

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 میگویند Clear Text

به اطلاعات رمز شده Cipher میگویند

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 میذاره 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 میگویند) 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.

3. Availability : 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



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

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

3. Accounting : 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 متفاوت. 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 نمیگیره.

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 برنامهس. 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.

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، شاید 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

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

