KẾT QUẢ THỬ NGHIỆM BỘ GIẢI PHÁP BẢO MẬT CỦA McAfee & Intel

TS.Phạm Việt Trung - NLSI

NLSI
Đối tác:
Mi2
PARTNERING SUCCESS
FASTEST
SERVER WORKSTATION
McAfee
An Intel Company
intel

Nội dung

- Giới thiệu chung về Dự án
- Giới thiệu công cụ thực hiện
- Kết quả thử nghiệm đánh giá
- Kết luận.

Nội dung

- **Giới thiệu chung về Dự án**
- Giới thiệu công cụ thực hiện
- Kết quả thử nghiệm đánh giá
- Kết luận.

Giới thiệu chung về Dự án

Tên dự án: "*Thử nghiệm công nghệ của Intel và McAfee*".

Thành phần tham gia:

- Phòng thí nghiệm trọng điểm an toàn thông tin (NLSI)
- Intel
- McAfee
- Công ty Cổ phần tin học Mi Mi – nhà phân phối McAfee tại Việt Nam
- Fastest - Công ty Cổ phần Anh Đức, đối tác cao cấp về máy chủ, thương hiệu Fastest của Intel tại Việt nam

Thời gian thực hiện: tháng 7- tháng 11 năm 2013

Địa điểm triển khai: Phòng Thí nghiệm trọng điểm an toàn thông tin

NLSI

Đối tác: Mi2 PARTNERING SUCCESS FASTEST SERVER WORKSTATION McAfee An Intel Company intel

Lĩnh vực hợp tác & Hoạt động

	Loại	Công nghệ	Mô tả
1	Thử nghiệm	Intel	Ổ cứng Intel SSD Công nghệ vPro tích hợp với McAfee ePO Deep Command
		McAfee	Bảo mật Kết nối
2	Đào tạo	Công nghệ Intel & McAfee	Bảo mật Công nghệ Intel với máy chủ thương hiệu Việt

	Hoạt động	Thời gian	Đơn vị thực hiện
1	Chuẩn bị	Tháng 7 & 8	Mi2
2	Bàn giao thiết bị	Tháng 8	Intel/ McAfee/Fastest/Mi2 -> MOD
3	Triển khai thử nghiệm	Tháng 8 & 9	Intel/Mi2/Fastest/ MOD
4	Tài liệu	Tháng 10/2013	Intel/Mi2/Fastest/ MOD
5	Training	Mỗi tháng	Mi2/Intel (Fastest)

Nội dung

- Giới thiệu chung về Dự án
- **Giới thiệu công cụ thực hiện**
- Kết quả thử nghiệm đánh giá
- Kết luận.

Thiết bị Công nghệ thông tin – Phần cứng

	Type	Type	Unit Configuration
1	Server	2 Fastest servers	Xeon E5-2620 (15M Cache, 2.00 GHz, 7.20 GT/s Intel QPI) HDD 1TB SAS; 240GB SSD; 8GB RAM
2	PC	2 PC with vPro	Core i5-2500/4G/160GB/DVDRW

Phần mềm

	Type	Name
1	Software for client	McAfee Complete Endpoint Protection - Enterprise
2	Software for server	McAfee Total Protection for Server

	Type	Product
1	Server	McAfee Virus Scan Enterprise McAfee Policy Auditor McAfee Desktop Firewall McAfee Application Control McAfee Change Control McAfee ePO
2	PC	McAfee Virus Scan Enterprise McAfee Desktop Firewall McAfee Device Control McAfee Site Advisor

Nhóm dự án

ID	Role	Contact
1	Project Manager – Technical Solution	Mi2: Luan
2	Project Manager – Overall	Intel: Tam
3	Project Coordinator – Deployment	MOD: Trung Intel: Hung Anh Duc: Linh
4	Other members - Intel Solution Architecture - McAfee BDM	 Intel APAC: Cheah Bernard McAfee: Vu Nguyen

Nội dung

- Giới thiệu chung về Dự án
- Giới thiệu công cụ thực hiện
- **Kết quả thử nghiệm đánh giá**
- Kết luận.

Kết quả đánh giá thử nghiệm - McAfee

Bộ giải pháp bảo mật áp dụng cho máy chủ		
VirusScan Enterprise (VSE)	Bảo vệ máy chủ theo thời gian thực	- McAfee VSE ngăn chặn các mã độc thực thi và thông báo cho người dùng
	Quét Virus theo lịch và kiểm soát CPU khi tiến hành quét	- Trong quá trình quét Virus, tài nguyên CPU của tiến trình McAfee VSE trong quá trình quét không vượt quá 30%
	Tùy chỉnh update signature cho máy chủ từ những nguồn khác nhau	- Máy chủ 01 update từ ePO server - Máy chủ 02 update từ Distribute Repository
	Khả năng tự bảo vệ của VSE	- Không thể stop được dịch vụ McAfee McShield

Kết quả đánh giá thử nghiệm - McAfee

Bộ giải pháp bảo mật áp dụng cho máy chủ		
Host Firewall	Thiết lập mở port HTTP, FTP tới Server	Máy trạm truy cập được vào HTTP, FTP trên Server
	Thiết lập chế độ Adaptive mode, kết nối tới Server thông qua port 3389	Máy trạm có thể remote vào Server Trong rule của Server có thêm 1 rule Allow port 3389
Application Control	Tính năng ngăn chặn thực thi chương trình/cài đặt phần mềm vào máy chủ	Có thông báo lỗi không thể thực thi được chương trình/phần mềm từ thư mục Software
	Người dùng đặc quyền có thể thực thi chương trình/cài đặt phần mềm trên máy chủ	Với tài khoản Mi2.lab\Administrator có thể thực thi được chương trình/phần mềm từ thư mục Software
	Người dùng bất kỳ thực thi chương trình/cài đặt phần mềm trong 1 thư mục nhất định	Với tài khoản Mi2.lab\User01 có thể thực thi được chương trình/phần mềm từ thư mục Setup
	So sánh chương trình trên máy chủ với máy mẫu	Đưa ra danh sách các chương trình/phần mềm của máy chủ 02 không giống với máy chủ 01

Kết quả đánh giá thử nghiệm - McAfee

Bộ giải pháp bảo mật áp dụng cho máy chủ		
Change Control	Tính năng cấm đọc nội dung file	-Không mở được file hosts
	Cấm thay đổi nội dung file	Có thông báo cấm không cho thay đổi nội dung file boot.ini
Policy Auditor	Kiểm tra tính tuân thủ của các máy chủ theo chuẩn PCI-DSS	- Đưa ra kết quả kiểm toán những chính sách pass/fail theo chuẩn PCI-DSS
	Kiểm tra tính tuân thủ của các máy chủ theo theo chuẩn ISO	- Đưa ra kết quả kiểm toán những chính sách của máy trạm theo chuẩn ISO 27002
Deep Defender	Khả năng ngăn chặn rootkit (Tích hợp với công nghệ bảo mật tại mức chip của Intel)	- McAfee ngăn chặn các mã độc rootkit xâm nhập vào máy trạm.

Kết quả đánh giá thử nghiệm - McAfee

Bộ giải pháp bảo mật áp dụng cho máy trạm		
VirusScan Enterprise	Bảo vệ máy trạm theo thời gian thực	- McAfee VSE ngăn chặn tiến trình và thông báo cho người dùng
	Quét Virus theo lịch và kiểm soát CPU khi tiến hành quét	- Trong quá trình quét Virus, tài nguyên CPU của tiến trình McAfee VSE trong quá trình quét không vượt quá 30%
	Update signature cho máy trạm theo lịch từ những nguồn khác nhau	- Client01 update signature từ ePO Server - Client01 update signature từ Distributed Repository
	Khả năng tự bảo vệ của VSE	- Không thể stop được dịch vụ McAfee McShield
Host Firewall	Thiết lập mở port HTTP, FTP tới Server	- Máy trạm truy cập được vào HTTP, FTP trên Server
	Thiết lập chế độ Adaptive mode, kết nối tới Server thông qua port 3389	- 2 Máy trạm có thể remote vào Server - Trong rule của Server có thêm 1 rule Allow port 3389

Kết quả đánh giá thử nghiệm - McAfee

Bộ giải pháp bảo mật áp dụng cho máy trạm		
Device Control	Kiểm soát thiết bị ngoại vi	- Tất cả hành vi kết nối USB đều được ngăn chặn
	Kiểm soát người dùng truy cập internet thông qua USB 3G	- Ngăn hặn người dùng truy cập internet thông qua USB 3G
	Kiểm soát chạy file thực thi từ thiết bị ngoại vi	- Ngăn chặn hành file .exe được thực thi
	Kiểm soát thiết bị ngoại vi tại chế độ read-only	- Lần 1: Copy thành công - Lần 2: Ngăn chặn hành vi copy
	Khả năng định nghĩa thiết bị mềm dẻo, xây dựng chính sách linh hoạt.	- Lần 1: Ngăn chặn người dùng sử dụng USB 1 - Lần 2: Cho phép người dùng sử dụng USB 2
Site Advisor	Cảnh báo cho người dùng về mức độ an toàn của các trang web	- McAfee đưa ra đánh giá về mức độ an toàn của các trang web theo các mức độ sau: Red, Yellow, Green.
	Chế độ bảo vệ người dùng duyệt web 1 cách toàn diện	- McAfee ngăn chặn người dùng truy cập các trang web không an toàn
Deep Defender	Khả năng ngăn chặn rootkit (Tích hợp với công nghệ bảo mật tại mức chip của Intel)	- McAfee ngăn chặn các mã độc rootkit xâm nhập vào máy trạm

Kết quả đánh giá thử nghiệm - McAfee

Khả năng báo cáo tổng hợp của máy chủ quản trị ePO		
VSE	Computers with Threats Detected per Week	- Có được báo cáo danh sách các máy trạm phát hiện threat hàng tuần
	Spyware Detected in the Last 7 Days	- Có được báo cáo danh sách spyware phát hiện trên máy trạm trong 7 ngày
		- Có được báo cáo danh sách 10 máy trạm xảy ra nhiều threat nhất trong 3 tháng.
Host Firewall	Desktop High Triggered Signatures	- Có báo cáo danh sách 10 hành vi vi phạm nhiều nhất ở mức High
	Desktop Medium Triggered Signatures	- Có báo cáo danh sách 10 hành vi vi phạm nhiều nhất ở mức Medium
	Top 10 IPS Events by Target	- Có báo cáo 10 máy trạm thực hiện nhiều hành vi vi phạm nhất
Application Control – Change Control	Top 10 Systems with Most Violations Detected in the Last 7 Days	- Có báo cáo 10 máy trạm có nhiều hành vi vi phạm nhất trong vòng 7 ngày
	Top 10 Users with Most Violations Detected in the Last 7 Days	- Có báo cáo 10 người dùng có nhiều hành vi vi phạm nhất trong vòng 7 ngày
	Attempted Violations Detected in the last 7 Days	- Có báo cáo tất cả các hành vi vi phạm trong vòng 7 ngày

Kết quả đánh giá thử nghiệm - Intel

McAfee ePO Deep command sử dụng công nghệ Intel vPro		
Quản trị khi máy trạm ở trạng thái Power Off/Sleep	Kết nối giao diện ePO Tiến hành Wakeup Agent từ xa	- Client cập nhật chính sách
		- Triển khai các gói dịch vụ
		- Quét virus
Truy cập từ xa vào máy trạm ở trạng thái Power Off/Sleep	Dùng KVM để kết nối từ xa	- Remote tới được tới máy trạm và thao tác bình thường.
So sánh Intel SSD với HDD thường và SSD khác		
Kiểm thứ tốc độ	Test hiệu năng ổ cứng intel SSD	Các thông số đọc, ghi dữ liệu, tốc độ truy xuất của ổ cứng
	Kiểm tra tốc độ HDD	Các thông số đọc, ghi dữ liệu, tốc độ truy xuất của ổ cứng

Nội dung

- Giới thiệu chung về Dự án
- Giới thiệu công cụ thực hiện
- Kết quả thử nghiệm đánh giá
- **Kết luận**

Kết luận

Giải pháp bảo mật McAfee CEE và TSR:

- Nâng cao tính bảo mật hệ thống trước các nguy cơ từ Virus/Malware và các tấn công.
- Bảo vệ an toàn cho người dùng truy cập Web
- Nâng cao bảo mật cho hệ thống Mail
- Ngăn chặn thất thoát dữ liệu nhạy cảm
- Đảm bảo tính tuân thủ trong tổ chức
- Giảm thiểu tối đa chi phí vận hành, quản trị hệ thống bảo mật cho máy chủ/máy trạm
- Nhận được hỗ trợ tốt từ dịch vụ hỗ trợ Gold Support.

Kết luận

Công nghệ Intel

- Intel® vPro™ Active Management Technology (AMT) tích hợp từ phần cứng cho phép cấu hình, quản lý và xử lý lỗi cho máy trạm bằng cách truy cập vào hệ thống mà không phụ thuộc vào hệ điều hành, cũng như trạng thái của máy (kể cả khi máy đang đang bị tắt). Phần mềm McAfee ePO Deep Command sẽ cho phép Quản trị mạng sử dụng công nghệ Intel AMT một cách đơn giản & hiệu quả.
- Ổ cứng Intel SSD có tốc độ IOPS cao cho phép tăng khả năng bảo mật của thiết bị cũng như cả hệ thống, và Intel SSD dùng cho doanh nghiệp có chế độ bảo hành rất đặc biệt lên đến 5 năm (so với chế độ bảo hành từ 1-3 năm thông thường trên thị trường)

CHÂN THÀNH CẢM ƠN QUÍ VỊ ĐÃ CHÚ Ý LẮNG NGHE!