ thuật được dùng để đột nhập vào hệ thống hoặc mạng công ty. Đó là quá trình đánh lừa người dùng của hệ thống, hoặc thuyết phục họ cung cấp thông tin có thể giúp các hacker đáng bại bộ phận an ninh. Có hai hình thức tấn công chính: Dựa vào kỹ thuật khai thác mối quan hệ giữa người với người (human-base) và dựa vào sự trợ giúp của máy tính (computer-base). (BTV)

Trong đống quà đặc trưng của họ hàng và những người tham dự buổi tiệc sau lễ trưởng thành ở nhà hàng Odyssey, tôi thu được một tấm trái phiếu chính phủ Mỹ với con số lớn đến kinh ngạc.

Tôi là một tên mọt sách. Một lần săn sách đã dẫn bước tôi tới tiệm Survival ở Bắc Hollywood. Đây là một tiệm sách nhỏ nằm trong một khu dân cư nhớp nhúa bẩn thỉu. Chủ tiệm, một người phụ nữ trung niên tóc vàng thân thiện, đã đề nghị tôi gọi cô bằng tên riêng thay vì họ. Bên trong cửa tiệm hệt như một chiếc rương kho báu. Thần tượng của tôi thời đó là Bruce Lee, Houdini, Jim Rockford – gã thám tử tư do James Garner thủ vai trong The Rockford Files (tạm dịch: Hồ sơ của Rockford), người có thể bẻ khóa, thao túng mọi người và khoác lên mình bất kỳ thân phận nào trong nháy mắt. Tôi muốn mình có thể làm tất cả mọi thứ chất như Rockford đã làm.

Tiệm sách Survival chứa đầy những cuốn sách mô tả cách để làm được mọi thứ giống như Rockford và cả nhiều thứ khác. Từ năm 13 tuổi, tôi đã dành rất nhiều dịp cuối tuần tại đây, nghiên cứu hết cuốn sách này đến cuốn sách khác suốt cả ngày – chẳng hạn như The Paper Trip (tạm dịch: Hành trình giấy) của Barry Reid với nội dung kể về cách tạo ra một thân phận mới bằng giấy khai sinh của ai đó đã qua đời.

Cuốn The Big Brother Game (tạm dịch: Trò chơi Anh Cả) của Scott French đã trở thành Thánh Kinh của tôi. Cuốn sách hướng dẫn cụ thể cách có được bằng lái xe, giấy sở hữu tài sản, lịch sử tín dụng, thông tin ngân hàng, số điện thoại không đăng ký và cả thông tin từ sở cảnh sát. (Rất lâu sau này, khi một người Pháp viết tiếp câu chuyện, anh ta đã gọi điện đề nghị tôi viết một

https://thuviensach.vn

chương về các phương pháp tấn công bằng kỹ thuật xã hội nhắm tới các công ty điện thoại. Tại thời điểm đó, tôi và đồng sự đang viết cuốn sách thứ hai, The Art of Intrusion (tạm dịch: Nghệ thuật xâm nhập), tôi quá bận nên không thể nhận dự án này dù khá thích thú vì sự trùng hợp này cũng như khá vui vì đã được mời.)

Tiệm sách chứa đầy những cuốn sách "ngầm" dạy bạn những điều lẽ ra không được biết – với một kẻ luôn mang trong mình khao khát có được thứ tri thức từ trái táo cấm, chúng chính là một kho vàng. Tôi đắm chìm trong những kiến thức này, để rồi cuối cùng chúng trở nên vô giá trong suốt thời gian trốn chạy gần hai thập niên sau đó.

Ngoài sách ra, còn có một món đồ hấp dẫn khác trong cửa tiệm: những dụng cụ bẻ khóa giảm giá. Tôi mua vài loại khác nhau. Bạn có nhớ câu chuyện hài cổ này: "Làm thế nào để đến được Carnegie Hall? Luyện tập, luyện tập, luyện tập"?[9] Đó chính là những gì tôi đã làm để thành thạo nghệ thuật bẻ khóa. Đôi khi, tôi cũng xuống khu vực có dãy tủ chứa đồ của người thuê nhà trong tòa chung cư, cạy mở vài chiếc khóa bấm, đổi chỗ cho nhau rồi khóa lại. Lúc ấy, tôi chỉ nghĩ đó là một trò đùa vui vẻ, giờ nghĩ lại, một số người hẳn đã phát điên và rơi vào một đống rắc rối cộng thêm việc phải mua một chiếc khóa mới sau khi xoay xở vứt bỏ chiếc khóa cũ. Tôi đoán là trò đùa chỉ vui khi bạn còn là một tên nhóc con.

[9] Carnegie Hall là hội trường biểu diễn hòa nhạc nổi tiếng thế giới tại New York, Mỹ. Câu chuyện cười về Carnegie có nội dung về một người đi đường hỏi một nghệ sĩ đàn vừa bước ra khỏi taxi: "Làm thế nào để đến được Carnegie Hall?" Nghệ sĩ đàn đã trả lời không hề do dự: "Luyện tập". (ND)

Năm 14 tuổi, một hôm tôi đi chơi cùng bác Mitchell, ngôi sao sáng của đời tôi thuở ấy. Chúng tôi ghé qua Cục Cấp phép Phương tiện Cơ giới (DMV) và thấy rất đông người ở đó. Tôi đứng ngoài đợi trong khi bác Mitchell bước thẳng vào quầy thu ngân – lướt thẳng qua mặt tất cả những người đang xếp hàng. Nhân viên sở, một người phụ nữ với vẻ mặt chán nản, ngước lên đầy

https://thuviensach.vn

ngạc nhiên. Bác Mitchell cũng chẳng buồn đợi cô ta xong việc đang làm với người đàn ông bên cửa sổ mà cất lời luôn. Bác chỉ nói vài lời, sau đó cô nhân viên kia gật đầu, ra hiệu cho người đàn ông nọ bước sang một bên, rồi xử lý việc gì đó mà bác Mitchell yêu cầu. Bác tôi có một loại tài năng đặc biệt trong cách đối xử với mọi người.

Có vẻ tôi cũng được thừa hưởng gen đó. Đây là lần đầu tiên tôi ý thức được về phương pháp tấn công bằng kỹ thuật xã hội.

Mọi người nói gì về tôi thời còn học cấp ba ở trường Monroe? Các thầy cô có lẽ sẽ nói rằng tôi chỉ luôn làm những điều kỳ quặc. Trong khi bạn bè làm việc trong các tiệm sửa chữa tivi thì tôi lại nối gót Steve Jobs và Steve Wozniak tạo ra một chiếc hộp xanh cho phép tôi thao túng hệ thống điện thoại, thậm chí là để gọi điện miễn phí. Tôi luôn mang bên mình chiếc ham radio cầm tay và nói chuyện vào đó suốt giờ ăn và giờ nghỉ.

Một cậu bạn đồng môn đã làm thay đổi cuộc đời tôi. Steven Shalita là một anh chàng kiêu căng không ngừng mơ tưởng sau này trở thành một cảnh sát mật – xe của hắn gắn đầy ăng-ten radio. Hắn thích thể hiện mấy trò bịp bằng điện thoại, và thực sự có thể làm ra những điều kỳ diệu. Shalita biểu diễn cách người khác gọi điện cho hắn mà không để lộ cho họ biết số điện thoại thực của mình bằng cách dùng mạch kiểm tra của công ty điện thoại gọi là “loop-around” (vòng lặp vòng quanh); hắn có thể gọi đến một trong những số điện thoại của một vòng (loop) trong khi người khác đang gọi số thứ hai của vòng đó. Hai người gọi sẽ kết nối với nhau một cách thần kỳ. Hắn có thể có được tên và địa chỉ của bất kỳ số điện thoại nào, dù họ có đăng ký hay không, nhờ gọi tới Cục Tên và Địa chỉ Khách hàng (Customer Name and Addres – CAN) của công ty điện thoại. Chỉ với một cuộc gọi, hắn đã có được số điện thoại chưa từng đăng ký của mẹ tôi. Quá tuyệt! Hắn có thể có được số điện thoại và địa chỉ của bất kỳ ai, thậm chí là một ngôi sao điện ảnh với số không đăng ký. Cứ như thể mấy gã ở công ty điện thoại sinh ra để phục vụ hắn vậy.

https://thuviensach.vn

Tôi bị mê hoặc, thích thú và ngay lập tức trở thành chiến hữu của Shalita, luôn háo hức tìm cách học được tất cả những mánh khóe thần kỳ nhất đó. Nhưng Shalita chỉ có hứng thể hiện mánh khóe của mình thay vì chỉ cho tôi cách, làm sao hắn có thể áp dụng các kỹ năng tấn công bằng kỹ thuật xã hội với những người hắn đang trò chuyện.

Không lâu sau đó, tôi đã học được gần như mọi thứ mà Shalita sẵn lòng chia sẻ về phone phreaking,[10] đồng thời dành hầu hết thời gian rảnh để khám phá mạng viễn thông, tự mày mò và học được cả những gì Shalita không biết. Các phreaker có một mạng xã hội riêng. Tôi bắt đầu làm quen với những người có chung sở thích và đến các buổi giao lưu, dù phải nói rằng vài người trong số họ khá lập dị – xa rời xã hội và chẳng có gì thú vị.

[10] Phone phreaking (Lừa bịp qua điện thoại, hay còn gọi tắt là phreaking): Trò sửa đổi hệ thống điện thoại trái phép để thực hiện các cuộc gọi đường dài mà không phải trả phí; một dạng đùa nghịch phạm pháp. Người thực hiện hành vi này được gọi là phreaker. (Wikipedia)

Có vẻ tôi khá có khiếu với trò tấn công bằng kỹ thuật xã hội của phreaking. Liệu tôi có thể thuyết phục kỹ thuật viên của công ty điện thoại lái xe tới một "CO" (văn phòng trung tâm – trung tâm chuyển mạch của khu dân cư, nơi kết nối các cuộc gọi đến và đi từ điện thoại) vào nửa đêm để kết nối một mạch "khẩn cấp" chỉ vì anh ta nghĩ tôi thuộc một CO khác, hay là nhân viên gác đường dây trong vùng không ư? Quá dễ. Tôi vốn biết mình có tài trong khoản này, nhưng chính Shalita đã dạy cho tôi biết năng lực này có sức mạnh tới cỡ nào.

Mẹo rất đơn giản. Trước khi bắt đầu tấn công phi kỹ thuật vì mục đích nào đó, bạn phải thăm dò trước. Bạn cần kết nối các mẩu thông tin rời rạc về công ty này với nhau, bao gồm các ban ngành hay đơn vị kinh doanh hoạt động thế nào, chức năng là gì, nhân viên trong đó có quyền truy nhập những thông tin nào, quy trình chuẩn để đưa ra yêu cầu ra sao, họ thường đưa ra

https://thuviensach.vn

yêu cầu với ai, ở điều kiện nào thì các thông tin mong muốn được tiết lộ, cả tiếng lóng và các thuật ngữ thường dùng trong công ty nữa.

Tấn công bằng kỹ thuật xã hội thường hiệu quả đơn giản vì mọi người có xu hướng tin tưởng ai đó vốn tạo dựng được sự tín nhiệm, ví dụ như một nhân viên ủy quyền của công ty. Đó chính là lúc cần nghiên cứu. Khi đã chuẩn bị đầy đủ để có được số điện thoại không công khai, tôi gọi điện cho một trong những đại diện phòng kinh doanh của công ty điện thoại và nói: “Tôi là Jake Roberts từ Cục Không Công khai. Tôi cần nói chuyện với người phụ trách.”

Khi người phụ trách cầm máy, tôi giới thiệu bản thân một lần nữa và nói: “Chị đã nhận được thông báo về việc chúng ta thay đổi số điện thoại chưa?”

Cô ta kiểm tra một chút, sau đó quay lại và nói: “Chúng tôi chưa biết việc đó.”

Tôi nói: “Chị đang dùng số 213 687-9962 đúng không?”

“Không,” Cô ta đáp. “Chúng tôi dùng số 213 320-0055.”

Tèn ten!

“Được rồi,” tôi trả lời. “Chúng tôi sẽ gửi thư báo cấp 2 liên quan đến việc thay đổi” – đây là tiếng lóng của công ty điện thoại mà các quản lý thường dùng. “Tạm thời cô cứ tiếp tục dùng số 320-0055 nhé.”

Nhưng khi gọi cho Cục Không Công khai, tôi mới biết hóa ra tên tôi nằm trong danh sách những người được ủy quyền và phải có số điện thoại nội bộ thì mới được cung cấp thông tin khách hàng. Một người thực hiện tấn công bằng kỹ thuật xã hội còn non tay hoặc thiếu khả năng có lẽ sẽ bỏ cuộc. Điều không hay là việc này sẽ làm dấy lên nghi ngờ.

Vận dụng khả năng ứng khẩu của mình, tôi nói: “Quản lý của tôi nói anh ấy đã đưa tên tôi vào danh sách. Tôi sẽ báo lại là cô vẫn chưa nhận được thư

https://thuviensach.vn

báo.”

Còn một chướng ngại khác: Bằng cách nào đó, tôi phải trình ra được số điện thoại nội bộ của công ty.

Tôi phải gọi tới ba phòng kinh doanh khác nhau để tìm ra một vị quản lý thứ cấp là nam giới – người mà tôi có thể giả mạo được. Tôi nói với anh ta, “Tôi là Tom Hansen tới từ Cục Không Công khai. Chúng tôi đang cập nhật lại danh sách các nhân viên có thẩm quyền. Anh có cần ở trong danh sách không?”

Đương nhiên anh ta nói có.

Sau đó, tôi nói anh ta đánh vần tên và cho tôi biết số điện thoại. Dễ như ăn kẹo vậy.

Cuộc gọi kế tiếp là tới RCMAC – Trung tâm Ủy quyền Lưu trữ Thay đổi,[11] một đơn vị của công ty điện thoại có nhiệm vụ thêm vào hoặc bỏ đi các dịch vụ điện thoại khách hàng, chẳng hạn như các tính năng gọi điện tùy chỉnh. Tôi gọi điện trên danh nghĩa quản lý phòng kinh doanh, dễ dàng thuyết phục viên thư ký thêm dịch vụ chuyển tiếp cuộc gọi tới đường dây của viên quản lý bởi số điện đó thuộc về công ty Pacific Telephone.

[11] Các hệ thống chuyển mạch điện tử thường dùng một bộ nhớ gọi là Vừa Thay đổi (Recent Change). Lý do là vì sự thay đổi người dùng và số điện thoại của họ khá thường xuyên, nên dữ liệu này được ghi vào một vùng đặc biệt của bộ nhớ. Trung tâm RCMAC có nhiệm vụ cập nhật Dữ liệu Vừa Thay đổi nếu có yêu cầu. (ND)

Mọi chuyện diễn ra cụ thể như sau: Tôi gọi điện cho kỹ thuật viên ở văn phòng trung tâm. Nghĩ rằng tôi là kỹ sư sửa chữa hiện trường, anh ta nối máy cho tôi vào đường dây của quản lý thông qua một thiết bị cầm tay của nhân viên đường dây và gọi tới số tôi đã đưa, nhờ đó, chuyển tiếp thành công cuộc gọi từ điện thoại của quản lý vào mạch vòng “loop-around” của

https://thuviensach.vn

công ty điện thoại. Mạch vòng là một mạch đặc biệt có hai con số gắn liền với nó. Khi hai bên gọi vào mạch vòng nhờ quay các số tương ứng, họ sẽ được kết nối một cách thần kỳ như thể là họ đã gọi cho nhau.

Tôi quay số vào mạch vòng và kết nối ba chiều bằng một số chỉ đổ chuông. Khi Cục Không Công khai gọi điện tới máy vị quản lý được ủy quyền kia, cuộc gọi sẽ được chuyển tiếp vào vòng, và người gọi có thể nghe tiếng điện thoại chờ kết nối. Tôi để bên kia nghe vài lần chuông đổ, sau đó trả lời: "Steve Kaplan của công ty điện thoại Pacific Telephone xin nghe."

Lúc này, người bên kia đầu dây có thể cung cấp cho tôi bất kỳ thông tin không công khai nào mà tôi cần. Sau đó, tôi gọi điện lại cho tay kỹ thuật viên và hủy chế độ chuyển tiếp cuộc gọi.

Thử thách càng lớn, tôi càng thấy hào hứng. Mẹo này đã hiệu quả trong nhiều năm và tới giờ có lẽ vẫn có tác dụng.

Qua một loạt các cuộc gọi khác nhau – người ta sẽ nghi ngờ nếu tôi gọi cho Cục Không Công khai để hỏi số điện thoại của nhiều người nổi tiếng một lúc – tôi đã có được số điện thoại và địa chỉ của Roger Moore, Lucille Ball, James Garner, Bruce Springsteen và nhiều người khác. Đôi khi, họ quả thực đã nhấc máy, tôi sẽ chào vài câu đại loại như: "Chào Bruce, dạo này anh thế nào?" Việc này chẳng gây hại gì cho ai, chỉ đơn giản là tôi thấy thích thú khi có được bất kỳ số điện thoại nào mình muốn mà thôi.

Có một khóa học về máy tính ở trường cấp ba Monroe. Tôi vốn không đủ điều kiện đăng ký do chưa qua môn Toán và Khoa học như yêu cầu, nhưng thầy Christ phụ trách môn đã nhận tôi vào học sau khi thấy sự hào hứng của tôi và biết tôi đã tự học được khá nhiều. Tôi nghĩ hẳn sau đó thầy sẽ thấy hối hận về quyết định này của mình: Tôi là một tay gây rối khó chịu. Tôi thường ăn trộm mật khẩu kết nối vào máy tính cỡ trung[12] của trường mỗi khi thầy đổi mật khẩu mới. Tuyệt vọng và cố gắng tỏ ra trên cơ tôi, thầy đã dập lỗ mã mật khẩu trên băng giấy máy tính[13], một phương thức lưu trữ dữ liệu thường

https://thuviensach.vn

dùng trước thời đĩa mềm (floppy disk). Như vậy, thầy có thể đưa giấy vào máy đọc băng mỗi lần cần đăng nhập máy tính. Nhưng thầy Christ để mẩu giấy đục lỗ đó trong túi áo sơ mi và không khó để nhìn ra các chấm lỗ qua lớp vải áo mỏng. Một vài người bạn cùng lớp đã giúp tôi đoán được dải lỗ trên băng và biết được mật khẩu mới nhất của thầy sau mỗi lần thầy thay mới. Thầy chưa từng phát hiện ra điều này.

[12] Máy tính cỡ trung (minicomputer): Những máy tính có kích thước lớn hơn máy tính cá nhân. Chúng thường được sử dụng trong kiểm soát quá trình sản xuất, chuyển mạch điện thoại và kiểm soát thiết bị phòng thí nghiệm. (BTV)

[13] Băng giấy máy tính (punched tape): Băng đục lỗ bằng giấy, đây là phương thức lưu trữ dữ liệu bao gồm một dải giấy dài trên đó đục các lỗ mô phỏng dữ liệu. (ND)

Thế rồi nhà trường lắp điện thoại trong phòng thí nghiệm máy tính – một dạng điện thoại kiểu cũ với vòng quay số. Chiếc điện thoại này được lắp đặt chỉ để gọi cho các số nội bộ trong phòng giáo dục địa phương. Bằng việc gọi điện cho người phụ trách chuyển mạch: “Tôi là Christ đây. Tôi cần nối máy ra ngoài,” tôi đã có thể dùng điện thoại kết nối vào máy tính của Đại học Nam California (USC) để chơi điện tử. Sau vài cuộc gọi như vậy, khi người phụ trách bắt đầu nghi ngờ, tôi chuyển sang các mẹo phreaking, trực tiếp gọi điện tới phòng chuyển mạch của công ty điện thoại và đề nghị hủy các thiết lập hạn chế, để có thể nối máy tới USC bất kỳ khi nào muốn. Cuối cùng, thầy Christ cũng phát hiện ra việc tôi đã xoay xở để thực hiện rất nhiều cuộc gọi không giới hạn.

Không lâu sau, thầy tự hào tuyên bố với cả lớp rằng thầy sẽ dứt khoát chặn đứng tôi, và khoe một chiếc khóa được chế tạo đặc biệt dành cho điện thoại quay số: Khi khóa chốt ở vị trí số “1”, vòng quay sẽ không thể xoay tới các vị trí số khác.

https://thuviensach.vn

Ngay khi thầy gắn khóa trước mặt cả lớp, tôi nhấc tay cầm ống nghe điện thoại lên và bắt đầu ấn vào móc chuyển đổi: Chín lượt bấm nhanh để quay số "9" kết nối mạng bên ngoài, Bảy lượt bấm nhanh để quay số "7". Bốn lượt bấm nhanh cho số "4". Chỉ trong vòng một phút, tôi đã kết nối tới USC.

Với tôi, đây chỉ là một trò láu cá. Nhưng thầy Christ tội nghiệp đã bị bẽ mặt trước cả lớp. Thầy đỏ mặt tía tai tóm lấy chiếc điện thoại trên bàn và ném thẳng xuống cuối lớp.

Thời đó, khi tôi đang tự học về RSTS/E (đọc là RIS-tisEE), một hệ điều hành do Digital Equipment Corporation (DEC – Công ty trang thiết bị số) sản xuất, chuyên dùng trong các máy tính cỡ trung của trường học ở vùng trung tâm Los Angeles. Cơ sở Cal State của trường Northridge (SCUN) gần đó cũng dùng hệ điều hành RSTS/E cho máy tính của họ. Tôi đặt lịch hẹn với ngài Wes Hampton, trưởng khoa Khoa học Máy tính của trường, và nói: "Cháu thực sự muốn học về máy tính. Liệu cháu có thể mua một tài khoản để sử dụng máy ở đây không?"

"Không, máy chỉ dành cho các sinh viên của trường thôi."

Bỏ cuộc dễ dàng không phải là tính cách của tôi. "Phòng thí nghiệm máy tính ở trường cấp ba của cháu sẽ đóng cửa vào cuối ngày, tầm 3 giờ chiều. Liệu ngài có thể xây dựng một chương trình giúp các học sinh cấp ba học trên máy tính của trường ngài không?"

Lúc đó, ông từ chối nhưng sau đấy đã gọi lại cho tôi. "Chúng tôi đã quyết định cho phép cậu dùng máy ở đây," ông nói. "Chúng tôi không thể cung cấp cho cậu tài khoản bởi cậu không phải là sinh viên, do vậy tôi sẽ cho cậu dùng tài khoản cá nhân của tôi. Tài khoản là '5,4' và mật khẩu là 'Wes.'"

Người đàn ông này là trưởng khoa Khoa học Máy tính, và đối với ông ấy đây là một mật khẩu an toàn ấy hả – tên riêng ư? An ninh mạng cơ đấy!

https://thuviensach.vn

Tôi bắt đầu mày mò tự học ngôn ngữ Fortran và các ngôn ngữ lập trình cơ bản. Chỉ sau vài tuần ở lớp học máy tính, tôi đã viết một chương trình để đánh cắp mật khẩu của mọi người: Một sinh viên cố gắng đăng nhập vào một cửa sổ trông hệt như cửa sổ đăng nhập quen thuộc nhưng hóa ra đó là chương trình giả mạo hệ điều hành của tôi, được thiết kế để lừa các sinh viên nhập vào đó tài khoản và mật khẩu (tương tự như hình thức tấn công phising[14] ngày nay). Thực ra, một quản lý phòng thí nghiệm CSUN đã giúp tôi sửa lỗi các dòng mã – anh ta cho rằng việc một cậu học sinh cấp ba cố gắng tìm cách đánh cắp mật khẩu của người khác đúng là một chuyện khôi hài. Khi chương trình nhỏ của tôi hoàn thiện và bắt đầu chạy trong phòng thí nghiệm, bất kể khi nào có người đăng nhập, tên và mật khẩu của họ sẽ được bí mật lưu lại trong một tập tin.

[14] Phising (tạm dịch: Tấn công giả mạo): Một phương thức lừa đảo nhằm giả mạo các tổ chức uy tín như ngân hàng, trang web giao dịch trực tuyến và các công ty thẻ tín dụng để lừa người dùng chia sẻ thông tin tài chính như tên đăng nhập, mật khẩu giao dịch hay những thông tin nhạy cảm khác của họ. (BTV)

Tại sao ư? Tôi và bạn bè đều nghĩ thật tuyệt khi có được mật khẩu của tất cả mọi người. Không có kế hoạch gây họa nào cả, chỉ đơn thuần là thu thập thông tin vì thích vậy thôi. Chỉ vì đây là một trong những thử thách mà tôi không ngừng đặt ra cho bản thân trong suốt những năm tháng tuổi trẻ, từ khi tôi bắt đầu nhìn thấy trò ảo thuật đầu tiên. Liệu tôi có thể làm được như vậy không? Liệu tôi có học được cách qua mặt mọi người không? Liệu tôi có thể có được thứ quyền lực lẽ ra không nên có không?

Một thời gian sau đó, một quản lý phòng thí nghiệm đã tố cáo tôi với người quản lý hệ thống. Sau đó, ba bảo vệ an ninh trường đã xồng xộc lao vào phòng thí nghiệm. Họ bắt giữ tôi cho tới khi mẹ tôi đến đón.

Trưởng khoa, người đã cho tôi quyền sử dụng phòng thí nghiệm và cho phép tôi đăng nhập vào tài khoản của ông, đã nổi điên. Nhưng ông chẳng thể làm

https://thuviensach.vn

được gì: Thời đó vẫn chưa có luật chính thức về máy tính để phạt tôi. Dù vậy, đặc quyền dành cho tôi đã kết thúc và tôi được yêu cầu tránh xa khu vực trường học.

Mẹ tôi được cảnh báo: "Từ tháng sau, California sẽ chính thức ra luật định mới, khi đó hành vi của Kevin sẽ là phạm pháp." (Tới tận bốn năm sau đó, Quốc hội Mỹ mới thông qua đạo luật liên bang về tội phạm máy tính, nhưng có lẽ chuỗi hành vi của tôi cũng góp phần đẩy nhanh việc đó.)

Dù sao đi nữa, tôi cũng không chùn bước trước những lời dọa dẫm. Không lâu sau khi chuyện đó xảy ra, tôi đã tìm ra cách để làm chệch hướng các cuộc gọi từ những người ở Rhode Island tới tổng đài cung cấp số điện thoại và nối chúng tới máy của tôi. Tôi đã bày trò giỡn chơi với mấy người đang cần tìm số điện thoại như thế nào ư? Một cuộc gọi điển hình sẽ diễn ra như sau:

Tôi: Thành phố nào thưa ngài?

Người gọi: Providence.

Tôi: Tên gì thưa ngài?

Người gọi: John Norton.

Tôi: Cơ sở kinh doanh hay nhà riêng?

Người gọi: Nhà riêng.

Tôi: Số điện thoại là 836, 5 một-nửa 66

Tới lúc này, người gọi thường sẽ ngơ ngác hoặc nổi xung lên.

Người gọi: Tôi quay một-nửa thế nào?

Tôi: Ngài hãy ra ngoài kiếm cái điện thoại mới có số một-nửa trên đó ấy.

https://thuviensach.vn

Phản ứng của họ thực sự rất tức cười.

Thời đó, có hai công ty điện thoại riêng biệt cung cấp dịch vụ trên các khu vực khác nhau ở Los Angeles. Công ty General Telephone and Electronics (GTE) phụ trách phía bắc Thung lũng San Fernado nơi chúng tôi sống. Bất kỳ cuộc gọi nào có khoảng cách hơn 19km đều bị tính ở mức giá dành cho cuộc gọi đường dài. Dĩ nhiên, tôi không muốn tạo áp lực lên hóa đơn điện thoại của mẹ, do đó tôi đã thực hiện vài cú điện thoại qua miếng vá tự động của máy ham radio địa phương.

Một ngày nọ, tôi đã nổi xung lên với tay trực bộ chuyển tiếp sóng[15] chỉ vì "những cú điện thoại quái đản" của tôi, theo cách mà ông ta gọi. Ông ta để ý thấy tôi thường nhấn những chuỗi dài các số khi sử dụng miếng vá tự động. Tôi cũng không định giải thích rằng những dãy số đó là để gọi các cuộc gọi miễn phí thông qua một nhà cung cấp dịch vụ cuộc gọi đường dài có tên là MCI. Dù không biết rõ tôi thực sự làm gì, nhưng ông ta không thích tôi sử dụng miếng vá tự động theo kiểu kỳ lạ như vậy. Một người nghe được cuộc tranh cãi này đã liên lạc với tôi qua sóng vô tuyến điện. Cậu ta giới thiệu mình tên là Lewis De Payne và cho tôi số điện thoại. Tôi gọi điện cho cậu ta ngay tối hôm đó. Lewis nói cậu ta rất ấn tượng với những gì tôi đã làm.

[15] Bộ chuyển tiếp sóng (repeater): Thiết bị dùng để thu và chuyển tiếp sóng vô tuyến điện. Đối với wifi, đây là thiết bị dùng để thu và khuếch đại sóng wifi. (BTV)

Chúng tôi hẹn gặp và trở thành bạn bè, mối quan hệ kéo dài tới hai thập kỷ. Thừa hưởng dòng máu Argentina, Lewis là một kẻ nghiền công nghệ[16], trông khá mảnh khảnh với mái tóc đen ngắn, bóng mượt và vuốt ngược ra sau cùng hàng ria mép mà có lẽ cậu ta nghĩ có thể khiến mình trông già dặn hơn. Trong các dự án hacking, Lewis là người khiến tôi tin tưởng nhất dù con người cậu ta đầy mâu thuẫn. Lịch sự nhưng luôn muốn nắm quyền kiểm soát. Gã mọt sách với thứ thời trang áo cổ lọ và quần loe lỗi thời nhưng cũng đầy lịch thiệp. Không quá sôi nổi nhưng lại ngạo mạn, kiêu căng.

https://thuviensach.vn

[16] Từ gốc “geeky”: Tiếng lóng ám chỉ những người đam mê công nghệ và máy tính, có trình độ kiến thức nhất định. (ND)

Lewis và tôi đều có khiếu hài hước. Tôi cho rằng bất kỳ sở thích nào nếu không mang lại niềm vui và tiếng cười thì đều không đáng mất thời gian và tâm sức. Lewis và tôi bắt được sóng của nhau. Ví dụ như “Trò hack McDonald’s”. Chúng tôi phát hiện ra cách điều chỉnh vô tuyến điện sóng 2m giúp giọng nói của mình có thể phát ra từ loa đặt tại khu vực gọi đồ ăn drive-through[17] trong các quán ăn nhanh. Chúng tôi lái xe tới gần McDonald’s, đỗ xe gần đó để có thể quan sát mà không bị phát hiện, sau đó điều chỉnh tần số của chiếc radio cầm tay khớp với tần số của nhà hàng.

[17] Drive-through: Dịch vụ mua đồ trực tiếp ngay trên xe ô tô có làn đường riêng biệt, qua đó khách hàng có thể đặt món ở một cửa sổ và nhận đồ ở cửa sổ kế tiếp. (ND)

Một xe cảnh sát rẽ vào đường drive-through. Khi tới gần loa, Lewis và tôi sẽ đọc thông báo: “Rất xin lỗi. Ở đây chúng tôi không phục vụ cảnh sát. Anh hãy chuyển qua Jack in the Box đi!” Còn có một người phụ nữ dừng xe và nghe giọng phát thanh qua loa (của tôi): “Hãy cho tôi xem ngực cô, đổi lại chiếc Big Mac này sẽ miễn phí!” Cô ta phản ứng khá dữ dội, tắt xe, vớ lấy thứ gì đó sau cốp và chạy vào trong… tay cầm theo chiếc gậy bóng chày.

“Nước táo tặng kèm” là một trong những trò khoái trí nhất của tôi. Sau khi khách hàng gọi đồ, chúng tôi giải thích rằng máy làm đá bị hỏng, do đó, chúng tôi sẽ tặng nước quả miễn phí. “Chúng tôi có nước nho, nước cam, và… a xin lỗi, có vẻ như chúng tôi đã hết nước nho và cam. Anh có thích nước táo không?” Khi khách hàng nói có, chúng tôi sẽ bật đoạn ghi âm một người đang tè vào cốc, và nói: “Được rồi. Nước táo của anh đã xong. Mời anh lái xe tới cửa sổ để nhận.”

Chúng tôi khoái trá khi khiến mọi người phát điên vì không thể gọi được đồ. Mỗi khi có khách hàng dừng xe và đặt đồ, một người bạn của chúng tôi sẽ

https://thuviensach.vn

lặp lại yêu cầu của họ qua loa bằng thứ giọng Ấn Độ rất nặng, khó mà nhận ra anh ta đã nói từ gì. Vị khách trả lời rằng anh ta không hiểu, và bạn tôi lại nói gì đó mà vị khách kia cũng không thể hiểu, cứ lặp đi lặp lại như vậy – cho đến khi khách hàng phát điên, hết người này tới người khác.

Phần tuyệt nhất là mọi lời chúng tôi nói tại cửa drive-through sẽ phát ra om sòm trên loa, và nhân viên bên trong cửa hàng không thể chèn tiếng họ vào. Thỉnh thoảng, chúng tôi thấy mấy vị khách ngồi bàn ngoài vừa ăn bánh kẹp vừa cười sặc sụa. Không ai phát hiện ra chuyện gì đã diễn ra.

Có lần, người quản lý chạy ra ngoài để xem ai đã bày trò với chiếc loa phát. Ông ta liếc quanh khu đỗ xe, rồi gãi đầu. Không có ai xung quanh. Mọi chiếc xe đều trống không. Không có ai núp sau những tấm biển. Ông ta bước tới chiếc loa và nghiêng người tới gần, liếc nhìn như thể trông đợi có thể phát hiện ra một người tí hon nào đó ở trong.

“Ông nhìn cái quái gì thế?” Tôi gào lên như thể đang giận dữ.

Ông ta có lẽ đã lăn đùng ngã ngửa.

Đôi khi, cũng có những người sống ở khu chung cư quanh đó đứng trên ban công cười bò trước trò giỡn của chúng tôi. Cả những người đi bộ trên đường cũng không nhịn được cười. Vài lần, Lewis và tôi cũng rủ thêm bạn bè theo, vì trò này thực sự rất khôi hài.

Thôi được, tôi biết việc tôi làm thật trẻ con, nhưng dạo đó tôi cũng chỉ 16, 17 tuổi thôi mà.

Một số hành động bừa bãi của tôi không hề vô thưởng vô phạt. Tôi có một nguyên tắc riêng, đó là không đột nhập vào các công ty điện thoại, dù điều đó có thể giúp tôi đăng nhập vào hệ thống và đọc được vài tài liệu hướng dẫn kỹ thuật của họ. Dĩ nhiên, đối với tôi, đây là “định hướng” hơn là nguyên tắc.

https://thuviensach.vn

Một buổi tối năm 1981, khi 17 tuổi, tôi chơi với một tay phreaker khác có tên Steve Rhoades. Chúng tôi quyết định sẽ lẻn vào phòng trung tâm Sunset-Gover của công ty điện thoại Pacific Telephone ở Hollywood. Vì chúng tôi đã hack vào mạng lưới điện thoại trước đó, nên việc trực tiếp thâm nhập vào một công ty điện thoại là thử thách cuối cùng. Để vào được bên trong, chúng tôi cần ấn đúng mã số cửa. Nhờ tấn công bằng kỹ thuật xã hội, việc có được mã số cũng không phải là vấn đề gì to tát. Chúng tôi tiến thẳng vào trong.

Lạy Chúa – quá tuyệt! Đối với chúng tôi, đây là sân chơi cuối cùng. Nhưng chúng tôi nên tìm cái gì đây?

Một người đàn ông to lớn trong trang phục bảo vệ đi kiểm tra quanh tòa nhà và tóm được chúng tôi. Anh ta chẳng khác nào một gã vệ sĩ trong các câu lạc bộ đêm hay tiền vệ bóng bầu dục chơi trong Giải Bóng Bầu dục Mỹ – trông rất đáng sợ. Anh ta chỉ cần đứng yên đó, hai tay buông lơi đã đủ dọa người khác sợ đến tụt quần. Nhưng không hiểu sao, tình huống càng căng thẳng, tôi lại càng trở nên bình tĩnh.

Dù không có vẻ già dặn giống một nhân viên công ty, nhưng tôi vẫn chủ động tiến đến. “Chào anh,” tôi nói. “Anh thế nào?”

Gã bảo vệ nói: “Tốt, thưa ngài. Tôi có thể xem thẻ ID của ngài được không?”

Tôi kiểm tra các túi. “Chết tiệt! Chắc tôi để trên xe rồi. Để tôi chạy ra lấy nhé.”

Anh ta không dễ mắc lừa. “Không, mời cả hai anh cùng lên tầng trên với tôi.”

Chúng tôi không tranh cãi.

Anh ta đưa chúng tôi lên Trung tâm Kiểm soát Chuyển mạch ở tầng 9, nơi các nhân viên khác đang làm việc.

https://thuviensach.vn

Tim đập thình thịch. Thở không ra hơi.

Vài tay kỹ sư chuyển mạch tiến đến xem có chuyện gì xảy ra. Tôi nghĩ lựa chọn duy nhất lúc này là tháo chạy để thoát khỏi gã bảo vệ, nhưng dù vậy thì khả năng trốn được cũng rất mong manh. Tôi thấy tuyệt vọng, như thể tôi chỉ cách những chấn song nhà tù một bước nữa thôi.

Nhưng tại thời điểm đó, tôi đã biết đủ tên và các chức vụ ở Pacific Telephone để thử thêm vài mánh khóe. Tôi giải thích: "Tôi làm việc tại COSMOS ở San Diego, và tôi đang chỉ cho một người bạn thăm quan văn phòng trung tâm một chút. Anh có thể gọi cho sếp của tôi để kiểm tra." Và tôi đưa cho anh ta tên của một người giám sát ở COSMOS. Ơn giời, tôi có một trí nhớ khá tốt. Dù tôi biết chúng tôi trông không giống như người thuộc về nơi này và câu chuyện tôi bịa ra đúng là nhảm nhí.

Gã bảo vệ tìm tên của người giám sát trong sổ danh bạ liên công ty, tìm số máy bàn và gọi điện. Reng, reng, reng. Anh ta xin lỗi vì đã gọi điện vào giờ này và giải thích tình huống xảy ra.

Tôi nói: "Để tôi nói chuyện với cô ấy."

Anh ta đưa điện thoại cho tôi. Tôi dí sát ống nghe vào tai, hy vọng anh ta không nghe thấy tiếng người nói trong điện thoại và phát huy khả năng ứng biến của mình: "July, xin lỗi cô nhưng tôi đang đưa bạn đi thăm một vòng trung tâm chuyển mạch và để quên thẻ ID trong xe. Anh bảo vệ chỉ muốn xác minh việc tôi thuộc trung tâm COSMOS ở San Diego. Tôi hy vọng cô không để bụng."

Tôi ngừng vài nhịp, giả vờ đang lắng nghe câu trả lời. Cô ta gào lên trong điện thoại. "Anh là ai? Tôi có biết anh không? Anh đang làm gì ở đấy?"

Tôi lại bắt đầu. "Chỉ là đằng nào tôi cũng phải ở đây vào buổi sáng vì vụ sổ tay hướng dẫn đào tạo mới. Tôi còn có buổi gặp xét duyệt với Jim vào 11

https://thuviensach.vn

giờ thứ Hai nữa, nếu cô muốn tham gia. Chúng ta vẫn giữ lịch hẹn ăn trưa vào thứ Ba chứ?”

Tôi ngừng lại một chút. Cô ta vẫn tiếp tục quát mắng.

“Chắc rồi! Xin lỗi vì đã làm phiền cô,” tôi nói.

Và rồi tôi gác máy.

Gã bảo vệ và mấy tay kỹ sư chuyển mạch trông có vẻ bối rối; họ nghĩ tôi sẽ đưa lại máy cho bảo vệ để vị giám sát này có thể khẳng định mọi chuyển vẫn ổn. Các bạn có thể tưởng tượng được khuôn mặt của gã bảo vệ lúc đó: Liệu anh ta có dám gọi điện làm phiền cô ấy lần thứ hai không?

Tôi nói với anh ta: “Cô ấy khá bực vì bị đánh thức vào lúc hai rưỡi sáng.”

Sau đó tôi nói: “Tôi chỉ muốn chỉ cho bạn mình vài thứ nữa thôi. Tôi sẽ ở đây thêm chừng 10 phút.”

Tôi bước ra ngoài, Rhoades theo ngay sau.

Hiển nhiên là tôi muốn chạy nhưng tôi biết mình không thể.

Chúng tôi tiến đến thang máy. Tôi đập nút đi xuống tầng trệt. Chúng tôi thở phào khi bước ra khỏi tòa nhà, sợ thót tim nhưng thực hạnh phúc vì đã thoát khỏi đó.

Và tôi biết điều gì sẽ xảy ra sau đó. Người phụ nữ kia sẽ điên cuồng gọi điện khắp nơi lúc nửa đêm, cố gắng tìm ra ai đó biết số điện thoại phòng bảo vệ của trung tâm Sunset-Gower.

Chúng tôi vào xe. Tôi lái qua vài dãy nhà mà không bật đèn xe, sau đó dừng lại và ngồi yên, nhìn ra phía cửa trước của tòa nhà.

https://thuviensach.vn

Chỉ khoảng 10 phút sau, gã bảo vệ lực lưỡng lao ra, nhìn khắp xung quanh và biết rằng chúng tôi đã đi rất xa. Dĩ nhiên, hắn đã nhầm.

Tôi đợi đến khi hắn quay vào trong rồi mới lái xe đi và chỉ bật đèn xe sau khúc rẽ đầu tiên.

Một cú suýt chết. Nếu gã bảo vệ gọi cho cảnh sát, chúng tôi sẽ bị định tội đột nhập, và thậm chí tệ hơn là trộm cắp. Steve và tôi có lẽ đã bị tống ngay vào trại cải tạo dành cho thanh thiếu niên.

Tôi sẽ không quay lại công ty điện thoại sớm đâu, nhưng tôi đã quyết tâm phải tìm ra được điều gì đó – một điều lớn lao – để thử thách năng lực của mình.

https://thuviensach.vn

03
TỘI LỖI ĐẦU TIÊN

Nyrk grjjnfiu uzu Z xzmv k f jvk lg re rttflek fe Kyv Rib?

Sau khi tìm ra cách lấy được các số điện thoại không công khai, tôi rất háo hức tìm kiếm thông tin về mọi người – bạn bè, bạn của bạn bè, giáo viên, hay thậm chí là người lạ. Cục Cấp phép Phương tiện Cơ giới (Department of Motor Vehicles – DMV) là một kho thông tin tuyệt vời. Liệu có cách nào để tôi có thể động vào đó được không?

Để bắt đầu, tôi gọi đến văn phòng DMV từ điện thoại công cộng ở một quán ăn và nói đại loại rằng: "Tôi là sĩ quan Campbell, thuộc Phòng Cảnh sát Los Angeles, đồn Van Nuys. Máy tính của chúng tôi bị hỏng, mà vài sĩ quan ngoài hiện trường đang cần một số thông tin. Các anh có thể giúp tôi không?"

Người nhận điện ở DMV nói: "Tại sao anh không gọi bằng đường dây của lực lượng chấp pháp?"

Ồ, được rồi – có số điện thoại riêng dành cho cảnh sát. Làm thế nào để tìm được số điện thoại này đây? Dĩ nhiên, các cảnh sát ở đồn sẽ biết, nhưng… chẳng nhẽ tôi lại gọi đến đồn cảnh sát để lấy thông tin giúp mình phạm pháp ư? Ồ, tất nhiên rồi.

Gọi đến đồn cảnh sát gần nhất, tôi nói tôi đến từ Phòng Cảnh sát trưởng Los Angeles, chúng tôi cần gọi cho DMV nhưng viên sĩ quan biết số điện thoại dành cho lực lượng chấp pháp đã ra ngoài. Tôi cần người trực tổng đài cho tôi số điện thoại đó. Và cô ấy đã làm vậy. Chỉ đơn giản thế thôi.

https://thuviensach.vn

(Gần đây, khi nhớ lại câu chuyện này, tôi nghĩ rằng mình vẫn còn nhớ số của lực lượng chấp pháp ở DMV hoặc vẫn có thể lấy được nó. Tôi nhấc điện thoại lên và quay số. DMV có một hệ thống điện thoại Centrex, vì thế, tất cả các số điện thoại đều có chung mã vùng và đầu số: 916-657. Chỉ có phần số máy cuối – 4 số cuối – là khác nhau giữa các phòng ban. Tôi chọn 4 số cuối ngẫu nhiên, kiểu gì cũng gặp một ai đó ở DMV và có được sự tín nhiệm bởi tôi đã gọi đến một số điện thoại nội bộ.

Người nghe điện nói điều gì đó tôi không hiểu.

Tôi nói: "Đây có phải là số điện thoại dành cho lực lượng chấp pháp không?"

Cô ấy nói: "Không."

"Vậy chắc tôi gọi nhầm số rồi," tôi nói. "Số của lực lượng chấp pháp là gì vậy?"

Cô ấy cho tôi biết! Sau ngần ấy năm, họ vẫn chưa "khôn" ra.)

Sau khi gọi đến đường dây dành cho lực lượng chấp pháp ở DMV, tôi phát hiện ra có một lớp bảo vệ thứ hai. Tôi sẽ cần một "Mã yêu cầu". Cũng như trước kia, tôi phải bịa ra một câu chuyện ngay lúc tình thế nước sôi lửa bỏng này. Tôi nói với người nhân viên bằng giọng lo lắng: "Chúng tôi vừa có một tình huống khẩn cấp ở đây, tôi sẽ gọi lại sau."

Tôi lại gọi đến đồn cảnh sát Los Angeles Van Nuys, nói rằng tôi là người của DMV và hiện đang soạn một cơ sở dữ liệu mới. "Mã yêu cầu của các anh là 36472 phải không?"

"Không, là 62883."

(Tôi phát hiện ra mánh này thường rất hiệu quả. Nếu bạn hỏi một thông tin nhạy cảm nào đó, người khác sẽ lập tức sinh nghi. Nhưng nếu bạn giả vờ đã

https://thuviensach.vn

có thông tin đó và đưa cho họ thông tin sai, thường thì họ sẽ sửa lại cho bạn – trao cho bạn thông tin đang tìm kiếm.)

Chỉ với vài phút gọi điện, tôi đã có số bằng lái xe và địa chỉ nhà của bất cứ ai trong bang California, hay dùng biển số xe để lấy được các thông tin chi tiết như tên chủ xe và địa chỉ, hoặc dùng tên ai đó để lấy thông tin đăng ký xe của họ. Tại thời điểm đó, đây chỉ là một phép thử về kỹ năng của tôi nhưng sau này, DMV sẽ trở thành mỏ thông tin để tôi tận dụng theo vô vàn cách khác nhau.

Tất cả những công cụ mà tôi đã thu thập thêm giống như những món tráng miệng ở cuối bữa ăn vậy. Món chính của tôi vẫn là phone phreaking. Tôi gọi đến rất nhiều văn phòng Pacific Telephone và General Telephone, thu thập thông tin chỉ để thỏa mãn cơn khát "Mình có thể lấy được thông tin gì?", thực hiện các cuộc gọi để xây cho mình ngân hàng thông tin về các phòng ban, các quy trình, cách nói chuyện của các công ty và chuyển cuộc gọi của tôi qua các nhà mạng đường dài để chúng khó bị truy dấu hơn. Hầu hết đều là từ điện thoại của mẹ trong căn hộ của chúng tôi.

Tất nhiên, các phreaker muốn ghi điểm bằng cách cho các phreaker khác thấy những thứ mới mẻ họ đã học được cách làm. Tôi thích chơi khăm lũ bạn, dù chúng là phreaker hay không. Một hôm, tôi đã hack vào bộ chuyển mạch[18] của công ty điện thoại phục vụ khu vực mà anh bạn Steve Rhoades của tôi đang sống với bà, đổi "mã lớp đường dây" (line class code) từ khu dân cư sang điện thoại công cộng. Mỗi khi Steve hay bà của cậu ta định gọi điện, họ sẽ nghe thấy câu: "Xin hãy bỏ vào 10 xu." Tất nhiên, cậu ta biết ai đã làm trò đó và sẽ gọi điện để cằn nhằn. Tôi hứa sẽ chỉnh lại như cũ, và đúng là tôi đã làm vậy, nhưng là đổi sang dịch vụ điện thoại công cộng trong tù. Giờ thì mỗi khi họ định gọi điện, một viên trực tổng đài sẽ nói: "Đây là cuộc gọi tính phí người nghe. Xin cho biết tên." Steve gọi và nói, "Hay lắm – đổi lại đi." Tôi cười đủ rồi đổi lại.

https://thuviensach.vn

[18] Thiết bị chuyển mạch (switch): Thiết bị dùng để kết nối các đoạn mạng với nhau theo mô hình mạng hình sao. Theo mô hình này, thiết bị chuyển mạch đóng vai trò là thiết bị trung tâm, tất cả các máy tính đều được nối về đây. (BTV)

Các tay phreaker đã tìm ra cách thực hiện cuộc gọi miễn phí, tận dụng kẽ hở trong một số loại "chia nhánh điện thoại" (diverter) – các thiết bị được dùng để cung cấp tính năng chuyển tiếp cuộc gọi (ví dụ, chuyển cuộc gọi đến cho các dịch vụ trả lời) vào thời kỳ trước khi tính năng chuyển tiếp cuộc gọi được cung cấp bởi các công ty điện thoại. Một phreaker sẽ gọi đến vào thời điểm anh ta biết chắc đơn vị kinh doanh đã đóng cửa. Khi dịch vụ trả lời bắt máy, anh ta sẽ hỏi một câu đại loại như: "Chỗ các anh mở cửa lúc mấy giờ?" Khi người trả lời ngắt máy, phreaker sẽ tiếp tục giữ máy; sau đó một lúc, anh ta sẽ nghe thấy âm hiệu quay số[19]. Lúc này, phreaker có thể gọi miễn phí đến bất kỳ số điện thoại nào trên thế giới – tiền cước gọi sẽ bị tính cho đơn vị kinh doanh kia.

[19] Âm hiệu quay số (dial tone): Tiếng trong máy điện thoại phát ra cho biết có thể quay số điện thoại mà ta muốn gọi. (BTV)

Cũng có thể dùng bộ chia nhánh điện thoại để nhận các cuộc gọi đến cho các số gọi lại[20] trong một cuộc tấn công phi kỹ thuật.

[20] Số gọi lại (call-back): Khi Alice gọi cho Bob và máy của Bob đang bận, nếu dịch vụ điện thoại cho phép, Alice có thể để lại số điện thoại để Bob có thể gọi lại cho Alice. Lưu ý rằng câu chuyện xảy ra trước khi có điện thoại di động, người nghe điện thoại thường không có cách nào biết được mình vừa lỡ điện thoại cũng như lỡ điện thoại của ai. (ND)

Một cách tiếp cận bộ chia nhánh điện thoại khác là phreaker sẽ gọi đến một số "tự động xác định số điện thoại" (số ANI)[21] của các kỹ thuật viên công ty điện thoại. Một khi đã biết được số này, phreaker sẽ biến nó trở thành số gọi lại của mình. Để nhận cuộc gọi, phreaker sẽ gọi đến số chính của đơn vị

https://thuviensach.vn

kinh doanh nhận chuyển cuộc gọi. Nhưng lần này, khi bộ chia nhánh điện thoại chuyển sang đường dây thứ hai để gọi đến dịch vụ trả lời, về bản chất nó sẽ trả lời cuộc gọi đến.

[21] Tự động xác định số điện thoại (automatic number identification): Một tính năng tự động của mạng viễn thông nhằm xác định số điện thoại gốc trong các cuộc gọi nhằm mục đích tính tiền cước. (BTV)

Tôi dùng cách này để nói chuyện với anh bạn Steve vào một tối muộn. Cậu ta nghe máy thông qua đường dây chuyển hướng thuộc về một công ty có tên là Prestige Coffee Shop ở Thung lũng San Fernando.

Chúng tôi đang tán gẫu về phone phreaking thì bỗng nhiên có một giọng nói cắt ngang cuộc trò chuyện.

“Chúng tôi đang theo dõi các cậu đấy,” người lạ nói.

Steve và tôi cúp máy ngay lập tức. Chúng tôi gọi trực tiếp cho nhau, cười nhạo nỗ lực cỏn con của công ty điện thoại để dọa chúng tôi, nói với nhau rằng hội làm ở đó là một lũ ngớ ngẩn ra sao. Giọng nói cũ lại cắt ngang: “Chúng tôi vẫn đang theo dõi các cậu đấy!”

Bây giờ ai mới là bọn ngớ ngẩn?

Một thời gian sau, mẹ tôi nhận được một lá thư từ General Telephone (GTE), sau đó là một cuộc gặp mặt trực tiếp với Don Moody, trưởng Bộ phận An ninh của công ty, người đã cảnh báo mẹ tôi rằng nếu tôi không dừng mấy trò đang làm, GTE sẽ hủy dịch vụ điện thoại của chúng tôi vì tội lừa đảo và chiếm dụng. Mẹ đã bị sốc và bối rối bởi ý nghĩ sẽ bị cắt dịch vụ điện thoại. Và Moody đã không nói đùa. Khi tôi tiếp tục trò phreaking, GTE đã hủy dịch vụ của chúng tôi. Tôi nói mẹ đừng lo, tôi có một ý tưởng.

Công ty điện thoại gán mỗi đường dây điện thoại với một địa chỉ nhất định. Số điện thoại bị hủy của chúng tôi được gán cho Hộ 13. Giải pháp của tôi

https://thuviensach.vn

khá đơn sơ: Đến cửa hàng thiết bị và lục tìm bộ chữ cái và số mà bạn thường gắn lên cửa trước nhà mình. Tôi trở về căn hộ, bỏ số "13" xuống và đóng số "12B" lên đó.

Sau đó, tôi gọi đến GTE và nói chuyện với đơn vị xử lý việc cấp phát số. Tôi giải thích rằng có một căn hộ 12B mới vừa được thêm vào khu căn hộ và muốn họ sửa đổi hồ sơ cho phù hợp. Họ nói sẽ mất 24-48 tiếng để cập nhật hệ thống.

Tôi đợi.

Khi tôi gọi lại, tôi nói mình là người mới chuyển đến 12B và muốn đặt dịch vụ điện thoại. Người phụ nữ ở công ty điện thoại hỏi tôi muốn số điện thoại gán cho tên gì.

"Jim Bond," tôi nói. "À, không… tại sao không biến nó thành tên hợp pháp của tôi nhỉ? James."

"James Bond," cô ta nhắc lại, không có phản ứng gì – ngay cả khi tôi trả thêm phí để chọn số của riêng mình: 895-5…007[22].

[22] James Bond: Tên của điệp viên 007 trong loạt phim hành động cùng tên nổi tiếng của Mỹ. (ND)

Sau khi cài xong máy điện thoại, tôi gỡ số "12B" ngoài cửa và trả lại đó số "13". Phải mất vài tuần để ai đó bên GTE phát hiện ra và hủy dịch vụ.

Nhiều năm sau tôi mới biết rằng đó là khi GTE bắt đầu lập hồ sơ về tôi. Năm đó tôi 17 tuổi.

Cũng vào khoảng thời gian đó, tôi biết một gã tên là Dave Kompel, dù đã đầu hai đít chơi vơi nhưng vẫn chưa hết đống mụn tuổi dậy thì, tệ đến mức chúng làm mặt gã biến dạng. Trong vai trò phụ trách bảo trì máy tính cỡ trung PDP-11/70 chạy hệ điều hành RSTS/E của Khu học chánh Los

https://thuviensach.vn

Angeles, gã cùng một vài người bạn sở hữu những kiến thức về máy tính mà tôi rất khâm phục. Thèm khát được tiếp nhận vào hội của họ để được chia sẻ thông tin, tôi đưa ra đề nghị với Dave và một người trong số bạn của gã, Neal Goldsmith. Neal là một gã béo phì, tóc ngắn và có vẻ được một gia đình giàu có nuông chiều. Cuộc đời gã có lẽ chỉ xoay quanh đồ ăn và máy tính.

Neal nói với tôi rằng họ sẽ chỉ đồng ý cho tôi vào hội nếu tôi có thể chứng minh được mình trước. Họ muốn tôi truy cập vào một hệ thống máy tính gọi là "Ark". Đây là một hệ thống ở Digital Equipment do nhóm phát triển RSTS/E sử dụng. Gã bảo tôi: "Cậu phải hack vào Ark thì chúng tôi mới biết là cậu đủ trình để cùng chúng tôi chia sẻ thông tin." Và để giúp tôi bắt đầu, Neal đã có sẵn số dial-up[23] mà một người bạn làm ở Đội Phát triển RSTS/E cho gã.

[23] Dial-up: Thuật ngữ trong ngành công nghệ thông tin, chỉ việc kết nối Internet hoặc các mạng nội bộ thông qua giao thức kết nối sử dụng đường truyền điện thoại. Để truy cập vào giao thức này, bạn cần có tên và mật khẩu. (Wikipedia)

Gã ra thử thách này cho tôi bởi gã biết tôi sẽ không đời nào làm được.

Thử thách này có thể bất khả thi, nhưng chắc chắn tôi sẽ thử.

Số modem hiện ra trên màn hình đăng nhập của Ark, nhưng tất nhiên bạn phải nhập số và mật khẩu hợp lệ. Làm thế nào tôi có thể lấy được những thông tin xác minh này?

Tôi có một kế hoạch có thể sẽ thành công, nhưng để bắt đầu, tôi cần biết tên của người quản trị hệ thống – không phải người trong nhóm phát triển mà là người quản lý các hệ thống máy tính bên trong Digital. Tôi gọi đến phòng chuyển cuộc gọi cho cơ sở ở Merrimack, New Hampshire, nơi đặt Ark, và yêu cầu được nối máy đến phòng máy tính.

https://thuviensach.vn

“Anh muốn gọi đến phòng nào?”, người ở phòng chuyển cuộc gọi hỏi.

Á! Tôi chưa bao giờ nghĩ đến việc tìm hiểu xem Ark thuộc phòng nào. Tôi nói đại: “Phòng phát triển RSTS/E.”

“À, ý anh là phòng có sàn nâng. Tôi sẽ nối máy cho anh.” (Các hệ thống máy tính lớn thường được đặt trên các sàn nâng để hệ thống dây cáp cồng kềnh có thể chạy bên dưới.)

Một phụ nữ nhấc máy. Tôi đang tham gia một canh bạc, nhưng họ sẽ không thể truy dấu được cuộc gọi này, nên ngay cả khi họ có nghi ngờ, tôi cũng không mất gì nhiều.

“Có phải PDP-11/70 cho Ark đặt ở phòng này không?” tôi hỏi, đưa ra tên hệ thống máy tính DEC mạnh nhất bấy giờ, thứ mà tôi đoán nhóm phát triển đang sử dụng.

Câu trả lời của người phụ nữ kia đã khẳng định điều này.

“Tôi là Anton Chernoff,” tôi trơ trẽn khẳng định. Chernoff là một trong những nhà phát triển chủ chốt trong đội phát triển RSTS/E, vì thế, tôi đang liều mình chấp nhận rủi ro lớn rằng cô ta không quen giọng của Anton. “Tôi đang gặp trục trặc trong việc đăng nhập vào tài khoản ở Ark.”

“Vậy thì anh phải liên hệ với Jerry Covert.”

Tôi hỏi số máy lẻ của anh ta; cô ta đưa cho tôi không chút ngại ngần. Khi gọi cho Jerry Covert, tôi nói: “Hey, Jerry, Anton đây,” đoán rằng ngay cả khi anh ta không biết Chernoff ngoài đời thì hẳn cũng biết đến cái tên.

“Hey, anh dạo này thế nào?” anh ta trả lời vui vẻ, rõ ràng là chưa đủ quen với Chernoff ngoài đời để biết rằng giọng tôi không giống giọng anh ta.

“Tôi vẫn ổn,” tôi nói, “nhưng các anh vừa xóa một trong số tài khoản của tôi à? Tôi đã tạo một tài khoản để kiểm tra một vài đoạn mã tuần trước, nhưng

https://thuviensach.vn

giờ lại không đăng nhập vào được nữa.”

Anh ta hỏi tài khoản đăng nhập của tôi là gì.

Theo kinh nghiệm, tôi biết rằng trong hệ thống RSTS/E, số tài khoản là tổ hợp của số dự án và số lập trình viên, ví dụ như 1.119 – mỗi số có thể dao động đến 254. Các tài khoản truy cập luôn có số dự án là 1. Trước đó, tôi cũng phát hiện ra rằng đội phát triển RSTS/E sử dụng số lập trình viên bắt đầu từ 200.

Tôi nói với Jerry tài khoản thử nghiệm của mình là “1.119”, thầm cầu nguyện rằng nó chưa được gán cho ai.

Đó là một dự đoán ăn may. Anh ta kiểm tra và nói với tôi rằng chưa có tài khoản 1.119 nào. “Chết tiệt,” tôi nói. “Chắc ai đó đã xóa nó đi rồi. Anh tạo lại cho tôi được không?”

Chernoff muốn gì thì sẽ có đó. “Không thành vấn đề,” Jerry nói. “Anh muốn mật khẩu là gì?”

Tôi nhìn thấy một lọ mứt dâu trong tủ bếp phía đối diện, liền nói: “‘jelly’ đi”.

Trong chớp mắt, anh ta nói: “Được rồi đấy.”

Tôi bị choáng, adrenaline[24] tăng cao. Tôi không thể tin việc này lại dễ dàng như vậy. Nhưng liệu mọi chuyện có suôn sẻ như thế không?

[24] Adrenaline: Hoóc-môn có tác dụng trên thần kinh giao cảm, do cơ thể tiết ra khi con người sợ hãi, tức giận hay thích thú, khiến nhịp tim đập nhanh hơn và giúp cơ thể chuẩn bị cho những phản ứng chống lại nguy hiểm. (BTV)

Từ máy tính của mình, tôi gọi đến số mà Neal, người-sẽ-trở-thành-hướng-dẫn-viên-của-tôi, đã đưa cho. Cuộc gọi được kết nối và dòng chữ này xuất

https://thuviensach.vn

hiện:

*RSTS V7.0-07 * The Ark * Job 25 KB42 05-Jul-80 11:17 AM*

 # 1,119

Password:

Dialup password:

Chết tiệt, chết tiệt, chết tiệt. Tôi gọi lại Jerry Covert, vẫn giả là Chernoff. "Này, tôi đang gọi từ nhà, và nó yêu cầu mật khẩu kết nối."

"Anh không nhận được trong e-mail à? Mật khẩu là 'buffoon.'"

Tôi thử lại lần nữa và tôi đã vào được!

Trước hết, tôi phải bắt đầu lấy hết đống mật khẩu của tất cả mọi người trong đội phát triển đã.

Khi gặp Neal, tôi bảo gã,: "Truy cập vào Ark chỉ là chuyện nhỏ như con thỏ. Tôi còn có mật khẩu của mọi nhà phát triển RSTS/E." Gã đảo mắt ra vẻ: Thằng này ngáo à?

Gã quay số modem và vào đến màn hình đăng nhập của Ark. Bảo gã "dịch ra chỗ khác", tôi nhập thông tin xác minh và nhận được dấu nháy "Ready" (Sẵn sàng).

"Thỏa mãn chưa, Neal?" tôi hỏi.

Gã không thể tin nổi vào mắt mình, như thể tôi đã cho gã thấy một tấm vé trúng số. Sau khi vặn hỏi cặn kẽ cách tôi lấy được quyền truy cập, Neal, Dave và vài người bạn khác cùng đến một công ty tên là PSI gần thành phố Culver, nơi họ đặt chiếc modem mới nhất, nhanh nhất, chạy với tốc độ 1.200

https://thuviensach.vn

baud[25] – nhanh gấp bốn lần những modem 300 baud mà chúng tôi có. Họ bắt đầu tải về mã nguồn RSTS/E.

[25] Baud: Số đo tốc độ truyền dữ liệu giữa máy tính và các thiết bị khác, được đo bằng số bit trên giây (bps). (BTV)

Giang hồ cũng có luật. Thay vì tin tưởng và chia sẻ thông tin với tôi, bọn họ lại tải về mã nguồn RSTS/E và giữ cho riêng mình.

Sau này, tôi mới biết rằng lũ khốn đó thực ra đã gọi đến DEC và nói với họ rằng Ark đã bị hack, và khai ra tên của tôi. Bọn chúng đã chơi đểu tôi. Nào ngờ những gã đó đã định chỉ điểm tôi, đặc biệt là sau khi họ thu về được chiến lợi phẩm lớn như vậy. Đây là lần đầu tiên tôi bị những người mà mình tin tưởng phản bội.

Năm 17 tuổi, dù đang theo học trung học nhưng tôi đã quyết chí theo đuổi giấc mơ trở thành Tiến sĩ hacking RSTS/E. Tôi sẽ truy tìm mục tiêu bằng cách kiếm các công ty đăng quảng cáo tìm người có kinh nghiệm máy tính với RSTS/E. Tôi sẽ gọi, khẳng định mình đến từ đội hỗ trợ kỹ thuật của DEC, và thường nói chuyện với nhân viên quản trị hệ thống để họ đưa số dial-up và mật khẩu của tài khoản đặc quyền.

Tháng 12 năm 1980, tôi vô tình gặp Micah Hirschman, một tên nhóc có cha sở hữu một tài khoản ở Bloodstock Research, một công ty vốn cũng dùng RSTS/E. Đoán rằng công ty này đang lưu giữ các ghi chép lịch sử về huyết thống của ngựa đua dành cho những người phối giống và hội cá cược, tôi dùng tài khoản của Hirschman kết nối với Bloodstock Research để có thể khai thác một lỗ hổng an ninh và chiếm quyền truy cập bằng một tài khoản đặc quyền, sau đó Micah và tôi sẽ nghịch hệ điều hành để tự học về nó, đơn giản là cho vui.

Vụ việc này về sau đã để lại hậu quả nghiêm trọng cho chúng tôi. Một đêm muộn, Micah đăng nhập mà không có tôi, Bloodstock đã phát hiện ra vụ đột nhập và báo động cho FBI, thông báo vụ tấn công thông qua tài khoản của

https://thuviensach.vn

Hirschman. Cục điều tra đã đến thăm ngài Hirschman. Ông ta nói rằng mình không biết gì về vụ tấn công. Khi Cục gây áp lực lên ông ta, ông ta chỉ vào con trai, còn Micah thì nói ra tên tôi.

Tôi đang ở trong phòng ngủ trên tầng hai căn hộ của chúng tôi, lên mạng, hack vào các bộ chuyển mạch của Pacific Telephone thông qua một modem dial-up. Nghe thấy tiếng gõ cửa, tôi mở cửa sổ và gọi xuống, "Ai đấy?" Câu trả lời khiến tôi hãi hùng: "Tôi là Robin Brown đến từ FBI."

Tim tôi bắt đầu đập mạnh.

Mẹ gọi tôi: "Ai đấy?"

"Một gã nói hắn đến từ FBI," tôi trả lời.

Mẹ chỉ cười vang. Bà không biết đó là ai, nhưng bà không nghĩ đó có thể là FBI.

Tôi hoảng loạn, ngắt luôn điện thoại khỏi giá để modem máy tính và giấu dưới gầm giường thiết bị đầu cuối máy tính[26] TI-700 mà Lewis De Payne đã cho tôi mượn vài tuần trước. Thời đó, trước khi có máy tính cá nhân (PC), tất cả những gì tôi có là một thiết bị đầu cuối và một modem để kết nối đến một hệ thống ở công ty hay trường đại học. Không có màn hình máy tính: phản hồi cho câu lệnh của tôi sẽ được in ra trên một cuộn giấy nhiệt dài.

[26] Thiết bị đầu cuối máy tính (terminal computer): Thiết bị phần cứng điện tử hoặc điện cơ được sử dụng để nhập dữ liệu vào và hiển thị hoặc in dữ liệu ra từ một máy tính hoặc một hệ thống điện toán. (Wikipedia)

Tôi chợt nhớ ra một sự thật rằng tôi có cả tấn giấy nhiệt dưới gầm giường, chứa đầy thông tin sẽ chứng minh rằng tôi đã hack nhiều giờ mỗi tuần vào máy tính và bộ chuyển mạch của các công ty điện thoại, cũng như rất nhiều máy tính của các công ty cá nhân.

https://thuviensach.vn

Khi tôi đi xuống dưới nhà, viên đặc vụ chìa tay ra, tôi bắt tay ông ta. “Tôi đã tóm cổ Stanley Rifkin,” ông ta ngụ ý rằng tôi biết ông ta đang nhắc đến ai. Đó là kẻ đã thực hiện vụ trộm lớn nhất lịch sử, cuỗm đi 10 triệu đô-la từ Ngân hàng Security Pacific National (SPNB) thông qua một pha gài bẫy điện chuyển khoản ngân hàng. Tay đặc vụ nghĩ điều này sẽ dọa được tôi, có điều tôi biết Rifkin chỉ bị bắt bởi gã đã trở về Mỹ và khoe khoang chiến tích. Nếu không thì giờ này gã vẫn đang sống xa hoa ở nước ngoài.

Nhưng đây là một cảnh sát liên bang, và lúc đó vẫn chưa có bộ luật liên bang nào dành cho loại tội phạm đột nhập máy tính mà tôi đang làm. Ông ta nói: “Cậu có thể phải ngồi tù 25 năm nếu cứ tiếp tục quậy phá công ty điện thoại.” Tôi biết ông ta chẳng làm gì được mình, ông ta chỉ đang cố dọa tôi mà thôi.

Điều đó không có tác dụng. Ngay khi ông ta bỏ đi, tôi lại lên mạng. Tôi không đốt đống giấy đã in. Đúng, điều đó thật ngu ngốc. Tôi vốn đã là kẻ cứng đầu cứng cổ rồi.

Nếu chuyến viếng thăm của tay đặc vụ không làm tôi sợ, thì phản ứng của mẹ tôi mới là điều không ai ngờ đến. Với bà, toàn bộ việc này chỉ như một trò đùa ngớ ngẩn: Một thằng bé chỉ ngồi chơi máy tính ở nhà thì có thể gây hại gì được? Bà không có chút khái niệm nào về những gì tôi đang toan tính.

Cảm giác hồi hộp và thỏa mãn khi làm những việc mình không được phép làm thực sự quá tuyệt vời. Tôi bị cuốn theo sự mê hoặc của công nghệ điện thoại và máy tính. Tôi cảm thấy mình như một nhà thám hiểm, khám phá không gian mạng không giới hạn, lẻn vào các hệ thống với sự hồi hộp và thỏa mãn đơn thuần, cao tay hơn hẳn các kỹ sư với nhiều năm kinh nghiệm, tìm ra cách vượt qua các rào cản an ninh, học hỏi cách mọi thứ vận hành.

Chẳng mấy chốc tôi bắt đầu vướng phải một số rắc rối với các nhà chức trách. Micah sau đó đã đi Paris. Khi chuyến bay của hãng Air France đã cất cánh được vài giờ, một thông báo trên hệ thống PA vang lên: “Xin mời hành

https://thuviensach.vn

khách Micah Hirschman ấn nút gọi tiếp viên.” Khi cậu ta ấn nút, một tiếp viên đi về phía cậu ta và nói: “Cơ trưởng muốn nói chuyện với anh trong buồng lái.” Các bạn có thể tưởng tượng sự ngạc nhiên của cậu ta.

Cậu ta được dẫn vào buồng lái. Cơ phó đang nói với ai đó qua bộ đàm rằng Micah đã có mặt, rồi đưa micro cho cậu ta. Một giọng nói vang lên trên bộ đàm: “Đây là đặc vụ FBI Robin Brown. Cục điều tra đã phát hiện ra anh vừa rời nước, đang trên đường đến Pháp. Tại sao anh lại đến Pháp?”

Toàn bộ tình huống này thật lố bịch. Micah đưa ra câu trả lời, và tay đặc vụ vặn vẹo cậu ta thêm vài phút. Hóa ra FBI nghĩ rằng Micah và tôi đã thực hiện một vụ hack lớn kiểu như Stanley Rifkin, có thể chúng tôi đang chuẩn bị cho một vụ lừa đảo chuyển hàng triệu đô-la từ một ngân hàng ở Mỹ đến một ngân hàng nào đó ở châu Âu.

Mọi thứ giống như một cảnh quay trong một bộ phim cướp nhà băng, và tôi yêu thích sự hồi hộp của nó.

Sau khi được nếm mùi kích thích, tôi nghiện luôn – và tôi ngày càng thèm khát cảm giác đó. Ngồi trên ghế của trường trung học, nhưng đầu óc tôi chỉ toàn là những hoạt động hacking và phreaking tới mức chẳng còn chút tập trung và động lực nào cho trường lớp. Hạnh phúc thay, tôi đã phát hiện ra một giải pháp tốt hơn rất nhiều so với việc trở thành một gã bỏ học giữa chừng hay đợi cho đến khi Khu học chánh Los Angeles thể hiện sự không hài lòng và đuổi học tôi.

Vượt qua kỳ thi GED[27] sẽ giúp tôi có được tấm bằng tương đương với bằng tốt nghiệp cấp ba mà không làm phí phạm thêm thời gian của tôi cũng như của các giáo viên. Tôi đăng ký thi và hóa ra, nó dễ hơn rất nhiều so với những gì tôi nghĩ – chắc chỉ tương đương trình độ lớp 8.

[27] GED (General Education Development): Kỳ thi để lấy bằng tương đương bằng tốt nghiệp trung học ở Mỹ dành cho những người chưa tốt nghiệp phổ thông trung học, hoặc đã tốt nghiệp ở những quốc gia khác ngoài Mỹ nhưng

https://thuviensach.vn

vì lý do nào đó mà bằng cấp không sử dụng được, hoặc dành cho những người muốn ôn lại kiến thức phổ thông cơ bản để chuẩn bị bước vào đại học. (BTV)

Còn gì tuyệt vời hơn khi được trở thành một sinh viên đại học chuyên ngành máy tính, vừa lấy được tầm bằng vừa thỏa mãn cơn khát vô độ của tôi dành cho những kiến thức về máy tính? Mùa hè năm 1981, ở tuổi 17, tôi đăng ký vào Cao đẳng Pierce, một trường học hệ hai năm ở vùng Woodland Hills gần đó.

Quản lý phòng máy tính của trường, Gary Levi, nhận ra niềm đam mê của tôi. Ông đã nâng đỡ tôi, cho tôi một vị trí đặc biệt thông qua việc cấp cho tôi "tài khoản đặc quyền" – trên hệ thống RSTS/E.

Món quà của ông có hạn sử dụng. Ông rời trường; không lâu sau đó, trưởng khoa Khoa học Máy tính, Chuck Alvarez, để ý thấy tôi đang đăng nhập vào một tài khoản đặc quyền và bắt tôi thoát ra ngay lập tức. Tôi giải thích rằng Levi đã cho phép tôi, nhưng điều đó không có tác dụng; gã đá tôi ra khỏi phòng máy tính. Khi cha cùng tôi đến gặp Alvarez, gã đã đưa ra lời bào chữa: "Con anh đã biết quá nhiều về máy tính và trường Pierce không còn gì để dạy cậu ta nữa."

Tôi bỏ học.

Tôi đã mất quyền truy cập vào một hệ thống tuyệt vời, nhưng hồi cuối những năm 1970 đầu những năm 1980, thế giới máy tính cá nhân bước vào giai đoạn chuyển mình mạnh mẽ, đem đến những chiếc máy tính để bàn đầu tiên có cả màn hình hoặc thậm chí được tích hợp luôn. Máy Commodore PET, máy Apple II và máy tính cá nhân IBM đầu tiên bắt đầu biến máy tính trở thành công cụ cho mọi người, và giúp máy tính trở nên tiện lợi hơn rất nhiều cho người thường xuyên sử dụng… bao gồm cả các hacker. Đúng là không còn gì tuyệt hơn.

https://thuviensach.vn

Lewis De Payne luôn là chiến hữu hacking và phreaking thân thiết nhất của tôi ngay từ lần đầu tiên cậu ta gọi đến và nói rằng muốn gặp mặt để học hỏi tôi. Dù lớn hơn tôi 5 tuổi – điều này tạo ra khá nhiều khác biệt – nhưng chúng tôi vẫn cùng chia sẻ niềm vui sướng của bọn trẻ con đối với phreaking và hacking. Cả hai chúng tôi đều có chung mục tiêu: truy cập vào máy tính, truy cập vào mật khẩu, truy cập vào thông tin của các công ty mà chúng tôi không được phép. Tôi chưa bao giờ phá hỏng tập tin máy tính của bất kỳ ai hay kiếm chác một xu nào từ những truy cập mà tôi chiếm được; và theo như tôi biết, Lewis cũng vậy.

Chúng tôi tin tưởng nhau – dù giá trị quan của cậu ta khác với tôi. Một ví dụ điển hình là vụ hack U.S. Leasing.

Tôi xâm nhập vào hệ thống của U.S. Leasing thông qua một chiến thuật đơn giản đến lố bịch, tới mức tôi còn cảm thấy xấu hổ.

Tôi gọi đến một công ty đã xác định từ trước, hỏi phòng máy tính của họ, chắc chắn rằng mình đang nói chuyện với nhân viên quản trị hệ thống, và bảo anh ta: “Tôi là [một cái tên hư cấu nào đó hiện ra trong đầu tôi lúc đó], đến từ đội hỗ trợ kỹ thuật DEC. Chúng tôi phát hiện ra một lỗi nghiêm trọng trong phiên bản RSTS/E của các anh. Các anh có thể mất dữ liệu.” Đây là một đòn tấn công bằng kỹ thuật xã hội rất mạnh, bởi nỗi sợ mất dữ liệu lớn đến mức hầu hết mọi người đều không ngần ngại hợp tác.

Khi người bên kia đã nhận thức được nỗi sợ, tôi nói tiếp: “Chúng tôi có thể vá lại hệ thống của các anh mà không làm gián đoạn các hoạt động.” Lúc này anh ta (hoặc, đôi khi là cô ta) sẽ nóng lòng đưa cho tôi số điện thoại dial-up và quyền truy cập vào tài khoản của quản lý hệ thống. Nếu nhận được bất kỳ phản ứng nào, tôi sẽ nói mấy điều đại loại như: “Được rồi, tôi sẽ gửi thông tin cho các anh qua e-mail” và chuyển sang mục tiêu khác.

Người quản trị hệ thống ở U.S. Leasing đã cung cấp cho tôi mật khẩu để truy cập vào tài khoản quản lý hệ thống ngay lập tức. Tôi đăng nhập vào hệ

https://thuviensach.vn

thống, tạo một tài khoản mới, vá lại hệ điều hành bằng một cửa hậu – mã phần mềm cho phép tôi có quyền truy cập ẩn mỗi khi muốn vào lại.

Tôi chia sẻ thông tin về cửa hậu này với Lewis vào lần nói chuyện sau đó. Lúc đó, Lewis đang hẹn hò với một ả hacker có lúc nhận tên là Susan Thunder, người về sau đã trả lời một phóng viên rằng hồi đó thỉnh thoảng "đi khách" để kiếm tiền mua thiết bị máy tính. Tôi vẫn thấy ngán ngẩm mỗi khi nghĩ đến câu nói đó của ả. Dù sao thì Lewis đã nói với Susan rằng tôi đã đột nhập vào U.S. Leasing và đưa cho ả thông tin đăng nhập. Hoặc cũng có thể, như sau này cậu ta khẳng định, Lewis không hề đưa nó cho ả mà là ả đã nhìn thấy những thông tin này được viết lên một mảnh giấy mà cậu ta để quên cạnh máy tính của mình.

Không lâu sau đó, bọn họ "đường ai nấy đi", và tôi đoán là không vui vẻ gì. Sau đó ả đã trả thù tôi. Cho đến tận hôm nay, tôi vẫn không biết vì sao ả lại nhắm vào tôi, trừ khi ả nghĩ rằng Lewis chia tay với ả để có thể dành nhiều thời gian hơn với tôi, hacking, và vì thế, ả đổ lỗi vụ chia tay cho tôi.

Dù vì lý do gì, ả đã dùng thông tin đăng nhập ăn cắp được để xâm nhập vào hệ thống máy tính của U.S. Leasing. Những câu chuyện kể lại sau đó về vụ này nói rằng ả đã phá hoại rất nhiều tập tin của họ. Và ả đã gửi tin nhắn đến tất cả các máy in để in ra, in liên tục cho đến khi hết giấy:

MITNICK WAS HERE

MITNICK WAS HERE

(tạm dịch: *Mitnick đã ở đây*)

FUCK YOU

FUCK YOU

(tạm dịch: *Cha mày!*)

https://thuviensach.vn

Điều khiến tôi nóng máu nhất trong vụ này là trong một thỏa thuận nhận tội về sau, chính phủ đã khăng khăng buộc tội tôi dù tôi không hề làm việc này. Tôi đã phải đối mặt với lựa chọn nhận tội cho hành động lăng mạ và lố bịch này hoặc vào trại cải tạo thanh thiếu niên.

Susan đã trả thù tôi trong một thời gian dài, ngắt dịch vụ điện thoại của tôi, và nhiều lần yêu cầu công ty điện thoại ngắt số của tôi. Hành động trả đũa nho nhỏ của tôi đã diễn ra một cách tình cờ.

Một lần, trong khi đang hack một công ty điện thoại, tôi cần một đường dây điện thoại đổ chuông liên tục mà không có ai trả lời. Tôi đã gọi đến một bốt điện thoại công cộng mà tôi vô tình nhớ số. Trái đất thật tròn, Susan Thunder sống gần đó và đã đi ngang qua chính cái bốt điện thoại ấy vào đúng lúc đó. Ả nhấc máy, nói “A-lô” và tôi nhận ra giọng ả.

Tôi nói: “Susan, Kevin đây. Tôi chỉ muốn cho cô biết tôi đang theo dõi cô từng bước. Đừng đùa với tôi!”

Tôi hy vọng trò này dọa ả được vài tuần.

Tôi đã có quãng thời gian vui vẻ, nhưng quãng đời né tránh luật pháp của tôi không kéo dài mãi.

Tháng 5 năm 1981, vẫn 17 tuổi, tôi chuyển các hoạt động học ngoại khóa sang Đại học California tại Los Angeles (UCLA). Trong phòng thí nghiệm máy tính, các sinh viên thường làm bài tập về nhà hoặc học về máy tính và lập trình. Còn tôi ở đó để hack các máy tính từ xa bởi chúng tôi không đủ điều kiện để sắm một máy tính tại nhà, vậy nên tôi tìm đến các máy tính ở những nơi như trường đại học.

Tất nhiên, trong phòng thí nghiệm không có kết nối ra bên ngoài – bạn có thể kết nối từ modem tại mỗi trạm, nhưng chỉ đến một số nội bộ khác trong trường, không phải đến một số bên ngoài – điều đó có nghĩa là chúng không có giá trị với những gì tôi muốn làm.

https://thuviensach.vn

Không sao, trên tường phòng máy tính là một dây điện thoại duy nhất không có số: Nó chỉ dành cho các cuộc gọi đến. Cũng giống như hồi trung học trong phòng thí nghiệm máy tính của thầy Christ, tôi sẽ nhấc máy lên và gạt khóa công tắc, việc này cũng có tác dụng như quay số vậy. Gạt nhanh 9 lần liên tiếp, tương đương với quay số "9", sẽ có âm hiệu quay số cho một đường dây ra bên ngoài. Sau đó, tôi gạt 10 lần, tương đương với quay số "0", để gọi một nhân viên trực tổng đài.

Khi nhân viên trực tổng đài nghe máy, tôi nhờ cô ta gọi lại cho tôi vào số điện thoại dùng cho modem ở thiết bị đầu cuối máy tính tôi đang sử dụng. Các thiết bị đầu cuối máy tính trong phòng thí nghiệm thời đó chưa có modem đi kèm bên trong. Thay vào đó, để tạo kết nối modem, bạn phải đặt tai nghe điện thoại vào một bộ nối âm cạnh đó, bộ nối âm này sẽ gửi tín hiệu từ modem vào tai nghe điện thoại và truyền ra ngoài thông qua đường dây điện thoại. Khi nhân viên trực tổng đài gọi lại trên đường dây modem điện thoại, tôi đã nghe máy và nhờ cô ta gọi vào một số điện thoại hộ tôi.

Tôi đã dùng cách này để gọi đến rất nhiều công ty sử dụng DEC PDP-11 chạy RSTS/E. Nhờ vào trò giả danh hỗ trợ kỹ thuật của DEC, tôi có thể dùng kỹ thuật xã hội để lấy thông tin đăng nhập dial-up và hệ thống của họ. Vì không có máy tính cá nhân, tôi đã lang thang từ khuôn viên đại học này đến đại học khác để có thể có được vài lần truy cập máy tính mà tôi thèm khát. Tôi háo hức vô cùng mỗi khi lái xe đến một trường đại học để lên mạng. Tôi sẽ lái xe vượt quá tốc độ cho phép suốt 45 phút ngay cả khi điều đó chỉ đem lại 15 phút dùng máy tính.

Tôi không thể ngờ được rằng một sinh viên tại một trong các phòng thí nghiệm máy tính đã lén biết được những gì tôi đang làm và chỉ điểm tôi.

Mãi cho đến tận một tối nọ, khi ngồi trước thiết bị đầu cuối trong phòng thí nghiệm ở UCLA, nghe thấy tiếng ồn ào, tôi ngẩng đầu lên và nhìn thấy một toán nhân viên an ninh trường đang xông thẳng vào chỗ tôi. Tôi cố ra vẻ

https://thuviensach.vn

hóng hớt và tự tin, một thằng nhóc không biết tất cả những chuyện này nghĩa là gì.

Họ lôi tôi ra khỏi ghế và đưa tay tôi vào còng.

Đúng vậy, California lúc này đã có một bộ luật khép tội hacking. Nhưng tôi vẫn là trẻ vị thành niên, vì vậy, tôi không phải đối diện với án tù.

Dù vậy tôi vẫn hoảng loạn, sợ gần chết. Cái túi to đeo vai tôi để trong xe chứa đầy giấy tờ in ra cho thấy tất cả các công ty mà tôi đã đột nhập. Nếu họ lục soát xe, tìm thấy đống giấy đó và biết chúng là gì, tôi sẽ phải đối mặt với hậu quả thê thảm hơn rất nhiều so với bất cứ sự trừng phạt nào mà họ có thể đưa ra cho tội sử dụng máy tính của trường khi tôi không phải là sinh viên.

Một nhân viên an ninh trường lần ra được xe của tôi sau khi tịch thu chìa khóa xe và tìm thấy chiếc túi hack lậu.

Sau đó, họ đẩy tôi đến phòng an ninh của trường, giống như muốn bắt giam tôi, và nói rằng tôi bị giam giữ vì đã "xâm phạm trái phép". Họ gọi mẹ đến đón tôi.

Cuối cùng, UCLA không tìm được ai có thể hiểu đống giấy in của tôi. Trường cũng chưa bao giờ đâm đơn kiện nào. Chẳng có hình phạt nào ngoài việc đưa trường hợp của tôi lên Ban Quản chế Quận, nơi có thể yêu cầu Tòa án Vị thành niên xét xử vụ việc… nhưng họ đã không làm vậy.

Có lẽ tôi là kẻ bất khả xâm phạm. Có lẽ tôi có thể tiếp tục làm những thứ mình vẫn làm, thỉnh thoảng đối mặt với một vài vụ rắc rối nhưng không đáng bận tâm. Dù vụ này dọa tôi sợ chết khiếp, nhưng một lần nữa tôi lại tránh được một viên đạn.

https://thuviensach.vn

04

NGHỆ SĨ TRỐN CHẠY

Flle ujw esc wexp mo xsp kjr hsm hiwwcm, "Wplpll stq lec qma e wzerg mzkk!"?

Vào Lễ Tưởng niệm Liệt sĩ năm 1981, Lewis De Payne và tôi cùng tham gia một "bữa tiệc" với nhóm phreaker. Có dấu ngoặc kép kia là bởi ngoài lũ nhóc sáu tuổi muốn tổ chức sinh nhật và một nhóm tín đồ cuồng công nghệ thì còn ai chọn tiệm pizza Shakey làm chỗ tụ tập và đùa giỡn cơ chứ?

Hơn 20 người có mặt, gã nào trông cũng quái đản hệt như một tên cuồng ham radio hạng nhất. Nhưng một vài người trong số này có kiến thức kỹ thuật khá tốt, khiến tôi được an ủi rằng mình cũng không hoàn toàn lãng phí thời gian.

Buổi trò chuyện hiển nhiên xoay quanh một trong những mục tiêu ưa thích nhất của tôi, COSMOS (Computer System for Mainframe Operations), một trong những hệ máy tính tối quan trọng đầu tiên của Pacific Telephone, có thể mang lại quyền hạn to lớn cho bất kỳ phreaker nào truy cập được vào nó.

Lewis và tôi đã truy cập vào COSMOS. Đây cũng là một trong những máy tính đầu tiên của Pacific Telephone bị tôi tấn công, nhưng có lẽ chỉ có vài người có thể làm vậy tại thời điểm đó và tôi cũng không định tiết lộ mình đã làm thế nào. Khi cuộc trò chuyện bắt đầu, tôi nhận ra tòa nhà đặt hệ thống COSMOS ở ngay gần đó, chỉ cách vài dặm đường. Tôi cho rằng nếu vài người trong số chúng tôi tới đó và thử lục tìm thùng rác xung quanh một chút, có lẽ chúng tôi có thể kiếm được vài thông tin hữu ích.

https://thuviensach.vn

Lewis luôn sẵn sàng cho mọi ý tưởng. Chúng tôi chỉ rủ thêm Mark Ross, một gã khá quen thuộc với các hệ thống điện thoại và có thể tin tưởng được.

Trên đường đi, chúng tôi rẽ qua quầy thuốc 24 giờ để mua một ít găng tay cùng đèn pin, sau đó tiến thẳng tới tòa nhà COSMOS. Thùng rác có thể mang lại vài thứ hay ho nhưng không mấy giá trị cho lắm. Sau khoảng một giờ, tôi chán nản gợi ý: "Sao tụi mình không thử xem có vào trong được không?"

Cả hai đứa còn lại đều muốn tôi đi vào và thử xem có thể tấn công tay bảo vệ bằng kỹ thuật xã hội không, sau đó gửi tín hiệu bấm phím ra ngoài từ máy ham radio cầm tay. Không đời nào – chúng tôi sẽ là ba gã ngự lâm quân hoặc không gì cả.

Cả lũ bước vào. Tay bảo vệ trông có vẻ khoái hút cỏ thường xuyên. Tôi nói: "Xin chào, anh thế nào? Chúng tôi ra ngoài muộn chút. Tôi làm việc ở đây, đang muốn cho mấy anh bạn này ngó chỗ làm một chút."

"Được," anh ta nói. "Anh điền tên ở đây." Không buồn hỏi thẻ ID. Mọi chuyện suôn sẻ.

Chúng tôi từng gọi điện đến các phòng ban và phân tích hoạt động của công ty điện thoại trong suốt thời gian dài đủ để biết các nhân viên COSMOS làm việc ở đâu. "Phòng 108" liên tục xuất hiện trong các cuộc đối thoại của Pacific Telephone. Chúng tôi tìm đường tới đó.

COSMOS. Một mỏ vàng. Một món béo bở.

Trên tường đính một tệp thư mục gồm các bảng danh sách số dial-up nội bộ của tất cả trung tâm đấu dây[28] ở Nam California. Chúng nhìn hệt như những ấn phẩm quảng cáo bóng bẩy trong văn phòng bác sĩ với lời mời gọi: "Hãy lấy một tờ đi!" Chúng tôi gặp may đến khó tin. Đây là kho báu thực sự, một trong những kho báu mà tôi vẫn luôn thèm khát nhất.

https://thuviensach.vn

[28] Trung tâm đấu dây (wire center): Tòa nhà hay văn phòng trung tâm, nơi có các dây mạch được kết nối với nhau. (BTV)

Một văn phòng trung tâm thường có một hay vài trung tâm đấu dây. Nhiệm vụ chuyển mạch điện thoại ở mỗi văn phòng trung tâm sẽ do một trung tâm đấu dây riêng biệt phụ trách. Nếu có danh sách các số dial-up cho từng trung tâm đấu dây và tài khoản truy cập trong tay, tôi sẽ có khả năng thao túng bất kỳ đường dây điện thoại nào của Pacific Telephone trong khu vực dịch vụ cung cấp ở Nam California.

Thật là một phát hiện đầy kích thích. Nhưng tôi còn cần cả mật khẩu cho các tài khoản quản trị khác nữa. Tôi đi lòng vòng qua các phòng quanh phòng COSMOS, mở các tệp thư mục và ngó vào ngăn kéo. Tôi mở một tệp hồ sơ và tìm được tờ giấy có dán nhãn "Mật khẩu".

Ôi trời!

Quá tuyệt. Tôi cười ngoác miệng.

Chúng tôi lẽ ra đã nên rời đi ngay lúc ấy.

Nhưng tôi còn phát hiện ra một tập tài liệu hướng dẫn COSMOS chứa cả đống thông tin cần-phải-có. Một cám dỗ không thể cưỡng lại. Tập tài liệu hướng dẫn này có thể cho chúng tôi biết mọi thứ cần biết, từ đặt yêu cầu bằng các lệnh mã hóa cho tới mọi vấn đề về vận hành của hệ thống. Ngày nay, bạn có thể tìm được thông tin nhờ Google nhưng ở thời đó, chúng chỉ được lưu trong tập tài liệu hướng dẫn như thế này.

Tôi nói với đồng bọn: "Mang xấp tài liệu này ra tiệm photocopy đã, mỗi đứa một bản, sau đó trả lại họ trước khi mọi người quay lại làm việc vào sáng mai."

Gã bảo vệ không buồn hỏi lý do chúng tôi đi vào tay không mà lại đi ra với vài tập giấy, bao gồm cả mấy thứ nhét trong cặp hồ sơ mà Lewis kiếm được

https://thuviensach.vn

trong một căn phòng nào đó.

Đây là quyết định ngu ngốc nhất đời tôi thuở ấy.

Chúng tôi lái xe lòng vòng để tìm cửa hàng photocopy nhưng không thấy. Hiển nhiên là không có tiệm photocopy nào lại mở cửa vào lúc 2 giờ sáng. Chúng tôi cũng cho rằng đằng nào thì cũng quá nguy hiểm nếu quay trở lại tòa nhà lần nữa để trả lại tập hồ sơ, kể cả sau khi đã đổi người trực ca – ngay cả khả năng bịa chuyện trong chớp mắt của tôi cũng không thể đưa ra một lời giải thích nào đáng tin cậy.

Do đó, tôi mang tập hồ sơ về nhà. Nhưng tôi vẫn có cảm giác không ổn. Tôi nhét chúng vào mấy cái túi rác Hefty và Lewis giấu ở đâu đó. Tôi không muốn biết.

Dù không còn hẹn hò với Susan Thunder, Lewis vẫn liên lạc với cô ta và cậu ta quả là một gã nhiều chuyện. Không thể giữ kín những bí mật có thể mang lại rắc rối lớn cho chính mình và bạn bè, cậu ta đã kể cho Susan về những tập tài liệu hướng dẫn.

Susan báo ngay cho công ty điện thoại. Vài ngày sau, vào một buổi tối mùa hè nóng nực, khi tôi rời chỗ làm (khi đó, tôi là nhân viên trực điện thoại ở Steven S. Wise Temple) và lái xe ra khỏi bãi đỗ để về nhà, tôi vượt qua một chiếc Ford Crown Victory chở ba người đàn ông bên trong. (Chẳng hiểu sao mấy gã nhân viên chấp pháp cứ phải lái chung một mẫu xe? Chẳng lẽ không có gã nào nhận ra rằng điều đó chẳng khác nào "lạy ông tôi ở bụi này", như thể sơn cả dòng chữ "CỚM CHÌM" trên hông xe?)

Tôi tăng tốc để xem họ có quay đầu xe và theo đuôi không.

Có. Chết tiệt! Nhưng biết đâu đây chỉ là ngẫu nhiên?

Tôi tiếp tục tăng tốc, chuyển bánh lên con dốc dẫn ra đường I-405 hướng về Thung lũng San Fernando.

https://thuviensach.vn

Chiếc Crown Vic vẫn bám theo sau.

Tôi nhìn qua kính chiếu hậu, một cánh tay vươn ra đặt bộ đèn chớp lên nóc xe và đèn cảnh sát bắt đầu nháy. Chết tiệt! Tại sao họ lại tóm tôi? Tôi thoáng nghĩ tới việc tăng tốc hơn nữa. Một cuộc đuổi bắt tốc độ cao sao? Thật điên rồ!

Không đời nào tôi cố sống cố chết chạy đâu. Tôi dừng xe.

Xe họ dừng lại ngay sau tôi. Ba gã cảnh sát nhảy ra. Họ bắt đầu chạy về phía tôi.

Họ rút súng!!!!

Họ hét lên: “Ra khỏi xe!”

Chỉ trong nháy mắt, tôi đã bị còng tay. Chiếc còng khít chặt đau đớn.

Một gã hét vào tai tôi: “Mày sẽ phải ngừng ngay mấy trò khỉ với công ty điện thoại! Bọn tao sẽ dạy cho mày một bài học!” Tôi sợ tới mức bật khóc.

Một chiếc xe khác dừng lại. Lái xe nhảy ra và chạy về phía chúng tôi. Hắn ta gào lên với mấy tay cớm: “Tìm bom trong xe! Nó có bom logic[29]!”

[29] Bom logic: Một phần mã được thiết kế để kích hoạt các tính năng độc hại dưới các điều kiện nhất định nào đó về ngày, giờ hoặc dữ liệu. (ND)

Giờ thì tôi bật cười trong nước mắt. Bom logic là một phần mềm, nhưng mấy gã này có vẻ như không biết điều đó.

Họ nghĩ tôi mang bên mình cái gì đó có thể thổi tung tất cả mọi người! Họ bắt đầu tra hỏi tôi. “Tập tài liệu hướng dẫn đâu?”

Tôi nói với họ: “Tôi là trẻ vị thành niên, tôi muốn gọi luật sư.”

https://thuviensach.vn

Dù vậy, họ vẫn đối xử với tôi hệt như một thành phần khủng bố, dẫn tôi tới đồn cảnh sát ở Pasadena cách đó chừng 45 phút lái xe và tống tôi vào buồng tạm giam.

Cuối cùng, một giám sát viên tới để tra hỏi tôi. Dù có quyền thả tôi, nhưng ông ta đã bị mấy tay cảnh sát thuyết phục rằng một kẻ tội phạm như tôi có thể được coi là một Hannibal Lecter[30] về tấn công máy tính. Tôi được chuyển sang trại cải tạo thanh thiếu niên ở Đông Los Angeles trong đêm với chiếc còng trên tay và dẫn ra tòa ngay ngày hôm sau. Cả cha và mẹ tôi cùng có mặt ở đó, cố gắng để tôi được thả ra.

[30] Hannibal Lecter: Nhân vật hư cấu trong loạt truyện trinh thám của Thomas Haris, là một bác sĩ tâm lý có vốn hiểu biết sâu rộng nhưng cũng là một trong những kẻ sát nhân ăn thịt người đáng sợ nhất. (ND)

Tờ Pasadena Star-News đăng một bài khá dài về tôi. Sau đó là một câu chuyện còn lớn hơn nữa trên tờ Los Angeles Times số ra ngày Chủ nhật. Dĩ nhiên, vì tôi vẫn là trẻ vị thành niên, nên họ không được phép công khai tên thật của tôi.

Nhưng họ vẫn làm. Và điều này đã mang lại hậu quả lớn về sau.

(Ngoài lề một chút, sau này tôi phát hiện ra người đã hét lên báo có bom logic là Steve Cooley, Trợ lý công tố Quận được ủy quyền trong vụ của tôi. Hiện nay anh ta là người đứng đầu, một công tố viên của Quận Los Angeles. Dì tôi, Chickie Leventhal, điều hành công ty Chickie's Bail Bonds[31] đã lâu và do đó có quen biết với Cooley. Vài năm sau, khi cuốn The Art of Deception (tạm dịch: Nghệ thuật dối lừa) của tôi được xuất bản, dì đã dùng cuốn sách này làm quà trong một cuộc vận động gây quỹ cho trẻ em mà Cooley cũng tham dự. Dì nói với Cooley rằng tôi là cháu dì, anh ta nói anh ta cũng muốn có một cuốn. Anh ta đề nghị tôi ký và viết vào sách: "Chúng ta đã đi cả quãng đường dài." Quả thực là vậy. Tôi rất mừng vì đã làm vậy theo ý anh ta.)

https://thuviensach.vn

[31] Chickie’s Bail Bonds: Công ty chuyên cung cấp dịch vụ hỗ trợ bảo lãnh tạm tha. (ND)

Thẩm phán Phiên tòa xét xử trẻ vị thành niên có vẻ bối rối khi nghe nói về vụ của tôi: Tôi bị buộc tội vì là một hacker, nhưng tôi không hề ăn cắp hay sử dụng bất kỳ số thẻ tín dụng nào, tôi cũng không hề bán các phần mềm sở hữu hay bí mật doanh nghiệp. Tôi chỉ tấn công vào máy tính cũng như các hệ thống của công ty điện thoại vì sở thích đơn thuần. Viên thẩm phán không hiểu nổi tại sao tôi lại hành động không vì “mục đích lợi nhuận” nào. Việc tấn công chỉ vì thú vui có vẻ vô nghĩa.

Do không dám chắc về những gì tôi làm khi đột nhập vào các máy tính và hệ thống điện thoại, ông ta liền cho rằng có thể mình đã để lỡ điều gì đó. Có lẽ tôi đã nhận tiền hoặc thu lợi bằng phương thức công nghệ cao nào đó mà ông ta không hiểu. Toàn bộ sự việc đều có vẻ khả nghi.

Sự thực là, tôi đã đột nhập vào hệ thống điện thoại vì một lý do tương tự như khi một đứa trẻ đột nhập vào ngôi nhà bỏ hoang cuối phố: chỉ để xem thế nào. Cám dỗ muốn được khám phá và tìm ra điều gì ẩn trong đó quá lớn. Hiển nhiên, việc đó đi kèm với những nguy hiểm nhất định, nhưng chấp nhận rủi ro là một phần của cuộc vui.

Vì đây là trường hợp hacking đầu tiên, nên phía công tố Quận khá bối rối trong việc định tội tôi. Một số tội đã được hợp pháp hóa, như việc đột nhập vào công ty điện thoại, một số khác thì không. Công tố viên cho rằng qua việc hacking, tôi đã làm hư hại hệ thống máy tính ở U.S. Leasing. Sự thực là không hề, và đây cũng không phải là lần cuối cùng tôi bị buộc tội này.

Thẩm phán Phiên tòa xét xử trẻ vị thành niên gửi tôi tới Trại Cải tạo Thanh thiếu niên California (CYA) ở Norwalk, California để tiến hành đánh giá tâm lý trong suốt 90 ngày xem liệu tôi có phù hợp cải tạo ở đây không. Tôi chưa từng hoảng sợ như vậy. Những đứa khác bị ném vào đây vì các tội như hành hung, hãm hiếp, giết người hay tấn công có tổ chức. Đúng là ở đó có

https://thuviensach.vn

trẻ vị thành niên. Nhưng chúng thậm chí còn bạo lực và nguy hiểm hơn nữa bởi chúng luôn cảm thấy mình là kẻ vô địch.

Mỗi chúng tôi đều có phòng riêng và bị nhốt trong đó, chỉ được ra ngoài theo nhóm nhỏ chừng ba tiếng mỗi ngày.

Tôi viết thư về nhà, luôn mở đầu bằng câu "Kevin Mitnick bị bắt giam – Ngày 1", "Ngày 2", "Ngày 3". Dù Norwalk thuộc Quận Los Angeles, mẹ và bà tôi vẫn phải mất tới một tiếng rưỡi lái xe tới đó. Hơn những gì tôi xứng đáng được hưởng, họ đều đặn tới mỗi cuối tuần và mang theo đồ ăn. Họ luôn rời nhà từ rất sớm để là người xếp hàng đầu tiên.

Tôi trải qua sinh nhật lần thứ 18 ở trại giam Norwalk. Dù tôi không còn là trẻ vị thành niên nhưng CYA vẫn giam giữ tôi thêm một thời gian. Điều đó có nghĩa là với những lần phạm tội sau, tôi sẽ bị xét xử như một người trưởng thành và nếu bị kết tội, tôi sẽ phải ngồi tù.

Sau 90 ngày, CYA đề nghị tạm tha cho tôi và theo dõi thêm tại nhà. Đề nghị này được tòa chấp thuận.

Phụ trách giám sát tôi trong thời gian bị quản chế là một phụ nữ béo phì cực độ tên là Mary Ridgeway. Tôi có cảm tưởng niềm vui thú duy nhất của bà ta là ăn uống và đánh chửi lũ nhóc thuộc thẩm quyền phụ trách của mình. Có lần điện thoại của bà ta bị hỏng. Vài tháng sau, tôi được biết là công ty điện thoại đã sửa đường dây và họ cũng không rõ tại sao điện thoại lại hỏng. Bà ta đoán chuyện này hẳn liên quan đến tôi và ghi lại trên hồ sơ. Ngay lập tức, những thông tin này được coi là chính xác và có thể được sử dụng để chống lại tôi sau này. Thời đó, rất nhiều lần những vấn đề công nghệ không giải thích được ở đâu đó đều được cho là tại tôi.

Đi kèm với hoạt động quản thúc tại nhà là các buổi tư vấn tâm lý. Tôi được chỉ định đến một phòng khám chuyên điều trị cho mấy kẻ tấn công tình dục và nghiện nặng. Người tư vấn cho tôi là một bác sĩ thực tập người Anh tên là

https://thuviensach.vn

Roy Eskapa. Khi tôi giải thích về việc mình bị bắt vì phone phreaking, mắt anh ta sáng lên: “Cậu có biết điện thoại và điện tín quốc tế (ITT) không?”

“Đương nhiên,” tôi nói.

“Cậu biết làm sao để có được một mã không?”

Anh ta hỏi tôi về mã truy cập ITT. Một khi có mã, bạn có thể quay số truy cập ITT địa phương và thêm vào mã truy cập, sau đó là số điện thoại cho cuộc gọi đường dài mà bạn muốn gọi. Nếu bạn dùng mã truy cập của một ai đó, các cuộc gọi của bạn sẽ được tính tiền lên đầu kẻ tội nghiệp kia và bạn chẳng phải trả một xu nào.

Tôi mỉm cười. Roy và tôi hẳn sẽ làm việc ổn thỏa.

Trong suốt các buổi tư vấn theo yêu cầu của tòa án những năm 1981 và 1982, chúng tôi chỉ trò chuyện và sau đó, trở thành bạn tốt. Roy nói với tôi rằng những gì tôi đã làm quá thuần tính so với các tội ác mà những bệnh nhân khác của anh phạm phải. Nhiều năm sau, năm 1988, khi tôi lại gặp rắc rối, anh viết thư gửi tới tòa, giải thích rằng tôi ham muốn hacking không phải vì các động cơ hiểm độc hay tội ác mà chỉ là dạng rối loạn cưỡng chế. Theo lời anh nói, tôi bị “nghiện” hacking.

Theo những gì tôi và luật sư của mình có thể xác định, đây là lần đầu tiên hacking được đánh giá ở góc độ này và đặt ngang hàng cùng với thuốc kích thích, rượu, cờ bạc và chứng nghiện tình dục. Khi quan tòa nghe mô tả các chẩn đoán về chứng nghiện và nhận ra tôi bị bệnh, bà đã chấp nhận các thỏa thuận nhận tội của tôi.

Đêm ngày 22 tháng 12 năm 1982, ba ngày trước lễ Giáng sinh, tôi ở trong phòng máy tính Salvatori Hall thuộc Đại học Nam California (USC) gần khu trung tâm Los Angeles. Ở cùng tôi là Lenny DiCicco, một gã cao mét tám, gầy lêu nghêu, người sau này đã trở thành chiến hữu hacking thân thiết và đáng tin cậy… và cũng là kẻ phản bội tôi.

https://thuviensach.vn

Trước đó, chúng tôi đã cố hack vào hệ thống của USC qua modem điện thoại nhưng phát điên vì tốc độ kết nối chậm chạp. Thăm dò một hồi, sự hào hứng của chúng tôi chuyển sang sự thực là tòa nhà Salvatori Hall có một bộ máy chủ DEC TOPS-20 kết nối vào Arpanet, tiền thân của mạng Internet. Dùng máy trong khuôn viên trường giúp chúng tôi có thể truy cập nhanh hơn rất nhiều vào hệ thống của trường.

Nhờ vào đặc điểm dễ bị tấn công mà Lenny đã học lỏm được của Dave Kompel tại hội thảo của Hiệp hội Người dùng Máy tính Thiết bị Số (DECUS) mà chúng tôi tham dự một tuần trước đó, chúng tôi đã chiếm được toàn quyền đăng nhập vào toàn bộ hệ thống DEC 20 do sinh viên sử dụng. Nhưng chúng tôi muốn có được càng nhiều mật khẩu càng tốt, bởi dù chúng tôi có quyền quản trị trong tay, hệ thống đã được cấu hình để mã hóa toàn bộ mật khẩu.

Không việc gì phải lo hết. Tôi bắt đầu soát qua toàn bộ các tài khoản e-mail của nhân viên trong trường, những người có toàn quyền đăng nhập. Săn lùng bên trong hệ thống đã dẫn tôi tới hòm thư của phòng kế toán, chuyên phụ trách cấp tên đăng nhập và mật khẩu. Khi tìm kiếm trong e-mail của tài khoản này, tôi thấy đầy rẫy các tin nhắn trao đổi tên đăng nhập và mật khẩu dưới dạng văn bản thông thường. Vớ bẫm rồi!

Dù biết là nguy hiểm, nhưng tôi vẫn gửi toàn bộ tệp e-mail tới máy in. Khoảng 15 phút sau khi đặt lệnh in, nhân viên phụ trách ném tập giấy dày cộp vào khay đựng đồ sinh viên. Phòng máy tính đầy người, làm sao để biết được mình không bị theo dõi và có thể lấy được tài liệu mà không làm dấy lên nghi ngờ đâu đó? Vận dụng hết khả năng, tôi nhặt tập giấy in lên và mang lại chỗ tôi và Lenny đang ngồi.

Một lúc sau, hai nhân viên an ninh trường tiến vào, lao thẳng tới chỗ Lenny và tôi rồi hét lên: “Ngồi yên!”

https://thuviensach.vn

Có vẻ như tôi đã nổi danh. Họ biết rõ ai là mục tiêu thực sự và còn biết cả tên tôi. Sau này tôi mới biết một trong những quản trị viên, Jon Solomon, đã có mặt tại hội thảo DECUS mà tôi và Lenny tham dự trước đó. Jon đã thấy và nhận ra tôi trong phòng máy. Anh ta gọi cho Dave Kompel, người từng ở trong nhóm đặt ra thử thách tấn công vào hệ thống phát triển RSTS/E của DEC khi tôi còn là học sinh ở trường cấp ba Monroe. Kompel nói hãy gọi nhân viên an ninh trường tới và bắt tôi ngay lập tức.

Họ túm lấy chồng giấy in có tất cả mật khẩu trong đó. Do đang trong thời gian bị quản chế, tôi biết mình sẽ gặp rắc rối lớn. Nhân viên an ninh giải chúng tôi về trụ sở trong trường và còng tay chúng tôi vào ghế, sau đó biến mất khỏi văn phòng, để mặc chúng tôi ngồi một mình cạnh lối ra vào. Sau một lúc vặn vẹo, Lenny giơ tay ra trước mắt tôi – tay cậu ta không mang còng. Cậu ta có thói quen mang theo chìa khóa còng tay trong ví và đã xoay xở lấy nó ra để mở khóa.

Lenny mở khóa cho tôi và nói: “Cậu gặp rắc rối lớn hơn tớ, trốn nhanh đi.” Nhưng tôi trốn kiểu gì đây? Mấy gã nhân viên an ninh đã giữ chìa khóa xe của tôi và hơn nữa họ còn biết tôi là ai.

Bỗng có một gã quay lại. Tôi đóng còng lại sau lưng nhưng gã đã nghe thấy tiếng động và tới gần hơn để xem có chuyện gì. “Ê, có Houdini[32] này,” gã hướng về phía văn phòng và gào lên trong khi Lenny lặng lẽ vứt khóa xuống dưới sàn và đá ra xa vài mét. Chiếc chìa khóa văng xuống dưới gầm bánh xe ô tô được dựng bên tường gần đó.

[32] Harry Houdini: Nhà ảo thuật Mỹ nổi tiếng với khả năng thoát khỏi xích, còng tay hay các thùng khóa kín. (ND)

Mấy gã cớm nổi điên và tra vấn: “Chìa đâu?” Họ lần lượt đưa chúng tôi tới phòng vệ sinh để khám xét và khá bối rối khi không tìm thấy nó.

Cảnh sát thuộc Đội Phòng chống Gian lận và Giả mạo của Sở Cảnh sát Los Angeles (LAPD) xuất hiện và giải chúng tôi đi. Họ định đưa tôi đến phòng

https://thuviensach.vn

giam tại trung tâm Parker, trụ sở của LAPD. Lần này, tôi bị ném vào ngục có sẵn một vài máy điện thoại bên trong. Tôi gọi cho mẹ trước tiên để nói cho bà biết chuyện gì đã xảy ra, và sau đó là dì Chickie, van vỉ dì bảo lãnh cho tôi ra càng sớm càng tốt – đây là chuyện cấp thiết bởi tôi muốn lấy xe ô tô trước khi cảnh sát lục soát ở đó. Như mọi khi, trong xe chứa đầy các giấy tờ và đĩa mềm có thể dùng để buộc tội tôi. Một đồng nghiệp của dì giúp tôi ra khỏi đó sau vài tiếng, vào khoảng 5 giờ sáng.

Mẹ tôi, người đã phải chịu đựng quá nhiều nhưng vẫn luôn tin tưởng tôi, đã tới đón và đưa tôi tới trường để lấy xe. Bà thấy mừng vì tôi vẫn ổn và không bị giữ lại. Cho dù tôi có xứng đáng phải chịu một cơn thịnh nộ hay quát mắng thế nào, đó cũng không phải là phong cách của bà. Thay vào đó, bà lo lắng cho tương lai của tôi hơn.

Tôi được tạm tha nhưng tự do chẳng tày gang. Khi lái xe đi làm tối hôm đó, tôi gọi cho mẹ từ Fromin’s Deli, nơi chúng tôi cùng làm việc dạo đó, để xem có ai tới tìm tôi không. “Không hẳn,” mẹ nói. Bỏ qua câu trả lời kín đáo của bà, tôi đi bộ tới nơi làm việc. Mary Ridge, người phụ trách quản thúc tôi trong thời gian tạm tha, đang ở đó cùng hai thám tử. Khi thấy tôi, bà ta thông báo rằng tôi bị bắt vì phạm lỗi trong thời gian chịu quản chế. Gã thám tử lái xe đưa tôi tới Trung tâm Giam giữ Trẻ vị thành niên ở Sylmar.

Thực ra, tới Sylmar lại là một điều may mắn. Tôi đã qua 18 tuổi và là một người trưởng thành theo quan điểm luật pháp. Nhưng vì vẫn đang trong thời gian quản thúc của Tòa án Thanh thiếu niên, nên tôi vẫn thuộc phạm vi quản lý của họ. Tôi được xử lý tương tự như một trẻ vị thành niên.

Nhưng mẹ tôi thì không quan tâm tới sự khác biệt. Tôi lại bị bắt và bị bỏ tù. Điều này cứ lặp đi lặp lại. Cậu con trai yêu quý của bà sẽ trở thành người thế nào đây? Liệu cả đời tôi cứ vào tù ra tội mãi sao? Bà tới thăm tôi và bật khóc. Bà đã làm rất nhiều điều vì tôi, và đây là cách mà tôi đáp trả – bằng nỗi đau và sự lo lắng. Tim tôi vỡ vụn khi thấy mẹ khóc. Đã bao lần tôi hứa

https://thuviensach.vn

với bà sẽ từ bỏ hacking? Tôi đã thực tâm muốn làm vậy nhưng vẫn chẳng khác một gã say không ngừng nốc rượu.

Cuối cùng thì lần hacking đó đã mang tới hậu quả kéo dài hơn những gì tôi có thể tưởng tượng ở thời điểm đó rất nhiều. Một trong những tài khoản tôi đăng nhập từ phòng máy của trường thuộc về một người có tài khoản sinh viên nhưng thực ra lại làm việc ở Lầu Năm góc. Khi cảnh sát phát hiện ra điều này, họ đã mớm chuyện cho cánh báo chí và các tờ báo lại cho đăng những tựa báo gây sốt bóp méo sự thật. Họ viết rằng tôi đã tấn công vào Bộ Quốc phòng. Lời cáo buộc này vẫn theo tôi tới tận bây giờ, dù nó hoàn toàn sai.

Tôi thừa nhận mình đã phạm lỗi trong thời gian chịu quản thúc tại nhà và bị gửi tới Trại Cải tạo Thanh thiếu niên trong suốt ba năm tám tháng, đây là khoảng thời gian tối đa họ có thể xử phạt tôi.

Nhưng tôi đã mắc nghiện – dù bị giam giữ, tôi vẫn tìm cách đánh bại hệ thống.

https://thuviensach.vn

05

TẤT CẢ ĐƯỜNG DÂY ĐIỆN THOẠI CỦA CÁC ANH ĐỀU THUỘC VỀ TÔI

Bmfy ytbs ini N mnij tzy ns zsynq ymj Ozajsnqj Htzwy qtxy ozwnxinhynts tajw rj?

Sau khi bị kết án, tôi lại được chuyển đến cơ sở ở Norwalk, phụ trách phân loại sách. Tôi trú ngụ trong thư viện và nhận ra ở đó có cả một bộ sưu tập sách luật rất hay. Chúng trở thành mối quan tâm mới của tôi.

Một số thanh thiếu niên đang bị giam giữ ở đó muốn điền đơn phúc thẩm hoặc tìm hiểu xem chúng có những quyền lợi gì, và tôi bắt đầu giúp đỡ chúng bằng cách nghiên cứu hộ. Ít nhất tôi cũng đang làm một chút việc tốt cho người khác và thấy thỏa mãn với việc đó.

Bộ sưu tập sách của thư viện hóa ra còn bao gồm những tài liệu hướng dẫn điều hành CYA. Đúng là tiện thật, tôi nghĩ. Họ định cho mình tìm hiểu cách họ làm việc để mình có thể tìm ra các sai sót và kẽ hở rồi. Tôi cứ thế vùi đầu vào nghiên cứu tài liệu.

Tôi được phân cho một luật sư cố vấn. Ông ta nói chuyện với tôi vài lần rồi đưa ra đề nghị sẽ gửi tôi đến Preston, trại cai ngục thanh thiếu niên tương đương ở San Quentin, một nơi đầy những kẻ nguy hiểm và bạo lực nhất trong hệ thống các trại cai ngục thanh thiếu niên ở bang California. Tại sao ư? Bởi tôi chắc chắn là một trong số ít tội phạm "cổ cồn trắng"[33] mà hệ thống trại cai ngục thanh thiếu niên từng phải xử lý.

https://thuviensach.vn

[33] Tội phạm cổ cồn trắng: Loại hình tội phạm không có tính chất bạo lực, thường liên quan đến tiền và đối tượng phạm tội thường có mục đích kiếm lợi cho bản thân. (BTV, theo Wikipedia)

Gã luật sư thậm chí còn bảo tôi rằng hắn chọn chỗ đó một phần vì nó ở rất xa – phải lái xe mất khoảng 7-8 tiếng, nghĩa là mẹ và bà tôi lâu lâu mới đến thăm tôi một lần. Có thể gã nghĩ rằng thằng nhóc trung lưu này đã có tất cả các cơ hội mà những gã thô lỗ ở trung tâm thành phố chưa bao giờ có, và thay vì lấy một tấm bằng đại học cùng một công việc ổn định lương cao, tôi đã luôn đẩy mình vào rắc rối… Nếu gã gửi tôi tới một nơi nguy hiểm và khắc nghiệt, điều đó sẽ đủ để dọa tôi quay lại con đường chân chính. Hoặc có thể gã chỉ là một tên khốn độc ác, lạm dụng quyền hành của mình.

Nhưng có ai lường trước được tương lai? Trong tài liệu hướng dẫn điều hành CYA, tôi tìm thấy một danh sách các yếu tố bắt buộc phải xem xét khi quyết định trại giam dành cho thanh thiếu niên. Cậu ta phải được ở gần gia đình. Nếu đã tốt nghiệp trung học hoặc nhận được chứng chỉ GED, cậu ta phải được ở một trại giam có giảng dạy chương trình đại học – điều mà trại Preston chắc chắn không có. Trại phải được chọn dựa trên thiên hướng bạo lực tự nhiên và việc liệu cậu ta có vẻ sẽ trốn trại hay không. Tôi chưa bao giờ tham gia đánh nhau và chưa bao giờ thử trốn trại. Sau tất cả, theo tài liệu hướng dẫn, mục tiêu là cải tạo. Tuyệt vời.

Tôi chép lại những trang đó.

Quá trình giải quyết tranh chấp cũng mang lại một bài học thú vị: Một tù nhân có thể yêu cầu một chuỗi phiên xét xử, kết thúc bằng một phiên xử mà ở đó một thẩm phán tới từ bên ngoài sẽ đến nghe các chứng cứ và đưa ra phán quyết công bằng ràng buộc tất cả các bên.

Tôi đã trải qua các bước trong các phiên xử. Khi thẩm phán trung lập được đưa tới, các thành viên của hội đồng CYA – gồm năm người – đưa ra quan

https://thuviensach.vn

điểm về trường hợp của tôi, hoàn tất phần trình bày bằng những trang giấy chép lại từ tài liệu hướng dẫn điều hành để củng cố quyết định của họ.

Một nước cờ thông minh, ngoại trừ việc họ đã dùng phiên bản lỗi thời của cuốn tài liệu hướng dẫn, với những điều khoản không thực sự có lợi cho tôi.

Khi đến lượt mình trình bày, tôi nói: “Hãy để tôi cho ông xem bản sửa đổi hiện hành của cuốn tài liệu hướng dẫn mà những người kia đã không đưa cho ông.” Và tôi ra vẻ khẩn thiết cầu xin muốn được cải tạo bản thân.

Thẩm phán nhìn vào thời gian trên những trang giấy mà luật sư đưa ra, rồi lại nhìn vào thời gian trên những trang giấy của tôi.

Và ông ta thậm chí đã nháy mắt với tôi.

Ông ta yêu cầu gửi tôi đến một cơ sở có chương trình đại học. Họ gửi tôi đến Karl Holton, ở Stockton, phía đông San Francisco. Tuy cách nhà một quãng xa, nhưng tôi cảm thấy mình đã chiến thắng và rất tự hào về bản thân. Nhìn lại, tôi nhớ tới những lời ca trong bài hát của Tom Petty: “You could stand me up at the gates of hell but I won’t back down.” (tạm dịch: Các anh có thể bỏ rơi tôi bên cánh cửa địa ngục nhưng tôi sẽ không lùi bước).[34]

Với tôi, Karl Holton hóa ra lại là Holiday Inn[35] của CYA với điều kiện sống tốt hơn, thức ăn ngon hơn. Dù nơi đây cách nhà năm tiếng lái xe, nhưng mẹ và bà vẫn đến thăm tôi hai tuần một lần, và vẫn mang cho tôi hàng đống đồ ăn như trước. Chúng tôi nướng thịt hay tôm hùm trên những vỉ nướng ngoài trời như những con người văn minh, tôi và mẹ sẽ tìm những ngọn cỏ bốn lá trên bãi cỏ của khu thăm nom ngoài trời. Những chuyến thăm của họ khiến thời gian giam giữ của tôi như ngắn lại.

[34] Trích ca khúc “I won’t back down” của Tom Petty. (BTV)

[35] Thương hiệu khách sạn lớn, thuộc chuỗi khách sạn InterContinental Hotels Groups nổi tiếng khắp thế giới. (BTV)

https://thuviensach.vn

Các luật sư sẽ tới gặp các gia đình, và luật sư của tôi có vẻ lịch sự quá mức với mẹ tôi.

Những khía cạnh khác trong thời gian cải tạo của tôi không được êm ả như vậy. Loại dao cạo duy nhất được cho phép là loại dùng một lần và lần nào nó cũng cắt vào da tôi, vì thế tôi đã ngừng cạo râu. Râu mọc rậm và dày khiến tôi hoàn toàn thay đổi diện mạo; tôi sẽ giữ diện mạo đó tới chừng nào còn ở trong trại.

Tôi được thả sớm chỉ sau sáu tháng. Khi khai vào biên bản Điều kiện Tại ngoại, tôi bị hỏi: “Chúng tôi có thể đặt ra điều kiện gì để cậu không hack nữa?”

Làm sao tôi có thể trả lời được câu hỏi này? Tôi nói: “À, có hành động hacking có đạo đức và hacking vô đạo đức.”

“Tôi cần thuật ngữ chuyên ngành,” người kia đáp lại. “Tôi có thể viết gì vào đây?”

Bộ phim Star War (Chiến tranh giữa các vì sao) đột nhiên nảy ra trong đầu tôi. Tôi nói: “Ông có thể gọi đó là ‘hacking hắc ám (dark side hacking).’”

Và đó là cách nó được ghi vào biên bản Điều kiện của tôi: “Không hacking hắc ám.”

Tôi nghĩ một phóng viên của tờ LA Times bằng cách nào đó đã nhìn thấy cụm từ này. Nó được lựa chọn và được báo chí sử dụng rộng rãi, trở thành một dạng biệt danh cho tôi. Kevin Mitnick, Hacker Hắc Ám.

Sau khi tôi được thả, một cảnh sát đã gọi cho tôi, tự xưng là Dominick Domino và giải thích rằng ông ta là người đã lái xe đưa tôi đến Tòa án xét xử thanh thiếu niên khi tôi bị bắt ở Fromin. Ông ta đang thực hiện một video huấn luyện LAPD về tội phạm máy tính và hỏi tôi liệu có muốn đến ghi hình phỏng vấn không? Tất nhiên rồi, tại sao không?

https://thuviensach.vn

Tôi không nghĩ họ vẫn sử dụng chiếc đĩa này sau ngần ấy năm, nhưng trong suốt một thời gian dài, tôi từng góp phần giúp cảnh sát Los Angeles nỗ lực học cách bắt những kẻ như tôi.

Vào thời điểm đó, bà tôi đã buôn chuyện với một người bạn, bà Donna Russell, người đang giữ chức vụ Giám đốc Bộ phận Phát triển Phần mềm của hãng phim 20th Century Fox, để có thể xin việc cho tôi. Tôi nghĩ,Quá tuyệt – biết đâu mình thậm chí còn có thể sánh vai cùng một vài ngôi sao điện ảnh. Tôi yêu công việc này. Tôi làm việc ngay tại phim trường, đi bộ qua khu âm thanh để đến tòa nhà của mình; tiền lương khá hậu hĩnh, hãng phim đào tạo tôi phát triển các ứng dụng bằng COBOL và Basic Assembly Language của IBM, ngoài ra tôi còn học được cách làm việc với các máy tính cỡ lớn của IBM và máy tính cỡ trung của HP.

Nhưng người ta vẫn thường nói mọi cuộc vui sớm muộn đều đến lúc tàn – và trong trường hợp này, nó đã đến sớm thay vì đến muộn. Một nhân viên khác đã đâm đơn kiến nghị rằng, theo luật của công đoàn, công việc này đáng lẽ phải được giao cho các nhân viên hiện tại.

Chỉ sau hai tháng, tôi đã lại trắng tay, thất nghiệp.

Cú sốc ập đến khi viên quản chế của tôi, Melvin Boyer, gọi tới và nói: “Kevin, hãy ăn sáng thật no, ăn càng nhiều càng tốt, rồi đến gặp tôi.” Điều đó chỉ có thể có một ý nghĩa duy nhất: rắc rối.

Trong thế giới ham radio của Los Angeles, có một nhóm chuyển tiếp sóng trên tần số 147,435 Mhz được gọi là “trại thú vật”. Bọn chúng sẽ tấn công lẫn nhau, sử dụng ngôn ngữ bậy bạ, và chặn phá việc truyền phát sóng của người khác. Đối với tôi, đó chỉ là một trò chơi. Sau này, tôi biết rằng một gã trong nhóm trại thú vật hẳn có hận thù gì đó với tôi nên đã gọi cho Văn phòng Quản chế của Trại Cải tạo Thanh thiếu niên để than phiền rằng tôi đã hack vào mạng máy tính của công ty hắn. Tôi không hề làm vậy. Nhưng gã này làm cho Xerox, tôi đoán điều đó khiến gã có vẻ đáng tin cậy.

https://thuviensach.vn

Mẹ lái xe đưa tôi đến đó. Giám sát viên quản chế yêu cầu tôi đi theo ông ta đến văn phòng. Ông ta nói với mẹ tôi sẽ quay lại ngay và rằng bà có thể đợi ở phòng chờ. Thay vào đó, tôi lập tức bị viên giám sát còng tay khi họ dẫn tôi đi theo cửa phụ để ra một chiếc xe đã đợi sẵn. Tôi gào lên với mẹ rằng họ lén đưa tôi ra ngoài và bắt tôi vì những việc tôi chưa từng làm.

Tôi được viên quản chế và giám sát viên của ông ta đưa đến trại giam Van Nuys. Có một sự trùng hợp kỳ quặc khi bác Mitchell đã gọi cho tôi từ chính trại giam này chỉ vài tuần trước đó. Cuộc đời của bác cũng đầy thăng trầm: Bác trở thành triệu phú bất động sản, an cư trong một dinh thự ở Bel Air, khu cao cấp hơn cả Beverly Hills, tọa lạc ở khu đắc địa của Los Angeles. Nhưng rồi bác tìm đến cocain, heroin, rồi – chuyện xưa như Trái đất – mất nhà, tiền tài, danh dự và cả tự trọng.

Nhưng lúc đó, tôi vẫn dành rất nhiều tình cảm cho bác. Đêm bác gọi điện từ trại giam Van Nuys, tôi đã nói: “Bác có muốn cháu sửa máy điện thoại công cộng để bác có thể gọi điện miễn phí không?” Tất nhiên là bác muốn.

Tôi nói với bác: “Khi chúng ta cúp máy, hãy nhấc máy lại và quay số 211-2345. Lúc đó, sẽ có một thông báo tự động cho bác biết số điện thoại mà bác đang dùng. Hãy gọi lại cho cháu, cố nhớ và nói cho cháu biết số điện thoại đó.” Khi tôi có được số điện thoại đó, bước tiếp theo là thay đổi một trong số các bộ chuyển mạch của công ty điện thoại. Từ máy tính của mình, tôi gọi vào bộ chuyển mạch thích hợp và đổi “mã lớp đường dây” trên điện thoại đó thành mã cho một số điện thoại nhà riêng, cho phép các cuộc gọi đến và đi. Trong lúc đó, tôi đã thêm vào tính năng gọi ba bên và chờ cuộc gọi. Tôi đã lập trình chiếc điện thoại đó sao cho tất cả cước phí sẽ được tính vào hóa đơn của đồn cảnh sát LAPD Van Nuys.

Một tuần sau, tôi lại có mặt tại chính trại giam Van Nuys này, nơi mà nhờ vào việc tốt tôi đã làm cho bác Mitchell, tôi có thể thực hiện tất cả các cuộc gọi miễn phí mà mình muốn. Tôi ôm điện thoại xuyên đêm. Nói chuyện với bạn bè giúp tôi thoát khỏi thực tại về nơi tôi đang sống. Hơn nữa tôi cần tìm

https://thuviensach.vn

một luật sư có thể bào chữa cho tôi, bởi tôi biết khi bị gửi trả lại để đối mặt với Hội đồng Cai ngục của CYA, tôi sẽ phải đối mặt với một cuộc chiến vô cùng khó khăn. Những người bị cai ngục có rất ít quyền, và hội đồng chỉ cần tin tôi có thể đã làm bất cứ thứ gì mà tôi đang bị buộc tội; các chứng cứ không cần phải đạt tiêu chuẩn "vượt ngoài nghi ngờ có căn cứ" như trong một buổi xét xử hình sự.

Mọi việc dần trở nên tồi tệ hơn. Họ chuyển tôi đến Trại giam của Quận Los Angeles, nơi tôi được chào đón bằng việc cởi bỏ hết quần áo để họ có thể xịt thuốc diệt côn trùng lên khắp người. Tôi bị dẫn đến một khu trại khiến tôi sợ hết hồn. Tôi không biết còn có hạng người nào đáng sợ hơn: Những gã bặm trợn có thể sẽ móc mắt bất kỳ ai nếu có cơ hội, hay những gã điên khùng có thể làm hại ai đó mà thậm chí còn không biết mình đang làm gì. Tất cả các giường đều có người nằm, vì thế tôi không có chỗ ngủ. Tôi chỉ đứng dựa vào tường, cố gắng giữ mình tỉnh táo để đến khi mặt trời mọc, tôi vẫn còn tất cả những thứ đã mang theo khi đến đây.

Boyer, viên quản chế Trại Cải tạo Thanh thiếu niên, nói với mẹ tôi: "Trại giam của Quận Los Angeles là một nơi rất nguy hiểm. Thằng bé có thể sẽ bị ăn đòn ở đó", rồi chuyển tôi về Norwalk ngay hôm sau. Giờ đây, nếu gặp lại Boyer, tôi chắc sẽ ôm ông ấy thật chặt vì việc đó.

Dù đã 20 tuổi nhưng nhờ đang trong thời gian quản chế, tôi vẫn thuộc quyền xét xử của Trại Cải tạo Thanh thiếu niên. Đây là lần thứ ba Trung tâm Tiếp nhận Norwalk chào đón tôi; một số lính gác ở đây cũng nhẵn mặt tôi rồi.

Trong lần hầu tòa của tôi trước hội đồng cai ngục, họ rõ ràng không coi trọng đơn kiện tôi, có lẽ vì không có bằng chứng gì ngoài một báo cáo từ viên cai ngục kia dựa trên một khiếu nại duy nhất. Họ kết luận rằng tôi đã vi phạm lệnh cấm sử dụng ham radio từ Phòng Quản chế. Nhưng đó không phải là một lệnh cấm hợp pháp: Chỉ có Ủy ban Truyền thông Liên bang (FCC) mới có thẩm quyền tước quyền sử dụng ham radio của tôi. Họ bắt

https://thuviensach.vn

giam tôi 60 ngày; lúc đó, tôi đã ở trong trại được khoảng 57 ngày, vì vậy, tôi được thả vài ngày sau đó.

Khi mẹ đến đón, tôi đã lái xe đưa bà đến Học viện Cảnh sát Los Angeles. Tôi nghe nói họ có bán một khung biển số xe được cho là thân thiện với cảnh sát – nếu cảnh sát nhìn thấy nó, họ có thể sẽ không tấp bạn vào lề đường khi bạn vi phạm luật giao thông. Trong cửa hàng, tôi đã để ý thấy một chồng sách niên giám LAPD. Tôi nói muốn một cuốn "làm quà cho chú tôi, người đang ở LAPD". Tuy tốn 75 đô-la nhưng với tôi, cuốn niên giám thật tuyệt vời, hệt như tôi đã tìm thấy Chén thánh vậy: Nó có ảnh của tất cả sĩ quan LAPD, kể cả những gã hoạt động ngầm được giao giải quyết tội phạm có tổ chức.

Tôi tự hỏi không biết họ có xuất bản cuốn sách đó hằng năm… và bán cho bất kỳ ai chịu trả tiền hay không.

Một người bạn của mẹ tôi, một doanh nhân tên là Don David Wilson, lúc đó đang điều hành vài công ty thuộc một công ty mẹ có tên Franmark. Ông ta đã thuê tôi hỗ trợ những việc có liên quan đến máy tính – lập trình, nhập dữ liệu… Công việc này rất buồn chán, vì vậy để tìm niềm vui, hứng thú và thử thách trí tuệ – hẳn bạn sẽ chẳng lấy gì làm ngạc nhiên – tôi quay lại với hacking và phreaking với ông bạn cũ Steve Rhoades, người sẽ đến vào buổi tối để dùng máy tính ở Franmark.

Một ngày nọ, trên đường đi ăn trưa với một nữ đồng nghiệp trẻ ở chỗ làm, tôi phát hiện thấy một nhóm mặc đồng phục cảnh sát và viên cai ngục cũ cùng một người từng lục soát xe tôi nhiều năm trước để tìm "bom logic". Tôi biết bọn họ không ở đây để thăm hỏi xã giao. Chết tiệt! Tôi lo sốt vó. Tôi không thể co cẳng chạy hay đi đủ nhanh mà không bị chú ý. Vì thế, tôi quay lưng về phía nhóm người mặc đồng phục và ôm nữ đồng nghiệp kia thật chặt, thì thầm vào tai cô ấy rằng tôi vừa nhìn thấy một người bạn cũ và không muốn anh ta thấy tôi. Chúng tôi chui vào xe của cô ấy, vẫn nằm trong tầm mắt của nhóm người kia.

https://thuviensach.vn

Tôi cúi thấp xuống và nhờ cô ấy lái xe đi thật nhanh bởi tôi cần phải thực hiện một cuộc gọi quan trọng. Từ máy điện thoại công cộng, tôi gọi đến chi nhánh West Valley của LAPD và yêu cầu được nối máy đến phòng lưu trữ. "Đây là thám tử Schaffer," tôi nói. "Tôi cần kiểm tra một đối tượng xem anh ta có vi phạm gì tại địa phương và cả Trung tâm Thông tin tội phạm của FBI (NICC) không. Mitnick, M-I-T-N-I-C-K, Kevin David. Ngày sinh của đối tượng là ngày 6 tháng 8 năm 1963."

Tôi khá chắc câu trả lời sẽ là gì.

"Có, chúng tôi có một vụ với anh ta. Có vẻ như là vi phạm trát của CYA."

Tiên sư…! Nhưng ít nhất họ đã không bắt được tôi.

Tôi gọi cho mẹ và nói: "Mẹ ơi, con đang ở 7-Eleven, mẹ con mình cần nói chuyện."

Đó là một mật mã của hai mẹ con tôi. Bà biết 7-Eleven nào, và tôi cần nói chuyện bởi tôi đang gặp rắc rối. Khi bà có mặt, tôi đã kể cho bà câu chuyện và rằng tôi cần một nơi để trốn cho đến khi quyết định sẽ làm gì.

Bà tôi thu xếp với bà bạn Donna Russell, người đã thuê tôi ở Fox, để tôi có thể ngủ trên salon phòng khách vài hôm.

Mẹ lái xe đưa tôi đến đó, dừng giữa đường để tôi có thể mua bàn chải, dao cạo râu và một ít đồ lót cùng với tất. Ngay khi ổn định, tôi tìm trường luật gần nhất trong cuốn Những trang Vàng, và dành cả ngày lẫn đêm ở đó nghiền ngẫm Bộ luật Phúc lợi và Định chế, nhưng không có nhiều hy vọng.

Tuy nhiên, "Chỉ cần có niềm tin…" Tôi tìm thấy một điều khoản nói rằng với tội danh phi bạo lực, quyền pháp lý của Tòa án xét xử Thanh thiếu niên sẽ hết hiệu lực khi bị can 21 tuổi hoặc hai năm sau ngày phạm tội, tùy điều kiện nào xảy ra sau. Với tôi, điều đó có nghĩa là hai năm tính từ tháng 2 năm 1983, khi tôi bị kết án ba năm tám tháng.

https://thuviensach.vn

Tôi gãi đầu gãi tai. Một phép toán nhỏ nói với tôi rằng việc đó sẽ diễn ra sau khoảng bốn tháng nữa. Tôi nghĩ:Nếu mình biến mất cho đến khi quyền pháp lý của họ hết hiệu lực thì sao nhỉ?

Tôi gọi cho luật sư và trình bày ý tưởng đó với ông ta. Ông ta có vẻ phật ý: ”Chắc chắn là cậu sai rồi. Nguyên tắc cơ bản của luật pháp là nếu bị can biến mất khi có lệnh bắt, thời gian sẽ bị gián đoạn cho đến khi tìm thấy cậu ta, kể cả sau nhiều năm.”

Ông ta còn nói thêm: “Cậu phải dừng ngay trò làm luật sư này đi. Tôi là luật sư. Hãy để tôi làm việc của mình.”

Tôi nài nỉ ông ta xem kỹ lại điều khoản, tuy khó chịu nhưng cuối cùng ông ta cũng đồng ý. Hai ngày sau khi tôi gọi lại, ông ta đã nói chuyện với Melvin Boyer, viên cai ngục giàu lòng trắc ẩn đã chuyển tôi khỏi chốn rừng rú nguy hiểm ở Trại giam Quận Los Angeles. Boyer bảo ông ta: “Kevin nói đúng đấy. Nếu cậu ta biến mất từ giờ đến tháng 2 năm 1985, chúng tôi sẽ không thể làm gì được. Đến lúc đó, lệnh bắt giữ sẽ hết hiệu lực và cậu ta sẽ thoát nguy.”

Quanh tôi có một số thiên thần. Donna Russell đã liên hệ với bố mẹ bà, họ có một căn hộ ở Oroville, California, cách San Francisco khoảng 240km về phía Đông Bắc. Và tất nhiên, họ sẽ sẵn lòng nhận một người giúp việc loanh quanh, và được mẹ anh ta trợ cấp tiền hằng tháng, vào ở trọ.

Ngay hôm sau, tôi bắt xe buýt Greyhound và lên đường. Quãng đường dài giúp tôi có thêm thời gian để chọn lấy một cái tên tạm thời: Michael Phelps (phần họ được lấy từ series phim truyền hình Mission Impossible(Nhiệm vụ bất khả thi)).

Có lẽ một trong những người “bạn” hacker đáng tin tưởng của tôi đã tung tin đồn rằng tôi chạy trốn đến Israel. Thực tế, tôi không hề đến đó – và cho đến nhiều năm sau này – tôi thậm chí còn chưa bao giờ bước qua biên giới đến Canada hay Mexico, nói gì đến đi sang bờ kia đại dương. Nhưng đây là một

https://thuviensach.vn

trong những câu chuyện về sau sẽ trở thành một phần của huyền thoại, một trong những "sự thật" không đúng về quá khứ của tôi. Sau này, nó được dùng làm lý do để thuyết phục quan tòa không cho phép tôi được bảo lãnh.

Chủ nhà của tôi ở Oroville, bà Jessie và ông Duke, đã nghỉ hưu và sống trong một trang trại rộng nửa mẫu đất trong khu nông nghiệp. Họ là những người tốt nhưng lối sống có phần cứng nhắc. Lịch trình của họ ngày nào cũng nhất nhất là: Thức dậy vào 5 giờ sáng, ăn bánh mì ngô và uống sữa vào bữa sáng. Sau bữa tối, ngồi xem chương trình giải trí trên truyền hình. Không máy tính. Không modem. Không ham radio. Đây đúng là một cuộc sống khó chịu đối với một gã như tôi, nhưng vẫn tốt hơn nhiều so với việc ngồi sau bức tường của Trại Cải tạo Thanh thiếu niên.

Đôi vợ chồng già nuôi gà và lợn cùng hai con chó. Đối với tôi, khung cảnh ở đây hệt như trong bộ phimGreen Acres (tạm dịch: Vùng đồng cỏ xanh)[36]. Tôi thề là một trong số những con lợn ở đây nhìn hệt như Arnold, con lợn trong phim luôn!

[36] Loạt phim truyền hình ở Mỹ kể về một cặp vợ chồng chuyển từ New York về vùng thôn quê. (ND)

Hiển nhiên là tôi không thể lái xe, bởi bằng lái xe duy nhất mà tôi có đang để tên thật của tôi, và hiện đang có lệnh truy bắt tôi. Vì thế, để đi loanh quanh, tôi mua một chiếc xe đạp.

Tôi đạp xe đến một thư viện trong vùng và dành hàng giờ đọc sách. Ngoài ra, để giữ cho đầu óc linh hoạt, tôi đăng ký một khóa học về Tư pháp Hình sự ở một trường địa phương. Giảng viên là một thẩm phán tòa án hình sự ngồi ở Quận Butte. Trong suốt khóa học, ông ta cứ bật những chiếc đĩa ghi lời thú tội. Và ông ta giảng giải các nghi phạm đã ngây thơ ra sao khi khai với cảnh sát mà không có luật sư. Một lần, ông ta nói: "Hầu hết tội phạm đều tin rằng họ có thể tự bào chữa để thoát khỏi rắc rối." Tôi mỉm cười, biết rằng đó là một lời khuyên rất tuyệt vời. Tôi thích thú tự hỏi không biết ông

https://thuviensach.vn

ta sẽ nghĩ gì nếu phát hiện ra một sinh viên ngồi hàng đầu trong lớp hiện đang lĩnh trát truy nã.

Tôi mắc kẹt với lối sống Green Acres trong bốn tháng, cho đến khi nhận được cuộc gọi từ luật sư xác nhận rằng ông ta đã nhận được một bản sao giấy miễn trừ từ CYA nói rằng họ không còn quyền pháp lý với tôi nữa. Tay luật sư nói rằng đó là tờ giấy miễn trừ "nhục nhã". Tôi chỉ cười lớn. Ai thèm quan tâm liệu nó có nhục nhã hay không? Ngay từ đầu, tôi đã không màng đến danh dự rồi. Việc này đâu có giống như việc tôi đào ngũ.

Chỉ trong vài ngày, tôi đã trở về Los Angeles với đầy hy vọng. Lenny DiCicco vừa nhận được công việc điều khiển máy tính ở Hughes Aircraft và đang nóng lòng đợi tôi ghé thăm. Còn hơn thế, Lenny nói cậu ta có thứ muốn chia sẻ với tôi, một thứ cậu ta không muốn nói qua điện thoại. Tôi tự hỏi không biết đó có thể là gì.

https://thuviensach.vn

06
HACK VÌ YÊU

Kyoo olxi rzr Niyovo Cohjpcx ojy dn T apopsy?

Thời còn làm ở Hughes Aircraft, Lenny DiCicco kể với tôi việc cậu ta đã kết thân với một nữ bảo vệ. Do đó, tôi định tới thăm Lenny vào đêm cô gái kia trực và nói rằng tôi là nhân viên DEC. Khi tôi tới, cô ấy nháy mắt và cho tôi vào, không buồn hỏi tới thẻ ID.

Lenny ra đón tôi từ ngoài sảnh, không nén nổi sự hào hứng nhưng cũng không kém phần kiêu căng tự mãn. Cậu ta dẫn tôi tới máy tính VAX của Hughes, thiết bị có thể đăng nhập vào Arpanet và được kết nối với một loạt các trường đại học, phòng nghiên cứu, đối tác chính phủ... Gõ vài dòng lệnh, cậu ta nói mình đang truy cập vào hệ thống máy tính có tên là Dockmaster, do Trung tâm An ninh Máy tính Quốc gia (NCSC), một đơn vị thuộc Cơ quan An ninh Quốc gia (NSA) sở hữu. Trong niềm hân hoan, chúng tôi biết rằng đây là cơ hội tiến gần nhất có thể tới NSA.

Khi huênh hoang về khả năng tấn công bằng kỹ thuật xã hội của mình, Lenny khoe rằng cậu ta đã giả vờ là một thành viên của đội IT thuộc NCSC và lừa phỉnh được một nhân viên ở đó có tên là T. Arnold để lộ thông tin đăng nhập vào hệ thống của anh ta. Lenny gần như nhảy nhót trong niềm hứng chí và tự hào. Cậu ta vốn là một kẻ cuồng công nghệ và giờ thì có vẻ giống như một kẻ vừa chơi thuốc khi nói rằng: “Tớ cũng giỏi tấn công bằng kỹ thuật xã hội hệt như cậu vậy, Kevin ạ!”

Chúng tôi tìm kiếm trong khoảng một tiếng nhưng chỉ thu được vài thông tin không mấy thú vị.

https://thuviensach.vn

Rất lâu sau này, một tiếng đồng hồ đó đã trở thành nỗi ám ảnh trong tôi.

* * *

Tôi chắc rằng cách nhanh nhất để nâng cao kỹ thuật máy tính nhằm đạt được công việc mà tôi hằng ao ước chính là làm việc cho General Telephone. Tôi cũng biết rằng công ty đang tích cực tuyển sinh viên tốt nghiệp từ một trường kỹ thuật có tên là Trung tâm Giảng dạy Máy tính. Từ nhà tôi lái xe tới trung tâm này khá tiện và tôi có thể có được chứng chỉ tốt nghiệp chỉ sau sáu tháng học.

Quỹ Liên bang Pell và khoản vay sinh viên đã giúp tôi có tiền trang trải để thực hiện mục tiêu của mình, thêm vào đó là một chút hỗ trợ của mẹ cho các khoản phụ phí. Trường học yêu cầu các sinh viên nam phải mặc âu phục và đeo cà vạt tới lớp hằng ngày. Tôi chưa từng mặc lại trang phục kiểu đó kể từ lễ trưởng thành bar mitzvah năm 13 tuổi. Giờ đây tôi đã 23, bự lên khá nhiều và bộ âu phục cũ hẳn là đã quá chật. Mẹ mua cho tôi hai bộ đồ mới.

Tôi thích lập trình bằng các dạng "hợp ngữ"[37], thường khó hơn nhiều bởi lập trình viên phải thông thạo nhiều chi tiết kỹ thuật, nhưng bù lại, họ sẽ thu được các mã hiệu quả hơn nhiều trong điều kiện sử dụng ít không gian bộ nhớ hơn. Lập trình bằng ngôn ngữ bậc thấp này rất thú vị. Tôi có cảm giác mình được kiểm soát các ứng dụng của mình nhiều hơn. So với việc sử dụng các ngôn ngữ bậc cao như COBOL, tôi có thể lập trình gần với ngôn ngữ máy tính hơn. Chương trình ở lớp thường đưa ra các thử thách có chút khó khăn, nhưng cũng rất hấp dẫn. Tôi được làm những gì mình yêu thích: học thêm về các hệ máy tính và lập trình. Đôi khi trên lớp bàn tới chủ đề hacking, tôi chỉ lắng nghe, vờ như không biết.

[37] Hợp ngữ (assembly language): Ngôn ngữ lập trình bậc thấp dùng để viết các chương trình máy tính. Ngoài ra nó còn đặc biệt được sử dụng để viết hệ điều hành. (BTV)

https://thuviensach.vn

Dĩ nhiên, tôi vẫn tiếp tục hack. Tôi đã chơi trò mèo đuổi chuột với Pacific Bell, tên mới của Pacific Telephone sau khi cải tổ, được một thời gian. Mỗi lần tôi tìm ra cách mới để đột nhập vào bộ chuyển mạch của công ty, luôn có ai đó nghĩ ra phương thức khác để chặn tôi lại. Tôi dùng các số điện thoại mà RCMAC sử dụng để kết nối vào các bộ chuyển mạch khác nhau nhằm thực hiện các cuộc gọi dịch vụ, sau đó họ sẽ phát hiện ra, rồi thay đổi số dial-up hoặc hạn chế chúng để tôi không thể thực hiện cuộc gọi. Tôi lại loại bỏ các hạn chế đặt ra khi họ không chú ý. Mọi việc cứ tiếp diễn như vậy trong vài tháng trời. Sự can thiệp không ngừng của họ khiến thú vui hacking vào bộ chuyển mạch của Pacific gần như là công việc hằng ngày của tôi.

Sau đó, tôi nghĩ ra một phương thức tiếp cận ở mức độ cao hơn: tấn công vào Hệ thống Trung tâm Điều khiển Chuyển mạch (SCCS). Nếu làm được, tôi sẽ nắm quyền kiểm soát tương đương với việc ngồi trực tiếp ngay trước hệ thống chuyển mạch, làm bất kỳ việc gì tôi muốn mà không cần tiến hành tấn công bằng kỹ thuật xã hội với nhóm kỹ thuật viên mù mờ ngày qua ngày. Quyền truy cập và sức mạnh tối thượng sẽ nằm trong tay tôi.

Tôi bắt đầu bằng một đợt tấn công vào SCCS ở Oakland, Bắc California. Trong cuộc gọi đầu tiên, tôi dự định sẽ nói rằng tôi đến từ Trung tâm Hỗ trợ Hệ thống Điện tử (ESAC), cung cấp hỗ trợ về mặt kỹ thuật cho toàn bộ phần mềm SCCS triển khai trên toàn công ty. Tôi tìm hiểu thông tin trước, chọn tên một nhân viên chính thức của ESAC và đưa ra yêu cầu: “Tôi cần truy cập vào SCCS ở Oakland nhưng bộ công cụ Dữ liệu đang trong thời kỳ bảo dưỡng, vậy nên tôi cần đăng nhập qua đường dây điện thoại.”

“Không thành vấn đề.”

Người đàn ông vừa nói chuyện cho tôi biết số dial-up và một chuỗi mật khẩu, sau đó vẫn giữ máy, hướng dẫn tôi thao tác qua từng bước.

Ồ, đây là một hệ thống có chế độ bảo mật “gọi lại” (dial-back), tức là bạn phải nhập số điện thoại và đợi máy tính gọi lại cho bạn. Giờ thì sao đây?

https://thuviensach.vn

“Anh này, hiện tôi đang có việc ra ngoài,” tôi tuôn ra những gì xuất hiện trong đầu lúc đó. “Vậy nên tôi không nhận cuộc gọi được.”

Thực may mắn đây là một lý do nghe có vẻ hợp lý. “Được thôi, tôi sẽ thiết lập bỏ qua bước gọi lại khi anh đăng nhập bằng tên đăng nhập của mình,” anh ta cam đoan, đồng thời hủy bỏ chế độ bảo mật phức tạp của công ty vốn yêu cầu tôi phải đưa ra được một số điện thoại ủy quyền để gọi lại.

Lenny cũng tham gia vào nỗ lực đột nhập SCCS. Mỗi lần tấn công giúp chúng tôi có được quyền truy cập vào 5-6 trạm chuyển mạch của văn phòng trung tâm với toàn quyền kiểm soát. Do vậy, chúng tôi có thể làm bất kỳ điều gì mà một kỹ thuật viên thuộc văn phòng trung tâm có thể làm khi ngồi trước máy. Chúng tôi có thể theo dấu đường dây, tạo số điện thoại mới, ngắt kết nối của bất kỳ số điện thoại nào, thêm hay bớt một vài tính năng cuộc gọi, cài đặt lưu số gọi đến và truy cập vào dữ liệu lưu lại này.

Lenny và tôi tốn rất nhiều thời gian cho việc này, từ cuối năm 1985 tới cuối năm 1986. Cuối cùng, chúng tôi đã đột nhập được vào toàn bộ trạm chuyển mạch của Pacific Bell, sau đó là Manhattan, Utah và Nevada cũng như nhiều nơi khác trên khắp cả nước. Trong số này có công ty điện thoại Chesapeake and Potomac (C&P) chuyên cung cấp dịch vụ cho khu vực Washington, D.C., bao gồm tất cả các phòng ban của chính quyền Liên bang đặt tại D.C. cũng như Lầu Năm góc.

NSA là một nơi hấp dẫn mà tôi khó có thể cưỡng lại. Dịch vụ điện thoại của NSA được cung cấp bởi một trạm chuyển mạch của công ty điện thoại ở Laurel, Maryland mà chúng tôi đã chiếm được quyền truy nhập. Số điện thoại công bố của NSA là 301 688-6311. Sau vài lần kiểm thử ngẫu nhiên các số khác nhau với dãy số đầu tương tự, tôi có linh cảm rằng toàn bộ số điện thoại có chung dãy số đầu này đều thuộc về NSA. Sau đó, tôi thiết lập một mạch có thể giúp tôi nghe được các cuộc gọi ngẫu nhiên nhờ sử dụng hàm kiểm tra mà các kỹ thuật viên chuyển mạch thường gọi là “Nói và Giám sát”. Tôi thử một đường dây và có tiếng một người đàn ông cùng một

https://thuviensach.vn

người phụ nữ đang trò chuyện với nhau. Khó có thể tin được tôi đang nghe một cuộc đàm thoại của NSA, thật là vừa phấn khích lại vừa lo lắng. Thật mỉa mai làm sao: Tôi đang nghe lén một cơ quan chuyên nghe lén lớn nhất thế giới.

Được rồi, tôi đã chứng tỏ khả năng của mình… giờ đã đến lúc biến thật nhanh. Tôi không lưu lại quá lâu để nghe xem họ nói gì, mà tôi cũng chẳng muốn biết. Nếu cuộc gọi có tính nhạy cảm, hẳn họ đã sử dụng đường dây bảo mật hơn và dù có vậy thì điều này cũng quá nguy hiểm. Khả năng bị tóm sẽ là rất nhỏ nếu như tôi chỉ thử đúng một lần và không bao giờ lặp lại.

Chính phủ chưa từng phát hiện ra tôi có thể đột nhập vào đường dây của họ. Và tôi cũng không định kể chuyện đó ở đây nếu như không phải thời hạn hiệu lực để truy cứu trách nhiệm đã qua từ rất lâu rồi.

Với Lenny và tôi, mỗi lần đột phá thành công vào một SCCS lại đem tới sự phấn khích vô cùng – hệt như việc lên cấp bậc trong trò chơi điện tử.

Đây là lần tấn công có ý nghĩa nhất trong sự nghiệp hacking của tôi bởi mức độ kiểm soát và quyền lực to lớn mà chúng tôi có được đối với hệ thống điện thoại trên hầu hết nước Mỹ. Và chúng tôi chưa từng lợi dụng điều đó. Với chúng tôi, sự phấn khích chỉ đơn giản nằm ở việc có được quyền lực mà thôi.

Pacific Bell cuối cùng đã phát hiện ra sự việc. Tuy nhiên, chúng tôi không bị bắt hay bị buộc tội bởi sau này tôi nghe nói, lãnh đạo công ty lo sợ khi tính tới hậu quả nghiêm trọng có thể xảy ra nếu hành vi của tôi được công bố và người khác có thể bắt đầu làm theo.

Trong khi đó, lần truy nhập vào Dockmaster của Lenny đã bị phát giác. NSA lần theo vụ tấn công Hughes trước đó, truy ra được phòng máy tính Lenny đã dùng vào đêm tôi ghé thăm. Trước tiên là bộ phận an ninh của Hughes truy vấn Lenny, sau đó, cậu ta bị triệu đến gặp FBI trong một cuộc điều tra chính thức. Lenny thuê một luật sư đi cùng mình tới buổi gặp này.

https://thuviensach.vn

Lenny nói với các đặc vụ FBI rằng cậu ấy và tôi chưa hề làm gì với Dockmaster. Bên quản lý của Hughes đã tra hỏi Lenny vài lần và cậu ta chưa từng khai ra tôi. Dù vậy rất lâu sau đó, để tự bảo vệ mình, cậu ta thừa nhận tôi đã tấn công vào Dockmaster vào đêm tôi ghé qua Hughes. Khi được hỏi tại sao lại che giấu sự can dự của tôi ngay từ đầu, Lenny nói hắn sợ vì bị tôi dọa giết nếu dám tiết lộ. Rõ ràng là hắn ta đã quá tuyệt vọng trong việc tìm cách nói dối các đặc vụ FBI.

Thông tin lưu lại đã chỉ rõ Kevin Mitnick đăng ký vào Hughes với tư cách khách mời của Lenny. Dĩ nhiên, hắn ta đã bị đuổi khỏi Hughes ngay lập tức.

Hai năm sau, tôi bị buộc tội nắm giữ mã số đăng nhập bí mật vào NSA. Trên thực tế, tôi chỉ có dữ liệu đầu ra của lệnh "whois" – cho thấy danh sách tên và số điện thoại của người dùng đăng ký bằng tài khoản trên Dockmaster – đó đều là những dữ liệu dễ có nếu ai đó truy nhập vào Arpanet.

Thuở đó, tại phòng máy của trường học không phải chỉ toàn nam sinh. Trong đám con gái học cùng có một cô gái dáng người nhỏ nhắn, dễ thương tên là Bonnie. Tôi không hẳn là tên nhóc cuốn hút nhất, tính đến đống mỡ dư trên người, hậu quả của những năm tháng lấy đồ ăn nhanh làm món chính khi còn ngồi xe buýt tới trường. Tôi thừa khoảng 25kg, "béo phì" có lẽ vẫn còn là một cách mô tả lịch sự.

Dù vậy, tôi vẫn nghĩ Bonnie thực sự dễ thương. Khi chúng tôi cùng ở phòng máy làm bài tập thực hành, tôi gửi tin nhắn cho nàng từ cuối phòng, đề nghị nàng đừng tắt những chương trình tôi đang chạy ở mức ưu tiên cao, và nàng trả lời khá thân thiện. Tôi mời nàng ăn tối. Nàng đáp: "Xin lỗi, mình đã đính hôn." Nhưng nhờ hacking, tôi học được rằng mình không thể bỏ cuộc dễ dàng, sẽ luôn có cách nào đó. Vài ngày sau, tôi lại mời nàng ăn tối, và nói rằng nàng có nụ cười thật đẹp. Bạn biết không, lần này nàng đồng ý.

Sau đó, nàng kể với tôi rằng nàng nghĩ vị hôn phu của mình đang nói dối về tình hình tài chính của anh ta – việc anh ta sở hữu xe gì và còn nợ bao nhiêu.

https://thuviensach.vn

Tôi nói với nàng: “Mình có thể tìm hiểu nếu cậu muốn.” Nàng nói, “Giúp mình nhé, được không?”

Hồi còn học cấp ba, tôi đã từng may mắn tấn công vào TRW, một công ty báo cáo tín dụng. Cũng không có gì trí tuệ cho lắm. Một đêm, tôi mò tới phía sau đại lý xe Galpin Ford ở Thung lũng San Fernando và lục tìm trong đống rác. Chỉ mất khoảng 15 phút nhưng cuộc thám hiểm nho nhỏ của tôi khá ra trò. Tôi tìm được cả đống báo cáo tín dụng của những người mua xe từ môi giới. Điều khó tin nhất là trong mỗi tờ giấy in ra đều có mã đăng nhập của Galpin vào TRW. (Đáng kinh ngạc hơn nữa là nhiều năm sau đó, họ vẫn liên tục in mã đăng nhập lên các bản báo cáo của mình.)

Thời đó, TRW rất tận tâm đối với khách hàng. Nếu bạn gọi điện tới và đọc tên người bán cũng như mã đăng nhập chính xác, đồng thời giải thích rằng bạn không hiểu rõ lắm về quy trình làm việc, một người phụ nữ tốt bụng sẽ hướng dẫn bạn từng bước một để có được bản báo cáo tín dụng của ai đó. Việc này rất hữu ích đối với khách hàng và cũng rất hữu ích đối với một hacker như tôi.

Do đó, khi Bonnie nói nàng muốn nhờ tôi kiểm tra tình hình tài chính của bạn trai, tôi đã có đủ các mánh khóe mình cần. Một cuộc gọi tới TRW cùng vài giờ thao tác trên máy tính đã giúp tôi có được bản báo cáo tín dụng của hắn ta cũng như tài khoản ngân hàng và danh mục tài sản sở hữu. Sự nghi ngờ được chứng thực: Hắn ta còn khuya mới đạt tới mức độ dư dả như vẫn tỏ vẻ, một số tài sản của hắn cũng đã bị đóng băng. Bản báo cáo của DMV cho thấy hắn vẫn sở hữu chiếc xe mà hắn nói với Bonnie mình đã bán. Tôi cảm thấy hơi tệ – tôi không định phá hỏng mối quan hệ của nàng. Nhưng sau đó, nàng đã chia tay vị hôn phu.

Mất khoảng 2-3 tuần để nàng vượt qua được sự đổ vỡ và chúng tôi bắt đầu hẹn hò. Dù lớn hơn tôi tới 6 tuổi và từng trải hơn tôi rất nhiều trong chuyện này, nàng vẫn nghĩ rằng tôi thực thông minh và bảnh trai, cho dù có hơi thừa

https://thuviensach.vn

cân. Đây là mối quan hệ nghiêm túc đầu tiên trong đời; tôi thấy mình như đang ở trên mây.

Bonnie và tôi đều thích ăn đồ Thái và đi xem phim. Nàng còn dụ được tôi leo núi, một thú vui vốn khác xa với những gì tôi vẫn muốn làm và chỉ cho tôi những con đường mòn xinh đẹp quanh ngọn núi San Gabriel. Nàng rất ấn tượng với khả năng trích nhặt thông tin từ mọi người của tôi. Còn có một sự tình cờ khiến tôi cười ngất: Bạn gái mới của tôi được nhận lương và học bổng từ một trong những đối tượng hacking chủ yếu của đời tôi, công ty điện thoại GTE.

Sau khi hoàn thành khóa học chứng chỉ kéo dài nửa năm tại phòng máy của trường, tôi quyết định ở lại thêm một thời gian. Adriel, quản trị viên (admin) hệ thống VM/CMS của trường, đã cố tóm được tôi khi tôi thử giành quyền quản trị hệ thống. Cuối cùng, anh ấy đã bắt quả tang tôi nhờ náu mình sau tấm rèm phòng thiết bị đầu cuối, trong lúc tôi đang nhòm ngó bên trong thư mục của anh. Tuy vậy, thay vì tống tôi ra khỏi chương trình, anh rất ấn tượng với những kỹ năng cho phép tôi hack vào máy tính của trường. Do đó, anh đề nghị nếu tôi có thể viết một chương trình giúp các máy tính cỡ trung của IBM có độ bảo mật tốt hơn, anh sẽ coi đó như một “dự án danh dự”. Nhà trường đang trang bị cho các sinh viên kiến thức vượt chuẩn về máy tính, nhưng lại nhờ một sinh viên giúp cải thiện khả năng bảo mật của trường. Đây là nhiệm vụ lớn đầu tiên của tôi. Tôi coi nó như một lời khen và chấp nhận yêu cầu. Sau khi hoàn thành dự án, tôi được tốt nghiệp với tầm bằng danh dự.

Về sau, Ariel và tôi trở thành bạn bè.

Trung tâm Giảng dạy Máy tính có một sức hấp dẫn lớn đối với sinh viên theo học chương trình của họ: Một số công ty lớn sẽ tuyển dụng các sinh viên tốt nghiệp tại đây. Một trong số này có GTE, công ty của Bonnie, mục tiêu hacking của tôi trong nhiều năm. Thật tuyệt làm sao!

https://thuviensach.vn

Sau buổi phỏng vấn với phòng IT của GTE, tôi lọt vào vòng trong với ba người khác từ phòng Nhân sự và được nhận vào vị trí lập trình viên. Giấc mơ đã trở thành hiện thực. Không còn phải hacking nữa – tôi không cần tới nó. Tôi sẽ được trả lương để làm việc mà tôi yêu thích, tại nơi mà tôi hằng mong muốn.

Công việc bắt đầu bằng buổi hướng dẫn nhân viên về tên và chức năng của các hệ thống máy tính trong GTE. Ố ồ! Đây là một công ty điện thoại: Tôi có thể đảm nhiệm vai trò giáo viên ở đây ấy chứ. Nhưng dĩ nhiên, tôi chỉ ngồi ở đó, ghi ghi chép chép hệt như mọi người.

Công việc mới tuyệt vời, những cuộc hẹn chớp nhoáng với bạn gái vào bữa trưa, khoản thu nhập chính thức – tôi đã có tất cả. Bước qua các văn phòng làm việc, tôi mỉm cười trước hàng trăm tên đăng nhập và mật khẩu viết trên các mẩu giấy nhớ dán ngay trước mắt. Tôi hệt như một gã cai nghiện trong chuyến thăm nhà máy cất rượu Jack Daniel, tự tin nhưng cũng đầy choáng váng bởi câu hỏi “Sẽ ra sao nếu..?” vang lên trong đầu.

Bonnie và tôi thường ăn trưa với một người bạn của nàng, một gã làm ở Phòng An ninh. Tôi luôn cẩn thận quay mặt thẻ ID của mình ra sau. Gã hiển nhiên cũng không để ý tên đầy đủ của tôi khi mới giới thiệu, vậy tội gì tôi phải để gã đọc được nó trên thẻ ID, như vậy thì khác gì tấm bảng nhấp nháy dòng chữ “Kẻ thù công khai số một của công ty điện thoại”?

Nhìn chung, đây chính là một trong những khoảng thời gian tuyệt vời nhất trong đời tôi – ai cần tới hacking cơ chứ?

Nhưng chỉ sau một tuần, vị sếp mới ném cho tôi một tin khủng bố. Ông ta đưa cho tôi tờ giấy đăng ký bảo mật để đăng ký lấy thẻ đăng nhập toàn quyền, đồng nghĩa với quyền ra vào trung tâm dữ liệu 24/7, vì tôi sẽ phải trực trong trường hợp khẩn cấp. Ngay lập tức, tôi biết mình sẽ bị tống cổ. Ngay khi nhân viên Phòng An ninh GTE nhìn vào giấy đăng ký của tôi, họ

https://thuviensach.vn

sẽ nhận ra tên tôi và tự hỏi làm thế quái nào tôi có thể vượt qua mọi quy trình kiểm tra lý lịch để được nhận vào làm ở vị trí lập trình viên.

Vài ngày sau, tôi đi làm trong cảm giác thấp thỏm lo âu. Sáng hôm đó, cấp trên cho gọi tôi đến và sếp của ông ta, Russ Trombley, đưa tôi tiền lương đã làm và khoản bồi thường nghỉ việc. Họ nói họ phải để tôi đi vì kết quả kiểm chứng với những người giới thiệu trong hồ sơ không tốt lắm. Rõ ràng là lấy cớ. Tôi vốn chỉ đưa ra tên những người sẽ nói tốt về tôi.

Tôi được đưa về chỗ ngồi để thu thập đồ dùng cá nhân. Trong vòng vài phút, một đội bảo vệ từ Phòng An ninh kéo đến, bao gồm cả người đã từng ăn trưa với tôi và Bonnie. Vài người trong số họ bắt đầu lục soát hộp đựng đĩa mềm của tôi xem có tài sản công ty không. Bất kể là gì. Không có gì ngoài vài phần mềm hợp pháp. Cả đội an ninh áp giải tôi ra cửa, tới tận xe ô tô. Liếc qua gương chiếu hậu khi lái xe xa dần, tôi thấy tất cả đều vẫy tay tạm biệt mình.

Sự nghiệp của tôi tại GTE kéo dài tổng cộng chín ngày.

Sau này, tôi biết rằng mấy người trong Phòng An ninh Pacific Bell đã chế giễu đồng nghiệp của họ tại GTE một trận lớn, thật nực cười khi một công ty nào đó có thể ngu ngốc tới mức nhận một phreaker tai tiếng như Kevin Mitnick vào làm việc – người mà Pacific Bell đã lưu trữ hồ sơ trong nhiều năm trời.

Một bước lùi, một bước tiến. Một thầy giáo ở Trung tâm Giảng dạy Máy tính, đồng thời là chuyên viên bảo mật thông tin tại Ngân hàng Security Pacific National đã gợi ý tôi có thể thử xin việc ở đó xem sao. Tôi tham dự ba cuộc phỏng vấn trong suốt vài tuần, buổi phỏng vấn cuối cùng là với Phó Chủ tịch ngân hàng. Sau đó là thời gian dài chờ đợi. Cuối cùng, tôi cũng nhận được cuộc gọi: “Một trong những ứng viên khác có cả bằng đại học, nhưng chúng tôi quyết định anh mới là người chúng tôi muốn.” Mức lương của tôi là 34.000 đô-la, với tôi đây là một khoản tuyệt vời.

https://thuviensach.vn

Họ gửi một thông báo nội bộ tới tất cả nhân viên: “Chào mừng nhân viên mới Kevin Mitnick, anh ấy sẽ bắt đầu làm việc từ tuần sau.”

Hẳn các bạn còn nhớ tờ Los Angeles Times từng đăng một bài báo viết về lần tôi bị bắt thời niên thiếu và ghi đầy đủ cả họ tên tôi, một sự vi phạm pháp luật và xâm phạm quyền riêng tư cá nhân vì lúc đó tôi vẫn chỉ là trẻ vị thành niên. Tệ thay, một trong số nhân viên ở Ngân hàng Security Pacific National vẫn còn nhớ bài báo đó.

Một ngày trước khi vào làm, tôi nhận được một cuộc gọi kỳ lạ của Sandra Lambert, người đã nhận tôi vào làm và cũng là người sáng lập ra tổ chức an ninh có tên Hiệp hội An ninh Hệ thống Thông tin (ISSA). Buổi nói chuyện gần như một cuộc thẩm vấn:

SL: “Anh có chơi Hearts không?”

Tôi: “Trò chơi bài ấy hả?”

SL: “Đúng.”

Lòng tôi trĩu nặng, bữa tiệc có lẽ đã kết thúc.

SL: “Anh là người dùng ham radio với dấu hiệu gọi WA6VPS?”

Tôi: “Vâng.”

SL: “Anh có lục thùng rác sau mấy tòa văn phòng không?”

Tôi: Ậm ừ. “Chỉ khi nào tôi đói thôi.”

Nỗ lực tỏ ra hài hước của tôi thất bại. Lambert nói tạm biệt và kết thúc cuộc gọi. Tôi nhận được cú điện thoại từ Phòng Nhân sự ngay ngày hôm sau để hủy bỏ việc nhận tôi vào làm. Một lần nữa, quá khứ đã ngáng chân tôi thật đau đớn.

https://thuviensach.vn

Một thời gian sau, các cơ quan ngôn luận nhận được báo cáo từ Ngân hàng Security Pacific National thông báo họ đã tổn thất 400 triệu đô-la trong vòng một quý. Báo cáo đó chỉ là một trò chơi khăm, không hoàn toàn do ngân hàng gửi bởi họ không hề mất xu nào trong quý đó. Dĩ nhiên, nhóm lãnh đạo nghĩ ngay rằng tôi là người đứng sau trò này. Tôi không hề biết gì tới tận vài tháng sau đó trong buổi điều trần tại tòa, khi bên khởi tố tố cáo với tòa rằng chính tôi đã thực hiện hành vi phá hoại này. Tôi chỉ nhớ mình có nói với Lewis De Payne về việc hủy lời mời làm việc. Nhiều năm sau, tôi hỏi liệu có phải cậu ta đã đứng sau vụ công bố giả mạo đó không. Nhưng cậu ta phản đối kịch liệt. Sự thực là, tôi không hề làm chuyện này. Đây không phải là phong cách của tôi: Tôi chưa từng có bất kỳ ý định trả thù xấu xa nào.

Cho tới giờ, bản báo cáo giả mạo đó vẫn là một trong những truyền thuyết về Kevin Mitnick.

Mặc cho mọi chuyện, tôi vẫn còn Bonnie, một trong những điều tuyệt vời nhất trong đời tôi. Nhưng bạn đã bao giờ cảm thấy khi một điều gì đó quá tốt đẹp, nó khó có thể tồn tại bền lâu chưa?

https://thuviensach.vn

07
KẾT HÔN VỘI VÃ

Kvoh wg hvs boas ct hvs Doqwtwq Pszz sadzcmss kvc fsor hvs wbhsfboz asac opcih am voqywbu oqhwjwhwsg cjsf hvs voa forwc?

Gần đây, Bonnie nói rằng nàng vẫn còn nhớ "Kevin đã từng là người thú vị như thế nào, anh ấy ngọt ngào ra sao."

Tôi cũng cảm thấy điều tương tự về nàng. Tôi từng có cảm tình với các cô gái khác, nhưng Bonnie là người đầu tiên khiến tôi cảm thấy thực sự nghiêm túc và quan tâm nhiều đến thế. Chúng tôi đã cùng tận hưởng rất nhiều điều, thậm chí cả những điều nhỏ nhặt như cốc bơ lạc Reese's mà chúng tôi phải lái ra khỏi tuyến đường chính để mua ở 7-Eleven trên đường về. Chắc bạn cũng biết cảm giác thỏa mãn khi thấy thoải mái và hạnh phúc bên một người đặc biệt. Không nghi ngờ gì nữa, việc có nàng ở bên sau hai lần mất việc chớp nhoáng chính là những gì bác sĩ yêu cầu. Tôi dành rất nhiều thời gian ở chỗ nàng tới mức bắt đầu chuyển một ít quần áo của mình đến đó. Chúng tôi chưa bao giờ thực sự quyết định, mình hãy sống cùng nhau đi. Mọi thứ cứ thế diễn ra.

Chúng tôi thích đạp xe cùng nhau. Chúng tôi thích đi bộ ở Chantry Flat, Arcadia, khu vực xinh đẹp với thác nước ngay trong Quận Los Angeles nhưng cảm giác như ở trong rừng – rất hay, đó thực sự là một cuộc lẩn trốn tươi mát đối với một gã lúc nào cũng nhợt nhạt vì ngồi trước máy tính cả ngày lẫn đêm như tôi.

Tôi thậm chí không bận tâm chuyện nàng rất lười chăm sóc nhà cửa, với một đống quần áo bẩn thường chiếm dụng không gian trên sàn phòng ngủ. Tôi chưa bao giờ là một người gọn gàng quá mức như cha mẹ tôi, nhưng tôi

https://thuviensach.vn

thích mọi thứ sạch sẽ và ngăn nắp. Hai đứa tôi hợp nhau trong quá nhiều việc khác nên khi nghĩ về tình hình căn hộ, tôi chỉ lờ nó đi.

* * *

Vì thất nghiệp, nên tôi đăng ký một khóa học mở rộng ở UCLA tại Westwood, không xa chỗ chúng tôi. Bonnie cùng tôi đến đăng ký.

Nhưng đó chỉ là một sự dối trá – lần đầu tiên tôi lừa dối nàng. Tôi ra ngoài ba tối mỗi tuần với lý do đến lớp, nhưng thay vào đó, tôi lại lái xe đến chỗ làm của Lenny DiCicco và hack với cậu ta cho đến gần sáng. Đó quả là một hành vi tệ hại.

Vào những tối không ra ngoài, tôi ngồi trước máy tính của mình trong căn hộ, sử dụng đường điện thoại của Bonnie để hack trong lúc nàng một mình đọc sách, một mình xem tivi, rồi một mình đi ngủ. Tôi cho rằng đó là cách mình đối mặt với nỗi thất vọng của hai công việc suýt-có-nhưng-đã-vuột-mất, nhưng đó cũng chỉ là lời biện hộ. Tất nhiên, tôi cũng gặp vấn đề khi phải đối mặt với nỗi thất vọng khủng khiếp đó. Nhưng đó không phải là lý do. Lý do thực sự đơn giản chỉ là tôi đã trở thành nô lệ của nỗi ám ảnh quyền lực.

Dù chuyện đó hẳn khiến nàng cảm thấy rất khó chịu, nhưng bằng cách nào đó, nàng đã chấp nhận nó như cách tôi đã chấp nhận chuyện thu xếp nhà cửa chưa-đến-mức-đáng-khen của nàng. Sau vài tháng sống chung, chúng tôi nhận ra cả hai đều rất nghiêm túc với mối quan hệ này. Chúng tôi yêu nhau, chúng tôi bắt đầu bàn về việc kết hôn và chúng tôi bắt đầu để dành tiền. Cứ dư dả được đồng nào (tôi được Fromin’s Delicatessen thuê để nâng cấp thiết bị của họ sang hệ thống máy thanh toán), tôi lại tích thành từng tờ 100 đô-la rồi nhét chúng vào ngực áo khoác trong tủ quần áo của chúng tôi.

Lúc đó tôi 23 tuổi, sống trong căn hộ của bạn gái và dành hầu hết thời gian bên máy tính trừ lúc ngủ. Tôi là David trên PC, chuyên tấn công những

https://thuviensach.vn

mạng lưới Goliath khổng lồ[38] của các công ty điện thoại lớn trên khắp nước Mỹ.

[38] David và Goliath là câu chuyện cổ trong Kinh thánh về cuộc chiến không cân sức nhưng có kết quả ngoài dự đoán giữa nhân vật David nhỏ bé yếu ớt và người khổng lồ hùng mạnh Goliath. Hiện nay, người ta hay dùng hình ảnh David và Goliath để hàm chỉ tình huống tương tự khi hai bên đối đầu (một người hay tổ chức nào đó) có thực lực chênh lệch hoàn toàn nhưng phần thắng lại thuộc về kẻ yếu thế. (ND)

Hệ thống điều khiển của công ty điện thoại sử dụng một phiên bản biến thể của Unix, và tôi muốn học thêm về nó. Một công ty ở Bắc California có tên Santa Cruz Operations (SCO), đang phát triển một hệ điều hành dựa trên Unix gọi là Xenix dành cho máy tính cá nhân (PC). Nếu tôi có thể tiếp cận được bản sao của mã nguồn, tôi sẽ có cơ hội tìm hiểu cách thức hoạt động bên trong hệ điều hành trên máy tính của mình. Thông qua Pacific Bell, tôi đã lấy được số dial-up bí mật của SCO dành cho mạng máy tính của họ và lừa được một nhân viên tiết lộ tài khoản đăng nhập của cô ta, đổi mật khẩu của cô ta thành mật khẩu mới của tôi và chiếm quyền truy cập.

Một hôm, trong khi đang chìm đắm trong các chi tiết của hệ thống SCO nhằm tìm ra nơi đặt mã nguồn mà tôi muốn nghiên cứu, tôi phát hiện ra một quản trị viên hệ thống đang theo dõi mọi đường đi nước bước của mình. Tôi gửi cho anh ta một tin nhắn: “Sao anh lại theo dõi tôi?”

Tôi ngạc nhiên khi thấy anh ta trả lời: “Đó là việc của tôi.”

Để xem anh ta cho phép tôi đi xa tới đâu, tôi viết lại rằng tôi muốn có một tài khoản của riêng mình trên hệ thống. Anh ta đã tạo một tài khoản cho tôi, thậm chí còn cho tôi tên đăng nhập mà tôi yêu cầu: “hacker”. Biết rằng anh ta sẽ theo dõi tài khoản này, tôi chỉ đánh lạc hướng anh ta bằng cách nghịch ngợm linh tinh không cụ thể. Tôi đã tìm được mã nguồn mong muốn, nhưng

https://thuviensach.vn

cuối cùng, tôi không bao giờ thử tải nó về bởi nó sẽ chẳng bao giờ tải xong trên modem 2400 baud của tôi.

Nhưng đây chưa phải là kết thúc của câu chuyện.

Vào một ngày đầu tháng Sáu, Bonnie trở về nhà từ chỗ làm và thấy mọi thứ bị xáo trộn: Chúng tôi bị trộm. Nàng nhắn tin cho tôi. Tôi gọi lại, có thể nghe được nỗi sợ hãi và lo lắng qua giọng nói của nàng.

Tôi nhờ nàng kiểm tra số tiền tôi đã tiết kiệm cho đám cưới ở trong túi áo khoác. Nhưng rồi nàng để ý thấy xấp tờ 100 đô-la của tôi – tổng cộng khoảng 3.000 đô-la – đã được xếp ngay ngắn trên bàn bếp... cùng một lệnh khám nhà.

Chúng tôi không bị trộm mà bị khám xét. Bởi Phòng cảnh sát Santa Cruz. Santa Cruz! Tôi biết việc này có liên quan đến những cuộc hacking buổi đêm vào máy tính ở Santa Cruz Operations.

Khi Bonnie nói máy tính và đĩa của tôi đã biến mất, thế giới dưới chân tôi đột nhiên đổ sụp. Tôi bảo nàng nhanh chóng gói ghém quần áo và gặp tôi. Tôi biết rất nhiều rắc rối sắp ập đến. Tôi cần kiếm một gã luật sư để kiểm soát hậu quả. Ngay lập tức!

Bonnie gặp tôi ở một công viên trong vùng, và mẹ tôi cũng đến. Tôi nói với hai người họ rằng không có gì phải lo lắng, bởi tôi chỉ nhòm ngó loanh quanh – tôi chưa hề phá hoại bất cứ tập tin nào của SCO hay thậm chí tải mã nguồn của họ về. Tôi lo đối đầu với pháp luật thì ít mà lo về những nỗi đau tôi đem đến cho hai người và bà tôi thì nhiều, họ là những người quan trọng nhất trong cuộc đời tôi.

Mẹ lái xe về, tôi đưa Bonnie đến một nhà nghỉ gần đó. Nàng rất buồn và cảm thấy bị xúc phạm. Nếu nàng rời bỏ tôi ngay lúc đó, tôi cũng đáng bị như thế. Nhưng ngược lại, không chút đắn đo, nàng đã thể hiện sự chung

https://thuviensach.vn

thủy của mình. Thái độ của nàng không phải là “Anh đã làm gì với em vậy?” mà là “Giờ chúng ta làm gì đây?”

Sáng hôm sau, nàng gọi đến chỗ làm và xin nghỉ phép vì việc gia đình. Sếp của nàng nói một vài sĩ quan cảnh sát đã đến và muốn phỏng vấn. Suy nghĩ đầu tiên của tôi là: Tôi đã hack từ căn hộ của Bonnie qua đường dây điện thoại của nàng, họ cho rằng nàng là thủ phạm. Nhưng rồi tôi kết luận rằng chiến thuật của họ có lẽ là bắt giữ bạn gái tôi để thương lượng: “Hãy thú nhận mọi thứ hoặc bạn gái anh sẽ đi tù.”

Tôi dành vài ngày sau đó gọi cho các luật sư, giải thích tình hình, lập ra kế hoạch. Theo như Bonnie nhớ lại: “Chúng tôi đã cùng khóc rất nhiều nhưng vẫn dính lấy nhau.”

Tại sao nàng lại không bỏ đi? “Tôi đã phát điên vì Kevin,” giờ nàng nói.

Chúng tôi bớt được chút băn khoăn và lo lắng bằng cách dành rất nhiều thời gian yêu đương. Tôi cảm thấy rất hối hận khi đặt Bonnie vào tình cảnh này, trong khi tôi đã gây ra quá nhiều lo lắng cho mẹ và bà. Tôi đoán Bonnie và tôi đều muốn tìm bình yên theo cách đó.

Dì Chickie lái xe đưa Bonnie và tôi xuống trạm West Hollywood của Phòng Cảnh sát Trưởng Quận Los Angeles. Chúng tôi ra đầu thú và dì Chickie ngay lập tức trả tiền bảo lãnh 5.000 đô-la cho mỗi đứa. Bằng cách nào đó, cảnh sát đã bỏ qua việc lăn tay và chụp ảnh chúng tôi. Chính bởi sai sót nghiêm trọng về thủ tục này mà không hề có hồ sơ nào được lập cho chúng tôi. Cho đến tận hôm nay, không hề có một ghi chép chính thức nào về việc tôi từng bị bắt giam vì vụ SCO.

Suốt vài tháng sau, mỗi lần phải trình diện trước tòa án Santa Cruz, tôi phải mua bốn vé máy bay khứ hồi – Bonnie thuê một luật sư khác – thêm vào đó là tiền khách sạn, tiền thuê xe và ăn uống. Cả hai luật sư đều yêu cầu trả tiền trước. Số tiền đó quá lớn so với những gì tôi đã tiết kiệm được cho đám

https://thuviensach.vn

cưới. Toàn bộ 3.000 đô-la đã ra đi để trả trước cho luật sư của tôi. Mẹ và bà cho tôi vay tiền để trả cho luật sư của Bonnie và những chi phí khác.

Và thế là chúng tôi không còn tiền cho một đám cưới tử tế, nhưng mọi chuyện còn tệ hơn thế. Không có cách tình tứ, lãng mạn nào để kể lại việc này: Tôi nói với Bonnie rằng chúng tôi cần kết hôn để nàng không bị buộc phải đứng ra làm chứng chống lại tôi, và cũng để nàng có thể đến thăm tôi nếu tôi phải vào tù, việc có vẻ như cuối cùng cũng sẽ tới.

Tôi tặng Bonnie một chiếc nhẫn đính hôn bằng kim cương và chúng tôi kết hôn tại nhà của chính người làm chứng ở Woodland Hills. Bà ngoại đã ở đó, cùng với mẹ tôi và bạn trai lúc đó của mẹ, một doanh nhân khởi nghiệp bán đồ ăn tên là Arnie Fromin. Không có người thân nào bên nhà Bonnie đến dự; có thể hiểu mẹ nàng đã tức giận với tình cảnh tôi đặt ra cho con gái bà như thế nào.

Đó không phải là một câu chuyện lãng mạn mà nhiều thiếu nữ vẫn ao ước khi còn trẻ. Bonnie mặc quần dài, áo phông, chân đi dép tông. Nàng thậm chí chẳng buồn chỉnh trang bản thân. Sau đó, chúng tôi về căn hộ của mình, bà tôi đem theo một đĩa thức ăn.

Tình hình pháp lý chuyển từ tệ sang tồi tệ. Ngoài án hình sự, SCO còn đâm đơn kiện tôi 1,4 triệu đô-la vì những phá hoại. Và một đơn tương tự cho Bonnie.

Rồi bỗng nhiên có chút hy vọng. Hóa ra đơn kiện đó chỉ là đòn bẩy: Bên công tố nói rằng người của SCO sẽ bỏ đơn kiện dân sự nếu tôi nói cho họ biết tôi đã hack như thế nào. Họ chưa bao giờ tìm ra được cách.

Tất nhiên là tôi đồng ý. Tôi ngồi cùng một tay quản trị viên hệ thống tên là Stephen Marr, hắn hành động như thể chúng tôi sẽ nói chuyện như những người bạn tốt. Còn tôi thì hành xử như bị hỏi cung: Hắn hỏi, tôi trả lời. Nhưng không có gì nhiều để nói. Không có bí mật hacking công nghệ cao

https://thuviensach.vn

nào. Tôi bảo hắn, tôi chỉ đơn giản gọi một thư ký và đò đưa cô ta nôn ra tên đăng nhập và đổi mật khẩu thành cái tôi đưa – không có gì phức tạp.

Dù mẹ của Bonnie không đến đám cưới, nhưng bà vẫn tổ chức cho chúng tôi một bữa tiệc sau lễ cưới ở nhà tại San Dimas. Lần này, Bonnie mặc một bộ váy cưới và tôi thuê một bộ âu phục. Cha và em trai tôi, Adam, đã ở đó và tất nhiên là cả mẹ và bà tôi, cùng anh chị em của Bonnie, thậm chí cả bạn trai cũ của Bonnie. Hôm đó là một ngày hạnh phúc hơn rất nhiều so với đám cưới thật với đầy đủ cả bánh cưới và thợ chụp ảnh.

Án hình sự cho vụ đột nhập SCO hóa ra nhẹ hơn rất nhiều so với những gì tôi nghĩ. Họ cũng hủy án của Bonnie, và luật sư của tôi, Michael Barton, quen với bên công tố nên đã đem về cho tôi một thỏa hiệp hợp lý. Nếu là bất kỳ ai khác – với lần phạm tội đầu tiên trên phương diện pháp lý, bởi hồ sơ vị thành niên của tôi đã bị niêm phong – vụ này sẽ bị khép vào tội nhẹ. Nhưng vì tôi là Kevin Mitnick danh tiếng lẫy lừng, nên phía công tố lúc đầu khăng khăng muốn kết trọng tội – dù theo luật, việc đột nhập mạng SCO của tôi chỉ gắn với tội nhẹ. Tôi đồng ý nhận tội đột nhập để dàn xếp vụ việc và để hủy án nhắm vào Bonnie. Tôi sẽ không phải ngồi tù mà chỉ phải trả một khoản phí khiêm tốn 216 đô-la và bị "giam lỏng" trong 36 tháng – có nghĩa là tôi không cần phải báo cáo cho nhân viên Quản chế. Điều kiện duy nhất mà hiển nhiên tôi phải hứa là "không tái phạm thêm lần nào nữa".

Vài ngày sau, tôi lái xe đến Santa Cruz để lấy lại đồ đạc đang bị giữ. Cảnh sát đưa cho tôi chiếc máy tính đầu cuối nhưng không có đĩa, việc này khiến tôi lo lắng vì những chiếc đĩa đen đó có chứa bằng chứng về những vụ hack vào Pacific Bell cùng với một số nơi thú vị khác. Họ cũng không trả lại một chiếc hộp khác dù họ hắn cũng chưa xem xét kỹ hay quan tâm đến: Nó có chứa cần sa và điếu hút của Bonnie. Nhưng dù sao thì đây cũng là Santa Cruz, với một sở cảnh sát địa phương nhỏ.

Câu chuyện Santa Cruz để lại một dư chấn. Đúng như tôi đã lo sợ, các thanh tra ở Santa Cruz hắn đã tìm cách xem xét đống đĩa vi tính đó và thông báo

https://thuviensach.vn

cho Pacific Bell về những gì tôi đã làm với hệ thống của họ. Phòng An ninh Pacific Bell đã bị báo động đủ để lập một bản ghi nhớ nội bộ gửi tới tất cả các cấp quản lý. Tôi biết về việc này theo cách vô cùng lạ lùng: Một nhân viên của Pacific Bell tên là Bill Cook, cũng là một gã chơi ham radio hay dùng tần số tiếp sóng tai tiếng 147,435 MH ở Los Angeles, đã đọc bản ghi nhớ này trên sóng chỉ để kích động tôi.

Tất nhiên, tôi phải tận mắt nhìn thấy bản ghi nhớ này. Nhưng làm thế nào tôi có thể lấy được nó?

Tôi liên hệ với Lewis De Payne trong giờ làm việc và nhờ cậu ta tạm thời lập trình lại máy fax để các cuộc gọi đến sẽ được trả lời tự động rằng chúng thuộc về Phòng An ninh Pacific Bell.

Sau đó, tôi quay số đến bộ chuyển mạch của công ty điện thoại xử lý dịch vụ cho Phòng An ninh Pacific Bell, và lập trình lại đường điện thoại cho máy fax sao cho nó sẽ chuyển tiếp cuộc gọi đến số máy fax ở chỗ làm của Lewis. Thế là xong phần chuẩn bị.

Sau đó, tôi gọi cho văn phòng Phó Giám đốc Pacific Bell, Frank Spiller.

Thư ký của gã nhận điện. Tôi nói tôi gọi từ Phòng An ninh của Pacific Bell và nói tên của một trong những điều tra viên có thật – hình như tôi đã nói tôi là Steve Dougherty.

Tôi hỏi: “Frank đã nhận được bản ghi nhớ về vụ của Kevin Mitnick chưa?”

“Đó là ai thế?” cô ta hỏi.

“Hacker đã đột nhập vào máy tính của công ty chúng ta.”

“Ồ, phải rồi. Tôi có nó rồi đây.”

Tôi nói: “Tôi nghĩ tôi đã gửi một bản cũ và từ đó đến nay đã có sửa đổi. Cô có thể fax bản cô có cho tôi không?” Tôi đưa cô ta số fax nội bộ của Phòng

https://thuviensach.vn

An ninh Pacific Bell ở Bắc California.

“Tất nhiên,” cô ta nói. “Tôi làm ngay đây.” Ngay khi Lewis nhận được bản fax, cậu ta fax lại cho tôi, sau đó tôi và cậu ta cùng làm ngược lại các bước chuẩn bị.

Đây là danh sách những thứ mà bản ghi nhớ ghi lại những thứ tìm thấy trong đĩa mềm của tôi:

- Mitnick đã kiểm soát tất cả máy tính SCC/ESAC ở Nam California. Trong tập tin là tên, tên đăng nhập, mật khẩu và số điện thoại nhà riêng của các nhân viên ESAC ở phía Bắc và phía Nam.
- Số dial-up và tài liệu định mạch cho các máy tính SCC và bộ dữ liệu.
- Các lệnh kiểm thử và chiếm đoạt các đường dây và kênh kiểm thử.
- Các lệnh và thông tin đăng nhập tại các trung tâm đấu dây COSMOS ở Bắc và Nam California.
- Các lệnh để giám sát đường dây và chiếm âm hiệu quay số.
- Các dấu hiệu cho thấy hành vi giả mạo đặc vụ an ninh của Nam California và nhân viên của ESAC để lấy thông tin.
- Các lệnh để đặt bẫy ngắt và khởi tạo.
- Địa chỉ của các văn phòng của Pacific Bell cùng mã cửa ra vào tại các văn phòng trung tâm phía Nam California ELSG12, LSAN06, LSAN12, LSAN15, LSAN56, AVLN11, HLWD01, HWTH01, IGWD01, LOMT11 và SNPD01.
- E-mail nội bộ của công ty chứa thông tin chi tiết về thủ tục đăng nhập/mật khẩu mới cũng như các lớp bảo mật.
- Bản ghi của một tập tin hacker về bộ giải mã hóa UNIX. Nếu thành công, chương trình này có thể đột nhập vào bất kỳ hệ thống UNIX nào.

Tôi tưởng tượng ra cảnh nhiều người trong công ty ắt phải rất tức tối khi biết tôi đã thâm nhập sâu vào hệ thống của họ, vượt qua tất cả các lớp bảo mật an

https://thuviensach.vn

ninh phức tạp của họ đến mức nào. Dựa theo những gì tìm thấy trong đống đĩa, tôi thấy kỳ lạ khi FBI vẫn chưa gõ cửa nhà tôi.

Vài tháng sau, vào mùa thu năm 1988, tôi trở lại làm việc với Don David Wilson ở Franmark. Bonnie vẫn làm ở GTE, dù nàng chắc chắn Phòng An ninh của công ty đã cố tìm bằng chứng cho thấy việc nàng hack vào máy tính của công ty. Chúng tôi lại tiết kiệm tiền, cố gắng gom đủ để đặt cọc mua nhà. Có một vài căn nhà xinh đẹp phù hợp với chúng tôi, nhưng lại quá xa thành phố khiến việc đi lại trở nên ngán ngẩm và bào mòn trí lực cũng như sự kiên nhẫn của chúng tôi.

Để giúp chúng tôi đạt được mục tiêu mua nhà, mẹ cho vợ chồng tôi ở lại một phòng ngủ trống trong nhà để tiết kiệm tiền thuê. Dù cả tôi và Bonnie đều không thích ý tưởng đó, nhưng chúng tôi vẫn quyết định thử xem.

Việc sống chung với mẹ tôi hóa ra lại là một ý tưởng tồi tệ. Dù bà rất nhiệt tình giúp đỡ, nhưng chúng tôi gần như không có chút riêng tư nào. Về sau, trong một tờ giấy nhớ nàng để lại ở nhà mẹ, Bonnie phàn nàn rằng nàng thấy "miễn cưỡng và có chút cay đắng... về chuyện đó".

Chúng tôi ngày một xa rời nhau và tôi ngày càng lún sâu vào hacking. Tôi dành cả ngày ở chỗ làm tại Franmark và cả đêm với Lenny DiCicco, chủ yếu là tập trung hack vào công ty Digital Equipment.

Khi Lenny bảo tôi cậu ta đã đăng ký một lớp học máy tính ở trường Cao đẳng Pierce gần đó, tôi nói tôi cũng sẽ đăng ký cùng cho có bạn, bất chấp quá khứ trước đó của tôi với ông thầy trưởng khoa Khoa học Máy tính, vụ đó đã khiến tôi phải bỏ dở chương trình. Hóa ra phòng quản lý vẫn chưa quên tôi, nhưng lúc đó tôi chưa hay biết gì về việc này.

Một ngày nọ, Lenny và tôi vào phòng máy tính dành cho sinh viên, nơi đặt một đống thiết bị đầu cuối kết nối với một hệ thống MicroVAX VMS. Chúng tôi nhanh chóng hack máy và chiếm được toàn bộ đặc quyền. Lenny viết một đoạn mã cho phép chúng tôi tạo ra bản sao của toàn bộ hệ thống.

https://thuviensach.vn

Chúng tôi không có mục đích sử dụng gì cho nó cả: Chúng tôi chỉ coi nó như một chiến tích. Vì thế, ngay khi vào được hệ thống, Lenny đặt một chiếc đĩa từ vào ổ đĩa của máy tính, và chạy đoạn mã lệnh để bắt đầu sao lưu, rồi chúng tôi rời đi. Chúng tôi định sẽ quay lại sau vài tiếng, khi việc sao chép đã hoàn tất.

Một lúc sau, khi chúng tôi đang đi bộ trong trường, tôi nhận được tin nhắn của Eliot Moore, một người bạn đã lâu không nói chuyện. Tôi đến máy điện thoại công cộng và gọi lại cho cậu ta.

“Cậu đang ở trường Pierce đấy à?” cậu ta hỏi.

“Ừ.”

“Cậu để đĩa trong ổ đĩa đấy à?”

“Ôi chết tiệt... sao cậu biết?” tôi nói.

“Đừng quay lại phòng máy tính,” cậu ta cảnh báo tôi. “Họ đang đợi cậu ở đó.” Nhờ sự tình cờ lạ lùng nào đó, Eliot đã ở trong phòng máy tính khi giáo viên để ý thấy ánh đèn chớp nháy từ ổ đĩa MircoVAX. Rõ ràng là có ai đó đã nhét một chiếc đĩa từ vào và đang sao chép các tập tin.

Giáo viên lớp Khoa học Máy tính, Pete Schleppenbach, đã ngay lập tức nghi ngờ chúng tôi. Eliot nghe lỏm được thầy giáo đang bàn bạc tình hình với các nhân viên khác và ngay lập tức gọi cho tôi. Nếu cậu ta không gọi, chúng tôi đã sa bẫy.

Sau đó, trường đã liên hệ với LAPD để báo cáo vụ việc.

Do chúng tôi chưa đến lấy chiếc đĩa, nên họ không có bằng chứng và chúng tôi vẫn tiếp tục được ở lại trường, lên lớp và dùng phòng máy. Nhưng LAPD để mắt đến chúng tôi, điều động người giám sát trên trần lớp học và theo dõi chúng tôi nhiều ngày liền. Hẳn bạn sẽ nghĩ họ phải có vụ gì thú vị hơn để xử

https://thuviensach.vn

lý. Đêm đến, họ theo chúng tôi đến chỗ làm của Lenny, nơi chúng tôi ở đó hack đến tận sáng sớm. Họ biết chúng tôi đang làm việc xấu, nhưng không chứng minh được.

Hắn là mấy gã ở Cao đẳng Pierce cảm thấy rất thất vọng, nhưng họ vẫn chưa chịu dừng lại. Tôi để ý thấy một chiếc xe của công ty DEC trong bãi đỗ xe của trường. Vậy là tôi gọi đến văn phòng bên ngoài của DEC ở Los Angeles, nói rằng mình đến từ Phòng Thanh toán của Cao đẳng Pierce, và hỏi rằng họ đang hỗ trợ chúng tôi chuyện gì.

"Ồ," gã đó nói với tôi, "chúng tôi đang cố giúp các anh bắt mấy tay hacker."

Ở một thiết bị đầu cuối trong phòng máy ở Pierce, tôi đã truy ra được một địa chỉ bộ nhớ từ tài khoản sinh viên của mình, trong đó chỉ ra rằng tài khoản của tôi đã được kích hoạt "kiểm định bảo mật".[39] Lenny cũng kiểm tra tài khoản của cậu ta bằng kỹ thuật tương tự và cũng thu được kết quả tương tự. Gã từ DEC nấp trong một căn phòng nhỏ với máy tính và máy in, theo dõi mọi việc chúng tôi làm từ tài khoản sinh viên. (Tôi phát hiện ra việc này nhờ một hôm đến sớm trước khi gã đến và theo gã vào phòng.) Tôi nghĩ việc này hơi quá bởi sinh viên chỉ dùng hệ thống để hoàn thành bài thực hành và nó không được kết nối mạng hay nối với dây điện thoại. Nhưng tôi đã tìm ra cách khiến cho gã bận rộn: Tôi viết một đoạn chương trình rất đơn giản liệt kê tất cả các tập tin trong thư mục của tôi, lặp đi lặp lại. Vì chương trình kiểm định bảo mật được thiết kế để gửi cảnh báo chi tiết về tất cả các tập tin được mở hoặc được đọc, tôi biết máy in của gã sẽ hoạt động không ngừng. Tôi có thể hình dung ra việc gã ngồi trong căn phòng nhỏ xíu đó, vò đầu bứt tai khi máy in liên tục chạy cho đến khi hết giấy. Và ngay khi gã đưa thêm giấy vào, danh sách tập tin sẽ lại tiếp tục được in ra.

[39] Kiểm định bảo mật (security auditing): Quy trình kiểm tra các ứng dụng và hệ điều hành trong nội bộ để tìm ra lỗ hổng bảo mật. (BTV)

https://thuviensach.vn

Một thời gian ngắn sau đó, thầy giáo lôi tôi và Lenny ra khỏi phòng thí nghiệm máy tính và kết tội chúng tôi đã gõ lệnh trái phép. Tôi hỏi: “Chúng em không được phép liệt kê tập tin của chính mình ạ?” Cả Lenny và tôi đều bị tống lên văn phòng khoa để xử lý.

Vài tuần sau, phòng quản lý của trường Pierce tổ chức một phiên tòa không chính quy nhằm xử vụ của chúng tôi. Họ vẫn nghi chúng tôi là thủ phạm đứng đằng sau vụ hacking, nhưng không chứng minh được. Không nhân chứng. Không dấu vân tay. Không lời thú tội. Bất chấp những điều đó, cả Lenny và tôi vẫn bị đuổi khỏi Pierce, dựa trên những chứng cứ gián tiếp.

https://thuviensach.vn

08

LEX LUTHOR

Iwh xwqv wpvpj fwr Vfvyj qks wf nzc ncgsoo esg psd gwc ntoqujvr ejs rypz nzfs?

Lenny và tôi muốn có mã nguồn cho hệ điều hành VMS của DEC để nghiên cứu nhằm tìm ra các lỗ hổng bảo mật trong đó. Chúng tôi cũng có thể tìm các bình luận của lập trình viên về việc vá lỗ hổng, từ đó truy ngược lại xem các vấn đề đó là gì và làm sao để tận dụng chúng. Chúng tôi cũng muốn tự mình biên soạn một phần của hệ điều hành, như vậy sẽ dễ cấy vài mã gián điệp vào trong đó hơn. Kế hoạch đề ra là chúng tôi sẽ thực hiện một vụ tấn công bằng kỹ thuật xã hội vào DEC nhằm đột nhập vào cụm máy phát triển VMS. Tôi đã có số dial-up kết nối modem pool của cụm phát triển VMS.

Khi Lenny vẫn còn đi làm, cậu ta từng đến hộp đầu cuối (terminal box) của tòa nhà nơi mình làm việc để tìm đường fax của các công ty khác. Bởi có rất nhiều công ty cùng đặt văn phòng trong một tòa nhà, nên Lenny có thể đấu đường dây của văn phòng nào đó vào một cặp dây cáp không sử dụng đi thẳng tới phòng máy tính của VPA, và không ai có thể truy ra được các cuộc gọi đi của chúng tôi.

Trong lúc đó, tôi tới khách sạn Country Inn gần văn phòng của cậu ta và dùng điện thoại công cộng để gọi cho Lenny. Khi cậu ta nhấc máy, tôi dùng một điện thoại khác để gọi tới số điện thoại chính của DEC ở Nashua, New Hampshire, nơi đặt các phòng nghiên cứu và phát triển của họ.

Tôi đứng đó giữa hai máy điện thoại, với mỗi ống nghe một bên tai.

https://thuviensach.vn

Tôi nói với người phụ nữ nghe máy ở Nashua rằng tôi cũng làm việc ở DEC và hỏi được vị trí phòng máy cũng như số điện thoại phòng quản lý.

Lúc gọi điện tới phòng này, tôi dùng tên của một nhân viên trong phòng bảo vệ và hỏi xem liệu phòng quản lý có hỗ trợ nhóm "Star cluster" của hệ điều hành VMS đang chạy trên máy phát triển VMS hay không. Nhân viên của DEC nói có. Tôi dùng tay che kín nửa dưới của ống nghe điện thoại, sau đó nói chuyện với Lenny bằng ống nghe còn lại, bảo cậu ta quay số modem.

Sau đó, tôi nói người trực máy gõ lệnh "show users" để hiển thị người đăng nhập. (Nếu bạn đang trong quá trình đăng nhập như Lenny lúc đó, trên màn hình sẽ hiển thị dòng chữ "<LOGIN>" cùng với tên máy tính đang dùng để đăng nhập.) Còn đây là những gì nhân viên DEC thấy trên màn hình của cô ta:

VMS User Processes at 9-JUN-1988 02:23 PM

Total number of users = 3, number of processes = 3

Username	Node	Process	NamePID	Terminal
GOLDSTEIN	STAR	Aaaaaa_fta2:	2180012D	FTA2:
PIPER	STAR	DYSLI	2180011A	FTA1:
<LOGIN>			2180011E	TTG4:

https://thuviensach.vn

Bởi không phải gõ bất kỳ tên đăng nhập hay mật khẩu nào, nên nhân viên DEC không để ý những việc tôi yêu cầu cô ta làm. Cô ta có lẽ cũng biết một lệnh spawn để làm gì, nhưng một nhân viên trực máy hiếm khi phải dùng tới nó, do vậy hiển nhiên là cô ta đã không nhận ra.

Lệnh này tạo ra quá trình đăng nhập trên thiết bị modem mà Lenny đang kết nối dưới điều kiện tài khoản của nhân viên trực máy. Ngay khi người này gõ lệnh, một ký hiệu "$" sẽ xuất hiện trên màn hình của Lenny. Điều đó đồng nghĩa với việc cậu ta đã đăng nhập và có toàn quyền hệ thống của một nhân viên trực phòng máy. Khi thấy ký hiệu "$" xuất hiện, Lenny đã kích động tới mức bắt đầu hét lên trên điện thoại: "Có prompt[40] rồi! Có prompt rồi!"

[40] Prompt: Dấu nhắc lệnh, tức ký hiệu xuất hiện trên cửa sổ thông báo sẵn sàng đợi lệnh. (ND)

Tôi kéo ống nghe của Lenny ra xa và bình thản nói với người trực máy: "Xin lỗi chị một chút, tôi sẽ quay lại ngay."

Tôi ghì điện thoại bằng chân để chặn âm thanh vào ống nói, nhấc ống nghe còn lại và nói với Lenny, "Câm miệng!" Sau đó, tôi tiếp tục cuộc gọi với nhân viên DEC.

Lenny ngay lập tức kiểm tra xem kiểm định bảo mật đã được kích hoạt hay chưa. Có rồi. Vì vậy, thay vì lập một tài khoản mới có thể kích hoạt báo động kiểm định và gây nghi ngờ, Lenny chỉ thay đổi mật khẩu của một tài khoản không còn hoạt động với toàn quyền hệ thống.

Trong lúc đó, tôi cảm ơn nhân viên phụ trách đầu dây bên kia và nói rằng cô ta có thể thoát khỏi hệ thống. Một lúc sau, Lenny kết nối lại và đăng nhập vào tài khoản bằng mật khẩu mới của mình.

Khi chúng tôi đã tấn công được vào cụm phát triển VMS, mục tiêu tiếp theo là có được mã nguồn mới nhất của VMS. Việc này không quá khó khăn. Khi

https://thuviensach.vn

chúng tôi liệt kê các đĩa mềm đã được kết nối, một trong số chúng có gắn nhãn “VMS_SOURCE.” Dễ như ăn kẹo vậy.

Tại thời điểm này, chúng tôi tải lên một công cụ nhỏ được thiết kế để tắt chế độ kiểm định bảo mật mà không kích hoạt chuông báo. Khi chuông báo đã bị tắt, chúng tôi lập thêm vài tài khoản đăng nhập có toàn quyền điều hành và thay đổi vài mật khẩu của các tài khoản đặc quyền chưa được dùng tới trong sáu tháng. Kế hoạch của chúng tôi là sao chép bản mới nhất của mã nguồn VMS vào USC, nhờ vậy, chúng tôi có thể duy trì toàn quyền đăng nhập vào mã nguồn ngay cả khi đã bị đá khỏi cụm Star cluster.

Sau khi thiết lập các tài khoản mới, chúng tôi mở hòm thư của Andy Goldstein. Goldstein từng là thành viên của đội thiết kế VMS thuở đầu ở Digital và nổi tiếng trong giới VMS với vai trò là bậc thầy về hệ điều hành. Chúng tôi biết anh ta cũng làm việc có liên quan tới các vấn đề bảo mật VMS, do đó, chúng tôi đoán rằng e-mail của anh có thể là nơi phù hợp để tìm hiểu thông tin về các vấn đề bảo mật mới nhất mà DEC đang cố sửa chữa.

Goldstein quả có nhận được các báo cáo về lỗi lập trình bảo mật (security bug) từ một người có tên Neill Clift. Tôi nhanh chóng biết được Clift là sinh viên cao học của Đại học Leeds ở Anh, chuyên ngành Hóa học hữu cơ. Nhưng anh ta rõ ràng là một kẻ say mê máy tính và có một tài năng đặc biệt: rất nhạy bén trong việc tìm ra các điểm yếu của hệ điều hành VMS và thành thực báo lại cho DEC về các lỗi này. Anh ta không nhận ra là giờ đây, anh ta đã cho cả tôi biết nữa.

Điều này đặt nền móng cho nước đi tiếp theo, có thể coi là một mỏ vàng đối với tôi.

Sau khi soát qua một lượt hòm thư của Goldstein, tôi tìm thấy một bản phân tích đầy đủ về bản vá lỗi[41] cho “Loginout”, một chương trình đăng nhập của VMS. Bản vá lỗi được phát triển bởi một nhóm hacker người Đức trực thuộc

https://thuviensach.vn

“Câu lạc bộ máy tính hỗn loạn” (Chaos Computer Club – CCC). Vài thành viên trong nhóm tập trung phát triển các bản vá lỗi cho những chương trình VMS chuyên biệt cho phép bạn có toàn quyền kiểm soát hệ điều hành.

[41] Bản vá lỗi (patch): Một loạt các thay đổi dành cho chương trình máy tính hay các dữ liệu hỗ trợ chương trình được thiết kế nhằm cập nhật, chỉnh sửa hay cải thiện chương trình đó. Bản vá lỗi có thể bao gồm việc chỉnh sửa lỗ hổng bảo mật và các lỗi lập trình khác, hay nâng cao tính khả dụng hoặc hiệu suất. (BTV)

Bản vá lỗi của VMS Loginout do nhóm hacker kia phát triển cũng cải biến chương trình đăng nhập ở nhiều phương diện, đưa ra chỉ thị bí mật lưu trữ mật khẩu trong một tập tin được cho phép bởi hệ điều hành ở khu vực giấu kín; ẩn người dùng; và chặn tất cả chuông báo bảo mật khi có ai đó đăng nhập vào hệ thống bằng mật khẩu đặc biệt.

Những câu chuyện trên báo chí về CCC có nhắc tới tên nhóm trưởng. Tôi dò theo số điện của người này và gọi cho anh ta. Ở thời điểm đó, tôi cũng dần gây dựng được tiếng tăm trong giới hacking, do đó anh ta nhận ra tôi ngay. Anh ta nói tôi nên nói chuyện với một thành viên khác trong nhóm, nhưng đáng tiếc là người này đang bị ung thư giai đoạn cuối. Tôi gọi tới bệnh viện cho người đó và giải thích rằng mình đã có được bản phân tích của nhóm về bản vá lỗi cửa hậu cho VMS Loginout cùng chương trình “Show” và thấy chúng thật tuyệt. Tôi hỏi liệu anh ta có công cụ hay bản vá lỗi thú vị nào sẵn lòng chia sẻ hay không.

Đầu dây bên kia là một người siêu ngầu và nói nhiều. Anh đề nghị gửi cho tôi một vài không tin. Đáng tiếc là anh phải gửi thư chậm qua đường bưu điện vì bệnh viện không có máy tính. Vài tuần sau, tôi nhận được một gói nhỏ gồm các tài liệu chứa thông tin cụ thể về các kỹ thuật hacking chưa từng được công bố của nhóm.

https://thuviensach.vn

Mở rộng công trình của CCC, Lenny và tôi đã phát triển và cải thiện thêm vài bản vá lỗi có thể thêm vào nhiều tính năng hơn nữa. Về cơ bản, CCC đã tạo ra bộ khung để chúng tôi có thể phát triển dựa vào đó. Khi các phiên bản mới của VMS phát hành, Lenny và tôi vẫn tiếp tục chỉnh sửa bản vá lỗi cho phù hợp. Do Lenny luôn làm việc ở các công ty có hệ điều hành VMS, nên chúng tôi có thể thử nghiệm bản vá lỗi của mình trên hệ điều hành cậu ta dùng ở công ty và ứng dụng chúng vào các hệ điều hành mà chúng tôi muốn duy trì khả năng đăng nhập.

Sau khi phát hiện ra một số khách hàng chính của DEC bị tấn công, các lập trình viên của công ty đã viết một công cụ bảo mật có thể nhận biết bản vá lỗi của Chaos. Lenny và tôi xác định vị trí của phần mềm nhận diện và phân tích nó, rồi chỉnh sửa phiên bản bản vá lỗi của Chaos sao cho công cụ của DEC không thể tìm ra nó. Việc này thực sự rất dễ dàng. Điều này còn khiến việc cài đặt bản vá lỗi của chúng tôi vào vô số hệ điều hành VMS trên Easynet, mạng toàn cầu của Digital, trở nên dễ dàng hơn.

Dù xác định vị trí mã không khó, nhưng việc di chuyển nó lại không hề dễ dàng. Có rất nhiều mã. Để giảm thiểu độ lớn của mã, chúng tôi phải nén nó lại. Mỗi thư mục chứa tới hàng trăm tập tin. Chúng tôi nén tất cả vào một tập tin đơn lẻ và mã hóa nó, như vậy nếu có ai đó tìm thấy, trông nó chỉ như một tập tin rác mà thôi.

Cách duy nhất để lưu giữ các tập tin này và có thể nghiên cứu chúng khi rảnh rỗi là tìm các hệ thống trên mạng Easynet của DEC có kết nối với Arparnet, nhờ vậy chúng tôi có thể chuyển chúng ra ngoài hệ thống của DEC. Chúng tôi chỉ thấy có bốn hệ thống trên Easynet có kết nối với Arparnet, nhưng chúng tôi có thể sử dụng cả bốn để chuyển mã ra ngoài theo từng phần.

Kế hoạch ban đầu là chúng tôi sẽ lưu lại một bản sao mã ở USC, điều này có vẻ khá thiển cận. Thứ nhất là nên có nhiều hơn một nơi lưu trữ các bản sao giống nhau, có như vậy thì khi các mã bị lộ, mọi công sức mới không đổ

https://thuviensach.vn

xuống biển. Nhưng vấn đề là codebase[42] quá lớn. Nếu cố lưu tất cả tại một nơi thì rủi ro bị phát hiện là rất lớn. Do vậy, chúng tôi bắt đầu tấn công vào các hệ thống trên Arpanet, cố tìm ra một "tủ bảo quản" an toàn hơn để trữ đồ. Tôi bắt đầu có cảm giác rằng lấy được mã nguồn từ DEC vẫn còn là phần việc dễ dàng, thử thách thực sự là làm sao tìm được nơi cất giấu chúng. Chúng tôi có quyền đăng nhập vào hệ máy tính của Trạm Hàng không Hải quân Patuxent River ở Maryland và nhiều nơi khác. Nhưng thật đáng tiếc, hệ thống ở Patuxent River chỉ có khả năng lưu trữ rất nhỏ.

[42] Codebase: Toàn bộ mã nguồn cho một phần mềm hoặc ứng dụng nào đó. (ND)

Chúng tôi cũng cố tấn công vào hệ thống máy tính của Trung tâm Nghiên cứu Sức đẩy Phản lực của NASA (Jet Propulsion Laboratory – JPL) ở Pasadena, California bằng cách sử dụng bản vá của Chaos đã được chỉnh sửa.

Cuối cùng, JPL cũng phát hiện ra hệ thống của họ bị tấn công, có thể là nhờ họ đã để ý tới những thay đổi không được phép trên các chương trình Loginout và Show trên VMS. Hắn là họ đã truy ngược lại mã nhị phân nhằm tìm ra cách thức các chương trình đã bị thay đổi và xác định được thủ phạm chính là CCC. Ban lãnh đạo của JPL công bố với truyền thông nhận định này, dẫn đến bản tin chấn động trên mặt báo về một gã hacker người Đức bị bắt sống khi đang xâm nhập vào hệ thống máy tính của JPL. Lenny và tôi cười khoái trá, nhưng bù lại chúng tôi cũng có chút lo lắng nếu bị phát hiện.

Khi bắt đầu thực hiện chuyển tập tin, chúng tôi buộc phải duy trì liên tục cả ngày lẫn đêm, từng chút từng chút một. Đó quả là một quá trình vô cùng chậm chạp. Tốc độ dial-up thời điểm đó (nếu bạn thực sự muốn dùng từ "tốc độ") tối đa là T1, tương đương với khoảng 1.544 megabit/giây. Ngày nay, ngay cả điện thoại di động bình thường cũng còn chạy nhanh hơn thế nhiều.

https://thuviensach.vn

DEC ngay lập tức phát hiện ra động thái của chúng tôi. Mấy gã phụ trách duy trì vận hành hệ thống đã nhận ra sự bất thường nhờ sự gia tăng lưu lượng truy cập mạng rất lớn vào giữa đêm. Tình hình càng tệ hơn khi họ cũng nhận ra các khoảng lưu trữ còn trống trên bộ nhớ đã biến mất. Họ vốn không có nhiều dung lượng trên hệ thống thường chỉ được tính bằng megabyte, trong khi chúng tôi đang vận chuyển tới hàng gigabyte.

Các hoạt động vào ban đêm và những khoảng trống dung lượng biến mất đã cho thấy vấn đề bảo mật nào đó. Họ nhanh chóng thay đổi tất cả mật khẩu tài khoản và xóa toàn bộ tập tin của chúng tôi trên hệ thống. Đây quả là một thách thức, nhưng Lenny và tôi không hề nhụt chí. Chúng tôi không ngừng tấn công qua từng đêm, mặc cho họ nỗ lực ra sao. Trên thực tế, nhân viên của DEC và những người sử dụng hệ thống không phát hiện ra họ đã bị chúng tôi kiểm soát trạm làm việc cá nhân và qua đó có thể theo dõi thao tác bàn phím, vì vậy, chúng tôi sẽ chẳng mấy khó khăn để lấy được quyền đăng nhập ngay khi họ vừa thay đổi tài khoản.

Trong suốt quá trình, kỹ sư mạng lưới của DEC có thể thấy rất nhiều tập tin cỡ lớn được chuyển đi, họ chỉ không biết làm sao để dừng việc đó lại. Hoạt động chẳng mấy vô hại của chúng tôi khiến họ tin rằng mình là đối tượng của một dạng tấn công gián điệp có tổ chức nào đó do mấy tay đánh thuê quốc tế được thuê để đánh cắp các bí mật công nghệ tân tiến nhất của họ. Chúng tôi đọc được các giả thuyết này trong e-mail của DEC. Rõ ràng, mọi chuyện khiến họ phát điên. Tôi luôn đăng nhập vào hòm thư để xem họ đã tiến triển đến đâu và dự định làm gì, đồng thời cố gắng hết sức để đánh lạc hướng họ. Nhờ sở hữu toàn quyền kết nối với Easynet, chúng tôi có thể đăng nhập vào hệ thống từ Anh và các nước khác trên toàn thế giới. DEC không thể xác định được chính xác điểm đầu ở đâu bởi chúng tôi cứ liên tục thay đổi.

Chúng tôi cũng phải đối mặt với thử thách tương tự diễn ra ở USC. Nhóm quản trị ở đây cũng nhận ra dung lượng ổ đĩa trên vài MicroVAX đã biến mất. Họ ngắt kết nối mạng khi chúng tôi chuyển dữ liệu vào ban đêm.

https://thuviensach.vn

Chúng tôi bắt đầu lại và rồi họ tắt nguồn cả hệ thống suốt đêm. Chúng tôi lại đợi tới khi họ bật máy và lại bắt đầu chuyển tập tin. Trò chơi này cứ diễn ra như vậy trong nhiều tháng trời.

Đôi khi, giữa những lần chống chọi với đội ngũ quản trị viên hệ thống, cố níu lấy dung lượng đồ sộ của mã nguồn và cam chịu tốc độ đường truyền chậm đến phát điên, chúng tôi có cảm giác như mình đang dùng một chiếc ống hút để hút cả đại dương vào vậy. Nhưng chúng tôi không bỏ cuộc.

Khi tất cả mã nguồn VMS đã được chuyển tới hệ thống ở USC, chúng tôi cần ghi chúng vào đĩa từ để có thể từ từ chọn lọc mà không phải lo tới việc bị tấn công ngược lại khi kết nối tới Easynet. Và chuyển mã nguồn vào đĩa là loại công việc của ba người.

Lewis De Payne được cử xâm nhập vào khuôn viên trường trong vai một sinh viên. Cậu ta có thể nhờ một trong những nhân viên phụ trách phòng máy tính gắn đĩa của mình lên ổ đĩa của hệ thống.

Ở một nơi khác trong thị trấn, tại văn phòng anh bạn Dave Harrison, tôi có thể kết nối vào một hệ thống VMS gọi là “ramoth” qua modem dial-up đã có đĩa của Lewis gắn vào ổ. Tôi lưu nhiều hết mức có thể các mã nguồn VMS vào đây. Sau đó, Lewis đưa cho nhân viên phụ trách phòng máy một đĩa trắng khác và chuyển đĩa đã ghi cho Lenny DiCicco. Cuối mỗi giai đoạn, Lenny sẽ cầm tất cả các đĩa mới để giấu trong một tủ khóa trữ đồ mà chúng tôi đã thuê. Chúng tôi lặp đi lặp lại vòng làm việc này cho tới khi có chừng 30-40 đĩa chứa toàn bộ mã nguồn của VMS phiên bản 5.

Trong khoảng thời gian dài ở phòng làm việc của Dave, tôi phát hiện ra một công ty khác cũng đặt văn phòng trong tòa nhà có tên là GTE Telenet đang chạy một trong những hệ thống “X25” lớn nhất nhằm phục vụ cho những khách hàng lớn nhất thế giới. Có lẽ, tôi có thể chiếm được quyền quản trị vào hệ thống của họ và theo dõi lưu lượng khách hàng. Trước đó, Dave đã từng bẻ khóa hộp cứu hỏa và lấy được chìa khóa tổng của cả tòa nhà. Vào

https://thuviensach.vn

một đêm muộn, Dave và tôi dùng chìa mở văn phòng GTE Telenet chỉ để nhòm ngó xung quanh. Khi thấy họ dùng VMS, tôi vô cùng phấn chấn; cảm giác như thể ở nhà.

Tại đây có một hệ VMS với tên nút mạng là "Snoopy". Sau khi mò mẫm một hồi, tôi phát hiện ra Snoopy đã đăng nhập vào một tài khoản đặc quyền, cho phép tôi có toàn quyền đăng nhập hệ thống. Đây đúng là cám dỗ quá lớn. Dù nhân viên Telenet vẫn thường ra vào văn phòng 24/7, nhưng tôi vẫn ngồi xuống máy tính và bắt đầu khám phá, nhìn vào script và ứng dụng bên thứ ba nhằm truy ra công cụ mà họ có cũng như cách thức chúng có thể được sử dụng để theo dõi mạng lưới. Chỉ trong một khoảng thời gian rất ngắn, tôi đã tìm ra cách lén theo dõi lưu lượng truy cập mạng lưới khách hàng. Tôi bừng tỉnh. Nút này có tên là Snoopy bởi nó cho phép các kỹ thuật viên có thể theo dõi lưu lượng truy cập trên mạng lưới khách hàng: Nó cho phép họ rình mò (snoop).

Vì đã có sẵn địa chỉ X25 nên tôi kết nối với hệ thống VMS tại khoa Hóa hữu cơ của Đại học Leeds, nơi Neill Clift đang theo học. Tôi không có bất kỳ quyền đăng nhập nào; mọi nỗ lực phỏng đoán đều không chính xác. Do khác biệt về múi giờ, Clift đăng nhập vào hệ thống, anh ta nhận ra mấy lần cố đăng nhập của tôi và viết thư cho quản trị viên của Snoopy để thông báo rằng có ai đó đang cố kết nối vào hệ thống của trường. Dĩ nhiên là tôi đã xóa thư.

Dù không kết nối được vào Đại học Leeds đêm đó, những gì tôi cố làm đã tạo tiền đề cho việc đưa Clift vào mục tiêu sau này và đem đến những thành công to lớn.

Lenny và tôi thường đấu trí với nhau. Cậu ta sẽ đóng vai nhân viên phụ trách máy tính ở một công ty có tên là VPA, còn tôi thì làm ở CK Technologies, Newbury Park. Chúng tôi cược xem ai có thể đột nhập vào hệ thống VMS dành cho nhân viên mà người còn lại đang quản lý. Ai hack được vào hệ thống VMS của công ty người kia thì người đó sẽ thắng cuộc. Nó hệt như

https://thuviensach.vn

trò chơi "cướp cờ", được thiết kế để kiểm tra khả năng bảo vệ hệ thống trước đối phương.

Lenny không đủ tinh khôn để chặn được tôi. Tôi liên tục tấn công vào hệ thống của cậu ta. Tiền cược luôn là 150 đô-la, đủ cho một bữa tối hai người ở Spago, nhà hàng của đầu bếp nổi tiếng Wolfgang Puck ở Beverly Hills. Tôi thắng cược liên tục tới mức Lenny bắt đầu cảm thấy khó chịu. Tại một trong những buổi hacking thâu đêm, Lenny than phiền rằng cậu ta chưa từng thắng lấy một lần. Tôi nói mình có thể dừng bất kỳ lúc nào, nhưng Lenny muốn thắng.

Công ty của Lenny mới lắp một loại khóa kỹ thuật số trên cánh cửa phòng máy; cậu ta thách tôi đoán được mã số để mở khóa và biết rằng đây gần như là một việc bất khả thi. "Nếu cậu không vào được," cậu ta nói, "cậu sẽ phải trả tớ 150 đô-la ngay đêm nay."

Tôi nói tôi sẽ không lấy tiền của Lenny vì nhiệm vụ lần này quá đơn giản, cậu ta hẳn sẽ rất bực mình bởi dù thế nào thì tôi cũng luôn thắng. Lời chế nhạo khiến Lenny càng thêm lo lắng khi tôi nhận kèo.

Thực ra để thắng được lần này một cách thắng thắn cũng không hề đơn giản. Nhưng thần may mắn đã mỉm cười với tôi. Khi đang dùng máy tính của Lenny để tấn công vào mạng lưới của Digital, tôi vô tình phát hiện ra một chiếc ví rơi trên sàn ngay dưới bàn làm việc. Tôi "chẳng may" làm rơi bút, sau đó cúi xuống nhặt và nhồi chiếc ví vào trong tất. Tôi nói với Lenny mình phải đi vệ sinh một lát.

Trong ví, tôi tìm thấy một mẩu giấy có ghi mã số cửa. Tôi không thể tin vào mắt mình: Lenny là một hacker lõi đời, vậy mà cậu ta lại không thể nhớ được dãy số đơn giản này ư? Chưa kể cậu ta lại còn ngu ngốc tới mức viết mã số đó ra rồi nhét vào ví? Điều này ngớ ngẩn tới mức tôi đã nghĩ rằng mình đang bị đặt bẫy. Liệu cậu ta có cố tình vứt ví ở đó để làm bẽ mặt tôi không?

https://thuviensach.vn

Tôi quay trở lại bàn, đặt ví vào chỗ cũ và nói với Lenny tôi cần 1 giờ để đoán mã số cửa. Chúng tôi thống nhất rằng điều kiện duy nhất là tôi không được phá khóa. Những cách thức khác đều được chấp nhận.

Vài phút sau, Lenny đi xuống tầng dưới để lấy thứ gì đó. Khi quay lại, cậu ta không thấy tôi. Lenny tìm kiếm khắp nơi, cuối cùng mở mã khóa cửa phòng máy. Tôi đã ngồi sẵn trong đó, gõ trên màn hình lệnh VMS và đăng nhập với toàn quyền quản trị. Tôi cười.

Lenny nổi điên. “Cậu chơi ăn gian!” cậu ta hét lên.

Tôi ngó ra. “Cậu nợ tớ 150 đô-la.” Khi cậu ta cự nự, tôi nói: “Tớ sẽ cho cậu một tuần.” Thật tuyệt khi hạ gục được một người luôn tự mãn như Lenny. Cậu ta không chịu trả tiền, còn tôi thì liên tục kéo dài thời hạn và tuyên bố sẽ tính lãi suất sau đó. Tôi vẫn chẳng nhận được gì cả. Cuối cùng, trong một trò đùa không hơn không kém, tôi gọi tới phòng kế toán phụ trách khoản phải trả của công ty Lenny và vờ là nhân viên thuộc phòng Truất hữu Lương bổng[43] của Sở Thuế vụ (IRS). “Leonard DiCicco có còn làm việc ở chỗ chị không?” tôi hỏi.

[43] Truất hữu Lương bổng (Wage Garnishment): Khoản khấu trừ trong lương được tòa án Mỹ cho phép nhằm giúp người cho vay có thể thu một phần tiền của người vay nợ thông qua bên thứ ba như công ty tuyển dụng bên vay nợ. (ND)

“Vâng, còn,” giọng phụ nữ trả lời điện thoại.

“Chúng tôi có lệnh báo truất hữu,” tôi nói. “Chúng tôi đề nghị bên công ty chị tạm giữ lương của anh ấy lại.” Người phụ nữ nói chị ta cần phải có giấy ủy quyền. Tôi nói với chị ta: “Chị sẽ nhận được fax vào thứ Hai, hiện tại tôi chỉ muốn đưa ra thông báo chính thức đề nghị tạm giữ toàn bộ khoản chi trả cho tới khi bên chị nhận được các giấy tờ cụ thể.”

https://thuviensach.vn

Tôi chỉ đơn giản nghĩ rằng Lenny có lẽ sẽ phải chịu bất tiện một chút. Khi không có bức fax nào chuyển tới vào thứ Hai, hắn cậu ta sẽ nhận được tiền.

Khi nhân viên phòng kế toán báo với Lenny về cuộc gọi của IRS, cậu ta ngay lập tức đoán được ai đứng sau chuyện này.

Nhưng cơn giận bùng nổ của Lenny đã vượt quá tầm kiểm soát khiến cậu ta mất hết lý trí và làm việc ngu xuẩn nhất: Lenny tới văn phòng của sếp và báo với ông ta rằng hai chúng tôi đã tấn công DEC từ văn phòng VPA.

Sếp của Lenny không gọi cho cảnh sát. Thay vào đó, ông ta và Lenny cùng gọi cho đội an ninh của DEC và nói với họ về thủ phạm đã quấy rối họ trong suốt nhiều tháng qua. Sau cùng, FBI vào cuộc và bắt đầu giăng bẫy.

Người của FBI và DEC đóng quân tại VPA ngay trước một trong những buổi hacking đêm muộn của chúng tôi. Họ đặt phần mềm giám sát trên các máy tính của VPA nhằm ghi lại mọi hành động chúng tôi sẽ làm. Trên người Lenny có gắn máy ghi âm lại mọi cuộc đối thoại. Đêm đó, mục tiêu của tôi là Đại học Leeds ở Anh. Sau lần xác định trước đó rằng Neill Clift là một trong những nguồn cung cấp thông tin chính về các lỗi bảo mật của Digital, tôi muốn đột nhập vào hệ thống VMS của khoa Hóa hữu cơ thuộc trường Leeds, nơi có tài khoản của Clift.

Đã có lúc tôi cảm nhận được điều gì đó kỳ quái diễn ra với Lenny và hỏi cậu ta: “Mọi chuyện ổn chứ hả? Cậu có vẻ hơi lạ đấy.” Lenny nói cậu ta chỉ hơi mệt, và tôi lại bỏ qua những hành vi bất thường này. Lenny có lẽ đã lo sợ tôi có thể phát hiện ra điều gì đang thực sự diễn ra. Sau vài giờ hacking, chúng tôi bỏ cuộc. Tôi muốn tiếp tục, nhưng Lenny nói cậu ta cần phải dậy sớm.

Vài ngày sau, tôi nhận được cuộc gọi của Lenny: “Này, Kevin, tớ mới được nghỉ phép. Tới đây đi, tớ trả cậu tiền.”

Hai giờ sau, tôi lái xe vào một ga-ra nhỏ dưới tầng hầm của tòa nhà VPA đặt văn phòng. Lenny đứng đó, không nhúc nhích. Cậu ta nói: “Tớ cần phần

https://thuviensach.vn

mềm mô phỏng máy VT100 để sao ra cho cậu," ý chỉ phần mềm trên đĩa mà cậu ta biết tôi đặt trên xe. Lúc đó đã là 5 giờ chiều, tôi nói cả ngày nay mình chưa ăn gì cả và sắp chết đói rồi. Tôi thậm chí còn mời cậu ta cùng dùng bữa tối. Lenny vẫn cương quyết. Tôi muốn ra khỏi đó càng sớm càng tốt: Có gì đó không ổn. Nhưng rồi tôi bỏ cuộc, để xe nổ máy, bước ra ngoài để lấy mấy chiếc đĩa.

"Mày có biết cảm giác khi bị tóm là thế nào không?" Lenny chế nhạo. "Chuẩn bị tinh thần đi!"

Cả ga-ra đột nhiên ầm ĩ tiếng động cơ. Đèn ô tô chiếu thẳng vào chúng tôi từ mọi hướng, dừng lại thành một vòng tròn bao quanh. Mấy gã trong trang phục cảnh sát nhảy ra khỏi xe và bắt đầu hét lên với tôi: "FBI đây!"

"Anh đã bị bắt!"

"Đặt tay lên xe!"

Tôi nghĩ, nếu Lenny sắp đặt mọi chuyện chỉ để dọa tôi một mẻ, thì đây thực sự là một màn ấn tượng.

"Mấy anh không phải là FBI. Hãy cho tôi xem ID."

Họ lấy thẻ ra khỏi ví và mở chúng ra. Huy hiệu FBI ở khắp thẻ. Là hàng thật.

Tôi nhìn sang Lenny. Hắn ta đang nhún nhảy vui sướng, như thể ăn mừng việc thắng tôi.

"Lenny, sao mày có thể làm vậy?"

Sau khi bị một điệp vụ FBI còng tay, tôi nhờ Lenny gọi cho mẹ tôi và nói với bà rằng tôi đã bị bắt. Tên khốn đó thậm chí còn không buồn thể hiện chút tử tế cuối cùng.

https://thuviensach.vn

Hai nhân viên FBI đưa tôi tới Nhà tù Liên bang Terminal Island. Tôi chưa từng nhìn thấy thứ gì như vậy ngoại trừ trong phim hay một chương trình truyền hình: Những dãy phòng giam kéo dài với mấy cánh tay vắt vẻo ra ngoài chấn song. Hình ảnh trước mắt khiến tôi cảm thấy mình như đang gặp ác mộng trong mơ. Thật bất ngờ, mấy tù nhân khác tỏ ra khá thân thiện và dễ chịu. Họ còn đề nghị cho tôi mượn một vài món đồ. Khá nhiều người trong số họ đều từng là "cổ cồn trắng".

Nhưng tôi không được tắm. Tôi cảm thấy kinh tởm cho tới khi vài đặc vụ FBI đến đón và đưa tôi tới trụ sở chính của FBI tại phía Tây Los Angeles để chụp ảnh hồ sơ tội phạm. Tôi biết trông mình rất thảm hại – chưa tắm rửa, chưa chải tóc, mặc nguyên bộ đồ từ ba ngày trước và ngủ được rất ít mỗi đêm trên chiếc giường nhỏ. Nhưng ít ra, bức ảnh đó cũng mang tới cho tôi một chút an ủi nhỏ tại những thời điểm quan trọng sau này.

Sau cả ngày cuối tuần bị giam giữ, tôi được đưa tới trước mặt thẩm phán Venetta Tassopulos vào sáng thứ Hai cho buổi điều trần đầu tiên, với dự tính sẽ được bảo lãnh tạm tha sau đó. Tay luật sư mà tòa chỉ định cho tôi hỏi liệu có phải tôi từng bỏ trốn hay không. Hóa ra hắn đã nói chuyện với ủy viên công tố, người này nói với hắn rằng tôi từng chạy tới Isarel vào năm 1984, điều này không đúng sự thật.

Khi buổi điều trần bắt đầu, tôi ngồi đó sững sờ nghe tay ủy viên công tố, phụ tá luật sư Leon Weidman, không ngừng rót tội tôi trước tòa. Weidman nói với thẩm phán: "Vấn đề này thực sự rất nghiêm trọng, chúng tôi phải tìm hiểu khắp nơi để nắm được những gì anh ta đã làm." Và đây là những gì hắn nói tôi đã làm, bên cạnh nhiều điều khác:

- Tấn công vào NSA và chiếm đoạt mã đăng nhập bí mật
- Ngắt điện thoại của viên giám sát tạm tha trước đây
- Xáo trộn báo cáo về công ty TRW của tòa án sau khi nhận được đối xử bất lợi

https://thuviensach.vn

- Cài tin giả cho báo chí về việc ngân hàng SPNB thất thoát hàng triệu đô-la sau khi bị hủy tuyển dụng
- Liên tục quấy rối và cắt dịch vụ điện thoại của diễn viên Kristy McNichol
- Tấn công máy tính của phòng cảnh sát và xóa tư liệu phạm tội trước đó của bản thân.

Rõ ràng, tất cả đều trật lất.

Luận điệu cho rằng tôi đã tấn công vào NSA hoàn toàn nực cười. Một trong những chiếc đĩa mềm bị cảnh sát Santa Cruz tịch thu có tập tin "NSA.TXT". Đây là kết quả của lệnh "whois" liệt kê tất cả người dùng đăng ký trên Dockmaster, hệ thống máy tính phi bảo mật của NSA mà Lenny đã thực hiện tấn công bằng kỹ thuật xã hội để thâm nhập thời hắn còn làm ở Hughes Aircraft. Mọi thứ trên tập tin đều là thông tin công khai, bao gồm cả danh sách các số máy phụ của Trung tâm Bảo mật Máy tính Quốc gia. Tay luật sư, hiển nhiên là không hiểu hắn đang thấy cái gì, đã liệt kê số máy phụ công khai là "mã đăng nhập bí mật". Thật không thể tin nổi.

Một luận điệu khác, ý cho rằng tôi đã tấn công vào máy tính của cảnh sát và xóa đi dữ liệu phạm tội của mình, có liên quan tới lần tôi đã hack vào SCO, nhưng những dữ liệu đã mất thực sự là lỗi của cơ quan chấp pháp. Hãy nhớ rằng Bonnie và tôi đã tự thú ở phòng cảnh sát phía Tây Hollywood. Chính vì họ đã bỏ qua, không buồn lấy dấu vân tay hay chụp ảnh chúng tôi nên mới không có dữ liệu liên quan đến vụ bắt giữ đó. Nói tóm lại, đó là lỗi của họ vì đã tắc trách: Họ không làm công việc lẽ ra phải làm.

Tất cả các luận điệu còn lại cũng sai nốt. Chúng được chỉnh sửa lại từ những tin đồn mà rõ ràng nhằm thuyết phục quan tòa rằng tôi là một mối lo ngại nghiêm trọng tới vấn đề an ninh quốc gia.

Điều khiến tôi hoang mang nhất là ý kiến cho rằng tôi liên tục ngắt dịch vụ điện thoại của nữ diễn viên Kristy McNichol chỉ vì si mê cô ấy. Thứ nhất, tôi

https://thuviensach.vn

không thể tưởng tượng nổi sao người ta có thể nghĩ rằng việc ngắt điện thoại của ai đó là cách thể hiện tình yêu. Tôi không hiểu câu chuyện bắt đầu như thế nào. Những trải nghiệm này đã hằn sâu trong ký ức tôi. Tôi phải chịu nỗi nhục lớn khi xếp hàng ở tiệm tạp hóa và trông thấy ảnh mình đính ngay trên trang bìa tờ National Examiner với dòng chữ hoa mỹ ngay bên cạnh nói rằng tôi là một kẻ rình mò điên cuồng bị ám ảnh bởi Kristy McNichol! Thứ cảm giác tôi phải trải qua khi vội liếc sang xung quanh, mong mỏi không có người mua hàng nào nhận ra mình trên trang bìa là thứ cảm giác tôi không muốn ngay cả kẻ thù tồi tệ nhất của mình phải chịu đựng.

Vài tuần sau, mẹ tôi, lúc đó đang làm việc tại Jerry's Famous Deli ở Studio City, trông thấy McNichol dùng bữa trưa tại quán. Bà tự giới thiệu bản thân và nói: "Kevin Mitnick là con trai tôi."

McNichol nói ngay sau đó: "Vâng, vậy làm sao anh ta cứ ngắt điện thoại của tôi vậy?" Bà nói rằng chuyện này chưa từng xảy ra với mình và cũng như tôi, chính bà cũng tự hỏi tin đồn đã bắt đầu như thế nào. Một thời gian sau, một tay thám tử tư đã khẳng định rằng không hề có chuyện như vậy.

Nhiều năm sau, khi mọi người hỏi tại sao tôi lại chạy trốn thay vì đối mặt với những cáo buộc chống lại mình, tôi đã nhớ lại những khoảnh khắc này. Thành thực mà nói, tôi được lợi gì nếu những kẻ buộc tội tôi rồi cũng sẽ tìm cách chơi bẩn? Nếu không thể chắc rằng mình sẽ được đối xử công bằng và chính quyền lại luôn sẵn lòng kết án dựa trên tin đồn thất thiệt, thì cách phản ứng thông minh nhất chính là trốn chạy!

Khi đến lượt mình trình bày trước tòa, tay luật sư chỉ định phát biểu rằng tôi quả thực có tới Israel vào cuối năm 1984, có điều tôi không hề bỏ trốn mà chỉ là ghé thăm. Tôi lại sững sờ. Chúng tôi đã nói về chuyện này chỉ 10 phút trước khi phiên tòa bắt đầu, tôi đã giải thích rằng mình chưa từng rời khỏi đất nước này trong nhiều năm, cũng như thực tế là tôi chưa từng đi nước ngoài. Mẹ, bà tôi và Bonnie đều kinh ngạc bởi họ biết anh ta đã nói những điều không đúng sự thật. Làm sao mà một luật sư lại có thể bất tài tới vậy?

https://thuviensach.vn

Trong nỗ lực cuối cùng nhằm đe dọa tòa án, Leon Weidman đã đưa ra một tuyên bố có lẽ là vô nhân đạo nhất được phát ra từ miệng một luật sư công tố liên bang: Hắn nói với thẩm phán Tassopulos rằng tôi có thể sẽ khởi xướng một cuộc tàn sát hạt nhân. “Anh ta có thể thì thầm qua điện thoại và ra lệnh phóng tên lửa hạt nhân từ NORAD,”[44] hắn nói. Ý niệm kỳ cục cỡ này có thể nảy ra từ đâu cơ chứ? Máy tính của NORAD thậm chí còn không kết nối với thế giới bên ngoài. Và hiển nhiên là họ không dùng đường dây điện thoại công cộng để phát lệnh phóng tên lửa rồi.

[44] NORAD (North American Aerospace Defense Command): Bộ Tư lệnh Phòng không Bắc Mỹ, cơ quan quân sự phối hợp của Mỹ và Canada có nhiệm vụ cảnh báo và bảo vệ không phận của hai quốc gia này. (BTV)

Những phát ngôn khác của hắn, tất cả đều hoàn toàn sai lệch, đều là những câu chuyện bịa đặt có vẻ được góp nhặt từ đâu đó qua các bài báo thêu dệt. Có điều tôi chưa từng nghe tới vụ NORAD này, thậm chí là trong các câu chuyện khoa học viễn tưởng. Khả năng duy nhất mà tôi có thể nghĩ tới là hắn ta đã lấy nó từ bộ phimWar Games (tạm dịch: Mật mã chết) đình đám của Hollywood. (Sau này mọi người đều cho rằng bộ phim War Games đã khai thác một phần câu chuyện thật của tôi nhưng không phải vậy.)

Weidman đã thêu dệt nên hình ảnh của tôi như một Lex Luther trong thế giới máy tính (tôi đoán chắc hắn phải là siêu nhân thật!). Ý tưởng thì-thầm-qua-điện-thoại nhảm nhí tới mức tôi đã phá lên cười khi nghe hắn nói vậy. Hắn là quan tòa có thể nói với hắn điều đó thật lố bịch.

Thay vào đó, tòa tuyên bố tôi bị giam giữ và không được quyền bảo lãnh tại ngoại bởi tôi là một mối nguy hại cho cộng đồng khi được “trang bị vũ khí bàn phím” (hắn là “trang bị vũ khí”!). Và quan tòa còn nói thêm rằng tôi phải được tạm giam tại nơi không có kết nối điện thoại. Khu vực giam giữ dành cho những tù nhân thông thường đều có điện thoại để tù nhân có thể nhận cuộc gọi. Chỉ có một khu vực duy nhất không có điện thoại: vùng biệt giam, còn được biết đến dưới cái tên “cái lỗ”.

https://thuviensach.vn

Trong một số báo của tạp chí Time phát hành ngày 9 tháng 1 năm 1989 có một bài viết với tựa "Technology" (tạm dịch: Công nghệ) có đoạn trích như sau: "Ngay cả nghi phạm nguy hiểm nhất cũng thường được phép sử dụng điện thoại, nhưng Kevin Mitnick thì không – ít nhất là anh ta không được phép nếu không có sự giám sát của cai ngục. Sau đó, anh ta được quyền gọi cho duy nhất vợ, mẹ và luật sư. Lý do là vì đặt điện thoại vào tay Mitnick như thể đưa súng vào tay sát thủ. Một sinh viên đại học 25 tuổi đã bị quan chức liên bang buộc tội sử dụng hệ thống điện thoại để trở thành một trong những nghệ sĩ tấn công hệ thống máy tính đáng gờm nhất mọi thời đại."

"Như thể đưa súng vào tay sát thủ" – là những từ dùng để nói về một người mà vũ khí duy nhất của anh ta là dòng mã máy tính và tấn công bằng kỹ thuật xã hội!

Tôi không có cơ hội nào để bào chữa. Buổi xét xử trước tòa chỉ quan tâm tới một vấn đề duy nhất là quyết định tống giam ban đầu. Trong hệ thống luật pháp liên bang, bạn phải "quay vòng quay" và sẽ có một thẩm phán liên bang được chỉ định ngẫu nhiên. Tôi nghe nói thực ra mình vẫn còn may mắn vì "quay" trúng thẩm phán Mariana Pfaelzer. Không hẳn thế.

Luật sư mới được chỉ định cho vụ của tôi, Alan Rubin, đã cố bào chữa rằng tôi không nên bị tống vào khu biệt giam, vốn chỉ dành cho những tù nhân phạm tội nguy hiểm trong tù và có thể là mối nguy hại tới chính tù lao. Thẩm phán Pfaelzer nói: "Đó mới chính là nơi dành cho cậu ta."

Vậy là tôi được đưa tới Trung tâm Giam giữ Đô thị ở Los Angeles, nơi tôi bị áp tải lên tầng 8, phòng 8 phía Bắc và được giới thiệu ngôi nhà mới của mình, một khoảng không gian chừng 2 mét rưỡi tới 3 mét, với một khe cửa sổ hẹp đứng, mà qua đó tôi có thể thấy xe cộ, ga tàu và mọi người bước qua lại đầy tự do; còn cả khách sạn Metro Plaza mà dù có xập xệ thì trong mắt tôi lúc đó vẫn là thiên đường. Tôi thậm chí không thể thấy cai ngục hay những tù nhân khác, bởi cánh cửa buồng biệt giam là cửa thép kín chỉ có một khe hẹp đủ để khay đồ ăn trượt qua.

https://thuviensach.vn

Nỗi cô đơn khiến tâm trí tôi tê liệt. Tù nhân ở trong "lỗ" suốt thời gian dài thường mất liên hệ với thực tại. Một vài người vĩnh viễn không thể phục hồi và sẽ sống suốt phần đời còn lại trong vùng đất tưởng tượng đầy u ám, mất khả năng sinh hoạt xã hội, mất khả năng đảm nhiệm một công việc nào đó. Để có thể hiểu được điều đó là như thế nào, bạn hay thử mường tượng cảnh bị mắc kẹt 23 giờ mỗi ngày trong một chiếc tủ quần áo được thắp sáng bởi một bóng đèn 40W duy nhất.

Mỗi khi rời phòng giam, dù chỉ để bước chừng 3m tới chỗ tắm rửa, tôi sẽ bị cùm xích cả chân lẫn tay. Đây là cách đối xử hệt như với một phạm nhân vừa tấn công người cai ngục. Để "tập thể dục", tôi lê bước chân một lần mỗi ngày để tới cũi ngoài trời, chỉ rộng cùng lắm gấp đôi phòng giam của mình. Tại đây, tôi có một giờ để hít thở không khí trong lành và chống đẩy vài cái.

Tôi đã sống sót như thế nào? Những cuộc ghé thăm của cha, mẹ, bà và vợ là tất cả những gì tôi mong ngóng. Để cứu rỗi linh hồn mình, tôi cố giữ cho đầu óc hoạt động. Vì không bị tống vào khu biệt giam do vi phạm quy định nhà tù, nên những điều khoản chặt chẽ dành cho phạm nhân tại đây được nới lỏng đôi chút đối với tôi. Tôi có thể đọc sách và tạp chí, viết thư, nghe đài Walkman (kênh yêu thích của tôi là kênh tin tức KNX 1070 và rock cổ điển). Việc viết lách gặp khó khăn vì tôi chỉ được cho một mẩu bút chì ngắn và cùn đến nỗi chỉ có thể dùng được vài phút mỗi lần.

Nhưng dù đơn độc và mặc cho những nỗ lực lớn nhất của phía tòa án, tôi vẫn thực hiện được một chút phone phreaking. Tôi được phép thực hiện cuộc gọi cho luật sư, cha, mẹ và dì Chickie cũng như Bonnie, nhưng chỉ khi nàng ở nhà chứ không phải tại nơi làm việc. Đôi khi tôi thèm khát được nói chuyện với nàng suốt cả ngày. Để được gọi điện, tôi sẽ bị cùm lại và bước tới một hành lang có ba chiếc điện thoại. Cai ngục sẽ tháo bớt cùm xích khi chúng tôi tới được khu vực điện thoại và ngồi cách đó chừng mét rưỡi, nhìn thẳng vào tường treo điện thoại.

https://thuviensach.vn

Gọi điện cho ai đó không nằm trong danh sách tòa cho phép là việc bất khả thi, như kiểu cố gắng hối lộ cai tù vậy – và tôi biết đây là cách ngắn nhất để có được vài đặc quyền mà tôi đã bị cắt bỏ.

Nhưng liệu không có cách nào để tôi có thể gọi cho Bonnie khi nàng ở chỗ làm hay sao? Tôi nghĩ ra một kế hoạch tuy khá liều lĩnh nhưng dù sao thì tôi cũng chẳng còn gì để mất. Tôi đã bị tống vào khu biệt giam, đã bị coi là một mối nguy hại đối với an ninh quốc gia. Tôi đã chạm đáy rồi.

Tôi nói với cai ngục: "Tôi muốn gọi cho mẹ tôi" và anh ta tìm số điện trên sổ. Anh ta bước vài bước tới quay số rồi đưa ống nghe cho tôi. Người phụ trách nghe máy và hỏi tên tôi, sau đó đặt máy cho tới khi mẹ tôi trả lời đồng ý nhận cuộc gọi từ Kevin, và thế là chúng tôi kết nối.

Khi nói chuyện với mẹ, tôi thường cọ cọ lưng mình vào máy điện thoại như thể đang bị ngứa. Cuối buổi nói chuyện, tôi đặt một tay ra sau lưng, giả vờ làm động tác gãi lưng. Trong khi vẫn tiếp tục nói chuyện như thể cuộc đối thoại đang diễn ra, bàn tay sau lưng tôi sẽ giữ móc chuyển đổi[45] trong vài giây để kết thúc cuộc gọi. Sau đó, tôi sẽ thu tay lại đặt trước người.

[45] Móc chuyển đổi (Switch hook): Điện thoại bàn thời trước thường được trang bị một móc chuyển đổi với chuông được gắn vào đường dây điện thoại. Khi thực hiện cuộc gọi, móc chuyển đổi được tách ra, đường dây điện thoại sẽ kết nối tới mạch truyền dẫn của hệ thống điện thoại. Còn khi kết thúc cuộc gọi, móc chuyển đổi được nhấn xuống, đường dây điện thoại sẽ ngắt kết nối. (BTV)

Tôi biết mình chỉ có 18 giây để quay số mới trước khi máy điện thoại phát ra tín hiệu máy bận rất nhanh và ồn ào tới mức cai ngục chắc chắn sẽ nghe thấy.

Do vậy, tôi lại đưa tay ra sau lần nữa và giả vờ gãi lưng, đồng thời nhanh chóng quay bất kỳ số điện nào mà tôi muốn gọi – bắt đầu bằng số 0 để thực

https://thuviensach.vn

hiện cuộc gọi. Tôi thường lắc mình theo nhịp khi gãi lưng, do vậy, cai ngục đã quen thuộc với hành động này và không lấy làm nghi ngờ.

Dĩ nhiên tôi không thể nhìn bảng quay số, do đó tôi phải chắc chắn mình bấm đúng số ngay cả khi không nhìn. Và tôi phải giữ điện thoại áp chặt vào tai để che giấu âm thanh kết nối vào số mới.

Sau một hồi, tôi vẫn hành động như thể đang nói chuyện với mẹ. Tôi gật gù và tạo vẻ trước cái nhìn của gã cai ngục.

Sau khi bấm số, tôi phải thiết kế cuộc trò chuyện giả sao cho thật chuẩn, để khi bên tổng đài nhấc máy và hỏi: "Đã nhận cuộc gọi. Tôi nên nói rằng ai đang gọi?" thì từ kế tiếp tôi phải nói là "Kevin" – trong một câu nghe có vẻ bình thường khi đến tai cai ngục. (Lúc tổng đài hỏi tên, tôi sẽ nói một câu gì đó kiểu như: "Mẹ nhớ nói bác John rằng…" Tổng đài ngừng nói và đợi tôi trả lời, đúng lúc đó tôi sẽ nói: "… KEVIN... gửi lời thăm hỏi.")

Giọng Bonnie cất lên, trái tim tôi đập rộn ràng. Tôi cố kìm nén bản thân, ép mình phải nói bằng giọng điệu kém sôi nổi hơn, như thể đang thực sự nói chuyện với mẹ.

Thành công rồi. Tôi phấn chấn như thể vừa hoàn thành một trận hack hoành tráng.

Lần đầu tiên là khó nhất. Tôi duy trì hoạt động này mỗi ngày. Thực kỳ lạ là tại sao mấy gã cai ngục không mua tặng tôi tuýp kem ngứa.

Vài tuần sau khi tôi bắt đầu mánh khóe này, một đêm cửa phòng giam bật mở khi tôi đang ngủ. Đứng đó là một đám người trong bộ cảnh phục; vài gã cai tù và giám đốc trại giam. Tôi bị còng tay, cùm chân và đẩy đến một phòng họp cách đó chừng 10m. Tôi ngồi xuống, một trong những gã cai ngục lên tiếng: "Mitnick, cậu đã làm vậy bằng cách nào? Làm sao cậu có thể quay số khác?" Tôi giả vờ không hiểu, cho rằng có điên mới thừa nhận điều gì. Cứ để họ tự chứng minh điều đó đi.

https://thuviensach.vn

Giám đốc trại giam chen vào: “Chúng tôi đã theo dõi các cuộc gọi. Cậu quay số bằng cách nào? Cai ngục vẫn luôn để ý đến cậu.” Tôi mỉm cười và nói: “Tôi không phải là David Copperfield – tôi quay số lại thế quái nào được? Mấy tay cai ngục cũng chưa từng rời mắt khỏi tôi.”

Hai ngày sau, tôi nghe thấy tiếng ồn bên ngoài phòng. Đó là kỹ thuật viên đến từ Pacific Bell. Chuyện quái gì vậy? Hắn ta đang lắp một ổ cắm giắc điện thoại trên hành lang phía bên kia phòng tôi, và lần tới khi yêu cầu được gọi điện thoại, tôi đã đoán được tình hình: Tay cai ngục sẽ mang một chiếc điện thoại có dây nối với ống nghe dài tới 6m và cắm vào ổ, quay số điện thoại mà tôi yêu cầu, sau đó chuyển ống nghe qua lỗ cửa sắt vào phòng tôi. Còn bản thân chiếc điện thoại thì nằm xa ngoài tầm với của tôi. Lũ chết tiệt!

Ngoài chuyện nhận các cuộc gọi đến thì Bonnie còn trực tiếp ủng hộ tôi trên nhiều mặt. Ba lần mỗi tuần sau khi tan việc, nàng lái xe cả đoạn đường dài tới nhà tù, đứng xếp hàng rất lâu để tới lượt gặp tôi trong phòng thăm, bên cạnh là cai ngục đứng quan sát cả buổi. Chúng tôi được phép ôm hôn nhanh chóng. Hết sức thành khẩn, tôi không ngừng đảm bảo với nàng rằng đây sẽ là lần cuối mình làm những chuyện tương tự. Và cũng như những lần trước, tôi đã thực sự tin như vậy.

Tôi tiếp tục ngồi yên trong cô độc trong khi luật sư Alan Rubin thương lượng với bên công tố về lý lẽ biện hộ cho phép tôi ra tù mà không bị đưa ra xét xử. Tôi bị buộc tội tấn công vào DEC và chiếm đoạt các mã đăng nhập MCI, gây tổn thất tới 4 triệu đô-la cho DEC – một cáo buộc lố bịch. Tổn thất thực sự của DEC có liên quan tới việc điều tra sự cố; 4 triệu đô-la chỉ là một con số ngẫu nhiên được chọn ra nhằm ép tôi phải nhận mức án ngồi tù lâu dài dựa trên Bản hướng dẫn Tuyên án Liên bang. Án phạt dành cho tôi lẽ ra phải dựa trên mức phí cấp phép của những mã nguồn tôi đã sao chép, con số này thấp hơn rất, rất nhiều.

Dù vậy, tôi vẫn muốn giải quyết cho xong và thoát khỏi phòng giam chẳng khác nào cỗ quan tài kia càng sớm càng tốt. Tôi không muốn có thêm một

https://thuviensach.vn

vụ xét xử bởi tôi biết quan chức liên bang sẽ dễ dàng có đủ bằng chứng để buộc tội tôi: Họ đang nắm trong tay các ghi chép và đĩa mềm, Lenny thì háo hức muốn làm chứng chống lại tôi, họ có đĩa ghi âm từ máy ghi mà Lenny đã đeo trong buổi hacking cuối cùng đó.

Sau cùng, luật sư biện hộ của tôi đã dàn xếp xong xuôi với công tố viên liên bang để đưa ra án tù một năm dành cho tôi. Họ muốn tôi đứng ra làm chứng chống lại Lenny. Điều này khiến tôi bất ngờ, vì tôi vẫn nghe rằng kẻ quay đầu trước tiên sẽ thoát tội một cách dễ dàng, có khi còn chẳng phải ngồi tù. Nhưng giờ đây họ lại muốn tôi quay lại cắn trả kẻ chỉ điểm cho mình, người bạn cũ của tôi. Được, tôi nói. Lenny đã tung bằng chứng chống lại tôi, tại sao tôi lại không đền đáp hắn ta thật hậu hĩnh cơ chứ?

Nhưng khi chúng tôi ra tòa, thẩm phán Pfaelzer hiển nhiên đã bị ảnh hưởng lớn bởi rất nhiều tin đồn và cáo buộc vô lý về tôi. Bà bác bỏ thỏa thuận nhận tội của tôi, cho rằng như vậy thì quá khoan dung. Dù vậy, bà đồng ý với một phiên bản thỏa thuận khác, trong đó tôi sẽ phải ngồi tù một năm và sau đó là nửa năm ở trung tâm tái hòa nhập dành cho phạm nhân mới ra tù. Ngoài ra, tôi được yêu cầu nói cho Andy Goldstein của DEC biết tôi đã hack vào DEC và sao chép hầu hết mã nguồn của họ như thế nào.

Ngay khi tôi chấp thuận thỏa thuận nhận tội, trạng thái “mối nguy hại đối với an ninh quốc gia” đã bị gỡ bỏ một cách thần kỳ. Tôi được chuyển từ khu biệt giam tới phòng giam dành cho tù nhân thông thường. Mới đầu, tôi có cảm giác thật tuyệt như thể mình đã được tự do vậy, nhưng sau đó, thực tại nhanh chóng nhắc nhở tôi rằng đây vẫn là nhà tù.

Khi tôi ở khu vực tù chung thuộc nhà giam Metropolitan Detention Center, bạn tù của tôi, một gã đầu sỏ buôn thuốc phiện người Colombia, đã đề nghị cho tôi 5 triệu đô-la nếu tôi có thể hack vào Sentry, hệ thống máy tính của Cục Giam giữ Liên bang và giúp gã được thả tự do. Tôi vờ chấp thuận để giữ mối quan hệ hòa hảo với gã, nhưng tuyệt đối không định làm theo ý gã.

https://thuviensach.vn

Rất nhanh chóng, tôi được chuyển tới trại tù liên bang ở Lompoc. Nơi đây quả là một sự khác biệt: có ký túc xá thay vì phòng giam, thậm chí còn không có cả hàng rào bao quanh. Tôi sống cùng những cái tên khét tiếng trong giới tội phạm cổ cồn trắng. Bạn tù của tôi thậm chí còn có cả cựu thẩm phán liên bang bị kết tội trốn thuế.

Tôi lên cân vù vù, đạt mức 109kg, trong khoảng thời gian biệt giam do sống chủ yếu dựa vào nguồn thực phẩm có tính an ủi từ cửa hàng bách hóa trong tù với những loại đồ ăn như thanh kẹo Hershey phủ bơ lạc. Này, chẳng phải lúc bạn cô đơn quạnh quẽ, bất kỳ thứ gì có thể khiến bạn cảm thấy khá hơn đều tốt sao?

Nhưng giờ đây, tại Lompoc, một bạn tù khá dễ thương có tên Roger Wilson đã thuyết phục tôi đi bộ và tập thể dục nhiều hơn, cũng như giữ thói quen ăn uống thực phẩm lành mạnh như gạo, rau… Lúc bắt đầu thực sự rất khó khăn, nhưng với sự động viên của anh ấy, tôi đã thành công. Chính những thay đổi trong phong cách sinh hoạt đã giúp tôi như được tái sinh, ít ra là về mặt hình ảnh cơ thể.

Một lần, khi tôi đang ngồi trên băng ghế gỗ chờ tới lượt dùng điện thoại, Ivan Boesky tới ngồi cạnh tôi, trên tay là một cốc cà phê. Mọi người đều biết gã là ai: triệu phú một thời, thiên tài tài chính bị kết tội giao dịch nội gián[46]. Hóa ra gã cũng biết tôi. “Này, Mitnick,” gã mở lời, “cậu kiếm được bao nhiêu từ việc tấn công mấy cái máy tính đó?”

[46] Giao dịch nội gián (insider trading): Là hoạt động mua hoặc bán chứng khoán bởi một người có khả năng tiếp cận các thông tin bí mật, chưa được công bố về loại chứng khoán đó. Việc mua bán nội bộ có thể bị coi là phạm pháp hay không phụ thuộc vào thời gian mà hành động này được thực hiện. Nó là phạm pháp nếu các thông tin, tài liệu vẫn chưa được công bố ra ngoài vì như vậy sẽ không công bằng đối với các nhà đầu tư khác không nắm được các thông tin này. Những người thực hiện mua bán nội bộ thường sẽ phải trả tiền để mua lại bất kỳ thông tin nào chưa được công bố. (BTV)

https://thuviensach.vn

“Tôi không làm vì tiền; tôi làm chỉ để giải trí thôi,” tôi trả lời.

Gã nói gì đó kiểu như: “Cậu bị tống vào tù và cậu chẳng kiếm được xu nào. Như thế không phải là quá ngu xuẩn à?” Chính trong khoảnh khắc gã đang nhìn tôi đầy khinh miệt, tôi vô tình trông thấy một con gián nổi lều phều trong cốc cà phê của gã. Tôi mỉm cười, chỉ vào nó và nói: “Ở đây chẳng giống như Helmsley nhỉ?”

Boesky không đáp lại. Gã đứng dậy và bước thẳng.

Sau gần bốn tháng ở Lompoc, tôi chuẩn bị được chuyển tới trung tâm tái hòa nhập Beit T’Shuvah. Tôi nghe nói đó là tên tiếng Do Thái, có nghĩa là “Ngôi nhà của sự trở về”. Beit T’ Shuvah có chương trình 12 giai đoạn dành cho những người nghiện thuốc, rượu và các thói gây nghiện khác.

Lần chuyển chỗ tới trung tâm tái hòa nhập là một tin tốt. Tin xấu là một nhân viên quản chế đã gọi cho Bonnie để đặt lịch “kiểm tra” căn hộ nàng đang sống, với lời giải thích rằng hắn ta phải xét duyệt chỗ ở tương lai của tôi trước khi tôi được thả. Với Bonnie, đây là giọt nước cuối cùng làm tràn ly. Nàng cảm thấy mình không thể chịu đựng thêm được nữa. “Anh không cần phải khám nhà tôi,” nàng nói với gã. “Chồng tôi sẽ không sống ở đây.” Trong lần thăm sau đó, nàng nói với tôi tin xấu: Nàng đã nộp đơn ly hôn.

Nàng nói: “Đúng là thời điểm vô cùng đau đớn với em. Em nghĩ mình đã gục ngã. Điều đó thật đáng sợ. Em sợ viễn cảnh phải xa anh, nhưng cũng quá sợ hãi để ở lại. Nỗi sợ đó trở nên quá lớn.”

Tôi sững sờ. Chúng tôi đã lên kế hoạch sống bên nhau trọn đời và giờ nàng đổi ý ngay khi tôi sắp được thả ra. Tôi cảm thấy như thể cả tấn gạch nện vào người. Tôi thực sự đau đớn và hoàn toàn choáng váng.

Bonnie đồng ý tới trung tâm tái hòa nhập để tham dự vài buổi tư vấn hôn nhân cùng tôi. Nhưng chẳng ích gì.

https://thuviensach.vn

Tôi thực sự thất vọng về quyết định chấm dứt của Bonnie. Đâu là nguyên nhân khiến trái tim nàng thay đổi? Hẳn phải có một gã khốn nào đó – một ai đó trong ảnh. Tôi nghĩ mình có thể tìm ra đó là ai bằng cách kiểm tra các tin nhắn trên máy trả lời điện thoại của nàng. Tôi thấy mình thật tệ hại khi làm việc này, nhưng tôi muốn biết sự thật.

Tôi biết máy trả lời tin thoại của Bonnie là một sản phẩm của Radioshack bởi tôi đã nhận ra tiếng chuông vang lên khi đề nghị người gọi để lại tin nhắn. Tôi cũng biết chính xác dòng máy này, bạn có thể lấy lại tin nhắn từ xa trong điều kiện có được thiết bị cầm tay đi kèm với máy, thiết bị này sẽ phát ra một cụm âm thanh đặc biệt để khởi động bộ phát phát lại. Làm sao tôi có thể xử lý chuyện này và nghe được tin nhắn của nàng mà không dùng tới máy bấm từ xa kia?

Tôi gọi cho cửa hàng Radioshack và mô tả dòng máy trả lời thoại của Bonnie, sau đó nói thêm rằng tôi bị mất thiết bị điều khiển từ xa kia và cần mua cái mới. Nhân viên bán hàng trả lời có bốn loại máy bấm có thể dùng cho nhiều loại model của máy trả lời tin thoại kia – A, B, C và D – mỗi loại lại có một chuỗi âm báo khác nhau. Tôi nói: “Tôi là nhạc công, tai tôi rất thính.” Anh ta muốn tôi trực tiếp tới cửa hàng, nhưng tôi không thể rời trung tâm bởi những người mới đến không được phép rời đi trong 30 ngày đầu tiên. Tôi khẩn khoản đề nghị anh ta mở hộp các mẫu thiết bị, lắp pin vào và bật điều khiển cho tôi nghe.

Sự kiên trì của tôi đã được đền đáp: Tay bán hàng rất chịu khó lắp bốn loại điều khiển và bật từng âm báo lên cho tôi. Tôi chạy máy thu âm trong suốt khoảng thời gian đó, ấn chặt vào ống nghe điện thoại để ghi vào băng cát-sét.

Kế tiếp, tôi gọi vào máy Bonnie và bật âm vừa thu qua điện thoại. Âm thứ ba có tác dụng. Tôi nghe thấy Bonnie để lại tin nhắn trên máy của chính nàng, có lẽ là từ công ty. Khi cuộc gọi kết nối, một gã nào đó trong căn hộ

https://thuviensach.vn

của nàng nhấc máy và máy thu âm ghi lại cuộc nói chuyện từ cả hai đầu dây, nàng nói với gã ta về việc "thời gian bên anh thật tuyệt".

Nghe lén tin nhắn của Bonnie là một việc làm ngu ngốc bởi nó khiến nỗi đau trong lòng tôi càng trở nên tồi tệ hơn rất nhiều. Nhưng điều đó đã khẳng định mối nghi ngờ của tôi. Tôi vô cùng giận dữ vì nàng đã nói dối. Tôi cũng tuyệt vọng đến mức định trốn khỏi trung tâm để đi gặp nàng. Thực may mắn khi tôi biết kiềm lòng với suy nghĩ đó hắn phải là một sai lầm lớn nếu phạm phải.

Khi tháng đầu tiên kết thúc, tôi được phép rời trung tâm tới vài buổi hẹn và chuyến thăm định sẵn. Tôi thường tới thăm Bonnie, cố gắng giành lại nàng. Tại một trong những buổi ghé thăm đó, tôi nhận ra nàng vô ý để quên hóa đơn điện thoại tháng trước trên bàn. Nó cho thấy nàng đã nói chuyện điện thoại hàng giờ với Lewis De Payne, người đến tận giây phút đó tôi vẫn nghĩ là bạn thân thiết nhất của mình.

Đương nhiên, tôi phải tìm ra câu trả lời chắc chắn. Tôi hỏi vu vơ rằng liệu nàng có nghe được tin tức gì về những người bạn của tôi không, như Lewis chẳng hạn.

Nàng nói dối, thẳng thừng phủ nhận việc đã từng liên lạc với hắn ta – và điều này đã khẳng định nỗi sợ hãi lớn nhất trong lòng tôi. Nàng đã giáng một đòn thật mạnh vào tâm trí tôi. Còn đâu niềm tin tôi vẫn đặt trọn vẹn vào nàng? Tôi vạch rõ mọi chuyện để thẳng thắn nhưng rồi chúng cũng chẳng đi tới đâu cả. Tôi đã thất bại hoàn toàn. Liếm láp vết thương trên mình, tôi bỏ đi và cắt đứt liên lạc với nàng trong một thời gian dài.

Không lâu sau, nàng chuyển đến sống cùng Lewis. Với tôi, chuyện này chẳng có nghĩa lý gì: Nàng đã rời bỏ một con nghiện hacking để đến bên một gã khác với khuynh hướng tương tự. Nhưng điều quan trọng hơn cả là Bonnie không phải chỉ là bạn gái của tôi, nàng còn là vợ tôi. Và giờ đây, nàng lại đến với người bạn thân nhất của tôi.

https://thuviensach.vn

Sau khi được tại ngoại, tôi chuyển từ thói nghiện hacking sang một thói nghiện khác: Tôi bị ám ảnh với việc tập gym và ngày nào cũng vùi mình trong phòng tập vài tiếng.

Tôi cũng tìm được một công việc ngắn hạn trong ba tháng, trở thành nhân viên hỗ trợ kỹ thuật cho một công ty có tên Case Care. Khi tôi xong việc, giám sát viên đồng ý để tôi chuyển tới Las Vegas, nơi mẹ tôi đang sống và sẵn lòng chào đón tôi tới ở với bà cho tới khi tìm được chốn riêng.

Sau nhiều tháng, tôi giảm được 45kg và đạt được hình thể tuyệt nhất trong đời. Tôi đã không còn hacking nữa. Tôi cảm thấy mọi thứ thật tuyệt. Nếu bạn hỏi tôi lúc đó, tôi hẳn sẽ nói rằng những ngày tháng hacking đã lùi sâu vào quá khứ.

Đó là những gì tôi nghĩ lúc đó.

https://thuviensach.vn

09

GÓI CƯỚC GIẢM GIÁ KIỂU KEVIN MITNICK

Hsle td esp epcx qzc dzqehlcp mfcypo zy esp nsta esle Yzglepw dpye xp?

Hãy tưởng tượng một khu triển lãm rộng tới 200.000m2, ních chặt 200.000 người, ồn ào như thể tất cả đều đang nói cùng lúc, chủ yếu là tiếng Nhật, tiếng Đài Loan và tiếng Quan Thoại. Đó chính là quang cảnh tại Trung tâm Hội nghị Las Vegas năm 1991 trong thời gian diễn ra Triển lãm Điện tử Tiêu dùng (CES) hằng năm – hệt như một cửa hàng kẹo thu hút một trong những đám đông lớn nhất thế giới.

Tôi đã đi qua cả thành phố để đến đây trong ngày diễn ra triển lãm, không chỉ đơn giản để thăm các gian hàng hay nhìn ngắm những đồ dùng điện tử làm lóa mắt khách hàng dịp Giáng sinh. Tôi đến đây vì tạp âm môi trường. Nó rất cần thiết để nâng độ tin cậy cho cuộc gọi mà tôi chuẩn bị thực hiện.

Đây là một thử thách: Tôi có Novatel PTR-825, một trong những chiếc điện thoại di động hot nhất thị trường lúc đó. Tôi muốn an tâm nói chuyện với bạn bè mà không phải băn khoăn xem liệu có ai từ FBI hay lực lượng chấp pháp địa phương đang nghe lén hay không. Tôi biết có một cách khả thi. Giờ thì tôi sẽ thử tìm hiểu xem kế hoạch này có thực sự hiệu quả không.

Kế hoạch dựa trên một mánh khóe dùng mã sê-ri[47] điện tử của điện thoại, hay còn gọi là "ESN". Tất cả hacker đều biết, mỗi chiếc điện thoại đều có một ESN riêng biệt, ESN này sẽ được chuyển đi cùng số điện thoại di động, hay còn gọi là MIN, đến trạm thu phát sóng gần nhất. Đó là một phần trong

https://thuviensach.vn

quy trình xác thực của công ty điện thoại xem người gọi có phải là một thuê bao hợp lệ hay không và nên thu cước phí cuộc gọi từ ai.

[47] Mã sê-ri (Serial number): Mã hàng hóa do nhà sản xuất quy định để quản lý hàng hóa sản xuất và trong bảo hành sản phẩm. (BTV)

Nếu tôi có thể sửa chiếc điện thoại của mình sao cho nó sẽ gửi đi MIN và ESN của các thuê bao hợp lệ khác, những cuộc gọi của tôi sẽ tuyệt đối an toàn: Tất cả nỗ lực theo dấu cuộc gọi sẽ dẫn đến một người khác, người sở hữu điện thoại thực gán với ESN mà tôi đã dùng lúc đó. (Thuê bao đó cũng sẽ phải giải thích với công ty điện thoại rằng anh ta không hề thực hiện những cuộc gọi phụ trội vừa bị tính cước, và anh ta sẽ không phải chịu trách nhiệm trả tiền cước cho những cuộc gọi không hợp lệ đó.)

Từ máy điện thoại công cộng ở Trung tâm Hội nghị, tôi gọi đến một số máy ở Calgary, Alberta, Canada. “Novatel,” một giọng phụ nữ vang lên phía bên kia dây.

“Xin chào,” tôi nói. “Tôi cần nói chuyện với người ở bộ phận Kỹ thuật.”

“Anh gọi từ đâu vậy?” cô ta muốn biết.

Như mọi khi, tôi đã nghiên cứu trước. “Tôi thuộc đội Kỹ thuật ở Fort Worth.”

“Anh nên nói chuyện với quản lý kỹ thuật, Fred Walker, nhưng hôm nay anh ấy không ở đây. Tôi có thể lấy số của anh và Walker sẽ gọi lại cho anh vào ngày mai được chứ?”

“Việc này rất gấp,” tôi nói. “Hãy cho tôi nói chuyện với bất cứ ai có mặt ở bộ phận của anh ấy.”

Lát sau, một người đàn ông có ngữ điệu Nhật Bản nhấc máy và nói anh ta tên là Kumamoto.

https://thuviensach.vn

“Kumamoto-san[48], tôi là Mike Bishop từ Fort Worth,” tôi nói, dùng một cái tên mà tôi vừa đọc được từ bảng tin điện tử tại CES. “Tôi thường nói chuyện với Fred Walker, nhưng hôm nay anh ấy lại không ở đây. Tôi đang tham dự CES ở Vegas.” Tôi cho rằng tạp âm môi trường thực tế sẽ làm cho câu nói của tôi đáng tin hơn. “Chúng tôi đang thử nghiệm để trình diễn sản phẩm. Anh có cách nào để đổi ESN từ bàn phím điện thoại không?”

[48] Trợ từ trong xưng hô của người Nhật, thể hiện sự tôn trọng với người đối diện. (BTV)

“Hoàn toàn không. Việc này trái với quy định của Ủy ban Truyền thông Liên bang (FCC).”

Chán thật. Ý tưởng vĩ đại của tôi vừa bị bắn hạ.

Không, đợi đã. Kumamoto-san vẫn đang nói.

“Chúng tôi có một phiên bản firmware[49] đặc biệt, phiên bản 1.05. Nó sẽ cho phép anh đổi ESN từ bàn phím điện thoại nếu anh biết các bước lập trình bí mật.”

[49] Firmware: Phần mềm hệ thống, chương trình máy tính cố định quy định các quy trình cơ bản, cấp thấp của thiết bị. (ND)

Bỗng nhiên tôi trở lại cuộc chơi. “Firmware” của một chiếc điện thoại chính là hệ điều hành của nó, được nhúng trên một dạng chip máy tính đặc biệt có tên là EPROM.

Mánh khóe lúc này là không được để lộ sự phấn khích trong giọng nói. Tôi hỏi một câu nghe có vẻ như một thử thách: “Tại sao nó lại cho phép đổi ESN?”

“FCC yêu cầu để thử nghiệm,” anh ta nói.

https://thuviensach.vn

“Tôi phải làm gì để có được một bản sao?” Tôi nghĩ có thể anh ta sẽ gửi cho tôi một chiếc điện thoại có phiên bản firmware đặc biệt đó.

“Tôi có thể gửi anh con chip,” anh ta nói. “Anh có thể thay nó vào điện thoại.”

Tuyệt vời! Việc này có khi còn hay hơn cả việc có một chiếc điện thoại hoàn toàn mới, nếu tôi có thể ép anh chàng này thêm chút nữa.

“Anh có thể ghi 4 hoặc 5 EPROM cho tôi được không?”

“Được chứ.”

Tuyệt thật, nhưng giờ tôi đang gặp một trở ngại: Làm thế nào tôi có thể nhờ họ chuyển chúng cho mình mà phải không đưa tên thật và địa chỉ chuyển phát có thể bị theo dõi?

“Hãy ghi chúng ra cho tôi,” tôi bảo anh ta. “Tôi sẽ gọi lại cho anh sau.”

Tôi khá chắc rằng những con chip này sẽ khiến tôi trở thành người duy nhất ngoài Novatel có thể đổi mã số điện thoại Novatel chỉ bằng cách bấm phím. Không chỉ giúp tôi có thể gọi điện thoại miễn phí, nó còn mang lại cho tôi một chiếc áo choàng tàng hình, giúp đảm bảo các cuộc hội thoại của tôi sẽ hoàn toàn riêng tư. Và nó cũng sẽ cho tôi một số gọi lại an toàn bất cứ khi nào tôi muốn tấn công bằng kỹ thuật xã hội với công ty mục tiêu.

Nhưng làm thế nào tôi có thể yêu cầu chuyển món hàng cho mình mà không bị tóm?

Nếu ở trong hoàn cảnh của tôi lúc đó, các bạn sẽ sắp xếp thế nào để lấy được những con chip đó? Hãy thử nghĩ xem.

Câu trả lời không khó. Tôi lập tức vạch ra một kế hoạch gồm hai phần trong đầu. Tôi gọi lại cho Novatel lần nữa và tìm gặp thư ký của Fred Walker. Tôi nói với cô ta: “Kumamoto-san ở phòng kỹ thuật sẽ đem vài thứ tới cho tôi.

https://thuviensach.vn

Tôi đang làm việc với người của chúng ta ở gian hàng tại CES, nhưng tôi sẽ về Calgary hôm nay. Tôi sẽ qua và lấy nó vào buổi chiều."

Kumamoto-san đang bận ghi chip cho tôi khi tôi gọi lại cho anh ta và nhờ anh ta gói chúng lại khi xong việc rồi để ở chỗ thư ký của Walker. Sau khi dành vài tiếng đi lang thang trong khu vực hội nghị, chìm đắm trong những điều mới mẻ của thế giới điện tử và điện thoại, tôi đã sẵn sàng cho bước tiếp theo.

Khoảng 20 phút trước khi bế mạc (đồng hồ ở Calgary chạy nhanh hơn Las Vegas một tiếng), tôi gọi lại cho nhân viên thư ký kia một lần nữa. "Tôi đang ở sân bay trên đường về Las Vegas khẩn cấp – họ gặp rắc rối ở gian hàng. Gói hàng mà Kumamoto-san để lại cho tôi, cô có thể chuyển FedEx đến khách sạn của tôi ở đây được không? Tôi đang ở Circus Circus." Trước đó, tôi đã đặt phòng cho hôm sau ở Circus Circus với cái tên "Mike Bishop"; nhân viên lễ tân thậm chí còn không buồn hỏi thẻ tín dụng của tôi. Tôi đưa cho nhân viên thư ký địa chỉ của khách sạn và đánh vần tên Mike Bishop để đảm bảo cô ta đã nghe đúng.

Tôi lại thực hiện một cuộc gọi nữa đến Circus Circus, giải thích rằng mình sẽ đến trễ và cần đảm bảo rằng bàn lễ tân sẽ nhận gói hàng FedEx được chuyển đến cho tôi trước khi tôi nhận phòng. "Tất nhiên rồi, ông Bishop. Nếu đó là một bưu phẩm lớn, người trực tầng sẽ để nó trong phòng chứa đồ. Nếu chỉ là một bưu phẩm nhỏ, chúng tôi sẽ giữ nó ở bàn lễ tân." Không vấn đề gì.

Trong cuộc gọi tiếp theo, tôi tìm đường đến một khu vực yên tĩnh và bấm số máy đến cửa hàng Circuit City yêu thích của tôi. Khi gặp nhân viên phụ trách quầy điện thoại di động, tôi nói: "Tôi là Steve Walsh, đến từ công ty LA Cellular. Chúng tôi đang gặp sự cố máy tính trong hệ thống kích hoạt. Các anh có kích hoạt chiếc điện thoại nào trên LA Cellular trong hai giờ vừa qua không?"

https://thuviensach.vn

Có, cửa hàng đã bán bốn điện thoại. “Hừm, xem nào,” tôi nói. “Tôi cần các anh đọc cho tôi số điện thoại và ESN của mỗi chiếc để chúng tôi có thể kích hoạt lại số của họ trên hệ thống. Chúng ta không muốn làm khách hàng thất vọng, đúng không?” Tôi cười ra vẻ châm biếm và anh ta đã đọc cho tôi các con số.

Vậy là giờ tôi có bốn ESN và số điện thoại đi kèm với chúng. Cuộc chờ đợi kéo dài đến hết buổi chiều quả thực rất tra tấn thần kinh. Tôi không biết liệu mình có thể thực hiện vụ này trót lọt hay không. Liệu người của Novatel có đánh hơi thấy điều gì mờ ám và không gửi các con chip đi không? Liệu có nhân viên FBI nào đang mai phục ở sảnh khách sạn, đợi bắt tôi không? Hay sau buổi chiều hôm đó, liệu tôi có khả năng đổi số điện thoại di động thường xuyên như mong muốn không?

Ngày hôm sau, anh bạn cũ Alex Kasperavicius đến. Anh là một người thông minh, thân thiện và là chuyên gia trong lĩnh vực IT cùng các hệ thống điện thoại. Alex thích cảm giác phiêu lưu khi được mời tham gia vào những lần khai thác lỗ hổng của tôi, nhưng anh không hẳn là một chiến hữu hacking. Tôi có thể lì lợm bám lấy một nỗ lực tháng này qua tháng khác cho đến khi thành công nhưng Alex thì không; anh có những mối bận tâm khác. Anh khiến mình bận rộn với công việc cố vấn học viện ở Griffith Park, chơi nhạc cổ điển bằng chiếc kèn Pháp và tìm kiếm những cô bạn gái mới.

Tôi cho anh biết tình hình. Nhìn thấy phản ứng của Alex mới khoái làm sao! Lúc đầu là sự ngờ vực nhà sản xuất sẽ không gửi con chip đi, sau đó là tưởng tượng viễn cảnh tuyệt vời khi chúng tôi thực sự có thể thực hiện cuộc gọi mà không để lộ thân phận thật.

Kumamoto-san đã cung cấp cho tôi hướng dẫn lập trình để cài một ESN mới vào điện thoại, sử dụng một phiên bản firmware đặc biệt. Giờ đây, sau gần 20 năm, tôi vẫn có thể nhớ chính xác mã đó:

Function-key

https://thuviensach.vn

Function-key

#

39

#

Last eight digits of the new ESN

#

Function-key

(Dành cho những ai tò mò về mặt kỹ thuật, mã ESN thực chất là một dãy số gồm 11 chữ số thập phân, ba chữ số đầu tiên sẽ cho biết tên của nhà sản xuất điện thoại. Với con chip và mã này, tôi có thể tái lập trình bất kỳ một ESN Novatel nào vào điện thoại, nhưng không thể từ một nhà sản xuất điện thoại khác – dù sau này khi tôi đã có được mã nguồn của Novatel thì điều đó lại hoàn toàn khả thi).

Vào lúc 3 giờ chiều, khá chắc chắn là FedEx đã mang hàng đến Circus Circus, chúng tôi không kìm được sự háo hức nữa. Alex tình nguyện đến lấy hàng, không cần nói cũng biết nếu tôi đến và cảnh sát đang đợi ở đó, tôi sẽ phải quay lại nhà tù. Tôi dặn Alex hãy nói tên mình là Mike Bishop, anh phải trực tiếp đem gói hàng đến Trung tâm Hội nghị và sẽ quay lại đăng ký nhận phòng sau. Tôi đứng đợi ở ngoài.

Trong tình huống này, luôn có khả năng có ai đó nhìn thấu được tất cả mưu mẹo và báo với FBI. Cả hai chúng tôi đều biết Alex có thể sẽ sa bẫy. Ngay từ khi bước vào, anh đã phải nhìn ngó khắp khu vực để tìm những người có khả năng là cảnh sát mặc thường phục. Nhưng anh không thể soi xét kỹ tất cả mọi người, những người có vẻ chỉ đang ngồi giết thời gian; như thế quá khả nghi. Anh phải nhìn lướt qua.

https://thuviensach.vn

Alex rất ngầu khi không cần phải nhìn ngó trước sau hay tỏ vẻ bồn chồn lo lắng. Nếu có gì không ổn, anh sẽ bước ra ngay lập tức – không phải theo kiểu vội vã rõ ràng, nhưng cũng không lề mề.

Cứ mỗi phút trôi đi, tôi lại càng thêm lo lắng. Phải mất bao thời gian để lấy một bưu phẩm nhỏ đây? Được rồi, tôi nghĩ, hãy bình tĩnh lại, hẳn là có rất nhiều người đang xếp hàng ở quầy lễ tân và anh ấy phải đợi đến lượt.

Thời gian tiếp tục trôi đi. Tôi bắt đầu nghĩ mình sẽ phải tự vào xem có đám đông cảnh sát nào không, hay đi hỏi một vị khách casino xem liệu có vụ nào liên quan đến cảnh sát vài phút trước không.

Nhưng Alex đã ở đó, bước ra khỏi cửa, nhàn nhã tiến về phía tôi với nụ cười rạng rỡ trên mặt.

Lòng ngập tràn mong chờ, tim đập thình thịch, chúng tôi đứng ngay giữa đường mở bưu phẩm. Bên trong là một chiếc hộp nhựa màu trắng, đúng như dự đoán, cùng năm EPROM điện thoại 27C512. Tôi đã tiến hành tấn công bằng kỹ thuật xã hội vài năm qua, nhưng đây có lẽ là chiến lợi phẩm lớn nhất cho đến lúc đó nếu những con chip thực sự hoạt động. Chúng tôi băng qua Đại lộ Las Vegas để đến Peppermill, tránh xa những quán cocktail đầy khách du lịch với mấy ả bồi bàn khiêu gợi để tìm một quán giải khát trong khu nhà hàng, nơi chúng tôi trông có vẻ đỡ khả nghi hơn.

Lewis De Payne tham gia với chúng tôi. Phải, giờ cậu ta là người yêu của vợ cũ của tôi.

Tôi không chắc mình có thể giải thích được lý do vì sao tôi vẫn giữ liên lạc với Lewis sau khi đã bị cậu ta cướp mất vợ. Rõ ràng, tôi không bao giờ có thể tin tưởng hay tôn trọng cậu ta thêm một lần nào nữa. Nhưng thực lòng mà nói, có rất ít người tôi dám giữ liên lạc và vì thế, tôi cần ai đó hiểu được những khó khăn trước đó của mình. Và ai có thể hiểu được những điều đó hơn Lewis? Cậu ta đã là bạn hacking của tôi từ những ngày đầu. Chúng tôi đã cùng trải qua rất nhiều chuyện.

https://thuviensach.vn

Chẳng có gì lạ khi tôi chỉ nghĩ về Lewis với niềm cay đắng, hay nhìn nhận cậu ta như kẻ thù không đội trời chung. Cậu ta chắc chắn thừa đủ điều kiện. Nhưng cùng lúc, Lewis cũng thực sự là một trong những người bạn tốt nhất của tôi. Và Bonnie là một người bạn tốt nhất khác. Cuối cùng, tôi đã vượt qua niềm đau và bắt đầu gặp lại họ. Chúng tôi dần trở thành những người bạn, giống như những cặp vợ chồng đã ly hôn cùng những đứa con cuối cùng lại có dịp đi picnic với nhau cùng người bạn đời mới của họ trong những kỳ nghỉ gia đình.

Chúng ta thường được khuyên rằng "hãy quên đi và tha thứ". Trong trường hợp này, "tha thứ" nghe có vẻ hơi quá. Tôi phải buông bỏ nỗi phẫn uất vì chính bản thân, nhưng tôi cũng không thể cố quên. Dù Lewis là một chiến hữu hacking tốt và tôi trân trọng kỹ năng của cậu ta, nhưng tôi chỉ hack chung khi có một chốt an toàn – khi cả hai chúng tôi sẽ đều bất lợi nếu cậu ta dám tố cáo tôi.

Với những điều kiện mới đó, Lewis và tôi đã quay lại hacking cùng nhau và tạo ra một kiểu tình bạn mới vốn đã thay đổi mãi mãi giữa hai chúng tôi.

Giờ đây, trong quán giải khát ở Peppermill, tôi nghĩ Lewis chắc phải trố mắt khi nhìn thấy những con chip. Cậu ta nhanh chóng ngồi xuống và bắt đầu tháo tung chiếc điện thoại của tôi, cẩn thận sắp xếp lại các bộ phận lên bàn và ghi chép lại các chi tiết vào một cuốn sổ để biết cái gì nằm ở đâu khi đã sẵn sàng lắp mọi thứ lại với nhau.

Chưa đầy năm phút, Lewis đã tháo tung chiếc điện thoại, tháo đến bo mạch chính, làm lộ ra con chip được gắn cố định bởi một chân cắm ZIF (chân cắm không cần lực). Tôi đưa cho cậu ta một con chip mới. Lewis gài nó vào vị trí và bắt đầu lắp ráp lại cẩn thận. Tôi không muốn nói bất cứ điều gì có thể khiến cậu ta phân tâm, nhưng tôi bắt đầu thấy bồn chồn, chỉ mong cậu ta làm nhanh lên một chút để tôi có thể biết mình có đào trúng mỏ vàng hay không.

https://thuviensach.vn

Ngay khi mọi thứ được lắp lại hoàn chỉnh, tôi giật lấy chiếc điện thoại và bấm mã chức năng mà Kumamoto-san đã đưa. Để thử nghiệm, tôi lập trình ESN và đổi số điện thoại sao cho trùng với số của điện thoại Lewis.

Chiếc điện thoại tự tắt và khởi động lại. Tôi có thể cảm thấy từng mạch máu chảy rần rật dưới da đầu. Chúng tôi chụm đầu vào bàn, chăm chú nhìn vào màn hình nhỏ xíu của chiếc điện thoại.

Điện thoại sáng lên với màn hình khởi động. Tôi bấm vào lệnh hiển thị ESN của điện thoại. Con số hiện lên là ESN mà tôi đã nhập vào trước đó.

Cả ba chúng tôi reo vang, không quan tâm đến những vị khách khác đang quay lại nhìn.

Nó hoạt động! Nó thực sự hoạt động!

Ngày đó, một số công ty điện thoại có một số máy mà bạn có thể gọi tới để biết giờ giấc chính xác. Tôi bấm 213 853-1212 và đặt điện thoại xuống bàn. Cả ba chúng tôi cùng nghe thấy giọng ghi âm của một phụ nữ: “Sau tiếng chuông này thời gian trong ngày sẽ là...” Điện thoại của tôi đã thực hiện thành công một cuộc gọi đi như một bản sao điện thoại của Lewis – và công ty điện thoại sẽ ghi lại những cuộc gọi này được thực hiện bởi Lewis, từ máy của cậu ta chứ không phải của tôi.

Tôi đã tấn công bằng kỹ thuật xã hội với Novatel và lấy được một quyền năng khổng lồ. Tôi có thể thực hiện các cuộc gọi mà không ai có thể truy ngược được mình.

Nhưng tôi đã sa ngã chỉ để hack duy nhất một lần này... hay tôi mới chỉ bắt đầu hacking lại lần nữa? Ngay lúc đó, tôi cũng không dám chắc.

Dù sao, tôi cũng biết chắc rằng mình đã có được chiếc áo khoác tàng hình.

https://thuviensach.vn

10
HACKER BÍ ẨN

Bprf cup esanqneu xmm gtknv amme U biiwy krxheu Iwqt Taied?

"Trông em tuyệt lắm!”

Cô nàng đáp lại: “Anh cũng vậy.”

Đây quả là liều thuốc cho lòng tự cao của tôi! Trước đây, chưa ai từng nói với tôi điều tương tự, thậm chí là Bonnie. Và đương nhiên bao gồm cả cô gái trẻ đẹp nhường này với cơ thể, khuôn mặt và mái tóc khiến tôi mường tượng ra cảnh nàng đang đứng trên sân khấu của một sòng bạc nào đó, ưỡn ngực trên đôi giày cao gót lênh khênh và bộ đồ thiếu vải. Hoặc… nửa bộ đồ.

Nàng chạy trên một chiếc StairMaster 6000, mồ hôi nhễ nhại. Tôi trèo lên chiếc kế bên và chủ động bắt chuyện. Nàng tỏ ra thân thiện đủ để đem tới cho tôi chút mong đợi. Nhưng niềm vui ngắn chẳng tày gang. Nàng nói mình là vũ công làm cùng Siegfried và Roy – cặp ảo thuật gia nổi tiếng chuyên thực hiện những trò ảo thuật thị giác cỡ lớn và dùng tới cả con hổ thật.

Hiển nhiên, tôi muốn biết họ đã thực hiện những mánh khóe của mình như thế nào. Bất kỳ một nhà ảo thuật nào cũng muốn điều đó. Tôi bắt đầu dò hỏi. Nàng ném cho tôi ánh nhìn “Biến đi” đầy lạnh lẽo và nói: “Tôi phải ký thỏa thuận bảo mật thông tin. Tôi không thể nói gì cho anh biết.” Nàng tỏ ra lịch sự, nhưng cứng rắn. Hàm ý “Mời anh biến” đã quá rõ ràng.

Chết tiệt!

https://thuviensach.vn

Điện thoại reo, cho tôi cơ hội rút chân ra khỏi tình huống xấu hổ này. “Này, Kevin,” giọng trên điện thoại vang lên.

“Chào, Adam.” Cậu em cùng cha khác mẹ – người thân thiết nhất với tôi mà không phải là hacker. Cậu ấy thậm chí còn không có cả máy tính.

Sau một hồi trò chuyện, nó nói: “Người yêu cũ của em biết một gã siêu hacker tên là Eric Heinz. Cô ấy nói hắn biết vài thứ về công ty điện thoại mà anh có thể không biết và hắn thực sự muốn gặp anh.”

Sau đó, nó nói thêm: “Cẩn thận đấy Kevin. Em không nghĩ là cô ta đáng tin.”

Phản ứng đầu tiên của tôi là mặc kệ. Tôi đã gặp đủ rắc rối trong chuyện hacking dù là với những người tôi quen biết nhiều năm và cảm thấy mình có thể tin tưởng.

Vậy nhưng chống lại cám dỗ không phải là tính cách của tôi. Tôi gọi tới số mà Adam đã đưa.

Người nhấc máy không phải là Eric mà là một gã có tên Henry Spiegel, phát âm là “Shpeegel”. Spiegel là một trong những nhân vật đa tài nhất mà tôi từng biết, danh sách này của tôi ngoài Ivan Boesky thì còn có Marvin Mitchelson, luật sư có tiếng chuyên về thủ tục ly hôn đã bị kết tội trốn thuế và Barry Minkow, tay lừa đảo đình đám của ZZZZ Best. Spielgel là một trường hợp đặc biệt, gã nổi danh trên mọi lĩnh vực từ cướp nhà băng, sản xuất phim khiêu dâm tới việc sở hữu một câu lạc bộ đêm Hollywood mới nổi. Đó là một trong những nơi thường xuyên được nhắc tới, nơi các diễn viên trẻ và những kẻ tìm kiếm danh vọng thường xếp hàng dài để được bước vào.

Khi tôi nhờ Spiegel chuyển máy cho Eric, anh ta nói: “Tôi sẽ gọi cậu ta cho cậu. Tôi phải nhắn tin cho cậu ta rồi gọi hội nghị[50] cho cậu. Cậu ta rất cảnh giác.”

https://thuviensach.vn

[50] Gọi hội nghị (conference call): Dịch vụ gọi điện thoại giúp các thuê bao thiết lập cuộc gọi tới nhiều thuê bao khác tại cùng một thời điểm. (ND)

“Cảnh giác?” Tôi cũng là người cảnh giác, nhưng gã này có vẻ vượt ngoài ngưỡng đó, tới mức siêu hoang tưởng.

Tôi chờ. Tôi đang làm cái quái gì không biết. Nếu gã này thực sự quan tâm tới hacking, chỉ riêng việc nói chuyện với gã trên điện thoại cũng đã là một ý tưởng tồi. Trong điều khoản trả tự do có ghi rõ tôi không được liên lạc với bất kỳ hacker nào và việc kết giao với De Payne cũng đã đủ rủi ro. Chỉ một lời từ gã Eric Heinz này cũng đủ để tống tôi vào tù thêm hai năm nữa. Từ sau vụ hack điện thoại cầm tay Novatel, tôi hầu như tuân thủ đúng luật trong suốt hai năm hoàn lương. Tôi vẫn còn một năm bị quản chế nữa. Vậy thì thế quái nào mà tôi lại gọi cuộc điện thoại này cơ chứ?

Giờ thì tôi đã liên lạc với gã Eric này và cố thuyết phục bản thân rằng mình chỉ đang làm vậy cho đủ phép lịch sự với cậu em trai mà thôi.

Làm sao tôi biết được cuộc gọi vô hại này chính là khởi đầu cho một cuộc phiêu lưu điên rồ sẽ làm thay đổi cuộc đời tôi mãi mãi?

Khi Eric nghe máy lần đầu, hắn ta không ngừng ám chỉ để tôi hiểu rằng mình biết rất nhiều về phone phreaking và tấn công máy tính.

Hắn nói chuyện kiểu như: “Tôi đã làm việc với Kevin. Anh biết đấy – một Kevin khác, Kevin Poulsen.” Hắn đang cố xây dựng niềm tin đối với tôi thông qua một gã hacker mới sập bẫy vì lừa đảo trong cuộc thi ham radio và có lẽ còn đánh cắp bí mật an ninh quốc gia.

Hắn nói: “Tôi đã đột nhập vào văn phòng công ty điện thoại cùng anh ta.” Nếu điều này là thực thì chuyện quả là có chút hấp dẫn. Điều đó có nghĩa là Eric có thông tin nội bộ từ việc thực sự sử dụng và kiểm soát thiết bị ở văn phòng trung tâm và các cơ sở khác của công ty điện thoại. Hắn ta quả thực

https://thuviensach.vn

đã gây được sự chú ý của tôi. Việc hắn khẳng định mình biết được khối mẹo mực của Poulsen quả là một mồi câu hữu hiệu.

Để dụ tôi, hắn phun ra những chi tiết về các bộ chuyển mạch của công ty điện thoại như 1AESS, 5E và DMS-100, đồng thời nói về các hệ thống như COSMOS, Mizar, LMOS và hệ thống BANCS mà hắn nói mình và Pouslen đã đăng nhập từ xa. Hắn nói như thể hắn là một phần của một nhóm nhỏ đã làm việc cùng Poulsen để hack các cuộc thi ham radio. Báo chí nói Pouslen đã kiếm được tới vài chiếc Porsches từ những cuộc thi như thế này.

Chúng tôi nói chuyện khoảng 10 phút. Một tuần sau, tôi còn gọi cho Spiegel thêm vài lần để nói chuyện với Eric.

Có vài điều khiến tôi cảm thấy không ổn. Eric không nói chuyện như mấy gã hacker khác; giọng hắn giống như Joe Friday, một gã cớm, thì đúng hơn. Hắn thường đặt những câu hỏi dạng như: “Anh có đang theo đuổi dự án nào gần đây không? Dạo này anh hay nói chuyện với ai?”

Hỏi một hacker mấy câu kiểu này chẳng khác gì tới quán bar ưa thích của mấy gã trộm nhà băng rồi hỏi: “Ernie bảo tôi tới. Vụ cuối anh làm với ai vậy?”

Tôi nói với hắn ta: “Tôi không hack nữa rồi.”

“Tôi cũng vậy,” hắn đáp.

Đây đúng là kiểu lấp liếm điển hình khi nói chuyện với ai đó mà bạn không biết. Đương nhiên, hắn ta nói dối và hắn cố tình cho tôi biết điều đó. Hắn là hắn cũng nhận ra tôi đang nói dối. Trong trường hợp của tôi thì việc đó lại khá thành thật. Nhưng chính nhờ gã này mà sự thành thật ấy không còn kéo dài thêm bao lâu nữa.

Tôi nói với hắn: “Tôi có một người bạn có lẽ anh sẽ muốn nói chuyện cùng. Tên anh ta là Bob. Anh ta nên gọi cho anh theo số nào?”

https://thuviensach.vn

“Hãy bảo anh ta gọi cho Henry theo cách mà anh vẫn gọi tôi đó,” hắn đáp. “Cậu ấy sẽ gọi hội nghị cho tôi.”

“Bob” là biệt danh vừa nảy ra trong đầu tôi dành cho Lewis De Payne.

Không dễ gì tìm được một hacker có thông tin nội bộ như Eric. Đúng, như vậy tức là tôi đang kéo Lewis ngày càng lún sâu hơn vào các phi vụ hacking của mình, nhưng nếu có cậu ta làm lá chắn, tôi có thể tìm ra được những thông tin mà Eric có nhưng Lewis và tôi thì không mà vẫn bảo vệ được bản thân.

Tại sao tôi lại dễ dàng trao đổi thông tin với Eric khi mà chỉ nói chuyện với cậu ta thôi cũng đã vi phạm điều kiện quản chế rồi? Bạn hãy thử nghĩ xem: Tôi đang sống tại Las Vegas, một thành phố tôi không biết rõ và cũng chẳng mấy thích, liên tục phải lái xe qua những khách sạn và sòng bài xa hoa, tất cả đều được tô điểm nhằm thu hút khách du lịch và những con nghiện bài bạc. Với tôi, đây là thành phố chả có gì thú vị. Không có tia hy vọng nào trong đời, không có được sự kích thích và những thử thách trí tuệ tôi từng trải qua khi tấn công vào các công ty điện thoại. Không có dòng adrenaline tuôn trào khi phát hiện ra các lỗi phần mềm giúp tôi tiến sâu vào hệ thống của một công ty nào đó – sự kích thích có được từ những ngày tôi còn được biết tới trong thế giới ngầm trực tuyến với tên “Condor”. (Trước đây, tôi chọn cái tên này là vì sự ngưỡng mộ dành cho người hùng trong lòng, một nhân vật luôn-đi-trước-người-khác-một-bước do Robert Redford thủ vai trong bộ phim Three Days of the Condor (tạm dịch: Ba ngày của Condor).

Lúc đó, Phòng Quản chế đã phân cho tôi một nhân viên quản chế mới, một người có vẻ cho rằng tôi đã phạm quá nhiều tội và cần phải nhận được vài bài học. Hắn gọi cho một công ty đang xem xét hồ sơ tuyển dụng của tôi và hỏi những câu hỏi kiểu như: “Liệu Kevin có thể tiếp cận với nguồn vốn công ty không?” dù tôi chưa từng kiếm một xu từ việc hacking, mặc cho điều đó có dễ thế nào. Điều này đã khiến tôi tức điên.

https://thuviensach.vn

Dù sao thì tôi cũng được nhận vào làm việc. Nhưng mỗi ngày trước khi rời sở, họ luôn dò xét người tôi xem có bất kỳ phương tiện lưu trữ bên ngoài nào như đĩa mềm hay đĩa từ không. Chỉ mình tôi chứ không ai khác. Tôi ghét điều này.

Sau năm tháng, tôi hoàn thành một dự án lập trình rất lớn và bị tạm thôi việc. Rời đi cũng chẳng có gì đáng tiếc.

Nhưng tìm được một công việc mới là cả một thử thách bởi tay quản chế không ngừng gọi điện tới từng công ty tuyển dụng và đặt những câu hỏi đầy cảnh giác: "Liệu Kevin có quyền tiếp cận với các thông tin tài chính không?" hay tương tự thế.

Điều này khiến tôi suy sụp và thất nghiệp.

Việc dành 2-3 tiếng mỗi ngày ở phòng tập gym giúp tôi căng duỗi cơ bắp nhưng trí óc thì không. Tôi đăng ký một lớp lập trình máy tính và một lớp dinh đưỡng (bởi tôi muốn tìm hiểu thêm về lối sống khỏe mạnh) ở Đại học Nevada, Las Vegas (UNLV). Trong tuần đầu tiên ở đây, tôi không ngừng gõ "Control-C" để bật tắt máy tính lặp đi lặp lại. Việc này ngắt dòng script khởi động của máy tính giữa chừng và cho tôi quyền quản trị tuyệt đối, hay còn gọi là "root"[51]. Vài phút sau, một quản trị viên lao vào phòng và hét lên: "Cậu đang làm cái quái gì vậy?"

Tôi cười với anh ta. "Tôi tìm thấy lỗi[52] này. Nhìn xem, tôi có quyền tuyệt đối đây này."

[51] Root: Quá trình cho phép người dùng giành quyền truy cập ưu tiên nhằm kiểm soát hệ thống của thiết bị, giúp họ tùy chỉnh cài đặt để vượt qua rào cản bảo mật nghiêm ngặt của nhà sản xuất. (BTV)

[52] Lỗi (bug): Các lỗi phần mềm trong chương trình hoặc hệ thống máy tính làm cho kết quả không chính xác hoặc không mong muốn. (BTV)

https://thuviensach.vn

Hắn yêu cầu tôi ra khỏi phòng và nói với viên giám sát rằng tôi đã dùng Internet. Điều này không đúng sự thực nhưng cũng đủ lý do để buộc tôi phải dừng tất cả các lớp lập trình.

Nhiều năm sau, tôi phát hiện ra một quản trị viên hệ thống ở trường đã gửi tin nhắn tới một gã có tên là Tsutomu Shimomura với tựa đề "Về anh bạn của chúng ta", để mô tả sự việc này. Nhân vật Shimomura sẽ xuất hiện nhiều hơn ở những chương cuối của cuốn sách nhưng tôi rất ngạc nhiên khi biết hắn ta đã nhòm ngó những gì tôi dự tính làm ngay từ lúc đó, khi chúng tôi chưa từng liên lạc và tôi thậm chí còn không biết tới sự tồn tại của hắn.

Dù bị đá đít ra khỏi khóa học lập trình của UNLV, nhưng tôi đã hoàn thành xuất sắc lớp học dinh dưỡng, sau đó chuyển qua Cao đẳng Công đồng Quận Clark với học phí thấp hơn dành cho dân địa phương. Lần này, tôi chọn mấy khóa về điện tử nâng cao và viết lách.

Những lớp học này có lẽ đã cuốn hút hơn nếu mấy cô nàng học cùng đủ xinh xắn và sôi nổi để tạo cảm hứng cho tôi, nhưng đây chỉ là một trường cao đẳng cộng đồng. Nếu muốn gặp những cô nàng hay ho hơn, hắn là không thể trông chờ gì ở những lớp học buổi tối như thế này.

Khi chán nản, tôi phải hướng về những điều đem lại cảm hứng cho mình. Không phải vậy sao?

Khi ở cùng Eric, tôi thấy có điều gì đó thú vị, có thể đem tới những thử thách lớn hơn về khả năng của bản thân. Điều gì đó lại khiến dòng adrenaline tuôn trào.

Sẽ chẳng có vấn đề gì nếu tôi không vượt qua được nỗi bất hạnh do Lewis gây ra và kể về cậu ta trong suốt những cuộc trò chuyện cùng Eric. Eric luôn sẵn lòng nghe tôi nói, hào hứng được biết thêm về người này và tò mò muốn biết liệu hắn có cùng đẳng cấp hay không.

https://thuviensach.vn

Lewis gọi lại cho tôi vào hôm sau để nói rằng anh ta đã liên lạc với Spiegel và nói chuyện cùng Eric. Cậu ta có vẻ khá bất ngờ khi thừa nhận rằng mình thích hắn.

Thậm chí, Lewis cũng đồng ý với tôi rằng Eric, theo cách nói của cậu ta, "có vẻ biết khá nhiều về các quy trình nội bộ và bộ chuyển mạch của Pacific Bell. Hắn có thể là một nguồn tin quý giá." Lewis nghĩ rằng chúng tôi nên qua lại với hắn.

Khi đó, tôi đã bắt đầu dấn thân vào một cuộc chơi mà sau này trở thành cuộc vờn bắt kiểu mèo đuổi chuột đầy phức tạp – một trò chơi sẽ đặt tôi vào tình thế rủi ro khôn lường và phải vận dụng tới toàn bộ kỹ năng của mình.

https://thuviensach.vn

Phần hai

ERIC

https://thuviensach.vn

11
MỜ ÁM

Lwpi idlc sxs bn upiwtg axkt xc lwtc X bdkts xc lxiw wxb?

Đầu tháng 1 năm 1992, cha tôi gọi từ Los Angeles và nói rằng ông khá lo lắng về cậu em cùng cha khác mẹ của tôi, Adam, đứa con còn lại của ông. Tôi vẫn luôn ghen tỵ với mối quan hệ của Adam và cha, bởi tôi chỉ thỉnh thoảng mới được gặp cha trong những năm đầu đời.

Adam sống với cha ở Calabasas, gần Los Angeles, trong khi theo học một chương trình dự bị luật tại Cao đẳng Pierce. Tối hôm trước nó không về nhà, cha nói việc này không bình thường. Tôi cố trấn an ông, nhưng tôi có thể nói gì đây khi thực sự tôi cũng chẳng rõ tình hình?

Mối lo âu của cha hóa ra lại có lý. Suốt nhiều ngày, người cha khốn khổ gần như phát điên khi không nghe ngóng được tin gì về Adam. Tôi cố kiềm chế và trấn an ông trong khi vẫn gọi điện cho bác Mitchell và anh bạn Kent của Adam để nghe ngóng, đồng thời không ngừng nhắn tin cho nó.

Vài ngày sau, cha tôi gọi, giọng thổn thức và bấn loạn. Ông nhận được điện thoại từ cảnh sát. Họ đã tìm thấy Adam trên ghế sau xe của nó, đỗ tại khu tụ tập chính của lũ nghiện hút, công viên Echo Park. Adam đã qua đời vì dùng thuốc quá liều.

Adam và tôi lớn lên cách xa nhau, sống khác thành phố, ngoại trừ khoảng thời gian ngắn cùng sống với cha ở Atlanta. Dù vậy, trong vài năm gần đây, chúng tôi đã trở thành cặp anh em cùng cha khác mẹ thân thiết hơn nhiều anh em ruột thịt. Khi bắt đầu kết thân với Adam ở Los Angeles, tôi đã không thể chịu nổi thể loại âm nhạc mà nó quan tâm – rap và hip-hop, bất cứ thứ gì

https://thuviensach.vn

của 2 Live Crew, Dr. Dre hay N.W.A. Nhưng càng nghe nhiều thứ nhạc này mỗi khi chúng tôi ở cùng nhau, tôi càng yêu thích nó và điều này đã trở thành một phần gắn kết, kéo chúng tôi lại gần nhau hơn.

Giờ thì nó đã đi rồi.

Mối quan hệ của cha và tôi không mấy suôn sẻ, nhưng tôi cảm thấy ngay lúc này ông đang rất cần tôi. Tôi liên hệ với nhân viên quản chế và được phép quay lại Los Angeles một thời gian để giúp cha đối diện với cái chết của Adam, tìm cách giúp ông thoát khỏi cơn trầm cảm mà ông đang phải chịu đựng, ngay cả khi tôi biết điều đó sẽ chỉ làm nỗi buồn của riêng tôi ngày một lớn hơn. Ngày hôm sau, tôi lái xe về phía Tây trên con đường I–15 ra khỏi sa mạc, chuẩn bị cho chuyến hành trình kéo dài năm giờ đồng hồ tới Los Angeles.

Chuyến đi dài cho tôi thời gian suy nghĩ. Cái chết của Adam rất bất thường. Cũng giống như nhiều đứa trẻ khác, nó đã qua giai đoạn nổi loạn. Đã có lúc Adam diện quần áo theo mấy ban nhạc “Goth” nó ưa thích và khiến tôi thấy thật xấu hổ khi đi cùng nó ở nơi công cộng. Hồi đó, Adam không hòa hợp với cha chút nào, nó cũng chuyển đến sống với mẹ và tôi một thời gian. Nhưng gần đây, có vẻ như nó đã tìm lại được chính mình ở trường cao đẳng. Kể cả nếu Adam dùng chất kích thích để thư giãn, tôi vẫn không hiểu nổi việc nó chơi thuốc quá liều. Tôi mới gặp Adam gần đây, nó không có vẻ gì là một kẻ nghiện ngập trong cách hành xử. Cha cũng nói với tôi rằng cảnh sát không thấy có vết chích nào khi tìm thấy thi thể của Adam.

Lái xe trong đêm để đến gặp cha, tôi bắt đầu nghĩ tới việc dùng kỹ năng hacking của mình để tìm hiểu xem Adam đã ở với ai vào đêm đó và ở đâu.

Sau chặng đường lái xe buồn tẻ từ Las Vegas, tận khuya tôi mới tới căn hộ của cha ở đường Las Virgenes, thị trấn Calabasas, cách bờ biển Santa Monica khoảng 20km và 45 phút lái xe. Cha hoàn toàn suy sụp vì Adam và ông cũng nghi ngờ có điều gì đó mờ ám. Lịch trình sinh hoạt thường ngày

https://thuviensach.vn

của cha – điều hành công ty đấu thầu tổng thể của ông, xem tin tức trên tivi, đọc báo trong bữa ăn sáng, đến Channel Islands để đi thuyền, thỉnh thoảng tham gia làm lễ ở giáo đường Do Thái – đã bị phá hỏng. Tôi biết việc chuyển đến ở với ông sẽ gặp phải nhiều vấn đề – ông chưa bao giờ là người dễ chịu – nhưng tôi không thể để những chuyện đó ngăn cản mình. Ông cần tôi.

Khi ông mở cửa đón tôi, tôi đã choáng váng khi thấy sự suy sụp và gương mặt xám xịt của cha. Đầu hói, râu ria nhẵn nhụi và dáng người cân đối, nhưng bỗng dưng tôi thấy ông thật bé nhỏ.

Cảnh sát bảo ông rằng: “Chúng tôi không điều tra những vụ án kiểu này.”

Nhưng họ đã phát hiện ra giày của Adam như thể được ai đó thắt dây, chứ không phải theo kiểu tự buộc. Khám nghiệm kỹ hơn cho thấy có một vết tiêm trên cánh tay phải, dấu vết chỉ hợp lý trong trường hợp có ai đó đã tiêm cho nó một liều chí mạng: Adam thuận tay phải, vì thế việc tự tiêm cho mình bằng tay trái là hoàn toàn không tự nhiên. Rất rõ ràng, Adam đã ở cùng người khác khi qua đời – ai đó đã tiêm cho nó một liều chí mạng, do thuốc chất lượng kém hoặc do quá liều, rồi vứt xác nó vào xe, lái đến một nơi vắng vẻ nhưng nhan nhản chất kích thích ở Los Angeles, rồi bỏ đi.

Nếu cảnh sát không làm gì, thì tôi sẽ tự trở thành thám tử.

Tôi dùng phòng cũ của Adam và lao vào nghiên cứu hồ sơ của công ty điện thoại. Suy đoán có khả năng nhất là hai người mà tôi đã gọi lúc mới nghe tin từ cha: Kent, bạn thân nhất của Adam, người đáng lẽ phải ở cùng nó vào cuối tuần đó; và đáng buồn thay, bác Mitchell, người đã hủy hoại cuộc đời mình vì ma túy. Adam là người rất gần gũi với bác Mitchell. Cha có linh cảm rằng bác Mitchell có liên quan tới cái chết của Adam, thậm chí là phải chịu trách nhiệm cho cái chết ấy.

Tại lễ tang, việc nhìn mặt lần cuối diễn ra trong một căn phòng biệt lập. Tôi bước vào một mình và nhìn Adam nằm trong chiếc quan tài mở nắp. Đến dự

https://thuviensach.vn

đám tang của một người gần gũi với mình thực quá sức chịu đựng. Adam biến dạng đến mức tôi không thể nhận ra nổi nó. Tôi không ngừng hy vọng rằng mình chỉ đang mắc kẹt trong một cơn ác mộng tàn khốc nào đó. Một mình trong phòng đứa em trai duy nhất, tôi sẽ không bao giờ còn được nói chuyện với nó nữa. Tôi biết điều này nghe thật sáo rỗng nhưng nỗi buồn khiến tôi nhận ra chúng ta thực sự có ít thời gian trên cuộc đời này đến thế nào.

Một trong những việc đầu tiên của tôi ở Los Angeles là liên hệ với nhân viên quản chế mới phụ trách trường hợp của tôi, Frank Gulla. Ở độ tuổi cuối tứ tuần, với thân hình trung bình cùng tính tình điềm đạm, thân thiện, ông thậm chí còn thả lỏng cả đống luật lệ – ví dụ, không cứng nhắc về những chuyến thăm "bắt buộc" hằng tháng sau khi biết về tôi. Khi tôi thu xếp thời gian để đến trình diện ở văn phòng, ông bảo tôi điền vào đống báo cáo hằng tháng mà tôi bỏ lỡ và điền lại ngày tháng cho những báo cáo đó. Tôi không cho rằng ông xuề xòa như thế cả với những gã bị buộc tội nghiêm trọng hơn, nhưng tôi trân trọng sự thoải mái mà ông dành cho mình.

Tôi lao đầu vào điều tra. Cha và tôi đều nghi ngờ Kent, gã bạn của Adam, biết nhiều hơn những gì đã kể cho chúng tôi. Liệu hắn có thấy nhẹ nhõm hơn khi mở lòng nói chuyện với người khác? Nếu vậy, liệu hắn có bất cẩn đến mức làm việc đó qua điện thoại không? Cùng với anh bạn Alex của mình, tôi lái xe đến Long Beach, nơi Kent sống. Sau một hồi dò la ở khu căn hộ gần đó, tôi đã tìm ra thứ mình cần: Một đường dây điện thoại hiện không nối với điện thoại của bất cứ khách hàng nào. Tất cả những gì cần làm là một cuộc gọi đến văn phòng trung tâm (CO) địa phương để nhân viên kỹ thuật "bấm" kết nối từ đường điện thoại của Kent vào đường dây không ai sử dụng đó, để biến nó, về bản chất, trở thành một đường dây kéo dài bí mật cho điện thoại của hắn. Alex và tôi thiết lập máy ghi âm kích hoạt bằng giọng nói bên trong hộp đầu cuối của công ty điện thoại để ghi lại mọi cuộc trao đổi điện thoại của Kent.

https://thuviensach.vn

Trong vài ngày sau đó, tôi dành một tiếng rưỡi đi từ chỗ cha đến căn hộ đặt máy ghi âm giấu kín ở Long Beach. Mỗi lần đến, tôi lại lấy cuộn băng của ngày hôm trước, thay vào đó một cuộn băng mới, và cho cuốn băng vào đầu đọc băng di động để nghe các cuộc hội thoại của Kent trên đường lái xe về chỗ cha. Trong vô vọng. Hàng giờ hàng giờ nỗ lực và không thu được bằng chứng nào.

Cùng lúc đó, tôi cũng cố ghép lại bức tranh về những người mà bác Mitchell đã nói chuyện cùng trong vài tiếng trước khi Adam mất. Tôi đã tấn công bằng kỹ thuật xã hội với nhân viên của PacTel Cellular và lấy được hồ sơ chi tiết các cuộc gọi của bác, hy vọng nó sẽ cho tôi thấy liệu bác có gọi liên tục hết cuộc này đến cuộc khác, dấu hiệu cho thấy sự nguy cấp hay lo lắng, hoặc gọi đến những người bạn khác của bác để cầu xin sự giúp đỡ hay không.

Không có gì cả.

Tôi thử lại PacTel Cellular lần nữa, hy vọng tìm ra khu sóng mà các cuộc điện thoại của bác Mitchell đã được tiếp sóng qua, nó có thể giúp chỉ ra liệu bác có ở gần Echo Park, nơi thi thể của Adam bị bỏ lại hay không. Tuy nhiên, tôi không thể tìm ra bất kỳ ai biết cách truy cập vào những hồ sơ tôi muốn. Hoặc PacTel không lưu lại những dữ liệu đó, hoặc tôi đơn giản không thể tìm ra người biết hệ thống nào có quyền truy cập đến cơ sở dữ liệu cũng như cách để lấy chúng.

Tất cả đều vì một lý do chính đáng nhưng cuối cùng lại vô nghĩa, tôi sa đà vào lối sống của một hacker như trước.

Cuộc truy tìm của tôi lâm vào ngõ cụt. Tôi đã thử tất cả chiến thuật mình biết nhưng không đi đến đâu: Tôi không có thêm chút thông tin nào về cái chết của Adam so với những gì đã biết khi cha gọi báo cho tôi. Tôi tức giận và bực dọc, khốn khổ vì không thể giải tỏa được nỗi niềm cho cha và bản thân khi khám phá ra ít nhất vài mẩu thông tin hữu dụng.

Cái kết của câu chuyện buồn này chỉ được hé lộ nhiều năm sau đó.

https://thuviensach.vn

Cha tôi đoạn tuyệt với bác Mitchell, cho rằng bác chính là nguyên nhân dẫn đến cái chết của Adam. Hai anh em họ không nói chuyện với nhau cho đến tận những ngày cuối đời cha, khi ông phải chật vật chống chọi với căn bệnh ung thư phổi.

Khi tôi viết những dòng này, bác Mitchell vừa mất. Trong buổi gặp mặt gia đình, một trong những người vợ cũ của bác kéo tôi sang một bên. Trong nỗi xấu hổ, bà nói: "Bác đã rất muốn cho cháu biết điều này suốt một thời gian dài. Mitchell không phải là một người tốt. Đêm Adam qua đời, Mitchell đã gọi cho bác. Ông ấy hoảng loạn đến mức khó hiểu. Mitchell nói ông ấy và Adam đã ngồi chích thuốc với nhau, Adam đã chích một liều rất lớn và nằm vật ra. Mitchell đã rất hoảng sợ. Ông ấy lay Adam và đưa thằng bé vào vòi hoa sen, nhưng không gì có thể giúp được."

"Ông ấy gọi cho bác cầu xin sự giúp đỡ nhưng bác từ chối tham gia. Vì thế, ông ấy đã gọi cho một gã buôn ma túy quen biết, hắn đã giúp lấy đôi giày của Adam và đưa thi thể thằng bé vào xe. Họ lái hai chiếc xe đến Echo Park, để Adam chết trong xe và rời đi."

Vậy là ngay từ đầu cha tôi đã đúng. Thay vì gọi 911, Mitchell đã hy sinh đứa cháu mà ông ấy yêu mến để cứu lấy thân mình.

Tôi đã vô cùng giận dữ khi viết những dòng này.

Ngay từ đầu, tôi đã cho rằng bác Mitchell có liên quan theo một cách nào đó. Ấy vậy mà lúc này đây, khi nghe được sự thật, tôi lại cảm thấy đau thắt tim, không ngờ ông ấy có thể làm vậy và rằng ông còn mang bí mật ấy xuống mồ. Người đàn ông mà tôi từng yêu mến, quý trọng và noi theo đã không thể nói cho tôi biết sự thật ngay cả khi trút hơi thở cuối cùng.

https://thuviensach.vn

12
KHÔNG THỂ GIẤU GIẾM

Yhlt xak tzg iytfrfad RanBfld squtpm uhst uquwd ce mswf tz wjrwtsr a wioe lhsv Ecid mwnlkoyee bmt oquwdo't ledn mp acomt?

Tôi đã chìm đắm vào việc điều tra cái chết của Adam tới mức cần phải nghỉ ngơi – phải có thứ gì đó không thiên về cảm xúc để tôi có thể tập trung vào. Không khó để tôi tìm ra trò tiêu khiển nhằm đánh lạc hướng bản thân: Tôi sẽ quay trở lại và xử lý Neill Clift, gã người Anh chuyên tìm kiếm các lỗ hổng bảo mật trong hệ điều hành VMS của DEC. Làm sao để tôi có thể lừa anh ta cho tôi biết mọi lỗi bug mà anh ta tìm thấy?

Từ những tin nhắn đọc được, tôi biết Clift khao khát được làm việc cho DEC từ lâu; có lẽ nên ra tay từ đây. Tôi lừa công ty điện thoại British Telecom cho tôi số điện thoại nhà riêng của Clift, sau đó gọi cho anh ta, tự giới thiệu mình là Derrell Piper, mượn tên của một kỹ sư phần mềm kỹ thuật số ở phòng phát triển VMS. Tôi nói với anh ta: "Đợt tuyển dụng đã kết thúc rồi nhưng chúng tôi vẫn muốn tìm thêm vài kỹ sư bảo mật. Chúng tôi nghĩ tới tên cậu vì cậu đã giúp đỡ chúng tôi rất nhiều trong việc tìm kiếm và báo cáo các điểm yếu bảo mật." Sau đó, tôi tiếp tục câu chuyện về những tài liệu hướng dẫn ở DEC mà tôi biết anh ta muốn có.

Kết thúc cuộc gọi, tôi nói: "Rất vui được nói chuyện với cậu, lâu lắm rồi nhỉ."

Ố ồ – đây quả là một sai lầm lớn. Hai người này chưa từng gặp nhau trước đó.

https://thuviensach.vn

Về sau tôi mới biết được rằng Neill đã gọi cho Ray Kaplan, một cố vấn bảo mật nổi tiếng mà anh ta biết từng phỏng vấn tôi trong chuỗi hội thảo "Meet the Enemy" (Gặp gỡ kẻ thù). Ray bật một đoạn trong băng ghi âm cuộc phỏng vấn.

Neill chỉ cần nghe qua một thoáng là có thể khẳng định. "Đúng – gã gọi cho tôi là Kevin Mitnick." Sau này khi gặp nhau, Ray bảo tôi: "Tôi đoán anh vẫn đang chơi trò tấn công bằng kỹ thuật xã hội."

Hơi bối rối, tôi hỏi lại: "Anh nói vậy là ý gì?"

"Neill đã gọi cho tôi. Tôi bật một đoạn băng phỏng vấn của anh. Cậu ấy nhận ra ngay giọng anh và nói anh đã gọi điện."

Đương nhiên, trong thời gian này tôi vẫn thường liên lạc với Eric Heinz và hắn vẫn không ngừng nhắc tới Kevin Poulsen. Tôi chưa từng gặp Poulsen nhưng đã đọc và nghe về cậu ta đủ nhiều để ngưỡng mộ những gì cậu ta đạt được trong hacking. Thật lạ là chúng tôi chưa từng gặp mặt, chưa từng hack cùng nhau, dù chúng tôi cùng tuổi và lớn lên chỉ cách nhau vài cây số. Sau này, cậu ta giải thích rằng mình bắt đầu học về phone phreaking sau tôi – khi cậu ta mới chập chững vào nghề thì tôi đã rất nổi tiếng trong giới hacking rồi.

Lewis và tôi đều rất nóng lòng biết thêm về những gì Eric và Poulsen đã làm cùng nhau. Trong một cuộc trò chuyện qua điện thoại, Eric lại bắt đầu luyên thuyên về những hệ thống của Pacific Bell mà hắn và Poulsen từng giành quyền kiểm soát. Danh sách khá quen thuộc, trừ duy nhất một cái tên tôi chưa từng nghe tới: "SAS".

"SAS là gì?" tôi hỏi.

"Đó là hệ thống kiểm tra nội bộ có thể dùng để giám sát đường dây."

https://thuviensach.vn

Trong thuật ngữ của các công ty điện thoại thì “giám sát” là một cách nói nhã nhặn về việc nghe lén.

Tôi nói với Eric: “Nếu truy nhập vào bộ chuyển mạch, cậu có thể giám sát đường dây bất kỳ lúc nào mà.” Tôi biết Eric hiểu rằng các bộ chuyển mạch 1A ESS có tính năng “nói và giám sát”, chúng sẽ cho phép bạn nhảy vào một đường dây và nghe lén cuộc hội thoại.

Eric nói: “SAS còn tốt hơn.”

Eric kể hắn và Poulsen đã thực hiện một chuyến thăm đêm tới CO của Sunset ở phía Tây Hollywood. Chuyến đi này mang lại một thứ mà họ chưa từng nhìn thấy trước đó. Họ tìm ra một nơi lạ mắt: Không giống như các CO khác, văn phòng này được trang bị các máy tính và ổ đĩa rất khác thường, “trông như thể từ ngoài hành tinh vậy”. Một chiếc thùng to cỡ tủ lạnh với các loại thiết bị kêu ầm ì bên trong. Họ bắt gặp một cuốn hướng dẫn cho biết đây là máy Switched Access Service – Dịch vụ Truy cập Chuyển mạch – gọi tắt là SAS. Khi Poulsen lướt qua các trang hướng dẫn, cậu ta nhận ra SAS vốn dùng để kiểm tra đường dây, nghe như là nhờ nó bạn có thể kết nối tới bất kỳ đường dây điện thoại nào.

Nhưng nó chỉ dành để kiểm tra các đường dây xem chúng có đang hoạt động không thôi hay sao? Hay bạn có thể nghe lén cả cuộc gọi? Poulsen bắt đầu vọc vạch máy tính kiểm soát SAS.

Gõ vào dãy số điện thoại công cộng vẫn thường dùng, Poulsen đã khẳng định được rằng đúng là bạn có thể nhảy vào một đường dây nào đó và nghe lén cuộc hội thoại.

Cậu ta quay lại CO vào một đêm khác, cầm theo máy ghi đĩa để ghi lại dữ liệu được gửi ra từ thiết bị SAS. Poulsen muốn thử truy ngược lại giao thức và thu được thêm vài khả năng nào đó ở nhà.

https://thuviensach.vn

Tôi phải truy cập được vào hệ thống này. Nhưng khi hỏi thêm chi tiết, Eric liền ngậm miệng và nhanh chóng đổi chủ đề. Tôi bắt đầu nghiên cứu về nó ngay ngày hôm sau.

Thiết bị SAS bí ẩn chính là điều tôi còn thiếu trong đời: Một bài toán khó phải giải, một cuộc phiêu lưu với nhiều rủi ro. Thật không thể tin được khi tôi chưa hề nghe về nó trong suốt những năm phone phreaking của mình. Nó thật hấp dẫn. Tôi phải tìm ra nó.

Nhờ những chuyến thăm đêm tới các văn phòng công ty điện thoại, tất cả tài liệu hướng dẫn của công ty mà tôi có thể có được và đọc kỹ, cũng như những lần thực hiện tấn công bằng kỹ thuật xã hội với các nhân viên công ty điện thoại từ thời trung học, tôi có được kiến thức khá phong phú về các phòng ban, quy trình, thủ tục và số điện thoại khác nhau ở Pacific Bell. Có lẽ không nhiều người làm trong công ty nắm rõ được cấu trúc tổ chức ở đó hơn tôi.

Tôi bắt đầu gọi điện tới các bộ phận khác nhau. Chiến thuật của tôi là: “Tôi ở bộ phận Kỹ thuật. Nhóm anh có dùng SAS không?” Sau khoảng nửa tá cuộc gọi, tôi tìm được một gã ở Pasadena hiểu tôi muốn nói gì.

Với hầu hết mọi người thì có lẽ phần khó nhất trong mánh khóe dạng này là phải tìm ra cách tóm được thứ tri thức mà mình mong muốn. Tôi muốn biết cách có được quyền đăng nhập vào SAS, cũng như các lệnh cho phép tôi kiểm soát nó. Nhưng tôi cũng muốn có được nó một cách an toàn hơn so với cách mà Eric và Poulsen đã làm; tôi muốn có nó mà không cần phải trực tiếp đột nhập vào cơ sở của Pacific Bell.

Tôi nhờ gã nhân viên biết về SAS ở Pasadena lấy bản hướng dẫn từ trên giá xuống cho tôi. Khi anh ta quay trở lại điện thoại, tôi nhờ anh ta mở nó ra và đọc dòng chú ý về bản quyền.

Chú ý bản quyền?

https://thuviensach.vn

Chính nó – thứ này sẽ cho tôi biết tên công ty phát triển sản phẩm. Nhưng từ đoạn này thì tôi gặp khó khăn. Công ty này đã dừng hoạt động.

Cơ sở dữ liệu LexisNexis duy trì một lượng khổng lồ các nội dung trực tuyến của những bài báo và tạp chí, hồ sơ pháp lý cũng như tài liệu công ty. Có lẽ bạn đã đoán ra, việc một công ty ngừng hoạt động không có nghĩa là LexisNexis đã xóa bỏ dữ liệu về nó. Tôi tìm ra tên vài người từng làm việc cho công ty phát triển SAS, bao gồm cả một trong những lãnh đạo công ty. Công ty đặt ở Bắc California. Tôi truy tìm danh mục điện thoại ở vùng đó và có được số điện thoại của tay lãnh đạo.

Khi tôi gọi điện thì gặp anh ta ở nhà. Tôi nói với anh ta hiện mình đang làm việc với nhóm kỹ thuật của Pacific Bell và muốn thực hiện vài tùy chỉnh nhằm cải thiện "cơ sở hạ tầng SAS" của chúng tôi. Tôi muốn nói chuyện với ai đó hiểu về công nghệ này. Anh ta chẳng chút nghi ngờ, nói tôi đợi vài phút rồi quay trở lại đường dây, cho tôi biết tên và số điện thoại của tay kỹ sư trưởng trong nhóm phát triển sản phẩm.

Còn một điều phải làm trước khi thực hiện cuộc gọi mấu chốt này. Tại thời điểm đó, các số điện thoại nội bộ của Pacific Bell đều bắt đầu bằng đầu số 811; bất kỳ ai hợp tác với công ty này đều biết điều đó. Tôi tấn công vào bộ chuyển mạch của Pacific Bell và thiết lập một số điện thoại 811 chưa dùng, rồi thêm vào tính năng chuyển cuộc gọi, và chuyển nó tới số điện thoại nhái số mà tôi sử dụng lúc đó.

Tôi vẫn còn nhớ tên mình dùng khi gọi điện cho tay kỹ sư phát triển: Marnix van Ammers, tên của một kỹ sư chuyển mạch thực sự ở Pacific. Tôi kể cho anh ta câu chuyện tương tự về việc cần phải tích hợp mấy máy SAS ở công ty. "Tôi đã có bản hướng dẫn dành cho người dùng, nhưng nó không có ích lắm cho mấy việc chúng tôi cần làm. Chúng tôi cần giao thức thực sự được dùng giữa các thiết bị SAS ở trung tâm kiểm tra và văn phòng trung tâm."

https://thuviensach.vn

Tôi đã viện tới tên của một lãnh đạo ở công ty cũ của anh ta và còn sử dụng tên thực của một kỹ sư Pacific Bell. Tôi cũng không hề tỏ ra lo lắng; tôi không nói vấp điều gì cả. Không hề có chút gì đáng ngờ trong cuộc gọi đó. Anh ta nói: "Tôi vẫn còn các tập tin trong máy tính. Đợi chút."

Sau vài phút, anh ta trở lại. "Tôi tìm thấy rồi đây. Anh muốn tôi gửi chúng tới đâu?"

Tôi đã quá nóng vội. "Tôi đang sốt sình sịch lên đây," tôi nói. "Anh có thể gửi fax được không?" Anh ta nói có quá nhiều tài liệu để có thể fax tất cả, nhưng anh ta có thể gửi fax những trang mà anh ta nghĩ là hữu ích nhất, sau đó gửi bưu điện hoặc chuyển phát nhanh đĩa mềm có tập tin hoàn chỉnh. Tôi đọc cho anh ta số điện thoại nhận fax mà mình đã thuộc nằm lòng. Đương nhiên đó không phải là máy fax của Pacific Bell mà là một máy có cùng mã vùng, số fax của một trạm in tiện lợi ở Kinko's. Điều này thường có chút rủi ro bởi rất nhiều máy fax khi gửi tài liệu sẽ hiển thị tên của máy mà chúng đang kết nối. Tôi luôn lo ngại ai đó sẽ nhận ra dòng hiển thị "Cửa hàng Kinko's #267" hoặc gì đó, vậy thì tôi sẽ lộ hết bài vở. Nhưng trong trí nhớ của tôi thì chưa có ai phát hiện ra điều này.

Chuyển phát nhanh FedEx có vẻ dễ dàng hơn. Tôi cho tay kỹ sư địa chỉ của những nơi bạn có thể thuê hòm thư và lưu trữ kiện hàng, đồng thời đánh vần tên của nhân viên Pacific Bell mà tôi đang giả dạng, Marnix van Ammers. Tôi cảm ơn anh ta và nói chuyện thêm một chút. Trò chuyện vẩn vơ là một dạng xã giao thân thiện bổ sung nhằm mang tới cảm xúc tích cực và hạn chế những nghi ngờ có thể xảy ra.

Dù đã thực hiện nghệ thuật tấn công bằng kỹ thuật xã hội trong nhiều năm, nhưng tôi vẫn chưa hết ngừng ngạc nhiên bởi độ dễ dàng của nó. Đó là một trong những khoảnh khắc bạn cảm nhận được sự hưng phấn kích thích, hay như thể bạn trúng quả ở Vegas – endorphins[53] cứ rần rật chảy trên khắp cơ thể bạn.

https://thuviensach.vn

[53] Endorphins: Chất dẫn truyền thần kinh trong não bộ, có tác dụng tạo cảm xúc tích cực, cải thiện tâm trạng, giảm đau, v.v… (BTV)

Ngay chiều hôm đó, tôi lái xe tới cửa hàng cho thuê hòm thư để đặt một địa chỉ hòm thư dưới tên Marnix van Ammer. Họ luôn đòi phải có thẻ ID. Không thành vấn đề. Tôi giải thích: "Tôi vừa chuyển tới đây từ Utah và bị đánh cắp mất ví. Tôi cần có địa chỉ để họ gửi bản sao giấy khai sinh để làm lại giấy phép lái xe. Tôi sẽ cho anh xem chứng minh thư ngay khi có nó." Đúng, họ đã vi phạm luật bưu chính khi cho tôi thuê một hòm thư ngay cả khi không xuất trình được thẻ ID, nhưng những chỗ thế này thường rất sốt sắng mở rộng hoạt động kinh doanh: Họ thực sự không muốn phải từ chối khách hàng. Tất cả những gì tôi cần là một lời nói dối ngon ngọt.

Và đến tối cùng ngày, tôi đã có bản fax trong tay – những thông tin cơ bản hy vọng có thể giúp tôi nghe lén được điện thoại của Pacific Bell ở vùng Nam California. Nhưng chúng tôi vẫn cần phải tìm ra cách sử dụng giao thức SAS.

* * *

Để tìm ra cách thức hoạt động của SAS, Lewis và tôi tiếp cận vấn đề từ một số góc độ khác nhau. Hệ thống cho phép kỹ thuật viên có khả năng kết nối với bất kỳ đường dây điện thoại nào, nhờ vậy, anh ta có thể chạy các bài kiểm tra để tìm ra lý do tại sao khách hàng thường nghe thấy tiếng nhiễu trong đường dây hay vấn đề nào đó. Kỹ thuật viên sẽ chỉ thị cho SAS gọi tới CO có đường dây đang cần kiểm tra. Việc này sẽ kích hoạt cuộc gọi tới một bộ phận trong cơ sở hạ tầng của SAS ở CO có tên là "điểm kiểm tra đăng nhập từ xa" (remote access test point) hay còn gọi là RATP.

Đó là bước đầu tiên. Để nghe được âm thanh trên đường dây điện thoại – giọng nói, tạp nhiễu, tiếng tĩnh điện hay bất kỳ thứ gì – kỹ thuật viên phải cài đặt kết nối âm thanh tới bộ phận SAS ở CO. Những bộ phận này được thiết kế với một điều khoản bảo mật khá thông minh: Chúng có một danh

https://thuviensach.vn

sách các số điện thoại được cài sẵn trong bộ nhớ. Kỹ thuật viên sau đó sẽ phải gửi lệnh tới bộ phận SAS để quay số gọi ngược lại tới một trong những số có sẵn đó – số điện thoại của nơi anh ta làm việc.

Làm sao để chúng tôi có thể vượt qua biện pháp an toàn thông minh mà rõ ràng là không thể sai lầm này?

À, hóa ra cũng không khó lắm. Phải là một kỹ thuật viên của công ty điện thoại hay phone phreaker thì bạn mới hiểu được tại sao nó lại hiệu quả, nhưng đây là cách mà tôi đã làm. Tôi dùng điện thoại của mình để quay số gọi vào đường dây mà tôi biết chắc SAS sẽ dùng để thực hiện cuộc gọi đi, sau đó ngay lập tức kích hoạt SAS để nó gọi lại vào một số đã được lập trình sẵn trong bộ nhớ.

Khi SAS dùng một đường dây để thực hiện cuộc gọi đi, thực ra là nó đang trả lời cuộc gọi đến từ điện thoại của tôi. Nhưng nó phải đợi âm điệu quay số và không thể kết nối đường dây được vì đã bị tôi chặn.

Tôi ừmmmmmmmmmmmmm một tiếng dài vào điện thoại.

Tôi không thể ầm ừ ra âm thanh chính xác bởi âm điệu quay số ở Mỹ thực chất được tạo thành từ hai tần số. Nhưng điều này không quan trọng, bởi thiết bị này không được thiết kế để có thể đo được tần số chính xác; nó chỉ cần nghe được đại loại một tiếng ầm ừ. Tiếng ừmmmmmm như đang thưởng thức món súp Campbell của tôi là đủ xài rồi.

Tại thời điểm này, SAS vẫn cố gắng thực hiện cuộc gọi đi… nhưng không thể bởi tôi đã kết nối với đường dây mà nó định sử dụng.

Bước cuối cùng: Tôi gõ vào máy tính dòng lệnh mật chỉ thị cho SAS nhảy vào số điện thoại của người dùng mà tôi muốn giám sát.

Trong lần thử đầu tiên, tôi kích động tới mức nghẹt thở.

https://thuviensach.vn

Làm được rồi!

Sau đó, Lewis nói: “Kevin, cậu không ngồi yên được à? Cứ nhảy nhót lung tung thế? Như chúng ta đã tìm ra Chén thánh vậy.”

Chúng tôi đã có thể nghe lén bất kỳ số điện thoại nào của Pacific Bell rồi!

Tôi thực sự lo sốt vó, muốn tìm ra sự thật về Eric. Có quá nhiều thứ đáng ngờ về hắn.

Eric không có vẻ đang đi làm. Vậy làm sao hắn có đủ khả năng tài chính để tụ tập ở những câu lạc bộ mà hắn nhắc đến? Những nơi có tiếng như Whiskey à Go-Go, nơi Alice Cooper và nhóm the Doors, còn cả những tay rock thần sầu thuở ấy như Jimi Hendrix đôi khi vẫn thường ghé tới.

Và cả cái kiểu không cho tôi số điện thoại nữa? Eric thậm chí còn không cho tôi số máy nhắn tin của hắn. Thật đáng ngờ!

Lewis và tôi cùng bàn bạc về vấn đề này và quyết định chúng tôi cần phải tìm hiểu ngọn ngành xem điều gì đang diễn ra. Bước đầu tiên là xuyên thủng tấm màn “Tôi không thể cho các cậu số điện thoại được”. Sau khi đã có số điện thoại, chúng tôi sẽ dùng nó để tìm ra địa chỉ sinh sống của hắn.

Thời ấy, khách hàng ở California chưa được sử dụng tính năng Caller ID[54] bởi Hội đồng các Ngành dịch vụ Công cộng của bang vẫn còn lo ngại về vấn đề quyền riêng tư và chưa phê chuẩn cho phép nó được sử dụng rộng rãi. Nhưng cũng như hầu hết các công ty điện thoại khác, bộ chuyển mạch ở văn phòng trung tâm của Pacific Bell đều do Bell Labs phát triển và AT&T sản xuất. Giới phreaker đều biết rằng những bộ chuyển mạch này đều có gắn tính năng nhận diện người gọi cài sẵn trong phần mềm.

[54] Caller ID (Định danh người gọi): Dịch vụ cho phép người dùng nhìn thấy tên của người đang gọi tới trên các máy điện thoại analog thế hệ thời xưa. (BTV)

https://thuviensach.vn

Ở tòa nhà nơi anh bạn Dave Harrison của tôi làm việc, thiết bị đầu cuối đặt tại tầng một có hàng trăm đường dây điện thoại chạy tới. Tôi lén đi xuống đây bởi có khu trực của nhân viên an ninh ngay gần đó, khá may là nó không nằm ở hướng trực diện. Sử dụng thiết bị cầm tay của người đặt đường dây đặt ngay cạnh chỗ ngồi của Dave trong văn phòng, tôi kết nối tới vài cặp dây cáp, tìm một cặp có âm hiệu quay số. Khi tìm ra, tôi quay mã đặc biệt để có được số điện thoại. Đây sẽ là số điện thoại mồi nhử mà tôi định lừa Eric gọi vào.

Sau đó, Dave kéo cặp dây ra khỏi thiết bị đầu cuối, kết nối đường dây đó với một đường đây điện thoại không dùng trong văn phòng. Ở trên tầng, chúng tôi nối máy điện thoại vào đường dây trộm được và vào hộp hiển thị Caller ID.

Từ thiết bị đầu cuối VT100 cũ của mình, tôi gọi vào bộ chuyển mạch của văn phòng trung tâm trên đường Webster và thêm tính năng Caller ID vào đường dây điện thoại mồi nhử.

Tối hôm đó, tôi quay trở lại căn chung cư của cha ở Calabasas, đặt chuông báo thức lúc 3 rưỡi sáng và leo lên giường đi ngủ. Khi chuông reo, tôi nhắn tin cho Eric bằng chiếc điện thoại mạo danh thuê bao của người khác. Lúc này, Eric đã bắt đầu thoáng hơn chút và cho tôi số máy nhắn tin của hắn. Tôi để lại số điện thoại mồi để hắn gọi lại cho tôi. Khi Eric quay số, dữ liệu định danh người gọi sẽ được gửi đi ngay giữa hồi chuông thứ nhất và thứ hai, cho thấy số máy của hắn. Bắt được mày rồi!

Dave thường lén sinh hoạt và ngủ ngay tại văn phòng của cậu ta. Ngay khi tôi cho rằng Eric đã trả lời tin nhắn, tôi gọi cho Dave. Lúc đó là 3 giờ 40 phút sáng. Tôi liên tục gọi điện cho Dave cho tới khi cậu ta nhấc máy và vô cùng giận dữ. “Cái gì đấy?!” cậu ta gào lên trong điện thoại.

“Thấy Caller ID chưa?”

“Rồi!”

https://thuviensach.vn

“Dave, rất quan trọng đấy. Số bao nhiêu?”

“Sáng mai gọi lại đi!” cậu ta lại gào lên trước khi dập máy.

Tôi đi ngủ tiếp và không liên lạc với cậu ta cho tới tận chiều hôm sau. Lúc này, cậu ta mới đọc cho tôi số điện thoại một cách khiên cưỡng: 310 837-5412.

Được rồi, vậy là tôi đã có số điện thoại của Eric. Tiếp đến là địa chỉ của hắn.

Giả vờ là một kỹ thuật viên hiện trường, tôi gọi cho Trung tâm Phân bổ Vòng lặp Cơ học (MLAC), hay còn được biết tới dưới cái tên đơn giản là Văn phòng Phân bổ Đường dây của Pacific Bell. Một phụ nữ nhấc máy: “Chào chị, tôi là Terry đang ở hiện trường. Tôi cần F1 và F2 của số 310 837-5412.” F1 tức là đường cáp ngầm từ văn phòng trung tâm còn F2 là đường cáp tải thứ cấp kết nối một căn nhà hay tòa văn phòng tới (hộp vùng dịch vụ). F2 cuối cùng sẽ kết nối với F1, quay lại về văn phòng trung tâm.

“Terry, mã kỹ thuật của anh là gì?” cô ta hỏi.

Tôi biết cô ta sẽ chẳng tra lại đâu – họ chẳng bao giờ làm vậy. Bất kỳ mã nào có ba số đều được, miễn sao là tôi tỏ vẻ tự tin và không ngập ngừng.

“Sáu ba bảy,” tôi nói, lấy bừa một số.

“F1 là số 416 ở cáp 23, đầu cực 416,” cô ta nói. “F2 là số 36 ở cáp 10204, đầu cực 36.”

“Thiết bị đầu cuối ở đâu?”

“Không-chấm-một ở 3636 Nam Sepulveda.” Đó là vị trí hộp đầu cuối, nơi kỹ thuật viên hiện trường đặt kết nối tới nhà hay văn phòng khách hàng.

Tôi vốn không quan tâm đến những gì vừa hỏi. Chúng chỉ để giúp cho tôi có vẻ hợp lý thôi. Thông tin kế tiếp mới là điều tôi thực sự muốn.

https://thuviensach.vn

“Địa chỉ thuê bao là gì nhỉ?” Tôi hỏi.

“Cũng là 3636 Nam Supulveda.” Cô ta nói. “Phòng 107B.”

Tôi hỏi: “Còn số nào khác đang dùng cho 107B không?”[55]

[55] Trong đoạn hội thoại này, Kevin Mitnick có sử dụng một số từ lóng trong ngành nhưng đã bị lược bỏ khi dịch. (ND)

Cô ta nói, “Có, còn một số khác nữa,” và cho tôi số thứ hai cùng với F1 và F2 của nó. Dễ như vậy đó. Tôi chỉ mất vài phút đồng hồ để biết được địa chỉ của Eric và cả hai số điện thoại của Eric.

Khi tấn công bằng kỹ thuật xã hội, hay “pretexting”[56], bạn phải trở thành một diễn viên đang sống trong vai diễn của mình. Tôi đã nghe nhiều người cố gắng giả danh người khác và trở thành một trò cười lớn. Không phải ai cũng có thể lên sàn diễn và thuyết phục khán giả; không phải ai cũng có thể pretexting và hoàn thành nhiệm vụ.

[56] Pretexing: Kỹ thuật giả danh người khác để lấy được thông tin mong muốn. (ND)

Với bất kỳ ai thành thạo pretexting như tôi, mọi việc sẽ trôi chảy như thể một nhà vô địch bowling ném bóng xuống đường băng. Cũng như người ném bóng, tôi không kỳ vọng mình sẽ ghi điểm mỗi lần. Nhưng khác với người ném bóng, nếu thất bại, tôi thường có cơ hội thử lại mà không bị mất điểm.

Nếu bạn biết tiếng lóng và từ trong ngành, điều này giúp bạn có được sự tín nhiệm – bạn chính là một đồng nghiệp thực sự cũng đang vật vã với công việc hệt như đối tượng của mình và họ hầu như sẽ không bao giờ đặt câu hỏi về uy tín của bạn. Ít ra là thuở đó, họ không làm như vậy.

https://thuviensach.vn

Tại sao người phụ nữ ở phòng phân bổ đường dây lại sẵn lòng trả lời mọi câu hỏi của tôi? Đơn giản là vì tôi đã đưa ra câu trả lời đúng và hỏi những câu hỏi đúng, sử dụng tiếng lóng đúng. Do đó, đừng cho rằng nhân viên ở Pacific Bell, người đã cho tôi địa chỉ của Eric, là ngu ngốc hay không nhanh trí. Những người làm việc ở văn phòng thường bỏ qua nghi ngờ khi nhận được những yêu cầu có vẻ xác thực.

Con người, như tôi đã nhận ra ngay từ thuở còn thơ, thường rất cả tin.

Có lẽ sự liều lĩnh trở lại với con đường hacking của tôi có thể tha thứ được, hoặc chí ít thì cũng được thông cảm, khi xét tới mong muốn tìm ra được bí ẩn trong cái chết của em trai. Nhưng đột nhiên tôi nhận ra mình đã vượt quá sự ngu ngốc thông thường: Tôi đã dùng một trong ba đường dây điện thoại ở căn hộ của cha để thực hiện tất cả các cuộc gọi tấn công bằng kỹ thuật xã hội tới Pacific Bell, truy dấu điều tra về Adam và để nói chuyện với Lewis.

Đây là sự vi phạm rõ ràng điều kiện quản chế. Điều gì sẽ xảy ra nếu cảnh sát liên bang theo dõi đường dây điện thoại của cha tôi và nghe được các cuộc hội thoại đó?

Tôi cần phải tìm hiểu xem họ đã biết những gì.

https://thuviensach.vn

13
KẺ NGHE LÉN

Zkdw lv wkh qdph ri wkh SL ilup wkdw zdv zluhwdsshg eb Sdflilf Ehoo?

Ngay cả những gã bị hoang tưởng đôi khi cũng có kẻ thù thực sự. Một ngày nọ, tôi có cảm giác ai đó đang theo dõi mình – hay nói cách khác, nghe lén các cuộc điện thoại của tôi.

Ý tưởng này đã thực sự khiến tôi phát hoảng. Tôi sợ hãi nghĩ tới việc nhận được cuộc gọi từ nhân viên quản chế đề nghị tôi đến gặp trong cuộc hẹn nào đó, đồng nghĩa với việc tôi sắp sửa bị tống giam lần nữa và sẽ bị chuyển về nhà tù Liên bang, hay thậm chí là biệt giam. Tôi sợ muốn chết.

Dịch vụ điện thoại nhà riêng của chúng tôi do văn phòng trung tâm PacBell ở Calabasas cung cấp, nơi đây vốn chỉ phụ trách một khu vực nhỏ, vì vậy nếu có bất kỳ hành vi chặn sóng nào, tôi đoán khả năng lớn là họ đang nhắm tới tôi. Tôi gọi đến CO và một kỹ thuật viên bắt máy. “Xin chào,” tôi nói. “Tôi là Terry Atchley bên Phòng An ninh. Tôi nghĩ chúng tôi có một số thiết bị ở đó. Chúng tôi đang thiếu thiết bị theo dõi và cần lấy lại một số hộp của mình để phòng cho vụ khác. Các anh còn hộp nào không?” Tay kỹ thuật viên hỏi tôi trông chúng thế nào. Hmm – tôi không biết. Tôi mấp máy đôi chút và nói: “Nó phụ thuộc vào model các anh đang dùng ở đó. Chắc nó là một cái hộp nhỏ với một máy in mini đi kèm để ghi lại các số đã gọi.”

Anh ta đi tìm. Tôi lo lắng phát điên, đi đi lại lại trong lúc đợi anh ta quay lại đầu dây. Tôi đã cầu nguyện anh ta không tìm thấy gì.

Cuối cùng anh cũng quay lại nhấc máy. “Vâng,” anh ta nói. Tim tôi bắt đầu đập nhanh hơn, adrenaline bơm trào trong mạch máu.

https://thuviensach.vn

“Tôi tìm thấy ba chiếc. Chúng là các hộp nhỏ màu xám, nhưng theo tôi thấy, chúng không có máy in,” kỹ thuật viên nói.

Ba hộp – chắc là mỗi hộp cho một đường dây điện thoại tại căn hộ tôi đang ở với cha. Khốn nạn! Không hay chút nào.

“Được rồi,” tôi bảo anh ta. “Nếu các anh không cần nữa, sẽ có người qua và đem chúng đi vào ngày mai. Tôi cần các anh lần ra dây các kết nối.”

“Ở dây nào?”

“Hãy thử cái đầu tiên xem.”

Nhân viên kỹ thuật hỏi tôi xem nên theo dấu đầu dây nào. Lại một phút ậm ừ – lại một lần nữa tôi không biết phải trả lời thế nào. Anh ta bảo tôi hộp có hai kết nối. “Hãy thử lần theo cả hai và xem chúng nối đến đâu,” tôi nói.

Sau vài phút lo lắng chờ đợi, tôi nghe thấy anh ta quay lại nhấc máy. “Tôi đã phải lần theo cái dây này xuyên qua khung,” anh ta nói. Tôi nhận ra đó là gì: Một lời than phiền khó chịu vì tôi đã bắt anh ta lần theo sợi dây một quãng dài, xuyên qua một mê cung phức tạp dọc theo khung chia dây. Anh ta cũng bảo tôi: “Ở một đầu, tôi nghe thấy âm báo 1000Hz.” Lạ thật. “Ở đầu còn lại, tôi nghe thấy âm hiệu quay số.”

Tôi sẽ không thể hiểu được những chiếc hộp này hoạt động ra sao cho đến khi tôi biết chúng được nối đến đâu. Tôi nhờ anh ta ngắt các dây từ khung và thực hiện xác minh đường dây để tìm xem mỗi đầu hộp kết nối với số điện thoại nào. “Chờ tôi vài phút,” anh ta nói.

Xác minh đường dây là một việc thường kỳ. Nhân viên kỹ thuật đơn giản chỉ cần tháo lần lượt mỗi cặp dây, kẹp bộ tai nghe của anh ta vào đường dây và quay mã số để xác định số điện thoại mỗi đầu.

https://thuviensach.vn

Âm báo 1000Hz thì lạ quá. Thật đáng tò mò. Tôi không biết nó có nghĩa là gì nhưng tôi không có thời gian đào sâu vào câu hỏi. Tim tôi đập nhanh, người vã mồ hôi vì lo sợ, biết rằng anh ta chuẩn bị đọc cho tôi một trong các số điện thoại của cha.

Anh ta quay lại, nhấc máy và đọc cho tôi hai số điện thoại kết nối đến một trong những cái hộp. Không có số nào của cha.

Tôi thở phào không ra tiếng. Cuối cùng, tôi cũng thở được. Hệt như vừa có một tấn gạch được nhấc ra khỏi lồng ngực.

Nhưng còn hai chiếc hộp còn lại thì sao? Tay kỹ thuật viên có vẻ hơi khó chịu khi tôi bảo anh ta rằng mình cần lần theo cả dây cho hai hộp còn lại. Dù sao thì anh ta cũng sẽ không tự kiếm chuyện cho mình bằng việc than phiền to tiếng.

Dù lần này tôi phải đợi lâu hơn rất nhiều, nhưng anh ta cuối cùng cũng quay lại và đưa cho tôi những số điện thoại kết nối đến hai chiếc hộp còn lại. Một lần nữa, không có số nào của cha tôi.

Không có ai đang theo dõi tôi.

Tôi khó lòng đợi được đến bước tiếp theo: gọi đến cả hai số điện thoại gán với mỗi hộp.

Đầu tiên tôi thử những số máy có âm tần 1000Hz. Chuông đổ ba lần và có tiếng trả lời bíp-bíp-bíp. Tôi thử lại lần nữa. Rồi lại lần nữa. Dù gọi lúc nào thì kết quả vẫn giống hệt nhau. Nó có thể là gì nhỉ? Có lẽ nó đang đợi một dạng mã nào đó. Mặc cho lời giải thích là gì, với tôi, rõ ràng đường dây này không phải là đường dây đang bị nghe lén.

Sau này tôi sẽ rất thích thú khám phá và tìm hiểu bí mật của số này.

https://thuviensach.vn

Số kết nối còn lại đến chiếc hộp đầu tiên có người nhấc máy trả lời "Alo" – chắc hẳn phải là người đang bị nghe lén. Vì tò mò, tôi gọi đến Trung tâm Phân bổ Vòng lặp Cơ học để tìm hiểu xem nạn nhân thiếu may mắn đang bị nghe lén là ai.

Đó không phải là một Ông A hay Bà B; mà là một công ty tên là Văn phòng Điều tra Teltec. Tôi thử dây trên hộp thứ hai và rồi hộp thứ ba. Cả ba đều thuộc về cùng một công ty, Văn phòng Điều tra Teltec.

Tối hôm đó trong bữa tối, tôi nói chuyện với cha rằng mình đã kiểm tra xem có phải đường dây điện thoại của chúng tôi đang bị nghe lén không. Ông đảo mắt. Tôi có thể tưởng tượng ông đang nghĩ: Chắc con trai mình đang mơ mộng được làm James Bond nên mới nghĩ có ai thèm nghe lén nó. Đó là mấy thứ chỉ xuất hiện trong phim điệp viên thôi.

Tôi cố thuyết phục ông rằng đây là một khả năng nghiêm túc dù không có gì phải lo lắng. Thực sự họ có đang nghe lén khu này, nhưng là nghe lén một công ty nào đó tên là Teltec Investigations, không phải chúng tôi.

Tôi cười và cho ông biết không có gì phải lo lắng.

Ông nhìn tôi ngạc nhiên. "Teltec?!"

Tôi gật đầu.

Lại một sự tình cờ của Trái đất tròn, cha tôi biết Teltec, ông giải thích, đó vốn là một công ty thám tử tư – một công ty chuyên thuê các thám tử tư và người lần theo dấu vết để truy tìm tài sản của các đối tác làm ăn đã cuỗm đi quá mức phần chia lợi nhuận của họ, mấy gã ly hôn có cả tấn tiền trong các tài khoản kín, hay tương tự thế. "Cha biết Mark Kasden, quản lý ở đó," cha bảo tôi. Rồi ông nói thêm: "Hay để cha gọi cho ông ta một cuộc? Cha cược rằng lão muốn biết về những gì con vừa phát hiện."

https://thuviensach.vn

Tôi nói: “Tại sao không nhỉ?” Tôi nghĩ ông ta sẽ trân trọng những thông tin này.

20 phút sau, có tiếng gõ cửa căn hộ. Kasden không phí chút thời gian nào để đến đây. Cha dẫn ông ta vào và giới thiệu tôi. Ông ta thấp lùn và đậm người nhưng rắn chắc, với mái tóc đuôi ngựa nhìn như thể nó đang đánh lạc hướng bạn khỏi đỉnh đầu đang hói dần của ông ta. Kasden trông không giống với tưởng tượng của tôi về Sam Spade hay Anthony Pellicano[57], dù về sau tôi phát hiện ra ông ta là một trong những người chơi xe Harley máu lửa và luôn nói về những chiếc xe của mình với thứ cảm xúc mãnh liệt. Chưa kể ông ta còn luôn chăn gái, tập trung cho cuộc chinh phục tiếp theo.

[57] Sam Spade là một thám tử hư cấu, còn Anthony Pellicano là một thám tử tư nổi tiếng tại Los Angeles. (ND)

Tôi nhìn người đàn ông này và tự hỏi tại sao công ty của ông ta lại đang bị điều tra, dù tôi khá chắc chắn ông ta sẽ không chia sẻ bất cứ thứ gì đen tối với tôi. Tôi giải thích rằng tôi đã kiểm tra xem đường dây điện thoại của cha tôi có bị nghe lén không.

“Đường dây điện thoại của cha tôi thì không sao, nhưng ba đường dây của Teltec thì đang bị theo dõi,” tôi nói với ông ta.

Phản ứng của ông ta cũng gần giống với phản ứng của cha tôi. Ông ta nhìn tôi như thể đang nghĩ: Thằng nhóc này lại bịa chuyện đây. Không thể có chuyện nó biết liệu một đường dây điện thoại có đang bị nghe lén không. Tôi hào hứng chia sẻ khả năng của mình. Việc này thật ngầu bởi đây là những chuyện bạn thường giữ cho riêng mình, trừ khi bạn muốn kết thúc ở một phòng giam tập thể trong tù.

“Ông không nghĩ tôi có thể nghe lén đúng không? Chỉ bằng máy tính của mình và bất kỳ chiếc điện thoại, tôi có thể theo dõi bất cứ ai tôi muốn.”

https://thuviensach.vn

Vẻ mặt ông ta như kiểu: Tại sao mình lại phí thời gian với thằng khoác lác này?

Tôi hỏi liệu ông ta có muốn xem một màn trình diễn không. Ông ta trả lời với thái độ ngờ vực, vênh váo: “Tất nhiên rồi. Để xem cậu có nghe được đường dây điện thoại của bạn gái tôi không.” Ông ta bảo tôi rằng cô ta sống ở Agoura Hills.

Trong cuốn sổ của mình, tôi có những ghi chép viết tay các số dial-up đến các điểm truy cập kiểm tra từ xa (remote access test points – RATP) của SAS ở vài CO trong Thung lũng San Fernando. Tôi tìm số RATP trong CO Agoura cung cấp dịch vụ khu vực của cô bạn gái kia. Có bốn số được liệt kê.

Do đã biết các đường điện thoại của cha không bị nghe lén, nên tôi có thể dùng một trong số đó để kết nối vào SAS: Vì đây là cuộc gọi nội hạt, nên sẽ không có hồ sơ hóa đơn nào được tạo ra, nghĩa là sau này cảnh sát sẽ không thể tìm ra bằng chứng nào chứng minh ai đó đã kết nối đến SAS từ đường điện thoại này. Tôi ngồi bên chiếc máy tính để bàn – người bạn thực sự của tôi, dù cha đã đồng ý sẽ nói nó là của ông nếu nhân viên quản chế có ghé qua, bởi tôi đáng ra không được dùng máy tính trừ khi được cho phép. Tôi dùng modem máy tính kết nối đến bộ phận SAS ở CO Agoura.

Trên đường điện thoại thứ hai của cha, tôi gọi đến một số khác và bật chế độ loa ngoài. Họ nghe thấy tiếngreng, reng, reng.

Tôi gõ vài lệnh vào máy tính. Bỗng nhiên, tiếng đổ chuông dừng hẳn với một tiếng click rất lớn, như thể ai đó vừa nhấc máy. Họ nhìn tôi chăm chú, đầy tò mò, khi tôi huýt sáo to vào loa ngoài: mmmmmmmm. Ngay lập tức, chúng tôi nghe thấy một loạt tiếng bấm bàn phím như thể có ai đó vừa nhấc máy và bắt đầu thực hiện cuộc gọi.

Tôi hỏi Mark số điện thoại của bạn gái ông ta và nhập vào một chuỗi lệnh trên máy tính. Giờ chúng tôi đang nghe đường điện thoại của cô ta.

https://thuviensach.vn

Chán thật. Cô ả không nghe điện. Đường dây im ắng.

“Mark, bạn gái ông không nghe điện,” tôi bảo ông ta. “Ông thử gọi cho cô ta từ điện thoại di động của ông xem.” Trong lúc ông ta rút điện thoại di động của mình ra và bấm quay số nhanh, cha nhìn tôi thiếu tin tưởng, như thể ông đang xem một kẻ học đòi làm Harry Houdini cố biểu diễn một trò ảo thuật mà không thực sự biết phải làm thế nào.

Từ loa ngoài trên đường điện thoại của cha, chúng tôi nghe thấy tiếng bừmmmmm brừmmmm, tức là số máy đang đổ chuông. Sau bốn tiếng chuông, chúng tôi nghe thấy máy trả lời tự động nhận tin, rồi đến tin nhắn phát đi của cô bạn gái. “Xin hãy để lại lời nhắn,” tôi nhe răng cười bảo ông ta. Khi ông ta nói vào điện thoại di động của mình, chúng tôi có thể nghe được từng từ của ông ta đi ra khỏi loa ngoài điện thoại của cha.

Mark há hốc mồm. Mắt ông ta mở to và nhìn tôi chăm chú bằng ánh mắt choáng ngợp và ngưỡng mộ. “Việc này thật không thể tin được,” ông ta nói. “Cậu làm thế nào vậy?!”

Tôi trả lời bằng một câu thoại sáo rỗng có phần nhàm chán, “Tôi có thể cho ông biết, nhưng sau đó tôi sẽ phải giết ông.”

Đi ra đến cửa, ông ta nói: “Tôi nghĩ cậu sẽ sớm nhận được tin từ tôi.” Ý tưởng làm việc cho một công ty thám tử tư nghe thật tuyệt. Có thể tôi sẽ học thêm được một số kỹ năng điều tra tuyệt vời mới. Tôi nhìn ông ta bước ra khỏi cửa và hy vọng sẽ thực sự nhận được tin từ ông ta lần nữa.

https://thuviensach.vn

14

ANH NGHE LÉN TÔI, TÔI NGHE LÉN ANH

Plpki ytw eai rtc aaspx M llogw qj wef ms rh xq?

Vài ngày sau cuộc gặp với người bạn của cha tôi, Mark Kasden, đến từ công ty thám tử tư, tôi lên đường thực hiện chuyến đi dài trở lại Vegas để thu thập quần áo và đồ dùng cá nhân. Phòng Quản chế đã chấp thuận yêu cầu của tôi được chuyển đến sống lâu dài với cha.

Tôi rời nhà từ rất sớm, dù không hợp lắm với lối sống về đêm nhưng như vậy tôi mới có thể thoát khỏi Los Angeles trước giờ cao điểm buổi sáng. Trong suốt thời gian lái xe, tôi lên kế hoạch thực hiện một đòn tấn công bằng kỹ thuật xã hội nho nhỏ để điều tra mấy cái hộp mà lúc đầu tôi đã nghĩ là để giám sát đường dây điện thoại của cha.

Tôi chuyển hướng vào cao tốc 101 về phía I-10, đi theo hướng Tây qua vùng sa mạc. Điện thoại trên tay tôi vẫn là số nhái của một người khác.

Có một câu chuyện thú vị về đường cao tốc. Vài tuần trước, tôi đã bị một gã lái BMW tạt đầu. Khi tôi đang bận trò chuyện trên điện thoại, gã đột nhiên đổi làn, chệch sang làn đường của tôi vài phân, dọa tôi sợ gần chết, thiếu chút nữa là chúng tôi đã cùng bắn ra khỏi đường.

Tôi vồ lấy điện thoại và thực hiện một cú điện thoại giả danh tới Cục Cấp phép Phương tiện cơ giới, cung cấp biển số xe BMW và có được tên cùng địa chỉ của gã lái xe. Sau đó, tôi gọi tới bộ phận của PacTel Cellular (chỉ có hai công ty điện thoại cung cấp dịch vụ cho Nam California tại thời điểm đó,

https://thuviensach.vn

do vậy tôi có 50% khả năng chọn trúng trong lần thử đầu tiên), đọc tên và địa chỉ của gã kia, quả đúng là PacTel Cellular có tài khoản của gã. Người phụ nữ cho tôi số điện thoại cầm tay của gã và chỉ năm phút sau khi tên khốn đó tạt đầu xe của tôi, tôi đã gọi cho gã. Vẫn run lên trong cơn giận dữ, tôi gào lên: “Này, thằng mất dạy, tao chính là người bị mày tạt đầu xe năm phút trước và cùng suýt chết với mày. Tao ở Cục Cấp phép Phương tiện cơ giới đấy, nếu mày còn lặp lại trò khốn này thêm một lần nữa thì bọn tao sẽ hủy bằng lái của mày đấy!”

Hẳn là tới giờ gã vẫn còn thắc mắc làm sao mà một người lái xe trên đường cao tốc có thể có số điện thoại của gã. Tôi vẫn thích thú cho rằng cú điện đó đã dọa hắn một trận vãi tè.

Thành thực mà nói, dù vậy thì bài học về sự nguy hiểm khi dùng điện thoại trong lúc lái xe cũng chẳng có mấy tác động tới tôi. Ngay khi tiếng ồn ào xe cộ trên đường cao tốc vào giờ cao điểm lùi lại sau lưng và tôi đã yên vị trên đường tới Vegas, tôi cầm điện thoại trên tay. Cuộc gọi đầu tiên là tới một số điện thoại đã khắc sâu trong trí óc tôi: Số của trung tâm chuyển mạch Pacific Bell phụ trách tất cả các bộ chuyển mạch trong khu vực phía Tây Thung lũng San Fernando.

“Canoga Park SCC xin nghe, tôi là Bruce,” một tay kỹ thuật viên nhấc máy.

“Chào Bruce,” tôi nói. “Tôi là Tom Bodett thuộc đội Kỹ thuật ở Pasadena.”

Tên tôi giới thiệu quá quen thuộc dạo ấy: Bodett là một tác giả kiêm diễn viên, người đã tham gia một loạt các quảng cáo trên đài phát thanh cho Motel 6, kết thúc bằng câu; “Tôi là Tom Bodett và tôi sẽ để đèn sáng cho các bạn.” Tôi chỉ buột miệng ra cái tên đầu tiên xuất hiện trong đầu. Nhưng Bruce không có vẻ để ý, do vậy tôi lại tiếp tục. “Mọi chuyện ổn chứ?” tôi hỏi.

“Vẫn ổn, Tom, anh cần gì?”

https://thuviensach.vn

“Tôi đang gặp phải một trường hợp bất thường ở Calabasas. Chúng tôi nghe thấy tín hiệu ở âm tần rất cao – tần số phải đến cả nghìn hertz. Không hiểu cuộc gọi tới từ đâu. Anh xem hộ tôi được không?”

“Được. Số gọi lại của anh là bao nhiêu?”

Bruce không nhận ra giọng tôi, còn tôi thì biết chắc anh ta là ai. Anh ta là mục tiêu tấn công bằng kỹ thuật xã hội của tôi cùng các phone phreaker khác trong nhiều năm, và đã bị lừa đủ nhiều để dần trở nên đa nghi và có tính cảnh giác cao hơn. Do đó, bất kỳ khi nào anh ta nhận được cuộc gọi từ ai đó mình không biết và tự xưng là nhân viên công ty, anh ta sẽ hỏi số gọi lại – tốt nhất đó nên là một dãy số mà anh ta có thể nhận ra là thuộc về Pacific Bell. Bruce sẽ tắt máy và gọi lại.

Hầu hết các phone phreaker thậm chí còn không buồn chế ra một số điện thoại hoặc có thể là không biết phải làm thế nào. Họ cố lờ đi bằng vài lý do yếu ớt kiểu như “Tôi đang chuẩn bị đi họp”. Nhưng Bruce đã quá quen với việc này và sẽ không bị bịp một lần nữa. Do đó, trước khi bấm máy, tôi đã thuyết phục được một nhân viên của Pacific Bell rằng tôi là kỹ sư công ty hiện đang công tác ở Los Angeles để xử lý một vấn đề kỹ thuật và cần có số điện thoại tạm thời. Sau khi có số, tôi đặt chế độ chuyển cuộc gọi vào số điện thoại nhái của tôi thời đó. Khi Bruce gọi lại vào số điện thoại nội bộ mà tôi cho anh ta, cuộc gọi sẽ được chuyển đến di động của tôi.

“Phòng kỹ thuật xin nghe, tôi Tom đây,” Tôi trả lời.

“Tom, tôi là Bruce gọi lại cho anh.”

“Ồ, cảm ơn anh. Anh có thể xem giúp tôi số máy 880-0653 ở bộ chuyển mạch Calabasas không? Cho tôi tin phát sinh nhé.” Tôi đang nhờ anh ta truy dấu cuộc gọi đến.

Tôi lo lắng bồn chồn. Nếu Bruce nghe thấy tiếng còi xe hay các tiếng ồn không giống như ở nơi công sở, tôi sẽ bị phát hiện. Việc này rất quan trọng –

https://thuviensach.vn

cũng rất thú vị – nếu hỏng chuyện. Tôi nghe thấy tiếng Bruce gõ máy tính và tôi biết chính xác anh ta đang làm gì: Anh ta đang đặt lệnh yêu cầu bộ chuyển mạch truy nguồn cuộc gọi.

“Tom, được rồi, cuộc gọi từ LA70 tandem” – điều đó có nghĩa rằng đây là một cuộc gọi đường dài từ ngoài khu vực Los Angeles.

Sau đó, Bruce cho tôi thông tin trung kế[58] chi tiết để tiếp tục truy dấu cuộc gọi. Tôi hỏi luôn anh ta số điện thoại của trung tâm chuyển mạch phụ trách LA70 tandem. Khả năng ghi nhớ số điện thoại kỳ diệu của tôi lại một lần nữa phát huy tác dụng: Tôi không cần phải dùng một tay ghi nó ra giấy trong khi tay kia đang giữ bánh lái. (Thục tế thì hầu hết các số điện thoại và tên người trong cuốn sách này đều là thực, chúng vẫn in sâu trong trí nhớ tôi từ tận 20 năm trước.)

[58] Trung kế (trunking): Đường truyền tín hiệu giữa nhà cung cấp dịch vụ thoại tới khách hàng. (ND)

Cuối cuộc gọi, tôi nói với anh ta: “Đừng quên tôi nhé, Bruce. Tôi có thể sẽ cần anh giúp nữa đấy.” Hy vọng anh ta vẫn nhớ ra tôi cho lần gọi kế tiếp và không cần phải làm mấy thủ tục gọi lại một lần nữa.

Khi tôi gọi đến trung tâm chuyển mạch, có tiếng trả lời: “LA70 xin nghe, tôi là Mary”.

Tôi nói: “Chào Mary, tôi là Carl Randolph từ phòng Kỹ thuật ở San Ramon. Tôi đang truy dấu mạch và có vẻ nó bắt nguồn từ chỗ chị.” Rõ ràng là mọi việc rất suôn sẻ bởi Mary không hề ngần ngừ, chỉ hỏi tôi thông tin trung kế. Tôi báo cho cô ta biết và chờ đợi trong lúc kiểm tra. Vì phone phreaker hiếm khi nhắm vào tổng đài trục chính, nên cô ta thậm chí còn không buồn hỏi tôi thông tin xác minh.

Mary trở lại đường dây. “Carl, tôi đã truy theo thông tin trung kế anh đưa. Cuộc gọi bắt nguồn từ San Francisco 4E.” Cô ta cho tôi thông tin trung kế

https://thuviensach.vn

và mạng lưới mình tìm được. Tôi hỏi thêm số điện thoại của văn phòng 4E, rất mừng là cô ta cũng tìm giúp tôi.

Tôi đã lái xe tới gần đường 15. Hành trình của tôi đi qua đèo Cajon, chạy giữa dãy San Bernardino và dãy San Gabriel, rất có khả năng cuộc gọi của tôi sẽ bị ngắt. Tôi sẽ phải đợi tới khi đến Victorville ở tít phía xa con đèo.

Trong lúc đó, tôi bật radio trên xe và tận hưởng vài bản nhạc cổ điển từ những năm 1950. “Đây là K-Earth-101,” DJ nói. “Chúng tôi sẽ tặng tới 1.000 đô-la mỗi giờ cho người gọi may mắn thứ bảy sau khi các bạn nghe K-Earth – ‘bản nhạc cũ nhất tuyệt vời nhất trên radio.’”

Ồ! Hẳn phải rất tuyệt vời nếu dành được giải thưởng này! Nhưng sao phải thử cơ chứ? Tôi chưa từng thắng bất kỳ cuộc thi nào. Dù vậy thì ý nghĩ này vẫn luẩn quẩn trong đầu tôi và cuối cùng, nó cũng chuyển từ mộng tưởng thành cơn cám dỗ.

Gần tới Victorville, tôi quay số mà Mary đã cho, gặp một gã có tên là Omar. “Chào Omar, tôi là Tony Howard thuộc ESAC ở Nam California. Có một tình huống khá kỳ lạ ở đây. Chúng tôi đang theo dấu một mạch có âm tần lên tới hàng nghìn hertz.” Tôi cho anh ta thông tin trung kế từ LA tandem để kiểm tra.

Qua Victorville, tôi tiến vào một vùng sa mạc vắng vẻ và e ngại cuộc gọi sẽ bị ngắt một lần nữa. Tôi giảm tốc từ 130km/giờ xuống để không đi xa Victorville quá nhanh.

Mất một lúc để Omar quay trở lại cuộc gọi. “Tôi nghe thấy tiếng cao tần đó rồi,” anh ta trả lời và bắt đầu “iiiiiiiiiiiiiiiiiiiiiiiiiii” để mô phỏng lại nó. Tôi bật cười – tôi đã nghe thấy âm đó rồi và không cần phải nghe anh ta cố bắt chước lại nó làm gì.

Omar nói cuộc gọi bắt nguồn từ Oakland. “Tuyệt,” tôi nói. “Cảm ơn anh vì đã giúp. Anh cho tôi thông tin trung kế từ bộ chuyển mạch của anh để chúng

https://thuviensach.vn

tôi có thể tra tiếp nhé."

Anh ta tìm thông tin bộ chuyển mạch và báo lại cho tôi.

Cuộc gọi kế tiếp là tới Trung tâm Kiểm soát Chuyển mạch Oakland. "Chúng tôi đang theo dấu một cuộc gọi từ San Francisco 4E," tôi nói và đưa ra thông tin trung kế cùng mạng lưới. Sau một hồi chờ đợi, kỹ thuật viên quay trở lại máy và cho tôi con số 510 208-3XXX.

Vậy là tôi đã truy được cuộc gọi từ nơi bắt nguồn. Đây là số điện thoại gọi đi từ một trong những hộp ở CO Calabasas đang giám sát Teltec.

Tôi vẫn muốn biết liệu âm thanh kia có thay đổi gì không. Nếu có thì chuyện gì sẽ xảy ra? Liệu tôi có nghe thấy tín hiệu dữ liệu nào đó? Hay tôi sẽ nghe được nội dung điện thoại gì?

Tôi gọi cho Omar. "Xin chào, có gì thay đổi với âm thanh đó không anh bạn?"

Anh ta trả lời rằng anh ta đã nghe nó tới 15 phút và chẳng có gì thay đổi cả.

Tôi hỏi: "Anh có thể đặt ống nghe gần loa để tôi nghe một chút không? Tôi muốn chạy thử vài bài kiểm tra." Anh ta nói anh ta sẽ đặt ống nghe gần loa và tôi có thể dập máy khi xong việc.

Quá tuyệt – khi âm thanh đó chuyển tới di động của tôi, nó hệt như lần tôi nghe lén mấy kẻ nghe lén ở NSA vậy. Tôi đang nghe lén máy nghe lén – vậy mới châm biếm làm sao?

Nhưng giờ thì tôi lại cảm thấy vừa lo lắng vừa hào hứng. Sau hàng giờ nghe điện thoại trong lần tấn công bằng kỹ thuật xã hội này, tôi đã rất đau tai rồi và cánh tay cũng nhức mỏi. Khi tôi đi tới dải sa mạc dẫn vào Barstow, được nửa đường tới Las Vegas, sóng điện thoạt rất yếu và cuộc gọi lại bị ngắt. Chết tiệt!

https://thuviensach.vn

Tôi gọi lại cho Omar để anh ta đặt máy lại một lần nữa cho tôi nghe tín hiệu kia qua loa. Hy vọng rằng tại thời điểm nào đó âm thanh này sẽ kết thúc và tôi có thể nghe được điều gì đó cho tôi biết chuyện gì đang xảy ra và âm thanh đó có nghĩa là gì.

Trước mắt là trạm nghỉ lớn chuyên phục vụ các tài xế xe tải, những người lái xe 18 bánh cả ngày lẫn đêm. Tôi dừng xe để đổ xăng và quyết định gọi điện cho cha, ông vẫn đang chịu cú sốc lớn sau cái chết của Adam.

Di động của tôi vẫn đang bận với âm tín hiệu kia, do đó, tôi tìm một chiếc điện thoại công cộng để gọi cho cha. Tôi quay số ông và giữ máy trong lúc chuông điện thoại reo. Âm tín hiệu tần số cao từ điện thoại đột nhiên tắt.

Cái quái gì vậy?!

Tôi nắm điện thoại trong tay và đặt ở bên tai kia.

Giọng cha tôi vang lên từ ống nghe:

“Alô!”

Tôi nghe thấy giọng ông từ máy công cộng và đồng thời phát ra từ điện thoại di động!

Chết tiệt!

Không thể tin được.

Thiết bị giám sát này không còn nhắm tới Teltec… mà là điện thoại của cha tôi. Đường dây nối đã bị đổi.

Họ nghe lén chúng tôi.

Thật điên rồ!

https://thuviensach.vn

Tôi cố gắng tỏ ra bình tĩnh nhưng đầy quả quyết và kiên trì. “Cha, cha dùng máy điện thoại công cộng ở chợ Village phía bên đường đi. Con có tin tức quan trọng về Adam,” tôi nói với ông.

Lời nói của tôi phải mang tính vô thưởng vô phạt, để không bị lộ qua máy nghe lén.

“Kevin, có chuyện gì vậy?” Cha nói, ông nổi điên lên với tôi. “Cha chán mấy cái trò James Bond này lắm rồi.”

Tôi nài nỉ và cuối cùng cũng thuyết phục được ông.

Tôi vã mồ hôi. Họ đã nghe lén tôi bao lâu rồi mà tôi không biết? Hàng nghìn câu hỏi chạy qua đầu tôi. Liệu Teltec có phải là mục tiêu hay đây chính là một kế hoạch tinh vi của đội An ninh Pacific Bell nhắm vào tôi – một cách để thực hiện tấn công bằng kỹ thuật xã hội với lũ hacker? Trái tim tôi đập loạn xạ khi tôi cố gắng nhớ lại những gì mình đã nói và làm từ điện thoại ở nhà cha tôi. Họ đã nghe thấy gì? Họ đã biết được bao nhiêu?

Sau năm phút, tôi gọi vào điện thoại công cộng ở chợ. “Cha,” tôi nói với ông, “hãy ném ngay cái máy tính ra khỏi nhà. Cha phải làm ngay lập tức! Đừng đợi gì nữa! Những thiết bị nghe lén đó không nhắm đến Teltec nữa mà bọn chúng đang nghe lén chúng ta! Cha phải mang cái máy tính đi ngay – nhanh lên!”

Ông đồng ý nhưng rất bực bội.

Cuộc gọi kế tiếp là tới Lewis, với nội dung tương tự: “Phải chạy cleanup mode[59] ngay.” Chúng tôi thống nhất cả hai sẽ giấu đống giấy ghi và đĩa floppy ở những nơi không ai có thể tìm thấy.

[59] Cleanup mode: Chế độ xóa dữ liệu. (ND)

https://thuviensach.vn

Cứ để lũ chính quyền khởi tố đi: Không có bằng chứng thì sẽ không có án nào được lập.

Tôi lái xe tới chỗ mẹ ở Las Vegas, đầu vẫn còn căng lên. Tôi không ngừng lặp đi lặp lại trong tâm trí tất cả những cuộc hội thoại có thể đã bị nghe lén.

Điều gì sẽ xảy ra nếu họ đã nghe thấy tôi bàn với Lewis về SAS? Nếu họ nghe thấy tôi thực hiện tấn công bằng kỹ thuật xã hội với các phòng ban của Pacific Bell thì sao? Chỉ tưởng tượng ra mấy khả năng này thôi cũng khiến tôi thấy phát sốt. Tôi gần như đã chờ đợi Sở Cảnh sát Tư pháp Liên bang và Phòng Quản chế xuất hiện trước cửa để bắt tôi.

Tôi cần phải biết thiết bị nghe lén đã được cài ở dây điện thoại của cha tôi từ lúc nào.

Có lẽ nếu biết ai đã yêu cầu đặt giám sát, tôi có thể tìm hiểu được liệu họ có nghe ra điều gì đó đáng lo ngại hay không.

Gần đây, các công ty điện thoại đã nhận quá nhiều cuộc gọi từ phone phreak và thám tử tư tới mức họ bắt đầu yêu cầu xác minh. Tôi gọi tới Dispatch, bộ phận chuyên giao nhiệm vụ cho các kỹ thuật viên hiện trường ở Pacific Bell và nói: “Tôi gặp tình huống phá hoại ở đây, tôi cần nhắn tin cho vài kỹ thuật viên khác. Ai sẽ trực đêm nay?”

Người trực máy báo cho tôi bốn cái tên và số máy nhắn tin. Tôi nhắn cho từng người yêu cầu gọi đến một số nội bộ của Pacific Bell mà tôi đã dựng lên, sau đó lại thiết lập để các cuộc gọi đó chuyển tới số điện thoại cầm tay của tôi. Khi từng kỹ thuật viên phản hồi lại tin nhắn, tôi sẽ bắt đầu trò “thành lập cơ sở dữ liệu” của mình.

Tại sao tôi lại làm thế? Bởi tôi đang hỏi họ những thông tin rất nhạy cảm và họ sẽ không tự nhiên nói cho bất kỳ ai đó quan tâm. Do đó, kỹ thuật pretexting như sau: “Tôi đang thành lập một cơ sở dữ liệu về các nhân viên làm nhiệm vụ xử lý các vấn đề trọng yếu.” Tôi hỏi một chuỗi những câu hỏi

https://thuviensach.vn

vô thưởng vô phạt tới từng người một – “Tên anh là gì?” “Anh xử lý những vấn đề gì ở Dispatch?” “Quản lý của anh là ai?” Khi họ đã quen dần với việc trả lời các câu hỏi đưa ra, tôi mới bắt đầu hỏi những gì mình thực sự muốn biết: “UUID của anh là gì? Mã kỹ thuật viên của anh nữa?”

Lần nào tôi cũng thu được thông tin mình cần, tất cả đều khai báo thông tin xác minh (UUID và mã kỹ thuật viên) của họ, tên quản lý và số gọi lại. Dễ như ăn cháo.

Với các thông tin bí mật này trong tay, tôi đã có thể quay lại bộ phận phân bổ đường dây để có được những thông tin cần thiết tiếp theo.

Sau khi xác minh xong, tôi đưa ra yêu cầu: “Tôi có một số nội bộ ở Calabasas – một trong những thuê bao của chúng ta. Anh có thể tìm ra số CBR của người đặt yêu cầu không?”

“CBR” là thuật ngữ điện tử viễn thông của “can be reached” (có thể liên lạc). Tôi đang hỏi số điện thoại để có thể liên lạc với người đặt yêu cầu thiết lập đường dây – trong trường hợp này, đó là đường dây điện thoại của âm tín hiệu cao tần trên hộp giám sát điện thoại của cha tôi.

Người phụ nữ tìm kiếm một hồi, sau đó trả lời: “Yêu cầu được thực hiện bởi đội An ninh Pacific Bell; tên liên lạc là Lilly Creeks.” Cô ta cho tôi số điện thoại có đầu mã vùng của San Francisco.

Kế tiếp là phần yêu thích của tôi: Tấn công bằng kỹ thuật xã hội đối với Phòng An ninh của công ty điện thoại.

Bật tivi lên, tôi tìm được một chương trình có tiếng trò chuyện mà tôi có thể vặn nhỏ tiếng để tạo cảm giác tiếng ồn đặc trưng ở một văn phòng làm việc nào đó. Tôi cần tạo ảnh hưởng tới nhận định của mục tiêu rằng tôi đang ở trong một tòa nhà với những người khác nữa.

Sau đó, tôi quay số gọi.

https://thuviensach.vn

“Lilly Creeks đây,” cô ta trả lời.

“Chào cô Lilly,” tôi nói. “Tôi là Tom ở Calabasas. Chúng tôi có mấy hộp thiết bị của cô ở đây và phải ngắt kết nối chúng. Chúng tôi cần chuyển vào một số trang thiết bị lớn, chúng sắp đến rồi.”

“Anh không thể ngắt mấy hộp đó được,” cô ta trả lời, gần như rít lên.

“Nghe này, không có cách nào khác cả, nhưng tôi sẽ gắn chúng lại vào chiều mai.”

“Không,” cô ta kiên quyết. “Chúng tôi thực sự cần giữ nguyên trạng mấy chiếc hộp đó.”

Tôi thở dài một tiếng lớn, hy vọng là nó nghe có vẻ cáu kỉnh và bực bội. “Chúng tôi có rất nhiều thiết bị phải thay đổi trong ngày hôm nay. Mong là việc của cô phải rất quan trọng, để tôi xem có thể làm gì được không.”

Tôi tắt âm điện thoại và chờ đợi. Sau khi nghe thấy tiếng thở của cô ta trong ống nghe khoảng chừng năm phút, tôi quay trở lại cuộc thoại. “Thế này có được không? Cô giữ nguyên điện thoại nhé, tôi sẽ ngắt kết nối của mấy chiếc hộp đó để chuyển thiết bị vào, sau đó tôi sẽ nối lại cho cô. Tôi chỉ có thể làm đến vậy thôi – được chứ?”

Cô ta miễn cưỡng đồng ý. Tôi nói với cô ta rằng sẽ mất chừng vài phút.

Tôi tắt âm thoại một lần nữa, sau đó gọi cho đội thiết bị ở Calabasas bằng một chiếc di động khác, giải thích với đầu dây bên kia rằng tôi đang ở cùng đội An ninh của Pacific Bell. Tôi báo cho anh ta cả ba số và các thiết bị văn phòng gắn kèm. Anh ta dò số trên COSMOS để tìm vị trí khung dựa trên “OE”. Khi tìm ra các số trên khung, anh ta ngắt kết nối từng máy giúp tôi.

Creeeks lúc này đang ngồi bên bàn làm việc đã có thể thấy các kết nối bị ngắt.

https://thuviensach.vn

Khi đợi kỹ thuật viên thiết bị quay trở lại đường dây và thông báo đã ngắt mạch, tôi bước ra tủ lạnh để kiếm một chai Snapple trong khi mường tượng trong đầu hình ảnh Lilly đang ngồi ôm điện thoại bên tai và lo lắng biết bao.

Bây giờ mới đến màn chính, tất cả trước đó chỉ để dẫn dắt mà thôi. Quay trở lại với Lilly, tôi nói: “Tôi xong rồi đây. Cô có muốn kết nối lại với các hộp không?”

Cô ta có vẻ bực mình. “Đương nhiên rồi!”

“Tôi cần thông tin kết nối của từng đường dây dẫn vào các hộp.” Cô ta hẳn phải nghĩ tôi có chút trì độn khi không nhớ được vị trí gắn đầu nối dù chỉ mới tháo ra vài phút trước đó, nhưng yêu cầu này có vẻ đáng tin cậy vì chính mắt cô ta đã thấy kết nối bị ngắt: Rõ ràng là cô ta đang nói chuyện với kỹ thuật viên thiết bị ở CO.

Cô ta cho tôi thông tin. Tôi nói: “Được rồi, tôi sẽ quay lại ngay.”

Tôi tắt âm thoại một lần nữa, sau đó gọi lại cho kỹ thuật viên ở CO Calabasas và nhờ anh ta kết nối cáp lại vào “các hộp bảo mật của chúng tôi”.

Khi anh ta làm xong, tôi cảm ơn và quay lại đầu dây bên kia. “Cô Lilly,” Tôi nói: “Tôi đã gắn lại hết rồi đó. Chúng hoạt động bình thường chưa?”

Cô ta có vẻ yên tâm. “Mọi thứ đều bình thường rồi. Có vẻ là vẫn ổn.”

“Được rồi. Để kiểm tra lại cho chắc, số thuê bao nào đang gắn với các hộp này vậy? Tôi sẽ xác minh đường dây để đảm bảo mọi thứ đã được kết nối đúng.”

Cô ta cho tôi các số điện thoại.

Khốn kiếp! Họ không chỉ theo dõi một đường điện thoại của cha tôi mà là cả ba! Tôi chắc chắn sẽ không gọi thêm một cú điện thoại nào bằng máy của ông nữa.

https://thuviensach.vn

Tôi vẫn cần phải biết những thiết bị này được cài đặt từ bao giờ, có vậy tôi mới có thể lường được cuộc gọi nào của mình đã bị nghe lén.

Sau đó, chỉ để cho vui, Lewis và tôi muốn nghe lén một trong những đường dây điện thoại khác mà Pacific đang theo dõi.

Có một vướng mắc ở đây: Để tăng thêm tính bảo mật, những chiếc hộp này sẽ không theo dõi đường dây điện thoại cho tới khi nhập vào một số PIN hợp lệ, hay còn gọi là "mã số nhận dạng cá nhân" (Personal Identification Number). Tôi có một ý tưởng tuy hơi viển vông với khả năng thành công rất thấp nhưng tôi vẫn thử.

Đầu tiên, tôi phải gọi vào các hộp giám sát ở CO. Sau đó, tôi gọi cho CO và nói với kỹ thuật viên thiết bị ở đầu dây bên kia: "Tôi cần ngắt đường dây để kiểm tra." Anh ta làm theo và thế là kết nối của Pacific Bell bị ngắt khỏi hộp giám sát.

Tôi gọi vào hộp và bắt đầu đoán mật khẩu do nhà sản xuất cài đặt: "1 2 3 4"… không có gì. Mãi cho đến số cuối cùng mà tôi cho là đáng để thử: "1 2 3 4 5 6 7 8".

Chính xác! Thật kỳ diệu, mấy gã ở Phòng An ninh Pacific Bell chưa từng thử đổi số PIN mặc định của nhà sản xuất trên mấy chiếc hộp này.

Có được mật khẩu, giờ tôi đã có đủ kỹ thuật để nghe lén bất kỳ một máy giám sát nào của Pacific Bell trên toàn California. Giả sử, nếu Phòng An ninh có một trong các hộp đặt tại CO Kester hay CO Webster, tôi có thể yêu cầu kỹ thuật viên thiết bị ngắt đường dây mà Pacific Bell dùng để gọi tới hộp giám sát và sau đó, tôi sẽ tự gọi vào hộp giám sát để nhập mã PIN mặc định, vốn giống hệt nhau trên mọi máy. Từ đó, Lewis và tôi có thể nghe lén và tìm ra được ai là người đang bị theo dõi.

Chúng tôi làm việc này chỉ để cho vui, bởi chúng tôi có thể, thường là hai đến ba lần một tuần. Sau khi xác định được số điện thoại của đối tượng, tôi

https://thuviensach.vn

sẽ gọi cho Cục Tên và Địa điểm Khách hàng (CNL) để báo cho họ số điện thoại và lấy được tên của người bị giám sát. Có lần, tôi còn biết được số điện thoại thuộc về Quý-Ngài-Tôn-Quý[60]. Đào sâu hơn một chút thì phần còn lại đã sáng tỏ: Máy giám sát được đặt trên đường dây của một thẩm phán liên bang.

[60] Từ gốc "Your honor": Danh xưng tôn trọng thường dùng khi đề cập tới quan tòa hoặc thị trưởng trong tiếng Anh. (ND)

Với Lewis và tôi, nghe trộm mấy cuộc nghe lén chỉ là một trò chơi, một trò nghịch ngợm. Còn đối với những kẻ điều tra thuộc tổ An ninh của Pacific Bell thì đó là một phần công việc. Một trong những nhân viên điều tra, Darell Santos, đã gặp bất ngờ lớn. Anh ta bước vào văn phòng làm việc vào một buổi sáng, lắng nghe những gì được tiết lộ qua máy giám sát đặt trên điện thoại của cha tôi và phát hiện ra tất cả thiết bị giám sát điện tử của Pacific Bell đã tạm ngừng hoạt động. Không có ghi âm cuộc gọi nào; mọi thứ đều chết cứng. Santos gọi cho kỹ thuật viên thiết bị ở Calabasas và hỏi: "Mấy chiếc hộp của chúng tôi vẫn còn hoạt động đó chứ?"

"À, không," anh ta nghe thấy câu trả lời. "Nhân viên an ninh từ Los Angeles đã gọi tới và yêu cầu chúng tôi ngắt kết nối."

Santos nói với nhân viên kỹ thuật: "Chúng tôi không thực hiện giám sát ở Nam California: Tất cả đều ở Bắc California. Không có ai tên là nhân viên an ninh ở Los Angeles hết."

Ngay đêm đó, Santos bay từ chi nhánh ở San Francisco tới Los Angeles và tự mình nối lại tất cả các hộp giám sát. Để đảm bảo không ai có thể ngắt kết nối một lần nữa, anh ta giấu những chiếc hộp trên xà nhà, phía trên đống trang thiết bị chuyển mạch.

Rất lâu sau, trong một buổi phỏng vấn để thực hiện cuốn sách này, Santos nhớ lại: "Đây là vấn đề lớn đối với chúng tôi, bởi khi nó hiển hiện trước mắt, đó là vấn đề mang tính cá nhân. Kevin đã nghe được tất cả cuộc gọi của

https://thuviensach.vn

chúng tôi, trong khi chúng tôi thì cố gắng nghe được các cuộc gọi của anh ta. Sau đó, anh ta ngắt toàn bộ máy giám sát. Điều này khiến chúng tôi phải thay đổi cách nói chuyện trên điện thoại và các tin nhắn lưu lại. Và chúng tôi phải tìm ra các phương thức mới để che giấu việc làm của mình (trước Kevin), bởi chúng tôi cần hoàn thành nhiệm vụ hợp tác với cảnh sát trong việc giám sát theo chỉ thị từ phía tòa án."

Đây là việc vô thưởng vô phạt bởi tôi đã không nhận thức được những rắc rối mình mang tới cho họ – bởi nếu biết, có lẽ tôi đã không làm như vậy.

Và tôi hẳn phải rất vinh dự khi biết rằng vào thời điểm đó, khi có bất kể sự việc gì tương tự diễn ra ở Pacific Bell, tôi sẽ là đối tượng tình nghi đầu tiên. Theo Santos, Kevin Poulsen đứng đầu tiên trong danh sách truy lùng của họ. Tới khi Poulsen bị tống vào tù, danh sách chỉnh sửa đã có cái tên mới ở hàng đầu: tên tôi. Tất cả tư liệu họ có về tôi từ tận những ngày niên thiếu đã dày bằng một cuốn sổ danh bạ điện thoại ở thành phố lớn.

Santos nói: "Có cả các hacker khác cũng làm rất nhiều việc khác nữa, nhưng theo tôi, Kevin là người mà tất cả bọn họ muốn noi theo. Tôi cho rằng Kevin là chuột còn tôi là mèo, nhưng hóa ra đôi khi lại ngược lại."

Anh ta còn thêm vào: "Nhiều khi mấy gã từ đội an ninh của các công ty khác đã hỏi chúng tôi, 'Này, chúng tôi có vụ này, có một gã đang cố chơi chúng tôi, anh có nghĩ rằng đó là Kevin không?' Khi có một vụ nào đó xảy ra, mọi người đều nghĩ đến Kevin."

Tôi có thể nói rằng, thời ấy tôi hẳn phải rất tự hào khi biết những điều này, nhưng sau đó là một nỗi chán nản. Tính tới thời điểm đó, tài năng của tôi chưa giúp được gì trong việc tìm hiểu về Eric Heinz. Lewis và tôi rơi vào vòng luẩn quẩn những mối nghi ngờ về hắn. Đúng là hắn biết nhiều thứ về hệ thống và các quy trình của công ty điện thoại, thậm chí cả những điều tôi và Lewis chưa từng nghe nói tới. Nhưng thứ nhất, hắn không sẵn lòng chia

https://thuviensach.vn

sẻ. Thứ hai, hắn vẫn luôn đặt những câu hỏi mà các hacker không bao giờ hỏi nhau: “Cậu đang làm cùng ai đấy?” và “Gần đây cậu làm vụ gì đấy?”…

Đã đến lúc chúng tôi phải trực tiếp đối mặt với hắn và xem xem liệu chúng tôi có thể vơi bớt sự nghi ngờ khi biết thêm về hắn nhiều hơn một chút không. Và nếu là thực, biết đâu hắn có thể giúp tôi tìm hiểu xem những máy giám sát đó đặt trên đường dây điện thoại của cha tôi từ lúc nào.

https://thuviensach.vn

15

“LÀM THẾ QUÁI NÀO CÁC CẬU CÓ ĐƯỢC NÓ?”

Ituot oaybmzk ymwqe ftq pqhuoq ftmf Xqiue geqp fa buow gb mzk dmpua euszmxe zqmd Qduo?

Thật ngạc nhiên khi Eric rất sẵn lòng gặp chúng tôi vào bữa tối. Chúng tôi dàn xếp một cuộc hẹn vài ngày sau đó tại nhà hàng Hamburger Hamlet gần Tây Los Angeles. Lewis và tôi đều lo lắng về buổi gặp tới mức Lewis nói cậu ta sẽ mang một loại đồ nghề đặc biệt được thiết kế để xoa dịu nỗi hoảng loạn trong tôi.

Chúng tôi gặp nhau tại một bãi đỗ xe trước giờ hẹn khoảng nửa tiếng. Khi tôi chui vào xe, Lewis đang chăm chú nghe một máy quét sóng phát thanh. Không cần hỏi tôi cũng biết Lewis đang nghe gì: Máy quét này được lập trình để bắt tất cả các tần số do FBI, Cục Tình báo và Cục Cảnh sát Tư pháp sử dụng. Chưa kể, bởi FBI đang phải đương đầu với một kẻ được cho là rất hiểu biết về công nghệ, nên họ thường trở nên tinh quái và quyết định dùng tần số của một số cơ quan khác như Cục Nhà tù. Cơ quan Bài trừ Ma túy hay thậm chí là Dịch vụ Giám sát Bưu chính, v.v... Vì vậy, Lewis đã lập trình cả những tần số này.

Máy quét không thể bắt được những tín hiệu từ xa mà chỉ bắt được những tín hiệu đủ mạnh đến từ một nơi gần đó. Trong khu vực này, hầu hết tất cả cơ quan hành pháp liên bang đều đủ khôn ngoan để mã hóa liên lạc của họ. Nhưng chúng tôi không cần biết họ đang nói gì mà chỉ muốn biết họ có đang nói điều đó ở gần đây không. Nếu các tần số của lực lượng chấp pháp bắt đầu rung, chúng tôi sẽ chuồn ngay lập tức.

https://thuviensach.vn

Giờ thì, tất cả đều đang im lặng, nhưng để đề phòng, Lewis luồn vài thiết bị điện tử hay ho vào túi khi chúng tôi bước ra khỏi xe.

Chúng tôi đã đồng ý gặp nhau ở nhà hàng này bởi địa điểm này rất thuận tiện. Quán Hamburger Hamlet hóa ra có một kiểu trang trí cổ lỗ với gương, đồng thau và gạch, có tác dụng phụ là biến các cuộc hội thoại trong một khu vô cùng đông đúc thành tiếng vo ve ồn ã. Thật hoàn hảo, bởi chúng tôi muốn chắc chắn không ai ngồi bàn bên nghe lỏm được mình.

Eric bảo chúng tôi tìm một người đàn ông có mái tóc vàng dài ngang vai và một chiếc laptop. Ngay cả giữa một rừng các kiểu người trông như Hollywood ngồi gặm những chiếc bánh burger to dày, không mấy khó khăn để nhận ra hắn. Dáng người gầy trong chiếc áo lụa để hở ngực, nhìn hắn chẳng khác nào một nghệ sĩ nhạc rock – hay đúng hơn là một gã đang cố ăn vận để có được phản ứng thường gặp: “Tôi biết khuôn mặt này, nhưng không thể nhớ ra anh ta ở nhóm nhạc nào.”

Chúng tôi mở lời chào, giới thiệu bản thân, ngồi xuống và cho anh ta biết rõ ngay từ đầu chúng tôi không có lý do gì để nghĩ rằng mình có thể tin anh ta. Lewis và tôi mỗi người đều mang máy dò cầm tay RadioShack Pro-43 và chúng tôi để chúng ngay trên bàn. Lewis cũng mang theo máy phát hiện tần số vô tuyến điện quang điện tử – một thiết bị được thiết kế để phát hiện các tín hiệu phát đi từ micro gắn trên người – và anh ta công khai vung vẩy nó khắp người Eric. Cái máy không bắt được gì cả.

Suốt buổi hôm đó, Eric có vẻ háo hức ngó nghiêng rào đón các cô nàng, trong khi vẫn kể những câu chuyện không dứt về lịch hẹn hò của hắn chật kín ra sao, cũng như chi tiết về sự phóng túng trong tình dục của mình. Lewis có vẻ cam chịu chuyện đó và thậm chí còn cổ vũ câu chuyện tràng giang đại hải mang đầy tính huênh hoang này, nhưng tôi chưa bao giờ tin mấy gã có nhu cầu tô vẽ bản thân trước những thằng đàn ông khác rằng mình là một tay Sở Khanh thực thụ. Việc này khiến tôi tự hỏi liệu mình có tin được bất kỳ thông tin nào Eric có thể sẽ cho chúng tôi biết về các công ty

https://thuviensach.vn

điện thoại hay không – mục đích duy nhất của nhiệm vụ lần này – ngay cả khi chúng tôi có thể moi được từ hắn.

Dù sao thì, cuối cùng, hắn cũng chịu nhả ra một mẩu thông tin trong buổi nói chuyện khiến tôi thực sự chú ý. Hắn khẳng định mình có một chiếc chìa khóa vạn năng cho phép đột nhập vào CO của mọi công ty điện thoại, được để lại từ thời hắn và Kevin Poulsen còn hay ghé thăm các CO buổi đêm ở khắp Los Angeles.

Tôi gần như chỉ ngồi nghe. Bởi đáng lý ra tôi không được phép có bất kỳ giao thiệp nào với các hacker khác, tôi đã bảo Lewis nói thay phần cả hai chúng tôi. Eric ba hoa rằng mình từng là một kỹ sư âm thanh trên đường phố, nhưng hắn không kể tên bất kỳ ban nhạc nào hắn từng làm việc cùng, tôi đoán họ là những nhóm vô danh. Rồi hắn cố gây ấn tượng với chúng tôi bằng những thứ hắn có nhưng chúng tôi thì không: Ngoài chiếc chìa khóa vạn năng hay mã cửa của tất cả CO, hắn khẳng định hắn còn có cả chìa khóa vạn năng cho tất cả các "B-box" – những chiếc hộp của công ty điện thoại nằm rải rác trên các con đường ở mọi thành phố, thứ các kỹ thuật viên hiện trường viện tới khi họ cần mắc dây điện thoại đến các hộ dân và doanh nghiệp. Nghe như thể hắn đang hy vọng điều này sẽ hấp dẫn được chúng tôi, khiến chúng tôi phải cầu xin: "Liệu chúng tôi có thể đi cùng trong một lần đột nhập tới của anh không?"

Rồi hắn bắt đầu nói về những lần đột nhập buổi đêm vào các CO của công ty điện thoại với Kevin Poulsen và một hacker khác, Ron Austin, để thu thập thông tin và lấy quyền truy cập vào các hệ thống nội bộ của Pacific Bell. Và hắn đã tham gia vào cuộc thi hack điện thoại trên radio ra sao, khi Poulsen đã trúng lớn khi thắng hai chiếc Porsche. Ngoài ra, Eric còn nhắc tới hai chuyến du lịch đến Hawaii.

Eric nói hắn cũng thu được một chiếc Porsche trong lần hack đó.

https://thuviensach.vn

Có một sự việc có vẻ có chút sự thật: Hắn kể lại việc FBI đã tóm Poulsen ra sao. Họ phát hiện ra cậu ta thường đi mua tạp hóa ở khu Hughes Market nên đã qua đó và cho nhân viên xem ảnh của hắn. Một ngày nọ, khi Poulsen bước vào, một vài nhân viên xếp hàng lên giá nhận ra cậu ta. Họ xô ngã cậu ta và giữ lại cho đến khi cảnh sát đến.

Lewis, người có nhu cầu thể hiện mình thông minh ra sao, lôi chiếc điện thoại di động Novatel PTR-825 của anh ra và thực hiện một bài diễn văn về việc anh đã "thay ESN trên chiếc điện thoại này" ra sao. Và thế là Eric cũng huênh hoang rằng hắn đã làm điều tương tự với chiếc Oki 900 của hắn, việc này không thực sự có gì to tát bởi lúc bấy giờ đã có phần mềm trên mạng rồi. Rồi hắn nói về việc tiếp sóng ham radio ở tần số 147,435, tần số mà tôi vốn coi như một "trại gia súc". Ố ồ, tôi không nghĩ là hắn biết việc này, từ nay về sau, tôi sẽ phải cẩn thận không nói những gì mình không muốn Eric nghe thấy qua bộ tiếp sóng đó.

Rồi chúng tôi đi đến mối quan tâm chính: hack vào Pacific Bell. Eric rõ ràng đang cố gây dựng niềm tin với chúng tôi qua việc hắn có quyền truy cập vào mọi hệ thống của Pacific Bell.

Được rồi, tôi đã nghĩ có rất ít phreaker – khó có ai – biết nhiều về các hệ thống của Pacific Bell bằng Lewis và tôi. Vậy mà Eric lại có vẻ có kiến thức ngang bằng chúng tôi. Thật ấn tượng!

Điều khiến tôi choáng váng là hắn khẳng định Poulsen đã đột nhập vào văn phòng của Terry Atchley ở Phòng An ninh Pacific Bell và nhanh tay lấy được hồ sơ về cậu ta... và về tôi. Hắn nói Poulsen đã lập một bản sao toàn bộ hồ sơ của tôi và đưa cho hắn như một món quà.

"Anh có bản sao hồ sơ của tôi?"

"Đúng vậy."

https://thuviensach.vn

Dù tập hồ sơ này đã được thó khỏi văn phòng của Terry Atchley nhiều năm trước, nhưng tôi vẫn nói: “Này anh, tôi thực sự muốn xem bản sao đó.”

“Tôi không chắc nó ở đâu. Tôi phải kiếm lại đã.”

“Vậy ít nhất hãy cho tôi biết trong đó có gì đi. Họ biết gì về những việc tôi làm ngày đó?”

Bỗng dưng hắn lưỡng lự, lảng tránh câu hỏi của tôi thay vì trả lời. Có thể hắn chưa bao giờ có tập hồ sơ hoặc có thể hắn đã giữ lại thông tin về tôi vì lý do nào đó. Tôi thấy bực bội khi hắn không cho mình biết thông tin trong hồ sơ. Nhưng tôi không muốn ép hắn quá mức, đặc biệt là trong buổi gặp đầu tiên.

Cuộc nói chuyện tiếp tục và Eric luôn quay sang hỏi chúng tôi đang làm gì – nghĩa là chúng tôi đang hack gì. Việc này chẳng hay ho gì. Cả Lewis và tôi đều đưa cho hắn những câu trả lời kiểu như “Anh hãy nói cho chúng tôi một số thứ anh biết, chúng tôi sẽ nói cho anh một số thứ chúng tôi biết.”

Giờ là lúc Lewis và tôi khiến tay cộng sự mới học đòi của mình phải choáng váng rụng rời. Lewis nhập vai tới bến. Bằng giọng nói ngạo mạn kinh hoàng, cậu ta nói: “Eric, chúng tôi có một món quà cho anh.” Lewis lấy ra một chiếc đĩa mềm, với tay qua bàn và với phong thái đúng chất bỗ bã của mình, nhét nó vào ổ đĩa laptop.

Sau một hồi kêu vù vù, màn hình hiện ra danh sách liệt kê tất cả các phương thức SAS, các mục như một lệnh dạng “;ijbe” ra lệnh cho đơn vị SAS thực hiện một số chức năng như “Báo cáo tình trạng hiện tại”. Chúng là những lệnh ẩn, nằm sâu trong bộ điều khiển SAS, các kỹ thuật viên kiểm tra của công ty điện thoại không bao giờ biết hay cần đến chúng, nhưng chúng mang lại rất nhiều quyền kiểm soát SAS so với những gì họ có.

Eric đủ hiểu về SAS để nhận ra danh sách đó là thật và đó là thứ bản thân hắn chưa bao giờ được tiếp cận.

https://thuviensach.vn

Trông hắn ta vừa choáng váng vừa giận giữ khi Lewis và tôi có thể chiếm được một thứ mà hắn không thể. Hắn gằn giọng gầm rú: “Làm thế quái nào các cậu có được nó?” Tôi nghĩ việc này thật kỳ quặc – tại sao hắn ta lại tức giận? Có thể hắn đang thực sự cảm thấy đố kỵ, bực bội khi hắn chỉ có thể đọc hướng dẫn sử dụng trong khi chúng tôi lại có tài liệu của các nhà phát triển hé lộ thêm rất nhiều bí mật và quyền năng.

Eric bắt đầu lật qua các trang tài liệu trên màn hình và có thể thấy chúng cũng có đầy đủ các đặc tả và yêu cầu kỹ thuật vận hành. Hắn hiểu đây là nguồn thông tin giá trị sẽ ban cho bất kỳ phone phreaker nào quyền năng mà anh ta chỉ có thể thấy trong mơ.

Lúc này là khoảng một tháng sau khi hắn nhắc đến SAS lần đầu tiên với tôi trong một cuộc điện thoại. Bối rối hơn, những thứ mà chúng tôi cho hắn xem không phải là bản sao mà là một tập tin điện tử. Tôi có thể thấy hắn đang quay mòng mòng: Hắn không hiểu nổi tôi đã làm việc đó như thế nào – lấy được tài liệu thiết kế của các nhà phát triển, và thậm chí, một phiên bản điện tử của chúng, vốn có thể không tồn tại ở bất kỳ đâu trong Pacific Bell.

Hắn lại hỏi lần nữa, “Làm... thế... quái... nào các cậu có được nó?”

Tôi nói với hắn điều mà chúng tôi đã nói vài lần: “Khi anh chia sẻ thông tin với chúng tôi, chúng tôi sẽ chia sẻ thông tin với anh.” Trong lúc tôi nói, Lewis với tay qua bàn, rút chiếc đĩa ra khỏi máy tính và bỏ vào túi áo.

Eric cảnh báo chúng tôi: “FBI biết về SAS bởi họ biết Poulsen đã dùng nó. Họ đang theo dõi nó rất sát sao. Họ chắc hẳn đã cài bẫy tất cả các số điện thoại rồi.”

Với một giọng gần như hăm họa, hắn nói: “Hãy tránh xa thứ này. Các anh sẽ bị tóm nếu dùng nó.” Nếu đó chỉ là một lời cảnh báo thân thiện, tại sao nó lại nhiều cảm xúc đến vậy?

https://thuviensach.vn

Vừa đến đó, Eric nói hắn phải đi giải quyết. Hắn đứng dậy và đi về phía nhà vệ sinh nam. Có một thủ tục ứng xử tiêu chuẩn của bất kỳ hacker nổi danh nào đang sở hữu những loại tập tin hay mật khẩu trên máy tính có thể khiến anh ta bị quăng vào tù. Nếu anh ta đến đâu đó và có mang theo laptop, anh ta sẽ không bao giờ để nó khuất khỏi tầm nhìn, ngay cả khi chỉ rời bàn một, hai phút đi vệ sinh. Vậy mà Eric lại vô tư đi khỏi và để lại laptop của hắn không chỉ trên bàn mà còn đang bật, như một lời mời kiểm tra xem chúng tôi có thể tìm thấy gì trong lúc hắn không có mặt. Lewis lôi bộ đếm tần ra và ve vẩy nó chậm chạp qua lại, tìm các tín hiệu phát ra. Không có gì cả. Chiếc máy tính này không phát đi cuộc nói chuyện của chúng tôi đến bất cứ đội cớm hay cảnh sát liên bang nào đang ẩn nấp gần đó, sẵn sàng đánh úp chúng tôi.

Tôi nghiêng qua chiếc laptop và báo với Lewis: “Này, gã này quả là biết hắn đang làm gì!” Thật nực cười – tôi chỉ nói vậy bởi tôi chắc chắn có một dạng máy ghi âm siêu nhỏ nào đó được cài trong laptop, ghi lại mọi lời nói. Nếu không hắn sẽ không bao giờ để nó lại trên bàn. Đây là gã vài tuần trước còn hoang tưởng đến mức không cho chúng tôi số máy nhắn tin của hắn, giờ bỗng dưng lại tin tưởng cho chúng tôi xem laptop của hắn? Không đời nào.

Tôi đoán có thể hắn có một cộng sự nào đó ở bàn khác, theo dõi chúng tôi để chắc chắn rằng chúng tôi không chỉ đơn giản chộp lấy và chạy. Nếu không, hắn sẽ không dám để chiếc máy tính với cả tấn thông tin có thể định tội hắn nằm dưới sự kiểm soát của hai gã hắn chỉ mới gặp lần đầu.

Khi chúng tôi xong bữa tối và chuẩn bị rời đi, Eric hỏi: “Nếu các cậu có xe, có thể cho tôi đi nhờ không? Không xa lắm đâu.” Tất nhiên rồi, tôi nói, tại sao không?

Hắn bắt đầu thân thiện, nói với tôi về khoảng thời gian cách đây chưa lâu khi hắn lượn lờ trên Đại lộ Sunset bằng chiếc xe máy rồi có một chiếc xe rẽ trái cắt ngang làn của hắn. Vụ va chạm làm hắn bay qua chiếc ô tô, lăn xuống đất mạnh đến nỗi gãy ống chân và phần bàn chân bị trẹo ra sau một

https://thuviensach.vn

góc 90o. Các bác sĩ và trị liệu viên đã tiến hành hồi phục chân cho hắn trong năm tháng, cuối cùng, Eric đành nói với họ hãy tiến hành cắt bỏ nó đi. Nhưng cái chân giả tốt đến mức sau khi vật lý trị liệu ở trung tâm, hắn đã có thể đi lại mà không thấy khập khiễng.

Câu chuyện có lẽ là để tôi thông cảm với hắn. Giờ hắn sang số và nói: “Tôi rất tức giận về chuyện các cậu đột nhập SAS. Sau bốn tuần, các cậu đã có nhiều thông tin hơn cả tôi.”

Tôi dùng chuyện đó để khích hắn: “Chúng tôi biết nhiều hơn rất nhiều so với cậu nghĩ, Eric.”

Nhưng tôi vẫn đang cẩn trọng, nên tôi bảo hắn: “Lewis và tôi hiện không còn hack nữa; chúng tôi chỉ muốn trao đổi thông tin.”

Khi hắn rời xe vào một câu lạc bộ nhạc jazz trên Đại lộ Sunset, tôi nghĩ thầm gã này có vẻ có trí tuệ sắc bén và trí thông minh nhanh nhạy. Bất chấp những ngờ vực của mình, tôi vẫn tin Lewis và tôi có thể trao đổi thông tin với hắn một dịp nào đó sau này.

https://thuviensach.vn

16
KHÁCH KHÔNG MỜI MÀ TỚI

Kwth qzrva rbq lcq rxw Svtg vxcz zm vzs lbfieerl nsem rmh dg ac oef'l cwamu?

Từ sau bữa tối hôm đó, tôi không ngừng nghĩ về chiếc chìa khóa Eric nói, chiếc chìa khóa giúp hắn có thể đi vào bất kỳ CO nào của Pacfic Bell. Tôi quyết định hỏi mượn chìa. Tôi không định nói mình cần nó để làm gì nhưng kế hoạch là tôi sẽ đột nhập vào CO ở Calabasas, đăng nhập vào máy tính COSMOS và cố tìm hiểu xem những thiết bị giám sát kia được cài đặt vào đường dây của cha tôi từ lúc nào. Và liệu có đúng là có ghi chú trong COSMOS rằng khi có ai đó đặt câu hỏi về những đường dây này thì không ai được đưa ra bất kỳ thông tin nào hoặc gọi ngay tới đội An ninh.

Vào được CO, tôi có thể biết được những hộp nào kết nối tới điện thoại của cha tôi và xác minh được những số mà mấy kẻ nghe lén dùng để gọi tới. Có được những số này rồi, tôi có thể tra trong COSMOS và tìm ra ngày kích hoạt, từ đó biết được việc giám sát bắt đầu từ khi nào.

Vào khoảng 10 giờ một đêm tháng Hai, Lewis và tôi lái xe tới khu chung cư của Eric, lần theo địa chỉ mà tôi có được từ Pacific Bell sau khi lấy được số của hắn nhờ sử dụng một chút mánh khóe Caller ID. Một tòa nhà ấn tượng, một khu tổ hợp có phần sang chảnh và cao cấp quá mức đối với một người như hắn – tòa nhà đắp hình nổi hai tầng với cửa vào khóa kín và cửa ga-ra điều khiển từ xa. Chúng tôi đợi tới khi có người lái xe ra khỏi ga-ra và bước vào. Tôi thậm chí có thể tưởng tượng ra bên trong từ trước khi nhìn thấy nó. Hành lang trải thảm, sân tennis, bể bơi có bồn sục, những cây cọ và phòng giải trí với màn hình tivi thật lớn.

https://thuviensach.vn

Gã hacker chuyên xuất hiện ở câu lạc bộ ban đêm này làm gì ở một khu chung cư vốn dành cho nhân viên của các công ty lớn, những người chỉ ở Los Angeles trong các đợt công tác ngắn ngày và sinh hoạt bằng tiền công?

Căn hộ 107B nằm trên một hành lang dài. Lewis và tôi thay phiên nhau áp tai vào cửa với hy vọng tiếng ồn bên trong có thể gợi ý cho chúng tôi biết là ai đang ở trong. Nhưng không có gì cả.

Chúng tôi tìm tới khu giải trí của tòa nhà và gọi đến phòng Eric từ một máy điện thoại công cộng. Tôi cười khi Lewis quay số, lấy làm thích thú bởi bất kỳ gã hacker có trình độ nào cũng phải nhớ rõ số điện thoại của máy điện thoại công cộng trong chung cư mình ở. Nếu Eric quả thực là một tay ra trò như hắn khẳng định, hắn phải thêm tính năng nhận diện cuộc gọi trên máy và nhận ra Lewis và tôi đang gọi từ chính căn hộ này.

Tội nghiệp Eric. Hắn tức điên khi thấy tôi tìm được số điện thoại của hắn và còn phát điên hơn nữa khi chúng tôi chỉ cách hắn vài mét. Tôi nói chúng tôi cần nói chuyện. Hắn nói: “Tôi không bao giờ mời hacker lên nhà.” Cuối cùng, hắn nói chúng tôi đợi năm phút và đi xuống gặp chúng tôi ở phòng giải trí.

Tôi lại bất ngờ một lần nữa khi hắn ta trông hệt như một tay nghệ sĩ nhạc rock, dáng cao gầy lêu nghêu, mái tóc vàng ngang vai, chân đeo bốt và mặc chiếc áo sơ mi thùng thình. Hắn nhìn chằm chằm vào chúng tôi. “Các cậu phải tôn trọng quyền riêng tư của tôi,” hắn rít lên. “Làm sao các cậu tìm ra tôi?” Hắn ta có vẻ lo lắng, như thể hắn nghĩ chúng tôi mang súng theo vậy.

Câu trả lời của tôi đầy chế nhạo. “Tôi rất giỏi mấy việc mình làm.”

Trên mặt tôi là nụ cười nhăn nhở. Hắn tiếp tục quay lại chủ đề trong ngày về việc chúng tôi không tôn trọng sự riêng tư của hắn ra sao. Tôi nói: “Chúng tôi không tới đây để xâm phạm quyền riêng tư của anh mà tới để nhờ giúp đỡ. Điện thoại của bạn tôi có thể đã bị Pacific Bell giám sát. Anh nói anh có chìa khóa vào CO nên chúng tôi muốn nhờ anh giúp.”

https://thuviensach.vn

Người “bạn” ở đây đương nhiên chính là tôi. Và chẳng có gì là “có thể đã bị” ở đây cả.

“CO nào?” hắn hỏi. Tôi không muốn nói cho hắn biết cụ thể. “Một ESS vệ tinh,” tôi trả lời, mô tả một loại bộ chuyển đổi. “Không người điều khiển vào ban đêm.”

“Hiện giờ chìa khóa không có ở đây,” hắn nói. “Tôi không muốn bị tóm cổ vì nó.”

“Cậu cho chúng tôi mượn được không?”

Không, hắn không thoải mái.

Lúc này, tôi nói sự thật. “À, thực ra không phải là bạn. Tôi tìm thấy họ đặt giám sát trên đường dây nhà tôi và có chút lo sợ vì không rõ họ đã biết được chừng nào. Tôi không biết ai đứng sau việc đó và cũng không biết nó bắt đầu từ bao giờ.”

Hắn ta hỏi làm sao tôi biết, tôi kể lại mình đã thực hiện tấn công bằng kỹ thuật xã hội với mấy tay kỹ thuật thiết bị ở Calabasas thế nào. Tôi cũng thể hiện rằng mình có thể tin tưởng được. Tôi nài nỉ hắn ta và cố bày ra cảm giác cấp bách bởi tôi cần có nó ngay lập tức. Tôi thực sự cần hắn đi lấy chiếc chìa khóa.

“Eric,” tôi nói, “nếu tôi tìm ra họ đã có đủ bằng chứng để tống tôi vào tù, tôi sẽ biến mất.” Ba chúng tôi nói chuyện thêm một hồi về các quốc gia không có hiệp ước dẫn độ với Mỹ.

Tôi thúc giục thêm về chuyện đột nhập, nhưng Eric không hứa hẹn gì cả, hắn nói hắn sẽ trả lời sau. Chúng tôi dành nhiều thời gian bàn luận xem các công ty điện thoại giám sát mọi người thế nào. Hắn thậm chí còn nói với tôi rằng hắn thường tới CO hằng tuần để đảm bảo không có thiết bị ghi âm cuộc gọi (Dial Number Recoders – DNR) nào gắn trên đường dây của mình.

https://thuviensach.vn

Eric vẫn không đồng ý cho tôi mượn chìa khóa, có điều hắn nói hắn sẵn lòng đưa tôi tới CO và vào cùng tôi. Do không thể hoàn toàn tin tưởng, tôi chỉ cho hắn một trong ba số giám sát mình có và không cho hắn biết mình có cả các số khác. Đây là một dạng kiểm tra, để xem gã này có đáng tin cậy hay không.

Cuối cùng, Lewis và tôi chào tạm biệt và bỏ đi.

Bất kỳ ai đề nghị Pacific Bell cài đặt giám sát đường dây đó có lẽ đã có đủ chứng cớ để tống tôi vào tù. Việc không rõ những kẻ nghe lén đã biết được điều gì khiến tôi thực sự hoảng hốt. Đôi khi tôi sợ phải ngủ ở nhà tới mức còn đặt một phòng trong nhà nghỉ bình dân để giải tỏa bớt căng thẳng.

Chúng tôi dự tính đột nhập cùng nhau, nhưng chỉ sau vài ngay, Eric liên tục đưa ra lý do này nọ về việc hắn ta không thể đi vào tối nay, rồi tối mai, rồi hắn phải làm việc cả cuối tuần. Trong khi đó, nỗi nghi ngờ trong tôi ngày càng lớn. Cách hành xử của hắn rất đáng ngờ; và tôi thì ngày càng lo lắng về mối nguy cơ này. Tôi nói với hắn ta: “Tôi sẽ không vào trong mà chỉ đứng quan sát thôi.” Cuối cùng cũng chọn được một ngày và chúng tôi quyết định cả ba sẽ cùng đi vào đêm sau đó.

Nhưng tới sáng hôm sau, Eric gọi điện và nói: “Tôi đã vào đó tối qua” và cho tôi số giám sát – tôi có thể nói rằng hắn đã cho tôi đúng số cần thiết. Hắn nói mình đã dò số trong COSMOS. Các số đó được thiết lập vào ngày 27 tháng 1, như vậy là mấy chiếc hộp phải được gắn vào khoảng sau đó.

Tôi hỏi Eric làm sao hắn ta qua được khóa bấm ở cổng ngoài. Hắn nói không có chiếc khóa nào ở đó cả. Nhưng tôi đã lái xe qua CO hằng ngày và ngày nào tôi cũng nhìn thấy chiếc khóa bấm đó. Đây là một tín hiệu cảnh báo. Giờ thì tôi thực sự bất an. Tại sao hắn lại nói dối tôi về điều này khi mà hắn biết nó quan trọng với tôi như thế nào?

Tôi chưa bao giờ tỏ ra cảnh giác với gã hơn lúc này. Tôi không thể tin gã.

https://thuviensach.vn

Bí mật về nơi ở của Eric đã không còn là bí mật, hắn đã mất bình tĩnh. Cả vụ này chỉ khiến mọi chuyện càng trở nên bí ẩn… nhưng tôi sẽ lần ra manh mối để làm sáng tỏ tất cả.

https://thuviensach.vn

17
PHÂN TÍCH LƯU LƯỢNG

Khkp wg wve kyfcqmm yb hvh TBS oeidr trwh Yhb MmCiwus wko ogvwgxar hr?

Bạn từng bước trên con đường tối om hay đi qua khu vực đỗ xe của trung tâm thương mại vào lúc nửa đêm khi không có ai xung quanh và luôn cảm giác rằng ai đó đang dõi theo mình chưa?

Hẳn là lạnh xương sống lắm!

Đó cũng chính là cảm giác của tôi về sự bí ẩn xoay quanh cái tên Wernle và Martinez. Đó là người thực, hay chỉ là các biệt danh của Eric Heinz?

Tôi biết mình nên dừng việc tìm kiếm và cũng không nên đánh liều để bị bắt quả tang tiếp tục hacking một lần nữa… nhưng biết đâu tôi có thể thu được thêm một phần sự thật nào đó. Hóa đơn điện thoại của Martinez cho tôi danh sách các số mà hắn đã gọi. Có lẽ tôi có thể có thêm chút manh mối từ việc tìm ra ai đã gọi cho hắn.

Tôi cần thực hiện "phân tích lưu lượng". Quá trình này bắt đầu từ việc xem xét hồ sơ chi tiết cuộc gọi của một ai đó sau khi xác định được số điện thoại của họ và lấy được thông tin từ những hồ sơ này. Anh ta thường gọi cho ai? Ai gọi cho anh ta? Liệu anh ta có thực hiện hay nhận được một chuỗi các cuộc gọi liên tiếp từ một người nhất định nào đó? Liệu có ai đó mà anh ta hầu như chỉ gọi vào buổi sáng? Còn buổi tối thì sao? Các cuộc gọi với người kia có đặc biệt dài không? Hay đặc biệt ngắn? v.v…

Sau đó, bạn lại tiến hành phân tích tương tự những người mà anh ta hay nói chuyện nhất.

https://thuviensach.vn

Kế tiếp bạn đặt câu hỏi, những người này hay gọi cho ai?

Chắc bạn đã bắt đầu mường tượng ra được. Tôi phải cực kỳ cố gắng vì quá trình này chiếm hầu hết thời gian rảnh của tôi, tới vài giờ mỗi ngày. Nhưng tôi cần phải biết. Không có cách nào khác: Nỗ lực này là cần thiết bất kể rủi ro có lớn chừng nào.

Tôi có cảm giác tương lai của tôi phụ thuộc vào việc này.

Tôi đã có chi tiết cuộc gọi di động của Martinez trong ba tháng gần nhất. Để bắt đầu, tôi phải hack vào PacTel Cellular để tìm xem chi tiết cuộc gọi của họ lưu ở đâu trong hệ thống, có vậy tôi mới có thể tìm kiếm danh mục các thuê bao của PacTel đã gọi tới máy nhắn tin, hòm thư thoại và điện thoại cố định của Eric.

Khoan đã, tốt hơn nữa là nếu đằng nào tôi cũng hack vào PacTel, tôi còn có thể nhân tiện lấy hồ sơ dịch vụ khách hàng của tất cả các số điện thoại mà Martinez đã gọi trong hệ thống của họ, nhờ đó biết được chủ sở hữu của các điện thoại này.

Tôi không biết nhiều lắm về quy ước đặt tên hệ thống nội bộ của công ty, do đó để bắt đầu, tôi gọi tới số công khai của dịch vụ khách hàng, thường dành cho những người muốn đăng ký gói cước cuộc gọi. Giả vờ là nhân viên hỗ trợ nội bộ của PacTel, tôi hỏi: “Chị có dùng CBIS không?” (tên viết tắt này được dùng trong một số công ty điện tử viễn thông, có nghĩa là Customer Billing Information System – hệ thống thông tin hóa đơn khách hàng).

“Không,” người phụ nữ ở đầu dây bên kia nói. “Tôi đang dùng CMB.”

“À, vâng, cảm ơn chị.” Tôi dập máy, giờ thì đã có thêm một mẩu thông tin để tăng độ tin cậy cho bản thân. Tôi gọi vào số nội bộ của Phòng Điện tử Viễn thông, đưa tên của một vị quản lý ở Phòng Kế toán và nói rằng chúng tôi có một khách thầu tới làm việc tại công ty và cần được phân cho một số thuê bao để có thể nhận thư thoại. Người phụ nữ ở đầu dây bên kia đã giúp

https://thuviensach.vn

tôi thiết lập một tài khoản thư thoại. Tôi quay số và đặt mật khẩu là “3825”. Sau đó, tôi để lại tin báo thư thoại. “Đây là Ralph Miller. Tôi hiện không có ở bàn làm việc, xin hãy để lại tin nhắn.”

Cuộc gọi kế tiếp là tới phòng IT để tìm xem ai quản lý CMB; đó là một gã có tên Dave Fletchall. Khi anh ta nhấc máy, câu hỏi đầu tiên là: “Số gọi lại của anh là gì?” Tôi cho anh ta số nội bộ của hòm thư thoại mà tôi vừa mới kích hoạt trước đó.

Khi tôi thử tiếp cận bằng mẹo “tôi phải đi công tác và cần đăng nhập từ xa”, anh ta trả lời: “Tôi có thể cho anh số truy cập, nhưng vì lý do bảo mật, chúng tôi không được phép thông báo mật khẩu qua điện thoại. Chỗ ngồi của anh ở đâu?”

Tôi nói: “Giờ tôi không có mặt ở văn phòng. Anh có thể cho vào phong bì và gửi lại Mimi hộ tôi được không?” – Mimi là thư ký của phòng, tôi đã tìm được cái tên này trong cuộc điều tra trước đó. Anh ta không phản đối. “Anh giúp tôi một chút được không?” Tôi nói. “Tôi đang trên đường tới cuộc họp, anh có thể gọi vào máy tôi và để lại số điện thoại được không?”

Anh ta tiếp tục đồng ý.

Sau đó, vào buổi chiều, tôi gọi cho Mimi, nói rằng tôi bị kẹt ở Dallas. Tôi nhờ cô ấy mở phong bì mà Dave Fletchall đã gửi và đọc thông tin đó cho tôi. Sau khi có được thông tin cần dùng, tôi nhờ cô ấy bỏ phong bì vào sọt rác vì tôi không cần đến chúng nữa.

Endorphins lại tuôn trào và những ngón tay tôi như đang nhảy múa. Thực sự kích thích!

Đâu đó trong suy nghĩ, tôi luôn e ngại rằng những người bị tôi tấn công bằng kỹ thuật xã hội nửa chừng có thể phát hiện ra và mớm thông tin ma để tóm tôi.

https://thuviensach.vn

Lần này thì không có gì đáng lo. Cũng như mọi lần, tôi lại thành công trót lọt.

À không – cũng không hoàn toàn thế. Tôi đăng nhập vào hệ thống CMB, thật dễ dàng bởi hóa ra nó là máy tính VAX sử dụng hệ điều hành yêu thích của tôi, VMS. Nhưng tôi không phải là nhân viên của PacTel Cellular, do đó tôi không có tài khoản hợp lệ trên máy.

Tôi gọi điện cho Phòng Kế toán trong vai một nhân viên IT và đề nghị được nói chuyện với ai đó đang đăng nhập vào CMB.

Melanie nghe máy. Tôi nói mình làm việc cùng Dave Fletchall ở phòng IT và chúng tôi phát hiện ra CMB có chút vấn đề – liệu cô ta có thể dành ra vài phút được không?

Đương nhiên.

Tôi hỏi cô ta: “Gần đây cô có thay đổi mật khẩu không? Bởi chúng tôi mới nâng cấp phần mềm để thay đổi mật khẩu và chúng tôi muốn thử xem nó có hiệu quả không.”

Không, gần đây cô ta không đổi mật khẩu.

“Melanie, địa chỉ e-mail của cô là gì?” Ở PacTel Cellular, địa chỉ e-mail của nhân viên đồng thời chính là tên tài khoản của người đó và tôi cần tên đăng nhập của cô ta để đăng nhập vào hệ thống.

Tôi yêu cầu cô ta đóng tất cả các ứng dụng đang mở, thoát khỏi hệ thống và sau đó đăng nhập lại để tôi có thể xác định được liệu cô ta có thể truy cập vào giao diện dòng lệnh của hệ điều hành hay không. Sau khi, cô ta nói mình có thể, tôi nói: “Cô gõ ‘set password’ (đặt mật khẩu) vào đi.”

Sau đó, cô ta sẽ thấy một dấu nhắc có ghi “Old password” (mật khẩu cũ).

https://thuviensach.vn

“Giờ cô gõ mật khẩu cũ của cô vào đó, không cần nói cho tôi biết đâu,” tôi còn bổ sung thêm một bài học nho nhỏ về việc không được nói cho ai biết mật khẩu của mình.

Lúc này, cô ta hẳn đã thấy dấu nhắc ghi “New password” (mật khẩu mới).

Giờ thì tôi đã mở giao diện hệ điều hành ra và chờ đợi. “Giờ cô hãy nhập mật khẩu ‘pactel1234’, khi nào hiện dấu nhắc mới thì cô gõ lại mật khẩu đó một lần nữa giúp tôi. Sau đó nhấn Enter.” Ngay lúc cô ta làm xong bước cuối, tôi lập tức đăng nhập vào VMS bằng tên đăng nhập và mật khẩu “pactel1234”.

Giờ thì não tôi căng ra để làm đồng thời hai việc một lúc. Tôi gõ điên cuồng vào bàn phím, nhập chương trình 15 dòng lệnh nhằm khai thác một điểm yếu chưa được sửa lỗi của VMS, biên dịch và chạy chương trình, sau đó lập tài khoản mới với toàn quyền quản trị trong hệ thống.

Cùng lúc đó, tôi vẫn tiếp tục đưa ra chỉ dẫn cho Melanie. “Giờ cô thoát khỏi tài khoản… Giờ lại đăng nhập lại với tài khoản mới… cô vào được chưa? Tốt. Giờ cô mở lại các ứng dụng vừa mới tắt và kiểm tra xem nó có hoạt động bình thường không… Có hả? Tốt rồi.” Sau đó, tôi lại hướng dẫn cô ta đặt lại mật khẩu một lần nữa, không quên nhắc cô ta không được để lộ ra cho tôi hay bất kỳ ai mật khẩu mới thiết lập.

Giờ thì tôi đã có toàn quyền đăng nhập vào cụm VMS của PacTel, đồng nghĩa với việc tôi có thể truy cập được toàn bộ thông tin tài khoản khách hàng, hồ sơ hóa đơn, dãy số điện tử và nhiều thông tin khác nữa. Một chuyện phi thường. Tôi cảm ơn Melanie vì đã giúp đỡ.

Vẫn còn nhiều việc phải làm. Tôi dành vài ngày sau đó để tìm kiếm vị trí lưu trữ CDR và tìm cách truy cập vào hồ sơ đăng ký dịch vụ khách hàng, có vậy tôi mới có thể dễ dàng thăm dò tên, địa chỉ và tất cả thông tin khác của mỗi thuê bao điện thoại.

https://thuviensach.vn

CDR được đặt trong một ổ cứng có dung lượng lớn, chứa dữ liệu thời gian thực của mọi cuộc gọi đi và của các khách hàng tại Los Angeles trong vòng 30 ngày – một lượng tập tin vô cùng khổng lồ. Tôi có thể dò tìm ngay trên hệ thống, dù phải mất 10-15 phút mỗi lần tìm như vậy.

Số máy nhắn tin của Eric chính là điểm xuất phát. Liệu có ai ở PacTel gọi vào máy nhắn của Eric không, số 213 701-6852? Có khoảng nửa tá cuộc gọi từ hai số khác nhau. Đây là danh sách, chính xác như những gì xuất hiện trên hồ sơ của PacTel:

2135077782 0 920305 0028 15 2137016852 LOS ANGELE CA

2135006418 0 920304 1953 19 2137016852 LOS ANGELE CA

Số "213" ở đầu mỗi dòng là số gọi đến. Cụm số bắt đầu với "92" thể hiện năm, ngày và tháng – tức là cuộc gọi đầu tiên thực hiện vào ngày 5 tháng 3 năm 1992, kéo dài 28 phút vào nửa đêm.

Tôi nhận ra số điện thoại đầu tiên: Đây là số điện thoại trên hợp đồng thuê nhà của Eric, được đăng ký dưới tên Mike Martinez. Một lần nữa, đây là dấu hiệu cảnh báo rõ ràng. Tôi đã nghĩ "Martinez" có lẽ chỉ là tên giả của Eric, hoặc "Eric" là tên giả của Martinez, nhưng nếu vậy thì khá vô nghĩa, bởi Martinez không thể gọi điện đến số nhắn tin riêng của hắn.

Vậy gã Martinez còn gọi cho ai nữa và ai gọi cho hắn?

Tôi tìm trên CDR của PacTel. Không có gì cho thấy hắn gọi cho FBI, thông tin tôi đã phát hiện ra sau khi có số điện thoại từ hợp đồng của Eric. Có khá ít cuộc gọi tương tác từ các số điện thoại thuê bao PacTel; tôi chép những số này vào sổ tay. Giờ là lúc kiểm tra hồ sơ cuộc gọi của từng thuê bao này.

Tất cả các số trong danh sách đều thuộc về những người hay liên lạc với nhau, cũng như với văn phòng FBI ở Los Angeles và các cơ sở chấp pháp khác.

https://thuviensach.vn

Khốn kiếp! Tôi đã thuộc nằm lòng những số này. Số để bàn và di động của Terry Atchley thuộc đội An ninh của Pacific Bell. Quản lý của Phòng An ninh Pacific Bell ở Bắc California, John Venn. Còn có cả số máy nhắn tin của Eric, hòm thư thoại và các số máy bàn nhà hắn. Và số điện thoại của nhiều đặc vụ FBI khác (số của họ đều bắt đầu bằng mã số vùng giống nhau, số tổng đài và số kéo dài đầu tiên: 310 996-3XXX). Cụm số cuối cho thấy rõ ràng Martinez cũng là một đặc vụ, đồng nghĩa với việc tất cả các đặc vụ khác có lẽ thuộc cùng một tổ nhiệm vụ.

Các cuộc gọi khác vào máy nhắn tin của Eric hiện ra trước mắt tôi đều đến từ số 213 500-6418. Dò theo số này, tôi tìm được cả một mỏ vàng. Có khá ít cuộc gọi ngắn vào buổi tối tới một số máy nội bộ duy nhất của FBI. Một giải thích hợp lý đấy chứ? Gã này hắn là muốn kiểm tra hòm thư thoại của mình.

Tôi quay số.

“Tôi là Ken McGuire, hãy để lại tin nhắn.”

Ken McGuire là gã khốn nào và tại sao hắn lại theo dõi tôi?

Tôi nhấn phím “0”, dự đoán sẽ kết nối với quầy lễ tân.

Thay vào đó, một người phụ nữ nhấc máy và trả lời: “Phòng Tội phạm Cổ cồn trắng, đội 3 xin nghe.” Chỉ bằng một vài câu hỏi vô thưởng vô phạt, tôi đã có mảnh ghép kế tiếp trong bộ xếp hình: Đặc vụ Ken McGuire thuộc đội 3 phòng Tội phạm Cổ cồn Trắng của trụ sở FBI ở Los Angeles, hay còn gọi là WCC3. Hắn có lẽ là sếp chỉ đạo của Eric.

Khốn kiếp! Làm gì có ai dám điều tra FBI ngay lúc FBI cũng đang điều tra hắn?

Mọi việc dồn dập xuất hiện cùng lúc và dường như cả một trận cuồng phong sắp xuất hiện. Tôi có cảm giác mình đã không còn đường để quay lại, nhưng tôi sẽ không từ bỏ khi chưa thử vùng vẫy.

https://thuviensach.vn

18
SÁNG TỎ

Rcvo dn ivhz ja ocz omvinvxodji oj adiy v kzmnji'n njxdvg nzxpmdot iphwzm pndib oczdm ivhz viy yvoz ja wdmoc?

Chúng ta đều biết rằng hồ sơ y tế của mọi người là tài liệu tuyệt mật, nó chỉ được chia sẻ khi ai đó được cấp phép cụ thể. Nhưng sự thật là bất cứ cảnh sát liên bang, cớm, hay công tố viên nào cũng có thể thuyết phục một thẩm phán rằng anh ta có lý do chính đáng để có thể đi vào cửa hàng thuốc và in ra tất cả đơn thuốc cũng như ngày tháng bạn đã mua. Thật đáng sợ!

Chúng ta cũng biết rằng hồ sơ của mọi người được lưu giữ bởi các cơ quan chính phủ – Sở Thuế vụ, Sở An sinh Xã hội hay DMV ở bất cứ bang nào, v.v… – luôn an toàn trước những cặp mắt dòm ngó. Có thể giờ chúng đã an toàn hơn đôi chút so với trước kia – dù tôi vẫn nghi ngờ điều đó – nhưng vào thời của tôi, việc lấy bất kỳ thông tin gì tôi muốn đều rất dễ dàng.

Chẳng hạn như tôi đã lừa Sở An sinh Xã hội thông qua một cuộc tấn công bằng kỹ thuật xã hội công phu. Việc này bắt đầu bằng những nghiên cứu tôi vẫn hay tiến hành – các phòng ban khác nhau của Cục, địa điểm của chúng, ai là giám sát và quản lý của mỗi phòng ban, ngôn ngữ nội bộ thường dùng, v.v... Các nhóm chuyên biệt gọi là "Mod" sẽ chuyên xử lý những vụ khiếu nại, tôi nghĩ cái tên này xuất phát từ từ "module", mỗi module có thể giải quyết một chuỗi các số An sinh Xã hội. Tôi tấn công bằng kỹ thuật xã hội vào số điện thoại của một Mod và cuối cùng cũng gặp được một nhân viên có tên là Ann. Tôi bảo cô ta rằng tôi là Tom Harmon, đến từ Văn phòng Giám sát Chung của Cục.

https://thuviensach.vn

Tôi nói: “Chúng tôi cần sự trợ giúp thường xuyên,” giải thích rằng dù văn phòng của chúng tôi đang tiến hành điều tra một vụ lừa đảo, nhưng chúng tôi lại không có quyền truy cập vào Hệ thống Khiếu nại Hiện đại hóa (Modernized Claims System – MCS), một cái tên nghe vụng về đến hài hước cho hệ thống máy tính tập trung của họ.

Kể từ lúc bắt đầu cuộc gọi đầu tiên đó, chúng tôi đã trở thành bạn thân qua điện thoại. Tôi có thể gọi cho Ann và nhờ cô ấy tìm kiếm bất cứ thứ gì tôi muốn – số An sinh Xã hội, ngày tháng năm và nơi sinh, tên thời con gái của người mẹ, phúc lợi khuyết tật, lương bổng, v.v…. Mỗi khi tôi gọi, cô ấy sẽ bỏ ngang việc đang làm để tìm kiếm bất kỳ thứ gì tôi nhờ.

Ann có vẻ yêu thích các cuộc gọi của tôi. Cô ấy rõ ràng thích thú với việc chơi trò thay mặt cho một người ở Văn phòng Điều tra Chung, người đang tiến hành các điều tra quan trọng nhắm vào những kẻ thực hiện hành vi lừa đảo. Tôi cho rằng việc đó đã phá vỡ vòng quay của một ngày làm việc bình thường, mệt mỏi. Cô ấy thậm chí còn gợi ý cho tôi những thứ cần tìm: “Liệu biết tên cha mẹ có giúp ích gì không?” Và rồi cô ấy sẽ đi qua một loạt các bước để đào thông tin đó lên.

Một dịp, tôi lỡ mồm hỏi: “Thời tiết chỗ cô hôm nay thế nào?”

Đáng lý ra tôi phải làm cùng thành phố với cô ấy. Cô ấy hỏi lại tôi: “Anh không biết thời tiết thế nào á!?”

Tôi nhanh chóng đỡ lời: “Hôm nay tôi làm nhiệm vụ ở Los Angeles.” Chắc cô ấy đã nghĩ: Ồ, tất nhiên rồi – anh ấy hẳn phải đang đi công tác.

Chúng tôi là bạn bè trên điện thoại trong khoảng ba năm, cả hai đều tận hưởng những câu bông đùa và niềm vui hoàn thành công việc.

Nếu gặp mặt ngoài đời, tôi sẽ trao cho cô ấy một nụ hôn để cảm ơn tất cả sự giúp đỡ tuyệt vời của cô ấy. Ann, nếu cô đọc được những dòng này, tôi vẫn đang đợi được hôn cô đấy.

https://thuviensach.vn

Tôi đoán các thám tử ngoài đời hẳn phải có rất nhiều đầu mối để tìm ra dấu vết mỗi khi họ xử lý một vụ án và một vài trong số đó cần thời gian để thu được kết quả. Tôi vẫn chưa quên hợp đồng thuê căn hộ của Eric dưới tên Joseph Wernle; tôi chỉ chưa lần theo manh mối đó mà thôi. Đây là một trong số ít lần chơi trò thám tử khiến tôi tìm đến cô bạn thân Ann ở Sở An sinh Xã hội.

Ann tra trên MCS và lấy được một tập tin "Alphadent", vốn dùng để tìm số An sinh Xã hội của các cá nhân cùng họ tên và ngày sinh của họ.

Sau đó, tôi hỏi tìm "Numident" để lấy địa chỉ và ngày sinh, tên cha và tên thời con gái của mẹ đối tượng mục tiêu.

Joseph Wernle sinh ở Philadelphia, là con của Joseph Wernle Sr. và Mary Eberle.

Sau đó, Ann chạy lệnh "truy vấn thu nhập chi tiết", kết quả trả về sẽ cho biết lịch sử công việc cũng như hồ sơ thu nhập của một cá nhân.

Hả? ... Cái quái gì đây?

Josepth Wernle Jr. 40 tuổi. Theo hồ sơ An sinh Xã hội của hắn ta, hắn chưa bao giờ kiếm được một xu nào.

Hắn thậm chí còn chưa bao giờ có công việc.

Lúc này bạn sẽ nghĩ gì?

Gã này thực sự tồn tại, bởi Sở An sinh Xã hội có hồ sơ về hắn. Nhưng hắn chưa bao giờ có việc làm và chưa bao giờ kiếm được thu nhập.

Càng đào sâu vào gia cảnh của hắn, mọi thứ càng trở nên hấp dẫn. Mọi thứ đều vô lý, việc này chỉ càng khiến tôi thêm quyết tâm tìm ra lời giải đáp.

https://thuviensach.vn

Nhưng ít nhất thì giờ tôi đã có tên cha mẹ hắn. Chuyện này giống như chơi trò Sherlock Holmes vậy.

Joseph Wernle Jr. – người con[62] – sinh ra ở Philadelphia. Có thể cha mẹ hắn vẫn ở đó, hoặc ít nhất là đâu đó gần đấy. Tôi chỉ cần thực hiện một cuộc gọi đến trung tâm trợ giúp danh bạ cho mã vùng 215, thuộc địa bàn Philadelphia và các khu vực xung quanh Pennsylvania, để tìm ra ba người tên là Joseph Wernle.

[62] Ở Mỹ, đôi khi tên con được đặt giống hệt tên cha, có thêm chữ Junior (con) để phân biệt với Senior (cha). (ND)

Tôi bắt đầu gọi đến các số mà nhân viên trung tâm trợ giúp danh bạ đã cung cấp. Ở lần thử thứ hai, có một người trả lời. Tôi hỏi đó có phải là ông Wernle không và ông ta nói đúng.

“Tôi là Peter Browley đến từ Cục Quản lý An sinh Xã hội,” tôi bắt đầu. “Tôi có thể làm phiền ông vài phút được không?”

“Có việc gì vậy?”

“À, chúng tôi đang trả tiền An sinh Xã hội cho một người tên là Joseph Wernle, nhưng vì lý do nào đó mà hồ sơ có vẻ đã bị xáo trộn. Có vẻ chúng tôi đang trả tiền cho nhầm người.”

Tôi dừng lại để ông ta nắm được câu chuyện và cảm thấy bối rối hòng đẩy ông ta vào tình huống bất lợi. Ông ta cứ nghe máy mà không nói gì.

Tôi tiếp tục: “Có phải tên vợ ông là Mary Eberle không?”

“Không,” ông ta nói. “Đó là chị gái tôi.”

“À, thế ông có người con nào tên là Joseph không?”

https://thuviensach.vn

“Không.” Sau một lúc, ông ta nói thêm: “Mary có một đứa con trai tên là Joseph Ways. Nhưng không thể là nó được. Nó đang sống ở California.”

Câu chuyện đang dần sáng tỏ; sắp có kết quả rồi. Nhưng chưa hết, người ở đầu dây bên kia vẫn đang nói.

“Nó là một đặc vụ FBI.”

Thằng chó đẻ!

Không có ai tên là Joseph Wernle Jr. cả. Một đặc vụ FBI tên Joseph Ways đã lấy danh tính giả và sử dụng những cái tên thật trong gia đình hắn ta để có thể dễ dàng ghi nhớ. Và đặc vụ đó giả làm một hacker tên là Eric Heinz.

Hoặc ít nhất, đó là suy đoán khả thi nhất, dựa theo những gì tôi đã biết.

Lần tiếp theo khi tôi thử gọi Eric trên đường dây điện thoại cố định của hắn, số đã bị cắt.

Hồi mới bước chân vào sự nghiệp hacking, đã có thời điểm tôi cho rằng việc có quyền truy cập vào một công ty dịch vụ công cộng khác của Los Angeles, chẳng hạn như Cục Điện Nước (DWP), có thể sẽ có lúc hữu ích. Tất cả mọi người đều cần dùng điện nước, vì thế công ty điện nước có vẻ là nguồn thông tin cực kỳ giá trị để tìm ra địa chỉ cá nhân.

DWP duy trì đơn vị được gọi là “Tổ Chuyên trách Đặc biệt” để xử lý các cuộc gọi từ cơ quan chấp pháp, bố trí những người được huấn luyện để xác minh người gọi đến đều nằm trong danh sách những người được cấp phép để lấy thông tin khách hàng.

Tôi gọi đến văn phòng của DWP, tự nhận mình là cảnh sát và giải thích sĩ quan có số điện thoại của Tổ Chuyên trách Đặc biệt đang được phân công công tác, vì thế chúng tôi cần lấy lại nó. Tôi đã lấy được số điện thoại mà không gặp vấn đề gì.

https://thuviensach.vn

Sau đó, tôi gọi đến đơn vị tinh nhuệ SIS của LAPD. Lôi mấy tay này vào cuộc vui có vẻ công bằng, bởi họ là những người đã theo đuôi Lenny và tôi tại Cao đẳng Pierce nhiều năm trước. Tôi yêu cầu nói chuyện với một trung sĩ, và I. C. Davidson nghe máy. (Tôi vẫn nhớ rõ tên ông ta, bởi sau này tôi vẫn tiếp tục dùng cái tên đó trong một thời gian dài, bất cứ khi nào tôi cần thông tin từ DWP.)

Tôi nói với ông ta: “Trung sĩ, tôi ở Tổ Chuyên trách Đặc biệt của DWP, chúng tôi đang thiết lập cơ sở dữ liệu của những người được cấp phép cho các yêu cầu của cơ quan chấp pháp và tôi gọi để hỏi xem có bất cứ sĩ quan nào trong đơn vị của anh cần truy cập vào Tổ Chuyên trách Đặc biệt không.”

Ông ta nói: “Tất nhiên.”

Như mọi khi, tôi bắt đầu bằng cách hỏi xem ông ta có trong danh sách này không và lấy tên.

“Được rồi, có bao nhiêu sỹ quan của ông cần đưa vào danh sách này?” Ông ta cho tôi một con số.

“Được rồi, tiếp tục, hãy cho tôi tên của họ và tôi sẽ đảm bảo họ đều được cấp phép thêm một năm nữa.” Việc người của mình được truy cập thông tin từ DWP rất quan trọng đối với ông ta, nên ông ta vẫn dành thời gian nhẫn nại đọc to và đánh vần từng tên.

Vài tháng sau, Tổ Chuyên trách Đặc biệt bổ sung thêm một mật khẩu vào quá trình xác minh của họ. Không vấn đề gì: Tôi lại gọi đến Đơn vị Điều tra Tội phạm Có tổ chức của LAPD và lôi được một trung úy ra nghe điện.

Giới thiệu bản thân là “Jerry Spencer ở Tổ Chuyên trách Đặc biệt”, tôi chọn cho ván cược mở màn của mình một phiên bản hơi khác câu chuyện ở trên: “Tiện đây, ông có được cấp phép cho Tổ Chuyên trách Đặc biệt không?” Ông ta nói có.

https://thuviensach.vn

“Tốt. Tên ông là gì, thưa ông?”

“Billingsley. David Billingsley.”

“Xin đợi chút trong lúc tôi tìm tên ông trong danh sách.”

Tôi dừng lại một chút và sột soạt mấy tờ giấy. Rồi tôi nói: “Ồ, đúng rồi. Mật khẩu của ông là ‘0128.’”

“Không, không, không. Mật khẩu của tôi là ‘6E2H’”

“Ồ ồ, xin lỗi, đó là một David Billingsley khác.” Tôi khó mà nhịn được cười. Sau đó, tôi nhờ ông ta tìm danh sách các sĩ quan được cấp phép với Tổ Chuyên trách Đặc biệt trong Đơn vị Điều tra Tội phạm Có tổ chức và nói cho tôi biết tên cùng mật khẩu của họ. Tới lúc đó, tôi đã kiếm chác đủ rồi. Tôi sẽ chẳng lấy gì làm ngạc nhiên nếu một vài mật khẩu trong số đó vẫn còn dùng được cho tới bây giờ.

Với quyền truy cập đến Tổ Chuyên trách Đặc biệt của DWP, tôi chỉ mất năm phút để khám phá ra địa chỉ mới của Eric: Hắn đã chuyển đến một căn hộ khác trong cùng tòa nhà. Lewis và tôi đã đến chỗ hắn, ba tuần sau hắn không còn sống ở căn hộ đó và có một số điện thoại mới – nhưng có phải hắn vẫn ở trong tòa nhà đó không?

Đường dây điện thoại mới vẫn được ghi với tên trước đây, Joseph Wernle. Nếu Eric đã thực sự chuyển sang “chế độ an toàn” như hắn nói, tại sao hắn vẫn dùng tên cũ? Đây là gã vẫn tự nhận mình là một hacker giỏi ư? Có vẻ như hắn không có ý niệm gì về những thông tin liên quan đến hắn mà chúng tôi có thể tra ra. Tôi vẫn còn một chặng đường dài để giải đáp tất cả thắc mắc, nhưng tôi biết mình sẽ phải tiếp tục khi giờ đây tôi đã tiến rất gần đến sự thật rồi.

https://thuviensach.vn

19
VÉN MÀN

Epib qa bpm vium wn bpm ixizbumvb kwuxtmf epmzm Q bziksml lwev Mzqk Pmqvh?

Giờ đây, khi chúng tôi đã có quyền truy cập SAS, Lewis và tôi muốn lấy số dial-up của tất cả các CO để có thể theo dõi mọi điện thoại trong khu vực phủ sóng của Pacific Bell. Thay vì phải tấn công bằng kỹ thuật xã hội với nhân viên Pacific Bell để lấy được số dial-up mỗi lần muốn truy cập, chúng tôi sẽ có tất cả.

Tôi đã học được từ một nhân viên ở Pasadena, người đã đọc dòng chú ý bản quyền cho tôi về cách họ dùng SAS như thế nào. Nhân viên kiểm tra sẽ phải nhập thủ công số dial-up cho RATP cho văn phòng trung tâm của đường dây cần kiểm tra. Các nhân viên kiểm tra có một danh sách các số dial-up cho RATP trong tất cả các văn phòng trung tâm mà họ quản lý.

Có một vấn đề nho nhỏ là: Làm thế nào tôi có thể có được bản sao số dial-up SAS cho tất cả các văn phòng trung tâm khi mà tôi không biết bản danh sách chết tiệt đó gọi là gì? Rồi tôi nghĩ ra một cách. Có thể thông tin này đã có sẵn trong một cơ sở dữ liệu. Tôi gọi đến nhóm ở Pasadena sử dụng SAS để chạy các bài kiểm tra đường dây khi một thuê bao gặp vấn đề về điện thoại. Tôi tự nhận mình "từ phòng Kỹ thuật" và hỏi rằng liệu tôi có thể tìm thấy các số dial-up SAS trong một cơ sở dữ liệu không. Câu trả lời là "Không, nó không có trong cơ sở dữ liệu mà chỉ có trong bản cứng thôi."

Tệ thật! Tôi hỏi: "Anh sẽ gọi cho ai khi gặp một vấn đề kỹ thuật với một đơn vị SAS?"

https://thuviensach.vn

Lại thêm một ví dụ nữa về việc mọi người sẵn lòng giúp đỡ người mà họ tin là đồng nghiệp: Anh ta đưa cho tôi số điện thoại của một văn phòng Pacific Bell ở Thung lũng San Fernando. Hầu hết mọi người đều rất sẵn lòng giúp đỡ.

Tôi gọi đến đó, một viên quản lý nhấc máy và tôi nói với anh ta: “Tôi tới từ phòng Kỹ thuật ở San Ramon”, một cơ sở kỹ thuật lớn của Pacific Bell tại Bắc California. “Chúng tôi đang nhập các số dial-up SAS vào một cơ sở dữ liệu, vì thế, chúng tôi cần mượn một bản danh sách đầy đủ có liệt kê tất cả các số. Có ai có bản sao như vậy không?”

“Tôi có,” anh ta nói, thừa nhận câu chuyện của tôi không chút đắn đo. Hắn nhân viên ẩn sâu trong nội bộ tổ chức của Pacific Bell không thể nghĩ rằng một gã bên ngoài nào đó có thể tra ra mình.

“Fax sang đây có dài lắm không?”

“Khoảng 100 trang.”

“À, vậy tôi muốn mượn một bản copy trong mấy hôm. Tôi sẽ tự đến đó hoặc có ai đó qua lấy hộ tôi. Thế được không?” Anh ta cho tôi biết địa chỉ văn phòng.

Alex lại tiếp tục hứng thú với việc thay mặt cho tôi. Khoác một bộ vest doanh nhân, anh ta lái xe đến cơ sở của Pacific Bell ở Thung lũng San Fernando. Nhưng viên quản lý kia không đơn giản chỉ đưa Alex gói hàng như chúng tôi nghĩ. Thay vào đó, anh ta hỏi Alex tại sao lại cần những thông tin này.

Thoáng chút lúng túng. Giờ là mùa xuân, ở Nam California. Ngoài trời rất ấm. Và Alex đang đeo găng tay.

Khi viên quản lý nhìn thấy đôi tay đeo găng của Alex, anh ta nhìn Alex và nói: “Cho tôi xem ID của anh được không?”

https://thuviensach.vn

Lại một thoáng khó chịu khác.

Trên đời này, không gì có giá trị bằng khả năng ứng biến trong một tình huống toát mồ hôi hột.

Alex uể oải nói: “Tôi không phải là người của Pacific Bell. Tôi là cộng sự của nhóm kinh doanh đang trên đường đến buổi họp của Pacific Bell ở trung tâm thành phố. Họ nhờ tôi qua đây và lấy nó.”

Viên quản lý nhìn anh một lúc.

Alex nói: “Được rồi – nếu đây là vấn đề thì không sao cả” và quay người như thể anh chuẩn bị bỏ đi.

Viên quản lý nói: “Ồ, không, không – nó đây,” và chìa gói hàng ra cho Alex.

Alex cười nhe nhởn như thể “Tôi làm được rồi!” khi đưa cho tôi tập tài liệu chứa tất cả số dial-up của các đơn vị SAS ở mọi văn phòng trung tâm tại Nam California.

Sau khi sao chép tập tài liệu, Alex đến một văn phòng thu phí khách hàng của Pacific Bell và thuyết phục thư ký đặt gói hàng vào hệ thống thư tín nội bộ của công ty để trả lại người đã cho mượn – che đi dấu vết của chúng tôi bằng cách tránh gây ra bất kỳ câu hỏi nào về tập tài liệu bị mất, vốn có thể dẫn đến việc Pacific Bell phát hiện ra SAS đã bị xâm nhập, nhân tiện cũng cắt đuôi cho Alex.

Một ngày nọ, tôi có linh cảm Lewis cũng có thể là mục tiêu của một cuộc điều tra. Để phòng xa, tôi thử kiểm tra và phát hiện ra tất cả đường điện thoại tại công ty Lewis đang làm, Impac Corporation, đã bị nghe lén. Tại sao vậy? Liệu Eric có liên quan đến chuyện này không? Lewis và tôi quyết định gọi cho Eric và xem xem liệu chúng tôi có lừa hắn khai ra được gì không.

Lewis xử lý cuộc gọi, còn tôi nghe ngóng và nhắc lời.

https://thuviensach.vn

Eric chủ yếu trả lời với một giọng Hừmmm lảng tránh. Cuối cùng, hắn nói: "Nghe như các cậu đang gặp rắc rối." Ờ, cảm ơn. Chẳng giúp ích được gì cả.

Eric hỏi, "Một trong các số theo dõi cậu là gì? Tôi muốn thử gọi vào xem có lấy được gì không." Lewis đưa cho hắn số theo dõi đang dùng để nghe lén một trong các đường dây tại Impac: 310-608-1064

Lewis bảo hắn: "Còn một điều lạ lùng nữa – Giờ tôi còn bị nghe lén cả đường dây điện thoại ở nhà riêng nữa."

"Lạ thật đấy," Eric trả lời.

Lewis nói: "Cậu nghĩ chuyện gì đang xảy ra, Eric? Kevin cứ hỏi tôi những câu đó. Cậu ấy muốn cậu phán đoán. Liệu có thể có liên quan đến cơ quan chấp pháp không?"

"Tôi không biết."

Lewis ép: "Cứ nói có đi, để cậu ta hết hỏi."

Eric nói: "Tôi nghĩ là không. Tôi nghĩ chỉ là công ty điện thoại thôi."

"Ờ, nếu họ định theo dõi tất cả đường dây điện thoại chỗ tôi làm, họ sẽ phải nghe hàng nghìn cuộc gọi mỗi tháng," Lewis trả lời.

Hôm sau, tôi lại ngồi nghe ngóng qua loa ngoài điện thoại, Eric gọi cho Lewis, hắn ta bắt đầu bằng câu hỏi: "Cậu có đang gọi từ một đường dây an toàn không?"

Eric trả lời: "Có, tôi đang gọi từ máy điện thoại công cộng" và tuôn ra một trong những lời phàn nàn thường thấy: "Các cậu phải tôn trọng sự riêng tư của tôi."

Rồi, như từ trên trời rơi xuống, hắn hỏi Lewis: "Các cậu có cài đặt bất cứ tính năng CLASS nào ở chỗ làm không?"

https://thuviensach.vn

Hắn đang nhắc đến "các dịch vụ báo hiệu địa phương tùy biến" (Custom Local Area Signaling Services), ví dụ như định danh người gọi, chuyển tiếp cuộc gọi có chọn lọc, trả lời cuộc gọi, hay các tính năng khác không dành cho người dùng đại chúng. Nếu Lewis nói có, anh sẽ thú nhận một hành vi phạm pháp.

Trước khi Lewis có cơ hội để phủ nhận, chúng tôi nghe thấy tín hiệu chờ cuộc gọi ở bên đầu dây của Eric.

Tôi nói với Lewis: "Từ khi nào máy điện thoại công cộng có chờ cuộc gọi vậy!?"

Eric càu nhàu rằng hắn phải gác máy một phút. Khi hắn quay lại, tôi vặn hắn về việc liệu hắn có đang gọi từ máy điện thoại công cộng hay không. Eric thay đổi câu chuyện, nói rằng giờ hắn đang gọi từ nhà của một người bạn gái.

Trong khi Lewis tiếp tục cuộc điện thoại, tôi gọi đến căn hộ của Eric. Một người đàn ông nghe máy. Tôi thử lại lần nữa, phòng trường hợp tôi gọi nhầm. Vẫn gã đó. Tôi bảo Lewis ép hắn về chuyện này.

Lewis nói: "Có gã nào đó đang trả lời điện thoại nhà cậu. Chuyện quái quỷ này là sao, Eric?"

Hắn nói: "Tôi không biết."

Nhưng Lewis lại tiếp tục ép: "Ai đang ở trong căn hộ của cậu thế, Eric?"

"Hừm, tôi không biết chuyện gì đang xảy ra. Đúng ra làm gì có ai đang ở trong căn hộ của tôi. Tôi sẽ đi kiểm tra," hắn trả lời. "Với tất cả những gì đang diễn ra, tôi sẽ chuyển sang chế độ an toàn. Hãy tiếp tục cho tôi biết tin." Và hắn gác máy.

Có quá nhiều lời dối trá về những điều nhỏ nhặt không đáng.

https://thuviensach.vn

Eric đang trở thành một bí ẩn cần giải mã, tương đương với bí ẩn về những chiếc hộp nghe lén. Cho đến giờ, tất cả những gì tôi có là ba con số xuất phát từ đâu đó ở Oakland kết nối đến mấy chiếc hộp.

Trên thực tế, những cuộc gọi theo dõi đó bắt nguồn từ đâu? Không quá khó để tìm ra câu trả lời. Tôi chỉ đơn giản gọi đến Trung tâm Phân bổ Vòng lặp Cơ học (MLAC), cung cấp một trong những số đó và lấy được địa chỉ thực tế nơi đặt đường dây điện thoại đó: số 2150, phố Webster, Oakland, cụm văn phòng của Phòng An ninh Pacific Bell. Trước đó, chúng được đặt ở San Francisco nhưng giờ đã chuyển sang phía bên kia vịnh.

Thật tuyệt vời! Nhưng đó chỉ là một trong các số điện thoại. Tôi muốn biết tất cả số điện thoại Phòng An ninh Pacific Bell đang dùng để kết nối đến những chiếc hộp theo dõi bí mật. Tôi đã nhờ quý cô ở MLAC tìm hộ yêu cầu dịch vụ gốc đã thiết lập số điện thoại mà tôi vừa khám phá ra. Đúng như tôi đã dự đoán, yêu cầu này cho thấy nhiều số điện thoại khác – khoảng 30 số – đã được thiết lập vào cùng khoảng thời gian. Chúng đều xuất phát từ "phòng nghe lén", nơi họ giữ lại bản ghi âm các cuộc điện thoại. (Thực ra, một thời gian dài sau đó, tôi phát hiện ra rằng không có phòng nghe lén chuyên biệt nào cả; khi bắt đầu cuộc gọi trên bất kỳ đường dây bị theo dõi nào, nó sẽ được ghi lại bởi một máy ghi âm kích hoạt bằng giọng nói nằm trên bàn của nhân viên điều tra an ninh đang thụ lý vụ án, để họ có thể nghe lại vào bất cứ lúc nào có dịp.)

Có trong tay các số theo dõi, giờ tôi cần phải tìm ra mỗi số này đang gọi đến đâu. Đầu tiên, tôi gọi từng số, biết rằng bất cứ số nào trong chúng nếu không có tín hiệu máy bận thì chắc chắn không thể đang nghe lén; tôi sẽ bỏ qua những số đó.

Với tất cả các số khác, những số đang được dùng để nghe lén, tôi gọi đến SCC Oakland và tấn công bằng kỹ thuật xã hội với kỹ thuật viên trực bộ chuyển đổi để thực hiện lệnh truy vấn bộ nhớ cuộc gọi (Query Call Memory – QCM) trên bộ chuyển đổi DMS-100 cung cấp số máy đó (QCM trả về số

https://thuviensach.vn

điện thoại cuối cùng gọi từ điện thoại đó). Với những thông tin mới này, giờ tôi đã có danh sách các số dial-up theo dõi cho mỗi máy nghe lén của Pacific Bell trong bang California.

Mã vùng và tiền tố của một số theo dõi chỉ ra văn phòng trung tâm nào đang đặt máy nghe lén. Nếu Lewis hay tôi biết bất cứ ai có một số điện thoại do CO cung cấp mà ở đó có một máy nghe lén đang hoạt động, tôi sẽ gọi đến CO đó, nói rằng mình ở Phòng An ninh PacBell và giải thích: “Chúng tôi có một trong số các hộp ở đó. Tôi cần lần theo kết nối.” Sau một vài bước, tôi sẽ có số điện thoại mục tiêu bị nghe lén. Nếu nó không thuộc về ai mà tôi biết, tôi sẽ tiếp tục đến số tiếp theo.

Tôi tiếp tục kiểm tra việc nghe lén để đề phòng, nhòm ngó trước sau trong khi tập trung vào việc quan trọng là cố tìm ra Eric đang thực sự làm trò gì. Tôi chợt nảy ra một cách tiếp cận chưa từng nghĩ đến trước đây. Tôi gọi đến Trung tâm Điều khiển Chuyển mạch quản lý bộ chuyển mạch cung cấp dịch vụ điện thoại cho Eric và thuyết phục nhân viên kỹ thuật thực hiện một block lịch sử-đường dây (line history block – LHB), một cách để lấy được báo cáo về số điện thoại cuối cùng được gọi đi từ một đường dây do bộ chuyển mạch 1A ESS thực hiện.

Sau đó, tôi bắt đầu gọi lấy LHB của hắn vài lần một ngày để tìm hiểu các số hắn đang gọi.

Một trong những số điện thoại đó khiến tôi đổ mồ hôi lạnh. Eric đã gọi đến 310 477-6565. Tôi không cần tiến hành bất cứ điều tra nào nữa. Đây là số điện thoại mà tôi vẫn luôn nhớ như in trong tâm trí.

Trụ sở Los Angeles của FBI!

Ôi...

Tôi gọi tới chỗ làm của Lewis từ một trong những chiếc điện thoại nhái số của tôi và nói: “Bật ham radio của cậu lên đi.” Anh ta hiểu ngay câu nói đó

https://thuviensach.vn

mang một nghĩa hoàn toàn khác. Nó có nghĩa là: “Bật điện thoại nhái số của cậu lên đi.” (Lewis là mẫu người chỉ muốn tập trung vào mỗi việc một lúc; khi đang xử lý công việc hiện tại, cậu ta sẽ tắt điện thoại di động và máy nhắn tin để chúng không cắt ngang luồng suy nghĩ.)

Kéo được Lewis đến máy điện thoại an toàn, tôi bảo cậu ta: “Này, chúng ta gặp rắc rối rồi. Tôi đã thực hiện LHB trên đường dây của Eric. Tiên sư, hắn đang gọi cho FBI.”

Cậu ta không có vẻ gì bận tâm. Hoàn toàn không cảm xúc. Là saoooo?!

À, có thể có ai đó đang ở trong văn phòng, nên cậu ta không thể phản ứng. Hoặc có thể đó là do sự cứng đầu của cậu ta, thái độ cao ngạo, thể hiện rằng cậu ta là kẻ bất khả xâm phậm.

Tôi nói: “Cậu cần chuyển đống đĩa mềm và ghi chép ra khỏi căn hộ và văn phòng của mình. Hãy giấu bất cứ thứ gì cậu làm với SAS vào chỗ an toàn. Tôi cũng sẽ làm thế.”

Cậu ta có vẻ không cho rằng một cú điện thoại đến FBI là một điều gì to tát.

“Cứ làm đi!” tôi nói với cậu ta, cố không gào lên.

Linh tính mách bảo tôi hãy tiếp tục gọi đến Cục Tên và Địa chỉ Khách hàng của Pacific Bell. Đây là công việc thường ngày nhưng luôn mang tới kết quả không ngờ. Một quý cô vui vẻ nhận cuộc gọi của tôi và hỏi PIN; tôi dùng một trong những mã PIN đã lấy được vài tháng trước bằng cách hack vào cơ sở dữ liệu của CNL và đưa cho cô ta hai số điện thoại trong căn hộ của Eric.

“Số đầu tiên, 310 837-5412, được ghi nhận thuộc về ông Joseph Wernle, ở Los Angeles,” cô ta nói với tôi. “Và nó là một số non-pub” – tên gọi tắt của “non-published” (không công khai), số điện thoại mà nhân viên trực tổng đài không thể cung cấp thông tin. “Số thứ hai, 310 837-6420, cũng được ghi

https://thuviensach.vn

nhận thuộc về Joseph Wernle và cũng là non-pub.” Tôi bảo cô ta đánh vần cái tên cho tôi.

Vậy ra “Eric Heinz” là tên giả, tên thật của hắn là Joseph Wernle. Hoặc Eric có một người bạn cùng nhà... Giả thuyết có vẻ không hợp lý lắm với một gã khẳng định mỗi đêm lại có một ả khác nhau đến qua đêm. Hoặc có thể đơn giản là hắn đã đăng ký số điện thoại bằng một cái tên giả.

Nhiều khả năng Eric Heinz là tên giả và Joseph Wernle là tên thật của hắn. Tôi cần phải tìm ra gã này thực sự là ai và tôi cần làm việc đó thật nhanh.

Bắt đầu từ đâu đây?

Giấy thuê nhà mà hắn điền tại khu căn hộ phức hợp có thể có chút thông tin về gia cảnh – những mối quan hệ hay gì cũng được.

Khu căn hộ Oakwood, nơi Lewis và tôi đã đến thăm hắn bất ngờ, hóa ra chỉ là một trong những chuỗi bất động sản cho thuê trên toàn quốc do một tập đoàn địa ốc khổng lồ sở hữu. Khu phức hợp này được các công ty thuê để nhân viên đến ở khi công tác tạm thời, hay cho người vừa chuyển đến một thành phố mới và cần một chỗ để ở trong khi tìm nhà. Ngày nay, công ty này mô tả họ là “công ty giải pháp cho thuê nhà lớn nhất thế giới”.

Để sắp xếp mọi thứ, tôi tìm số fax của trụ sở toàn cầu của Oakwood, rồi hack vào bộ chuyển mạch của công ty điện thoại và tạm thời chuyển tiếp đường điện thoại đó để bất cứ cuộc gọi fax đến nào cũng sẽ được chuyển đến chiếc máy fax ở Kinko’s tại Santa Monica.

Trong một cuộc gọi đến trụ sở Tập đoàn Oakwood, tôi hỏi tên viên quản lý rồi gọi đến văn phòng cho thuê ở tòa nhà của Eric. Một phụ nữ trẻ với giọng nói dễ chịu và thái độ niềm nở nghe máy. Tự xưng mình là viên quản lý mà tôi vừa lấy được tên, tôi nói: “Chúng tôi có vấn đề pháp lý với một trong số những người thuê nhà ở đó. Tôi cần cô fax cho tôi đơn đăng ký thuê nhà của

https://thuviensach.vn

Joseph Wernle.” Cô ấy nói sẽ giải quyết ngay. Tôi chắc chắn số fax cô ấy có là số mà tôi đã chuyển tiếp đến Kinko’s.

Tôi đợi cho đến khi bản fax được gửi đi, gọi đến tiệm Kinko’s mà bản fax được chuyển đến. Tôi nói với viên quản lý ở đó rằng tôi là trưởng gian hàng ở một địa điểm Kinko’s khác và giải thích: “Tôi có một khách hàng ở đây đang đợi một bản fax. Anh ta vừa nhận ra anh ta gửi đến nhầm tiệm Kinko’s.” Tôi nhờ anh ta tìm bản fax và gửi lại đến Kinko’s “của tôi”. Bước thứ hai này khiến cho bất cứ cảnh sát liên bang nào muốn truy lần ra tác phẩm của tôi cũng gặp phải nhiều khó khăn hơn. Tôi gọi nó là “rửa fax”.

Nửa tiếng sau, tôi đến một tiệm Kinko’s địa phương và lấy bản fax, trả tiền mặt.

Nhưng sau tất cả những nỗ lực đó, tờ đăng ký cũng không làm sáng tỏ điều gì. Nó chỉ làm tăng thêm sự bí ẩn. Các chủ sở hữu của những tòa nhà cho thuê thường yêu cầu thông tin cá nhân để chắc chắn người thuê mới của họ không đem đến rủi ro tài chính nào. Nhưng trong trường hợp này, Oakwood đã cho một gã thuê nhà gần như không cung cấp thông tin gì. Không người thân. Không tài khoản ngân hàng. Không địa chỉ trước đó.

Và đáng kể nhất, không đề cập đến tên của Eric. Căn hộ được cho thuê với cùng một cái tên trong dịch vụ điện thoại, Joseph Wernle. Thông tin khác duy nhất trong cả tờ đơn là số điện thoại chỗ làm, 213 507-7782. Nhưng ngay cả số điện thoại đó cũng rất bí hiểm: Tôi có thể dễ dàng xác định, nó không phải là số điện thoại văn phòng, mà là một số điện thoại di động do PacTel Cellular cung cấp dịch vụ.

Nhưng ít nhất nó cũng cho tôi một đầu mối để lần theo.

Tôi thực hiện một cuộc gọi đến PacTel Cellular để lấy tên cửa hàng đã bán số điện thoại được liệt kê trong đơn xin thuê nhà của Eric: One City Cellular, ở khu lân cận Westwood của Los Angeles, khu vực bao gồm khuôn

https://thuviensach.vn

viên UCLA. Tôi thực hiện một cú điện thoại giả danh đến cửa hàng này và nói rằng tôi muốn một ít thông tin về tài khoản "của tôi".

"Tên ông là gì, thưa ông?" người phụ nữ đầu dây bên kia hỏi.

Tôi nói với cô ta: "Nó nằm dưới mục 'Chính phủ Mỹ'" – hy vọng là cô ta sẽ sửa sai cho tôi... hy vọng là tôi đã nói sai. Và tôi cũng hy vọng cô ta có thể đưa giúp tôi tên tài khoản.

Cô ta nói. "Ông là Mike Martinez phải không?"

Cái quái gì vậy?!

"Phải, tôi là Mike. Nhân tiện, phiền cô nhắc lại số tài khoản của tôi là gì vậy?"

Đó chỉ là thử vận may, nhưng cô ta là nhân viên bán hàng ở một cửa hàng điện thoại di động, không phải là một nhân viên chăm sóc khách hàng đầy hiểu biết ở một công ty điện thoại di động. Cô ta không chút nghi ngờ đọc số tài khoản cho tôi.

Heinz ... Wernle... Martinez.

Cái quái gì đang xảy ra vậy?

Tôi gọi lại cho cửa hàng điện thoại. Vẫn cùng một người phụ nữ trả lời. Tôi gác máy, đợi thêm một chút và thử lại. Lần này tôi tóm được một anh chàng. Tôi đưa cho anh ta tên, số điện thoại và số tài khoản "của tôi". "Tôi làm mất ba hóa đơn gần nhất rồi," tôi nói và nhờ anh ta fax chúng cho tôi ngay lập tức. "Tôi lỡ xóa danh bạ khỏi điện thoại di động và cần những hóa đơn này để làm lại nó," tôi nói.

Trong vòng vài phút, anh ta đã gửi tôi bản fax của những tờ hóa đơn. Tôi tăng tốc xe, nhưng hy vọng không nhanh đến mức khiến tôi bị tấp vào lề

https://thuviensach.vn

đường, vì vội đến Kinko's. Tôi muốn biết càng sớm càng tốt xem có gì trong những hóa đơn kia.

Bản fax hóa ra đắt giá hơn rất nhiều so với tôi dự tính. Khi nhìn vào hóa đơn của Martinez, tôi há hốc mồm. Mỗi một tờ hóa đơn trong ba tháng đó dài gần 20 trang, liệt kê hơn trăm cuộc gọi. Rất nhiều trong số đó đến từ mã vùng 202 – Washington, D.C. – và cũng có rất nhiều cuộc gọi đến 310 477-6565, trụ sở Los Angeles của FBI.

Ôi, chết tiệt! Tôi lại thêm phần khẳng định rằng Eric chắc chắn là một đặc vụ FBI. Tình thế càng lúc càng đáng lo ngại mỗi khi tôi tiến thêm một bước. Tất cả đầu mối tôi lần theo đều dẫn tôi đến những người mà tôi muốn tránh xa nhất.

Bình tĩnh nào! Đó không phải là khả năng duy nhất. "Người bạn" mới Eric Heinz của tôi có thể thực sự là một đặc vụ, nhưng nghĩ lại thì điều đó thật khó tin – lúc đó, tôi đã phát hiện ra hắn ta không chỉ giao du ở các câu lạc bộ rock-and-roll. Đám người mà hắn hay đi cùng bao gồm cả người trung gian ban đầu của chúng tôi, Henry Spiegel, người đã nói với tôi rằng anh ta từng thuê cả Susan Headley, hay còn gọi là Susan Thunder, ả điếm hacker, người đã chỉ điểm tôi vụ đột nhập vào trung tâm COSMOS và cũng từng cắt hết đường dây điện thoại đi ra từ khu chung cư của mẹ tôi để trả thù. Còn có cả những câu chuyện của chính Eric về việc làm tình mỗi đêm với các vũ nữ khỏa thân khác nhau.

Không, hắn có vẻ không giống dạng người có thể vượt qua vòng sát hạch của FBI để thành đặc vụ tương lai. Vì vậy, tôi đoán hắn không thể nào là đặc vụ. Có thể gã chỉ bị một kẻ ở FBI tóm gáy và bị buộc trở thành người đưa tin bí mật – một kẻ chỉ điểm. Nhưng tại sao?

Chỉ có một lời giải thích hợp lý: FBI đang cố tập hợp một vài hacker.

FBI trước đây từng nhắm đến tôi, và muốn triển khai một vụ truy quét lớn. Giờ đây, nếu những nghi ngờ của tôi là đúng, hắn họ đang lúc lắc củ cà rốt

https://thuviensach.vn

trước mặt tôi. Bằng cách khiến Eric xuất hiện trong đời tôi, các đặc vụ đang thực hiện hành động dí một chai Scotch vào mũi một gã cai nghiện rượu để xem hắn có lầm đường lạc lối nữa không.

Bốn năm trước, vào năm 1988, tờ USA Today thậm chí còn in đè mặt tôi lên một tấm ảnh lớn của Darth Vader[61] trên trang nhất của chuyên mục Money, bôi xấu tôi là "Darth Vader của thế giới hacking" và đào biệt danh cũ "Hacker Hắc ám" của tôi lên.

[61] Nhân vật phản diện nổi tiếng trong loạt phim Star Wars (Chiến tranh giữa các vì sao). (BTV)

Do đó, có lẽ cũng chẳng có gì ngạc nhiên khi FBI quyết định biến tôi thành đối tượng ưu tiên.

Và cũng chẳng khó khăn gì. Sau cùng, thời tôi còn là một chàng trai trẻ, bên phía công tố đã cảm thấy thích đáng khi thao túng một thẩm phán bằng một câu chuyện lố bịch rằng tôi có thể phóng tên lửa hạt nhân chỉ bằng một cuộc gọi đến NORAD và huýt sáo vào điện thoại. Tôi chắc rằng họ sẽ không ngần ngại làm lại chuyện đó lần nữa nếu có cơ hội.

Địa chỉ trên hóa đơn điện thoại của Mike Martinez hóa ra là văn phòng của một tay luật sư nào đó ở Beverly Hills.

Tôi gọi đến văn phòng đó, tự nhận mình đến từ One City Cellular, nhà cung cấp di động của Martinez. "Hóa đơn của các anh quá hạn rồi," tôi nói với cô gái nghe máy. "Ồ, chúng tôi không thanh toán những hóa đơn này," cô ta nói. "Chúng tôi chỉ chuyển nó đến một hộp thư ở Los Angeles" và đưa cho tôi số hộp thư kèm địa chỉ – Tòa nhà Liên bang tại số 11000 Đại lộ Wilshire. Không hay rồi.

Cuộc gọi tiếp theo của tôi là đến Dịch vụ Giám sát Bưu chính ở Pasadena. "Tôi cần gửi khiếu nại," tôi nói. "Ai là giám sát viên khu vực Westwood ở Los Angeles vậy?"

https://thuviensach.vn

Dùng tên của giám sát viên này, tôi gọi đến bưu điện trong Tòa nhà Liên bang, hỏi người quản thư, và nói: “Tôi cần ông tìm đơn đăng ký cho hộp thư này rồi đưa tôi tên và địa chỉ người nhận.”

“Hộp thư này được đăng ký cho FBI ở đây tại 11000 Wilshire.” Tin này không có gì bất ngờ.

Vậy ai là người đã nhận mình là Mike Martinez? Mối quan hệ của anh ta với FBI là gì?

Dù rất nóng lòng muốn biết chính phủ đã biết gì về tôi, nhưng việc đào sâu hơn không hợp lý chút nào. Nếu lún sâu hơn nữa vào chuyện này, khả năng tôi bị tóm và tống lại nhà tù sẽ cao hơn. Tôi không thể đối mặt với việc đó. Nhưng liệu tôi có thể thực sự chối bỏ ham muốn đó?

https://thuviensach.vn

20
CẮN NGƯỢC

Wspa wdw gae ypte rj gae dilan lbnsp loeui V tndllrhh gae awvnh "HZO, hzl jaq M uxla nvu?"

Cục Cấp phép Phương tiện Cơ giới (DMV) California là một trong những nguồn khai thác thông tin lớn nhất và cũng là nguyên nhân của một trong những lần chạy trốn suýt chết sau này của tôi. Làm sao để đăng nhập vào DMV thì lại là cả một câu chuyện dài.

Bước đầu tiên là tìm số điện thoại mà mấy tay cớm thường dùng cho các cuộc gọi chính thức tới DMV. Tôi gọi tới trụ sở cảnh sát Quận Orange, hỏi thăm Đơn vị Điện tín và nói với tay cảnh sát trực máy rằng: "Tôi cần số DMV để tìm hiểu một Soundex đã yêu cầu vài ngày trước." (theo thuật ngữ của DMV, khi bạn muốn bản sao ảnh bằng lái xe của một ai đó, bạn sẽ hỏi về Soundex.)

"Anh là ai?" anh ta hỏi.

"Trung úy Moore," tôi đáp. "Tôi gọi số 916 657-8823 nhưng có vẻ số đó không còn hoạt động nữa." Có ba điểm được vận dụng để tăng khả năng thành công ở đây. Thứ nhất, tôi gọi tới sở bằng số nội bộ mà người ngoài thường không thể tiếp cận. Thứ hai, có chút rủi ro nhưng khá hợp lý, tôi đưa ra một số điện thoại sai nhưng với mã vùng và đầu số mà tôi đoán chắc là chính xác, bởi tại thời điểm đó (như đã đề cập đến), DMV được phân cho toàn bộ đầu số 657, như vậy, các số điện thoại mà cơ quan hành pháp sử dụng rất có khả năng là 916 657-XXXX. Tay cảnh sát trực máy sẽ để ý thấy tôi đọc dãy số gần đúng chỉ trừ bốn số cuối. Và thứ ba, tôi đã nâng cấp cho

https://thuviensach.vn

bản thân lên hàng trung úy. Nhân viên sở cảnh sát cũng có suy nghĩ tương tự như trong quân đội: Không ai muốn từ chối một người ở cấp bậc cao hơn.

Anh ta cho tôi số điện thoại đúng.

Kế tiếp, tôi cần phải biết có bao nhiêu đường dây điện thoại trong DMV phụ trách các cuộc gọi xử lý vấn đề hành pháp và số điện thoại của mỗi máy. Tôi tìm hiểu được rằng bang California dùng bộ chuyển mạch điện thoại của Northern Telecom có tên DMS-100. Tôi gọi tới Sở Điện tử Viễn thông bang California và đề nghị gặp kỹ thuật viên làm việc về DMS-100. Tay kỹ thuật viên cầm máy không chút nghi ngờ khi tôi nói rằng mình thuộc Trung tâm Hỗ trợ Kỹ thuật của Northern Telecom ở Dallas, do đó, tôi bắt đầu bài diễn văn: "Chúng tôi gặp trục trặc với phần mềm mới ra bởi các cuộc gọi đều bị chuyển hướng nhầm số. Chúng tôi đã có bản vá sửa lỗi đơn giản thôi và các anh sẽ không gặp vấn đề gì đâu. Nhưng tôi không tìm được số dial-up cho bộ chuyển mạch của các anh trong cơ sở dữ liệu khách hàng."

Giờ mới tới phần khó nhằn. Tôi thích hoàn thiện phần này nhờ thêm vào vài từ ngữ khiến đối tượng không thể phản đối. Tôi nói: "Vậy số dial-in[63] là bao nhiêu và lúc nào thì chúng tôi có thể sửa lỗi được?"

[63] Số dial-in: Số điện thoại được dùng để kết nói tới dịch vụ hay hệ thống máy tính thông qua đường dây điện thoại. (BTV)

Tay kỹ thuật mừng rỡ cho tôi số dial-in của bộ chuyển mạch, bởi như vậy anh ta sẽ không phải tự mình cập nhật phần mềm.

Ngày đó, một số bộ chuyển mạch điện thoại đã có mật khẩu bảo vệ tương tự như các hệ thống máy tính của công ty. Tên tài khoản mặc định rất dễ đoán: "NTAS", viết tắt của "Northern Telecom Assistance Support" (Trung tâm Hỗ trợ Kỹ thuật của Northern Telecom). Tôi quay số tay kỹ thuật viên vừa cho, nhập tên tài khoản và bắt đầu thử dò mật khẩu.

"ntas"? Không được.

https://thuviensach.vn

“update”? Không được.

Thế “bản vá lỗi”? Cũng không được nốt.

Tôi thử thêm một mật khẩu khác thường được dùng cho bộ chuyển mạch của Northern Telecom ở một công ty khác cũng tách ra từ AT&T: “helper”.

Trúng quả rồi!

Do Northern Telecom muốn đơn giản hóa công việc dành cho các kỹ thuật viên hỗ trợ, mọi bộ chuyển mạch đều có thể truy cập cùng một mật khẩu. Ngu ngốc làm sao. Nhưng rất tốt cho tôi.

Có tên tài khoản và mật khẩu, giờ đây, tôi đã có thể toàn quyền đăng nhập vào bộ chuyển mạch và kiểm soát toàn bộ số điện thoại thuộc về DMV ở Sacramento.

* * *

Từ máy tính riêng, tôi tra số điện thoại chuyên dùng cho cơ quan hành pháp mình mới lấy được và phát hiện ra bộ phận này có 20 đường đây trong một “hunt group” (nhóm đi săn) – tức là khi tất cả các đường dây điện thoại dành cho cảnh sát đều bận, cuộc gọi kế tiếp sẽ tự động được chuyển sang số máy rảnh tiếp theo trong số 20 đường dây đó. Bộ chuyển mạch sẽ “săn” một đường dây không bận.

Tôi quyết định đặt cho mình số thứ 18 trong danh sách (bởi nếu chọn số máy bên dưới danh sách, tôi sẽ chỉ nhận cuộc gọi khi hầu hết các đường dây đều bận, còn nếu chọn số máy bên trên, tôi sẽ liên tục bị làm phiền bởi các cuộc gọi tới). Tôi nhập lệnh vào bộ chuyển mạch để thêm tính năng chuyển cuộc gọi và tự động chuyển cuộc gọi tới đường dây đó để chúng chuyển tới máy di động của tôi.

https://thuviensach.vn

Hắn là không mấy ai liều như tôi hồi đó. Các cuộc gọi bắt đầu đến từ Cục Tình báo, Cục Quản lý Đất đai, Cơ quan Hành pháp chống Ma túy, Cục Rượu, Vũ khí, Thuốc lá và Chất nổ.

Bạn biết không, tôi thậm chí còn nhận được cuộc gọi từ các đặc vụ FBI – những người có quyền còng tay và tống tôi vào ngục một lần nữa.

Mỗi khi những gã này gọi đến, cứ ngỡ mình đang nói chuyện với ai đó ở DMV, tôi sẽ hỏi một loạt các thông tin bí mật – tên, cơ quan, mã yêu cầu, số bằng lái xe, ngày sinh và tương tự. Tôi cũng không gặp nguy hiểm gì khi làm vậy, vì dù sao, không ai trong số họ có thể nghĩ rằng người ở đầu dây bên kia lại không thuộc DMV.

Tôi phải thừa nhận rằng khi nhận được những cuộc gọi như vậy, đặc biệt là từ ai đó thuộc cơ quan hành pháp, tôi thường nhận máy và phải cố gắng nhịn cười.

Có lần, tôi nhận được điện thoại khi đang ăn trưa với ba người bạn ở Bob Burns, một quán nướng xuất sắc ở Woodlands. Tôi ra dấu yêu cầu mọi người giữ yên lặng khi chuông reo, và họ đều nhìn tôi như thể: “Chuyện quái gì thế?” Sau đó, họ nghe thấy tôi trả lời: “DMV xin nghe, tôi có thể giúp gì cho bạn?” Họ trao đổi với nhau bằng ánh mắt “Mitnick lại có vụ gì vậy?” Trong lúc đó, tôi trả lời và gõ ngón tay trái lên mặt bàn để tạo âm thanh như thể đang gõ vào bàn phím.

Mấy gã bạn dần hiểu ra vấn đề, miệng há hốc.

Khi tôi đã thu thập đủ các thông tin bí mật, tôi gọi lại vào bộ chuyển mạch, tạm thời tắt tính năng chuyển cuộc gọi cho tới khi cần thêm các thông tin khác.

Hack được vào DMV khiến tôi thực sự vui sướng. Đây là một công cụ siêu giá trị rất có tác dụng về sau này.

https://thuviensach.vn

Nhưng tôi vẫn vô cùng khao khát muốn biết cảnh sát liên bang đã biết được chừng nào, họ đã nắm trong tay những bằng chứng gì, tôi sẽ gặp rắc rối lớn ra sao và liệu có cách gì để tôi thoát khỏi chuyện đó. Liệu tôi còn có thể tự cứu lấy mình?

Tôi biết sẽ thực ngu ngốc nếu tiếp tục điều tra về Eric. Nhưng cũng giống như trong quá khứ, cám dỗ trong cuộc mạo hiểm và thử thách trí tuệ này khiến tôi thấy rất kích thích.

Đây là một câu đố cần có lời giải. Và tôi sẽ không dừng lại.

Mark Kasden của Teltec gọi điện mời tôi ăn trưa cùng ông ta và Michael Grant, con trai của người đồng sở hữu.

Tôi dùng bữa cùng Michael và Mark ở nhà hàng Coco gần văn phòng làm việc của họ. Michael có dáng người mập lùn và có vẻ rất hài lòng về bản thân, thậm chí có phần vênh váo. Cả hai đều cảm thấy thích thú khi dụ tôi kể lại những trải nghiệm của bản thân. Tôi cũng chứng minh rằng mình giỏi tấn công bằng kỹ thuật xã hội ra sao. Đây cũng là trò mà họ hay dùng, dù họ gọi nó là "trò phỉnh". Hai người họ cũng tỏ ra ấn tượng về những gì tôi biết cũng như những gì tôi đã làm với máy tính và đặc biệt là với các công ty điện thoại. Họ thậm chí còn ấn tượng hơn nữa với kinh nghiệm của tôi về dò tìm địa chỉ, số điện thoại và các thông tin khác của mọi người. Tìm người có vẻ là một phần quan trọng trong công việc của họ, một quá trình mà họ gọi là "định vị".

Sau bữa trưa, họ dẫn tôi tới văn phòng làm việc trên tầng hai của một tòa nhà nằm trong khu mua sắm. Ngoài cửa ra vào là khu đón khách với một quầy lễ tân, kế đó là chuỗi phòng làm việc riêng dành cho ba tay thám tử tư và ba lãnh đạo.

Chừng một hai ngày sau, Mark rẽ qua nhà cha tôi và nói: "Chúng tôi muốn cậu đến làm việc cùng chúng tôi." Mức lương chẳng có gì đáng để khoe khoang nhưng cũng đủ để trang trải sinh hoạt phí.

https://thuviensach.vn

Họ đặt cho tôi chức danh “Nghiên cứu viên” để không gây nghi ngờ cho viên giám sát phụ trách quá trình quản chế của tôi.

Tôi có một phòng làm việc riêng nhỏ, đơn giản hết mức với bàn, ghế, máy tính và điện thoại. Không sách, không đồ trang trí, toàn bộ là tường trống.

Tôi nhận thấy Michael là một người khá thông minh và rất dễ nói chuyện. Những cuộc hội thoại với anh ta thường giúp củng cố lòng tự tôn trong tôi, bởi tôi có thể cho anh ta thấy những gì các nhân viên khác không làm được, sau đó, anh ta sẽ thể hiện rõ sự khâm phục của mình.

Trước tiên, Mark và Michael muốn tôi tập trung vào một tình huống mà họ vẫn băn khoăn. Những thiết bị giám sát điện thoại tôi đã phát hiện ra trên đường dây của Teltec – tại sao cơ quan hành pháp lại nghi ngờ những gì họ làm?

Họ có tên của hai người mà họ cho rằng đang phụ trách việc này: Thám tử David Simon ở Sở Cảnh sát Quận Los Angeles và Darrell Santos ở Phòng An ninh Pacific Bell. “Cậu có cách nào để theo dõi điện thoại của tay thám tử kia không?” sếp của tôi hỏi.

“Đương nhiên, nhưng vậy thì rủi ro quá.” Tôi đáp.

“Ừm, để xem cậu có thể tìm ra được gì trong cuộc điều tra này.”

Vừa đúng lúc tôi cũng phát hiện ra những gì mấy gã quản lý của Teltec còn giấu giếm: Trước đó vài tháng, tay thám tử này đã chỉ đạo cả một đội quân chuyên đi lùng sục tất cả công ty thám tử tư vì tội sử dụng mật khẩu trái phép để tiếp cận báo cáo tín dụng của TRW.

Mừng là tôi không có hứng điều tra cảnh sát – nhưng theo dõi Phòng An ninh PacBel lại là chuyện khác. Đối với tôi, việc này như thể trò chơi thử thách tài khéo léo, một thử thách mà tôi có lẽ sẽ hứng thú.

https://thuviensach.vn

21
MÈO VÀ CHUỘT

4A 75 6E 67 20 6A 6E 66 20 62 68 65 20 61 76 70 78 61 6E 7A 72 20 74 76 69 72 61 20 67 62 20 47 72 65 65 6C 20 55 6E 65 71 6C 3F

Do Lewis hạn chế rất nhiều thời gian hacking để khiến Bonnie vui lòng, nên tôi lại sa vào hacking với một người bạn khác của anh ta. Terry Hardy chắc chắn không phải là kiểu người mà bạn có thể gặp hằng ngày. Anh ta có dáng người dong dỏng và vầng trán cao, cùng giọng nói đều đều như rô-bốt. Chúng tôi đặt cho anh ta biệt danh là "Klingon", dựa theo một chủng người ngoài hành tinh trong loạt phim Star Trek (tạm dịch: Du hành giữa các vì sao), bởi chúng tôi cho rằng anh ta có một vài đặc trưng ngoại hình giống họ. Là một người uyên bác, anh ta có thể liên tục vừa nhìn thẳng vào mắt bạn nói chuyện vừa gõ 85 chữ một phút trên máy tính. Bạn sẽ phải ngạc nhiên và kinh sợ khi chứng kiến khả năng này.

Một ngày nọ, khi Terry, Lewis và tôi đang ở cùng Dave Harrison ở văn phòng của Dave, tôi nói: "Này, chúng ta hãy cùng xem liệu mình có thể lấy được mật khẩu hòm thư thoại của Darrell Santos không." Đây sẽ là một cách để chứng tỏ bản thân với những người ở Teltec. Nếu tôi thực sự có thể thực hiện thành công.

Tôi gọi đến khung dây cung cấp các số điện thoại tại văn phòng của Phòng An ninh Pacific Bell và nhờ một kỹ thuật viên tìm cáp đôi cho một số điện thoại mà tôi đã đưa cho anh ta: số của nhân viên điều tra an ninh thuộc Pacific Bell, Darrell Santos.

Mục đích của tôi là đặt một kết nối SAS lên đường dây của Santos, nhưng tôi muốn thực hiện việc này theo cách thật đặc biệt. Sau khi nghiên cứu về

https://thuviensach.vn

SAS, tôi biết có một thứ được gọi là “giày SAS”, một kết nối vật lý cho phép bạn nhảy vào một đường dây và ở lại đó, nghe thấy mọi cuộc gọi mà thuê bao đó gọi đi hoặc nhận được. Và với phương pháp này, sẽ không có tiếng click trên đường dây khi kết nối SAS được thiết lập.

Nhân viên kỹ thuật này sẽ nghĩ gì nếu anh ta biết nhánh điện thoại mà anh ta đang cài đặt lại nằm trên đường dây thuộc về Phòng An ninh Pacific Bell?

Giờ là thời điểm thích hợp nhất. Ngay khi vừa nhảy vào đường dây, tôi nghe thấy một giọng nữ nói: “Xin hãy nhập mật khẩu.” Terry Hardy cũng vô tình ở cạnh tôi khi đó. Một trong những khả năng dị thường khác của Terry là anh ta có khả năng cảm âm hoàn hảo hiếm gặp: Anh ta có thể nghe được âm bàn phím của một số điện thoại đang được nhập và nói cho bạn biết số đó.

Tôi gào qua phòng để Lewis và Dave trật tự rồi nói: “Terry, nghe đi, nghe đi!” Anh ta tiến gần tới loa ngoài điện thoại vừa đúng lúc nghe được tiếng bấm phím khi Santos nhập mật khẩu hòm thư thoại của ông ta.

Terry đứng đó, như thể lạc theo dòng suy nghĩ. Trong khoảng 20 giây. Tôi không dám chen ngang.

Rồi anh ta nói, “Tôi nghĩ đó là ‘1313.’”

Trong 2-3 phút sau đó, chúng tôi đều đứng đó chết lặng trong khi Santos – và cả bốn chúng tôi – cùng nghe các tin nhắn trong hộp thư thoại của ông ta. Sau khi Santos gác máy, tôi gọi đến số truy cập hòm thư thoại của ông ta và nhập vào mật khẩu “1313”.

Vào được rồi.

Chúng tôi choáng váng! Dave, Lewis, Terry và tôi đều nhảy lên đập tay nhau.

https://thuviensach.vn

Terry và tôi cùng lặp lại quy trình tương tự và cuối cùng, chúng tôi đã lấy được cả mật khẩu hòm thư thoại của Lilly Creek.

Tôi bắt đầu coi việc kiểm tra hộp thư thoại của Creek và Santos là công việc thường ngày, sau giờ làm, khi tôi có thể khá chắc chắn họ sẽ không thử gọi vào cùng lúc: nhận được tin nhắn rằng hộp thư thoại của họ đang được sử dụng sẽ tạo ra một báo động đỏ to đùng.

Vài tuần sau, tôi nghe được một chuỗi tin nhắn do thám tử Simon để lại, thông báo cho Santos tình hình điều tra của ông ta ở Teltec. Khi biết họ không phát hiện ra điều gì mới, các sếp của tôi sẽ rất an tâm. (Còn có một sự ngẫu nhiên khó tin nổi trong thế giới nhỏ bé này, thám tử Simon – khi đó vẫn đang đương chức tại Sở Cảnh sát Los Angeles, giờ là Cảnh sát trưởng Dự bị – lại là anh em sinh đôi với đồng tác giả cuốn sách này của tôi, Bill Simon.)

Trong lúc đó, cứ thỉnh thoảng tôi lại nhớ đến thông tin như trêu ngươi đó, khi tôi nhận được một trong những lời cáo buộc chống lại Kevin Poulsen vì một vụ hack mà Eric nói hắn đã tham gia: Cuộc thi trên sóng phát thanh được cho là đã đem về cho Eric một chiếc Porsche và bản thân Poulsen hai cái nữa. Vào một khoảnh khắc lạ thường khác, tôi lại nhớ ra cuộc thi từng nghe trên radio, trong lúc lái xe đến Vegas, vào cái ngày thê lương không lâu sau cái chết của người em trai cùng cha khác mẹ. Cuối cùng, tôi đã móc nối hai sự việc này lại với nhau.

Eric từng nói với Lewis và tôi rằng bước đầu chuẩn bị cho cuộc thi trên sóng phát thanh của Poulsen dựa vào việc hack vào bộ chuyển mạch của công ty điện thoại ở văn phòng trung tâm chuyên xử lý các đường dây điện thoại của đài radio. Tôi nghĩ có thể có cách làm việc đó mà không cần phải chọc phá bộ chuyển mạch. KRTH phát thanh từ các văn phòng không quá xa chỗ Dave và cả hai đều do cùng một văn phòng trung tâm cung cấp dịch vụ.

https://thuviensach.vn

Để bắt đầu, tôi sẽ cần một số điện thoại khác số 800 mà người dẫn chương trình đã thông báo trên sóng. Gọi đến một ban nội bộ Pacific Bell, tôi hỏi số "POTS" cho số 800. ("POTS" là từ viết tắt của "plain old telephone service" – số dịch vụ điện thoại cũ; đây là một thuật ngữ chuẩn, được sử dụng hằng ngày tại các công ty điện thoại.) Tôi cần số POTS bởi số 800 dùng cho cuộc thi trên sóng phát thanh có đặt một "van điều tiết", giới hạn luồng cuộc gọi đến từ mỗi vùng phát thanh của đài và kế hoạch sẽ bị đổ bể nếu bất cứ cuộc gọi nào của tôi bị nghẽn. Người phụ nữ nhấc máy thậm chí còn không buồn hỏi tên tôi hay liệu tôi có làm ở Pacific Bell hay không; cô ta cứ thế đưa tôi con số.

Tại văn phòng của Dave Harrison, tôi lập trình tính năng gọi nhanh trên bốn đường điện thoại, sao cho tất cả những gì tôi cần làm để quay số trực tiếp đến số POTS ở đài radio là ấn "#9". Dựa theo thực tế, tôi tính toán sao cho các cuộc gọi định tuyến đến số 800 sẽ mất nhiều thời gian kết nối hơn một chút. Ngoài ra, các số trong văn phòng của Dave cũng được chuyển mạch qua cùng một văn phòng trung tâm với số POTS của đài, nghĩa là các cuộc gọi của chúng tôi sẽ được hoàn tất ngay lập tức. Nhưng liệu những lợi thế nhỏ nhoi đó, cộng với việc sử dụng nhiều đường dây điện thoại, có đủ để tạo nên sự khác biệt?

Khi tất cả đã được thiết lập, Lewis, Terry Hardy, Dave và tôi mỗi người ngồi ôm một chiếc điện thoại và sẵn sàng gọi. Chúng tôi khó có thể chờ đến khi cuộc thi được phép bắt đầu. Người gọi đến thứ bảy sẽ là người thắng cuộc. Chúng tôi chỉ cần gọi liên tục cho đến khi một trong số chúng tôi là người gọi thứ bảy.

Ngay khi chúng tôi nghe thấy nhạc hiệu thông báo bắt đầu nhận cuộc gọi – giai điệu "The best oldies on radio" (tạm dịch: Những khúc nhạc cũ tuyệt vời nhất trên radio) – chúng tôi sẽ nhanh chóng bấm "#9". Mỗi lần chúng tôi kết nối thành công và nghe DJ nói: "Bạn là người gọi thứ ___," và đưa ra một con số nhỏ hơn bảy, chúng tôi sẽ ngắt máy ngay lập tức và lại gọi "#9" một lần nữa. Chúng tôi cứ lặp đi lặp lại hành động đó liên tục.

https://thuviensach.vn

Lần thứ ba quay số nhanh, tôi nghe thấy giọng nói thông báo: “Bạn là người gọi thứ bảy!”

Tôi đã gào toáng lên trên điện thoại: “Tôi thắng rồi! Không thể nào, tôi đã thắng rồi ư? Các anh đang đùa à? Không thể tin được! Tôi chưa bao giờ thắng bất cứ thứ gì!” Tất cả chúng tôi đứng dậy và đập tay. Giải thưởng là 1.000 đô-la và chúng tôi đồng ý sẽ chia nhau. Mỗi khi bất kỳ ai trong chúng tôi thắng, chúng tôi sẽ bỏ tiền số thắng cuộc vào một chiếc lọ.

Sau bốn lần thắng đầu tiên, dù biết hệ thống đã hoạt động, nhưng chúng tôi còn phải đối mặt với một thử thách mới: Nhà đài có quy định rằng không ai có thể thắng cuộc thi quá một lần một năm. Chúng tôi bắt đầu đề nghị thỏa thuận với gia đình, bạn bè hay bất kỳ ai đủ tin tưởng: “Khi tấm séc được chuyển đến, cậu hãy giữ lại 400 đô-la cho mình và chuyển 600 đô-la cho chúng tôi.”

Trong ba hay bốn tháng sau đó, chúng tôi đã thắng cuộc thi khoảng 50 lần. Cuối cùng, chúng tôi chỉ chịu dừng lại khi không còn bạn bè nào nữa! Thật tiếc là Facebook lúc đó chưa tồn tại – chúng tôi sẽ có thêm rất nhiều bạn bè cùng đồng hành.

Cái hay của chuyện này là nó thậm chí không hề bất hợp pháp. Tôi đã xác nhận lại với luật sư rằng miễn là chúng tôi không tiếp cận bất hợp pháp thiết bị của công ty điện thoại hoặc dùng danh tính của bạn bè không xin phép, thì đây không phải là hành vi lừa đảo. Thậm chí, khi lần đầu lấy số POTS, tôi còn không tự nhận mình là nhân viên công ty điện thoại, tôi chỉ hỏi số và người phụ nữ đó đã đưa nó cho tôi.

Về mặt kỹ thuật, chúng tôi cũng tuân thủ luật của trò chơi. Đài radio có quy định rằng một người chỉ được thắng một lần một năm. Chúng tôi cũng tuân thủ điều đó. Chúng tôi chỉ đơn giản khai thác một kẽ hở. Chúng tôi chưa bao giờ vi phạm bất cứ quy định nào.

https://thuviensach.vn

Một lần, tôi đã tự khiến mình ngạc nhiên khi thử vận may. Đài phát thanh đưa ra một số điện thoại để bạn có thể gọi đến chương trình. Tôi đã gọi từ phòng khách căn hộ của mẹ tôi tại Las Vegas và khi chương trình lên sóng, tôi gọi, không dám nghĩ mình có thể gọi đến đài kịp lúc để trở thành người gọi thứ bảy. Nhưng khi tôi nghe thấy những từ kỳ diệu kia, những lời chúc mừng... theo sau là câu hỏi của người phát thanh viên: "Anh tên là gì?", tôi cứ ậm ừ cho đến khi nghĩ ra tên của một người bạn mà tôi chưa dùng tới. Tôi dùng tên anh ta và bao biện cho khoảnh khắc ngập ngừng bằng cách phun ra: "Tôi vui quá, nghẹn ngào tới mức không thể thốt ra tên của chính mình!"

Bốn người chúng tôi thu về gần 7.000 đô-la mỗi người trong cả phi vụ. Có lúc, khi tôi gặp Lewis ở một nhà hàng và đưa cho cậu ta phần của mình, tôi còn cầm nhiều tiền mặt đến mức tôi cảm giác như mình đang thanh toán một vụ buôn ma túy hay gì đó.

Tôi dùng phần lớn số tiền kiếm được để mua cho mình chiếc laptop tân tiến nhất đầu tiên, một chiếc Toshiba T4400SX có vi xử lý 486 với tốc độ ấn tượng vào thời điểm đó, 25 megahertz, nhanh đến nỗi chóng cả mặt. Tôi đã chi 6.000 đô-la. Và đó là giá bán buôn!

Thật buồn khi chúng tôi đã không còn ai có thể tin tưởng để hợp tác.

Một tối nọ, không lâu sau khi chúng tôi bắt đầu cuộc thi trên sóng phát thanh, khi tôi đang lái xe về lại căn hộ của cha thì một ý tưởng bỗng nảy ra trong đầu tôi, một kế hoạch có thể đem về cho tôi một chút không khí dễ chịu khi đang cố vạch ra chân tướng vụ bí ẩn về Eric Heinz/Mike Martinez/Joseph Wernle/Joseph Ways.

Ý tưởng của tôi là để Lewis buột miệng mớm thông tin về tôi cho Eric. Cậu ta sẽ nói một số chuyện kiểu như: "Kevin đang nghĩ đến việc cộng tác với vài hacker ở châu Âu. Cậu ta chắc rằng việc đó sẽ khiến mình trở nên rất giàu có."

https://thuviensach.vn

Tôi nghĩ rằng: Bất cứ thông tin gì FBI biết về tôi sẽ chỉ nhỏ như hạt cát trên sa mạc khi đặt cạnh viễn cảnh bắt được tận tay tôi trong một cuộc hacking lớn, cướp đi hàng núi đô-la hay franc Thụy Sĩ hoặc mark Đức từ một tổ chức tài chính hay tập đoàn nào đó. Họ sẽ muốn giữ kỹ hồ sơ về tôi nhưng sẽ sẵn sàng nhẫn nại chờ đến khi tôi thực hiện phi vụ lớn này, với hy vọng sẽ xông vào, lấy lại tiền và bắt tôi diễu hành trong chiếc còng tay trước đám đông thèm muốn scandal và lũ truyền thông đói khát: FBI đang cứu nước Mỹ thoát khỏi tay một gã ác nhân.

Trong khi chờ dàn xếp vụ hack, tôi hy vọng lệnh quản chế của tôi sẽ hết hiệu lực. Đây có vẻ là một cách trì hoãn tuyệt vời và cho tôi thêm chút thời gian.

Luật sư của Lewis, David Roberts, không thể tìm ra bất cứ vấn đề gì với kế hoạch này. Lewis và tôi đã gặp và bàn chi tiết với ông ta vài lần. Việc Lewis nói dối không vi phạm bất kỳ luật nào, bởi cậu ta sẽ không trực tiếp nói chuyện với một cảnh sát liên bang.

Lệnh quản chế của tôi sẽ hết hiệu lực trong vài tháng tới. Khi Cục mất bình tĩnh vì chờ đợi vụ hack châu Âu của tôi xảy ra, thời gian hết hiệu lực đã trôi qua, họ sẽ để lỡ mất cơ hội tóm lấy và đưa tôi về lại nhà tù vì những vi phạm điều khoản trong điều kiện quản chế.

Họ có chịu đợi lâu đến thế không? Tôi chỉ có thể hy vọng. Vài ngày sau, Lewis báo lại rằng anh ta đã nhắc tới vụ hack quy mô lớn ở châu Âu của tôi với Eric và hắn đã ép anh ta cung cấp thêm thông tin. Lewis bảo hắn rằng vụ hack lớn đến mức tôi không hé lộ chút thông tin nào về nó.

Xuân qua hè tới, tôi bắt đầu cảm thấy mọi việc ở Los Angelino dần đi vào ổn định một lần nữa. Nhưng tôi cần lưu tâm đến việc sắp xếp cuộc sống. Ban đầu, việc chuyển về ở với cha khiến tôi có cảm giác đó như là cách bù đắp cho ngần ấy năm sống xa ông hơn 3.000km khi ông xây dựng gia đình mới. Tôi đã dùng phòng của Adam, một phần bởi cảm giác muốn giúp cha

https://thuviensach.vn

và ở bên ông trong quãng thời gian khó khăn sau cái chết của Adam, và bởi tôi hy vọng chúng tôi sẽ trở nên gần gũi hơn.

Nhưng mọi việc không suôn sẻ như tôi đã hy vọng, còn không gần được như vậy. Chúng tôi đã có vài quãng thời gian tốt đẹp bên nhau nhưng cũng có cả những khoảng thời gian khó khăn như khi tôi còn thơ ấu, khi mối quan hệ của chúng tôi hệt như một bãi chiến trường dày đặc bom mìn.

Tất cả chúng ta đều nhượng bộ khi ở bên những người khác. Dù nghe thật sáo rỗng, nhưng đúng là chúng ta không thể được chọn gia đình. Nhưng đâu đó vẫn có một lằn ranh giữa những thứ chúng ta chọn bỏ qua và chấp nhận, và những thứ khiến mỗi ngày trôi qua trở nên thật khó chịu. Những người phụ nữ đi qua đời tôi đều nhận ra rằng, bản thân tôi không phải là một người dễ sống cùng, vì vậy, tôi chắc lỗi không chỉ nằm ở một phía.

Cuối cùng, cũng đến thời điểm tôi không thể chịu được nữa, tôi thấy khó chịu bởi những lời than phiền thường xuyên của cha rằng tôi đã dành quá nhiều thời gian với điện thoại, nhưng còn khó chịu hơn bởi sự tôn sùng của ông dành cho sự chính xác. Tôi thích sống ở một nơi sạch sẽ và gọn gàng, nhưng với ông, đó lại là nỗi ám ảnh. Nếu bạn nhớ Felix, nhân vật trong phim The Odd Couple (tạm dịch: Cặp đôi lập dị), do Jack Lemmon đóng phiên bản điện ảnh và Tony Randall đóng phiên bản truyền hình, hẳn bạn sẽ nhớ ông ta là kẻ ám ảnh sạch sẽ tới mức ác cảm với những thứ lộn xộn dù là nhỏ nhất.

Felix chỉ là con mèo con so với cha tôi.

Một ví dụ để chứng minh cho điều này là khi cha tôi dùng thước đo để chắc chắn đống mắc treo quần áo trong tủ của ông cách nhau chính xác đến từng phân.

Phiền phức đó sẽ nhân lên gấp bội khi nó được áp dụng vào mọi chi tiết trong căn hộ ba phòng ngủ và bạn sẽ bắt đầu hiểu kiểu ác mộng mà tôi đã trải qua.

https://thuviensach.vn

Mùa xuân năm 1992, tôi bỏ cuộc và quyết định chuyển ra ngoài. Tôi thấy hạnh phúc vì vẫn ở cùng khu căn hộ đó, đủ gần để đến thăm cha thường xuyên nhưng không quá gần khiến tôi bị ông kiểm soát thái quá. Tôi không muốn cha nghĩ tôi đang quay lưng lại với ông.

Tôi đã vô cùng choáng váng khi người phụ nữ ở văn phòng cho thuê bất động sản nói với tôi rằng đang có một danh sách đợi và tôi có thể sẽ phải mất tới vài tháng cho đến khi tìm được một căn hộ. May thay, tôi không mắc kẹt ở chỗ của cha: Mark Kasden ở Teltec đã đồng ý cho tôi dọn đến phòng ngủ dành cho khách của ông ta cho đến khi tìm được nhà.

Sau khi ổn định chỗ ở mới, tôi lao vào một dự án chống lại sự giám sát khác. Từ văn phòng của Dave Harrison, dùng laptop mới, tôi quyết định sẽ xem xem mình có thể thu thập được gì thông qua việc sử dụng SAS để nghe lén các cuộc điện thoại của quản lý Phòng An ninh Pacific Bell, John Venn. Thỉnh thoảng tôi lại nhảy vào đường dây của Venn. Thường thì tôi sẽ vớ phải một cuộc gọi đang diễn ra, cũng không có gì quá thú vị và tôi sẽ chỉ nghe một tai trong khi làm việc khác.

Nhưng vào một ngày mùa hè năm đó, tôi nhảy vào đường dây của Venn khi ông ta đang tiến hành một cuộc điện họp với vài đồng nghiệp. Nếu đây là một cảnh trong phim, hẳn bạn sẽ phải hét toáng lên bởi khả năng nó thực sự xảy ra nghe có vẻ thật xa vời. Nhưng nó đã thực sự xảy ra: Khi nghe thấy ai đó nhắc đến “Mitnick”, tôi lập tức dỏng tai lên nghe ngóng. Cuộc điện thoại thật say sưa, nhiều thông tin... và thật kích thích. Hóa ra mấy gã này vẫn không hiểu làm thế nào tôi có thể đánh bại tất cả hệ thống, đánh sập bẫy của họ và điều đó khiến họ phát cáu.

Họ nói về việc đặt bẫy tóm gọn tôi, có khả năng mang lại bằng chứng đanh thép chống lại tôi để giao tôi cho FBI. Họ đang băn khoăn tôi có thể sẽ làm gì tiếp theo, để chuẩn bị sẵn tận tay tóm tôi.

https://thuviensach.vn

Ai đó gợi ý một kế hoạch hết sức ngu xuẩn. Tôi rất muốn nhảy vào cuộc hội thoại của họ và nói: “Tôi không nghĩ nó sẽ hiệu quả đâu. Tay Mitnick này khá thông minh đấy. Các anh chả bao giờ biết được đâu – hắn có thể đang nghe lén chúng ta ngay lúc này đấy!”

Đúng, tôi từng làm những việc khác cũng liều lĩnh và bất cẩn như vậy, nhưng lần này tôi đã kiềm chế được cơn ham muốn.

Mặt khác, tôi lại ít kiềm chế hơn khi làm những việc liều lĩnh nếu ai đó cần nhờ. Một ngày thứ Năm đầu tháng Sáu, khi không đến chỗ làm do vướng phải một số việc vặt cần làm, tôi nhận được một cuộc gọi điên rồ từ Mark Kasden: Armand Grant, người đứng đầu Teltec, vừa bị bắt. Con trai ông ta là Michael và Kasden đang cố đứng ra bảo lãnh, nhưng phía cảnh sát nói rằng, có thể phải chờ đến một ngày rưỡi sau khi nộp tiền bảo lãnh, Grant mới được thả ra ngoài.

Tôi nói: “Không thành vấn đề. Hãy cho tôi biết khi nào xong, bởi một khi ông ta được bảo lãnh, tôi sẽ đưa ông ta bước ra khỏi đó trong vòng 15 phút.”

Kasden nói: “Không thể nào.”

Vì biết nhân viên chấp pháp rất tôn trọng cấp bậc, tôi chỉ cần gọi đến một trại giam khác ở phía bắc Los Angeles – Wayside – và hỏi: “Chiều nay, trung úy nào trực ca ở đó?” Họ đưa cho tôi tên ông ta. Sau đó, tôi gọi đến Trại giam Trung tâm dành cho nam giới, nơi Grant đang bị giam giữ. Trước đó, tôi đã biết số nội bộ và gọi trực tiếp cho Phòng Ra lệnh bắt. Khi một phụ nữ nghe máy, tôi hỏi số máy lẻ của Phòng Tiếp nhận và Phóng thích. Với một người như tôi, trong tình huống như thế này, việc từng vào tù có rất nhiều lợi thế. Tôi nói với cô ta rằng tôi là Trung úy này nọ (sử dụng cái tên tôi vừa được cho) ở Wayside. “Cô có một tù nhân vừa được nộp tiền bảo lãnh. Anh ta là người đưa tin mật cho một vụ chỗ chúng tôi và tôi cần đưa anh ta ra ngay lập tức” và cung cấp tên của Grant.

https://thuviensach.vn

Tiếng gõ phím máy tính vang lên qua điện thoại. “Chúng tôi vừa nhận được lệnh, nhưng chưa nhập vào.”

Tôi nói tôi muốn nói chuyện với viên hạ sĩ. Khi anh ta nhấc máy, tôi diễn lại vở cũ và nói rằng: “Hạ sĩ, anh có thể giúp tôi một việc cá nhân được không?”

“Vâng, thưa ngài,” anh ta nói. “Ngài cần gì?”

“Khi tiền bảo lãnh của người kia được nộp, anh có thể trực tiếp hướng dẫn anh ta các bước và đưa anh ta ra khỏi đó càng sớm càng tốt được không?”

Anh ta trả lời: “Không vấn đề gì, thưa ngài.”

20 phút sau, tôi nhận được cuộc gọi từ Michael Grant nói rằng cha anh ta đã ra ngoài.

https://thuviensach.vn

22
CÔNG VIỆC THÁM TỬ

Gsig cof dsm fkqeoe vnss jo farj tbb epr Csyvd Nnxub mzlr ut grp lne?

Nếu có thể giúp Grant một cách dễ dàng như vậy, tại sao đến giờ tôi vẫn chưa tìm ra được sự thật về Wernle? Rất may là bí mật sắp được hé mở.

Eric liên tục nói về việc hắn ta phải đi làm, nhưng lại luôn đổi chủ đề mỗi khi tôi hỏi hắn làm nghề gì.

Vậy ai là người trả tiền cho hắn? Có lẽ việc hacking vào tài khoản ngân hàng của hắn sẽ giúp tôi có được câu trả lời. Do tên của Eric không xuất hiện trên hợp đồng thuê nhà cũng như các hóa đơn điện nước, nên tôi tìm tài khoản dưới tên Wernle.

Hắn dùng ngân hàng nào vậy? Các ngân hàng đương nhiên sẽ bảo vệ thông tin khách hàng rất chặt chẽ. Nhưng họ cũng cần đảm bảo rằng các nhân viên có thẩm quyền có thể lấy được thông tin từ các chi nhánh khác nhau.

Thời đó, hầu hết các ngân hàng đều sử dụng một hệ thống cho phép nhân viên xác minh bản thân với đồng nghiệp làm việc ở chi nhánh khác nhờ cung cấp một mã số thay đổi theo ngày. Ví dụ như Bank of America (Ngân hàng Mỹ) dùng năm mã số mỗi ngày, đánh dấu "A", "B", "C", "D" và "E", mỗi chữ cái tương ứng với một số có bốn chữ số khác nhau. Khi một nhân viên ngân hàng gọi điện tới chi nhánh khác để lấy thông tin, anh ta sẽ phải đưa ra con số chính xác cho mã A, mã B hay gì đó. Đây là ý tưởng bảo mật hết sức ngu ngốc của ngành ngân hàng.

Chỉ cần tấn công bằng kỹ thuật xã hội đảo ngược[64], tôi có thể dễ dàng vượt qua lớp bảo mật này.

https://thuviensach.vn

[64] Tấn công bằng kỹ thuật xã hội đảo ngược (reverse social engineering): Một hình thức tấn công phi kỹ thuật, trong đó, hacker sẽ giả mạo những người có đủ thẩm quyền để truy cập thông tin mật, hay giả vờ đóng vai trò chuyên viên hỗ trợ để dò hỏi thông tin. (BTV)

Kế hoạch của tôi có vài bước. Trước tiên vào buổi sớm, tôi gọi tới chi nhánh mục tiêu, hỏi gặp ai đó ở Phòng Tài khoản Mới, giả vờ là một khách hàng tiềm năng với số tiền kha khá trong tay đang quan tâm tới việc làm sao để có được lãi suất cao nhất. Sau khi tạo được mối quan hệ với nhân viên ngân hàng, tôi nói mình có một cuộc họp bây giờ và sẽ gọi lại sau.

Tôi hỏi tên nhân viên ngân hàng và nói: “Cô nghỉ ăn trưa lúc mấy giờ nhỉ?”

“Tôi là Ginette,” cô ta nói. “Tôi sẽ ở đây đến 12 giờ rưỡi.”

Tôi đợi qua 12 giờ 30 phút, gọi điện lại và đòi gặp Ginette. Khi nghe trả lời rằng cô ta đã ra ngoài, tôi giới thiệu bản thân và nói tôi thuộc chi nhánh khác của ngân hàng. “Ginette gọi cho tôi lúc nãy,” tôi giải thích, “cô ấy cần tôi gửi fax thông tin khách hàng. Nhưng tôi có hẹn gặp bác sĩ ngay giờ nên tôi gửi qua cho anh được không?”

Tay đồng nghiệp sẽ nói không vấn đề gì và cho tôi số fax.

“Tốt,” tôi nói. “Tôi gửi giờ đây. À khoan đã… Anh cho tôi biết mã bảo mật ngày hôm nay nhé?”

“Nhưng anh gọi cho tôi cơ mà!” nhân viên ngân hàng kêu lên.

“À vâng, nhưng Ginette gọi cho tôi trước. Mà anh cũng biết chính sách của chúng ta yêu cầu mã bảo mật trước khi gửi đi thông tin khách hàng rồi còn gì...,” tôi bịp bợm. Nếu người đó phản đối, tôi sẽ nói mình không thể gửi thông tin được. Rồi tiếp tục nói thêm kiểu: “Anh nói với Ginette giúp tôi là tôi không gửi tài liệu cho cô ấy được vì anh không xác minh mã bảo mật nhé. Nói thêm với cô ấy là tôi sẽ không ở đây tới tận tuần tới và chúng tôi sẽ

https://thuviensach.vn

bàn thêm sau.” Như vậy là đủ cưỡng ép anh ta phải quyết định, bởi không ai lại muốn làm hỏng việc của đồng nghiệp.

Sau đó, tôi nói: “Vâng, vậy mã E là gì?”

Anh ta cho tôi mã E, ngay lập tức tôi lưu lại trong trí nhớ.

“Không, không phải!” tôi nói.

“Cái gì?”

“Anh nói ‘6214’ đúng không? Mã đó không đúng,” tôi kiên trì.

“Đó đúng là mã E mà!” anh ta sẽ nói vậy.

“Không, tôi không hỏi mã E, tôi nói ‘B’ cơ!” Và sau đó anh ta đọc cho tôi mã B.

Giờ thì tôi có 40% cơ hội có được thông tin mình muốn khi gọi cho bất kỳ chi nhánh ngân hàng nào trong ngày hôm đó, vì tôi đã biết được 2 trong số 5 mã. Nếu gặp một nhân viên ngân hàng nào đó có vẻ dễ tính, tôi sẽ thử dò thêm một mã khác. Đôi khi, tôi thậm chí còn lấy được ba mã số trong một cuộc gọi. (Rất may là các ký tựB, D và E nghe có vẻ na ná nhau.)

Khi gọi tới một chi nhánh và họ hỏi mã A trong khi tôi chỉ có B và E, tôi sẽ nói: “Giờ tôi không ở bàn làm việc. Tôi báo mã B hay E có được không?”

Những cuộc hội thoại này thường rất thân thiện khiến các nhân viên ngân hàng không có lý do gì để nghi ngờ và vì không muốn tỏ ra vô lý quá mức, họ sẽ đồng ý. Nếu không, tôi chỉ đơn giản nói là mình sẽ quay lại bàn làm việc để lấy mã A. Tôi gọi lại sau đó, gặp một một nhân viên khác.

Với Wernle, tôi thử Ngân hàng Mỹ đầu tiên. Mẹo này có tác dụng, nhưng lại không có tên khách hàng nào ứng mã số An sinh của Joseph Wernle. Vậy ngân hàng Wells Fargo thì sao? Dễ hơn một chút: Tôi không cần tới mã bảo

https://thuviensach.vn

mật vì Danny Yelin, một trong những tay thám tử ở Teltec, có bạn làm ở đó. Do các đường dây điện thoại đều bị giám sát, nên Danny và Greg có cách nói chuyện bằng ám hiệu riêng và giờ họ cũng cho tôi biết.

Tôi gọi cho Greg và nói chuyện với anh ta về việc hẹn xem trận bóng vào cuối tuần hay đại loại thế, rồi nói gì đó kiểu như: "Nếu anh muốn tham gia thì gọi cho Kat nhé, cô ấy sẽ kiếm vé cho anh."

"Kat" là ám hiệu. Điều đó đồng nghĩa với việc tôi muốn có mã số của ngày hôm đó. Anh ta sẽ trả lời: "Được, cô ấy vẫn dùng số máy 310 725-1866 chứ hả?"

"Không," tôi đọc cho anh ta một số khác, chỉ để đánh lạc hướng.

Bởi bốn số cuối cùng trong số điện thoại ảo kia chính là mã bí mật trong ngày.

Khi đã có mã, tôi gọi tới một chi nhánh và nói tôi từ chi nhánh xyz nào đó: "Chúng tôi gặp vấn đề với máy tính, máy chạy chậm quá khiến tôi không thế xử lý công việc được. Cô có thể tra giúp tôi được không?"

Để tìm thông tin Wernle, tôi đưa ra mã bảo mật và nói kiểu như: "Tôi cần thông tin tài khoản khách hàng."

"Số tài khoản là gì?"

"Cô tìm bằng mã số An sinh hộ tôi." Và tôi đưa số của Wernle.

Một lúc sau, cô ta đáp: "Tôi thấy có hai tài khoản."

Tôi nhờ cô ta đọc cả hai số tài khoản và số tiền trong đó.

Phần đầu của tài khoản ngân hàng thể hiện chi nhánh lập tài khoản đó; cả hai tài khoản của Wernle đều ở chi nhánh Tarzana tại Thung lũng San Fernando.

https://thuviensach.vn

Một cú điện tới chi nhánh ngân hàng để yêu cầu “sig card” (thẻ chữ ký mẫu) của Wernle đã giúp tôi có được câu trả lời hằng mong đợi cho câu hỏi: “Chủ sở hữu lao động là ai?”

“Alta Services, 18663 Ventura Boulevard.”

Khi gọi tới Alta Services và hỏi thăm Joseph Wernle, đáp lại tôi là câu trả lời lạnh nhạt: “Hôm nay anh ấy không có ở đây.” Có vẻ đáng nghi như thể câu tiếp theo sẽ là “Và chúng tôi cũng không nghĩ anh ấy sẽ ở đây.”

Trong kỷ nguyên “thông tin ngân hàng nằm gọn trong tay bạn”, không khó để có được các thông tin còn lại. Với số tài khoản ngân hàng và bốn số cuối mã An sinh của Wernle, tôi chỉ cần gọi điện cho hệ thống tự động của ngân hàng và lấy được toàn bộ chi tiết giao dịch mình muốn.

Thông tin nhận được khiến cho bí ẩn này càng thêm bí ẩn: Joselp Wernle có nguồn quỹ ra vào tài khoản tới vài nghìn đô-la mỗi tuần.

Ái chà – điều đó nghĩa là sao? Tôi không thể tưởng tượng ra nổi.

Với từng này tiền giao dịch qua tài khoản ngân hàng, hẳn là khoản hoàn thuế của hắn ta sẽ cho tôi vài gợi ý hữu ích về chuyện đang xảy ra.

Tôi biết mình có thể dễ dàng lấy được thông tin thuế từ Cục Thuế Nội địa (IRS) nhờ thực hiện tấn công bằng kỹ thuật xã hội với mấy nhân viên sử dụng máy tính ở đó. Khu tổ hợp IRS ở Fresno, California có tới vài trăm đường dây điện thoại; tôi gọi cho một trong số đó một cách ngẫu nhiên. Nhờ đã tìm hiểu từ trước, tôi sẽ nói kiểu như: “Tôi gặp trục trặc trong việc truy cập vào IDRS – máy của anh/chị có sao không?” (“IDRS” là viết tắt của “Integrated Data Retrieval System” – Hệ thống phục hồi dữ liệu tích hợp”.)

Đương nhiên máy của anh ta hay cô ta vẫn làm việc bình thường và hầu như mọi người đều sẵn lòng giúp đỡ đồng nghiệp.

https://thuviensach.vn

Lần này, khi tôi đưa mã số An sinh của Wernle, nhân viên ở đó nói dữ liệu hoàn thuế trong hai năm gần đây trên hệ thống cho thấy không có nguồn thu nhập nào được ghi lại.

Vậy là đã rõ, ít ra là ở một khía cạnh nào đó. Hồ sơ An sinh của Wernle trước đó đã cho thấy anh ta không có thu nhập nào. Giờ thì dữ liệu từ IRS đã xác thực thông tin này.

Một đặc vụ FBI không đóng tiền An sinh và thuế thu nhập… nhưng lại thường xuyên có hàng nghìn đô-la giao dịch qua tài khoản ngân hàng. Điều đó tức là sao?

Có một câu nói cũ đại loại là: “Những thứ chắc chắn nhất trên đời chính là cái chết và tiền thuế.” Có vẻ như đối với một đặc vụ FBI thì vế thứ hai không còn chính xác.

Tôi cố gọi điện cho Eric và phát hiện ra số điện thoại của hắn không còn liên lạc được nữa. Tôi thử số thứ hai; cũng tương tự.

Tôi sử dụng phương pháp tấn công bằng kỹ thuật xã hội gọi tới văn phòng bất động sản khu Eric ở và được biết hắn đã chuyển đi. Không, hắn không chuyển sang căn hộ khác cùng tổ hợp như lần trước – lần này là chuyển đi hoàn toàn. Người phụ nữ ở văn phòng tra cứu thông tin giúp tôi, nhưng đúng như dự đoán, hắn không để lại bất kỳ địa chỉ nào để liên lạc.

Tôi trở lại Tổ Chuyên trách Đặc biệt của DWP lần nữa. Tuy ít có cơ hội nhưng đây là một xuất phát điểm tốt. Tôi nhờ thư ký tra cứu các dịch vụ mới dưới tên Wernle. Chỉ mất một lúc, cô ta đã trả lời: “Vâng, chúng tôi có tài khoản mới đứng tên Joseph Wernle” và cho tôi địa chỉ ở McCadden Place, Hollywood.

Không thể tin được một cảnh sát liên bang lại có thể ngu ngốc tới mức dùng tên của chính mình để đăng ký tài khoản dịch vụ sinh hoạt cho thân phận mà họ đang cố gắng che giấu.

https://thuviensach.vn

Tôi có số máy nhắn tin của Eric. Số đó vẫn hoạt động và từ đó tôi có thể suy ra công ty tin nhắn nào cung cấp dịch vụ cho hắn. Tôi gọi và lừa tay trực máy nói cho tôi biết một mã số riêng biệt chỉ thuộc về máy của Eric: mã CAP ("Channel Access Protocol" – Giao thức Truy cập Kênh). Sau đó, tôi mua một chiếc máy nhắn tin cùng hãng, nói với nhân viên ở đây rằng tôi làm rơi cái máy cũ xuống toilet khi đi vệ sinh. Anh ta cười tỏ vẻ rất đồng cảm – anh ta cũng từng gặp những người khác gặp tình huống tương tự – và không ngại lập trình cho chiếc máy mới của tôi với mã CAP tôi đưa cho anh ta.

Từ thời điểm đó, bất kỳ ai từ FBI (hay người nào khác) nhắn tin cho Eric, tôi sẽ thấy nội dung tin nhắn hiển thị chính xác trên máy nhắn tin nhái số của tôi.

Còn việc khi tôi nghe lén hai cuộc hội thoại liên tiếp và chúng đều nhắc tới tôi thì sao? Không lâu sau khi nghe được mấy gã ở Phòng An ninh Pacific Bell bàn cách đặt bẫy tôi, tôi lại tiếp tục phải nghe những lời rầy la về mình.

Tôi không thử nghe lén Eric bởi hắn biết chúng tôi có thể truy cập vào SAS và tôi e ngại rằng mấy tay kỹ thuật viên thiết bị có thể đã được yêu cầu gọi ngay tới Phòng An ninh của Pacific Bell hay FBI khi có bất kỳ ai định gắn thiết bị vào đường dây của hắn. Eric nghĩ hắn đã phòng hộ an toàn cho đường điện thoại của mình. Hắn nghịch SAS đủ nhiều để biết rằng bạn có thể nghe được tiếng click đặc trưng khi ai đó định dùng nó nghe lén đường dây của bạn. Nhưng hắn không biết rằng việc tạo kết nối với giày SAS, như tôi đã giải thích, là kết nối trực tiếp, sử dụng chính cáp mà kỹ thuật viên thiết bị đặt trực tiếp trên đường dây của khách hàng và do đó, nó sẽ không tạo ra tiếng click nghe được trên điện thoại.

Rất tình cờ một ngày nọ, tôi đã kết nối được vào đường dây của Eric nhờ dùng giày SAS và nghe được cuộc hội thoại của hắn ta với một người tên là "Ken".

https://thuviensach.vn

Tôi cũng không buồn thắc mắc Ken là ai: Chính là đặc vụ đặc biệt của FBI, Ken McGuire.

Họ nói chuyện về chứng cứ cần thiết để Ken có thể có lệnh khám xét Mitnick.

Cuộc gọi khiến tôi hoảng loạn thực sự. Tôi tự hỏi liệu họ có đang theo dõi tôi hay thậm chí là chuẩn bị bắt tôi hay không. Eric không có vẻ giống một người đưa tin mật; thay vào đó, kiểu nói chuyện của hắn với McGuire "Ken" nghe như hai đặc vụ nói chuyện với nhau. Như thể McGuire, một đặc vụ già hơn, có kinh nghiệm hơn, đang hướng dẫn một đặc vụ trẻ về những gì họ cần để có lệnh khám xét.

Lệnh khám xét! Bằng chứng chống lại Mitnick!

Khỉ thật, tôi nghĩ. Lại một lần nữa tôi cần phải loại bỏ từng mẩu nhỏ chứng cứ có thể được dùng để chống lại mình.

Ngay khi họ dập máy, tôi tái lập trình điện thoại của mình ngay lập tức, nhái nó sang một số điện thoại khác, một số tôi chưa từng dùng trước đó.

Sau đó, tôi gọi cho Lewis đang ở chỗ làm việc. "Có việc khẩn cấp đây!" tôi nói với anh ta. "Cậu phải ra bốt điện thoại công cộng bên ngoài tòa nhà ngay lập tức" – để phòng ngừa trường hợp cảnh sát liên bang đang theo dõi cả đường truyền điện thoại di động gần nơi làm việc của anh ta.

Tôi lao ra xe, lái tới một nơi mà tôi biết có rất nhiều bốt điện thoại công cộng – một lần nữa, để phòng trường hợp các đặc vụ giám sát cả bốt gọi quanh khu vực của Teltec.

Ngay khi Lewis trả lời điện thoại, tôi nói với cậu ta: "Chính phủ đã lập án chống lại chúng ta rồi, Eric là một thành viên trong đó! Chắc chắn 100% rằng chúng ta là mục tiêu. Hãy thay số điện thoại của cậu ngay lập tức."

https://thuviensach.vn

“Ôi, khốn kiếp!” Đó là tất cả những gì anh ta có thể nói.

“Chúng ta phải hủy hết dữ liệu,” tôi nói.

Lewis nghe có vẻ chán nản và sợ hãi. “Ừ, được rồi,” anh ta nói. “Tớ biết phải làm gì rồi.”

Trong suốt thời gian cố gắng tìm hiểu về Eric, tôi đoán rằng mình sẽ tìm ra hắn là một kẻ chỉ điểm của FBI, nếu không phải là một đặc vụ. Nhưng giờ thì chắc chắn, đây không còn là một trò chơi nữa. Đây là đời thực. Tôi gần như có thể cảm nhận được độ lạnh của chấn song nhà tù. Tôi cũng có thể cảm nhận được vị nhạt nhẽo khó nuốt của đồ ăn của trại giam trong miệng.

Tôi đợi trước cửa nhà Kasden khi ông ta đi làm về, với đống thùng chứa đầy những đĩa mềm tôi nhờ giữ hộ. Cùng tối hôm đó, tôi lái xe tới nhà một người bạn khác của cha, người đã đồng ý cho tôi đặt máy tính và các ghi chép ở nhà ông ấy.

Hủy tài liệu ở chỗ Lewis không dễ gì. Cậu ta hệt như một con chuột, với cả đống bừa bộn chất đầy trong căn hộ. Đào bới hàng chồng đồ đạc để tìm ra các dữ liệu có thể được dùng để lập án chống lại cậu ta là cả một thử thách lớn. Và đây không phải là việc ai đó có thể hỗ trợ: Cậu ta là người duy nhất biết đĩa cứng và đĩa mềm nào an toàn cũng như cái nào có thể tống mình vào tù. Nhiệm vụ này khiến cậu ta phải mất tới mấy ngày, thời gian như áp lực nặng nề đè lên vai cậu ta, liệu điều gì sẽ xảy ra nếu cảnh sát liên bang xuất hiện trước khi cậu ta kịp hoàn thành.

Tôi biết đáng lẽ ra mình nên tận dụng mọi nguồn thông tin có được để tìm hiểu về Eric trước khi chuyện này xảy ra. Nhưng muộn còn hơn không. Tôi gọi cho Ann, người tôi thường liên lạc ở SSA. Cô ấy tra tên Eric Heinz và cho tôi mã số An sinh, nơi sinh và ngày tháng năm sinh của hắn. Ann nói với tôi rằng hắn thuộc nhóm nhận trợ cấp thương tật vì mất một chân.

https://thuviensach.vn

Tôi nói với Ann: “Đây là một trường hợp giả mạo. Để xem chúng ta có thể tìm thấy tên bố mẹ hắn không.” Bằng lái xe của Eric cho thấy tên hắn có chữ Junior, điều này giúp việc tìm kiếm dễ hơn rất nhiều. Ann tra trong danh sách tất cả những người có tên Eric Heinz Sr. với năm sinh trong khoảng phù hợp với bố của Eric. Cô ấy tìm thấy một người sinh vào ngày 20 tháng 6 năm 1935.

Tối hôm đó, tôi và Danny Yelin, một đồng nghiệp ở Teltec hẹn nhau cùng ăn tối tại Solley, một quán ăn khá ngon ở Sherman Oaks. Sau khi gọi món, tôi ra trạm điện thoại công cộng và gọi vào số điện thoại tìm được dưới tên Eric Heinz Sr.

Điều xảy ra tiếp theo có lẽ sẽ không khiến tôi bất ngờ, nhưng sự thật là có.

“Cháu định liên lạc với Eric,” tôi nói. “Cháu là bạn học cấp ba cùng cậu ấy.”

“Ai thế?” người đàn ông hỏi, giọng đầy nghi ngờ. “Tên cậu là gì?”

“Có khi cháu gọi nhầm. Ở đây có ai là Eric Jr. không ạ?”

“Con tôi qua đời rồi,” ông ta nói.

Người đàn ông có vẻ khó chịu, dường như cố kìm nén cơn giận dữ. Ông ta nói ông ta muốn biết số điện thoại của tôi để gọi lại – rõ ràng là muốn trình báo tôi với những người có thẩm quyền. Không vấn đề gì: Tôi cho ông ta số điện thoại công cộng ở cửa hàng bán thức ăn và dập máy.

Ông ta gọi lại ngay lập tức. Chúng tôi bắt đầu vờn nhau, tôi thì cố kéo ông ta lại phía mình, còn ông ta thì cố gắng giữ khoảng cách.

Tôi hỏi: “Cậu ấy mất từ khi nào thế ạ?”

Câu trả lời là: “Con trai tôi mất từ khi còn rất nhỏ.”

https://thuviensach.vn

Tôi cảm thấy adrenaline tuôn trào trong người. Lời giải thích rõ rành rành: “Eric Heinz” là danh tính ăn trộm.

Bằng cách nào đó, tôi cố gắng bình tĩnh để lảm nhảm điều gì đó như là rất tiếc vì nỗi đau mất mát này qua điện thoại.

Vậy hắn ta thực sự là ai, gã nghệ sĩ một chân chết tiệt làm việc cùng FBI và dùng tên giả này?

Lúc này, tôi cảm thấy cần phải thỏa mãn với lời giải thích của Eric Heinz Sr. rằng con trai ông ta đã chết từ khi còn rất nhỏ. Lại một lần nữa, với sự giúp đỡ của cô bạn Ann ở Phòng Quản lý An sinh, tôi tra theo địa chỉ anh trai của Eric Cha và nhận được lời xác nhận: Eric Con đã chết trong một tai nạn giao thông năm 1962 khi mới hai tuổi, trên đường tới hội chợ Settle World cùng mẹ mình, người cũng qua đời trong vụ đụng xe.

Đấy là lý do mà Eric Cha rất lạnh nhạt khi tôi nói con trai ông ta và tôi cùng học cấp ba.

Theo suốt câu chuyện cho đến khi nó kết thúc đem tới một kiểu thỏa mãn riêng. Trong trường hợp này thì điều đó có nghĩa là tôi phải có được bản sao giấy chứng tử của Eric Heinz từ Cục Thống kê Dân số ở Quận King, Seattle. Tôi gửi yêu cầu, kèm theo khoản phí yêu cầu và đề nghị nó được gửi tới hòm thư của tôi ở Teltec.

Bố và bác của Eric Heinz đã nói sự thật. Còn “Eric Heinz” mà tôi biết chỉ đang chơi trò đánh cắp danh tính của trẻ em.

Oa! Cuối cùng, tôi đã vén được bức màn bí mật về hắn ta.

Tên “Eric Heinz” là hoàn toàn giả mạo.

Vậy cái gã chết tiệt này là ai, một gã khốn đã chết nhưng vẫn cố đặt bẫy tôi?

https://thuviensach.vn

Quay lại với bản phân tích lưu lượng về các cuộc gọi di động của FBI, tôi nhận thấy McGuire thực hiện rất nhiều cuộc gọi tới số 213 894-0336. Tôi biết rằng 213 894 là mã vùng và mã tổng đài của điện thoại ở Văn phòng Luật sư ở Los Angeles. Tôi gọi tới số đó và biết được đây là số điện thoại của David Schindler, trợ lý công tố, luật sư công tố trong vụ của Poulsen. Hắn hẳn phải là người được giao nhiệm vụ phụ trách vụ hacker lớn kế tiếp của Los Angeles.

Như vậy là chính phủ đã có cả công tố viên cho vụ của tôi. Không ổn rồi!

Từ lần đầu tiên chiếm quyền đăng nhập vào hồ sơ chi tiết cuộc gọi của PacTel Cellular và thấy được danh sách chi tiết cập nhật về các cuộc gọi đến và đi từ tất cả thuê bao của công ty, tôi vẫn thường kiểm tra nó – đối tượng là những người trong tổ tội phạm cổ cồn trắng thường liên lạc với Eric, đặc biệt là đặc vụ đặc biệt McGuire.

Nhờ đó, tôi phát hiện ra một chuỗi các cuộc gọi đáng-chú-ý: Trong vài phút, McGuire đã gọi tới máy nhắn tin của Eric vài lần. Và cuộc gọi tiếp theo của McGuire sau lần nhấc máy cuối cùng là tới một số điện thoại tôi chưa từng nhìn thấy.

Tôi gọi tới số này. A ha – giọng trả lời rất quen thuộc. Người nhấc máy là Eric. Với số điện thoại mới, ở khu vực khác của Los Angeles. Hắn đã chuyển nhà một lần nữa.

Tôi dập máy, cười sung sướng. Eric hẳn sẽ biết cuộc gọi dập máy này là của tôi. Có lẽ tôi đã phát hiện ra hắn chuyển nhà trước cả khi hắn kịp dỡ đồ đạc.

Trung tâm phân bổ đường dây của Pacific Bell có lẽ là nơi có thể moi được địa chỉ mới của Eric.

Nơi ở mới của hắn nằm ở số 2280 Đại lộ Laurel Canyon, một khu dân cư đắt đỏ cách phía bắc Đại lộ Hollywood ở Hollywoods Hills khoảng 1,5km, bằng nửa đường tới Mullholland Drive.

https://thuviensach.vn

Đây là địa chỉ thứ tư trong vòng vài tháng kể từ khi tôi quen biết Eric. Không khó để hiểu lý do: FBI đang cố bảo vệ hắn. Mỗi lần tôi lần ra địa chỉ, họ sẽ chuyển hắn tới nơi ở mới. Ba lần tôi tìm ra địa chỉ, cả ba lần họ đều đưa hắn đi.

Lúc này, họ hắn đã hiểu ra nơi ở của Eric không phải là bí mật mà họ có thể giữ kín đối với tôi.

Ban đêm, tôi ngồi trước máy tính được đặt ở một nơi an toàn dành cho hacking, ban ngày tôi ngồi trước máy tính của Teltec để làm công việc "điều tra". Nhiệm vụ ở Teltec chủ yếu xoay quanh các dự án kiểu như tìm hiểu xem người chồng trong một vụ ly hôn sẽ giấu tài sản của anh ta ở đâu, giúp luật sư quyết định xem liệu một vụ kiện có đáng để đệ đơn hay không nhờ tìm hiểu tình hình tài chính của bị cáo, hay như truy tìm mấy kẻ vô công rỗi nghề. Có một vài trường hợp khá gây hứng thú, ví như định vị một người cha/mẹ nào đó bắt cóc chính con mình và bay tới Canada, châu Âu, v.v…. Thành công trong những vụ kiểu này khiến tôi vô cùng hài lòng và cảm thấy mình đã làm được điều gì đó tốt đẹp cho thế giới.

Nhưng làm việc tốt cho xã hội không có nghĩa là tôi sẽ ghi điểm với các cơ quan hành pháp. Tôi tìm ra cách thiết lập một hệ thống cảnh báo sớm sẽ reo chuông nếu cảnh sát liên bang lượn lờ xung quanh để theo dõi tôi khi tan sở. Tôi mua một chiếc máy quét sóng RadioShack đã bỏ giới hạn tần số. (Dạo ấy, FCC bắt đầu yêu cầu các nhà sản xuất máy quét phải thêm tính năng hạn chế nhằm ngăn chặn việc nghe lén điện thoại di động). Tôi mua thêm một thiết bị gọi là "máy phiên dịch dữ liệu kỹ thuật số" (Digital-Data Interpreter – DDI) – một chiếc hộp đặc biệt có thể giải mã các thông tin tín hiệu trên mạng điện thoại di động. Tín hiệu từ máy quét dẫn vào DDI vốn đã kết nối với máy tính của tôi.

Thông thường, một chiếc điện thoại di động sẽ đăng ký và thiết lập kết nối với trạm thu phát gần nhất, nhờ vậy, khi có cuộc gọi tới, hệ thống tổng đài sẽ biết được nên chuyển tiếp cuộc gọi tới trạm gốc nào để đi tới điện thoại của

https://thuviensach.vn

bạn. Nếu không sắp đặt như vậy, các nhà mạng sẽ không có cách nào để định hướng cuộc gọi không dây tới cho bạn. Tôi lập trình máy quét để giám sát tần số của trạm thu phát gần nhất quanh Teltec, nhờ đó, nó có thể thu được dữ liệu từ trạm, xác định được số điện thoại của bất kỳ chiếc điện thoại di động nào trong khu vực hoặc thậm chí là các máy di động chỉ đi ngang qua khu vực đó.

Tất cả các dữ liệu này không ngừng được chuyển tới DDI từ máy quét của tôi, sau đó lại được DDI chuyển đổi thành các phần tách biệt dạng như:

618-1000 (213) Registration

610-2902 (714) Paging

400-8172 (818) Paging

701-1223 (310) Registration

Từng dòng dữ liệu cho thấy tình trạng của điện thoại di động hiện có trong khu vực do trạm thu phát xử lý; cụm chữ số đầu tiên là số điện thoại của một máy di động nào đó. “Paging” có nghĩa là trạm đang nhận cuộc gọi cho máy và báo hiệu máy thiết lập kết nối. “Registration” chỉ ra rằng điện thoại đang ở trong khu vực trạm thu phát này và đã sẵn sàng để thực hiện cuộc gọi đi hoặc nhận cuộc gọi tới.

Tôi thiết lập cấu hình cho phần mềm DDI trên máy tính của mình để nó reo chuông báo nếu DDI phát hiện ra bất kỳ số điện thoại nào trong danh sách các số tôi đã lập trình sẵn trong phần mềm: Số điện thoại di động của tất cả đặc vụ FBI mà tôi xác định được là có liên lạc với Eric. Phần mềm liên tục quét các số điện thoại được gửi dữ liệu trên máy quét, đến DDI và đến máy tính của tôi. Nếu bất kỳ máy di động của cảnh sát liên bang nào xuất hiện trong khu vực quanh Teltec, hệ thống của tôi sẽ reo chuông báo.

https://thuviensach.vn

Tôi đã cài bẫy FBI, giúp tôi đi trước họ một bước. Nếu cảnh sát liên bang xuất hiện, tôi sẽ được cảnh báo.

https://thuviensach.vn

23
BỊ VÂY BẮT

Fqjc nunlcaxwrl mnerln mrm cqn OKR rwcnwcrxwjuuh kanjt fqnw cqnh bnjalqnm vh jyjacvnwc rw Ljujkjbjb?

Vào một ngày thứ Hai cuối tháng 9 năm 1992, tôi là người đến chỗ làm sớm nhất. Khi đi dọc hành lang, tôi bắt đầu nghe thấy tiếng bíp, bíp, bíp nhỏ. Tôi nghĩ hẳn là mình đã ấn nhầm mã báo động để vào văn phòng Teltec. Nhưng càng đi sâu vào hành lang, tiếng bíp càng to hơn.

Bíp-bíp, bíp-bíp, bíp-bíp . . .

Tiếng bíp phát ra từ văn phòng của tôi.

Ai đó đã nhét một chiếc đồng hồ báo thức vào bàn tôi chăng?

Không. Đó là một thứ khác.

Hệ thống cảnh báo sớm của tôi.

Tiếng bíp được kích hoạt bởi gói phần mềm theo dõi máy quét của tôi.

Máy quét đang bắt được điện thoại di động của FBI trong khu vực.

Chết tiệt!

Máy tính hiện ra số điện thoại di động đã kích hoạt cảnh báo: 213 500-6418

Điện thoại di động của Ken McGuire.

https://thuviensach.vn

Phần mềm DDI trên máy tính cho thấy cảnh báo đã được kích hoạt lúc 6 giờ 36 phút sáng, tức là từ vài tiếng trước.

McGuire đã ở khu vực này, đâu đó gần Teltec.

Máy tính của tôi cũng đang hiện các số mà McGuire đã gọi: 818 880-9XXX. Vào thời đó, ở Los Angeles, số "9" ở vị trí đó trong số điện thoại thường có nghĩa là máy điện thoại công cộng. McGuire đã gọi tới một máy điện thoại công cộng trong khu vực của tôi.

Giây lát sau, tôi bừng tỉnh và xác nhận nỗi sợ lớn nhất: McGuire đã gọi đến máy điện thoại công cộng gần Village Market, một cửa hàng tiện lợi ngay đối diện bên kia căn hộ của tôi.

Chỗ đó chỉ cách Teltec vài cây số, chưa đến năm phút lái xe.

Hàng nghìn thứ cứ lướt qua đầu tôi. Tại sao họ lại ở đây? Họ đang bài binh bố trận để theo dõi tôi, hay họ theo tôi đến đây để bắt tôi? Tôi có nên chạy không? Trốn đi hay ngồi và đợi họ đến phá cửa xông vào?

Tôi rùng mình. Sợ hãi. Hoảng loạn.

Đợi đã. Nếu họ đến đây để bắt tôi, họ sẽ phải gõ cửa khi tôi vẫn đang ở trong nhà.

Tại sao McGuire lại gọi đến Village Market? Bỗng nhiên, câu trả lời trở nên rõ ràng: Để có lệnh khám xét, họ cần một bản mô tả khu chung cư của tôi và địa chỉ chính xác phòng tôi. Có thể McGuire chưa sẵn sàng bắt tôi – ông ta chỉ đang lấy thông tin chi tiết về địa điểm mà ông ta cần để bổ sung tờ lệnh khám trước khi trình nó cho thẩm phán.

Michael và Mark đều đã đến chỗ làm. Tôi cho họ biết tin: "Ken McGuire đã đến căn hộ của tôi sáng nay, trong khi tôi vẫn đang ngủ." Vẻ mặt của họ thật vô giá: "Thế quái nào mà gã này luôn biết những chuyện đó vậy?!" Từ đầu

https://thuviensach.vn

đến cuối, họ bị mê hoặc bởi những câu chuyện của tôi, về việc tôi đã thâm nhập vào toàn bộ chiến dịch chống lại chính mình của FBI ra sao. Họ đã nuốt lấy từng lời và đây là cú hạ màn.

Tôi thu dọn tất cả đồ đạc cá nhân và đi xuống cầu thang ra xe, hoảng loạn và khó chịu, sợ phải nghe thấy ai đó hét lên: "Mitnick, ĐỨNG IM!" bất cứ lúc nào. Trong bãi đỗ xe, tôi chủ ý liếc từng chiếc xe xem có gã nào mặc vest đang theo dõi mình hay không.

Khi cẩn thận lùi xe ra khỏi ga-ra, tôi không thể rời mặt khỏi tấm gương chiếu hậu. Tôi tập trung vào những gì có thể xảy ra ở phía sau hơn là phía trước.

Tôi phi vào cao tốc 101 và phóng đến Aguora Hills, cách đó một thành phố, đủ xa để tôi có thể thoải mái dùng điện thoại di động của mình.

Ra khỏi cao tốc, tôi tấp xe vào bãi đỗ của một nhà hàng McDonald's.

Rất tự nhiên, tôi nhấc máy gọi cho Lewis trước tiên. "FBI đang đến," tôi bảo anh ta.

Hầu hết chẳng có chuyện gì có thể làm Lewis lung lay. Thật hiếm khi thấy dáng vẻ ngạo mạn đó bị đánh gục.

Nhưng lần này thì không. Tôi có thể nghe thấy tin tức này khiến anh ta khó chịu và lo lắng. Nếu FBI đang nhắm vào tôi, họ phải biết anh ta cũng tham gia vào những vụ hack của tôi. Gần như chắc chắn, họ tuyệt đối sẽ không chỉ muốn một mình Mitnick.

Tôi quay trở lại căn hộ của mình và dò xét kỹ càng, từng xentimet một, thu dọn mọi thứ tôi đã tích lũy từ lần dọn dẹp trước, những thứ có thể làm chứng chống lại tôi. Giấy, đĩa, mảnh vụn của bất cứ thứ gì có chữ viết trên đó và làm điều tương tự với xe của tôi.

https://thuviensach.vn

Tối hôm đó, tôi gõ cửa nhà Mark Kasden và hỏi xem liệu tôi có thể cất đồ trong tủ của ông ta cùng đống đồ đã để lại chỗ ông ta lần trước không.

Tôi trở lại căn hộ của mình và chuyển máy tính đến chỗ bạn của cha một lần nữa, chỗ tôi đã giấu nó lần trước. Khi xong việc, tôi thấy hài lòng vì đã xóa sạch dấu vết.

Tôi thuê một phòng tại nhà nghỉ nhỏ ngay cuối đường vì không dám ngủ tại nhà mình. Tôi ngủ không ngon và dậy sớm, cứ trở người và cựa quậy.

Sáng thứ Ba, tôi lái xe đến chỗ làm, cảm giác mình giống như một nhân vật trong một bộ phim điệp viên dở tệ: Có trực thăng không? Còn xe Crown Victorias thì sao? Mấy gã khả nghi mặc vest cắt tóc ngắn đâu?

Không gì cả.

Tôi cảm thấy mọi chuyện có thể đến bất cứ lúc nào.

Nhưng ngày hôm đó lại trôi qua trong bình lặng. Tôi thậm chí còn thu xếp giải quyết được một số công việc.

Lái xe về nhà, tôi dừng lại ở một tiệm bánh vòng và mua hơn chục loại.

Trên cửa tủ lạnh, tôi dán băng dính ghi: “Bánh vòng của FBI”.

Trên hộp, tôi viết to:

BÁNH VÒNG CỦA FBI

Tôi hy vọng họ sẽ thực sự phát điên lên khi tôi không chỉ biết mình sẽ bị khám xét, mà còn biết chính xác khi nào.

* * *

Sáng hôm sau, ngày 30 tháng 9 năm 1992, tôi về lại căn hộ của mình, ngủ chập chờn, cảm giác lo lắng và bồn chồn, không lúc nào thực sự ngủ sâu.

https://thuviensach.vn

Khoảng 6 giờ sáng, tôi bị đánh thức dậy. Ai đó đang day chìa khóa cửa căn hộ của tôi. Tôi đang đợi FBI, nhưng họ sẽ không dùng chìa, họ đập cửa. Ai đó đang cố đột nhập vào nhà tôi ư? Tôi hét lên: "Ai đó?", hy vọng sẽ dọa được lũ đột nhập kia đi.

"FBI đây – mở cửa ra!"

Tôi thầm nghĩ: Đây rồi. Mình sẽ trở lại nhà tù.

Dù biết họ sẽ đến, nhưng tôi vẫn chưa chuẩn bị về mặt tinh thần. Sao tôi có thể làm thế được? Tôi còn đang sợ bị bắt chết khiếp đây này.

Tôi mở cửa, thậm chí không hề nhận ra mình đang hoàn toàn khỏa thân. Đi đầu là một nữ đặc vụ, người còn không thể kiềm chế liếc nhìn xuống.

Rồi cả đội lao xộc vào phòng. Họ xáo tung căn hộ lên trong khi tôi mặc đồ, thậm chí khám xét cả đồ trong tủ lạnh. Không ai bình luận gì hay bật cười trước tấm bảng "Bánh vòng của FBI", cả chục cái bánh đều không có ai đụng vào.

Nhưng tôi đã dọn dẹp sạch sẽ. Họ không tìm thấy thứ gì có thể buộc tội tôi từ tủ lạnh và họ cũng không thấy bất cứ thứ gì ở những chỗ khác có thể giúp cho vụ án.

Tất nhiên, họ không thích điều này và họ cũng không thích thái độ ngây thơ, giả ngu của tôi.

Một đặc vụ khác ngồi xuống bàn bếp và nói: "Hãy lại đây, nói chuyện nào." Các đặc vụ FBI thường rất lịch sự, gã này và tôi biết nhau. Hắn là đặc vụ Richard Beasley, người đã tham gia vụ DEC của tôi. Hắn nói bằng một giọng thân thiện và lè nhè kiểu Texas: "Kevin, đây là lần thứ hai của cậu. Ngay lúc này, chúng tôi đang khám xét nhà De Payne. Anh ta rất hợp tác. Trừ khi cậu hợp tác, nếu không cậu sẽ ngồi sau xe áp giải đấy."

https://thuviensach.vn

Tôi chưa từng thấy điều này trước đây, nhưng ý nghĩa thì đã rõ: Người đầu tiên phản bội người còn lại sẽ nhận được thỏa hiệp tốt hơn rất nhiều. Lewis và tôi đã nói về chuyện này rất nhiều lần. “Cậu sẽ làm gì nếu cảnh sát hỏi cung?” một trong hai chúng tôi hỏi người còn lại.

Câu trả lời luôn là: “Hãy bảo họ nói chuyện với luật sư của tôi.”

Tôi sẽ không phản bội anh ta và tôi biết anh ta cũng sẽ là người đứng về phía tôi.

* * *

Beasley lôi ra một cuộn băng cát-sét. Hắn hỏi tôi: “Cậu có máy chạy băng cát-sét không?”

“Không!”

Tôi không thể hiểu được chuyện này. FBI thích nghĩ họ là cơ quan hành pháp xuất sắc nhất nước Mỹ, nếu không muốn nói là toàn cầu, họ mang theo một cuộn băng muốn tôi nghe nhưng lại không có ai nghĩ đến chuyện mang theo máy đọc băng?

Một đặc vụ nhìn thấy máy boom box[65] lớn của tôi và mang nó ra. Beasley cho băng vào và ấn nút Play.

[65] Máy boom box: Máy nghe nhạc CD và nghe radio cỡ lớn có thể mang theo bên người. (BTV)

Tôi nghe thấy một cuộc gọi được quay số và Mark Kasden đang nói phía sau. Rồi có giọng tôi. Nghe như Mark và tôi đang nói chuyện trong phòng. Tôi có thể nghe thấy tiếng chuông sau khi các số được quay.

Sau đó, boom box phát ra giọng nói đại loại như: “Chào mừng bạn đến với hộp thư thoại của Pacific Bell. Xin hãy nhập số hộp thư thoại của bạn.” Có thêm vài số được quay.

https://thuviensach.vn

“Xin hãy nhập mật khẩu.”

“Bạn có ba tin nhắn mới.”

Và rồi, “Xin chào Darrell, David Simon đây. Xin hãy gọi cho tôi theo số 818 783-42XX.”

Rồi một cuộc gọi nữa. Lại là giọng tôi: “Này, thám tử Simon vừa gọi cho Santos.” Beasley tắt máy chạy băng.

“Anh có gì để nói không?” hắn thách thức.

Tôi e là mình đã cười nhạo hắn. “Những gì FBI có thể làm với công nghệ thật kỳ diệu.”

Tôi nói một cách ngạo mạn, nhìn thẳng vào mắt hắn.

Một đặc vụ khác đã đứng cạnh chúng tôi suốt cả cuộc nói chuyện liền với tay qua, lấy chiếc boom box và giật mạnh cửa băng cat-xét. Hệt như một đứa trẻ bốn tuổi nổi cơn thịnh nộ vậy.

Các đặc vụ tỏa ra tìm kiếm. Tôi ngồi ở bàn quan sát.

Một đặc vụ khác tiến đến. Anh ta đưa tôi tấm thẻ, có ghi: Đặc vụ giám sát.” Anh ta mở một cuốn sổ tờ rời mang theo và bắt đầu ghi chú. Sau một hồi, anh ta nhìn lên và hỏi: “Máy tính của anh ta đâu?” “Chúng tôi không tìm thấy cái nào,” họ nói. Trông anh ta rất điên tiết.

Họ tiếp tục tìm kiếm.

Cuối cùng, tôi hỏi tay đặc vụ kia: “Tôi có bị bắt giam không?” “Không,” anh ta nói.

Cái gì?!?!?! Không bị bắt?! Tôi không thể tin được. Thật vô lý. Nhưng anh ta không trêu tôi. Không có đặc vụ nào tỏ ý như vậy. Chắc là đúng rồi. Phải

https://thuviensach.vn

thử xem sao.

“Nếu không bị bắt giam thì tôi đi đây,” tôi nói.

“Đi đâu?” tay đặc vụ giám sát hỏi.

“Đến chỗ cha tôi để hỏi ông ấy xem tôi có nên hợp tác không.” Hợp tác – tất nhiên rồi. Nhưng đó là những gì tôi cần nói để ra khỏi đây, đến nơi tôi có thể cảm thấy dễ chịu.

Tay đặc vụ suy nghĩ một lúc. Nếu tôi không bị bắt giam, họ sẽ chẳng có lý do gì để bắt tôi ở đây chứng kiến họ lục soát căn hộ của mình?

“Được rồi,” anh ta nói.

Họ lục soát người tôi, tìm thấy ví và khám xét nó, nhưng không thấy gì thú vị bên trong. Và họ cho tôi đi.

Ba đặc vụ theo tôi ra tận xe. Sau khi tôi mở cửa, họ bắt đầu lục soát. Chết tiệt! – họ tìm thấy một hộp đĩa mềm mà tôi đã bỏ qua trong ngăn để găng tay. Tôi nao núng và lo lắng. Họ vui sướng.

Khám xét xe tôi xong, họ mở cửa xe và chui vào, ngồi đó như thể chúng tôi là những người bạn thân thiết chuẩn bị đi ra ngoài với nhau. Tôi choáng váng.

Tôi nói: “Các anh đang làm gì trong xe tôi vậy?!”

“Chúng tôi sẽ đi với anh đến chỗ của cha anh.”

“Không, các anh không được phép. Đi ra khỏi xe tôi ngay!” Và các bạn biết gì không? Họ chui ra thật.

Họ ngồi vào hai chiếc xe FBI và theo đuôi khi tôi lái xe đến chỗ cha tôi đang sống với bạn gái mới mà tôi không ưa lắm.

https://thuviensach.vn

Khi tôi đến nơi, họ nói họ muốn vào cùng tôi. Tôi bảo họ rằng họ không thể, rằng tôi muốn nói chuyện với ông một mình.

Họ không rời đi, chỉ chui vào xe và ngồi đó trong khi tôi vào nhà.

Tôi chưa dọn dẹp xong ở Teltec và vẫn cần quay lại đó mà không có đội theo dõi của FBI. Khi tôi nhìn ra ngoài, họ vẫn ngồi đó. Tôi ra ngoài và nói với họ rằng cha tôi và tôi đã quyết định rằng tôi sẽ tham khảo ý kiến của luật sư trước khi nói chuyện với họ. Tôi đang cố cho họ một tia hy vọng rằng tôi sẽ hợp tác, dù tôi không hề có ý định làm việc đó.

Cuối cùng, họ cũng rời đi.

Ngay khi họ rời khỏi tầm mắt tôi, tôi nhảy lên xe và phóng nhanh đến Teltec.

Tại sao tôi không gặp được đặc vụ Ken McGuirce hay Terry Atchley của Pacific Bell vào cái ngày định mệnh đó? Bởi họ đã đến chỗ Lewis De Payne, hy vọng sẽ khiến cậu ta lật lọng, khai ra tôi.

Chính xác thì Lewis đã đề nghị làm việc đó. Tôi đã đọc báo cáo của FBI về cuộc trò chuyện: Lewis liên tục đề nghị khai, nhưng cũng liên tục đòi hỏi bảo đảm. Cậu ta liên tục nói rằng tôi rất nguy hiểm và cậu ta rất sợ tôi.

Vậy là tôi đã không bị bắt giam và tôi biết các đặc vụ sẽ không tìm thấy gì có thể buộc tội tôi trong căn hộ. Tôi đoán họ đang tìm kiếm những thứ nghiêm túc hơn là vào hùa với Lewis để buộc tội tôi.

Khi đó, tôi vẫn chưa biết Teltec đã bị khám xét vài tháng trước đó, nên tôi không có lý do gì để nghĩ FBI có thể đang xới tung căn hộ của Kasden cùng lúc họ tìm kiếm căn hộ của tôi. Nhưng đó chính xác là những gì họ đã làm, rõ ràng họ đã đoán được việc hack của tôi có thể liên quan gì đó đến những hành động phi pháp ở Teltec – truy cập TRW với thông tin đánh cắp được

https://thuviensach.vn

của doanh nghiệp, v.v... Vậy là quá đủ cho ý tưởng lợi hại của tôi rằng tôi có thể an tâm nhét đống đĩa và ghi chép ở chỗ của Mark.

Nhưng thời gian đang ủng hộ tôi. Lệnh quản chế từ lần kết án vụ tôi hack vào DEC với Lenny DiCicco của tôi sẽ hết hạn trong chưa đầy ba tháng. Nếu FBI không đến với một lệnh bắt vào thời điểm đó, tôi sẽ bình an vô sự.

Máy tính tôi dùng ở Teltec không có bất cứ công cụ mã hóa nào trên đó và tôi phải chắc chắn các đặc vụ không tìm thấy thêm gì về tôi.

Tôi tấp vào Teltec và chạy nhanh lên cầu thang. Tuyệt vời – không có đội cảnh sát liên bang nào ở chỗ làm. Thật không thể tin được!

Tôi ngồi xuống máy tính trong văn phòng và gõ lệnh xóa tất cả dữ liệu. Trong trường hợp bạn chưa biết (việc này thỉnh thoảng lại lên báo, có lẽ đáng kể nhất là khi nỗ lực che giấu vụ Iran-Contra của nhân viên Nhà Trắng, Trung úy Hải quân Oliver North bị đổ bể), chỉ gõ lệnh “Delete” sẽ không thể thực sự xóa dữ liệu từ ổ cứng máy tính. Thay vào đó, nó chỉ thay tên của mỗi tập tin để đánh dấu rằng nó đã bị xóa; các tập tin này sẽ không còn hiện lên khi tìm kiếm, nhưng chúng vẫn được lưu trên ổ đĩa và có thể được khôi phục.

Vì vậy, thay vì chỉ đơn giản gõ lệnh Delete, tôi sẽ dùng một chương trình có tên là “WipeInfo”, một tính năng trong gói phần mềm Norton Utilities. WipeInfo được thiết kế để không chỉ đánh dấu các tập tin đã xóa mà còn ghi đè lên chúng nhiều lần để chúng không còn có thể khôi phục được. Khi chương trình kết thúc, cảnh sát sẽ không cách nào có thể khôi phục được thông tin từ ổ cứng của tôi.

Tôi gọi cho vị sếp ở Teltec, Michael Grant, và nói với anh ta về vụ khám xét. Anh ta muốn biết: “Giờ cậu đang ở đâu?”

“Tôi đang ở văn phòng.”

https://thuviensach.vn

“Cậu đang làm gì vậy?”

“Dọn sạch máy tính của tôi.”

Anh ta phẫn nộ và cố bảo tôi dừng lại. Thật không thể tin được. Tôi đã nghĩ chúng tôi là một đội; tôi đã nghĩ anh ta và cha mình sẽ đứng về phía tôi. Thay vào đó, anh ta lại cố thuyết phục tôi để lại bằng chứng trên máy tính của mình. Có vẻ các sếp ở Teltec đang hy vọng có thể luồn lách qua được mớ rắc rối họ đang gặp phải bằng cách giúp Cục tạo nên một vụ chống lại tôi.

Trên thực tế, một trong số các cộng sự của tôi ở Teltec – một điều tra viên khác, người đã trở thành bạn tôi – sau này xác nhận với tôi rằng đó chính xác là những gì Michael Grant đã cố làm ngay sau đó: Anh ta thỏa thuận với FBI hãy nhẹ tay với hai cha con họ để đổi lấy lời khai làm chứng chống lại tôi.

Tôi đã buồn và thất vọng khi nghi ngờ của tôi được xác nhận. Tôi đã nghĩ Michael Grant là bạn mình. Tôi chưa bao giờ đưa ra chứng cứ chống lại ai, kể cả khi tôi đã có thể có một thỏa thuận rất có lợi cho mình.

Tôi đoán khi bạn bè của bạn là những kẻ phạm pháp, sẽ thật ngây thơ nếu bạn cứ kỳ vọng vào lòng trung thành của họ.

Hai ngày sau, Michael Grant bảo tôi đã xong việc ở Teltec.

Tôi cũng đã đoán vậy nên không thấy bất ngờ.

https://thuviensach.vn

24
HÔ BIẾN

Xvof jg qis bmns lg hvq thlss ktffb J cifsok EAJ uojbthwsbhlsg?

Tới tháng 11, tôi vẫn đang thất nghiệp nhưng đã kiếm được chút tiền nhờ làm việc cho Danny Yelin, nhân viên cũ của Teltec. Anh ta có vài công việc bên ngoài và chuyển sang cho tôi làm. Những việc kiểu như tìm người cho các vụ thu hồi xe cộ: Tôi có thể tra ra họ dựa theo thông tin sử dụng dịch vụ công cộng (điện, nước…) và qua Phòng Phúc lợi Xã hội.

Trong khi đó, tôi như ngồi trên một quả bom hẹn giờ: Cảnh sát liên bang hẳn đang nghiền ngẫm đồng đồ của tôi mà họ đã lấy được từ căn hộ của Mark, cộng thêm bất kể thứ gì kiếm được ở chỗ Lewis và có thể đã tìm ra bằng chứng để tống tôi vào tù.

Tôi nên làm gì đây?

Thật dễ chịu nếu được ở cùng mẹ và bà trong lễ Tạ ơn, do đó, tôi gọi lên Phòng Quản chế và xin phép, tính trước trong lòng là họ có thể sẽ từ chối. Thực ngạc nhiên, viên giám sát chấp thuận, miễn sao tôi sẽ quay trở lại trước ngày 4 tháng 12.

Sau này, tôi mới biết từ ngày 6 tháng 11, Phòng Quản chế đã đệ đơn lên tòa án yêu cầu lệnh bắt giữ tôi, trích dẫn việc tấn công vào hộp thư thoại của nhân viên an ninh Pacific Bell và đã qua lại cùng Lewis De Payne. Lệnh bắt giữ được đưa ra ngay ngày hôm sau, với mức bảo lãnh là 25.000 đô-la.

Vậy tại sao Gulla lại cho phép tôi rời khỏi thị trấn thay vì đề nghị tôi tới gặp ông ấy? Cho đến tận bây giờ, tôi vẫn không hiểu lý do.

https://thuviensach.vn

Trong thời gian phóng thích có điều kiện, quản chế hay giám sát sau khi ra tù, bạn cần phải báo cáo với Phòng Quản chế địa phương mỗi khi di chuyển đến một đặc khu liên bang nào khác. Buổi sáng khi vừa tới Las Vegas, tôi đi thẳng tới văn phòng ở Đại lộ Bonneville để đăng ký.

Bản năng mách bảo tôi cần phải chắc chắn không có chuyện gì có thể xảy ra. Tôi có linh cảm rằng sẽ có vấn đề gì đó.

Trong xe của tôi có một chiếc ham radio đã được điều chỉnh để có thể truyền và tiếp nhận các dải tần số được cấp phép cho người dùng ham radio. Tôi dò một trong những tần số của Sở Cảnh sát Las Vegas.

Tôi lắng nghe chừng nửa giờ để nắm được phương thức một cảnh sát sẽ dùng khi anh ta muốn hỏi xem có lệnh bắt giữ có hiệu lực nào đối với một lái xe anh ta vừa giữ lại hay không. Anh ta sẽ nói: “Tôi cần 10-28 của biển số __.”

Trong lúc đó, tôi cố nhớ cách xưng hiệu của cảnh sát khi gọi cho Dispatch – ví dụ như, “1 George 21”. Người trực tổng đài sẽ đáp lại: “Nói đi, 1 George 21.”

Họ sẽ nói gì khi muốn nghỉ ăn trưa hay gì đó? Cuộc gọi truyền qua sóng sẽ bao gồm các cụm từ kiểu như: “Mã 7, Denny’s, Rancho Drive.”

Tôi đợi khoảng 10 phút, sau đó nhấn phím “Transmit” trên radio, sử dụng cách xưng hiệu của mấy tay cớm lúc đó đang tận hưởng bữa trưa ở Denny, và nói: “Tôi cần 10-28 biển số California___” và đưa ra biển số xe của tôi.

Sau vài giây, tay trực máy đáp: “Anh có đang tránh 440 không?”

Tim tôi nảy mạnh. “440” nghĩa là sao? Tôi hoàn toàn mù tịt.

Tôi nói: “Chờ một chút.”

https://thuviensach.vn

Dùng một chiếc điện thoại nhái số khác, tôi gọi cho cảnh sát ở thị trấn gần Henderson và nói: “Tôi là đặc vụ Jim Casey thuộc DEA. Tôi đang ở Las Vegas với Lực lượng Phòng chống Ma túy Đa ngành. Tôi cần biết ‘440’ có nghĩa là gì ở Las Vegas.”

“Cái đó có nghĩa là người bị truy nã.”

Khốn kiếp! Vậy “Anh có đang tránh 440 không?” có nghĩa là “Anh có đang đứng cách xa gã tội phạm bị truy nã đó không, tôi sẽ nói cho anh lý do tại sao hắn bị truy bắt?” Vậy là cảnh sát Las Vegas đã có trong tay lệnh bắt giữ tôi, truy theo biển số xe.

Nếu tôi bước vào Phòng Giám sát kia, khả năng cao là tôi sẽ bị còng tay và gửi ngay tới phòng giam! Tôi thấy thực may mắn khi mình đã tránh được viên đạn lần này, nhưng sau đó nỗi sợ hãi ào tới.

Vừa tới khu cổng vào khách sạn Sahara, tôi ngoặt bánh lái vào bãi đỗ xe của họ, đỗ xe ở đó và bỏ đi.

Khách sạn Sahara. Không thể thuận tiện hơn. Thật tình cờ, mẹ tôi đang làm nhân viên phục vụ quán cà phê trong đó. Tôi thơ thẩn bước xuyên qua sòng bài hào nhoáng và lấp lánh, lướt qua những tay cờ bạc om sòm, hau háu ném súc sắc trên bàn và đám phụ nữ tóc nhuộm bạch kim, mặt vô cảm trực bên máy đánh bài.

Tôi ngồi đợi tới khi ca làm việc của mẹ kết thúc để bà lái xe đưa tôi về. Khi tôi nói với mẹ và bà ngoại rằng mình rất có khả năng lại bị tống vào tù một lần nữa, cả gia đình bỗng rơi vào tình trạng rối loạn. Lễ Tạ ơn lẽ ra là khoảng thời gian hạnh phúc, rộn ràng, vậy nhưng với chúng tôi năm ấy, chẳng có chút niềm vui nào, cũng chẳng có “Ơn” để “Tạ”’.

Vài ngày sau đó, thay vì tới Phòng Quản chế, tôi gọi hai cuộc gọi ngoài giờ làm việc, để lại tin nhắn trên máy trả lời tự động rằng tôi phải báo cáo qua điện thoại vì mẹ tôi đang ốm và tôi không thể rời đi được.

https://thuviensach.vn

Liệu viên giám sát của tôi có gọi điện cho họ để thông báo về việc bắt giữ không? Tôi nhận ra âm thoại trả lời tự động của máy đặt trong phòng giám sát, do đó tôi có thể đoán được họ dùng hãng máy nào. Hãng sản xuất loại máy này thường đặt mã mặc định là "000" để phục hồi tin nhắn. Tôi thử vận may, và vâng, lại một lần nữa, không ai buồn đổi mã mặc định. Cứ vài giờ tôi lại gọi một lần, nghe tất cả tin nhắn. Thực mừng là không có tin nào tới từ viên giám sát phụ trách tôi.

Bà, mẹ và bạn trai mẹ, Steve Knittle, đưa tôi quay trở lại Los Angeles. Chắc chắn là tôi không đời nào tự lái xe của mình. Chúng tôi đến nơi vào tối muộn ngày 4 tháng 12, ngày cuối cùng trong hạn được phép dịch chuyển của tôi. Tôi bước vào nhà, không hề hay biết rằng viên cảnh sát tư pháp Brian Salt đã tới bắt tôi vào sáng hôm đó. Tôi ở lại nhà thêm ba ngày, sợ hãi và lo lắng, hiểu rằng FBI có thể xuất hiện bất kỳ lúc nào. Buổi sáng, tôi rời nhà từ rất sớm, tối nào cũng đi xem phim để cố quên đi. Có lẽ với người khác thì uống rượu và tiệc tùng cả đêm là lựa chọn không tồi, nhưng đầu óc tôi đang căng cứng. Tôi biết đây có thể là những ngày tự do cuối cùng trong thời gian sắp tới.

Tôi không rời khỏi Los Angeles cho tới khi hạn quản chế sau phóng thích của tôi kết thúc. Tôi cho rằng nếu họ đến bắt tôi thì cứ việc đến đi. Nhưng nếu họ không đến trước khi hạn giám sát kết thúc, tôi sẽ tự quyết định tương lai của chính mình: Tôi sẽ hóa thân thành một người khác và bốc hơi. Tôi sẽ tới sống ở một thành phố khác thật xa California. Sẽ không còn Kevin Mitnick nữa.

Tôi cố gắng nghĩ thông suốt kế hoạch chạy trốn của mình. Tôi sẽ sống ở đâu trong khi tạo ra một danh tính mới? Tôi nên chọn thành phố nào làm ngôi nhà mới của mình? Tôi sẽ kiếm sống ra sao?

Ý nghĩ về việc phải sống xa mẹ và bà khiến tôi vô cùng đau khổ bởi tôi yêu họ rất nhiều. Tôi ghét việc mình đã chuốc thêm nỗi đau khổ cho họ.

https://thuviensach.vn

Khi đồng hồ điểm 12 giờ đêm ngày 7 tháng 12 năm 1992, kỳ hạn giám sát của tôi chính thức kết thúc.

Không có cuộc gọi nào từ viên giám sát, không có bất kỳ cuộc vây bắt nào vào sáng sớm. Thật nhẹ nhõm. Tôi là người tự do.

Tôi đã nghĩ như vậy.

Mẹ tôi, bà ngoại và Steve sống tạm ở nhà họ hàng tôi, Trudy. Sau đó, chúng tôi đổi chỗ ở, mẹ và Steve thì đến ở tại nhà tôi để dọn dẹp đồ đạc, còn tôi thì chuyển đến với bà ở nhà Trudy. Chẳng có lý gì tôi lại loanh quanh ở khu nhà cũ khi mà hạn quản chế đã hết hiệu lực.

Những người mang huy hiệu cảnh sát thường có kiểu làm việc rất khó hiểu. Vào sáng sớm ngày 10 tháng 12, ba ngày sau khi thời hạn giám sát của tôi kết thúc, khi mẹ và Steve vẫn ở căn hộ của tôi để đóng đồ và xếp lịch chuyển đồ đạc, một tiếng gõ cửa bỗng vang lên. Nhóm người hành pháp cuối cùng cũng xuất hiện, lần này là một tổ ba người: cảnh sát tư pháp Brian Salt, một đặc vụ FBI mà mẹ tôi không rõ tên và đối thủ lâu năm của tôi, Ken McGuire, người mà tôi vẫn chưa thấy qua hay gặp trực tiếp. Mẹ nói tôi đã bỏ đi và bà không có tin tức gì, cũng không biết tôi hiện đang ở đâu. Bà còn nói: “Hạn giám sát của Kevin đã hết hiệu lực rồi.”

Khi Salt nói ông ta có lệnh bắt giữ tôi và đã để giấy nhắn trên cửa yêu cầu tôi liên lạc, lần này thì mẹ nói với ông ta sự thực: “Con tôi chưa bao giờ thấy mẩu giấy nhắn đó. Nếu không nó đã nói với tôi rồi.”

Sau đó là một trận cãi vã giữa đôi bên về việc rốt cục là kỳ hạn giám sát của tôi đã kết thúc hay chưa.

Sau này, bà nói với tôi rằng bà chẳng hề sợ. Họ hành xử như một lũ ngốc – đặc biệt là cái gã mở tủ lạnh ra rồi ngó nghiêng bên trong, như thể hắn ta nghĩ tôi trốn ở đó vậy. Bà nhìn gã đặc vụ rồi cười lớn. (Có lẽ gã kiểm tra tủ

https://thuviensach.vn

lạnh xem tôi có để lại cái bánh vòng nào nữa không.) Cuối cùng, họ bỏ đi mà cũng chẳng thu được tin tức gì.

Với những gì tôi có dính líu tới, tôi vẫn là một người tự do – tự do rời Los Angeles trước khi bị buộc thêm tội mới.

Nhưng tôi biết mình không thể lái xe quay trở lại Las Vegas với mẹ. Như vậy thì quá nguy hiểm; họ có lẽ đã theo dõi mẹ tôi. Do vậy, bà ngoại đề nghị bà sẽ lái xe đưa tôi trở lại Vegas sau khi tôi thu xếp xong công việc tại đây.

Có một việc còn đang dang dở vẫn ám ảnh tôi. Tôi đã lừa được DMV gửi cho mình bản sao ảnh bằng lái xe của Eric Heinz, nhưng để phòng ngừa bất trắc, tôi chuyển tiếp ảnh từ tiệm Kinko's thứ nhất sang tiệm thứ hai – tránh trường hợp cánh hành pháp có thể phát hiện ra và giám sát tiệm in để đợi tôi. Vì ảnh in được gửi fax hai lượt, tới tay tôi nó đã rất mờ nhiễu nên chẳng có ích gì. Tôi vẫn muốn có ảnh bằng lái xe của Wernle, Ways và Heinz để xem liệu có ai trong số này là cùng một người không.

Đêm Giáng sinh năm đó, ngay trước khi bắt đầu chuyển đồ lên xe, tôi gọi cho DMV dưới danh nghĩa Larry Currie, tên của một tay điều tra viên thuộc Đơn vị Lừa đảo Phúc lợi Los Angeles. Đưa ra mã yêu cầu của đơn vị, cùng với số PIN của Currie, ngày sinh và số bằng lái xe, tôi yêu cầu lấy Soundex của Eric Heinz, Joseph Wernle và Josephn Ways.

Nhân viên kỹ thuật ở đầu dây bên kia đã được cảnh báo trước. Cô ta báo với Ed Loveless, điều tra viên đặc biệt ở DMV, người mà theo báo cáo sau này, đã kiểm tra thông tin và phát hiện ra số máy fax tôi cung cấp thuộc về tiệm in Kinko's ở thành phố Studio.

Loveless đề nghị đưa ra một Soundex giả và họ dùng ảnh của "Annie Driver", một nhân vật không có thực mà DMV thường dùng trong các tài liệu hướng dẫn. Sau đó, Loveless liên lạc với điều tra viên của văn phòng DMV ở Van Nuys và đề nghị cô ta giám sát tiệm Kinko's kia, đồng thời bắt giữ người đến nhận fax. Điều tra viên này kéo theo vài đồng nghiệp đi cùng.

https://thuviensach.vn

FBI cũng được thông báo và đồng ý cử theo một đặc vụ của họ. Tất cả việc này đã diễn ra khi việc duy nhất mọi người muốn làm lúc đó là được ở nhà, sẵn sàng cho tiệc Giáng sinh đêm ấy.

Vài giờ sau cuộc điện thoại tới DMV để yêu cầu lấy Soundex, đồ đạc của tôi đã yên vị trên xe bà ngoại và chúng tôi cùng ăn trưa với Trudy. Tôi nói lời tạm biệt và rất biết ơn cô vì đã đồng ý cho tôi ở cùng. Cô và tôi không gần gũi lắm, do vậy sự giúp đỡ của Trudy càng trở nên đặc biệt.

Khi bà và tôi lên đường, tôi nói với bà rằng tôi còn một việc nhỏ cần làm và chỉ mất vài phút. Chúng tôi lái xe tới Kinko's.

Tại thời điểm đó, bốn nhân viên kiểm định của DMV trong bộ thường phục đã bắt đầu mất kiên nhẫn. Họ đã đợi hơn hai giờ đồng hồ. Đặc vụ FBI được chỉ định tham gia cũng có mặt, quanh quẩn ở đó một lúc rồi lại bỏ đi.

Các bạn hẳn phải cho rằng Kinko's khá vắng vẻ vào đêm Giáng sinh. Nhưng sự thực là ở đó có rất đông người, không khác gì những ngày làm việc thông thường. Tôi xếp hàng ở quầy tới 20 phút và cũng bắt đầu mất kiên nhẫn. Người bà tội nghiệp của tôi đang ngồi chờ và tôi không muốn gì hơn là lấy được Soundex rồi biến ra khỏi thị trấn.

Cuối cùng, tôi cũng bước được tới quầy nhận fax, lướt nhanh qua tập bì thư chứa fax gửi đến và kéo ra một tờ có nhãn "Larry Curry [DMV viết nhầm – thực ra phải là "Currie"], Đơn vị Lừa đảo Phúc lợi Los Angeles." Khi kéo tờ giấy in ra khỏi bì thư nâu vàng, tôi như bị chọc điên: Đây không phải là thứ tôi yêu cầu, chỉ có ảnh của một người phụ nữ rất khó nhận diện. Cái chết tiệt gì vậy? Tôi biết nhân viên của DMV thường làm biếng và vô năng, nhưng việc này chẳng phải là quá dễ sao. Một lũ ngu! Tôi nghĩ.

Tôi muốn gọi cho DMV và nói chuyện với mụ kỹ thuật viên ngu ngốc đó, nhưng lại quên điện thoại trên xe. Đi đi lại lại trong tiệm Kinko's, tôi ngẫm xem liệu có quá rủi ro nếu hỏi mượn điện thoại của cửa tiệm, hay là nên ra ngoài dùng điện thoại công cộng.

https://thuviensach.vn

Sau này, tôi mới nhận ra cảnh tượng lúc đấy đã gây chú ý thế nào đối với những người có mặt ở đó: Khi tôi bước qua lại nhìn chằm chằm vào máy fax và nghĩ xem phải làm thế nào, mấy tay điều tra của DMV cũng theo sát bước chân tôi. Mỗi lần tôi quay ngoắt theo chiều ngược lại, họ cũng xoay người ngay phía sau tôi, như thể chúng tôi đang diễn một đoạn kịch hề ở rạp xiếc vậy.

Cuối cùng, tôi bước ra theo lối cửa sau và lao tới bốt điện thoại công cộng. Khi cầm ống nghe lên và bắt đầu quay số, tôi nhận ra bốn gã mặc cảnh phục đang bước về phía mình.

Hừ, tôi nghĩ. Tôi vẫn chưa trả tiền fax và giờ hẳn là tôi đang gặp rắc rối liên quan đến mấy đô-la còn thiếu đó. Cả bốn người đều nhìn thẳng vào tôi.

Tôi nói: “Các người muốn gì?” rồi nhìn chằm chằm vào người phụ nữ đứng gần tôi nhất.

“Điều tra viên của DMV đây – chúng tôi muốn nói chuyện với anh!”

Thả ống nghe, tôi gào lên: “Mấy người biết sao không? Tôi không muốn nói chuyện với mấy người!” cùng lúc đó, tôi ném tung đống fax lên trời, dự tính rằng sẽ có một hay vài người trong số họ lao đến nó.

Tôi chạy qua bãi đỗ xe. Tim đập thình thịch, adrenaline tăng vọt. Tôi tập trung toàn bộ năng lượng mình có để chạy khỏi mấy gã đuổi theo sau.

Khoảng thời gian tập gym ngày qua ngày, tháng qua tháng cuối cùng cũng có giá trị. Mấy chục cân tôi giảm được cũng làm nên điều khác biệt. Tôi chạy về phía bắc bãi đỗ xe, lao nhanh ra khỏi cây cầu hẹp bằng gỗ dẫn tới khu dân cư lốm đốm bóng cọ dừa và chạy nhanh hết mức có thể, không hề ngoái đầu nhìn lại lấy một chút. Tôi đã dự tính rằng máy bay trực thăng có thể bay tới bất kỳ lúc nào. Tôi cần phải thay đổi diện mạo của mình thật nhanh. Như vậy, nếu đơn vị không quân được phái đến bắt tôi, tôi có thể đi chậm lại và ẩn mình vào dòng người qua lại trên đường phố.

https://thuviensach.vn

Khi chạy đủ xa để thoát khỏi tầm nhìn của mấy gã đuổi bắt phía sau, tôi bắt đầu cởi đồ mà không giảm tốc độ. Vốn là một tay nghiện gym, tôi mặc quần soóc và áo tập phía trong trang phục thông thường, Tôi cởi phăng sơ mi ngoài và ném vào một bụi rậm. Lò dò qua một lối đi nhỏ, tôi tháo quần dài và dúi nó vào một bụi cây trong vườn nhà ai đó, sau đó lại bắt đầu chạy.

Tôi duy trì nhịp chạy trong khoảng 45 phút cho tới khi chắc chắn mấy tay DMV đã bỏ cuộc. Bụng tôi quặn lại, cảm giác như muốn nôn mửa sau lần ráng sức, tôi chui vào một quán ba gần đó để nghỉ lấy hơi.

Tôi thấy mừng sau lần hút chết nhưng đồng thời cũng rất tuyệt vọng. Tìm được một bốt điện thoại công cộng phía sau quán bar, tôi quay số gọi vào di động của mình, lúc này vẫn ở trên xe bà. Tôi gọi đi gọi lại. Không ai nhấc máy.

Lại một lần nữa. Vẫn không ai nhấc máy. Chết tiệt! Tại sao bà không trả lời điện thoại? Tôi sợ bà đã vào Kinko’s để tìm tôi, có lẽ còn hỏi nhân viên ở đó và các khách hàng xem họ có trông thấy tôi không. Chết tiệt! Tôi phải tìm được bà.

Kế hoạch B. Tôi gọi tới siêu thị và nói với người ở đầu dây kia rằng bà tôi đỗ xe ở khu vực dành cho người tàn tật ngay bên ngoài siêu thị. “Tôi lẽ ra phải đón bà,” tôi giải thích, “nhưng tôi bị kẹt xe. Liệu ai đó có thể giúp tôi ra ngoài và bảo bà nghe máy được không? Tôi hơi lo cho sức khỏe của bà.”

Tôi đi đi lại lại, chờ đợi và chờ đợi. Cuối cùng thì người đàn ông nói chuyện với tôi cũng quay trở lại điện thoại và nói anh ta không nhìn thấy bà. Chết tiệt! Hay là bà đã vào trong Kinko’s rồi? Tôi phát điên khi cố gắng nghĩ xem chuyện gì đã xảy ra.

Cuối cùng, tôi cũng liên lạc được với Trudy và nói với cô chuyện gì đã xảy ra. Sau khi quát vào mặt tôi, cô lái xe tới bãi đỗ và vòng quanh theo từng hàng xe để tìm được xe của bà – hóa ra không phải trước cửa siêu thị mà là

https://thuviensach.vn

ngay ngoài Kinko’s. Người bà 66 tuổi tóc bạc của tôi vẫn đang ngồi trong xe chờ đợi.

Cả hai người họ tới gặp tôi ở nhà hàng Dupar gần đó. Tôi đã đi bộ tới đây và cảm thấy tệ hại vô cùng khi để bà phải ngồi trong xe trong suốt ba tiếng đồng hồ. Nhìn thấy họ bước vào cửa, tôi thở phào nhẹ nhõm vì thấy bà ngoại trông vẫn ổn.

“Cháu gọi cho bà liên tục – tại sao bà không nhấc máy?” tôi hỏi.

“Ta nghe thấy chuông nhưng không biết làm sao để mở máy,” bà đáp.

Không thể tin được! Tôi chưa từng nghĩ đến việc điện thoại di động có thể là một bí ẩn đối với bà tôi.

Đợi khoảng chừng một giờ, bà nói, bà đã vào trong Kinko’s. Rõ ràng là có chuyện gì đó xảy ra, có vẻ như có một hoạt động gì đó của cảnh sát. Một người phụ nữ cầm túi nilon, bên trong có đĩa từ. Khi tôi hỏi người phụ nữ đó trông thế nào, bà mô tả chính xác người đặc vụ DMV đã đuổi theo tôi.

Trong vô số lần hacking, tôi chưa từng cảm thấy áy náy vì đã lấy thông tin lẽ ra không được phép, hay dụ dỗ các nhân viên công ty để lộ ra những thông tin độc quyền, nhạy cảm. Nhưng khi nghĩ về bà, người đã làm rất nhiều điều cho tôi và luôn quan tâm tới tôi trong suốt cuộc đời, đã phải ngồi trong xe lâu như vậy, chờ đợi và lo lắng, lòng tôi ngập tràn nỗi ân hận.

Còn đĩa từ mà bà nhắc đến thì sao? Các bạn có lẽ không để ý nhưng mỗi cửa tiệm của Kinko’s đều có camera an ninh lưu lại dòng hình ảnh liên tục tương đương với 24 giờ dữ liệu. Chiếc đĩa đó hẳn sẽ chứa nhiều hơn một vài hình ảnh sắc nét của tôi.

Chỉ những hình ảnh đó vẫn không đủ để các đặc vụ DMV chỉ đích danh người họ muốn truy bắt, nhưng những thứ khác thì có thể. Những tài liệu fax tôi ném lên trời sẽ được đem tới phòng thí nghiệm tội phạm. Ở đây, họ sẽ

https://thuviensach.vn

lấy được dấu vân tay của tôi trên đó. Rất nhanh họ sẽ có được cái tên: Kevin Mitnick.

Khi các đặc vụ FBI có được "six-pack" – bộ sáu ảnh gồm một của tôi và năm cái khác của những gã ngẫu nhiên nào đó – thì Shirley Lessiak, nhân viên giám định DMV, người đã đuổi theo tôi, sẽ không gặp khó khăn gì trong việc chỉ ra người mà cô ta đuổi bắt trước đó.

Tôi đã chạy thoát khỏi Lessiak và đồng nghiệp của cô ta, nhưng ở một khía cạnh khác, tôi vẫn phải tiếp tục chạy trốn. Giờ đây, tôi luôn phải ở trong tình trạng "trốn chạy" – bắt đầu một cuộc sống mới như một kẻ chạy trốn pháp luật.

https://thuviensach.vn

Phần ba

TRỐN CHẠY

https://thuviensach.vn

25

HARRY HOUDINI

Cngz zuct ngy znk grsg sgzkx lux znk xkgr Kxoi Ckoyy?

Vậy là tôi đang trên đường trốn chạy, một kẻ bị truy nã. Với những gì cảnh sát trưởng Salt đã nói với mẹ tôi – rằng ông ta có lệnh bắt giữ tôi – thì đây có vẻ là lựa chọn duy nhất dành cho tôi.

Thế nhưng nhiều năm sau, David Schindler, trợ lý công tố được phân công phụ trách vụ của tôi, đã tâm sự rằng ông rất ngạc nhiên khi nghe tin tôi biến mất. Ông ấy nghĩ gì vậy? Eric đã báo cho FBI rằng tôi vẫn liên hệ với Lewis, như vậy là vi phạm điều khoản quản chế. Tôi chắc rằng hắn cũng báo cáo về việc tôi có toàn quyền truy cập SAS và có thể dùng nó để nghe lén mọi người. Tổ An ninh của Pacific Bell đã phát hiện ra tôi nghe lén hộp thư thoại của ít nhất một nhân viên của họ: Đó sẽ là một án mới khác có thể được trình lên để chống lại tôi. Ngoài ra, Lewis cũng đã ba hoa bốc phét với Eric về những vụ hack khác mà cả hai chúng tôi thực hiện.

Bà lái xe suốt cả chặng đường dài năm tiếng đưa tôi đến Vegas; tôi không lái xe kể từ khi biết được FBI có lệnh bắt tôi. Đó không hẳn là một chuyến đi vui vẻ. Làm sao có thể vui được chứ?

Chúng tôi đến nơi khi trời đã tối, bà cho tôi xuống ở Budget Harbor Suites. Một người bạn đã rộng lòng đặt một phòng cho tôi tại đây bằng tên của anh.

Việc đầu tiên tôi phải làm là tạo ra một thân phận mới cho bản thân rồi biến mất – dù điều đó cũng đồng nghĩa với việc phải bỏ lại bạn bè và người thân cũng như cuộc sống tôi đã và đang tận hưởng. Mục tiêu của tôi là xóa đi quá khứ và tạo dựng khởi đầu mới hướng về một tương lai khác.

https://thuviensach.vn

Nhưng bằng cách nào đây? Nếu còn nhớ nguồn sách ưa thích của tôi ở tiệm sách Survival, nơi tôi thường xuyên ghé qua khi còn bé, hẳn bạn đã biết câu trả lời. Cuốn sách yêu thích của tôi thời đó, The Paper Trip, đã giải thích cặn kẽ các bước để có được danh tính mới. Tôi áp dụng đúng các nguyên tắc đó nhưng theo một hướng tiếp cận khác: Tôi cần một thân phận mới dùng tạm ngay lập tức; ngay khi chuyển chỗ ở, tôi có thể dành thời gian để tạo ra thân phận thứ hai và sống với nó suốt phần đời còn lại.

Tôi gọi giả danh đến Oregon DMV, tự nhận mình là Giám sát Bưu chính, tôi nhờ thư ký ở đây tra cứu xem có ai tên là Eric Weiss, sinh trong giai đoạn 1958-1968 – khoảng thời gian xoay quanh năm 1963, năm sinh thực tế của tôi. Tôi muốn tìm một người trạc tuổi mình, nhưng càng trẻ càng tốt. Tôi sẽ nộp đơn xin cấp bằng lái xe và thẻ An sinh Xã hội mới. Đơn khai xác nhận giấy khai sinh mới cho người càng lớn tuổi sẽ càng nhận được nhiều ánh mắt nghi ngờ: Chẳng hạn như tại sao một người đã ngoài 30 mà lại chưa bao giờ cần tới số An sinh Xã hội?

Cô thư ký ở DMV tìm ra vài kết quả, nhưng chỉ có một người phù hợp với tiêu chí của tôi. Eric Weiss mà tôi chọn sinh năm 1968, tức là anh ta trẻ hơn tôi khoảng năm tuổi.

Tại sao lại là “Eric Weiss”? Bởi đó là tên thật (dù một số nguồn cũng đánh vần là “Erich Weiss” hay “Erik Weisz”) của Harry Houdini. Tôi chọn cái tên đó một phần vì sự tôn sùng dành cho vị anh hùng trong lòng tôi, hoài niệm còn sót lại từ những đắm say xưa kia với ảo thuật. Chỉ cần có tên mới, vậy thì tại sao lại không bày tỏ lòng thành kính với thần tượng tuổi thơ của mình cơ chứ?

Tôi gọi đến tổng đài và phát hiện ra Eric Weiss “của tôi” có một số điện thoại. Sau khi gọi và thấy anh ta bắt máy, tôi hỏi: “Anh có phải là Eric Weiss, sinh viên trường PSU không?”

Anh ta đáp: “Không, tôi tốt nghiệp Ellensburg.”

https://thuviensach.vn

Eric Weiss, thân phận mà tôi sẽ sử dụng, có bằng Quản trị Kinh doanh của Đại học Central Washington, tại thị trấn Ellensburg. Đó là những gì tôi sẽ ghi vào sơ yếu lý lịch.

Lá thư tôi gửi tới Cục Thống kê Sinh sản Oregon hoàn toàn chỉ mang tính thủ tục. Nó có vẻ như đến từ Eric Weiss thật, trong đó ghi nơi sinh và ngày sinh thật, tên cha và tên thời con gái của mẹ anh ta (như thường lệ, những thông tin này vẫn do cô bạn Ann ở Sở An sinh Xã hội nhiệt tình cung cấp cho tôi) với yêu cầu "một bản sao giấy khai sinh của tôi". Tôi đã trả thêm tiền để họ chuyển phát nhanh. Phần địa chỉ người nhận, tôi dùng một trong những hòm thư cho thuê.

Tôi sẽ cần dùng tới thân phận thứ hai này khi đăng ký bằng lái xe, vì thế, tôi làm giả một tờ khai W-2, vốn sẽ yêu cầu cung cấp Số Đăng ký Kinh doanh (EIN) của nơi cấp tờ W-2. Đối với hầu hết các công ty được lựa chọn một cách ngẫu nhiên, việc tìm ra số này không khó. Tôi gọi đến Phòng Thu nợ của Microsoft và hỏi EIN của họ "để chúng tôi có thể đệ trình việc chi trả". Người phụ nữ ở đầu dây bên kia đã cung cấp ngay cho tôi mà không thèm hỏi tôi gọi đến từ công ty nào.

Mọi cửa hàng đồ văn phòng đều có tờ khai thuế trắng; bạn chỉ cần làm giả ra một tờ W-2, thế là xong.

Mục tiêu trước mắt của tôi là lấy được tấm bằng lái xe vô cùng quan trọng, nhưng tôi không thể manh động cho đến khi nhận được giấy khai sinh "mới". Đó là khoảng thời gian rất khó khăn đối với tôi: Không có bằng lái xe hay chứng minh thư, ngay cả việc bị cảnh sát bắt gặp khi đi bộ cắt ngang đường cũng có thể trở thành thảm họa.

Có một trở ngại là tôi sẽ cần một chiếc xe để thi lấy bằng. Tôi phải mượn của mẹ hay của bà đây? Không được. Nếu đang cố gắng tạo ra một thân phận mới, bạn chắc chắn sẽ không muốn để lại "những vụn bánh mì" giúp công việc của mấy gã cớm hay đặc vụ thích rình mò trở nên dễ dàng hơn.

https://thuviensach.vn

Thế còn việc nhờ một người bạn hay thành viên trong gia đình thuê hộ một chiếc xe trong khoảng thời gian đủ lâu để thi lấy bằng lái thì sao? Không thể nào – việc này quá lộ liễu, các điều tra viên sẽ lần dấu ra chiếc xe được sử dụng cho bài thi, và đẩy người đã giúp đỡ bạn vào tình huống khó khăn.

Và đây là giải pháp tôi đã nghĩ ra. Đầu tiên, tôi đến DMV đăng ký thi lý thuyết; dù không thực sự cần phải làm thế, nhưng người ở DMV sẽ bớt phần nghi ngờ hơn nếu một người trưởng thành thi lý thuyết trước khi thi thực hành để lấy được bằng lái đầu tiên. Tôi không rõ lý do tại sao lại như vậy. Nhưng việc này hiệu quả đối với tôi: Hầu hết những người cố tạo thân phận giả đều không lấy bằng thi lý thuyết trước, do đó, trông tôi có vẻ ít khả nghi hơn.

Sau đó, tôi gọi đến trường dạy lái xe và nói mình vừa từ Australia, Nam Phi hay Anh về. Tôi giải thích rằng mình từng có bằng lái xe ở Mỹ, nhưng sau một thời gian lái xe bên trái, tôi cần rèn luyện thêm để có thể lái ở làn bên phải trước khi thi lấy bằng lái xe. Sau vài "buổi học", thầy hướng dẫn bảo tôi có thể tham gia thi và trường lái sẽ cho bạn mượn xe để thi.

Dù sao thì đó cũng là những gì tôi đã làm hơn một lần và luôn thành công. Với bằng lái mới trong tay, tôi đến phòng An sinh Xã hội ở trung tâm Las Vegas để lấy thẻ An sinh Xã hội "thay thế", sử dụng giấy khai sinh của Eric Weiss và bằng lái xe của tôi làm hai giấy tờ chứng minh. Tôi có chút lo lắng: Những cảnh báo về việc sử dụng thẻ An sinh Xã hội bằng danh tính giả là hành vi vi phạm pháp luật được treo và dán khắp tòa nhà. Còn có cả poster vẽ hình người bị còng tay nữa. Tuyệt!

Tôi trình giấy tờ tùy thân và một tờ khai đã điền sẵn. Họ nói phải mất khoảng ba tuần mới xong, lâu hơn nhiều so với khoảng thời gian tôi có thể thoải mái sống ở Vegas, nhưng tôi biết mình không thể kiếm việc ở bất cứ đâu mà không có tấm thẻ này.

https://thuviensach.vn

Trong thời gian chờ đợi, tôi đi loanh quanh đến thư viện gần nhất. Thủ thư ở đây vui vẻ cung cấp thẻ thư viện cho tôi ngay sau khi nhập thông tin của tôi vào hệ thống từ tờ khai của tôi.

Dù mối quan tâm chính của tôi là có được thân phận mới và quyết định xem nên đi đâu làm gì, nhưng Danny Yelin, cựu nhân viên của Teltec và lúc hành nghề tự do, vẫn cho tôi chút việc để làm. Một trong số đó là gửi trát hầu tòa cho một gã từng sống ở Vegas nhưng giờ đang lẩn trốn. Dan cho tôi số điện thoại cuối cùng mà hắn dùng.

Tôi gọi đến số đó, một người phụ nữ đứng tuổi trả lời, tôi hỏi bà ta rằng hắn có ở đó không. Bà ta đáp "không".

Tôi bảo bà ta: "Tôi nợ hắn một số tiền. Tôi có thể trả một nửa ngay bây giờ và một nửa vào tuần sau. Nhưng tôi sắp rời thành phố rồi, nên tôi cần gọi cho hắn và hỏi xem hắn muốn gặp tôi ở đâu để có thể trả cho hắn trước một nửa." Tôi nói sẽ gọi lại sau nửa tiếng nữa.

Khoảng 10 phút sau, tôi gọi đến Trung tâm Điều khiển Chuyển mạch ở Centel, một công ty điện thoại địa phương. Đóng vai một nhân viên nội bộ, tôi đã nhờ một kỹ thuật viên chuyển mạch DMS-100 thực hiện lệnh QCM (Truy vấn bộ nhớ cuộc gọi) tới số của người phụ nữ đó.

Bà ta đã thực hiện cuộc gọi gần nhất khoảng năm phút trước, đến Motel 6[66] ở gần sân bay. Tôi gọi đến và được nối máy đến phòng của hắn ta, tôi nói mình gọi điện từ bàn lễ tân và hỏi xem hắn có còn cần giường gấp như đã yêu cầu trước đó hay không. Tất nhiên, hắn nói hắn chưa bao giờ đề nghị việc này.

[66] Tên một chuỗi nhà nghỉ giá rẻ của Mỹ. (ND)

Tôi nói: "Đó có phải là phòng 106 không thưa ông?"

Hắn nói bằng giọng khó chịu: "Không, đây là phòng 212." Tôi xin lỗi hắn.

https://thuviensach.vn

Bà tôi đã tốt bụng lái xe chở tôi đến đó.

Trả lời tiếng gõ cửa của tôi là giọng nói: “Gì vậy?”

“Dọn phòng đây, ông có phiền không?”

Hắn mở cửa. Tôi nói: “Ông là ông____?”

“Phải.”

Tôi đưa tập tài liệu cho hắn và nói: “Tôi xong việc rồi. Chúc ông một ngày tốt lành.”

Tôi kiếm được 300 đô-la dễ dàng. Khi ký nhận dịch vụ, tôi còn cười với chính mình và tự hỏi: Gã sẽ nghĩ gì nếu biết mình vừa nhận được lệnh hầu tòa từ tay của một tội phạm bị truy nã cấp Liên bang?

Thỉnh thoảng, tôi lại đi bộ đến Sahara để ăn tại nhà hàng nơi mẹ làm, để chúng tôi có thể gặp nhau. Những lúc khác tôi gặp bà, mẹ và bạn trai của mẹ, Steve, ở một trong các casino khác, nơi tôi hy vọng chúng tôi có thể biến mất trong đám đông. Thỉnh thoảng, tôi sẽ xuất hiện tại Eureka, một casino nhỏ, nơi mẹ thích chơi video poker sau khi kết thúc ca làm.

Tiền là một vấn đề. Tôi có một ít nhưng không đủ. Thật khó tin, ở tuổi 28, tôi vẫn giữ hầu hết tiền lễ trưởng thành dưới dạng trái phiếu Kho bạc và giờ tôi rút ra hết. Ngoài khoản tiền đó, mẹ và bà cũng hỗ trợ thêm cho đến khi tôi có thể ổn định và tìm được một công việc. Tôi có tất cả khoảng 11.000 đô-la tiền mặt, đủ để sống cho đến khi tôi làm lại cuộc đời.

Và từ chính xác đúng là “tiền mặt”: Toàn bộ chỗ tiền tôi có là tiền mặt, được nhét vào một chiếc ví để trong túi hành lý xách tay mà tôi mang theo khắp nơi.

Do vẫn chưa có thẻ An sinh Xã hội “thay thế” của Eric Weiss, nên tôi không thể mở tài khoản tại các quỹ tín dụng hay ngân hàng. Khách sạn tôi ở không

https://thuviensach.vn

có két trong phòng như những chỗ xịn hơn. Tôi nên thuê một hộp gửi đồ ở ngân hàng chăng? Cũng không ổn vì tôi không thể mở tài khoản ngân hàng: Tôi sẽ phải chìa ra các giấy tờ tùy thân do chính phủ cấp.

Tất nhiên, khỏi cần nghĩ đến chuyện giấu tiền ở phòng khách sạn làm gì. Vậy để tiền ở chỗ bà thì sao? Không được, như vậy chúng tôi sẽ phải gặp nhau mỗi khi tôi hết tiền. Đó cũng không phải là kế hay khi FBI đã bắt đầu theo dõi bà.

Tuy vậy, nếu được làm lại một lần nữa, đó chính là những gì tôi sẽ làm: Tôi sẽ để nó ở chỗ bà, giữ lại vừa đủ số tiền tôi cần để sống qua ngày và không cần phải về nhà bà quá thường xuyên.

Ngay phía sau Stardust Casino & Hotel, gần nơi tôi sống, có một phòng gym cao cấp tên là Sporting House. (Nó thực sự là một phòng tập gym, dù ở Nevada, tên của nó dễ bị nhầm với một số thứ khác. Trên thực tế, tên gọi này hóa ra lại là lời tiên tri: Giờ đây, nơi này là câu lạc bộ khỏa thân dù dưới một cái tên khác.) Con gái của ông trùm khách sạn ở Las Vegas, Steve Wynn, cũng tập ở đây, nên tôi đoán đó phải là một nơi rất tuyệt.

Tôi đăng ký thẻ tập hằng tuần, quyết tâm duy trì chế độ tập luyện hai hoặc ba tiếng mỗi ngày. Ngoài việc giữ dáng, luyện tập còn đem lại cho tôi cơ hội ngắm các em gái khi tôi tập theo nhạc trên chiếc Walkman.

Một ngày nọ, sau khi hoàn thành buổi tập, tôi trở vào phòng thay đồ và phát hiện ra mình đã quên khóa tủ để đồ. Tôi đi vòng quanh, kiểm tra mọi tủ.

Khóa cá nhân của tôi không ở tủ nào cả.

Tôi xem xét lần nữa. Không thấy gì cả.

Tôi bắt đầu mở tất cả các tủ không có khóa treo trên cánh tủ. Cuối cùng, tôi đã tìm thấy tủ đựng quần áo của tôi.

https://thuviensach.vn

Quần áo vẫn ở đó nhưng chiếc túi đã không cánh mà bay: Tim tôi chùng xuống. Tất cả tiền của tôi, giấy tờ cho danh tính mới đều đã bốc hơi. Tôi đã mua một khóa móc cực kỳ chắc chắn để dùng ở phòng tập gym. Nếu là một tên tội phạm có hiểu biết, hẳn là hắn sẽ biết cách nào đó tốt hơn, nhưng gã này chắc chắn đã cậy tủ bằng một chiếc máy cắt khóa. Có thể chính chiếc khóa đôi nặng trịch này đã gợi ý rằng có gì đó trong tủ khóa đáng để bảo vệ. Ôi, Chúa ơi!

Tôi hoảng hồn. Toàn bộ 11.000 đô-la giấu kỹ của tôi đã bị mất. Tôi trở thành kẻ không xu dính túi, không thu nhập, đang đối mặt với thử thách phải chuyển đến một thành phố mới, thuê một căn hộ và trang trải mọi thứ cho đến khi kiếm được việc và bắt đầu nhận được lương. Tôi thấy mình như một thằng ngu hết thuốc chữa khi cứ mang theo toàn bộ số tiền giễu khắp nơi, không khác gì mời lũ trộm xơi.

Khi thông báo sự việc với quản lý đang trực ở phòng gym, tôi chỉ nhận được sự cảm thông hà tiện. Cô ta gượng gạo cố khiến tôi cảm thấy tốt hơn bằng việc nói rằng đã có một loạt những vụ đột nhập tương tự vào phòng tập gym gần đây. Giờ cô ta mới nói cho tôi biết! Và cô ta xoáy thêm vào nỗi đau của tôi bằng việc đề nghị tặng tôi bốn phiếu tập gym ngày để đền bù. Không phải bốn tháng, thậm chí không phải một tháng, mà là bốnngày!

Đương nhiên, tôi không thể liều lĩnh báo vụ mất cắp với cảnh sát.

Phần tồi tệ nhất là nói với mẹ và bà về tình trạng khó khăn không may đó. Tôi không thể chịu được ý nghĩ khiến họ thêm phần lo lắng và đau khổ. Họ đã luôn ở đó vì tôi, sẵn sàng giúp tôi trong bất kỳ tình cảnh nào bởi họ yêu tôi quá nhiều. (Điều này không có nghĩa là họ không thể hiện sự bực mình với tôi.) Và giờ họ lại bên tôi một lần nữa, dồn góp được 5.000 đô-la cho đến khi tôi sẵn sàng. Phải nói rằng đây rõ ràng là món quà mà tôi không xứng đáng được hưởng.

https://thuviensach.vn

Để quên đi điều đó, tôi đi xem phim và thỉnh thoảng chơi xì dách tại một trong số các casino. Tôi đã đọc cuốn sách của Kenny Uston về đếm bài và phát hiện ra mình khá giỏi nhớ các lá bài có thứ tự cao – dù tôi hiếm khi có thể bước ra khỏi bàn với số tiền rủng rỉnh hơn so với số tôi đã đặt xuống lúc đầu.

Trong khi đợi thẻ An sinh Xã hội mới, tôi quay lại DMV để báo mất giấy phép lái xe và được cấp lại ngay lập tức.

Trong ba tuần chờ đợi, tôi gom các dạng giấy tờ tùy thân khác nhau nhiều nhất có thể. Vào thời điểm tôi sẵn sàng rời Las Vegas, ngoài thẻ thư viện, tôi còn có thẻ của Câu lạc bộ Điền kinh Las Vegas, Blockbuster Videos, một thẻ ATM ngân hàng, một Sổ Y tế Nevada mà những người chuẩn bị thức ăn hay các nhân viên casino khác phải có.

Thư viện Quận Clark trong vùng trở thành điểm đến quen thuộc của tôi. Tôi vùi đầu vào các tạp chí kinh doanh và du lịch để tìm kiếm nơi đến tiếp theo ngay khi danh tính mới của tôi hoàn tất. Danh sách rút gọn của tôi bao gồm Austin và Tampa cùng vài thành phố khác, nhưng quyết định cuối cùng thật dễ dàng.

Không lâu trước đó, tạp chí Money đã xếp hạng Denver là một trong những nơi tốt nhất để sống trong cả nước. Nghe có vẻ ổn. Nó không quá xa và có vẻ thị trường việc làm cho ngành máy tính sôi động, được xếp hạng tốt về chất lượng cuộc sống và việc ổn định ở đó sẽ đem đến cho tôi cơ hội đầu tiên được trải nghiệm các mùathực sự – thứ mà miền đất Nam California luôn từ chối tôi. Thậm chí, tôi còn có thể thử trượt tuyết.

Tôi mua máy nhắn tin cho mẹ và tôi – tất nhiên là sử dụng tên giả để mua và trả tiền mặt. Tôi mua một chiếc thứ ba cho Lewis. Phải, Lewis, cậu ta sẽ là nguồn cung cấp thông tin tốt cho tôi. Tôi sẽ thiết lập kênh để trao đổi an toàn. Bất chấp quá khứ giữa chúng tôi, tôi vẫn tin Lewis đủ để cảm thấy

https://thuviensach.vn

chắc chắn rằng nếu cậu ta nghe ngóng được gì từ FBI, cậu ta sẽ báo động cho tôi.

Chúng tôi thiết lập mã và giao thức để dùng trong trường hợp khẩn cấp. Nếu cần liên lạc, mẹ tôi sẽ nhắn tin xác định một trong các khách sạn lớn ở Las Vegas. Mã của chúng tôi cho Mirage, ví dụ là "7917111" – số điện thoại của Mirage bỏ đi mã vùng. Tất nhiên, mã vùng là như nhau cho mọi khách sạn ở Las Vegas và việc bỏ nó đi sẽ khiến bất cứ ai có thể chặn được trao đổi nhắn tin của chúng tôi khó đoán được địa chỉ. Một phần khác của mã chỉ ra mức khẩn cấp: "1" nghĩa là "Nếu tiện, hãy gọi cho mẹ"; "2" là "Hãy gọi cho mẹ càng sớm càng tốt"; "3" là "Hãy gọi cho mẹ ngay lập tức, đây là tình huống khẩn cấp." Khi tôi là người muốn liên lạc, tôi sẽ nhắn cho mẹ một số ngẫu nhiên cùng mã khẩn cấp và mẹ sẽ nhắn lại cho tôi số khách sạn mẹ đang ở.

Dù ai là người bắt đầu cuộc trao đổi, giao thức cũng giữ nguyên. Sau khi nhận được số casino mẹ đang ở, tôi sẽ gọi và nhờ nhân viên tổng đài nhắn gọi một người cho tôi và cung cấp tên một người bạn cũ của mẹ. Tên này không bao giờ trùng nhau hai lần liên tiếp; tôi luôn quay vòng họ (chẳng hạn như tên "Mary Schultz").

Khi nghe thấy một cái tên quen, mẹ sẽ nhấc máy điện thoại và nhân viên tổng đài sẽ nối máy cuộc gọi.

Nếu FBI thực sự muốn tìm một ai đó, tôi biết họ sẽ tìm cách nghe lén các máy điện thoại công cộng mà người thân hay những người có liên quan thường dùng. Vậy tại sao tôi lại liều lĩnh như vậy? Casino khách sạn thường xuyên phải xử lý cả tá cuộc gọi mỗi lần, có thể cả trăm. Ngay cả khi McGuire và cộng sự hạ quyết tâm theo dõi mẹ tôi với hy vọng tôi sẽ gọi cho bà và hé lộ địa điểm của mình, họ sẽ không dễ lần theo cuộc gọi đi qua mạch chuyển bận rộn tại một nơi như Ceasars Palace.

Do chưa từng bị truy nã trước đây ngoại trừ vài tháng ở Oroville hồi còn niên thiếu, tôi không thể biết nên phản ứng ra sao. Rời khỏi mạng lưới thật

https://thuviensach.vn

đáng sợ, nhưng tôi có thể nói mình thích việc này. Có cảm giác như đây chính là khởi đầu của một hành trình thú vị.

https://thuviensach.vn

26
THÁM TỬ TƯ

Aslx jst nyk rlxi bx ns wgzzcmgw UP jnsh hlrjf nyk TT seq s cojorpdw pssx gxmyeie ao bzy glc?

Đây là lần đầu tiên tôi chỉ có một mình. Sống ở Denver khi không có mẹ và bà ở bên đem lại cảm giác lạ lẫm nhưng cũng đầy phấn khích. Lúc máy bay cất cánh rời Las Vegas, tôi sẽ biến mất trên chín tầng mây theo đúng nghĩa đen, đến thị trấn mới và bắt đầu ẩn náu.

Bạn có thể tưởng tượng ra cảm giác tự do khi bắt đầu một cuộc sống mới với tên mới và thân phận mới không? Hiển nhiên bạn sẽ nhớ gia đình và bạn bè, nhớ cảm giác dễ chịu ở những nơi chốn quen thuộc, nhưng nếu có thể tạm gạt nó sang một bên, chẳng phải toàn bộ việc này sẽ giống như một cuộc phiêu lưu vĩ đại hay sao?

Trong suốt chuyến bay tới "Thành phố cao một dặm"[67], niềm mong đợi trong tôi ngày càng lớn. Khi máy bay của hãng United Airlines hạ cánh, thời tiết Denver vô cùng xấu: Bầu trời u ám và ảm đạm. Tôi bắt taxi và nhờ tài xế đưa tới khách sạn nào đó ở một khu dân cư tốt, có thể thuê phòng theo tuần. Ông ta đưa tôi tới nơi mà ông ta gọi là "chuỗi khách sạn".

[67] Denver được gọi là "Thành phố cao một dặm" do nằm trên mực nước biển đúng một dặm, tương đương với khoảng 1.600m. (ND)

Tôi đánh giá khách sạn này vào khoảng hai sao rưỡi, ngang Motel 6. Hóa ra ở đây không cho thuê phòng theo tuần, nhưng chỉ cần thuyết phục một chút, tôi đã có được mức giá thỏa đáng theo thời hạn mình định lưu lại.

https://thuviensach.vn

Do ảnh hưởng từ các bộ phim, mọi người thường cho rằng cuộc sống của một kẻ chạy trốn pháp luật luôn đồng nghĩa với việc phải cảnh giác khắp nơi cùng nỗi sợ thường trực rằng mình có thể bị phát hiện. Tôi hiếm khi cảm thấy như vậy. Sau khi có được thân phận mới, cầm trong tay tấm thẻ căn cước có thể xác minh do chính phủ cấp, tôi gần như luôn cảm thấy an toàn. Để phòng xa, lúc nào tôi cũng kích hoạt hệ thống cảnh báo sớm để lường trước việc có ai đó đến tìm. Nếu phát hiện có ai đó tới gần, tôi có thể hành động ngay lập tức. Nhưng ngay từ những giây phút đầu tiên, tôi đã tận hưởng cuộc sống của mình.

Công việc đầu tiên mỗi khi tôi tới thành phố mới nào đó là tấn công vào công ty điện thoại địa phương nhằm ngăn chặn ai đó có thể dễ dàng tìm ra tôi. Để bắt đầu, tôi cần các số điện thoại mà kỹ thuật viên hiện trường thường dùng để gọi vào bộ chuyển mạch của công ty. Tôi lấy được số điện của CO phụ trách tổng đài điện thoại mà tôi muốn kiểm soát. Tôi sẽ gọi cho họ và nói gì đó kiểu như: “Chào anh, tôi là Jimmy ở Phòng Kỹ thuật. Anh thế nào?”

Câu kế tiếp sẽ là: “Số dial-up của VDU là gì nhỉ?” – VDU là từ viết tắt của Visual Display Unit (Thiết bị Hiển thị Hình ảnh), một thiết bị cho phép kỹ thuật viên có toàn quyền đăng nhập vào bộ chuyển mạch từ xa. Nếu bộ chuyển mạch đó là 1AESS, bạn thậm chí không cần tới mật khẩu để truy cập. Gã nào đặt ra điều kiện này hẳn phải hiểu rằng bất kỳ ai chỉ cần có số điện thoại tới bộ chuyển mạch là đã có quyền truy cập.

Thường thì kỹ thuật viên tôi gặp sẽ cho tôi số điện thoại để kết nối với bộ chuyển mạch ở CO của anh ta. Nhưng nếu anh ta đặt nghi vấn, tôi cũng đủ hiểu biết về hệ thống để bịa ra một lý do tức thì. Kiểu như: “Chúng tôi đang thiết lập hệ thống quay số và muốn lập trình tất cả các số dial-up vào phần mềm quay số gọi đi. Nếu có kỹ sư chuyển mạch nào cần kết nối, họ chỉ cần bấm modem gọi tới văn phòng thôi.”

https://thuviensach.vn

Khi đã có số điện thoại để kết nối tới bộ chuyển mạch, tôi có thể làm khá nhiều việc mình thích. Nếu muốn thực hiện chuỗi cuộc gọi cho ai đó, ví dụ như ở Nhật Bản chẳng hạn, tôi sẽ tìm một số điện thoại chưa được phân cho thuê bao nào, sử dụng nó, thêm tính năng chuyển tiếp cuộc gọi và kích hoạt để chuyển cuộc gọi tới bất kỳ nơi nào tôi muốn. Sau đó, từ điện thoại di động của mình, tôi có thể thực hiện cuộc gọi trong nước tới số điện thoại chưa được phân cho ai kia, rồi lại từ đó kết nối trực tiếp tới thuê bao ở Nhật Bản, thay vì phải sử dụng cuộc gọi di động quốc tế không đáng tin chút nào.

Tôi cũng thường dùng kỹ thuật “masking” (ngụy trang) nhằm thiết lập chuỗi các số chuyển tiếp cuộc gọi ở những bộ chuyển mạch thuộc các thành phố khác nhau ở những vùng khác nhau trên khắp cả nước. Nhờ vậy, khi tôi gọi số đầu tiên trong chuỗi, cuộc gọi của tôi sẽ được truyền dọc theo chuỗi từ thành phố này qua thành phố khác, rồi cuối cùng mới tới số tôi muốn gọi – việc này sẽ khiến kẻ nào muốn truy tìm tôi thông qua các cuộc điện thoại sẽ phải mất rất nhiều thời gian.

Các cuộc gọi của tôi không chỉ miễn phí mà còn khó truy dấu.

Buổi sáng đầu tiên ở Denver, tôi ngồi nghiên cứu tờ báo địa phương và bắt đầu khoanh tròn các quảng cáo tuyển dụng có liên quan đến máy tính. Tôi muốn tìm một công ty có sử dụng hệ điều hành yêu thích của mình, VMS.

Tôi viết các sơ yếu lý lịch khác nhau cho từng tin quảng cáo, điều chỉnh nội dung phù hợp theo các yêu cầu trình độ được liệt kê trên đó. Về nguyên tắc, tôi đã đọc tất cả các yêu cầu của họ và thiết kế sơ yếu lý lịch của mình sao cho tôi có thể đáp ứng khoảng 90% kỹ năng mà các công ty đòi hỏi. Nếu tôi ghi mình có hết thảy kỹ năng đó, hẳn là mấy người bên phòng Nhân sự hay sếp phòng IT sẽ ngạc nhiên: Nếu anh ta giỏi vậy thì việc gì phải nộp hồ sơ ứng tuyển vào công việc bậc thấp này?

Sơ yếu lý lịch của tôi chỉ gồm duy nhất một công việc từng làm, do đó tôi không cần phải thay đổi tên người giới thiệu trong các đơn. Vấn đề ở đây là

https://thuviensach.vn

phải giữ bản sao của tất cả các đơn tôi gửi đi, để nếu có người gọi phỏng vấn, tôi còn biết được mình đã viết gì trong đơn gửi cho họ. Ngoài sơ yếu lý lịch, tôi còn gửi kèm thư xin việc được viết chỉn chu nhằm giới thiệu bản thân.

Những bản sơ yếu lý lịch kèm thư xin việc giả mạo này đã thu được kết quả chỉ sau vài tuần. Tôi được mời đến phỏng vấn ở văn phòng địa phương của một công ty luật quốc tế khá nổi danh có tên là Hohme, Roberts & Owen. Công ty này có văn phòng ở Denver, Salt Lake City, Boulder, London và cả Moscow.

Mặc âu phục, đeo cà vạt và trông có vẻ hoàn toàn phù hợp với công việc ở một công ty luật đẳng cấp, tôi được đưa tới phòng hội nghị để gặp quản lý IT, một phụ nữ rất thân thiện tên là Lori Sherry.

Tôi khá giỏi trả lời phỏng vấn, nhưng lần này thì thú vị hơn nhiều bởi tôi luôn phải đấu trí để tránh bị xao nhãng: Lori thực sự rất quyến rũ. Nhưng thật không may, cô ấy đang đeo nhẫn cưới.

Lori bắt đầu bằng một câu mở đầu đúng chuẩn: “Anh hãy giới thiệu về bản thân đi.”

Tôi cố gắng tỏ ra duyên dáng và lôi cuốn, bắt chước theo phong cách của phim Ocean’s Eleven (11 tên cướp thế kỷ) mới chiếu vài năm trước. “Tôi mới chia tay bạn gái và muốn có một cuộc sống mới. Công ty cũ đã đề nghị tăng lương để giữ tôi lại nhưng tôi nghĩ sẽ tốt hơn nếu mình có một khởi đầu mới ở một thành phố khác.”

“Tại sao lại là Denver?”

“À, tôi vẫn luôn yêu thích dãy Rocky Mountains.”

Vậy đó, một lời giải thích hợp lý cho việc từ bỏ công việc cũ. Gạt mục này ra khỏi danh sách đã.

https://thuviensach.vn

Trong khoảng một giờ kế tiếp, chúng tôi lần lượt điểm qua các ý cơ bản về mục tiêu ngắn hạn và dài hạn cũng như các nội dung phỏng vấn đặc trưng khác. Cô ấy dẫn tôi đi thăm phòng máy tính, sau đó tôi phải thực hiện một bài kiểm tra viết dài khoảng bốn hay năm trang giấy để đánh giá kỹ năng quản lý hệ thống, chủ yếu là về Unix và hệ điều hành VMS. Tôi cố tình trả lời sai vài câu, cũng là để không vượt quá mức yêu cầu công việc.

Tôi nghĩ buổi phỏng vấn diễn ra tốt đẹp. Về phần người giới thiệu, tôi đã tạo ra một công ty ảo ở Las Vegas có tên là Green Valley Systems, sau đó thuê hòm thư và đăng ký dịch vụ trả lời điện thoại bằng người thật, người này được yêu cầu nhận các cuộc gọi đến và nói: "Hiện không có người trả lời cuộc gọi của bạn", sau đó đề nghị họ để lại tin nhắn. Sau khi kết thúc cuộc phỏng vấn, tôi liên tục gọi đến dịch vụ này để kiểm tra. Ngày hôm sau, có một tin nhắn dành cho tôi: Lori muốn nói chuyện với Giám đốc IT của Green Valley. Thật tuyệt!

Tôi thăm dò được một khách sạn có đại sảnh rất lớn, tạo môi trường âm thanh hệt như khu vực văn phòng và ở đây cũng có một bốt điện thoại công cộng không nhiều người sử dụng. (Tôi không liều mình gọi cho Lori từ điện thoại nhái số của mình bởi cuộc gọi đó sẽ xuất hiện trên hóa đơn thuê bao di động.) Hạ thấp giọng chừng một quãng tám và thể hiện phong cách có phần tự mãn, tôi đã nói những điều tốt đẹp về Eric Weiss.

Tôi nhận được đề nghị làm việc sau vài ngày với mức lương 28.000 đô-la – không đáng để huênh hoang nhưng cũng đủ đáp ứng nhu cầu cá nhân.

Công việc của tôi bắt đầu sau đó hai tuần. Điều này giúp tôi có đủ thời gian để tìm một căn hộ, chuyển vào đống đồ đạc đi thuê rồi tập trung vào một kế hoạch quan trọng mà tôi vẫn luôn quan tâm. Danh tính Eric Weiss của tôi hiện đã an toàn và có thể xác minh được. Tuy nhiên, vẫn có một gã Eric Weiss thực sự đang lượn lờ ở Portland với mã số An sinh, ngày sinh và học hiệu tương tự. Điều này sẽ không thành vấn đề trong một thời gian, vì gã

https://thuviensach.vn

Eric kia sống đủ xa nơi này để chúng tôi không dễ chạm mặt nhau. Nhưng tôi cần có một danh tính an toàn khác để sử dụng trong suốt cuộc đời.

19 tiểu bang, bao gồm cả California và Nam Dakota, thời đó đều cung cấp hồ sơ chứng tử "mở" – đồng nghĩa với việc các tài liệu này được công bố công khai với người dân. Các bang này không biết rằng họ đang "tạo điều kiện" cho những người như tôi. Còn có nhiều tiểu bang khác thuận tiện cho việc đăng ký hơn nhưng Nam Dakota có vẻ cách nơi này khá xa, như vậy, sẽ ít có khả năng rằng một gã nào đó đang ở trong tình huống giống tôi cũng tìm kiếm hồ sơ và quyết định chọn một hay vài danh tính khả dĩ.

Tôi cần chuẩn bị một chút trước khi bắt đầu. Điểm dừng chân đầu tiên của tôi là siêu thị King Soopers, ở đây có loại máy in mà bạn có thể nhập dòng chữ mình muốn và in ra 20 tấm danh thiếp lấy ngay chỉ với 5 đô-la. Danh thiếp mới của tôi có ghi:

ERIC WEISS

Thám tử tư

Bên dưới những dòng này là mã số hành nghề giả do Nevada cấp, một địa chỉ ảo ở Vegas và một số điện thoại văn phòng kết nối tới dịch vụ trả lời điện thoại bằng người thực, đề phòng trường hợp có ai đó muốn kiểm tra tôi. 30 đô-la một tháng là mức phí quá rẻ để tạo dựng độ tin cậy.

Nhét danh thiếp vào ví, tôi xếp vài bộ âu phục, ít quần áo và đồ dùng cá nhân vào túi xách, đặt chuyến bay tới Sioux Falls. Khi tới đây, tôi thuê xe tự lái tới thủ phủ Piere (hay "Peer" như cách người dân ở đây gọi). Tôi lái xe suốt bốn tiếng đồng hồ với chế độ tự động thẳng về hướng Tây trong ánh trời chiều, dọc theo con đường Interstate 90 với các thị trấn nhỏ nằm rải rác mà tôi chưa từng nghe tới tên. Với một gã trai thành thị như tôi, những nơi đó thật quá thôn dã: Tôi thấy mừng là mình chỉ đi qua đây.

https://thuviensach.vn

Giờ mới tới phần “khó nhằn”. Sáng hôm sau, mặc nguyên bộ âu phục từng dùng trong buổi phỏng vấn, tôi tìm đến văn phòng của Phòng Quản lý Hộ tịch, đề nghị được nói chuyện với người phụ trách. Trong vòng vài phút, người phụ trách trực tiếp bước ra quầy. Đây là việc không tưởng ở các bang lớn như New York, Texas hay Florida, nơi các viên chức cấp cao thường quá bận rộn hay lên mặt ta đây và không chịu gặp gỡ ai không hẹn trước.

Tôi giới thiệu bản thân và đưa cho cô ấy tờ danh thiếp, giải thích rằng mình là một thám tử tư đến từ Las Vegas đang điều tra một vụ án. Trong đầu tôi thoáng hiện lên một trong những chương trình truyền hình yêu thích, The Rockford Files. Tôi mỉm cười khi cô ấy xem tờ danh thiếp bởi chất lượng của nó hệt như loại mà Rockford đã chế ra nhờ máy in danh thiếp anh ta để trên xe ô tô.

Người phụ trách hộ tịch không chỉ sẵn lòng gặp tôi, cô ấy còn rất vui được hỗ trợ một thám tử tư đang làm nhiệm vụ điều tra mật liên quan đến án mạng.

“Anh cần tìm ai vậy?” cô ấy hỏi, thể hiện sự nhiệt tình. “Chúng tôi sẽ giúp anh.”

Ừm. Đây không phải là thứ tôi muốn.

“Chúng tôi muốn tìm người chết do vài nguyên nhân xác định,” tôi đánh bạo. “Tôi cần xem qua tất cả hồ sơ trong vòng vài năm gần đây.”

Dù tôi e rằng yêu cầu này có phần kỳ quặc, nhưng Nam Dakota vẫn là một nơi rất thân thiện. Người phụ trách chẳng có lý do gì để nghi ngờ, do đó, tôi sẽ nhận được mọi sự trợ giúp có thể.

Người phụ trách rất-thân-thiện đề nghị tôi đi vòng qua quầy lễ tân, tôi theo cô ấy tới một căn phòng riêng không có cửa sổ, lưu trữ những giấy chứng tử cũ trên tấm vi phim. Tôi nhấn mạnh rằng mình cần phải nghiên cứu một khối lượng lớn công việc và có lẽ phải mất tới vài ngày. Cô ấy chỉ mỉm cười

https://thuviensach.vn

và nói rằng tôi có thể sẽ bị làm phiền nếu có nhân viên nào cần dùng tấm vi phim, còn không thì chẳng vấn đề gì. Cô ấy nhờ một nhân viên ở đó chỉ cho tôi cách sử dụng tấm vi phim và làm sao để tìm phim trong khoảng năm nào đó. Như vậy, tôi sẽ làm việc ở phòng vi phim, không có ai giám sát và có thể tiếp cận toàn bộ hồ sơ sinh tử mà tiểu bang còn lưu giữ. Tôi tìm những trẻ nhỏ chết ở độ tuổi 1-3, trong giai đoạn 1965-1975. Tại sao tôi lại quan tâm tới năm sinh quá trẻ so với tuổi thực của mình? Bởi tôi có thể lấy năm sinh đó mà không ai nghi ngờ gì và nếu cảnh sát liên bang có tra tìm giấy phép lái xe được cấp gần đây theo khoảng tuổi thực của tôi ở tiểu bang họ nghi ngờ tôi đang sống, tôi hy vọng là họ sẽ bỏ qua tôi.

Tôi cũng tìm một cậu bé da trắng với tên họ có vẻ giống gốc Âu, dễ phát âm. Nếu thử dùng danh tính của trẻ gốc Ấn, Latin hay da đen thì hiển nhiên là không ổn, trừ khi tôi có một nghệ sĩ hóa trang tài giỏi bên mình mọi lúc mọi nơi.

Một vài tiểu bang bắt đầu tham chiếu chéo các hồ sơ sinh tử, có lẽ là nhằm ngăn chặn người nhập cảnh bất hợp pháp sử dụng giấy khai sinh của người đã chết. Khi nhận được yêu cầu xin cấp giấy khai sinh, việc đầu tiên họ làm sẽ là kiểm tra xem có giấy chứng tử nào gắn với người đó hay không; nếu có, họ sẽ đóng dấu là đã qua đời bằng dòng chữ in đậm lớn trên bản sao giấy khai sinh.

Như vậy, tôi cần tìm một trẻ nhỏ đã chết phù hợp với mọi tiêu chuẩn của tôi và sinh ra ở một tiểu bang khác. Thận trọng hơn một chút, tôi đoán rằng trong tương lai, các tiểu bang gần nhau sẽ bắt đầu trao đổi hồ sơ chứng tử nếu người chết được sinh ra ở bang lân cận. Đây có thể sẽ là vấn đề lớn – ví dụ, trong trường hợp tôi muốn nộp hồ sơ làm hộ chiếu dưới danh tính mới. Khi xác minh đơn đăng ký làm hộ chiếu, Bộ Ngoại giao sẽ kiểm tra hiệu lực của giấy khai sinh và có thể phát hiện ra gian lận nếu chương trình tham chiếu chéo được phát triển trong tương lai. Để tránh những rủi ro đó, tôi chỉ có thể dùng danh tính của những người sinh cách chỗ tôi ở vài tiểu bang.

https://thuviensach.vn

Tôi dành cả tuần để tìm kiếm trên các tấm vi phim. Khi có một ứng cử viên tiềm năng, tôi nhấn nút Sao chép, và một bản sao giấy chứng tử sẽ được in ra. Tại sao tôi phải cố gắng tìm được nhiều lựa chọn hết mức có thể? Chỉ để dự phòng, trong trường hợp tôi sẽ cần phải thay đổi danh tính một lần nữa.

Tất cả mọi người ở đây đều ấm áp và thân thiện hệt như người phụ trách. Có hôm, một nhân viên đến chỗ tôi và nói: “Tôi có họ hàng ở Las Vegas bị mất tích. Anh là thám tử tư nên tôi tự hỏi không biết anh có thể tìm anh ấy giúp tôi không.”

Cô ấy cho tôi mọi thông tin mình có. Đêm đó, trong phòng khách sạn, tôi chạy một chương trình tìm kiếm, sử dụng dịch vụ cơ sở dữ liệu của công ty môi giới thông tin để tìm ra địa chỉ của người họ hàng kia. Sau đó, tôi gọi tới bộ phận phân phối đường dây của công ty điện thoại địa phương để có được số điện thoại không có trong danh bạ. Chẳng mấy tốn công tốn sức. Tôi cảm thấy vui vì giúp được người phụ nữ này, vì tất cả mọi người đều rất tốt bụng và giúp đỡ tôi rất nhiều. Tôi có cảm giác như mình đã đền đáp được lòng tốt của họ.

Khi báo tin cho người nhân viên vào sáng hôm sau, cô ấy sung sướng tới mức ôm chầm lấy tôi, một phần thưởng quá lớn so với công sức ít ỏi tôi đã bỏ ra. Từ khoảnh khắc đó, các đồng nghiệp của cô thậm chí còn thân thiện với tôi hơn nữa, họ mời tôi cùng ăn bánh vòng và chia sẻ vài chuyện vặt trong cuộc sống.

Mỗi ngày làm việc, tôi lại thấy các máy in gần đó hoạt động không ngừng để in giấy chứng nhận mà mọi người yêu cầu. Máy kêu inh ỏi đến nhức óc. Sang đến ngày thứ ba, khi đứng dậy để duỗi chân tay sau vài giờ ngồi tra cứu, tôi bước tới máy in để quan sát kỹ hơn và thấy hàng chồng hộp giấy xếp cạnh đó. Phát hiện ra những thứ được xếp trong hộp khiến tôi há hốc mồm: Đó là vài trăm tờ giấy khai sinh chưa điền thông tin. Tôi có cảm giác như thể mình đã vô tình bước vào kho báu hải tặc vậy.

https://thuviensach.vn

Còn một kho báu nữa: Thiết bị dập nổi hoa văn trên giấy chứng nhận của Nam Dakota được đặt ngay trên một chiếc bàn gỗ dài ngoài phòng vi phim. Các nhân viên trong phòng chỉ việc tới đó và dập dấu vào giấy chứng nhận trước khi gửi đi.

Buổi sáng hôm sau, thời tiết xấu hơn nhiều, tuyết rơi dày và trời lạnh cóng. Thật may mắn khi tôi mang theo áo khoác dày trước khi tới Phòng Quản lý Hộ tịch. Tôi làm việc suốt buổi sáng và chờ tới giờ ăn trưa. Khi hầu hết nhân viên đã ra khỏi phòng hoặc mải ăn uống trò chuyện, tôi vắt áo khoác trên tay và đi tới nhà vệ sinh, hờ hững kiểm tra xem những nhân viên còn lại đang ở đâu, liệu họ có để ý gì tới xung quanh hay không. Trên đường quay trở lại phòng vi phim, tôi bước tới bàn gỗ đặt thiết bị dập nổi. Chỉ bằng một động tác đơn giản nhẹ nhàng mà không cần dừng bước, tôi đã vớ lấy nó, giấu dưới áo khoác và quay trở lại phòng vi phim. Bước vào phòng, tôi liếc ra ngoài cửa: Không có ai buồn chú ý tới tôi.

Với thiết bị dập nổi đang yên vị trên bàn, gần đống giấy khai sinh để trống, tôi bắt đầu dập dấu của tiểu bang lên, thật nhanh và thật khẽ. Tôi cố gắng kiểm soát nỗi sợ trong lòng, nếu ai đó bước vào và trông thấy những gì tôi đang làm, tôi biết mình sẽ bị bắt giữ và giải đi ngay lập tức.

Khoảng năm phút sau, tôi đã có một xấp chừng 50 tờ giấy khai sinh trống đã dập nổi. Tôi quay lại phòng vệ sinh, trả lại thiết bị dập nổi vào đúng vị trí như trước khi “mượn tạm”.

Sứ mệnh đã hoàn thành. Tôi đã thành công trong một nhiệm vụ nguy hiểm.

Cuối ngày, tôi nhét đống giấy khai sinh vào sổ và bước ra ngoài.

Gần hết một tuần làm việc, tôi đã có thông tin cần thiết cho vô số danh tính khác nhau. Sau đó, tôi chỉ việc viết thư đến Cục Thống kê Sinh tử tại bang mà đứa trẻ được sinh ra và yêu cầu một bản sao giấy khai sinh. Có nó trong tay, tôi sẽ trở thành một “tôi” mới. Tôi cũng có tới 50 tờ giấy khai sinh để trống, tất cả đều được dập nổi dấu của bang Nam Dakota. (Vài năm sau, khi

https://thuviensach.vn

các cảnh sát liên bang trả lại tài sản đã tịch thu, họ vô tình gửi cả tập giấy khai sinh có đóng dấu nổi của Nam Dakota. Alex Kasperavicius, người nhận đồ giúp tôi, đã trầm tư nói rằng lẽ ra họ không nên làm vậy.)

Các cán bộ ở phòng hộ tịch rất lấy làm tiếc khi thấy tôi đi: Tôi đã tạo ấn tượng tốt tới mức một vài chị em ở đó còn ôm tạm biệt khi tôi nói lời chào họ.

Cuối tuần đó, tôi lái xe quay trở lại Sioux Falls và tự chiêu đãi mình buổi học trượt tuyết đầu tiên. Thực sự tuyệt vời. Tôi có thể nghe thấy tiếng người hướng dẫn gào lên với tôi: “Gạt tuyết ra! Gạt tuyết ra!” Vốn rất hứng thú với các môn thể thao, tôi nhanh chóng chọn trượt tuyết làm một trong những hoạt động cuối tuần đều đặn của mình. Không có nhiều thành phố lớn ở Mỹ như Denver, nơi có các dốc trượt rất gần và thuận tiện đi lại bằng ô tô.

Không nhiều các bậc phụ huynh làm thẻ An sinh Xã hội cho con nhỏ. Nhưng khi một thanh niên ở độ tuổi 20 bước vào phòng An sinh Xã hội để yêu cầu cấp thẻ và nói rằng anh ta chưa từng sở hữu thẻ trước đó thì việc này rất đáng ngờ. Do vậy, tôi đặt hy vọng vào một vài cái tên có được từ đống hồ sơ ở Nam Dakota rằng bố mẹ họ đã làm thẻ An sinh cho họ rồi. Ngay khi tôi quay trở lại chỗ ở mới ở Denver, tôi gọi cho cô bạn Ann ở phòng Quản lý An sinh Xã hội và nhờ cô ấy kiểm tra vài cái tên cùng ngày tháng năm sinh tương ứng để xem liệu có thẻ nào đã được cấp chưa. Cái tên thứ ba, Brian Merrill, là một thành công: Em bé Brian đã có mã số An sinh. Tuyệt vời! Vậy là tôi đã tìm được một thân phận lâu dài.

Vẫn còn một việc phải làm. Tôi phát hiện được rất nhiều thông tin về hoạt động của FBI, dù vậy, chìa khóa để giải được vấn đề trọng tâm vẫn nằm ngoài tầm với: Gã đàn ông mà tôi biết dưới cái tên “Eric Heinz” là ai? Tên thật của hắn là gì?

Dù không hiểu nhiều về Sherlock Holmes nhưng cũng như công việc của Holmes là tập trung vào giải đố, truy bắt tội phạm và những kẻ vô lại, công

https://thuviensach.vn

việc hacking của tôi cũng vậy. Tôi cũng phải đối mặt với việc làm sáng tỏ những điều bí ẩn và vượt qua thử thách.

Cuối cùng, tôi đã nghĩ ra một hướng đi mới. Eric nắm rất rõ về vụ của Poulsen. Hắn khẳng định đã hỗ trợ Kevin Poulsen trong vài vụ đột nhập vào Pacific Bell và khoác lác rằng cả hai bọn họ đã cùng tìm ra SAS.

Tôi dành hàng giờ trên mạng, sục sạo trong các cơ sở dữ liệu pháp luật trực tuyến như Westlaw và LexisNexis để tìm ra các bài báo và tạp chí có nhắc đến Eric nhưng không đem lại kết quả khả quan. Nếu hắn thực sự làm điều đó cùng Poulsen như hắn đã nói, có lẽ tôi có thể truy tìm theo hướng ngược lại theo tên những kẻ đồng lõa cùng Poulsen.

Ơ-rê-ka! Rất nhanh chóng, tôi đã tìm ra một bài báo trên LexisNexis có nhắc đến hai đồng phạm của Poulsen, Robert Gilligan và Mark Lottor. Có lẽ một trong những gã này chính là Eric Heinz giả mạo. Tôi vồ lấy điện thoại, cố nén sự kích động khi gọi vào số điện thoại của cơ quan hành pháp ở DMV California và tra ra bằng lái xe của hai gã đồng phạm kia.

Tôi lại đâm phải ngõ cụt rồi. Một gã thì quá thấp, một gã lại quá béo để có thể là Eric.

Tôi vẫn kiên trì. Rồi đến một ngày, tôi cũng tìm được một bài báo mới xuất hiện trên Westlaw. Một tờ báo nhỏ có tên là Daily News của Los Angeles đã đăng tải câu chuyện về vụ Poulsen được đưa ra xét xử. Mẩu tin này nhắc tới hai cái tên khác bị buộc tội đồng phạm với Poulsen, Ronald Mark Austin và Justin Tanner Petersen.

Tôi khá quen thuộc với Austin và biết cậu ta trông thế nào; cậu ta chắc chắn không phải là Eric. Nhưng còn Petersen? Nuôi hy vọng trong lòng và chuẩn bị sẵn sàng để lại thất vọng một lần nữa, tôi gọi tới DMV và nhờ nhân viên ở đó mô tả hình thể của Petersen.

https://thuviensach.vn

Cô ta nói hắn ta có mái tóc và đôi mắt màu nâu, cao 1,8m và nặng chừng 66kg. Tôi vẫn luôn cho rằng tóc Eric màu vàng hoe nhưng ngoài chuyện đó thì phần mô tả hoàn toàn trùng khớp với hắn.

Cuối cùng, tôi cũng tìm ra thân phận thực sự của hắn. Giờ thì tôi đã biết tên thật của người đàn ông tự nhận là Eric Heinz. Hắn không phải là một cảnh sát liên bang mà là một kẻ chỉ điểm đang cố bẫy tôi và có thể là cả nhiều hacker khác để tự bảo vệ bản thân.

Sau bao nhiêu lo lắng và cố công suy nghĩ về con người thật của Eric, tôi đã có thể cười ngoác miệng. Tôi thấy vô cùng hưng phấn. FBI hắn rất hãnh diện về danh tiếng của mình trên khắp thế giới, nhưng họ lại chẳng thể bảo vệ cho một kẻ chỉ điểm thoát khỏi tay của một hacker đơn độc.

* * *

Sau vụ điều tra ở Nam Dakota và buổi trượt tuyết cuối tuần, đã đến lúc tôi bắt tay vào buổi làm việc đầu tiên ở hãng luật. Tôi được chỉ tới bàn làm việc ở một văn phòng bên trong phòng máy tính, gần chỗ ngồi của hai thành viên khác trong nhóm là Liz và Darren. Cả hai đều khiến tôi cảm thấy mình được chào đón, một đặc trưng của người Denver, nơi đây mọi người đều có vẻ thoải mái, cởi mở và thân thiện. Đồng nghiệp Ginger có một văn phòng riêng ở đầu bên kia phòng máy; cô ấy cũng rất thân thiện.

Tôi bắt đầu cảm thấy thoải mái với cuộc sống mới, nhưng chưa từng có giây phút nào tôi quên rằng mình có thể bị buộc phải chạy trốn một lần nữa để tránh khỏi cuộc đời cô độc bị khóa kín sau song sắt. Công việc ở hãng luật mang tới những lợi ích không ngờ. Hãng luật chiếm hết năm tầng gần đỉnh của một tòa nhà chọc trời cao tới 50 tầng được biết tới dưới cái tên Cash Register (Máy đếm tiền) bởi phần đỉnh của tòa nhà có dáng cong cong như một chiếc máy đếm tiền. Sau nhiều giờ, tôi đăng nhập vào tài khoản của Westlaw và đọc sách luật ở thư viện luật, nghiên cứu xem làm sao để thoát khỏi cơn khốn đốn mà mình đang mắc kẹt.

https://thuviensach.vn

27

MẶT TRỜI[68] LÊN

85 102 121 114 32 103 113 32 114 102 99 32 108 121 107 99 32 109 100 32 114 102 99 32 122 109 109 105 113 114 109 112 99 32 71 32 100 112 99 111 115 99 108 114 99 98 32 103 108 32 66 99 108 116 99 112 63

[68] Sun (mặt trời) trong tiêu đề gốc "Here Comes the Sun" còn mang ý ám chỉ công ty máy tính Sun. (ND)

Công việc chính của tôi ở Phòng Công nghệ Thông tin của hãng luật là "điều hành máy tính": giải quyết các vấn đề có liên quan đến máy in và tập tin máy tính, chuyển đổi tập tin từ WordPerfect sang Word và vài định dạng khác, viết lệnh để tự động hóa các thủ tục, quản trị mạng và hệ thống. Tôi được giao cho hai dự án quan trọng: kết nối Internet cho hãng (đây là lúc Internet đang bắt đầu được sử dụng rộng rãi hơn trước), cài đặt cũng như quản lý một sản phẩm có tên là SecurID, vốn cung cấp xác thực "hai bước". Người dùng được cấp phép phải cung cấp mã gồm sáu chữ số hiện trên thiết bị SecurID với mã PIN bí mật để truy cập từ xa vào hệ thống máy tính của hãng.

Một trong những nhiệm vụ ngoài dự tính – và nếu được tự phân việc cho mình thì tôi cũng không thể làm tốt hơn – là chịu trách nhiệm hỗ trợ hệ thống quản lý hóa đơn điện thoại của hãng. Điều đó có nghĩa là nghiên cứu ứng dụng kế toán điện thoại trong giờ làm. Đây là cách tôi đã học được chính xác chỗ để chèn vào các chỉ thị lập trình, biến ứng dụng này thành một hệ thống cảnh báo sớm cho tôi.

Tôi viết một chương trình nhỏ để kiểm tra bất cứ cuộc gọi đi nào của hãng luật tới một danh sách chứa các mã vùng và đầu số điện thoại. Bạn thử đoán

https://thuviensach.vn

xem danh sách của tôi gồm những gì nào? Đúng vậy: văn phòng FBI và Công tố Hoa Kỳ ở Los Angeles và Denver. Nếu có ai gọi đến bất kỳ số nào trong các cơ quan đó, chương trình nhỏ tôi viết sẽ gửi một tin nhắn đến máy nhắn tin của tôi với mã "6565" – một số rất dễ nhớ với tôi bởi đó là bốn số cuối của số điện thoại chính được gán cho văn phòng FBI ở Los Angeles.

Khi còn ở hãng luật, tôi thực sự đã nhận được mã này hai lần và cả hai lần đều dọa tôi chết khiếp. Lần nào tôi cũng phải chịu đựng cơn co thắt dạ dày trong vài phút, rồi xem số vừa gọi và tự mình gọi đến.

Cả hai cuộc gọi đều đến Phòng Công tố ở Los Angeles... nhưng là đến Ban Dân sự, không phải Ban Hình sự.

Phù!

Thời gian rảnh rỗi, tôi vẫn tiếp tục luyện tập ở YMCA mỗi ngày và tất nhiên vẫn tiếp tục bận rộn với những dự án hacking của mình. Tuy nhiên, tôi cũng dành thời gian để tận hưởng các hoạt động đa dạng ở Denver. Đài thiên văn, ngoài việc đánh thức niềm yêu thích thuở nhỏ của tôi với thiên văn học, còn có cả những buổi biểu diễn ánh sáng laze cùng nhạc rock, thường là của những nhóm nhạc tôi ưa thích như Pink Floyd, Journey và the Doors – đó là một trải nghiệm thực sự tuyệt vời.

Tôi bắt đầu ổn định cuộc sống với danh tính giả mới và trở nên cởi mở hơn. Thỉnh thoảng, tôi đến một trong những câu lạc bộ khiêu vũ địa phương chỉ để tìm người nói chuyện. Tôi gặp một cô gái và đã hẹn hò với cô ấy vài lần, nhưng tôi không nghĩ sẽ công bằng với cô ấy nếu chúng tôi tiến xa hơn: Nếu tôi bị FBI tóm được, bất cứ ai gần gũi với tôi sẽ bị đẩy vào tình huống khó xử, hoặc là bị ép đưa ra bằng chứng chống lại tôi, hoặc có thể sẽ bị buộc tội trở thành tòng phạm. Chưa kể tới khả năng tôi sẽ nói gì đó để lộ bản thân, hay cô ấy có thể thấy một vài giấy tờ xác nhận tôi dưới một cái tên khác, hay nghe lỏm một cuộc điện thoại. Tâm tình bên gối cũng có những nguy hiểm của riêng nó. Từ những lời bình phẩm của bạn tù thời tôi còn trong trại, tôi

https://thuviensach.vn

đã biết được rằng hầu hết họ đều bị tóm bởi chính nửa kia của mình. Tôi sẽ không lặp lại sai lầm đó.

Có một cửa hàng sách trong khu vực Cherry Creek của Denver tên là Tattered Cover, nơi tôi sẽ uống cà phê và đọc sách về máy tính hết cuốn này đến cuốn khác. Tôi thử tham gia vào một vài câu lạc bộ rock, nhưng ở đó chỉ có đám đông cuồng dòng nhạc heavy-metal với những gã vạm vỡ đầy xăm trổ, nên tôi cảm thấy có đôi chút lạc lõng.

Đôi lúc, tôi dành thời gian đạp xe và tận hưởng cảnh quan rực rỡ của Denver với những ngọn núi phủ tuyết đẹp say lòng người vào mùa đông. Hay ghé thăm casino tại một trong những khu bảo tồn người da đỏ để chơi xì dách.

Tôi luôn trông ngóng cuộc nói chuyện tiếp theo với mẹ, mẹ sẽ gọi từ một trong số các casino với tín hiệu đã được sắp đặt từ trước. Đôi lúc, bà cũng ở đó với mẹ. Những cuộc gọi đó rất quan trọng với tôi, chúng khiến tôi cảm thấy hạnh phúc và cho tôi sức mạnh, dù đó là nỗi bất tiện rất lớn cho gia đình tôi cũng như là rủi ro lớn với tôi nếu FBI quyết định tăng cường điều tra giám sát. Không được ở gần bà và mẹ, những người đã dồn hết tình yêu thương, sự quan tâm chăm sóc và giúp đỡ cho tôi quả là một việc rất khó khăn.

Cùng lúc đó, tôi cũng thay đổi ngoại hình và có thể cũng do bản thân sắp bước sang tuổi 30, tôi bắt đầu nuôi tóc dài, thậm chí còn để tóc ngang vai.

Tôi thích rất nhiều điều trong cuộc đời mới của mình.

Sau vài tháng ở Denver, tôi bắt đầu sẵn sàng cho chuyến về thăm gia đình, lần này tôi sử dụng dịch vụ tàu hỏa Amtrak. Mẹ và bà đến ga tàu đón tôi. Giờ đây, tóc tôi đã dài và tôi còn để ria mép, mẹ gần như không còn nhận ra tôi. Đó là một cuộc hội ngộ thú vị và tôi lại pha trò bằng các câu chuyện về công việc và những cộng sự mới ở hãng luật.

https://thuviensach.vn

Tôi cảm thấy thoải mái hơn khi về Vegas lần này, nhờ có thân phận mới Eric Weiss của mình, nhưng tôi vẫn rất đề phòng. Mẹ và tôi thường gặp nhau ở những nơi khó ngờ. Tôi leo lên xe trong một bãi đỗ xe và nằm xuống ghế sau cho đến khi bà lái xe về ga-ra tại nhà và đóng cửa lại. Mẹ quấn quýt bên tôi và làm những món tôi thích, bắt tôi ăn hết đĩa này đến đĩa khác dù mẹ bảo rất vui khi thấy tôi chỉnh tề với thân hình cân đối.

Tôi có thể nhận ra áp lực đang đặt lên vai bà ngoại, thậm chí còn nhiều hơn trên vai mẹ. Dù bà hạnh phúc và thoải mái khi được gặp tôi, thấy tôi bằng xương bằng thịt, nhưng dường nhưng việc này lại khiến bà nhận ra bà nhớ tôi và lo cho sự an toàn của tôi ở Denver nhiều đến mức nào. Tôi luôn cảm thấy trong lòng bà là sự đấu tranh giữa niềm vui trong chuyến trở về của tôi và nỗi lo sợ việc này sẽ đặt tôi vào mối nguy hiểm lớn hơn.

Trong một tuần tôi ở đó, chúng tôi đã gặp nhau khoảng chục lần.

* * *

Trở về Denver, không khí ở chỗ làm không còn được như lúc đầu sau khi sếp tôi, Lori thân thiện, rời hãng để cùng chồng điều hành công ty riêng, Rocky Mountain Snowboards. Người thay thế cô là một phụ nữ tóc đen tên là Elaine Hill, có phần nghiêm khắc. Dù khá thông minh, nhưng cô ta khiến tôi cảm thấy đây là một người toan tính và là tuýp giáo viên trường học, không phải kiểu "được lòng người khác" như Lori.

Các cộng sự của tôi trong phòng IT quá khác nhau đến mức họ như thể những nhân vật trong một vở kịch. Ginger sở hữu hàm răng to và hơi mập lùn, 31 tuổi và đã lập gia đình. Cô ấy có vẻ quý tôi và chúng tôi thỉnh thoảng lại cùng nhau bông đùa vui vẻ. Tuy nhiên, tôi không nghĩ mình nên làm gì để thể hiện hứng thú chăn gối với cô ta – và chắc chắn không nên làm gì để phải chịu những điều tiếng mà cô ấy rêu rao khắp văn phòng. Một tối muộn, khi cả hai đang ở trong phòng máy tính, cô ấy bảo tôi: "Tôi tự hỏi điều gì sẽ xảy ra nếu anh đè tôi ra chiếc bàn này và có ai đó bước vào?" Hở?

https://thuviensach.vn

Hoặc có thể những lời mời gọi đó của cô ta thực ra là để tôi mất cảnh giác, không nghi ngờ cô ta.

Hồi còn ở Los Angeles, trước khi lên đường trốn chạy, trong hội của tôi và Lewis có một gã tên là Joe McGuckin, một gã bệu với khuôn mặt tròn và bụng bự, đeo kính, râu ria lún phún, mái tóc nâu của gã rũ một phần xuống trán như mái ngố của đám con gái. Ba chúng tôi thường đi với nhau, đi ăn ở Sizzler rồi đi xem phim nhiều đến mức Lewis và tôi đặt cho gã biệt danh "Sizzler và bộ phim".

Trong một cuộc trò chuyện khi tôi đang ở Denver, Lewis bảo tôi rằng Joe đã đưa cho cậu ta tài khoản của một máy trạm Sun mà gã có ở nhà. Lewis đưa lại thông tin đăng nhập cho tôi, với một yêu cầu. Cậu ta hy vọng tôi có thể lấy được quyền root trên máy trạm của Joe rồi bảo lại cho cậu ta biết cách thâm nhập để Lewis có thể châm chọc Joe về chuyện đó. Đây có vẻ là một cơ hội thú vị cho tôi: Bởi Joe là nhân viên hợp đồng cho Sun Microsystems, nên rất có khả năng gã có quyền truy cập từ xa vào mạng của công ty và đó sẽ là cách để tôi hack vào Sun.

Mỗi khi chúng tôi nói về hacking ở Los Angeles ngày đó, Joe luôn khăng khăng rằng máy trạm của gã an toàn như Fort Knox[69]. Tôi nghĩ: Ồ, chọc hắn sẽ vui lắm đây! Niềm đam mê với những trò chơi khăm là điểm chung đã kéo Lewis và tôi lại với nhau kể từ hồi chơi khăm cửa nhận đồ ăn ở McDonald's. Tôi gọi đến số điện thoại nhà riêng của Joe để chắc rằng gã không ở đó, rồi gọi đến đường dây modem nhà hắn. Khi đăng nhập bằng tài khoản của Lewis, tôi chỉ mất vài phút để phát hiện ra Joe không cập nhật các bản vá lỗ hổng bảo mật. Thế mà cũng đòi là Fort Knox. Bằng cách khai thác một lỗ hổng trong một chương trình có tên là "rdist", tôi đã lấy được root trên hệ thống của Joe. Bắt đầu trò chơi thôi nào! Khi liệt kê các tiến trình Joe đang chạy, tôi ngạc nhiên khi thấy "crack", một chương trình phổ biến để giải mã mật khẩu, do một người tên là Alec Muffett viết. Tại sao Joe lại chạy nó nhỉ?

https://thuviensach.vn

[69] Kho lưu trữ vàng lớn nhất thế giới, nổi tiếng vì bất khả xâm phạm. (BTV)

Tôi không mất nhiều thời gian để tìm tập tin mật khẩu mà chương trình giải mã đang chạy. Tôi nhìn vào màn hình, choáng váng bởi những gì đang thấy.

Joe McGuckin, nhân viên hợp đồng của Sun Microsystems, đang giải mã mật khẩu của Nhóm Kỹ thuật của công ty.

Thật không thể tin được. Như thể đi dạo trong công viên và vớ được một túi đầy những tờ tiền 100 đô-la vậy.

Sau khi sao chép tất cả số mật khẩu đã được giải mã, cuộc đi săn tiếp theo của tôi là qua các e-mail của Joe, tìm từ khóa modem và dial-up. Trúng rồi! Tôi tìm thấy một e-mail nội bộ của Sun chứa những thông tin đang cần tìm kiếm. Một phần nội dung như sau:

Từ: kessler@sparky (Tom Kessler)

Đến: ppp-announce@comm

Tiêu đề: Máy chủ PPP mới

Máy chủ ppp mới của chúng ta (mercury) giờ đã hoạt động, nó đã sẵn sàng để các anh kiểm tra kết nối. Số điện thoại đến mercury là 415 691-9311.

Tôi cũng sao chép các tập tin mật khẩu gốc của Sun (chứa các mật khẩu được mã hóa băm) mà Joe đang trong quá trình giải mã, phòng trường hợp tôi không vào được máy của gã nữa. Trong danh sách mật khẩu đã được giải mã có cả mật khẩu Sun của chính Joe, mà tôi nhớ đại loại là “party5”. (Phần mềm giải mã cũng tìm ra được nó). Dễ như ăn kẹo.

Đêm đó, tôi định kỳ đăng nhập vào xem Joe có đang ở trên mạng và hoạt động không. Kể cả nếu gã để ý thấy có cuộc gọi đến trên modem, nó cũng sẽ không khiến gã nghi ngờ (tôi hy vọng là thế), bởi gã sẽ nhớ ra là đã cho Lewis quyền truy cập. Sau nửa đêm, máy tính của Joe không còn động tĩnh

https://thuviensach.vn

gì, tôi nghĩ gã đã ngủ. Sử dụng giao thức "Point-to-Point"[70], tôi đăng nhập vào máy chủ "mercury" của Sun, đóng giả là máy trạm của Joe, lấy tên là "oilean". Ố ồ! Giờ máy tính của tôi đã chính thức trở thành máy chủ trên mạng toàn cầu của Sun!

[70] Trong mạng máy tính, Point-to-Point (hay còn viết tắt là PPP) là giao thức liên kết dữ liệu, thường được dùng để thiết lập một kết nối trực tiếp giữa hai nút mạng. Nó có thể cung cấp kết nối xác thực, mã hóa việc truyền dữ liệu... (BTV, theo Wikipedia)

Trong vòng vài phút, với sự trợ giúp của rdist, tôi đã lấy được root, bởi Sun, cũng như Joe, đã không tuân thủ việc cập nhật các bản vá lỗ hổng bảo mật. Tôi thiết lập một tài khoản "shell" và cài đặt một cửa hậu đơn giản cho phép tôi có quyền truy cập root trong tương lai.

Từ đây, tôi nhắm vào Nhóm Kỹ thuật. Đây là hành động hết sức quen thuộc, nhưng đồng thời cũng hết sức thú vị. Tôi có thể đăng nhập vào hầu hết các máy Sun trong Nhóm Kỹ thuật nhờ công sức giải mã mật khẩu của Joe.

Và thế là Joe đã giúp tôi đào được một kho báu khác mà tôi cũng không hề hay biết: phiên bản mới nhất và tân tiến nhất của SunOS, biến thể của hệ điều hành Unix do Sun Microsystems phát triển cho các hệ thống máy chủ và máy trạm của họ. Tìm ra máy chủ chứa mã nguồn SunOS không khó. Tuy nhiên, ngay cả khi đã nén lại, đây vẫn là một gói dữ liệu khổng lồ – tuy không đồ sộ như hệ điều hành VMS của DEC, nhưng vẫn đủ lớn để khiến tôi nản chí.

Sau đó, tôi có một ý tưởng có thể giúp chuyển dữ liệu dễ dàng hơn. Nhắm vào văn phòng của Sun ở El Segundo, ngay phía nam Sân bay Quốc tế Los Angeles, tôi bắt đầu thực hiện truy vấn đến nhiều máy trạm để xem các thiết bị đang được gắn vào chúng. Tôi tìm người dùng có ổ đĩa gắn vào máy. Tìm được người rồi, tôi gọi cho anh ta và nói rằng mình thuộc Nhóm Kỹ thuật Sun ở Mountain View. "Tôi biết anh có một ổ đĩa kết nối với máy trạm của

https://thuviensach.vn

mình,” tôi nói. “Một trong các kỹ sư của tôi đang ở chỗ khách hàng tại Los Angeles và tôi cần chuyển một số tập tin cho anh ta, nhưng chúng khá lớn để chuyển qua modem. Anh có đĩa trắng nào có thể cho vào ổ, để tôi có thể ghi dữ liệu vào đó không?”

Anh ta để tôi đợi máy trong khi tìm một chiếc đĩa trắng. Sau vài phút, anh ta quay lại ống nghe và nói đã cho nó vào ổ. Tôi mã hóa mã nguồn được nén thành một tệp dữ liệu vô nghĩa, đề phòng trường hợp anh ta tò mò nhòm ngó. Tôi chuyển bản copy đến máy trạm của anh ta và nhập vào lệnh thứ hai để ghi nó ra đĩa.

Khi việc truyền dữ liệu đến chiếc đĩa cuối cùng đã xong, tôi gọi lại cho anh ta. Tôi hỏi liệu anh ta có muốn tôi gửi một chiếc đĩa thay thế không, nhưng đúng như tôi dự đoán, anh ta nói không cần. Tôi nói: “Anh có thể cho nó vào phong bì hộ tôi và điền tên ‘Tom Warren’ được không? Anh có ở văn phòng trong vài ngày tới không?”

Anh ta liệt kê thời gian tại văn phòng của mình. Tôi ngắt lời: “Này, có cách khác dễ dàng hơn. Anh có thể để nó ở quầy lễ tân và tôi sẽ bảo Tom đến hỏi cô ta?” Tất nhiên, anh ta rất vui lòng làm vậy.

Tôi gọi cho Alex và hỏi xem liệu anh có thể lượn qua văn phòng của Sun và lấy phong bì mà nhân viên lễ tân đang giữ cho “Tom Warren” được không. Alex hơi lưỡng lự, hiểu rằng luôn có rủi ro. Nhưng một lúc sau, anh đã vượt qua nỗi e ngại và đồng ý bằng giọng vui vẻ – tôi đoán là Alex vẫn nhớ cảm xúc khi tham gia những chuyến phiêu lưu hacking cùng tôi.

Tôi đắc thắng. Nhưng đây mới là phần lạ lùng: Khi có được chiếc đĩa, tôi thậm chí còn không dành nhiều thời gian nhìn lại chỗ mã nguồn đó. Tôi đã thành công trong việc thử thách chính mình và bản thân mã nguồn đó không thú vị bằng chiến tích kia.

Tôi tiếp tục lấy được mật khẩu và kho báu phần mềm của Sun, nhưng liên tục phải kết nối đến các modem ở Mountain View cũng tiềm ẩn rất nhiều rủi

https://thuviensach.vn

ro. Tôi muốn có một điểm truy cập khác vào mạng của Sun.

Đã đến lúc tấn công bằng kỹ thuật xã hội. Sử dụng điện thoại nhái số của mình, tôi lập trình một số với mã vùng 408 của Mountain View, tôi sẽ cần đến nó nếu quản trị hệ thống ở đại lý bán hàng tại Denver của Sun muốn gọi lại cho tôi để xác minh xem tôi có phải là người mà mình đang tự nhận không. Sử dụng một công cụ có sẵn cho tất cả nhân viên Sun, tôi lấy danh sách các nhân viên, chọn ngẫu nhiên cái tên Neil Hansen, viết ra tên, số điện thoại, số tòa nhà và số nhân viên của anh ta. Sau đó, tôi gọi đến số máy chính ở đại lý bán hàng tại Denver của Sun và yêu cầu gặp người hỗ trợ máy tính.

“Xin chào, tôi là Neil Hansen ở Sun Mountain View. Xin hỏi ai đang ở đầu dây vậy?” tôi hỏi.

“Tôi là Scott Lyons, nhân viên hỗ trợ ở văn phòng Denver.”

“Tốt quá. Cuối ngày hôm nay tôi sẽ bay đến Denver để dự vài cuộc họp. Tôi đang băn khoăn không biết các anh có một số dial-up nội bộ nào để tôi có thể truy cập e-mail của mình mà không phải thực hiện các cuộc gọi từ xa về Mountain View không.”

“Tất nhiên, chúng tôi có số dial-up, nhưng tôi phải lập trình nó để kết nối lại cho anh. Hệ thống phải làm vậy vì lý do bảo mật,” anh ta bảo tôi.

“Không vấn đề gì,” tôi nói. “Khách sạn Brown Palace có các số kết nối trực tiếp cho phòng của khách. Khi tôi đến Denver tối nay, tôi sẽ cho anh số.”

“Tên anh là gì nhỉ?” anh ta hỏi tôi, giọng có vẻ nghi ngờ.

“Tôi là Neil Hansen.”

“Số nhân viên của anh là gì?” anh ta yêu cầu.

“10322.”

https://thuviensach.vn

Anh ta để tôi đợi một lúc, có vẻ là để kiểm tra. Tôi biết anh ta sẽ dùng chung công cụ mà tôi đã dùng để lấy thông tin của Hansen.

“Xin lỗi, Neil, tôi vừa phải xác minh anh trong cơ sở dữ liệu nhân viên. Khi nào anh đến thì gọi cho tôi, tôi sẽ cài đặt nó cho anh.”

Tôi đợi đến lúc sắp hết giờ làm, gọi lại cho Scott và đưa anh ta số địa phương 303 (Denver) mà tôi đã nhái lại trong di động của mình. Khi tôi bắt đầu kết nối, di động sẽ nhận được một cuộc gọi lại, tôi sẽ trả lời cuộc gọi đó, rồi modem của tôi sẽ tạo kết nối. Trong vài ngày, tôi dùng điểm truy cập này để vào mạng nội bộ của Sun.

Nhưng rồi đột nhiên các cuộc gọi lại đều không hoạt động nữa. Chết tiệt! Chuyện gì đã xảy ra vậy?

Tôi kết nối lại vào Mountain View và truy cập vào hệ thống ở Denver. Ôi, chết tiệt! Scott đã gửi một e-mail khẩn cấp đến Brad Powell ở Phòng An ninh của Sun. Anh ta đã khởi chạy tính năng ghi chép trong dial-up tôi sử dụng và thu lại tất cả dữ liệu trao đổi trong phiên kết nối của tôi. Scott đã nhanh chóng phát hiện ra tôi không kiểm tra thư của mình mà đi nhòm ngó lung tung những nơi không được phép. Tôi xóa tất cả tập tin ghi chép đó để không còn bằng chứng gì về những cuộc viếng thăm của tôi và ngay lập tức ngừng sử dụng số điện thoại mà tôi đã cung cấp cho anh ta.

Việc này có khiến tôi nản chí ngừng hack vào Sun không? Tất nhiên là không. Tôi quay lại dùng dial-up Mountain View của Sun và tìm thêm nhiều kết nối vào SWAN (Sun’s Wide-Area Network – Mạng lưới khu vực rộng của Sun) phòng trường hợp tôi bị hất ra khỏi hệ thống. Tôi nhắm vào tất cả các đại lý bán hàng của Sun trên toàn nước Mỹ và Canada, bởi đại lý nào cũng đều có kết nối dial-up nội bộ riêng để nhân viên có thể truy cập vào SWAN mà không cần thực hiện các cuộc gọi đường dài về trụ sở công ty ở Mountain View.

https://thuviensach.vn

Trong khi khám phá mạng lưới của Sun, tôi tình cờ gặp một máy chủ có tên là “elmer” có chứa toàn bộ cơ sở dữ liệu về lỗi tập hợp từ mọi hệ điều hành của Sun. Mỗi ghi chép lại bao gồm mọi thứ từ báo cáo hay lần đầu phát hiện lỗi, tên của kỹ sư được giao giải quyết vấn đề, cho đến các mã nguồn mới cụ thể để giải quyết vấn đề.

Một bản báo cáo lỗi điển hình sẽ có dạng như sau:

Tóm tắt: syslog có thể được dùng để ghi đè bất cứ tập tin hệ thống nào.

Từ khóa: bảo mật, mật khẩu, syslog, ghi đè, hệ thống.

Mức nghiêm trọng: 1

Ưu tiên: 1

Quản lý chịu trách nhiệm: kwd

Mô tả:

Tính năng syslog và syslogd của LOG_USER có thể được dùng để ghi đè *bất kỳ* tập tin hệ thống nào. Vi phạm bảo mật rõ ràng là dùng syslog để ghi đè /etc/passwd. Việc này có thể được thực hiện bằng các hệ thống từ xa nếu LOGHOST không được đặt là localhost.

Bpowell: đoạn mã bị lỗi đã được xóa vì lý do bảo mật

Nếu cần bản ghi chép của đoạn mã bị lỗi hãy liên hệ Staci Way (nhân viên hợp đồng) (staciw@castello.corp)

Khắc phục tạm thời: KHÔNG CÓ, ngoại trừ việc tắt syslog vốn không thể chấp nhận được.

Danh sách quan tâm: brad.powell@corp, dan.farmer@corp, mark.graff@corp

https://thuviensach.vn

Bình luận: lỗi này khá nghiêm trọng. Nó đã được sử dụng trong sun-barr để bẻ khóa root và là một trong số ít lỗi bảo mật hoạt động trên 4.1.X cũng như 2.X, hay nói cách khác là BẤT KỲ phiên bản OS nào được phát hành.

Việc này giống như thể tìm thấy Chén thánh một lần nữa vậy. Giờ đây, tôi đã có thể truy cập đến tất cả mọi lỗi được phát hiện trong nội bộ Sun cũng như báo cáo của mọi người từ bất kỳ nguồn nào. Nó giống như việc cho một đồng 25 xu vào máy xèng và trúng lớn lũy tiến ngay từ lần giật cần đầu tiên vậy. Thông tin từ cơ sở dữ liệu này sẽ đi vào túi khôn của tôi. Tôi bắt đầu nghĩ đến giai điệu trong một bản nhạc phim cũ của Felix the Cat (Chú mèo Felix): "Mỗi lần rơi vào tình thế khó khăn, chú lại cho tay vào túi khôn."

Sau khi viên quản trị hệ thống Sun ở Denver báo cáo sự việc, công ty hiểu ra rằng có một con quỷ nhỏ đang đào sâu vào hệ thống của họ. Dan Farmers và Brad Powell, hai người đứng đầu bộ phận an ninh của Sun, đã gửi email tới toàn công ty cảnh báo các nhân viên cẩn thận với các cuộc tấn công của hacker có dùng kỹ thuật xã hội. Sau đó, họ bắt đầu chuyển các thông báo lỗi ra khỏi cơ sở dữ liệu với hy vọng giấu được tôi. Nhưng tôi vẫn đang đọc e-mail nội bộ của họ đây. Rất nhiều thông báo lỗi chứa những câu hệt như trong đoạn tin bên trên – các bạn có để ý thấy không?

Nếu cần bản sao đoạn mã bị lỗi hãy liên hệ Staci Way (nhân viên hợp đồng) (staciw@castello.corp).

Hẳn bạn biết tôi sẽ làm gì khi thấy một tin nhắn như vậy.

Phải, tôi sẽ gửi e-mail cho Staci từ một tài khoản nội bộ của Sun và tấn công cô ta bằng kỹ thuật xã hội để lấy được lỗi. Tôi chưa bao giờ thất bại, chưa một lần.

Bất chấp những thành công của tôi trong việc hacking vào công ty, một năm sau đó, Powell đã nhận được "giải công trạng" từ Giám đốc Thông tin của Sun "vì vai trò của anh trong công tác bảo đảm an ninh cho Sun và ngăn cản các vụ tấn công trên SWAN của Kevin Mitnick". Powell rất tự hào về giải

https://thuviensach.vn

thường này đến mức anh ta đã liệt kê nó trong sơ yếu lý lịch của mình, mà tôi đã khám phá ra trên Internet.

Sau khoảng sáu tháng di chuyển ngày đêm trên xe buýt đến chỗ làm, thì việc chuyển đến gần chỗ làm hơn có vẻ là một ý tưởng hay với tôi. Tôi muốn ở đủ gần để đi bộ đến chỗ làm mỗi sáng nhưng phải loanh quanh trong khu vực đi bộ của đường 16th Mall tại trung tâm thành phố Denver, địa điểm vui chơi ưa thích của tôi vào cuối tuần. Tòa căn hộ kiểu cũ, Grosvenor Arms, trên đường East 16th, có một căn trống trên tầng năm mà tôi đã rất hào hứng khi tìm ra – một nơi rất hay ho, rộng rãi, có nhiều cửa sổ và cả những chiếc hộp kiểu cũ nơi người giao sữa thường để sữa vào mỗi sáng. Lần này, tôi lại bị kiểm tra tín dụng, nhưng không sao, bằng cách hack vào cơ quan báo cáo tín dụng TRW, tôi có thể xác định được vài Eric Weiss với khoản tín dụng đủ tốt. Tôi điền số An sinh Xã hội của một trong số họ trong đơn xin thuê nhà (khác với số tôi dùng để đi làm). Giấy tờ của tôi được thông mà không gặp chút trở ngại nào.

Khu du lịch của Denver cách căn hộ mới của tôi chỉ khoảng năm dãy nhà với rất nhiều quán bar và nhà hàng tuyệt vời. Một trong số đó là quán ưa thích của tôi, một nhà hàng Mexico trên đường 16th cắt đường Larimer, nơi tụ tập của rất nhiều cô nàng xinh đẹp. Tôi vẫn tránh các mối quan hệ nghiêm túc, nhưng trò chuyện tán tỉnh với những cô gái trẻ hấp dẫn ở quán bar không đi quá giới hạn cảnh giác của tôi giúp tôi cảm thấy mình giống như một con người. Đôi khi, một cô nàng sẽ ngồi xuống cạnh tôi và cho phép tôi mời nàng một vài ly... hay thậm chí là nàng mời tôi. Thật tuyệt!

Có rất nhiều nhà hàng xung quanh với những nét hấp dẫn riêng biệt: Hầu như bữa nào tôi cũng ăn ngoài, ít khi tự nấu dù chỉ là ngũ cốc hay thịt xông khói và trứng.

Ổn định trong căn hộ mới giúp tôi cảm thấy dễ chịu hơn với cuộc sống ở Denver, nhưng tôi biết mình không thể mất cảnh giác. Nắm trong tay toàn quyền truy cập vào PacTel Cellular, tôi vẫn tiếp tục theo dõi các cuộc gọi di

https://thuviensach.vn

động mà các đặc vụ FBI gọi đến cho Justin Petersen, hay còn gọi là Eric Heinz và cũng theo dõi xem liệu họ có đang thực hiện bất cứ cuộc gọi nào đến các số ở Denver không. Tôi thực hiện một cuộc kiểm tra đến số máy bàn của Justin ở nơi trú ẩn và phát hiện ra dịch vụ đường dài của hắn, MCI, vẫn dùng tên Joseph Wernle – nghĩa là hắn vẫn đang được FBI trả tiền. Lần mách lẻo của Justin đã không giúp FBI bắt được tôi, nhưng rõ ràng họ vẫn giám sát hắn thường xuyên. Tôi tự hỏi giờ hắn đang nhắm đến và cố tóm được hacker nào khi tôi ở ngoài tầm với.

Một ngày nọ, khi làm việc trong phòng máy tính với Darren và Liz, tôi để ý thấy Darren xoay máy tính để không ai có thể nhìn xem hắn đang làm gì, đương nhiên điều này khiến tôi rất nghi ngờ. Tôi khởi động một chương trình "Theo dõi"; đặt tên rất hợp lý, cho phép tôi theo dõi mọi thứ trên màn hình của hắn.

Tôi không dám tin vào mắt mình. Hắn đang vào thư mục Nhân sự của hãng luật và lôi ra tập tin bảng lương, hiển thị lương và thưởng của các luật sư, trợ lý, nhân viên hỗ trợ, lễ tân và nhân viên IT, cũng như các nhân viên khác của hãng, từ cộng sự kiếm được nhiều nhất cho đến người được trả lương thấp nhất.

Hắn cuộn xuống đến mục ghi:

WEISS, ERIC Comp Oper MIS $28,000.00 04/29/93

Hắn thật cả gan dám nhìn trộm lương của tôi! Nhưng tôi khó có thể phàn nàn: Tôi biết hắn đang theo dõi tôi chỉ bởi tôi cũng đang theo dõi hắn!

https://thuviensach.vn

28
SĂN LÙNG CHIẾN TÍCH

Phtm zvvvkci sw mhx Fmtvr VOX Ycmrt Emki vqimgv vowx hzh L cgf Ecbst ysi?

Tôi bắt đầu quen thuộc với lịch trình thường nhật ở Denver. Tôi làm việc ở hãng luật từ 9 giờ sáng đến 6 giờ tối. Sau đó, tôi dành vài giờ ở phòng gym, ăn tối ở một nhà hàng địa phương rồi về nhà hoặc quay trở lại công ty. Tới giờ đi ngủ, tôi làm gì hẳn các bạn cũng đoán được.

Hacking là thú vui của tôi. Bạn có thể nói rằng đây là một phương thức để tôi trốn tránh hiện thực luân phiên[71] – giống như chơi trò chơi điện tử vậy. Nhưng để chơi trò chơi mà tôi đã chọn, bạn phải luôn cảnh giác. Chỉ một chút xao nhãng hay một sai lầm tùy tiện nào đó, cảnh sát liên bang có thể sẽ xuất hiện ngay trước cửa nhà bạn. Không phải là dạng mô phỏng kiểu G-men[72], cũng không phải là những pháp sư hắc ám trong Dungeons and Dragon[73], mà là những tay cớm hàng thật giá thật, những kẻ sẽ khóa-bạn-lại-và-ném-phắt-chìa-đi.

[71] Hiện thực luân phiên (Alternate reality): Những trò chơi điện tử buộc người chơi phải liên tục sống trong cả thế giới thật lẫn môi trường số. (ND)

[72] Tên của một nhân vật trong loạt game Half-Life. G-man là nhân vật bí ẩn nhất trong game, mọi danh tính và hành động của ông ta đều không thể giải thích nổi. (BTV)

[73] Tên của một trò chơi nhập vai kỳ ảo. (BTV)

https://thuviensach.vn

Lúc này, tôi đang dành nhiều thời gian để tìm hiểu hệ thống mới nhằm tìm kiếm các phương thức đấu trí với những chuyên gia bảo mật, quản trị viên mạng lưới và hệ thống cũng như các tay lập trình viên tài giỏi mà tôi gặp trong hiện thực luân phiên. Tôi làm vậy đơn thuần chỉ vì niềm vui sướng.

Không có ai cùng tôi chia sẻ thành công, tôi dồn tâm trí vào việc thu thập mã nguồn cho những gì mình thực sự hứng thú, ví dụ như hệ điều hành và điện thoại di động. Các mã nguồn có được sẽ là chiến tích của tôi. Tôi dần trở nên thành thạo tới mức đôi khi mọi chuyện thật quá dễ dàng.

Giờ đây, khi đã hoàn toàn cắt đứt liên hệ với cuộc sống cũ, tôi không còn gì để mất. Tôi đã sẵn sàng. Làm sao để chơi lớn hơn nữa đây? Tôi phải làm gì để những cuộc hacking trong quá khứ chỉ còn là mấy trò trẻ con?

Các công ty công nghệ hàng đầu thường có hệ thống bảo mật tốt nhất thế giới. Nếu tôi thực sự muốn đạt được chiến tích gì đó có ý nghĩa, tôi cần phải thử tấn công vào đây và có được mã nguồn của họ.

Tôi đã khá thành công với Sun. Giờ tôi sẽ nhắm tới Novell, công ty mà tôi phát hiện có dùng máy chủ chạy hệ điều hành SunOS làm gateway[74] tường lửa của họ. Tôi tận dụng một lỗi trong chương trình gọi là “sendmail” do chương trình này thường được dùng để nhận e-mail từ bên ngoài. Mục tiêu của tôi là lấy được mã nguồn của một trong những hệ điều hành mạng lưới hàng đầu thế giới, NetWare của Novell.

[74] Gateway: Thiết bị cho phép chuyển đổi tín hiệu giữa các mạng với nhau. Qua gateway, các máy tính trong các mạng sử dụng các giao thức khác nhau có thể dễ dàng “nói chuyện” được với nhau. (BTV).

Tôi có thể tạo bất kỳ tập tin nào với nội dung mong muốn nhờ tận dụng lỗi bảo mật chưa vá trong chương trình sendmail. Qua hệ thống, tôi kết nối với chương trình sendmail và gõ vào vài dòng lệnh kiểu như sau:

mail from: bin rcpt to: /bin/.rhosts

https://thuviensach.vn

[text omitted]

mail from: bin rcpt to: /bin/.rhosts

data + +

Quit

Những dòng lệnh này chỉ thị chương trình sendmail tạo một tập tin ".rhosts" (đọc là dot-R-hosts"), cho phép đăng nhập mà không cần mật khẩu.

(Dành cho độc giả có kiến thức chuyên ngành: Tôi có thể tạo ra một tập tin .rhosts trong tài khoản bin nhằm cho phép mình đăng nhập mà không cần nhập mật khẩu. Tệp .rhosts là tệp cấu hình dùng kèm các chương trình hệ thống cũ nhất định gọi là "R-services", được dùng để đăng nhập hay chạy lệnh từ xa. Ví dụ, tệp .rhosts có thể được cài đặt để cho phép người dùng "kevin" từ máy có hostname "condor" đăng nhập mà không cần cung cấp mật khẩu. Trong ví dụ kể trên, hai dấu cộng cách nhau một dấu cách tạo thành ký tự đại diện cho cả user và hostname – tức là bất kỳ user nào cũng có thể đăng nhập vào tài khoản và chạy lệnh. Bởi tài khoản bin có quyền chỉnh sửa trong thư mục "/etc", nên tôi có thể thay thế mật khẩu của tập tin bằng mật khẩu của riêng mình, cho phép tôi chiếm quyền quản trị root access.)

Kế tiếp, tôi cài một phiên bản bị hack của "telnetd" có nhiệm vụ thu thập và lưu giữ mật khẩu của bất kỳ ai đăng nhập vào thiết bị gateway. Khi đã yên vị trong mạng lưới của Novell, tôi thấy có hai user khác cũng đăng nhập và đang hoạt động. Nếu họ vô tình phát hiện ra có người đăng nhập vào hệ thống từ xa, họ sẽ ngay lập tức biết rằng công ty mình đã bị tấn công. Do đó, tôi cần thực hiện thêm vài bước để ẩn thân: Nếu bất kỳ quản trị viên hệ thống nào mở danh sách người dùng hiện đang có mặt trên hệ thống, họ sẽ không thấy tên tôi.

https://thuviensach.vn

Tôi tiếp tục quan sát cho tới khi một trong những quản trị viên đăng nhập vào gateway; lúc này tôi có thể lấy được mật khẩu của anh ta cho tài khoản quản trị toàn quyền. Mật khẩu là “4kids=$$”. Thật dễ thương!

Không mất quá nhiều thời gian để đột nhập vào một hệ thống khác gọi là “ithaca”, một trong những hệ thống của Nhóm Kỹ thuật ở Sandy, Utah. Một khi tấn công được vào hệ thống này, tôi có thể thu được tập tin mã hóa chứa mật khẩu của toàn bộ Nhóm Kỹ thuật và khôi phục được một lượng lớn các mật khẩu của user thông thường.

Tôi tìm kiếm trong e-mail của các quản trị viên hệ thống theo từ khóa “modem”, “dial-up” và “dial-in” ở các dạng khác nhau – số nhiều, số ít, có và không có dấu gạch ngang ở sau chữ “dial”, v.v... Nhờ vậy, tôi đã tìm được các tin nhắn trả lời câu hỏi của nhân viên công ty kiểu như: “Tôi cần gọi theo số nào để kết nối?” Rất thuận tiện.

Sau khi tìm ra số điện thoại, tôi dùng nó làm điểm truy nhập thay vì kết nối qua Internet gateway của Novell như trước.

Để bắt đầu, tôi muốn tìm hệ thống có chứa mã nguồn của hệ điều hành NetWare. Tôi bắt đầu tìm trong hòm thư lưu trữ của các nhà phát triển, tra những cụm từ có thể giúp tôi tìm được quy trình cập nhật thay đổi lên kho mã nguồn. Cuối cùng, tôi tìm ra một hostname của kho lưu trữ mã nguồn: “ATM”. Đây đương nhiên không phải là một máy rút tiền, nhưng với tôi nó đáng giá hơn thế. Tôi quay lại tìm kiếm trong hòm thư bằng từ khóa “ATM” và tìm ra tên của vài nhân viên hỗ trợ hệ thống.

Tôi dành ra hàng giờ cố gắng đăng nhập vào ATM bằng các tài khoản đã hack được trên Unix nhưng đều không thành công. Cuối cùng, tôi tìm được một tài khoản hợp lệ, nhưng lại không có quyền truy cập vào kho lưu trữ mã nguồn. Đã đến lúc dùng tới đòn tấn công bằng kỹ thuật xã hội. Tôi gọi tới số của một phụ nữ làm công việc hỗ trợ trên ATM. Giả danh là tay kỹ sư mà tôi đã ăn trộm được mật khẩu, tôi nói với cô ta rằng mình đang thực hiện một

https://thuviensach.vn

dự án và cần quyền truy cập vào mã nguồn khách hàng Netware 3.12. Tôi linh cảm có điều gì đó không ổn nhưng người phụ nữ này lại không có vẻ gì nghi ngại.

Khi cô ta nhấc máy lên lần nữa và nói rằng tôi đã có đủ quyền truy cập mình yêu cầu, tôi cảm thấy dòng adrenaline quen thuộc lại trào dâng. Nhưng chỉ sau 15 phút, tôi đã bị ngắt kết nối và không thể kết nối lại – tôi bị đá văng ra ngoài. Vài phút sau, tay kỹ sư kia thay đổi mật khẩu. Không mất nhiều thời gian để hiểu được lý do tại sao. Sau này tôi mới biết người phụ nữ đó đã từng nói chuyện với tay kỹ sư mà tôi mượn tên và nhận ra giọng tôi không hề giống. Cô ta biết tôi là kẻ mạo danh.

Chết tiệt! Cái được cái mất.

Tôi lại gọi cho một quản trị viên khác cũng hỗ trợ ATM và thuyết phục anh ta cho tôi quyền đăng nhập vào một trong những tài khoản khác mà tôi chiếm được, để rồi tôi lại bị khóa trái một lần nữa. Tôi cài thêm phần mềm gián điệp trên nhiều hệ thống để ăn cắp các tài khoản đã đăng nhập.

Tính tới thời điểm này, tôi đã mất vài ngày cho phi vụ này. Tìm kiếm e-mail là cách nhanh chóng nhất để khám phá ra nguồn thông tin hấp dẫn, cho tôi biết cách đăng nhập vào hệ thống, các lỗi phần mềm hay các mã nguồn tôi yêu thích.

Giờ thì tôi biết họ đang giám sát hệ thống gắt gao và sẽ không đời nào để bị lừa một lần nữa, vậy nên tôi thay đổi chiến thuật. Nếu nhắm vào một nhà phát triển có toàn quyền đăng nhập và lừa anh ta sao chép mọi thứ cho mình thì sao? Tôi thậm chí còn chẳng tìm cách đăng nhập vào ATM để có được những gì mình muốn nữa.

Sau khi tìm hiểu hệ thống nội bộ của Novell trong vài ngày, tôi phát hiện ra một công cụ thú vị mà bất kỳ nhân viên Novell nào cũng có thể sử dụng. Đó là chương trình “411”, liệt kê toàn bộ tên, số điện thoại, tên đăng nhập và phòng ban của từng nhân viên. Vận may đã tới. Tôi chuyển toàn bộ danh

https://thuviensach.vn

sách nhân viên vào một tập tin để phân tích. Nhìn lướt qua danh sách, rõ ràng là tất cả các nhà phát triển đều làm việc trong một nhóm gọi là “ENG SFT”. Các dự án phát triển Netware thường được giao cho trụ sở chính của công ty ở Provo, Utah.

Tìm kiếm trong thư mục theo hai điều kiện này, tôi lấy ngẫu nhiên một cái tên:

Nevarez, Art:801 429-3172:anevarez:ENG SFT

Có mục tiêu trước mắt rồi, giờ tôi cần phải giả danh một nhân viên chính thức của Novell. Tôi muốn chọn một nhân viên hợp đồng hay ai đó mà đối tượng của tôi khó có thể quen biết. Trong danh bạ có bộ phận Univel, có lẽ được thành lập khi Novell và Phòng Nghiên cứu Hệ thống Unix của AT&T bắt đầu liên doanh vào năm 1991. Thêm nữa, tôi cần phải tìm một nhân viên hiện không làm việc tại văn phòng. Lựa chọn đầu tiên của tôi là:

Nault, Gabe:801 568-8726:gabe:UNIVEL

Tôi gọi tới văn phòng và nghe lời chào của hộp thư thoại, thông báo rằng anh ta sẽ không có mặt ở công ty trong vài ngày tới, không thể sử dụng e-mail và hộp thư thoại. Từ danh mục nhân viên, tôi chọn ra một người phụ nữ làm việc ở Phòng Viễn thông và quay số gọi cho cô ta:

“Xin chào Karen,” tôi nói. “Tôi là Gabe Nault gọi từ Midvale. Tối qua, tôi thay đổi mật khẩu hộp thư thoại mà không được. Cô có thể reset nó được không?”

“Được. Số của anh là gì?” Tôi cho cô ta số của Gabe.

“Được rồi, mật khẩu mới của anh là 5 số cuối điện thoại nhé.”

Tôi lịch sự cảm ơn cô ta, sau đó quay số gọi cho Gabe ngay lập tức, nhập mã mật khẩu mới và ghi âm giọng chào mới bằng giọng của mình, thêm vào

https://thuviensach.vn

một đoạn. “Tôi có vài cuộc gọi hôm nay, nên tốt nhất là bạn hãy vui lòng để lại tin nhắn thoại. Xin cảm ơn.” Giờ thì tôi đã là một nhân viên hợp lệ với số điện thoại nội bộ của riêng mình.

Tôi gọi cho Art Nevarez, nói với anh ta rằng tôi là Gabe Nault ở Phòng Kỹ thuật và hỏi: “Anh có làm trên NetWare không? Tôi ở Univel.”

“Có,” anh ta đáp.

“Tốt quá. Anh có thể giúp tôi được không? Tôi đang dùng NetWare cho một dự án Unix và tôi cần chuyển bản sao mã nguồn khách hàng NetWare 3.12 tới đây, ở Sandy. Tôi sẽ lập một tài khoản của anh trên máy chủ ‘enchilada’ để anh có thể chuyển mã giúp tôi nhé.”

“Được. Số của anh là gì? Tôi sẽ gọi khi xong việc,” anh ta nói.

Sau khi dập máy, tôi thấy vô cùng phấn chấn. Không cần phải chiếm quyền đăng nhập vào ATM – chỉ cần thuyết phục ai đó có quyền là được.

Tôi tới phòng gym, kiểm tra hộp thư thoại của Gabe lúc nghỉ giải lao và phát hiện ra một tin nhắn từ Art nói rằng anh ta đã làm xong. Tuyệt vời! Giờ thì tôi đã có được sự tín nhiệm, tại sao không đi xa hơn một chút để nhờ thêm một sự hỗ trợ nhỏ nữa? Tôi gọi lại cho Nevarez ngay tại phòng tập và nói: “Cảm ơn anh, Art. À xin lỗi, nhưng tôi mới phát hiện ra mình cần cả client utility 4.0 nữa.”

Anh ta có vẻ hơi khó chịu: “Có rất nhiều tập tin trên máy chủ đó, không còn chỗ chứa nữa.”

“À được, để tôi chuyển chúng ra khỏi ‘enchilada’ để có thêm chỗ chứa. Tôi sẽ gọi lại cho anh.”

Sau khi tập gym xong, tôi về nhà, đăng nhập và chuyển các tập tin vào một tài khoản mà tôi đã tạo cho mình ở Colorado Supernet, nhà cung cấp dịch vụ

https://thuviensach.vn

Internet lớn nhất ở Denver. Ngày hôm sau, Nevarez chuyển toàn bộ số tập tin còn lại cho tôi, việc này mất rất nhiều thời gian bởi có quá nhiều mã.

Khi tôi nhờ Nevarez chuyển mã nguồn máy chủ, anh ta đã bắt đầu nghi ngờ và lẩn tránh. Ngay lúc đó, tôi gọi vào hộp thư thoại của Gabe và cài đặt lại lời chào thoại tiêu chuẩn để xóa đi giọng mình. Hiển nhiên, tôi không muốn lưu nó lại để dành cho một phiên tòa trong tương lai rồi.

Không nản lòng, tôi thầm nghĩ: Sẽ luôn có thứ gì đó còn thử thách và thú vị hơn để mình hack.

Dạo ấy, điện thoại di động có kích thước nhỏ hơn rất nhiều so với loại to như chiếc cặp ca táp thuở ban đầu. Nhưng chúng vẫn to bằng một chiếc giày nam giới và nặng gấp vài lần. Sau đó, hãng Motorola đã thực hiện một cú nhảy vọt đi trước mọi hãng điện thoại khác nhờ chiếc MicroTAC Ultra Lite nhỏ, nhẹ và thiết kế đẹp mắt. Trông nó giống như một chiếc máy điện đàm trong loạt phim Star Trek, thiết bị mà Captain Kirk vẫn dùng để ra lệnh: "Đưa tôi ra khỏi đây, Scotty!" Ngoài hình thức bên ngoài vô cùng khác biệt, phần mềm chạy trong điện thoại cũng có cải tiến đáng kể.

Tôi vẫn đang dùng chiếc Novatel PTR-825, chính là chiếc điện thoại tôi đã lừa Novatel gửi cho mình con chip đặc biệt để có thể thay đổi ESN bằng phím bấm. Nó không thể sánh với kiểu dáng cuốn hút của chiếc MicroTAC Ultra Lite. Có lẽ đã đến lúc tôi cần đổi một chiếc điện thoại mới – nếu tôi có thể tìm ra cách để có những tính năng tương tự như chiếc Novatel. Vậy tức là bằng cách nào đó tôi phải có được mã nguồn của Motorola. Việc này khó biết chừng nào? Đây hẳn là một thử thách thú vị.

Quá háo hức với ý tưởng mới, tôi đã hỏi Elaine, sếp của tôi ở hãng luật, xem mình có thể rời sở sớm để giải quyết vấn đề cá nhân hay không và cô ta đồng ý. Tôi ra khỏi công ty lúc 3 giờ chiều. Trong khoảng thời gian dài trên thang máy đi xuống qua 50 tầng, hai nhân viên cộng tác với hãng có lời bông đùa về một vụ lớn họ đang làm: Hãng luật đại diện cho Michael

https://thuviensach.vn

Jackson. Tôi cười thầm, nhớ đến thời tôi từng làm ở Fromin's Delicatessen. Gia đình Jackson có một tòa nhà lớn ngay dưới đường, ở Hayvenhurst, thi thoảng họ vẫn dừng chân tại chỗ tôi làm để dùng bữa trưa hay bữa tối. Giờ thì tôi ở đây, trong một thang máy cách xa cả nghìn cây số, lẩn trốn khỏi FBI và Sở Cảnh sát Tư pháp, làm việc ở một hãng luật danh tiếng đang đại diện cho một trong những nhạc sĩ nổi tiếng nhất thế giới.

Khi bắt đầu đi bộ về nhà trong cơn mưa tuyết, tôi thực hiện một cuộc gọi miễn phí đến tổng đài để hỏi số của Motorola. Sau đó, tôi gọi đến số của hãng và nói với người trực máy thân thiện rằng mình muốn tìm gặp quản lý dự án MicroTAC Ultra Lite.

"Ồ, bộ phận thuê bao di động của chúng tôi đặt tại Schaumburg, Illinois. Anh có cần số của họ không?" cô ta hỏi. Đương nhiên là tôi cần.

Tôi gọi tới Schaumburg và nói: "Xin chào, tôi là Rick ở Motorola Arlington Heights. Tôi muốn gặp quản lý dự án MicroTAC Ultra Lite." Sau khi được chuyển máy qua vài người khác nhau, cuối cùng tôi đã gặp được vị phó Giám đốc Phòng Nghiên cứu và Phát triển. Tôi nhắc lại nội dung về Arlington Heights và việc muốn liên lạc với quản lý dự án MicroTAC.

Tôi khá lo rằng vị lãnh đạo này có thể dấy lên nghi ngờ bởi tiếng xe cộ qua lại trên đường và đôi khi là còi xe ầm ĩ từ mấy gã tài xế thiếu kiên nhẫn muốn về nhà sớm trước khi tuyết bắt đầu dồn đống. Nhưng không. Ông ta chỉ nói: "Đó là Pam, cô ấy làm việc cho tôi" rồi cho tôi số máy lẻ của cô ấy. Tin nhắn trên hộp thư thoại của Pam thông báo rằng cô đang đi nghỉ hai tuần và rằng: "Nếu bạn cần bất kỳ sự giúp đỡ nào, hãy gọi cho Alisa," rồi thông báo số máy lẻ của Alisa.

Tôi gọi tới số này và nói: "Chào Alisa. Tôi là Rick ở Phòng Nghiên cứu và Phát triển ở Arlington Heights. Tôi đã nói chuyện với Pam tuần trước và được biết cô ấy sẽ đi nghỉ. Pam đã đi chưa nhỉ?"

Đương nhiên Alisa nói: "Cô ấy đi rồi."

https://thuviensach.vn

“À,” tôi nói tiếp, “Pam lẽ ra phải gửi mã nguồn của MicroTAC Ultra Lite cho tôi. Nhưng cô ấy nói nếu không kịp thì tôi nên gọi điện cho cô để nhờ giúp đỡ.” Đáp lại đề nghị của tôi là: “Anh cần phiên bản nào?” Tôi mỉm cười.

Tuyệt – cô ấy không buồn dò xét thân phận của tôi và còn sẵn lòng giúp đỡ. Nhưng dĩ nhiên, tôi không có chút ý niệm nào về phiên bản hiện tại, thậm chí là hệ số nào được dùng để đặt tên. Do vậy, tôi chỉ nói một cách hời hợt: “Bản mới nhất và tốt nhất thì sao?”

“Ok, để tôi kiểm tra,” cô ấy nói.

Tôi mệt mỏi lê từng bước. Tuyết bắt đầu dính cả tảng ở chân. Tôi kéo mũ trùm xuống một bên tai và bên còn lại là chiếc điện thoại cồng kềnh, không thành công lắm trong nỗ lực giữ ấm bằng cách áp thật chặt điện thoại vào tai. Trong khi Lisa đang bận rộn gõ bàn phím, tôi ngó quanh tìm một tòa nhà để trốn tiếng xe cộ ồn ào, phòng trường hợp bị nghi ngờ, nhưng không có chỗ nào để đi. Vài phút trôi qua.

Cuối cùng, cô ấy nói: “Tôi tìm thấy một văn bản trong thư mục của Pam cho phép tôi lấy được bất kỳ phiên bản phần mềm nào của Ultra Lite. Anh cần định dạng ‘doc’ hay ‘doc2’?”

“doc2,” tôi trả lời, đoán rằng nó hẳn là phiên bản mới hơn.

“Đợi một chút. Tôi đang giải nén nó ra một thư mục tạm,” cô nói. Và rồi, “Rick, có chút vấn đề.” Số nhọ rồi.“Có rất nhiều tập tin trong vô số thư mục. Tôi phải làm sao đây?”

Nghe có vẻ như đã đến lúc phải gom và nén các tập tin lại. “Cô có biết dùng ‘tar’ và ‘gzip’ thế nào không?” Cô ấy nói không biết. Tôi hỏi thêm, “Cô có muốn học không?”

https://thuviensach.vn

Cô ấy nói rất thích học thêm kiến thức mới, do vậy tôi trở thành người hướng dẫn để cô ấy có thể từng bước tổng hợp và nén tất cả tập tin mã nguồn vào một tập tin duy nhất.

Lúc này, ô tô như đang trượt trên con đường trơn tuyết, càng thêm nhiều tiếng còi xe vang lên. Tôi không ngừng nghĩ trong đầu: Cô ấy có thể nhận ra tiếng còi và bắt đầu đặt câu hỏi bất kỳ lúc nào. Nhưng nếu Alisa nghe thấy, cô ấy hẳn phải cho rằng đó là tiếng xe cộ bên ngoài cửa sổ văn phòng của tôi; cô ấy không thắc mắc gì về chuyện đó. Cuối bài hướng dẫn, chúng tôi đã có một tập tin nặng 3 megabyte không chỉ chứa mã nguồn mới nhất mà còn cả bản sao thư mục "/etc" của máy chủ, trong này lại chứa bản sao tập tin mã băm mật khẩu của tất cả người dùng cùng nhiều thứ khác. Tôi hỏi Alisa có biết dùng "FTP" không.

"Chương trình chuyển tập tin (File Transfer Program) ấy hả? Đương nhiên," cô ấy đáp.

Như vậy, cô ấy đã biết rằng FTP cho phép chuyển tập tin giữa các hệ máy tính.

Lúc này, tôi chỉ muốn tự đá cho mình một cái vì đã không chuẩn bị kỹ hơn. Tôi không thể ngờ mình sẽ đi tới bước này chỉ trong một khoảng thời gian ngắn. Khi Alisa tìm được phiên bản mới nhất của các mã nguồn, nén chúng thành một tập tin đơn, tôi cần phải hướng dẫn cô ấy các bước cần thiết để gửi chúng cho tôi. Nhưng tôi không thể cho cô ấy một trong các hostname mà tôi đang dùng, và hiển nhiên tôi không có hostname có đuôi "mot.com" của Motorola. Tôi nghĩ ra một cách giải quyết: Nhờ vào sở trường nhớ số của mình, tôi biết địa chỉ IP của một trong những máy chủ của Colorado Supernet, có tên "teal". (Mỗi máy tính và thiết bị trên hệ thống TCP/IP đều có địa chỉ riêng của mình, ví dụ như 128.138.213.21.)

Tôi nhờ cô ấy gõ vào "FTP", kế đó là địa chỉ IP. Như vậy lẽ ra đã có thể kết nối vào Colorado Supernet, nhưng không hiểu sao mỗi lần cô ấy thử đều bị

https://thuviensach.vn

dừng lại.

Alisa nói: “Tôi nghĩ có vấn đề bảo mật. Để tôi hỏi quản lý bảo mật về việc này.”

“Không, khoan đã…,” tôi nói đầy tuyệt vọng. Quá muộn rồi: Tôi đã bị chuyển sang chế độ chờ.

Sau vài phút, tôi cảm thấy bồn chồn. Chuyện gì sẽ xảy ra nếu họ đặt máy ghi âm và thu lại giọng của tôi? Cho tới khi Alisa quay trở lại đường dây sau đó vài phút, cánh tay tôi đã bắt đầu tê cứng vì phải giữ điện thoại.

“Rick, tôi mới nói chuyện với quản lý bảo mật. Địa chỉ IP anh cho tôi nằm ngoài trụ sở của Motorola,” cô ta nói.

Tôi không muốn nói thêm nhiều trừ những gì thực sự cần thiết, để phòng xa.

“Ừm,” tôi trả lời.

“Nhưng quản lý bảo mật nói tôi có thể dùng một proxy server (máy chủ ủy nhiệm) để gửi tập tin cho anh, vì các lý do bảo mật.”

Tôi bắt đầu cảm thấy thất vọng lớn, thầm nghĩ: Vậy là trò hacking nho nhỏ đã kết thúc.

Thế rồi cô ấy lại nói tiếp: “Tin tốt là anh ấy đã cho tôi username và mật khẩu của proxy server nên tôi có thể gửi tập tin cho anh.” Quá tuyệt vời! Không thể tin nổi. Tôi cảm ơn cô ấy thật nhiều và nói rằng tôi có thể sẽ gọi lại sau nếu còn cần sự giúp đỡ.

Khi về tới nhà, toàn bộ mã nguồn cho sản phẩm mới nhất của Motorola đã chờ sẵn. Chỉ bằng khoảng thời gian lê bước về nhà trong trận mưa tuyết, tôi đã dụ được Alisa trao cho mình một trong những bí mật thương mại được lưu giữ cẩn mật nhất của công ty cô ấy.

https://thuviensach.vn

Tôi gọi lại cho cô ấy thêm vài lần nữa trong những ngày tiếp theo để lấy các phiên bản khác nhau của mã nguồn MicroTAC Lite. Việc này giống như thể Cơ quan Tình báo Trung Ương (CIA) đang cài cắm một điệp viên ở đại sứ quán Iran, người thậm chí còn không nhận ra mình đã chuyển thông tin cho kẻ thù của đất nước vậy.

Nếu việc lấy mã nguồn của một chiếc điện thoại di động dễ như vậy, có khi tôi có thể bằng cách nào đó đột nhập vào máy chủ của nhóm phát triển Motorola và sao chép mọi mã nguồn mình cần mà không cần nhờ tới sự giúp đỡ của Alisa hay các nhân viên khác. Alisa có nhắc tới hostname của một máy chủ nơi chứa tất cả các mã nguồn là “lc16”.

Thử vận may của mình, tôi kiểm tra thời tiết ở Schaumburg, Illinois, nơi Nhóm Thuê bao Di động đặt ở đó. Và tình hình là: “Cơn bão tuyết bắt đầu từ hôm qua sẽ còn tiếp diễn tới tận sáng ngày mai, với sức gió 50km/giờ.”

Hoàn hảo.

Tôi lấy được số điện thoại tới Trung tâm Vận hành Mạng lưới (NOC) của họ. Theo những gì tôi tìm hiểu được, chính sách bảo mật của Motorola yêu cầu những nhân viên muốn quay số kết nối từ xa phải cung cấp thêm thông tin ngoài tên đăng nhập và mật khẩu.

Họ đòi hỏi phải xác minh bằng hai loại mã số bảo mật – trong đó có một SecurID đã nhắc tới ở trên, đây là sản phẩm của một công ty có tên là Security Dynamics. Tất cả các nhân viên muốn kết nối từ xa sẽ được cấp một mã PIN bí mật và nhận được một thiết bị nhỏ cỡ chiếc thẻ tín dụng. Thiết bị này sẽ hiển thị một mật khẩu gồm sáu ký tự ở màn hình. Mã bảo mật này sẽ thay đổi 60 giây một lần. Việc đoán mã có vẻ bất khả thi đối với người không phận sự. Bất kỳ khi nào người dùng muốn đăng nhập từ xa vào hệ thống nằm trong trụ sở của Motorola, họ phải nhập mã PIN và sau đó là mã bảo mật hiện trên thiết bị SecurID của mình.

https://thuviensach.vn

Tôi gọi tới trung tâm vận hành mạng lưới và gặp một gã mà tôi sẽ gọi là Ed Walsh. “Chào anh,” tôi nói. “Tôi là Earl Roberts ở Nhóm Thuê bao Di động” – đây là tên và nơi làm việc của một nhân viên có thực.

Ed hỏi tôi công việc thế nào và tôi nói: “Ừm, không ổn lắm. Tôi không thể đến văn phòng vì bão tuyết. Vấn đề là tôi cần kết nối với máy tính từ nhà nhưng lại để quên SecurID trên bàn làm việc. Anh có thể qua lấy nó giúp tôi không? Hoặc là ai đó cũng được? Rồi đọc giúp tôi mã số? Dự án của nhóm tôi sắp đến kỳ hạn rất quan trọng mà tôi thì chưa thể làm xong. Tôi không làm sao đến văn phòng được, đường phố nguy hiểm quá.”

Anh ta nói: “Tôi không thể rời NOC được.”

Tôi tiếp lời ngay: “Vậy anh có SecurID cho Nhóm Vận hành không?”

“Có một cái ở NOC đây,” anh ta nói. “Chúng tôi giữ để đề phòng trường hợp khẩn cấp.”

“Nghe này,” tôi nói, “anh có thể giúp tôi được không? Khi tôi cần đăng nhập vào hệ thống, anh có thể đọc cho tôi mã bảo mật trên SecurID của anh không? Chỉ cần chờ tới khi tôi có thể lái xe tới văn phòng.”

“Anh là ai đấy nhỉ?” anh ta hỏi.

“Earl Roberts.”

“Anh làm việc cho ai?”

“Pam Dillard.”

“À, vâng, tôi biết cô ấy.”

Vì luôn phải đối mặt với những tình huống khó khăn có thể xảy đến, nên một hacker tấn công bằng kỹ thuật xã hội giỏi cần tìm hiểu thông tin nhiều hơn mức bình thường. “Tôi ở tầng hai,” tôi tiếp tục. “Ngồi gần Steve Littig.”

https://thuviensach.vn

Anh ta biết rất rõ cái tên đó. Giờ thì tôi tiếp tục thúc đẩy. “Tới bàn làm việc của tôi lấy SecurID có lẽ tiện hơn.”

Walsh không muốn từ chối một người đang rất cần giúp đỡ, nhưng anh ta cũng không muốn đồng ý. Do vậy, anh ta tránh né việc phải đưa ra quyết định: “Để tôi hỏi sếp đã. Đợi chút.” Anh ta đặt máy xuống và tôi có thể nghe thấy tiếng Walsh nhấc một chiếc điện thoại khác lên, thực hiện cuộc gọi và giải thích yêu cầu của tôi vào đầu dây. Sau đó, anh ta lại làm một việc không thể hiểu nổi: Walsh nói với sếp mình: “Tôi biết anh ấy. Anh ấy làm việc cho Pam Dillard. Chúng ta có thể cho anh ta dùng tạm SecurID không? Tôi sẽ báo mã bảo mật cho anh ấy qua điện thoại.” Walsh đứng ra đảm bảo cho tôi – thật kinh ngạc!

Một lúc sau, Walsh quay trở lại đường dây và nói với tôi: “Quản lý của tôi muốn trực tiếp nói chuyện với anh” và cho tôi tên cũng như số di động của ông ta.

Tôi gọi cho quản lý của Walsh và nói lại toàn bộ tình huống một lần nữa, thêm một chút chi tiết về dự án mà tôi đang làm việc, đồng thời nhấn mạnh rằng nhóm sản phẩm của tôi đang phải chạy một kỳ hạn quan trọng. “Sẽ dễ hơn rất nhiều nếu có ai đó đi lấy SecurID giúp tôi,” tôi nói. “Bàn của tôi không khóa, nó ở ngay ngăn kéo trên phía bên tay trái.”

“Ừm,” vị quản lý nói, “chỉ cuối tuần này thôi, tôi nghĩ anh có thể dùng tạm cái ở NOC cũng được. Tôi sẽ báo nhân viên trực máy đọc giúp anh mã bảo mật khi anh gọi” và ông ta cho tôi số PIN để dùng.

Trong suốt cuối tuần đó, mỗi khi cần kết nối vào mạng nội bộ của Motorola, tất cả những gì tôi cần làm là gọi tới Trung tâm Vận hành Mạng lưới và đề nghị ai đó ở đầu dây bên kia đọc giúp tôi sáu ký tự hiện trên màn hình SecurID.

Nhưng đó vẫn chưa phải là thắng lợi. Khi tôi gọi tới dial-up máy chủ đầu cuối[75] của Motorola thì các hệ thống mà tôi cố tiếp cận ở Nhóm Thuê bao

https://thuviensach.vn

Di động vẫn chưa sẵn sàng. Tôi phải tìm cách khác để thâm nhập.

[75] Dial-up máy chủ đầu cuối (dial-up terminal server): Máy chủ có vai trò trung gian giúp một máy tính nào đó có thể kết nối với các hệ thống khác qua đường dây điện thoại thay vì mạng Internet. (ND)

Cần cả gan để làm bước tiếp theo: Tôi gọi lại cho Walsh ở NOC và giải thích: "Dial-up của máy chủ đầu cuối không thể đăng nhập được vào các hệ thống, tôi không thể kết nối được. Anh có thể giúp tôi lập một tài khoản trên máy của NOC để tôi có thể kết nối với máy tính của mình không?"

Quản lý của Walsh đã đồng ý đọc cho tôi mã bảo mật trên SecurID, như vậy yêu cầu này cũng không quá phận. Walsh tạm thời thay đổi mật khẩu tài khoản của chính mình trên máy tính của NOC và cho tôi thông tin để đăng nhập, sau đó nói: "Hãy gọi cho tôi khi xong việc để tôi đổi lại mật khẩu nhé."

Tôi thử kết nối với một hệ thống bất kỳ trong Nhóm Thuê bao Di động nhưng liên tục bị chặn; hiển nhiên là chúng đều đã được tường lửa bảo vệ. Dò dẫm quanh mạng lưới của Motorola, cuối cùng tôi đã tìm ra được một hệ thống cho phép tài khoản "khách mời" (guest) – đồng nghĩa với việc cổng vào để mở và tôi có thể đăng nhập được. (Tôi khá ngạc nhiên khi phát hiện ra hệ thống này là một máy tính của NeXT, được sản xuất bởi công ty yểu mệnh do Steve Jobs lập ra trước khi quay trở lại Apple.) Tôi tải về tập tin mật khẩu và cố giải mã của người có quyền đăng nhập vào máy tính đó, một gã có tên là Steve Urbanski. Tôi không mất quá nhiều thời gian: Tên đăng nhập trên máy tính NeXT của anh ta là "steveu" và mật khẩu "mary".

Từ máy tính NeXT, tôi thử đăng nhập vào host "lc16" trong Nhóm Thuê bao Di động ngay lập tức nhưng mật khẩu không đúng. Trở ngại lớn đây rồi.

Được thôi. Thông tin tài khoản của Urbanski sẽ có ích sau này. Giờ cái tôi cần không phải là tài khoản NeXT của anh ta mà là mật khẩu để anh ta đăng

https://thuviensach.vn

nhập vào máy chủ của Nhóm Thuê bao Di động, nơi chứa tất cả mã nguồn mà tôi muốn.

Tôi dò theo số điện thoại nhà riêng của Urbanski và gọi cho anh ta. Giả danh là nhân viên từ NOC, tôi thông báo: “Chúng tôi gặp một vấn đề lớn về đĩa cứng. Anh có bất kỳ tập tin dữ liệu nào cần phục hồi không?”

Tất nhiên là anh ta cần.

“Chúng tôi có thể phục hồi vào thứ Năm,” tôi nói. Thứ Năm tức là anh ta sẽ không có tập tin làm việc trong suốt ba ngày. Tôi kéo ống nghe ra xa tai khi anh ta nổi điên lên như dự tính.

“Vâng, tôi hiểu,” tôi tỏ vẻ đồng cảm. “Tôi nghĩ mình có thể tạo một ngoại lệ để phục hồi dữ liệu của anh trước tiên, nhưng anh phải giữ kín chuyện này. Chúng tôi đang cài đặt máy chủ trên một máy mới tinh và tôi cần phải tái lập tài khoản của anh trên hệ thống mới. Tên đăng nhập của anh là ‘steveu’ đúng không?”

“Đúng,” anh ta đáp.

“Được rồi, Steve, chọn một mật khẩu mới mà anh thích đi.” Sau đó, như thể mới nảy ra ý tưởng hay hơn, tôi nói tiếp: “À, không cần đâu, anh chỉ cần nói mật khẩu cũ của mình, tôi lập theo đó là được.”

Việc này đương nhiên sẽ khiến anh ta nghi ngờ. “Anh là ai cơ?” anh ta muốn biết. “Anh nói anh làm việc cho ai?”

Tôi lặp lại những gì mình đã nói, rất bình tĩnh, coi như một chuyện thường ngày.

Tôi hỏi anh ta có SecurID không. Đúng như dự đoán, câu trả lời là có, do vậy tôi bèn nói: “Để tôi xem đơn đăng ký SecurID của anh.” Đây chỉ là trò đánh cược. Tôi biết anh ta có lẽ đã điền đơn từ cả thế kỷ trước và hẳn sẽ

https://thuviensach.vn

không nhớ xem trên đó có hỏi mật khẩu hay không. Và vì đã biết mật khẩu anh ta dùng là ‘mary’, tôi cho rằng anh ta sẽ thấy nó quen thuộc và nghĩ rằng mình cũng dùng mật khẩu đó trên đơn SecurID.

Tôi bỏ đi, mở một ngăn kéo, đóng sập nó lại và quay trở lại điện thoại, bắt đầu xáo lật đống giấy.

“Ok, đây rồi… anh dùng mật khẩu là ‘mary’ nhỉ?”

“Đúng rồi,” anh ta nói, giọng thỏa mãn. Sau một chút ngần ngại, anh ta buột miệng: “Được rồi, mật khẩu của tôi là ‘bebop1.’”

Được cả chì lẫn chài rồi.

Tôi kết nối với máy chủ mà Alisa đã nhắc tới, lc16, ngay lập tức. Sau đó, tôi đăng nhập bằng tài khoản “steveu” với mật khẩu là “bebop1”. Xong!

Không mất nhiều thời gian để tìm được vài phiên bản mã nguồn của MicroTAC Ultra Lite; tôi gom lại và nén bằng tar và gzip, sau đó chuyển tới Colorado Supernet. Tôi dành thêm chút thời gian xóa tập tin cũ mà tôi đã nhờ Alisa lập. Xóa bỏ dấu vết luôn là việc nên làm.

Tôi dành thời gian cuối tuần còn lại để nghịch ngợm. Vào sáng thứ Hai, tôi dừng việc gọi điện cho NOC để lấy mã bảo mật SecurID. Quả là một cuộc hacking thú vị, nhưng chẳng có lý gì phải liều mình thêm nữa.

Tôi không thể ngừng cười trong suốt thời gian đó. Thêm một lần nữa, tôi không thể tin nổi mọi chuyện lại dễ dàng đến thế, không có trở ngại nào xuất hiện trước mắt tôi. Tôi có cảm giác mình đã đạt được một thành tựu lớn và cả sự thỏa mãn như đã từng có khi còn chơi bóng chày ở Liên đoàn Bóng chày Nhí và đánh được một cú home run[76].

[76] Home run: Cú đánh cho phép người đánh chạy quanh ghi điểm mà không phải dừng lại. (BTV)

https://thuviensach.vn

Nhưng rồi sau đó, chết tiệt, tôi nhận ra mình không hề nghĩ tới việc lấy cả trình biên dịch (compiler) – chương trình dịch mã nguồn do lập trình viên viết sang loại mã mà máy tính có thể đọc, loại mã này gồm các dãy số 1 và 0 mà máy tính hay bộ xử lý trong điện thoại di động có thể hiểu được.

Như vậy, đây sẽ là thử thách kế tiếp. Liệu Motorola có phát triển trình biên dịch của riêng họ cho bộ xử lý 68HC11 dùng trong MicroTAC không, hay họ sẽ mua nó từ một nhà sản xuất phần mềm khác? Và làm sao để tôi có thể lấy được nó đây?

Tới cuối tháng Mười, quy trình rà soát thường lệ của tôi trên Westlaw và LexisNexis đã giúp tìm ra một bài báo viết về cuộc phiêu lưu mới nhất của Justin Petersen. Đôi khi FBI thường nhắm mắt cho qua khi người đưa tin mật của họ phạm pháp, nhưng cũng có giới hạn. Hóa ra, một cộng sự của Kevin Poulsen, Ron Austin, người đã bị Justin Peterson gài bẫy, hiện đang tiến hành một chiến dịch cá nhân nhằm ăn miếng trả miếng với gã chỉ điểm và tống gã vào tù. Austin đã tìm ra nơi Justin sống – cùng địa chỉ ở Đại lộ Laurel Canyon mà tôi đã lần ra được theo số điện thoại của McGuire. Justin đã quá sơ ý: Hắn quên mất không hủy những ghi chép cá nhân trước khi ném chúng vào sọt rác. Austin đã lục-thùng-rác trước nhà và phát hiện ra chứng cứ cho thấy Justin vẫn đang giả mạo thẻ tín dụng. Hắn báo ngay cho FBI về việc này.

Khi đã có đủ chứng cứ trong tay, trợ lý công tố, David Schindler, đã triệu tập Justin và luật sư của hắn tới Tòa án Liên bang ở Los Angeles. Đứng trước vị đặc vụ FBI và tay luật sư công tố, Justin biết rằng những ngày tháng tự do của hắn sắp kết thúc.

Trong buổi điều trần, Justin đề nghị được nói chuyện riêng với luật sư bào chữa của mình. Hai người họ bước ra khỏi phòng. Vài phút sau, tay luật sư quay lại và ngập ngừng nói rằng thân chủ của hắn đã biến mất. Tòa án ra lệnh bắt giữ không-được-bảo-lãnh đối với Justin.

https://thuviensach.vn

Như vậy, tên khốn chỉ điểm cố đẩy tôi vào tù cũng đã rơi vào tình trạng tương tự như tôi. Hắn đang đi trên con đường của tôi. Hoặc có thể nói là chạy.

Tôi cười toét miệng. Vậy là kẻ đưa tin cho chính phủ đã biến mất. Dù họ có tìm được hắn một lần nữa, thì giá trị của hắn cũng bằng 0. Chính phủ sẽ không bao giờ có thể dùng hắn để làm chứng cứ chống lại tôi được nữa.

Sau này, tôi nghe nói rằng Justin đã từng thử cướp nhà băng trong lúc lẩn trốn. Hắn tấn công vào máy tính của Heller Financial và lấy được các mã cần thiết nhằm thực hiện hành động chuyển tiền từ ngân hàng đó tới một tài khoản ngân hàng khác. Sau đó, hắn gọi điện tới Heller Financial đe dọa đã gài bom. Trong lúc cả tòa nhà sơ tán, hắn tranh thủ chuyển 150.000 đô-la từ Heller Financial vào Union Bank thông qua Mellon Bank. Rất may cho Heller Financial, vụ việc đã được phát hiện trước khi Peterson kịp rút tiền từ Union.

Tôi lấy làm thích thú khi biết hắn đã bị bắt, đồng thời cũng ngạc nhiên khi thấy hắn thực hiện trò lừa đảo này. Điều đó cho thấy hắn thực sự là một tên xấu xa, thậm chí còn khốn kiếp hơn tôi tưởng.

https://thuviensach.vn

29

RỜI ĐI

126 147 172 163 040 166 172 162 040 154 170 040 157 172 162 162 166
156 161 143 040 145 156 161 040 163 147 144 040 115 156 165 144 153
153 040 163 144 161 154 150 155 172 153 040 162 144 161 165 144 161
040 150 155 040 122 172 155 040 111 156 162 144 077

Hãng luật tổ chức buổi tiệc Giáng sinh thường niên vào giữa tháng Mười hai. Tôi đến chỉ bởi không muốn mọi người nghi ngờ lý do vắng mặt của mình. Tôi gặm đống thức ăn thừa mứa nhưng tránh xa rượu, sợ mình sẽ nói hớ điều gì đó. Dù sao tôi cũng không phải là một người thích uống; những con số 0 và 1 mới là nguồn say của tôi.

Bất kỳ tên trộm có trình độ nào cũng đều nhòm ngó trước sau để chắc chắn đối thủ không theo kịp những nỗ lực mình. Trong suốt quãng thời gian đó, tôi đã dùng Colorado Supernet – suốt tám tháng, kể từ lần đầu đặt chân đến Denver – tôi luôn phải cảnh giác với những tay quản trị hệ thống trong thế giới ảo để chắc rằng họ không tóm được việc tôi đang dùng các máy chủ của họ như những tủ khóa lưu trữ miễn phí khổng lồ, một bệ phóng để vào các hệ thống khác. Việc này bao gồm giám sát họ trong giờ làm; đôi lúc tôi đăng nhập vào máy chủ đầu cuối họ dùng và giám sát các phiên làm việc trực tuyến của họ trong vài giờ hoặc tương tự. Và tôi cũng kiểm tra xem họ có đang theo dõi bất cứ tài khoản nào tôi đang sử dụng hay không.

Một đêm nọ, tôi quyết định sẽ nhắm vào máy trạm cá nhân của tay quản trị chính để xem gã có phát hiện ra bất cứ hoạt động nào của tôi hay không. Tôi tìm trong e-mail của gã các từ khóa có thể là dấu hiệu cho thấy gã để ý thấy bất kỳ vấn đề bảo mật nào đang diễn ra.

https://thuviensach.vn

Tôi vô tình nhìn thấy một tin nhắn thu hút sự chú ý. Tay quản trị này đang gửi hồ sơ đăng nhập của tôi về vụ đột nhập ở Novell cho một ai đó. Vài tuần trước, tôi đã dùng một tài khoản tên là “rod” để nhét mã nguồn của NetWare lên một máy chủ tại Colorado Supernet. Rõ ràng, việc này không trót lọt và có người đã để ý đến nó.

Hồ sơ đăng nhập của “rod” trong khoảng thời gian đội an ninh ở Novell báo cáo về cuộc thâm nhập và các kết nối TỪ Novell trong thời điểm đó. Lưu ý rằng có vài lần đăng nhập bắt nguồn qua dial-up của Colorado Springs (719 575-0200).

Tôi bắt đầu điên cuồng duyệt qua những e-mail của tay quản trị viên này.

Và nó đây, ẩn hai đầu liên lạc: một e-mail tới từ quản trị viên sử dụng tài khoản từ tên miền cá nhân – “xor.com” – thay vì tài khoản Colorado Supernet của gã. Nó được gửi đến tài khoản của ai đó không dùng tên miền chính phủ nhưng dù sao, họ cũng đã nhận được ghi chép về hành động của tôi, bao gồm cả việc đăng nhập vào Colorado Supernet từ mạng của Novell và chuyển tập tin qua lại.

Tôi gọi đến văn phòng FBI ở Denver, đưa ra cái tên mà những e-mail kia đã gửi đến và được trả lời rằng không có đặc vụ FBI nào tên như vậy ở văn phòng Denver. Nhân viên trực tổng đài gợi ý tôi có thể thử gọi sang văn phòng Colorado Springs xem sao. Vậy là tôi gọi đến đó, chết tiệt, gã đó đúng là một đặc vụ FBI.

Ôi, điên mất!

Tôi phải che giấu thân phận. Và phải làm thật nhanh. Nhưng bằng cách nào đây?

Tôi phải thú nhận rằng kế hoạch tôi nghĩ ra có thể không tuyệt diệu hay bí mật đến mức đó, dù tôi biết mình sẽ phải rất, rất cẩn thận.

https://thuviensach.vn

Tôi gửi một tập tin ghi chép giả từ tài khoản của tay quản trị viên đó đến cho gã đặc vụ FBI, bảo hắn rằng "chúng tôi" còn nhiều ghi chép chi tiết về hoạt động của tay hacker kia. Tôi hy vọng hắn sẽ điều tra và cuối cùng sẽ đi theo hướng do tôi ngụy tạo trong khi tôi vẫn tiếp tục tiến hành những dự án hacking khác của mình.

Tôi gọi chiến thuật này là "giương đông kích tây".

Tuy biết FBI đang săn tìm tay hacker tại Novell, nhưng tôi vẫn không chịu dừng bước.

Do Art Nevarez đã nghi ngờ, nên tôi nghĩ Đội An ninh Novell sẽ lập một đội chuyên trách, cố tìm hiểu xem chuyện gì xảy ra và có bao nhiêu mã nguồn bị lộ. Tôi thay đổi mục tiêu, nhắm đến các văn phòng của Novell ở San Jose và tìm các số dial-up ở California. Các cuộc gọi tấn công bằng kỹ thuật xã hội dẫn tôi đến gặp một người tên là Shawn Nunley.

"Chào, Shawn, tôi là Gabe Nault đến từ Đội Kỹ thuật ở Sandy. Tôi đang trên đường đến San Jose vào ngày mai và cần một số dial-up nội bộ để kết nối mạng," tôi nói.

Sau một hồi qua lại, Shawn hỏi: "Được rồi, tên anh là gì?"

"g-n-a-u-l-t," tôi đánh vần chậm rãi.

Anh ta cung cấp cho tôi số dial-up đến một máy chủ đầu cuối 3Com, 800-37-TCP-IP và nói: "Gabe, giúp tôi một việc. Hãy gọi vào số hộp thư thoại của tôi ở văn phòng và để lại lời nhắn với mật khẩu mà anh muốn." Anh ta đưa số cho tôi và tôi để lại lời nhắn như hướng dẫn: "Xin chào, Shawn, tôi là Gabe Nault. Xin hãy đặt mật khẩu của tôi là "snowbird". Cảm ơn anh lần nữa," tôi nói.

Không đời nào tôi gọi số miễn cước 800-gì đó mà Shawn đã đưa: Khi bạn gọi một số miễn cước, số điện thoại bạn dùng để gọi đến sẽ tự động bị lưu

https://thuviensach.vn

lại. Thay vào đó, chiều hôm sau, tôi gọi tới Pacific Bell và dùng tấn công bằng kỹ thuật xã hội lấy được số POTS gán với số Shawn đã đưa tôi: 408 955-9515. Tôi kết nối với máy chủ đầu cuối 3Com và thử đăng nhập vào tài khoản gnault. Nó hoạt động rồi. Hoàn hảo!

Tôi bắt đầu dùng máy chủ đầu cuối 3Com như điểm truy cập vào mạng lưới. Khi nhớ ra Novell đã mua lại Phòng Nghiên cứu Hệ thống Unix từ AT&T, tôi dò theo mã nguồn UnixWare tìm thấy trên các máy chủ ở New Jersey nhiều năm trước. Trước đó, tôi đã đột nhập vào AT&T để lấy quyền truy cập đến mã nguồn SCCS (Switching Control Center System – Hệ thống Điều khiển Chuyển mạch Trung tâm) và từng có thời gian ngắn lọt vào được Nhóm Phát triển Unix của AT&T ở Cherry Hill, New Jersey. Giờ tôi cảm thấy việc này có chút giống ảo giác bởi tên máy chủ của hệ thống phát triển vẫn như trước. Tôi lấy nó, nén lại thành mã nguồn mới nhất và chuyển đến một hệ thống ở Provo, Utah, rồi lại chuyển gói dữ liệu khổng lồ này đến ổ khóa lưu trữ điện tử của tôi ở Colorado Supernet suốt cuối tuần. Thật khó tin khi chứng kiến dung lượng đĩa tôi đang sử dụng, tôi thường phải tìm thêm các tài khoản không hoạt động để giấu số dữ liệu của mình.

Một dịp nọ, tôi bỗng có cảm giác kỳ lạ sau khi kết nối vào máy chủ đầu cuối 3Com, như thể có ai đó đang đứng sau và theo dõi mọi thứ tôi gõ. Giác quan thứ sáu hay bản năng mách bảo tôi rằng những quản trị viên hệ thống ở Novell đang theo dõi mình. Tôi gõ:

Này, tôi biết là các anh đang theo dõi tôi, nhưng các anh sẽ không bao giờ bắt được tôi đâu!

(Sau này, tôi có dịp nói chuyện với Shawn Nunley ở Novell. Anh ấy kể lại rằng họ thực sự đang theo dõi tôi lúc đó rồi cả nhóm bỗng cười phá lên tự hỏi: “Thế quái nào hắn lại có thể biết được chuyện này nhỉ?”)

Dù sao thì, tôi vẫn tiếp tục hacking vào nhiều hệ thống nội bộ của Novell, nơi tôi đã cài cắm vô số công cụ để lấy cắp thông tin đăng nhập và nhìn trộm

https://thuviensach.vn

tình hình giao thông mạng để có thể mở rộng quyền truy cập thêm một chút vào các hệ thống Novell.

Vài ngày sau, tôi cảm thấy có chút khó chịu. Tôi gọi đến RCMAC ở Pacific Bell và nói với thư ký xử lý yêu cầu cho bộ chuyển mạch ở San Jose. Tôi nhờ cô ta truy vấn số dial-up trong bộ chuyển mạch và nói cho tôi biết chính xác tin nhắn đầu ra của bộ chuyển mạch. Nhờ vậy, tôi phát hiện ra bộ chuyển mạch đó có gắn kèm một thiết bị tóm-và-lần. Khốn nạn! Thiết bị này đã chạy được bao lâu rồi? Tôi gọi đến Trung tâm Điều khiển Chuyển mạch của khu vực đó, giả làm nhân viên Phòng An ninh Pacific Bell và được nối máy gặp người có thể tìm kiếm thông tin về thiết bị tóm-và-lần.

“Nó đã đi vào hoạt động từ ngày 22 tháng 1,” anh ta nói. Chỉ ba ngày trước. Oa – khỏi lo rồi! May thay, tôi chưa gọi nhiều trong thời gian đó; Pacific Bell có thể theo dấu các cuộc gọi của tôi nếu đó là cuộc gọi đường dài, nhưng không thể theo dấu các cuộc gọi về tận chỗ tôi.

Tôi thở phào nhẹ nhõm và quyết định để yên cho Novell. Mọi chuyện vẫn chưa đâu vào đâu.

Nhiều năm sau, tin nhắn thoại mà tôi từng để lại cho Shawn Nunley đã quay ngược lại cắn tôi. Shawn vì lý do nào đó đã lưu lại tin nhắn của tôi, và khi có người của Phòng An ninh Novell liên hệ, anh ta đã cho gã đó nghe. Người này sau đó đưa nó lại cho Đơn vị Phòng chống Tội phạm Công nghệ Cao San Jose. Cảnh sát không thể liên hệ giọng tôi với một nghi phạm cụ thể nào. Nhưng vài tháng sau, họ gửi chiếc đĩa đến cho FBI ở Los Angeles để xem FBI có tìm hiểu được gì không. Chiếc đĩa cuối cùng cũng tìm được đường đến bàn của Đặc vụ Kathleen Carson. Cô ta cho nó vào máy chạy đĩa trên bàn, ấn nút Chạy, lắng nghe và ngay lập tức nhận ra: Đó là Kevin Mitnick, hacker mà chúng tôi đang tìm kiếm!

Kathleen gọi cho Phòng An ninh Novell và nói: Tôi có vài tin tốt và vài tin xấu. Tin tốt là chúng tôi biết danh tính hacker các anh đang tìm – đó là

https://thuviensach.vn

Kevin Mitnick. Tin xấu là, chúng tôi không có cách nào tìm ra hắn.”

Mãi sau này, tôi gặp lại Shawn Nunley và chúng tôi trở thành bạn tốt. Tôi vui vì giờ đây chúng tôi có thể cùng cười đùa về toàn bộ chuyện này.

Bỏ lại sau lưng việc hack vào Novell, tôi quyết định sẽ nhắm vào một trong những nhà sản xuất điện thoại lớn nhất thế giới, Nokia.

Tôi gọi tới công ty Nokia Mobile Phones ở Salo, Phần Lan, đóng giả là một kỹ sư từ Nokia Mỹ tại San Diego. Cuối cùng, tôi được nối máy gặp một quý ông tên là Tapio. Ông ấy có vẻ rất lương thiện, điều đó khiến tôi cảm thấy khá tồi tệ khi phải dùng đòn tấn công bằng kỹ thuật xã hội với ông ấy. Nhưng tôi vẫn gạt bỏ tất cả cảm xúc đó sang một bên và nói với ông ấy rằng tôi cần bản phát hành mã nguồn hiện tại của điện thoại Nokia 121. Ông ấy trích phiên bản mới nhất ra từ một thư mục tạm trong tài khoản của mình. Sau đó, tôi nhờ ông ấy chuyển nó (thông qua FTP) đến Colorado Supernet. Cuối cuộc gọi, ông ấy vẫn không mảy may nghi ngờ điều gì và thậm chí còn đề nghị tôi gọi lại nếu cần giúp gì khác.

Việc này diễn ra quá êm xuôi tới mức tôi cân nhắc đến việc lấy quyền truy cập trực tiếp vào mạng lưới của Nokia ở Salo. Tôi gặp vấn đề khi thực hiện cuộc gọi đến nhân viên IT ở đó vì tiếng Anh của anh ta hóa ra không được tốt lắm. Có lẽ cơ sở Nokia ở một nước nói tiếng Anh sẽ hiệu quả hơn. Tôi tìm được một văn phòng của Nokia Mobile Phones tại thị trấn Camberly ở Anh và gặp được một phụ nữ ở bộ phận IT tên là Sarah, với giọng Anh đặc sệt rất quyến rũ nhưng lại dùng quá nhiều từ lóng lạ tai khiến tôi phải tập trung và chú ý từng chi tiết một.

Tôi viện ra lý do thường dùng “gặp vấn đề với kết nối mạng giữa Phần Lan và Mỹ, trong khi có một tập tin quan trọng phải chuyển đi.” Cô ấy nói công ty không có kết nối dial-up trực tiếp nhưng cô ấy có thể cho tôi số dial-up và mật khẩu cho “Dial Plus”, nó sẽ giúp tôi kết nối đến hệ thống VMS ở Camberley thông qua mạng chuyển mạch packet X25. Cô ấy cung cấp địa

https://thuviensach.vn

chỉ thuê bao X25 – 234222300195 – bảo rằng tôi sẽ cần một tài khoản trên VAX và cô ấy sẽ thiết lập nó cho tôi.

Lúc này, tôi đang ở trong trạng thái phấn khích tột độ, bởi tôi khá chắc mình có thể đạt được mục tiêu “Mobira”, một trong các hệ thống VMS do Nhóm Kỹ thuật Di động của Nokia sử dụng. Tôi đăng nhập vào tài khoản và nhanh chóng khai thác lỗ hổng sẽ mang lại cho tôi toàn quyền ưu tiên hệ thống, sau đó gõ lệnh “show users” để liệt kê tất cả người dùng đang đăng nhập, danh sách đó trông như thế này:

https://thuviensach.vn

Username	Process Name	PID	Terminal
CONBOY	CONBOY	0000C261	NTY3: (conboy.uk.tele.nokia.fi)
EBSWORTH	EBSWORTH	0000A419	NTY6: (ebsworth.uk.tele.nokia.fi)
FIELDING	JOHN FIELDING	0000C128	NTY8: (dylan.uk.tele.nokia.fi)
LOVE	PETER LOVE	0000C7D4	NTY2: ([131.228.133.203])
OGILVIE	DAVID OGILVIE	0000C232	NVA10: (PSS.23420300326500)
PELKONEN	HEIKKI PELKONEN	0000C160	NTY1: (scooby.uk.tele.nokia.fi)
TUXWORTH	TUXWORTH	0000B52E	NTY12: ([131.228.133.85])

https://thuviensach.vn

Sarah chưa đăng nhập vào tài khoản này. Tuyệt vời, như vậy có nghĩa là cô ấy không để tâm nhiều đến những gì tôi đang làm trên hệ thống.

Sau đó, tôi cài đặt biến thể của bản vá lỗi Chaos Computer Club của mình vào chương trình VMS Loginout, nó cho phép tôi có thể đăng nhập vào tài khoản của bất kỳ ai với một mật khẩu đặc biệt. Việc đầu tiên tôi làm là kiểm tra tài khoản của Sarah xem cô ấy có quyền truy cập vào Mobira ở Salo không. Tôi chạy một bài kiểm tra đơn giản và nhận ra tôi đã có quyền truy cập vào tài khoản của cô ấy thông qua một giao thức mạng có tên là DECNET, tôi thậm chí còn không cần mật khẩu của cô ấy: Mobira được thiết lập để tin tưởng vào hệ thống VMS ở Anh. Tôi chỉ cần tải lên một chương trình nhỏ để chạy các lệnh của tôi bằng tài khoản của Sarah.

Tôi sẽ vào được! Tôi thấy mình như trên mây.

Tôi dùng một lỗi bảo mật để giành toàn quyền ưu tiên hệ thống rồi tạo tài khoản toàn quyền ưu tiên cho mình – tất cả những việc này chỉ mất khoảng năm phút. Trong khoảng một giờ, tôi đã có thể tìm được một chương trình nhỏ cho phép tôi trích xuất mã nguồn của bất kỳ chiếc điện thoại Nokia nào đang được phát triển. Tôi chuyển mã nguồn của vài phiên bản firmware khác nhau được phát hành cho Nokia 101 và Nokia 121 đến Colorado Supernet. Sau đó, tôi quyết định xem các quản trị viên cảnh giác với vấn đề bảo mật đến mức nào. Hóa ra, họ có quy trình kiểm định bảo mật được kích hoạt cho những việc như tạo tài khoản hay thêm quyền cho tài khoản đã có. Đó đơn giản chỉ là một gờ giảm tốc nữa trên con đường chiếm được mã nguồn của tôi.

Tôi tải lên một chương trình Macro VAX nhỏ đánh lừa hệ điều hành và cho phép tôi tắt mọi báo động an ninh mà không bị phát hiện, vừa đủ lâu để đổi mật khẩu và thêm quyền ưu tiên vào một vài tài khoản đã lâu không hoạt động – chúng có thể thuộc về những nhân viên bị hủy hợp đồng – trong trường hợp tôi cần quay lại.

https://thuviensach.vn

Tuy nhiên, rõ ràng là một trong số các quản trị viên hệ thống đã để ý thấy các báo động được kích hoạt khi lần đầu tôi tạo tài khoản cho mình trước khi tắt cảnh báo. Vì vậy, trong lần đăng nhập tiếp theo thử vào hệ thống VMS Camberkey, tôi thấy mình đã bị khóa ở ngoài. Tôi gọi cho Sarah để dò hỏi về việc này. Cô ấy bảo tôi: "Hannu đã vô hiệu hóa truy cập từ xa do có mấy vụ hackering đang diễn ra."

"Hackering" – đây là cách người Anh gọi nó à?

Vào ga chuyển số, tôi quyết định nhắm đến việc lấy bản sao mã nguồn của một sản phẩm được gọi tên trong nội bộ là "HD760": Chiếc điện thoại kỹ thuật số đầu tiên của Nokia hiện đang được phát triển. Tiếp cận lập trình viên trưởng, Markku, ở Oulu, Phần Lan, tôi đã thuyết phục được ông ta trích xuất và nén bản mã nguồn mới nhất gửi cho mình.

Tôi muốn ông ta chuyển nó thông qua kết nối FTP đến một máy chủ ở Mỹ, nhưng Nokia đã chặn các kết nối truyền tập tin ra ngoài sau vụ đột nhập Mobira.

Thế cho vào đĩa thì sao? Markku không có ổ đĩa. Tôi bắt đầu gọi đến những người khác ở Oulu, tìm kiếm ổ đĩa. Cuối cùng, tôi xác định được một người ở bộ phận IT có vẻ rất thân thiện, có khiếu hài hước và quan trọng hơn là có một ổ đĩa. Tôi nhờ Markku gửi cho anh ta một gói tập tin có chứa mã nguồn tôi muốn và thuyết phục anh ta chuyển chiếc đĩa, sau khi đã sao chép mã nguồn vào đó, đến văn phòng Nokia Mỹ ở Largo, Florida. Việc này tốn rất nhiều công sắp xếp, nhưng cuối cùng tôi đã móc nối mọi thứ thành công.

Canh thời gian gói hàng đến nơi, tôi bắt đầu gọi đến phòng bưu chính ở Largo để xem họ có nhận được gì không. Trong cuộc gọi gần đây nhất, họ bắt tôi chờ máy khá lâu. Khi người phụ nữ quay lại nhấc máy, cô ta xin lỗi và nói rằng văn phòng đang chuyển địa điểm, cô ta sẽ phải "tìm kỹ" lại bưu phẩm của tôi. Phải, chính xác thì linh cảm mách bảo tôi rằng họ đang nghi ngờ tôi.

https://thuviensach.vn

Vài ngày sau, tôi nhờ tới sự trợ giúp của Lewis De Payne, người rất hứng thú với ý tưởng lấy mã nguồn của chiếc điện thoại đang nổi tiếng đó. Cậu ta đã nghiên cứu qua và tìm hiểu được rằng Chủ tịch Nokia Mỹ là một người tên là Kari-Pekka ("K-P") Wilska. Vì một vài lý do ngớ ngẩn đáng xấu hổ, Lewis quyết định đóng giả làm Wilska, một người Phần Lan và gọi đến văn phòng Largo để yêu cầu chuyển gói hàng đi.

Mãi sau này chúng tôi mới biết được rằng các đặc vụ của FBI đã được cảnh báo và đến văn phòng Largo, nơi họ đã chuẩn bị để ghi âm lại cuộc gọi đến tiếp theo của bất kỳ ai trong hai bọn tôi.

Lewis giả danh là Wilska gọi đến đó. Cậu ta xác nhận gói hàng đã tới và yêu cầu chuyển nó đến Ramada Inn gần văn phòng mình. Tôi gọi đến khách sạn đặt phòng cho Wilska, biết rằng lễ tân sẽ giữ gói hàng gửi cho khách đặt phòng đang tới.

Chiều hôm sau, tôi gọi đến khách sạn để chắc rằng gói hàng đã sẵn sàng chờ lấy. Người phụ nữ mà tôi nói chuyện nghe có vẻ không thoải mái và bắt tôi chờ máy nhưng rồi lại quay sang nói vâng, gói hàng đã ở đây. Tôi hỏi cô ta nó to bằng nào. Cô ta nói: "Họ để nó ở quầy lễ tân, để tôi ra xem đã."

Cô ta lại cho tôi chờ máy và đi một lúc lâu. Tôi bắt đầu bồn chồn, có chút hoảng sợ. Đây là một báo động to đùng.

Cuối cùng, cô ta trở lại nghe máy và mô tả kích cỡ gói hàng, nghe có vẻ khá phù hợp với một chiếc đĩa máy tính.

Nhưng giờ tôi lại cảm thấy thực sự khó chịu. Liệu quầy lễ tân có thực sự có gói hàng không, hay đây chỉ là một màn dàn dựng, một cái bẫy? Tôi hỏi: "Gói hàng được chuyển đến bằng FedEx hay UPS vậy?" Cô ta nói sẽ xem và lại bắt tôi chờ máy. Ba phút. Năm phút. Khoảng tám phút trôi qua trước khi tôi nghe thấy giọng cô ta nói với tôi lần nữa: "Là FedEx."

"Được rồi," tôi nói. "Cô có gói hàng ngay trước mặt mình không?"

https://thuviensach.vn

“Tôi có.”

“Được rồi, hãy đọc số tracking cho tôi.”

Thay vào đó, cô ta lại bắt tôi chờ máy thêm lần nữa.

Tôi không cần phải là nhà khoa học siêu việt để phát hiện ra có gì đó không ổn ở đây.

Đắn đo chừng nửa tiếng, tôi tự hỏi mình nên làm gì. Tất nhiên, lựa chọn hợp lý duy nhất là quay lưng bước đi và quên đi toàn bộ câu chuyện.

Nhưng tôi đã trải qua quá nhiều khó khăn để lấy được mã nguồn này, tôi thực sự muốn có nó. “Hợp lý” hay không đã không còn nằm trong tính toán.

Sau nửa tiếng, tôi gọi đến khách sạn lần nữa và xin nói chuyện với quản lý đang trực.

Khi anh ta nhấc máy, tôi nói: “Tôi là đặc vụ Wilson ở FBI. Anh có biết tình hình trong khách sạn không?” Tôi mong anh ta trả lời rằng anh ta không hiểu tôi đang nói về điều gì.

Thay vào đó, anh ta lại trả lời: “Tất nhiên tôi biết! Cảnh sát đã cho giám sát cả tòa nhà rồi!”

Những lời của anh ta như cả tấn gạch nện vào người tôi.

Anh ta bảo tôi rằng một sĩ quan vừa vào văn phòng của anh ta và tôi nên nói chuyện với viên sĩ quan đó.

Viên sĩ quan nhấc máy. Lấy giọng ra vẻ quyền chức, tôi hỏi tên anh ta. Anh ta trả lời tôi.

Tôi nói mình là đặc vụ Jim Wilson ở Đội Tội phạm Cổ cồn Trắng. “Chuyện gì đang xảy ra dưới đó vậy?” tôi hỏi. Viên sĩ quan nói: “Mấy gã của chúng ta

https://thuviensach.vn

vẫn chưa đến.” Tôi nói: “Được rồi, cảm ơn vì đã cho tôi biết tình hình” và gác máy.

Đúng là suýt chết.

Tôi gọi cho Lewis. Cậu ta vừa bước chân ra khỏi cửa để đi lấy gói hàng. Tôi hét vào điện thoại: “Khoan đã! Là bẫy đấy.”

Nhưng tôi không thể để gói hàng ở đó. Tôi gọi đến một khách sạn khác và đặt phòng cho K-P Wilska, rồi gọi lại cho người phụ nữ ở Ramada Inn và bảo với cô ta: “Tôi cần cô chuyển lại gói hàng đến một khách sạn khác. Kế hoạch của tôi vừa có chút thay đổi và tôi sẽ ở đó tối nay để kịp cuộc họp sáng sớm mai.” Tôi đưa cô ta tên và địa chỉ khách sạn mới.

Tôi đoán tôi có thể cũng nên để FBI theo đuổi một đầu mối giả khác trong một thời gian.

Khi nhìn thấy quảng cáo cho chiếc điện thoại di động mới nhất của NEC, tôi không quan tâm quá nhiều đến bản thân chiếc điện thoại; tôi chỉ biết rằng mình phải có được mã nguồn. Việc tôi lấy được mã nguồn của nhiều chiếc điện thoại đang sốt khác không phải là vấn đề: Đây sẽ là chiến tích tiếp theo của tôi.

Tôi biết rằng NEC, một công ty con của NEC Electronics, có một tài khoản của nhà cung cấp dịch vụ Internet Netcom. ISP này đã trở thành một trong những tuyến chính của tôi để truy cập vào Internet, một phần bởi họ sẵn tiện cung cấp tất cả các số dial-up cho gần như mọi thành phố lớn.

Tôi gọi đến trụ sở NEC của Mỹ tại Irving, Texas và được biết rằng công ty đang phát triển tất cả phần mềm điện thoại di động tại Fukuoka, Nhật Bản. Chỉ bằng vài cuộc gọi đến NEC Fukuoka, tôi đã tiếp cận được Ban Radio Di động, nơi người trực điện thoại đã tìm được một người nói tiếng Anh để phiên dịch cho tôi. Đây luôn là một lợi thế, bởi người phiên dịch sẽ cung cấp tính xác thực: Cô ta có thể ở ngay trong cùng tòa nhà, nói cùng ngôn ngữ

https://thuviensach.vn

với mục tiêu của bạn. Người ở cuối chuỗi này sẽ có xu hướng tin tưởng bạn là người đã được xét duyệt rồi. Và trong trường hợp này, mức độ tin cậy rất cao trong văn hóa Nhật Bản cũng góp phần tạo nên sự tin tưởng đó.

Người phiên dịch tìm được một người có thể giúp tôi, người mà cô giới thiệu là một trong những kỹ sư phần mềm đứng đầu nhóm. Tôi bảo cô ấy hãy nói với anh ta: "Đây là Ban Radio Di động ở Irving, Texas. Chúng tôi đang gặp khủng hoảng ở đây. Chúng tôi vướng phải một tai nạn khủng khiếp có liên quan đến việc hư hỏng ổ cứng và làm mất phiên bản mã nguồn mới nhất cho một vài chiếc điện thoại di động."

Câu trả lời của anh ta là: "Tại sao các anh không lấy nó trên mrdbolt?"

Hừmmm. Nó là cái gì vậy?

Tôi thử nói: "Chúng tôi không thể truy cập máy chủ do sự cố đó." Tôi đã vượt qua bài kiểm tra – "mrdbolt" rõ ràng là tên máy chủ của nhóm phần mềm này.

Tôi nhờ kỹ sư FTP nó đến tài khoản NEC Electronics trên Netcom. Nhưng tôi lại gặp phản ứng bởi việc đó đồng nghĩa với việc gửi dữ liệu nhạy cảm đến một hệ thống bên ngoài công ty.

Giờ phải làm sao đây? Để kiếm thêm thời gian, tôi nói với phiên dịch viên rằng tôi phải nghe một cuộc điện thoại và sẽ gọi lại sau ít phút.

Đầu tôi nảy số, dựng lên một giải pháp nghe có vẻ ổn hơn: Tôi sẽ nhờ Bộ phận Chuyển giao của NEC, phân nhóm sản xuất ô tô của công ty, làm trung gian, nơi nhân viên có lẽ không phải làm việc nhiều với những thông tin nhạy cảm, tuyệt mật của công ty và vì vậy, họ sẽ ít để tâm đến an ninh hơn. Ngoài ra, tôi thậm chí sẽ không hỏi thêm thông tin gì nữa.

Tôi nói với người tôi gặp ở Nhóm Sản xuất ô tô: "Chúng tôi đang gặp trục trặc về đường mạng giữa NEC Nhật Bản và Texas." Tôi nhờ anh ta thiết lập

https://thuviensach.vn

một tài khoản tạm thời để tôi có thể FTP một tập tin về chỗ anh ta. Anh ta không thấy việc này có vấn đề gì. Trong khi tôi đợi điện thoại, anh ta đã thiết lập một tài khoản và cho tôi tên máy chủ của NEC, cũng như thông tin đăng nhập.

Tôi gọi lại cho bên Nhật Bản và cung cấp thông tin này để phiên dịch viên truyền đạt lại. Giờ thì họ sẽ chuyển mã nguồn đến một cơ sở NEC khác, dù việc này có vẻ hơi miễn cưỡng với họ. Họ mất khoảng năm phút để hoàn tất việc chuyển tập tin. Khi tôi gọi lại cho người ở Bộ phận Chuyển giao, anh ta xác nhận tập tin đã được chuyển đến. Do cách tôi thiết lập, anh ta mặc nhiên cho rằng tôi đã gửi nó. Tôi đưa anh ta hướng dẫn để FTP tập tin đến tài khoản NEC Electronics tại Netcom.

Sau đó, tôi truy cập vào Netcom và chuyển mã nguồn về một trong những máy chủ tại USC mà tôi đang dùng làm tủ khóa.

Vụ hack này quả là một mẻ lớn, nhưng với tôi, nó lại quá dễ dàng. Tôi vẫn chưa thấy được thỏa mãn.

Vì vậy sau đó, tôi đặt mình vào một thử thách còn lớn hơn: đột nhập vào mạng của NEC và tải về mã nguồn của tất cả các điện thoại NEC tại Mỹ. Trong lúc làm việc đó, có lẽ tôi cũng nên thiết lập ở cả Anh và Úc nữa, đề phòng một ngày nào đó, tôi lại quyết định thử sống ở một trong các quốc gia đó thì sao?

Matt Ranney, nhân viên ở NEC Dallas, đã tạo sẵn một tài khoản dial-in cho tôi dựa trên câu chuyện về chuyến ghé thăm ngắn ngày của tôi tại cơ sở NEC ở San Jose, California cùng với nhu cầu kết nối nội bộ – dù lúc đầu tôi đã phải thuyết phục cả sếp của anh ta. Một khi đã đăng nhập thành công, tôi rất dễ lấy được quyền root thông qua một trong những lỗ hổng mà tôi tìm được từ cuộc hacking lần trước vào Sun. Thêm một cửa hậu vào chương trình log-in, tôi tự tạo cho mình một mật khẩu bí mật – ".hackman." – cho phép tôi đăng nhập vào tài khoản của bất kỳ ai, kể cả root. Sử dụng một

https://thuviensach.vn

công cụ khác từ những mẹo mực hacking của mình, tôi "sửa checksum[77]", để phiên bản đã bị cài cửa hậu của phần mềm log-in ít có khả năng bị phát hiện hơn.

[77] Checksum (từ viết tắt của SUMmation CHECK). Trong truyền thông dữ liệu, đây là một phương pháp kiểm lỗi, trong đó số bit trong một đơn vị dữ liệu được cộng lại và truyền đi cùng với dữ liệu. Sau đó máy tính thu nhận sẽ kiểm tra lại tổng số này. Nếu tổng số này bị sai, thì có thể có một lỗi đã xuất hiện trong quá trình truyền. (BTV)

Vào thời đó, quản trị viên hệ thống sẽ phải thực hiện checksum trên một chương trình hệ thống, ví dụ như "log-in", để xem nó có bị thay đổi hay không. Sau khi dịch xong một phiên bản mới của log-in, tôi sửa lại checksum về giá trị ban đầu, nhờ vậy, ngay cả khi phần mềm đã bị cài cửa hậu, mọi bài kiểm tra trả về đều không thể tìm thấy kết quả những gì tôi đã làm.

Lệnh "finger" của Unix cho tôi biết tên người dùng đang đăng nhập vào mrdbolt. Một trong số họ là Jeff Lankford; danh sách cho tôi biết số điện thoại văn phòng của ông ta và ông ta vừa gõ lệnh trên bàn phím hai phút trước.

Tôi gọi cho Jeff, giả là "Rob ở bộ phận IT" và hỏi: "Bill Puknat có đó không?" tôi đưa tên của một kỹ sư khác trong Ban Radio Di động. Bill không có ở đó.

"Ôi, chết thật. Anh ấy vừa gọi cho chúng tôi yêu cầu trợ giúp, nói rằng mình không thể tạo được các tập tin bắt đầu bằng một dấu chấm. Các anh có gặp phải vấn đề đó không?"

Không.

"Các anh có tập tin .rhosts không?"

https://thuviensach.vn

“Nó là cái gì vậy?”

À, nghe thật êm tai, giống như một người trong đoàn diễu hành phệt một vết phấn lên lưng áo của ai đó để những người diễu hành khác biết nạn nhân là một gã khờ, hay một “dấu” (mark) (người dễ bị lợi dụng, đây là nguồn gốc của nghĩa này).

“Ồ, được rồi,” tôi nói. “Anh có thể dành ra vài phút chạy bài kiểm tra để tôi có thể chốt phiếu trợ giúp[78] này không?”

[78] Phiếu trợ giúp (trouble ticket): Phiếu yêu cầu hỗ trợ ghi thông tin về vấn đề của khách hàng hoặc yêu câu dịch vụ hỗ trợ. (ND)

“Tất nhiên.”

Tôi bảo ông ta gõ:

echo “+ +” >~ .rhosts

Đúng, một dạng hack .rhosts. Tôi giải thích hợp lý cho ông ta từng bước một, rất chậm rãi, để ông ta nghĩ ông ta hiểu chuyện gì đang diễn ra.

Sau đó, tôi nhờ ông ta gõ “ls -al” để lấy thư mục chứa toàn bộ tập tin của ông ta.

Trong lúc thư mục của ông ta hiện trên màn hình máy trạm, tôi gõ:

rlogin lankforj@mrdbolt

để đăng nhập vào tài khoản của ông ta, “lankforj”, trên máy chủ mrdbolt.

Và tôi đã vào được tài khoản của ông ta mà không cần mật khẩu.

Tôi hỏi Jeff có thấy tập tin .rhosts chúng tôi vừa tạo không và ông ta xác nhận có thấy. “Tuyệt vời,” tôi nói. “Giờ tôi có thể chốt phiếu trợ giúp này rồi. Cảm ơn đã dành thời gian kiểm tra nó.”

https://thuviensach.vn

Rồi tôi nhờ ông ta xóa tập tin đó đi để khiến mọi thứ trở về như trạng thái ban đầu.

Tôi thấy rất phấn khích. Ngay khi ngắt máy, tôi nhanh chóng chiếm quyền root và cài đặt cửa hậu log-in lên máy chủ mrdbolt. Tôi bắt đầu gõ với tốc độ siêu nhanh, sự phấn khích khiến tôi không thể ngừng tay lại.

Phán đoán của tôi là chính xác: mrdbolt là đường dẫn chính, kết nối dùng để chia sẻ công việc phát triển giữa Ban Radio Di động, NEC Mỹ và NEC Nhật Bản. Tôi tìm thấy nhiều phiên bản mã nguồn cho nhiều mẫu điện thoại di động NEC khác nhau. Nhưng mã nguồn tôi thực sự muốn, cho NEC P7, lại không có trên mạng. Chết tiệt! Tất cả nỗ lực đó của tôi vẫn chưa được trả công.

Vì đã ở sẵn trên mạng nội bộ của họ, nên tôi có thể lấy mã nguồn từ NEC Nhật Bản. Vài tuần sau, tôi lấy thêm được quyền truy cập đến tất cả máy chủ do Ban Radio Di động ở Yokohama sử dụng mà không gặp mấy khó khăn.

Tôi tiếp tục tìm kiếm mã nguồn cho chiếc điện thoại đó nhưng lại phát hiện ra có quá nhiều thông tin dư thừa: Công ty đang phát triển điện thoại cho một số thị trường khác nhau, bao gồm Anh, các quốc gia châu Âu khác và Úc. Vậy là quá đủ; đã đến lúc tôi tìm ra một cách tiếp cận đơn giản hơn.

Tôi kiểm tra máy chủ mrdbolt để xem ai đã đăng nhập vào đó. Jeff Lankford có vẻ như rất thích thú với việc này: Ông ta ở trên mạng rất muộn sau khi đã hết ngày làm việc bình thường.

Theo kế hoạch đã vạch sẵn trong đầu, tôi cần sự riêng tư. Darren và Liz đã rời sở, Ginger chuyển ca, nên cô ta vẫn ngồi loanh quanh, nhưng văn phòng của cô ta ở phía đối diện phòng máy tính. Tôi khép hờ cửa vào chỗ tôi ngồi cùng các đồng nghiệp, chỉ để lại khe hở đủ để nhìn xem có ai đến không.

Những gì tôi sắp làm rất liều lĩnh. Dù không phải là Rich Bé bỏng khi nói đến việc giả ngữ điệu, nhưng tôi đang chuẩn bị đóng giả là Takada-san, đến

https://thuviensach.vn

từ Ban Radio Di động của NEC Nhật Bản.

Tôi gọi đến số máy bàn của Lankford. Khi ông ta nhấc máy, tôi bắt đầu màn diễn:

“Ôngggg, ahhhh, Lahngfor, tôi Takada-san... đến từ Nhật Bản.” Ông ta biết cái tên này và hỏi mình có thể giúp gì.

“Ông ggg Lahng...for – chúng tôi tìm thấy không, ahhhh, phiên ba khôngggggg năm cho hotdog dự án” – sử dụng tên mã tôi tìm thấy cho mã nguồn NEC P7. “Ông có thể, ahhh, cho lên mrdbolt?”

Ông ta đảm bảo với tôi rằng ông ta có phiên bản 3.05 trên đĩa mềm và có thể tải nó lên.

“Ahhh, cảm ơn ... ahhh, cảm ơn, ông Jeff ... tôi sẽ kiểm tra mrdbolt sớm. Tạm biệt.”

Ngay khi tôi vừa rũ bỏ ngữ điệu rõ ràng là không quá tệ của mình, cánh cửa bật mở và Ginger đang đứng đó.

“Eric... anh đang làm gì vậy?” cô ta hỏi.

Không đúng lúc chút nào.

“À, chỉ chơi khăm một anh bạn của tôi thôi,” tôi trả lời.

Cô ta nhìn tôi với vẻ kỳ lạ, rồi quay lưng bỏ đi.

Oa! Suýt chết!

Tôi đăng nhập vào mrdbolt và đợi Jeff tải xong mã nguồn, rồi lập tức chuyển nó đến một hệ thống ở USC để lưu trữ.

Trong suốt thời gian đó, tôi luôn tìm trong tất cả e-mail của quản trị viên ở NEC các từ khóa như: FBI, theo dấu, hacker, gregg (tên tôi đang dùng), bẫy

https://thuviensach.vn

và bảo mật.

Một ngày, tôi đọc được một tin nhắn khiến tôi nổi da gà toàn thân:

FBI gọi đến vì mã nguồn xuất hiện tại nơi họ đang theo dõi tại Los Angeles. Ngày 10 tháng 5, các tập tin này được FTP từ netcom7 đến một nơi tại Los Angeles. 5 tập tin, chứa khoảng 1 meg dữ liệu. 1210-29.lzh p74428.lzh v3625dr.lzh v3625uss.lzh v4428us.scr. Kathlenn gọi Bill Puknat.

Puknat – người tôi đã dùng tên trong cuộc gọi đầu tiên với Jeff Lankford – kỹ sư phần mềm đứng đầu Ban Radio Di động tại Mỹ. "Kathleen" chắc chắn là Kathleen Carson, đến từ FBI Los Angeles. Và "nơi họ đang theo dõi tại Los Angeles" chắc chắn có nghĩa là FBI đang theo dõi các hệ thống tôi đang lưu trữ tập tin của NEC: USC. Họ đã theo dõi hầu hết hoặc tất cả các hoạt động chuyển tập tin của tôi đến USC.

Khốn kiếp!

Tôi cần phải tìm hiểu xem tôi đã bị theo dõi như thế nào và việc này đã diễn ra trong bao lâu.

* * *

Xem xét hệ thống đang dùng tại USC, tôi phát hiện ra một chương trình theo dõi được sử dụng để bí mật giám sát các hoạt động của tôi và thậm chí còn có thể xác định được quản trị viên hệ thống USC đã cài đặt nó – một người tên là Asbed Bedrossian. Núi cao còn có núi cao hơn, tôi tìm ra máy chủ nơi gã này và các quản trị viên USC khác nhận e-mail – sol.usc.edu – để lấy quyền root và thử tìm từ khóa FBI trong mail của Asbel. Tôi đọc được những dòng này:

Chú ý! Chúng ta gặp phải vấn đề về bảo mật. Chúng ta có hai tài khoản do FBI và quản trị viên hệ thống ASBED theo dõi. Các tài khoản này đã bị

https://thuviensach.vn

chiếm đoạt. Nếu anh nhận được cuộc gọi từ ASBED, hãy cộng tác bằng cách chụp lại và sao chép tập tin. Cảm ơn!

Mấy gã đó tìm ra một tài khoản của tôi đã đủ tệ rồi; giờ tôi còn biết họ đã tìm ra cả cái thứ hai. Tôi lo lắng nhưng đồng thời cũng tức giận vì đã không phát hiện ra việc bị giám sát sớm hơn.

Tôi đoán ASBED hẳn đã phát hiện ra một lượng lớn dung lượng trong ổ cứng đã bị chiếm dụng mà không rõ lý do. Chỉ cần liếc qua, anh ta sẽ ngay lập tức nhận ra có tay hacker nào đó đang lưu trữ phần mềm ăn cắp trên hệ thống. Vì từng chiếm dụng nhiều hệ thống USC để lưu trữ mã nguồn trong lần hack DEC hồi năm 1988, nên tôi cho rằng mình sẽ đứng đầu danh sách nghi phạm.

Sau này, tôi biết được rằng FBI đã xem qua các tập tin và gọi cho các công ty để cảnh báo rằng mã nguồn độc quyền của họ đã bị đánh cắp khỏi hệ thống và đang nằm trên máy chủ tại USC.

Jonathan Littman đã viết cuốn sách The Fugitive Game (tạm dịch: Trò chơi lẩn trốn) kể về cuộc gặp diễn ra hồi đầu năm 1994 tại văn phòng FBI ở Los Angeles do ủy viên công tố David Schindler triệu tập. Tham dự buổi gặp là các nhà đại điện "xấu hổ và tràn đầy cảnh giác" đến từ các công ty sản xuất điện thoại di động lớn mà tôi từng hack. Không ai muốn người khác biết công ty mình là nạn nhân của một vụ hack – ngay cả trong căn phòng chỉ toàn là nạn nhân này. Littman kể Schindler bảo với ông ấy rằng: "Tôi phải dùng đến tên giả. Ông này đến từ công ty A, ông kia đến từ công ty B. Họ sẽ không làm gì đâu."

"Mọi người đều nghi ngờ Mitnick," Littman viết, không quên kể thêm rằng Schindler đã hỏi to: "Mục đích của việc lấy tất cả chỗ mã nguồn này là gì? Có ai đó đang trả tiền cho hắn? Hắn có đang rao bán nó không? Hãy đánh giá hiểm họa xem hắn có thể làm gì với nó?"

https://thuviensach.vn

Rõ ràng, không ai trong số họ nghĩ đến chuyện tôi làm việc đó chỉ vì thử thách. Schindler và những người khác đang mắc kẹt trong "lối tư duy Ivan Boesky[79]": Với họ, hacking là vô nghĩa nếu không được sử dụng để kiếm tiền.

[79] Ivan Frederick Boesky: Là một cựu thương nhân chứng khoán người Mỹ đã trở nên nổi tiếng với vai trò nổi bật của mình trong một vụ bê bối thương mại nội bộ đã xảy ra tại Mỹ vào giữa những năm 1980. (BTV)

https://thuviensach.vn

30
ĐÁNH LÉN

Ouop lqeg gs zkds ulv V deds zq lus DS urqstsn't wwiaps?

Tới cuối mùa xuân năm 1994, tôi vẫn dùng thân phận Eric Weiss và làm việc tại hãng luật ở Denver. Tôi thường dành cả giờ nghỉ trưa trên điện thoại. Thời ấy, mỗi phút dùng mạng Wi-fi tốn 1 đô-la, và còn xa mới tới thời kỳ người người rảnh rang tán gẫu trên mạng không dây. Nghĩ lại thì khi ấy trông tôi hẳn phải rất đáng ngờ vì dành nhiều thời gian trên điện thoại di động đến như vậy, đặc biệt là khi tôi chỉ kiếm được 28.000 đô-la mỗi năm.

Một ngày nọ, tất cả nhân viên của Phòng IT cùng ăn trưa với Elaine và sếp của cô ta, Howard Jenkins. Trong lúc tán gẫu, Howard hỏi tôi: "Eric, anh học ở Washington nhỉ? Anh cách Seattle bao xa?"

Tôi cho rằng mình đã nghiên cứu đủ sâu để che giấu bản thân, nhớ được tên của vài vị giáo sư dạy tại Ellenburg trong những năm tương ứng với nội dung ghi trong sơ yếu lý lịch và những điều tương tự. Nhưng thú thực, tôi không biết phải trả lời câu hỏi này thế nào. Tôi giả vờ ho sù sụ, vẫy tay xin thứ lỗi và nhanh chóng lao vào nhà vệ sinh nam, miệng vẫn không ngừng ho.

Từ trong buồng vệ sinh, tôi gọi tới Đại học Central Washington bằng di động và nói với người phụ nữ ở phòng giáo vụ rằng tôi đang suy nghĩ về việc nộp hồ sơ và tự hỏi sẽ mất bao lâu để lái xe từ Seattle tới đó. "Khoảng hai giờ đồng hồ," cô ta nói, "nếu không phải giờ cao điểm."

Tôi nhanh chóng quay lại bàn, xin lỗi vì đã chạy mất, giải thích rằng có lẽ mình bị nghẹn đồ ăn. Khi Howard nhìn tôi, tôi nói: "Xin lỗi, nhưng ban nãy

https://thuviensach.vn

anh hỏi gì tôi nhỉ?" Ông ta nhắc lại câu hỏi trước.

"À, khoảng hai giờ nếu đường không đông lắm," tôi trả lời. Tôi mỉm cười và hỏi ông ta từng tới Seattle bao giờ chưa. Trong suốt phần còn lại của bữa trưa, không còn câu hỏi nào nhắm tới tôi nữa.

Trừ mối lo ngại liên quan đến việc che giấu thân phận, công việc của tôi khá suôn sẻ trong hơn một năm. Sau đó, tôi bị đánh lén. Khi tìm một số tài liệu trên bàn Elaine vào buổi tối nọ, tôi bắt gặp một bì thư mở có chứa nội dung quảng cáo đăng tin cần tìm chuyên gia IT. Mô tả nhiệm vụ trên tin tuyển dụng hoàn toàn khớp với công việc của Darren. Hoặc tôi.

Đây quả là một hồi chuông cảnh báo. Elaine chưa từng nhắc tới việc hãng muốn tuyển thêm người, như vậy chỉ có một giải thích duy nhất: Cô ta và sếp mình đã sẵn sàng sa thải một trong số chúng tôi. Nhưng ai sẽ là kẻ chịu trận?

Ngay lập tức, tôi lao vào tìm kiếm câu trả lời. Càng cố khám phá, việc đâm lén này càng trở nên phức tạp. Tôi biết Elaine không hài lòng với Darren, liên quan tới việc anh ta bị phát hiện đã gặp gỡ tư vấn khách hàng riêng trong giờ làm việc. Tôi lại phát hiện ra một manh mối khác trong e-mail của Ginger gửi cho Elaine có đoạn: "Eric ở đây suốt ngày, chăm chú làm việc gì đó mà tôi không biết."

Tôi cần thêm thông tin. Sau giờ làm, tôi xuống Phòng Nhân sự ở tầng 41. Tôi đã nghiên cứu khu vực này vài ngày trước đó. Công nhân dọn vệ sinh thường có thói quen bắt đầu ca trực bằng việc mở toang tất cả các cửa, thật hoàn hảo. Tôi lách mình vào, hy vọng có thể nhờ cậy vào khả năng bẻ khóa của mình.

Khóa wafer[80] trên tủ hồ sơ của vị quản lý bật mở ngay lần thử thứ hai – tuyệt. Tôi kéo tập hồ sơ của mình ra và phát hiện phán quyết đã được định sẵn: Khi mọi người trở lại với công việc sau cuối tuần ngày Tưởng niệm Thương binh liệt sĩ, tôi sẽ nhận được thông báo sa thải.

https://thuviensach.vn

[80] Khóa wafer: Sử dụng lẫy là các tấm kim loại thay vì các cặp pin như trong loại khóa thông thường. Các tấm kim loại này được đẩy xuống nhờ các lò xo vào các rãnh then, do đó trục khóa không thể xoay được. (BTV)

Lý do ư? Elaine nghĩ tôi đang làm việc tự do, nhận tư vấn khách hàng bên ngoài trong giờ làm việc của công ty. Điều đáng mỉa mai đó là công việc này có lẽ là hoạt động đáng ngờ duy nhất mà tôi không làm tại thời điểm này. Elaine hẳn đã đưa ra kết luận dựa trên việc tôi sử dụng di động trong suốt bữa trưa và giờ nghỉ giải lao, và cô ta đã hoàn toàn sai lầm.

Nhân tiện, tôi kéo cả hồ sơ của Darren và phát hiện ra anh ta cũng sẽ bị sa thải. Tuy nhiên, trong trường hợp này, họ có chứng cớ rõ ràng rằng anh ta đã nhận tư vấn cho các khách hàng khác. Tệ hơn cả là anh ta đã làm việc này trong giờ làm. Có vẻ như tôi và anh ta bị đánh đồng vào làm một. Họ biết Darren phá luật và hiển nhiên cho rằng tôi cũng vậy, dù chẳng có chứng cứ gì.

Ngày tiếp theo, để mò thêm thông tin, tôi tiếp cận Ginger: “Tôi nghe nói họ đang tìm người mới cho đội IT. Ai sẽ bị sa thải thế?” Chỉ trong vòng vài phút, cô ta chuyển câu hỏi của tôi cho Elaine và trong vòng chưa tới một giờ, tôi được báo rằng Howard Jenkins muốn gặp tôi trong văn phòng của Maggie Lane, nhân viên Phòng Nhân sự, ngay lập tức. Đúng là ngu ngốc, tôi nghĩ. Tự dưng lại ngứa mồm.

Nếu tôi biết chuyện này sẽ xảy đến, lẽ ra tôi nên dành cả ngày cuối tuần để xóa bỏ dấu vết, xóa sạch khỏi máy tính mọi thứ (có rất nhiều tập tin ở trong đó), những thứ có thể dùng để buộc tội tôi. Đến lúc cao trào nhất, tôi ném đĩa từ, đĩa mềm và bất kỳ thứ gì tôi có thể nghĩ tới vào túi rác, sau đó kéo lê chúng đi và ném vào thùng rác trong khu vực đỗ xe ở bên đường.

Khi tôi quay trở lại, Elaine hết sức tức giận: “Họ đang đợi anh!” cô ta nói. Tôi nói rằng mình cảm thấy cồn cào trong ruột và sẽ quay trở lại sớm nhất có thể.

https://thuviensach.vn

Dự định giả ngu khi bị buộc tội nhận tư vấn thêm trong giờ làm việc không có tác dụng. Tôi đã thử cách tiếp cận: “Tôi không nhận tư vấn, bằng chứng là gì?” nhưng họ không thèm để tâm. Đơn giản là sa thải.

Vậy là tôi đã bị cắt hoàn toàn nguồn thu nhập. Tệ hơn là hãng luật có vẻ đã điều tra quá trình học hành của tôi, hoặc Sở Thuế vụ đã phát hiện ra số An sinh Xã hội mà tôi sử dụng thuộc về Eric Weiss thực sự.

Không dám ở trong căn hộ của mình qua đêm, tôi tìm một nhà nghỉ gần Cherry Creek, khu vực yêu thích của tôi ở Denver. Sáng hôm sau, tôi thuê một chiếc xe tải U-Haul dài 4m, đóng gói toàn bộ đồ đạc cá nhân và trên đường quay trở lại nhà nghỉ thì rẽ ngang vào một cửa hàng cho thuê đồ đạc, bịa ra câu chuyện khẩn cấp trong gia đình, trao lại chìa khóa căn hộ, thanh toán tiền và đề nghị nhân viên ở đây tới lấy lại giường, bàn, tủ, tivi, v.v...

Khi dừng xe tại nhà nghỉ, không để ý thấy chiếc U-Haul quá cao, tôi đâm xe vào trần bãi đỗ. Lo lắng rằng cảnh sát có thể được gọi tới để lập biên bản tai nạn, tôi đề nghị đền bù phần hư hại đó. Gã ở đó ra giá 500-đô-la, có thể hợp lý mà cũng có thể không, nhưng tôi vẫn trả tiền ngay lập tức, dù đó đúng là thời điểm tệ hại để tiêu mất số tiền tôi cần trang trải cuộc sống – cái giá của sự bất cẩn, nhưng cũng là cái giá của việc không muốn phải đối mặt với cảnh sát.

Dĩ nhiên, nhiệm vụ tiếp theo của tôi là tìm cách xóa sạch dữ liệu trên máy tính tôi dùng ở hãng luật. Nhưng phải làm sao đây khi tôi không còn làm việc ở đó nữa?

Vài tuần sau, Elaine đồng ý cho tôi quay lại và chuyển các tập tin “cá nhân” sang đĩa mềm, tức là tất cả số mã nguồn tôi có được từ những lần hacking gần đây. Cô ta ngồi cạnh bên khi tôi làm việc này và trông có vẻ nghi ngại khi thấy tôi xóa từng tập tin một sau khi đã chuyển chúng vào đĩa. Để đánh lạc hướng cô ta, tôi tạo một thư mục mang tên “Eric” trên máy tính và chuyển các tập tin vào đó thay vì xóa chúng. Sau này, tôi sẽ phải tìm cách

https://thuviensach.vn

nào đó để kết nối với máy tính từ xa hoặc lẻn vào công ty để xóa sạch các tập tin trong thư mục này.

Không lâu sau đó, tôi xốc lại tinh thần và quyết định gọi cho Ginger, lấy lý do "muốn giữ liên lạc" nhưng thực ra là hy vọng có thể lấy được chút thông tin hữu ích nào đó. Trong suốt cuộc gọi, cô ta luôn nhắc tới việc gặp rắc rối với hệ thống "BSDI" mà tôi đã cài đặt và quản lý nhằm kết nối hãng luật với mạng Internet.

Tôi nói với cô ta mình có thể giúp qua điện thoại. Trong quá trình hướng dẫn, tôi lừa cô ta gõ vào dòng lệnh:

nc –l –p 53 –e /bin/sh &

Ginger không nhận ra dòng lệnh đó đã cho tôi toàn bộ quyền tiếp cận root vào gateway máy chủ của công ty. Khi cô ta gõ dòng lệnh đó, nó sẽ chạy một chương trình có tên là "netcat", thiết lập một root shell[81] vào cổng 53, do đó, tôi có thể kết nối vào cổng và được trao cho một root shell tức thì, không cần tới mật khẩu. Cô ta hoàn toàn không phát hiện ra mình đã cài đặt thành công một cửa hậu đơn giản, cho tôi quyền tiếp cận root.

[81] Shell là chương trình phần mềm được phát triển dành cho các máy tính chạy hệ điều hành Unix và Linux. Shell cung cấp giao diện cho phép người dùng nhập và chạy các câu lệnh dưới (dạng văn bản) trên máy tính. Root shell là phần mềm chạy với quyền quản trị tối cao. (BTV)

Khi đã đăng nhập thành công, tôi kết nối vào hệ thống máy tính AViiON Data General của công ty, chạy ứng dụng kế toán điện thoại của hãng. Tôi đã cài đặt hệ thống cảnh báo sớm của mình tại đây trước đó. Lý do tôi phải kết nối với AViiON trước tiên là vì vấn đề an toàn: Nếu các sếp quyết định thay đổi mật khẩu trên cụm VMS sau khi sa thải tôi, tức là mọi nỗ lực thử đăng nhập trực tiếp vào cụm VMS với mật khẩu không chính xác sẽ kích hoạt cảnh báo bảo mật đăng nhập-sai từ hệ thống đóng vai trò gateway Internet của công ty. Với việc đăng nhập vào cụm VMS từ AviiON, tôi có

https://thuviensach.vn

thể đảm bảo rằng mật khẩu sai đó được thực hiện từ bên trong công ty. Như vậy, nếu có bất kỳ cảnh báo bảo mật nào thì cũng không phải là xuất phát từ gateway Internet, tránh chỉ thẳng vào tôi vì tôi vốn là người duy nhất từng đăng nhập vào đó.

Sau khi đăng nhập thành công vào hệ thống VMS, tôi mount[82] ổ cứng trên máy tính của mình từ xa; có như vậy tôi mới có quyền chỉnh sửa các tập tin và bí mật xóa toàn bộ những gì có thể dùng làm bằng chứng.

[82] Vì trên Linux chỉ có thư mục, không có khái niệm ổ đĩa A, B, C, D… như trên Windows, nên khi muốn sử dụng một thiết bị lưu trữ nào đó (ví dụ như ổ cứng), người dùng phải kết nối nó vào một thư mục để có thể truy cập nội dung trên thiết bị từ chỗ đó. (BTV)

Tìm kiếm e-mail của Elaine có nhắc tới tên tôi, tôi phát hiện ra công ty đang cố gắng tổng hợp bằng chứng tự bào chữa đề phòng trường hợp tôi muốn khởi kiện vì bị sa thải một cách vô lý – tôi hoàn toàn có căn cứ để làm việc này nhưng hiển nhiên là tôi không muốn liều lĩnh. Liz được yêu cầu viết tất cả những quan sát cho thấy tôi đã thực hiện tư vấn riêng trong giờ làm việc, cô ta đã trả lời như sau:

Tôi không biết cụ thể về các vấn đề tư vấn riêng của Eric… Anh ấy luôn bận rộn nhưng tôi không rõ anh ấy đang làm gì. Anh ấy dùng điện thoại di động và máy tính rất nhiều.

Đó là tất cả những gì họ có thể thu được từ bất kỳ ai để biện hộ cho việc sa thải tôi. Nhưng đó là một kết quả tìm kiếm có giá trị, bởi điều đó có nghĩa là các vị sếp cũ của tôi chưa phát hiện ra sự thực về tôi.

Tôi tiếp tục kiểm tra các e-mail của công ty trong nhiều tháng sau đó để đảm bảo không có ai lật ngược vụ việc có tên tôi. Không có gì quan trọng xảy ra.

Dù vậy, tôi vẫn duy trì liên lạc với Ginger, thỉnh thoảng lại gọi điện cho cô ta trong vai một người đồng nghiệp cũ để nghe vài mẩu tin vịt trong công ty.

https://thuviensach.vn

Khi tôi nói mình định nộp hồ sơ xin trợ cấp thất nghiệp, cô ta thừa nhận rằng công ty đã rất lo lắng về việc tôi có thể đâm đơn kiện vì bị sa thải vô lý.

Vậy là sau khi tôi bị sa thải, họ nhận ra cần phải điều tra để xem có thể tìm được một lý do hợp thức hóa việc sa thải tôi hay không. Tôi đã không còn lý do gì để duy trì dịch vụ trả lời điện thoại ở Las Vagas cho công ty ảo Green Valley Systems, do đó, khi thử xác minh lại lịch sử tuyển dụng của tôi, họ đã phát hiện ra không có công ty nào như vậy tồn tại. Thêm nhiều nghi vấn khác được đặt ra.

Lần kế tiếp tôi gọi điện, Ginger nghĩ cô ta đã tung một quả bom chí mạng vào tôi: "Hãng luật đã kiểm tra lại. Và, Eric… anh không tồn tại!"

Ồ, vậy là cuộc đời thứ hai của Eric Weiss đã chấm dứt.

Không còn gì để mất, tôi nói với Ginger rằng tôi là một thám tử tư được thuê để thu thập chứng cứ chống lại hãng luật. Và "tôi không được phép thảo luận về chuyện này".

Tôi tiếp tục: "Có một việc tôi có thể nói với cô. Mọi thứ đều đã bị đặt thiết bị nghe lén – trong văn phòng của Elaine và dưới sàn nâng trong phòng máy tính." Tôi chắc là ngay sau đó Ginger hẳn phải đi – à không, chạy – tới văn phòng của Elaine để báo tin này. Tôi hy vọng chiến thuật giương đông kích tây này có thể khiến những câu chuyện tôi đã kể với Ginger trong quá khứ đều trở nên đáng ngờ – do đó, họ sẽ không biết phải tin vào đâu.

Tôi vẫn kiểm tra tài khoản Netcom của Lewis hằng ngày xem có tin nhắn gì của cậu ta cho tôi không. Chúng tôi bảo vệ nội dung trao đổi của mình bằng một chương trình mã hóa gọi là "PGP" (viết tắt của "Pretty Good Privacy" – Khá riêng tư).

Một ngày nọ, tôi thấy có tin nhắn, sau khi giải mã, nội dung là: "LITTMAN ĐÃ BỊ 2 ĐẶC VỤ FBI GHÉ THĂM!!!" Điều này khiến tôi lo sợ bởi tôi từng nói chuyện với Jon Littman qua điện thoại, lúc ấy anh ta đang viết một

https://thuviensach.vn

bài báo về tôi cho tờ Playboy. (Thực ra, đó là những gì anh ta nói ban đầu; sau này, anh ta còn kiếm được hợp đồng viết cả một cuốn sách về câu chuyện của tôi mà không thèm báo cho tôi biết. Nói chuyện với anh ta để viết một bài báo thì không vấn đề gì. Nhưng Littman không để lộ ra rằng anh ta đang viết cả cuốn sách về cuộc đời tôi mãi đến khi tôi bị bắt ở Raleigh. Trước đó, tôi từng từ chối lời mời hợp tác của John Markoff và vợ hắn, Katie Hafner, và sẽ không bao giờ đồng ý nói chuyện với Littman nếu anh ta nói cho tôi biết mình đang viết sách.)

Tôi thực sự thích Denver. Danh tính mới cố định dưới cái tên Brian Merrill đã sẵn sàng. Đã có lúc tôi loay hoay với ý tưởng chuẩn bị cho một cuộc đời hoàn toàn mới – công việc, căn hộ, nơi thuê đồ đạc, xe thuê, tất cả – để ổn định ở Denver mãi mãi. Tôi thích ở lại đây. Tôi đã tính tới chuyện chuyển sang phía bên kia thành phố và bắt đầu lại từ đầu với danh tính mới.

Nhưng rồi tôi mường tượng ra cảnh mình đang ngồi ăn ở nhà hàng với một đồng nghiệp mới, hoặc trong một buổi hẹn hò, hay thậm chí là vợ mình sau này, và ai đó sẽ bước tới với nụ cười rạng rỡ cùng một cái bắt tay: “Xin chào, Eric!” Có lẽ tôi có thể thoái thác rằng họ đã nhầm trong lần đầu tiên, nhưng nếu điều này xảy ra nhiều hơn một lần…

Không, đó không phải là sự mạo hiểm tôi sẵn lòng chấp nhận.

Vài ngày sau, tôi lái chiếc U-Haul chất đầy quần áo và đồ đạc rời khỏi Denver, đi về phía Tây Nam tới Las Vegas để thăm mẹ cùng bà ngoại, và lên kế hoạch cho những bước tiếp theo.

Đăng ký nhận phòng ở Budget Harbor Suites khiến tôi có cảm giác déjà vu[83] kỳ quái. Ngay cả lúc ngồi trong phòng và vùi đầu nghiên cứu nơi đặt chân kế tiếp tôi cũng thấy như vậy.

[83] Déjà vu: Cảm giác đã từng trải nghiệm một điều gì đó mà trên thực tế mình biết hoặc chưa từng trải qua. (ND)

https://thuviensach.vn

Tôi không ngừng cảnh giác, chưa từng quên Las Vegas là một nơi nguy hiểm như thế nào. Khi còn ở trong tù, tôi đã thấy mấy gã ở đó nếu không phải bị người yêu hoặc vợ tố cáo thì cũng là bị bắt khi đang tới thăm vợ, mẹ hoặc một thành viên nào đó trong gia đình hoặc bạn bè thân thiết. Nhưng tôi không thể vào thành phố mà không gặp mẹ và bà – họ là tất cả lý do tôi đến đây, mặc kệ những mối nguy hiểm triền miên.

Tôi chuẩn bị sẵn hệ thống cảnh báo sớm quen thuộc, một chiếc ham radio có thể dễ dàng điều chỉnh để truyền tiếp các bước sóng mà mấy sở liên bang thường dùng.

Việc tín hiệu của các sở bị mã hóa khiến tôi thấy thực sự bực mình. Tôi có thể nhận ra một trong số các đặc vụ ở quanh đây, nhưng không thể nắm được các tin truyền đi là về tôi hay ai khác. Tôi thử gọi tới văn phòng Motorola địa phương, phỉnh rằng mình là một đặc vụ FBI và dò hỏi xem liệu có thể lấy được chìa khóa mã hóa hay không. Không ổn rồi, gã nhân viên Motorola nói rằng anh ta không thể giúp được gì qua điện thoại, “nhưng nếu anh tới đây với bộ nạp khóa thì được.”

Phải – hẳn là tôi sẽ bước vào văn phòng của Motorola rồi nói rằng tôi là FBI và… hả? “Tôi quên mang theo mấy thứ chứng minh thân phận rồi.” Không đời nào.

Nhưng phải làm thế nào để phá được mã khóa của FBI đây? Sau khi suy nghĩ một hồi, tôi nghĩ ra phương án B.

Để giúp các đặc vụ có thể trao đổi đường dài, chính phủ đã lắp đặt các “bộ chuyển tiếp sóng” (repeater) trên cao nhằm chuyển tiếp tín hiệu. Sóng vô tuyến điện từ các đặc vụ được truyền tại một tần số và nhận ở một tần số khác; các bộ chuyển tiếp sóng có tần số đầu vào để nhận tín hiệu truyền tới kèm một tần số đầu ra để phát tín hiệu mà các đặc vụ có thể nghe được. Khi muốn biết xem có đặc vụ nào gần đó hay không, tôi chỉ cần đơn giản là theo dõi độ lớn của tín hiệu trên bước sóng đầu vào của bộ chuyển tiếp sóng.

https://thuviensach.vn

Cài đặt này cho phép tôi chơi một trò chơi nho nhỏ. Bất cứ khi nào tôi nghe thấy tiếng xì xào truyền tin, tôi sẽ giữ chặt phím "Transmit" (Truyền đi). Hành động này sẽ gửi đi một tín hiệu vô tuyến điện có tần số y hệt, nhờ vậy, tôi có thể làm nhiễu tín hiệu của họ.

Vì thế, đặc vụ thứ hai không thể nghe được tin truyền đi từ đặc vụ thứ nhất. Sau khoảng hai đến ba lần thử đi thử lại, các đặc vụ sẽ phát điên với máy bộ đàm của họ. Tôi có thể tưởng tượng được một trong số họ sẽ nói kiểu như: "Lỗi bộ đàm rồi. Để tôi tới chỗ nào nghe rõ hơn."

Và rồi họ sẽ bấm công tắc trên máy bộ đàm để tắt nó khỏi chế độ mã hóa, lúc này tôi đã có thể nghe được cuộc nói chuyện từ cả hai phía! Cho tới tận bây giờ, tôi vẫn thấy ngạc nhiên khi nhớ tới việc giải quyết dễ dàng đống mã hóa ra sao khi còn không cần đến bẻ mã.

Nếu nghe thấy ai đó nhắc tới "Mitnick" hay bất kỳ tín hiệu radio nào cho thấy tôi là đối tượng đang giám sát của họ, tôi sẽ biến mất ngay lập tức. Nhưng điều đó đã không xảy ra.

Tôi dùng mẹo nhỏ này mỗi lần ở Las Vegas. Các bạn có thể tưởng tượng điều này khiến tôi thoải mái hơn rất nhiều. Và cảnh sát liên bang chưa từng phát hiện ra việc đó. Họ hẳn đã phàn nàn với nhau về tính năng mã hóa dở hơi trên máy bộ đàm không ngừng làm hỏng chuyện. Xin lỗi nhé Motorola, họ có lẽ đang đổ lỗi cho các anh đấy.

Trong suốt khoảng thời gian ở Las Vegas, tôi liên tục tự hỏi, Mình sẽ đi đâu tiếp đây? Tôi muốn tới nơi nào đó có nhiều công việc liên quan tới công nghệ, nhưng Thung lũng Silicon có vẻ nằm ngoài suy nghĩ, bởi với tôi thì việc quay trở lại California chẳng khác nào tự chuốc lấy họa.

Nghiên cứu chỉ ra rằng dù ở Seattle nhiều mưa nhưng những ngày nắng hiếm hoi thường rất đẹp, đặc biệt là quanh vùng Lake Washington. Và trên hết thảy, thành phố còn có vô vàn nhà hàng và quán cà phê Thái. Đây có vẻ

https://thuviensach.vn

là một yếu tố kỳ quặc để đưa ra cân nhắc nhưng lúc đó, tôi đặc biệt thích đồ ăn và cà phê Thái, và đến giờ cũng vẫn vậy.

Đương nhiên, nhờ trụ sở của Microsoft ở ngay gần Redmond, nên Seattle trở thành vùng đất màu mỡ cho giới công nghệ. Sau khi xem xét mọi thứ, có vẻ như đây chính là thành phố đáp ứng tốt nhất các nhu cầu của tôi. Vậy là tôi quyết định sẽ đến Seattle.

Tôi mua vé dịch vụ tàu hỏa Amtrak một chiều, ôm tạm biệt mẹ và bà ngoại rồi lên tàu. Chuyến tàu dừng ở ga King Street của Seattle hai ngày sau đó. Bộ danh tính mới của tôi gồm có một bằng lái xe, một thẻ An sinh Xã hội và những món đồ quen thuộc để tăng cường độ tin cậy – tất cả đều được làm dưới cái tên mới, Brian Merrill. Tôi tìm thấy một nhà nghỉ và đăng ký bằng danh tính mới.

Tôi đã định thiêu hủy toàn bộ tài liệu có liên quan đến thân phận Eric Weiss nhưng sau cùng, tôi vẫn quyết định giữ chúng lại để phòng xa, trong trường hợp tôi phải loại bỏ thân phận Brian Merrill ngay lập tức vì một lý do nào đó. Tôi nhét chúng vào một chiếc tất, xếp tất cả xuống dưới đáy va-li hành lý.

Với tôi, Denver đúng là một nơi tuyệt vời chỉ trừ chương cuối tệ hại kia. Và chương cuối tại Seattle sẽ còn tệ hại hơn thế nhiều.

https://thuviensach.vn

31
VÂY BẮT TỪ TRÊN CAO

Alex B25 rixasvo hmh M ywi xs gsrrigx xs xli HQZ qemrjveqi?

Ngay ngày đầu tiên ở Seattle, máy nhắn tin đã rung lên vào lúc 6 giờ sáng khiến tôi sợ chết khiếp: Không ai ngoài Lewis và mẹ tôi có số máy này và Lewis luôn biết là không nên gọi tôi dậy sớm thế này. Dù gì thì đây cũng không thể là tin tốt.

Mắt nhắm mắt mở, tôi với tay lên bàn cạnh giường để chụp lấy máy nhắn tin và nhìn vào màn hình. Trên đó hiển thị chuỗi số "385912303". Chuỗi chữ số đầu tiên tôi đã thuộc nằm lòng: số điện thoại của Showboat Hotel & Casino.

Số "3" ở cuối có nghĩa là mã 3: KHẨN CẤP.

Chụp lấy máy điện thoại vốn đã được lập trình để luôn dùng số máy nhái không thể truy ngược về tôi, tôi gọi đến khách sạn và nhờ người trực tổng đài thông báo có "Mary Schultz" gọi. Mẹ tôi lúc đó hẳn phải đứng ngay cạnh điện thoại chờ tin, bởi bà đã nhấc máy luôn trong chưa đầy một phút.

"Có chuyện gì vậy mẹ?" tôi hỏi.

"Kevin, kiếm ngay một tờ New York Times đi. Con hãy làm ngay đi."

"Có chuyện gì thế mẹ?"

"Con lên trên trang nhất rồi!"

"Chết tiệt! Có ảnh không mẹ?"

"Có, nhưng đó là ảnh cũ – nhìn không giống con chút nào."

https://thuviensach.vn

Không quá tệ, tôi nghĩ.

Tôi đi ngủ tiếp với suy nghĩ rằng: Việc này thật vô lý. Tôi không hề cướp hàng triệu đô-la bằng máy tính giống Stanley Rifkin. Tôi cũng không hề làm tê liệt hệ thống máy tính ở bất kỳ công ty hay cơ quan chính phủ nào. Tôi không đánh cắp thông tin thẻ tín dụng và dùng thẻ của người khác để trả hóa đơn. Tôi không nằm trong top 10 Những tên tội phạm bị truy nã của FBI. Tại sao tờ báo danh tiếng nhất nước Mỹ lại cho đăng bài về tôi?

Khoảng 9 giờ sáng, tôi tỉnh dậy lần nữa và ra ngoài để tìm nơi có bán tờ New York Times – việc này thật chẳng dễ gì tại khu nhà nghỉ cho thuê theo tuần ở Seattle.

Cuối cùng, tôi cũng kiếm được báo và hoàn toàn choáng váng. Tựa báo đập thẳng vào mắt tôi:

Kẻ bị truy nã gắt gao nhất không gian mạng: Hacker lẩn tránh cuộc rượt đuổi của FBI

Tôi bắt đầu đọc bài báo và không thể tin vào mắt mình. Chỉ có đoạn đầu câu chuyện là dễ chịu, họ trao cho tôi danh hiệu “pháp sư kỹ thuật”. Sau đó, John Markoff, phóng viên tờ Times viết bài báo, tiếp tục nói rằng “các nhân viên chấp pháp có vẻ không thể theo kịp anh ta.” Điều này chắc hẳn sẽ khiến đặc vụ Ken McGuire và đồng sự phải nóng mặt cũng như bị mất mặt với cấp trên – họ sẽ càng ráo riết tìm kiếm tôi hơn.

Bài báo viết sai lệch sự thật và đầy phỉ báng này khẳng định tôi đã nghe lén FBI – một việc mà tôi chưa từng làm. Và như một điềm báo trong bộ phim War Games (tạm dịch: Trò chơi chiến tranh) ra mắt năm 1983, tôi đã đột nhập vào máy tính của Bộ Chỉ huy Phòng không Không quân Bắc Mỹ (NORAD) – đó không chỉ là việc tôi chưa bao giờ và sẽ không bao giờ làm mà còn gần như là một việc bất khả thi với bất cứ ai, bởi các máy tính trọng yếu của cơ quan này đều không kết nối với thế giới bên ngoài, nên chúng dĩ nhiên cũng miễn nhiễm với việc bị người ngoài hack được.

https://thuviensach.vn

Markoff đã gọi tôi là “kẻ bị truy nã gắt gao nhất không gian mạng” và “một trong những tội phạm máy tính bị truy nã gắt gao nhất nước Mỹ”.

Tất cả những chuyện này xảy ra vào đúng ngày Quốc khánh, khi lòng ái quốc nhiệt thành của những người Mỹ gan dạ trở nên mạnh mẽ hơn bất kỳ ngày nào trong năm. Nỗi sợ máy tính và công nghệ của mọi người hẳn đã dâng đến cao trào khi họ đọc về một thằng oắt con trong lúc ngồi ăn trứng ốp-la hay ngũ cốc sáng, một mối hiểm họa đối với an ninh và sự an toàn của người Mỹ.

Sau này tôi mới biết được rằng nguồn tin của những lời dối trá trắng trợn này và nhiều đơm đặt khác đều đến từ một phone phreaker không đáng tin cậy, Steve Rhoades, hắn đã từng là một người anh em của tôi.

Tôi nhớ mình đã ở trong trạng thái nửa mê nửa tỉnh sau khi đọc xong bài báo, cố đọc hết câu này đến câu khác mà không hề có câu nào đúng sự thật. Qua lời bài báo này, Markoff đã một tay tạo ra “Huyền thoại về Kevin Mitnick” – một huyền thoại làm xấu hổ FBI, khiến họ phải đặt việc tìm ra tôi trở thành ưu tiên hàng đầu và dựng lên những hình ảnh hư cấu, gây ảnh hưởng đến các công tố viên và thẩm phán, khiến họ coi tôi như một mối nguy hiểm cho an ninh quốc gia. Tôi không thể không nhớ lại, năm năm trước tôi đã từ chối tham gia vào cuốn sách mà Markoff và vợ hắn thuở ấy, Katie Hafner, muốn viết về tôi và một số hacker khác, bởi họ muốn kiếm tiền từ câu chuyện của tôi trong khi bản thân tôi lại không kiếm được xu nào từ nó. Tôi cũng nhớ lại việc John Markoff nói với tôi trong một cuộc điện thoại rằng, nếu tôi không đồng ý phỏng vấn, bất kỳ điều gì người khác nói về tôi sẽ được coi là sự thật bởi tôi đã không ở đó để phản bác lại.

Thật đáng sợ khi phát hiện ra tôi đã trở thành mục tiêu vô cùng quan trọng của FBI.

Ít nhất bức ảnh đó cũng là một món quà. Tờ Times đã dùng bản sao tấm ảnh chụp mặt tôi năm 1988, tấm ảnh được chụp sau khi tôi bị giam ở Nhà tù

https://thuviensach.vn

Liên bang Terminal Island trong ba ngày mà không hề được tắm rửa, cạo râu, hay có quần áo để thay – tóc tôi rối bù, trông dơ dáy và lôi thôi, giống như một gã vô gia cư trên phố vậy. Người đang nhìn tôi trên trang nhất tờ báo có gương mặt béo phị, nặng hơn tôi vào ngày 4 tháng 7 khi đó khoảng 40-45kg.

Ngay cả vậy, bài báo đã nâng mức độ nguy hiểm của tôi thêm vài bậc. Tôi bắt đầu đeo kính râm đều đặn, ngay cả khi ở trong nhà. Nếu bất cứ ai hỏi: "Có chuyện gì với cái kính vậy?" tôi sẽ nói mắt tôi đang nhạy cảm với ánh sáng.

Đọc lướt qua mục Căn hộ Cho thuê được liệt kê trong tờ báo địa phương, tôi quyết định sẽ tìm một căn tại "Quận U", gần Đại học Washington, hy vọng nơi đó sẽ giống như khu vực hấp dẫn, giàu sức sống Westwoo, cạnh UCLA tại Los Angeles. Tôi chọn một căn tầng hầm, tự nhủ rằng nó buồn tẻ hơn so với nhà nghỉ tôi vừa ở, nhưng hợp lý trong thời điểm hiện tại nhờ giá rẻ. Tòa nhà thuộc sở hữu của một ông chủ tên là Egon Drews, do anh con trai David của ông ta quản lý. Thật may, Egon cũng cả tin và không để tâm đến việc kiểm tra tín dụng hay lý lịch, việc một công ty quản lý thường yêu cầu.

Khu vực này hóa ra không phải là một lựa chọn quá tốt. Đây không phải là Westwood dễ chịu, nắng ấm, mà thay vào đó là khu vực xuống cấp, buồn bã của thành phố, la liệt những người ăn xin trên phố. Có thể tôi sẽ sống tốt hơn một khi có công việc ổn định. Nhưng ít nhất cũng có một YMCA gần đó để tôi có thể tiếp tục tập gym gần như hằng ngày.

Với tôi, một trong số ít điểm sáng của Quận U là nhà hàng Thái sạch sẽ với đồ ăn ngon, rẻ cùng một bồi bàn người Thái dễ thương. Cô ấy rất thân thiện, có nụ cười ấm áp và chúng tôi đã hẹn hò vài lần. Nhưng nỗi sợ hãi ngày xưa vẫn lởn vởn trong tôi – mối nguy về một mối quan hệ gần gũi, hay trong cơn mê sau vài phút đắm say, tôi có thể lỡ mồm để lộ ra điều gì đó về mình. Tôi vẫn tiếp tục tới dùng bữa ở nhà hàng nhưng nói với cô ấy rằng mình quá bận rộn để nghĩ tới chuyện tình cảm.

https://thuviensach.vn

Dù có làm gì khác đi nữa, tôi luôn hack để giữ cho đầu óc được bận rộn. Đó là lý do tôi phát hiện ra Neill Clift, người đã tìm ra lỗi trong hệ điều hành VMS của DEC, đang dùng một tài khoản e-mail trên một hệ thống có tên là Hicom, ở Đại học Loughborough tại Anh.

Thật thú vị! Tôi gần như đã bỏ qua Clift khi phát hiện ra DEC đã cung cấp cho anh ta một chiếc Vaxstation 4000 và trả cho anh ta 1.200 bảng mỗi năm (quá rẻ) để tìm ra các lỗi bảo mật. Sau đó, tôi không hy vọng anh ta sẽ dùng bất cứ hệ thống nào khác để sử dụng e-mail ngoại trừ ở nhà hay ở chỗ làm. Có lẽ đây là điều may mắn hiếm hoi của tôi.

Sau khi đào bới chút ít xung quanh, tôi biết được rằng Hicom là hệ thống truy cập công cộng và ai cũng có thể đăng ký tài khoản. Thiết lập tài khoản của riêng mình xong, tôi khai thác một lỗ hổng bảo mật mà rõ ràng là Neill chưa biết về nó, chiếm toàn quyền điều khiển hệ thống cùng quyền ưu tiên của quản trị hệ thống. Tôi rất thích thú nhưng không kỳ vọng mình sẽ tìm được gì nhiều, bởi tôi không cho là anh ta sẽ bất cẩn tới mức gửi DEC những kết quả nghiên cứu bảo mật của anh ta từ một hệ thống công cộng.

Việc đầu tiên tôi làm là lấy một bản sao thư mục e-mail của Neill và xem từng tập tin. Chết tiệt! Không có gì thú vị cả – không có lỗi nào! Tôi thất vọng. Vừa gần lại vừa xa. Nhưng tôi có một ý tưởng: Có thể anh ta đã gửi e-mail và xóa các tin nhắn đi ngay lập tức. Vì vậy, tôi kiểm tra ghi chép hệ thống e-mail.

Mắt tôi sáng lên: Các tập tin ghi chép e-mail cho thấy Neill đang gửi tin nhắn cho một ai đó tên là Dave Hutchins ở DEC, đôi khi hai đến ba tin một tuần. Chết tiệt! Tôi thực sự muốn xem nội dung những tin nhắn này. Lúc đầu, tôi nghĩ mình sẽ xem tất cả các tập tin bị xóa trên đĩa hệ thống để tìm các e-mail bị xóa đã gửi cho Hutchins, nhưng rồi tôi có một kế hoạch hay hơn.

https://thuviensach.vn

Bằng cách cấu hình lại phần mềm trao đổi e-mail trên Hicom, tôi chỉnh sao cho mỗi khi Neill gửi một tin nhắn đến bất kỳ địa chỉ e-mail nào ở DEC, nó sẽ được chuyển đến một tài khoản tôi đã hack ở USC. Việc này giống như thêm một lệnh chuyển tiếp vào tất cả các địa chỉ "dec.com" để chuyển tiếp đến tài khoản của tôi ở USC. Vậy thì tôi sẽ lấy được tất cả e-mail gửi đến bất cứ địa chỉ "dec.com" nào từ bất cứ ai trên Hicom.

Thử thách tiếp theo là tìm ra cách hiệu quả để "nhái lại"[84] e-mail đến Clift sao cho chúng giống như đến từ DEC. Thay vì làm giả tin nhắn qua Internet – một bước có thể dễ dàng bị phát hiện nếu Neil nhìn kỹ tiêu đề e-mail – tôi viết một chương trình làm giả e-mail từ hệ thống nội bộ để làm giả cả tiêu đề, khiến cho e-mail giả gần như không thể bị phát hiện.

[84] Từ gốc "spoofing": Một dạng tấn công trong đó một đối tượng hay một chương trình đóng giả thành một đối tượng hay một chương trình khác bằng cách làm giả dữ liệu hòng chiếm được lợi thế bất hợp pháp. (BTV)

Mỗi khi Neill gửi báo cáo về lỗ hổng bảo mật đến Dave Hutchins ở DEC, e-mail sẽ được chuyển đến tôi (và chỉ tôi). Tôi sẽ ngấu nghiến mọi chi tiết và gửi lại một tin nhắn "cảm ơn" trông giống như được gửi từ Hutchins. Vẻ đẹp của kiểu hack này – còn được biết đến dưới tên gọi cuộc tấn công "người-đứng-giữa" – đó là Hutchins thật, cũng như DEC, sẽ không bao giờ nhận được thông tin Neill gửi cho họ. Việc này rất thú vị, bởi điều đó có nghĩa rằng, DEC sẽ không thể sớm khắc phục được các lỗ hổng đó, bởi các nhà phát triển không biết gì về chúng – ít nhất là từ Neill.

Sau khi dành vài tuần chờ đợi Neill bận rộn với việc tìm lỗi, tôi trở nên thiếu kiên nhẫn. Còn những lỗ hổng bảo mật mà tôi đã bỏ lỡ thì sao? Tôi muốn tất cả chúng. Việc cố gắng đột nhập vào hệ thống của anh ta thông qua dial-up rất khó thành công, bởi tôi không thể làm gì nhiều tại màn hình đăng nhập ngoại trừ việc ngồi đoán mò mật khẩu, hoặc thử tìm một lỗi trong bản thân phần mềm log-in, và chắc chắn anh ta đã kích hoạt cảnh báo an ninh cho những lần log-in thất bại.

https://thuviensach.vn

Tôi cũng chẳng nên nghĩ tới một cuộc tấn công bằng kỹ thuật xã hội qua điện thoại làm gì, bởi Neill sẽ nhận ra giọng tôi từ vài năm trước. Nhưng gửi e-mail giả có thể giúp tôi chiếm được tất cả lòng tin và sự tín nhiệm cần có để anh chia sẻ lỗi với tôi. Cách này có một điểm bất lợi: Nếu anh ta phát hiện ra, tôi sẽ mất quyền tiếp cận tất cả các lỗi trong tương lai của anh ta bởi anh ta chắc chắn sẽ phát hiện ra tôi đã đột nhập vào Hicom.

Nhưng thế thì sao? Tôi là một kẻ ưa thích rủi ro. Tôi muốn xem liệu mình có thể thực hiện được việc này hay không.

Tôi gửi cho Neill các tin nhắn giả từ Dave Hutchins, báo rằng Derrell Piper thuộc Đội Kỹ thuật của VMS – người mà tôi đã giả danh khi gọi cho anh ta lần trước – muốn liên lạc với anh ta qua e-mail. Đội Kỹ thuật VMS đang thắt chặt quá trình an ninh, tôi viết, và Derrel sẽ quản lý dự án.

Neill trên thực tế đã liên lạc với Derrell Piper thật vài tháng trước, nên tôi biết yêu cầu này nghe có vẻ ổn.

Sau đó, tôi gửi một e-mail giả nữa đến Neill, tự nhận mình là Derrell và làm giả địa chỉ e-mail thật của anh ta. Sau khi trao đổi vài tin nhắn qua lại, tôi nói với Neill rằng “tôi” đang tổng hợp lại cơ sở dữ liệu để theo dõi mọi vấn đề bảo mật nhằm giúp DEC có thể đơn giản hóa quá trình giải quyết.

Để tăng thêm độ tin cậy, tôi thậm chí còn gợi ý Neill rằng chúng tôi nên dùng mã hóa PGP để không ai như Mitnick có thể đọc được e-mail của mình! Không lâu sau, chúng tôi đã trao đổi khóa PGP với nhau để mã hóa trao đổi e-mail của mình.

Đầu tiên, tôi nhờ Neill gửi cho tôi danh sách tất cả lỗ hổng bảo mật mà anh đã gửi cho DEC trong hai năm qua. Tôi bảo anh ta rằng tôi đang duyệt qua danh sách và đánh dấu lại những cái mình còn thiếu. Tôi giải thích rằng hồ sơ của Đội Kỹ thuật VMS rất lộn xộn – lỗi được gửi đến các nhà phát triển khác nhau và rất nhiều e-mail cũ đã bị xóa – nhưng cơ sở dữ liệu mới của chúng tôi sẽ sắp xếp lại các thành quả và giải quyết những vấn đề này.

https://thuviensach.vn

Neill gửi cho tôi danh sách lỗi tôi yêu cầu, nhưng tôi chỉ xin một hay hai báo cáo lỗi chi tiết một lần để tránh bất cứ nghi ngờ nào từ phía anh ta.

Nhằm củng cố lòng tin của Neill, tôi bảo anh ta rằng tôi muốn chia sẻ một vài thông tin nhạy cảm về lỗ hổng với anh ta vì anh ta đã giúp đỡ công ty khá nhiều. Tôi có chi tiết một lỗ hổng khác mà Brit đã tìm ra và báo cáo về DEC cách đây khá lâu. Lỗi này đã trở thành một tin tức lớn khi truyền thông biết đến và DEC đã cuống cuồng gửi bản vá lỗi đến các khách hàng sử dụng VMS của họ. Tôi đã tìm được người khám phá ra lỗi và thuyết phục anh ta gửi chi tiết cho mình.

Giờ tôi sẽ gửi những dữ liệu này cho Clift, nhắc anh phải giữ nó tuyệt mật bởi đây là thông tin của riêng DEC. Thêm vào đó, tôi còn gửi cho Clift hai lỗi khai thác vấn đề bảo mật khác mà anh ta chưa biết.

Vài ngày sau, tôi nhờ anh ta đáp lại. (Tôi không trực tiếp dùng từ đó, nhưng tôi đang tính đến hiệu quả trong việc đền đáp qua lại như một kỹ thuật tạo ra sức ảnh hưởng mạnh mẽ.) Tôi giải thích rằng ngoài danh sách kia, nếu anh ta có thể gửi cho tôi tất cả báo cáo lỗi chi tiết mà anh ta đã gửi cho DEC trong suốt hai năm qua, cuộc sống của tôi sẽ dễ thở hơn rất nhiều. Tôi nói tôi chỉ đơn giản là đưa tất cả vào cơ sở dữ liệu theo trình tự thời gian. Yêu cầu của tôi đầy tính rủi ro. Tôi đang yêu cầu Neill gửi cho tôi tất cả những gì anh ta có; nếu điều đó không khiến anh nghi ngờ, thì chẳng điều gì có thể. Tôi như ngồi trên đống lửa trong vài ngày chờ đợi và khi nhìn thấy e-mail từ anh ta gửi đến hòm thư USC của tôi, tôi lo lắng mở ra, nửa chờ đợi thư sẽ viết: “Hay lắm, Kevin.” Nhưng nó chứa mọi thứ! Tôi đã trúng số độc đắc với các lỗi của VMS rồi.

Sau khi có được bản sao cơ sở dữ liệu lỗi của anh ta, tôi nhờ Neill kiểm tra kỹ hơn chương trình log-in và Loginout của VMS. Neill đã biết Derrel phát triển chương trình Loginout và tôi tò mò muốn biết liệu anh ta có tìm được lỗi bảo mật nào trong đó không.

https://thuviensach.vn

Neill e-mail lại cho tôi một vài câu hỏi kỹ thuật về Đa thức Purdy, thuật toán dùng để mã hóa mật khẩu của VMS. Anh ta đã tốn vài tháng, thậm chí vài năm để cố hạ gục thuật toán mã hóa này – hay nói khác đi, tối ưu hóa mã nguồn của anh ta để bẻ khóa mật khẩu của VMS. Một trong những câu hỏi của anh ta là một câu hỏi có hay không lý thuyết toán đằng sau thuật toán Purdy. Thay vì nghiên cứu nó, tôi chỉ đoán mò câu trả lời – tại sao lại không? Tôi có 50% cơ hội đoán đúng cơ mà. Cuối cùng, tôi đã đoán sai. Sự lười nhác của tôi đã dẫn đến việc làm lộ tẩy cú lừa.

Tuy vậy, thay vì nói cho tôi biết, Neill gửi cho tôi e-mail khẳng định anh ta đã tìm ra lỗi bảo mật lớn nhất từ trước đến nay – trong chính chương trình log-in VMS mà tôi nhờ anh ta phân tích. Anh ta nói rằng nó nhạy cảm đến nỗi anh ta sẽ chỉ sẵn lòng gửi nó cho tôi qua đường bưu điện.

Anh ta nghĩ tôi ngu chắc? Tôi chỉ trả lời với địa chỉ hòm thư thật của Derrell ở DEC, hiểu rằng mọi chuyện đã bại lộ.

Lần tiếp theo tôi đăng nhập vào Hicom để kiểm tra trạng thái mọi thứ, một tin nhắn bỗng nhảy ra trên màn hình của tôi:

Gọi cho tôi đi, anh bạn.

Neill.

Nó khiến tôi mỉm cười. Nhưng sao chứ? Tôi nghĩ: Anh đã biết mình bị tôi lừa rồi, giờ tôi không có gì để mất hết.

Tôi gọi.

“Chào Neill, có chuyện gì vậy?”

“Chào anh bạn.” Không giận dữ, không đe dọa, không thù hằn. Chúng tôi như hai người bạn cũ.

https://thuviensach.vn

Chúng tôi nói chuyện suốt vài giờ và tôi đã chia sẻ mọi tình tiết phức tạp trong việc tôi đã hack anh ta suốt những năm qua như thế nào. Tôi quyết định sẽ nói cho anh ta nghe, bởi có vẻ như tôi sẽ không bao giờ hack anh ta nữa.

Chúng tôi trở thành bạn bè trên điện thoại, đôi khi lại nói chuyện hàng giờ trên điện thoại nhiều ngày liền. Sau cùng, chúng tôi chia sẻ một sở thích chung: Neill yêu thích việc tìm ra các lỗ hổng bảo mật còn tôi yêu thích việc sử dụng chúng. Anh ta bảo tôi rằng Cảnh sát Quốc gia Phần Lan đã liên hệ với anh ta về lần tôi hack vào Nokia. Anh ta đề nghị dạy cho tôi một số kỹ thuật tìm lỗi thông minh, dù phải đợi cho đến khi tôi hiểu hơn về "nội bộ" của VMS – cách hoạt động bên trong hệ điều hành, chi tiết của những thứ "sâu xa ẩn tàng". Anh ta nói tôi đã dành quá nhiều thời gian để hack vào các thứ thay vì tự học về những thứ bên trong. Thật ngạc nhiên, anh ta thậm chí còn cho tôi mấy bài tập để thực hành, để học thêm về nó, sau đó kiểm tra thành quả của tôi và phê bình. Người săn lỗi VMS lại đang huấn luyện hacker – thật trái khoáy làm sao!

Sau này, tôi chặn được một e-mail mà tôi nghĩ là Neill đã gửi cho FBI. Nội dung như sau:

Kathleen

Chỉ có một kết quả trong ghi chép mail của nyx:

Sep 18 23:25:49 nyxsendmail[15975]: AA15975: message- id= <00984B0F.85F46A00.9@hicom.lut.ac.uk>

Sep 18 23:25:50 nyxsendmail[15975]: AA15975: from=<kevin@hicom

.lut.ac.uk>, size=67370, class=0

Sep 18 23:26:12 nyxsendmail[16068]: AA15975: to=<srush@nyx.cs

https://thuviensach.vn

.du.edu>, delay=00:01:15, stat=Sent

Hy vọng điều này có ích.

Ngày và tháng trên ghi chép là khi tôi gửi e-mail từ tài khoản của mình trên Hicom đến một trong những tài khoản tôi có trên hệ thống truy cập công cộng ở Denver tên là "nyx". Và ai là "Kathleen" mà tin nhắn gửi tới? 99% khả năng, một lần nữa, lại là đặc vụ Kathleen Carson.

E-mail đó là bằng chứng rõ ràng cho thấy Neill đã làm việc với FBI. Tôi không ngạc nhiên; sau cùng, tôi là người đã khai chiến và theo đuôi anh ta, vì thế tôi đáng bị như vậy. Tôi đã vui thú với những cuộc trò chuyện giữa hai chúng tôi và học hỏi nhiều điều từ anh ta; thật thất vọng khi biết rằng anh ta chỉ đang chèo kéo tôi với hy vọng có thể giúp FBI bắt tôi. Dù luôn thực hiện các biện pháp phòng ngừa khi gọi điện, nhưng tôi quyết định tốt nhất là cắt đứt mọi liên lạc, để tránh cung cấp thêm cho FBI bất kỳ đầu mối nào.

Khi khởi tố một phạm nhân, như bạn đã biết, chính phủ được yêu cầu phải chia sẻ bằng chứng với bị can. Trong những tài liệu sau này được đưa cho tôi, có một bức thư cho thấy mức độ hợp tác của Neill và tầm quan trọng của nó với FBI. Lần đầu tiên đọc bản sao bức thư này, tôi đã rất ngạc nhiên.

Bộ Tư pháp Mỹ, Cục Điều tra Liên bang

11000 Wilshire Boulevard #1700

Los Angeles, CA 90014

Ngày 22 tháng 9 năm 1994

Ngài Neill Clift, Đại học Loughborough

Gửi anh Neill:

https://thuviensach.vn

Hắn anh phải rất bức bối và băn khoăn liệu FBI hay các lực lượng chấp pháp của Anh rốt cục có định làm gì để bắt người "bạn" của chúng ta, KDM, hay không. Tôi chỉ có thể đảm bảo với anh rằng bất kỳ manh mối nào tôi đang nắm trong tay có liên quan đến Kevin đều được theo đuổi rất quyết liệt.

Trên thực tế, tôi vừa xác minh thông tin anh cung cấp... Hắn là hệ thống máy tính này đã bị Kevin truy cập và chiếm đoạt. Tuy nhiên, chúng tôi đang gặp phải một tình thế khó xử, quản trị viên hệ thống có tên "NYX" này không hề có ích với lực lượng chấp pháp như anh; và chúng tôi cũng bị giới hạn trong việc tiếp tục theo dõi tài khoản này bởi những thủ tục pháp lý của Mỹ.

Qua thư này, tôi muốn anh biết được rằng FBI trân trọng sự hợp tác của anh ra sao. Bất kỳ liên lạc nào qua điện thoại giữa anh và Kevin đều rất quan trọng – ít nhất là với tôi.

... Tôi có thể báo cáo rằng anh (và chỉ anh) là đầu mối liên hệ cụ thể mà chúng tôi có với Kevin bên ngoài thế giới máy tính. Tôi không tin chúng ta có thể tìm được hắn qua theo dấu điện thoại, telnet hay kết nối FTP, hay/và bất kỳ biện pháp công nghệ nào khác. Chỉ có qua trao đổi cá nhân (hay trong trường hợp của anh là điện thoại) với Kevin, chúng ta mới có thể biết thêm về hoạt động và kế hoạch của hắn. Sự trợ giúp của anh là vô cùng quan trọng cho cuộc điều tra này.

[Thêm in nghiêng để nhấn mạnh.]

... Tôi chỉ có thể đảm bảo với anh, một lần nữa, rằng những nỗ lực của anh trong việc "theo đuổi" Kevin rất đáng trân trọng... Nếu anh tiếp tục chọn cộng tác với FBI thông qua việc cung cấp cho tôi thông tin về những gì đã trao đổi với Kevin, tôi xin hứa rằng một ngày nào đó, tất cả những mẩu thông tin nhỏ được lọc để gửi cho tôi từ khắp nơi trên thế giới sẽ quy về một

https://thuviensach.vn

mối và dẫn đến chiếc máy tính đầu cuối nơi tôi sẽ tìm ra Kevin và ngay lập tức cho hắn vào còng.

Cảm ơn anh một lần nữa, Neill.

Trân trọng,

Kathleen Carson

Đặc vụ Cục Điều tra Liên bang

Đọc lại bức thư này khiến tôi giật mình bởi đặc vụ Carson đã bức bối ra sao khi không thể tóm được tôi – và cô ta sẵn sàng thú nhận điều đó như thế nào trong thư.

Trong quá trình nỗ lực tìm kiếm việc làm ở Seattle, tôi tìm thấy một quảng cáo trên báo cho vị trí phân tích Bộ phận Giải đáp hỗ trợ tại Trung tâm Y tế Virginia Mason. Tôi đến buổi phỏng vấn kéo dài vài giờ và vài ngày sau thì nhận được hợp đồng làm việc. Nghe không giống như công việc sẽ đem lại thử thách như công việc cũ ở hãng luật tại Denver. Nhưng căn hộ của tôi trông thật chán đời và tôi không muốn tìm một nơi tốt hơn cho đến khi tôi ổn định thu nhập và biết mình sẽ làm tại khu vực nào của thành phố, vì vậy, tôi vẫn nhận công việc này bất chấp những trở ngại của nó.

Khi tôi nhận gói phong bì dành cho nhân viên mới của Phòng Nhân sự, tôi phát hiện ra đơn đăng ký yêu cầu tôi lấy dấu vân tay.

Đây đúng là tin xấu. Liệu những dấu vân tay này có bị gửi đi để so sánh với hồ sơ của FBI không? Tôi thực hiện một cuộc gọi dàn xếp khác, lần này là đến Đội Tuần tra bang Washington, tự nhận mình đến từ Phòng Xác nhân Cảnh sát bang Oregon.

“Chỗ chúng tôi đang thiết lập một chương trình hỗ trợ các tổ chức trong thành phố và quận bằng cách quét hồ sơ xin việc của họ để kiểm tra hồ sơ

https://thuviensach.vn

phạm tội," tôi nói. "Vì vậy, chúng tôi đang muốn xin một số lời khuyên. Các anh có yêu cầu vân tay không?"

"Có, chúng tôi có."

"Các anh cho chạy các dấu vân tay này đối chiếu với hồ sơ bang, hay gửi chúng đến FBI?"

"Chúng tôi không gửi đến cơ quan bên ngoài nào," người ở đầu dây bên kia bảo tôi. "Chúng tôi chỉ kiểm tra hồ sơ của bang thôi."

Tuyệt vời! Tôi không có hồ sơ phạm tội nào ở bang Washington, vì vậy, tôi biết nộp hồ sơ với vân tay của tôi sẽ an toàn.

Tôi bắt đầu công việc vài ngày sau đó, cùng chung văn phòng với một gã cao kều, rất hay chú ý đến tiểu tiết tên là Charlie Hudson và một đồng nghiệp nữa. Công việc không thú vị chút nào; việc của tôi chủ yếu là trả lời các câu hỏi ở Bộ phận Tư vấn từ các bác sĩ và những viên chức trong bệnh viện khác, những người khiến tôi nhớ lại câu chuyện cười về những kẻ mù công nghệ cố gắng sao chép đĩa mềm trên một chiếc máy photocopy của Xerox.

Chẳng hạn như, hầu hết tất cả nhân viên ở đây đều dùng mã số An sinh Xã hội của mình làm câu hỏi bảo mật để khôi phục mật khẩu. Tôi cố thuyết phục sếp của tôi rằng nó thiếu an toàn ra sao, nhưng ông ta lại gạt phắt đi. Tôi từng thoáng nghĩ về việc sẽ cho ông ta thấy việc lấy mã số An sinh Xã hội của bất kỳ ai dễ ra sao, nhưng ngay lập tức nhận ra đó là một ý tưởng rất tồi. Khi tôi bắt đầu viết mấy chương trình nhỏ trên hệ thống VMS để giải quyết một số vấn đề trợ giúp kỹ thuật, tôi được thông báo rằng dự án này nằm ngoài trách nhiệm của tôi và tôi nên dừng ngay việc đó lại.

Thái độ tâm lý của tôi khá ổn. Trong suốt thời gian trốn chạy, tôi chưa bao giờ nhận được các cảnh báo làm tôi lo lắng đến an toàn của bản thân. Nhưng tôi không bao giờ để mình hoàn toàn mất cảnh giác. Một ngày nọ, tôi bước

https://thuviensach.vn

ra khỏi tòa nhà căn hộ và nhìn thấy một chiếc Jeep Cherokee đỗ bên vệ đường. Điều khiến tôi chú ý là gần như không có chiếc xe nào đỗ trên đường giờ đó, vậy mà chiếc xe này lại đỗ ở một nơi không tiện ra vào bất kỳ căn nhà hay căn hộ nào. Và có một gã ngồi trong đó. Như thể thách thức, tôi lườm thẳng vào mắt hắn. Chúng tôi chạm mắt trong giây lát rồi hắn liếc đi chỗ khác, không để tâm. Cẩn thận là hợp lý nhưng tôi quyết định rằng mình đã hơi hoang tưởng và tiếp tục đi.

Hai tháng sau khi tôi chuyển đến Seattle, Lewis giới thiệu tôi với Ron Austin, bạn hacking của Poulsen, một người tôi đã nghe tên nhưng chưa bao giờ nói chuyện. Chủ đề chính của cuộc nói chuyện với Ron là Justin Peterson, người đã bước chân vào cuộc đời cả ba chúng tôi bằng cách chỉ điểm. Austin và tôi bắt đầu liên lạc thường xuyên. Anh ta cung cấp cho tôi danh sách các số điện thoại công cộng ở khu vực phía Tây Los Angeles và tôi cho anh ta biết mình sẽ gọi cho anh ta bằng số nào và vào lúc nào.

Tôi chuyển hướng tất cả cuộc gọi từ Seattle đến các bộ chuyển mạch ở Denver, Portland, Sioux Falls và Salt Lake City, thêm vào một lớp bảo vệ nữa bằng cách sửa phần mềm chuyển mạch sao cho bất kỳ ai theo dấu cuộc gọi của tôi sẽ đều tốn rất nhiều thời gian. Dù không tin tưởng Austin, nhưng tôi vẫn cảm thấy an toàn khi nói chuyện với anh ta bởi chúng tôi dùng rất nhiều điện thoại công cộng, mỗi lần một máy khác nhau.

Có một lý do khác khiến tôi cảm thấy an tâm về anh ta: Anh ta chia sẻ cho tôi một công cụ nghiên cứu rất mạnh mà anh ta đã học được từ Justin. Trong một lần tình cờ đến kỳ lạ, Justin – rất lâu trước khi tôi gặp anh ta – đã chui vào tòa nhà tôi rất quen thuộc: số 5150 Đại lộ Wilshire, nơi có văn phòng của Dave Harrison. Justin có hứng thú với việc ăn cắp dữ liệu thẻ tín dụng khi chúng được gửi đến máy xử lý thẻ để xác minh và hắn ta cũng nhắm vào mạng GTE Telenet mà tôi đang theo, dù với một ý định khác.

Khi Justin bắt đầu bật lại bản thu âm tiếng modem qua một cài đặt sẽ dịch tiếng này thành chữ trên màn hình, hắn nhận ra lẫn trong những dữ liệu khác

https://thuviensach.vn

là thông tin chứng thực đăng nhập của vài cơ quan đang truy cập vào hồ sơ của DMV ở California – những thông tin chứng thực mà hắn ta và mọi hacker khác có thể dùng để moi bất kỳ thông tin gì từ DMV. Thật không thể tin được! Tôi có thể tưởng tượng ra Justin lúc đó đã há hốc mồm ra sao. Có lẽ chính hắn cũng không thể tin được vào vận may của mình và bắt đầu tự mình dùng những thông tin chứng thực này để quét biển số xe và bằng lái xe.

Ron không chỉ kể cho tôi nghe câu chuyện về Justin. Anh ta còn thực sự kể chi tiết cho tôi biết: “Địa chỉ của GTE Telenet là 916268,05. Ngay khi màn hình trống, anh hãy gõ ‘DGS’. Mật khẩu là ‘LU6’. Và thế là anh đã đăng nhập xong!”

Tôi không thể cúp máy đủ nhanh để bắt tay vào thử. Nó hoạt động thật!

Kể từ đó, tôi không bao giờ phải dùng đến tấn công bằng kỹ thuật xã hội với DMV để moi thông tin nữa. Tôi có thể lấy mọi thứ tôi muốn, nhanh chóng, gọn gàng và an toàn.

Việc Austin chia sẻ cách hack này giúp tâm trí tôi được thả lỏng trong việc nghi ngờ xem liệu anh ta có phải là kẻ chỉ điểm cố lấy thông tin để giúp FBI tìm ra tôi hay không. Nếu anh ta là kẻ chỉ điểm, FBI sẽ không bao giờ cho phép anh ta cho tôi truy cập vào các hồ sơ được bảo vệ ở DMV. Tôi bị thuyết phục rằng chơi với anh ta là an toàn.

Trong quá trình điều tra về Eric, tôi đã dành không biết bao nhiêu giờ lên mạng và ôm điện thoại cùng “RGB”, một hacker Hà Lan nổi tiếng chuyên đi tìm lỗi và hack vào các hệ thống khác nhau. Anh đã bị bắt vào tháng 5 năm 1992 tại nhà riêng ở Utrecht, Hà Lan bởi các đặc vụ chính phủ giả dạng là người bán hàng của một công ty máy tính – một lực lượng liên ngành gồm cảnh sát địa phương và đội PILOT, nhóm chấp pháp được thành lập để chiến đấu với các cuộc tấn công có liên quan đến hacking. RGB bảo tôi cảnh sát có hàng trăm trang bản ghi các cuộc nói chuyện với tôi.

https://thuviensach.vn

Sau khi RGB được thả, chúng tôi quay lại hacking cùng nhau lần nữa. Anh ấy bắt đầu chọc ngoáy các hệ thống ở Đại học Carnegie Mellon và theo dõi lưu lượng truy cập mạng của họ thông qua một chương trình gọi là "tcpdump". Sau hàng tuần trời theo dõi, cuối cùng anh ấy cũng tóm được mật khẩu của một nhân viên CERT. Ngay khi xác nhận mật khẩu này dùng được, anh ấy liên lạc với tôi, giọng đầy phấn khích và nhờ tôi tìm thứ gì đó thú vị, chủ yếu là các lỗ hổng bảo mật được báo cáo mà chúng tôi có thể tận dụng trong công cuộc hacking của mình.

CERT (Computer Emergency Response Team – Đội Ứng cứu Khẩn cấp Máy tính) đặt trụ sở tại Đại học Carnegie Mellon, Pittsburgh là trung tâm nghiên cứu và phát triển đầu tư do liên bang thành lập vào tháng 11 năm 1988, sau khi sâu máy tính Morris Worm làm tê liệt 10% mạng Internet. CERT ngăn chặn các sự cố an ninh nghiêm trọng thông qua việc thiết lập Trung tâm Điều hành Mạng để liên lạc với các chuyên gia an ninh. Trung tâm này tạo ra một chương trình tiết lộ lỗ hổng với nhiệm vụ tư vấn về các lỗ hổng bảo mật, thường là sau khi các nhà sản xuất phần mềm đã phát triển một bản vá lỗi hoặc tạo ra một giải pháp tạm thời để giảm thiểu rủi ro của các lỗi bảo mật đó. Các chuyên gia an ninh dựa vào CERT để bảo vệ hệ thống và an ninh mạng của khách hàng khỏi những kẻ đột nhập. (Chức năng của CERT được Bộ An ninh Nội địa tiếp quản từ năm 2004.)

Giờ hãy nghĩ tới chuyện này một chút: Nếu ai đó phát hiện ra và báo cáo một lỗ hổng an ninh, CERT sẽ đưa ra tư vấn. Hầu hết các tư vấn an ninh của CERT đều tập trung vào "các dịch vụ mạng công khai" – các yếu tố trong hệ điều hành có thể bị truy cập từ xa – nhưng đồng thời họ cũng báo cáo các lỗ hổng bảo mật có thể bị "người dùng nội bộ", những người đã có sẵn tài khoản trên hệ thống, khai thác. Các lỗ hổng này thường liên quan đến hệ điều hành chạy trên nền tảng Unix – bao gồm SunOS, Solaris, Irix, Ultrix và một số khác – hình thành nên phần lớn mạng Internet lúc bấy giờ.

Các báo cáo lỗi bảo mật mới thường được gửi về CERT, đôi khi là trong các e-mail không mã hóa. Đây là những lỗi mà RGB và tôi đang theo đuổi,

https://thuviensach.vn

những lỗi mới chúng tôi có thể tận dụng để đột nhập vào các hệ thống, như thể chúng tôi có chìa khóa vạn năng đến máy chủ vậy. Mục đích của chúng tôi là tận dụng "giai đoạn nhiễm", khoảng thời gian chờ đến khi nhà sản xuất làm xong bản vá lỗi và các công ty có thể cài đặt nó. Những lỗ hổng bảo mật này sẽ có thời gian sống giới hạn: Chúng tôi phải nhanh tay tận dụng thời gian vàng đó trước khi chúng được sửa hoặc bị chặn.

Tôi đã biết về kế hoạch của RGB nhưng vẫn nghi ngờ việc anh ấy có thể lấy được thông tin chứng thực của một tài khoản nhân viên CERT. Vậy mà anh ấy đã làm được trong một thời gian ngắn. Tôi choáng váng nhưng vẫn rất vui vẻ chia sẻ chiến lợi phẩm cùng anh. Chúng tôi cùng hack vào máy trạm của vài nhân viên CERT khác và lấy được vùng lưu trữ e-mail tạm thời của tất cả nhân viên, nghĩa là tất cả e-mail của họ. Rồi chúng tôi lại đào trúng một mạch ngầm khác, bởi rất nhiều e-mail trong số đó chứa những tin nhắn không mã hóa để lộ ra các lỗ hổng gọi là zero-day – nghĩa là chúng chưa bao giờ được tìm ra và các nhà sản xuất phần mềm chưa phát triển hay tung ra các bản vá lỗi để sửa chúng.

Khi RGB và tôi phát hiện ra hầu hết các lỗi gửi đi đều "sạch sẽ" – không mã hóa – chúng tôi càng khó lòng kiềm chế bản thân.

Như tôi đã nói, tất cả chuyện đó đã diễn ra vài năm trước. Nhưng giờ, một ngày tháng 9 năm 1994, một tin nhắn không mong đợi hiện ra từ RGB đã khiến tôi phải chú ý tới CERT:

Xin chào, đây là một vài thông tin cho anh:

Có một hệ thống vax/vms tại 145.89.38.7 có tên đăng nhập là opc/nocomm có thể có truy cập x.25 trên đó nhưng tôi không chắc, trên mạng đó có một máy chủ tên là hutsur, máy chủ này chắc chắn có truy cập đến x.25.

Có thể anh đang băn khoăn tại sao e-mail này lại bí mật như vậy, nhưng tôi đang bắt đầu hack trở lại và không muốn đánh động tới phía cảnh sát. Để bắt đầu lại từ đầu, tôi cần anh giúp tôi một việc. Anh có thể lấy cho tôi vài số

https://thuviensach.vn

của các máy chủ đầu cuối trên khắp nước Mỹ được không, tôi sẽ dùng vài đường kết nối ra ngoài để kết nối đến chúng, và đi từ những máy chủ đầu cuối này lên Internet.

Lần này tôi thực sự sẽ thiết lập mọi thứ ổn thỏa, không để lại dấu vết gì đâu. Việc chuẩn bị mọi thứ có thể sẽ mất khoảng một tháng hoặc đại khái vậy, sau đó anh có thể liên lạc với tôi thường xuyên trên Internet, tới lúc đó tôi sẽ cho anh biết thêm thông tin về dự án tôi đang làm. Tôi đang bận truy cập lại vào CERT, tôi đã lấy được những mật khẩu khác nhau cho các hệ thống CMU và tôi sẽ dùng chúng ở giai đoạn sau.

Cảm ơn anh,

Tái bút

Đính kèm là khóa pgp của tôi

Anh ấy muốn đột nhập vào CERT một lần nữa!

Một ngày đầu tháng 10 năm 1994, không lâu sau khi nhận được e-mail của RGB, tôi ra ngoài ăn trưa, mang theo một chiếc hộp nhỏ bên trong có chứa chiếc điện thoại di động OKI 900 hỏng mà tôi định gửi trả cửa hàng hôm đó. Như mọi khi tôi vừa đi bộ vừa nói chuyện điện thoại. Tôi đi xuống Đại lộ Brooklyn hướng về trung tâm Quận U. Khi băng qua đường 52, cách căn hộ của tôi khoảng hai dãy nhà, tôi loáng thoáng nghe thấy tiếng trực thăng.

Tiếng động mỗi lúc một lớn, rồi bỗng nhiên trở nên rất lớn ngay trên đầu tôi, rất thấp, như thể rõ ràng chiếc trực thăng đang định hạ cánh ở một sân trường gần đó.

Nhưng nó không hạ cánh.

Khi tôi rảo bước, nó ở ngay trên đầu tôi và nhìn như thể đang hạ xuống. Chuyện quái gì đang diễn ra thế? Đầu óc tôi bắt đầu rối tung lên. Chuyện gì

https://thuviensach.vn

sẽ xảy ra nếu – nếu chiếc trực thăng đang tìm tôi? Tôi cảm thấy tay bắt đầu túa mồ hôi và tim bắt đầu đập mạnh. Nỗi lo lắng trào dâng khắp mạch máu.

Tôi chạy vào sân của một khu chung cư, hy vọng những ngọn cây cao sẽ che chắn mình khỏi tầm nhìn của chiếc trực thăng. Tôi quăng gói hàng vào bụi cây và bắt đầu chạy thục mạng, ngắt cuộc gọi khi bắt đầu chạy. Một lần nữa, chế độ luyện tập hằng ngày trên máy StairMaster của tôi đã phát huy tác dụng.

Trong lúc chạy, tôi tính đường tẩu thoát: chạy đến hẻm, rẽ trái và chạy như ma đuổi qua hai khu nhà, qua đường 50 và rẽ vào khu tài chính.

Tôi đoán họ có lực lượng hỗ trợ mặt đất đang trên đường đến và có thể nghe thấy tiếng hú của còi xe cảnh sát bất kỳ lúc nào.

Tôi rẽ vào hẻm. Tôi chạy bên trái hẻm, cạnh khu chung cư sẽ làm lá chắn tốt cho tôi.

Đường 50th đang ở ngay phía trước rồi. Giao thông đông đúc thật.

Tôi đang chạy hoàn toàn bằng adrenaline.

Tôi chạy xuống phố, tránh xe cộ để băng qua đường.

Khốn nạn! Suýt bị đâm – hút chết.

Tôi chạy vào quầy thuốc Walgreen’s, giờ mới cảm thấy buồn nôn. Tim tôi đập mạnh, mồ hôi chảy ròng ròng.

Tôi rời khỏi quầy thuốc lần nữa và lao vào hẻm. Không có trực thăng – thật nhẹ nhõm làm sao! Nhưng tôi vẫn tiếp tục đi. Bước nhanh về Đại lộ University.

Cuối cùng cũng được an toàn, tôi rẽ vào một cửa hàng và gọi một cú điện thoại khác.

https://thuviensach.vn

Chưa đầy năm phút trước khi tôi nghe thấy tiếng trực thăng lớn hơn, lớn hơn và lớn hơn.

Nó bay ngay trên cửa hàng và cứ lởn vởn trên đó. Tôi cảm thấy mình như bác sĩ Richard Kimble trong phimThe Fugitive (tạm dịch: Kẻ trốn chạy). Dạ dày tôi cuộn lên, nỗi lo sợ nhanh chóng quay lại. Tôi cần phải trốn chạy.

Tôi rời khỏi cửa hàng qua lối cửa sau. Chạy vào khu nhà, nấp vào một cửa hàng khác.

Mỗi khi tôi bật điện thoại lên để thực hiện cuộc gọi, chiếc trực thăng chết tiệt lại xuất hiện. Khốn kiếp!

Tôi tắt máy và chạy.

Khi tắt điện thoại, chiếc trực thăng không còn theo tôi nữa. Giờ thì tôi đã hiểu. Không còn nghi ngờ gì nữa. Họ đang theo dõi tôi thông qua tín hiệu điện thoại.

Tôi dừng lại dưới một bóng cây và dựa vào thân cây vững chắc để thở lại. Mọi người đi qua nhìn tôi với sự nghi ngờ hiện rõ trên mặt.

Sau vài phút không thấy chiếc trực thăng, tôi bắt đầu bình tĩnh lại.

Tôi tìm tới một bốt điện thoại công cộng và gọi cho cha tôi. “Cha hãy tới một bốt điện thoại công cộng ở Ralph’s,” tôi nói với ông, nhắc tên siêu thị gần căn hộ của cha. Một lần nữa, trí nhớ đáng ngạc nhiên và dị thường của tôi về các số điện thoại lại trở nên hữu ích.

Gặp lại cha, tôi kể cho ông nghe câu chuyện về vụ truy đuổi bằng trực thăng. Tôi thèm khát sự cảm thông và hỗ trợ, thấu hiểu của ông.

Cái tôi nhận được là một điều khác:

https://thuviensach.vn

“Kevin, nếu con nghĩ có ai đó đang truy đuổi con bằng trực thăng, con thực sự cần được giúp đỡ rồi đấy.”

https://thuviensach.vn

32
ĐÊM TRẮNG Ở SEATTLE

Caem alw Ymek Xptq'd tnwlchvw xz lrv lkkzxv?

Nếu cảnh sát liên bang phản đối việc hacking của tôi, liệu họ có phản đối cả việc tôi hack một hacker khác không?

Có một gã tên là Mark Lottor, đang bị truy tố và đợi hầu tòa vì tội đồng phạm với Kevin Poulsen. Gã có một công ty tên Network Wizards, chuyên quảng bá cho cái mà gã gọi là "Bộ công cụ của nhà thử nghiệm điện thoại di động". Nó được thiết kế nhằm cho phép các hacker, phone phreaker và những kẻ lừa đảo có thể kiểm soát điện thoại di động OKI 900 và OKI 1150 từ máy tính cá nhân của mình. Một số người tin rằng Lottor có mã nguồn của OKI 900; một số khác thì cho rằng hắn đã dùng kỹ thuật truy ngược[85] đối với firmware để phát triển bộ công cụ này. Tôi muốn có bản sao của bất kỳ thứ gì đang nằm trong tay hắn – mã nguồn hay chi tiết kỹ thuật truy ngược.

[85] Kỹ thuật truy ngược (reverse engineering): Quá trình tìm ra các nguyên lý kỹ thuật của một phần mềm ứng dụng hay thiết bị cơ khí qua việc phân tích cấu trúc, chức năng và hoạt động của nó. Trong quá trình này, người ta thường phải tháo dỡ đối tượng (ví dụ một thiết bị cơ khí, một thành phần điện tử, một phần mềm) thành từng phần và phân tích chi tiết hoạt động của nó, thường là với mục đích xây dựng một thiết bị hoặc phần mềm mới hoạt động giống hệt nhưng không sao chép bất cứ thứ gì từ đối tượng nguyên bản. (Wikipedia)

Qua tìm hiểu, tôi tìm ra tên người yêu của Mark: Lile Elam. Bạn biết sao không? Cô ta làm việc ở Sun! Thật hoàn hảo, không thể tốt hơn được nữa.

https://thuviensach.vn

Tôi vẫn còn quyền truy cập vào mạng lưới nội bộ nhờ một số hệ thống mà tôi đã hack vào ở Canada, và nhờ đi theo hướng này, tôi không phải mất quá lâu để thâm nhập vào máy tính làm việc của Lile ở Sun. Cài đặt "sniffer" – một chương trình có thể thu thập toàn bộ lưu lượng truy cập mạng của Lile – tôi kiên nhẫn đợi tới khi cô ta kết nối vào hệ thống của Mark hay hệ thống ở nhà riêng. Cuối cùng thì cũng trúng quả:

PATH: Sun.COM(2600) => art.net(telnet)

STAT: Thu Oct 6 12:08:45, 120 pkts, 89 bytes [IDLE TIMEOUT] DATA:

lile

m00n$@earth

Hai dòng cuối là tên đăng nhập, tiếp đó là mật khẩu. Vậy là tôi đã có thể đăng nhập vào tài khoản tại máy chủ của cô ta ở nhà riêng. Nhờ tận dụng một lỗi bảo mật chưa được vá, tôi đã có quyền root.

Tôi cài thêm một sniffer cho máy ở nhà riêng của Lile, "art.net", và sau vài ngày, cô ta cũng đăng nhập vào hệ thống của Mark, tiếp tục cung cấp cho tôi tên đăng nhập và mật khẩu để vào máy của gã đó. Tôi đợi tới tầm sáng sớm, đăng nhập và chiếm quyền root nhờ tận dụng cùng một lỗi bảo mật tương tự như khi thâm nhập vào máy tính ở nơi làm việc của Lile.

Ngay lập tức, tôi tra trong máy của Mark để tìm "*oki*" (dấu sao là ký tự đại diện mà trong trường hợp này có nghĩa là "tìm kiếm mọi tên tập tin có chứa ký tự 'oki' trong đó). Tôi kiểm tra tất cả số tập tin của Mark và phát hiện thấy hóa ra hắn ta không có mã nguồn cho OKI 900 mà là nhờ kỹ thuật truy ngược để có được nó – và hắn đã nhận sự giúp đỡ từ một hacker khác.

Ai là người đã giúp Lottor trong dự án này? Thật bất ngờ, chính là Tsutomu Shimomura, một chuyên gia bảo mật máy tính với danh tiếng lẫy lừng và một cái tôi còn lớn hơn nữa, đang làm việc tại Trung tâm Siêu máy tính ở

https://thuviensach.vn

San Diego. Điều kỳ quặc là tại thời điểm đó, Lottor đang bị truy tố về vụ của Kevin Poulsen, vậy mà hắn vẫn nhận được sự giúp đỡ của một chuyên gia bảo mật máy tính đang làm việc cho chính phủ. Điều đó là sao?

Tôi từng có dịp chạm trán với Shimomura, nhưng anh ta chưa bao giờ phát hiện ra chuyện này. Năm trước, hồi tháng 9 năm 1993, sau khi thâm nhập vào mạng lưới của Sun, tôi phát hiện ra anh ta đang tìm kiếm và báo cáo lỗi bảo mật trong SunOS, một trong những hệ điều hành tiên tiến của Sun. Vì muốn có thông tin đó, tôi đã nhắm vào máy chủ của anh ta. Sau khi tấn công vào một máy chủ có tên "euler" tại Đại học California ở San Diego UCSD, tôi đã chiếm được quyền root và cài đặt sniffer vào hệ thống.

Hắn là ông trời cũng muốn giúp tôi. Chỉ trong vài giờ, tôi đã tóm được một tên đăng nhập, "david", và đăng nhập vào "ariel", một trong những máy chủ của Shimomura. Sau khi lấy được mật khẩu của david nhờ nghe lén đường dây, tôi truy cập vào hệ thống của Shimomura và hoạt động trên đó vài ngày trước khi bị phát hiện và đá ra ngoài. Shimomura cuối cùng đã phát hiện ra david bị hack, cố dò theo tôi nhưng chỉ đâm đầu vào ngõ cụt. Có lẽ anh ta đã theo dõi lưu lượng truy cập mạng của mình và phát hiện ra vấn đề, dù có muộn màng.

Trước khi bị đá ra ngoài, tôi đã thu được rất nhiều tập tin. Hầu hết những thứ thú vị này đều vượt quá tầm hiểu biết của tôi, nhưng tôi biết mình có thể quay lại nghiên cứu chúng một lúc nào đó. Giờ đây, nhờ Lottor, tôi lại có hứng thú với đống tài liệu này.

Trong quá trình thăm dò hệ thống của Lottor, tôi còn phát hiện ra một tập tin liệt kê các hướng dẫn thay đổi ESN từ bàn phím của điện thoại OKI.

to set the esn, enter debug mode.

the command is #49 NN SSSSSSSS <SND>

NN is 01 or 02

https://thuviensach.vn

SSSSSSSS is new ESN# in hex set security code to 000000 for easier access!

Có vẻ như Lottor và Shimomura đã dùng kỹ thuật truy ngược và xây dựng một phiên bản đặc biệt của firmware cho phép người sử dụng điện thoại dễ dàng thay đổi ESN từ bàn phím. Việc này không gì ngoài mục đích nhái số điện thoại của người khác. Tôi mỉm cười và lắc đầu. Đây là một bí ẩn còn lớn hơn: Tại sao một hacker bị truy tố và một chuyên gia bảo mật lại muốn nhái số điện thoại? Đây là bí ẩn tôi chưa bao giờ khám phá ra.

Dù sao thì tôi cũng chẳng thu được gì với mục tiêu ban đầu: tìm kiếm mã nguồn của nhà sản suất OKI. Khi nhìn qua đống tập tin dữ liệu của Lottor, tôi phát hiện ra Shimomura đã viết một chương trình phân tách "disassembler" 8051 mà Lottor dùng để truy ngược firmware. Tôi cũng đọc được vô số e-mail giữa Lottor và Shimumora thảo luận về dự án kỹ thuật truy ngược của họ. Trong một e-mail thú vị, Lottor gửi cho Shimomura một ứng dụng dòng lệnh[86] có tên là "modesn.exe".

[86] Ứng dụng dòng lệnh (console application): Ứng dụng không có giao diện đồ họa để thao tác chuột, tương tác bằng cách gõ lệnh. (ND)

OKI ESN Modifier. Copyright (C) 1994 Network Wizards.

Cái tên đã thể hiện tất cả: Đây là chương trình dùng để điều chỉnh ESN trên điện thoại OKI. Thật thú vị. Lại một lần nữa, tôi chỉ có thể nghĩ tới một mục đích có khả năng nhất: lừa đảo.

Tôi gom tất cả các tập tin liên quan tới điện thoại di động và nén chúng lại, bao gồm cả thư trao đổi với Shimomura. Nhưng quá trình này rất mất thời gian. Trong lúc chuyển tập tin, đột nhiên tôi bị rớt kết nối. Hắn là Lottor đã rút cáp mạng và dừng việc chuyển tập tin. Chết tiệt! Hắn ta đã ngắt máy tính ra khỏi mạng Internet.

Máy chủ của Lottor kết nối lại vào mạng Internet ngày hôm sau, sau khi hắn đã thay đổi tất cả mật khẩu của máy chủ. Không nản lòng, tôi tìm cách khác

https://thuviensach.vn

và phát hiện ra hắn đang hỗ trợ vài máy chủ ở “pagesat.com”, một dịch vụ tin tức tốc độ cao. Chỉ mất chưa tới một ngày, tôi đã có được root và cài đặt một sniffer.

Tôi liên tục quan sát sniffer. Chỉ trong vài giờ, Mark đã đăng nhập vào pagesat và từ đó kết nối với máy chủ của mình để đăng nhập. Sniffer của tôi ngay lập tức tóm được tài khoản đăng nhập của hắn.

Thực sự kích thích! Tôi chờ đến 6 giờ sáng, hắn là lúc này Mark đã đi ngủ. Tôi kết nối vào máy chủ của hắn và đăng nhập một lần nữa. Tuyệt vời, tập tin dữ liệu tôi định chuyển đi hôm trước vẫn còn ở đó. 30 phút sau, tôi sao chép nó vào một trong những tài khoản hack được ở Netcom.

Từ e-mail và các tập tin họ đã trao đổi, có vẻ như Lottor là trưởng dự án trong khi Shimomura chỉ làm việc khi rảnh rỗi. Rõ ràng là Shimomura cũng có mã của OKI trên máy anh ta và thậm chí còn có nhiều thông tin hơn những gì tôi lấy được từ Lottor. Tôi quyết tâm phải tìm ra bằng được. Một lúc nào đó tôi sẽ cần phải quay lại thâm nhập vào máy tính của Shimomura.

Tôi nghĩ mình không giỏi lắm trong việc che giấu cảm xúc. Sau khi làm việc Bộ phận Giải đáp hỗ trợ tại Trung tâm Y tế Virginia Mason được ba tháng, một hôm sếp nói với tôi: “Chúng tôi biết ở đây cậu thấy rất nhàm chán.”

“Vâng, đúng rồi,” tôi nói. “Tôi sẽ thử tìm việc khác.”

Dù điều này có nghĩa là tôi lại thất nghiệp và không có thu nhập, nhưng tôi thấy mừng là mình không còn phải đối mặt với sự nhàm chán mỗi ngày. Người ta vẫn thường nói rằng cuộc đời quá ngắn ngủi mà.

Quay trở lại tiệm in Kinko’s để chế thêm vài sơ yếu lý lịch, tôi mang theo chiếc máy quét cầm tay RadioShack Pro-43, vốn đã được cài đặt với các tần số vô tuyến điện được FBI, DEA, Cục Đặc trách Nhà tù Liên bang, Cảnh sát Tư pháp cũng như Sở Mật vụ sử dụng. Như tôi đã nói, cảnh sát liên bang thường “mượn” tần số của các sở ngành khác nếu họ nghi ngờ đối tượng có

https://thuviensach.vn

thể đang nghe lén. Thiết bị khử tiếng ồn của máy quét được thiết lập để bắt sóng các cuộc đàm thoại ở khu vực xung quanh.

Bản sơ yếu lý lịch đang dần thành hình thì có tiếng người phát ra từ radio. Tôi mở mạch giảm ồn một chút và chờ đợi. Một lúc sau, tín hiệu phát ra từ một trong những tần số của Sở Mật vụ.

“Có hoạt động gì không?”

“Không có.”

Thật thú vị. Rõ ràng là họ đang tiến hành hoạt động giám sát. Tôi tăng âm lượng và đặt máy quét lên nóc máy tính để bắt sóng tốt hơn.

Rất nhanh, máy quét bắt đầu xì xào đầy tiếng người nói: nghe như dần đến đoạn cao trào trong các bộ phim hình sự. Hẳn là cuộc vây bắt đã bắt đầu.

“Không có hoạt động gì ở đây,” một giọng vang lên.

“Chúng tôi đang ở ngõ, chắn phía sau,” một giọng khác đáp lại.

Một cô gái ở máy tính bên cạnh hỏi tôi đang nghe gì. Tôi mỉm cười và nói rằng đó là Sở Mật vụ, sau đó cười lớn khi nói thêm: “Nghe có vẻ như ai đó sắp có một đêm buồn.” Cô ấy cũng cười lớn. Chúng tôi chăm chú nghe để xem chuyện gì sẽ xảy ra tiếp theo.

“Liệu hắn có ở cửa hàng máy tính không?” một giọng nói phát ra từ radio.

Giờ thì có vẻ kỳ quái rồi đấy. “Cửa hàng máy tính” – đối tượng của bọn họ đang làm việc ở cửa hàng máy tính hay đó là một khách hàng?

Không có lời đáp.

Tôi bắt đầu thấy bồn chồn và lo lắng – có khi nào họ đang đợi tôi không? Tôi ngừng làm việc trên máy tính và tập trung chú ý vào radio.

https://thuviensach.vn

Sau đó, tôi lại nghe thấy: “Hắn lái loại xe gì?”

Ồ như vậy không phải là tôi: Tôi dùng phương tiện công cộng. Nhưng tôi vẫn lo lắng về vụ cửa hàng máy tính. 20 phút sau, “Chúng tôi vào đây.” Và sau đó radio im bặt.

Tôi tiếp tục làm việc chăm chỉ, chỉnh sửa khoảng 15 bản sơ yếu lý lịch cho các công việc khác nhau tại khu vực Seattle, vẫn điều chỉnh để đáp ứng khoảng 90% yêu cầu trên quảng cáo như thường lệ, mánh tuyệt nhất để có thể được gọi phỏng vấn.

Vẫn không có gì trên radio. Cô gái cạnh tôi đứng dậy, mỉm cười và chúc tôi một buổi tối tốt lành. Chúng tôi cùng nhìn chiếc máy quét và cười lớn, tự hỏi điều gì đã xảy ra với gã mà họ đang đợi.

Quá nửa đêm, tôi đã hoàn thành tất cả các hồ sơ sơ yếu lý lịch và đơn xin việc của mình. Tôi phải đợi một hàng dài chủ yếu toàn những sinh viên muốn in sơ yếu lý lịch trên các tấm giấy trắng ngà. Sau cùng cũng đến lượt mình, tôi được báo rằng hồ sơ của tôi sẽ được in ra vào sáng hôm sau. Chết tiệt! Tôi muốn gửi chúng đi ngay lập tức. Nhân viên ở quầy gợi ý tôi có thể thử một tiệm Kinko’s khác cách đó vài khu phố. Tôi bước tới cửa hàng khác nhưng câu chuyện vẫn tương tự: “Chúng tôi không thể in xong cho tới sáng.” Được rồi. Tôi nói tôi sẽ lấy tài liệu vào buổi sáng, dù biết rằng mình rất có thể sẽ lên mạng cả đêm, ngủ qua buổi sáng và sẽ không quay trở lại Kinko’s cho tới tầm trưa.

Sự việc hóa ra không phải vậy.

Trên đường về nhà, tôi dừng lại ở cửa hàng 24 giờ Safeway gần khu chung cư và mua vài đồ lặt vặt cộng với một chiếc bánh kẹp thịt gà tây cùng ít khoai tây rán cho bữa đêm muộn.

Hơn 1 giờ sáng tôi mới về gần đến nhà. Cuộc vây bắt của Sở Mật vụ mà tôi nghe lén được qua máy quét khiến tôi có chút bồn chồn. Như một nhân vật

https://thuviensach.vn

trong cuốn tiểu thuyết trinh thám, tôi phòng xa và bước dọc theo phía đường đối diện để quan sát xem có chiếc xe đáng ngờ nào không và để đảm bảo đèn trong căn hộ mình vẫn còn sáng.

Nhưng không. Trong nhà tối om. Không ổn rồi – tôi luôn để đèn sáng. Là do lần này tôi quên mất hay có chuyện gì đã xảy ra? Có một chiếc xe tải đỏ bên đường, tôi có thể thấy hai dáng người ngồi trên ghế trước: Một người đàn ông và một người phụ nữ đang hôn nhau. Điều này khiến tôi nghĩ tới một hình ảnh khá buồn cười: Liệu có phải là hai cảnh sát liên bang đang hôn hít nhau để cải trang không? Không thể nào, nhưng ý nghĩ này cũng làm tôi bớt phần căng thẳng.

Tôi bước thẳng tới xe tải và hỏi người trong đó: “Này, xin lỗi vì đã làm phiền nhưng tôi có hẹn với bạn ở đây. Anh có thấy ai đứng đợi quanh khu vực này không?”

“Không, nhưng mọi người mang rất nhiều thùng từ căn hộ kia ra” – người phụ nữ chỉ vào cửa sổ phòng tôi.Cái quái gì vậy? Tôi cảm ơn và nói rằng đó không phải là nơi bạn tôi sống.

Tôi lao lên cầu thang tới chỗ quản lý tòa nhà, David, và bấm chuông dù biết mình có thể đánh thức anh ta dậy. Một giọng ngái ngủ gào lên: “Ai thế?” Khi tôi không trả lời, anh ta hé cửa mở, chào tôi bằng giọng ngái ngủ và khó chịu: “Ồ, chào anh Brian.”

Tôi cố hết sức để che giấu sự lo lắng: “Anh có để ai vào phòng tôi không?”

Đáp lại là câu trả lời gây choáng váng mà tôi không thể ngờ đến: “Không, nhưng cảnh sát và Sở Mật vụ đã phá cửa phòng anh. Cảnh sát Seattle đã để lại lệnh bắt và một tấm danh thiếp nói rằng họ muốn anh gọi cho họ ngay lập tức.”

Có vẻ anh ta đã bắt đầu tỉnh táo để nổi cơn bực tức thực sự: “Anh sẽ trả tiền cho cái cửa chứ hả – phải không?”

https://thuviensach.vn

“Ừm, đương nhiên rồi.”

Tôi nói với anh ta rằng tôi sẽ gọi cho họ ngay.

Mồ hôi vã ra, vị chua của nỗi hoang mang tứa đầy khoang miệng, ruột gan cồn cào, tôi lao nhanh xuống bậc cầu thang và ra ngõ, tìm kiếm một vài dấu hiệu rắc rối – một chiếc xe không đánh dấu[87], chuyển động trên mái nhà hay bất kỳ thứ gì.

[87] Xe cảnh sát không được đánh dấu, trông như một chiếc xe thông thường. (ND)

Không có gì và cũng chẳng có ai.

Tôi vẫn còn một chút may mắn: Nếu là cảnh sát Seattle chứ không phải FBI thì hẳn họ đang tìm Brian Merrill, người đã thực hiện các cuộc gọi di động trái phép, chứ không phải là gã hacker lẩn tránh pháp luật Kevin Mitnick.

Drews nói cảnh sát Seattle và Sở Mật vụ đã qua khám xét phòng tôi rồi rời đi. Hẳn là họ sẽ không ngu ngốc tới mức lục tung phòng tôi mà không lưu lại quanh đây để tóm tôi.

Tôi bỏ đi thật nhanh, không dám chạy. Chắc hẳn gã quản lý đã gọi điện cho cảnh sát hoặc FBI để báo rằng tôi đã xuất hiện và bỏ đi sau đó.

Thật may, tôi đã mang theo mình chiếc cặp tài liệu chứa tất cả giấy tờ liên quan đến thân phận mới của tôi – tôi đã lường trước rằng mình có thể bắt gặp cảnh sát hay một chiếc xe không đánh dấu bất kỳ lúc nào. Tôi ném túi đồ lặt vặt mới mua vào thùng rác.

Tim tôi đập càng lúc càng gấp. Tôi đi nhanh hết mức có thể mà không cuống lên thành chạy, tránh các trục phố chính cho tới khi cách xa căn hộ vài khu phố. Tôi không ngừng nghĩ về những thứ trong cặp, bao gồm cả đống giấy khai sinh trống lấy từ Nam Dakota.

https://thuviensach.vn

Tôi không thể ném những tài liệu đó đi được, hiện giờ tôi cần chúng hơn bao giờ hết. Danh tính "vĩnh viễn" mới của tôi đã bị ném đi rồi, nó đã vô dụng mãi mãi. Tôi giữ chặt chiếc cặp. Tôi dám chắc vẫn có một nhóm cảnh sát liên bang đang lởn vởn gần đó để đợi. Ở một trong những chiếc xe đỗ ở đó sao? Đằng sau mấy cái cây? Hay trước cửa tòa nhà cuối phố?

Miệng tôi khô khốc như thể chưa uống giọt nước nào trong suốt vài ngày. Tôi lo lắng tới mức bắt đầu cảm thấy choáng váng. Mồ hôi túa khắp mặt.

Tôi bước vào một quán bar, thở hổn hển, hoàn toàn lạc lõng giữa những con người đang tiệc tùng vui thú, trút từng hớp rượu và tận hưởng không khí. Tôi trốn vào một phòng vệ sinh nam. Tôi muốn gọi cho mẹ nhưng không dám dùng di động, vì vậy, tôi chỉ ngồi ở đó để nghĩ xem mình có thể làm gì. Bắt taxi và biến khỏi khu vực này càng sớm càng tốt ư? Sở Mật vụ hẳn đang lái xe vòng quanh để tìm kiếm. Tôi chỉ muốn biến mất vào giữa đám đông.

Khi đã nghỉ ngơi đủ lâu để có thể trấn tĩnh lại, tôi bước ra vỉa hè, vẫy một chiếc taxi có thể đưa tôi ra khỏi khu vực. Một chiếc xe buýt lăn qua.

Xe buýt! Tấm vé ra khỏi nơi này!

Tôi chạy nhanh hết mức để bắt xe tại trạm dừng ở khu phố kế tiếp. Đi đâu cũng không thành vấn đề. Miễn là ra khỏi đây.

Tôi ngồi trên xe chừng một giờ cho tới bến cuối, sau đó bước xuống và đi bộ trong khí trời se lạnh để đầu óc thảnh thơi.

Tại cửa hàng tiện lợi 7-Eleven, tôi gọi vào máy nhắn tin của mẹ từ bốt điện thoại công cộng, gửi bà mã số 3 – "Khẩn cấp". Tôi đợi, chờ bà có thời gian thức giấc, mặc đồ, lái xe tới sòng bạc và nhắn lại cho tôi để tôi biết bà đang ở đâu. Khoảng chừng 40 phút sau, máy nhắn tin của tôi rung lên, cho tôi số điện thoại của Caesar's Palace. Tôi gọi vào khách sạn, nhờ chuyển máy tới mẹ và đợi đến khi bà nhấc máy.

https://thuviensach.vn

Các bạn hẳn có thể mường tượng ra, không dễ dàng gì khi nói với mẹ tôi về cú bắt hụt lần này và rằng tôi không dám quay trở lại căn hộ của mình. Tôi tuyệt vọng, nhưng mọi chuyện có thể đã tệ hơn. Tôi nói rằng mình có thể phải ngồi tù rồi.

Khi dập máy, tôi chọn một nhà nghỉ từ danh bạ Những Trang Vàng có địa chỉ ở khu trung tâm Seattle gần chợ Pike Place, nơi có cửa hàng Starbucks đầu tiên. Tôi gọi một chiếc taxi và nhờ lái xe dừng ở một trạm ATM để rút khoản tiền tối đa có thể, 500 đô-la.

Tôi dùng tên Eric Weiss để đăng ký nhà nghỉ, thân phận cũ mà tôi vẫn còn giữ giấy tờ trong cặp tài liệu.

Sáng hôm sau tôi sẽ biến khỏi đây, biến khỏi Seattle không một dấu vết – hy vọng là vậy.

Tôi nằm trên giường với cảm giác mất mát lớn lao. Tài sản duy nhất còn lại là quần áo trên người, vài món đồ ở tiệm giặt là và chiếc cặp táp chứa đầy giấy tờ chứng minh thân phận. Tất cả những thứ còn lại đều ở căn hộ.

Sáng hôm sau, tôi dậy rất sớm.

Cuộc vây bắt diễn ra vào buổi đêm. Tôi hy vọng cảnh sát liên bang đã dừng lại sau khi lập xong hồ sơ và thu thập mọi chứng cứ – và rằng họ sẽ không buồn tra tới máy tính cũng như đống giấy tờ của tôi, nơi họ có thể tìm ra hóa đơn giặt là và một cuốn sổ ngân hàng chỉ rõ nơi tôi cất giấu tiền bạc.

Điểm dừng chân đầu tiên là tiệm giặt là bởi nó mở cửa rất sớm. Tôi lấy số quần áo duy nhất còn lại ngoài chiếc quần jeans, áo da đen và áo phông Hard Rock đang mặc trên người.

Ngân hàng mở cửa lúc 9 giờ sáng, và bạn thử đoán xem ai là vị khách đầu tiên bước qua cửa? Tôi đóng tài khoản ngân hàng – chỉ có 4.000 đô-la trong đó, nhưng tôi sẽ cần tới từng số tiền ít ỏi đó cho màn hô biến sắp tới.

https://thuviensach.vn

Cảnh sát địa phương đã tóm được laptop, đĩa mềm, chiếc máy quét vô tuyến điện thứ hai, thiết bị ngoại vi và đống đĩa lưu trữ không mã hóa. Việc phát hiện ra Brian Merrill, gã giả mạo điện thoại di động, thực ra là Kevin Mitnick, kẻ bị cảnh sát liên bang truy nã, sẽ chỉ là vấn đề theo ngày.

Hay họ đã biết điều đó?

Tôi gọi điện tới văn phòng luật sư quận Seattle, hỏi thăm xem luật sư nào hay phụ trách các vụ giả mạo điện tử.

“Ivan Orton,” họ trả lời tôi.

Gọi điện cho thư ký của Orton, tôi nói với cô ta: “Tôi là đặc vụ Robert Terrent của Sở Mật vụ. Cô có bản sao lệnh bắt giữ và tờ khai tuyên thệ của vụ điện thoại di động tối qua không?”

“Không, anh phải gọi cho Phòng Lưu trữ,” và cô ta cho tôi số điện thoại.

Người phụ nữ ở Phòng Lưu trữ hỏi tôi địa chỉ cuộc vây bắt. Sau khi nghe tôi trả lời, cô ta nói: “À vâng, tôi có ngay đây.”

“Tuyệt, tôi đang ở hiện trường, cô có thể gửi fax bản sao cho tôi được không?”

“Tiếc quá,” cô nói. “Chúng tôi không có máy fax ở đây.”

Điều này không làm tôi bối rối. “Không vấn đề gì,” tôi nói. “Tôi sẽ gọi lại cho cô sau.”

Không có máy fax ở Phòng Lưu trữ hồ sơ? Thật kỳ lạ làm sao. Chúng ta đang nói về năm 1994; tất cả mọi người đều có một chiếc máy fax. Nhưng không – những cuộc gọi tới các văn phòng trong cùng tòa nhà cho thấy thành phố Seattle rõ ràng là không có nguồn ngân sách cho máy fax.

https://thuviensach.vn

Cuối cùng, tôi phát hiện ra Thư viện Luật có một chiếc. Ngay khi tôi sắp xếp xong thì người phụ nữ ở Thư viện Luật đã trên đường tới Phòng Lưu trữ để lấy một bản sao tờ khai có tuyên thệ và gửi fax cho vị "nhân viên Sở Mật vụ" đang cần. Bản fax được gửi tới tiệm Kinko's ở Bellevue. Tôi đợi một lúc, đoán chừng nó đã tới nơi, tiếp tục chuyển tiếp fax như thường lệ, rồi nhận nó vài phút sau đó ở tiệm Kinko's thứ hai – tất cả đều diễn ra trong khoảng thời gian rất ngắn để cảnh sát hay nhân viên Sở Mật vụ không kịp xuất hiện.

Tôi ngồi trong một quán cà phê và mải mê nghiên cứu tờ khai, như nuốt từng từ một. Tôi biết có hai gã thám tử điều tra vụ giả mạo điện thoại di động đã theo đuôi tôi trong vài tuần. Tôi nhớ lại chiếc xe Jeeep đỗ bên đường một ngày nọ, trong xe là một gã đàn ông. Khốn kiếp! Linh cảm của tôi đã đúng – hắn là một trong số hai kẻ điều tra tôi. Nội dung trong lệnh bắt giữ cho thấy những gã này đã nghe lén các cuộc gọi của tôi trong vài tuần. Tôi nhớ lại những cuộc gọi cho mẹ vài lần một tuần; đôi khi bà có nhắc đến tên tôi khi nghe điện thoại từ sòng bạc. Tuy nhiên, họ đã để lỡ điều này. Họ hẳn phải biết, hoặc ít ra cũng cảm thấy rằng, tôi không chỉ là một thằng nhóc nào đó nhái số điện thoại, dù vậy họ cũng không rõ danh tính thực của tôi là gì. Nếu nghi ngờ tôi là Kevin Mitnick, kẻ đang bị truy nã, họ hẳn đã khoanh vùng giám sát quanh căn hộ của tôi và đợi suốt đêm đến khi tôi trở về.

Tôi khá lo việc họ đã ghi âm các cuộc gọi và có lẽ còn chụp cả ảnh tôi. Biết rằng họ đã nghe thấy giọng tôi, tôi gọi cho Lewis để cậu ta có thể cập nhật tình hình và giúp tôi đánh giá tình huống. Tôi có một kế hoạch. Lewis sẽ gọi cho một trong hai gã thám tử tư để xem hắn đã thu được thông tin gì. Tôi thực sự cần phải biết họ có băng ghi âm hay ảnh gì không.

Tôi cũng ở trên đường dây để nghe lén, tắt âm điện thoại. Lewis gọi cho một gã thám tử tư tên là Kevin Pazaski và giả vờ là công tố viên Ivan Orton.

Pazaki nói: "Chúng ta có một cuộc hẹn ngày mai ở văn phòng của anh."

https://thuviensach.vn

Lewis chớp lấy cơ hội và trả lời: “Đúng, cuộc gặp vẫn diễn ra như cũ nhưng tôi có vài câu hỏi gấp.” Cậu ta hỏi liệu gã có băng ghi âm nào không. Pazaski nói không – họ đã giám sát các cuộc hội thoại và ghi chép lại, nhưng không thu âm.

Phù! Thật là nhẹ lòng! Tiếp đó, Lewis hỏi xem họ có bất kỳ ảnh chụp nào của đối tượng không. Lại một lần nữa, câu trả lời là không. Lạy Chúa! Lewis kết thúc cuộc gọi: “Được rồi, Kevin, tôi sẽ có thêm vài câu hỏi chuẩn bị cho buổi gặp ngày mai. Gặp lại anh sau.”

Mặc kệ tôi đã căng thẳng thế nào, Lewis và tôi bắt đầu cười lớn sau khi dập máy, tưởng tượng ra phản ứng của mấy gã này vào buổi gặp quan trọng ngày mai khi họ nhận ra mình đã bị lừa. Nhưng lúc đó thì đã quá muộn để họ có thể hành động. Tôi đã có thông tin mình cần.

Thật đáng với công sức bỏ ra. Từ các tài liệu này, tôi có thể đảm bảo rằng cuộc vây bắt nhắm vào một kẻ đã thực hiện rất nhiều cuộc gọi trái phép. Không hề liên quan tới Mitnick.

Đó là lý do tại sao cảnh sát lại để lại danh thiếp nói tôi nên gọi điện cho Sở Cảnh sát Seattle. Họ không cho rằng lưu lại quanh đấy để bắt một gã sinh viên đại học nào đó biết cách gọi điện miễn phí là cần thiết.

Nếu ở trong hoàn cảnh khác thì có lẽ tôi đã cảm thấy nhẹ nhõm hơn nhiều.

Tôi rời Seattle trên chuyến xe buýt Greyhound đi Tacoma, nơi tôi có thể lên tàu đi Portland và sau đó bay một chuyến bay mệt nhoài về Los Angeles. Trên đường đi, tôi gọi cho Ron Austin và kể lại cho anh ta nghe vụ vây bắt. Hóa ra cuộc gọi cho Ron không phải là một ý tưởng hay ho: Cũng như Peterson, anh ta đã trở thành kẻ chỉ điểm của cảnh sát với hy vọng được giảm mức án phạt. Anh ta ghi âm cuộc gọi của chúng tôi và chuyển cho FBI, chơi nước đôi với cả hai bên: Một mặt là bạn bè với tôi, cho tôi quyền đăng nhập vào DMV ở California… mặt khác, anh ta lại hợp tác với cảnh sát. Anh ta đang trong thời gian bảo lãnh, thu thập thông tin về Lewis và tôi cho

https://thuviensach.vn

đặc vụ FBI McGuire và công ty. Tôi phải thừa nhận rằng anh ta rất thông minh khi lấy được lòng tin của tôi nhờ đưa cho tôi quyền truy cập vào cơ sở dữ liệu của DMV.

Ngay sau đó, anh ta gọi cho người phụ trách ở FBI để báo rằng người mà Sở Mật vụ mới vây bắt vì tội danh giả mạo điện thoại thực ra chính là Kevin Mitnick. Tôi không nói với anh ta rằng mình ở thành phố nào, nhưng khẳng định người của Sở Mật vụ không mất quá lâu để tìm ra.

(Trong một cuộc trò chyện khi tôi thực hiện cuốn sách này, Austin đã tiết lộ một mẩu chuyện nhỏ lý thú: Cảnh sát liên bang đã nhái số máy nhắn tin của anh ta và đợi cuộc gọi của tôi nhằm lấy được số điện thoại công cộng cùng khoảng thời gian tôi gọi nhằm truy ra cuộc gọi kế tiếp. Họ không biết rằng tôi đã có được quyền truy cập tuyệt đối vào các bộ chuyển mạch kiểm soát số điện thoại mà tôi đang gọi – và tôi luôn kiểm tra các loại bẫy cũng như để ý đến bất kỳ tin nhắn chuyển mạch nào cho thấy sự truy dò tại thời điểm đó. Tôi cần phải cảnh giác, đặc biệt là với những hacker giỏi như Austin. Biện pháp đối phó của tôi hoàn toàn có hiệu quả: Cảnh sát chưa từng xuất hiện trước cửa nhà tôi.)

Tới Los Angeles, tôi chọn một khách sạn gần Union Station rất thuận tiện. Thức giấc vào giữa đêm, tôi bật đèn và thấy hơn chục con gián bò khắp phòng. Eoooo! Tôi phải lấy giày chỉ để bước vài bước tới nhà vệ sinh, trước tiên cẩn thận giũ từng chiếc giày để đảm bảo không có con gián nào trong đó. Cơn lạnh dọc sống lưng càng lúc càng rõ. Không dành lấy một khắc chần chừ, tôi dọn đồ ra khỏi khách sạn ngay sau đó 15 phút, chuyển tới khách sạn Metro Plaza, nơi được chọn vì cái tên có ý nghĩa đặc biệt đối với tôi. Hồi bị giam trong phòng biệt giam ở Trung tâm Giam giữ Đô thị của Los Angeles, phòng giam của tôi đã trông ra chính khách sạn này. Tôi từng ao ước được ở đó biết bao thay vì căn phòng 2x3 mét vuông với đệm nằm cứng như đá!

https://thuviensach.vn

Tôi không gặp cha trong suốt một thời gian dài. Ông lắng nghe tôi kể về việc bị bắt hụt và mấy gã cớm thậm chí còn không biết họ suýt tóm được người mà FBI đã săn lùng suốt hai năm nay. Đáp lại là sự im lặng, như thể ông không biết làm sao để giúp được tôi. Giống như tôi vừa mới mô tả một cảnh trong phim hay gì đó đến từ cái đầu tưởng tượng đầy sáng tạo của mình.

Tôi gọi cho Bonnie, nói rằng tôi đang ở Los Angeles và muốn gặp cô ấy. Tại sao lại là Bonnie? Bởi không có nhiều người tôi có thể nói về tình trạng gay go của mình. Các chiến hữu hacking của tôi, từng người từng người một, đã phản bội tôi. Không còn ai ở Los Angeles tôi có thể tin tưởng.

Cô ấy có lý do riêng để sẵn lòng gặp tôi. Lewis biết rằng các máy tính, đĩa từ và đĩa mềm của tôi đã bị tịch thu ở Seattle và cậu ta muốn biết cảnh sát có thể tìm ra quan hệ của chúng tôi ở mức độ nào – và chừng nào trong số đó có thể dùng để buộc tội cậu ta. Bonnie có lẽ chỉ muốn vì người yêu mình, hy vọng có được chút đảm bảo từ tôi rằng cảnh sát Seattle và Sở Mật vụ sẽ không lôi được bất kỳ thông tin gì có thể gây rắc rối cho Lewis trong đống tài liệu điện tử đó.

Chúng tôi gặp nhau, tôi nói với Bonnie rằng mình đã mất mọi thứ và cần phải bắt đầu lại từ đầu. Dù tất cả các tập tin trong máy tính của tôi đã bị mã hóa, tôi đã sao chép dự phòng hầu hết số đó trong các đĩa từ, không mã hóa. Tôi đã định giấu chúng trong các hộp ở ngân hàng ký gửi an toàn, nhưng tôi đã không kịp đến đó, đồng nghĩa với việc hoặc là cảnh sát liên bang, hoặc là cảnh sát Seattle, đã nắm trong tay toàn bộ thông tin đó, không mã hóa.

Cô ấy nhận ra tôi đang rất hoảng loạn. Bonnie cố gắng trấn an tôi và đưa ra vài lời khuyên, nhưng chúng tôi đều hiểu rằng lựa chọn duy nhất của tôi là đi tự thú và chấp nhận vài tháng, nếu không phải là vài năm, trong khu biệt giam đó. Nếu không thì sẽ là tiếp tục cuộc chơi “hãy bắt tôi nếu các anh có thể”. Tôi vẫn luôn hướng theo lựa chọn thứ hai và hậu quả đón đợi thậm chí còn cao hơn nữa khi giờ đây tôi không chỉ bị buộc tội vi phạm điều kiện tạm

https://thuviensach.vn

tha: Với bằng chứng từ máy tính đã bị tịch thu của tôi ở Seattle, cảnh sát liên bang giờ đây đã có đầy đủ chứng cứ cho các vụ hacking mà tôi từng thực hiện.

Tôi hiểu trực giác của Bonnie: Cô ấy chắc rằng việc tôi bị bắt chỉ còn là vấn đề thời gian và cô ấy đang lo lắng cho tôi. Nhưng tôi sẽ cố gắng đến cùng và chịu hậu quả sau. Thật tốt vì được gặp lại Bonnie kể từ khi tôi bắt đầu chạy trốn, nhưng nghĩ đến việc vợ cũ đang sống với chiến hữu hacking tốt nhất của mình, khoảng cách tồn tại giữa chúng tôi là điều tự nhiên.

Tại thời điểm tôi quay lại Vegas một tuần sau đó, mẹ và bà ngoại đã bình tĩnh lại so với lúc tôi bị bắt hụt. Khi gặp lại, tôi thấy mình đắm chìm trong tình yêu và sự quan tâm của họ.

Tuy đang rất cần một thân phận mới nhưng tôi cũng hiểu rằng việc dùng bất kỳ cái tên nào trong danh sách ở Nam Dakota cũng đều rất nguy hiểm bởi tất cả thông tin đó đều nằm trong đĩa lưu trữ không bị mã hóa mà cảnh sát đã tóm được trong vụ vây bắt ở Seattle. Tôi nhắm tới trường đại học lớn nhất ở thành phố lớn nhất của Oregon, Đại học Tiểu bang Portland.

Sau khi tấn công vào máy chủ của Phòng Tuyển sinh, tôi gọi cho quản trị viên cơ sở dữ liệu. “Tôi là nhân viên mới ở Phòng Tuyển sinh,” tôi nói với anh ta. “Tôi cần xem…” sau đó mô tả tham số mình quan tâm: Những người nhận được bằng tốt nghiệp trong giai đoạn 1985-1992. Anh ta nói chuyện điện thoại với tôi suốt 45 phút, giải thích các hồ sơ đó được sắp xếp thế nào và tôi cần các lệnh gì để có thể lấy được tất cả các dữ liệu về sinh viên tốt nghiệp trong năm nhất định nào đó.

Khi kết thúc, tôi đã truy cập được vào hồ sơ của 13.595 sinh viên, mỗi hồ sơ đều có chứa đầy đủ tên họ, ngày tháng năm sinh, bằng cấp, năm cấp bằng, mã số An sinh và địa chỉ nhà.

Tại thời điểm đó, tôi chỉ cần một danh tính trong số đó. Tôi sẽ trở thành Michael David Stanfill.

https://thuviensach.vn

Tình thế ngày càng gấp rút. Cảnh sát liên bang giờ đây có lẽ đã phát hiện ra tôi lại lọt qua tay họ một lần nữa. Hành trình ở Las Vegas lần này sẽ rất ngắn, chỉ cần vừa đủ để tôi có thể lo liệu một thân phận mới – hai đến ba tuần. Sau đó, tôi cần biến mất thật nhanh tránh trường hợp cảnh sát liên bang có thể bế tắc tới mức bắt đầu theo dõi cả mẹ tôi, người yêu mẹ và bà ngoại.

Công cuộc làm lại danh tính mới dưới cái tên Michael Stanfill cần phải tiến triển thật nhanh. Đối với bằng lái xe, bước quen thuộc sau khi lấy được bản sao giấy khai sinh và một số điện thoại nhái W-2 là xin lấy giấy phép học lái, đưa ra lý do quen thuộc với nhân viên ở DMV rằng tôi cần học vài buổi tập lái vì trước đó sống ở London, nơi mọi người thường lái xe phía bên trái đường.

Do mới lấy bằng lái dưới cái tên Eric Weiss ở DMV Las Vages vài năm trước, tôi có chút lo lắng khi quay lại đây một lần nữa – đặc biệt là khi tôi biết cảnh sát liên bang giờ đã được cảnh báo về việc tôi có thể muốn lấy một danh tính mới. Văn phòng DMV gần nhất ngoài Las Vegas là ở một thị trấn nằm trên sa mạc ở Pahrump, thường được biết tới nhờ hai điều: Art Bell, nhân vật nổi tiếng trên đài radio, cũng sống ở đây, và đây là nơi có Chicken Ranch, một nhà chứa hợp pháp ô danh. Theo luật của Nevada, mại dâm được cấp phép ở khu vực này của tiểu bang.

Tôi tra trên danh bạ Những Trang Vàng, tìm kiếm một trường lái ở Pahrump. Không tìm được địa điểm nào, tôi bắt đầu gọi tới các trường ở Las Vegas (đương nhiên là tránh xa nơi tôi đã học lái dưới cái tên Eric Weiss vài năm trước) và hỏi xem liệu mình có thể dùng một chiếc xe của họ để thi lái ở Pahrump hay không. Sau vài lần được đáp lại rằng: “Xin lỗi, chúng tôi không đưa người tới tận Pahrump”, cuối cùng tôi đã tìm được một trường lái nhận cấp xe và bài học lái trong chừng một giờ cho một gã “mới quay trở lại từ London và cần được luyện lại để có thể lái xe bên phải”, và chờ đợi để tôi thi lấy bằng xong – tất cả chỉ với 200 đô-la. Thật tuyệt. 200 đô-la là cái giá quá rẻ cho một danh tính mới.

https://thuviensach.vn

Bà ngoại lái xe đưa tôi tới Pahrump; tôi đề nghị bà đợi tôi trong một nhà hàng dưới đường vì sẽ rất nguy hiểm cho cả hai chúng tôi nếu có chuyện gì đó bất ngờ xảy ra như lần ở Kinko's đêm Giáng sinh.

Chúng tôi đến sớm chừng 20 phút. Tôi ngồi trên chiếc ghế nhựa rẻ tiền trong văn phòng DMV nhỏ xíu đó, hồi hộp chờ xe trường lái tới. Chỉ chưa tới hai giờ đồng hồ nữa, tôi có thể bước ra ngoài với một thân phận hoàn toàn mới dưới cái tên Michael David Stanfill.

Khi tôi ngước nhìn lên, một hướng dẫn viên lái xe bước vào cửa. Chết tiệt! Chính là cái gã đã từng dạy tôi hai năm trước đó. Hắn ta chắc đã đổi trường lái. Đúng là vận c*t chó.

Thật phi thường khi bộ óc vô thức của tôi đã lao vào hành động và vạch ra một kế hoạch ngay tức khắc. Tôi mở lời, từ ngữ tuôn ra: "Này, tôi biết anh. Anh thường mua sắm ở đâu ấy nhỉ?"

"Ở Smith's, trên Maryland Parkway," anh ta trả lời, có vẻ như đang cố nhớ xem đã gặp tôi ở đâu.

"À đúng rồi," tôi nói. "Tôi hay gặp anh ở đó. Tôi vẫn mua đồ ở đó suốt."

"Ồ, tôi cũng nghĩ đã từng gặp anh," anh ta nói, có vẻ chấp nhận lời giải thích này.

Giờ thì tôi phải thay đổi câu chuyện bởi lần trước tôi đã dùng bối cảnh "London" rồi. Thay vào đó, tôi nói với anh ta rằng tôi phục vụ trong Tổ chức Hòa bình của Mỹ ở Uganda và đã không lái xe năm năm nay rồi.

Lời nói dối này đã phát huy tác dụng. Anh ta rất hài lòng với việc tôi đã lấy lại khả năng lái xe của mình một cách nhanh chóng.

Tôi vượt qua bài kiểm tra không chút vấn đề và rời đi với bằng lái xe có tên Michael David Stanfill.

https://thuviensach.vn

Phần bốn

KẾT THÚC VÀ KHỞI ĐẦU

https://thuviensach.vn

33
HACK GÃ SAMURAI

Ozg ojglw lzw hshwj gf AH Khggxafy lzsl BKR skcwv ew stgml?

Giấy tờ tùy thân mới đã đâu vào đấy, đã đến lúc tôi dọn khỏi Las Vegas trước khi vận may cũng không cánh mà bay. Dịp nghỉ lễ Giáng sinh/Năm mới 1994 đang đến gần và tôi không thể không trở lại thăm Denver, thành phố mà tôi đã dần yêu. Gói ghém đồ đạc, tôi mang theo một chiếc áo khoác trượt tuyết cũ, nghĩ rằng mình có thể có thêm chút thời gian thảnh thơi trên các sườn núi trong dịp lễ.

Khi tôi đến Denver và ổn định tại một khách sạn hấp dẫn với giá cả phải chăng, có hai người mà tôi chưa gặp bao giờ, những người rồi đây sẽ trở thành diễn viên trong một vở kịch làm thay đổi toàn bộ phần đời còn lại của tôi. Một là gã chuyên gia bảo mật người Mỹ gốc Nhật ngạo mạn đã bị tôi hack vào máy chủ một năm trước, người còn lại là một hacker máy tính trình độ cao phi thường ở Israel.

Tôi vô tình gặp một anh bạn người Israel có tên viết tắt là “JSZ”; chúng tôi gặp nhau qua Internet Relay Chat, một dịch vụ trực tuyến giúp tìm kiếm và tán gẫu với những người lạ cùng sở thích. Trong trường hợp của chúng tôi, sở thích đó là hacking.

Cuối cùng, anh ấy khoe với tôi rằng mình đã hack hầu hết, nếu không phải là tất cả, các nhà sản xuất phần mềm lớn phát triển hệ điều hành – Sun, Silicon Graphics, IBM, SCO, v.v... Anh ấy đã sao chép mã nguồn từ các hệ thống phát triển nội bộ của họ và cài đặt cửa hậu để có thể quay lại bất cứ khi nào mình muốn. Đó thực sự là một chiến tích – rất ấn tượng.

https://thuviensach.vn

Chúng tôi bắt đầu chia sẻ với nhau những cuộc chinh phục hacking, những thông tin mới về các lỗ hổng, hệ thống cửa hậu, điện thoại nhái số, cách lấy mã nguồn cũng như cách xâm nhập hệ thống của các nhà nghiên cứu lỗ hổng.

Trong một cuộc gọi, anh ấy hỏi tôi đã đọc "nghiên cứu của Morris về giả mạo IP" chưa, nó tiết lộ một lỗ hổng lớn trong giao thức lõi của Internet.

Robert T. Morris, một thần đồng máy tính, đã tìm ra một lỗ hổng an ninh thông minh có thể bị khai thác bằng một kỹ thuật gọi là "IP spoofing" (giả mạo IP) để vượt qua quá trình xác nhận dựa trên địa chỉ IP của người dùng từ xa. 10 năm sau khi Morris công bố bài báo, một nhóm hacker, bao gồm cả JSZ ở Israel, đã tạo ra công cụ cho nó. Bởi tại thời điểm đó, nghiên cứu này đơn thuần chỉ mang tính lý thuyết, không ai nghĩ đến việc bảo vệ nó.

Dành cho những ai đam mê kỹ thuật, thuật tấn công giả mạo IP trong trường hợp này dựa trên một công nghệ đã lỗi thời gọi là R-service, vốn yêu cầu mỗi hệ thống máy tính cần được cấu hình sao cho hệ thống đó sẽ chấp nhận các kết nối được tin tưởng, tức là người dùng có thể đăng nhập vào một tài khoản – tùy vào cấu hình – mà không cần nhập mật khẩu. Việc này cho phép quản trị viên hệ thống cấu hình máy chủ sao cho nó có thể tin tưởng các máy tính khác nhằm hướng tới mục đích xác thực. Ví dụ, một quản trị viên hệ thống quản lý nhiều máy mỗi khi đăng nhập bằng tài khoản root sẽ không bị yêu cầu cung cấp mật khẩu để đăng nhập vào các hệ thống khác cần sự tin tưởng của máy chủ nữa.

Trong một cuộc tấn công giả mạo IP, đầu tiên, kẻ tấn công sẽ tìm kiếm các hệ thống khác có vẻ được tài khoản root trên máy chủ mục tiêu tin tưởng, tức là người dùng đăng nhập vào root trên một hệ thống được tin tưởng có thể đăng nhập vào tài khoản root trên máy chủ mục tiêu mà không cần nhập mật khẩu.

https://thuviensach.vn

Trong trường hợp này việc đó không quá khó. Bằng lệnh “finger”, kẻ tấn công có thể nhận ra nạn nhân đang kết nối tới hệ thống mục tiêu từ một máy tính khác trong cùng mạng LAN. Nhiều khả năng hai hệ thống này sẽ tin tưởng quyền truy cập root của nhau. Bước tiếp theo là thiết lập kết nối tới hệ thống mục tiêu bằng cách làm giả địa chỉ IP của máy tính được tin tưởng.

Tới đây thì mọi việc bắt đầu trở nên phức tạp. Khi hai hệ thống đang thiết lập kết nối ban đầu thông qua TCP, một chuỗi các gói tin[88] (packet) sẽ được trao đổi qua lại để tạo ra một “phiên” giữa chúng. Quá trình này được gọi là “bắt tay ba bước” (three-way handshake). Trong quá trình bắt tay, hệ thống mục tiêu chuyển một gói tin trở lại máy tính đang cố gắng thiết lập kết nối. Do máy chủ mục tiêu tin rằng nó đang hồi đáp lại yêu cầu của hệ thống thật để thiết lập kết nối, quá trình bắt tay sẽ thất bại bởi hệ thống của kẻ tấn công sẽ không bao giờ nhận được các gói tin nhằm hoàn tất quá trình bắt tay ba bước.

[88] Gói tin (packet): Khối thông tin được truyền trên máy tính. Gói tin có chứa địa chỉ của người gửi và người nhận, các thông tin về kiểm lỗi và các dữ liệu được thông báo. (BTV)

Giờ là lúc nói về số chuỗi TCP: Giao thức TCP sử dụng các số chuỗi để xác nhận việc nhận dữ liệu. Nếu kẻ tấn công có thể dự đoán số chuỗi của gói tin đang được gửi từ hệ thống mục tiêu tới máy chủ thật trong quá trình bắt tay ban đầu, hắn ta có thể hoàn thành quá trình bằng cách gửi một gói tin xác nhận (với số chuỗi chính xác) và thiết lập kết nối nhìn như xuất phát từ một máy tính được tin tưởng.

Quá trình này đã thiết lập hiệu quả một phiên kết nối thông qua việc đoán số chuỗi TCP. Vì hệ thống mục tiêu bị lừa rằng nó đã thiết lập kết nối tới một máy tính được tin tưởng, do đó, nó sẽ cho phép kẻ tấn công khai thác mối quan hệ tin tưởng này và vượt qua yêu cầu phải nhập mật khẩu – cho phép toàn quyền truy cập vào máy tính. Lúc này, kẻ tấn công có thể ghi đè lên tập

https://thuviensach.vn

tin .rhosts trên máy tính mục tiêu, cho phép bất cứ ai truy cập vào tài khoản root mà không cần mật khẩu.

Tóm lại, kỹ thuật tấn công này phụ thuộc vào việc kẻ tấn công có thể đoán được số chuỗi TCP của gói tin do máy tính mục tiêu gửi đi trong lần đầu liên lạc hay không. Nếu kẻ tấn công có thể đoán được số chuỗi TCP mà mục tiêu sẽ dùng trong quá trình bắt tay, hắn có thể giả dạng thành một máy tính được tin tưởng và vượt qua bất kỳ cơ chế bảo mật nào dựa trên địa chỉ IP của người dùng.

Tôi bảo JSZ mình đã đọc nghiên cứu này rồi. “Nhưng đó chỉ là lý thuyết. Chưa ai từng làm cả.”

“Ồ, bạn tôi ơi, tôi nghĩ là rồi đó. Chúng tôi đã phát triển xong công cụ và nó đã hoạt động rồi – thật tuyệt vời!” JSZ nói, ám chỉ phần mềm mà anh ấy và vài cộng sự rải rác khắp châu Âu đã làm.

“Không thể nào! Anh đùa đấy à!”

“Tôi không đùa đâu.”

Tôi hỏi anh ấy liệu có thể cho tôi một bản sao hay không.

“Để sau đã,” anh ấy nói. “Nhưng tôi sẽ chạy nó cho cậu bất cứ khi nào cậu muốn. Chỉ cần đưa tôi mục tiêu là được.”

Tôi chia sẻ với JSZ chi tiết cuộc tấn công vào máy chủ của Mark Lottor và mối quan hệ thú vị giữa anh ta và Tsutomu Shimomura, thông qua nickname của anh ta. Tôi giải thích mình đã hack vào UCSD và “đánh hơi” trên mạng cho đến khi ai đó có tên là “ariel” kết nối đến máy chủ của Shimomura, sau đó tôi vào được đó. “Bằng cách nào đó, Shimmy nhận ra một người có quyền truy cập đến máy tính của gã đã bị hack và gã đá tôi ra khỏi máy chủ sau vài ngày,” tôi nói.

https://thuviensach.vn

Tôi thấy vài lỗi bảo mật mà Shimmy báo lại cho Sun cùng DEC và rất ấn tượng với trình độ phát hiện lỗi của gã. Sau đó, tôi biết hắn có mái tóc đen dài chấm vai, thích đi dép lê, mặc quần jeans "nát" đến chỗ làm và có niềm đam mê với môn thể thao trượt tuyết băng đồng. Gã có vẻ giống hình mẫu "anh bạn" (dude) mà người California hay nhắc đến – như trong câu: "Này anh bạn, dạo này sao rồi?"

Tôi bảo JSZ rằng Shimmy có thể có mã nguồn của OKI hay nội dung chi tiết về nỗ lực truy ngược của gã và Lottor, chưa kể những lỗi bảo mật mới mà gã có thể đã tìm ra.

Vào dịp Giáng sinh năm 1994, khi bước ra khỏi rạp chiếu phim tại Tivoli Center ở trung tâm Denver, tôi bật chiếc điện thoại nhái số của mình lên và gọi JSZ để trêu đùa anh ấy bằng một câu chúc mừng Giáng sinh tiếng Do Thái.

"Tôi rất vui vì cậu đã gọi."Anh ấy nói với tôi bằng giọng điệu lạnh lùng và điềm tĩnh: "Tôi có một món quà Giáng sinh cho cậu đây. Bạn của tôi, tôi đã truy cập được vào ariel tối nay." Rồi anh ta đưa cho tôi số hiệu cổng (port) đã cài cửa hậu. "Khi cậu kết nối, sẽ không có dấu nhắc lệnh nào. Cứ gõ ".shimmy." và cậu sẽ lấy được root shell."

"Không thể nào!"

Đây quả là món quà Giáng sinh vô cùng tuyệt vời. Tôi đã luôn muốn đột nhập vào máy tính của Shimmy để tìm hiểu xem hắn và Mark Lottor đang toan tính điều gì với dự án điện thoại OKI và tôi muốn biết liệu ai trong số họ có quyền truy cập vào mã nguồn. Dù thế nào tôi cũng sẽ lấy bất kỳ thông tin gì có liên quan đến điện thoại OKI 900 và 1150 trên máy chủ của gã.

Shimmy vốn nổi tiếng trong cộng đồng hacker bởi thái độ rất ngạo mạn – gã ta nghĩ mình thông minh hơn tất thảy mọi người xung quanh. Chúng tôi quyết định sẽ hạ bệ cái tôi của gã xuống vài bậc để gã có thể ý thức được thực tế – đơn giản vì chúng tôi có thể.

https://thuviensach.vn

20 phút ngồi trong chiếc xe đi thuê để trở về khách sạn là 20 phút dài nhất trong đời tôi. Nhưng tôi không dám lái nhanh hơn luồng giao thông. Nếu tôi bị yêu cầu tấp vào lề và cảnh sát phát hiện ra thứ gì đó khả nghi ở bằng lái xe của tôi, tôi sẽ phải chờ lâu hơn rất nhiều so với 20 phút trước khi có thể lại được lên mạng. Bình tĩnh, phải bình tĩnh.

Ngay khi vừa bước vào phòng khách sạn, tôi bật laptop lên và kết nối tới Colorado Supernet, giấu cuộc gọi như mọi khi bằng cách nhái số của tôi sang số điện thoại của một cư dân Denver ngẫu nhiên nào đó.

Tôi khởi động chương trình giao tiếp mạng để tạo kết nối trực tiếp tới máy của JSZ ở Israel để chúng tôi có thể giao tiếp với nhau tại một cửa sổ trong lúc tấn công Shimmy ở một cửa sổ khác. Tôi kết nối tới máy của Shimmy thông qua cửa hậu mà JSZ đã cài đặt. Bingo! – Tôi đã truy cập vào với quyền root.

Không thể tin được! Phấn khích làm sao! Chắc hẳn đây là cảm giác của một đứa trẻ khi đến được màn cuối cùng trong trò chơi điện tử mà nó đã chật vật giải quyết hàng tháng trời. Hay như khi lên được đỉnh Everest vậy. Run lên vì sung sướng, tôi chúc mừng JSZ đã làm tốt công việc.

Để bắt đầu, JSZ và tôi thăm dò hệ thống của Shimmy nhằm tìm kiếm những thông tin quý giá nhất – bất kỳ thứ gì có liên quan đến lỗi bảo mật, e-mail của gã, hay bất cứ tập tin nào có chữ “oki” ở tên. Gã có hàng tấn tập tin. Trong lúc tôi gom và nén lại bất kỳ thứ gì khớp với mục tiêu đề ra, JSZ cũng nhòm ngó xung quanh để tìm kiếm những thứ hữu dụng khác. Cả hai chúng tôi đều lo rằng Shimmy có thể giữa chừng đăng nhập để xem thiệp mừng Giáng sinh trong e-mail và phát hiện ra mình đã bị hack. Chúng tôi muốn lấy mọi thứ trước khi gã phát hiện ra. Tôi lo ngại gã có thể sẽ rút dây mạng, như Lottor đã làm vài tháng trước.

Chúng tôi cấp tốc lấy thông tin trong máy tính của Shimmy. Endorphin trong người tôi đang trào lên quá mức.

https://thuviensach.vn

Sau khi tìm kiếm, gom lại và nén, tôi cần một chỗ để lưu trữ an toàn đống mã nguồn. Không thành vấn đề: Tôi đã có quyền truy cập root đến mọi máy chủ tại Whole Earth ‘Lectronic Link, còn được gọi là “the Well”. Được sáng lập bởi Stewart Brand và cộng sự, the Well có những người dùng rất nổi tiếng trên Internet, nhưng tôi không để tâm tới danh tiếng của nó. Điều duy nhất tôi quan tâm là liệu nó có đủ dung lượng còn trống và liệu tôi có thể giấu các tập tin đủ tốt để các quản trị viên hệ thống không nhận ra không. Trên thực tế, tôi đã dành rất nhiều thời gian trên trang này. Vài ngày sau khi bài báo trên trang nhất của New York Times của John Markoff ra mắt, tôi phát hiện ra hắn có một tài khoản trên the Well. Một mục tiêu dễ dàng: Tôi đã đọc e-mail của hắn từ lúc đó, tìm kiếm bất kỳ thứ gì có liên quan đến tôi.

Sau khi di chuyển dữ liệu mục tiêu xong, chúng tôi quyết định sẽ lấy mọi thứ trong thư mục chính[89] của Shimmy. JSZ gom và nén toàn bộ thư mục chính vào một tập tin duy nhất nặng hơn 140 megabyte.

[89] Thư mục chính (Home directory): Thư mục chứa tập tin của người dùng. (BTV)

Chúng tôi nín thở chờ đến khi tập tin được chuyển đi thành công, rồi đập tay nhau qua màn hình chat.

JSZ chuyển một bản sao của tập tin này sang châu Âu đề phòng trường hợp quản trị viên hệ thống của the Well tình cờ phát hiện ra tập tin cỡ lớn và xóa nó đi. Tôi cũng sao chép nó sang một vài địa điểm khác.

JSZ liên tục bảo tôi rằng Shimmy sẽ rất dễ phát hiện ra cửa hậu mà anh ấy đã cài đặt cho lần truy cập của tôi. Tôi cũng nghĩ vậy, nó quá dễ tìm. Tôi gợi ý chúng tôi có thể xem xét đặt một cửa hậu phức tạp hơn vào chính hệ điều hành, để nó khó bị phát hiện hơn.

“Hắn sẽ tìm ra thôi,” JSZ phản bác.

“Ừ, chúng ta có thể quay lại theo cách cũ sau,” tôi nói.

https://thuviensach.vn

Tôi đăng xuất khỏi hệ thống và JSZ dọn dẹp, xóa cửa hậu đơn giản đó cùng toàn bộ ghi chép hoạt động của chúng tôi.

Đó là khoảnh khắc rất hứng khởi. Chúng tôi đã đột nhập vào máy chủ của một chuyên gia bảo mật – trong trường hợp của tôi, đây là lần thứ hai chỉ trong hơn một năm. JSZ và tôi quyết định mỗi người sẽ tự xem xét đống tập tin của Shimmy và báo lại cho nhau những gì mình tìm được.

Nhưng dù chúng tôi có cẩn thận xóa dấu vết đến đâu, tôi biết gần như chắc chắn Shimmy sẽ bắt gặp một trong những dấu vết mà chúng tôi đã bỏ qua.

Xem xét e-mail cũ của Shimmy, tôi thấy các tin nhắn trao đổi qua lại giữa gã và kẻ thù truyền kiếp của tôi, cây bút công nghệ John Markoff của tờ New York Times. Từ đầu năm 1991, họ đã trao đổi e-mail về tôi – những mẩu tin về những gì tôi đang mưu tính, một trao đổi đầu năm 1992 cho thấy Shimmy đã chịu khó tìm kiếm trên mạng giấy phép ham radio của tôi, dấu hiệu gọi N6NHG. Gã cũng e-mail cho Markoff hỏi liệu FCC có luật nào ngăn cản việc cấp phép ham radio cho một người bị kết trọng án hay không. Lý do vì sao họ lại hứng thú với tôi đến vậy tới giờ vẫn còn là một ẩn số.

Tôi chưa bao giờ gặp Shimmy, chưa bao giờ tương tác với gã theo bất kỳ cách nào ngoại trừ mấy lần hack gần đây vào hệ thống của gã.

Vậy tại sao họ lại hứng thú với những gì tôi đang làm đến vậy?

Tôi đã đúng về một chuyện: Shimmy đã rất nhanh chóng phát hiện ra vụ đột nhập của chúng tôi. Do quá tập trung vào việc lấy bản sao các tập tin nên JSZ và tôi đã không để ý tới việc gã đang chạy “tcpdump” – một công cụ theo dõi mạng thu lại tất cả lưu lượng truy cập mạng. Chúng tôi cũng không để ý tới một chương trình có tên là “cron” đang đều đặn gửi e-mail ghi chép hệ thống cho Andrew Gross, trợ lý của Shimmy. Gross nhận ra các ghi chép đang nhỏ dần và nói với Shimmy chuyện khả nghi đang diễn ra. Ngay khi Shimmy nhìn qua các tập tin ghi chép, gã đã nhận ra mình bị hack.

https://thuviensach.vn

Không có gì quá quan trọng. Chúng tôi đã có các tập tin của hắn và chúng tôi sẽ dành nhiều thời gian để xem xét kỹ càng.

Tại sao Shimmy lại chạy một công cụ theo dõi mạng để ghi lại mọi thứ đi ra khỏi máy chủ của gã? Gã bị hoang tưởng ư? Hay đó chỉ là một máy mồi bẫy? Vốn nổi tiếng trong giới an ninh máy tính, gã biết việc sẽ có người chơi gã bằng một vụ tấn công thông minh. Tôi nghĩ đó có thể là máy mồi bẫy, được thả cho truy cập để gã có thể theo dõi mọi cuộc tấn công đến và lập hồ sơ các phương pháp được sử dụng. Nhưng trong trường hợp đó, tại sao gã lại để tất cả tập tin của mình trên máy, kể cả công cụ nghe lén mạng "bpf"– viết tắt của Berkeley Packet Filter (bộ lọc gói Berkeley) – mà gã đã làm cho Không quân Mỹ, thứ có thể tự chèn nó trực tiếp vào hệ điều hành mà không cần khởi động lại?

Có thể đơn giản chỉ là gã đã đánh giá thấp đối thủ của mình và cho rằng không ai có thể đột nhập được máy tính của gã. Chuyện này đến nay vẫn là một bí ẩn.

Nhiều người tưởng rằng tôi chính là người đã phát triển phần mềm hack vào máy chủ của Shimmy thông qua tấn công giả mạo IP. Tôi sẽ rất tự hào nếu mình thực sự là người đã làm nên chiến tích huy hoàng đó và rất vui lòng nhận công về mình. Nhưng công trạng này không thuộc về tôi. Thay vào đó, vinh hạnh này thuộc về JSZ thông minh quái kiệt, người đã thực sự tham gia vào việc phát triển công cụ đó và dùng nó cho cuộc tấn công của chúng tôi hôm Giáng sinh vào máy chủ của Shimmy.

* * *

Tôi đã tận hưởng khoảng thời gian quay lại Denver vào dịp lễ, đặc biệt là bởi chúng tôi đã vào được hệ thống của Shimmy. Nhưng cũng đã đến lúc tôi cần để lại thành phố tuyệt vời này sau lưng và tiến tới điểm đến tiếp theo.

Tôi vẫn đang phấn khích vì hack thành công Shimmy. Nhưng sau này tôi sẽ phải hối tiếc vì điều đó. Vài tiếng huy hoàng đó cuối cùng đã dẫn đến sự tàn

https://thuviensach.vn

lụi của tôi. Tôi đã chạm vào vảy ngược của một anh hùng chống hacker, người sẽ không dừng lại cho đến khi ăn thua đủ với tôi.

https://thuviensach.vn

34
LÁNH VỀ PHƯƠNG NAM

Nvbx nte hyv bqgs pj gaabv jmjmwdi whd hyv UVT'g Giuxdoc Gctcwd Hvyqbuvz hycoij?

Hãy tưởng tượng bạn đang ở một thành phố xa lạ, không có người quen và đáng tin cậy nào. Bạn phải tránh những người sống cùng khu căn hộ bởi ảnh chụp của bạn đã bị bày chình ình trên khắp các trang báo lớn và các tạp chí tin tức hằng tuần. Bạn đang bị FBI, Sở Cảnh sát Tư pháp và Sở Mật vụ săn lùng, do đó bạn không dám quá thân thiết với bất kỳ ai. Và phương thức giải sầu tốt nhất lại chính là thứ mà vì nó bạn đang bị săn lùng

Dù chưa cần phải vội vã rời khỏi Seattle, nhưng tôi đã bắt đầu nghĩ về điểm dừng chân tiếp theo trong trường hợp mình phải chuyển đi. Tôi tính tới Austin bởi đó là nơi nổi tiếng về công nghệ. Và Manhattan bởi nó là… ừm, Manhattan. Nhưng cũng như lựa chọn Denver trước đây, tôi vẫn dựa vào đánh giá thường niên của tạp chí Money về 10 thành phố tốt nhất ở Mỹ. Năm đó, Raleigh ở Bắc Carolina được xếp ở vị trí đầu tiên. Mô tả nghe có vẻ hấp dẫn: Người dân khá dễ chịu và thư thái, những khu thôn dã bao quanh với các dãy núi phía xa xa.

Đi máy bay khiến tôi căng thẳng, vì thế lần này tôi quyết định đi tàu. Được nhìn ngắm các vùng đất còn lại của đất nước là một trải nghiệm tuyệt vời. Sau lần tạm dừng chân tại Denver vào dịp Giáng sinh và đột kích vào máy chủ của Shimmy, tôi đáp một chuyến tàu Amtrak khác vào đêm đầu năm mới để tham gia chuyến đi kéo dài ba ngày tới Raleigh với thân phận Michael Stanfill. Khoang tàu nằm còn có giá vé đắt hơn vé máy bay, nhưng rút cục đây quả thực là một trải nghiệm mở mang đầu óc khi được nhìn ngắm phong cảnh nước Mỹ trôi trước mắt.

https://thuviensach.vn

Những người gặp gỡ trên tàu cho tôi cơ hội hoàn hảo để diễn tập câu chuyện về thân phận mới với các chi tiết về cuộc đời và quá khứ của Stanfill. Tại thời điểm tới Bắc Carolina, tôi đã hoàn toàn nhuần nhuyễn thân phận mới của mình.

Tàu dừng bánh tại ga Raleigh khi trời sẩm tối. Tôi đã được nghe kể nhiều về miền Nam, về sự khác biệt trong văn hóa và con người, về nhịp sống chậm rãi nơi đây. Biết đâu cái danh này chỉ là những gì còn sót lại của một miền Nam xưa cũ. Tôi thật tò mò muốn được tự mình khám phá.

Tối hôm đó, tôi đi dạo quanh khu vực phía Bắc Raleigh để cảm nhận cuộc sống thành phố. Tôi từng mường tượng phía Nam hẳn phải có thời tiết ấm áp dễ chịu, nhưng không, tiết trời ở đây cũng lạnh như ở Denver. Nhiệt độ vào mùa đông ở Raleigh cũng tương tự như ở Thành phố Cao một dặm.

Nhưng khi đi loanh quanh để cảm nhận nơi đây, tôi phát hiện ra một quán ăn quen thuộc, một cửa hàng trong chuỗi Boston Market. Nó không hẳn mang hương vị miền Nam nhưng tôi vẫn bước vào để dùng bữa tối.

Bồi bàn là một cô gái dễ thương độ ngoài 20 với mái tóc dài sẫm màu, nụ cười ấm áp cùng chất giọng lè nhè miền Nam đầy khêu gợi mà tôi không nghĩ là vẫn còn tồn tại. Cô ấy chào tôi đầy thân thiện: “Xin chào, anh thế nào?”

Đọc thẻ tên của cô, tôi nói, “Chào Cheryl, tôi ổn. Tôi mới tới thị trấn – đây là lần đầu tiên tôi tới Bắc Carolina.” Sau khi gọi món, tôi nói: “Tôi đang tìm một căn hộ. Cô có biết nơi nào trong thị trấn phù hợp để ổn định không?” Cô ấy cười và nói sẽ quay trở lại.

Sau khi phục vụ đồ ăn, cô ấy cùng một vài bồi bàn khác ngồi cạnh tôi để nói chuyện trong lúc tôi dùng bữa. Tôi không thể tưởng tượng được điều này sẽ xảy ra ở Los Angeles hay Seattle. Hay thậm chí là ở Denver phóng khoáng. Những cô gái nói với tôi: “Chúng tôi chỉ muốn làm bạn với anh thôi.” Tôi bị kinh ngạc bởi trải nghiệm đầu tiên về lòng hiếu khách của con người miền

https://thuviensach.vn

Nam, sự thân thiện ngọt ngào hơn bất kỳ điều gì tôi từng biết tới. Những cô gái nói về cuộc sống ở Raleigh. Họ kể cho tôi nghe về sự khác nhau giữa các khu vực của thị trấn, nên sống ở đâu, nên làm gì. Đây vẫn là một vùng quê trồng thuốc lá nhưng đã trở nên tân tiến hơn nhờ các công ty về công nghệ quanh khu Research Triangle Park. Họ là những nhân tố thúc đẩy thành phố và vì lý do nào đó, với tôi đây là dấu hiệu tốt về một nơi đáng sống.

* * *

Chỉ một tuần sau khi đặt chân tới Raleigh, tôi đã tìm được một căn hộ dễ chịu ở phía Tây Bắc trong khu tổ hợp "The Lakes", một cái tên khá phù hợp bởi khuôn viên hơn 4.000m2 của nó còn bao gồm đường ven bờ của hai con sông riêng biệt. Nơi đây không chỉ gồm bể bơi có kích cỡ tiêu chuẩn Olympic, các sân tennis, sân bóng quần mà còn có cả hai sân bóng chuyền được thiết kế hệt như bãi biển nhờ rất nhiều xe tải cát đổ tới. The Lakes cũng tổ chức các bữa tiệc cuối tuần cho cư dân của họ, với tôi thì đây hẳn là những cuộc tụ tập ồn ã, náo nhiệt, với những cô nàng miền Nam tươi cười. Căn hộ của tôi khá nhỏ, nhưng ai thèm quan tâm cơ chứ? Tôi cảm thấy như mình đang sống trong một giấc mơ vậy.

Tôi ghé vào trạm thuê xe U-Save Auto Rental do một người đàn ông quản lý, kiểu cửa hàng mà chủ sở hữu sẽ săm soi kỹ từng người bước vào, như thể anh ta cho rằng rất có thể họ sẽ không đem xe giao trả lại. Anh ta cũng nhìn tôi đầy nghi ngờ, nhưng sau cuộc trò chuyện thân thiện không hấp tấp của tôi, anh ta thấy thoải mái hơn.

"Tôi vừa mới trải qua một vụ ly hôn khốn kiếp," tôi nói. "Tôi tới Raleigh bởi nó cách xa Vegas, anh hiểu ý tôi chứ?" Đây là lời giải thích cho việc tại sao tôi lại thanh toán bằng tiền mặt. Như một phần trong vở diễn, tôi đưa cho anh ta tấm danh thiếp của công ty mà tôi đã "làm" ở Vegas – chính là công ty giả mạo tôi đã chế ra để được nhận vào làm trong hãng luật ở Denver.

https://thuviensach.vn

Ngay khi tôi sẵn sàng để leo lên chiếc xe cà tàng tạm thời, anh ta đã để tôi lái xe đi mà không cần kiểm tra kỹ càng.

Tôi liên tục nghĩ về bước cuối cùng trong vụ hack Motorola: lấy được trình biên dịch có thể dịch các mã nguồn sang một dạng ngôn ngữ mà chip điện thoại hiểu được. Có được trình biên dịch đó sẽ cho phép tôi thay đổi mã nguồn và biên soạn một phiên bản firmware mới cho phép thu nhỏ sự hiện diện của tôi – ví như, tôi có thể bật và ngắt liên lạc điện thoại với nhà cung cấp dịch vụ nhằm chặn chế độ theo dấu và thêm vào các chức năng giúp thay đổi ESN từ bàn phím điện thoại di động một cách dễ dàng hơn, nhờ vậy, tôi có thể giả mạo số điện thoại của bất kỳ thuê bao nào.

Khi đã vào đà thực hiện mục tiêu, với chút nỗ lực tìm hiểu cho thấy Motorola hiện đang dùng một trình biên dịch có tên là Intermetrics, tôi đưa nó trở thành mối ưu tiên hàng đầu trong danh sách mục tiêu tấn công của mình. Tôi xác định được một máy tính có tên “blackhole.inmet.com” thuộc hệ thống nội bộ của Intermetrics có thể kết nối trực tiếp từ Internet.

Khi phát hiện ra các hệ thống của công ty này đã được vá để chống lại tất cả các lỗi bảo mật mới nhất, tôi nhanh chóng thay đổi chiến thuật. Thật tiện cho tôi khi “blackhole” hóa ra cũng dễ bị tấn công trước cùng một dạng công kích giả mạo IP mà JSZ và tôi đã dùng để chống lại Shimmy.

Khi đột nhập vào hệ thống, tôi nhận thấy đã có hai quản trị viên hệ thống hiện đang hoạt động và rõ ràng là họ rất bận rộn với công việc của mình. Thay vì mạo hiểm để bị phát hiện nếu một trong số họ kiểm tra các kết nối hiện tại, tôi nên tìm kiếm các cách thay thế để có thể đăng nhập từ xa mà không dễ bị phát giác. Có lẽ, tôi có thể tìm được số dial-up và kết nối qua modem của mình.

Trong các tệp tin của một trong những quản trị viên, Annie Oryell, tôi tìm được một tệp tin có cái tên khá hứa hẹn: “modem”. Chuẩn rồi! Tệp tin này

https://thuviensach.vn

chứa đoạn văn bản của một e-mail mà cô ta đã gửi tới các nhân viên khác để thông báo các số dial-up. Một phần nội dung như sau:

Hiện chúng ta đang có hai nhóm săn số (hunt group) dial-in. Nhóm 661-1940 gồm 8 Telebit modem 9600bps kết nối trực tiếp vào máy chủ thiết bị đầu cuối Annex. Nhóm 661-4611 gồm 8 Zoom modem 2400bps kết nối trực tiếp vào máy chủ thiết bị đầu cuối.

Đây rồi: "661-1940" và "661-4611" là các số dial-in mà tôi đang tìm kiếm. Tôi thay đổi mật khẩu của vài tài khoản có vẻ không còn hoạt động trên máy chủ Annex và kết nối để tránh nguy cơ bị phát hiện trên các hệ thống có mạng Internet.

Có vẻ như quản trị viên hệ thống Oryell đang dùng máy chủ blackhole cho mục đích cá nhân. Tôi đoán cô ta sẽ cần tới quyền ưu tiên root để thực hiện các nhiệm vụ quản trị và sẽ dùng lệnh chuyển người điều khiển "su", do vậy, tôi thiết lập cách để bắt được mật khẩu root khi cô ta làm việc này. (Dành cho các độc giả am hiểu kỹ thuật: Nhờ dùng mã nguồn có được từ Sun Microsystems, tôi đã thêm vài mã vào chương trình "su" và tái biên soạn nó để khi quản trị viên thực hiện "su", nó sẽ bí mật ghi lại mật khẩu vào một tập tin ẩn trên máy tính của cô ta.)

Kết quả đúng như tôi đã dự đoán. Mật khẩu root là "OMGna!" Lạy Chúa – mật khẩu không phải là một từ có nghĩa thường xuất hiện trong từ điển, kèm thêm là dấu chấm than khiến việc đoán ra nó trở nên khó khăn hơn.

Mật khẩu root này cũng được dùng trong mọi máy chủ khác mà tôi đã thử.

Có được mật khẩu giống như có được chìa khóa vào vương quốc, ít nhất là đối với hệ thống nội bộ của Intermetrics.

Tại thời điểm này, tôi đăng nhập vào "inmet.com", domain của công ty dùng để nhận thư điện tử từ bên ngoài gửi đến. Tôi tải về bản sao của tệp tin chứa

https://thuviensach.vn

mật khẩu chủ[90] (tệp tin này cũng đồng thời chứa các mã băm mật khẩu) để có thể lấy được tất cả mật khẩu mà không cần lên mạng.

[90] Mật khẩu chủ (Master password): Mật khẩu dùng để lấy được tất cả các mật khẩu khác. Một người dùng có thể lưu trữ các mật khẩu của mình trong một tệp mã hóa và chỉ có thể mở nó ra bằng một mật khẩu chủ. (ND)

Giờ đến việc tra thư điện tử để tìm ra người thường liên lạc với Motorola. Kết quả đầu tiên là một e-mail được gửi tới Marty Stolz, kỹ sư của Intermetrics, người này đã nhận được tin nhắn từ ai đó ở Motorola giải thích các vấn đề họ gặp phải với trình biên dịch. Tôi đột nhập vào máy tính làm việc của Stolz và tra "shell history" (lịch sử lệnh) của anh ta, lấy được danh sách các câu lệnh mà anh ta đã gõ trước đó. Stolz đã chạy một chương trình đặc biệt, một "shell script" có tên "makeprod", để xây dựng các trình biên dịch mà công ty phát triển. Trong trường hợp này, tôi muốn có trình biên dịch 68HC11 để có thể biên soạn mã nguồn Motorola cho chiếc MicroTAC Ultra Lite.

Tay kỹ sư viết mã script cũng đính kèm các bình luận chi tiết trong mã nguồn của anh ta, giúp tôi tìm ra được vị trí mà những kỹ sư phát triển phần mềm lưu trữ các sản phẩm trình biên dịch chip Motorola cho rất nhiều nền tảng hệ điều hành khác nhau.

Nhân tiện đó, tôi cũng phát hiện ra rằng Intermetrics đang sản xuất trình biên dịch này dưới dạng các phiên bản khác nhau cho các nền tảng OS khác nhau, bao gồm Apollo, SunOS, VMS và Unix. Vậy nhưng tôi không thể tìm thấy gì trên máy chủ nơi các phiên bản này lẽ ra phải được lưu giữ. Tôi dành hàng giờ tìm kiếm các máy chủ và máy tính làm việc của các kỹ sư phát triển khác nhưng vẫn không sao tìm ra trình biên soạn nào – không mã nguồn, không mã máy[91]. Thật kỳ lạ!

[91] Mã máy (machine code): Loại mã được dùng để viết các chỉ dẫn mà máy tính có thể đọc hiểu và thực thi. Một trong các hệ số dùng để viết mã máy là

https://thuviensach.vn

hệ nhị phân chỉ gồm số 0 và 1. (ND)

Tôi kiểm tra tệp tin "aliases", liệt kê các địa chỉ chuyển tiếp của e-mail gửi tới các cá nhân hay nhóm làm việc. Nhờ tra cứu tệp tin này, tôi có thể xác định được các nhân viên đã liên hệ với phòng ban nào và tìm được tên của một nhân viên công ty ở Washington là David Burton.

Đã đến lúc thực hiện một chút tấn công bằng kỹ thuật xã hội. Tôi gọi cho Marty Stolz, tự giới thiệu bằng tên của David và nói: "Tôi có buổi giới thiệu quan trọng trước khách hàng vào sáng mai nhưng không thể tìm ra trình biên dịch cho 68HC11 trên máy chủ chứa sản phẩm lưu hành. Tôi đã có một phiên bản cũ nhưng giờ tôi cần phiên bản mới nhất."

Anh ta hỏi tôi vài câu hỏi – tôi thuộc phòng ban nào, địa chỉ, tên của quản lý, v.v…. Sau đó, anh ta nói: "Nghe này, tôi sẽ cho anh biết điều này nhưng anh phải giữ bí mật nhé." Anh ta chuẩn bị nói cái gì thế?

"Tôi không nói cho ai đâu."

Anh ta thì thầm: "FBI đã gọi cho chúng ta và nói rằng có một gã có lẽ đang muốn tấn công chúng ta – một siêu hacker từng đột nhập vào Motorola và ăn cắp mã nguồn của họ. FBI cho rằng gã sẽ cần trình biên dịch cho mã nguồn của Motorola và sẽ nhắm tới chúng ta!"

Vậy là đặc vụ liên bang đã tính được rằng tôi cần trình biên dịch và đã gọi cho Intermetrics để chặn đầu tôi? Ôi, tôi phải đánh giá cao họ đấy, tính toán tốt lắm.

"Hắn đã tấn công CIA và đột nhập ở mức độ ba," Marty nói với tôi. "Không ai có thể chặn được gã! Gã luôn đi trước FBI một bước."

"Không thể tin được – anh đang đùa tôi đấy à! Nghe như kiểu thằng nhóc trong phim WarGames ấy nhỉ!"

https://thuviensach.vn

“Nghe này, FBI nói rằng tốt nhất là chúng ta nên để mấy trình biên dịch đó trên mạng, nếu không gã ta chắc chắn sẽ mò ra chúng.”

Tôi máy mắt. Sau khi lấy được mã nguồn của Motorola, tôi đã mất tới vài ngày để nghĩ ra ý tưởng đó. Vậy mà FBI còn nghĩ ra trước cả tôi? Thực sự là không thể tin được.

“Xời, tôi cần duyệt buổi chạy thử tối nay để sẵn sàng giới thiệu cho khách hàng vào sáng mai. Giờ tôi phải làm thế nào đây? Có cách nào để lấy được bản sao không?”

Marty nghĩ một lúc. “Ừm… để tôi xem nào,” anh ta nói. “Tôi sẽ để trình biên dịch trong máy làm việc của tôi đủ lâu để anh lấy được nó nhé.”

“Tuyệt! Ngay khi nó lên hệ thống, tôi sẽ chuyển qua ổ di động luôn để khỏi giữ trong máy của tôi. Sau đó, tôi sẽ gọi lại cho anh khi đã xong,” tôi nói. “À này, Marty?”

“Ừ?”

“Tôi hứa tôi sẽ giữ bí mật.”

Marty cho tôi tên máy chủ của anh ta để tôi chuyển tập tin bằng FTP. Thật ngạc nhiên là anh ta còn bật chế độ cho phép truy cập từ tài khoản vô danh, do đó, tôi không cần phải có tài khoản để lấy được tập tin.

Dễ như cướp kẹo của con nít vậy.

Theo những gì tôi biết thì Marty chưa từng biết rằng anh ta đã bị lừa và sẽ chỉ phát hiện ra điều đó nếu đọc được cuốn sách này.

* * *

Vẫn còn phấn khích vì lấy được trình biên dịch thành công, tôi ngủ dậy và phát hiện ra điện thoại đã chết. Tôi đã làm một việc thực sự ngu ngốc uy

https://thuviensach.vn

hiếp đến sự tự do của chính mình.

Không dám mạo hiểm thực hiện một cuộc gọi công việc gắn với danh tính mới từ điện thoại nhái số, tôi mặc quần áo và tới trạm điện thoại công cộng gần nhất để gọi tới công ty điện thoại Southern Bell và hỏi xem tại sao điện thoại của tôi không hoạt động. Sau khi bắt tôi chờ đợi rất lâu, giám sát viên cầm máy và bắt đầu đặt ra rất nhiều câu hỏi. Sau đó, bà ta nói với tôi: “Một Michael Stanfill đã gọi cho chúng tôi từ Portland và nói rằng anh đang dùng danh tính của anh ta.”

“Anh ta hẳn đã nhầm lẫn rồi,” tôi nói. “Ngày mai tôi sẽ gửi fax cho bà bản sao bằng lái xe của tôi để chứng minh thân phận của mình.”

Đột nhiên tôi nhận ra có điều gì đó đã xảy ra. Công ty Điện ở Raleigh, công ty Điện và Ánh sáng Carolina yêu cầu phải có một khoản tiền cọc lớn. Nếu nhận được đảm bảo từ công ty dịch vụ cũ, bạn sẽ không cần phải trả những khoản này. Do đó, tôi gọi tới công ty điện mà Michael Standfill sử dụng dịch vụ ở Oregon – Portland General Electric – và đề nghị cung cấp một thư giới thiệu gửi qua fax. Tôi nói với người phụ nữ ở đầu dây bên kia rằng tôi vẫn muốn duy trì tài khoản của mình ở Oregon nhưng đang mua bất động sản ở Raleigh. Khi gửi thư giới thiệu, hẳn là họ đã gửi cả một bản cho Standfill thực sự. Tôi cảm thấy mình đúng là một thằng ngu: Chỉ vì tiết kiệm 400 đô-la tiền đặt cọc mà tôi đã phá hủy danh tính mới của mình.

Tôi phải chuyển đi ngay lập tức.

Tôi phải có một danh tính mới ngay lập tức.

Tôi phải cuốn gói khỏi căn hộ này ngay lập tức!

Tôi còn chưa có cơ hội tham dự một trong những bữa tiệc cư dân kia hay gặp gỡ cô nàng dễ thương nào đó.

https://thuviensach.vn

Tìm được việc đương nhiên là một trong những ưu tiên hàng đầu của tôi. Tôi đã gửi sơ yếu lý lịch và hồ sơ xin việc dưới danh nghĩa Michael Standfill tới hơn 20 chỗ khác nhau – hầu hết là các nhà tuyển dụng tiềm năng trong khu vực này. Giờ thì với chiếc điện thoại bị ngắt kết nối, không một nhà tuyển dụng nào có thể liên lạc được với tôi! Tệ hơn cả là sẽ rất rủi ro nếu gửi thư tới những nơi đó dưới một cái tên khác. Điều này đặt tôi vào một tình thế cực kỳ bất lợi.

Tôi đã ký hợp đồng thuê nhà sáu tháng, vì vậy, tôi nói với người phụ nữ có khuôn mặt tròn ở văn phòng: “Tôi rất thích nơi này nhưng giờ tôi đang có chuyện gấp liên quan đến sức khỏe của người thân nên phải rời đi ngay.”

Chị ta nói: “Nếu đó là chuyện khẩn cấp thì công ty sẽ để anh cắt hợp đồng. Nhưng họ sẽ không bồi hoàn cho anh tiền thuê tháng này đâu.” Tôi thực muốn trả lời chị ta rằng: “Hãy quên khoản bồi hoàn đó đi, chị cứ coi đó là phần bù đắp để nếu đặc vụ liên bang có tới đây hỏi gì thì nhớ nói là tôi chưa từng ở đây.”

Ngay hôm sau, tôi dọn đến nhà trọ Friendship Inn để sống tạm trong khi tìm một căn hộ mới. Dù chẳng có mấy tài sản, thế nhưng tôi cũng mất tới vài chuyến đi đầy căng thẳng trong chiếc xe đi thuê nhỏ bé để chuyển mọi thứ tới hầm trú ẩn tạm thời mới. Áp lực phải tìm được công việc mới và tạo ra danh tính mới đè nặng lên tôi.

Tôi đã không nhận ra mình còn có những việc lớn hơn cần phải lo lắng. Tôi đã không tưởng tượng ra được tấm lưới vây bắt bắt đầu chụp xuống người tôi ra sao.

Sau khi ổn định tại Friendship Inn, tôi chọn một cái tên tạm thời khác từ hồ sơ của Đại học bang Portland, Glenn Thomas Case. Do người này cũng như Standfill, là một người đang còn sống và sẽ có chút mạo hiểm khi mượn thân phận của anh ta, nên tôi quyết định đổi sang tên “G. Thomas Case” để khác đi một chút.

https://thuviensach.vn

Ba ngày sau, giấy khai sinh có chứng nhận mà tôi yêu cầu đã được gửi tới hòm thư tôi mới thuê. Tôi tới DMV và lại bước ra với giấy phép lái xe mới ở Bắc Carolina trên tay. Nhưng vẫn còn rất nhiều việc phải làm để lấy được các giấy tờ chứng minh thân phận khác mà tôi cần có.

Ngay sau hôm lấy được bằng lái xe lý thuyết, tôi tìm được một căn hộ nhỏ trong khu tổ hợp Players Club, khá phù hợp nhưng không thể sánh được về độ hấp dẫn như nơi ở trước đó. Căn hộ này tuy nhỏ nhưng ấm áp; và tôi cũng chẳng có quyền khảnh chọn. Giá thuê là 510 đô-la một tháng, đồng nghĩa với việc tôi chỉ có thể chi trả sáu tháng tiền nhà trước khi hết sạch tiền. Tôi không gặp nhiều khó khăn khi tìm việc cho lắm, vì vậy đây là một rủi ro chấp nhận được.

Cùng lúc đó, nhiều tờ báo đang đăng tải các câu chuyện mới về hacker Kevin Poulsen. Cậu ta đã bị chuyển từ phòng giam ở Bắc California tới một nơi quá quen thuộc đối với tôi: Trung tâm Giam giữ Đô thị (MDC) ở Los Angeles. Poulsen bị buộc tội hacking bất hợp pháp và thu thập thông tin quốc phòng, một hành vi phạm pháp có liên quan tới hoạt động tình báo.

Tôi quyết định nói chuyện với cậu ta – khát vọng gắn liền với thiên hướng trọn đời của tôi trong việc mưu đồ những điều bất khả thi. Tôi không yêu thích điều gì hơn việc đặt ra thử thách cho bản thân, làm những việc mà chính tôi cũng cho là không thể và chờ xem tôi có thể thực hiện được nó hay không.

Việc tới thăm Poulsen hiển nhiên là không cần phải bàn. Với tôi, Trung tâm Giam giữ Đô thị hệt như Khách sạn California trong bài hát ngày xưa của Eagles: Tôi có thể làm thủ tục ra khỏi đó bất kỳ lúc nào muốn, nhưng tôi sẽ không bao giờ rời đi được.

Các cuộc nói chuyện với Poulsen sẽ phải thực hiện qua điện thoại. Nhưng tù nhân không thể nhận cuộc gọi, chưa kể các cuộc gọi trong tù đều bị giám sát

https://thuviensach.vn

hoặc ghi âm. Với những cáo buộc mà Poulsen đang phải đối mặt, cai ngục hẳn phải liệt cậu ta vào dạng cực kỳ nguy hiểm và liên tục giám sát cẩn mật.

Dù vậy, tôi vẫn tự nhủ, sẽ luôn có cách nào đó.

Mỗi khu giam giữ ở MDC có một "điện thoại cho Luật sư Công". Đây là chiếc điện thoại được cài đặt dịch vụ mà các công ty điện thoại thường gọi là dịch vụ "kết nối trực tiếp": Khi một tù nhân cầm ống nghe lên, anh ta sẽ được kết nối trực tiếp tới Văn phòng Luật sư Công Liên bang. Tôi biết đây là chiếc điện thoại duy nhất tù nhân có thể sử dụng mà không bị giám sát – nhờ đặc quyền của mối quan hệ luật sư bào chữa-khách hàng. Nhưng chúng cũng được lập trình tại các bộ chuyển mạch của công ty điện thoại để không thể nhận được cuộc gọi đến (theo ngôn ngữ điện tử viễn thông thì đó là "tự động từ chối cuộc gọi") và không thể kết nối với bất kỳ số điện thoại nào khác ngoài số chính của Văn phòng Luật sư Công. Dù sao thì cứ đến đâu hay đến đó đã.

Đầu tiên, tôi cần lấy được các số điện thoại này đã. Chỉ mất khoảng 20 phút để tiến hành tấn công bằng kỹ thuật xã hội với Pacific Bell và lấy được 10 số dịch vụ kết nối trực tiếp trong trại giam.

Sau đó, tôi gọi cho RCMAC. Tôi nói mình gọi từ văn phòng hành chính của Pacific Bell và yêu cầu hủy bỏ ngay lập tức dịch vụ tự động từ chối cuộc gọi cho 10 số kia. Nhân viên của RCMAC vui vẻ chấp thuận.

Kế tiếp, hít một hơi dài, tôi gọi tới Phòng Tiếp nhận và Phóng thích của chính trại giam đó.

"Tôi là Taylor, Quản lý Đơn vị buồng giam ở Terminal Island," tôi nói, cố diễn lại chất giọng uể oải buồn chán của một gã cai ngục. Mượn tên hệ thống máy tính chính của Cục Đặc trách Nhà tù Liên bang cùng với mã số đăng ký phạm nhân của Poulsen, tôi tiếp tục. "Sentry không hoạt động được ở đây. Anh có thể tìm phạm nhân mã 95596-012 giúp tôi không?"

https://thuviensach.vn

Khi gã ở trại giam dò số của Poulsen, tôi hỏi thăm xem cậu ta bị giam ở khu nào. “Khu Sáu phía Nam,” anh ta đáp.

Phạm vi được thu hẹp lại một chút, nhưng tôi vẫn chưa biết số điện thoại nào trong 10 số kia được đặt tại khu buồng giam khu Sáu phía Nam.

Trên máy chạy băng micro cát-sét của mình, tôi ghi âm khoảng một phút loại chuông reo mà bạn vẫn thường nghe thấy trên điện thoại khi gọi ai đó. Việc này chỉ có tác dụng nếu một phạm nhân nhấc máy để gọi cho luật sư công của mình trong khoảng thời gian hai đến ba phút tôi gọi vào máy điện thoại đó. Tôi đã phải thử rất, rất nhiều lần cho đến khi có người nhấc máy. Và đây lại là một trong những thời điểm mà lòng kiên nhẫn cùng sự quyết tâm bền bỉ có vai trò rất quan trọng.

Khi tôi gọi đúng thời điểm và một tù nhân nhấc máy, tôi để anh ta nghe vài tiếng chuông reo trên băng cát-sét rồi dừng băng lại và nói: “Văn phòng Luật sư Công xin nghe, tôi có thể giúp được gì cho anh?”

Khi người tù kia đề nghị gặp luật sư của anh ta, tôi sẽ đáp: “Để tôi xem anh ấy có ở đây hay không,” sau đó giả vờ bỏ đi chừng một phút. Quay trở lại đường dây, tôi nói với anh ta rằng luật sư của anh ta hiện không có mặt tại văn phòng và hỏi tên anh ta. Sau đó, tôi hỏi đầy hờ hững như thể chỉ đang lấy những thông tin liên quan: “Anh ở khu buồng giam nào nhỉ?”

Sau đó, tôi sẽ nói: “Anh hãy thử gọi lại sau một đến hai giờ nữa nhé,” để không ai có thể nhận ra rằng rất nhiều luật sư công có vẻ như chẳng hề nhận được các tin nhắn gửi tới họ. Mỗi lần một tù nhân trả lời điện thoại, tôi lại xác định được số điện của khu buồng giam và loại bỏ nó ra khỏi danh sách. Chép lại tất cả chi tiết vào sổ tay, tôi chậm rãi dựng lên sơ đồ kết nối của số điện thoại với khu buồng giam. Cuối cùng, sau vài ngày quay số, tôi đã kết nối được với một tù nhân ở khu Sáu phía Nam.

Tôi vẫn còn nhớ số máy lẻ nội bộ của khu Sáu phía Nam từ hồi bị giữ trong khu biệt giam ở MDC. Một trong những điều tôi vẫn làm trong khoảng thời

https://thuviensach.vn

gian đó để giữ cho đầu óc được hoạt động và duy trì sự tỉnh táo của bản thân là lắng nghe mọi thông báo trên hệ thống phát thanh của nhà tù và ghi nhớ tất cả các số máy lẻ nghe được. Nếu một thông báo có nội dung: "C.O. Douglas, gọi Quản lý Đơn vị Chapman số 427", tôi sẽ lưu vào trí nhớ của mình cái tên kèm con số này. Như đã nhắc tới, tôi rất giỏi nhớ các số điện thoại. Thậm chí cho đến giờ, sau rất nhiều năm, tôi vẫn nhớ kha khá số điện thoại trong trại giam đó cũng như hàng chục, thậm chí hàng trăm số điện thoại của bạn bè, văn phòng công ty điện thoại, cũng như các số điện thoại khác mà tôi có lẽ sẽ không bao giờ dùng đến nữa nhưng chúng vẫn in hằn trong trí nhớ của tôi.

Điều kế tiếp tôi cần làm có vẻ bất khả thi. Tôi cần phải tìm cách gọi tới chính trại giam đó và sắp xếp một cuộc hẹn điện thoại không bị giám sát với Kevin Poulsen.

Tôi gọi vào số chính của trại giam, giới thiệu mình là "một quản lý đơn vị ở TI" (Nhà tù Liên bang Terminal Island) và hỏi số máy lẻ 366, số máy dành cho khu giam giữ số Sáu phía Nam.

Nhân viên trực tổng đài nối máy cho tôi.

Một cai ngục trả lời: "Khu số Sáu phía Nam xin nghe, đây là Agee."

Tôi biết gã này từ khi còn ở trong tù, gã là người đã luôn tìm cách khiến đời tôi khốn khổ. Nhưng tôi phải kìm nén cơn giận. Tôi nói: "Tôi là Marcus ở Phòng Tiếp nhận và Phóng thích. "Tù nhân Poulsen ở chỗ anh đúng không?"

"Đúng."

"Chúng tôi muốn bỏ đi vài tài sản cá nhân của anh ta ở đây. Tôi cần biết anh ta muốn gửi trả thứ gì về nhà."

"Poulsen!" tên cai ngục gào lên to hơn mức cần thiết.

https://thuviensach.vn

Khi Kevin nhấc máy, tôi nói: “Kevin, hãy giả bộ như thể cậu đang nói chuyện với ai đó ở Phòng Tiếp nhận và Phóng thích.”

“Ừ,” cậu ta nói giọng hoàn toàn vô cảm.

“Tôi là Kevin đây,” tôi nói. Chúng tôi chưa từng gặp nhau, nhưng tôi đã được nghe về danh tiếng của cậu ta và đoán rằng cậu ta hẳn cũng biết về tôi. Và tôi cũng đoán cậu ta biết rằng sẽ chẳng còn Kevin nào khác gọi cho cậu ta trong tù!

Tôi nói: “Ở máy điện thoại nối tới Phòng Luật sư Công vào đúng 1 giờ. Hãy nhấc máy lên và cứ 15 giây lại nháy móc chuyển đổi một lần cho tới khi tôi kết nối.” (Vì tất cả chuông gọi đến đã bị tắt đi, cậu ta sẽ không biết chính xác tôi sẽ gọi đến vào lúc nào.) “Giờ thì đọc cho tôi địa chỉ nhà cậu để tên Agee nghe được. Tôi đã nói với hắn rằng tôi sẽ gửi đồ của cậu về nhà.” Sau tất cả những gì Agee đã gây ra cho tôi, thật tuyệt khi lừa được hắn gọi Poulsen tới nghe điện.

Đúng 1 giờ, tôi gọi tới điện thoại kết nối tới Phòng Luật sư Công ở khu số Sáu phía Nam. Vì Poulsen không nói gì nhiều trong cuộc gọi đầu tiên và tôi cũng không quen thuộc lắm với giọng của cậu ta, nên tôi muốn đảm bảo mình đang nói chuyện với cậu ta, do đó tôi làm phép thử. “Cú pháp tăng giá trị biến trong C là gì?”

Cậu ta dễ dàng đưa ra câu trả lời chính xác và rồi chúng tôi ung dung nói chuyện, không hề lo lắng gì về việc đặc vụ liên bang có thể sẽ nghe được cuộc đàm thoại này. Tôi lấy làm thích thú khi nghĩ tới việc vừa lẩn tránh họ vừa đột nhập vào trại giam để nói chuyện với một tù nhân bị buộc tội gián điệp.

* * *

Vào ngày 27 tháng 1, may mắn đã đưa tới sợi dây thừng đầu tiên dệt nên tấm lưới giúp Shimmy và đội của hắn ta tóm được tôi. The Well có một

https://thuviensach.vn

chương trình tự động tên là “disk hog” có thể gửi e-mail định kỳ tới các khách hàng đang sử dụng rất nhiều dung lượng ổ cứng. Một trong những e-mail này đã được gửi tới Bruce Koball, người chịu trách nhiệm tổ chức một sự kiện chính sách công thường niên có tên là Hội thảo về Máy tính, Tự do và Bảo mật (CFP).

Nội dung trong e-mail lưu ý rằng tài khoản của hội nghị này đang chiếm tới hơn 150 megabyte trên máy chủ của the Well. Koball kiểm tra tài khoản và phát hiện ra không có tập tin nào thuộc về CFP. Xem kỹ các tệp tin có chứa e-mail, hắn thấy rằng tất cả đều được gửi tới tsutomu@sdsc.com.

Đêm đó, Koball đọc tờ New York Times và bắt gặp câu chuyện trên trang nhất của John Markoff ở mục Kinh doanh với tựa đề “Taking a Computer Crime to Heart” (tạm dịch: Chuyện nghiêm túc về một tội ác máy tính). Trong đó có đoạn:

Như thể cánh trộm cướp bẻ khóa của người thợ khóa để chứng tỏ năng lực của mình. Đây cũng là lý do tại sao Tsutomu Shimomura, người giữ khóa trong trường hợp này, đã coi vụ đột nhập như một điều sỉ nhục mang tính cá nhân – và đó là lý do tại sao anh ta coi chuyện giải quyết tội ác này là vấn đề danh dự.

Ông Shimomura, một trong những chuyên gia bảo mật máy tính giỏi nhất nước Mỹ, là người đã thúc đẩy Cơ quan Máy tính Chính phủ đưa ra lời cảnh báo đanh thép vào thứ Hai. Cơ quan này cảnh báo, một kẻ đột nhập không rõ tên đã sử dụng kỹ thuật đột nhập tinh vi để đánh cắp các tập tin dữ liệu từ máy tính cá nhân được bảo mật kỹ càng đặt tại nhà riêng của ông Shimomura gần San Diego.

Ngày hôm sau, Koball gọi cho Markoff và được kết nối tới Shimmy. Không cần mất quá nhiều thời gian để khẳng định hầu hết các tập tin bí ẩn lưu trữ trên tài khoản CFP đều đến từ cuộc tấn công hôm Giáng sinh nhằm vào máy

https://thuviensach.vn

tính của Shimmy. Đây là đầu mối đầu tiên. Giờ thì hắn ta đã có dấu vết để lần theo.

Cũng trong khoảng thời gian này, anh họ[92] của tôi, Mark Mitnick, một người mà tôi khá gần gũi, dự định đi nghỉ cùng bác tôi tại Hilton Head, Bắc Carolina. Anh ấy cũng rủ tôi cùng tham gia.

[92] Hoặc có thể là em họ, đại từ nhân xưng trong tiếng Anh không chỉ rõ mối quan hệ này. (ND)

Mark hiện đang điều hành một công ty ở Sacramento có tên là Ad Works và đề nghị sẽ giúp tôi thành lập một công ty ở bờ Đông với mô hình kinh doanh tương tự. Anh ấy cung cấp các cuộn giấy in hóa đơn miễn phí ở những siêu thị lớn với quảng cáo được in ở mặt sau. Mark kiếm tiền nhờ tìm ra các công ty đồng ý chi tiền để in quảng cáo đằng sau cuộn giấy in đó. Tôi cần một khoản thu nhập ổn định và ý tưởng về việc được người anh họ giúp đỡ để khởi nghiệp nghe có vẻ rất hấp dẫn, dù nó chẳng liên quan gì đến máy tính.

Chúng tôi gặp nhau ở Raleigh và lái xe qua vài thành phố trên đường tới Hilton Head để Mark có thể thực hiện vài phi vụ bán hàng. Anh mời tôi đi cùng để chỉ cho tôi về công việc. Tôi thích ý tưởng dịch chuyển bởi điều đó khiến tôi khó bị tìm ra hơn.

Lẽ ra tôi đã được tận hưởng chuyến đi nhiều hơn nếu không bắt gặp một bài báo xuất hiện khi đang tiến hành kiểm tra trên mạng như thường lệ xem có dấu hiệu gì về việc đặc vụ liên bang đã tới gần mình không. Các câu chuyện trên khắp các phương tiện truyền thông về một buổi họp báo của Bộ Tư pháp. Tựa đề của một trong những câu chuyện đó là: “Mỹ đang săn lùng một tội phạm máy tính chuyên nghiệp.” Trong đó có viết:

WASHINGTON, D.C., Mỹ., ngày 26 tháng 1 năm 1995 (NB) – Sở Cảnh sát Tư pháp đang theo dấu một hacker máy tính đã biến mất sau khi bị kết án phạm tội điện tử cùng một số tội danh khác. Các nhà chức trách nói rằng họ đang cố gắng tìm ra nơi ẩu náu của Kevin David Mitnick, 31 tuổi, tới từ

https://thuviensach.vn

Sepulveda, California. Đại diện Sở Cảnh sát Tư pháp, Kathleen Cunningham, cho Newsbytes biết rằng Sở đã có lệnh bắt giữ Mitnick vì đã vi phạm điều kiện quản chế từ tháng 11 năm 1992 và đã suýt bắt được hắn ta tại Seattle vào tháng 10 năm ngoái. Cunningham cho biết Mitnick là một gã cuồng ham radio, người ta tin rằng hắn đã sử dụng máy quét sóng để theo dõi cảnh sát trong khu vực hắn ẩn náu. "[Cảnh sát địa phương] đã không sử dụng chế độ bảo mật radio, do đó, hắn đã biến mất ngay khi cảnh sát nhắc tới địa chỉ của hắn. Hắn bỏ lại mọi thứ." Minick được coi là chuyên gia trong việc chiếm quyền kiểm soát máy tính nhằm theo dõi và sử dụng các hệ thống giao tiếp cũng như hiểu rõ cách thức tạo ra các danh tính giả thông qua máy tính.

Tôi như thể bị hàng tấn gạch đè lên người. Tôi ngạc nhiên, kinh hoàng và gần như hoảng loạn. Các đặc vụ liên bang và cánh truyền thông đã biến việc vi phạm điều kiện quản chế thành một cuộc truy lùng trên toàn cầu. Tôi không thể rời đất nước nếu muốn – tôi ngờ rằng đặc vụ liên bang hắn đã yêu cầu Interpol đưa ra "Thông báo đỏ" nhằm khởi động một cuộc tìm kiếm trên toàn thế giới đối với tôi. Và tấm hộ chiếu duy nhất mà tôi đã giấu đi, không còn được sử dụng, lại có tên Mitnick.

Khi Mark và bác tôi từ sân golf quay về khách sạn, tôi cho họ xem bài báo. Cả hai đều choáng váng. Tôi hơi lo lắng vì đã cho họ thấy bài báo này, sợ rằng họ sẽ bảo tôi biến đi vì sự có mặt của tôi sẽ đem lại nguy hiểm cho họ. Thật may mắn, họ chưa từng nhắc tới chủ đề này, nhưng cơn hoang tưởng của tôi đã tăng thêm vài bậc. Tất cả đều đang lùng sục tôi. Liệu đặc vụ liên bang có nghi ngờ tôi là kẻ duy nhất tấn công vào máy tính của Shimmy không?

Vào ngày 29 tháng 1, ngày Chủ nhật diễn ra Siêu Cúp Super Bowl, sẽ có trận đấu giữa hai đội San Francisco 49ers và San Diego Chargers. Mark và bác tôi rất hào hứng với trận bóng nhưng tôi thì chẳng màng tới nó. Có rất nhiều thứ quay mòng mòng trong đầu và tôi chỉ muốn được nghỉ ngơi. Thay

https://thuviensach.vn

vì quay lại phòng để lên mạng, tôi quyết định đi bộ trên bãi biển để hít thở chút không khí trong lành.

Tôi quyết định gọi cho Jon Littman. “Tôi đang đi bộ ngoài biển và thư giãn,” tôi nói với anh ta.

“Ngoài biển á? Có thực là cậu đang ở ngoài biển không?”

“Ừ, tôi không làm phiền anh thêm nữa. Chắc là anh đang chuẩn bị xem bóng.”

Littman nói với tôi rằng trận đấu vẫn chưa bắt đầu. Anh ta hỏi: “Sóng trông như thế nào?”

Tại sao anh ta lại hỏi tôi một câu hỏi ngớ ngẩn như vậy? Tôi không định nói về tình trạng lướt sóng và để lộ cho anh ta đầu mối về vị trí hiện tại của mình.

Tôi nói: “Tôi không thể nói được, nhưng anh có thể nghe được chúng đấy,” sau đó giơ điện thoại lên cao.

Tôi hỏi xem anh ta có nghe ngóng được gì về buổi họp báo UPI của Sở Cảnh sát Tư pháp đề nghị công chúng hỗ trợ truy tìm tôi không. Tôi phàn nàn rằng có rất nhiều thứ nhảm nhí trong các bài báo, bao gồm cả cái huyền thoại cũ nát của Markoff rằng tôi đã hack vào NORAD.

Littman hỏi tôi đã đọc câu chuyện hôm qua của Markoff chưa. Khi tôi nói chưa đọc, anh ta đọc cho tôi nghe qua điện thoại. Tôi đoán anh ta muốn biết phản ứng của tôi. Tôi phát hiện ra yêu cầu hỗ trợ của Sở Cảnh sát Tư pháp đã được công bố ngay sau khi Markoff tung ra câu chuyện về vụ tấn công Shimmy vào lễ Giáng sinh. Tôi không cho đó là một sự ngẫu nhiên. “Tôi có cảm giác đây là một phần trong chiến thuật nhằm kích động nỗi sợ hãi của công chúng về không gian mạng để nhắm vào tôi,” tôi nói với anh ta.

https://thuviensach.vn

“Markoff đã hỏi về cậu,” Littman nói. “Và hắn nghĩ hắn biết cậu đang trốn ở đâu.” Tôi hối thúc anh ta nói rõ thêm nhưng không thu được kết quả gì. Tôi đổi chiến thuật và đề nghị anh ta đoán xem tôi đang sống ở đâu.

“Cậu đang sống đâu đó ở Trung Tây phải không?”

Thật mừng, anh ta đã đoán còn mướt mới tới. Nhưng có vẻ như Markoff có một số thông tin quan trọng có liên quan tới tôi và tôi cần nghĩ cách áng xem hắn đã biết tới chừng nào.

Vài ngày sau, tôi nhận ra nếu đặc vụ liên bang đang ráo riết truy tìm tôi, họ hẳn phải theo dõi điện thoại của bà tôi ở Las Vegas. Đó là điều mà tôi sẽ làm.

Bộ phận Phân bổ Đường dây của Centel có thông tin của mọi nhánh điện thoại ở Las Vegas. Tôi biết số điện thoại đó rất rõ. Giả danh là một kỹ sư hiện trường, tôi đề nghị một trong những nhân viên ở đây mở thông tin về số điện thoại của bà trên máy tính. Tôi nhờ cô ta đọc cho tôi “thông tin cáp”, và đúng như tôi nghi ngờ, có một “thiết bị đặc biệt” đã được gắn vào đường dây của bà gần đây.

Cô ta nói yêu cầu này được đưa ra vài ngày trước bởi một nhân viên bảo mật của Centel tên Sal Luca. Tôi cảm thấy có thể đảo ngược tình huống đối với Luca nếu mình giám sát đường dây của anh ta, nhưng điều đó cũng chẳng đem lại thông tin giá trị gì cho tôi. Ý định tiếp theo của tôi là mớm cho cánh theo đuôi vài thông tin sai lệch nhờ gọi điện cho bà và nói huyên thuyên rằng tôi đang ở Great White North. Nhưng tôi không muốn gây thêm sức ép cho bà ngoài những gì bà đang phải chịu.

Trong lúc nghĩ tới hướng đi kế tiếp, tôi vẫn phải tiếp tục tạo ra thân phận mới. Vào ngày 2 tháng 2, tôi có hẹn thi lái xe để nâng cấp bằng lý thuyết thành bằng lái xe dưới cái tên G. Thomas Case. Để làm vậy, tôi cần phải tìm được một chiếc xe không có bất kỳ liên quan nào tới những cái tên cũ.

https://thuviensach.vn

Tôi chặn một chiếc taxi. “Này, anh có muốn kiếm 100 đô-la ngon ăn không?” tôi hỏi tài xế. Anh ta đáp lại bằng nụ cười nhăn nhở để lộ ra một chiếc răng móm và trả lời bằng câu gì đó nghe như “Tic, ticku”, tiếp theo là: “Đương nhiên, được rồi.” Những từ nước ngoài kia hóa ra là tiếng Hindi có cùng ý như vậy. (Chết tiệt, lẽ ra tôi nên đề nghị 50 đô-la thôi!) Chúng tôi thống nhất là anh ta sẽ đến đón tôi vào hôm sau và anh ta cho tôi số máy nhắn tin.

Ngày hôm sau ở DMV, khi tay coi thi nhận ra tôi sẽ thực hiện bài thi bằng một chiếc taxi, anh ta nhìn tôi đầy nghi ngờ. Chúng tôi vào xe, tôi tắt công tơ đo quãng đường và nói với anh ta: “Tôi sẽ phải thu tiền xe của anh đó.” Phản ứng trên mặt anh ta quả là vô giá. Khi anh ta thấy tôi cười, anh ta cũng cười lớn và chúng tôi có một khởi đầu thuận lợi.

https://thuviensach.vn

35

TRÒ CHƠI KẾT THÚC

2B 2T W 2X 2Z 36 36 2P 36 2V 3C W 3A 32 39 38 2Z W 3D 33 31 38 2V 36 3D W 2R 2Z 3C 2Z W 3E 3C 2V 2X 2Z 2Y W 3E 39 W 2R 32 2V 3E W 2V 3A 2V 3C 3E 37 2Z 38 3E W 2X 39 37 3A 36 2Z 2S 1R

Đến thứ Ba, ngày 7 tháng 2, một đội cảnh sát có vũ trang được thành lập để bắt tôi. Trợ lý công tố Kent Walker giờ đã tham gia vào vụ án, gặp gỡ Shimmy cùng bạn gái gã là Julia Menapace và tay trợ lý Andrew Gross, hai đặc vụ FBI và Phó Chủ tịch cùng quản trị viên hệ thống của the Well cùng luật sư của họ, John Mendez, người có tiếng nói trong phòng bởi trước đây anh ta từng ở Văn phòng Công tố và từng là sếp của Walker.

Walker vốn ở Bắc California và chẳng liên quan gì đến vụ của tôi. Theo hồ sơ, hắn sẵn sàng bẻ luật và đi quá một số giới hạn để trao cho Shimmy một vai trò khác thường trong suốt những ngày sắp tới. Điều này cũng giống như đội súng miền Tây hoang dã xa xưa, nơi Cảnh sát trưởng cử ra dân thường để hỗ trợ ông ta đi săn lùng một tên tội phạm bị truy nã.

Rõ ràng, Walker đã bí mật thỏa hiệp về việc cung cấp cho Shimmy những thông tin tóm-và-lần tuyệt mật, cũng như những thông tin tuyệt mật từ hồ sơ của FBI về tôi. Shimmy có thể nghe lén những liên lạc của tôi mà không cần lệnh từ tòa án với lý do gã không phải đang giúp chính phủ mà chỉ đang làm việc cho các nhà cung cấp dịch vụ Internet. (FBI sẽ không bao giờ buộc tội tôi đã hack Shimomura; tôi tin rằng đó là vì họ không thể liều lĩnh làm lộ ra hành động sai trái ghê tởm của mình, vốn có vẻ vi phạm các đạo luật nghe lén liên bang.)

https://thuviensach.vn

Có vẻ Shimmy chính là người chịu trách nhiệm lãnh đạo cuộc điều tra như một nhân viên chính phủ thực thụ. Việc này chưa từng có tiền lệ. Có lẽ Cục hiểu rằng họ sẽ không bao giờ có thể tìm ra tôi nếu không có tinh thần hành hiệp bền bỉ của Shimmy.

Cuộc nói chuyện với Littman tiếp tục quấy nhiễu tâm trí tôi. Sau khi nói chuyện với Markoff, Littman nghĩ anh ta biết tôi đang ở đâu. Đã đến lúc tôi truy cập vào e-mail của Markoff để xem hắn biết những gì.

Việc lần theo dấu vết rất đơn giản: Tất cả e-mail gửi đến địa chỉ "nyt.com" của hắn đều được gửi đi từ Internex, một nhà cung cấp dịch vụ Internet nhỏ ở Bắc California. Sau khi nhòm ngó máy chủ Solaris của Internex vài phút, tôi thở phào nhẹ nhõm. Gã đần quản trị viên hệ thống đã xuất thư mục chính của tất cả mọi người (sử dụng Hệ thống Tập tin Mạng của Sun) và để mở chúng trên Internet, có nghĩa là tôi có thể mount từ xa thư mục chính của bất kỳ người dùng nào – tức là, biến toàn bộ thư mục đó thành nơi có thể truy cập được từ hệ thống nội bộ của tôi. Tôi tải một tập tin .rhosts lên một thư mục người dùng mà tôi đã cấu hình để tin tưởng bất kỳ người dùng nào có kết nối từ máy chủ, và tôi có thể đăng nhập vào tài khoản của họ mà không cần mật khẩu. Một khi đã đăng nhập, tôi có thể khai thác một lỗ hổng khác để lấy quyền root. Tất cả mất khoảng 10 phút. Ước gì tôi có thể gửi đến gã quản trị viên hệ thống kia một lá thư cảm ơn vì đã để hệ thống rộng mở như vậy.

Chỉ bằng vài thao tác dễ dàng, tôi đã có quyền truy cập vào e-mail của Markoff. Thật không may, hắn đã thiết lập phần mềm xóa tin nhắn nhận trong e-mail. Chỉ còn vài tin nhắn sót lại trên máy chủ, nhưng chúng không chứa thông tin gì liên quan đến tôi.

Tôi thêm một thay đổi cấu hình nhỏ để mọi e-mail mới gửi đến cho Markoff cũng sẽ được chuyển tiếp đến một địa chỉ e-mail khác do tôi kiểm soát. Tôi đã hy vọng tìm ra nguồn tin của hắn – những người báo cho hắn nơi họ nghĩ

https://thuviensach.vn

tôi đang ở. Tôi cũng nóng lòng muốn biết hắn đã tham gia vào vụ của tôi đến đâu rồi.

Sau này tôi được biết, trong lúc tôi làm việc này, Shimmy và đội của hắn đã theo dõi tôi. Họ theo dõi thụ động lưu lượng truy cập mạng đến cả the Well và Netcom. Việc này rất dễ thực hiện bởi các nhà cung cấp dịch vụ Internet đã cho đội của hắn toàn quyền truy cập vào mạng lưới của họ.

Sau khi thiết lập giám sát ở Netcom vào khoảng ngày 7 tháng 2, Shimmy yêu cầu một trong những quản trị viên mạng lưới tra cứu trong hệ thống hồ sơ ở Netcom để tìm những người dùng đã đăng nhập trong khoảng thời gian các tài khoản ở the Well bị truy cập trái phép bởi một người dùng nào đó ở Netcom. Quản trị viên này tra cứu trong các hồ sơ ghi chép bằng cách đối chiếu những lần đăng nhập và đăng xuất đã xảy ra trong khoảng thời gian đột nhập và cuối cùng đã tìm ra một trong những tài khoản truy cập the Well từ mạng của Netcom. Tài khoản "gkremen" đã được dùng để kết nối đến Netcom thông qua các modem của công ty ở Denver và Raleigh.

Ngày hôm sau, khi đang tìm trong e-mail của Markoff những thứ có liên quan đến mình, tôi đã cho chạy truy vấn tìm chuỗi "itni" (bởi tìm tên "Mitnick" sẽ là gợi ý chết người). Nhưng Shimmy và đội của hắn khi đó đã theo dõi tôi rồi nên ngay khi nhìn thấy truy vấn này, họ đã xác nhận mối nghi ngờ rằng tôi chính là kẻ đột nhập.

Shimmy liên hệ với Kent Walker và báo cho anh ta biết kẻ đột nhập đến qua các modem dial-up ở Denver và Raleigh. Shimmy nhờ Walker đặt một thiết bị tóm-và-lần vào số dial-up đến Netcom ở Denver mà tôi đang dùng. (Xin nhắc lại, đây là một yêu cầu rất không bình thường của một người dân đối với trợ lý công tố: Thường chỉ có các cơ quan chấp pháp mới có quyền đưa ra các yêu cầu này.)

Walker liên lạc với FBI ở Denver và Denver đã liên hệ với văn phòng FBI ở Los Angeles để được bật đèn xanh. Nhưng văn phòng ở Los Angeles muốn

https://thuviensach.vn

Denver đứng ngoài vụ này. Thay vào đó, chuyện này lại nghe như thể một vụ đấu đá nội bộ tranh giành địa bàn, một đặc vụ ở văn phòng Los Angeles nói với người ở Denver rằng họ sẽ không hỗ trợ lắp đặt thiết bị tóm-và-lần. Tất cả đều muốn tranh giành tôi. Nếu biết tất cả lùm xùm lúc đó, tôi đã có thể tận dụng nó để giành lợi thế cho mình.

Ngay khi "gkremen" đăng nhập vào từ Raleigh, đội của Shimmy đã nhờ một đặc vụ FBI liên hệ với General Telephone, công ty điện thoại cung cấp các số dial-up của Netcom ở Research Triangle Park và yêu cầu cuộc gọi đó được truy dấu trong thời gian thực. Sau vài lần thử, các kỹ thuật viên của General Telephone đã truy dấu thành công. Họ gửi số đến FBI và góp ý rằng nó đến từ mạng di động của Sprint.

Nhưng thông tin này sẽ không dẫn cuộc truy lùng đi đến đâu. Để có thêm một lớp bảo vệ nữa, tôi đã thiết lập từ trước thứ tôi gọi là "số cắt đuôi". Bước đầu của quá trình này là hack vào bộ chuyển mạch của công ty điện thoại, tìm một số điện thoại chưa sử dụng và thêm tính năng chuyển tiếp cuộc gọi vào số máy đó. Sau đó, tôi thiết lập một số hóa đơn khác trong bộ chuyển mạch để mọi cuộc gọi được thực hiện từ số đó trông có vẻ như xuất phát từ số hóa đơn thay vì từ số thực. Tại sao tôi lại làm như vậy? Tôi đã phát hiện ra lỗi trong phần mềm của bộ chuyển mạch: Đôi khi, nó sẽ không báo số điện thoại tạo cuộc gọi mà báo số hóa đơn. Vì vậy, nếu các kỹ thuật viên của công ty điện thoại thử truy dấu một số cuộc gọi của tôi, họ sẽ không thể ngay lập tức phát hiện ra số cắt đuôi của tôi – số tôi đã định tuyến cho cuộc gọi của mình đi qua – mà sẽ nhận được một số điện thoại được gán cho một khách hàng ngẫu nhiên nào đó mà tôi đã chọn. Tôi biết một vài kỹ thuật viên thậm chí còn không biết việc truy dấu có thể trả về số hóa đơn, việc này sẽ giúp tôi có thêm một lớp bảo vệ đặc biệt nữa. Theo kinh nghiệm của tôi,dù có chuyện gì xảy ra, các công ty điện thoại cũng sẽ không bao giờ phát hiện ra việc tôi dùng số cắt đuôi để khiến việc truy dấu cuộc gọi khó khăn hơn, bởi họ chưa bao giờ nghĩ đến chuyện có thể có ai đó đã hack vào bộ chuyển mạch của họ.

https://thuviensach.vn

Trước đó vài tuần, JSZ đã lập một tài khoản cho tôi trên “escape.com” (do anh bạn Ramon Kazan của anh ta sở hữu) để hai chúng tôi có thể liên lạc trực tiếp với nhau qua hệ thống này. Nó đã trở thành một trong rất nhiều điểm truy cập mà tôi dùng để kết nối Internet. Vì có quyền root, nên tôi cũng đã nhét vào đó hàng đống công cụ hack, các lỗi và mã nguồn từ nhiều công ty mà tôi đã hack được gần đây. (Tài khoản của tôi trên escape.com được đặt tên là “marty”, lấy từ nhân vật trong bộ phim Sneakers (tạm dịch: Những kẻ vụng trộm).)

Mỗi khi tôi đăng nhập vào tài khoản của mình ở escape.com, luôn có một thông báo hiển thị ngày giờ đăng nhập gần nhất của tôi. Việc đầu tiên tôi làm mỗi lần đăng nhập là xóa phần cuối danh sách ghi chép này để loại bỏ bất kỳ dấu vết nào về những lần xuất nhập của tôi. Nhưng ở lần đăng nhập này, ngay lập tức tôi phát hiện ra có ai đó đã đăng nhập vào tài khoản của tôi... từ the Well. Ai đó đã ở đây. Chuyện quái gì vậy?

Tôi truy cập vào the Well ngay lập tức và bắt đầu nhòm ngó nhưng không tìm thấy gì dẫn tôi đến chỗ tên điệp viên bí ẩn này.

Tôi ngắt luôn kết nối, cảm thấy như mình đang bị theo dõi.

Trong khi đó, một kỹ sư của Sprint đang cố gắng giải thích số GTE đã truy dấu xuất phát từ mạng của Sprint. Khi tra cứu hồ sơ khách hàng của công ty, anh ta không hề thấy số này, nó rất lạ. Nhưng rồi tay kỹ sư này nhận ra đó không phải là một số điện thoại của Sprint – trên thực tế, nó thậm chí còn không có đầu số của một số điện thoại di động. Shimmy yêu cầu FBI thiết lập một cuộc gọi hội nghị để gã có thể trao đổi chuyện lạ thường này với tay kỹ sư ở Sprint. Sau đó, gã quyết định tự mình gọi đến số này để xem có ai trả lời không. Ngay khi cuộc gọi được kết nối, gã bắt đầu nghe thấy tiếng kerchunk nhỏ dần nhỏ dần cho đến khi cuộc gọi bị ngắt. Chuyện này khiến gã và mấy tay kỹ sư rất tò mò. Có vẻ như tôi đã thiết lập một biện pháp dự phòng để ngăn cản việc truy dấu của họ và họ băn khoăn không biết liệu tôi có động tay vào bộ chuyển mạch hay không.

https://thuviensach.vn

Việc tôi dùng mạng di động Sprint để kết nối đến Netcom thông qua số cắt đuôi khiến số cắt đuôi nhìn như xuất phát từ mạng Sprint trong khi thực tế không phải như vậy. Đó là bởi cả số cắt đuôi và số dial-up của Netcom đều nằm trên cùng một bộ chuyển mạch. Giờ thì tay kỹ sư của Sprint quyết định đổi chiến thuật, anh ta sẽ tiến hành "tìm kiếm số gọi đến". Thay vì tìm kiếm các cuộc gọi xuất phát từ số được truy ra, anh ta sẽ tìm bất kỳ thuê bao nào gọi đến số đó.

Anh ta không mất nhiều thời gian để dò được trúng mạch. Truy vấn qua các hồ sơ chi tiết cuộc gọi chỉ ra rằng số được truy ra đó đã được gọi đến nhiều lần từ một số điện thoại của Sprint – hay nói cách khác, từ số điện thoại tôi đang dùng để kết nối đến Netcom, số điện thoại với mã vùng của Raleigh.

Nhân viên kỹ thuật này phát hiện ra các cuộc gọi này thường được định tuyến qua cùng một cột thu phát sóng. Điều này có nghĩa rằng số điện thoại ở đầu kia rất có khả năng ở một vị trí cố định. Vậy là họ biết tôi đang ở Raleigh.

Ngay khi tay kỹ sư này báo với Shimmy những gì anh ta phát hiện ra, hắn đã đáp luôn máy bay đến Raleigh.

Tôi cố gọi và e-mail cho JSZ ở Israel vài lần để loại trừ khả năng nhỏ rằng gần đây anh ấy đang thử truy cập vào tài khoản "escape.com" của tôi từ the Well. Vào chiều Chủ nhật, trong lúc Shimmy đang trên đường bay tới Releigh, JSZ gửi cho tôi một tin nhắn khiến tôi chưng hửng:

Xin chào,

Sáng nay cha tôi bị trụy tim nặng và đang nằm viện rồi; tôi đã ở bệnh viện cả ngày và chắc sẽ ở đây cả ngày mai nữa; đừng kỳ vọng tôi sẽ dùng máy tính trong 3-4 ngày tới – Hy vọng là cậu hiểu.

Thân,

https://thuviensach.vn

Jonathan

Càng lúc càng lo lắng, tôi đăng nhập ngay vào bộ chuyển mạch của công ty điện thoại cung cấp các số dial-up tới Netcom qua Research Triangle Park – một trong những tuyến tôi đã dùng để truy cập Internet ở Raleigh. Trên thực tế, đó là tuyến ưa thích của tôi bởi các cuộc gọi di động trực tiếp đến Netcom ở Denver và những nơi khác thường cho các phiên dial-up dài có chất lượng không được tốt.

Khi xem xét số dial-up của Netcom trong bộ chuyển mạch, tôi phát hiện ra số modem có một thiết bị tóm-và-lần được kích hoạt! Tôi bắt đầu lo lắng thực sự.

Những kẻ truy lùng tôi đang dần đến gần. Họ đã biết được chừng nào rồi?

Tôi cần phải biết liệu thiết bị theo dõi tóm-và-lần này đã được cài đặt đủ lâu để có thể tóm được bất kỳ cuộc gọi nào của tôi hay chưa.

General Telephone có một Trung tâm Điều hành Mạng ở Texas chuyên xử lý giám sát bộ chuyển mạch ngoài giờ làm. Tôi gọi đến đó và đóng giả là người của Phòng An ninh GTE. Tôi nhờ được nối máy đến người xử lý bộ chuyển mạch Durham Parkwood ở Raleigh. Một phụ nữ nhấc máy.

“Tôi đang giải quyết một vụ tự tử,” tôi nói với cô ta. “Số máy là 558-9800. Bẫy được đặt từ khi nào vậy?”

Cô ta nói mình sẽ đi tìm hiểu. Tôi đợi. Và đợi. Và đợi thêm, càng lúc càng thêm cẩn trọng. Cuối cùng, sau khoảng 5 phút, cuộc gọi lại được tiếp tục – không phải với người phụ nữ lúc nãy mà là một người đàn ông.

Tôi hỏi: “Chúng ta có thông tin gì không?”

Anh ta bắt đầu đặt ra một loạt các câu hỏi: Số gọi lại của tôi là gì? Tôi làm việc cho ai? Tôi đã nghiên cứu trước và đưa cho anh ta những câu trả lời phù

https://thuviensach.vn

hợp.

“Bảo quản lý của anh gọi cho tôi,” anh ta nói.

“Anh ta sẽ không ở đây cho đến sáng,” tôi nói. “Tôi sẽ để lại lời nhắn để anh ta gọi cho anh.”

Giờ tôi vô cùng nghi ngờ: Họ đã được cảnh báo có thể sẽ có ai gọi đến. Chuyện này có đầy đủ dấu hiệu về một cuộc điều tra an ninh quốc gia. Liệu có phải có người nào đó sắp định vị được vị trí của tôi hay không?

Để đề phòng, ngay lập tức tôi nhái điện thoại của mình sang một nhà cung cấp dịch vụ di động khác – Cellular One – trong trường hợp có ai đó thực sự đang theo dõi tôi.

Ngay khi Shimmy đến Raleigh, một nhân viên kỹ thuật của Sprint đã đến đón gã, lái xe đưa gã đến trạm. Tại trạm, các nhân viên kỹ thuật có một máy Cellscope 2000 để dò sóng, thiết bị đã được các điều tra viên ở Seattle sử dụng để theo dõi vị trí của tôi. Các kỹ thuật viên ở Cellular One đã được cảnh báo theo dõi bất cứ hành vi lạ nào xuất phát từ mạng của họ. Khi tôi thực hiện cuộc gọi đến Netcom, Cellular One đã xác định được dữ liệu cuộc gọi đang diễn ra và báo cho đội. Họ nhảy lên xe và bắt đầu lái lòng vòng, theo các chỉ dấu từ Cellscope 2000 để săn lùng nguồn gốc tín hiệu sóng di động của tôi. Chỉ mất vài phút, Shimmy và các thành viên khác của đội đã lái xe quanh Players Club và tìm kiếm bất kỳ căn hộ nào vẫn còn sáng đèn vào tờ mờ sáng.

Sau một lúc, họ đã gặp may. Kỹ thuật viên đang vận hành thiết bị giám sát thu được một cuộc hội thoại. John Markoff, người vừa đến Raleigh để tham gia cuộc truy bắt, nhận ra một trong các giọng nói. Đó là nhà sáng lập nổi tiếng của tạp chí 2600: Hacker Quarterly, Eric Corley (dù ông ta thích dùng cái tên tự chọn Emmanuel Goldstein hơn, tên gọi này được đặt theo một nhân vật trong cuốn tiểu thuyết 1984). Một lúc sau, lẫn trong những tiếng rít,

https://thuviensach.vn

tạp âm cùng tín hiệu chập chờn, họ nghe thấy một giọng nói ở đầu bên kia cuộc nói chuyện. Markoff cũng nhận ra.

“Đó là hắn,” Markoff gào lên. “Đó là Mitnick!”

https://thuviensach.vn

36
NGÀY LỄ TÌNH YÊU CỦA FBI

Lsar JSA cryoi ergiu lq wipz tnrs dq dccfunaqi zf oj uqpctkiel dpzpgp I jstcgo cu dy hgq?

Ngày 14 tháng 2, ngày Valentine. Tôi ngồi viết một vài sơ yếu lý lịch và thư giới thiệu, rồi vào tối muộn thì bắt đầu nhìn ngó lại lần nữa các tài khoản của tất cả quản trị viên hệ thống trên the Well. Tôi muốn tìm kiếm bất kỳ dấu hiệu nào cho thấy mình đang bị theo dõi hoặc đống phần mềm của tôi đã bị phát hiện. Nhưng chẳng có gì đáng báo động.

Để khuây khỏa một chút, tầm 9 giờ tối, tôi đi tập gym và dành khoảng một giờ trên máy Stair Master cộng thêm một giờ đẩy tạ. Sau khi tắm thật lâu dưới vòi sen đầy sảng khoái, tôi ăn tối ở một nhà hàng phục vụ 24 giờ. Dạo đó, tôi là một người ăn chay nên thực đơn ở đây không mấy hấp dẫn với tôi, nhưng đây là nơi duy nhất mở muộn đến giờ này.

Đến nửa đêm, tôi lái xe vào bãi đỗ ở Players Club. Hầu hết các căn hộ đều đã tắt đèn. Tôi không ngờ FBI đã giăng mạng lưới giám sát khắp nơi vào lúc tôi ra ngoài.

Tôi đăng nhập vào the Well để nhòm ngó. Khi thay mật khẩu một vài tài khoản không người dùng cho an tâm, một lần nữa tôi lại có cảm giác rờn rợn rằng mình đang bị ai đó theo dõi. Tôi quyết định chuyển sang chế độ dọn dẹp bán phần, nhưng trước hết tôi cần đảm bảo rằng mình đã sao chép tất cả tập tin chuyển đến the Well. Bởi không có kho lưu trữ an toàn nào khác ngoài hệ thống đã dùng trong vài tuần nay, tôi quyết định sao chép các tập tin sang các tài khoản không người dùng khác trên the Well. Khi chúng đã được an toàn, tôi sẽ tìm một chỗ khác để chuyển tới.

https://thuviensach.vn

Thế rồi tôi phát hiện ra một vài cửa hậu mình vẫn dùng để truy cập vào một số hệ thống đã biến mất một cách bí ẩn.

FBI làm việc rất chậm chạp. Ngay cả khi một cuộc gọi của tôi bị truy dấu, họ sẽ phải mất vài ngày hay vài tuần để điều tra. Ai đó có vẻ đang theo rất sát dấu vết của tôi, nhưng tôi vẫn còn nhiều thời gian. Hoặc chỉ là tôi đã nghĩ như vậy.

Khi di chuyển các tập tin, tôi có một cảm giác rất, rất không thoải mái, một cảm giác nôn nao trong dạ dày rằng sẽ có chuyện tồi tệ gì đó sắp xảy ra. Có thể tôi chỉ đang hoang tưởng. Ai đã đăng nhập vào tài khoản escape.com của tôi? Tại sao lại có bẫy trên dial-up của Netcom? Liệu Netcom có gửi đơn khiếu nại bị hack lên FBI không? Đầu óc tôi đang vẽ ra rất nhiều tình huống khác nhau.

Một tiếng sau, tôi vẫn như đang ngồi trên đống lửa. Tôi nghĩ việc này có thể hơi điên rồ nhưng linh tính tiếp tục mách bảo tôi có điều gì đó không đúng. Không ai biết tôi đang ở đâu, nhưng tôi không thể bỏ qua cảm giác nguy hiểm đang rình rập đâu đây.

Tôi tự thuyết phục bản thân rằng chẳng có chuyện gì, rằng tôi chỉ đang tự hù dọa bản thân. Cửa phòng nhìn ra một hành lang bên ngoài hướng xuống bãi đỗ xe. Tôi mở cửa, thăm dò bãi đỗ. Không có gì. Chỉ là trí tưởng tượng của mình thôi. Tôi đóng cửa lại và quay vào máy tính.

Cái thò đầu đó hóa ra lại là thảm họa. FBI đã theo dõi tín hiệu điện thoại di động của tôi đến tòa Players Club từ chập tối hôm đó nhưng lại nhầm lẫn rằng tín hiệu phát ra từ căn hộ phía bên kia tòa nhà. Lúc trở lại sau bữa tối, tôi đã lái xe vào bãi đỗ Players Club và bước ngay ra ngoài mạng lưới giám sát của FBI. Nhưng khi tôi thò đầu ra khỏi cửa, một viên cảnh sát tư pháp đã thoáng thấy tôi và cho rằng thật đáng ngờ khi muộn thế này lại có người nhìn ra ngoài căn hộ, thăm dò xung quanh rồi biến mất vào trong.

https://thuviensach.vn

30 phút sau, vào lúc khoảng 1 giờ 30 phút, tôi nghe thấy tiếng gõ cửa. Không để ý là đã quá muộn, tôi tự động gào lên: “Ai đấy?”

“FBI đây.”

Tôi cứng người. Lại một tiếng gõ cửa nữa. Tôi nói vọng ra: “Các anh tìm ai?”

“Kevin Mitnick. Anh có phải là Kevin Mitnick không?”

“Không,” tôi trả lời, cố ra vẻ khó chịu. “Các anh kiểm tra hòm thư thì biết.”

Xung quanh bỗng yên lặng như tờ. Tôi bắt đầu tự hỏi có phải họ thực sự đã cử ai đó đi kiểm tra hòm thư không. Họ cho rằng tôi sẽ dán nhãn “MITNICK” lên cửa hòm thư của mình chắc?

Không hay rồi! Rõ ràng tôi đã đánh giá thấp thời gian FBI cần để xác định vị trí của mình. Tôi tìm đường thoát. Tôi ra ngoài ban công và không thấy ai canh bên ngoài phía sau tòa nhà. Tôi nhìn vào bên trong tìm thứ gì có thể dùng làm dây leo. Ga giường? Không được, tốn quá nhiều thời gian để buộc thành dây. Hơn nữa, chuyện gì sẽ xảy ra nếu một trong số các đặc vụ thử bắn tôi trong lúc tôi đang trèo xuống.

Lại thêm những tiếng gõ cửa.

Tôi gọi cho mẹ ở nhà. Không còn thời gian cho quy trình “đến casino” của chúng tôi. “Con đang ở Raleigh, Bắc Carolina,” tôi nói với bà. “FBI đang ở ngoài cửa. Con không biết họ sẽ dẫn con đi đâu.” Chúng tôi nói chuyện vài phút, cả hai đều cố trấn an người còn lại. Mẹ mất bình tĩnh, rất buồn giận, quẫn trí, biết rằng tôi sẽ phải quay lại nhà tù. Tôi nói tôi yêu mẹ và bà, mong mọi người hãy mạnh mẽ và rằng đến một ngày nào đó mọi chuyện rồi sẽ qua.

https://thuviensach.vn

Trong lúc nói chuyện điện thoại, tôi lùng sục khắp căn phòng nhỏ, cố giấu đi bất kỳ thứ gì có thể gây rắc rối. Tôi tắt máy và tháo dây máy tính. Không có thời gian để xóa ổ cứng. Laptop vẫn ấm vì mới sử dụng. Tôi giấu một chiếc điện thoại di động dưới giường, chiếc còn lại trong túi đi tập gym. Mẹ bảo tôi hãy gọi cho dì Chickie và xem dì có ý tưởng gì không.

Dì Chickie cho tôi số điện thoại nhà riêng của John Yzurdiaga, luật sư đã làm việc cùng tôi từ vụ lục soát ở Calabasas.

Những tiếng gõ cửa lại vang lên cùng lời yêu cầu mở cửa.

Tôi hét lên: “Tôi đang ngủ – các anh muốn gì?”

Có tiếng trả lời: “Chúng tôi muốn hỏi anh vài câu.”

Cố ra vẻ căm phẫn hết sức có thể, tôi gào lên: “Hãy quay lại đây vào ngày mai khi tôi đã dậy!”

Họ sẽ không rời đi. Còn cách nào để thuyết phục họ rằng tôi không phải là người họ đang tìm không?

Vài phút sau, tôi gọi lại cho mẹ và nói: “Con sẽ ra mở cửa. Mẹ giữ máy nhé.”

Tôi hé cửa. Người gọi tôi nãy giờ có lẽ gần 40 tuổi, da đen với hàng ria bạc.

Đang là giữa đêm và ông ta mặc com-lê – tôi đoán ông ta hẳn là nhân viên FBI. Sau này, tôi mới biết ông ta là Levord Burns, người chịu trách nhiệm chỉ huy chiến dịch này. Cửa chỉ hé mở nhưng vẫn đủ để ông ta thò chân vào và ngăn không cho tôi đóng lại. Một số người theo sau, ào vào phòng.

“Cậu có phải là Kevin Mitnick không?”

“Tôi đã bảo ông là tôi không phải.”

https://thuviensach.vn

Một đặc vụ khác, Daniel Glasgow, bắt đầu xét hỏi tôi. Ông ta có vẻ già hơn, đậm người, tóc bạc. “Tắt điện thoại đi,” ông ta nói.

Tôi bảo mẹ: “Con dập máy đây.”

Một số gã bắt đầu lục soát.

Tôi hỏi: “Các anh có lệnh khám xét không?”

“Nếu anh là Kevin Mitnick, chúng tôi có lệnh bắt,” Burns nói.

Tôi bảo ông ta: “Tôi muốn gọi cho luật sư của mình.” Họ không cản tôi.

Tôi gọi cho Yzurdiaga. “Này John, Thomas Case đây, tôi đang ở Raleigh, Bắc Carolina. FBI vừa xuất hiện trước cửa nhà tôi. Họ nghĩ tôi là một gã có tên Mitnick và đang lục soát căn hộ của tôi, nhưng họ chưa cho tôi xem lệnh khám xét. Anh có thể nói chuyện với họ được không?”

Tôi đưa điện thoại cho đặc vụ đang đứng trước mặt tôi, Glasgow. Ông ta lấy điện thoại và bắt đầu hỏi ai đang ở đầu dây bên kia. Tôi nghĩ Yzurdiaga không muốn nói tên bởi anh ấy biết tôi đang dùng tên giả và việc này sẽ gây rắc rối cho anh về mặt đạo đức.

Glasgow đưa điện thoại cho Burns. Giờ thì tôi đã biết ai là người đứng đầu.

Tôi nghe thấy tiếng của Yzurdiaga: “Nếu các anh cho thân chủ của tôi xem lệnh hợp pháp, các anh có thể lục soát.”

Họ kết thúc cuộc gọi. Tất cả mọi người tiến hành lục soát căn hộ.

Burns đòi tôi cho xem giấy tờ tùy thân. Tôi lôi ví ra và cho ông ta xem bằng lái xe của G. Thomas Case.

Một gã lục soát đi vào phòng và lôi ra chiếc điện thoại hắn vừa tìm thấy dưới giường tôi rồi cho Burns xem.

https://thuviensach.vn

Trong lúc đó, Burns đang lần mò túi gym của tôi và cuối cùng cũng tìm thấy chiếc điện thoại kia. Thời đó, cước điện thoại vẫn tốn khoảng 1 đô-la một phút, vì vậy việc tôi sở hữu hai chiếc điện thoại không thể không gây ra nghi vấn.

Burns hỏi tôi số điện thoại di động. Tôi không nói gì cả. Tôi hy vọng ông ta sẽ bật điện thoại lên. Đó là một cái bẫy tôi đã thiết lập trong trường hợp chuyện này xảy ra: Nếu bạn không nhập mã số bí mật trong vòng 60 giây kể từ khi khởi động, tất cả bộ nhớ điện thoại, kể cả số điện thoại và ESN được lập trình trong đó sẽ bị xóa sạch. Bùm! Thế là tiêu tan bằng chứng.

Chết tiệt! Ông ta chỉ đưa nó cho một đặc vụ khác mà không bật lên.

Tôi lại đòi một lần nữa: “Lệnh khám nhà của các anh đâu?!” Burns lấy trong tập hồ sơ và đưa cho tôi một tờ giấy.

Tôi nhìn và nói: “Đây không phải là lệnh khám xét hợp pháp. Không có địa chỉ.” Nhờ đọc sách luật, tôi biết Hiến pháp Mỹ không cho phép các lệnh khám xét chung chung; một tờ lệnh khám xét chỉ hợp lệ nếu nó có địa chỉ nơi khám xét cụ thể và chính xác.

Họ quay lại lục soát. Như một diễn viên, tôi đặt mình vào tình thế của một người đang bị xâm hại. Tôi nói to: “Các anh không có quyền ở đây. Hãy cút ra khỏi căn hộ của tôi. Các anh không có lệnh khám xét. Cút ra khỏi căn hộ của tôi NGAY!”

Một số đặc vụ đứng vòng tròn quanh tôi. Một người dí tờ giấy vào mặt tôi. Anh ta nói: “Nhìn có giống anh không?”

Tôi không thể không cười trong lòng. Sở Cảnh sát Tư pháp đã tạo ra cả hình truy nã cho tôi. Thật không thể tin được!

Nội dung trên đó viết:

https://thuviensach.vn

LỆNH TRUY NÃ VÌ VI PHẠM ĐIỀU KHOẢN QUẢN CHẾ

Nhưng bức ảnh trên đó là bức ảnh đã chụp hơn sáu năm trước tại văn phòng FBI ở Los Angeles, chính là tấm ảnh tờ New York Times đã sử dụng. Hồi đó, tôi béo hơn bây giờ rất nhiều và trông rất bẩn thỉu lôi thôi vì không được tắm rửa cạo râu trong ba ngày.

Tôi nói với tay đặc vụ đó: “Nhìn chẳng giống tôi gì cả.”

Trong đầu tôi là ý nghĩ: Họ không chắc. Có thể mình sẽ thoát được chuyện này.

Burns rời căn hộ.

Hai gã quay lại lục soát. Hai người khác đứng quanh và quan sát; khi tôi hỏi, một trong số họ nói họ là sĩ quan địa phương đến từ Lực lượng Chức năng Phòng chống Tội phạm bị Truy nã Raleigh-Durham. Hả, FBI nghĩ rằng ba người của họ vẫn không đủ để hạ một gã hacker hiền lành sao?

Đặc vụ Glasgow lôi ra chiếc cặp tài liệu của tôi, trong đó chứa đầy những giấy tờ ghi lại tất cả các danh tính khác nhau của tôi, tờ khai sinh trắng và những thứ tương tự – tấm vé một chiều đến thẳng nhà tù. Ông ta đặt nó xuống chiếc bàn ăn nhỏ và mở ra.

Tôi hét: “Này!” và ngay khi ông ta nhìn lên, tôi đóng nắp lại, lật khóa chốt và ấn, xoay mã khóa chiếc cặp.

Ông ta gào lên với tôi: “Tốt nhất là anh nên mở nó ra!”

Tôi không thèm để ý. Ông ta vào bếp, kéo vài ngăn kéo, tìm thấy một con dao khắc lớn và quay ra.

Mặt ông ta đỏ lựng lên.

https://thuviensach.vn

Ông ta đâm con dao vào chiếc cặp, để cắt nó ra. Một đặc vụ khác tên là Lathell Thomas tóm lấy tay ông ta. Những người khác trong phòng đều biết nếu Glasgow cắt chiếc cặp ra khi chưa có lệnh khám xét hợp lệ, thì bất kỳ thứ gì tìm thấy bên trong có thể sẽ không được chấp nhận trước tòa.

Đặc vụ Burns đã đi được nửa tiếng. Giờ thì ông ta quay lại và đưa cho tôi một tờ lệnh khám khác, tất cả được gõ và ký bởi một thẩm phán liên bang nhưng với địa chỉ của tôi được viết bằng tay. Tính đến lúc này, hai đặc vụ kia đã lục soát – bất hợp pháp – hơn hai giờ đồng hồ.

Đặc vụ Thomas bắt đầu lục soát tủ quần áo của tôi. Tôi cố hét đuổi ông ta đi, nhưng ông ta vẫn mặc kệ tôi và mở cửa. Sau một lúc, ông ta quay lại, tay cầm một chiếc ví.

“Ái chà chà, chúng ta có gì đây nhỉ?!” ông ta nói bằng chất giọng miền Nam lè nhè đặc trưng.

Ông ta bắt đầu lôi ra các bằng lái xe với những cái tên mà tôi đã dùng trước đó. Những người khác dừng việc đang làm lại để nhìn.

“Ai là Eric Weiss?” ông ta hỏi. “Ai là Michael Stanfill?”

Tôi muốn giật mọi thứ khỏi tay ông ta, nhưng sợ rằng như vậy lại trông có vẻ muốn tấn công ông ta – đó không phải là ý hay trong một căn phòng toàn những gã có súng.

Giờ thì họ đã biết tôi không phải là một công dân lương thiện, chăm chỉ. Nhưng họ đến để bắt Kevin Mitnick và không có gì trong ví có thể giúp họ gán cái tên đó cho tôi.

Rõ ràng, tôi đã nhập vai rất ngọt – một công dân nổi giận với việc bị quấy rối bất công. Giờ thì họ đang bàn xem liệu có nên lôi tôi đến trung tâm thành phố lấy vân tay để chứng minh tôi thực sự là Mitnick và đang cố gạt họ hay không.

https://thuviensach.vn

Tôi nói: “Ý hay đấy. Mấy giờ sáng mai các anh muốn tôi có mặt ở văn phòng của các anh?” Họ bỏ qua tôi. Giờ thì cả ba người của FBI đều quay lại tìm kiếm. Cho đến giờ vận may của tôi vẫn đang cầm cự được.

Thế rồi chuyện đó đã diễn ra: Thomas lục đống quần áo trong tủ của tôi. Ông ta lục lọi trong chiếc áo khoác trượt tuyết cũ.

Từ một túi khóa kéo bên trong, ông ta lôi ra một mảnh giấy.

“Một cuống séc lương,” ông ta thông báo. “Trả cho Kevin Mitnick.”

Đặc vụ Thomas hét lên: “Anh đã bị bắt!”

Không giống như trên tivi: Không ai thèm đọc cho tôi nghe quyền Miranda[93] của mình.

[93] Quyền Miranda: Ở Mỹ, người bị bắt giữ trước khi thẩm vấn hoặc lấy cung phải được cho biết rõ rằng họ có quyền giữ im lặng và bất kỳ điều gì người đó nói sẽ được dùng để chống lại họ trước tòa. (BTV, theo Wikipedia)

Tôi đã rất cẩn thận và giờ thì cuống séc từ một công ty tôi từng làm việc trong một khoảng thời gian ngắn sau khi rời Beit T’Shuvah, ẩn nấp nhiều năm trong chiếc túi trong bị bỏ qua của chiếc áo khoác trượt tuyết đó, đã trở thành cái kết cho tôi.

Cổ họng tôi đắng nghét và thậm chí không thể đến bồn để nhổ. Tôi nói với các đặc vụ rằng mình cần lấy thuốc trào ngược dạ dày. Họ nhìn nhãn thuốc và nhận ra đó là thuốc kê theo đơn nhưng từ chối cho tôi một viên.

Thật khó tin, tôi đã giữ chân họ suốt ba tiếng rưỡi. Và tôi đã lẩn trốn công khai gần ba năm trong khi FBI, Sở Cảnh sát Tư pháp và cả Sở Mật vụ đều truy tìm tôi.

Nhưng giờ thì mọi chuyện đã kết thúc.

https://thuviensach.vn

Đặc vụ Thomas lườm tôi và nói: “Mitnick, hết rồi!”

Thay vì còng tay tôi ra sau lưng, quyền Cảnh sát Trưởng cùm tôi bằng còng, xích bụng và kiềng chân bằng sắt. Họ áp giải tôi ra khỏi cửa. Chính vào lúc đó, tôi biết mình sẽ không thể ra ngoài sớm được.

https://thuviensach.vn

37

THOÁT NẠN VẬT TẾ THẦN

V2hhdCBGQkkgYWdlbnQgYXNrZWQgU3 VuIE1pY3Jvc3lzdGVtcyB0 byBjbGFpbSB0aGV5IGxvc3QgODA gbWlsbGlvbiBkb2xsYXJzPw==

Nơi ở mới của tôi là Nhà tù Quận Wake thuộc trung tâm Raleigh mang phong cách hiếu khách khác biệt của miền Nam rất rõ ràng. Khi tôi vào trại, các đặc vụ liên bang đã đưa ra các chỉ thị nghiêm ngặt hết lần này đến lần khác rằng không được để tôi lại gần điện thoại.

Cứ mỗi lần thấy bóng áo đồng phục nào đi ngang qua buồng giam, tôi đều hỏi xin gọi điện cho gia đình. Nhưng họ đều giả điếc.

Nhưng có một cai ngục có vẻ thông cảm hơn một chút. Tôi kể cho cô ấy nghe việc mình cần phải gọi cho gia đình để thu xếp chuyện bảo lãnh. Cô ấy tỏ lòng thương hại và chuyển tôi đến một buồng giam khác có điện thoại.

Cuộc gọi đầu tiên của tôi là cho mẹ; bà tôi cũng đã đến ở cùng mẹ để hai người có thể cùng lo lắng cho tôi. Cả hai đều đang rất sốc, rất buồn giận và rối trí. Tôi đã bao lần gây ra chuyện, khiến họ phải gánh chịu nỗi đau lớn lao khi con trai/cháu trai mình phải quay lại nhà tù và có thể còn phải ngồi đó rất lâu.

Sau đó, tôi gọi cho Lewis. Vì tất cả cuộc gọi từ buồng giam đều bị giám sát, nên tôi không thể nói nhiều.

“A lô?” Lewis lầm bầm trong cơn ngái ngủ. Đang là 1 giờ sáng ở California, buổi sáng ngày 15 tháng 2 năm 1995.

https://thuviensach.vn

“Đây là một cuộc gọi người nhận trả tiền,” nhân viên trực tổng đài nói. “Người gọi, tên cậu là gì?”

“Kevin. ”

“Anh có chấp nhận trả tiền không?”

“Có,” Lewis nói.

“Tớ vừa bị FBI bắt tối nay. Giờ tớ đang ở trong tù tại Raleigh, Bắc Carolina. Tớ chỉ nghĩ là cậu nên biết,” tôi nói với kẻ đồng mưu của mình.

Cậu ta không cần tôi phải nói thẳng ra rằng hãy chuyển sang chế độ dọn dẹp ngay lập tức đi.

Sáng hôm sau, tôi được đưa đến tòa trình diện lần đầu, vẫn mặc chiếc áo len đen khi đi tập gym khoảng 12 tiếng trước, vào đêm tự do cuối cùng của mình.

Tôi sững sờ khi thấy cả phòng xử xôn xao và chật cứng, không còn ghế nào trống. Có vẻ như một nửa số người ở đây đều có máy quay hoặc sổ tay phóng viên. Đây là một rạp xiếc truyền thông. Bạn sẽ nghĩ FBI vừa bắt được Manuel Noriega[94].

[94] Manuel Noriega (11/2/1934 - 29/5/2017): Cựu tướng lĩnh kiêm nhà độc tài quân sự của Panama trong giai đoạn 1983-1989. Ông từng được biết đến là một nhà lãnh đạo thân Mỹ nhưng sau đó, dưới thời kỳ của Tổng thống George Bush (Cha), ông bị Mỹ truy tố với tội danh tống tiền, rửa tiền, buôn lậu ma túy và bị tuyên án 40 năm tù. (BTV)

Ánh mắt tôi dừng lại ở một người đứng gần phía đầu phòng xử, một người tôi chưa từng gặp ngoài đời nhưng vẫn có thể nhận ra ngay lập tức: Tsutomu Shimomura. FBI có lẽ sẽ không bao giờ bắt được tôi nếu anh ta không tức

https://thuviensach.vn

giận vì các vụ đột nhập của tôi vào máy chủ của mình đến mức bỏ hết mọi việc khác và dẫn đầu đội truy tìm tôi.

Anh ta nhìn tôi trừng trừng.

Anh ta và cô bạn gái ném cho tôi cái nhìn sắc lẹm, đặc biệt là cô bạn gái. John Markoff bắt đầu ghi chép.

Phiên sơ thẩm chỉ diễn ra trong vòng vài phút, kết thúc bằng lệnh tôi sẽ bị giam giữ mà không được phép tại ngoại. Và một lần nữa, tôi sẽ không được tiếp xúc với điện thoại.

Tôi không thể chịu nổi ý nghĩ đó: Tôi sẽ quay lại phòng biệt giam.

Khi bị còng tay dẫn đi, tôi đi ngang qua Shimmy. Anh ta đã thắng. Công bằng và sòng phẳng. Tôi gật đầu với anh ta và ngã mũ tượng trưng: "Tôi khâm phục khả năng của anh," tôi nói với anh ta.

Shimmy gật đầu đáp lễ.

Bước ra khỏi phòng xử trong xiềng xích, tôi nghe thấy những tiếng la: "Này, Kev!" Tôi nhìn ra ngoài ban công, dường như có tới hàng trăm paparazzi đang chĩa máy ảnh về phía tôi và bấm liên tục, ánh đèn flash khắp nơi. Ôi, lạy Chúa, tôi nghĩ. Việc này còn ầm ĩ hơn mình tưởng nhiều. Tôi mất bình tĩnh. Thế nào mà tôi lại thành câu chuyện lớn thế này?

Tất nhiên, tôi không được đọc các bài báo khi đó nhưng bài viết của Markoff đăng trên New York Times vào ngày hôm sau – thậm chí còn dài hơn bài được đăng trong ngày lễ Quốc khánh của hắn một năm trước và một lần nữa trên trang nhất – dường như hắn đã đổ bê-tông hình ảnh Osama bin Mitnick[95] vào tâm trí mọi người. Markoff trích lời Kent Walker, Trợ lý công tố đến từ San Francisco, như sau: "[Mitnick] có thể được coi là tên hacker máy tính bị truy nã gắt gao nhất thế giới. Hắn được cho là đã tiếp cận được những bí mật kinh doanh trị giá hàng tỷ đô-la. Hắn là một hiểm họa rất lớn."

https://thuviensach.vn

[95] Tác giả tự ví mình giống như Osama bin Laden – trùm khủng bố, người lãnh đạo tổ chức cực đoan Hồi giáo al-Qaeda, tác giả của vụ khủng bố 11 tháng 9 – nỗi khiếp đảm của nước Mỹ một thời. (BTV)

Vào thời điểm bài báo đầu tiên ra mắt ngày 4 tháng 7 của Markoff, tôi chỉ bị truy nã vì vi phạm điều khoản quản chế, nhưng câu chuyện đó đã để lại trong lòng độc giả ấn tượng rằng tôi là một nhân vật siêu phản diện, mối hại nguy cho người dân Mỹ. Góc nhìn của hắn về vụ bắt giữ tôi lúc đó đã thổi bùng lên ngọn lửa đang nhen nhóm của cánh truyền thông. Câu chuyện được tiếp tục trên Dateline, Good Morning America và chỉ có Chúa mới biết được còn bao nhiêu chương trình lớn nhỏ khác. Vụ bắt giữ tôi xuất hiện trên khắp các bản tin trong suốt ba ngày liên tiếp.

Giọng điệu tiêu biểu của các bản tin cũng giống như trong một bài báo phát hành ngày 27 tháng 2 năm 1995 trên Time. Tiêu đề phụ của bài báo giật tít như sau:

HACKER BỊ TRUY NÃ GẮT GAO NHẤT NƯỚC MỸ ĐÃ SA LƯỚI

Tin tức từ luật sư được tòa chỉ định cho tôi ở Raleigh cũng không tốt. Tôi bị truy tố 23 tội giả mạo thiết bị truy cập. Trong đó, có 21 tội liên quan đến các cuộc gọi tôi đã thực hiện từ máy điện thoại nhái số. Hai tội còn lại là do tàng trữ thông tin, đặc biệt là các cặp số điện thoại và số sê-ri điện tử có thể dùng để nhái số. Mức án tối đa là 20 năm cho mỗi cuộc gọi miễn phí. 20 năm cho mỗi cuộc gọi! Tôi đang phải đối mặt với tình huống xấu nhất là 460 năm tù.

Tình huống có vẻ tồi tệ – 460 năm tù không phải là chuyện đơn giản. Tôi không thích thú gì với ý nghĩ sẽ bị nhốt trong tù suốt phần đời còn lại, không được sống một cuộc đời vui vẻ và có ích, đặc biệt là không thể dành thời gian quý báu bên mẹ và bà. Hiển nhiên là họ đã tóm được tôi với tội danh nhái số điện thoại (luật liên bang coi các số ESN là thiết bị truy cập không được cấp phép). Đúng là tôi đã vi phạm các điều khoản quản chế năm 1989 với việc hack vào hòm thư thoại của điều tra viên an ninh Pacific Bell,

https://thuviensach.vn

Darrell Santos, để lấy thông tin về vụ Teltec, cũng như liên hệ với các "hacker máy tính". Nhưng 460 năm tù cho những tội "xấu xa" này sao? Thế gian không còn tên tội phạm chiến tranh nào ư?

Tất nhiên, FBI cũng tìm thấy cơ sở dữ liệu khách hàng của Netcom chứa hơn 20.000 số thẻ tín dụng trên máy tính của tôi, nhưng tôi chưa bao giờ thử dùng bất kỳ số nào trong đó; không có công tố viên nào có thể lập hồ sơ kiện tôi về mục này. Tôi phải thú nhận rằng tôi thích ý tưởng mình có thể dùng mỗi ngày một chiếc thẻ tín dụng khác nhau cho đến hết phần đời còn lại mà không hết chỗ thẻ. Nhưng tôi chưa bao giờ có bất kỳ ý định nào về việc đốt tiền bằng chỗ thẻ đó và chưa bao giờ làm. Việc đó thật sai trái. Chiến lợi phẩm của tôi là bản sao cơ sở dữ liệu khách hàng của Netcom. Tại sao việc đó lại khó hiểu đến vậy? Các hacker và game thủ đều hiểu rằng đó là một dạng bản năng. Bất kỳ ai thích chơi cờ vua đều hiểu rằng họ chỉ cần thắng đối phương là đủ. Bạn không cần phải cướp bóc vương quốc hay tịch thu tài sản của người khác để khiến chiến thắng trở nên có giá trị.

Tôi luôn lấy làm lạ khi những kẻ bắt tôi gặp rất nhiều khó khăn để hiểu được niềm thỏa mãn sâu thẳm có thể có được từ một trò chơi kỹ năng. Đôi lúc tôi không thể không tự hỏi phải chăng lý do họ không hiểu được động cơ của tôi là bởi bản thân họ đều thấy hấp lực của tất cả những thẻ tín dụng đó là không thể khước từ.

Ngay cả Markoff, trong bài báo trên New York Times, cũng thừa nhận rằng tôi rõ ràng không hứng thú với viễn cảnh làm giàu. Mức độ về những gì tôi từ chối không làm đã được chuyển tải đến người đọc qua khẳng định của Kent Walker rằng tôi "được cho là đã tiếp cận được những bí mật kinh doanh trị giá hàng tỷ đô-la". Nhưng bởi tôi chưa bao giờ định dùng hay bán những thông tin này, nên việc chúng đáng giá đến đâu không làm tôi bận tâm. Vậy bản chất những tội của tôi là gì? Rằng tôi "được cho là đã tiếp cận được"?

https://thuviensach.vn

Cuối cùng thì tôi cũng đã bị bắt, các công tố viên ở nhiều khu vực tài phán liên bang điên cuồng soạn ra những danh sách dài gồm các tội và cáo trạng chống lại tôi, nhưng tôi vẫn có lý do để hy vọng. Mặc kệ những chứng cứ kia, hồ sơ của chính phủ không phải là không có kẽ hở. Có một số xung đột pháp lý cần phải được giải quyết trước. Ví dụ như Shimmy đã bí mật làm việc như một nhân viên chính phủ thực thụ và nghe lén liên lạc của tôi mà không có lệnh, có vẻ là một vụ vi phạm thủ tục ghê tởm của chính phủ. Luật sư của tôi cũng nộp một bản kiến nghị rằng lệnh khám xét của chính phủ có sai sót. Nếu tòa xử có lợi cho tôi, tất cả chứng cứ thu được ở Bắc Carolina sẽ vô giá trị, không chỉ ở Raleigh mà ở mọi nơi khác.

Với John Bowler, trợ lý công tố trẻ tuổi và đầy triển vọng đảm nhận vụ của tôi, đây chắc chắn phải là một cơ hội vàng. Nếu anh ta có thể lấy được lời thú tội trên tất cả cáo trạng và thuyết phục thẩm phán đập vào mặt tôi một phán quyết trừng phạt khủng khiếp, thì chỉ riêng sự chú ý của truyền thông đã đủ để đưa sự nghiệp của anh ta thăng hoa. Nhưng thực tế, các hướng dẫn xử án liên bang thường sẽ yêu cầu thẩm phán ra phán quyết dựa trên các tổn thất tối thiểu mà các công ty điện thoại phải chịu khi tôi thực hiện những cuộc gọi miễn phí đó.

Sau lần trình diện trước tòa đầu tiên, tôi được chuyển đến Nhà tù Quận Johnston ở Smithfield, Bắc Carolina, Sở Cảnh sát Tư pháp ra lệnh cho các cai ngục nhốt tôi vào nơi tôi sợ nhất: “cái hố”.

Tôi không thể tin được những gì đang diễn ra. Lê bước về phía cánh cửa đó trong cùm chân và xiềng xích, tôi ngần ngừ không muốn bước tiếp. Thời gian như chậm lại. Vào lúc đó, tôi biết động lực chính khiến tôi trốn chạy suốt ba năm qua chính là nỗi sợ hãi nơi này. Tôi không nghĩ mình có thể chịu được nơi đó thêm một lần nữa. Và giờ những tay lính gác đang ở ngay đây, dẫn tôi quay trở lại cơn ác mộng và tôi không thể làm gì để ngăn cản họ.

https://thuviensach.vn

Lần cuối cùng họ nhốt tôi vào phòng biệt giam hơn tám tháng để buộc tôi làm điều họ muốn là vào năm 1988: Ngay khi tôi ký thỏa thuận nhận tội, họ sẽ đưa tôi ra với những tù nhân bình thường khác. Và lần này, chính phủ không nhét tôi vào cái lỗ địa ngục đó để bảo vệ xã hội khỏi tay tôi, hay bảo vệ tôi khỏi các tù nhân khác. Nó là sự ép buộc, đơn giản và dễ hiểu. Thông điệp rất rõ ràng: Tất cả những gì tôi phải làm là đồng ý với các yêu cầu của bên công tố và từ bỏ một số quyền, chấp nhận chỉ gọi cho người thân nhất trong gia đình cùng tư vấn viên pháp lý, rồi họ sẽ rất vui lòng cho tôi ra khỏi phòng biệt giam, về lại với những tù nhân bình thường.

Tôi ước mình có thể mô tả cảm giác nặng nề khi bước vào bên trong. Sau khi sống trong nỗi sợ "cái hố" này suốt nhiều năm, tôi đã cố hết sức để không phát điên khi họ khóa cửa lại sau lưng tôi. Tôi thà ở chung buồng giam với một gã buôn ma túy mệt mỏi xăm trổ đầy người còn hơn là thấy bản thân bị nhốt lại một mình như thế này một lần nữa.

Có một bài rap về bọn nghiện máy tính, rằng chúng tôi đã dành không biết bao nhiêu thời gian trong những căn phòng nhỏ tăm tối, thu mình bên ánh sáng màn hình laptop, thậm chí không biết đang là ngày hay đêm. Với những người đi làm sáng đi tối về, cuộc sống đó nghe có vẻ giống như biệt giam, nhưng không hề.

Có một sự khác biệt vô cùng lớn giữa việc dành thời gian ngồi một mình với việc bị quăng vào cỗ quan tài kinh tởm, bẩn thỉu sẽ là nhà của bạn hôm nay, ngày mai, tháng tới. Chẳng có tia sáng nào nơi cuối đường hầm. Cỗ quan tài đó sẽ được chính những kẻ sẽ làm mọi việc có thể để khiến bạn khốn khổ đưa tiễn. Bất kể bạn có cố gắng mường tượng lại nó như thế nào trong đầu, thì chờ đợi bạn ở trong cái hố lúc nào cũng là sự tăm tối và suy sụp. Biệt giam thường được coi là một biện pháp tra tấn. Ngay cả ngày nay, Liên Hiệp Quốc vẫn đang đấu tranh để quy nó thành một hình phạt vô nhân đạo.

Rất nhiều chuyên gia nói rằng biệt giam kéo dài còn khủng khiếp hơn dìm nước hay các hình thức tra tấn thể chất khác rất nhiều. Trong cái lỗ này, tù

https://thuviensach.vn

nhân sẽ phải chịu đựng trạng thái nửa tỉnh nửa mê, tuyệt vọng, phẫn nộ, suy nhược trầm trọng và những bệnh lý tinh thần khác. Sự cách ly, việc không được hoạt động và thiếu đi những cấu trúc có thể dễ dàng làm rã rời đầu óc. Không có ai để tương tác, bạn sẽ không có cách nào để kiểm soát suy nghĩ của mình hay giữ được quan điểm của bản thân. Nó là một cơn ác mộng còn khủng khiếp hơn rất nhiều những gì bạn có thể tưởng tượng.

Đó là lý do tại sao tất cả các nghiên cứu về biệt giam hơn 60 ngày đều cho thấy những ảnh hưởng chấn thương tâm lý. Đôi khi chúng là vĩnh viễn. Tôi lo sợ điều đó. Đã hơn sáu năm kể từ khi tôi ở trong phòng biệt giam và đến giờ nó vẫn ám ảnh tôi. Tôi muốn ra khỏi đó càng nhanh càng tốt.

Một tuần sau khi bị quăng vào phòng biệt giam, công tố viên liên bang đề nghị một thỏa thuận chuyển tôi về với các tù nhân bình thường nếu tôi từ bỏ các quyền của mình và đồng ý:

- không xử bảo lãnh
- không xử sơ thẩm
- không gọi điện, trừ các cuộc gọi tư vấn pháp lý và tới một số thành viên trong gia đình.

Họ bảo tôi hãy ký vào thỏa thuận này và tôi sẽ được ra khỏi phòng biệt giam. Tôi đồng ý ký.

Luật sư ở Los Angeles của tôi, John Yzurdiaga và người cộng sự Richard Steingard, đã giúp tôi soạn thỏa thuận. Do tôi bị bắt ở Raleigh, nên cả hai vị luật sư đều hào phóng dành thời gian để giải quyết vụ của tôi. John đã tình nguyện đại diện cho tôi mà không tính phí kể từ thời điểm cuối năm 1992, khi FBI lục soát căn hộ tại Calabasas của tôi.

Khi quay lại với khu vực tù nhân thường, tôi nói chuyện với John Yzurdiaga và Richard Steingard qua điện thoại. Giọng nói của John thể hiện rõ sự căng thẳng mà tôi chưa bao giờ thấy trước đây. Trước sự ngạc nhiên của tôi, cả

https://thuviensach.vn

hai bắt đầu tra khảo tôi về các bí mật quốc gia. “Chính xác thì cậu đã tiếp cận được những thông tin tuyệt mật nào? Cậu đã hack vào bất kỳ cơ quan tình báo nào chưa?”

Khi hiểu ra họ đang định nói gì, tôi cười to: “Phải rồi. Kiểu như tôi là điệp viên tham gia vào một nhiệm vụ tuyệt mật nào đó ấy hả!” tôi nói.

Không ai trong số họ cười.

“Đừng nói dối chúng tôi, Kevin,” John nói, nghe thành thực đến đáng sợ.

“Đã đến lúc đầu thú rồi.”

Tôi không tin vào tai mình. “Thôi nào, các anh – các anh đang đùa, phải không?”

Rồi Richard tung ra tin dữ: “Trợ lý công tố Schindler đang yêu cầu anh đồng ý một buổi thẩm vấn với CIA.”

Chuyện quái gì đang xảy ra vậy? Phải, tôi đã hack các nhà sản xuất điện thoại nổi tiếng nhất thế giới, các công ty do Bell Pacific điều hành và các nhà phát triển hệ điều hành khắp nước Mỹ, nhưng tôi chưa bao giờ thử nhắm vào bất kỳ mục tiêu nào có liên quan đến chính phủ. Sao FBI lại có thể nghĩ ra điều này? Lời cáo buộc này hoàn toàn không có căn cứ.

“Tôi không có gì để giấu,” tôi nói với tiếng thở dài. “Tôi sẽ tham gia buổi thẩm vấn với điều kiện tất cả các anh phải hiểu rằng tôi sẽ không nói về bất kỳ ai khác.” Tôi không biết bất kỳ ai từng hack vào hệ thống của chính phủ hay quân đội, nhưng kể cả nếu biết, việc trở thành kẻ chỉ điểm cho quân đội cũng đi ngược với các nguyên tắc đạo đức và lương tâm của tôi.

Cuối cùng, không có gì diễn ra sau cuộc nói chuyện đó. Có lẽ Schindler hoặc Bộ Tư pháp đang bận đi câu cá. Việc này làm tôi nhớ lại lần Marty Stolz ở Intermetrics bí mật kể với tôi về một siêu hacker mà FBI đang truy

https://thuviensach.vn

lùng đã đột nhập vào được CIA. Tôi coi đó như một câu chuyện thần thoại nữa lại vượt ngoài tầm kiểm soát.

Thời Trung cổ, các câu chuyện thần thoại được thêu dệt quanh các ảo thuật gia thường khiến họ gặp rắc rối nghiêm trọng. Đôi lúc, các câu chuyện thần thoại và siêu nhiên này lại khiến họ bị giết hại. Một nghệ sĩ biểu diễn đường phố sẽ khiến dân làng địa phương trầm trồ bằng những mánh khóe và tay nghề khôn khéo. Bởi không biết anh ta làm những trò đó như thế nào, nên họ không thể đoán được khả năng của anh ta đến đâu. Anh ta có vẻ như có khả năng làm mọi thứ biến mất và xuất hiện theo ý muốn. Đó là vấn đề. Bất kỳ thứ gì không thường xuyên xảy ra – vài con bò chết, mùa màng thất thu, Sarah bé bỏng bị ốm – quá dễ để đổ tội cho nhà ảo thuật.

Nếu mọi thứ khác đi, có lẽ tôi đã được bí mật tận hưởng danh xưng "Hacker bị truy nã gắt gao nhất thế giới" và cười nhạo mỗi khi mọi người tin rằng tôi là một thiên tài siêu phàm có thể hack mọi thứ. Nhưng tôi có một linh cảm xấu rằng việc này sẽ làm hại tôi – và tôi đã đúng. "Huyền thoại về Kevin Mitnick" sắp sửa gây ra muôn vàn sóng gió cho cuộc đời tôi.

* * *

Vì là một tù nhân rất nổi tiếng, không lâu sau tôi cần John Yzurdiaga can thiệp lần nữa. Trưởng trại đã mở tất cả thư của tôi, bao gồm thư tôi viết cho các luật sư của mình, việc này đã vi phạm quyền luật sư-thân chủ của tôi. Tôi bảo hắn ta dừng lại nhưng hắn vẫn tiếp tục làm. Tôi cảnh cáo hắn rằng luật sư của tôi sẽ yêu cầu tòa án ra lệnh bắt hắn dừng lại. Hắn lờ tôi đi.

John lấy được lệnh của tòa. Tay cai ngục này buộc phải tuân thủ, nhưng hắn rất phẫn nộ về chuyện đó. Hắn gọi cho Sở Cảnh sát Tư pháp và yêu cầu họ chuyển tôi đến nhà tù khác và họ đã làm như vậy thật. Nhà tù quận Vance khiến nhà tù Johnston chẳng khác nào khách sạn Holiday Inn.

Khi tôi bị chuyển đi, một viên cảnh sát tư pháp với chất giọng miền Nam đặc sệt đến mức nghe như thể anh ta đang vụng về vào vai người cảnh sát

https://thuviensach.vn

trưởng trong Good Ol’ Boy đã cười và nói: “Cậu là tù nhân duy nhất của chúng tôi bị đá đít ra khỏi nhà tù!”

Sau khi tôi ngồi tù khoảng năm tháng, John Dusenbury, luật sư công được tòa án chỉ định cho tôi ở Raleigh đã khuyên tôi nên đồng ý với “Luật 20”. Tức là tôi sẽ nhận tội với một cáo trạng duy nhất về việc tàng trữ các cặp số điện thoại di động và số sê-ri điện tử mà tôi đã dùng để nhái điện thoại di động nhằm đổi lấy một án phạt tám tháng, dù tôi vẫn có thể phải đối mặt với một án tù lên đến 20 năm nếu thẩm phán quyết định không làm theo lời đề nghị này của bên công tố. Dù vậy, thẩm phán Terrence Boyle vẫn tán thành thỏa thuận này. Mọi việc giờ còn diễn biến hay hơn: Vụ của tôi đã được chuyển đến Los Angeles để xét xử và phân giải những vi phạm trong thời gian quản chế, tức là tôi sẽ được chuyển đi.

Chuyến đi từ Raleigh tới Los Angeles tồi tệ đến mức kinh ngạc. Các nhà tù liên bang khét tiếng với hình thức trừng phạt gọi là “liệu pháp diesel”. Nó khủng khiếp đến mức các tù nhân thường coi đó là khía cạnh tàn bạo nhất của việc bị tống giam. Thứ đáng ra là một chuyến xe đơn giản được mở rộng có chủ đích đầy ác tâm thành nhiều ngày thậm chí là nhiều tuần. Suốt dọc đường, các cảnh vệ ác độc càng nghĩ ra nhiều trò hành hạ thì các tù nhân càng phải chịu khổ cực.

Sau khi bị gọi dậy vào lúc 3 giờ 30 phút sáng, tù nhân được chuyển đi sẽ bị tống vào một căn phòng lớn và lột trần ra khám xét. Một sợi xích thòng từ eo mỗi tù nhân sẽ gắn chặt vào còng tay của anh ta ở tầm bụng, tức là anh ta gần như không thể nhúc nhích cánh tay. Chân cũng bị xích, nên anh ta rất khó có thể đi lại hay di chuyển. Rồi anh ta và các bạn tù khác bị tải lên xe và lái đi tám giờ mỗi ngày với những chặng dừng ngẫu nhiên ở các thành phố dọc đường, nơi mọi người bị cho xuống xe, qua đêm ở một buồng giam khác, và lại bị gọi dậy vào sáng hôm sau để trải qua toàn bộ quá trình một lần nữa. Cuối cùng, bạn sẽ đến nơi khi toàn thân rã rời.

https://thuviensach.vn

Trong liệu pháp diesel của tôi đến Los Angeles, tôi bị giữ lại ở Atlanta vài tuần. Trại cải tạo liên bang ở đây là nơi đáng sợ nhất trong tất cả các nhà tù tôi từng bị giam giữ. Những bức tường cao vút của nhà tù được phủ những hàng rào dây thép gai sắc như dao cạo. Không còn nghi ngờ gì, bạn đang bước vào ngục tối. Ở mỗi cửa, đều có các cánh cửa và cổng điện lớn. Càng vào sâu trong lòng nhà tù này, bạn càng nhận ra không có lối thoát nào cả.

Cuối cùng, khi được chuyển đi lần nữa, tôi bay tới vài nhà tù ở các bang khác nhau khắp đất nước. Đến khi tới được Los Angeles, tôi đã không còn tâm trạng nén nhịn nào nữa. Xuống máy bay, viên cảnh sát tư pháp cười nhe nhởn với tôi và tự mãn nói: “Này, Mitnick! Vậy là cuối cùng cảnh sát tư pháp cũng tóm được cậu! Tất cả là nhờ công tác giữ trật tự xuất sắc.”

“Cảnh sát tư pháp chả liên quan gì ở đây,” tôi nói với ông ta. “Đó là một dân thường thông minh hơn các ông đang làm việc cho FBI.”

Mặt tay cảnh sát kia xị ra, trong khi tất cả các bạn tù khác quanh tôi đều cười lớn.

Trở lại Los Angeles, tôi bị khép tội vi phạm các điều khoản trong lệnh quản chế với việc đã hack vào hòm thư thoại của nhân viên an ninh Pacific Bell, cùng với những vi phạm nhỏ hơn như liên hệ với Lewis De Payne.

Sau 10 tháng, hai nhân viên trợ giúp pháp lý đã tìm gặp tôi với một thỏa thuận nhận tội do công tố liên bang Schindler đề xuất. Tôi khó có thể tin được những gì mình đang nghe: Tám năm trong tù... và đó chưa phải là phần tệ nhất. Đây là thứ được gọi là “thỏa thuận nhận tội không ràng buộc”, tức là thẩm phán sẽ không bị ràng buộc bởi kiến nghị của bên công tố, mà thay vào đó, họ sẽ được tự do đưa ra một án tù cứng rắn hơn rất nhiều. Tệ hơn nữa, tôi sẽ phải đồng ý chi trả hàng triệu đô-la tiền bồi thường, một con số có lẽ còn nhiều hơn tổng số tiền tôi có thể kiếm được trong suốt phần đời còn lại của mình. Và tôi sẽ phải đưa một phần lợi nhuận từ việc kể lại câu chuyện

https://thuviensach.vn

của mình cho các "nạn nhân" hacking của tôi – Sun, Novell, Motorola, v.v….

John Yzurdiaga và Richard Steingard đúng là hai luật sư tận tụy, họ đã dành rất, rất nhiều thời gian để bào chữa cho tôi không công. Tuy vậy, tôi đã được đề nghị một thỏa thuận tệ đến mức không thể tin được. Rõ ràng, tôi cần lời bào chữa hùng hồn hơn tại tòa hoặc phải làm việc để có một thỏa thuận tốt hơn với chính phủ.

Vấn đề là giờ tôi đang không dư dả tài chính để thuê luật sư. Trái khoáy thay, nếu thực sự đã sử dụng 20.000 thẻ tín dụng kia trước khi bị bắt, tôi đã có thể thuê một luật sư với nguồn lực dồi dào bào chữa cho mình tại phiên xử hay tìm ra các lỗ hổng trong luận điểm của bên công tố nhằm thu được những điều khoản dàn xếp tốt hơn rất nhiều.

Trong lúc tôi cân nhắc nên làm gì, Bonnie đến thăm và nói với tôi rằng luật sư của Lewis De Payne, Richard Sherman, sẵn sàng đại diện cho tôi miễn phí. Cô ấy khẳng định ông ta muốn giúp vì không nghĩ rằng chính phủ đã khởi tố vụ của tôi một cách công bằng và ông ta tin tôi cần một luật sư hiếu chiến.

Nghe thì hay nhưng tôi vẫn thận trọng. Sherman không chỉ là luật sư của Lewis mà còn là bạn của cậu ta. Dù vậy, ông ta đã tự đến gặp tôi và nói rất thuyết phục về việc sẽ thắng phiên xử. Sau khi cân nhắc lựa chọn thỏa thuận tối thiểu tám năm và bàn bạc với gia đình, tôi quyết định chấp nhận lời đề nghị của Sherman.

Trong vài tuần, ông ta không làm gì với vụ của tôi ngoại trừ yêu cầu tòa cho tôi thêm thời gian nghiên cứu trong thư viện luật của nhà tù, một yêu cầu đã bị từ chối ngay lập tức. Lời bào chữa hiếu chiến ông ta hứa hẹn cũng chưa bao giờ thành hiện thực. Ông ta nhận vụ của tôi và gần như án binh bất động.

https://thuviensach.vn

Không lâu sau khi ông ta trở thành luật sư chính thức của tôi, tôi đã phát hiện ra quy mô của trò lừa đảo này. Một hôm, khi tôi gọi cho Sherman để bàn bạc về vụ án, Ron Austin đã trả lời điện thoại. Tôi nhận ra giọng nói này. Austin là kẻ chỉ điểm đã ghi âm các cuộc gọi của tôi và gửi tới đặc vụ FBI Ken McGuire.

Sherman nhanh chóng trấn an tôi rằng Ron không hề tiếp cận được hồ sơ vụ án của tôi, nhưng đó không phải là vấn đề. Những người này không đứng về phía tôi. Khi nhận ra điều này, tôi giận tím mặt một phần vì Sherman đã hứa lèo về một phiên bào chữa hiếu chiến, một phần vì bản thân đã tin lời ông ta.

Sherman không giống như bất kỳ luật sư đúng mực nào, thay vì cãi lý cho lệnh tha của tôi, ông ta thực ra lại yêu cầu chính phủ truy tố tôi: “Nếu các ông có gì chống lại thân chủ của tôi, cứ truy tố anh ta và hãy ra tòa,” ông ta khăng khăng. Một luật sư bào chữa làm như vậy có vẻ thật xấc xược. Nhưng đó chính xác là những gì chính phủ đã làm.

Vào 26 tháng 9 năm 1996, sau khi bị giam giữ hơn một năm rưỡi, tôi bị truy tố bởi bồi thẩm đoàn ở Los Angeles cho 25 tội danh, bao gồm lừa đảo qua mạng và máy tính (sao chép mã nguồn độc quyền), tàng trữ thiết bị truy cập (mật khẩu máy tính), phá hoại máy tính (cài cửa hậu) và lấy trộm mật khẩu. Tất nhiên, tội danh này bao gồm cả nhóm tội danh ban đầu về nhái điện thoại di động từ Raleigh.

Với một bị cáo nghèo khổ bần cùng – chính là tôi – thẩm phán cũng có thể ra lệnh cho một luật sư công liên bang được giao hoặc tìm đến những người được gọi là “ban luật sư”. Đây là những luật sư làm việc tư thường nhận những bị cáo khốn cùng chỉ với một phần nhỏ thù lao so với những gì một luật sư tên tuổi sẽ nhận (ngày đó, giá cho “ban luật sư” là 60 đô-la một giờ). Một luật sư trong ban, Donald Randolph, được chọn để xử lý trường hợp của tôi và những đơn kiện mới này sẽ do thẩm phán William Keller xét xử. Ông ta thường được đồn là “Keller sát thủ”, bởi những người quen mặt trong phòng xử án đều nói rằng nếu một bị cáo thiếu may mắn đến mức phải

https://thuviensach.vn

chịu kết tội trong phiên tòa của ông ta, hoặc thậm chí là cả những người đã nhận tội, đều có thể sẽ phải chịu mức án tối đa. Keller sát thủ là "quan tòa treo cổ" của Tòa án Trung tâm Bang California. Ông ta là cơn ác mộng kinh hãi nhất của mọi bị cáo.

Nhưng tôi vẫn chưa đến nỗi đường cùng. Những vụ khác của tôi sẽ do thẩm phán Mariana Pfaelzer xét xử. Đây chính là vị thẩm phán chịu trách nhiệm cho việc tôi bị biệt giam hơn tám tháng qua, nhưng ít ra bà ta không có danh tiếng đáng sợ như Keller sát thủ. Tôi thực sự đã tránh được một viên đạn ở đây.

Luật sư Randolph nhờ thẩm phán Pfaelzer chuyển vụ án mới về chỗ bà ta theo "luật số thấp" (cho phép các vụ liên quan đến nhau được gộp lại và được xét xử bởi thẩm phán đang giải quyết vụ có số sổ ghi án thấp nhất – tức là thẩm phán được giao trách nhiệm sớm nhất). Bởi các vụ án này đều liên quan đến nhau, nên bà ta đồng ý. Chín tháng sau khi tôi bị truy tố 25 tội, các tội nhỏ hơn – những cáo buộc ở Raleigh và lệnh quản chế – cuối cùng đã được dàn xếp xong. Tôi bị tuyên án 22 tháng tù. Tôi đã bị giam nhiều hơn án bốn tháng. Luật sư Randolph ngay lập tức yêu cầu một phiên tòa xét xử việc giam giữ, bởi giờ đây tôi đã có thể được tại ngoại. Tòa án tối cao đã tuyên rằng tất cả bị cáo đều có quyền có một phiên xử xét duyệt việc bảo lãnh.

Khi luật sư của tôi nói với thẩm Phán Pfaelzer rằng ông ta đã nộp đơn xin bảo lãnh để buổi xét xử diễn ra vào tuần sau, bên công tố đã phản đối, họ gọi tôi là kẻ "có nguy cơ bỏ trốn và là mối hiểm họa cho cộng đồng". Thẩm phán trả lời: "Tôi sẽ không cho anh ta được bảo lãnh đâu, không việc gì phải xử cả... Hãy xóa nó khỏi lịch đi."

Có thể coi đây là một sự phủ nhận trắng trợn những quyền được nêu trong hiến pháp của tôi.

Theo luật sư của tôi, chưa từng có ai trong lịch sử nước Mỹ bị từ chối tại một phiên tòa xét duyệt bảo lãnh. Kể cả kẻ mạo danh và nghệ sĩ trốn chạy

https://thuviensach.vn

khét tiếng Frank Abagnale Jr. Kể cả kẻ giết người hàng loạt và ăn thịt người Jeffrey Dahmer. Kể cả kẻ theo đuôi điên dại và sau này là kẻ ám sát Tổng thống John Hinckley Jr.

Như thể chưa đủ tồi tệ, tình huống của tôi còn nhanh chóng trở nên xấu hơn nữa. Một bị cáo có quyền được xem các bằng chứng mà bên công tố định dùng để chống lại anh ta trước tòa. Nhưng tại phiên tòa, các luật sư của chính phủ liên tục đưa ra lý do để không cung cấp chứng cứ cho luật sư của tôi. Hầu hết các chứng cứ có liên quan đều ở dạng điện tử – các tập tin thu được từ máy tính của tôi, các đĩa mềm và băng lưu trữ chưa mã hóa.

Luật sư của tôi sau đó đã xin thẩm phán cho phép ông mang một chiếc laptop vào trong khu thăm nom của nhà tù để có thể cùng xem các bằng chứng điện tử với tôi. Một lần nữa thẩm phán Pfaelzer lại từ chối yêu cầu này và nói thêm rằng: “Không đời nào chúng tôi làm vậy.” Rõ ràng bà ta tin rằng chỉ cần ngồi trước máy tính, ngay cả dưới sự giám sát của luật sư, tôi vẫn có thể bằng cách nào đó gây ra những thiệt hại khủng khiếp. (Vào năm 1998, Internet không dây còn chưa xuất hiện, nên việc tôi kết nối Internet bằng không khí là bất khả thi. Nhưng bà ta đơn giản là không có đủ kiến thức để hiểu được cách thức máy tính hoạt động cũng như không hề có bất kỳ khái niệm gì về việc liệu tôi có thể kết nối ra thế giới bên ngoài hay không.) Ngoài ra, các công tố viên tiếp tục cảnh báo vị thẩm phán rằng tôi có thể tiếp cận được mã nguồn độc quyền của các nạn nhân, hay tôi có thể viết một virus máy tính và bằng cách nào đó phát tán nó ra ngoài. Kết quả là, chúng tôi không được xem xét bất kỳ chứng cứ điện tử nào chống lại tôi, những thứ vốn là mấu chốt trong vụ án của chính phủ. Khi luật sư của tôi nhờ tòa án ra lệnh cho chính phủ in các tập tin ra, bên công tố nói rằng chúng quá nhiều, nhiều đến mức sẽ lấp đầy cả phòng xử án, vì thế thẩm phán lại tiếp tục từ chối ra lệnh cho chính phủ.

Khi tin tức về tình cảnh bất công của tôi lan đi, Eric Corley đã tập hợp một nhóm những người ủng hộ. Họ đã viết bài đăng trên các trang web, lan truyền tin tức trong cộng đồng mạng, rải truyền đơn và dán những miếng

https://thuviensach.vn

sticker vàng đen với dòng chữ: “Hãy trả tự do cho Kevin” lên khắp nơi. Eric cũng gửi cho tôi mấy cái trong tù.

Vào sinh nhật thứ 35 của tôi, trong lúc tôi đang bị giam giữ tại Trung tâm Giam giữ Đô thị ở Los Angeles, những người ủng hộ muốn đến thăm tôi, nhưng vì là một người bị giam trước khi xử án, tôi chỉ được phép gặp người thân trong gia đình và tư vấn viên pháp lý của mình.

Khi tôi nói chuyện với Eric trên điện thoại, tôi bảo anh rằng mình sẽ đến thư viện luật trên tầng ba trung tâm giam giữ vào đúng 1 giờ 30 chiều. Eric và những thành viên của cuộc vận động “Hãy trả tự do cho Kevin” đã tìm đến ô cửa sổ đó và sắp xếp đứng bên kia đường. Và khi các lính canh không để ý, tôi sẽ áp tấm sticker: “Hãy trả tự do cho Kevin” lên cửa sổ. Eric đã chụp lại một bức ảnh về sau được dùng làm bìa đĩa cho bộ phim tài liệu của anh về vụ án của tôi có tên Freedom Downtime (tạm dịch: Tự do mất đi).

Một thời gian sau, đám đông bắt đầu biểu tình phía bên kia con đường của trung tâm giam giữ. Tôi nhòm ra ngoài cửa sổ phòng của một phạm nhân khác để thấy đoàn người trên phố phía dưới: Một hàng người đang giơ khẩu ngữ in màu vàng và đen lớn: “Hãy trả tự do cho Kevin” cùng những bảng hiệu: “Hãy trả tự do cho Kevin.” Rõ ràng chuyện này đã khiến các nhân viên nhà tù lo lắng. Không lâu sau, toàn bộ nhà tù bị khóa kín vì “những lý do an ninh”.

Khi công chúng càng chú ý tới vụ án của tôi, gần hai năm sau khi luật sư của tôi yêu cầu chính phủ đưa ra các chứng cứ, thẩm phán Pfaelzer cuối cùng đành phải xuống nước và cho tôi dùng một chiếc laptop để xem xét các chứng cứ với luật sư của mình. Tôi chưa bao giờ biết điều gì đã khiến bà ta thay đổi ý kiến. Có thể là một thẩm phán khác đã chỉ ra rằng bà ta đang đánh liều với việc kháng cáo. Hoặc có thể ai đó đã giải thích rằng khi không có kết nối từ laptop đến modem và đường dây điện thoại, tôi sẽ không có cách nào phá hỏng bất kỳ thứ gì.

https://thuviensach.vn

Mỗi khi ở phòng xử án tại các phiên xử, tôi đều để ý thấy cảnh sát tư pháp sẽ quay phù hiệu của họ đi bất cứ khi nào lại gần tôi. Luật sư và tôi đều băn khoăn không biết chuyện đó nghĩa là gì. Sau đó, khi luật sư đến thăm tôi tại buồng giam của phòng xử, ông để ý thấy một số chữ bị tô bút xóa trên tờ khai mà ông phải ký. Khi soi nó dưới ánh đèn, vị luật sư có thể nhìn thấy phần chữ in trên giấy. Ông lắc đầu và bảo tôi: “Cậu sẽ không tin chuyện này đâu.” Rồi ông đọc những dòng chữ bị xóa cho tôi nghe:

Hãy lưu ý trong trường hợp Mitnick bị đưa vào phòng giam, hắn ta sở hữu khả năng phi thường có thể phá hoại đời sống cá nhân của một người thông qua kiến thức về máy tính , ví dụ, các thông tin của TRW, dịch vụ điện thoại, v.v… Hãy hành xử cẩn trọng và đừng để lộ bất kỳ thông tin cá nhân nào.

Thật không thể tin được! Tôi đoán họ thực sự nghĩ tôi có phép thuật.

* * *

Huyền thoại về Kevin Mitnick tiếp tục có thêm một diễn biến xấu. Trước khi vụ án được đưa ra tòa, Markoff và Shimmy đã kiếm tiền từ câu chuyện của tôi. Họ cùng viết một cuốn sách vào năm 1996 và giờ đã bán bản quyền chuyển thể thành bộ phim Takedown (tạm dịch: Hạ gục).

May mắn thay, một trong những nhà thiết kế trang phục cho bộ phim đã tiết lộ kịch bản một phân cảnh củaTakedown cho tạp chí 2600. Khi đọc kịch bản, tôi thực sự lộn ruột. Các nhà biên kịch đã biến tôi thành một kẻ phản diện độc ác và để tôi làm những việc mà mình chưa bao giờ làm trong đời thực, ví như hack vào các bệnh viện và làm nguy hiểm đến tính mạng bệnh nhân thông qua việc thay đổi bệnh án của họ. Thật kinh hoàng!

Một cảnh đặc biệt lố bịch thậm chí còn mô tả tôi đã hung hãn tấn công Shimmy bằng việc lấy nắp thùng rác bằng kim loại và đập vào đầu gã liên tục. Thú thực, tôi không thể tưởng tượng nổi liệu có ai trong hai chúng tôi sẽ tham gia vào một cuộc chiến lố bịch đến vậy.

https://thuviensach.vn

Khi đọc được kịch bản, Eric Corley đã viết trên mạng rằng nó "còn tồi tệ hơn rất nhiều so với những gì tôi tưởng tượng". Nếu kịch bản này được dựng thành phim, anh nói: "Kevin sẽ mãi là một con ác quỷ trong mắt công chúng." Trong một bài báo cho ZDTV, Kevin Poulsen đã viết:

Không ai có thể lường trước được rằng kịch bản này, đáng ra phải dựa trên cuốn sách cùng tên khô khan nhưng vô hại, lại chứa đầy những điều đơm đặt trắng trợn đến vậy. Không ai có thể ngờ tới việc Kevin Mitnick có thể trở thành một nhân vật phản diện đáng sợ và bị căm ghét nhất trên màn ảnh kể từ sau thời Hannibal Lecter.

Kinh hãi với hình ảnh sai lệnh về tôi trong kịch bản phim, những người ủng hộ tôi đã đến biểu tình tại Miramax Studios ở New York vào ngày 16 tháng 7 năm 1998. Eric Corley đã vạch trần sự thật rằng kịch bản này chỉ toàn những điều dối trá bịa đặt trước truyền thông quốc tế. Eric cũng chịu trách nhiệm loan tin rằng bộ phim có thể làm phát sinh các vấn đề tự do dân sự cho vụ án của tôi. Tất cả chúng tôi đều quan ngại rằng bộ phim sẽ gây ra định kiến cho phiên tòa xử tôi.

Trong một cuộc điện thoại khi tôi vẫn đang bị giam giữ chờ xét xử, Alex Kasperavicius nói rằng Brad Weston, một trong những nhà sản xuất của Takedown, rất nóng lòng được nói chuyện với tôi. Tôi đồng ý để Alex mời Weston vào nói chuyện tay ba trong cuộc gọi của chúng tôi. Brad nói ông ta muốn tôi cộng tác với bộ phim. Ông ta cũng nói Skeet Ulrich, người đã được chọn để đóng vai tôi, muốn nói chuyện với tôi.

Tôi bảo Brad rằng tôi đã đọc kịch bản và thấy nó hầu như chỉ toàn bịa đặt và phỉ báng. Tôi nói mình đang định thuê luật sư. Brad nói công ty sản xuất rất vui lòng trả tiền luật sư cho tôi; họ muốn dàn xếp vụ việc với tôi càng sớm càng tốt, thay vì chịu rủi ro khi phiên tòa có thể trì hoãn thời điểm ra mắt bộ phim.

https://thuviensach.vn

Hai luật sư chuyên xử lý các vụ bôi nhọ nổi tiếng ở Los Angeles, Barry Langberg và Debbie Drooz, đã giúp tôi xóa đi một số điều bịa đặt ngớ ngẩn trong kịch bản, dù không phải tất cả. Họ cũng giúp tôi lấy được một khoản tiền dàn xếp khá lớn, dù tôi không được phép nói chi tiết hơn.

Dù vụ dàn xếp diễn ra trước khi vụ án hình sự của tôi được giải quyết, tôi vẫn có đôi chút lo lắng rằng thẩm phán có thể tịch thu số tiền này như một phần trong khoản chi trả bồi thường của tôi. Luật sư của tôi đã kê khai khoản thu này trước ống kính (ý chỉ trước mặt thẩm phán) và thẩm phán đã đồng ý để tôi được giữ bí mật về nó. Vì vậy, các công tố viên chưa bao giờ biết tôi đã nhận được tiền từ các nhà sản xuất bộ phim.

Cuối cùng, phiên bản điện ảnh của Takedown vẫn bị ném đá tới tấp do chính chất lượng của nó khiến bộ phim chưa bao giờ được công chiếu tại các rạp chiếu ở Mỹ. Theo tôi tìm hiểu, sau vài cố gắng không đáng kể ở Pháp, bộ phim đành phải được phát hành thẳng trên DVD.

Cùng lúc đó, luật sư của tôi đã kháng án "không xử bảo lãnh" của thẩm phán Pfaelzer đến Tòa Phúc thẩm Liên bang Khu vực 9, theo nguồn ý kiến không công khai, tôi được cho là kẻ có nguy cơ bỏ trốn và là một mối nguy hiểm cho cộng đồng. Chúng tôi đem việc này lên tận Tòa án Tối cao, cùng việc luật sư của tôi gửi hồ sơ đến chánh án John Paul Stevens. Ông ta lấy làm thích thú và và đề nghị vụ việc của tôi cần được đưa ra xét xử, nhưng khi Stevens gửi nó cho toàn thể tòa để quyết định việc lên lịch, thì các đồng sự của ông đã không đồng ý.

Không lâu sau đó, tôi được đánh động rằng bên công tố đang lập luận con số thiệt hại do tôi gây ra lớn đến mức không hình dung nổi: hơn 300 triệu đô-la. Tất nhiên, chẳng có căn cứ nào cho con số này. Luật sư của tôi nhanh chóng chỉ ra rằng Ủy ban Chứng khoán yêu cầu các tập đoàn phải báo cáo các khoản thất thoát vật chất cho các nhà đầu tư, nhưng không có công ty nào trong số đó đưa ra được bất kỳ báo cáo quý hay năm nào khẳng định thất thoát dù chỉ một xu vì hậu quả hacking của tôi.

https://thuviensach.vn

Chỉ vài tuần sau khi tôi bị bắt, đặc vụ FBI Kathleen Carson đã đưa ra những con số thiệt hại phóng đại kia. Bản ghi nhớ nội bộ của Sun Microsystems cho thấy cô ta đã nói với Lee Patch, phó phòng Tư pháp của Sun, rằng mã nguồn Solaris mà tôi đã sao chép có thể được định giá 80 triệu đô-la, tương đương với mức án cao nhất dành cho tội danh lừa đảo xét theo hướng dẫn kết án của Liên bang – vì vậy, không cần phải là thiên tài mới biết cô ta lấy những con số đó từ đâu. Khi yêu cầu Sun đưa ra số tiền thiệt hại liên quan đến vụ đột nhập, cô ta đã khuyên họ rằng con số này nên dựa trên giá trị của mã nguồn.

Như thể khi bạn bắt ai đó vì tội lấy trộm một lon Coca và yêu cầu anh ta phải hoàn trả chi phí phát triển công thức bí mật của Coca-Cola vậy!

Ai đó ở FBI đã quyết định rằng cách tốt nhất để thổi phồng yêu cầu bồi thường thiệt hại là để các công ty báo cáo xem họ đã tốn bao nhiêu tiền để phát triển các phần mềm mà tôi đã sao chép. Nhưng họ vẫn có phần mềm của họ. Họ không bị tước đoạt nó, vì vậy việc khẳng định thất thoát bằng chi phí phát triển phần mềm là không công bằng. Con số hợp lý được đưa ra nên là giá trị của giấy phép mã nguồn, có lẽ là chưa tới 10.000 đô-la.

Dù các công ty muốn trừng phạt tôi đến thế nào đi nữa, chúng ta đều biết thiệt hại thực sự của họ còn nhỏ hơn rất, rất nhiều so với con số họ đang dẫn ra. Nếu có, chúng sẽ bao gồm chi phí thời gian dùng để điều tra vụ đột nhập của tôi, cài lại hệ điều hành và phần mềm ứng dụng trên những hệ thống tôi đã xâm nhập cùng các khoản tiền giấy phép họ thường thu của khách hàng mua giấy phép sử dụng mã nguồn.

Con số 300 triệu đô-la thiệt hại chống lại tôi điên rồ đến mức nó đã kích động những người ủng hộ tôi đẩy mạnh cuộc vận động: “Hãy trả tự do cho Kevin”. Mỗi khi chính phủ có động thái gì đó có vẻ không công bằng, số người ủng hộ tôi lại càng tăng thêm. “Hãy trả tự do cho Kevin” giờ đã trở thành phong trào đại chúng phát triển lan khắp cả nước – thậm chí nó còn vươn đến cả nước Nga xa xôi!

https://thuviensach.vn

Khi Eric tổ chức biểu tình, phóng sự truyền hình sẽ truyền đi hình ảnh đám đông diễu hành với bảng biểu: “Hãy trả tự do cho Kevin” bên ngoài tòa án liên bang ở 15 thành phố khác nhau, từ Portland, Maine, đến Los Angeles, từ Spokane đến Atlanta và ở Moscow, ngay gần Kremlin. Eric đã tóm tắt lại sự bất công tôi phải chịu đựng trên tạp chí 2600 như sau:

Từ ngày 15 tháng 2 năm 1995, Mintick đã bị giam trong khu tiền xử án mà không được xử bảo lãnh vì tội tàng trữ phần mềm được cho là trị giá hàng triệu đô-la. Tuy nhiên, các công ty khẳng định con số này chưa từng chứng minh được lời khẳng định hay báo cáo lại các “thất thoát” này cho cổ đông của mình, như pháp luật yêu cầu. Các chuyên gia máy tính và pháp lý nhìn chung đều đồng ý rằng khả năng thực sự xảy ra tổn thất là rất thấp và con số khổng lồ kia không thể ngầm mặc định rằng tất cả các tập tin và nghiên cứu có liên quan đến chúng đã bị xóa sổ. Trên thực tế, chưa hề có một tổn thất nào như vậy được báo cáo. Vậy nhưng, Mitnick vẫn đang lĩnh án tù như thể những việc đó đã xảy ra vậy.

Những người ủng hộ tôi muốn chính phủ tôn trọng quyền được giả định là vô tội và quyền được có một phiên tòa công bằng trong một khoảng thời gian hợp lý theo như trong hiến pháp.

Theo như tôi hiểu, những người biểu tình “Hãy trả tự do cho Kevin” ở khắp các thành phố trên thế giới không hẳn nghĩ rằng tất cả đơn kiện phải bị bác bỏ và tôi phải được bước ra khỏi nhà tù bình an vô sự. Nhưng họ phản đối việc thiếu công bằng rõ ràng trong vụ việc: Việc từ chối xử bảo lãnh; việc lục soát và tịch thu trái phép; việc bị can thiếu quyền tiếp cận với bằng chứng; việc tòa từ chối trả phí cho các luật sư được chỉ định của tôi; trên thực tế, tòa đã không cử một người nào đại diện cho tôi trong suốt bốn tháng; cùng với đó là những báo cáo thiệt hại trị giá hàng trăm triệu đô-la từ việc sao chép mã nguồn.

Khi mọi người nhận ra chuyện gì đang diễn ra, áp lực ngày một tăng lên. Báo chí thường đưa tin về những cuộc biểu tình. Mọi người dán sticker

https://thuviensach.vn

“Hãy trả tự do cho Kevin” lên xe và kính cửa sổ. Thậm chí còn có cả những người đi ra đường mặc áo phông “Hãy trả tự do cho Kevin” hay đeo huy hiệu và cúc áo có khẩu hiệu tương tự.

Trong các cuộc biểu tình phản đối phiên tòa, tôi nhìn ra ngoài cửa sổ nhỏ trong buồng giam và thực sự còn thấy cả một chiếc máy bay kéo theo băng rôn “Hãy trả tự do cho Kevin”. Tôi đã phải tự cấu bản thân, không thể tin chuyện này đang xảy ra.

Bốn năm trước, tôi đã phải đương đầu với những phóng viên chỉ giỏi buông lời phỉ báng, những thẩm phán kém hiểu biết, những cảnh sát mê tín, những người bạn trục lợi và các nhà làm phim trục lợi chỉ mong muốn thổi bùng lên ngọn lửa về Huyền thoại Kevin Mitnick vì mục đích cá nhân. Ý nghĩ rằng ngoài kia vẫn còn những người có thể thực sự cảm thông với những gì tôi đang trải qua khiến tôi thấy rất dễ chịu.

Trên thực tế, nguồn cổ vũ động viên này đã thôi thúc tôi chuẩn bị cho cuộc chiến. Tôi đã tìm được một vụ gần đây trong thư viện luật của nhà tù khiến tôi tin rằng mình có thể đánh bại cả những lời buộc tội nghiêm trọng nhất.

Khi tôi nói với luật sư Donald Randolph rằng tôi đã tìm thấy một tiền lệ pháp lý có thể thay đổi mọi thứ, ông ấy nói: “Hãy để tôi lo việc đó, Kevin. Tôi là luật sư.” Nhưng khi nghe tôi kể về vụ án, ông ấy đã phải tròn mắt.

Năm 1992, một nhân viên thuộc Sở Thuế vụ tên là Richard Czubinski đã dùng quyền truy cập vào mạng nội bộ để lấy tờ khai thuế của rất nhiều nhà chính trị, người nổi tiếng và các quan chức chính phủ khác. Anh ta làm vậy chỉ vì tò mò. Sau đó, cũng giống như tôi, Czubinski bị kiện với tội danh lừa đảo qua mạng và máy tính, và bị kết án vào tháng 12 năm 1995. Sau khi bị kết án sáu tháng tù, anh ta đã kháng án thành công. Tòa thượng thẩm liên bang cho rằng Czubinski, giống như tôi, chưa bao giờ định sử dụng hay phát tán những thông tin đó mà chỉ đơn giản là tiếp cận nó để thỏa mãn tính tò mò của bản thân. Anh ta được xóa án và không còn phải ngồi tù nữa.

https://thuviensach.vn

Với tiền lệ rõ ràng như vậy, tôi tin chúng tôi sẽ có cơ hội để thắng vụ kiện của chính phủ. Tôi nóng lòng nói với luật sư rằng tôi muốn ra tòa. Chiến thuật tôi đề xuất là: Tôi sẽ nhận tội hacking nhưng sẽ lý luận rằng mình không phạm tội lừa đảo qua mạng hay máy tính bởi, giống như Czubinski, tôi đã làm những việc đó chỉ để thỏa mãn trí tò mò của bản thân.

Randolph đồng ý rằng vụ của Czubinski đã đặt ra một tiền lệ hoàn hảo cho phần biện hộ của tôi. Nhưng có một vấn đề lớn hơn. Randolph có vẻ hơi lưỡng lự trước khi bảo tôi đó là gì; tôi có thể thấy ông đang cố khéo léo che giấu. Có vẻ đây là lúc để ông nói ra điều chưa từng được tiết lộ.

Một trong các công tố viên chính phủ đã dành nhiều tuần để thúc giục luật sư của tôi hãy thuyết phục tôi đồng ý với thỏa thuận nhận tội. Vài ngày gần đây, ông ta thậm chí còn đưa ra tối hậu thư: Nếu tôi không đồng ý nhận tội và dàn xếp vụ án, chính phủ sẽ đưa tôi vào vòng xử án hình sự. Nếu thua ở một khu vực tài phán, họ sẽ thử ở một nơi khác; nếu thắng, họ sẽ ép tôi phải nhận án phạt ở mức tối đa. Họ có được lời tuyên án hay không không quan trọng bởi họ đã nhốt tôi mà không có bảo lãnh suốt thời gian qua.

Tôi đã sẵn sàng để chiến đấu. Nhưng luật sư khi đó của tôi lại bảo tôi một cách khéo léo hết mức có thể: “Tôi nghĩ cậu nên chấp nhận thỏa thuận nhận tội này.”

Ông ấy giải thích: “Nếu ra trước tòa, cậu sẽ phải làm chứng. Và việc đó sẽ khiến cậu phải tiến hành các bước kiểm tra chéo về những thứ khác...”

“Thứ khác” đó là câu chuyện hoang đường đã lưu truyền suốt nhiều năm về những vụ hacking của tôi, những tin đồn rằng tôi đã đột nhập vào CIA, FBI và cả NORAD. Chưa nói đến rất nhiều thứ tôi đã làm trong sự nghiệp hacking nhưng chưa bị buộc tội: thao túng bộ chuyển mạch của các công ty điện thoại trên khắp nước Mỹ; lấy thông tin từ DMV California; nghe lén các cuộc điện thoại của người đưa tin cho FBI; nghe lén tin nhắn hòm thư thoại của các nhân viên an ninh Pacific Bell. Và còn rất nhiều nữa.

https://thuviensach.vn

Tôi có thể hiểu Randolph muốn nói gì. Trong quá trình kiểm tra chéo của bên công tố, tôi sẽ phải đối mặt với các án phạt khác bởi chính phủ có thể hỏi tôi bất cứ điều gì có liên quan đến các hoạt động hacking nếu tôi đứng lên bục làm chứng trước tòa. Chúng tôi thực sự không muốn dây vào tất cả những thứ đó.

Vậy là tôi nhận tội với những điều khoản tốt hơn rất nhiều so với thỏa thuận nhận tội ban đầu tôi được đề nghị gần ba năm trước.

Điều kiện trong lệnh quản chế của tôi là: Trong vòng ba năm tới, tôi sẽ không được phép chạm vào bất kỳ thiết bị điện tử nào, ví dụ như máy tính, điện thoại di động, máy fax, máy nhắn tin, máy đánh chữ, v.v… nếu không có giấy phép viết tay từ Phòng Quản chế. Tệ hơn nữa, tôi không được tiếp xúc với máy tính qua bên thứ ba. Chính phủ thậm chí còn không muốn tôi được đặt vé máy bay nếu không hỏi xin phép trước. Tôi tự hỏi có thể tìm được việc bằng cách nào đây? Tôi cũng không thể tư vấn cho bất kỳ hoạt động nào có liên quan đến máy tính. Rất, rất nhiều các điều kiện trong lệnh quản chế của tôi khắt khe đến vô lý và một số quá chung chung đến mức tôi lo ngại không biết mình có vô tình vi phạm hay không.

Chính phủ đặt ra các điều kiện chung chung đó không chỉ để trừng phạt tôi, mà còn bởi họ đang cố bao quát hết các hạng mục để ngăn tôi tìm ra các lỗ hổng, các cách lách qua điều khoản hạn chế.

Cuối cùng, vào ngày 16 tháng 3 năm 1999, tôi cũng đồng ý ký thỏa thuận. Lần này, bên công tố đồng ý với một thỏa thuận nhận tội “ràng buộc”, có nghĩa là thẩm phán Pfaelzer sẽ phải kết án dựa trên những điều khoản tôi đã đồng ý, hoặc tôi có thể rút lại lời thú tội và ra tòa. Tôi nhận tội với bảy mục được các bên công tố ở Bắc và Nam California tự tay chọn (các khu vực tài phán khác cũng muốn tranh giành tôi), bao gồm lừa đảo trên mạng (tấn công bằng kỹ thuật xã hội với người khác qua điện thoại để lấy được mã nguồn), lừa đảo máy tính (sao chép mã nguồn), tàng trữ thiết bị truy cập (mật khẩu)

https://thuviensach.vn

và nghe lén trao đổi dữ liệu (cài đặt phần mềm đánh hơi mạng để lấy mật khẩu).

Trong quá trình bàn bạc thỏa thuận, bên công tố yêu cầu tôi phải trả 1,5 triệu đô-la tiền đền bù. May thay, luật liên bang bắt buộc tòa phải cân nhắc đến khả năng chi trả của tôi, vậy nên ngay cả khi thẩm phán Pfaelzer hằn là muốn trừng phạt tôi mạnh tay, bà ta vẫn phải cân nhắc đến thu nhập khả thi của tôi. Vì những điều kiện trong lệnh quản chế rất hà khắc, nên Phòng Quản chế tính toán rằng tôi sẽ chỉ có thể kiếm được một công việc với mức lương tối thiểu như đứng rán bánh kẹp. Do đó, thẩm phán Pfaelzer sẽ phải tính mức tiền đền bù dựa trên ước tính của Phòng Quản chế về mức lương tối thiểu của tôi trong thời hạn ba năm. Thay vì hàng triệu đô-la như đề xuất trước đó, tôi bị bắt phải trả 4.125 đô-la.

Sau khi được phóng thích, tôi nhờ cha đăng thẻ tù nhân Nhà tù Lompoc của tôi lên đấu giá trên eBay. Khi các quản trị viên của eBay xóa tin bởi nó không đáp ứng "các tiêu chuẩn cộng đồng"của công ty, họ đã giúp tôi một việc rất lớn. Hành động đó đã tạo ra một cơn sốt truyền thông. Câu chuyện kỳ quái này đủ sức để trở thành một tin nóng trên kênh truyền hình CNN. Sau đó, tôi lại tiếp tục đăng thẻ tù lên Amazon và tin đăng bán đó cũng bị xóa vì cùng một lý do (cảm ơn, Amazon!). Cuối cùng, một người đàn ông ở châu Âu đã đồng ý mua nó với giá tận 4.000 đô-la – nhiều hơn rất nhiều số tiền tôi hy vọng thu được.

Với nụ cười lớn trên môi, tôi đem chỗ tiền đến Phòng Quản chế, cộng với 125 đô-la, và trả hết khoản tiền đền bù. Tôi thích thú với ý nghĩ rằng việc này đã biến thẻ tù nhân ở Lampoc của tôi thành một dạng "thẻ ra tù miễn phí"[96].

[96] Kevin Mitnick để từ này trong ngoặc kép bởi đây cũng là một tấm thẻ trong trò chơi "Cờ tỷ phú" (thẻ ra tù). (ND)

https://thuviensach.vn

Chính phủ vô cùng phẫn nộ với màn phô trương nho nhỏ này: Cục Đặc trách Nhà tù Liên bang công khai nói rằng tấm thẻ là "tài sản của chúng tôi" và cố tìm cách lấy lại chỗ tiền. Tôi chưa bao giờ nghe thêm tin gì về vụ này.

Vào ngày 9 tháng 8 năm 1999, tôi chính thức bị kết án thêm 46 tháng tù, kế tiếp đó là 22 tháng tù vì đã vi phạm điều khoản quản chế và thực hiện các cuộc gọi miễn phí. Vì đã chờ đợi trong tù bốn năm rưỡi, nên thời gian của tôi gần như đã hết.

Vài tuần sau, tôi được chuyển đến Trại Giáo dưỡng Liên bang ở Lompoc, nơi tôi gặp ba người mặc com-lê. Về sau, tôi được biết họ là quản lý đơn vị, đội trưởng (Trưởng phòng An ninh nhà tù) và cai ngục. Tôi biết chuyện này hẳn không thường diễn ra với những tù nhân mới đến.

Hóa ra họ ở đó để cảnh cáo tôi hãy tránh xa máy tính và điện thoại. Nếu tôi ngứa tay nghịch ngợm đống thiết bị, họ nói, "anh sẽ phải trả giá đắt đấy!"

Rồi họ yêu cầu tôi phải tìm việc làm trong tù trong vòng 72 tiếng, nếu không họ sẽ giao việc cho tôi – "và sẽ không dễ chịu lắm đâu".

Khi trò chuyện với một tù nhân khác, tôi phát hiện ra một tin tức thú vị, nhà tù đang cần tuyển một tù nhân làm việc ở Phòng Viễn thông.

"Cậu có kinh nghiệm với điện thoại không, Mitnick?" giám sát viên hỏi.

"Không nhiều lắm," tôi nói. "Tôi biết làm thế nào để cắm dây vào lỗ. Nhưng đừng lo. Tôi học nhanh lắm."

Ông ta đề nghị đào tạo tôi.

Trong hai ngày, công việc trong tù của tôi ở Lompoc là cài đặt và sửa chữa điện thoại của nhà tù.

Đến ngày thứ ba, hệ thống loa gào tướng lên: "Mitnick đang đến văn phòng của Đơn vị quản lý. Mitnick đang đến văn phòng của Đơn vị quản lý."

https://thuviensach.vn

Nghe không ổn rồi. Khi đến đó, tôi lại đối diện với ba gã vận com-lê trong "Ủy ban chào đón" tôi và họ giận tím mặt. Tôi cố chứng minh rằng chính họ đã yêu cầu tôi tìm việc mới và giám sát Phòng Viễn thông đã nhận tôi.

Họ nổi điên.

Vài tuần sau, công việc mới của tôi là một trong những việc khủng khiếp nhất trong nhà tù: Rửa nồi và chảo trong nhà bếp.

Ngày 21 tháng 1 năn 2000, khi trời còn tờ mờ sáng, tôi được đưa đến Phòng Tiếp nhận và Phóng thích. Tôi đã hết hạn tù và chuẩn bị được thả. Nhưng tôi vẫn lo lắng.

Vài tháng trước, có một vụ kiện ở bang California về việc tôi đã thử lừa DMV gửi ảnh của Joseph Wernle, Joseph Ways và Eric Heinz (hay Justin Petersen) bị bác bỏ, nhưng nó vẫn khiến tôi bất an. Trong lúc chờ đến ngày tự do, tôi luôn lo rằng sẽ có một vài cơ quan bang hay chính phủ nào đó có thể đang rình rập ngoài cửa để bắt mình. Tôi đã nghe chuyện một vài tù nhân được phóng thích chỉ để bị bắt lại vì một tội danh khác ngay lúc anh ta vừa bước chân ra khỏi cửa nhà tù. Tôi lo lắng đến mức đứng ngồi không yên trong buồng giam và chờ đợi.

Cuối cùng cũng đến ngày được bước chân ra khỏi Lompoc, tôi không thể ngờ mình đã được tự do. Mẹ và dì Chickie đến đón tôi. Cha cũng muốn đến nhưng không thể vì ông vừa bị trụy tim và phải trải qua một cuộc phẫu thuật rồi lại bị nhiễm khuẩn tụ cầu nặng. Có một nhóm phóng viên và đội ngũ quay phim đợi sẵn ở đó. Eric Corley cùng một đám đông lớn, náo nhiệt gồm những người hâm mộ chiến dịch "Hãy trả tự do cho Kevin" cũng ở đó. Khi chúng tôi đứng nói chuyện, nhà tù đã sử dụng các phương tiện giải tán để xua chúng tôi ra xa khỏi khu vực này. Nhưng tôi chẳng hề bận tâm. Tôi cảm thấy mình như một con người mới. Liệu điều gì đang chờ đợi tôi phía trước, là lịch sử lặp lại hay thứ gì đó hoàn toàn khác?

https://thuviensach.vn

Hóa ra, chờ đợi tôi phía trước lại là một cuộc đời hoàn toàn mới mà tôi không bao giờ có thể tưởng tượng ra.

https://thuviensach.vn

38

HỒI KẾT: VẬN MỆNH ĐỔI CHIỀU

100-1111-10-0 011-000-1-111 00-0100 1101-10-1110-000-101-11-0-1 0111-110-00-1001-1-101 111-0-11-0101-010-1-101 111-10-0100 11-00-11

Không dễ gì mô tả cuộc đời tôi từ khi bước ra khỏi nhà tù, nhưng câu chuyện sẽ không hoàn chính nếu thiếu đi phần thông tin này.

Vào tháng 3 năm 2000, hai tháng sau khi tôi được thả, Thượng nghị sĩ Fred Thompson đã gửi thư tới và hỏi tôi có muốn bay tới Washington để làm chứng trước Ủy ban Thường vụ Quốc hội của Thượng viện Mỹ không? Tôi rất bất ngờ, vui sướng và lấy làm hãnh diện vì người của Chính phủ đã thừa nhận và tôn trọng kỹ năng máy tính của mình, đủ để muốn nghe ý kiến của tôi về cách bảo vệ mạng lưới và hệ thống máy tính của chính phủ. Tôi phải xin phép Phòng Quản chế để được bay tới Washington, D.C.; tôi ắt phải là một trong số ít người nằm trong quyền quản lý của họ, nếu không phải là trường hợp duy nhất, lấy lý do "làm chứng trước Ủy ban Thượng viện" để xin chấp thuận cho chuyến đi.

Chủ đề của buổi điều trần là "Tấn công mạng: Liệu Chính phủ có an toàn?" Jack Biello, bạn thân và cũng là một người ủng hộ tôi, một cây bút khá cừ, đã giúp tôi phác thảo bài phát biểu trên giấy.

Chúng ta đều đã thấy các buổi điều trần trên C-SPAN, nhưng việc được dẫn tới và ngồi yên ở đó, trước một sàn nâng với những gương mặt quen thuộc gồm các chính trị gia đứng đầu đất nước, đang nhìn chằm chằm xuống bạn và sẵn sàng nuốt lấy từng lời bạn nói – ừm, trải nghiệm này quả là kỳ diệu.

https://thuviensach.vn

Phòng họp kín người. Tôi là người làm chứng chính trong buổi lễ do Thượng nghị sĩ Fred Thompson làm chủ tọa. Ban hội thẩm gồm có các Thượng nghị sĩ Joseph Lieberman và John Edwards. Dù có chút lo lắng lúc đầu khi đọc lời làm chứng nhưng tôi đã lấy lại sự tự tin khi phần Hỏi Đáp diễn ra. Tôi đã hoàn thành xuất sắc nhiệm vụ ngoài mong đợi, thậm chí còn đưa ra vài lời nói đùa khiến mọi người phải phì cười. (Bạn có thể tham khảo trên mạng lời làm chứng của tôi dưới dạng văn bản tại địa chỉ: http://hsgac.senate.gov/030200_mitnick.htm.)

Sau bài phát biểu của tôi, Thượng nghị sĩ Lieberman đã đặt ra vài câu hỏi về lịch sử hacking của tôi. Tôi đáp lại và nói động cơ của tôi là học hỏi, không phải vì lợi ích hay ý định gây hại cho ai. Tôi nhắc tới trường hợp nhân viên Sở Thuế vụ, Richard Czubinski, đã lật ngược bản án của mình khi tòa án chấp nhận lý lẽ của anh ta rằng Czubinski tiếp cận các thông tin mật chỉ vì lòng hiếu kỳ; anh ta chưa từng có ý định sử dụng hay để lộ ra các thông tin đó.

Lieberman, hiển nhiên rất ấn tượng với lời khai và án lệ do chính tôi phát hiện ra, đã gợi ý rằng tôi có thể trở thành một luật sư.

“Với trọng tội mình đã mắc phải, tôi khó có thể trở thành một luật sư,” tôi nói. “Nhưng có lẽ một ngày nào đó, ngài sẽ đạt tới vị trí có thể xá tội cho tôi[97]!”

[97] Ý Mitnick muốn nói đến vị trí Tổng thống Mỹ. (ND)

Mọi người cười ồ lên.

Như thể có một cánh cửa phép thuật đã mở ra. Mọi người bắt đầu gọi cho tôi đặt lịch phát biểu. Tôi từng tuyệt vọng khi các lựa chọn công việc của mình bị giới hạn chặt chẽ trong điều khoản quản chế. Vậy mà giờ đây, sau buổi điều trần, khả năng về một công việc diễn thuyết kiếm bộn tiền bỗng đột nhiên xuất hiện.

https://thuviensach.vn

Vấn đề duy nhất là tôi mắc chứng sợ đứng trên sân khấu nghiêm trọng! Tôi phải mất rất nhiều giờ luyện tập cùng hàng nghìn đô-la trả cho huấn luyện viên diễn thuyết mới có thể vượt qua nỗi sợ này.

Tôi tham gia một câu lạc bộ Toastmaster[98] địa phương nhằm cố gắng làm quen với nỗi sợ khi phải phát biểu trước đám đông. Điều buồn cười là các buổi gặp của họ thường được tổ chức tại văn phòng chính của General Telephone ở Thousand Oaks, nơi tôi từng làm việc trong một thời gian ngắn. Thẻ qua cửa của Toastmaster cho tôi quyền tự do đi tới bất kỳ văn phòng nào trong tòa nhà. Tôi không thể nén nổi nụ cười mỗi khi bước vào đó, nghĩ tới việc mấy gã trong tổ An ninh phải hoảng loạn thế nào nếu biết được chuyện này. Một trong những lời mời phỏng vấn tôi nhận được khi đó đến từ Hội đồng An ninh Quốc gia Mỹ trong Thế kỷ XXI, nhóm cố vấn có nhiệm vụ đưa ra khuyến nghị về an ninh tới Quốc hội và Tổng thống. Có hai người thuộc Bộ Quốc phòng, đại diện cho hội đồng, đã tới nhà tôi ở Thousand Oaks và dành hai ngày để hỏi ý kiến của tôi về việc làm thế nào để hệ thống máy tính của chính phủ và quân đội Mỹ có thể an toàn hơn.

[98] Câu lạc bộ nơi các thành viên luyện tập diễn thuyết bằng tiếng Anh với các chủ đề nhất định và độ khó tăng dần. (ND)

Thật ngạc nhiên, tôi cũng được mời xuất hiện trong một số chương trình thời sự và chương trình nói chuyện trên truyền hình. Bỗng dưng tôi trở thành nhân vật nổi tiếng trên các phương tiện truyền thông, nhận lời phỏng vấn của các trang báo hàng đầu thế giới, bao gồm Washington Post, Forbes, Newsweek, Time, Wall Street Journalvà Guardian. Trang tin trực tuyến Brill’s Content còn đề nghị tôi nhận viết một chuyên mục hàng tháng. Dù tôi không được phép tới gần máy tính, nhưng những người ở Brill nói họ sẵn lòng nhận các bản thảo viết tay.

Cùng lúc đó, những lời mời làm việc lạ thường khác cũng ập tới. Một công ty bảo mật muốn tôi trở thành thành viên trong ban cố vấn và hãng phim

https://thuviensach.vn

Paramount còn mời tôi tới cố vấn cho một loạt ý tưởng về phim truyền hình mới của họ.

Sau khi nghe nói về các lời đề nghị này, viên quản chế của tôi, Larry Hawley, đã nhắc nhở tôi rằng tôi không được phép viết các bài báo về công nghệ máy tính hay tham gia vào bất kỳ dạng công việc nào có thảo luận tới vấn đề này. Anh ta khăng khăng nói Phòng Quản chế cho rằng tất cả công việc đó đều là hoạt động "tư vấn về máy tính", điều mà tôi không được phép làm nếu không có sự đồng ý của anh ta. Tôi phản đối rằng viết về chủ đề đó không có nghĩa rằng tôi là một cố vấn. Những bài báo này vốn được dành cho toàn công chúng. Tôi chỉ làm cùng một loại việc mà cựu hacker Kevin Poulsen đã làm khi cậu ta còn trong thời gian quản chế thôi.

Không nản lòng, tôi tìm đến cố vấn pháp lý. Sherman Ellison, một người bạn luật sư, đã đồng ý đại diện cho tôi miễn phí. Hiển nhiên, điều này đồng nghĩa với việc tôi sẽ phải đứng ra tự bào chữa trước thẩm phán Pfaelzer. Mối quan hệ pháp lý kéo dài suốt ba năm gần đây không mấy có tác dụng trong việc tăng cường thiện ý mà chúng tôi dành cho nhau. Không ai muốn gặp lại người kia.

"Tòa không hề nghi ngờ việc sẽ còn gặp lại ngài Mitnick một lần nữa," thẩm phán Pfaelzer nói. Dĩ nhiên, ý của bà ta là bà ta biết rõ sẽ còn gặp lại tôi khi tôi bị buộc thêm các tội mới, hay khi tôi tiếp tục vi phạm các điều luật quản chế. Nhưng cuối cùng, bà ta nói rằng các luật sư sẽ phải tự làm việc với nhau về vấn đề này và nhấn mạnh thêm bà ta không muốn nhìn thấy tôi trong phiên tòa một lần nào nữa. Bà ta phát chán các vụ của Mitnick rồi.

Phòng Quản chế nhận được tin nhắn: "Hãy linh hoạt trong các vấn đề liên quan đến Mitnick để hắn ta không còn xuất hiện trong lịch làm việc của chúng tôi một lần nữa." Phòng Quản chế bắt đầu hợp lý và dễ dãi hơn đối với tôi.

https://thuviensach.vn

Vào mùa thu năm 2000, ngay sau khi kết thúc buổi phỏng vấn trên chương trình chào buổi sáng nổi tiếng của Bill Handel trên đài phát thanh KFI-AM 640 của Los Angeles, tôi đã nói chuyện với Giám đốc Chương trình của đài, David G. Hall. Anh ấy nói rằng người dẫn chương trình trò chuyện quốc tế Art Bell sẽ sớm về hưu và muốn giới thiệu tôi với công ty sản xuất, Premiere Radio Networks, để thay thế David Hall. Một lời ca ngợi quá bất ngờ! Tôi choáng váng. Phải thừa nhận rằng tôi không có chút kinh nghiệm nào trong việc dẫn chương trình trò chuyện trên sóng phát thanh và thực ra tôi còn chưa từng nghe bất kỳ chương trình nào, nhưng tôi vẫn nói mình sẵn sàng thử sức.

Vài ngày sau, tôi thử sức trong vai trò khách mời của chương trình Tim & Neil và David đã đề nghị tôi thực hiện một chương trình của riêng mình có tên là The Darkside of the Internet (tạm dịch: Góc khuất của Internet). Sau đó, tôi rủ anh bạn thân Alex Kasperavicius cùng dẫn chương trình với mình. Chúng tôi đã lột trần những góc khuất trên mạng Internet, nhắc nhở người nghe về việc bảo vệ sự riêng tư cũng như trả lời các câu hỏi do thính giả của chương trình gửi tới xin được tư vấn cách bảo mật máy tính cá nhân cùng nhiều vấn đề khác nữa. Chúng tôi cũng nói về tất cả các dạng trang web và dịch vụ thú vị đang dần xuất hiện trên mạng.

David Hall, một lãnh đạo có tiếng trong giới truyền thanh, đã cho tôi lời khuyên chỉ có ba từ: một chương trình cần phải có tính giải trí, thích hợp và giàu thông tin. Ngay lập tức, tôi mời các khách mời như Steve Wozniak, John Draper và thậm chí cả ngôi sao phim khiêu dâm Danni Ashe, người đã lột cả áo ngay tại trường quay để chứng tỏ mình nóng bỏng cỡ nào. (Nghe này, Howard Stern, tôi đang theo bước anh đó!)

Do tôi không được phép sử dụng máy tính, đài phát thanh đã rất tốt bụng cử riêng một nhà sản xuất hỗ trợ tôi, người này vừa đảm nhận các nhiệm vụ thông thường vừa giúp tôi tìm hiểu thông tin trên Internet. Chương trình dài cả tiếng đồng hồ cứ lên sóng đều đặn vào mỗi Chủ nhật. Trong suốt thời gian đó, đài phát thanh từ vị trí xếp hạng thứ 14 trên Aibitron[99] đã nhảy lên

https://thuviensach.vn

đứng thứ hai. Bất chấp giả định mà thẩm phán Pfaelzer đã dùng để tính toán khoản tiền tôi có thể bồi thường trước đó, tôi kiếm được tới 1.000 đô-la cho mỗi chương trình.

[99] Công ty nghiên cứu người dùng tại Mỹ, chuyên thu thập dữ liệu trên đài phát thanh và sử dụng các dữ liệu này để cung cấp dịch vụ xếp hạng phát thanh. (BTV)

Trong quá trình làm việc với cương vị người dẫn chương trình trò chuyện, J. J. Abrams, nhà sản xuất phim và truyền hình nổi tiếng, đã liên lạc với tôi. Anh nói anh là người hâm mộ của tôi và thậm chí còn từng đặt một sticker "Hãy trả tự do cho Kevin" trên xe ô tô trong loạt phim truyền hình mang tên Felicity (tạm dịch: May mắn) của mình. Sau khi gặp nhau ở một studio tại Burbank, anh đã mời tôi vào vai diễn khách mời, đặc vụ FBI, cho chương trình Alias (tạm dịch: Bí danh) của anh, một cách chọc cười tinh tế. Cuối cùng, khi kịch bản chương trình thay đổi, tôi đã vào vai một đặc vụ CIA làm việc chống lại kẻ phản bội SD6.

Chính phủ liên bang không cho phép tôi gõ máy tính thực sự trong khi quay phim, do đó, tổ đạo cụ phải đảm bảo rằng bàn phím máy tính phải được ngắt kế nối. Tôi xuất hiện trong cảnh quay cùng với Jenifer Garner, Michael Vartan và Greg Grunberg. Thật tuyệt vời – đó quả là một trong những trải nghiệm thú vị nhất mà tôi từng có.

Khoảng mùa hè năm 2001, tôi nhận được cuộc gọi từ một người đàn ông có tên là Eddie Muñoz. Anh ta đã tìm hiểu về quá khứ hacking của tôi và muốn thuê tôi giải quyết một vấn đề bất thường. Dịch vụ cung cấp "vũ công tay vịn" qua điện thoại ở Las Vegas của anh ta vốn vô cùng ăn nên làm ra nay lại sụt giảm khách hàng một cách đáng kể. Eddie cảm thấy chắc chắn là Mafia đã tấn công vào bộ chuyển đổi điện thoại của Sprint và tái lập trình nó để hầu hết các cuộc gọi tới dịch vụ của Eddie sẽ bị chuyển hướng tới dịch vụ gái gọi do nhóm Mafia dẫn dắt.

https://thuviensach.vn

Muñoz đã gửi khiếu nại lên Hội đồng các Ngành dịch vụ Công (PUC) nhắm vào Sprint, cho rằng ngành kinh doanh của anh ta đang phải chịu thiệt hại nặng nề bởi công ty Sprint đã không có chế độ an ninh thích đáng đối với cơ sở hạ tầng của mình nhằm chống lại các hacker. Muñoz muốn thuê tôi làm chứng trước tòa trong vai trò chuyên gia máy tính. Tôi khá nghi ngờ việc Sprint phải chịu trách nhiệm cho việc sụt giảm thu nhập của Eddie, nhưng cũng đồng ý đứng ra làm chứng về những thiếu sót trong bảo mật của họ.

Trong suốt phiên tòa, tôi đã mô tả lại việc mình đã tấn công vào các công ty điện thoại trong nhiều năm ra sao, bao gồm cả Sprint. Tôi giải thích rằng hệ thống CALRS mà Sprint sử dụng để kiểm tra cũng tương tự như hệ thống SAS của Pacific Bells, nhưng có khả năng bảo mật tốt hơn: Bất kỳ ai có ý định thâm nhập vào thiết bị kiểm tra CALRS từ xa ở các văn phòng trung tâm sẽ phải cung cấp được đáp án chính xác cho những thử thách mà hệ thống đưa ra. Hệ thống được lập trình với 100 thử thách khác nhau – gồm số hai ký tự từ 00 đến 99, mỗi câu hỏi tương ứng với một đáp án riêng gồm các cụm bốn ký tự như b7a6 hoặc dd8c. Không dễ gì vượt qua được… trừ khi đặt máy nghe lén hoặc tấn công bằng cách sử dụng kỹ thuật xã hội.

Tôi nói với hội đồng, cách tôi đã vượt qua thử thách này là gọi điện tới Northern Telecom, nhà sản xuất của hệ thống, giả vờ là một nhân viên phòng kỹ thuật của Sprint, rồi nói rằng tôi đang xây dựng một công cụ kiểm tra tùy chỉnh cần phải kết nối với thiết bị kiểm tra CALRS trong các văn phòng trung tâm. Tay kỹ thuật viên đã gửi fax cho tôi một “danh mục” liệt kê tất cả 100 câu hỏi cùng đáp án tương ứng.

Một trong các luật sư của Sprint phản bác lại lời khai của tôi: “Mitnick là người tấn công bằng kỹ thuật xã hội, nói dối là một phần công cụ kiếm ăn của anh ta, quý tòa không thể tin những gì anh ta nói được.” Không chỉ phủ nhận hoàn toàn việc Sprint từng bị tấn công hay có thể bị tấn công trong tương lai, gã luật sư còn chỉ ra rằng tôi chính là người đã viết “cuốn sách về nói dối”: The Art of Deception (tạm dịch: Nghệ thuật dối lừa) (tôi sẽ nói thêm về cuốn sách này sau).

https://thuviensach.vn

Một trong những nhân viên của PUC đối chất với tôi và nói: “Anh đã đưa ra tất cả lập luận này, nhưng chưa có lấy một mẩu bằng chứng nào. Anh có cách nào để chứng minh rằng Sprint có thể bị tấn công không?”

Dù không chắc chắn nhưng vẫn còn một cơ hội để tôi có thể chứng minh điều này. Trong giờ nghỉ trưa, tôi tới hộp chứa đồ mình đã mở ở Las Vegas ngay trước khi chạy trốn. Trong đó nhét đầy điện thoại di động, chip, giấy in, đĩa mềm và nhiều thứ khác – những thứ mà tôi không thể mang theo nhưng cũng không muốn để mất hay liều lĩnh để lại chỗ mẹ hay bà ngoại, nơi cảnh sát có thể xuất hiện bất kỳ lúc nào với một tờ lệnh khám xét và tìm ra tất cả.

Thật kỳ diệu, trong đống đồ xưa cũ đó, tôi tìm được thứ mà mình muốn có: Một tờ giấy, giờ đã khá rách nát, quăn góc và bụi bẩn, chứa toàn bộ danh mục câu hỏi của CALRS. Trên đường quay trở lại phòng xử án, tôi dừng lại tại một tiệm Kinko’s và in thành nhiều bản, đủ cho người của Hội đồng, các luật sư, thư ký cũng như nhân viên ở đây đều đọc được.

Kevin Poulsen, lúc này đã là phóng viên công nghệ rất được tôn trọng, đã bay tới Las Vegas để đưa tin về phiên tòa trong vai trò một phóng viên. Đây là những gì cậu ta viết về lúc tôi quay lại chỗ đứng của người làm chứng:

“Nếu hệ thống vẫn còn nguyên và họ chưa thay đổi danh mục câu hỏi của mình, quý tòa có thể dùng danh sách này để đăng nhập vào CALRS,” Mitnick khai. “Hệ thống sẽ cho phép quý tòa đặt thiết bị nghe lén một đường dây nào đó, hoặc chặn tín hiệu quay số.”

Mitnick quay trở lại phiên tòa với một danh sách khiến người của Sprint phản ứng mạnh mẽ; Ann Pongracz, cố vấn pháp lý của Sprint, cùng một nhân viên khác trong công ty lao nhanh ra khỏi phòng – Pongracz bấm điện thoại trên tay ngay khi vẫn đang bước vội.

Việc hai người của Sprint xám mặt phi nhanh ra khỏi phòng đã chứng minh một điều: Sprint có lẽ vẫn đang dùng thiết bị CALRS kiểu cũ, loại được lập

https://thuviensach.vn

trình với cùng một danh mục câu hỏi. Pongracz và đồng nghiệp hắn đã nhận ra tôi có thể tấn công vào hệ thống CALRS bất kỳ lúc nào mình muốn và có khả năng nghe lén bất kỳ đường dây điện thoại nào của họ ở Las Vegas.

Dù có tôi đứng ra làm chứng, Eddie cũng không thu được kết quả mong muốn. Chứng minh rằng Sprint có thể bị hack không có nghĩa là chứng minh được tổ chức Mafia hay bất kỳ ai đó cũng thực hiện hành vi này để chuyển hướng các cuộc gọi làm ăn. Eddie trắng tay trở về.

Mùa thu năm 2001 đã mở ra một chương mới trong cuộc đời tôi khi tôi được giới thiệu với đại diện nhà văn[100] David Fugate. David cho rằng câu chuyện của tôi thực đặc biệt. Anh nhanh chóng liên lạc với nhà xuất bản John Wiley & Sons và đề xuất rằng tôi có thể viết một cuốn sách về tấn công bằng kỹ thuật xã hội nhằm giúp các công ty và khách hàng có thể tự bảo vệ mình trước kiểu tấn công mà tôi đã thành công. Wiley rất nhiệt tình với dự án này và David gợi ý Bill Simon làm đồng tác giả, người sẽ hợp tác với tôi để cùng phát triển cuốn sách The Art of Deception (tạm dịch: Nghệ thuật dối lừa).

[100] Đại diện nhà văn (Literary agent): Đại diện cho các tác giả, đứng ra liên hệ với các nhà xuất bản và đàm phán hợp đồng viết sách. (ND)

Với hầu hết mọi người, có được một đại diện, một đồng tác giả đáng tin cậy và một hợp đồng xuất bản hợp lý, là phần khó nhất để xuất bản được cuốn sách của riêng mình. Còn với tôi, câu hỏi đặt ra là: Làm sao để viết được một cuốn sách mà không dùng tới máy tính?

Tôi nhìn vào thiết bị gõ văn bản tách rời mà mọi người vẫn thường dùng trước thời có máy tính cá nhân. Vì chúng thậm chí còn không thể kết nối được với các máy tính khác, tôi nghĩ mình sẽ có một cơ sở vững chắc để trình bày trước viên quản chế của mình.

Câu trả lời của anh ta hoàn toàn nằm ngoài dự đoán.

https://thuviensach.vn

Anh ta gạt bỏ ý tưởng về máy gõ văn bản và nói rằng tôi có thể sử dụng một chiếc máy tính xách tay, miễn sao không kết nối vào Internet và giữ bí mật với cánh truyền thông là được!

Khi Bill và tôi đang viết sách, Eric Corley đã cho ra mắt bộ phim tài liệu Freedom Downtime nói về cuộc vận động "Hãy trả tự do cho Kevin". Bộ phim dành rất nhiều thời gian để vạch trần những chi tiết thiếu chính xác trầm trọng trong bộ phim Takedown, thậm chí còn có cả một cảnh quay John Markoff thừa nhận rằng nguồn tài liệu duy nhất hắn có về việc tôi đã tấn công như thế nào vào NORAD bắt nguồn từ một người bị buộc tội phone phreak chuyên phát tán tin đồn sai lệch.

Sau khi xuất bản, The Art of Deception nhanh chóng trở thành cuốn sách ăn khách trên thế giới, được dịch sang 18 ngôn ngữ khác nhau. Thậm chí cho đến giờ, rất nhiều năm sau đó, nó vẫn là một trong những cuốn sách viết về hacking nổi tiếng nhất và là cuốn sách phải đọc trong các khóa học về máy tính ở một số trường đại học.

Khoảng tháng 2 năm 2003, tôi đột nhiên được mời tới Ba Lan để quảng bá cho cuốn sách. Ở trạm dừng đầu tiên tại Warsaw, phía đối tác đã cử bốn vệ sĩ mặc com-lê với bộ đàm cầm tay hệt như người của Sở Mật vụ để phụ trách vấn đề an toàn của tôi. Tôi cười lớn, cho rằng điều này thật kỳ cục. Hiển nhiên là tôi không cần được bảo vệ.

Những vệ sĩ này đưa tôi qua cửa sau tòa nhà, đi vào một trung tâm thương mại lớn. Tiếng người nói chuyện dần trở nên ầm ĩ cho tới lúc chúng tôi bước ra để vào trung tâm, nơi đây có tới hàng trăm người hâm mộ đang chen chúc sau đường dây phân cách. Khi trông thấy tôi, họ ùa tới và những nhân viên bảo vệ phải chặn họ lại.

Cho rằng họ đã nhầm tôi với một người nổi tiếng tầm cỡ thế giới nào đó, tôi bắt đầu nhìn xung quanh để xem có ngôi sao nào đang đứng quanh đó hay không. Nhưng thật kỳ diệu, đám đông thực sự ở đó vì tôi.

https://thuviensach.vn

Cuốn sách của tôi trở thành cuốn sách bán chạy nhất nước Mỹ, thậm chí còn vượt cả cuốn sách mới sách mới xuất bản của Giáo hoàng John Paul II. Một người bản địa giải thích: Ở Ba Lan sau thời Cộng sản, nếu bạn có thể đánh bại hệ thống, thì bạn chính là người hùng!

Sau cả cuộc đời hacking chỉ làm việc đơn lẻ hoặc với một người bạn nào đó, với mục tiêu chính là để học hỏi thêm nữa về cách hoạt động của hệ thống máy tính cũng như hệ thống điện tử viễn thông, cùng thành công trong việc hack vào bất kỳ thứ gì, tôi đã trở thành hình tượng tương tự như một ngôi sao nhạc rock. Đây là điều cuối cùng tôi có thể mường tượng ra.

Dù vậy, một trong những ký ức mang ý nghĩa cá nhân lớn nhất trong khoảng thời gian này chính là chuyến hành trình quảng bá sách đưa tôi tới New York. Ở đó, cuối cùng tôi cũng gặp được những người ủng hộ tạp chí2600 đã ở bên tôi trong những thời khắc đen tối nhất qua cuộc vận động "Hãy trả tự do cho Kevin". Khi tôi đang phải đối đầu với những khó khăn đến từ hệ thống tư pháp, việc có được cả một nhóm người làm việc không biết mệt mỏi để hỗ trợ tôi mang ý nghĩa vô cùng to lớn. Điều này mang lại cho tôi nhiều hy vọng và can đảm hơn hẳn những gì họ biết. Tôi không bao giờ có thể thể hiện hết lòng biết ơn sâu sắc của mình đối với những con người này.

Giây phút được phép sử dụng máy tính sau tám năm kể từ khi bị bắt hẳn phải là một trong những khoảnh khắc có ý nghĩa quan trọng trong cuộc đời sau khi ra tù của tôi. Đó là ngày hội lớn của tôi với sự góp mặt của gia đình và bạn bè từ khắp nơi trên thế giới.

Chương trình truyền hình cáp trực tiếp có tên The Screen Saver, do Leo Laporte và Patrick Norton đạo diễn, đã đề nghị được lên sóng lần tương tác Internet đầu tiên này của tôi.

Xuất hiện trong chương trình cùng với tôi, ngoài Eric Corley, người đứng đầu cuộc vận động "Hãy trả tự do cho Kevin" và cũng là người luôn hết mình ủng hộ tôi, còn có Steve Wozniak, nhà đồng sáng lập công ty Apple và

https://thuviensach.vn

cũng là một trong những người bạn thân nhất của tôi. Họ cùng đến để "giúp" tôi nghiên cứu mạng sau chừng đấy năm bị cấm đoán.

Woz đã tặng tôi một món quà bất ngờ là chiếc Apple PowerBook G4 mới tinh gói trong tờ giấy có in hình hoạt họa ngộ nghĩnh về một gã đang ra sức với tới chiếc máy tính bằng một cây gậy từ sau chấn song nhà tù. Xét trên nhiều góc độ, khoảnh khắc có được chiếc laptop từ chính cha đẻ của dòng máy tính cá nhân chính là lúc tôi biết rằng mình đã chính thức được trở lại cuộc sống trước đây.

Đã 11 năm trôi qua kể từ ngày tôi bước ra khỏi nhà giam. Tôi đã lập một công ty tư vấn với hoạt động kinh doanh khá ổn định. Công việc này đã đưa tôi đi khắp nước Mỹ và tất cả các châu trừ châu Nam Cực.

Với tôi, công việc hiện tại không khác gì một điều kỳ diệu. Các bạn hãy thử điểm tên một vài hoạt động phi pháp lại có thể được thực hiện một cách hợp pháp và có lợi cho tất cả mọi người xem. Chỉ có một cái tên duy nhất xuất hiện trong đầu tôi: hacking có đạo đức.

Tôi đã vào tù vì hacking. Giờ thì mọi người lại trả tiền để tôi làm điều tương tự, nhưng theo phương thức hợp pháp và có giá trị hơn.

Tôi chưa bao giờ có thể mường tượng ra điều này, nhưng nhiều năm sau khi ra tù, tôi đã xuất hiện tại vô số sự kiện trong giới và các cuộc họp công ty trong vai trò diễn giả chính, tôi đã viết bài cho tạp chí Harvard Business Review, cũng đã có các buổi trò chuyện với sinh viên và giáo sư tại Đại học Luật Harvard. Mỗi khi có tin tức liên quan tới các hacker, tôi sẽ được đề nghị đưa ra ý kiến trên kênh truyền hình Fox, CNN và các phương tiện truyền thông khác. Tôi đã xuất hiện trên chương trình 60 Minutes, Good Morning America (tạm dịch: 60 phút, nước Mỹ chào buổi sáng) và nhiều chương trình khác nữa. Tôi cũng được các văn phòng chính phủ như Cục Hàng không Liên bang Mỹ, Phòng Quản lý An sinh Xã hội thuê làm việc.

https://thuviensach.vn

Bất chấp những việc làm phạm pháp của tôi trong quá khứ, FBI và InfraGard cũng tìm đến tôi nhờ hỗ trợ.

Mọi người thường hỏi tôi đã hoàn toàn từ bỏ được thói quen hacking của mình chưa.

Thường thì tôi vẫn giữ thói quen của một hacker – thức khuya, ăn sáng khi tất cả mọi người đã kết thúc bữa trưa và bận rộn với máy tính đến ba, bốn giờ sáng.

Và tôi lại quay lại với nghiệp hacking… nhưng theo một cách khác. Với Công ty Tư vấn Bảo mật Mitnick LLC, tôi thực hiện việc hacking có đạo đức – dùng kỹ năng hacking của mình để kiểm tra khả năng bảo mật của các công ty nhờ xác định những điểm yếu trong hệ thống kiểm soát bảo mật vật lý, kỹ thuật và nhân lực, nhờ vậy các công ty này có thể nâng cao khả năng phòng thủ trước khi bị kẻ xấu tấn công. Tôi làm việc cho các công ty trên toàn thế giới và thường đảm nhiệm vai trò diễn giả chính cho khoảng 15-20 chương trình một năm. Chúng tôi còn kiểm tra sản phẩm bảo mật của các công ty khác trước khi nó được tung ra thị trường, để xem liệu chúng có đáp ứng được yêu cầu mà các công ty đề ra hay không. Công ty của tôi cũng cung cấp chương trình đào tạo nâng cao nhận thức về bảo mật, chủ yếu tập trung vào việc giảm nhẹ mối đe dọa từ tấn công bằng cách sử dụng kỹ thuật xã hội.

Những gì tôi đang làm cũng mang lại niềm đam mê hacking tương tự như hồi tôi còn thâm nhập bất hợp pháp trước đây. Sự khác biệt có thể được tóm tắt trong cụm từ: được ủy quyền.

Tôi không cần tới sự ủy quyền để thâm nhập.

Đó là cụm từ đã biến đổi tôi tức thì từ Hacker bị Truy nã Gắt gao nhất Thế giới thành một trong những Chuyên gia Bảo mật được Săn đón nhất Thế giới. Mọi việc cứ như thể một phép màu.

https://thuviensach.vn

LỜI CẢM ƠN

TỪ KEVIN MITNICK

Cuốn sách này xin được dành tặng người mẹ kính yêu của tôi, Shelly Jaffe, và bà tôi, Reba Vartanian, những người đã dành cả cuộc đời để hy sinh vì tôi rất nhiều. Dù tôi có rơi vào hoàn cảnh nào, mẹ và bà cũng luôn ở đó vì tôi, đặc biệt là trong những thời khắc tôi cần họ nhất. Cuốn sách này sẽ không thể thành hình nếu không nhờ có gia đình tuyệt vời của tôi, những người đã luôn dành cho tôi tình yêu thương và sự trợ giúp vô điều kiện. Tôi rất may mắn khi được nuôi dạy bởi một người mẹ giàu lòng yêu thương và tận tụy đến thế, người tôi luôn coi là bạn thân nhất của mình. Mẹ là một người tuyệt vời. Bà sẵn lòng làm bất kỳ điều gì để giúp đỡ những người gặp hoạn nạn. Mẹ luôn dành sự quan tâm chân thành đến những người khác, rất nhiều lần tới mức hy sinh cả bản thân mình. Bà tôi là một người tuyệt vời khác. Bà đã dạy tôi giá trị của sự lao động chăm chỉ và chuẩn bị cho tương lai bằng việc dạy tôi quản lý tài chính đúng cách như một biện pháp đề phòng những khi sa cơ lỡ vận. Trong suốt đời tôi, bà như người mẹ thứ hai luôn trao cho tôi rất nhiều tình yêu thương và sự giúp đỡ, luôn bên tôi bất chấp những chuyến phiêu lưu đầy tai quái của tôi.

Tháng 12 năm 2008, mẹ tôi bị chẩn đoán mắc bệnh ung thư phổi và phải trải qua rất nhiều tác động của căn bệnh cùng các đợt hóa trị. Tôi đã không nhận ra mình lãng phí nhiều thời gian bên mẹ biết bao cho đến khi tấn thảm kịch này ập đến. Là những người luôn quan tâm đến người khác và đầy nhiệt tình, cả mẹ và bà đã dạy tôi nguyên tắc về sự quan tâm đồng thời luôn giang tay giúp đỡ những người kém may mắn hơn. Vì thế, theo một nghĩa nào đó, qua việc noi theo tấm gương của họ, tôi sẽ bước tiếp trên con đường họ đã đi. Tôi hy vọng họ sẽ tha thứ cho tôi vì đã dành quá nhiều thời gian để viết cuốn sách này, bỏ qua cơ hội ngồi chơi bài hay xem video cùng họ vì lý do

https://thuviensach.vn

công việc và thời hạn phải đáp ứng. Tôi thấy hối hận sâu sắc vì tất cả những căng thẳng, lo lắng và bực mình tôi đã gây ra cho họ khi tham gia vào các cuộc phiêu lưu hacking của mình và cả những dư chấn sau khi tôi bị bắt. Giờ đây, khi đã hoàn lương và tiếp tục có những cống hiến tích cực cho xã hội, tôi hy vọng cuốn sách này sẽ đem đến thật nhiều hạnh phúc cho trái tim của mẹ và bà cũng như xóa đi một vài ký ức về những trải nghiệm tồi tệ đã được mô tả trong cuốn sách.

Tôi hằng mong cha tôi, Alan Mitnick, và người em cùng cha khác mẹ của tôi, Adam Mitnick, vẫn còn có mặt trên đời để cùng tôi nâng ly chúc mừng vào ngày cuốn hồi ký này xuất hiện trong các hiệu sách. Dù cha và tôi từng có khoảng thời gian khó khăn khi sống bên nhau, nhưng chúng tôi cũng có rất nhiều khoảng thời gian tuyệt vời, đặc biệt là khi lái thuyền câu cá quanh quần đảo Channel ở Oxnard, California. Quan trọng hơn, cha đã cho tôi tình yêu và sự tôn trọng cũng như giúp đỡ tôi rất nhiều khi tôi phải lèo lái đi qua đoạn đường gập ghềnh của hệ thống công lý tội phạm liên bang. Ông cũng tham gia cùng các tình nguyện viên khác đến từ tạp chí 2600 khi họ biểu tình tại một vài tòa án liên bang nhằm phản đối cách chính phủ xử lý vụ án của tôi. Vài tuần trước khi tôi được thả, ông đã phải trải qua một cơn trụy tim nhẹ. Bi kịch thay, sức khỏe của ông đã nhanh chóng đi xuống sau khi ông bị nhiễm khuẩn tụ cầu trong cuộc phẫu thuật rồi mắc cả bệnh lao phổi. Ông qua đời sau một năm rưỡi khi tôi được thả. Tôi không nhận ra mình đã lãng phí nhiều thời gian bên cha mình như thế nào cho đến khi ông không còn bên tôi nữa.

Dì Chickie Levanthal đã luôn bên tôi, đặc biệt là khi tôi cần dì nhất. Khi các đặc vụ FBI khám xét căn hộ của tôi ở Calabasas cuối năm 1992 trong khi tôi đang làm việc ở Văn phòng thám tử Teltec, dì đã liên hệ với luật sư thân thiết của mình, John Yzurdiaga, người đã hào phóng cho tôi những lời khuyên pháp lý và cuối cùng còn cùng với cộng sự Richard Steingard của ông đại diện cho tôi không công. Mỗi khi tôi cần lời khuyên hay chỗ trú chân tại Manhattan Beach, dì luôn ở đó để trao cho tôi tình yêu thương và sự

https://thuviensach.vn

hỗ trợ. Tôi không thể quên người bạn trai lâu năm của dì, Tiến sĩ Bob Berkowits, người tôi luôn coi như chú mình, đã luôn sẵn lòng trò chuyện mỗi khi tôi cần lời khuyên.

Còn cả em họ Trudy Spector rất tốt tính và rộng lượng khi đã cho mẹ và bà ở nhà cô mỗi lần họ di chuyển từ Los Angeles đến thăm tôi. Cô cũng cho tôi ở nhà cô trước khi tôi quyết định sẽ trốn đi sau khi lệnh quản chế hết hạn. Tôi ước cô có thể đọc những dòng này, nhưng buồn thay Trudy đã mắc phải một căn bệnh nan y và qua đời vào năm 2010. Tôi cảm thấy thương tiếc và buồn bã vô bờ khi mất đi một người yêu thương và quan tâm mình đến vậy.

Anh bạn thân Michael Morris đã luôn là người bạn chân thành của gia đình tôi. Cảm ơn anh, Mike, vì tất cả sự hỗ trợ tốt bụng và hào phóng của anh trong suốt những năm qua. Tôi biết anh sẽ nhớ ra rất nhiều chuyện được viết trong cuốn sách này. Tôi luôn trân trọng tình bạn của anh.

Tôi đã vô cùng may mắn khi thêm một lần nữa được cộng tác với tác giả của các cuốn sách bán chạy, Bill Simon, để viết cuốn hồi ký này. Một trong những kỹ năng nổi tiếng của Bill với vai trò của một người viết là khả năng kỳ diệu trong việc thu nhận những thông tin do tôi cung cấp và viết lại nó theo hình thức và giọng văn dễ hiểu. Ngoài việc là đối tác trong viết lách, Bill còn là một người bạn rất thân thiết, người đã lắng nghe những câu chuyện của tôi, đôi khi còn nghe đi nghe lại nhiều lần để chắc chắn câu chuyện được viết lại với độ chính xác cao. Dù cũng có những lúc mếch lòng và bất đồng trong việc thêm vào một vài câu chuyện hacking trong quá trình phác thảo cuốn sách, nhưng chúng tôi luôn thỏa hiệp để đi đến sự thống nhất chung. Cuối cùng, chúng tôi đã quyết định viết cuốn sách này hướng đến độc giả đại chúng, những người không cần phải có nền tảng kiến thức về hacking nâng cao hay kỹ năng mạng. Ngoài làm việc với Bill Simon, tôi còn có vinh hạnh làm việc với Donna Beech cho một số việc vào giai đoạn cuối dự án. Thật tuyệt khi được làm việc với cô.

https://thuviensach.vn

Tôi rất nóng lòng được cảm ơn những người đại diện cho sự nghiệp của tôi và đã rất tận tụy theo những cách đặc biệt. Đại diện văn chương của tôi, David Fugate ở LaunchBooks, đã dành rất nhiều thời gian đàm phán hợp đồng cuốn sách này và đóng vai trò cầu nối với nhà xuất bản Little, Brown. Đại diện diễn thuyết của tôi, Amy Gray, ở New Leaf Speakers, đã đại diện cho tôi trong suốt gần một thập kỷ. Cô luôn làm việc chu đáo và mẫn cán với biết bao nhiêu khách hàng trên khắp thế giới, những người muốn mời tôi đến nói chuyện tại sự kiện của họ. Cô đã và đang tiếp tục làm công việc tuyệt vời với vai trò là người đại diện cho tôi. Cảm ơn, Amy.

Tôi rất trân trọng cơ hội được làm việc với Little, Brown để phát triển dự án thú vị này. Tôi muốn gửi lời cảm ơn tới biên tập viên của tôi, John Parsley, vì những công việc vất vả anh đã làm cũng như những lời khuyên cho dự án này. Cảm ơn anh, John. Rất vui đã được gặp anh khi tôi ở New York.

Tôi muốn cảm ơn người anh hùng thuở thiếu thời, Steve Wozniak, vì đã dành thời gian quý báu của anh chắp bút cho phần lời tựa của cuốn hồi ký này. Đây là lời tựa thứ hai mà Steve đã hào phóng viết cho tôi. Lời đầu tiên được xuất bản trong cuối The Art of Deception (Nhà xuất bản Wiley, năm 2002). Tôi sẽ không bao giờ quên món quà "sau khi hết lệnh quản chế" mà anh đã tặng tôi trên chương trình Screen Savers – một chiếc PowerBook G4 mới tinh. Đó là món quà tuyệt vời đã khiến tôi không ngừng vui sướng trong suốt nhiều tháng. Tôi đã luôn mong được đi cùng Steve trong những chuyến chu du chung của chúng tôi. Chúng tôi đã cùng đến thăm Hard Rock Cafe ở mọi quốc gia mình đặt chân đến và sưu tập những chiếc áo phông. Cảm ơn anh, Steve, vì đã là một người bạn tuyệt vời đến vậy.

Và tất nhiên, tôi phải cảm ơn người bạn gái cũ Darci Wood của tôi vì tất cả tình yêu, sự giúp đỡ và chân thành trong thời gian chúng tôi bên nhau. Thật tiếc là có đôi khi những mối quan hệ lại không đi đến đâu vì lý do này hay lý do khác. Dù sao, thật dễ chịu khi tôi vẫn có Darci như một người bạn trung thành và đáng tin cậy. Giờ đây, tôi chỉ cần cô ấy ký vào tờ Thỏa thuận-Bảo

https://thuviensach.vn

mật có hiệu lực kể từ ngày đầu gặp mặt nữa là mọi chuyện đều ổn thỏa! Anh đùa thôi, Darci. (Mà cũng có thể là không.)

Jack Biello là người bạn thân thiết và cũng là một người chu đáo luôn lên tiếng chống lại những bất công khó tin tôi từng phải chịu dưới bàn tay của các phóng viên và bên công tố. Anh là tiếng nói tối quan trọng trong cuộc vận động "Hãy trả tự do cho Kevin" và là một cây bút với tài năng hiếm có đã viết những bài báo hấp dẫn phơi bày các thông tin mà chính phủ cố che giấu về vụ án của Kevin Mitnick. Jack đã luôn ở đó để cất tiếng nói mạnh bạo thay cho tôi và làm việc với tôi để chuẩn bị những bài diễn thuyết và bài báo. Đã có lúc, anh thậm chí còn đại diện cho tôi như một cầu nối đến với giới truyền thông. Tiếc thay, Jack đã qua đời trong lúc Bill và tôi đang hoàn thành bản thảo cuốn The Art of Deception, để lại cho tôi cảm giác mất mát và đau buồn lớn lao. Mặc dù đã gần chín năm trôi qua, tôi vẫn chưa lúc nào thôi nhớ đến anh ấy.

Dù anh bạn Alex Kasperavicius của tôi chưa bao giờ thực sự là một hacker, nhưng anh vẫn luôn sẵn lòng tham gia vào các dự án hacking của tôi, đó thường là các kế hoạch sử dụng đòn tấn công bằng kỹ thuật xã hội hấp dẫn nào đó. Sau này, chúng tôi đã cùng nhau phát triển khóa học về tấn công bằng kỹ thuật xã hội để giúp các doanh nghiệp phát hiện và giảm thiểu nguy cơ trước các vụ tấn công bằng kỹ thuật xã hội, và cung cấp những khóa học này cho các công ty trên toàn cầu. Chúng tôi thậm chí còn có vinh dự đào tạo Cục Quản lý Hàng không Liên bang tại Oklahoma City. Cuối năm 2000, chúng tôi đã tổ chức một chương trình trò chuyện về Internet trên sóng phát thanh với tên gọi The Darkside of Internet trên kênh KFI-AM 640 ở Los Angeles. Cảm ơn anh, Alex. Anh vẫn luôn là một người bạn chân thành và đáng tin cậy.

Eric Corley (hay còn gọi là Emmanuel Goldstein) luôn là người bạn và cũng là người ủng hộ tôi trong gần hai thập niên. Anh đã phát động cuộc vận động "Hãy trả tự do cho Kevin" đầu những năm 1988 sau khi tôi bị bắt hơn ba năm. Eric đã dành rất nhiều công sức, thời gian và tiền bạc để lan truyền

https://thuviensach.vn

câu chuyện trong thời gian tôi bị giam ở nhà tù liên bang. Anh cũng đã thực hiện một bộ phim tài liệu với tựa đề Freedom Downtime, phát hành năm 2001, ghi lại cuộc vận động "Hãy trả tự do cho Kevin" và thậm chí bộ phim còn giành được giải phim tài liệu xuất sắc nhất tại Liên hoan phim New York. Eric, lòng tốt, sự hào hiệp và tình bạn của anh có ý nghĩa rất lớn đối với tôi đến mức không bút mực nào tả xiết. Cảm ơn anh vì mọi thứ và vì anh đã luôn bên tôi.

Tôi muốn cảm ơn cộng sự hacking cũ tôi, Lewis De Payne, vì đã dành thời gian cùng tôi nhớ lại một vài cuộc phiêu lưu hacking trong quá khứ mà cả hai chúng tôi cùng tham gia. Cảm ơn cậu, Lewis. Đó là cuộc hành trình dài và điên rồ với cả hai chúng ta và tôi thực sự chúc cậu những điều tốt đẹp nhất.

Người bạn thân Christine Marie của tôi đã giúp đỡ tôi với bản thảo thô đầu tiên của phần lời kết ở cuối cuốn sách này. Cảm ơn Christine vì những đóng góp và cố gắng của cô.

Tôi muốn cảm ơn hai người bạn thân Kat và Matt Wagenknecht vì đã cùng tôi phát triển những đoạn mã xuất hiện ở đầu mỗi chương. Đó là một kết quả thật tuyệt vời! Hãy xem có bao nhiêu độc giả có thể giải những câu đố này và nhận được phần thưởng.

Tôi muốn cảm ơn Jari Tomminen vì đã cho phép tôi dùng tấm ảnh anh chụp tôi tại Helsinki, Phần Lan, cho bìa sách Bóng ma trên mạng.

Tôi muốn cảm ơn người bạn kiêm chuyên gia bảo mật David Kennedy, người đã vui lòng đọc duyệt một phần cuốn sách này và cung cấp cho tôi những lời khuyên có giá trị.

Cảm ơn anh, Alan Luckow, vì đã đồng ý để tôi đưa vào cuốn sách của mình tấm ảnh chụp bức tranh anh vẽ, vốn nằm trên tờ giấy gói quà bọc chiếc hộp đựng chiếc laptop Apple PowerBook G4 mà Steve Wozniak tặng cho tôi trong chương trình The Screen Savers.

https://thuviensach.vn

Nhờ có mạng xã hội Twitter, tôi có thể tìm được vài tình nguyện viên sẵn lòng chụp một số bức ảnh cho cuốn sách. Tôi muốn cảm ơn Nick Arnott, Shellee Hale, John Lester, hay còn gọi là Count Zero, Michelle Tackabery và nhiều người khác vì những đóng góp rộng rãi của họ và vì thời gian họ đã làm tình nguyện. Nếu các bạn muốn theo dõi tôi trên Twitter, xin hãy truy cập địa chỉ: twitter.com/kevinmitnick.

Tôi muốn gửi lời cảm ơn tới cựu công tố liên bang của tôi, David Schindler, người đã rộng lòng dành thời gian để tôi phỏng vấn ông cho cuốn sách.

Tôi muốn cảm ơn Justin Petersen, hay còn gọi là Eric Heinz và Ronald Mark Austin, những người đã vui lòng cho tôi phỏng vấn. Một thời gian ngắn sau khi Bill Simon và tôi phỏng vấn Justin Petersen, anh được tìm thấy đã qua đời trong căn hộ của mình ở Tây Hollywood, có thể là do dùng thuốc quá liều. Thật buồn khi anh đã phải chịu chung định mệnh với em trai tôi, người đã gợi ý tôi chủ động liên lạc với Petersen khi Justin còn đang dùng bí danh Eric Heinz.

Khi đang viết những dòng cảm ơn này, tôi nhận ra mình có rất nhiều người để cảm ơn và bày tỏ sự trân trọng vì họ đã dành cho tôi tình yêu, tình bạn và sự giúp đỡ. Tôi không thể nhớ hết tên của tất cả những người tốt bụng và rộng lượng mình đã gặp những năm gần đây, nhưng có thể nói rằng, tôi sẽ cần cả một ổ cứng để lưu giữ tất cả họ. Đã có rất nhiều người từ khắp nơi trên thế giới viết cho tôi những lời động viên, tán dương và ủng hộ. Đó là những lời lẽ có ý nghĩa rất lớn lao đối với tôi, đặc biệt là trong những thời điểm tôi cần chúng nhất.

Tôi đặc biệt cảm ơn tạp chí 2600 và tất cả những người ủng hộ đã bên tôi và dành thời gian quý báu cũng như năng lượng của họ để lan truyền câu chuyện đến bất kỳ ai chịu lắng nghe, những người đã cất lên tiếng nói quan ngại và phản đối cách đối xử thiếu công bằng với tôi cùng những câu chuyện cường điệu được tạo ra từ những người muốn kiếm lợi từ “Huyền thoại về Kevin Mitnick”.

https://thuviensach.vn

Tôi đã có rất nhiều trải nghiệm với các luật sư và rất nóng lòng muốn được bày tỏ lời cảm ơn của mình đến những người đã đứng lên và đề nghị giúp đỡ tôi trong những năm tháng tôi phải trải qua những trải nghiệm tiêu cực với hệ thống pháp lý hình sự và khẩn thiết cần tới sự giúp đỡ. Tôi tôn trọng, thán phục và trân trọng lòng tốt cùng sự rộng lượng của rất nhiều người đã trao tặng chúng cho tôi miễn phí. Tôi muốn cảm ơn Greg Aclin, Fran Campbell, Robert Carmer, Debbie Drooz, John Dusenbury, Sherman Ellison, Omar Figueroa, Jim French, Carolyn Hagin, Rob Hale, Barry Langberg, David Mahler, Ralph Peretz, Michelle Carswell Pritchard, Donald C. Randolph, Tony Serra, Skip Slates, Richard Steingard, the Honorable Robert Talcott, Barry Tarlow, Gregory Vinson và John Yzurdiaga.

TỪ BILL SIMON

Trong phần Cảm ơn của cuốn sách The Art of Deception, tôi đã viết về Kevin rằng “đây không phải là một câu chuyện hư cấu, dù nhân vật chính có thể là một nhân vật do tôi sáng tạo ra cho một kịch bản phim hồi hộp. Tôi dành cho đồng tác giả có-một-không-hai này sự tôn trọng rất trong sáng.” Và tôi cũng nói rằng “cách làm việc của anh về căn bản khác tôi đến mức mọi người có thể băn khoăn không hiểu chúng tôi làm sao có thể cùng trở thành đồng tác giả của một cuốn sách và còn lên kế hoạch thực hiện thêm các dự án khác cùng nhau. Cả hai chúng tôi đã thay đổi, học hỏi và tìm thấy niềm vui trong công việc vô cùng khó khăn là biến những kiến thức và trải nghiệm của anh thành một thứ đọc rất hài hước.” Dù cuốn sách này, cuốn sách thứ ba chúng tôi viết cùng nhau, đã ảnh hưởng nghiêm trọng nhất đến tình bạn của chúng tôi, nhưng tôi rất vui được thông báo rằng tình bạn và sự tôn trọng của chúng tôi vẫn sống sót và còn được thắt chặt hơn, bất chấp những va chạm dữ dội trong quá trình hợp tác. Tôi hy vọng cuốn sách này sẽ tồn tại trong một thời gian dài; tôi cũng hy vọng tình bạn của chúng tôi sẽ tồn tại được lâu như vậy hoặc thậm chí hơn thế.

Tôi rất khó qua mặt được tài năng biên tập của John Parsley. Anh là người biết cảm thông nhưng khắt khe và luôn mong muốn mang lại những điều tốt

https://thuviensach.vn

đẹp nhất. Anh vẫn luôn ở đó khi bạn cần đến anh. Hướng dẫn của John giúp cuốn sách này thêm tuyệt vời hơn và tôi nợ anh điều đó. Tổng biên tập đáng mến của anh, Peggy Freudenthal, đã chứng minh mình là một nhà vô địch – tự đặt bản thân vào những thử thách, làm việc theo cách có một không hai và chưa bao giờ để mất sự điềm tĩnh; cả Kevin và tôi đều mang ơn cô.

Tôi sẽ không dễ gì hoàn thành một cuốn sách nếu không có người vợ, người bạn đời nhiều năm của tôi, Arynne Simon đa tài, người luôn ủng hộ và cổ vũ tôi, người khiến tôi làm việc chăm chỉ thêm dù chỉ một chút để tìm ra được cụm từ thích hợp. Nụ cười của em đã tiếp thêm động lực cho anh.

Người đại diện Bill Gladstone và David Fugate, cả hai đều đã góp sức giúp biến dự án này thành hiện thực. Tôi xin ngả mũ trước hai anh.

Ngoài thông tin từ Kevin, tôi rất biết ơn những người khác đã giúp tôi hoàn chỉnh câu chuyện – cụ thể là mẹ của Kevin, Shelly Jaffe, và bà Reba Vartanian của anh; vợ cũ của anh, Bonnie; trợ lý công tố David Schindler; Kevin Poulsen; cựu điều tra viên an ninh Pacific Bell Darrell Santos; cựu thanh tra; giờ là cảnh sát trưởng David Simon thuộc Phòng Cảnh sát Trưởng Los Angeles (và là người anh em sinh đôi của tôi). Nhờ có sự sẵn lòng chia sẻ của họ mà cuốn sách đã trở nên phong phú hơn. Nhưng tôi đặc biệt muốn gửi lời cảm ơn tới Justin Petersen quá cố, hay còn gọi là Eric Heinz, người đã mở lòng vượt xa mong đợi của tôi.

Tôi đặc biệt muốn tri ân Sheldon Bermont vì những đóng góp của anh cho cuốn sách. Và đến những đứa cháu của tôi, Vincent và Elena Bermont, nụ cười và nhiệt huyết của các cháu đã giúp ông luôn vui vẻ.

Cuối cùng – nhắc đến sau cùng, ở vị trí trang trọng – tôi xin nghiêng mình trước Charlotte Schwarts, người đã tạo nên tất cả sự khác biệt.

https://thuviensach.vn

ĐÔI ĐIỀU VỀ TÁC GIẢ

Kevin Mitnick từng là hacker nổi tiếng nhất thế giới và giờ là một chuyên gia tư vấn về bảo mật. Anh là chủ đề của không biết bao nhiêu tin tức và báo đài tạp chí. Anh đã xuất hiện trên vô số chương trình truyền hình và phát thanh để đưa ra những bình luận chuyên sâu về bảo mật thông tin. Anh đã làm chứng trước Thượng viện Mỹ và viết bài cho tạp chí Harvard Business Review. Mitnick là đồng tác giả, cùng với William B. Simon, của những cuốn sách bán chạy nhất *The Art of Deception* (tạm dịch: *Nghệ thuật lừa dối*) và *The Art of Intrusion* (tạm dịch: *Nghệ thuật xâm nhập*). Anh hiện sống ở Las Vegas, Nevada.

https://thuviensach.vn

Table of Contents

An toàn thông tin trong kỷ nguyên số
Lời giới thiệu
Lời tựa
Lời nói đầu
PHẦN MỘT: SỰ RA ĐỜI CỦA MỘT HACKER
01. Khởi đầu chông gai
02. Chỉ là ghé thăm
03. Tội lỗi đầu tiên
04. Nghệ sĩ trốn chạy
05. Tất cả đường dây điện thoại của các anh đều thuộc về tôi
06. Hack vì yêu
07. Kết hôn vội vã
08. Lex Luthor
09. Gói cước giảm giá kiểu Kevin Mitnick
10. Hacker bí ẩn
PHẦN HAI: ERIC
11. Mờ ám
12. Không thể giấu giếm
13. Kẻ nghe lén
14. Anh nghe lén tôi, tôi nghe lén anh
15. “Làm thế quái nào các cậu có được nó?”
16. Khách không mời mà tới
17. Phân tích lưu lượng
18. Sáng tỏ
19. Vén màn
20. Cắn ngược
21. Mèo và chuột
22. Công việc thám tử
23. Bị vây bắt

https://thuviensach.vn

24. Hô biến
PHẦN BA: TRỐN CHẠY
25. Harry Houdini
26. Thám tử tư
27. Mặt trời lên
28. Săn lùng chiến tích
29. Rời đi
30. Đánh lén
31. Vây bắt từ trên cao
32. Đêm trắng ở Seattle
PHẦN BỐN: KẾT THÚC VÀ KHỞI ĐẦU
33. Hack gã samurai
34. Lánh về phương Nam
35. Trò chơi kết thúc
36. Ngày lễ tình yêu của FBI
37. Thoát nạn vật tế thần
38. Hồi kết: Vận mệnh đổi chiều
Lời cảm ơn
Đôi điều về tác giả

https://thuviensach.vn