Những công cụ Hacking luôn là rất quan trọng đối với người làm bảo mật. Họ cần phải nắm rõ được nguyên lý hoạt động của các phần mềm này, từ đó lên được phương án bảo mật thích hợp. Vì thế, bài viết này sẽ giới thiệu đến bạn đọc "Những Tool dành cho Hệ điều hành Kali Linux mà người làm bảo mật nên biết ", đây đều là những Tool thông dụng đối với các hacker, được sử dụng hàng ngày.
Bạn đang xem: Học kali linux
Hầu hết những Tool này cũng đã được đóng gói sẵn trong hệ điều hành Kali Linux. Nói về phần mềm hacking, hiện có hơn 300+ công cụ được thiết kế để phục vụ cho công việc này, An Ninh Mạng sẽ cố gắng có những bài viết chi tiết về từng công cụ sau này.
Để trở thành một Hacker mũ trắng chưa bao giờ là công việc dễ dàng. Ngay khi vừa bắt đầu tiếp xúc với lĩnh vực, bạn sẽ ngay lập tức nhận ra được điều này. Chỉ để thực hiện một thủ thuật hack bình thường, một hacker đã cần phải nắm vững được nhiều lĩnh vực khác nhau như code, mạng, bảo mật… Một số ngôn ngữ mà hacker cần phải nắm vững như là C++, Python, HTL …
Mặc dù vậy, với việc công nghệ luôn thay đổi không ngừng, việc tiếp tục học hỏi chưa bao giờ là đủ. Với hacker, thì tốc độ cập nhật công nghệ càng phải được tăng cao hơn nhiều.
Có gì mới trong hệ điều hành Kali Linux 2.0 ?
Đã từ lâu Kali Linux được xem là hệ điều hành hoàn hảo nhất cho hacker thực tập công việc hacking của mình. Kali Linux 2.0 với gói công cụ hacking được cài đặt sẵn giúp người dùng tiết kiệm thời gian để tìm các gói cài đặt trên mạng.
Top Kali Linux Tools :
Bây giờ chúng ta sẽ cùng nhau tìm hiểu về một số Tool được nhiều hacker dùng nhất.
Metasploit :
Là Framework dùng để phát triển lỗi khai thác, shellcodes, fuzzing tool, payloads. Bộ Framework này có rất nhiều công cụ khai thác được tích hợp. Framework có sẵn trên nhiều hệ điều hành phổ biến như Mac OSX, Windows, Linux và được cài đặt sẵn trong Kali Linux. Nó thường được dùng để các hacker mũ trắng tấn công vào hạ tầng mạng của họ, từ đó tìm ra những lỗi bảo mật để sửa chữa kịp thời.
Dưới đây là Video Demo cách sử dụng Metasploit :
Ngoài ra Metasploit còn được dùng để nhắm đến các mục tiêu như ứng dụng web, mạng và server… Giao diện của Metasploit có cả đồ họa và command line. Sẽ có 2 phiên bản miễn phí và Metasploit Pro trả phí.
Nmap (Network Mapper) :
Nmap được dùng để scan cả hệ thống và tìm ra các port nào đang được mở. Với hacker mũ trắng, công
cụ này được dùng để phát hiện máy tính nào đang online, và khảo sát bảo mật, các cổng đang mở cũng như service nào đang được chạy. Công cụ sử dụng các gói tin IP để biết host nào đang hoạt động trên hệ thống mạng, cổng nào đang mở cũng như các dịch vụ chạy trên nó. Tool có 2 giao diện GUI và command line. Zenmap là giao diện người dùng được khuyến khích sử dụng dành cho newbie, lần đầu tiên tiếp xúc với command line, và sau đó chuyển qua GUI nếu bạn thấy tự tin.
Armitage :
Armitage là một công cụ quản lý tấn công mạng đồ họa, cung cấp giao diện GUI, giúp người dùng dễ tiếp cận và sử dụng. Nếu bạn thực sự muốn nắm vững về cơ bản cũng như các tính năng nâng cao trong tấn công mạng, Armitage sẽ là lựa chọn phù hợp nhất với các tính năng dò tìm, truy cập, khai thác…
Ngoài ra, nếu bạn đang làm việc cùng với nhóm, phần mềm còn có nhiều chế độ hữu ích để chia sẻ cho các thành viên khác cùng làm việc :

Cùng sử dụng phiên.Share host bị tấn công, dữ liệu thu được, download file…Hỗ trợ giao tiếp cùng nhau thông qua một share log.Chạy bot tự động thực hiện công việc.**Jhon The Ripper (JTR) :**

Jhon The Ripper là công cụ phổ biến để phá Password, được biết đến nhiều hơn với tên viết tắt JTR. Jhon The Ripper sử dụng những text file, còn được gọi là "wordlist", file này chứa những password thông dụng và những password đã từng bị phá, sau đó công cụ sẽ lần lượt thử từng password cũng như những tổ hợp các text để tìm ra password nạn nhân.
Về phương pháp, Jhon The Ripper khá tương tự với THC Hydra, tuy nhiên JTR được dùng để crack password offline thì THC Hydra lại được dùng để crack password các service online.

Wireshark :

Wireshark là công cụ mã nguồn mở, được dùng để phân tích mạng, traffic của hệ thống, các

gói tin… Với tên gọi cũ là Ethereal, Wireshark có thể chặn lưu lượng mạng, từ những thông tin kết nối đến từng bit của gói tín hiệu. Tất cả tác vụ này được thực hiện trong thời gian thực và hiển thị cho người dùng ở định dạng có thể đọc được.
Trong nhiều năm qua, Wireshark đã có nhiều sự thay đổi, nâng cấp đáng giá như là các bộ lọc, màu sắc các gói tin… việc này đã giúp ích nhiều cho nhà quản trị mạng quản lý và phân tích được những gì đang diễn ra trong hệ thống mạng của họ.
Ghi chú : nếu bạn thực sự có hứng thú và muốn trở thành một nhà quản trị mạng chuyên nghiệp, thì việc sử dụng và nắm vững Wireshark là một kỹ năng bắt buộc. Hiện nay trên Internet có rất nhiều tài liệu về Wireshark để người dùng nghiên cứu.
Xem thêm: Giá Trứng Cút Bao Nhiêu 1 Chục, Trứng Cút Lộn, Trứng
THC Hydra :
Như đã trình bày ở trên, THC Hydra là tool để crack password và cùng với Jhon The Ripper là 2 tool được cấu hình thủ công. THC Hydra còn được biết đến với tên rút gọn là Hydra, là công cụ hack password thông dụng, được dùng để hack Password login qua mạng, sử dụng cả 2 phương pháp Brute Force Attack và Dictionary Attack tại trang đăng nhập. Phần mềm hỗ trợ tấn công nhiều giao thức mạng phổ biến như SSH, Mail (POP3, IMAP), Database, SMB, VNC, LDAP…
Dưới đây là Video Demo sử dụng Brute Force Attack :
Burp Suite :
Burp Suite là một ứng dụng nền Web, giúp kiểm tra khả năng thâm nhập. Phần mềm là công cụ mạnh mẽ, có nhiều tính năng hacking mà có thể bạn đang tìm kiếm. Dưới đây là danh sách các thành phần tính năng của Burp Suite :
Intercepting Proxy : tính năng này cho phép kiểm tra và chỉnh sửa tất cả các gói tin yêu cầu và phản hồi trả về của trình duyệt.
Spider : công cụ tiện dụng dùng để liệt kê tất cả các thư mục và tập tin trên máy chủ.
Web Scanner : phát hiện các lỗ hổng đang hiện hiện trên Website.
Intruder : tính năng cho phép tạo và tùy chỉnh các cuộc tấn công để tìm và khai thác các lỗi không mong muốn.
Repeater : chỉnh sửa và gửi trả lại bất cứ gói tin request riêng lẻ nào.
Sequencer : kiểm tra tính ngẫu nhiên của các token (csrf , authenticity_token).
Extensions : cho phép người dùng viết và add plugin tự phát triển này vào gói công cụ, hoặc download các bản plugin có sẵn để add thêm, giúp đa dạng hơn trong các cuộc tấn công.
Bản Pro cũng cho phép người dùng Donate những plugin này.
OWASP Zed :
OWASP Zed Attack Proxy (ZAP) được biết đến như một công cụ Proxy, có thể dự phòng khá tốt cho công cụ Burp Suite, ưu điểm của ZAP là miễn phí và mã nguồn mở.
Công cụ được phát triển với mục đích tìm những lỗ hổng trong ứng dụng Web. Với cộng đồng người dùng rộng lớn có tên OWASP security Community, người mới làm quen có thể dễ dàng sử dụng cũng như nhận được sự hỗ trợ khá tốt. Bạn có thể dùng OWASP Zed Attack Proxy để scan đối tượng, thực hiện các chiến dịch Scan tự động, tìm ra các lỗ hổng, thực hiện test thủ công…
Social Engineering Toolkit :
The Social-Engineering Toolkit còn được biết đến với tên thông dụng hơn là SET là công cụ hữu ích để thực hiện các cuộc tấn công nhắm vào yếu tố con người hơn là hệ thống. Công cụ có nhiều tính năng cho phép hacker gửi email, trong đó có kèm các backdoor Java applet. Phần mềm có giao diện command line và có thể chạy trên các hệ điều hành Linux, Mac OS X và Windows.
Aircrack-ng :

Thêm một tool để crack password, tuy nhiên đặc biệt hơn, Aircrack-ng được thiết kế để crack password Wifi. Đối với những người mới lần đầu tiếp xúc với phần mềm này, Aircrack-ng có thể phá các loại pass wifi theo chuẩn 802.11 WEP và WPA-PSK. Cơ chế hoạt động của Tool sẽ capture các gói tin có chứa password, sau đó thực hiện giải mã chúng. Aircrack-ng được xem là một trong những Tool hàng đầu trong việc bẻ khóa Password Wifi.

Maltego :

Tool này thu thập mọi dữ liệu của đối tượng từ internet như Email, Dns record… công cụ có thể thu thập dữ liệu cả cá nhân và network…

Ettercap :

Phần mềm mã nguồn mở này được cung cấp miễn phí, và thường được dùng để thực hiện các cuộc tấn công trong mạng Lan. Ettercap được dùng để phân tích các Protocol mạng và theo dõi an ninh hệ thống. Hiện phần mềm có mặt ở hầu hết các hệ điều hành như Windows, Unix, Linux BSD, và các distro khác.

Nikto Website Vulnerability Scanner :

Nikto là phần mềm mã nguồn mở, scan và tìm ra các lỗ hổng trên Web Server. Hệ thống search dựa vào cơ sở dữ liệu 6800 file / chương trình có ẩn chứa nguy hiểm, kiểm tra các hệ thống chưa được cập nhật bản vá.

Xem thêm: Nghĩa Của Từ Lion Là Gì ? Lion Nghĩa Là Gì Trong Tiếng Việt

Tổng kết :

Trên đây là bảng liệt kê một số công cụ hữu ích để test hệ thống, ngoài ra vẫn còn khá nhiều chương trình khác, nếu tận dụng linh hoạt sẽ mang đến cho nhà quản trị những kết quả tốt.

tool kali linuxtool kali linux hackingtool kali linux hack wifihack wifi kali linux

Chuyên mục: Hỏi Đáp