1/open source 2/hackers friendly

4/lost of flavors 3/easy packages installation

|  |  |
| --- | --- |
| To install package | apt-get install package name |
| بيعمل update لكل ال packages اللي في النظام | apt-get update |
| ............. | apt-get upgrade |
| بيشرح عمل ال command | man command name |
| بيظهر قائمة بأسماء ال packages و نوعها | Apt-cache searche package name |
| بيحذف package و ال packages اللي نزلت معاها | apt-get autoremove |
| لعرض المسارات اللي موجود فيها الملف | Locate file name |
| // // // // // | Find / -name "file name" |
| Transfer a URL | curl |
| بيحمل صفحة ال index على الجهاز لكن curl بيعرض محتوى الصفحة على terminal | wget |
| إنشاء ملف | Touch file name |
| لفتح ملف و التعديل عليه | Nano file name |
| لتغير محتوى الملف | Echo "text" >file name |
| للإضافة على المحتوى القديم | Echo "text" >>file name |
| To find active networks | ifconfig |
| لتطبيق أكثر من command في نفس الوقت  Ex: pwd;id | ; or && |
| بتخلي ال command يشتغل في ال background بالتالي تقدر تكمل كتابة في ال teminal | & |
| display the first 10 lines  لعرض عدد معين من الاسطر head -n file name | Head |
| display the last 10 lines  لعرض عدد معين من الاسطر tail -n file name | tail |
| للبحث عن كلمة معينة أو موضوع معين في ملف  Ex:  Cat index.html | grep -I -o “yahoo.com” | |grep |
| للحصول على نواتج غير مكررة من البحث | |sort -u |
| هيطبق ال command و يحط الخرج في ملف | |tee |
| report snapshot of the current processes | Ps |
| لإيقاف عملية | Kill |
| لو عايز أعرف ال memory مشغول منها قد ايه و كل directory أخد منها قد ايه | Df or df -h |
| بيسمح أشوف ايه شغال في ال memory في الووقت الحالي و استخدامه قد ايه | Top or htop |

***Permissons :-***

r….. permission to read …. this grants permottion only to open and view a file

w…. permission to write...this allows users to view and edit a file

x …. permission to execute….this allows users to execute a file

Ex: -rw-r—r—

أول رمز بيوضح هل هو file (-) و لا directory (d)

الرمز الثاني و الثالث و الرابع خاص ب root

الرمز الخامس و السادس و السابع خاص ب user

الرمز السابع و الثامن و التاسع خاص ب normal user

Convert user input into fixed size output

(هو عبارة عن كود برمجي بيعمل عمليات حسابية على ال input (

Irreversible (لا يمكن عكس العملية)

Ex : md4 , md5 , sha1 , sha2

استخداماته :

التأكد أنه لم يتم التلاعب على الرسا~ل المرسلة و التعديل عليها

زيادة أمان passwords

ليس له علاقة بالتشفير و الحماية و بيستخدم لتحويل البيانات لطريقة يقدر ال server و ال developer يتعامل معاها بشكل منطقي

Ex: rot13

***Two types***

***1/symmetric :***

يوجد مفتاح للتشفير و يتم فك التشفير بنفس المفتاح.

Ex: AES , DES , 3DES

***2/asymmetric :***

(الشيء الوحيد القادر على فك التشفير) and privet key (يستخدم للتشفير) Use public key

Ex : RSA , DH , DSA

*Encryption : 1/certificate chain. 2/browser trusted.*

Certificate :

هو عبارة عن اثبات هوية ل user أوserver معين بيحمل code أو digital sighature لايمكن تكرارها أو تخمينها و أي موقع https لازم يعمل check الأول على certificate يشوفها هل موجودة ولا لأ

وليها عنصرين أساسيين:public key & privet key

https connection بيستخدم طريقة sym & asym

Request على https

***server***

***Browser***

Public key الخاص بال server

why

لأن browser في الخطوة اللي بعدها بياخد ال public و يعمل بيه حاجتين :

1. يتأكد أن certificate سليمة عن طريق CRL (لينك عليه certificate اللي اتسرقت و تم مسحها )
2. بعد ماbrowser بيعمل create للمفتاح اللي بيستخدم في symmetric و يشفره باستخدام public key و يبعته لل server اللي معاه privet key فيقدر يفك الشفرة

و بالتالي تبادلوا المفتاح بطريقة مشفرة

|  |  |
| --- | --- |
| *Used with end user application (HTTP , SMTP)* | *Application* |
| *Decryption & encryption* | *Presentation* |
| *بيعرف الأجهزة على الشبكة (NetIOS)* | *Session* |
| *Protocols like (tcp ,udp)* | *Transport* |
| *فيه IP address وبيشتغل فيه ال routers* | *Network* |
| *Like switches و يوجد فيه جزء ال MAC address* | *Data link* |
| *Like cable* | *physical* |

*OSI model ……. 7 layers :*

*كيفية حصول الجهاز على IP على الشبكة*

عن طريق dhcp (يقوم باعطاء IP تلقائي عند الاتصال بالشبكة )

أو ممكن يكون ده يدوي زي ما في الشركات عن طريق مسؤول الشبكات

كيف يعمل dhcp ؟

1/ DHCP Discover

عندما يتم توصيل أحد الاجهزة علي الشبكة فإن هذا الجهاز لا يمتلك أي معلومات عن الشبكة لذلك فهو يقوم ببث حزمة من البيانات التي تسمي DHCP Discover والتي تحتوي علي بعض المعلومات مثل عنوان الماك Mac Address الخاص بالجهاز ويعتبر الماك أدرس في هذه المرحلة هو وسيلة الإتصال ويكون مصدر تلك الحزمة هو 0.0.0.0 لان الجهاز لايمتلك عنوان IP خاص به علي تلك الشبكة وتكون تلك الحزمة موجهة إلي العنوان 255.255.255.255 وهذا يعني إنها موجهة لجميع الاجهزة علي الشبكة .

2/ DHCP Offer

عندما يتم إرسال تلك الحزمة إلي الشبكة تصل إلي جميع الاجهزة الموجودة مسبقاً ومنها سيرفر DHCP عندها يعرف السيرفر إن هناك جهاز يريد الإنضمام إلي الشبكة وبالتالي يقوم بإرسال حزمة من البيانات للرد علي هذا الجهاز وعرض خدماته من خلال تلك الحزمة التي تحتوي علي بعض البيانات مثل عنوان IP و Subnet mask

3/ DHCP Request

في هذه المرحلة يقوم هذا الجهاز بالرد علي المرحلة السابقة او مرحلة العرض بالموافقة للإنضمام لتلك الشبكة بتلك البيانات التي منحها لك سيرفر DHCP لذلك بعد ان يحصل الجهاز علي عنوان IP الذي مُنح له يقوم بإرسال الرد إلي سيرفر DHCP يخبره بإن وافق علي العرض الخاص به بعنوان IP وبالإعدادات الاخرى التي عرضت عليه .

4/DHCP Ack

تلك هي المرحلة الاخيرة والتي يتم فيها التأكيد من قبل جهاز المستخدم علي تعيين عنوان IP المخصص حيث يتم إرسال إشعار للتأكيد علي تلك البيانات إلي سيرفر DHCP وإذا كانت المعلومات صحيحة يتم إتصالك بالشبكة بشكل سليم وفي حالة فشل البيانات يقوم جهاز المستخدم بإعادة المراحل الاربع مرة اخري ليحصل علي عنوان IP وباقي المعلومات الخاصة بتلك الشبكة ليتم الإتصال .

https with google (layer 6 …. Presentation):

هيعرف ip الخاص ب google عن طريق DNS

هينشأ مفتاح عشان يتكلموا symmetric و يشفره باستخدام public key

Public key

request

server

server

Browser

Browser

Browser

server

Every packet has ..

|  |  |
| --- | --- |
| هو ip المصدر اللي packet طلعت من عنده عشان تروح للطرف التاني (server) | Source IP |
| بيكون عشوائي من ضمن 65535 ports | Source port |
| IP الخاص بال server اللي هوصله | Destination IP |
| لو أنا https هيكون 443 و لو http هيكون 80 | Destination port |

TCP:

عند ارسال packet لازم يتأكد من وصولها و ان لم لتصل يرسلها مرة اخرى (connection passed)

يتم ارسال الحزم بالترتيب

UDP :

أسرع من TCP لأنه لا يتحقق من وصول الحزم

يعمل غى ترجمة domain name إلى IP address

... ptr هو عملية عكسية لل dns

Known attacks:

1/ DNS poisoning :

يتم التلاعب بنظام DNS مثلا لو اردت تسجيل الدخول في موقع [www.yahoo.com](http://www.yahoo.com) يتم توجيهك لموقع تاني بيختاره ال attacker .

2/ DNS amplification attacks :

3/ DNS cache snooping :

DNS مقسم إلى zones كل zone بتكون privet

في DNS cache snooping بقدر اشوف كل DNS zone

Tools :-

1/ nslookup google.com

عشان أعرف IP موقع معين

2/ dnschef

بتسمح بتزييف DNS query

3/ dig

بتعمل search لكل records الخاصة ب domain معين سواء dns records or ms server

DNS records type

1/ A record

/// sub domain /// IP version 4

2/ AAAA

/// IP version 6

3/ MX

خاص ب mail server

4/ CNAME or Alias

بديل ل domain معين (بيفتح نفس محتواه)

5/ PTR

Takeover :-

هي ثغرة من نوع misconfiguration ل cname DNS records

EX:

لو شركة أنشئت subdomain له CNAME يشير مثلا ل (Heroku or github ) لكن مع مرور الوقت انتهت صلاحية CNAME بيسجل الهاكر عن طريق ال CNAME المنتهي كأنه اسم جديد و يقدر يتحكم بال Subdomain الخاص بالشركة

تستخدم لعمل scan لل ports و الحصول على تفاصيل اكثر و بتعرفك ايه ports المفتوحة على server اللي ممكن متكونش ظاهرة في الوضع العادي (بتفحص أشهر 1000 بورت)

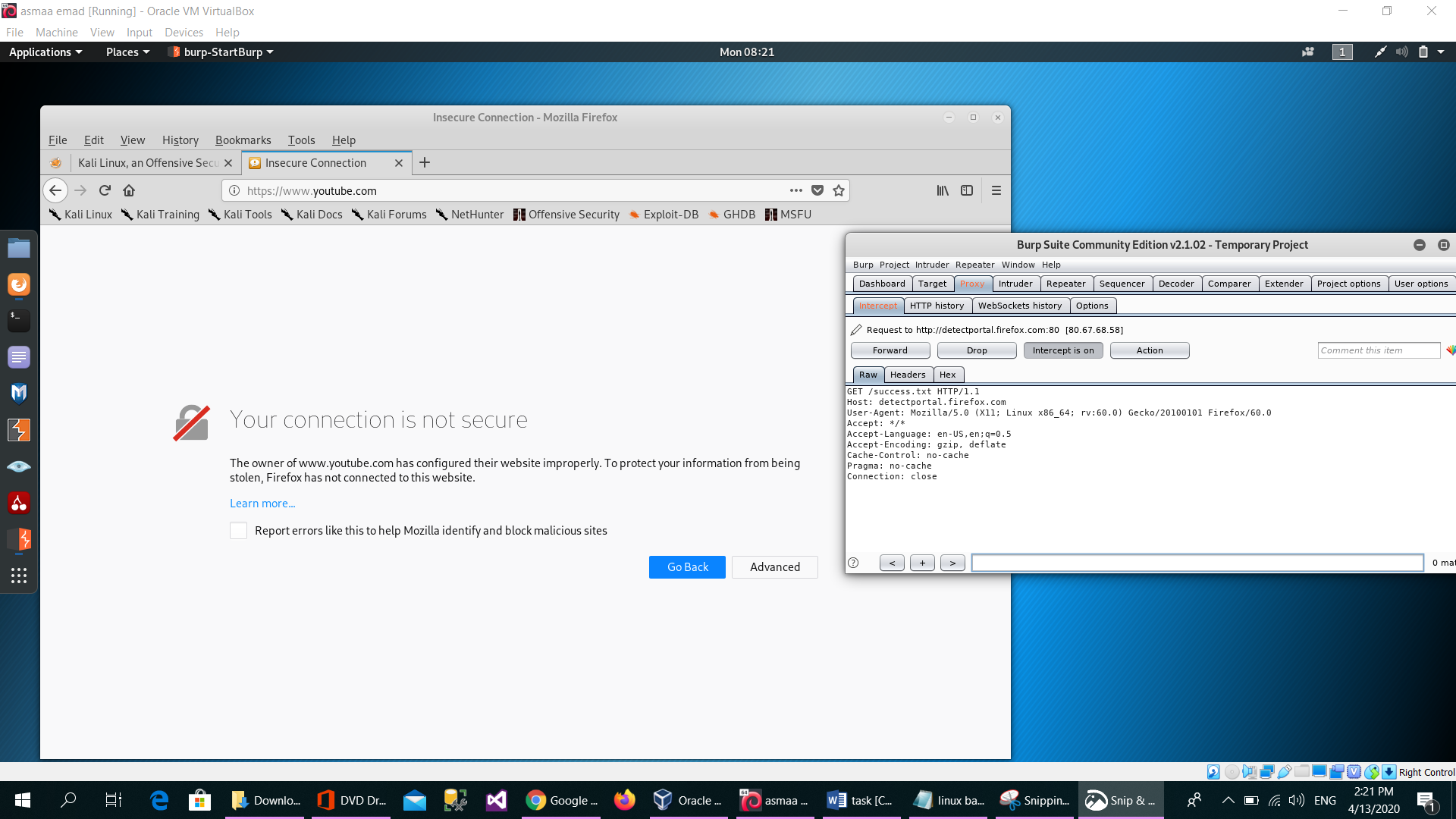
* أي خدمة بتشتغل على server لازم يكون ليها port عشان ال users يقدروا يوصلوا ليها على ال server

1/ يكون مفتوح و تقدر توصل ليه

2/ تكون الخدمة موجودة بس مقفولة

3/ يكون فيه firewall بيحجب الوصول ل port

|  |  |
| --- | --- |
| Help menu | 1/ -hh |
| UDP & TCP scan | 2/ -sU -sT |
| Scan specified ports | 3/ -p |
| TCP null scan | 4/ -sn |
| Input from list of networks | 5/ -iL |
| معرفة ال port يستخدم لأي خدمة | 6/ -A |
| Treat all hosts as online ….. skip host descovery | 7/ -Pn |
| Probe open ports to determine service | 8/ -sV |
| TSP SYN scan | 9/ -sS |
| Enable os detection | 10/ -o |
| Print version number | 11/ -v |
| Output scan in XML | 12/ -ox |
| Scan no most common ports | 13/ --top -port no |
| Show open ports | 14/ -open |
| Script scan | 15/ -sC |



<https://hackerone.com/reports/175070>

<https://0xpatrik.com/takeover-proofs/>

<https://hackerone.com/reports/172137>

<https://hackerone.com/reports/317005>

<https://hackerone.com/reports/779442>

<https://hackerone.com/reports/484420>

<https://hackerone.com/reports/202767>

<https://hackerone.com/reports/166826>

<https://hackerone.com/reports/407355>

<https://hackerone.com/reports/388622>

<https://hackerone.com/reports/365853>

<https://hackerone.com/reports/180393>

<https://forum.bugcrowd.com/t/need-help-azure-websites-subdomain-takeover/3870>

<https://blog.initd.sh/others-attacks/mis-configuration/subdomain-takeover-explained/>

<https://hackerone.com/reports/399165>

<https://www.hackerone.com/blog/Guide-Subdomain-Takeovers>