Số 52
12/2016

BẢN TIN dancisco

Được phát hành bởi Công Ty TNHH Tư Vấn và Dịch Vụ Chuyên Việt

Giải pháp bảo vệ trước cuộc tấn công mạng

Ngăn chặn mã độc xâm nhập hệ thống là vấn đề không thể giải quyết trọn vẹn. Do vậy, cần phải có cách tiếp cận nhằm phát hiện được các mối đe dọa tiềm tàng và ngăn chặn chúng.

Mã độc (malware) hiện nay có khả năng che dấu, ẩn mình và vượt qua các biện pháp phòng thủ truyền thống. Đội an ninh thông tin luôn phải đối mặt với nhiều thách thức vì những công cụ bảo mật mà họ được trang bị không đủ khả năng kiểm soát cũng như phát hiện và loại bỏ các mối đe dọa trước khi mã độc gây ra thiệt hại cho hệ thống.

[Trang 11]

VNPRO HÂN HOAN CHÀO MỪNG THÀNH VIÊN MỚI CỦA TỦ SÁCH CCLABPRO: "CCNP LABPRO SWITCH"

Tháng 11/2016 VnPro chính thức đón chào thành viên mới của tủ sách CCLabPro: "CCNP LabPro Switch". Quyển sách như lời khẳng định sứ mệnh của VnPro đối với cộng đồng "Mang đến cho xã hội những công dân có nghề nghiệp và trình độ đẳng cấp quốc tế".

[Trang 07]

Sáng kiến thiết bị viễn thông nguồn mở
Facebook sẽ khiến Cisco, Huawei, Alcatel lo lắng

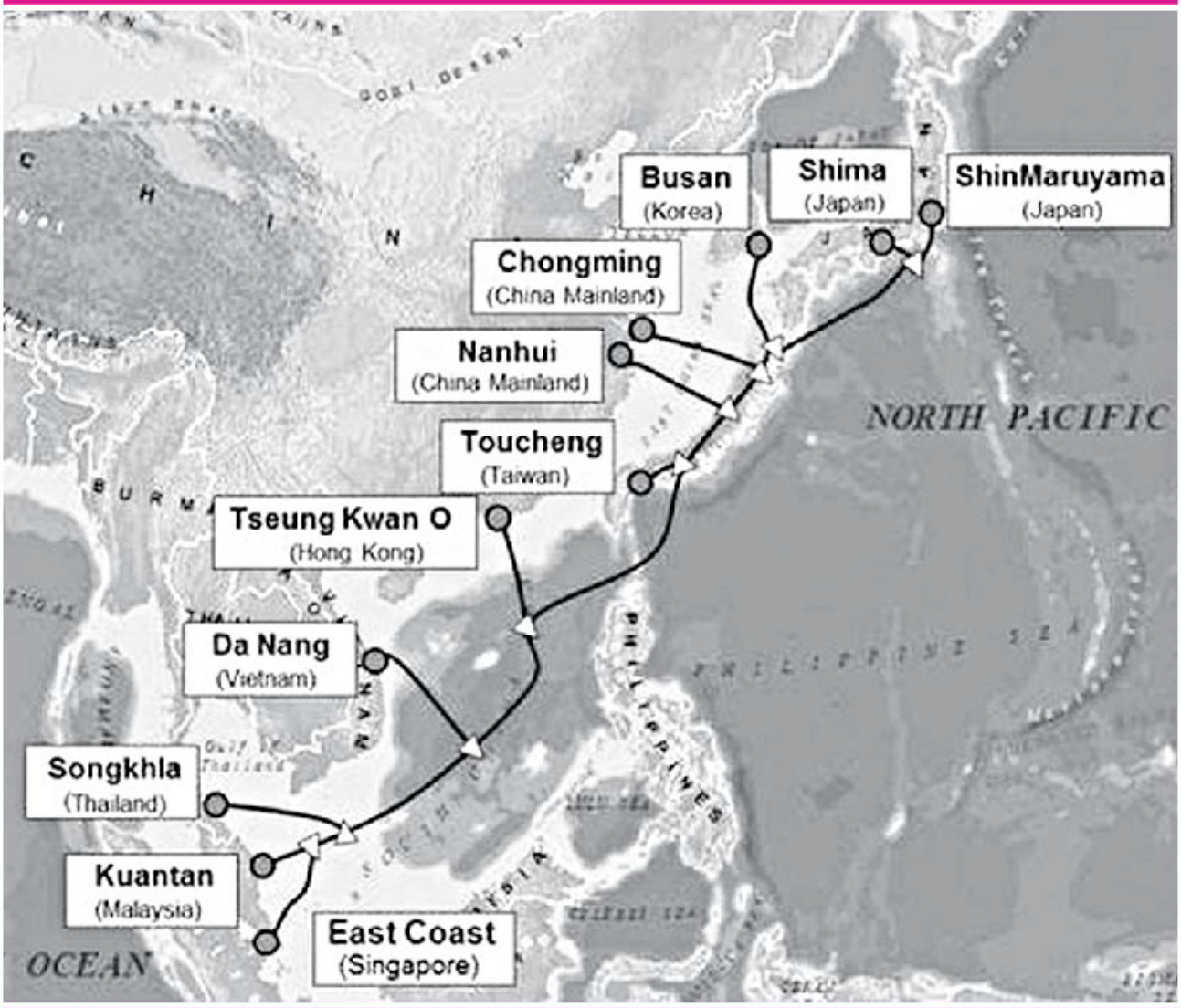
Vừa qua Facebook cho ra mắt một bộ switch quang học mang tên Voyager chuyên dùng trong các hạ tầng mạng, data center cùng như nhà mạng. Thiết bị này làm nhiệm vụ giải mã và truyền tín hiệu quang học với tốc độ cao trong khi giá thành rẻ vì được Facebook mở thiết kế nên bất kì ai cũng có thể tham gia sản xuất. Nhưng đây chỉ là một phần nhỏ trong kế hoạch OpenCellular của Facebook nhằm tạo ra một hệ sinh thái không dây mã nguồn mở, và khi dự án này phát triển đủ lớn thì nó sẽ làm mất nguồn thu của các công ty đang kiếm rất nhiều tiền từ mảng kinh doanh trị giá 500 tỉ USD này, ví dụ như Cisco, Huawei, Alcatel-Lucent...

[Trang 03]

TIN TỨC SỰ KIỆN KHÁC

Hoàn tất tuyến cáp quang APG băng thông 54 Tb/s chạy qua Việt Nam

Nhà thầu NEC (Nhật Bản) vừa tuyên bố đã hoàn tất việc xây dựng tuyến cáp quang ngầm dưới biển APG (Asia-Pacific Gateway) chạy qua các nước Nhật Bản, Trung Quốc, Hàn Quốc, Singapore, Malaysia, Thái Lan và Việt Nam. Đây cũng chính là tuyến cáp quang được kì vọng giúp mạng Internet Việt Nam giảm bớt sự phụ thuộc vào tuyến cáp AAG hiện nay.



Theo ZDNet, tuyến cáp quang APG vừa hoàn thành sẽ có khả năng cung cấp băng thông tới 54 Tb/s. Nếu so sánh với cáp quang AAG vốn chỉ có băng thông 2,88 Tb/s, cáp quang APG sẽ giúp người dùng có tốc độ Internet nhanh hơn khoảng gần 20 lần.

"NEC rất vinh dự khi được chọn là nhà thầu thi công tuyến cáp quang APG", Shunichiro Tejima, Phó Chủ tịch của NEC cho biết. APG là tuyến cáp quang dài 10.900 km và được kì vọng sẽ mở ra cuộc đua mới trong lĩnh vực kết nối Internet tại Châu Á-Thái Bình Dương. VNPT và Viettel là hai nhà mạng Việt Nam tham gia đầu tư và được quyền sử dụng cáp quang APG.

Trước đó, vào năm 2012, tuyến cáp quang APG đã được thúc đẩy nhờ vào một khoản tiền đầu tư của Facebook. Đại diện của hãng cho biết: "Tuyến cáp quang mới sẽ giúp cho sự phát triển của chúng tôi ở khu vực Nam Á và giúp cung cấp trải nghiệm tốt hơn cho người dùng ở nhiều nước như Ấn Độ, Indonesia, Malaysia, Philippines, Hong Kong và Singapore". Dự án APG sau đó đã nhận được sự quan tâm của nhiều doanh nghiệp viễn thông lớn của châu Á như NTT Docomo (Nhật Bản), China Telecom (Trung Quốc) hay KT (Hàn Quốc).

Sau khi được đi vào hoạt động, cáp quang APG sẽ giúp Việt Nam kết nối Internet cực nhanh với các trung tâm kinh tế hàng đầu trong khu vực như Trung Quốc, Nhật Bản và Hàn Quốc. Ngoài ra, APG còn giúp tăng đáng kể khả năng dự phòng cho các kênh kết nối Internet quốc tế hiện tại của Việt Nam.

Theo thông tin trong nước, cả VNPT và Viettel đều có kế hoạch triển khai việc kết nối Internet với tuyến cáp quang APG ngay sau khi được xây dựng xong trong năm 2016. Hi vọng, với tuyến cáp quang APG mới, tốc độ kết nối Internet của người dùng tại Việt Nam sẽ được tăng lên đáng kể và giảm bớt sự phụ thuộc vào tuyến cáp quang AAG thường xuyên gặp lỗi.

Theo VNReview.vn

Sáng kiến thiết bị viễn thông nguồn mở Facebook sẽ khiến Cisco, Huawei, Alcatel lo lắng

Vừa qua Facebook cho ra mắt một bộ switch quang học mang tên Voyager chuyên dùng trong các hạ tầng mạng, data center cũng như nhà mạng. Thiết bị này làm nhiệm vụ giải mã và truyền tín hiệu quang học với tốc độ cao trong khi giá thành rẻ vì được Facebook mở thiết kế nên bất kì ai cũng có thể tham gia sản xuất. Nhưng đây chỉ là một phần nhỏ trong kế hoạch OpenCellular của Facebook nhằm tạo ra một hệ sinh thái không dây mã nguồn mở, và khi dự án này phát triển đủ lớn thì nó sẽ làm mất nguồn thu của các công ty đang kiếm rất nhiều tiền từ mảng kinh doanh trị giá 500 tỉ USD này, ví dụ như Cisco, Huawei, Alcatel-Lucent...

Trước đây Facebook từng thành công với kế hoạch Open Compute Project (OCP) mở thiết kế của các server và phần cứng máy tính giúp các công ty khác có được cùng kiến trúc điện toán như những gì Facebook đang sử dụng để vận hành mạng xã hội khổng lồ của mình. OCP ra đời 5 năm trước với sự tham gia của Facebook, NVIDIA, Intel, Microsoft, IBM, AT&T. Apple đã từng một lần từ chối gia nhập OCP, và có tin đồn rằng toàn bộ đội ngũ về mạng của công ty đã bỏ việc chỉ trong tuần đó (sau đó Apple cũng đã vào OCP).

Nhóm cựu nhân viên Apple nói trên lập ra một startup tên SnapRoute, đứng đầu là Jason Forrester, với mục tiêu cung cấp phần mềm mạng mã nguồn mở dựa trên những gì họ đã làm ở Apple. Hiện phần mềm của SnapRoute cũng đang được sử dụng cho bộ switch Facebook Voyager mới.

Thông qua OCP, Facebook đã phát minh nhiều thứ từ server, ổ lưu trữ, các rack chứa server, và giờ là thiết bị mạng, đồng thời tạo cảm hứng cho cả một hệ sinh thái khởi nghiệp xoay quanh. Dự án có thể một ngày nào đó lật đổ ngôi thống trị của các công ty làm thiết bị mạng nổi tiếng như Cisco.

Nói riêng về dự án OpenCellular, việc làm của Facebook sẽ gây tổn hại tới những đơn vị cung cấp giải pháp viễn thông lớn như Huawei, Alcatel-Lucent, Ciena, Cisco, Fujitsu, Juniper Networks. Các đối tác của Facebook đã bắt đầu thử nghiệm Voyager trong những data center của họ. Facebook cũng ra mắt thêm một trung tâm thúc đẩy khởi nghiệp về viễn thông ở Seoul, Hàn Quốc, thành phố nổi tiếng vì các công nghệ mạng hiện đại. Cùng với nhà mạng SK Telecom, Facebook muốn khuyến khích người ta làm startup về viễn thông. Tham gia vào liên minh Telecom Infrastructure Project của Facebook còn có những công ty khác như Bell, Telstra, Accenture, Canonical, HP với số thành viên lên tới 300.

Nguồn: Business Insider

Routing & Switching

CISCO CERTIFIED CCNA ROUTING & SWITCHING

Chương trình CCNA R&S

CISCO CERTIFIED CCNP

Chương trình CCNP ROUTE

CISCO CERTIFIED CCNP

Chương trình CCNP SWITCH

CISCO CERTIFIED CCNP

Chương trình CCNP TSHOOT

CISCO CERTIFIED CCIE ROUTING AND SWITCHING

Chương trình CCIE

Security

CISCO CERTIFIED CCNA SECURITY

Chương trình CCNA Security

CISCO CERTIFIED CCNP SECURITY

Chương trình SECURE

CISCO CERTIFIED CCNP SECURITY

Chương trình FIREWALL

CCNA Voice

CISCO CERTIFIED CCNA VOICE

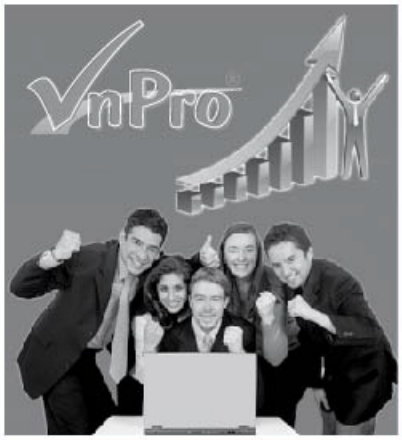
Chương trình ưu đãi các khóa học:

Lớp sáng, chiều:

* Tặng áo thun, tặng sách
* Giảm 5% khi đóng nhóm (trên 2 người)

Lớp tối:

* TẶNG KHÓA HỌC "BẢO MẬT MẠNG DOANH NGHIỆP CĂN BẢN"
* Ưu đãi 30% HP dành cho Sinh Viên
* Ưu đãi lên đến 20% HP dành cho Học viên cũ.
* Ưu đãi dành cho khách hàng doanh nghiệp.
* Tặng Balo, giáo trình khi đăng ký học.

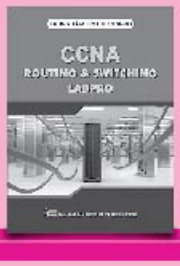


Cam kết lợi ích khi học tại VnPro

- Giáo trình giảng dạy chuẩn quốc tế và LabPro tiếng Việt.
- Thực hành >70% thời lượng chương trình và trực tiếp 100% trên thiết bị chính hãng, hiện đại. (>100 giờ lab)
- Được thực hành miễn phí ngoài giờ.
- Chứng chỉ VnPro được công nhận trên toàn quốc.
- Thi đậu quốc tế sau khi hoàn tất khóa học.

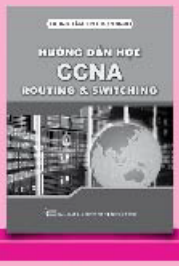
Là trung tâm duy nhất trong cả nước phát hành hơn 20 quyển sách mạng LabPro tiếng Việt. Giáo trình VnPro dược cập nhật, nâng cấp thường xuyên theo chuẩn giáo trình quốc tế

GIẢM* NGAY 10%

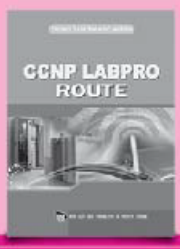


CCNA Routing & Switching
Giá: 150.000 VNĐ

CCDA
Giá: 250.000 VNĐ

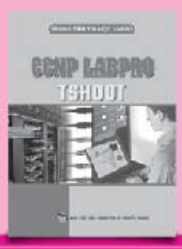


Hướng dẫn học CCNA Routing & Switching
Giá: 180.000 VNĐ



CCNP LABPRO ROUTE
Giá: 120.000 VNĐ

CCNP LABPRO SWITCH
Giá: 120.000 VNĐ



CCNP LABPRO TSHOOT
Giá: 120.000 VNĐ

Ôn thi Route
Giá: 90.000 VNĐ

Ôn thi Switch
Giá: 100.000 VNĐ

Ôn thi Tshoot
Giá: 80.000 VNĐ

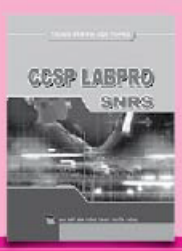
CCNP LABPRO BSCI
Giá: 95.000 VNĐ

CCNP LABPRO BCMSN
Giá: 70.000 VNĐ

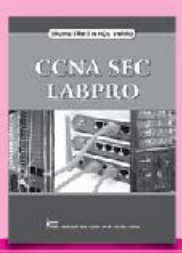
CCNP LABPRO ISCW
Giá: 120.000 VNĐ

CCSP LABPRO SNAF & SNAA
Giá: 120.000 VNĐ

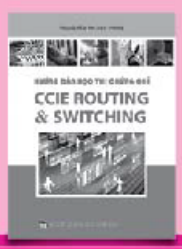
CCSP LABPRO IPS & CSMARS
Giá: 90.000 VNĐ



CCSP LABPRO SNRS
Giá: 140.000 VNĐ



CCNA SEC LABPRO
Giá: 150.000 VNĐ



CCIE R&S
Giá: 150.000 VNĐ

CWNA
Giá: 90.000 VNĐ

Chương trình ưu đãi sách: Áp dụng chính sách là giảm 10% khi đặt sách online

* Khi mua sách LabPro online. Link mua sách online:***http://www.vnpro.vn/sach-labpro/***

VNPRO HÂN HOAN CHÀO MỪNG THÀNH VIÊN MỚI CỦA TỦ SÁCH CCLABPRO: "CCNP LABPRO SWITCH"

Tháng 11/2016 VnPro chính thức đón chào thành viên mới của tủ sách CCLabPro: "CCNP LabPro Switch". Quyển sách như lời khẳng định sứ mệnh của VnPro đối với cộng đồng "Mang đến cho xã hội những công dân có nghề nghiệp và trình độ đẳng cấp quốc tế".

Quyển sách được viết lại mới hoàn toàn bởi chính những đội ngũ chuyên gia, giảng viên của VnPro. Quyển sách là tinh hoa chắt lọc từ những kiến thức cốt lõi, những kinh nghiệm thực tiễn được đúc kết thành. Đồng thời quyển sách cũng kế thừa những kiến thức tinh túy nhất của những quyển sách trước đó để tạo nên một quyển sách LabPro Switch hoàn chỉnh chính thức ra mắt cộng đồng quản trị mạng.

Với "CCNP LabPro Switch" con đường chinh phục CCNP của các bạn sẽ rộng mở hơn bao giờ hết.

Đăng ký mua sách

Để biết thêm thông tin chi tiết vui lòng liên hệ:
TRUNG TÂM TIN HỌC VNPRO
Địa chỉ: 149/1D Ung Văn Khiêm, P.25, Q.Bình Thạnh, Tp.Hồ Chí Minh
Điện Thoại: 083 5124 257 | Email: vnpro@vnpro.org
Website: www.vnpro.vn
Fanpage: www.facebook.com/VnPro
* Lê Uyên: tranleuyen@vnpro.org – 0903 834 636
* Thanh Trâm: thanhtram@vnpro.org – 0949 246 289
* Mỹ Trang: mytrang@vnpro.org – 0964 464 377
Bộ Phận Marketing – Phòng Kinh Doanh

VnPro

THƯ MỜI

TỌA ĐÀM CÙNG CHUYÊN GIA

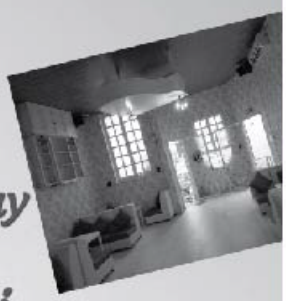
(Ngày 17/12/2016)

TRUNG TÂM TIN HỌC VNPRO
149/1D Ung Văn Khiêm, P25, Q.BT
ĐT: 083 5124257

VnPro trân trọng kính mời Quý Khách đến tham dự buổi Tọa đàm

Chủ Đề

NETWORKING
HIỆN TRẠNG VÀ XU HƯỚNG



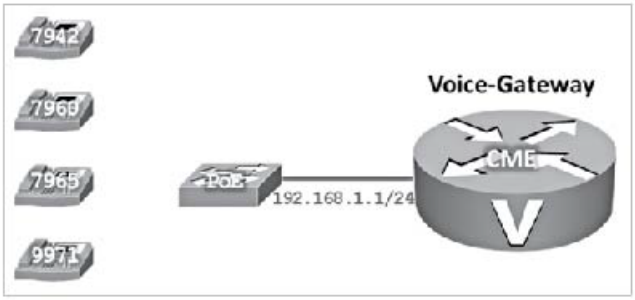
NỘI DUNG

* ***Tình hình ngành Network hiện nay***
* ***Các xu hướng mới trong tương lai***

MIỄN PHÍ THAM DỰ (*đã bao gồm nước uống*)

08h30, ngày 17/12/2016 CAFE UP NGƯỢC
269 Nguyễn Trọng Tuyển, P10, Q. Phú Nhuận
Liên hệ:
Thanh Trâm - 0949 246 829

Hướng dẫn Upgrade SIP Firmware cho Cisco 7965 IP Phone



Yêu cầu

1. Cấu hình cơ bản trên CME.
2. Upgrade SIP Firmware cho Cisco 7965 IP Phone.

Thực hiện

Yêu cầu 1. Cấu hình cơ bản trên CME.

```
hostname CME
interface f0/0
 description Ket noi toi switch PoE
 ip address 192.168.1.1 255.255.255.0
 no shutdown
 exit
line vty 0 4
 privilege level 15
 no login
 exec-timeout 0 0
 exit
line console 0
 logging synchronous
 exec-timeout 0 0
 exit
no ip domain-lookup
no service timestamps log
no service timestamps debug
ip dhcp excluded-address 192.168.1.1
ip dhcp pool Voice
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 option 150 ip 192.168.1.1
 exit
exit
clock set 12:00:00 12 Nov 2016
configure terminal
```

Yêu cầu 2. Upgrade SIP Firmware cho Cisco 7965 IP Phone.

Các bước upgrade SIP Firmware cho Cisco 7965 IP Phone.

- Bước 1. Tải SIP Firmware mới nhất cho 7965 Phone.

- Bước 2. Chuyển .ZIP file thành .TAR file.

- Bước 3. Tiến hành Import 7965 SIP Firmware vào bộ nhớ Flash của CME.

- Bước 4. Cấu hình thông tin SIP Firmware trên TFTP Server và CME.

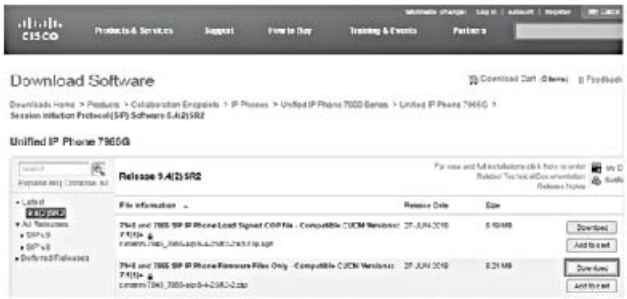
- Bước 5. Tiến hành Upgrade SIP Firmware trên Cisco 7965 IP Phone.

Bước 1. Tải SIP Firmware mới nhất cho 7965 Phone.

-https://software.cisco.com/download/release.html?mdfid=281346596&softwareid=282074288&release=9.4(2)SR2&relind=AVAILABLE&rellifecycle=&reltype=latest

- Firmware có đuôi là .cop.sgn thường được sử dụng trên CUCM.

- Firmware có đuôi là .zip được sử dụng trên CME.



Bước 2. Chuyển .ZIP file thành .TAR file.

Chuyển cmterm-7945_7965-sip.9-4-2SR2-2.zip thành định dạng cmterm-7945_7965-sip.9-4-2SR2-2.tar bằng chương trình ArcConvert.

Bước 3. Tiến hành Import 7965 SIP Firmware vào bộ nhớ Flash của CME.

Giải nén cmterm-7945_7965-sip.9-4-2SR2-2.tar vào thư mục 7965_SIP_Firmware trên bộ nhớ Flash của CME.

```
CME(config)# ip ftp username cisco
CME(config)# ip ftp password cisco
CME# archive tar /xtract ftp://192.168.1.2/cmterm-7945_7965-sip.9-4-2SR2-2.tar flash:7965_SIP_Firmware
CME#
```

```
CME#
Loading cmterm-7945_7965-sip.9-4-2SR2-2.tar
extracting apps45.9-4-2ES22.sbn (4638228 bytes)!!!!!!!!!!!!!!!!
extracting cnu45.9-4-2ES22.sbn (581773 bytes)!!
extracting cvm45sip.9-4-2ES22.sbn (2691631 bytes)!!!!!!!!
extracting dsp45.9-4-2ES22.sbn (364495 bytes)!!
extracting jar45sip.9-4-2ES22.sbn (1893534 bytes)!!!!!!
extracting SIP45.9-4-2SR2-2S.loads (667 bytes)
extracting term45.default.loads (667 bytes)
extracting term65.default.loads (667 bytes)
[OK - 10179584/4096 bytes]

CME#
```

Bước 4. Cấu hình thông tin SIP Firmware trên TFTP Server và CME.

Ta không thể upgrade trực tiếp SIP load từ một số SCCP load cũ, đôi khi ta cần phải upgrade phiên bản SCCP load chẳng hạn như upgrade từ SCCP 5.x/7.x thành SCCP 8.x hoặc các version mới hơn mới có thể upgrade thành SIP firmware trên IP Phone.

Cấu hình TFTP Server trên CME.

```
CME(config)# tftp-server flash:/7965_SIP_Firmware/apps45.9-4-2ES22.sbn
CME(config)# tftp-server flash:/7965_SIP_Firmware/cnu45.9-4-2ES22.sbn
CME(config)# tftp-server flash:/7965_SIP_Firmware/cvm45sip.9-4-2ES22.sbn
CME(config)# tftp-server flash:/7965_SIP_Firmware/dsp45.9-4-2ES22.sbn
CME(config)# tftp-server flash:/7965_SIP_Firmware/jar45sip.9-4-2ES22.sbn
CME(config)# tftp-server flash:/7965_SIP_Firmware/SIP45.9-4-2SR2-2S.load
CME(config)# tftp-server flash:/7965_SIP_Firmware/term45.default.loads
CME(config)# tftp-server flash:/7965_SIP_Firmware/term65.default.loads
```

Cấu hình DHCP Option 150 trỏ về IP của TFTP Server.

```
ip dhcp excluded-address 192.168.1.1
ip dhcp pool Voice
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 option 150 ip 192.168.1.1
 exit
```

Khai báo thông tin 7965 Phone SIP Firmware trên CME để hướng dẫn IP Phone tải về.

```
no ephone 1
telephony-service
 no create cnf-files
 exit
```

Khai báo SIP firmware load muốn upgrade.

```
voice register global
 mode cme
 source-address 192.168.1.1 port 5060
 max-dn 144
 max-pool 42
 load 7945 SIP45.9-4-2SR2-2S
 load 7965 SIP45.9-4-2SR2-2S
 tftp-path flash:
 create profile
 exit
```

```
voice register dn 1
 number 2001
 exit
voice register pool 1
 id mac b000.b4d9.a3b1
 type 7965
 number 1 dn 1
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
 apply-config
 exit
voice register global
 create profile
 exit
```

Bước 5. Tiến hành Upgrade SIP Firmware trên Cisco 7965 IP Phone. Để 7965 Phone tiến hành Load SIP Firmware vừa cấu hình về, ta có thể tiến hành Factory Reset 7965 như sau.

- Thao tác 1. Unplug cáp nguồn power cable trên 7965 Phone rồi sau đó cắm lại plug in.
- Thao tác 2. Trong khi Phone đang khởi động powering up, trước khi đèn Speaker button nhấp nháy (flashes on & off) ta nhấn giữ (press & hold) # key.
- Thao tác 3. Tiếp tục nhấn giữ hold # cho đến khi mỗi line button (phía bên phải LCD screen) sáng lần lượt từ trên xuống dưới (flashes on & off) theo thứ tự màu cam (orange colour).
- Thao tác 4. Thả phím # key và nhấn lần lượt 123456789*0#

Có thể kiểm tra Firmware Version bằng cách nhấn nút Setting button > Model Information.

```
CME# show voice register pool phone-load
Pool    Device Name      Current-Version      Previous-Version
===     =======          =========            ==========
1       SEPB000B4D9A3B1  Cisco-CP7965G/9.4.2
CME#
```

Giải pháp bảo vệ trước cuộc tấn công mạng

Ngăn chặn mã độc xâm nhập hệ thống là vấn đề không thể giải quyết trọn vẹn. Do vậy, cần phải có cách tiếp cận nhằm phát hiện được các mối đe dọa tiềm tàng và ngăn chặn chúng.

Mã độc (malware) hiện nay có khả năng che dấu, ẩn mình và vượt qua các biện pháp phòng thủ truyền thống. Đội an ninh thông tin luôn phải đối mặt với nhiều thách thức vì những công cụ bảo mật mà họ được trang bị không đủ khả năng kiểm soát cũng như phát hiện và loại bỏ các mối đe dọa trước khi mã độc gây ra thiệt hại cho hệ thống.

Thống kê cho thấy các tổ chức đang từng ngày phải đối mặt với những đợt tấn công âm thầm và liên tục. Doanh nghiệp bị tấn công mạng, mất cắp dữ liệu luôn là vấn đề nóng. Hacker trên toàn cầu đã và đang tạo ra những loại mã độc tinh vi, lây nhiễm vào hệ thống bằng nhiều cơ chế khác nhau. Những công cụ bảo mật hiện đại thường quan sát dữ liệu, tập tin ngay khi mã độc xâm nhập vào hệ thống mạng, nhưng lại cung cấp rất hạn chế thông tin về hoạt động của những mối đe dọa đang tìm cách vượt qua hệ thống phòng thủ. Vì vậy, các cuộc tấn công có chủ đích thường dễ dàng vượt qua những công cụ phòng thủ truyền thống như Firewall, IPS…

Như đã đề cập, việc ngăn chặn mã độc xâm nhập vào hệ thống là vấn đề không thể giải quyết trọn vẹn. Do vậy, cần phải có những cách tiếp cận nhằm phát hiện được các mối đe dọa tiềm tàng và ngăn chặn trước khi chúng gây thiệt hại.

Trong phần này chúng ta sẽ xem xét hai giải pháp điển hình: AMP của Cisco và MATD của Intel.

1. Advanced Malware Protection của Cisco

Cisco là một trong những nhà tiên phong trong việc đưa ra giải pháp giúp doanh nghiệp theo dõi được mọi hoạt động đang diễn ra trong hệ thống mạng, từ đó có khả năng chủ động ứng phó trước những đợt tấn công của hacker.

Advanced Malware Protection (AMP) là giải pháp bảo mật cho phép xử lý mã độc ở các giai đoạn phát tán hay đang ẩn mình trong hệ thống. Giải pháp mang lại khả năng kiểm soát, nhanh chóng phát hiện, cách ly và triệt tiêu các mối đe dọa bằng mã độc ngay cả khi chúng đã vượt qua được lớp tường lửa phòng thủ hay các hệ thống AntiVirus truyền thống hiện nay. AMP là một công cụ không thể thiếu cho công tác điều tra các sự cố an ninh mạng có liên quan tới mã độc. Giải pháp AMP không những mang lại hiệu quả về mặt chi phí mà còn gây ảnh hưởng tối thiểu đến khả năng vận hành của hệ thống.

Bảo mật là một chuỗi quá trình kiểm tra

AMP là giải pháp được tích hợp thông tin, khả năng phân tích và phòng chống mã độc hiện đại. Hệ thống sẽ được bảo vệ một cách toàn diện và liên tục: trước khi, trong khi và sau khi những cuộc tấn công đã vượt qua được lớp bảo mật truyền thống như tường lửa, antivirus.

- **Trước khi bị tấn công.** AMP sử dụng thông tin về các mối đe dọa trên toàn cầu được thu thập từ Cisco's Collective Security Intelligence, Talos Security Intelligence and Research Group, và AMP Threat Grid để ngăn chặn những cuộc tấn công bằng mã độc đã được biết đến trước đó hay đã được công bố trên thế giới, củng cố phòng thủ cũng như chống lại những mối đe dọa tiềm tàng.

- **Trong khi bị tấn công.** AMP sử dụng những thông tin có được từ những cuộc tấn công đã biết (signature), kết hợp với công nghệ AMP Threat Grid với khả năng tự động phân tích mã độc để xác định và ngăn chặn những tập tin nghi ngờ, nguy hiểm đang cố gắng xâm nhập vào hệ thống mạng.

- **Sau khi tin tặc đã thực hiện được xâm nhập.** AMP không chỉ kiểm tra, giám sát tại thời điểm bị tấn công mà vẫn tiếp tục theo dõi và phân tích toàn bộ hoạt động, đường đi của dữ liệu dù được coi trước đó là "sạch", tìm kiếm dấu hiệu của những hành vi nguy hiểm. Khi phát hiện một tập tin có chứa mã độc hại, AMP cung cấp cho nhà quản trị các thông tin trực quan về hoạt động trong mạng, trong từng thiết bị đầu cuối của mã độc, AMP cũng cho phép ứng phó nhanh và giải quyết sự cố thông qua giao diện web đơn giản. Những tính năng này cho phép đội an ninh có thể quản lý và kiểm soát sâu bên trong hệ thống, nhanh chóng phát hiện tấn công, xác định phạm vi lây lan và cô lập mã độc trước khi chúng gây ra thiệt hại đáng kể hơn cho hệ thống.

Phân tích & theo dõi liên tục mọi hành vi trong hệ thống

Hầu hết các hệ thống chống mã độc nằm trên mạng hoặc trên thiết bị đầu cuối chỉ kiểm soát dữ liệu khi chúng đi vào hệ thống. Nhưng mã độc ngày nay rất tinh vi và có khả năng vượt qua những phát hiện ban đầu nhờ vào kỹ thuật ẩn mình như mã hóa hay sử dụng những giao thức chưa từng được biết tới. Không thể ngăn chặn những thứ mà bạn không thể thấy, đó là nguyên nhân chính dẫn đến nhiều hệ thống thất thủ trước những cuộc tấn công. Đội an ninh không thấy được mối đe dọa và không hề hay biết về sự tồn tại của mã độc. Vì vậy, họ không thể tiến hành biện pháp cách ly và ngăn chặn. Thông thường, mã độc chỉ bị phát hiện sau một thời gian dài hoặc sau khi hacker đã đạt được mục tiêu đánh cắp dữ liệu và gây ra thiệt hại cho hệ thống.

AMP mang lại giá trị khác biệt trong phương thức và nhận thức về bảo mật, đó là phương pháp phòng ngừa, ngăn chặn ngay cả khi hệ thống phát hiện mã độc không phát huy hiệu quả 100%. AMP tiếp tục phân tích các tập tin, dữ liệu ngay cả đối với các tập tin được coi là "lành tính" . Với các tập tin này, AMP cùng hệ thống hỗ trợ thu thập thông tin và phân tích mã độc trên đám mây tiếp tục theo dõi, phân tích và ghi lại toàn bộ hoạt động của những tập tin, giao tiếp giữa các thiết bị đầu cuối và trên mạng nhằm nhanh chóng phát hiện những mối đe

dọa đang ẩn mình. Ngay khi có các kết quả phân tích mới về mã độc được cập nhật từ đám mây AMP sẽ đưa ra cảnh báo cũng như cung cấp đầy đủ thông tin dựa trên hành vi của mối đe dọa, từ đó người quản trị mạng có thể tự mình trả lời những câu hỏi quan trọng sau:

- Mã độc đến từ đâu?
- Mã độc xâm nhập vào hệ thống nào đầu tiên, bằng cách nào?
- Mã độc đã tác động vào những phân vùng nào của hệ thống và những hệ thống đã bị lây nhiễm?
- Mã độc đã và đang làm gì?
- Làm thế nào ngăn chặn và loại bỏ chúng?

Dựa trên những thông tin này, đội ngũ an ninh có thể nhanh chóng nắm bắt được điều gì đang xảy ra và tiến hành những biện pháp kỹ thuật để cách ly hoặc ngăn chặn mã độc tiếp tục xâm hại đến hệ thống cũng như các thiết bị đầu cuối như PC, server. Với khả năng liên tục kiểm tra, giám sát, đánh dấu lại toàn bộ lưu lượng mạng ra vào hệ thống, cũng như thông tin các tập tin được lưu trữ và thực thi tại những thiết bị đầu cuối nào, AMP có thể ngăn chặn được những đợt tấn công, cũng như là công cụ đắc lực cho công tác điều tra sự cố sau các đợt tấn công có sử dụng mã độc.

2. McAfee Advanced Threat Defense của Intel

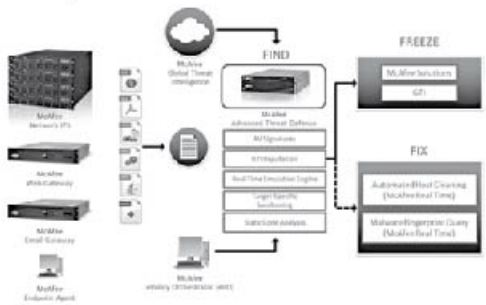
Việc đầu tư và triển khai các giải pháp bảo mật mới theo nhu cầu đã trở thành nỗi ác mộng dai dẳng của hầu hết các tổ chức hiện nay. Hệ thống bảo mật trở nên phức tạp, các chức năng trùng lặp đã gây khó khăn trong việc bảo vệ, phát hiện và xử lý sự cố an ninh. Bên cạnh đó, chi phí đầu tư mới cũng như bảo trì cho toàn bộ hệ thống bảo mật tăng lên một cách đáng kể.

Từ những vấn đề trên, Intel Security đưa ra chiến lược xây dựng hệ thống bảo mật "Threat Defense LifeCycle" trên nền tảng kiến trúc Enterprise Security Connected. Với kiến trúc này, các sản phẩm bảo mật được kết nối với nhau để chia sẻ thông tin về các mối nguy hại, đồng thời được tích hợp để tự động hóa các tác vụ phát hiện, xử lý sự cố và bảo vệ hệ thống CNTT nhanh và hiệu quả hơn.

McAfee Advanced Threat Defense (MATD) được thiết kế để phát hiện mã độc tàng hình, zero-day. Nó sử dụng một cách hiệu quả các nguồn thông tin: chữ ký để phát hiện virus, dịch vụ đánh giá mức độ uy tín, và mô phỏng thời gian thực, thông qua đó nhanh chóng xác định và ngăn chặn mã độc.

Việc phát hiện mã độc là quan trọng, nhưng đó chỉ là một phần của một giải pháp hiệu quả. Do đó, mở rộng tầm bảo vệ từ hệ thống mạng đến hệ thiết bị cuối là cần thiết, để không chỉ nhận dạng được mã độc mà còn bảo vệ chống lại các mối nguy hại từ nó. Một trong những điểm cốt lõi của an ninh tích hợp hệ thống là khả năng chia sẻ thông tin giữa các cơ sở hạ tầng với nhau để cung cấp khả năng bảo mật mạnh mẽ hơn.

Giải pháp của McAfee đã thay đổi hành vi "phát hiện" truyền thống bằng cách kết nối khả năng phân tích mã độc với các hệ thống phòng thủ, từ mạng vành đai đến các thiết bị đầu cuối, và chia sẻ thông tin về mối đe dọa đã được phân tích với toàn bộ môi trường CNTT.



McAfee tập trung vào ba yếu tố quan trọng để giải quyết vấn đề mã độc là: tìm mối đe dọa (Find), đóng băng nó (Freeze), và khắc phục (Fix).

Find: Khi các giải pháp Endpoint Security, Web Filtering, Network IPS không thể xác định chắc chắn 100% một tập tin đáng ngờ là mã độc, chúng chuyển thông tin này cho MATD, và MATD sẽ phân tích tập tin trong một môi trường ảo hóa, tương đồng với hệ thống thực. MATD không chỉ nhìn vào mã thực thi, mà còn nhìn những mã không hoạt động.

Freeze: Việc tích hợp chặt chẽ giữa các giải pháp của McAfee cho phép chia sẻ kết quả phân tích của MATD với Endpoint Security, Web Gateway và Network IPS… Từ đó giúp các thành phần này có thể chủ động phát hiện và ngăn chặn tập tin đáng ngờ do MATD đã dán nhãn mã độc. Network Security Platform thậm chí có thể cô lập hệ thống đã bị lây nhiễm để ngăn chặn mã độc lây lan.

Fix: Có thể sử dụng Real Time với ePO để khắc phục bất kỳ thiệt hại gây ra bởi mã độc. Real Time sẽ đặt "câu hỏi" cho các thiết bị đầu cuối trong mạng và sau đó hành động theo câu "trả lời" nhận được. Dựa trên kết quả phân tích của MATD, có thể nhanh chóng phát hiện hệ thống bị nhiễm. Sau đó, Real Time tự động loại bỏ các tập tin liên quan và các hành động đã được khởi tạo bởi mã độc.

Các thành phần của MATD

MATD dễ dàng tích hợp với các giải pháp bảo mật khác của McAfee như McAfee Network Security Platform, Web Gateway, Endpoint Protection. MATD kết hợp nhiều khả năng phát hiện phần mềm độc hại ở nhiều lớp khác nhau:

- McAfee Antivirus cung cấp chữ ký để nhanh chóng phát hiện các phần mềm độc hại đã được biết.
- McAfee Global Threat Intelligence theo dõi những hành vi bất bình thường và xác định danh tiếng các trang web độc để sản phẩm bảo mật McAfee có thể chặn truy cập.
- Real-Time Emulation Engine: mô phỏng việc thực thi của một file và ghi lại kết quả hành vi, kết quả phân tích tương ứng với thời gian thực.
- Dynamic analysis: là công nghệ chạy mã độc trong một môi trường an toàn (môi trường ảo, được gọi là sandbox) để quan sát hành vi của mã độc.
- Full Static Analysis: là công nghệ liên quan đến việc giải mã thực tế và phân tích mã độc để xác định nó sẽ thực thi như thế nào.

Cách tiếp cận theo nhiều lớp được thiết kế để đảm bảo bất cứ khi nào mã độc được lọc ra bởi nhiều lớp mà không mất thêm thời gian và nguồn lực để phân tích. Cách tiếp cận này nhằm để phân tích nhanh hơn và bảo vệ tốt hơn.

Thay vì triển khai riêng lẻ các giải pháp, MATD quản trị tập trung cùng với sự tích hợp liền mạch với các sản phẩm khác của McAfee, được thiết kế một cách thống nhất để đơn giản hóa việc quản trị và giảm chi phí vận hành trong khi tối đa hóa khả năng bảo vệ.

Theo PC World VN

10 TỪ TIẾNG ANH DỄ GÂY NHẦM LẪN

Cùng với phát âm và ngữ pháp, một trong những thách thứ lớn nhất cho những người học tiếng Anh là từ vựng. Bạn có thể không phải đánh vật với những từ mới khi nói, nhưng khi viết chúng ra, khả năng đọc của bạn sẽ được đánh giá.

Dù là một ngôn ngữ hay và tuyệt vời (xem chín lý do tại sao tiếng Anh trở nên phổ biến), đây cũng không phải là ngôn ngữ dễ đọc nhất. Các phát âm và ô hợp những cách kết hợp các chữ cái lạ lùng không phải lúc nào cũng là dấu hiệu cho cách viết – do đó bạn cũng đừng thắc mắc tại sao những người học (và cả người nói tiếng Anh bản xứ!) đôi khi phải vật vã mới viết được đúng.

Chúng tôi tập hợp mười từ tiếng Anh khó nhất và cũng đưa ra những gợi ý giúp bạn không viết sai chúng. Chúc may mắn!

1. Necessary

Đau đầu thật! Từ này có hai chữ "c", hai chữ "s" hay lai một trong hai trường hợp đó? Xử lý câu hỏi hóc búa này bằng cách tưởng tượng rằng bạn đang mặc một chiếc áo phông có một sleeve (tay áo). Mặc như thế có dễ không? Tất nhiên là không rồi – vì một cái áo cần phải có một collar (cổ áo, chữ c!) và hai sleeve (tay áo, chữ s!)

2. Stationary VÀ Stationery

Hai từ này hoàn toàn khác nghĩa nhau: "Stationary" có nghĩa là không dịch chuyển, trong khi "stationery" dùng để chỉ các vật dụng văn phòng như bút chì, tẩy, giấy, và phong bì. Nhưng làm thế nào để nhớ được từ nào chỉ cái nào. Lấy ERY, phần cuối của từ "stationery", theo manh mối: Giờ hãy nhớ rằng chữ "e" là của từ erasers và enlopers – hai thành phần rất thông dụng trong các stationery (vật dụng văn phòng)!

3. Separate

Khi đọc từ này, có vẻ cũng giống như từ "seperate". Tuy nhiên, viết theo cách này là sai, sai, và sai! Giờ để không mắc lại lỗi này nữa, hãy nghĩ về một con chuột cống béo và đầy lông. Đây là một hình ảnh bạn không thể quên được trong một thời gian! Hãy nhớ: there's a rat in "separate".

4. Affect VÀ Effect

Hai từ đồng âm này phát âm giống nhau nhưng có cách viết và/hoặc nghĩa khác nhau – gây rất nhiều tranh cãi trong các bài viết khắp toàn cầu! Làm thế nào để nhớ được cần phải dùng từ nào? Hãy lấy chữ cái đầu của từng từ làm gợi ý cho bạn. "Affect" bắt đầu bằng chữ "a" và chỉ một action, trong khi đó "effect" bắt đầu bằng chữ "e" và chỉ tác động khi end (kết thúc)

5. Embarrassed

Bạn xấu hổ khi không viết được từ này? Bạn không phải là người duy nhất đâu! Đây là một trường hợp hai chữ cái gây nhầm lẫn khác. Trong trường hợp này, chúng ta cần nhớ hai chữ "r" và "s". Để tập nhớ, hãy tưởng tượng một cậu bé xấu hổ vì giọng ca khủng khiếp của chị mình và nghĩ về câu: "He goes really red when his sister sings." (Cậu bé đỏ bừng mặt khi nghe chị gái hát.)

6. Compliment VÀ Complement

Compliment là lời khen một người nói về một người khác, trong khi đó complement là một điều gì đó bổ sung hoặc hoàn thiện cho một thứ khác (ví dụ, bơ là một món ăn bổ sung cho rượu). Để nhớ từ nào dùng cho cái nào, hãy nhìn vào chữ cái ở giữa: Ngược với compliment là insult (nhục mạ). Trong khi đó, complement lại có tác dụng enhance cho một thứ khác.

7. Accommodation

Ô, lại một từ dễ nhầm lẫn bởi hai chữ cái nữa! Để nhớ phải dùng hai cặp chữ cái trong từ này, hãy tự hình dung ra bạn đang nhận một phòng khách sạn cao cấp có hai giường ngủ lớn. Cuối cùng, accommodation tốt nhất sẽ có hai cặp giường.

8. Rhythm

Vâng, rhythm (giai điệu). Từ phát âm khó này không có nguyên âm và có nhiều âm "h" hơn bình thường. Bạn không phải là người duy nhất cho rằng từ này khó nhìn và khó nhớ. Giờ bạn hãy tưởng tượng một sàn nhảy toàn các vũ công đang nhảy hết mình và đọc rất dông dạc câu nói dễ nhớ: "Rhythm helps your two hips move." (Giai điệu khiến cho hông bạn không giữ yên được).

9. Dessert vÀ Desert

"Dessert" rất giống với "desert" đối với hầu hết những người học tiếng Anh – và với cả một vài người nói tiếng Anh bản xứ! Từ nào có hai chữ "s"? Hãy chụp ảnh bạn đang say mê một chiếc bánh sô cô la lộng lẫy, những lát chuối, hay loại kẹo nào bạn thích. Bạn muốn có thêm nữa không. Chúng tôi cũng tưởng thế! Hãy sẵn sàng để thêm một chữ "s" nữa: Khi nói đến dessert (món tráng miệng), chúng tôi luôn muốn một chút nữa.

10. Dilemma

Với tất cả những người phát âm từ dilemmas, chỉ cần học một lần! Thông thường, mọi người sẽ bỏ qua chữ "m" thứ hai khi phát âm từ khó này. Ghi nhớ điều này và đừng bỏ qua điều đó bằng cách nhớ câu "Emma có dilemma".

Những câu chuyện Độc lạ ít Người biết về GIÁNG SINH

Càng gần đến Giáng sinh, mọi người càng háo hức, chờ đợi nhưng rất ít người biết về những câu chuyện độc lạ về Giáng sinh này.

Mở đầu những câu chuyện độc lạ ít người biết về Giáng sinh là sự xuất hiện của ông già Noel. Truyền thuyết Bắc Âu nổi tiếng với vị thần Odin hung dữ nhưng không nhiều người biết rằng thần Odin chính là hình tượng thần thoại tạo cảm hứng xuất hiện của ông già Noel. Theo thần thoại dân gian Pagan, thần Odin luôn chỉ huy chuyến đi săn vào mỗi dịp lễ Yule, dịp lễ của các bộ lạc Pagan tương ứng với Giáng Sinh. Để đáp lại tấm lòng của những đứa trẻ ngoan, thần Odin sẽ để lại những món quà, đồ chơi, bánh kẹo mà những đứa trẻ mong muốn vào những chiếc ủng đó.

Hầu hết các con tuần lộc của ông già Noel có tên rất nam tính như Blitzen, Comet, Cupid... Tuy nhiên, sự thực thì tuần lộc đực sẽ rụng gạc vào dịp Giáng sinh, vì vậy những con tuần lộc kéo xe trượt tuyết của ông già Noel là có khả năng không phải là tuần lộc đực, nó có thể là tuần lộc cái hoặc tuần lộc đực bị thiến.

Thêm một câu chuyện thú vị nữa về những con tuần lộc. Các nhà khoa học Na Uy đã đưa ra giả thuyết rằng hình ảnh những con tuần lộc mũi đỏ là có thật và có lẽ chiếc mũi đỏ như cà chua là kết quả của việc chúng bị nhiễm ký sinh trong hệ thống hô hấp, tương tự như con người khi mắc cảm cúm.

"Jingle Bells" là bài hát Giáng sinh tất cả chúng ta đều có ít nhất một lần nghe thấy trong đời. Tần suất xuất hiện của nó dày đặc trên sóng phát thanh, truyền hình, các trung tâm mua sắm, thiệp nhạc... Tuy nhiên, có thể bạn không hề biết rằng "Jingle Bells" ban đầu có một cái tên khác là "One Horse Open Sleigh" và có liên quan đến lễ Phục sinh. Theo thời gian, tiêu đề và lời bài hát được thay đổi và trở thành bài hát độc quyền chỉ phát vào dịp Giáng sinh.

Có thể bạn không biết, ba màu sắc truyền thống của Giáng sinh là màu xanh lá cây, đỏ, và vàng. Màu xanh lá cây từ lâu đã là biểu tượng của cuộc sống và sự tái sinh. Màu đỏ tượng trưng cho máu của Chúa Kitô, và vàng tượng trưng cho ánh sáng tâm linh cũng như sự giàu có, hưng vượng, sung túc.

Bài hát đầu tiên được ghi âm trong không gian là bài "Jewel in the Night", có nội dung về Giáng sinh, được một phi hành gia có tên là Chris Hadfield sáng tác và gửi tới gia đình, bạn bè trên Trái đất. Nó được tải lên Youtube vào đêm Giáng sinh 2012 và nhiều người nói đùa rằng nếu người ngoài hành tinh ghé thăm Trái đất mừng Giáng sinh, đây sẽ là bài hát đầu tiên họ được nghe.

Cây thông đầu tiên trên thế giới được trang trí là bởi Martin Luther, người sáng lập ra đạo Tin lành. Theo những câu chuyện kể lại, khi Luther đi dạo trong rừng thì bất chợt ông ngước nhìn bầu trời. Với góc nhìn từ dưới lên, những vì sao như được gắn lên đỉnh cây thông, tỏa ra thứ ánh sáng kỳ diệu. Ngay lập tức, ông quyết định mang một cây thông nhỏ về nhà và đặt những ngọn nến lên cành cây để trang trí. Từ đó, ý tưởng về việc trang trí cây thông Giáng Sinh đã ra đời và ngày một biến hóa, cải tiến với những chuỗi đèn nhấp nháy, quả châu sáng bóng đẹp lộng lẫy.

LỊCH KHAI GIẢNG THÁNG 12/2016

Mã lớp	Tên khóa học	Ngày khai giảng	Ngày học	Giờ học	Học phí/khóa	Thời gian
CHƯƠNG TRÌNH CCNA						
A17	CCNAX (200-125)	03/12	Thứ 7	Sáng + Chiều	6.720.000	152 giờ
AK22		05/12	2 – 4 – 6	2:00 – 5:00PM	3.360.000	
AK24		09/12	2 – 4 – 6	8:30 – 11:30AM	3.360.000	
AK26				2:00 – 5:00PM	3.360.000	
A18				6:30 – 9:30PM	6.720.000	
AK15		15/12	3 – 5 - 7	8:30 – 11:30AM	3.360.000	
AK17				2:00 5:00PM	3.360.000	
A19				6:30 9:30PM	6.720.000	
AK28		21/12	2 – 4 – 6	8:30 11:30AM	3.360.000	
A20				6:30 – 9:30PM	6.720.000	
AK19		29/12	3 – 5 - 7	2:00 – 5:00PM	3.360.000	
A21				6:30 9:30PM	6.720.000	
AK4	CCNAX Online	16/12	2 4 6	6:30 9:30PM	2.900.000	72 giờ
AK5		17/12	Thứ 7	Sáng + Chiều	2.900.000	
AS9	CCNA Security (640-554)	22/12	3 – 5 – 7	6:30 – 9:30PM	5.500.000	72 giờ
AV7	CCNA Voice (640-461)	22/12	3 – 5 – 7	6:30 – 9:30PM	6.720.000	100 giờ
CHƯƠNG TRÌNH CCNP						
P1-8	ROUTE (300 - 101)	07/12	2 – 4 – 6	6:30 – 9:30PM	8.232.000	120 giờ
P1-K9		15/12	3 – 5 – 7	8:30 – 11:30AM	5.500.000	
P1-9				6:30 – 9:30PM	8.232.000	
P1-11		17/12	Thứ 7	Sáng +Chiều	8.232.000	
P2-K8	SWITCH (300 - 115)	09/12	2 – 4 – 6	8:30 – 11:30AM	5.500.000	120 giờ
P2-7				6:30 9:30PM	8.232.000	
P2-8		27/12	3 – 5 – 7	6:30 – 9:30PM	8.232.000	
P3-2	TSHOOT (300 - 135)	28/12	2 – 4 – 6	6:30 – 9:30PM	8.232.000	120 giờ
CHƯƠNG TRÌNH CCIE WRITTEN						
EW4	CCIE WRITTEN (Version 5)	08/12	3 – 5 – 7	6:30 – 9:30PM	11.760.000	120 giờ
KHÓA HỌC CHUYÊN ĐỀ						
PS1-1	FIREWALL	24/12	Thứ 7	Sáng + Chiều	5.500.000	54 giờ
PS1-3	VPN	27/12	3 – 5 – 7	6:30 – 9:30PM	5.500.000	54 giờ
PS1-5	MPLS Nguyên lý & Ứng Dụng	27/12	3 – 5 – 7	2:00 – 5:00PM	5.500.000	54 giờ
PS1-7				6:30 – 9:30PM	5.500.000	

Bản tin Dân Cisco - Được phát hành bởi **Công Ty TNHH Tư Vấn & Dịch Vụ Chuyên Việt**
Chịu trách nhiệm xuất bản: **Nguyễn Cảnh Hoàng**
Giấy phép xuất bản số: **69/QĐ - STTTT** Ngày ĐK: **26/10/2011**
Công ty in: **Sao Băng Design**
Số lượng in: **2.000 cuốn/kỳ**
Kỳ hạn xuất bản: **1 kỳ/tháng**