مقدمة في الأمن السيبراني

تقديم
عبدالله محمد الكثيري

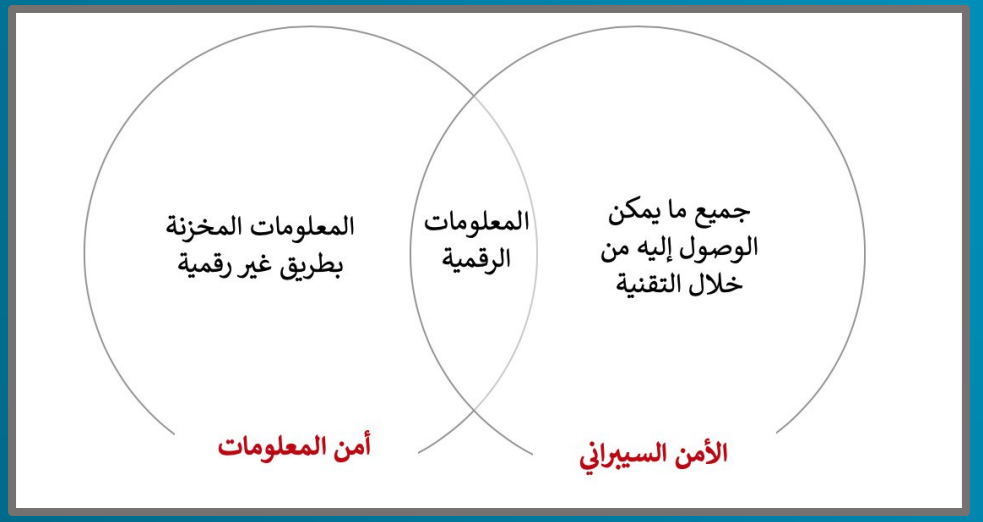
ماهو الأمن السيبراني ؟

الأمن السيبراني هو ممارسة حمايةٍ الأنظمة والشبكات والبرامج من الهجمات الرقمية. التي تهدف عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المال من المستخدمين أو مقاطعة العمليات التجارية.

ما الفرق بين أمن المعلومات والأمن السيبراني؟

امن المعلومات : يهتم بأمن المعلومات بشكل عام سواء داخل الحاسب او خارجه (المعلومات الفيزيائية)

الأمن السيبراني : حماية المعلومات من التعرض للسرقة من قبل مصادر خارجة على شبكة الانترنت



مصطلحات مهمة في الامن السيبراني

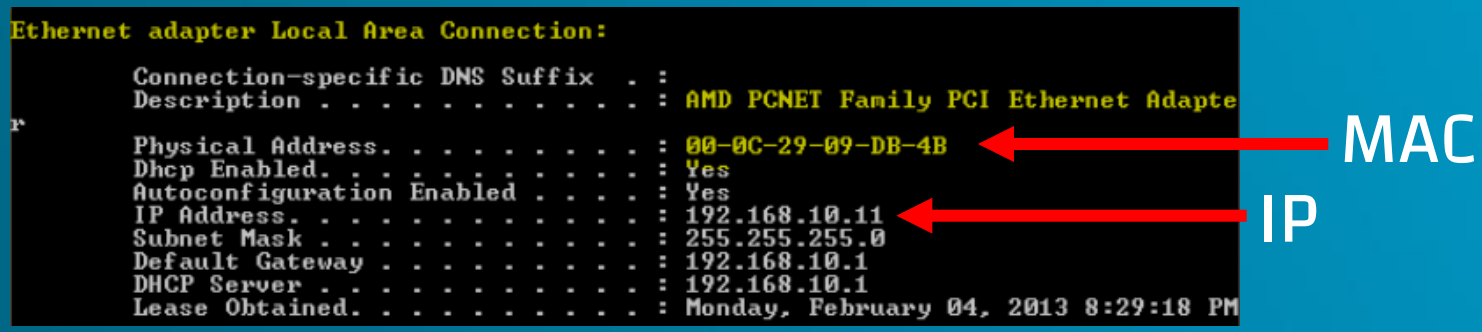
software : هو برنامج يحتوي مجموعة من الاوامر التي تخاطب جهاز الكمبيوتر لأداء مهام معينة

```
Command Prompt

C:\Users\Gic\Desktop>python software.py
Hello
My name is Abdullah
2
```

```
1  print('Hello')
2  print('My name is Abdullah')
3  x = 5
4  y = x - 3
5  print(y)
```

IP : هو عنوان الجهاز على الشبكة **MAC** : هو العنوان الفيزيائي للجهاز (ثابت)

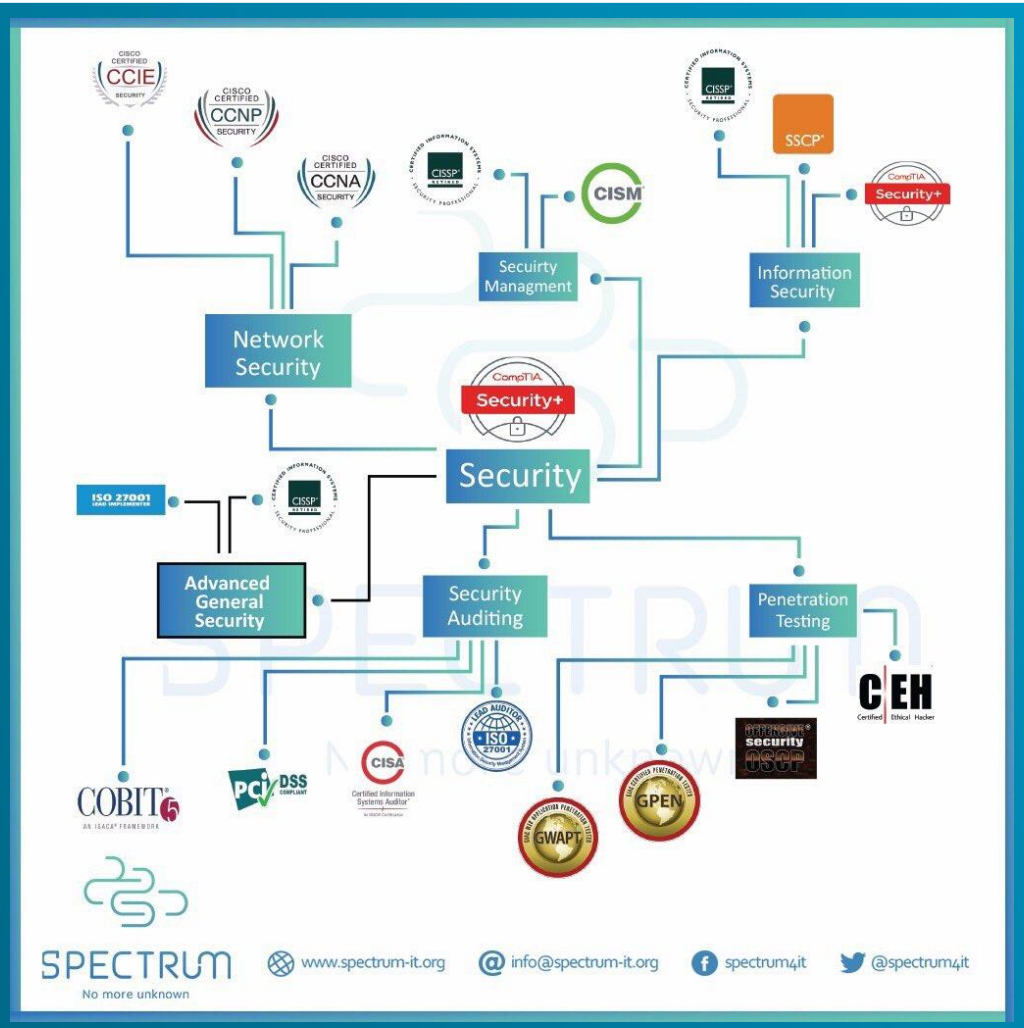


مصطلحات مهمة في الامن السيبراني

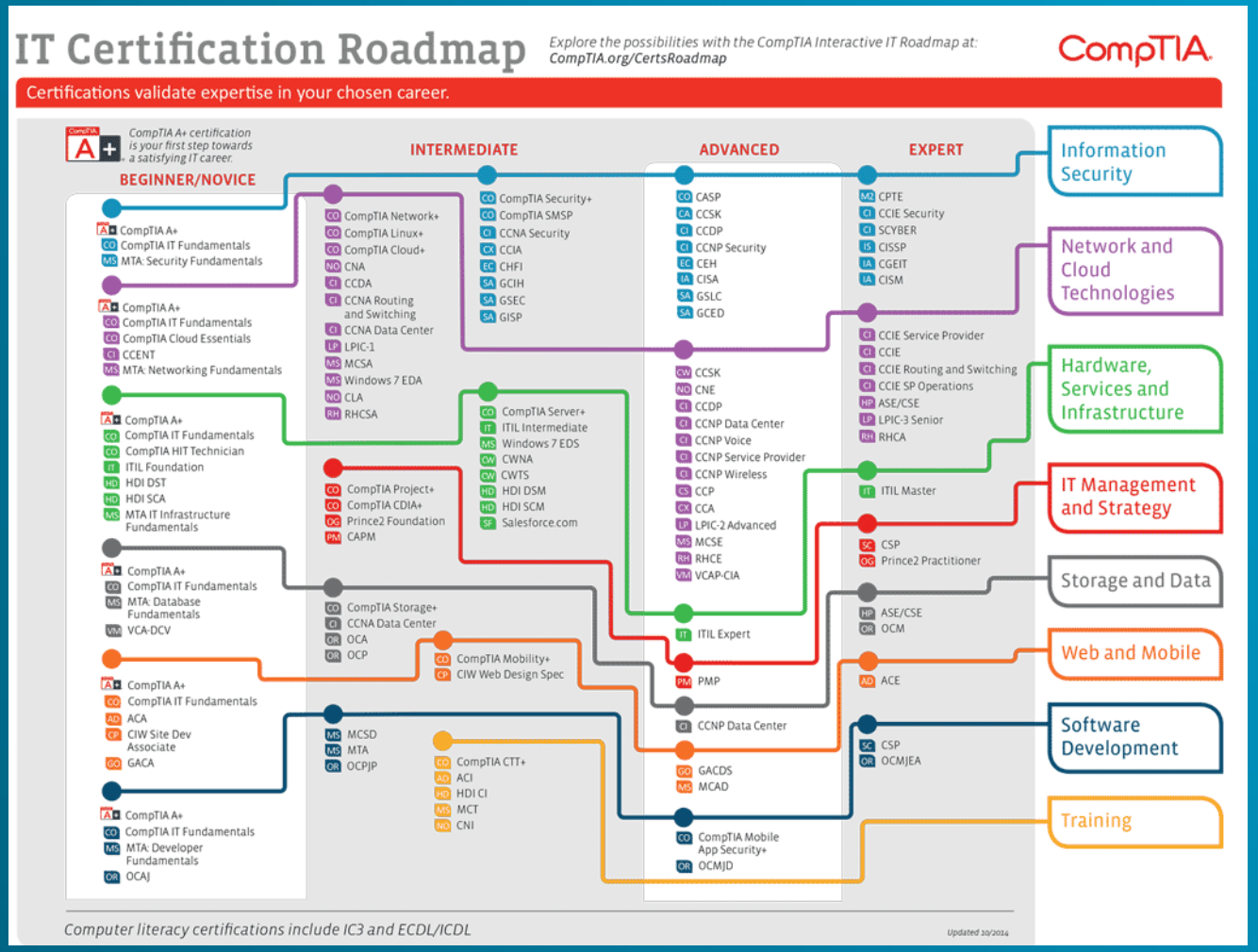
ثغرة Vulnerability : ثغرة في نظام معين
أستغلال Exploit : تطبيق ضار او برنامج نصي للحصول على صلاحيات وبيانات من داخل النظام عن طريق ثغرة

جدار الحماية Firewall : قد يكون برنامج او كمبيوتر يقوم بفرز العمليات المارة في الشبكة والفصل بين الاجهزة او الشبكات الاخرى
فحص Scan : فحص, سواء فحص شبكة او فحص نظام
نظام تشغيل OS or Operating system : نظام تشغيل (ويندوز, ماك, لينكس...)

تفرعات امن السيبراني



Roadmap certifications for Cyber Security



سؤال...

ماهو اكثر نظام تشغيل يتم استخدامه
في مجال الامن السيبراني؟ ولماذا؟

اساسيات الشبكات

http package


```
POST /login?mode=login HTTP/1.1
Host: testing-ground.scraping.pro
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testing-ground.scraping.pro/login
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Connection: keep-alive
Upgrade-Insecure-Requests: 1

usr=admin&pwd=12345HTTP/1.1 302 Found
Date: Sat, 20 Jun 2020 22:59:15 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.4-14+deb7u12
Set-Cookie: tdsess=TEST_DRIVE_SESSION
Location: /login?mode=welcome
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1609
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

http://testing-ground.scraping.pro/login

اعداد واحصائيات في الأمن السيبراني

كل 39 ثانية يوجد هجمة في الفضاء السيبراني من قبل احد الهاكرز

43% من الهجمات السيبرانية تستهدف منشأت الاعمال الصغيرة

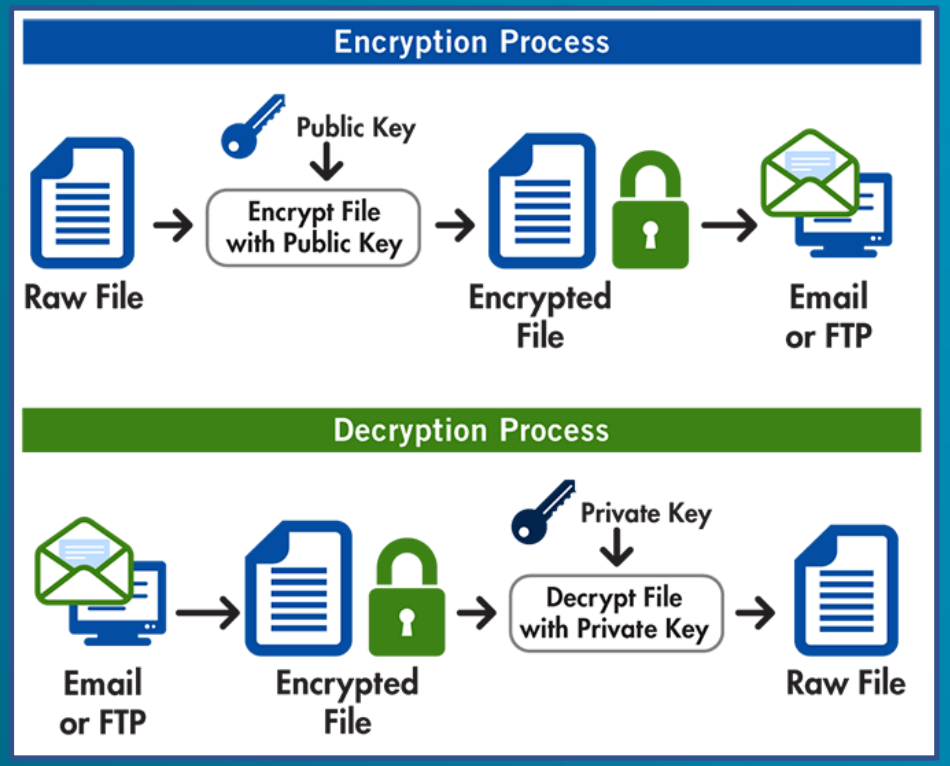
في عام 2020 المتوقع ان تصل تكلفة الهجمات السيبرانية على المؤسسات والحكومات الى 150 مليون دولار

DDos او هجمات حجب الخدمة ازدادت بمقدار 500%

https://cybermap.kaspersky.com/

تشفير Pretty Good Privacy (PGP)

برنامج يقدم خدمة تشفير البيانات عبر الأنترنت
عبر استخدام مفتاحين (عام – خاص)



تشفير Pretty Good Privacy (PGP)

احمد

الأنترنت

عبدالله

تشفير Pretty Good Privacy (PGP)

عبدالله

Public Key

Private Key

الأنترنت

احمد

Public Key

Private Key

تشفير Pretty Good Privacy (PGP)

احمد



Public Key
حق عبدالله

Public Key

Private Key

الأنترنت

عبدالله



Public Key
حق احمد

Public Key

Private Key

تشفير Pretty Good Privacy (PGP)

احمد



Public Key
حق عبدالله

Public Key

Private Key

السلام عليكم
كيف حالك ؟

مستند

Public Key
حق عبدالله

الأنترنت

عبدالله



Public Key
حق احمد

Public Key

Private Key

تشفير Pretty Good Privacy (PGP)

احمد



Public Key
حق عبدالله

Public Key

Private Key

الأنترنت

مستند

Public Key
حق عبدالله

d55d11gh
5cc885w1

عبدالله



Public Key
حق احمد

Public Key

Private Key

تشفير Pretty Good Privacy (PGP)

احمد

Public Key حق عبدالله

Public Key

Private Key

الأنترنت

عبدالله

Public Key حق احمد

Public Key

Private Key

مستند

d55d11gh
5cc885w1

Public Key
حق عبدالله

تشفير Pretty Good Privacy (PGP)

تشفير Pretty Good Privacy (PGP)

احمد

Public Key Public Key Private Key

حق عبدالله

الأنترنت

عبدالله

Public Key Public Key Private Key

حق احمد

مستند

دوال التشفير | Hash Function

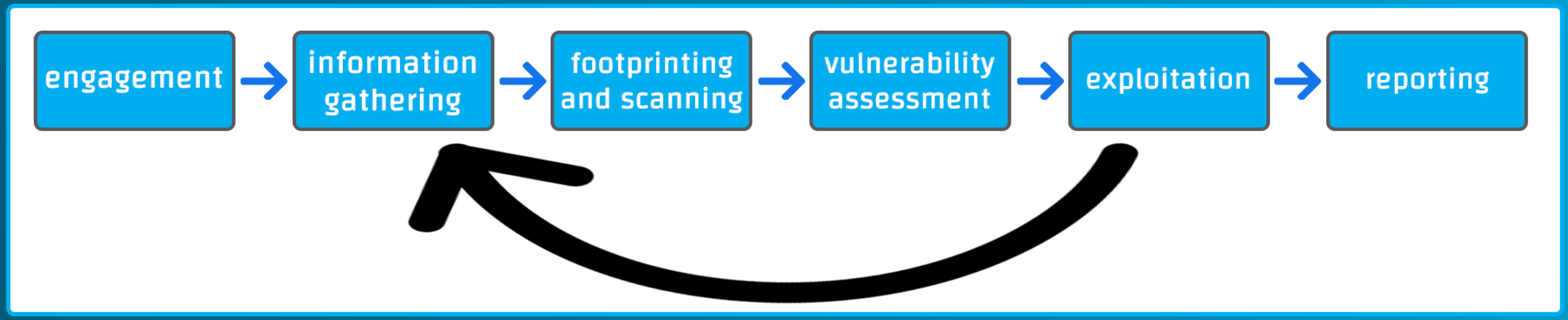
موقع لتحويل النص الى شيفرة : https://www.md5online.org/

موقع لتحويل الشيفرة الى نص : https://www.md5online.org/md5-decrypt.html

استراحة لمدة 10 دقائق

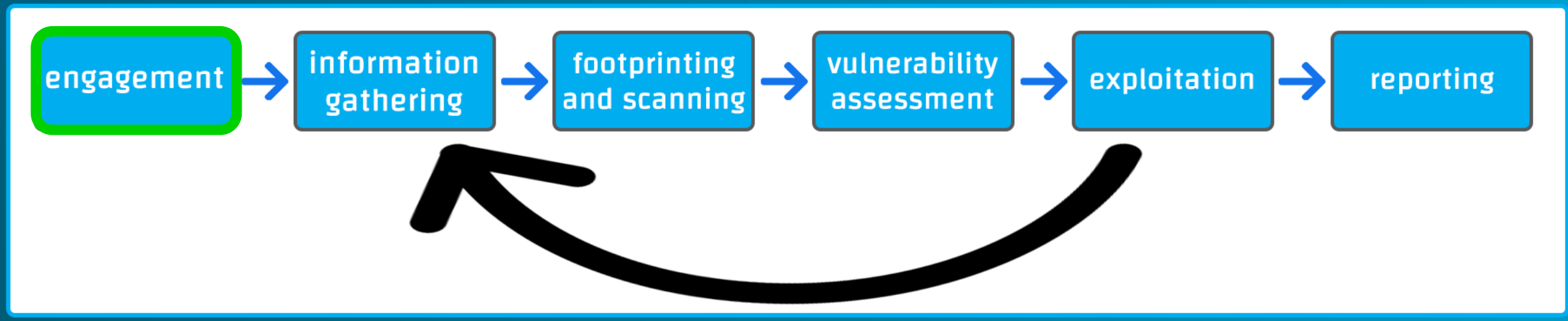
Penetration tester life cycle

لفهم معنى اختبار الاختراق يجب علينا معرفه الخطوات المتبعة
والاساليب المستخدمة والادوات المساعدة خلال هذه العملية



Engagement

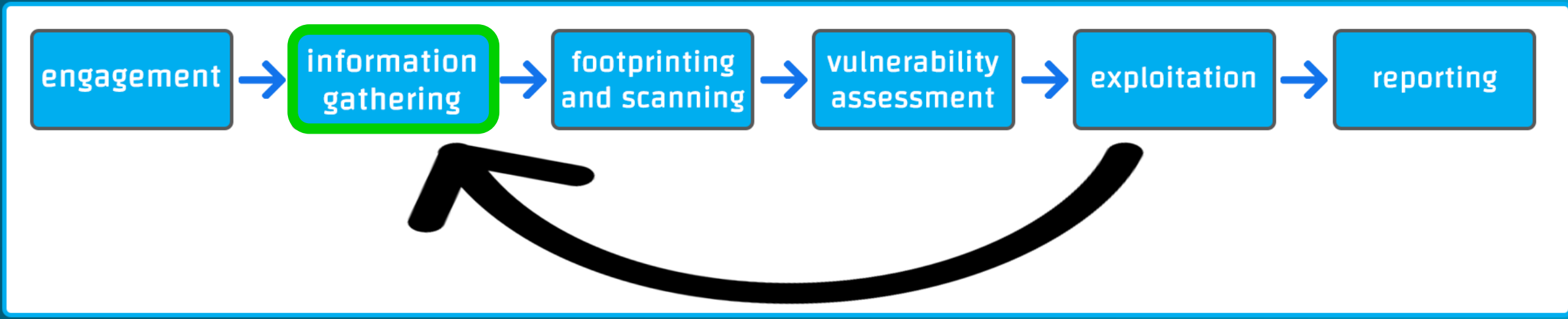
Type of engagement (Black, Greay,.....) Box نوع بيئة الاختبار
Time consumed الوقت المتوقع للعمل
Complexity مدة تعقيد وصعوبة انظمة التشغيل لدى الشركة
No. of targets (.....,أجهزة, شبكات, سيرفرات) عدد الاهداف



Information gathering

احد اهم الخطوات الأولية لعمل أختبار اختراق صحيح وفعال
- موقع الشركة (الشركة الأم, الفروع, الادارة)
- أعضاء الادارة و المشرفين والموظفين (أسماء, ارقام, بريد الكتروني)
يمكن استخدام الهندسة الأجتماعية (إن كانت مسموحة)

Google dorks, search engenes, social media, social eng.,.....



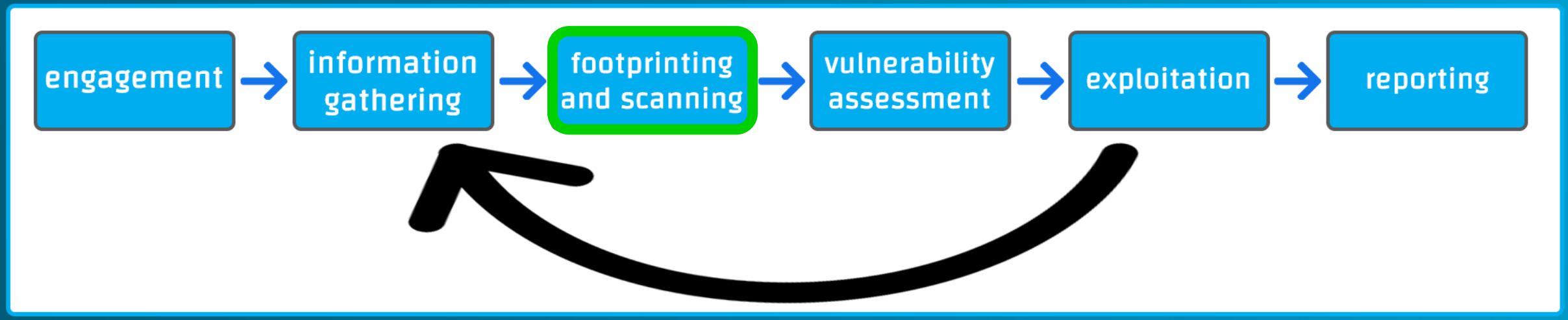
Footprinting and scanning

تهتم هذه الخطوة في فحص بيئة الهدف ومعرفه الخدمات وأنظمة التشغيل المستخدمة وعدد الشبكات والأجهزة و و و.....

أيضاَ البحث عن وجود اي ثغرة قد تم اكتشافها في نظام اخر من قبل

Port scanning, OS, services

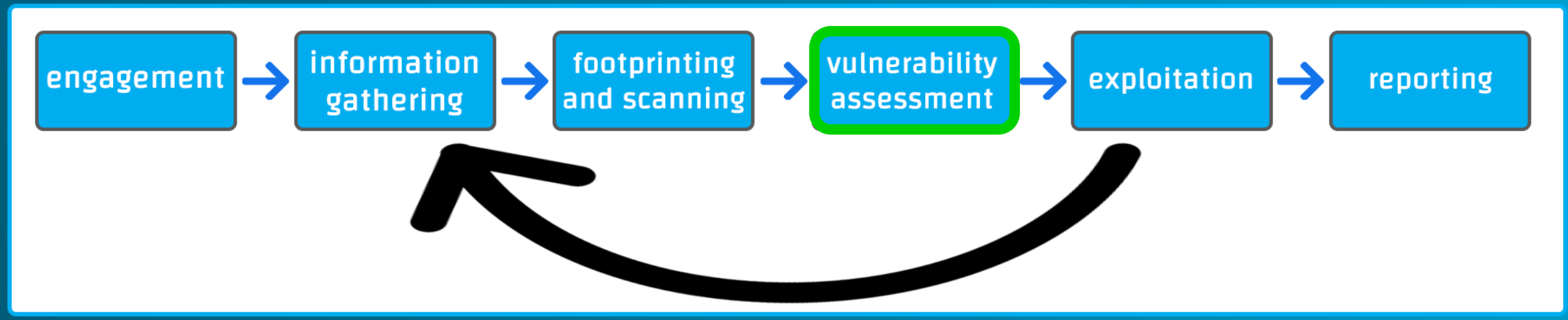
N-map, sqlmap, nikto, sn1per,.....



Vulnerability assessment

يتم تحديد الثغرات المتاحة حالياً على الشبكة
تحديد نطاق الثغرة (ويب, نظام تشغيل, قاعدة بيانات,.....)

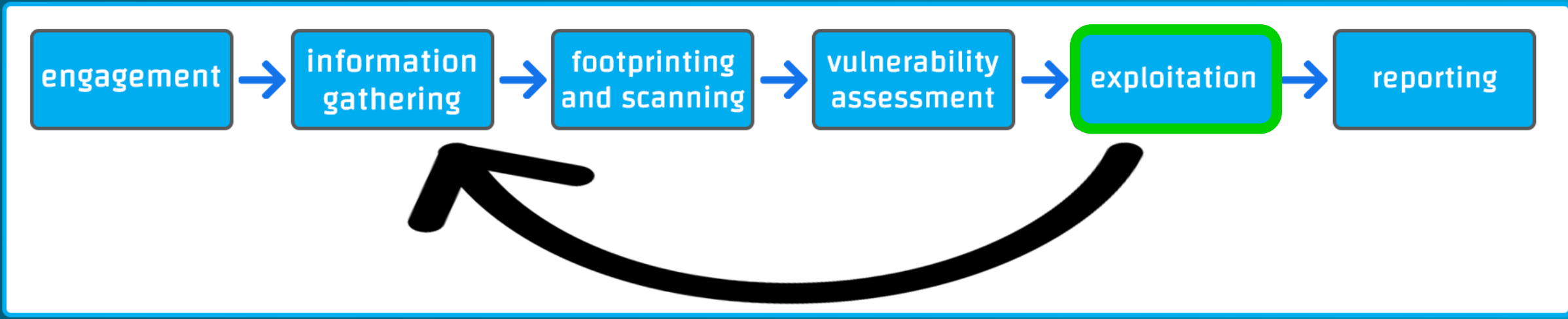
N-map, nessus,.....



Exploitation

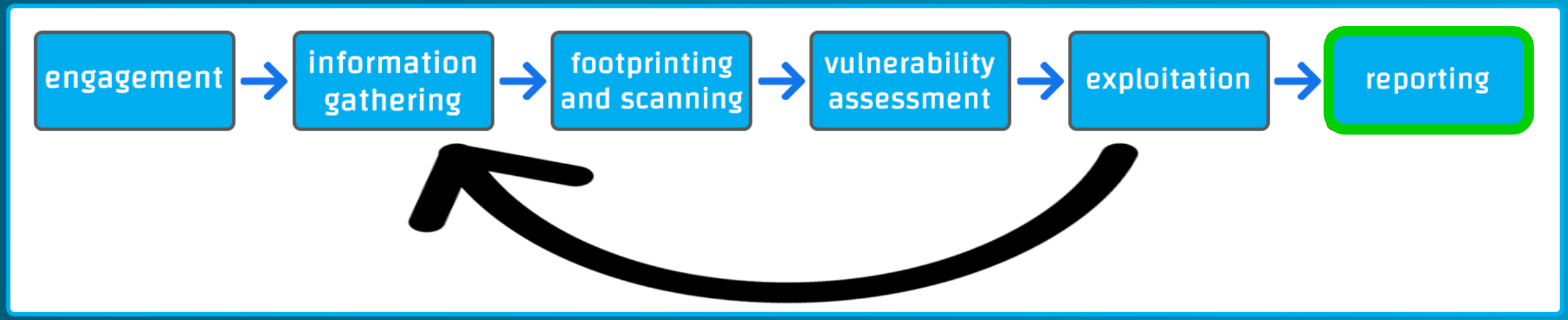
مرحلة تطوير برنامج او كود لأستغلال الثغرة
اثبات صحة وجود لثغرة من الأساس
الحصول على صلاحيات على النظام المستهدف

Metasploit, exploit-db, n-map,sqlmap,manuale



Reporting

اخر مرحلة من مراحل اختبار الاختراق, وهي تقديم تقرير شامل بجميع ماحصل في المراحل السابقة
الأجهزة التي تم فحصها, التقنيات المستخدمة, الثغرات الموجودة, نقاط الضعف



بعض اهم الشهادات في مسار اختبار الاختراق

الجهة المقدمة	المستوى	اسم الشهادة
Comptia	مبتدئ	A+, Network+, security+, server+
EC-Council		CEH, CHFI
eLearnSecurity		PTS
CISCO		CCNA
eLearnSecurity	متقدم	PTP
CISCO		CCNP
Offensive security		OSCP
	خبير	OSCE

أسئلة شائعة

هل يمكن للطالب التخصص في مسار الأمن السيبراني كدرجة بكالوريوس في جامعة الملك عبدالعزيز؟

هل الأمن السيبراني يندرج ضمن مجال علوم الحاسب أم تقنية المعلومات ؟

ماهي المجالات الوظيفية التي قد يعمل فيها المتخصص في الأمن السيبراني ؟

ماهي مميزات تخصص الأمن السيبراني ؟

ماهي المهارات التي يُفضل توفرها لدى الشخص المقدم على هذا التخصص ؟

مواقع التواصل

حساب كلية الحاسبات وتقنية المعلومات

@FCITKAU

حساب مقدم اللقاء : عبدالله الكثيري

@iiKatheri

عطاء تقني

شكرا لكم