Module 16
Chống IDS, Firewall Và Honeypot

Các Chủ Đề Chính Trong Chương Này

Các Loại IDS

Giới Thiệu Về Snort IDS

Kỹ Thuật Tránh Bị IDS Dò Tìm Của Hacker

Các Mô Hình Firewall

HoneyPot – Hệ Thống Đánh Lừa Hacker

Các Kỹ Thuật Phòng Tránh Fireall Và Honeypot

IDS, Firewall và Honeypot là các thành phần bảo vệ mạng, phòng chống và dò tìm hacker hữu hiệu nhất. Cả IDS và Firewall đều là những thiết bị lọc packet thiết yếu dùng để giám sát các luồng dữ liệu vào và ra hay đang lưu chuyển trên hệ thống mạng dựa trên tập hợp những quy tắt được định nghĩa thích hợp. Trong khi đó honeypit được xây dựng với mục đích đánh lừa hacker với một số lỗ hỗng bảo mật được tạo ra có chủ đích mời gọi hacker tấn công. Điều này không những bảo vệ được hệ thống thật sự mà còn lưu giữ các chứng cứ để có thể lần ra dấu vết của hacker, phát hiện các dạng tấn công mới hay thậm chí các tổ chức bảo mật còn sử dụng honeypot để phát hiện ra các hệ thống botnet. Vì vậy, các tổ chức tội phạm mạng rất ngại những hệ thống honeypot như vậy, và nếu như bọn chúng phát hiện ra các hệ thống như trên thì sẽ tiến hành các đợt tấn công DoS/DDoS nhằm đánh sập các "bẫy bảo mật" này.

Tuy nhiên, cũng như nhiều thành phần bảo vệ mạng khác IDS, Firewall và Honeypot cần được thiết kế, sắp đặt tại những vị trí hợp lý mới đem đến hiệu quả. Trong vai trò CEH chúng ta cần hiểu rõ cơ chế vận hành của các hệ thống trên cũng như những rũi ro của chúng.

Các Loại IDS - Hệ Thống Dò Tìm Xâm Phạm Trái Phép

IDS là viết tắt của Instruction Detect System, hệ thống dò tìm hay phát hiệm các sự xâm phạm trái phép. Hệ thống này tương tự như chuông báo động trong các tòa nhà dùng để cảnh báo khi có trộm xâm nhập. IDS hoạt động dựa trên các quy tắt và những dữ liệu nhận dạng, nếu một hành động xảy ra khớp với một dữ liệu nhận dạng thi hành động tương ứng đã được định nghĩa trong quy tắt sẽ được thực thi. Nói một cách đơn giãn khi các bạn triển khai một hệ thống IDS, và có một hacer đang tiến hành scan port để dò tìm các dịch vụ đang chạy thì hành động này sẽ tương ứng với qyuy tắt về scan port attack, do đó một hành động thích hợp sẽ được gởi đến sysadmin để có hành động thích ứng, việc cảnh báo này có thể thực hiện qua email, cuộc gọi thoại hay tin nhắn.

Cao cấp hơn, các hệ thống cảnh báo có khả năng thực hiện hành động ngăn ngừa thích hợp ví dụ như sẽ cô lập địa chỉ IP đã phát động cuộc tấn công, hay tạm đóng các dịch vụ … đây chính là IPS hay Instruction prevention system – hệ thống ngăn ngừa sự xâm nhập trái phép.

Như vậy, để IDS / IPS có thể phát hiện các sự xâm nhập trái phép cần có cơ sở dữ liệu nhận dạng đúng, do đó chúng ta cần phải cập nhật đầy đủ dữ liệu này để IDS luôn nhận biết được các hành động bất thường xảy ra. Nhưng cũng như những hệ thống cảnh báo trong đời thực, việc cảnh báo sai là một trong những hạn chế của những hệ thống này.

Có hai dạng IDS :

> **Host-based IDS (HIDS)** : Là ứng dụng được cài đặt trên một hệ thống hay một máy trạm và giám sát thông tin truyền thông dựa trên các dữ liệu nhận dạng cho riêng hệ thống hay máy tính được cài đặt, và không có khả năng giám sát cho các hệ thống khác. Một số HIDS thông dụng trên thị trường như Norton Internet

Security hay Cisco Security Agent (CSA). **Lưu ý** : Một số virus có khả năng vô hiệu hóa các HIDS.

Network-based IDS (NIDS) : Có chức năng tương tự như HIDS những phạm vi hoạt động bao phủ lên toàn mạng chứ không chỉ có tác dụng trên một máy tính hay máy trạm riêng rẽ. NIDS có khả năng dò tìm và phát hiện ra ra những dạng tấn công mà firewall không nhận biết được. Bao gồm các tình huốn tấn công vào những dịch vụ bị khiếm khuyết về bảo mật, tấn công leo thang mức ưu tiên hay còn gọi là leo thang đặc quyền, đăng nhập trái phép, truy cập vào khu vực dữ liệu nhạy cảm hay phát hiện các mã độc lan truyền trên mạng. Ví dụ khi hệ thống mạng bị lây nhiễm virus *conflicker* thì hệ thống NIDS Snort có khả năng nhận biết dựa trên dữ liệu nhận dạng của vrus này và gởi báo động về cho sysadmin, cũng cần lưu ý Snort có thể hoạt động như là NIDS hay HIDS.

Trong vai trò NIDS, hệ thống hoạt động như là một passive sniffer (lắng nghe thụ động) chuyên lưu giữ và phân tích các dữ liệu truyền và so sánh với các dữ liệu nhận dạng để dò ra những hành động gây ảnh hưởng đến an toàn thông tin như khai thác, quét lỗi, dò cổng … sau đó lưu lại trong các tập tin nhật kí và gởi tín hiệu cảnh báo.

Giới Thiệu Về Snort IDS

Snort (nguồn www.snort.org) là phần mềm IDS mạnh mẽ có khả năng hoạt động ở hai chế độ HIDS hay NIDS. Do là một phần mềm nguồn mở, miễn phí nên Snort được ứng dụng nhiều trên những hệ thống và là chương trình được bình chọn bởi các hacker trng danh sách những công cụ bảo mật hàng đầu. Snort có 4 chế độ hoạt dộng khác nhau đó là:

- Sniffer mode: ở chế độcnày snort sẽ lắng nghe và đọc các gói tin trên mạng sau đó sẽ trình bày kết quả trên giao diện hiển thị.

- Packet Logger mode : lưu trữ các gói tin trong các tập tin log.

- Network instruction detect system (NIDS) : đây là chế dộ hoạt động mạnh mẽ và được áp dụng nhiều nhất, khi hoạt động ở NIDS mode Snort sẽ phân tích các gói tin luân chuyển trên mạng và so sánh với các thông tin được định nghĩa của người dùng để từ đó có những hành động tương ứng như thông báo cho quản trị mạng khi xảy ra tình huống quét lỗi do các hacker /attacker tiến hành hay cảnh báo virus..

- Inline mode: khi triển khai snort trên linux thì chúng ta có thể cấu hình snort để phân tích các gói tin từ iptables thay vì libpcap do đó iptable có thể drop hoặc pass các gói tin theo snort rule.

Cơ Chế Hoạt Động Của Snort

Snort dùng một card mạng ở chế độ promocous mode để lưu giữ các gói tin trước khi phân tích chúng cho nên tốt nhất là các máy tính chạy Snort nên đặt ở các colision domain hay trên các máy chủ tập tung các truyền thông trên mạng như router hay gateway hoặc kết nối vào các cổng SPAN của Switch , bạn có thể đặt Snort trước hoặc sau một hệ thống firewall tùy yêu cầu bảo mật của tổ chức. Và nếu hệ thống mạng có nhiều phân đoạn mạng thì mỗi subnet (lớp mạng con) phải có một máy chủ Snort được cài đặt, không như các sản phẩm thương mại khác ngòai tính năng chi phí bản quyền cao thì thường đòi hỏi cấu hình phần cứng mạn, với Snort bạn có thể, vâng có thể cài đặt và cấu hình trên x386 computer, tuy nhiên ta cần có đĩa cứng có đủ không gian trống để lưu trữ các packet được bắt giữ, và với công nghệ lưu trữ hiện nay thì điều nầy không phải là một vấn đề.

Snort hoạt động như một network sniffer lắng nghe và lưu giữ các packet trên mạng sau đó so sánh các nội dung (payload) hoặc header của chúng với một tập các qui tắc đã được định nghĩa gọi là các Snort rule và khi một sự trùng khớp giữa rule và các packet thì những hành động của rule sẽ được tiến hành tùy theo định nghĩa. Một điểm thuận lợi là các rule này luôn được cập nhật nhanh chóng bởi cộng đồng phát triển cho nên khả năng đáp ứng của Snort trước các dạng tấn công hiện đại rất cao.
Snort sử dụng ba thành phần sau để tiến hành công việc của mình:

- Packet decoder : phân tích gói tin, kể cả IP Header và Data Payload
- Detect engineer : dò tìm các dâu hiệu khả nghi theo tập hợp các quy tắc.
- Logging và alert system : lưu giữ và cảnh báo.

Ba thành phần này dùng libcap để lưu giữ gói tin khi chúng ta cài Snort trên hệ điều hành linux. Còn nếu ta cài trên hệ thống windows thì phải thay libcap bằng winpcap.
Trong bài viết này tôi trình bày phương pháp cài đặt Snort trên hệ thống Windows XP Pro. Chúng ta có thể tải winpcap từ www.iltiloi.com và Snort từ trang web www.Snort.org và chọn bản cài trên Windows. Để tham khảo thêm về triển khai Snort trên hệ thống Windows các bạn hãy tham khảo các demo tại đây …

Kỹ Thuật Tránh Bị IDS Dò Tìm Của Hacker

Bên cạnh việc nhận biết những dấu hiệu khả nghi dựa trên dữ liệu nhận dạng gọi là các signature thì IDS còn có thể phát hiện ra các mối đe dọa dựa trên những hành động bất thường gọi là anomaly detection. Những hệ thống phát hiện theo cơ chế anomaly detection căn cứ vào một mốc chuẩn mà tại đó hệ thống hoạt động ổn định hay đạt mức an toàn, và khi có những hành vi làm thay đổi tình trạng này thì IDS sẽ đưa ra những cảnh báo tương ứng. Ví dụ thông thường CPU chỉ hoạt động ở mức 30 % hiệu suất nhưng đột nhiên tăng lên hơn 90 % thì đây chính là một tình huống bất thường cần quan tâm đặc

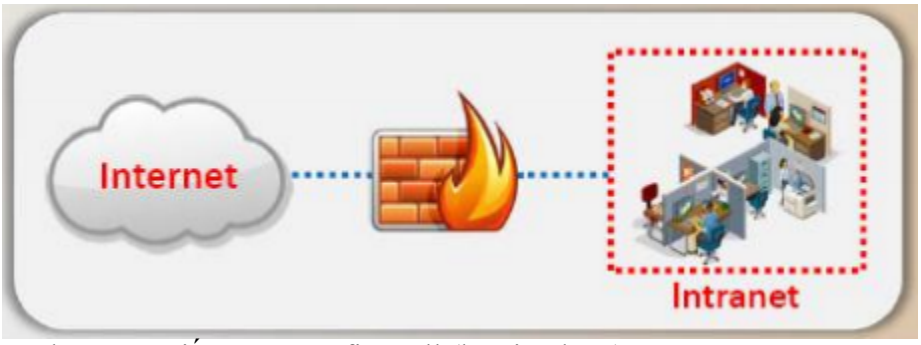
biệt, hoặc băng thông mạng đột nhiên bị tràn ngập bởi các gói tin thì có khả năng hệ thống đang bị một đợt tấn công từ chối dịch vụ.

Để tránh bị các hệ thống IDS phát hiện thì những hacker kinh nghiệm thường thay đổi dữ liệu truyền sao cho khung trùng khớp với dữ liệu nhận dạng như sử dụng một giao thức khác là UDP thay cho TCP hay HTTP thay cho ICMP để triển khai các đợt tấn công. Ngoài ra, những kẻ tấn công còn chia các gói tin thành nhiều gói tin nhỏ hơn nhằm qua mặt IDS nhưng khi tổng hợp thành dữ liệu gốc tại đích đến thì có khả năng gây nguy hiểm đến hệ thống. Cơ chế này được gọi là session splicing. Một số kỹ thuật qua mặt IDS khác có thể kể đến ví dụ như chèn thêm các dữ liệu mở rộng, obfuscating dữ liệu hay địa chỉ bằng cách mã hóa, truyền thông không đồng bộ hay chiếm quyền sở hữu session của client.

Mô Hình Firewall

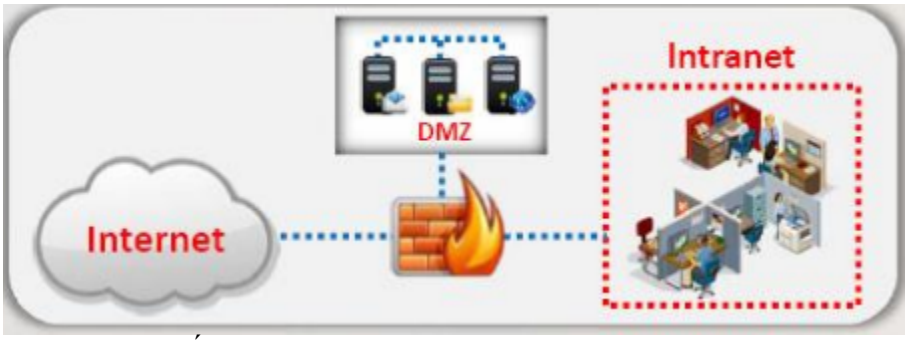
Firewall hay tường lữa là những thiết bị phần cứng hay phần mềm có tác dụng như hàng rào bảo vệ cho hệ thống mạng. Firewall kiểm soát các luồng dữ liệu vào và ra trên hệ thống mạng và đưa ra các hành động cho phép / từ chối (allow / deny) căn cứ trên tập hợp các quy tắt áp dụng cho những luồng dữ liệu này. Những thiết bị firewall phần cứng như Checkpoint Firewall, Cisco ASA, CyberRoam …, còn các firewall dạng phần mềm thì có IPCOP, ISA Server Firewall.

Khi triển khai firewall để bảo vệ hệ thống mạng chúng ta cần lưu ý đến vị trí của chúng. Thông thường thì những thành phần bảo vệ này được đặt tại các vùng biên (perimeter) để bảo vệ và ngăn cách lớp mạng bên trong với bên ngoài là internet. Vùng bên trong thường được gọi là vùng tin cậy trusted-zone, còn phía bên ngoài là untrusted-zone hay được mô tả bằng các màu tương ứng là xanh và đỏ.



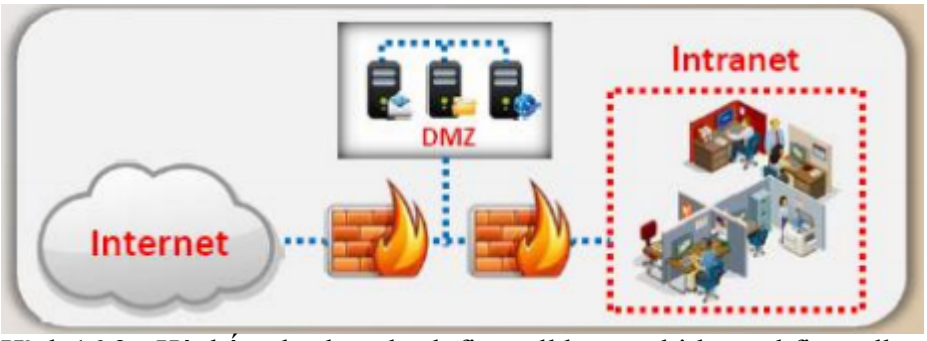
Hình 16.1 - Kiến trúc một firewall (bastion host)

Một số ứng dụng còn quy định vùng DMZ (lấy từ thuật ngữ quân sự chỉ những vùng phi quân sự) dùng để đặt các máy chủ quan trọng của tổ chức như máy chủ mail, web, cơ sở dữ liệu. Vùng này được gán mã màu cam tách biệt hoàn toàn với phí bên trong và phí bên ngoài, ngăn chặn các sự tương tác trực tiếp nhằm bảo vệ tối đa cho các máy chủ quan trọng.



Hình 16.2 - Kiến trúc một firewall (screened sunnet) với vùng DMZ

Ngoài ra, những mạng lớn hay dùng hai hệ thống firewall theo mô hình back-to-back tạo ra một hệ thống bảo vệ hai lớp đem đến sự an toàn cao hơn. Hai firewall này thường do các nhà cung cấp khác nhau hoạt động trên những nền tảng công nghệ khác với mục tiêu gia tăng sự trở ngại cho những cố gắng truy cập trái phép. Theo một số khuyến nghị thi firewall lớp trong hay dùng các hệ thống application firewall như ISA Server Firewall để dễ dàng quản trị hoặc có khả năng tích hợp với hệ thống quản trị vùng Active Directory, còn firewall lớp ngoài nên ứng dụng các thiết bị phần cứng với tính năng lọc gói tin mạnh mẽ nhằm nâng cao khả năng xử lý.

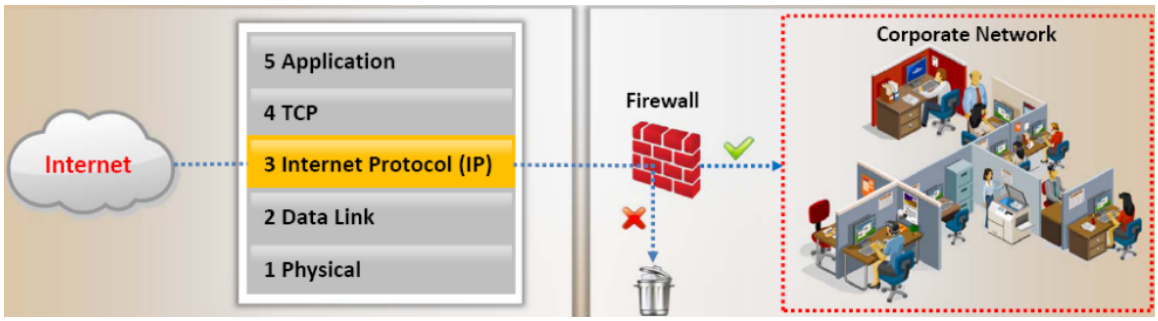


Hình 16.3 - Hệ thống back-to-back firewall hay multi-homed firewall

DMZ hay *Demilitarized Zone* là thuật ngữ chỉ những vùng phí quân sự dùng để đặt các máy chủ, ngăn chặn sự tương tác trực tiếp của các người dùng bên ngoài hệ thống và cả những người bên trong hệ thống. Tất cả những sự truy cập đến máy chủ đặt trongv ùng này đề được firewall kiểm soát chặt chẽ dựa trên các quy tắt.

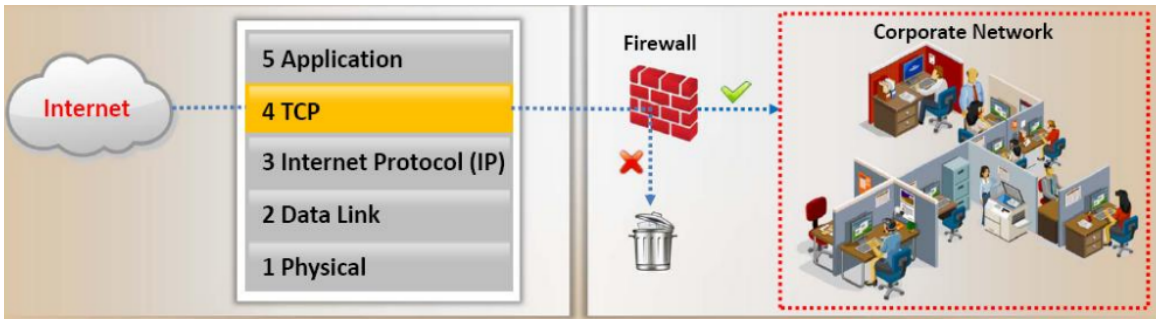
Các Loại Firewall

Packet Fitering Firewall : Hoạt động tại tầng mạng của mô hình OSI và thường là một thành phần mở rộng của các thiết bị định tuyến. Các *packet filtering firewall* có khả năng kiểm soát dựa trên địa chỉ IP nguồn và đích cũng như số hiệu cổng nguồn và đích của luồng truyền thông.



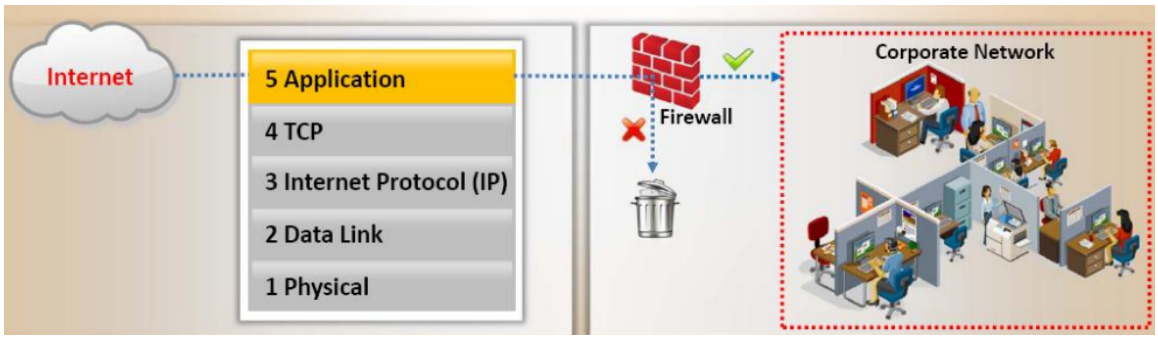
Hình 16.4 - Packet Filtering Firewall

Circuit Level Gateway Firewall : Hoạt động tại tầng Session của mô hình OSI dùng để giám sát quá trình *three-way handshake* để xác định các kết nối không hợp lệ.



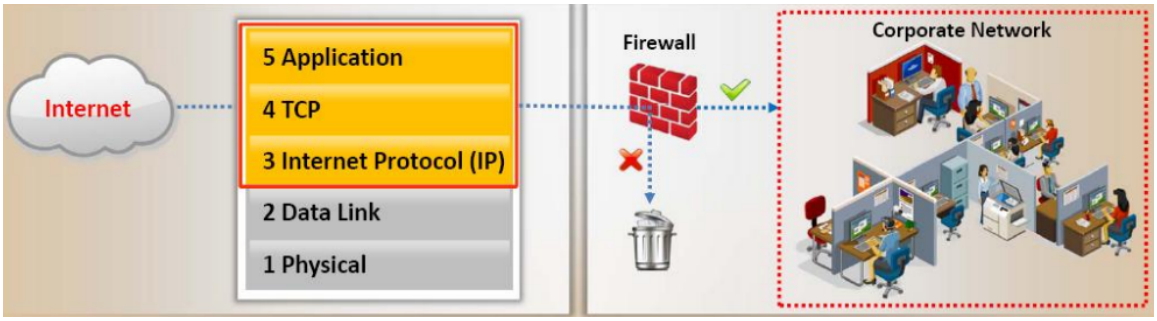
Hình 16.5 - Minh hoạt Circuit Level Gateway Firewall

Application Level Firewall : Hoạt động tại tầng ứng dụng, đây là những firewall cao cấp có khả năng kiểm soát dữ liệu truyền như data payload để phát hiện virus, trojan. Các máy khách trong vùng trusted-zone phải cấu hình sử dụng prozy để truy cập qua firewall dạng Application.



Hình 16.6 - Mô hình hoạt động của application fireall

Ngoài ra, các firewall hiện đại có thể chứa chức năng của cả ba loại firewall trên và đảm nhiệm công việc tại các tầng *network, session* và *application* trong mô hình OSI. Những hệ thống firewall kiểu này được gọi là *Stateful Multilayer Inspection Firewall* như hình minh họa dưới đây



Hình 16.7 - Mô hình Stateful Multilayer Inspection Firewall

Ngoài khả năng bảo vệ hệ thống dựa trên việc kiểm soát các dữ liệu vào và ra, kiểm tra các địa chỉ IP nguồn / đích hay các số hiệu cổng liên quan đến những dịch vụ thì các hệ thống firewall còn có khả năng phát hiện các dạng tấn công như *scan port, banner grabing* hay khả năng ẩn *port* để phòng tránh việc phát hiện. Khi có dấu hiệu khả nghi xảy ra thì firewall sẽ phát ra các tính hiệu cảnh báo hay hành động thích hợp do người quản trị thiết lập. Tuy nhiên, đa số các firewall cần phải tích hợp với các thành phần mở rộng để có thể quét virus, trojan cho dữ liệu tải về của người dùng.. Ví dụ như hệ thống mở rộng *Webmonitor GFI* dùng cho *ISA Server Firewall*.

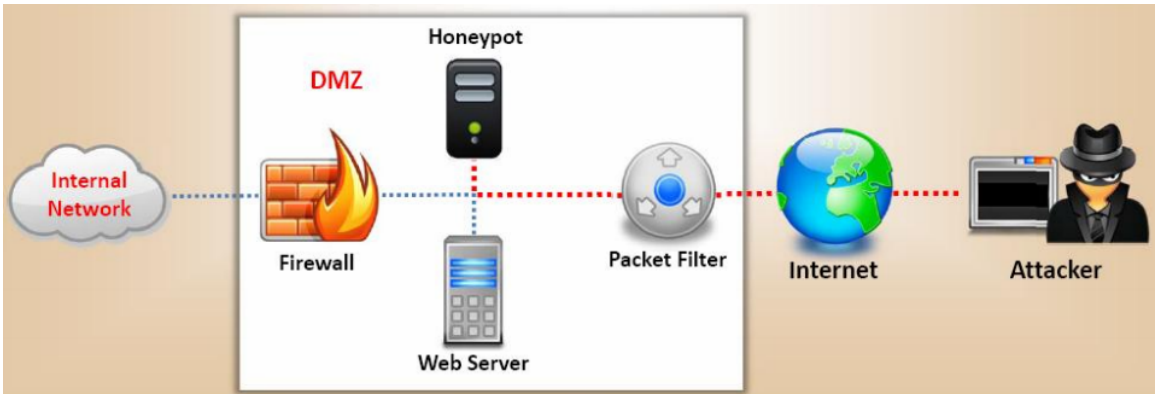
HoneyPot – Hệ Thống Đánh Lừa Hacker

Theo nghĩa đen thì honeypot là một hủ mật để bẫy côn trùng như câu thành ngữ của Việt Nam là " mật ngọt chết ruồi". trong môi trường an toàn thông tin thì honeyot còn được gọi là decoy server, một máy chủ giả mạo với những lỗ hỗng bảo mật được cố tình dựng lên nhằm đánh lừa các hacker, khi họ tấn công vào những hệ thống này sẽ bị dính bẫy và có khả năng bị truy lùng hay lưu lại các phương pháp tấn công mới dùng để dò tìm những trojan hay các mạng botnet nguy hiểm đang hoạt động. Nếu có nhiều máy tính giả được dựng lên để đánh lừa hacker thì hệ thống này được gọi là honeynet.

Có khá nhiều phần mềm được dùng để xây dựng các honeypot hay honeynet như dịch vụ honeyd, phần mềm kfsensor hoặc các bạn có thể tự mình triển khai một hệ thống hoenypot bằng cài đặt một máy chủ trên nền windows hay linux với những dịch vụ mà các hacker quan tâm như ftp, web server và bật các chế độ cảnh báo, ghi nhật kí đầy đủ nhằm lưu lại các dấu vết mà hacker để lại khi xâm nhập hệ thống. Một nguyên tắt khi triển khai các hệ thống này là hãy làm sao càng giống hệ thống thật càng tốt, vì như vậy càng dễ đánh lừa những kẻ tấn công hơn.

Trong quá trình tìm kiếm nguồn gốc tấn công của những mạng botnet thì các chuyên gia bảo mật cũng thường dùng các honeypot để tự lây nhiễm virus, torjan rồi cài đặt các chương trình giám sát nhằm theo dõi những kết nối hay hành động bất thường đến một website hay địa chỉ IP nào đó, rồi từ đó sẽ lần thoe những dấu vết khả nghi trên. Đa số cá hacker bị phát hiện theo cách này vì thiếu kinh nghiệm hay do chủ quan, họ thường sử dụng máy tính ở nhà để điều khiển hoặc các náy tính ở những nơi quen thuộc, trong quá trình tấn công thì ít khi dùng các biện pháp che dấu như ẩn danh nên việc bị lộ chân

tướng là điều không tránh khỏi. Vì vậy có một nhận xét khá thú vị về các hacker đó là "Nếu bạn là một hacker giỏi thì mọi người đều biết đến bạn. Còn nếu như bạn là một hacker xuất sắc thì sẽ không ai biết đến bạn! "



Hình 16.8 - Một honeypot đặt trong vùng DMZ

Các Kỹ Thuật Phòng Tránh Fireall Và Honeypot

"Võ quýt dày có móng tay nhọn", ý nói các hacker luôn tìm kiếm những cách thức vượt qua sự kiểm soát của những hệ thống phòng thủ và dò tìm. Một trong những cách thức vượt qua sự kiểm soát của firewall hiệu quả là đứng từ vùng tin cậy trusted-zone để tiến hành tấn công. Ví dụ như trong một mô hình lab được xây dựng bởi hacker mũ trắng Mati Aharoni (thành viên sáng lập dự án BackTrack) thì ông ta đã trình diễn cách thức vượt qua hệ thống firewall back – to – back bằng cách gởi email chứa trojan đến cho một nhận viên kinh doanh của doanh nghiệp để yêu cầu bảng báo giá dịch vụ. Khi nhân viên này mở thư sẽ bị nhiễm trojan và trojan này sẽ đứng từ bên trong mạng tải các công cụ từ một website ở bên ngoài hệ thống, do máy tính này ở trong mạng nội bộ nên firewall đã cho phép truy cập. Tiếp theo, các công cụ tải về sẽ tạo ra một kết nối được bao bọ bằng một gia thức khác để qua mặt firewall, vụ thể là hacker trên muốn kiểm sao1t màn hình máy tình của nhân viên kinh doanh này thông qua cổng 3389 của dịch vụ remote desktop, nhưng firewall không cho phép những kết nối đến các máy tính nhân viên qua cổng 3389 do đó giải pháp đưa ra là bọc giao thức sử dụng cổng 3389 bằng một giao thức được firewall cho phép thường là HTTP (80) hay SSH (22). Kỹ thuật này được gọi là tunneling, một phương pháp vượt firewall rất hiệu quả hiện nay.

SSH Tunneling

Trong vai trò quản trị hệ thống hay chuyên viên hỗ trợ kỹ thuật, đôi khi chúng ta cần kết nối từ máy tính trong văn phòng đến các máy tính ở nhà hoặc ở các chi nhánh để tiến hành các thao tác xử lý sự cố hoặc hổ trợ kỹ thuật nào đó thông qua các chương trình như VNC,Terminal Service hay RAdmin. Tuy nhiên khi công ty sử dụng Firewall như ISA, CheckPoint để bảo vệ hệ thống và kiểm sóat các luồng dữ liệu vào và ra một cách chặt chẽ thì ta sẽ gặp trở ngại lớn. Chúng ta không thể (hoặc không có quyền) mở các TCP

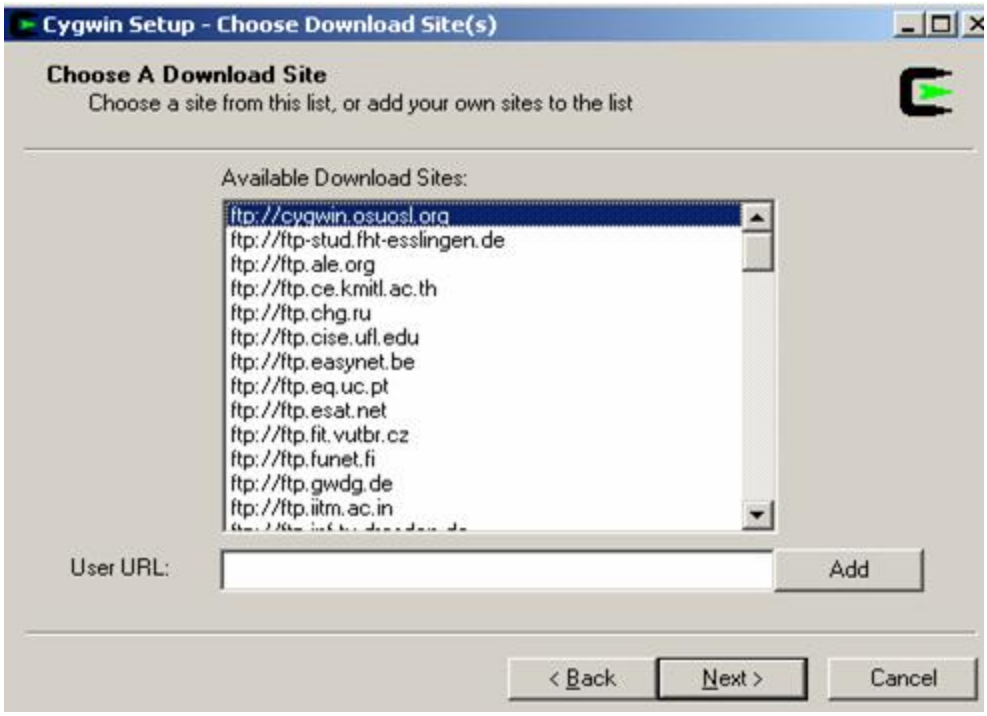
Port 4899 (Radmin), hay 5900 (VNC) để thực hiện các kết nối của mình. Vậy làm cách nào để chúng ta vẫn có thể hòan thành được công việc mà vẫn đảm bảo chính sách bảo mật của công ty không bị thay đổi?

Cho dù hệ thống của bạn có các Firewall bảo vệ thì các TCP Port quan trọng như 110 (pop3), 80 (http), 21 (ftp), 22 (ssh) vẫn thường mở để tiến hành các công việc cần thiết như duyệt web, e-mail.. đặc biệt TCP Port 22 của dịch vụ SSH có chức năng mã hóa phiên truyền thường được các firewall ưu ái cho qua, và chúng ta sẽ dựa vào dịch vụ này để tạo ra một SSH Tuneling đáp ứng cho công việc của mình.

Ta cần có ssh server cài trên các máy ở xa (remote computer), ssh client trên máy điều khiển (local computer) và những chương trình remote control như VNC, Terminal Services hay RAdmin. Trong phần này tôi sẽ dùng một chường trình rất thông dụng là RAdmin (ngòai ra VNC cũng là một phần mềm remote control 5 sao miễn phí rất được ưa thích, cách thực hiện tương tự chỉ khác là ta phải dùng TCP Port 5900 thay cho 4899).
Cài SSH Server trên remote computer thông qua Cygwin

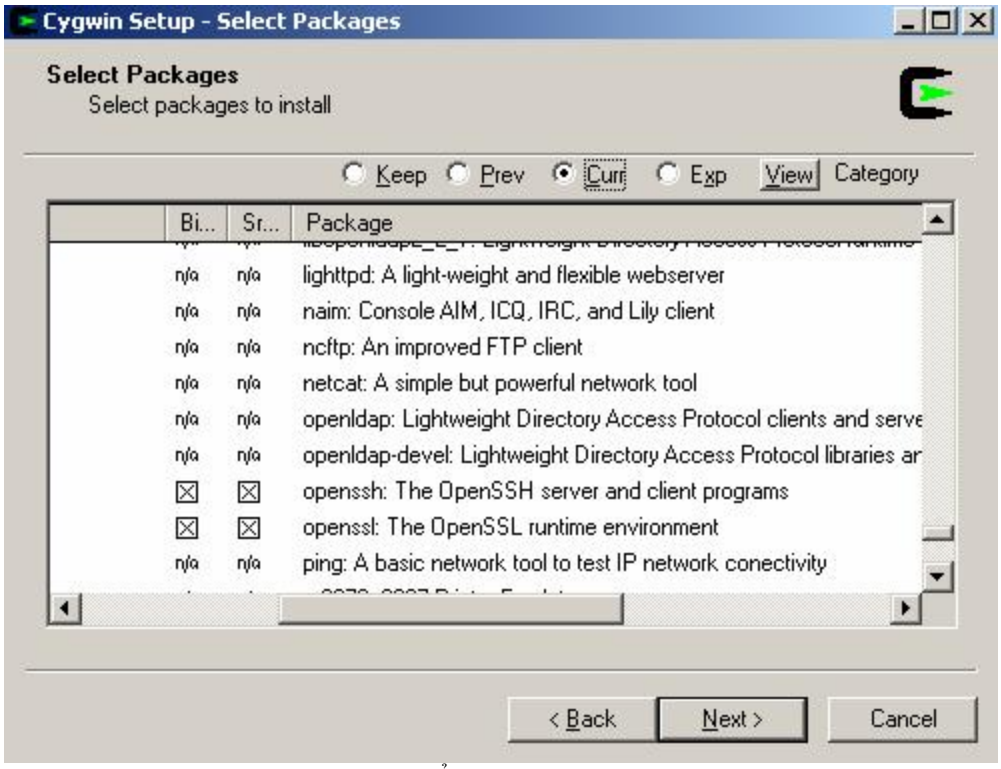
Nếu máy tính cần điều khiển chạy các hệ thống như Linux thì bạn có thể tải về các gói openSSH từ http://sourceforge.net (thông thường trên các bản Redhat, FC hay Mandrake đã có sẵn openSSH trên bộ đĩa source (ta chỉ cần vào Add/Remote Application và chọn gói openSSH để cài đặt SSH Server. Còn nếu như các máy xa dùng hệ điều hành Windows thì các bạn có thể cài Tectia SSH Server hay phần mềm Freeware Win_Open-SSH (tải về từ http://are-peace.com/v2/download.php). Trong phần này tôi trình bày giải pháp cấu hình SSH Server dựa trên phần mềm tạo môi trường Linux trên Windows là CYGWIN.

Cygwin là một phần mềm tuyệt vời có thể tạo một môi trường linux-like giúp các bạn muốn nghiên cứu Linux nhưng ngại cài đặt và vẫn dùng hệ thống Windows hiện có của mình. Cygwin có thể được cài trực tiếp từ Internet rất dễ dàng, mặc dù không phải là một môi trường Linux thuần túy nhưng cũng giúp các bạn nắm được các cấu trúc và dòng lệnh của Linux nhanh chóng. Các thông tin tham khảo và cài đặt cygwin có thể xem ở http://cygwin.com.



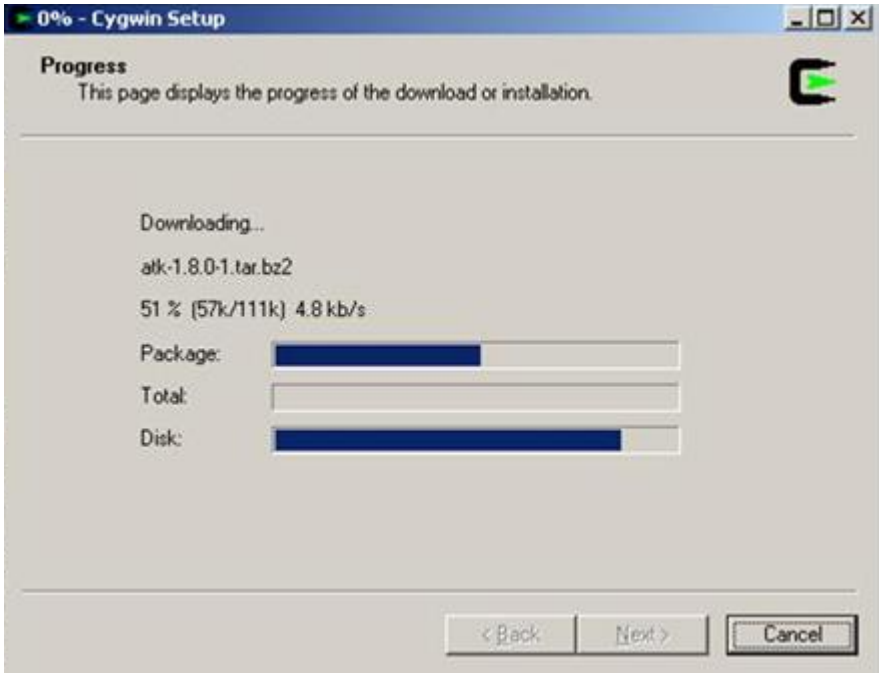
Hình 16.9 - Quá trình cài đặt từ http://cygwin.com

Chọn Ftp site và nhấn Next sau đó lựa các gói openssh và openssl trong khung Select Packages của chương trình cài đặt, tuy nhiên ta có thể cài thêm các gói khác nếu muốn:



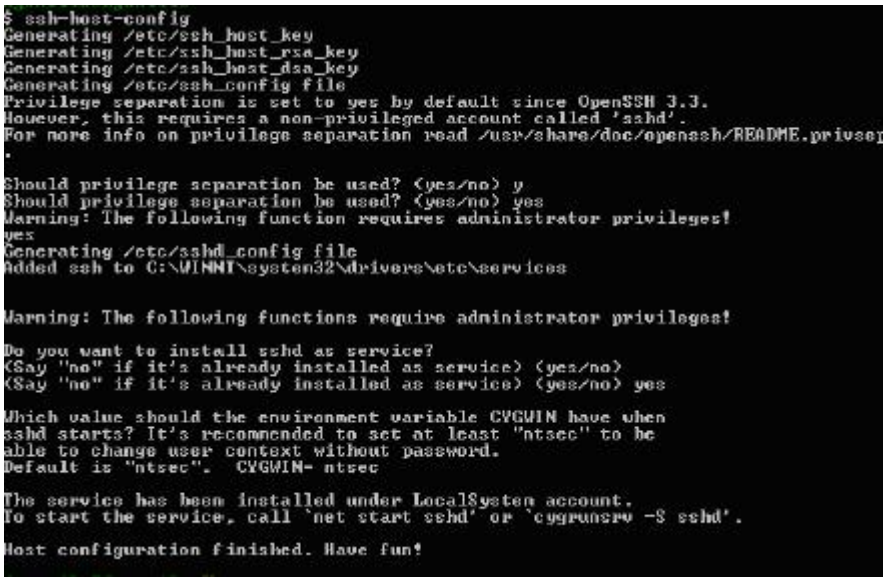
Hình 16.10 – Chọn các package để cài đặt

Hình vẽ các gói **openssh** và **openssl** trong *Seclect Packages*



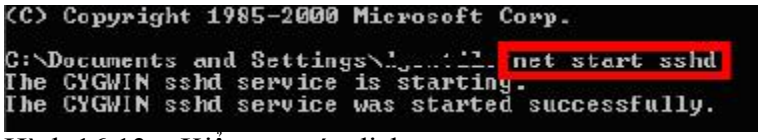
Hình 16.11 - Cài đặt cygwin với các package được chọn

Khi quá trình cài đặt hòan tất ta hãy nhấp vào biểu tượng cygwin trên Desktop để load shell của cygwin, và thực thi dòng lệnh ssh-host-config để cấu hình SSH Server như hình dưới đây:



Hình 16.12 – Khởi tạo SSH

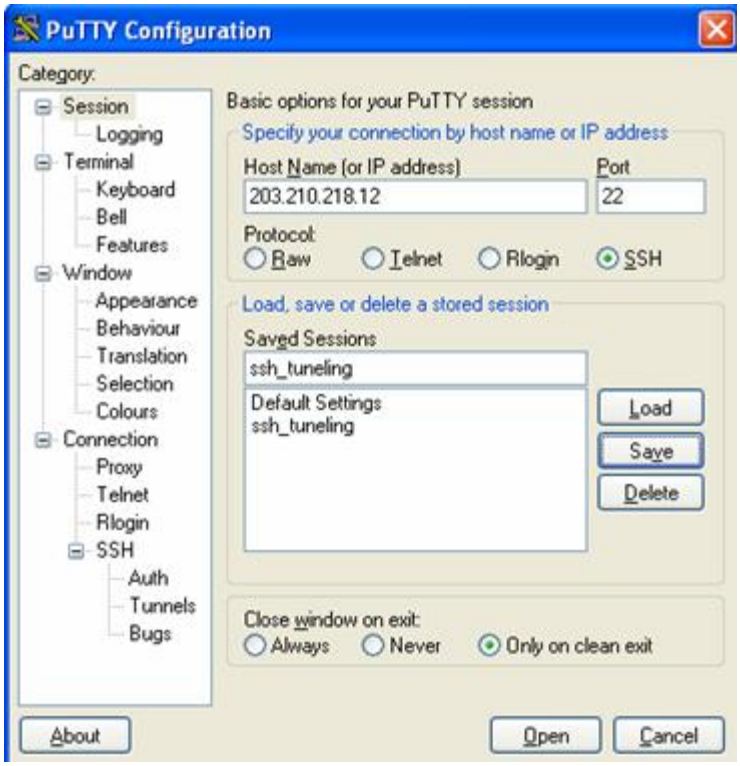
Sau đó khởi động SSHD bằng lệnh net start sshd thông qua giao diện dòng lệnh của Windows (nhấn Start->Run->CMD).



Hình 16.13 – Kiểm tra các dịch vụ

Vậy là chúng ta đã hòan tất quá trình cấu hình remote server phục vụ cho công việc của mình (ở đây tôi không trình bày phương pháp cài đặt VNC hay RAdmin).
Cài Đặt Và Cấu Hình SSH Client Trên Local Computer Bằng Putty

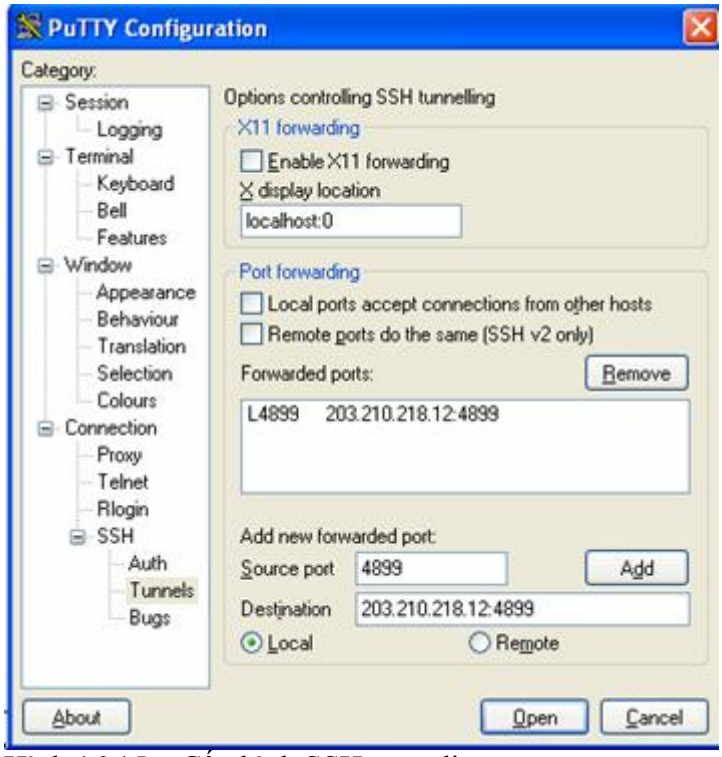
Một trong các chương trình *ssh client* miễn phí xuất sắc là Putty có thể tải về từ www.sectools.org. Sau khi tải về ta chỉ cần nhấn kép vào biểu tượng Putty để khởi động và nhập vào các tham số như dưới đây:



Hình 16.14 – Giao diện Putty

- Host Name (or IP address) 203.210.218.12 là địa chỉ *public* của *remote server* .
- Port 22 là TCP Port của SSH tại tầng vận chuyển

Tiếp theo hãy chọn mục *Tunnels* từ giao diện Putty để thiết lập *SSH tunnel* theo các thông số như hình bên (nhớ chọn nút Add để ghi các tham số này vào khung *Forwarded ports*)



Hình 16.15 – Cấu hình SSH tunneling

- Source port là port của chương trình remote control đang lắng nghe trên máy được điều khiển (VNC dung port 5900, RAdmin: 4899).

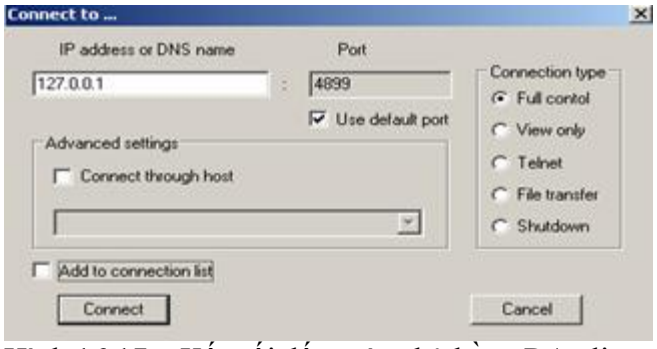
- Destination là địa chỉ remote server và port đang lắng nghe.

Bây giờ ta đã có thể tiến hành công việc remote control vượt qua firewall dựa trên ssh tunneling , hãy nhấn Open để tạo kết nối ssh đến remote server và đăng nhập với tài khỏan hợp lệ. Sau khi quá trình đăng nhập hòan tất kiểm tra lại bằng lệnh netstat –na sẽ thấy TCP Port 4899 trên máy ở xa đã được map đến máy nội bộ:

```
  TCP    longhorn:40019         longhorn.gateway.com:0  LISTENING
  TCP    longhorn:1055          longhorn.gateway.com:0  LISTENING
  TCP    longhorn:4899          longhorn.gateway.com:0  LISTENING
  TCP    longhorn:netbios-ssn   longhorn.gateway.com:0  LISTENING
  TCP    longhorn:1568          DELL:microsoft-ds       TIME_WAIT
```

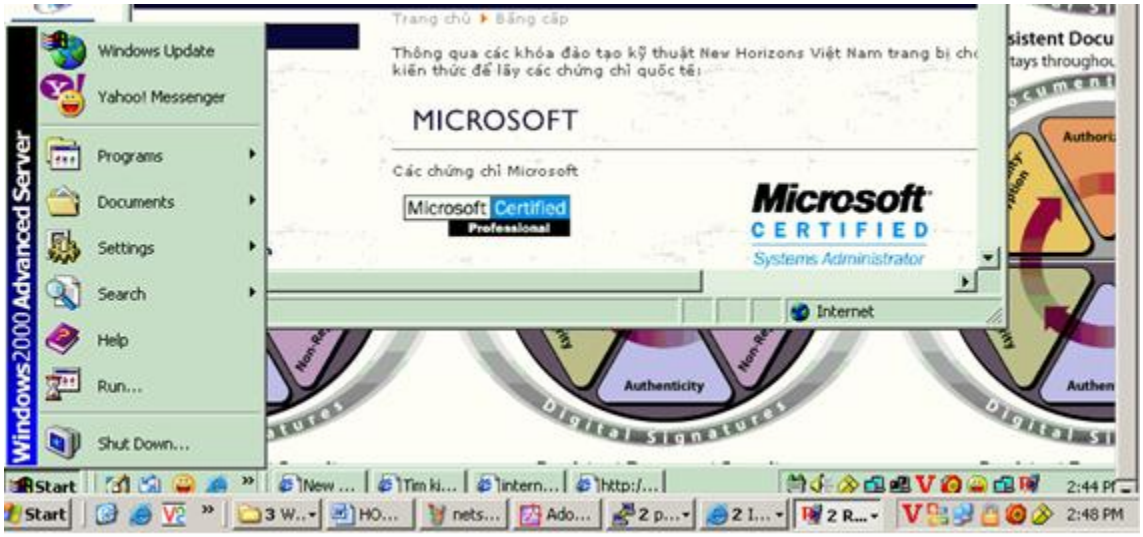
Hình 16.16 – Kết quả thực thi lệnh netstat

Tạo kết nối Remote Control bằng RA client :



Hình 16.17 – Kết nối đến máy chủ bằng RA client

Cuối cùng, hãy mở RAdmin client kết nối đến TCP Port 4899 của máy nội bộ (IP 127.0.0.1), với tài khoản hợp lệ là chúng ta đã có thể tương tác được với màn hình trên máy tính ở xa để tiến hành thao tác sửa chữa hay cài đặt thêm phần mềm mà không cần thay đổi policy của firewall như Hình 16.18



Hình 16.18 - Màn hình của remote computer với public IP 203.210.218.12

Video minh họa : http://youtu.be/tEDlUCEP3-s

> **Lưu ý** : Giải pháp này cũng được hacker sử dụng để tạo kết nối ngược ra ngoài internet, công cụ putty lúc này sẽ là ứng dụng dòng lệnh để hạn chế về mặt dung lượng.

Tổng Kết

Qua chương này chúng ta đã nắm về các hệ thống phòng thủ quan trọng như firewall, honetpot hay IDS cùng với những chức năng của chúng. Mỗi hệ thống có những đặc trưng riêng vì vậy khi ứng dụng vào hệ thống chúng ta cần có sự thiết kế hợp lý để việc triển khai mang lại hiệu quả cao. Bên cạnh đó là những kỹ thuật mà hacker dùng để vượt

qua các sự kiểm soát này mà các bài thi của CEH thường đề cập như tunnling, session splicing …