ورشة عمل

مفاهيم الأمن السيبراني واختبار الإختراق

إعداد وتقديم

يزيد بن سعد

شكر خاص لمنصة شوف المملكة
لتنظيمها ورشة العمل

مقدمة

تخسر المنظمات ملايين الدولارات نتيجة لخرق أمني واحد وفقًا لدراسة حديثة ستكلف تهديدات الأمن السيبراني الاقتصاد العالمي أكثر من تريليون دولار بين عامي 2017 و 2021

في عام 2019 ، واجهت ثلثا الشركات التي شملها الاستطلاع تهديدًا للأمن السيبراني ، وفقًا للتقرير نفسه. وقد أدى ذلك إلى زيادة الطلب على متخصصي الأمن السيبراني في الولايات المتحدة ، حيث اقترح (NIST 2018) توظيف أكثر من 300000 موظف جديد ، ارتفاعًا من الإجمالي الحالي الذي يزيد عن 700000 شخص.

ماهو الامن السيبراني؟

الأمن السيبراني | Cybersecurity حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من عتاد وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات، والأمن الإلكتروني، والأمن الرقمي ونحو ذلك.

مصطلحات مهمة

أصل | Asset

الموارد الملموسة، أو غير الملموسة، ذات قيمة للجهة. بما في ذلك الموظفين، والتقنيات، والمرافق، وبراءات الاختراع، والبرمجيات والخدمات، والمعلومات والخصائص (مثل: سمعة الجهة وهويتها وقدراتها المعرفية أو المهنية).

التشفير | Cryptography

القواعد التي تشتمل على مبادئ ووسائل وطرق تخزين ونقل البيانات أو المعلومات في شكل معين وذلك من أجل إخفاء محتواها الدلالي، ومنع الاستخدام غير المصرح به والتعديل غير المكتشف، بحيث لا يمكن للأشخاص غير المعنيين قراءتها ومعالجتها.

البرمجيات الضارة | Malware |

برنامج يصيب الأنظمة بطريقة خفية (في الغالب) بغاية انتهاك سرية أو سلامة أو توافر بيانات الضحية أو تطبيقاته أو نظم التشغيل الخاصة به.

ثغرة | Vulnerability |

أي نوع من نقاط الضعف في نظام الحاسب، أو برامجه أو تطبيقاته، أو في مجموعة من الإجراءات، مما يجعل الأمن السيبراني عرضة للتهديد.

CAI

What is CIA Triad?

Confidentiality | السرية

خاصية عدم الإفصاح عن المعلومات المستخدم أو إجراء أو نظام غير مصرح له إلا في حال وجود تصريح لهم للوصول إليها .

Integrity | السلامة

الحماية ضد تعديل المعلومات أو تخريبها بشكل غير مصرح به، كما تشمل ضمان عدم الإنكار للمعلومات والأصالة.

Availability التوافرا

ضمان إمكانية الوصول والاستخدام عند الطلب، من مستخدم أو إجراء أو نظام مصرح له بشكل يعتمد عليه.

SECURITY & PRIVACY

Security

الأمان: يشير إلى كيفية حماية معلوماتك الشخصية.

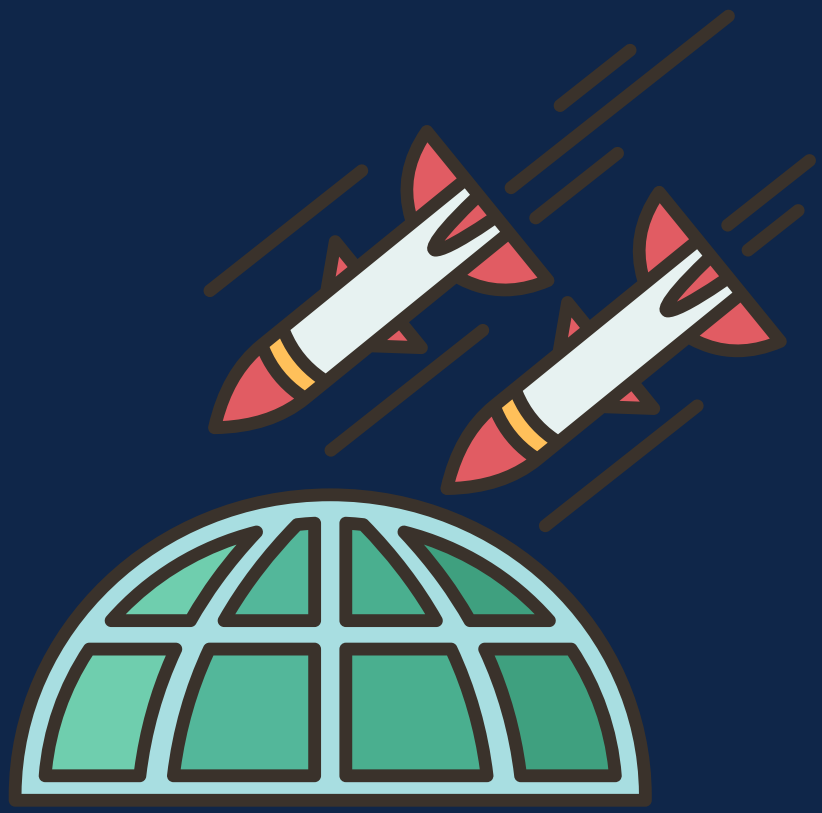
Privacy

الخصوصية: تتعلق بأي حقوق لديك للتحكم في معلوماتك الشخصية وكيفية استخدامها.

الهجوم سيبراني | Cyber Attack |

استغلال غير مشروع الأنظمة الحاسب والشبكات، والمنظمات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية؛ بهدف إحداث أضرار. وتشمل أي نوع من الأنشطة الخبيثة التي تحاول الوصول غير المشروع أو تعطيل، أو منع، أو تدمير موارد النظم المعلوماتية، أو المعلومات نفسها.

-تشمل مناطق الهجمات الرئيسية ما يلي:



- خوادم البيانات
- خوادم التطبيقات
- خوادم التخزين
- معلومات مالية
- أنظمة التشغيل
- شبكات الحاسب

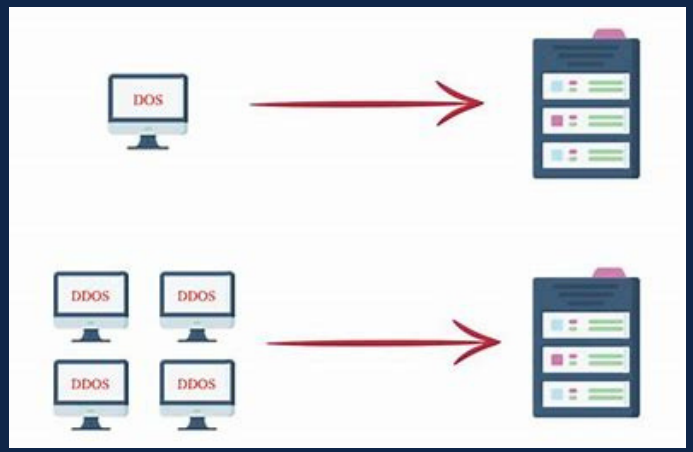
الأنواع والأساليب المستخدمة للهجوم السيبراني

Spamming

البريد العشوائي في مجال تكنولوجيا المعلومات هو اسم إرسال رسائل البريد العشوائي والرسائل إلى المستخدمين في بالجملة دون الحصول على موافقة من المستخدمين

هجمات حجب الخدمة الموزعة | Denail of Service Attack

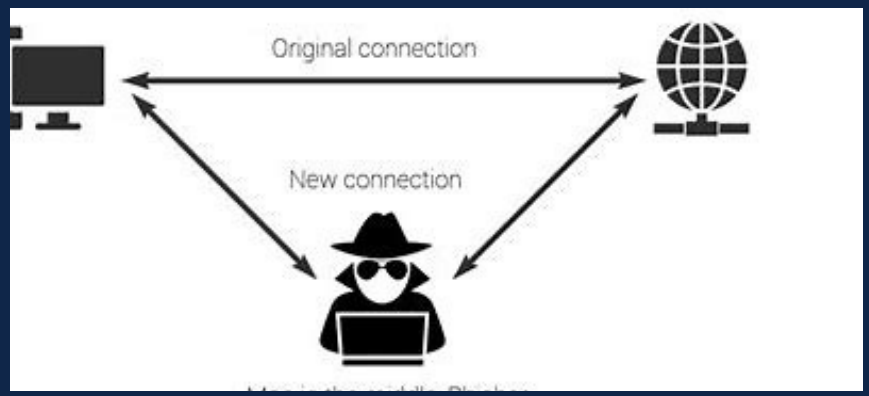
هي محاولة لتعطيل النظام، وجعل خدماته غير متوافرة؛ عن طريق إرسال طلبات كثيرة من أكثر من مصدر في الوقت نفسه.



الأنواع والأساليب المستخدمة للهجوم السيبراني

Man-in-the-Middle

في الهجوم الإلكتروني "Man-in-the-Middle" أو الهجوم الإلكتروني MITM ، يعترض المتسلل الاتصال العادي بين المستخدم وخادم الويب دون أي معرفة بكل من المستخدم او الخادم



(SQL) injection

يعد حقن لغة الاستعلام الهيكلية (SQL) نوعًا من الممارسات الضارة التي يتم إجراؤها سرقة البيانات القيمة من خادم قاعدة البيانات

رسائل التصيد الإلكتروني | Phishing Email |

التنكر على هيئة جهة جديرة بالثقة عن طريق رسائل بريد إلكترونية للحصول على معلومات حساسة، مثل أسماء المستخدمين، وكلمات المرور، أو تفاصيل بطاقة الائتمان، وذلك لأسباب ونوايا ضارة وخبيثة.

Malware

البرمجيات الضارة | Malware |

برنامج يصيب الأنظمة بطريقة خفية (في الغالب) بغاية انتهاك سرية أو سلامة أو توافر بيانات الضحية أو تطبيقاته أو نظم التشغيل الخاصة به.

01

virus

02

worms

03

Trojan horse

04

Rootkit

Malware

- **يستخدم المتسللون البرامج الضارة لأي عدد من الأسباب مثل استخراج البيانات الشخصية المعلومات أو كلمات المرور أو سرقة الأموال أو منع أصحابها من الوصول إلى أجهزتهم.**

- **الفيروسات virus**

فيروس الكمبيوتر هو برنامج كمبيوتر ضار ، تم تصميمه لتغيير وظائف الكمبيوتر ، وإبطاء أداء الكمبيوتر ، وإتلاف الملفات القيمة الموجودة على محرك الكمبيوتر

- **الديدانworms**

دودة الكمبيوتر هي أنواع برامج البرامج الضارة التي تتكاثر على أجهزة الكمبيوتر لاستهلاك الأجزاء الرئيسية من موارد الكمبيوتر مثل القرص الصلب والذاكرة.

- **حصان طروادةTrojan horse**

هو نوع من البرامج الضارة التي تتظاهر بأنها شيء مفيد أو ممتع بينما تسبب في الواقع ضررًا أو سرقة البيانات. غالبًا ما تقوم أحصنة طروادة بتنزيل برامج ضارة أخرى بصمت (مثل برامج التجسس والبرامج الإعلانية وبرامج الفدية) على جهاز مصاب أيضًا.

- **Rootkit**

هو نوع من البرامج الضارة التي تحصل على امتيازات على مستوى المسؤول على نظام تشغيل الكمبيوتر دون إظهار وجودها على الكمبيوتر.

Network security

شبكة الكمبيوتر
شبكة الكمبيوتر عبارة عن نظام موزع يتكون من أجهزة كمبيوتر وأجهزة أخرى مقترنة مع بعضها البعض.

الأمان هو عملية مستمرة لحماية كائن من الوصول غير المصرح به. إنها حالة الوجود أو الشعور بالحماية من الأذى. قد يكون هذا الكائن في تلك الحالة شخصًا أو مؤسسة مثل شركة أو ممتلكات مثل نظام كمبيوتر أو ملف

يمكن ضمان حالة الأمان هذه إذا كانت آليات الحماية الأربعة التالية موجودة: الردع والوقاية والكشف والاستجابة

Network security

شبكات الكمبيوتر عبارة عن شبكات موزعة من أجهزة الكمبيوتر المتصلة ، مما يعني أنها تشترك في الكثير من الموارد عندما نتحدث عن أمان شبكة الكمبيوتر ، فقد تغير نموذج التركيز لدينا الآن. لم يعد جهاز كمبيوتر واحد بل شبكة. لذا فإن أمن شبكات الكمبيوتر هو دراسة أوسع لأمن الكمبيوتر. لا يزال فرعًا من علوم الكمبيوتر ، ولكنه أوسع بكثير من أمن الكمبيوتر. يركز على إنشاء بيئة تكون فيها شبكة الكمبيوتر ، بما في ذلك كل ما لديها امن لموارد جميع البيانات الموجودة فيه سواء في التخزين أو أثناء النقل أو المستخدمون أمنون .

بناءً على التعريف أعلاه ، إذا كان هذا المورد محميًا من الوصول غير المصرح به داخليًا وخارجيًا. الموارد ، المادية أو غير المادية ، نحن نحمي كائنات النظام إما ملموسة أو غير ملموسة. في نموذج شبكة الكمبيوتر ، الكائنات الملموسة هي موارد الأجهزة في النظام ، والكائن غير الملموس هو المعلومات والبيانات في النظام ، سواء في مرحلة انتقالية أو ثابتة في التخزين

Network security

المعدات Hardware

- تشمل حماية موارد الأجهزة : كائنات المستخدم النهائي التي تتضمن مكونات أجهزة واجهة المستخدم مثل جميع مكونات إدخال نظام العميل ، بما في ذلك لوحة المفاتيح والماوس وشاشة اللمس وأقلام الإضاءة وغيرها.
- كائنات الشبكة مثل (**firewalls, hubs, switches, routers**) المعرضة للقراصنة.
- قنوات اتصال الشبكة لمنع المتسللين من اعتراض اتصالات الشبكة

البرمجيات

تشمل حماية موارد البرامج حماية البرامج القائمة على الأجهزة وأنظمة التشغيل وبروتوكولات الخادم والمتصفحات وبرامج التطبيقات والملكية الفكرية المخزنة على أقراص تخزين الشبكة وقواعد البيانات. كما يتضمن حماية برامج العميل مثل المحافظ الاستثمارية أو البيانات المالية أو السجلات العقارية أو الصور أو ملفات الصور والملفات الشخصية الأخرى التي يتم تخزينها

Network security

يتم تحقيق منع الوصول غير المصرح به إلى موارد النظام من خلال عدد من الخدمات التي تشمل التحكم في الوصول ،
والمصادقة ، والسرية ، والسلامة والنزاهة ، التوافر.

- تأتي بروتوكولات الأمان والحلول وأفضل الممارسات التي يمكنها تأمين نموذج عمل شبكة الكمبيوتر في العديد من الأنواع المختلفة وتستخدم تقنيات مختلفة تؤدي الى توحيد بين العديد من الأنظمة الموارد بتقنيات مختلفة داخل النظام وبين الأنظمة.

- يختار مديرو النظام ورؤساء الأمن والخبراء أو يفضلون المعايير ، في حالة عدم وجود معيار واقعي ، تستند إلى الخدمة ،الصناعة أو الحجم أو المهمة.

- يحدد نوع الخدمة التي تقدمها المؤسسة أنواع معايير الأمان المستخدمة. على غرار الخدمة ، طبيعة الصناعة وتحدد المنظمة أيضًا أنواع الخدمات التي يقدمها النظام ، والتي بدورها تحدد نوع المعايير التي يجب اعتمادها. تي

Network security

يجب أن تتكون الخطة الفعالة من ثلاثة مكونات: الوقاية والكشف و التحليل والاستجابة

- الوقاية

من المحتمل أن تكون الوقاية هي أفضل سياسة أمان للنظام ، ولكن فقط إذا عرفنا ما يجب منع الأنظمة منه.

هذه الأساليب الممكنة هي كما يلي:

- سياسة أمنية
- إدارة المخاطر
- أمن المحيط
- التشفير
- تشريع

الكشف

في حالة فشل المنع ، يجب أن تكون الإستراتيجية التالية الأفضل هي الاكتشاف المبكر. يشكل اكتشاف الجرائم الإلكترونية قبل وقوعها نظام مراقبة على مدار 24 ساعة لتنبيه أفراد الأمن عند حدوث شيء غير عادي (شيء ذو نمط غير عادي ، يختلف عن النمط المعتاد لحركة المرور داخل النظام وحوله).

الاستجابة

الاستجابة والاسترادا‌د
سواء تم نشر حلول المنع أو الكشف على النظام أم لا ، في حالة وقوع حادث أمني على النظام ، أو خطة الاسترداد ، على النحو المنصوص عليه في خطة أمنية ، يجب اتباعها

security standards

دعونا نلقي نظرة على الهيئات والمنظمات التي تقف وراء صياغة هذه المعايير وتطويرها والمحافظة عليها. تنقسم هذه الهيئات إلى الفئات التالية:

- المنظمات الدولية مثل فريق هندسة الإنترنت (IETF) ،
- معهد مهندسي الكهرباء والإلكترونيات (IEEE) الدولي
- منظمة (ISO) ،
- والاتصالات الدولية الاتحاد (ITU)

Computer security

ما هو أمن الكمبيوتر؟

أمان الكمبيوتر هو في الأساس حماية أنظمة الكمبيوتر والمعلومات من الأذى والسرقة والاستخدام غير المصرح به. إنها عملية منع واكتشاف الاستخدام غير المصرح به لنظام الكمبيوتر الخاص بك.

يمكن تعريف أمان الكمبيوتر على أنه ضوابط يتم وضعها لتوفير السرية والنزاهة والتوافر لجميع مكونات أنظمة الكمبيوتر.

مكونات نظام الكمبيوتر التي تحتاج إلى الحماية هي:

- الأجهزة ، الجزء المادي من الكمبيوتر
- البرمجيات ، البرمجة التي تقدم خدمات ،مثل نظام التشغيل ومتصفح الإنترنت للمستخدم

Computer security

تلخص إعدادات التصفح الآمن الإعدادات الرئيسية للمتصفح الخاص بك للحفاظ على جهاز الكمبيوتر الخاص بك في مأمن من أي محاولة ضارة لتغيير موارد الكمبيوتر وإعداداته.

- **اضبط إعدادات الخصوصية على مستوى عالٍ.**
- **لا تحفظ كلمات المرور على المتصفحات.**
- **قم بتنشيط إعدادات التصفح الآمن على المتصفح.**
- **يجب إرفاق حركة التصفح مع طلب "عدم التعقب".**
- **تنشيط إعدادات SSL و HTTPS.**
- **يجب رفض جميع النوافذ المنبثقة والمكونات الإضافية والأنشطة الأخرى أو طلب الحصول على إذن من مسؤول الكمبيوتر**
- **يجب أن تكون موارد الكمبيوتر وإعدادات الوصول إلى المحتوى قوية للغاية.**
- **تحقق دائمًا من البرامج الضارة المثبتة على المتصفح أو الكمبيوتر.**

Computer security

برنامج مكافحة الفيروسات

مضاد الفيروسات هو أحد أدوات الأمان الأساسية الموصى بها لكل جهاز كمبيوتر

- Panda Premium Antivirus
- AVG Internet Security
- Microsoft Security Essentials
- McAfee Total Protection
- Comodo Antivirus Software
- Avira Antivirus Pro

اختبار الاختراق

Penetration testing

Penetration testing

اختبار الاختراق

اختبار الاختراق هو محاولة قانونية ومسموح بها لاكتشاف أنظمة الكمبيوتر واختراقها بنجاح بهدف تحسين أمانها. يعد اختبار الاختراق عنصرًا مهمًا في إنشاء أي نظام آمن لأنه يشدد ليس فقط على تشغيل النظام ، ولكن أيضًا على تنفيذه وتصميمه.

أهداف اختبار الاختراق

- يساعد في تقليل المخاطر الأمنية وتحديد ما إذا كانت الإجراءات الأمنية الحالية فعالة أم لا.
- توفير نقطة بداية جيدة: اختبار الاختراق هو خطوة أولى جيدة في فهم الوضع الأمني الحالي للمؤسسة من خلال تحديد العيوب وخروقات الأمان
- تحديد المخاطر الأمنية وترتيبها حسب الأولوية: الهدف الفعلي من اختبار الاختراق هو تحديد المخاطر الأمنية. لا يساعد اختبار الاختراق في فهم المخاطر الأمنية فحسب ، بل يساعد أيضًا في تحديد أولويات مخاوف المخاطر ، فضلاً عن تقييم تأثيرها .
- تحسين أمان نظام الكمبيوتر: يتم إجراء اختبار الاختراق بهدف جعل أنظمة الكمبيوتر مثل جدران الحماية وأجهزة التوجيه والخوادم أكثر أمانًا.
- لتأمين البيانات ، يتم استخدام العديد من الإجراءات الأمنية مثل أنظمة الكشف عن التسلل وجدران الحماية والتشفير.
- لتأمين البيانات ، يتم استخدام العديد من الإجراءات الأمنية مثل أنظمة الكشف عن التسلل وجدران الحماية والتشفير.
- لاختبار مقدار المعرفة الأمنية العامة وكفاءة السياسات الأمنية واتفاقيات المستخدم ، يمكن استخدام تقنيات الهندسة الاجتماعية مثل الحصول على كلمات المرور عبر الهاتف.

Penetration testing

عادة ما يتم تحديد نوع اختبار الاختراق المستخدم من خلال نطاق المشروع واحتياجات المنظمة.

الأنواع الأكثر شيوعًا من اختبارات الاختراق مذكورة أدناه

- اختبار اختراق الصندوق الأسود
- اختبار اختراق الصندوق الأبيض
- اختبار اختراق الصندوق الرمادي
- محاولات الهندسة الاجتماعية
- ارتباطات الفريق الأحمر / الأزرق

Penetration testing

1- جمع المعلومات Information gathering

أول خطوة في عملية اختبار الاختراق حيث أن المعلومات التي يتم جمعها في هذه المرحلة مهمة و قد تكون غير تقنية حيث أنه يمكن أن نتعرف على السيرفرات و معلومات شخصية عمن يملكها لتسهيل العملية .

2- المسح Scanning

تشمل فحص IP’s لمعرفة “ports” المنافذ المفتوحة بالإضافة للتعرف على الثغرات و تقييم نقاط الضعف.

3- الاستغلالExploiting

بعد معرفة المعلومات التي تم الحصول عليها في المرحلتين السابقتين يمكن استغلال المنافذ المفتوحة و الثغرات الأمنية و البدء بالهجوم للتحكم الكامل بالنظام .

4-تثبيت الاختراق Maintaining Access

في الغالب بعد خروجنا من النظام الذي تم اختراقه لن نتمكن من دخوله مرة أخرى إلا بإعادة الخطوات السابقة , و لكن في هذه المرحلة نحاول خلق وسيلة دخول للنظام دون الحاجة لتكرار العمليات السابقة.

5-مسح آثار الاختراق Covering Tracks

المواقع و الأنظمة يتم التأكد من سلامتها باستمرار للكشف عن أي نشاط مريب , لذا من الأهمية بمكان العمل على إخفاء الآثار بعد عملية الاختراق.

تثبيت المعمل
جزء عملي

تنزيل البيئة الافتراضي

VirtualBox

عبارة عن برنامج افتراضية عبر الأنظمة الأساسية. يسمح للمستخدمين بتوسيع جهاز الكمبيوتر الحالي الخاص بهم لتشغيل أنظمة تشغيل متعددة بما في ذلك Microsoft Windows و Mac OS X و Linux و في نفس الوقت.

https://www.virtualbox.org/wiki/Downloads

تنزيل النظام (المعمل)

kali linux

يستخدم المخترقون Kali Linux لأنه نظام تشغيل مجاني ولديه أكثر من 600 أداة لاختبار الاختراق وتحليلات الأمان.

https://www.kali.org/get-kali/#kali-virtual-machines

الجميع الان يستطيع يطبق على
النظام المتاح بشكل مؤقت
parrot

https://www.onworks.net/os-distributions/special-os/free-parrot-security-os-online

نهاية الدورة الجميع يقوم الان بتطبيق 5 ادوات على النظام المباشر parrot

https://www.onworks.net/os-distributions/special-os/free-parrot-security-os-online

الادوات

nmap
nikto
zap
dimtry

المراجع

Guide to Computer Network Security (book)

Cybersecurity Fundamentals A Real-World Perspective Dr Kutub Thakur Dr Al-Sakib Khan Pathan (book)

الهيئة العامة للأمن السيبراني في المملكة العربية السعودية