الدرع الالكتروني

العدد الثاني

صحيفة نصف شهرية تصدر عن مؤسسة الدرع الالكتروني

IT5:MATRIX.ORG

العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

الفهرس

افتتاحية العدد..... 3
الهندسة الاجتماعية..... 4
العندسة الاجتماعية - تعريفها..... 5
االهندس الاجتماعية - الادوات المستخدمة فيها..... 6
الهندسة الاجتماعية اداة SET..... 6
الهندسة الاجتماعية اداة Sherlock..... 7
الهندسة الاجتماعية اداة Maltego..... 8
الهندسة الاجتماعية اداة Email2Phonenumber..... 9
الهندسة الاجتماعية اداة Karma..... 11
الهندسة الاجتماعية اداة whatsmyname.app..... 13
الهندسة الاجتماعية اداة UnknSMS..... 14
الهندسة الاجتماعية اداة DataFaker..... 16
انظمة اختبار الاختراق..... 17
مقدمة في نظام Linux..... 21
اهم اوامر نظام Linux..... 22
خاتمة العدد..... 23

الدرع الالكتروني

العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

افتتاحية العدد

بسم الله الرحمن الرحيم

عدد جديد من صحيفة الدرع الالكتروني يصدر ، حلقة جديدة تضاف الى حلقات السلسلة التي نريدها ان تكون اداة تواصل بين مؤسسة الدرع الالكتروني والقارئ الكريم سواء أكان مختصا في مجال الامن المعلوماتي او مهتم بالشأن التقني عموماً . نريدها صحيفة مفيدة ومصدرا للمعلومات وطاولة مستديرة تُطرح عليها الافكار وتُناقش ، وتنتج عنها اقتراحات قابلة للتطبيق ، ونافذة تفتح في مجال امن وحماية المعلومات ، فيتعرف المتلقي من خلالها على الجديد والمستجد في هذا الحقل الواسع والدائم التجدد والذي يستأثر باهتمام المجتمعات والافراد في كل انحاء العالم فَصَبْرٌ جَمِيلٌ وَاللَّهُ الْمُسْتَعَانُ عَلَى مَا تَصِفُونَ

العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

الهندسة الاجتماعية

نبذة عن الهندسة الاجتماعية

هل سمعت من قبل عن الهندسة الاجتماعية إذا كانت الإجابة بالنفي، فأنت بالتأكيد قد واجهت على الأقل أحد هذه المواقف

اولا :- يصل لك بريد إلكتروني يخبرك فيه صاحب الرسالة أن لديه ثروة ضخمة ولكنها للأسف محجوزة لسبب أو لآخر، ويريد منك أن ترسل له بياناتك البنكية حتى يتمكن من تحويل المبلغ إليك ثم تعيد تحويله له، لأنه يثق بك ثقة كبيرة، واختارك أنت عن جميع البشرية لأنك تبدو شخص أمين وذو خلق

ثانيا :- رسالة تصل إلى جوالك أو عبر البريد الإلكتروني تخبرك أن أحدهم يحاول اختراق حسابك على الفيس بوك وعليك تغيير كلمة السر الآن

ثالثا :- رسالة تصلك عبر تطبيق الواتس أب تخبرك أن شركة الواتس اب قررت تنفيذ خطوة جديدة لحماية بياناتك وعليك إرسال كلمة السر التي ستصل إليك

لو كنت من مستخدمي هذا الفضاء الإلكتروني الشاسع فأنت بلا شك صادفت موقف مشابه المذكورة أعلاه، أو ربما جميعهم ، هذا بالضبط ما يسمى ب الهندسة الاجتماعية، والذي يستهدف مرتكبيها نوع مختلف من الاحتيال من أجل إيهام الضحايا بصدق حجته، وبعدها يحصل على البيانات لتبدأ سلسلة من الابتزاز والنصب بغرض الحصول على المال

الدرع الالكتروني

العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

الهندسة الاجتماعية

تعريف الهندسة الاجتماعية

تعرف الهندسة الاجتماعية على أنها مجموعة من الأنماط والسلوكيات البشرية التي نمارسها بقصد أو دون قصد، والتي يستخدمها المختصون عامة في التسويق لإقناع الجمهور بمنتج بعينه والترويج لمؤسسات، كما تستخدم في عالم السياسة من أجل كسب تأييد الجماهير، كما يستخدمها الأطباء في بعض الأحيان لحث مرضاهم على اتباع نظام .غذائي معين على سبيل المثال من أجل صحتهم

أما الجانب السلبي لل الهندسة الاجتماعية هى أن المحتالين وعصابات الاختراق الإلكتروني تستخدمها من أجل استغلال نقاط الضعف في عقلية المستخدم من أجل تحقيق أهدافهم وتوجيه الأشخاص على شبكة الإنترنت لتنفيذ خططهم التخريبية، لذلك نجد أن القرصنة الإلكترونية تعتمد اعتمادًا أساسيًا على هذا العلم

وبالتالي فإن المهندسين الاجتماعيين قد يكونوا هم الأشخاص المعنيين بحماية أمن البيانات وحفظ المعلومات إلكترونيًا عن يد المخربين، ومن الممكن أيضًا أن يكونوا هم أنفسهم المخربين، وفي هذه الحالة يكون تأثيرهم أكثر خطورة من القرصنة

الهندسة الاجتماعية

الادوات المستخدمة في الهندسة الاجتماعية

تختلف ادوات الهندسة الاجتماعية على اختلاف العمل الذي تقوم به كل اداة حيث يُمكن الاطلاع على أدوات الهندسة الاجتماعية على النحو الآتي

اولا :- اداة SET

هي اداة مفتوحة المصدر مصممة لتنفيذ هجمات الهندسة الاجتماعية والتي تستخدم لاختراق أنظمة الحواسيب والشبكات ، حيث يمكن للاداة انشاء العديد من الهجمات بما في ذلك الاختراق عن طريق الصفحات المزورة والبريد الالكتروني المزيف وغيرها الكثير . يمكن تثبيت الاداة على نظام لنكس حيث يمكن تشغيلها بمجرد كتابة الامر setoolkit في واجهة سطر الاوامر لوسيتم فتح الواجهة الرسومية للاداة حيث تحتوي الواجهة الرسومية للاداة على العديد من الخيارات منها

رسائل البريد المزيفة : حيث تتيح هذا الخيار انشاء رسائل مزيفة وارسالها الى الضحية

انشاء صفحات مزيفة : حيث يمكن للمخترق انشاء صفحة تسجيل دخول مزيفة وارسالها للضحية لسرقة حسابه على مواقع التواصل الاجتماعي وغيرها من المواقع

الهجوم على شبكات WiFi

يتيح لك هذا الخيار تنفيذ هجمات تقنية بغية اختراق الشبكة المنزلية

وهناك العديد من الخيارات الاخرى داخل الاداة

العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

الهندسة الاجتماعية

ثانيا :- اداة sherlock

في بعض الأحيان تحتاج إلى البحث عن المعلومات المتاحة حول شخص ما على مواقع التواصل الإجتماعي مثل فيسبوك, إنستغرام, .يوتيوب, سناب شات, بلوجر و غيرهم أداة توفر عليك الكثير من الجهد و الوقت الذي تتطلبه عملية البحث حيث يمكنك تزويدها بإسم المستخدم الخاص بالشخص و هي ستقوم بالبحث عن الحسابات المرتبطة به في شبكات التواصل الإجتماعي أو بمواقع الويب التي يظهر للأداة وجودصلة محتملة بينهما هذه الأداة متاحة على نظام لينكس و على الهاتف المحمول الذي يعمل بنظام آندرويد (Android) على برنامج تيرمكس (Termux)

طريقه تنصيب الاداة كمثلها من الادوات الاخرى حيث يمكنك تحميل أداة من github موقع حيث يمكن تثبيت الاداة عن طريق كتابة الامر حيث التالي

```
git clone https://github.com/sher-lock-project/sherlock.git
```

بعد تثبيت الاداة على الجهاز نقم بتشغيلها بواسطة الامر التالي ساقوم بتجربة على حساب مؤسسة الدرع الالكتروني it5

```
python3 sherlock.py it5
```

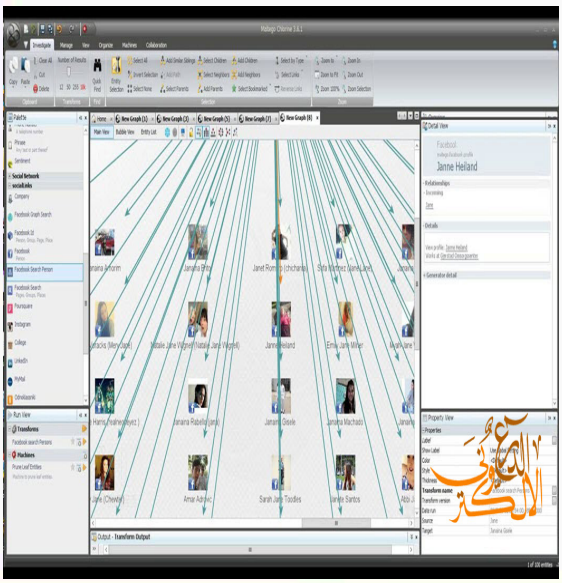
العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

الهندسة الاجتماعية

ثانيا :- اداة Maltego

هى اداة تم تصميمها خصيصا لجمع المعلومات عن اشخاص او شركات او مواقع او حتى شخص على فيسبوك تتمثل المعلومات التى يتم جمعها في التالى معرفة تفاصيل حول الشخص ومدي ارتباطه بأى معلومات اخرى او حزب او فريق معين معرفة مواقع مرتبطه او خاصه به معرفة صور خاصه به او الوصول الى صوره خاصه به معرفة رقم هاتفه او بريده الالكتروني والكثير من تلك الامور هذه الاداه تقوم بجمع جميع المعلومات المرتبطه باسم معين او موقع معين ومدى ارتباطه بها ويتم جمع تلك المعلومات من الانترنت - تتميز تلك الاداه بأنها قادره على جمع قدر كبير من المعلومات بعكس اى اداه اخري او محرك بحث حيث تعد سهلة الاستخدام لكونها تحتوي على واجهة رسومية

فكما ذكرت في الأول فهو برنامج لجمع المعلومات عن أي شخص ، حيث تجد في القائمة الجانبية للبرنامج معلومات كثيرة عن أي شئ تريد ، مثال الدومين والآشخاص ، كما يمكن استعمال الشبكات الإجتماعية كالفيسبوك مثلا للوصول إلى أرقام الهواتف والإيميل ثم معلومات أخرى عن أي شخص تريده

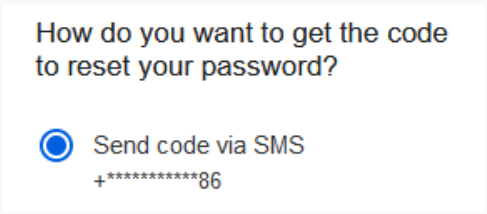


الهندسة الاجتماعية

رابعا :- اداة Email2Phonenumber

هي اداة مفتوحة المصدر لاستخراج رقم الهاتف المرتبط بالبريد الالكتروني كل ما تحتاجه هو عنوان البريد الإلكتروني للهدف، وبهذه المعلومات وحدها، من الممكن استرداد رقم هاتفه. تعمل الأداة بعدة طرق مختلفة. فهي يقوم باستخراج أرقام الهواتف من مواقع الويب (عن طريق إعادة تعيين كلمة المرور عبر عنوان البريد الإلكتروني)، وإنشاء أرقام هواتف بناءً على خطة ترقيم الهاتف الخاصة بالبلد وعمل تخمين على هذا الارقام ليتم استخراج رقم الهاتف الصحيح المرتبط بهذا البريد تعتبر هذه الاداه من اقوى الادوات في هذا المجال حيث يمكن استغلالها ايضا لاستخراج الارقام المرتبطة بحسابات الفيسبوك وهي من الادوات النادره في مجال استخراج معلومات حساسة مخفية غير مرخص لاي احد استخراجها

حيث ان الاداة قادره على استخراج ارقام الهواتف المتبطه على شكل نجوم مخفية

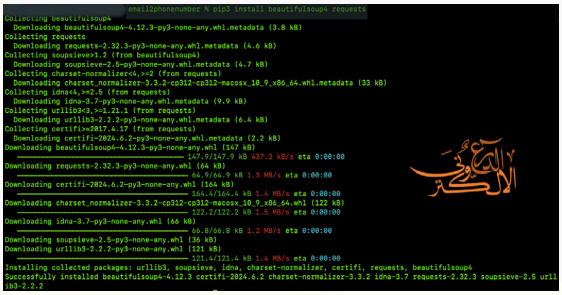


طريقة تثبيت الاداة

الاداة مبرمجة بلغة بايثون فيجب ان يتوفر في جهازك بايثون

بعد تحميل الاداة من موقع Github يتحتاج الى تنصيب pip3 عن طريق الامر التالي

pip3 install beautifulsoup4 requests



العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

الهندسة الاجتماعية

ومن ثم نقوم بتشغيل الاداة عن طريق الدخول الى مجلد الاداة في المكان الذي قمنا بتحميلة فية ومن ثم نكتب الامر التالي لاستهداف البريد المراد استخراج الرقم المرتبط به عن طريق استخدام الامر التالي

python3 email2phonenumber.py scrape -e Al-Batar@email.com

حيث نقوم باستبدال البريد الافتراضي في النهاية بالبريد المستهدف

```
python3 email2phonenumber.py scrape -e Al-Batar@mail.com
```

بعد استخراج جزء من رقم الهاتف نقوم بانشاء وفي نفس الاداة قاموس بارقام بالاعتماد على الارقام الثلاثة الظاهرة عن طريق الامر التالي

python3 email2phonenumber.py generate -m 555XXX1234 -o /tmp/dic.txt

بعدها نقوم وبنفس الاداة بعمل bruteforce لاستخراج الرقم المرتبط بالبريد المستهدف

عن طريق الامر التالي

python3 email2phonenumber.py bruteforce -m 555XXX1234 -e Al-Batar@email.com -p /tmp/proxies.txt -q

مع استبدال البريد الموجود بالامر بالبريد المستهدحيث ستقوم الاداة بالتخمين الى حين الحصول على الرقم المتبط بالبريد ويظهر باللون الاخضر كما مبين

```
Phone 4153008826 not registered
Phone 4153018826 not registered
Phone 4153028826 not registered
Phone 4153038826 not registered
Possible phone number for victimusa@martinvigo.com is: 4153048826
Phone 4153058826 not registered
Phone 4153068826 not registered
Phone 4153078826 not registered
```

تم استخراج الرقم بنجاح ، حيث يمكن استخدام الاداة لاستخراج الرقم من اغلب مواقع التواصل الاجتماعي وهي تعتبر من اهم الادوات المستخدمة في الهندسة الاجتماعية

الهندسة الاجتماعية

خامساً :- اداة Karma v2

يمكن أن يستخدمه باحثو أمن المعلومات، ومختبرو الاختراق، وصائدو الأخطاء للعثور على معلومات عميقة والتسريبات المكشوفة علنًا، وغير ذلك الكثير حول هدفهم حيث يمكن جمع معلومات عميقة عن الهدف اي كان موقع او شخص او رقم ايبي او تسريبات وحتى ثغرات المواقع الالكترونية وفي ما يلي طريقه عمل الاداة وبعض خصائصها

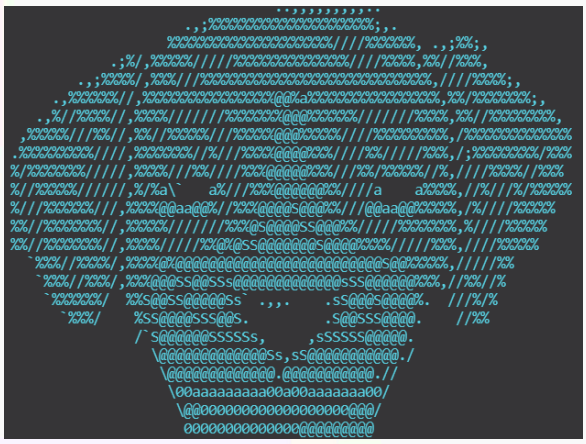
```
karma v2 is a Premium Shodan Recon based OSINT scanner.

Usage:
       karma_v2 [flags]

Flags:
TARGET:
       -d, --domain string     target DOMAIN.TLD to scan [* Required]
       -b, --banner            Karma Is My Bitch
       -h, --help              show this help message and exit
       -s, --silent            If set only findings will be displayed and banners will be redacted.
       -v, --version           show Karma version

DOWNLOAD-LIMIT:
       -l, --limit integer     Download <number of results>, Use -1 <negative integer> to unlimited download [* Required]

MODEs: [* Required]
       -ip                     Scan for In-Scope-IPs Validated by CN=*.{target} and Out-Of-Scope-IPs
       -asn                    Detailed Autonomous system number lookup with BGP stats, neighbours, IPv4 & IPv6 Prefixes
       -cve                    Scan hosts for such as OS, Host, Servers, Products, CVEs, Ports are open and which organization owns the IP
       -favicon                Search for Favicon Icons, Calculate Favicon Hashes and Technology Detection with nuclei custom template
       -cdn                    SSL/TLS, Hostnames, IPs Ignored any CDN Nodes [ Supported: Akamighost, Cloud(flare||front) ]
       -leaks                  Look for interesting findings
       -deep                   Deep Scan support all modules/modes [ count, ip, asn, cve, favicon, leaks ]
       -count                  Returns the number of results count for DORKs search [ No API Credit will use ]

UPDATE:
       -u, --update            Update karma to the latest released version

SECRET:
       --secret                Reveal me !!!
```

العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

الهندسة الاجتماعية

الاوامر المستخدمه في استخراج المعلومات

MODE	Examples
-ip	bash karma_v2 -d <DOMAIN.TLD> -l <INTEGER> -ip
-asn	bash karma_v2 -d <DOMAIN.TLD> -l <INTEGER> -asn
-cve	bash karma_v2 -d <DOMAIN.TLD> -l <INTEGER> -cve
-cveid	bash karma_v2 -d <DOMAIN.TLD> -l <INTEGER> -cveid CVE-2021-34473
-favicon	bash karma_v2 -d <DOMAIN.TLD> -l <INTEGER> -favicon
-leaks	bash karma_v2 -d <DOMAIN.TLD> -l <INTEGER> -leaks
-deep	bash karma_v2 -d <DOMAIN.TLD> -l <INTEGER> -deep
-count	bash karma_v2 -d <DOMAIN.TLD> -l <INTEGER> -count



وهنا مقاطع فديوية لطريقة عمل كل امر مع طريقة التحميل والتنصيب والاستعمال

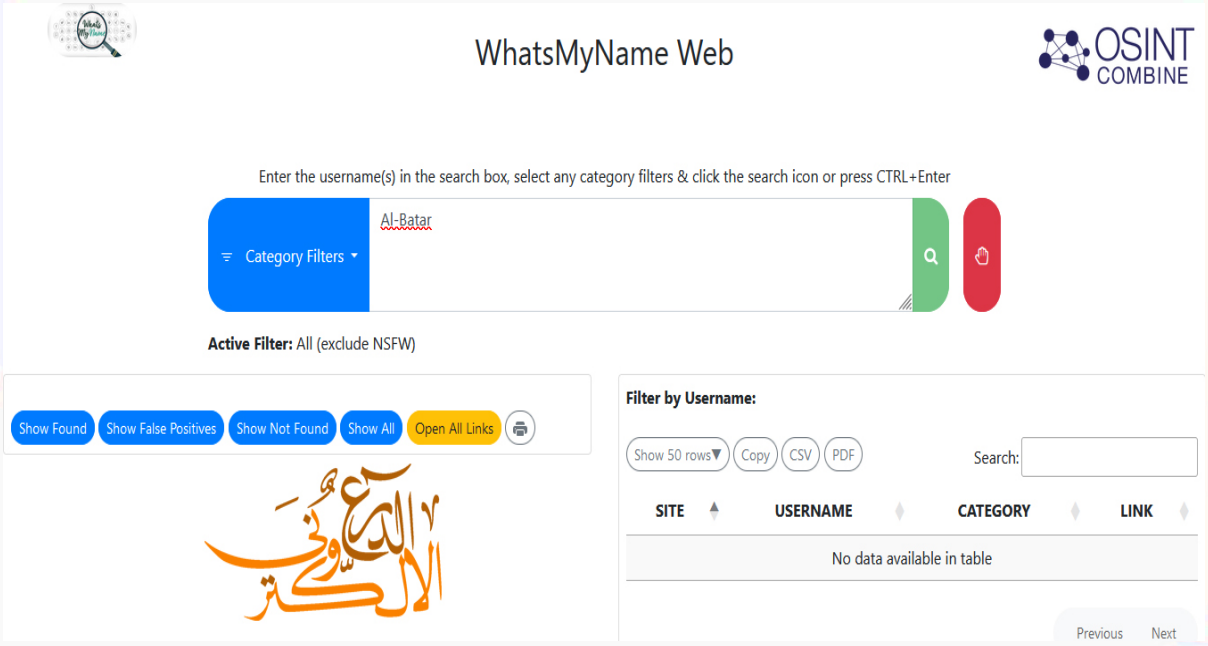
https://github.com/Dheerajmadhukar/karma_v2

الهندسة الاجتماعية

سادسا :- موقع whatsmyname.app

موقع الكتروني للبحث عن اسم المستخدم في اكثر من 500 موقع على شبكة الانترنت حيث بمجرد كتابة اسم المستخدم يقوم الموقع باستخدام دوال البحث داخل شبكة الانترنت واستخراج المواقع الالكترونية التي تحتوي هذا الاسم ومن مميزات هذا الموقع سهولة الاستخدام والدقه المتناهية في استخراج التفاصيل الحساسه وان كانت مخفية حيث لا تحتاج الى تسجيل دخول الى الموقع ولا الى المواقع التي يتم البحث فيها وهذه ما يميز هذا الموقع

رابط الدخول للموقع https://whatsmyname.app



الدرع الالكتروني

العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

الهندسة الاجتماعية

سابعا :- اداة UnknSMS

في بعض الاحيان نحتاج في عملية الهندسة الاجتماعية الى ارسال رساله مجهولة الى الشخص المستهدف من دون كشف هوية المرسل فوضعت بين يديكم اخوتي هذه الاداة الجبارة لارسال رسالة نصية الى اي هاتف مهما كان نوع الهاتف فقط نحتاج الى معرفة رقم الشخص المستهدف فبمجرد وضع رقم الهاتف للشخص المستهدف تم نقوم بكتابة نص الرساله وعن طريق الاداة يتم ارسالها الى الهدف بكل سهولة بعد ان نقوم بانتحال صفة اي شركة من شركات الاتصال او اي جهة حسب السيناريو المعد لاختراق الهدف ومن اهم مميزاتها انها سهلة الاستخدام وسريعه في الارسال تعمل على جميع الانظمة حيث تم تجربتها على نظام الوندوز ونظام اللنكس ونظام الاندرويد عن طريق تطبيق التيرمكس في الاندرويد وكما موضح مع طريقة التثبيت على كل نظام

الهندسة الاجتماعية

Kali Linux

طريقة تثبيت الاداة

- git clone https://github.com/R3LI4NT/UnknSMS
- cd UnknSMS
- python3 unknsms.py

Windows 10

- python3 installed --> https://www.python.org/downloads/
- download the repository manually
- open CMD
- pip3 install requests
- cd UnknSMS
- python3 unknsms.py

Termux

- pkg install git
- pkg install python3
- pip install requests
- git clone https://github.com/R3LI4NT/UnknSMS
- cd UnknSMS
- python3 unknsms.py

العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

الهندسة الاجتماعية

ثامناً :- اداة DataFaker

من الامور الاساسية والمهمة في عملية الهندسة الاجتماعية هي بناء شخصية وهمية تتلائم ومتطلبات الهدف الذي نقوم بجمع المعلومات عنه ، ويجب ان تكون هذه المعلومات كاملة من كل النواحي كالاسم والعمر وعنوان السكن ورقم الهاتف ورقم جواز السفر والوضيفه والعنوان الجغرافي لموقع السكن والبريد الالكتروني كل هذا المعلومات توفرها لنا هذه الاداة في مؤلة عن انشاء معلومات كاملة لشخصية وهمية قادره على اقناع الشخص المستهدف بان من يتكلم امامة هو شخص حقيقي وهذا سيساعدنا بشكل كبير بعملية الهندسة الاجتماعية

تعمل الاداة على نظام التشغيل لنكس عن طريق اتباع الاوامر التالية لتنصيب الاداة

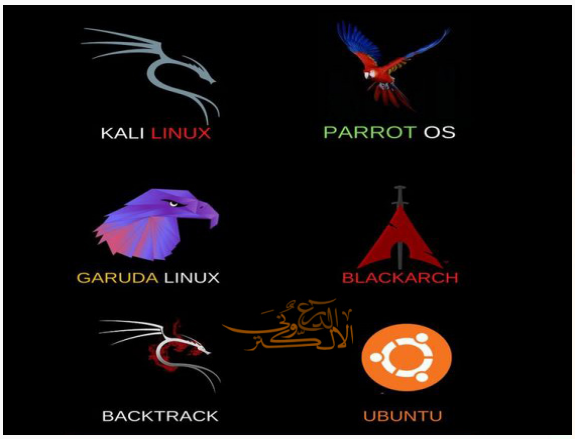
```
> git clone https://github.com/R3LI4NT/DataFaker
> cd DataFaker
> pip3 install -r requirements.txt
> python3 dataFaker.py --help
```

خصائص الاداة

COMANDO	DESCRIPCION
-l/--list	Lista de regiones disponibles
-r/--region	Region
-d/--data	Cantidad de data
-n/--name	Generar nombres falsos
-u/--url	Generar URL falsas
-a/--address	Generar direcciones falsas
-e/--email	Generar direcciones de correo falsos
--phone	Generar numeros telefonicos falsos
--passport	Generar numeros de pasaporte falsos

العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

انظمة اختبار الاختراق



تعتبر اختبارات الاختراق من الأدوات الأمنية الأساسية في عالم الامن السيبراني. فهي تُستخدم لتحديد ثغرات الأمان المحتملة في أنظمة المعلومات وتقييم قدرتها على التصدي للهجمات الخبيثة. ولتحقيق ذلك بنجاح، يتطلب المختصون في الأمان استخدام توزيعات مخصصة لاختبار الاختراق في هذا المقال، سنستعرض أفضل توزيعات اختبار الاختراق المتاحة حاليًا. سنناقش ميزاتها الرئيسية وأدواتها المتاحة وكيفية استخدامها لتحليل النظم واختبار الأمان. كما سنقدم نصائح قيمة لمساعدتك في الاختيار المناسب لاحتياجاتك الخاصة

أهمية اختبار الاختراق

تعتبر اختبارات الاختراق أداة فعالة لضمان أمان الأنظمة والشبكات والتطبيقات. عن طريق الكشف عن الثغرات والضعف في الأنظمة، يمكن للمؤسسات اتخاذ إجراءات استباقية للحد من مخاطر الهجمات السيبرانية الناجحة. يتم تحقيق عدة :أهداف رئيسية من خلال اختبار الاختراق، ومنها

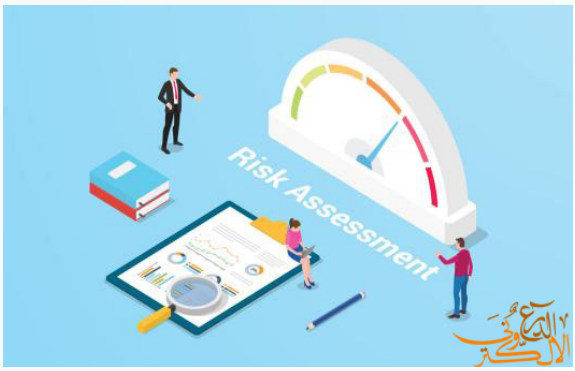
اولا :-تحديد الثغرات: يساهم اختبار الاختراق في تحديد الثغرات والضعف في أنظمة الكمبيوتر والشبكات والتطبيقات. يمكن أن تكون هذه الثغرات عرضة للاستغلال من قبل المهاجمين لاختراق النظام والوصول غير المصرح به وسرقة المعلومات أو تعطيل الخدمات. بعد اكتشاف وإصلاح هذه الثغرات، يمكن للمؤسسات تعزيز نظامها الأمني والوقاية من هجمات محتملة

الدرع الالكتروني

العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

انظمة اختبار الاختراق

ثانيا :- تقييم المخاطر: يساهم اختبار الاختراق في تقييم مدى خطورة الثغرات المكتشفة وتأثيرها على أمان النظام. يتم تصنيف المخاطر وفقًا لمستوى التهديد والاحتمالية وتأثيرها، مما يمكن المؤسسات من وضع استراتيجية للتعامل مع الثغرات الأكثر خطورة في المقام الأول



وهي عمليّة مستمرة في جميع خطوات الخطر المقصود دراسته، قبل المباشرة به، خلال العمل به وبعده. ويتمّ ذلك من خلال توثيق النّتائج المستحصلة للاستفادة منها وتحليلها، ولإعادة دراسة التّغيرات الّتي طرأت عليها

ثالثا :- تحسين الأمان: يمكن لاختبار الاختراق مساعدة المؤسسات في تحسين أمانها من خلال توفير توصيات وإرشادات لتعزيز الحماية وتطبيق التحديثات الأمنية اللازمة

بعد ما تطرقنا لعملية اختبار الاختراق واهميتها في مجال الامن السيبراني سنتناول اهم التوزيعات المختصة في مجال الاختراق واختبار الاختراق وكيفية استخدامها ونبذة عن كل توزيعة من هذه التوزيعات

العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

انظمة اختبار الاختراق

اولا Kali Linux

تُعد من بين أشهر توزيعات اختبار الاختراق في العالم. تحتوي هذه التوزيعة على مجموعة شاملة من الأدوات المتخصصة في اختبار الأمان واختبار الاختراق. تُستخدم على نطاق واسع في مجالات التحقيق الجنائي الرقمي والاختبار الأمني واختبار تطبيقات الويب والقرصنة الأخلاقية. تتميز عذع التوزيعة بواجهة سهلة الاستخدام ودعم واسع المدى من قبل مجتمع المطورين

ثانيا Parrot Security OS

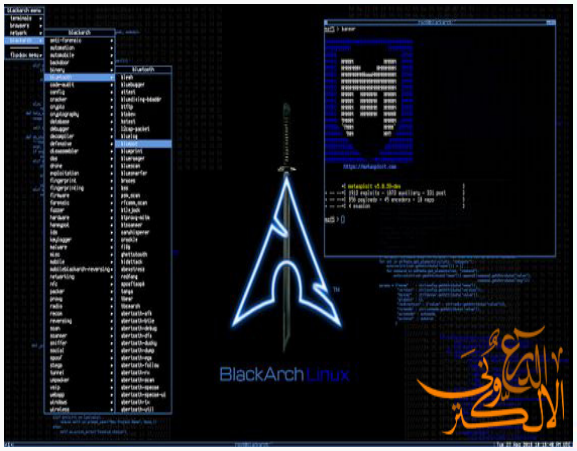
عتبر واحدة من أفضل توزيعات اختبار الاختراق المبنية على نظام اوبنتو . توفر هذه التوزيعة بيئة آمنة وشاملة للأمن وتحرص على الأداء الرائع والاستقرار. تأتي مُحمّلة بمجموعة كبيرة من الأدوات المتخصصة في اختبار الاختراق واختبار الشبكات وتحليل الثغرات وإدارة الهوية والتنصت والتشفير وغيرها الكثير. إن وجودها يُعد اختيارًا جيدًا للمستخدمين الذين يفضلون واجهة بسيطة وسرعة الاداء.

العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

انظمة اختبار الاختراق

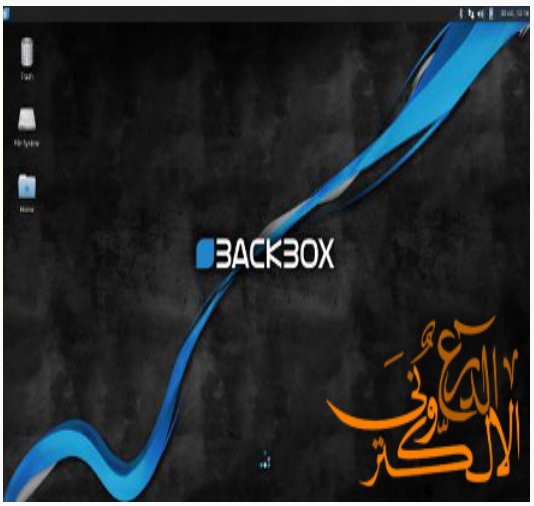
ثالثاً BlackArch Linux

إذا كنت تبحث عن توزيعة خفيفة الوزن ومتخصصة .في اختبار الاختراق، فإن قد تكون الخيار المثالي لك يعتبرة توزيعة متميزة نظرًا لتوفيرها أكثر من 2000 أداة مختلفة تغطي جميع جوانب اختبار الاختراق، بدءًا من التنصت والاختراق وحتى تحليل الثغرات واختبار التطبيقات والشبكات والتشفير وأدوات أخرى كثيرة. توفر للمستخدمين واجهة سهلة الاستخدام وقائمة شاملة للأدوات المتاحة، مما يوفر للمختصين في الأمان أدوات مرنة وقوية لاختبار الأنظمة وتحليل الثغرات



رابعا BackBox

تعتبر واحدة من التوزيعات الأخرى المشهورة في عالم اختبار الاختراق. تعتمد على نظام اوبنتو وتعتبر مفيدة جدًا للمختصين في الأمان ومحترفي اختبار الاختراق. تتميز بأدوات قوية لاختبار الثغرات والتنصت والتطبيقات والشبكات. ومن بين الميزات البارزة واجهة المستخدم البديهية والتي تجعل عملية اختبار الاختراق سهلة وفعالة



مقدمة في نظام Linux

ما هو نظام Linux

نظام لينكس عباره عن نظام تشغيل مفتوح المصدر مجاني ويستخدم في العديد من الاجهزة كالحواسيب والمتحكمات الصناعية والخوادم ، يتميز هذا النظام بالثباتية والأمان والسرعة العالية والمرورة الشديدة في التعامل معه كما يوفر النظام العدد من الادوات والبرامج المفتوحة المصدر التي يمكن استخدامها في ادارة وانشاء المواقع الالكترونية وتطوير البرامج والتطبيقات ، ويتميز النظام ايضا بسهولة اعداداته وتثبيته وتخصيصه لتلبية احتياجات المستخدم

حيث يحتوي نظام اللنكس على موجه اوامر من خلالها يتم التحكم به وانشاء المهام سنوضح اهم تلك الاوامر وطرق عملها وكيفية الاستفاده منها في عملنا

هل انت جديد على لينيكس, تعلم الان بعض الاوامر الاساسية التي تجعلك واثق و مرتاح في استعمالك لينيكس. ماذا تنتظر؟ غص في عالم لينيكس الان موجه اوامر لينكس او ما يعرف بـ التيرمنال هو واجهة نصية لجهازك. يتضمن كل نظام من موجه اوامر من نوع الى اخر, هذا الموجز التعليمي يتضمن بعض الاوامر لكن يجب ان يعمل معظم المحتوى بغض النظر عن توزيعة لينيكس الخاصة بك

العدد الثاني صحيفة تقنية نصف شهرية تصدر عن مؤسسة الدرع الالكتروني محرم 1446

مقدمة في نظام Linux

اهم اوامر نظام Linux

الأمر ls

هذا الأمر يقوم بسرد محتويات المسار الحالي

الامر pwd

كل ما يقوم به هو طباعة المسار الذي تتواجد فيه أنت

الامر cd

من خلاله يمكنك الانتقال إلى مجلد بمسار معين

الامر touch

يستخدم لانشاء ملف جديد كل ما نحتاجة هو كتابة الامر الامر ومن ثم اسم الملف وسكون لديك ملف جديد

الامر nano

هذا واحد من محررات النصوص الحديثة في لينيكس وهو من أسهل البرامج للإستخدام في التحرير. لتحرير ملف يمكنك كتابة الأمر، ومن ثم اسم أو مسار الملف الكامل

الامر rm

هذا الأمر يقوم بحذف الملفات والمجلدات

الامر cat

يقوم هذا الأمر بشكل عام بعرض محتويات الملفات

الامر shred

وهو امر لحذف الملفات بشكل نهائي بحيث لايمكن استرجاعها باي طريقة يقوم هذا الأمر بالكتابة على الملف 3 مرات بحيث يجعل عملية إستعادة البيانات الأصلية شبه مستحيل

الامر mkdir

هذا الأمر يمكنك من عمل مجلد جديد في المسار الذي تتواجد فيه أو في مسار آخر

الامر cp

من خلاله يمكنك نسخ الملفات والمجلدات من مكان لمكان آخر

الامر mv

يمكنك من خلال هذا الأمر أن تقوم بنقل الملفات والمجلدات من مكان لآخر

الامر find

هذا الأمر يقوم بالعثور على الملفات

خاتمة العدد

في خاتمة العدد الثاني من صحيفة الدرع الالكتروني المتعلق بالجانب التقني نرجو أن نكون قد وفقنا في وضع لبنات لبناء سد منيع يدحر كل من تسول له نفسه بمحاولة اعتراض تقدم اسود الدولة الاسلامية ، ونعلم علم اليقين بأن هناك من هم أعلى منا هامة وقدرًا وفكرًا، ويمكنهم أن يتوصلوا لنتائج أفضل مما تم التوصل إليها وهذا العدد يعتبر شرارة البداية للانطلاق في عالم الاختراق ففي الاعداد القامة ستكون هناك دروس عمليه وورشات حيه نستهدف فيها مواقع المرتدين من الصليبيين والفرس المجوس لنصل الى المستوى المطلوب وندعوا الله بالتوفيق لجميع الاخوة في سوح المعارك الذين يبذلون ارواحهم نصرتا للاسلام والمسلمين

مؤسسة الدرع الالكتروني