Security+

Teacher : Fallahzadeh

Start Date: 1404/05/31

Link : https://www.youtube.com/watch?v=geDkUSjfKu0&list=PL-mrTgDRWNRU3YALjzV_cruqYKyhDDfEB

1404/05/31

دیتا میتونه به دو شکل باشه :

Public.1

Private.2

اضافه کردن امنیت به اطلاعاتی که داریم information Security نامیده میشه

Security triangle —> CIA

Confidentiality.1 : محرمانگی اطلاعات یا دیتا

Data should not sniff

Data should encrypt

دو مدل رمزنگاری داریم:

same key : sym ALG.1

public key and private key <--- key pair : Asym ALG.2

دیتایی که رمز نشده میگن Clear Text

به اطلاعات رمز شده Cipher میگن

SYM Encryption ALG: دیتا توسط مبدا با یک کلید رمزنگاری میشه و دیتا در مقصد با همون کلید رمزگشایی میشه

DES,3DES,AES مدل هایی از این رمزنگاری هستند

DES=56bit, 3DES=168bit, AES=256bit

ASym Encryption ALG: هر نودی public key خودش رو در اختیار بقیه میزاره تا با اون دیتا رو رمزنگاری کنن و سپس دیتارو با private key خودش باز میکنه.

یه مرجع باید برای تایید نودها باشن چون ما نمیدونیم public key مال کیه

PKI: Public Key Infrastructure <-- CA <-- Certificate Authority

هر نودی میاد اطلاعات خودش رو که باید توی cert قرار بگیره واسه CA میفرسته (به این عمل که درخواست cert هست Certificate Enrollment میگن) CA میاد cert رو با public key خودش امضا میزنه و نود دریافت کننده امضای CA رو داره پس میگه این cert معتبره بعد میاد با public key ارسال کننده دیتارو رمزنگاری میکنه. مثل:

RSA, Diffie Hellman

Integrity.2 : صحت دیتا، یعنی کسی دیتارو تغییر نداده باشه.

Malware : بدافزارها

هکر میاد اون بدافزار رو اضافه میکنه به یه سری فایل دیگه مثل پی دی اف ها و.. برای گرفتن دسترسی از قربانی

Hash کردن دیتارو رمزنگاری نمیکنه، hash اون فایل به مقصد داده میشه و گفته میشه پس از دریافت دیتارو دوباره hash کنه و خروجی رو با خروجی که بهش داده شده مقایسه کنه
hash یک طرفه هستش یعنی نمیتونیم از هش اون دیتا به خود دیتا برسیم. الگوریتم هایی مثل MD5, SHA

1404/06/02

واحد امنیتی باید برنامه رو چک کنه که با جایی ارتباط نگیره یا قسمتی از سیستم رو نخواد تغییر بده بعد واسه اون فایل یه هش تولید کنن.

Availability.3 : در دسترس بودن اطلاعات

حملاتی مثل Distributed Denial of Service یا DDOS برای از دسترسی خارج کردن سرویس ها استفاده میشه

برای حفظ این موضوع باید Redundancy داشته باشیم.

Edge Router به روتری گفته میشه که ترافیک داخلی رو از ترافیک خارجی جدا میکنه

AAA

Authentication.1 : کی هستی که میخوای به سیستم وصل بشه

Authorization.2 : حالا که مشخص شد کی هستی الان باید مشخص بشه که چه کارهایی میتونی بکنی

Accounting.3 : تمام وقایع یک جا باید ثبت بشه

CISCO ISE این کار رو انجام میده

کجا باید پیاده سازی بشه: برنامه های تحت شبکه،پروتکل های تحت شبکه،سرویس ها،دستگاه ها

CIA و AAA مکمل همدیگه هستند.

Threat : تهدیدهایی که میتونن داخل شبکه باشن

ما باید از Asset هامون نگهداری کنیم.تهدیدها برای هر دارایی ما متفاوته. باید دارایی هامون مشخص بشه و ارزش هرکدوم مشخص بشه.

انواع تهدید:
Virus : بدافزارهایی که میان میچسبن به برنامه های دیگه تا یه کاری رو انجام بدن.هکرها با روش های مختلف آنتی ویروس رو bypass میکنن. ویروس ها نیاز دارن تا اجرا بشن.وجود آنتی ویروس جلوی آلوده شدن به همه ویروس هارو نمگیره.

Worm : شبیه به ویروسه و نیاز به اجرا از سمت کاربر نداره و میتونه داخل شبکه پخش بشه

هکرها فایل هارو جایی میزارن که دسترسی بهشون راحت باشه و مردم بهشون نیاز دارن

برای تست برنامه باید یک sandbox داشته باشیم (یک محیط ایزوله) بعد رفتار نرم افزار رو بررسی میکنیم.لاگ هاشو چک میکنیم،لاگ های فایروال رو چک میکنیم.

Key Logger : از اسمش مشخصه میاد لاگ کلید هارو بررسی میکنه و میگیره. خودش یه نوع malware به حساب میاد و یک برنامس. هم میتونن نرم افزاری باشن هم سخت افزاری

Trojan : یک malware و چسبیده میشه به یک فایل دیگه زمانی که اجرا بشه هکر از قربانی میاد دسترسی میگیره مثلا دسترسی shell میگیره.هکر میاد ایپی و پورت خودش رو داخل بد افزار میزاره تا ترافیک رو هدایت کنه سمت خودش

Ransomware : اگر رو سیستم قربانی دسترسی بگیره دیتای داخل سیستم قربانی رو رمز میکنه و کلیدش رو فقط خودش داره.

هنگام حمله مدارک و شواهد نباید از بین بره،شاااید کلیدی که باهاش رمزنگاری شده توی رم باقی مونده باشه

این نوع حمله ها پیشرفتس پس ما حتما باید بکاپ داشته باشیم. اون بکاپ باید کلا جدا باشه.

Spyware : نرم افزارهای جاسوسی

Adware : پیام های تبلیغاتی که میتونه باعث گرفتن دسترسی بشه

Rootkit : مجموعه ابزارهایی که هکر برای گرفتن دسترسی استفاده میکنه

1404/06/07

DLL : برنامه ها برای اجرا به یک سری dll یا Dynamic-Link Library نیاز دارن،اگر این dll ها مورد نیاز توی سیستم شما نباشه هکر میتونه یه جوری اون dll مورد نیاز رو برسونه به سیستم شما تا اجرا بشه ولی اون فایل رو خودش دستکاری کرده.

Sysinternal tools برای شناسایی باگ های مختلف مثل نمایش وضعیت dll ها

Devices : دستگاه ها و تجهیزات شبکه سه لایه کنترلی دارن :

Control plain : تمامی ترافیک هایی که وارد دستگاه میشن یا ازش خارج میشن و توسط cpu پردازش میشن

Data plain : لایه ای که دیتارو اماده میکنه و توسط NIC ارسال میکنه
Management plain : لایه ای که برای کارهای مدیریتی و دسترسی استفاده میشه مثل ssh

امنیت توی تمامی لایه ها باید انجام بشه

Route Injection یعنی تغییر مسیر ترافیک شبکه

1404/06/10

به روزرسانی مهمه هم توی سیستم عامل هم تجهیزات
Nessus نرم افزاریه واسه شناسایی باگ های امنیتی

Unauthorized Access : سطح دسترسی ها باید کامل مشخص باشه

System Failure : در دسترس بودن سیستم خیلی مهمه و هکرها از این برای تحت تاثیر قرار دادن سیستم استفاده میکنه

BotNet : شبکه ای که هکر میاد با گرفتن دسترسی از کاربرای زیادی واسه خودش میسازه و از اون کاربرها واسه حملاتش استفاده میکنه.

به سه دسته میشه تهدیدات رو کنترل کرد:

1. Physical : حفاظت فیزیکی باید رعایت بشه، کابل ها نباید از هرجا رد بشه،دسترسی فیزیکی به تجهیزات دسترسی رو به داخل شبکه ممکن میکنه،داشتن نیروی حراستی که بدونه باید به چه موضوعاتی دقت کنه مهمه
2. Technical : یک سری از فرایند ها باید پیاده سازی بشن مثلا داشتن ACL، رمزنگاری داده های مهم ، و جلوگیری از دسترسی های غیر مجاز
3. Administrative : یک سری مقررات و سیاست ها باید مشخص بشه و پیاده سازی بشه، استانداردهای ISMS و ISO 27001 شامل این دسته میشن.

دوره CSCU برای اموزش مناسب همه افراد.

روش های جلوگیری از تهدیدات:

1. بالا بردن دانش افراد از طریق اموزش مداوم
2. دسترسی ها نباید راحت باشه و باید حتما متدهای Authentication وجود داشته باشه.
3. Data Removal : مطمئن باشیم چیزی که پاک شده قابل بازیابی نیست.

1404/06/11

شاخه امنیت دو دسته میشه :

1. Offensive : شامل مهارت ها برای نفوذ میشه
2. Deffensive : شامل مهارت ها برای مقابله با نفوذ میشه

اگر مثل یک هکر فکر نکنی نمیتونی جلوی هکر رو بگیری

Network Operation Center : NOC

Security Operation Center : SOC -> ترافیک هارو از نظر امنیتی رصد میکنن

Image گرفتن از os,memory,disk با ابزارهایی مثل FTK Image در زمان اتک مهمه.

White hat : هکرهایی که برای افزایش امنیت تست نفوذ (pentest) انجام میدن.توی قرارداد تمامی مواردی که باید انجام بشه باید نوشته بشه

Gray hat : هکرهایی که میان یه تست نفوذ دیگه انجام میدن تا مشخص بشه علاوه بر باگ هایی که کلاه سفیدها پیدا کردن باگ هایی پیدا میکنن یا نه. دانش این افراد باید بالاتر از کلاه سفید ها باشه

Black hat : معمولا دانش بالاتری نسبت به دو دسته اول دارن که هم میتونن خطرناک باشن هم میتونن کمک کنن به سازمان ها

انواع pentest :
white box , gray box , black box

Ellite : هکرهای نخبه که اسیب پذیری هارو پیدا میکنن و برای نفوذ استفاده میکنن
Hacktivist : ترکیب دو کلمه Hack و Activist که هدفشون افشای اطلاعات یک دولت و کشور