Bài: 1.4 Giới thiệu về Ethical Hacking - Khái niệm và phạm vi của Ethical Hacking

Xem bài học trên website để ủng hộ Kteam: 1.4 Giới thiệu về Ethical Hacking - Khái niệm và phạm vi của Ethical Hacking

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!

Khái niệm và phạm vi của Ethical Hacking

Ethical Hacking

Các bài kiểm tra **Ethical hacking** và đánh giá mức độ an toàn bằng cách **thử tấn công vào hệ thống** (penetration test) đã trở thành những thuật ngữ phổ biến trong lĩnh vực an toàn môi trường thông tin một thời gian khá dài. Sự gia tăng các loại tội phạm công nghệ cao và tin tặc đã đặt ra thách thức lớn với các chuyên gia bảo mật, các nhà phân tích, điều chỉnh trong suốt thập kỷ qua. Một cuộc chiến, giữa tin tặc (Hacker) và các chuyên gia an ninh.

Thử thách đầu tiên và cơ bản đối với các chuyên gia an ninh là **tiên phong tìm kiếm, định vị những điểm yếu, những gì còn thiếu hụt** trong các hệ thống, thiết bị, phần mềm hiện hành lẫn trong tương lai. Khi bạn chủ động khảo sát, điều tra trước khi bị tấn công thay vì chờ đến lúc bị sập bẫy của những kẻ tấn công và cố gắng chống lại chúng, chi phí bạn phải bỏ ra sẽ thấp hơn nhiều. Về khía cạnh an toàn, bảo vệ và ngăn chặn, những tổ chức luôn có những đội ngũ nội bộ thành lập ra nhằm thực hiện "**penetration test**" cũng như ký hợp đồng với các chuyên gia bảo mật, phòng cho những trường hợp họ rơi vào cuộc tấn công nguy hiểm diện rộng

---

Vì sao Ethical Hacking quan trọng

Sự gia tăng số lượng các loại mã độc, tội phạm công nghệ cao và sự xuất hiện của nhiều loại hình tấn công tân tiến hơn đặt ra thách thức cho những nhà thử nghiệm an toàn của hệ thống bằng cách thử tấn công vào hệ thống đó (Penetration tester). Họ kiểm tra độ an toàn của hệ thống, để xác đinh, chuẩn bị phương án phòng ngừa và sửa chữa chống lại mối đe dọa từ các cuộc tấn công.

Những loại tấn công nguy hiểm và tân tiến bao gồm:

- Tấn công từ chối quyền dịch vụ
- điều khiển, vận hành dữ liệu
- Danh tặc
- Phá hoại
- Trộm thẻ tín dụng
- Ăn trộm bản quyền
- Ăn cắp dịch vụ

Sự gia tăng những phương thức tấn công, những vụ "hack", và tấn công công nghệ cao là bởi vì sự tăng trưởng của việc thực hiện công việc "online" và các dịch vụ online trong thập kỷ qua. Sức hấp dẫn đối với hacker sẽ càng lớn nếu đó là thông tin về tài chính. Luật máy tính hoặc luật về tội phạm công nghệ cao chỉ có thể làm giảm các trò chơi khăm, trong khi các cuộc tấn công thực sự và tội phạm công nghệ cao càng ngày càng cao.
Pentester, cách nói ngắn gọn của Penetration tester, là những người chủ yếu tìm kiếm các lỗ hổng, các điểm dễ tổn thương trong hệ thống trước khi bị tấn công

---

Các giai đoạn của Ethical Hacking

1. Nhận dạng dấu vết và thăm dò
2. Quét
3. Đánh số, liệt kê
4. Leo thang quyền lợi
5. Xóa dấu vết

Những kỹ năng cần biết về công nghệ

1. **Ethical hacker** có hiểu biết sâu sắc về hầu hết các hệ điều hành, bao gồm tất cả những hệ điều hành phổ biến như Windows, Linux, Unix và Macintosh
2. Những hacker này rất giỏi về mạng, có những khái niệm từ cơ bản đến chi tiết về công nghệ, và khả năng khám phá phần cứng và phần mềm.
3. Ethical hacker phải có sự kiểm soát mạnh mẽ trong lĩnh vực an ninh, những vấn đề liên quan và lĩnh vực công nghệ.
4. Họ phải có kiến thức chi tiết về các loại tấn công, từ cổ lỗ, cơ bản tới tiên tiến, phức tạp.

Những kĩ năng không cần công nghệ

1. Kỹ năng học hỏi
2. Kỹ năng giải quyết vấn đề
3. Kỹ năng giao tiếp
4. Cống hiến khả năng cho luật bảo mật
5. Có ý thức về pháp luật, tiêu chuẩn và điều lệ