التاريخ: / /

الموضوع:

Summary :-

* Cryptography :- تشفير البيانات بحيث تكون غير مقروءة عن طريق Specific Algorithms

* the importance of Programming in cybersecurity: it helps me to write scripts to do specific tasks for saving time and effort.

* info sec :- حماية المعلومات بشكل عام سواء بشكل Physically أو electronically

* cybersec :- حماية المعلومات الإلكترونية

* linux uses (CLI)(terminal)(Command line interface)
* Hacker definition is meant the person who try to find the basics of every thing.

* White Hacker (ethical hacker) vs BlackHacker (cracker)
* user vs malicious user (blackHacker but doesn't have the skills).
* Local attack (inside your network)
  Remote attack (outside your network)

* Vulnerability :- تغرة في الـ system بتؤدي لخلل فيه -
* EXPloit :- طريقة استغلال الـ Vulnerability -
* Session :- المدة اللي أنا بتحكم فيها في الجهاز بدون علم المؤسسة -
* Payload - الحاجة المضرة اللي عايزه أنفذها على الجهاز
* ZeroDay :- نوع من الثغرات ويعتبر أخطرها ودي بتكون تغرة أول مرة يتم اكتشافها.
* Security Through obsecurity : - يعمل Pentest على Techniques مش عارفاها
* Authentication :- - المصادقة والتوافق والربط بين الـ username والـ Password مثلاً
* AuthoriZation :- - مصادقة لصلاحيات الـ user بحيث إن كل user له صلاحيات معينة وميقدرش يوصل لصلاحيات وبيانات أي user تاني.
* script :- - بتعامل معاه من خلال (CLI) وده اللي بنشوفه في linux أسرع وأقوى
* Normal Program :- - GUI زي برامج الـ office
* Darkweb vs Deepweb vs Normalweb

له جزء كبير من الإنترنت — له معظم الإنترنت

ده اللي بنحصل منه على نتائج البحث وهي 16% فقط من النتائج الفعلية

التاريخ: / /

الموضوع:

* root :- المتحكم الرئيسي في الجهاز وهو اللي ليه كل الصلاحيات الكاملة على الجهاز (linux)
* administrator :- المتحكم الرئيسي في الجهاز (windows)
* user :- ليه صلاحيات معينة بس على سبيل المثال مينفعش يعدل على ملفات الـ System.

* Permissions كل Folder أو File في الجهاز ليه
* Privilege Escalation :- تصعيد الصلاحيات (عايزه أعلى من صلاحيات الـ user)

* Eavesdropping :- لقفة (اعتراض) الداتا اللي بتتبعت بين جهازين والتعديل فيها و~~استغلال~~ ده بيسمى MITM
↳ Man In The Middle attack

* Dos attack :- حجب الخدمة بتاعت server الـ عن المستخدمين بحيث إني أشغل الـ server عن طريق إرسال requests كتير (Denial of service)
* DDos attack :- حجب الخدمة عن المستخدمين عن طريق إنه أجهزة كتير بتعمل Dos attacks على الـ server.

* server vs Port vs service vs Protocol

كل Domain فيه مجموعة servers والـ Domain ده بيوجه الـ server المناسب، وكل server فيه مجموعة Ports وكل Port بيقدم Service

* Protocol :- هي طريقة موحدة للتواصل بين جهازين

unsecure ← → secure (use cryptography

* (HTTP) and (HTTPs) Protocols

ودول مخصصين للناس اللي عايزة خدمة من ال Web server

* Shellcode :- - ده جزء من ال script اللي من خلاله بعمل ال exploit

* Encoding :- - بغير شكل الداتا عن طريقة زخرفتها ولما أعرف نوع الزخرفة دي بقدر أعمل العملية العكسية (Decoding) زي تقنية Base 64

* Encryption :- - لازم الشخص يعرف ال Key بتاع الحل

← زي Rot 13 ← بحرك كل حرف 13 حرف

الناتج بيكون مقروء

* Hashing :- - دي عملية غير عكسية unreversable

- يعني مينفعش أرجع الداتا اللي محولها Hashing لأصلها

- بتتم عن طريقة إني أدخل داتا لـ Algorithm معينة وفي الآخر وتطلع Hash وهو ناتج غير مقروء.

- فيه مجموعة Techniques عشان أعرف قيمة ال Hash

① بدور في DB كبيرة جدًا وأقارن ال Hash بتاعي بال Hashes اللي موجودة في ال DB وأطلع ال Plain Text المقابل لل Hash ده لو كان موجود في ال DB.

② من خلال Tool بدخل لها Wordlist وبجيب لكل Plain Text ال Hash بتاعه وأقارنه بال Hash بتاعي لغاية ما يتطابق مع واحد فيهم.

الموضوع : التاريخ : / /

← نوع الـ Algorithm اللي هعمل بيه Hashing بيفرق في الـ length بتاع الـ Hash وكل ما الـ length كبير بصعب فك.

examples for Hashing algorithms: (SHA1 - SHA2 - LM - MD5 - NTLM)

دول Algorithms بتتم استخدامهم في الـ Windows لحفظ الـ Passwords

← أي تعديل صغير في الـ data حتى لو كان lowerCase لـ upperCase هيغير في الـ Hashing.

* Hashing Techniques: عمليات هنضفها على الـ Hashing عشان تزود من صعوبته

① Salt (static - Dynamic)

- بزود إضافات على الداتا بحيث تغير الهاشنج وبيصعب على الـ attacker انه يوصل للـ PlainText حتى لو معاه الـ hashing الصحيح.

static → لو هضيف قيمة ثابتة لكل المستخدمين

Dynamic → لو هضيف لكل مستخدم قيمة مختلفة عن التانية

② Pepper :- بضيف إضافات في آخر الـ Password

→ MITM نفس فكرة

* Sniffing (wireshark - TCP Dump)

أدوات بستخدمها عشان أعرض الـ Traffic جوه الشبكة

من الـ sniffing ⟸ بحاول أشوف الداتا اللي ماشية في النتورك عشان لو حد بعت حاجة في الـ Plain Text فأنا آخدها جاهزة بدل م أفك التشفير لداتا مشفرة

(VPN) ⟸ Virtual Private network بقدر من خلالها أخفي الداتا اللي في النتورك ما بين الجهازين عشان أمنع الـ sniffing

⟸ Tunnel ⟸ شبه الـ VPN بس بيكون خاص بجهازين فقط.

➡ Malwares (: Trojan - Worm - Virus - Scareware - Rootkit - Backdoor - Botnet - Ransomeware

⟹ Trojan: - بيان في الأول إنه تطبيق للتسلية ثبت على الجهاز بينا يعمل malicious activities.

⟹ Worm - بينتشر في كل الأجهزة المتصلة بالجهاز المصاب على نفس الشبكة.

⟹ Virus ⟹ ده malware بينتشر في الجهاز المصاب فقط

⟹ Scareware: - malware عرضه التخويف عشان تضغط على link أو attachment معين

⟹ Backdoor: - زي الـ Remote attack بس بعمل لنفسه Backdoor بحيث يخرج من الـ session ويدخل تاني في أي وقت.

⟹ Botnet - زي الـ Backdoor بس على مجموعة أجهزة

⟹ Ransomeware: - بيعملوا Encryption على الداتا ويطلبوا فدية عشان يعطوا الـ Key

* RootKit : Kernel هو الأصعب في الإكتشاف لإنه بيصيب الـ

* ByPass / EVasion :- إنا بعمل attacker أقدر أعدي وأتخطى الـ antivirus أو الـ Security solution.

* Active Directory :- الجهاز اللي هعمل عليه حاجة عايزاها تتم على كل الأجهزة اللي في نفس السيرفر (زي Software Update)

* Domain Controller : هو المتحكم في الـ ACtive Directory

/ / التاريخ:

الموضوع:

10 Terms about cybersecurity

1] Identity And access Management (IAM)

A security framework That Controls who Can access certain systems and data within an organization. it ensures That only authorized users have the necessary Permissions.

2] Route force attack :-

acyberattack That systematically tries all Possible Password Combinations until The Correct one is found. Hackers use automative tools That Can Generate millions of Guesses Per second.

3] EndPoint security :-

security measures designed to Protect devices Connected to a network (such as Computers, mobile Phones, and servers) Prom Cyber Threats .it includes antivirus software, firewalls and intrusion detection systems (IDS/IPS).

4] Credential stuffing :-

A Cyberattack where hackers use stolen username-Password Pairs from Previous breaches to try and access multiple accounts, exploiting People who reuse Passwords

/ / التاريخ:

الموضوع:

10 Terms about cybersecurity

1] Identity And access Management (IAM)

A security framework That Controls who Can access certain systems and data within an organization. it ensures That only authorized users have the necessary Permissions.

2] Route force attack :-

acyberattack That systematically tries all Possible Password Combinations until The Correct one is found. Hackers use automative tools That Can Generate millions of Guesses Per second.

3] EndPoint security :-

security measures designed to Protect devices Connected to a network (such as Computers, mobile Phones, and servers) Prom Cyber Threats .it includes antivirus software, firewalls and intrusion detection systems (IDS/IPS).

4] Credential stuffing :-

A Cyberattack where hackers use stolen username-Password Pairs from Previous breaches to try and access multiple accounts, exploiting People who reuse Passwords

الموضوع :

التاريخ : / /

5 **Zero Trust Architecture** :-

A security model That assumes no user or device should be Trusted by default, requiring strict authentication and continuous monitoring for access.

6 **Cloud security** :- A set of Policies and technologies designed to Protect data, apps, and infrastructure in cloud computing environments.

7 intrusion Detection system (IDS) & intrusion Prevention system (IPS).

IDS: A system That monitors network traffic for signs of cyber attacks or suspicious activity.

IPS: A system That actively blocks cyberattacks based on detected threats

8 **Exploit kit** :- A set of automated tools used by cybercriminals to exploit software vulnerabilities and launch attacks.

9 **Air GAP security** :- the Practice of Physically isolating a system or network from external connections such as The internet or other networks to Prevent cyber Threats

الموضوع :

التاريخ : / /

10 **Steganography** :- is the practice of hiding data within other files, such as images, videos or audio files, in a way that prevents detection, unlike encryption, which obscures the content of the data, but steganography hides the data itself, it can be used for secret communication, protecting intellectual property, or even by hackers to avoid detection.