ال Security Controls بنقول عليها ال Safe Guards يعني اجراءات حماية الاصول ويعني تحقيق ال CIA عن طريق الضوابط والطرق الامنية سواء كانت مادية او فنية او ادارية عن طريق تلات ضوابط ال

Operational Controls

Technical Controls (Logical Controls)

Managerial Controls (Administrative control)

ال Operational Controls يعني حماية الابواب وال DC والغرف المهمة عن طريق الاشخاص ال هما الحراس بس ميكونش حاجة متضمنة نظام يعني لو كاميرات وبصمة وكدة يبقي دي Physical controls

ال Logical Controls يعني التحكمات الامنة ال بعملها فالنظام واجهزة ال شبكة عامة او اعدادات ال firewall وزي ال proximity card ال هو بعرف انك ليك صلاحية الوصول للغرفة دي مثلا وغيرك لا

ال Managerial Controls بتعرفني مين الاشخاص ال مسؤلين عن ادارة المخاطر عندنا يعني الراجل الفلاني والعلاني هما المسؤلين لو عايزين نعمل تحديث للامان يعني ال تحكم فسلوكيات ال موظفين سواء مع بعض او مع ال شركات الخارجية والمنافسة يعني ممكن اقول للموظف انت مينفعش تتكلم مع ال موظف بتاع ال شركة دي فحاجة للامان وساعات كمان مش بخليه يتكلم مع ال موظف ال فقسم تاني ودي بتتحط فال procedures , policies بتاع ال شركة

اقدر اصنف بردو ال Security Controls علي حسب ال هدف بتاعي يعني مثلا

Preventive controls

Detective controls

Corrective controls

ال Preventive يعني انا عايز اجهزة فالشبكة عندي تشتغل وتمنع الاختراق قبل م يحصل زي ال IPS مثلا او نعمل ACL

ال Detective هي نفس الفكرة بس مش هتمنع هي هتدي تنبيه بس وهتكشفهولي زي ال IDS

ال Corrective دي تحكمات بتحصل بعد الاختراق وتقدر تقول بتحذف او تقلل الاختراق زي ال buck up مثلا او ال Patch system ال هو النظام ال بنحتاجة لما نيجي ننزل تحديثات للاجهزة عشان اقفل ال ثغرات

عندي بردو تلاتة Controls تانين اسمهم

Physical controls

Deterrent controls

Compensating controls

ال Physical يعني اني احمي المكان بتاعي ب حراس وبوابات معينة تفتش ال معادن وكاميرات والاقفال

ال Deterrent يعني التنبيهات الامنية يعني تلاقي ونتا فمكان يقولك المكان مراقب بالكاميرات او يقولك ال غرفة دي لناس معينة بس

ال Compensating يعني ال Control ال بيصحح او بيعوض الخطئ ال حصل ايا كان ال خطا ده بوابة عطلت مني او كاميرا باظت فمكان معين او حارس تعب فجاة او ال بصمة باظت وهكذا

عندي حاجة اسمها ال Frameworks ودي حاجة جاهزة بتوصفلي اي هي القوانين والاجراءات ال حنا بنطبقها عشان نحقق الامان زي منظمة ال ISO , IEEE , NIST واشهرهم ال ISO ودول مطلعين Standard رقم 27001 واختصاره K27 وده بينص علي كل الاجراءات ال ليها علاقة بالامان فمنظمتك وفي ناس بياخدو شهادات من ال ISO ال هما مديرين امن المعلومات وفي Standard تاني رقم K31 وده بينص ع ال ERM , CSA

ERM : Enterprise Risk Management

CSA : Cloud Security Alliance

1,2S**********

لازم كل يوم اعمل Risk Analysis وارفع تقرير للشركة بيه عشان اعرف الامان عندي واصل لفين واي هي النقط ال ضعيفة ال عندي ال الهاكر ممكن يستغلها ويخشلي

عندي المخاطر مكونة من حاجتين

Risk = Impact * Likelihood

ال Likelihood يعني احتمالية ال حدوث

يعني انت عليك انك تصحي كل يوم الصبح تدعبس وتشوف ال ثغرات ولو لقينا ندرس ال Impact بتاع ال ثغرة لو حد استغلها وممكن تحصل بنسبة كام

ال Vulnerability يعني نقاط الضعف ال موجودة ف ال نظام بتاعي زي مثلا اني انزل برنامج عندي او احط اي قطعه هارد وير ومعملتش اعدادات سليمة او تاخير تخديث ال ويندوز بتاعي او ال برامج ال عليه او تحديث ال برامج وال ويندوز من غير معملها اختبار الاول هل شغالة بكفاءة ولا لا او ممكن استعمال بروتوكولات غير مشفرة او ضعيفة ال تشفير او شبكة غير مؤمنة او مصممة بشكل غير صحيح او مجبتش اجهزة فايروول او IPS , IDS او باسورد سهل تخمينه

عندي ال Threat يعني ال تهديدات بكل انواعها سواء ان ممكن شخص يوصل لمعلوماتنا ال سرية عن طريق ال Vulnerability او زي اسمنا قرب ينزل فالارض بسبب شركة تاني ظهرت او فيرس هاجم الاجهزة بتاعتي اويكون ال موقع بتاعي Denial of service يعني خارج الخدمة بسبب ان في هاكر بيحاول يخترق الموقع وال راجل ال بيعمل ال تهديد بنسميه Threat actor او Threat agent والطريقة ال تم عمل بيها ال تهديد اسمها ال attack vector ال هي يعني الاداة والهاكر يبيكون من برا ال شبكة ي من جوا ال من برا اسمه malicious external actor يعني عايز يخرب اجهزتي عن طريق برامج خبيثة او بيعمل هندسة اجتماعية وممكن يعمل الاختراق يعن بعد ي اما بشكل local ال هو قرب من ال شركة وحاول يتصل بالوايفاي بتاعنا

وبعوز بردو اعرف ال intent يعني هو عايز يحقق اي فالهجوم ده هل يسرق ال بيانات ولا يعدل وكمان بعوز اعرف ال Motivation او ال سبب ال خلاه يعمل الاختراق ده هل طمع ولا انتقام ولا استعراض مهرات ولا فضول

عندي حاجة اسمها ال

APT : Advanced persistent threat

يعني الهجمات ال مستمرة ال متقدمة يعني ده نوع من الاختراق بيتم عن طريق فرق من الهاكرز بيتم تعينهم من ال دول يعني كل دولة ليها فرقة هاكر بتجمع معلومات عن دول تانية وممكن الاختراق ده يقعد بالشهور والسنين ومحدش بيكتشفو وبقدر اشوف ده عن طريق مواقع بتعرضلي الاختراقات ال بتتم دلوقتي بين ال دول زي لو كتبت ف السيرش cyber threat maps هلاقي مواقع كتير بتظهرلي ده

وفي موقع تاني اسمه the hacker news ده بيجبلك كل الاختراقات ال تمت انهاردة واي اخر ال فيروسات وبتعمل اي

من كتر الاختراقات ال بتحصل وال فيروسات ال بتطلع بقي في قسم فالشركات اسمه Threat research او ال Threat intelilgence بيجبلي اخر الاختراقات واامن نفسي منها ازاي وتم ازاي وكدة في بردو مفهوم تاني اسمه ال Honey net او ال شبكة ال وهمية وهي شبكة بحطها عندي فالشبكة واخلي فيها ثغرات واوصل بيها اجهزة فيه ثغرات عشان لما ال هاكر يخترقها اقفشه او اخليه يبعد عني يعني نفس المصيدة والمفروض بردو بدور علي المعلومات ال تم تسريبها دي ف ال دارك ويب

ال Dark web يعني المواقع والمحتوي وال خدمات ال محجوبة عن الانترنت ال هي مماواقع بيع الاسلحة واستاجار ال قتلة والحاجات الغير قانونية بشكل عام

وال Dark net هي ال شبكة ال عن طريقها هخش ال دارك ويب ال هي شبكة ال TOR

عشاان اشوف اخر تحديث للفيروسات في قدامي طريقين ي اما مواقع بدفعلها فلوس عشان اعرف التهديدات دي ي اما مواقع عامة زي ال شوفناها فوق او مواقع ميكروسوفت او سيسكو وهما بيقولولي اعمل كذة واعمل تحديث ومتحملش ال برنامج ال فلاني وفي مواقع كتير بتشوف لو الملف ده هاك ولا لا وهسبلك لينكاتهم تحت

زي موقع ميكروسوفت

http://microsoft.com/security/blog/microsoft-security-intelligence

في موقع عام ومفتوح زي

nationalisacs.org

او زي مواقع لازم تدفعلها عشان تعرفك بالتحديثات دي زي

IBM X-Force Exchange (exchange.xforce.ibmcloud.com(

FireEye (fireeye.com/solutions/cyber-threat-intelligence/threat-intelligence-

subscriptions.html(

Recorded Future (recordedfuture.com/solutions/threat-intelligence-feeds(

او مواقع مجانية بنستخدمهم عشان نتعرف ع ال تهديدات زي موقع VirusTotal ده بيعمل فحص ع الملف او اللينك ال تدهوله ويقولك هو ضار ولا كويس عن طريق 61 انتي فيرس

AT&T Security, previously Alien Vault Open Threat Exchange (OTX) (otx.alienvault.com)

Malware Information Sharing Project (MISP) (misp-project.org/feeds)

Spamhaus (spamhaus.org/organization)

VirusTotal (virustotal.com)

3s**********

عملية ال scan ال بنعملها ع ال شبكة اسمها

Network Reconnaissance , Network Discovery , Information Gathering

وال مفروض اني بعرف بالطريقة دي ال خريطة ال هههجم بيها لان ال هجوم بيجيلي عن طريق شبكة او نظام او برنامج فيه ثغرة

كمان ال هكر ممكن يعمل Topology Discovery او بنسميها بردو Foot printing يعني بيشوف الاجهزة ال عندي وال IP بتاعها ال وال راوترات ال بين ال شبكة عشان يحاول يلاقي ثغرة يخش بيها وال Foot printing ممكن اعمله ب اوامر جوا نظام ال ويندوز والماك واللينكس او ممكن عن طريق برامج بثبتها زي امر

ipconfig » windows

ifconfig » llinux

ping

arp

والامر arp مهم عشان بيجبلي الاجهزة ال فالشبكة ال اتواصلت معاها وال ماكات وال ايبيهات وطلاما عرفت ال ايبيهات سهل بقي ابعتله رسايل

في اوامر تانية بتخليني اعرف ال routing configuration او اعمل اختبار للاتصال زي ال ويندوز هكتب امر

route print

ف هيجبلي ال routing table ال جوا الجهاز بتاعي

وجوا لينكس اسمه route

في بردو امر

tracert » windows

traceroute » linux

ده بيتعقب ال رسالة هي مشيت من انهي طريق لحد متروح للمستقبل واللينكس اسرع بتكير

في الامر ده اكثر تفصيلا بيجبلك ال بنج ال وصل وال وقع وعدي من انهي طريق بس مش مشهور اوي pathping

وعندي من اشهر الادوات ال بتعمل فحص للشبكة ال NMAP وبديها ال IP بتاع ال شبكة او الجهاز ال عايز اعمل فحص عليه وبتعمل بنج وبتبعت باكت TCP ACK علي بورتات ال تصفح 443 و 80 ولما عملت ال Scan جابلي الاجهزة ال شغالة فشبكتي وال بورتات ال مفتوحة فيها

وبيبعت رسالة من نوع

TCP SYN (-sS)

UDP scans (-sU)

port range (-p)

عشان يعرف اي الخدمات ال بتتم فالشبكة دي ولما تعرف اي الخدمات تبحث بقي عن احدث ال ثغرات ال فالخدمة دي ويقولك هي كذة كذة وتبدا بقي تخش ع الشبكة من خلالها وبيحبلي عمل كل ده ف كام ثانية وممكن تشتغل بطريقة تانية عادي عن طريق بورتات تانية

ممكن بردو اعمل حاجة اسمها ال Fingerprint عشان اعرف ال OS ال شغال ده اي

وممكن اعمل banner grabbing يعني الجهاز ال انا بتواصل معاه بيستخدم انهي برتوكول وانهي اصدار وانهي بورت وفي بردو حروف كتير بكتبها عشان اجمع كل المعلوماات ال عايزها عن ال شبكة موجودة فشيت فالمحاضرة ال 4

في عندي بردو امر فاللينكس والويندوز بيخليني اعرف انا فاتح اتصالات مع مين وهوnetstat

وفي معاه بردو بعض ال حروف او بنسميها ال فلترز

في بردو امر

dig » linux

nslookup »windows

الاداتين دول بيجبولي ال IP بتاع الاسم ال بكتبه ليها يعني تقدر تقول عليها عاملة زي ال DNS سيرفر كدة وفي ادوات كتير او ف اللينكس نسخة ال kali وال Parrot وفي فالويندوز نسخة ال fireeye دي مخصصة للاختراق

في فاللينكس اداة اسمها Harvester ودي اداة تجميع معلومات وفي اداة اسمها dnsnum ودي بتجبلي معلومات اكتر عن ال DNS وفي اداة scanless و curl دول شبه ال NMAP كدة وفي اداة nessus ودي من اشهر الادوات ال بتخليني اشوف اي ال ثغرات ال عندي وازاي اصلحها

4s**********

مقدمة عن ازاي استخدم ال Cloud بتاع ال قورص

5s**********