

Ninja Hacking

Chiến Thuật Và Kỹ Thuật Kiểm Tra Thâm Nhập.

**Thomas Wilhelm**

**Jason Andress**

**Bryan Garner**

Ninjutsu Consultant

**Joshua Abraham**

Technical Editor



AMSTERDAM • BOSTON • HEIDELBERG • LONDON NEW YORK • OXFORD • PARIS • SAN DIEGO SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO



Syngress is an imprint of Elsevier

|  |  |
| --- | --- |
|  | **Chương** |
|  |  |
| Ninja Hiện Đại | 2 |
|  |

It is sad to say, but the modern vision of a ninja conjured up in most people’s minds is what has been paraded across the big screen by Hollywood in their oft-failed attempts to portray their interpretation of historic Japanese culture and war. If the modern vision of a ninja is not an image of a person garbed in all-black pajamas swinging from tree to tree or walking on the air, it is that of some self-proclaimed ninja caught on camera by news agencies doing foolish things, such as trying to bring a sword to a gun fight, or impaling himself on a metal fence. Either way, the reality of what the historical ninja actually was has been almost obliterated.

Thật đáng buồn khi phải nói rằng, hình ảnh ninja hiện đại mà phần lớn mọi người hình dung lại là hình ảnh đã được Hollywood phô trương trên màn ảnh rộng qua những cố gắng không thành công của họ trong việc thể hiện cách hiểu của họ về văn hóa và chiến tranh lịch sử của Nhật Bản. Nếu hình ảnh ninja hiện đại không phải là một người mặc bộ đồ đen toàn thân, đu qua lại từ cây này sang cây khác hoặc đi trên không trung, thì đó là hình ảnh của một kẻ tự xưng là ninja bị các cơ quan truyền thông ghi lại khi làm những việc ngu ngốc, như cố gắng mang kiếm đến một cuộc đấu súng, hoặc tự đâm mình vào hàng rào kim loạ. Dù thế nào đi nữa, thực tế về ninja lịch sử thực sự đã gần như bị xoá sạch.

There are some who have continued to carry the traditions of the historical ninja into today’s world, especially in the study of Ninjutsu. However, the question of the role of a ninja in today’s world is a difficult one to answer; most answers, by those that have actually studied and practiced Ninjutsu, tend to espouse Ninjutsu as a highly effective method of self-reflection and internal growth. It is hard to justify the need for advanced self-defense and espionage tactics when one lives in the well-manicured world of suburbia and works in the forests of cubicles, faxes, and copiers. Although some may have visions of brutally destroying uncooperative fax machines, the combat techniques of Ninjutsu serve better within the confines of a dojo.

Có một số người vẫn tiếp tục duy trì các truyền thống của ninja lịch sử trong thế giới ngày nay, đặc biệt là trong việc nghiên cứu Ninjutsu. Tuy nhiên, câu hỏi về vai trò của ninja trong thế giới hiện đại là một câu hỏi khó để trả lời; phần lớn các câu trả lời, từ những người thực sự đã nghiên cứu và thực hành Ninjutsu, thường cho rằng Ninjutsu là một phương pháp rất hiệu quả để tự phản chiếu và phát triển nội tâm. Rất khó để biện minh cho việc cần thiết các chiến thuật tự vệ và tình báo tiên tiến khi một người sống trong thế giới ngăn nắp của vùng ngoại ô và làm việc trong những "rừng" cubicle, fax và máy photocopy. Mặc dù một số người có thể mơ tưởng đến việc tàn phá những chiếc máy fax không hợp tác, nhưng các kỹ thuật chiến đấu của Ninjutsu lại phát huy tác dụng tốt hơn trong không gian của một dojo.

However, if we examine Ninjutsu tactics within the virtual world, we may find some interesting applications. Although we cannot rely on muscle memory to physi-cally protect us against a physical attack, we can use the teachings and techniques of Ninpō to better understand the chaotic and anarchistic world of the Internet, and how to best conduct attacks and defensive maneuvers to obtain victory against our adversaries – or at least elude defeat. In the information system security world, those that would best benefit by examining the tactics of the ninja include anyone who conducts professional penetration testing, or administrators intent on protecting corporate and government networks and systems. Traditional methods, used by pen-etration test engineers and administrators within the cat-and-mouse game of identi-fying flaws within the network or system before anyone else, have been effective in most instances; however, current defensive and penetration-test methodologies have inherent flaws in that they still abide by restrictive codes of ethics to keep a penetra-tion test project from getting out of control. The flaws come in the form of preven-tative constraints in the types of attacks that can be used, identification of off-limit systems or networks, time limitations within the project, and business-related “polit-ical” minefields that must be avoided. Worse yet, the mindset of the defender and attacker can be the greatest weakness­ in the whole penetration test process; if the players in this event cannot mentally escape the societal and ethical restrictions that inherently come with being part of the corporate culture, effective tactics will be left unused and vulnerabilities will be left undiscovered. To truly understand the threats against a target system, the attacker must be capable of easily discarding societal pressures and norms and examine attack vectors that are unconventional and radical; otherwise, penetration tests become rote, repetitive, and ineffective.

1. **Chương 2** Ninja HIện Đại

Tuy nhiên, nếu chúng ta xem xét các chiến thuật Ninjutsu trong thế giới ảo, chúng ta có thể tìm thấy một số ứng dụng thú vị. Mặc dù chúng ta không thể dựa vào trí nhớ cơ bắp để bảo vệ mình khỏi một cuộc tấn công vật lý, nhưng chúng ta có thể sử dụng các giáo lý và kỹ thuật của Ninpō để hiểu rõ hơn về thế giới hỗn loạn và vô chính phủ của Internet, và cách thức tiến hành các cuộc tấn công và các động tác phòng thủ để đạt được chiến thắng trước đối thủ – hoặc ít nhất là tránh được thất bại. Trong lĩnh vực bảo mật hệ thống thông tin, những người sẽ thu được lợi ích lớn nhất từ việc nghiên cứu các chiến thuật của ninja bao gồm bất kỳ ai thực hiện thử nghiệm xâm nhập chuyên nghiệp, hoặc các quản trị viên có mục tiêu bảo vệ các mạng lưới và hệ thống của doanh nghiệp và chính phủ. Các phương pháp truyền thống, được sử dụng bởi các kỹ sư thử nghiệm xâm nhập và các quản trị viên trong trò chơi mèo vờn chuột của việc xác định các lỗ hổng trong mạng hoặc hệ thống trước khi ai đó khác phát hiện ra, đã hiệu quả trong hầu hết các trường hợp; tuy nhiên, các phương pháp phòng thủ và thử nghiệm xâm nhập hiện tại có những khuyết điểm bẩm sinh vì chúng vẫn tuân thủ các mã đạo đức hạn chế để tránh dự án thử nghiệm xâm nhập vượt khỏi tầm kiểm soát. Những khuyết điểm này thể hiện dưới dạng các rào cản phòng ngừa trong các loại tấn công có thể sử dụng, việc xác định các hệ thống hoặc mạng lưới cấm, các giới hạn về thời gian trong dự án, và các "mê cung chính trị" liên quan đến công việc cần tránh. Tệ hơn nữa, tư duy của cả người phòng thủ và tấn công có thể là điểm yếu lớn nhất trong toàn bộ quy trình thử nghiệm xâm nhập; nếu các người tham gia sự kiện này không thể vượt qua được các hạn chế xã hội và đạo đức vốn có khi là một phần của văn hóa doanh nghiệp, các chiến thuật hiệu quả sẽ không được sử dụng và các lỗ hổng sẽ bị bỏ qua. Để thực sự hiểu các mối đe dọa đối với một hệ thống mục tiêu, kẻ tấn công phải có khả năng dễ dàng loại bỏ các áp lực và chuẩn mực xã hội, và xem xét các vectơ tấn công không chính thống và cực đoan; nếu không, các bài kiểm tra xâm nhập sẽ trở nên các bài kiểm tra xâm nhập sẽ trở nên máy móc, lặp đi lặp lại và không hiệu quả.

One challenge facing those that are willing to shed the orthodox methods of con-ducting a penetration test is dealing with the question of ethics; many professional penetration testers are constrained by rules of ethics, whether from a certification body or within formalized business policies. There seems to be a general misconception that unorthodox methods of attack, including those used by the historical ninja, are somehow unethical. To understand why “unorthodox” does not equate to “unethical,” a better understanding is required on the true nature of ethics, and how it is defined.

When the topic of ethics comes up in conversation within the context of pen-etration testing, the dichotomy between white hat and black hat hackers is often bantered about without properly defining the differences. In typical discussions, the label of “unethical” is often tied to the activities of black hats, whereas white hats are assumed to be the ones who act ethically. Unfortunately, ethics is perceived dif-ferently by different cultures and groups within the hacking community, and really does not belong in the discussion surrounding the differences between white hats and black hats.

Applying ninja tactics to modern-day penetration testing may seem anachronistic; however, there are many lessons that can be used to improve the technique of profes-sional penetration testers – the most significant lesson being how to think like a ninja. By shifting one’s perceptions about how to conduct attacks against network systems, the penetration test engineer can provide better value to the customer by identifying

and exploiting vulnerabilities that may have been undiscovered­ otherwise.

Một thử thách đối với những người sẵn sàng từ bỏ các phương pháp chính thống trong việc tiến hành thử nghiệm xâm nhập là đối mặt với câu hỏi về đạo đức; nhiều chuyên gia thử nghiệm xâm nhập bị ràng buộc bởi các quy tắc đạo đức, dù là từ các tổ chức cấp chứng nhận hay từ các chính sách kinh doanh chính thức. Có vẻ như có một sự hiểu lầm chung rằng các phương pháp tấn công không chính thống, bao gồm những phương pháp được sử dụng bởi ninja lịch sử, là vô đạo đức. Để hiểu tại sao "không chính thống" không đồng nghĩa với "vô đạo đức", cần phải có một hiểu biết rõ ràng hơn về bản chất thực sự của đạo đức và cách thức định nghĩa nó.

Khi chủ đề đạo đức được đưa ra trong cuộc trò chuyện trong bối cảnh thử nghiệm xâm nhập, sự phân biệt giữa hacker mũ trắng (white hat) và hacker mũ đen (black hat) thường được nhắc đến mà không có sự định nghĩa rõ ràng về sự khác biệt. Trong các cuộc thảo luận thông thường, nhãn hiệu "vô đạo đức" thường gắn liền với các hoạt động của hacker mũ đen, trong khi hacker mũ trắng được cho là những người hành động có đạo đức. Thật không may, đạo đức được nhìn nhận khác nhau ở các nền văn hóa và nhóm khác nhau trong cộng đồng hacker, và thực sự nó không nên là phần của cuộc thảo luận về sự khác biệt giữa hacker mũ trắng và hacker mũ đen.

Việc áp dụng các chiến thuật của ninja vào thử nghiệm xâm nhập ngày nay có thể có vẻ như không hợp thời, nhưng có nhiều bài học có thể được sử dụng để cải thiện kỹ thuật của các chuyên gia thử nghiệm xâm nhập – bài học quan trọng nhất là cách suy nghĩ như một ninja. Bằng cách thay đổi cách nhìn nhận về cách thức tiến hành các cuộc tấn công vào hệ thống mạng, kỹ sư thử nghiệm xâm nhập có thể mang lại giá trị tốt hơn cho khách hàng bằng cách xác định và khai thác các lỗ hổng có thể đã bị bỏ qua nếu không có phương pháp tiếp cận này.

Modern-Day Ninjutsu

In Chapter 1, “The Historical Ninja,” we examined the historical ninja, and the envi-ronment they lived in, which shaped the way they performed espionage work. Times change, and if we are to employ ninja tactics into penetration testing, we need to see how Ninjutsu has evolved over the last few centuries.

When we discuss the modern-day ninja, we have very limited examples to look toward; because of the nature of war and peace, numerous traditional Ninjutsu techniques

have suffered and been lost over the ages. The most notable example of modern­-day Ninjutsu that was able to persevere despite the threat of time is the Bujinkan Organi-zation, founded by thirty-fourth Grandmaster of the Togakure School, Dr. Masaaki Hatsumi. Within the Bujinkan Organization exist nine ­different martial arts lineages; however, only three of these schools of thoughts within the Bujinkan Organization’s current teachings can be considered unique to Ninjutsu, and Ninpō:

• Togakure-ryū

• Kumogakure-ryū

• Gyokushin-ryū

The other six lineages taught within the Bujinkan, intended to provide survival techniques for the ninja who become embroiled in combat, involve martial arts that are also used extensively by other traditions, including those displayed by samurai in ancient Japan (Garner B. personal communication, December 14, 2000).

Within each of these three unique Ninpō lineages, there are numerous tactics and skills that were shared in common – the differences between the lineages are largely centered on what tactics were emphasized, based on regional influences. These shared tactics and skills make up the following Shinobi Happō Hiken1:

1. Taijutsu, Hichō-justsu, Nawa-nage (body skills and rope throwing)
2. Karate Koppō-Taijutsu, Jūtaijutsu (unarmed fighting)A
3. Bō-jutsu, Jō-jutsu, Hanbō-jutsu (staff and stick arts)
4. Sō-jutsu, Naginata-jutsu (spear and halberd arts)
5. Senban-nage, Ken-nage-jutsu, Shuriken (throwing of blades)
6. Ka-jutsu, Sui-jutsu (use of fire and water)
7. Chikujō Gunryaku Hyōhō (military fortification, strategy and tactics)
8. Onshin-jutsu (concealment).

These eight branches have evolved and been rebranded over the hundreds of years of their formal existence, but they provide the student of Bujinkan Ninjutsu a structured method of training and a solid understanding of what the ninja skill set consisted of in times past. Additional martial techniques that aided ninja in their missions were added as needed, including the use of a short sword, truncheon, and metal fan

Ninjutsu Hiện Đại

Trong Chương 1, "Ninja Lịch Sử," chúng ta đã nghiên cứu về ninja lịch sử và môi trường mà họ sống, điều này đã ảnh hưởng đến cách thức họ thực hiện công việc gián điệp. Thời gian thay đổi, và nếu chúng ta muốn áp dụng các chiến thuật ninja vào thử nghiệm xâm nhập, chúng ta cần xem xét cách mà Ninjutsu đã phát triển trong suốt vài thế kỷ qua.

Khi nói về ninja hiện đại, chúng ta có rất ít ví dụ để tham khảo; do bản chất của chiến tranh và hòa bình, nhiều kỹ thuật Ninjutsu truyền thống đã bị mai một và mất đi theo thời gian. Một trong những ví dụ đáng chú ý nhất về Ninjutsu hiện đại có thể tồn tại dù đối mặt với thách thức của thời gian là Tổ chức Bujinkan, được sáng lập bởi Đại Sư thứ 34 của Trường Togakure, Dr. Masaaki Hatsumi. Trong Tổ chức Bujinkan có chín dòng võ thuật khác nhau; tuy nhiên, chỉ có ba trong số những trường phái này trong các giáo lý hiện tại của Tổ chức Bujinkan có thể được coi là đặc trưng cho Ninjutsu và Ninpō:

• Togakure-ryū

• Kumogakure-ryū

• Gyokushin-ryū

Sáu dòng võ thuật còn lại trong Bujinkan, nhằm cung cấp các kỹ thuật sinh tồn cho ninja khi tham gia chiến đấu, là các môn võ cũng được sử dụng rộng rãi trong các truyền thống khác, bao gồm những môn võ mà samurai đã thực hành ở Nhật Bản cổ đại (Garner B. giao tiếp cá nhân, 14 tháng 12, 2000).

Trong mỗi dòng Ninpō độc đáo này, có nhiều chiến thuật và kỹ năng chung – sự khác biệt giữa các dòng chủ yếu là về các chiến thuật nào được nhấn mạnh, dựa trên ảnh hưởng khu vực. Những chiến thuật và kỹ năng chung này tạo thành Shinobi Happō Hiken:

1. Taijutsu, Hichō-jutsu, Nawa-nage (kỹ năng cơ thể và ném dây)
2. Karate Koppō-Taijutsu, Jūtaijutsu (chiến đấu tay không)
3. Bō-jutsu, Jō-jutsu, Hanbō-jutsu (võ thuật gậy và gậy ngắn)
4. Sō-jutsu, Naginata-jutsu (võ thuật giáo mác và thương)
5. Senban-nage, Ken-nage-jutsu, Shuriken (ném dao và vũ khí)
6. Ka-jutsu, Sui-jutsu (sử dụng lửa và nước)
7. Chikujō Gunryaku Hyōhō (phòng thủ quân sự, chiến lược và chiến thuật)
8. Onshin-jutsu (ngụy trang).

Tám nhánh này đã phát triển và được tái cấu trúc qua hàng trăm năm tồn tại chính thức, nhưng chúng cung cấp cho học viên Bujinkan Ninjutsu một phương pháp huấn luyện có cấu trúc và một hiểu biết vững vàng về những kỹ năng của ninja trong quá khứ. Những kỹ thuật võ thuật bổ sung giúp ninja trong các nhiệm vụ của họ đã được thêm vào khi cần thiết, bao gồm việc sử dụng kiếm ngắn, gậy, và quạt kim loại.

WARNING

It should be pretty obvious, but the application of any martial arts in a real-world situation, outside of a training environment, is dangerous. Although the areas of Shinobi Happō Hiken were listed here, it does not mean they should be incorporated into professional penetration tests. The objective of this chapter is to understand that ninja had a very specific type of skillset, intended to keep them alive and successful in their era … and how we need to come up with our own skillset that follows the philosophy of Ninpō.

Although these eight methods make up the core of Ninjutsu, there is an additional component that has been brought forward in time that make Ninjutsu unique in the martial arts; specifically, a mindset that permits the ninja to be successful in their unique role in unconventional warfare. In an effort to define the mindset of a ninja, Hatsumi stated1:

The spirit of the ninja is […] based on the principle of bearing insults and swal-lowing the desire for revenge. In other words, the fundamental rule of the ninja when faced with an enemy’s attack is to evade it naturally and disappear, using Ninpō Taijutsu (concealment skills sometimes referred as “Tongyō no Jutsu”). Only when no other option is left open would a ninja make use of natural prin-ciples and methods to fell his opponent.

The traditions of the Bujinkan have been studied and used in training through-out the world, including military academies; however, popularity in the art has fluctuated over the years and been strained because of undesirable individuals with preconceived notions who misunderstood what Ninjutsu teachings truly encom-passed. Those with misconceptions were typically interested in tactics popular-ized in the movies, including use of poisons, deadly traps, and brutal techniques designed to severely hamper pursuing enemies (Garner B. personal communica-tion, December 14, 2000). Although, historically, the ninja used such techniques, the essence of ninja training was not one of aggression, but of evasion, as stated by Hatsumi, which unwaveringly precludes the use of deadly force unless absolutely necessary.

Although Hatsumi succinctly described what the spirit of a ninja entails, it is important to again stress the mission of a ninja was not to meet in face-to-face battle with the enemy; rather, the mission of a ninja was to subvert the enemy’s efforts through strategic employment of espionage, unconventional warfare, and guerilla warfare without detection. Absence of detection is such a critical component of a ninja’s activity that Ninjutsu has also been described as “if you can see it, it’s not Ninjutsu” (Garner B. personal communication, December 14, 2000).

As mentioned in Chapter 1, “The Historical Ninja,” the motivations of ninja were not one of greed or self-interest. Toshitsugu Takamatsu, the thirty-third Grandmaster of Togakure-ryū wrote that “family, community, homeland, and ‘appropriateness’ deter-mine when a ninja should act, not power, money, political obligation, or thrill of violence and adventure.”2 The belief structure that benefiting family, community, and homeland come first in any decision to act is the essence of the Ninpō ethical framework; it is this ethical framework we will reference extensively to throughout this book.

CẢNH BÁO

Điều này có lẽ khá rõ ràng, nhưng việc áp dụng bất kỳ môn võ thuật nào trong tình huống thực tế, ngoài môi trường huấn luyện, là rất nguy hiểm. Mặc dù các lĩnh vực trong Shinobi Happō Hiken đã được liệt kê ở đây, điều này không có nghĩa là chúng nên được áp dụng vào các bài kiểm tra xâm nhập chuyên nghiệp. Mục tiêu của chương này là hiểu rằng ninja có một bộ kỹ năng rất cụ thể, nhằm giúp họ sống sót và thành công trong thời đại của họ… và cách mà chúng ta cần phải phát triển bộ kỹ năng riêng của mình theo triết lý của Ninpō.

Mặc dù tám phương pháp này tạo thành cốt lõi của Ninjutsu, có một yếu tố bổ sung đã được duy trì qua thời gian, làm cho Ninjutsu trở nên độc đáo trong các môn võ thuật; đặc biệt là một tư duy cho phép ninja thành công trong vai trò độc đáo của họ trong chiến tranh phi truyền thống. Để định nghĩa tư duy của một ninja, Hatsumi đã nói:

"Tinh thần của ninja là […] dựa trên nguyên lý chịu đựng sự xúc phạm và nuốt xuống sự khao khát báo thù. Nói cách khác, quy tắc cơ bản của ninja khi đối mặt với một cuộc tấn công của kẻ thù là tự nhiên tránh né và biến mất, sử dụng Ninpō Taijutsu (kỹ năng ngụy trang, đôi khi được gọi là 'Tongyō no Jutsu'). Chỉ khi không còn lựa chọn nào khác, ninja mới sử dụng các nguyên lý và phương pháp tự nhiên để đánh bại đối thủ của mình."

Các truyền thống của Bujinkan đã được nghiên cứu và sử dụng trong huấn luyện trên toàn thế giới, bao gồm cả các học viện quân sự; tuy nhiên, sự phổ biến của nghệ thuật này đã dao động qua các năm và bị ảnh hưởng bởi những cá nhân không mong muốn, với những quan niệm sai lầm về những gì mà giáo lý Ninjutsu thực sự bao hàm. Những người có quan niệm sai lầm này thường quan tâm đến các chiến thuật đã được phổ biến trong các bộ phim, bao gồm việc sử dụng độc dược, bẫy chết người, và các kỹ thuật tàn bạo nhằm làm suy yếu kẻ thù đuổi theo (Garner B. giao tiếp cá nhân, 14 tháng 12, 2000). Mặc dù, lịch sử ghi nhận rằng ninja đã sử dụng các kỹ thuật như vậy, nhưng bản chất của huấn luyện ninja không phải là sự xâm lược, mà là sự né tránh, như đã được Hatsumi chỉ ra, điều này kiên quyết loại trừ việc sử dụng vũ lực chết người trừ khi thật sự cần thiết.

Mặc dù Hatsumi đã mô tả ngắn gọn tinh thần của một ninja, điều quan trọng là phải nhấn mạnh rằng nhiệm vụ của một ninja không phải là đối đầu trực diện với kẻ thù; mà nhiệm vụ của ninja là làm suy yếu nỗ lực của kẻ thù thông qua việc sử dụng chiến tranh gián điệp, chiến tranh phi truyền thống, và chiến tranh du kích mà không bị phát hiện. Việc không bị phát hiện là một yếu tố quan trọng trong hoạt động của ninja đến nỗi Ninjutsu còn được mô tả là "nếu bạn có thể nhìn thấy nó, đó không phải là Ninjutsu" (Garner B. giao tiếp cá nhân, 14 tháng 12, 2000).

Như đã đề cập trong Chương 1, "Ninja Lịch Sử," động cơ của ninja không phải là tham lam hay lợi ích cá nhân. Toshitsugu Takamatsu, Đại Sư thứ 33 của Togakure-ryū, đã viết rằng "gia đình, cộng đồng, tổ quốc và 'sự phù hợp' quyết định khi nào một ninja nên hành động, chứ không phải quyền lực, tiền bạc, nghĩa vụ chính trị, hay sự kích thích từ bạo lực và phiêu lưu." Niềm tin rằng lợi ích của gia đình, cộng đồng và tổ quốc đứng đầu trong mọi quyết định hành động là bản chất của khung đạo đức Ninpō; đây chính là khung đạo đức mà chúng ta sẽ tham chiếu nhiều lần trong suốt cuốn sách này.

**White Hats versus Black Hats**

In this book, we will identify similarities between professional penetration testers and practitioners of Ninjutsu. However, we also need to understand the function of those that attack networks and systems within the realm of computer security, and distin-guish between what has become a popular method of identifying “good guys” and “bad guys” – white hat hackers and black hat hackers, respectively. The ­concept of two types of “hats” originate from old Westerns movies, where the good guy wears a white cowboy hat and combats those with nefarious intent, who can be identified by their black cowboy hats. It would be fantastic if it was just as easy to identify the “criminal” element in computer crimes by what type of hat they wear, but reality is much more difficult to paint in colors of black and white.

Many definitions of a black hat hacker try to intertwine the concept of ethics and morality with the activities of these “bad” hackers. The problem with including eth-ics in any definition is that ethics is a matter of perspective; hypothetically speaking, a hacker located in China who attacks government systems within the United States may be seen as one of the good guys to the Chinese government in certain circum-stances, whereas that same hacker would be seen as one of the bad guys to those living in the United States. The inability to distinguish the good guy from the bad guy when incorporating ethical perspectives necessitates the need to define white and black hats differently.

To complicate matters, there have been others who have suggested gray hat hack-ers also exist, which can be identified as hackers who fall somewhere in between the actions of white and black hats. Gray hat hackers theoretically have the benefit of additional flexibility in conducting attacks when compared with white hats, yet somehow avoid the negative social (and legal) stigma of being a black hat hacker, because they don’t break the spirit of the law. The disadvantage of adding the concept of a gray hat into the mix means that it makes defining boundaries even that much more difficult when trying to distinguish differences between appropriate and inap-propriate behavior.

|  |  |
| --- | --- |
| Mũ trắng và Mũ đen | **27** |

Mũ Trắng So Với Mũ Đen

Trong cuốn sách này, chúng ta sẽ nhận diện sự tương đồng giữa những người kiểm tra xâm nhập chuyên nghiệp và những người hành nghề Ninjutsu. Tuy nhiên, chúng ta cũng cần phải hiểu chức năng của những người tấn công mạng và hệ thống trong lĩnh vực bảo mật máy tính, và phân biệt giữa những phương pháp phổ biến để nhận diện "người tốt" và "kẻ xấu" – những hacker mũ trắng và hacker mũ đen, tương ứng. Khái niệm về hai loại "mũ" này xuất phát từ những bộ phim miền Tây xưa, trong đó nhân vật chính diện thường đội mũ cao bồi trắng và chống lại những kẻ có âm mưu xấu, những kẻ này có thể nhận diện qua chiếc mũ cao bồi đen. Sẽ thật tuyệt vời nếu việc nhận diện yếu tố “tội phạm” trong các vụ tội phạm máy tính cũng đơn giản như vậy, nhưng thực tế phức tạp hơn nhiều, không thể phân biệt rõ ràng qua những màu sắc đen và trắng.

Nhiều định nghĩa về hacker mũ đen cố gắng kết hợp khái niệm đạo đức và lương tâm với hoạt động của những hacker "xấu" này. Vấn đề khi đưa đạo đức vào bất kỳ định nghĩa nào là đạo đức là vấn đề quan điểm; giả định rằng, một hacker ở Trung Quốc tấn công hệ thống chính phủ Mỹ có thể được coi là người tốt trong mắt chính phủ Trung Quốc trong một số tình huống, trong khi hacker đó sẽ bị coi là kẻ xấu đối với những người sống tại Mỹ. Sự không thể phân biệt được giữa người tốt và kẻ xấu khi kết hợp quan điểm đạo đức này đòi hỏi chúng ta phải định nghĩa lại khái niệm hacker mũ trắng và hacker mũ đen theo một cách khác.

Để vấn đề trở nên phức tạp hơn, có một số người cho rằng còn có hacker mũ xám, những người này được xem là những hacker ở giữa hành động của hacker mũ trắng và mũ đen. Hacker mũ xám lý thuyết có lợi thế là có thêm sự linh hoạt trong việc thực hiện các cuộc tấn công so với hacker mũ trắng, nhưng lại tránh được sự kỳ thị xã hội (và pháp lý) tiêu cực của hacker mũ đen vì họ không phá vỡ tinh thần của pháp luật. Tuy nhiên, việc thêm khái niệm hacker mũ xám vào cuộc thảo luận khiến cho việc xác định ranh giới giữa hành vi phù hợp và không phù hợp trở nên khó khăn hơn.

**Black Hat Hackers**

In an effort to remove confusion and perspective from the definition of white hat and black hat hackers, we can simply center our definitions around the concept of “permissions.” If we define a white hat hacker as someone who has permission by the system owner (typically a high-level manager) to attack a computer system, and a black hat hacker as someone that does not have the necessary permissions, we reach a much clearer understanding of what the differences are between the two groups. The important part in labeling white hats and black hats is removing the concept of morality and ethics from the definition. But what does this mean in practice, then, if we are going to remove ethics from the definition, and how can we justify the use of black hats?

In the reality of cyber warfare or industrial espionage, using our definition of a black hat, those individuals attacking a foreign or competitor’s system would cer-tainly be categorized as black hat hackers because they would be attacking without the approval of the system owners; however, the attackers would be motivated to conduct their attack within the belief that it benefits either family, community, home-land, or a combination of each; by framing their activities within this ethical frame-work, their attack would be seen as legitimate and appropriate by both the attacker and those who would benefit from the attack (such as a government entity).It seems difficult to justify the notion that black hats are potentially beneficial; however, we have already examined how ninja played a part in the development of Japan to undermine armies. To understand the need for unconventional warfare in modern times, we can also look at the need and existence of special military forces, which are designed to conduct clandestine and unconventional warfare and train insurgents in espionage and military tactics.3 An argument can be made that there is a need for clandestine operations in cyber space, just as there is a need to conduct spe-cial ground operations in foreign countries by special force teams. This forces us to accept the notion that black hats can do good, at least from a particular perspective.

1. **CHAPTER 2** The Modern Ninja

**Hacker Mũ Đen**

Để làm rõ sự khác biệt giữa hacker mũ trắng và hacker mũ đen mà không bị nhầm lẫn bởi quan điểm đạo đức và lương tâm, chúng ta có thể đơn giản hóa định nghĩa dựa trên khái niệm "quyền hạn." Nếu chúng ta định nghĩa hacker mũ trắng là những người có sự cho phép từ chủ sở hữu hệ thống (thường là một quản lý cấp cao) để tấn công vào hệ thống máy tính, và hacker mũ đen là những người không có quyền hạn cần thiết, thì chúng ta sẽ có một cái nhìn rõ ràng hơn về sự khác biệt giữa hai nhóm này. Phần quan trọng trong việc gắn nhãn hacker mũ trắng và hacker mũ đen là loại bỏ khái niệm đạo đức và lương tâm khỏi định nghĩa. Nhưng điều này có nghĩa gì trong thực tế, và làm thế nào để biện minh cho việc sử dụng hacker mũ đen?

Trong thực tế của chiến tranh mạng hoặc gián điệp công nghiệp, nếu áp dụng định nghĩa về hacker mũ đen, những cá nhân tấn công vào hệ thống của đối phương hoặc đối thủ chắc chắn sẽ được phân loại là hacker mũ đen vì họ đang tấn công mà không có sự chấp thuận của chủ sở hữu hệ thống; tuy nhiên, những kẻ tấn công này có thể được thúc đẩy bởi niềm tin rằng cuộc tấn công của họ sẽ mang lại lợi ích cho gia đình, cộng đồng, tổ quốc, hoặc một sự kết hợp của cả ba; khi đặt hoạt động của họ trong khuôn khổ đạo đức này, cuộc tấn công sẽ được xem là hợp pháp và phù hợp bởi cả kẻ tấn công lẫn những người sẽ hưởng lợi từ cuộc tấn công (chẳng hạn như một tổ chức chính phủ).

Có thể thấy khó khăn trong việc biện minh cho quan điểm rằng hacker mũ đen có thể mang lại lợi ích; tuy nhiên, chúng ta đã xem xét cách mà ninja đã đóng vai trò trong việc phát triển Nhật Bản, phá hoại các đội quân đối phương. Để hiểu về nhu cầu chiến tranh phi truyền thống trong thời hiện đại, chúng ta cũng có thể nhìn vào nhu cầu và sự tồn tại của các lực lượng quân sự đặc biệt, được thiết kế để thực hiện các chiến dịch bí mật và phi truyền thống, đồng thời huấn luyện những kẻ nổi dậy trong các chiến thuật gián điệp và quân sự. Một luận điểm có thể được đưa ra là có nhu cầu cho các hoạt động bí mật trong không gian mạng, giống như việc cần có các chiến dịch đặc biệt trên mặt đất tại các quốc gia ngoại quốc bởi các đội quân đặc biệt. Điều này buộc chúng ta phải chấp nhận quan điểm rằng hacker mũ đen có thể làm điều tốt, ít nhất là từ một góc độ nhất định.

**White Hat Hackers**

Now that we have a better understanding of what a black hat is, and the beneficial use of unconventional tactics by clandestine teams, let’s see if we can understand the role of a white hat better. When we mention professional penetration testing, or ethi-cal hacking, we conjure up images of professional engineers conducting an attack within a predefined scope of operation. In some cases, the scope can be extremely restricted, certain hacking tools may be excluded, and certain systems designated as “off limits.” Although this may allow the system owners to better understand the risk of a specific threat, penetration testing within a defined scope that limits the actions of the penetration test engineer does not provide the system owner a true understand-ing of the risks that confront an organization. To identify all threats, and thus the true risks to a network or system, the penetration test engineers must be given unre-stricted “movement” to conduct their attacks. The disadvantage to a comprehensive risk assessment and penetration test is often time and money, which forces a lot of organizations to tighten down the scope of the penetration test. Depending on the level of support, the black hat hackers may have significant funding, significant time, significant resources, or a combination of all three, in order to conduct their attack; white hat hackers working for the benefit of corporations rarely have this luxury. To make the most of the funds and time available, penetration testing by white hat hackers is therefore restricted within scope requirements. To ensure repeatability and cost-effectiveness, methodologies are used by the penetration test engineers. The specific methodology used may be obtained through open sources, such as the Infor-mation Systems Security Assessment Framework (ISSAF), Open Source Security Testing Methodology Manual (OSSTMM), the Open Web Application Security Proj-ect (OWASP), or government documents; or the methodology may be developed in-house by the penetration testers themselves by blending different methodologies and frameworks and regulatory requirements.

Regardless of which method is used, the techniques and tools tend to be similar between the methodologies. The use of methodologies does provide some significant advantages, and can be used to find the threats to a system or network using well-known attack vectors.

To complicate matters, those who conduct professional penetration tests under the guise of a white hat hacker are often indoctrinated in information security “best practices” when conducting assessments. This indoctrination exhibits itself in the penetration test by favoring repetitiveness over ingenuity; however, profession-als who have substantial experience in penetration testing will be able to modify and adopt their attacks in a way that deviates from published methodologies. New attack methods within the realm of white hats are relegated to research and develop-ment departments within universities and companies. When compared with black hat hackers, white hat penetration test engineers only improve their methodologies when someone else in the community has released a new approach, or they dedicate time to improve their own approach. It is unfortunate that many new attack vectors are developed by those considered as black hats by the information system security community – malicious hackers. To be truly effective in a professional penetration test, white hat hackers must expand their mindset to be closer to that of a black hat hacker.

|  |  |
| --- | --- |
| White Hats versus Black Hats | **29** |

.

**Hacker Mũ Trắng**

Bây giờ, chúng ta đã có cái nhìn rõ hơn về hacker mũ đen và cách thức sử dụng các chiến thuật phi truyền thống bởi các đội ngũ bí mật, chúng ta sẽ cố gắng hiểu rõ hơn về vai trò của hacker mũ trắng. Khi nhắc đến kiểm tra xâm nhập chuyên nghiệp hay hacking đạo đức, chúng ta hình dung những kỹ sư chuyên nghiệp thực hiện một cuộc tấn công trong phạm vi hoạt động đã được xác định trước. Trong một số trường hợp, phạm vi có thể bị hạn chế nghiêm ngặt, một số công cụ hacking có thể bị loại trừ, và một số hệ thống sẽ được chỉ định là "cấm truy cập." Mặc dù điều này có thể giúp chủ sở hữu hệ thống hiểu rõ hơn về nguy cơ của một mối đe dọa cụ thể, nhưng kiểm tra xâm nhập trong phạm vi hạn chế, giới hạn hành động của kỹ sư kiểm tra xâm nhập, không cung cấp cho chủ sở hữu hệ thống một sự hiểu biết đầy đủ về những rủi ro mà tổ chức phải đối mặt. Để xác định tất cả các mối đe dọa, và do đó là những rủi ro thực sự đối với mạng hoặc hệ thống, các kỹ sư kiểm tra xâm nhập phải được cấp quyền "di chuyển" không hạn chế để tiến hành tấn công. Tuy nhiên, nhược điểm của việc đánh giá rủi ro toàn diện và kiểm tra xâm nhập thường là thời gian và chi phí, điều này khiến nhiều tổ chức phải thu hẹp phạm vi của kiểm tra xâm nhập. Tùy thuộc vào mức độ hỗ trợ, hacker mũ đen có thể có nguồn tài trợ đáng kể, thời gian và tài nguyên, hoặc sự kết hợp của tất cả ba yếu tố, để tiến hành cuộc tấn công; trong khi đó, hacker mũ trắng làm việc vì lợi ích của các công ty lại hiếm khi có những đặc quyền này. Để tối đa hóa thời gian và nguồn lực có sẵn, kiểm tra xâm nhập của hacker mũ trắng vì thế bị giới hạn trong các yêu cầu phạm vi.

Để đảm bảo tính lặp lại và hiệu quả về chi phí, các phương pháp được sử dụng bởi các kỹ sư kiểm tra xâm nhập. Phương pháp cụ thể có thể được lấy từ các nguồn mở, như là Framework Đánh giá Bảo mật Hệ thống Thông tin (ISSAF), Hướng dẫn Phương pháp Kiểm tra Bảo mật Mã nguồn Mở (OSSTMM), Dự án Bảo mật Ứng dụng Web Mở (OWASP), hoặc các tài liệu chính phủ; hoặc phương pháp có thể được phát triển trong nội bộ bởi chính các kỹ sư kiểm tra xâm nhập bằng cách kết hợp các phương pháp và khuôn khổ khác nhau và các yêu cầu quy định.

Dù sử dụng phương pháp nào, các kỹ thuật và công cụ thường giống nhau giữa các phương pháp. Việc sử dụng phương pháp cung cấp một số lợi thế đáng kể và có thể được sử dụng để tìm ra các mối đe dọa đối với hệ thống hoặc mạng sử dụng các vector tấn công đã được biết đến.

Để làm phức tạp thêm vấn đề, những người thực hiện kiểm tra xâm nhập chuyên nghiệp dưới danh nghĩa hacker mũ trắng thường được huấn luyện trong các "thực hành tốt nhất" về bảo mật thông tin khi tiến hành đánh giá. Sự huấn luyện này thể hiện trong kiểm tra xâm nhập qua việc ưu tiên sự lặp đi lặp lại thay vì sáng tạo; tuy nhiên, những chuyên gia có kinh nghiệm đáng kể trong kiểm tra xâm nhập sẽ có thể sửa đổi và áp dụng các cuộc tấn công của họ theo cách khác biệt so với các phương pháp đã công bố. Các phương pháp tấn công mới trong phạm vi của hacker mũ trắng thường chỉ được nghiên cứu và phát triển bởi các phòng ban nghiên cứu trong các trường đại học và công ty. So với hacker mũ đen, các kỹ sư kiểm tra xâm nhập mũ trắng chỉ cải tiến phương pháp của họ khi có ai đó trong cộng đồng công bố một cách tiếp cận mới, hoặc họ dành thời gian để cải tiến phương pháp của chính mình. Thật không may, nhiều vector tấn công mới lại được phát triển bởi những người bị coi là hacker mũ đen trong cộng đồng bảo mật hệ thống thông tin – những hacker độc hại. Để thực sự hiệu quả trong một kiểm tra xâm nhập chuyên nghiệp, hacker mũ trắng phải mở rộng tư duy của mình để gần gũi hơn với tư duy của hacker mũ đen.