# ERRONKA:

**Er1-UD2-Barrido**

# Enuntziatua:

AEEAri txosten pare bat aurkeztu dizkiozu egindako lana justifikatzeko. Ez dira oso sakonak, baina erakundea nahiko pozik agertu da erakutsitakoarekin.   
Orain, behin ezagutza fasearekin bukatuta, zerrendatze fasearekin hasiko zara. Eta, hasteko, saiatu behar zara jakiten zeintzuk diren sarean dauden gailu guztiak. Bide sinpleenetik saiatuko zara lehenbizi.   
Scripta moldatu beharko duzu erabiltzaileak PING sweep edo ARP Sweep martxan jar dezan. Ondoren, mugarri bakoitzaren soluzioa bilatu beharko duzu.

# Mugarriak:

**Er1-UD2-Mug1: 9 puntu**

Hasteko, PING Sweep delakoa egingo duzu sare lokalean. Zein da agertutako bigarren makina aktiboaren IPa?

**Er1-UD2-Mug2: 11 puntu**

Oraingoan, ARP Sweep egingo duzu.   
Zein da agertutako makina berriaren IPa?   
  
Zergatik ez da IP hori agertu PING Sweepa egitean?  
A- Itzalita egon delako.   
B- Sare mailako konfiguraziorik ez duelako, helbide fisikoa soilik.   
C- Behintzat sarrerako ICMP trafikoa debekatuta daukalako Kali makinatik (gutxienez).   
D- Ausazkoa da. Batzuetan agertuko da eta beste batzuetan ez.   
E- ARP Sweep-a sudo-rekin exekutatu dugulako.   
  
ERANTZUNAREN FORMATUA: [Erantzun\_zuzenaren\_letra];[IPa]  
Adibidez: E;192.168.76.245

# Pistak:

**Er1-UD2-Pista2: -2 puntu**

if (funcion.lower() == "p"):  
  
else

**Er1-UD2-Pista1: -2 puntu**

for direccion\_ip in direccion\_red.hosts():

**Er1-UD2-Pista3: -8 puntu**

if respuesta == 0:  
 print(f"La dirección IP {direccion\_ip} está activa.")

#############################################################

# ERRONKA:

**Er2-UD2-Eskaneoak**

# Enuntziatua:

Aurreko urratsean ikusi dugunez, hainbat IP daude aktibo gure sarean; horietako batzuekin jolastu egin beharko duzu, ikusteko ea zerbitzuren bat eskuragarri utzi duten.   
Adi!! Administratzaile baimenekin exekutatu beharko duzu scripta.

# Mugarriak:

**Er2-UD2-Mug1: 7 puntu**

Zein da 21, 22 y 445 ataken egoera 192.168.1.160 IPdun makinan?  
Egin ezazu SYN Scan bat.   
  
ERANTZUNAREN FORMATUA: [21-egoera]; [22-egoera]; [445-egoera].   
Egoera:   
 Irekita: OP  
 Itxita: CL  
 Filtratua: FI  
 Ez-filtratua: NFI  
 Zehaztugabea: IN  
Adibidez: 21 ataka irekita badago, 22a itxita eta 445 filtratuta:   
 OP;CL;FI

**Er2-UD2-Mug2: 7 puntu**

Zein da 21, 22 y 445 ataken egoera 192.168.1.3 IPdun makinan?  
Egin ezazu ACK Scan bat.   
  
ERANTZUNAREN FORMATUA: [21-egoera]; [22-egoera]; [445-egoera].   
Egoera:   
 Irekita: OP  
 Itxita: CL  
 Filtratua: FI  
 Ez-filtratua: NFI  
Adibidez: 21 ataka irekita badago, 22a itxita eta 445 filtratuta:   
 OP;CL;FI

**Er2-UD2-Mug34: 7 puntu**

Zein da 21, 22 y 445 ataken egoera 192.168.1.4 IPdun makinan?  
Egin ezazu FIN Scan bat.   
  
ERANTZUNAREN FORMATUA: [21-egoera]; [22-egoera]; [445-egoera].   
Egoera:   
 Irekita: OP  
 Itxita: CL  
 Filtratuta: FI  
 Ez-filtratuta: NFI  
 Zehaztugabea: IN  
Adibidez: 21 ataka irekita badago, 22a itxita eta 445 filtratuta:   
 OP;CL;FI

**Er2-UD2-Mug4: 9 puntu**

Beheko testari erantzuteko, egindakoez gain, egin itzazu 192.168.1.3, 192.168.1.4 eta 192.168.1.7 IPen kontrako TCP eskaneoak.   
  
1) 192.168.1.3 IPari dagokionez:  
 a) 21 ataka filtratuta dago; 22 atakan zerbitzu bat dago, eta eskuragarri dugu; 80 eta 445 ataketan ez dago zerbitzurik;   
 b) 21 atakan zerbitzu bat dago, eta eskuragarri dugu; 22 ataka filtratuta dago; 80 eta 445 ataketan ez dago zerbitzurik.   
 c) 21 eta 22 ataketan ez dago zerbitzurik; 80 eta 445 ataketan, ezin da jakin.   
 d) 22 atakan zerbitzu bat dago, eta eskuragarri dugu; 21 eta 80 ataketan ez dago zerbitzurik; 445 ataka filtratuta dago.   
  
2) 192.168.1.4 IPari dagokionez:  
 a) 21 ataka filtratuta dago; 22 atakan zerbitzu bat dago, eta eskuragarri dugu; 80 eta 445 ataketan ez dago zerbitzurik;   
 b) 21 eta 80 ataketan zerbitzu bana dago, eta eskuragarri ditugu; 22 ataka filtratuta dago; 445 atakan ez dago zerbitzurik.   
 c) 21 eta 22 ataketan ez dago zerbitzurik; 80 eta 445 ataketan, ezin da jakin.   
 d) 22 atakan zerbitzu bat dago, eta eskuragarri dugu; 21 eta 80 ataketan ez dago zerbitzurik; 445 ataka filtratuta dago.   
  
3) 192.168.1.7 IPari dagokionez:  
 a) 21 ataka filtratuta dago; 22 atakan zerbitzu bat dago, eta eskuragarri dugu; 80 eta 445 ataketan ez dago zerbitzurik;   
 b) 21 atakan zerbitzu bat dago, eta eskuragarri dugu; 22 ataka filtratuta dago; 80 eta 445 ataketan ez dago zerbitzurik.   
 c) 21 eta 22 ataketan ez dago zerbitzurik; 80 eta 445 ataketan, ezin da jakin.   
 d) 21 eta 445 ataketan ez dago zerbitzurik; 22 atakan zerbitzu bat dago, eta eskuragarri dugu; 80 ataka filtratuta dago.   
  
ERANTZUNAREN FORMATUA: [1erantzun\_zuzena];[2erantzun\_zuzena][3erantzun\_zuzena]  
Adibidez: erantzun zuzenak 1b, 2c eta 3d badira:  
 b;c;d

# Pistak:

**Er2-UD2-Pista-Mug1-2-3: -9 puntu**

#\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
 #VALOR FLAGS. DECIMAL Y HEXADECIMAL\*  
 #FIN: Decimal: 1 Hexadecimal: 0x01 \*  
 #SYN: Decimal: 2 Hexadecimal: 0x02 \*  
 #RST: Decimal: 4 Hexadecimal: 0x04 \*  
 #PSH: Decimal: 8 Hexadecimal: 0x08 \*  
 #ACK: Decimal: 16 Hexadecimal: 0x10 \*  
 #URG: Decimal: 32 Hexadecimal: 0x20 \*  
 #\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
Adibidea: Flag PSH/ACK = 0x18

**Er2-UD2-Pista-Test: -7 puntu**

IP bakoitzeko:  
Egin SYN Scan bat jakiteko zein ataka dauden irekita.   
Jarraian, egin ACK Scan bat jakiteko itxita agertu direnak filtratuta dauden edo ez. Baldin badaude, firewall bat ataka horretaranzko trafikoa filtratzen egongo da; bestela, ondoriozta dezakegu ataka horretan ez dagoela zerbitzurik martxan.

#############################################################

# ERRONKA:

**Er3-UD2-Eskaneoak**

# Enuntziatua:

Gailu jakin batzuei buruzko informazio oso garrantzitsua lortu duzu, eta batzuek aurretik firewall bat badutela ere badakizu.   
Orain, proba askoz luzeagoari ekingo diozu, sare oso batean, helbidez-helbide, irekita edo itxita dauden zerbitzu guztiak ezagutu nahian.   
NMAP tresna ospetsua erabiliko duzu. Animo!

# Mugarriak:

**Er3-UD2-Mug1: 10 puntu**

192.168.1.0/24 sareko eskaneoa egin 21-80 ataka-tartean. Zein da 80 ataka irekita agertzen den IP baxuena?  
Erabili Er3\_UD2\_NMAP\_Atakak.py scripta.

**Er3-UD2-Mug2: 10 puntu**

192.168.1.0/24 sareko eskaneoa egin 20,21,22,53,80,443 eta 502 atakentzat. Zein dira 192.168.1.200 IParen ataka itxiak?  
Erabili Er3\_UD2\_NMAP\_Atakak.py scripta.  
ERANTZUNAREN FORMATUA: [ataka\_itxia1][ataka\_itxia2][ataka\_itxia3]  
Adibidez: 22,53,80

**Er3-UD2-Mug3: 10 puntu**

Lortu 22 eta 80 atakei lotutako ahuleziak 192.168.1.0/24 sarean. Zein da 192.168.1.200 IPdun gailuaren 22 atakako ahulezietatik larritasun handiena duena?   
EMAITZAREN FORMATUA: CVE-xxxx-yyyy  
Adibidez: CVE-2019-8743

# Pistak:

**Er3-UD2-Mug3-Pista1: -2 puntu**

nm=nmap.PortScanner()

**Er3-UD2-Mug3-Pista2: -4 puntu**

estructuraNmap=formateoNmapScan(????)  
......  
for puertoOpen in host.puertosAbiertos:  
  
**Er3-UD2-Mug1-2-Pista1: -4 puntu**

nm = nmap.PortScanner()  
 nm.scan(destino, puertos\_destino, arguments="-sV -n -T5")

**Er3-UD2-Mug1-2-Pista2: -8 puntu**

for host in estructuraNmap:  
 print("Host: "+ host.host)  
 if (funcion.lower() == "a"):  
 print ("Listado de puertos abiertos:")  
 for puertoOpen in host.puertosAbiertos:   
 #Imprimimos el puerto, nombre del servicio y la versión   
 else:  
 print ("Listado de puertos cerrados:")  
 for puertoClosed in host.puertosCerradosFiltrados:   
 #Imprimimos el puerto, nombre del servicio y la versión

# ERRONKA:

**Er4-UD2-Enum4Linux**

# Enuntziatua:

Orain arte ikusitakoaren ondoren, ematen du 192.168.1.200 IPan gozoki bat daukagula. Gai izango zara sistema horren datu esanguratsuren bat lortzeko?

# Mugarriak:

**Er4-UD2-Mug1: 4 puntu**

Zein da 192.168.1.200 IPdun makinaren pasahitz-politikaren konplexutasuna?  
Sartu hitz bat soluzio gisa.

**Er4-UD2-Mug2: 4 puntu**

Zein da Samba bertsioa?  
ERANTZUNAREN FORMATUA: n.n.nn  
Adibidez: 2.0.21

**Er4-UD2-Mug3: 12 puntu**

Gorde 192.168.1.200 IPdun makinako erabiltzaile guztien zerrenda fitxategi batean.   
Zein da 1. erabiltzailea?

# Pistak:

**Er4-UD2-Mug1-Pista1: -1 puntu**

XXXXXX= stdout\_texto

**Er4-UD2-Mug1-Pista2: -2 puntu**

print (informacion\_complejidad)

**Er4-UD2-Mug2-Pista1: -1 puntu**

if not hay\_info\_so:  
 print ("No se ha encontrado información sobre el sistema operativo")

**Er4-UD2-Mug2-Pista2: -2 puntu**

print (sistema\_operativo)

**Er4-UD2-Mug3-Pista1: -2 puntu**

stdout\_texto = subprocess.check\_output(["enum4linux", "-a", direccion], text=True)

**Er4-UD2-Mug3-Pista2: -2 puntu**

nombres\_usuario = re.findall(r'user:\[(\w+)\] rid:', stdout\_texto)

**Er4-UD2-Mug3-Pista3: -5 puntu**

archivo\_resultados = open("resultados\_usuarios.txt", "w")  
 archivo\_resultados.write("NOMBRES DE USUARIO:\n")  
 for nombre\_usuario in nombres\_usuario:  
 archivo\_resultados.write(nombre\_usuario + "\n")