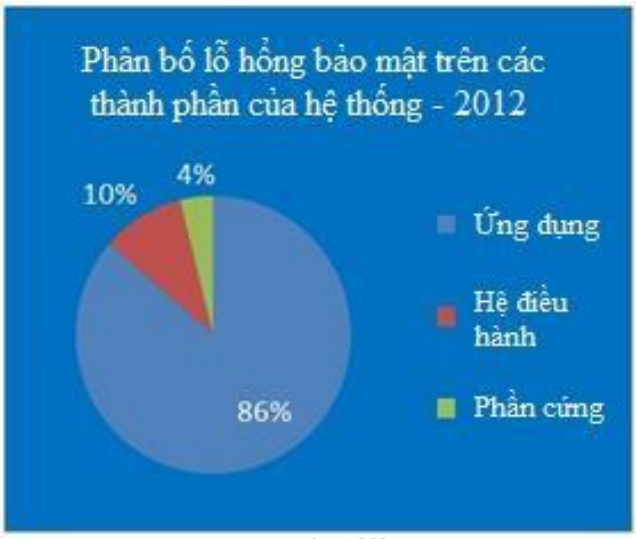
Chương 2 giới thiệu khái quát về mối đe dọa, điểm yếu, lỗ hổng tồn tại trong hệ thống và tấn công. Phần tiếp theo phân tích chi tiết các dạng tấn công điển hình vào các hệ thống máy tính và mạng, bao gồm tấn công vào mật khẩu, tấn công nghe lén, người đứng giữa, tấn công DoS, DDoS, tấn công sử dụng các kỹ thuật xã hội,… Nửa cuối của chương đề cập đến các dạng phần mềm độc hại, gồm cơ chế lây nhiễm và tác hại của chúng. Kèm theo phần mô tả mỗi tấn công, hoặc phần mềm độc hại, chương đề cập các biện pháp, kỹ thuật phòng chống.

1. Khái quát về mối đe dọa, điểm yếu, lỗ hổng và tấn công

1.1 Khái niệm mối đe dọa, điểm yếu, lỗ hổng và tấn công

Mối đe dọa (Threat) là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống. Các tài nguyên hệ thống bao gồm phần cứng, phần mềm, cơ sở dữ liệu, các file, dữ liệu, hoặc hạ tầng mạng vật lý,…

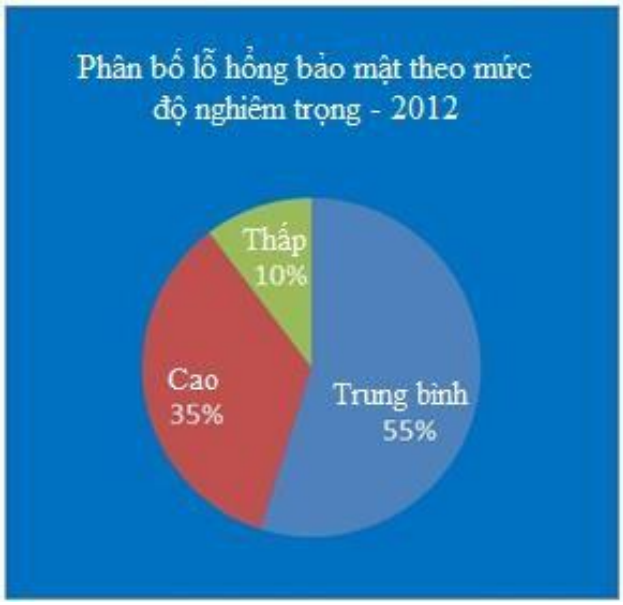
Các điểm yếu hệ thống (System weaknesses) là các lỗi hay các khiếm khuyết tồn tại trong hệ thống. Nguyên nhân của sự tồn tại các điểm yếu có thể do lỗi thiết kế, lỗi cài đặt, lỗi lập trình, hoặc lỗi quản trị, cấu hình hoạt động. Các điểm yếu có thể tồn tại trong cả các mô đun phần cứng và các mô đun phần mềm. Một số điểm yếu được phát hiện và đã được khắc phục. Tuy nhiên, có một số điểm yếu được phát hiện nhưng chưa được khắc phục, hoặc các điểm yếu chưa được phát hiện, hoặc chỉ tồn tại trong một điều kiện đặc biệt nào đó.



Hình 2.1. Phân bố lỗ hổng bảo mật trong các thành phần của hệ thống

Lỗ hổng bảo mật (Security vulnerability) là một điểm yếu tồn tại trong một hệ thống cho phép tin tặc khai thác gây tổn hại đến các thuộc tính an ninh của hệ thống đó, bao gồm tính toàn vẹn, tính bí mật, tính sẵn dùng. Nói chung, lỗ hổng bảo mật tồn tại trong tất cả các thành phần của hệ thống, bao gồm phần

cứng, hệ điều hành và các phần mềm ứng dụng. Theo số liệu thống kê từ Cơ sở dữ liệu lỗ hổng quốc gia Hoa Kỳ [6], trong năm 2012, phân bố lỗ hổng bảo mật được phát hiện trên các thành phần của hệ thống lần lượt là phần cứng – 4%, hệ điều hành – 10% và phần mềm ứng dụng – 86%, như minh họa trên Hình 2.1. Như vậy, có thể thấy các lỗ hổng bảo mật chủ yếu xuất hiện trong hệ thống phần mềm và phần lớn tồn tại trong các phần mềm ứng dụng.



Hình 2.2. Phân bố lỗ hổng bảo mật theo mức độ nghiêm trọng

Phụ thuộc vào khả năng bị khai thác, các lỗ hổng bảo mật có mức độ nghiêm trọng (severity) khác nhau. Theo Microsoft, có 4 mức độ nghiêm trọng của các lỗ hổng bảo mật: *nguy hiểm* (Critical), *quan trọng* (Important), *trung bình* (Moderate) và *thấp* (Low). Tuy nhiên, một số tổ chức khác chỉ phân loại các lỗ hổng bảo mật theo 3 mức độ nghiêm trọng: *cao* (High), *trung bình* (Medium) và *thấp* (Low). Cũng theo số liệu thống kê từ [6] cho trên Hình 2.2, các lỗ hổng có mức độ nghiêm trọng cao chiếm 35%, các lỗ hổng có mức độ nghiêm trọng trung bình chiếm 55% và các lỗ hổng có mức độ nghiêm trọng thấp chỉ chiếm 10%. Như vậy, ta có thể thấy, đa số các lỗ hổng bảo mật có mức độ nghiêm trọng từ trung bình trở lên và cần được xem xét khắc phục càng sớm càng tốt.

Tấn công (Attack) là một, hoặc một chuỗi các hành động vi phạm các chính sách an ninh an toàn của cơ quan, tổ chức, gây tổn hại đến các thuộc tính bí mật, toàn vẹn và sẵn dùng của thông tin, hệ thống và mạng. Một cuộc tấn công vào hệ thống máy tính hoặc các tài nguyên mạng thường được thực hiện bằng cách khai thác các lỗ hổng tồn tại trong hệ thống. Như vậy, tấn công chỉ có thể trở thành hiện thực nếu có sự tồn tại đồng thời của mối đe dọa và lỗ hổng, hay có thể nói:

Tấn công = Mối đe dọa + Lỗ hổng

Như vậy, mối đe dọa và lỗ hổng bảo mật có quan hệ hữu cơ với nhau: Các mối đe dọa thường khai thác một hoặc một số lỗ hổng bảo mật đã biết để thực hiện các cuộc tấn công phá hoại. Điều này có nghĩa là nếu tồn tại một lỗ hổng trong hệ thống, sẽ có khả năng một mối đe dọa trở thành hiện thực. Nói chung, không thể triệt tiêu được hết các mối đe dọa do đó là yếu tố khách quan, nhưng có thể giảm thiểu các lỗ hổng, qua đó giảm thiểu khả năng bị khai thác để thực hiện tấn công.

1.2 Các dạng mối đe dọa thường gặp

Trên thực tế, không phải tất cả các mối đe dọa đều là ác tính hay độc hại (malicious). Một số mối đe dọa là chủ động, cố ý, nhưng một số khác chỉ là ngẫu nhiên, hoặc vô tình. Các mối đe dọa thường gặp đối với thông tin, hệ thống và mạng:

- Phần mềm độc hại
- Kẻ tấn công ở bên trong
- Kẻ tấn công ở bên ngoài
- Hư hỏng phần cứng hoặc phần mềm
- Mất trộm các thiết bị
- Tai họa thiên nhiên
- Gián điệp công nghiệp
- Khủng bố phá hoại.

1.3 Các loại tấn công

Có thể chia tấn công theo mục đích thực hiện thành 4 loại chính như sau:

- Giả mạo (Fabrications): Tấn công giả mạo thông tin thường được sử dụng để đánh lừa người dùng thông thường;
- Chặn bắt (Interceptions): Tấn công chặn bắt thường liên quan đến việc nghe lén trên đường truyền và chuyển hướng thông tin để sử dụng trái phép;
- Gây ngắt quãng (Interruptions): Tấn công gây ngắt quãng làm ngắt, hoặc chậm kênh truyền thông, hoặc làm quá tải hệ thống, ngăn cản việc truy nhập dịch vụ của người dùng hợp pháp;
- Sửa đổi (Modifications): Tấn công sửa đổi liên quan đến việc sửa đổi thông tin trên đường truyền hoặc sửa đổi dữ liệu file.

Theo hình thức thực hiện, có thể chia các loại tấn công thành 2 kiểu chính như sau:

- Tấn công chủ động (Active attacks): Tấn công chủ động là một đột

nhập, xâm nhập (intrusion) về mặt vật lý vào hệ thống, hoặc mạng. Các tấn công chủ động thực hiện sửa đổi dữ liệu trên đường truyền, sửa đổi dữ liệu trong file, hoặc giành quyền truy nhập trái phép vào máy tính hoặc hệ thống mạng.

- Tấn công thụ động (Passive attacks): Tấn công thụ động thường không gây ra thay đổi trên hệ thống. Các tấn công thụ động điển hình là nghe trộm và giám sát lưu lượng trên đường truyền.

Trên thực tế, tấn công thụ động thường là giai đoạn đầu của tấn công chủ động, trong đó tin tặc sử dụng các kỹ thuật tấn công thụ động để thu thập các thông tin về hệ thống, mạng, và trên cơ sở thông tin có được sẽ lựa chọn kỹ thuật tấn công chủ động có xác suất thành công cao nhất.

2. Các công cụ hỗ trợ tấn công

Các công cụ hỗ trợ tấn công (Attacking assistant tools) là các công cụ phần cứng, phần mềm, hoặc các kỹ thuật hỗ trợ kẻ tấn công, tin tặc (attacker) thu thập các thông tin

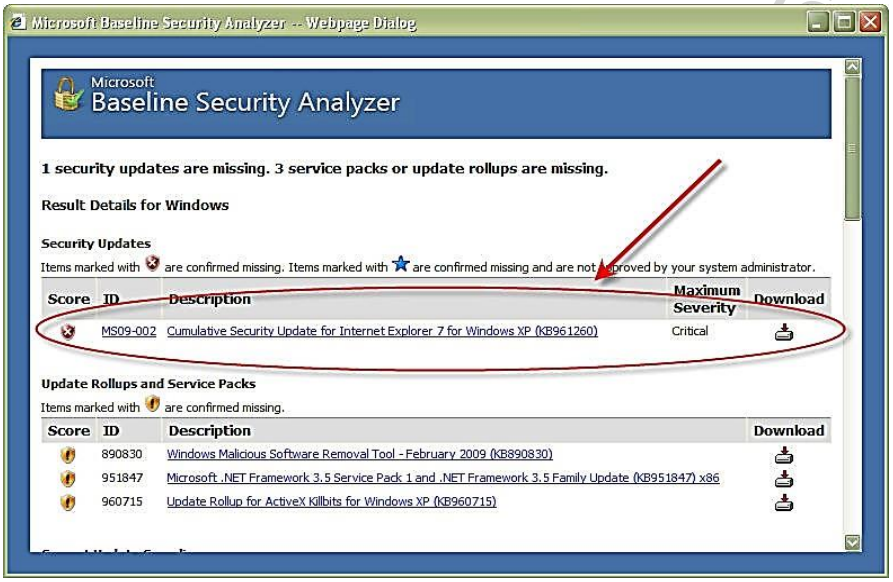
về các hệ thống máy tính, hoặc mạng. Trên cơ sở các thông tin thu được, tin tặc sẽ lựa chọn công cụ, kỹ thuật tấn công có xác suất thành công cao nhất. Các công cụ hỗ trợ tấn công bao gồm 4 nhóm chính: công cụ quét điểm yếu, lỗ hổng bảo mật, công cụ quét cổng dịch vụ, công cụ nghe lén và công cụ ghi phím gõ.

2.1 Công cụ rà quét lỗ hổng, điểm yếu hệ thống

Các công cụ rà quét các điểm yếu hệ thống và lỗ hổng bảo mật có thể được người quản trị sử dụng để chủ động rà quét các hệ thống, nhằm tìm ra các điểm yếu và lỗ hổng bảo mật tồn tại trong hệ thống. Trên cơ sở kết quả rà quét, phân tích và đề xuất áp dụng các biện pháp khắc phục phù hợp. Mặt khác, các công cụ này cũng có thể được kẻ tấn công sử dụng để rà quét hệ thống và dựa trên kết quả rà quét điểm yếu, lỗ hổng để quyết định dạng tấn công có khả năng thành công cao nhất. Các công cụ bao gồm, các công cụ rà quét lỗ hổng bảo mật hệ thống, và các công cụ rà quét lỗ hổng ứng dụng web, hay các trang web.

2.1.1 Công cụ rà quét lỗ hổng bảo mật hệ thống

Các công cụ rà quét lỗ hổng bảo mật hệ thống cho phép rà quét hệ thống, tìm các điểm yếu và các lỗ hổng bảo mật. Đồng thời, chúng cũng cung cấp phần phân tích chi tiết từng điểm yếu, lỗ hổng, kèm theo là hướng dẫn khắc phục, sửa chữa. Các công cụ được sử dụng rộng rãi là Microsoft Baseline Security Analyzer (Hình 2.3) cho rà quét các hệ thống chạy hệ điều hành Microsoft Windows và Nessus Vulnerability Scanner cho rà quét các hệ thống chạy nhiều loại hệ điều hành khác nhau.

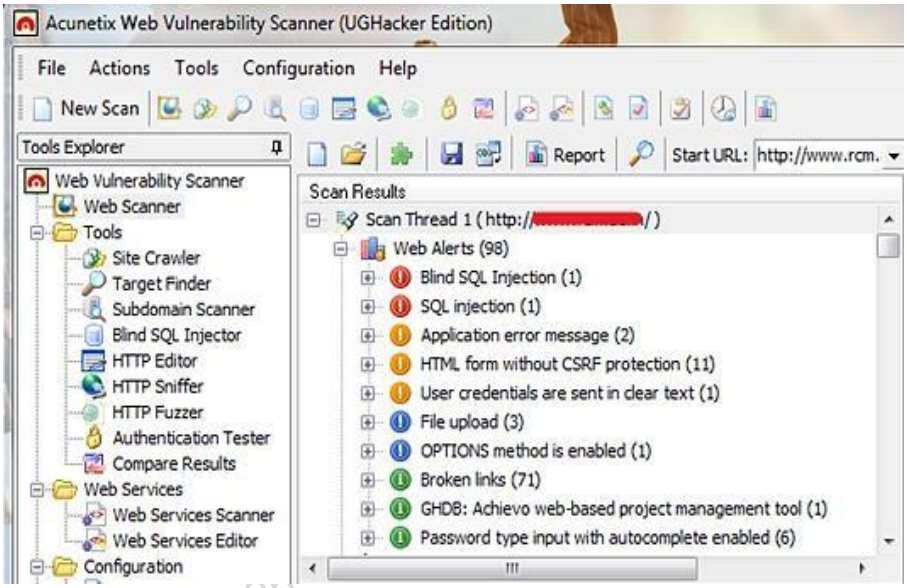


Hình 2.3. Báo cáo kết quả quét của Microsoft Baseline Security Analyzer

2.1.2 Công cụ rà quét lỗ hổng ứng dụng web

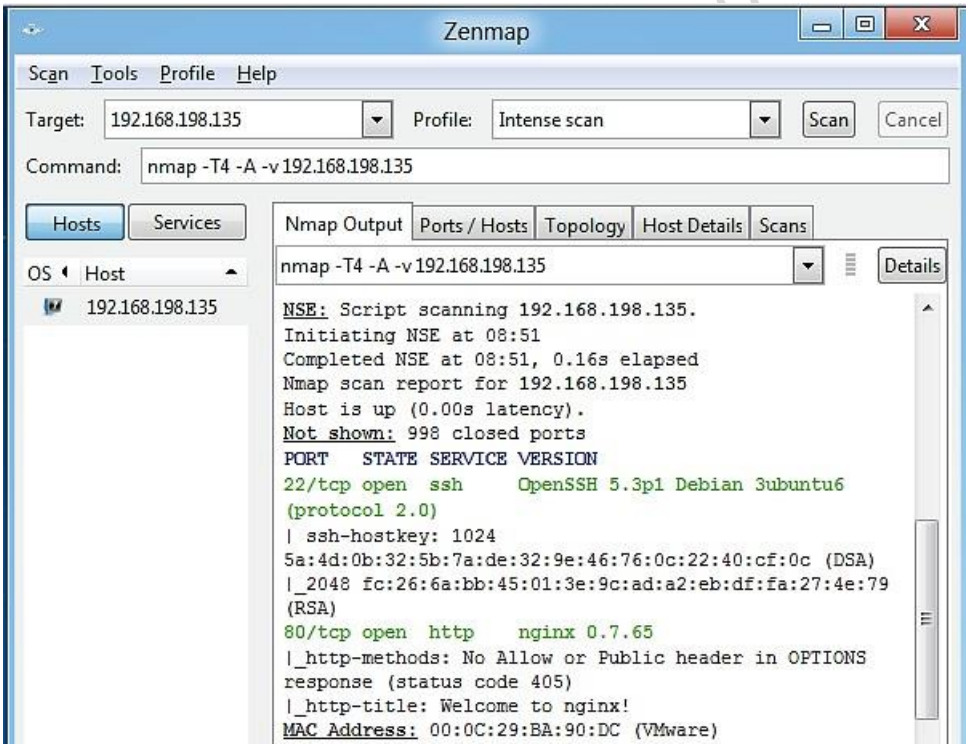
Các công cụ rà quét lỗ hổng ứng dụng web cho phép rà quét, phân tích các trang web, tìm các lỗi và lỗ hổng bảo mật. Chúng cũng hỗ trợ phân tích tình trạng các lỗi tìm được, như các lỗi XSS, lỗi chèn mã SQL, lỗi CSRF, lỗi bảo mật phiên,… Các công cụ được sử

dụng phổ biến bao gồm Acunetix Web Vulnerability Scanner (Hình 2.4), IBM AppScan, Beyond Security AVDS và SQLmap.



Hình 2.4. Kết quả quét website sử dụng Acunetix Web Vulnerability Scanner

2.2 Công cụ quét cổng dịch vụ



Hình 2.5. Giao diện của công cụ Zenmap

Các công cụ quét cổng dịch vụ (Port scanners) cho phép quét các cổng, tìm các cổng đang mở, đang hoạt động, đồng thời tìm các thông tin về ứng dụng, dịch vụ và hệ điều hành đang hoạt động trên hệ thống. Dựa trên thông tin quét cổng dịch vụ, có thể xác định được dịch vụ, ứng dụng nào đang chạy trên hệ thống:

- Cổng 80/443 mở có nghĩa là dịch vụ web đang hoạt động;
- Cổng 25 mở có nghĩa là dịch vụ gửi/nhận email SMTP đang hoạt động;
- Cổng 1433 mở có nghĩa là máy chủ Microsoft SQL Server đang hoạt động;
- Cổng 53 mở có nghĩa là dịch vụ tên miền DNS đang hoạt động,...

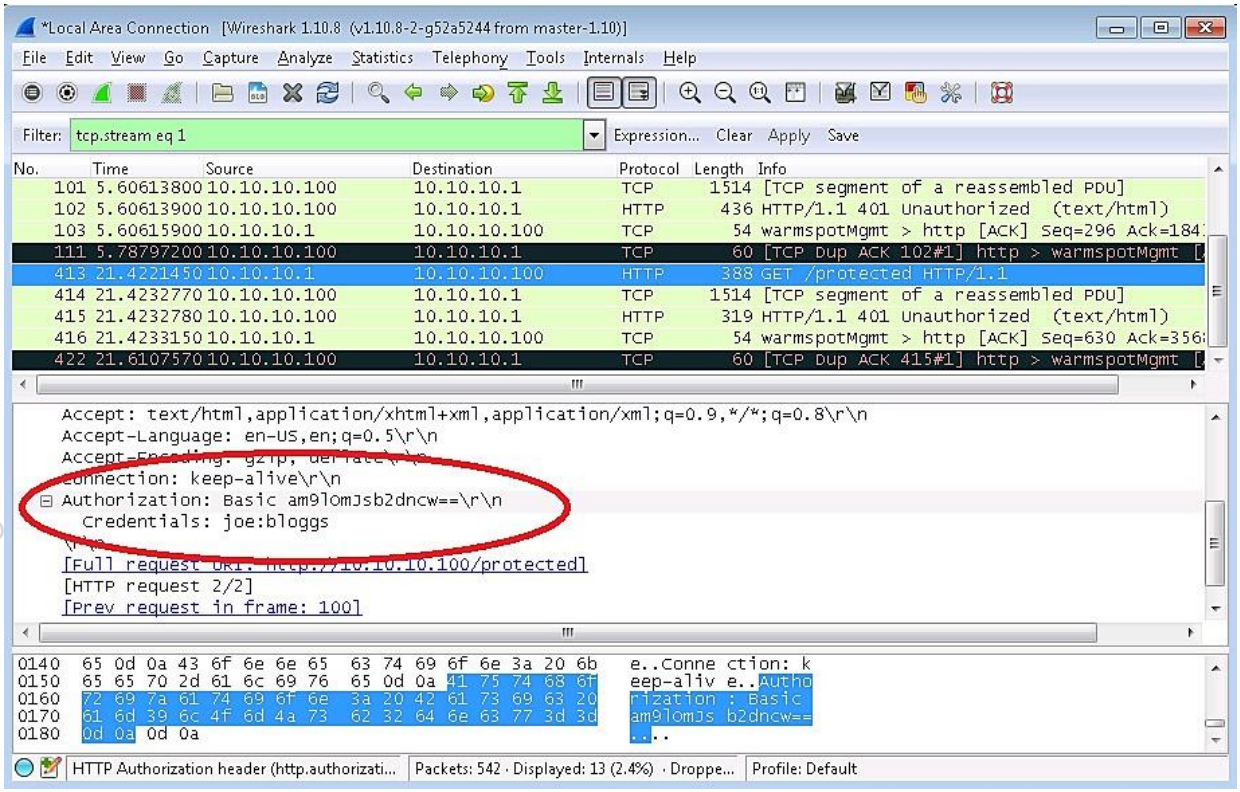
Các công cụ quét cổng dịch vụ được sử dụng phổ biến bao gồm: Nmap, Zenmap, Portsweep, Advanced Port Scanner, Angry IP Scanner, SuperScan và NetScanTools. Hình 2.5 là giao diện của công cụ quét cổng dịch vụ Nmap/ Zenmap – một trong các công cụ quét cổng dịch vụ được sử dụng rộng rãi. Nmap cung cấp tập lệnh rà quét rất mạnh. Tuy nhiên, Nmap hơi khó dùng do chỉ hỗ trợ giao diện dòng lệnh.

2.3 Công cụ nghe trộm

Công cụ nghe trộm hay nghe lén (Sniffers) cho phép bắt các gói tin khi chúng được truyền trên mạng. Công cụ nghe lén có thể là mô đun phần cứng, phần

mềm hoặc kết hợp. Các thông tin nhạy cảm như thông tin tài khoản, thẻ tín dụng, hoặc mật khẩu nếu không được mã hóa thì có thể bị kẻ tấn công nghe lén khi được truyền từ máy trạm đến máy chủ và bị lạm dụng. Một số công cụ phần mềm cho phép bắt gói tin truyền trên mạng:

- Tcpdump
- Wireshark (minh họa trên Hình 2.6)
- Pcap / Wincap / Libcap (Packet capture)
- IP Tools (http://www.softpedia.com).



Hình 2.6. Sử dụng Wireshark để bắt gói tin có chứa thông tin nhạy cảm

2.4 Công cụ ghi phím gõ

Công cụ ghi phím gõ (Keyloggers) là một dạng công cụ giám sát bằng phần cứng hoặc phần mềm có khả năng ghi lại mọi phím người dùng gõ và lưu vào một file. File đã ghi sau đó có thể được gửi cho kẻ tấn công theo địa chỉ chỉ định trước hoặc sao chép trực tiếp. Ngoài kẻ tấn công, người quản lý cũng có thể cài đặt Keylogger vào máy tính của nhân viên để theo dõi hoạt động của các nhân viên. Việc cài đặt Keylogger có thể được thực hiện tương đối đơn giản: Hình 2.7 minh họa một Keylogger dưới dạng một khớp nối phần cứng kết nối cổng bàn phím với đầu nối bàn phím, hỗ trợ cả giao diện cổng bàn phím PS/2 và USB. Với Keylogger phần mềm, kẻ tấn công có thể tích hợp Keylogger vào một phần mềm thông thường và lừa người dùng cài đặt vào máy tính của mình.

Hình 2.7. Mô đun Keylogger phần cứng và cài đặt trên máy tính để bà