Open-Sec

Real Pentesting / Real Red Teaming

Hacking Ético
level 1

Sesión 1
Conceptos e Infraestructura

Conceptos Básicos

Pentesting y metodologías

Diferenciando...

Ethical Hacking

Análisis de vulnerabilidades
(Automatizado)

Pruebas de Penetración / PenTest

Infraestructura:
- Sistema Operativo
- Software base
  - Web
  - VPN
  - Clientes delegados
  - Recursos compartidos
  - Directorios (AD)
  - Protocolos Inseguros
  - Interfaces expuestas

Completa:
Se busca un Vector de Ataque exitoso en servicio expuesto y se realiza la penetración a nivel de red.

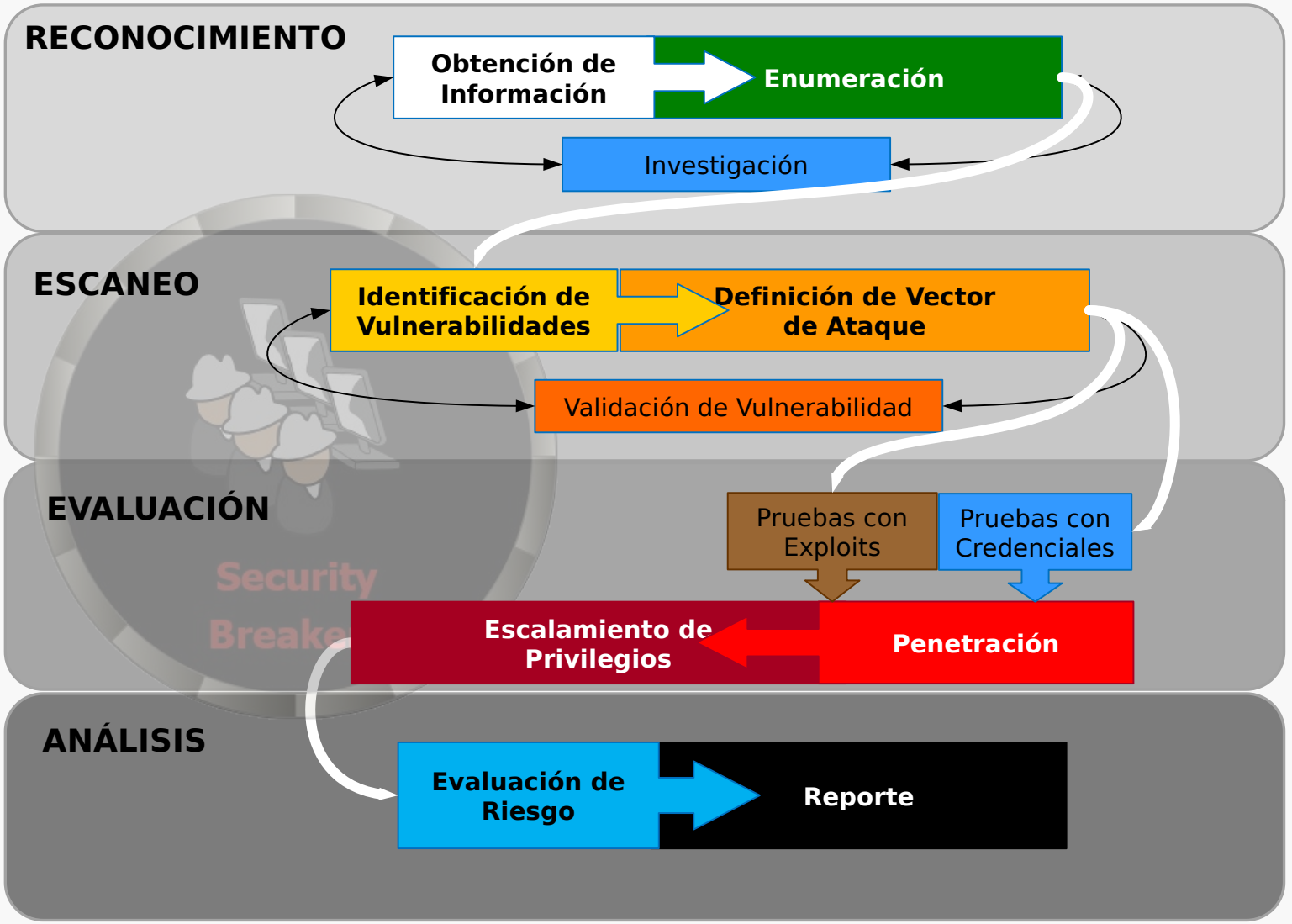
Extendida:
Se buscan Vectores de Ataque por cada uno de los servicios expuestos y se explotan todos los posibles. Se realiza la penetración a nivel de red por cada Vector de Ataque exitoso.

Aplicaciones Web:
- Sin credenciales
- Con credenciales
- DAST o SAST (los más comúnes)

Otros :
- Ingeniería social.
- Pruebas de intrusión física
- Switches Transaccionales
- Autorizadores
- Cajeros automáticos
- POS's
- Ticketeras

RED TEAM
- **Reconocimiento**
- **Compromiso Inicial**
- **Desplazamiento Lateral**
- **Establecimiento de un Centro de Comando y Control (C2)**
- **Persistencia**
- **Exfiltración**
- **Mayor tiempo de ejecución que un *pentest* o *ethical hacking*.**

Anatomía de un Pentest



Términos comunes

- Blackbox
- Graybox
- Whitebox
- DAST
- SAST
- Externo
- Interno

Términos comunes

- Confidencialidad
- Disponibilidad
- Integridad
- Autenticidad
- Trazabilidad

Términos comunes

- Cracker
- Lammer
- Script kiddie
- Hacktivistas
- Hacker ?
- Pentester
- Red Teamer / Operator

Bug Bounty

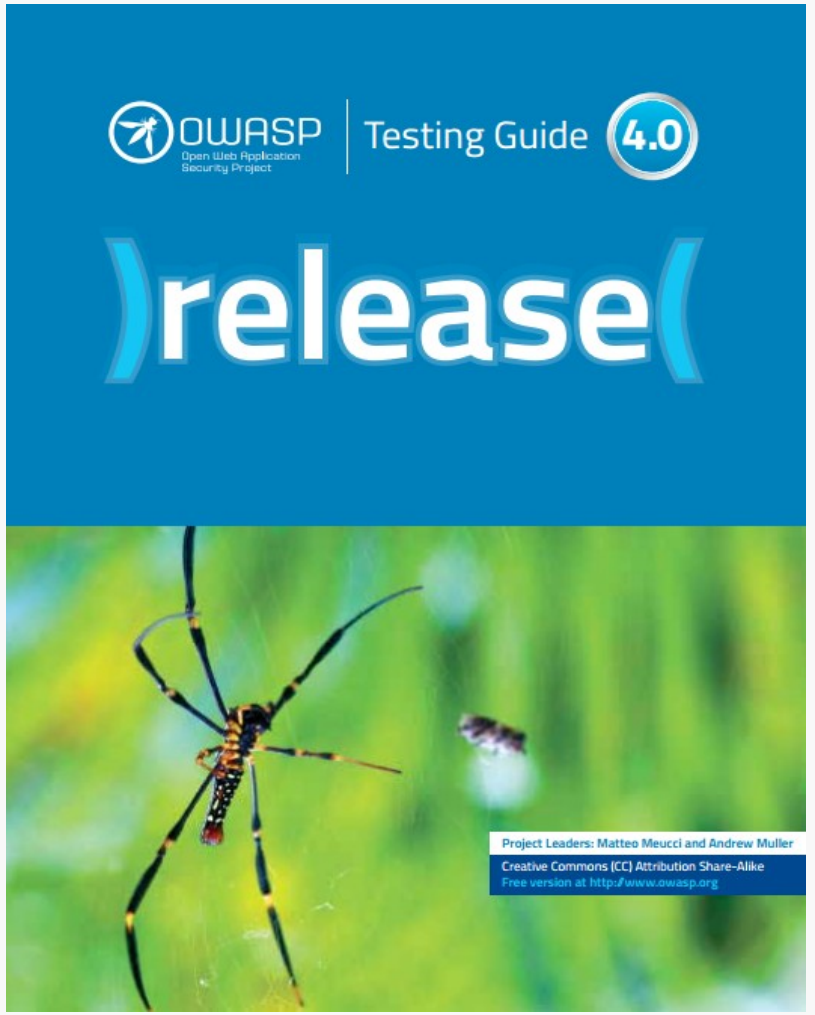
- Recompensas por encontrar vulnerabilidades o errores.
- Generalmente orientado a las aplicaciones
- Un programa de recompensas puede ser solicitado por los mismos fabricantes (Facebook, Google, Microsoft, etc.) o administrados por terceros (HackerOne, BugCrowd, OpenBugBounty, AntiHack.me)
- Las recompensas van desde USD 20.00 hasta cantidades diversas que pueden rondar los cientos de miles de Dólares (según publican en redes sociales).

Penteting as a Service (PTaaS)

- PTaaS es un modelo de Pentesting de evaluación de aplicaciones o infraestructura que provee visibilidad continua de los hallazgos bajo plataformas de gestión donde el cliente puede revisar durante y después del periodo contratado.
- El alcance del servicio está en función de costos mensuales o anuales y no por activos a evaluar.
- Informes en “tiempo real”

Metodologías de Pentesting y normativas

ISECOM



PCI Security Standards Council

Infraestructura

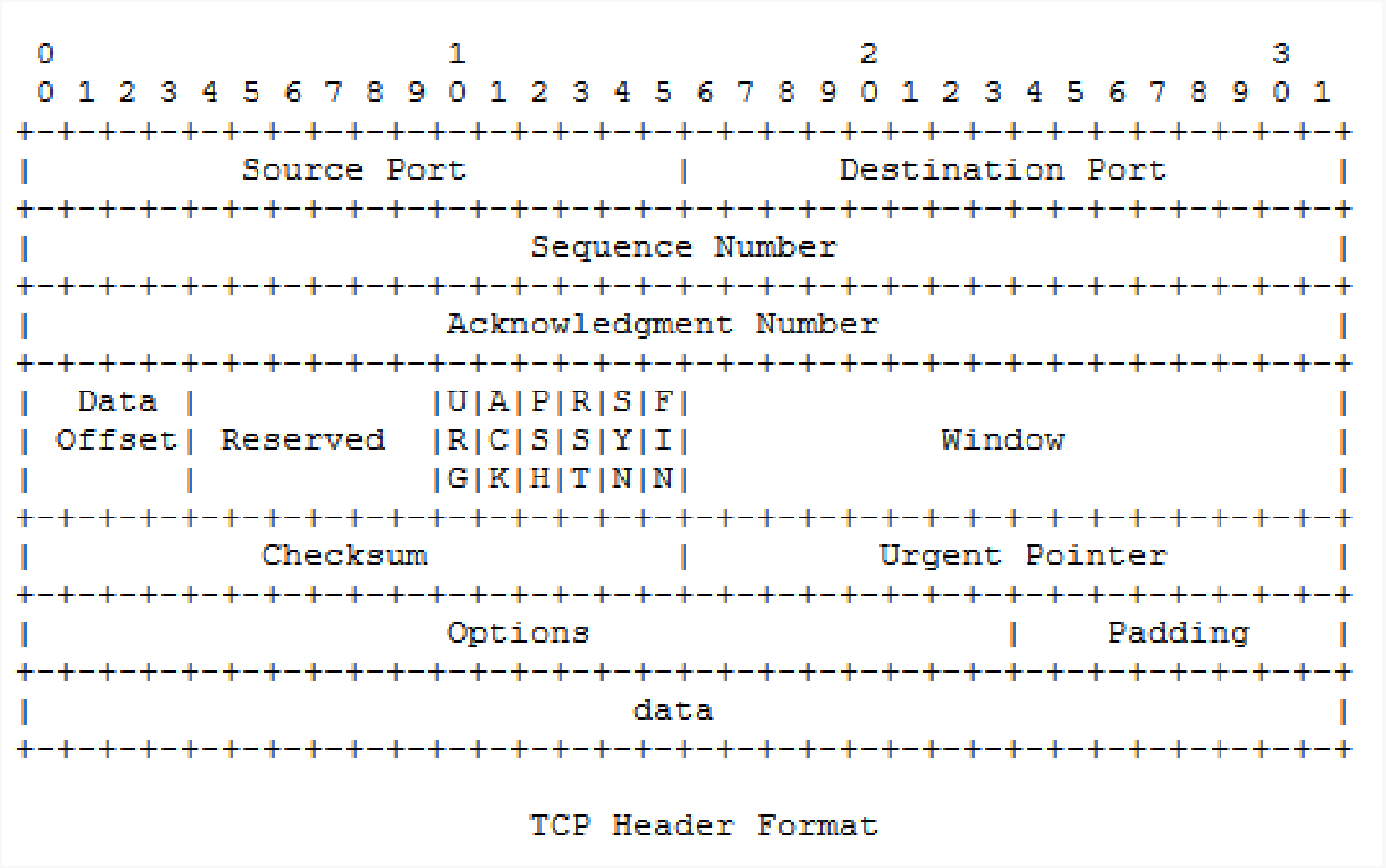
Conceptos básicos del modelo TCP/IP

Conceptos básicos de TCP/IP

APLICACIÓN	HTTP, FTP, SMTP, SNMP, DNS
TRANSPORTE	TCP, UDP
INTERNET	IP, ICMP
ACCESO A RED	ETHERNET, PPP, DHLC, ARP

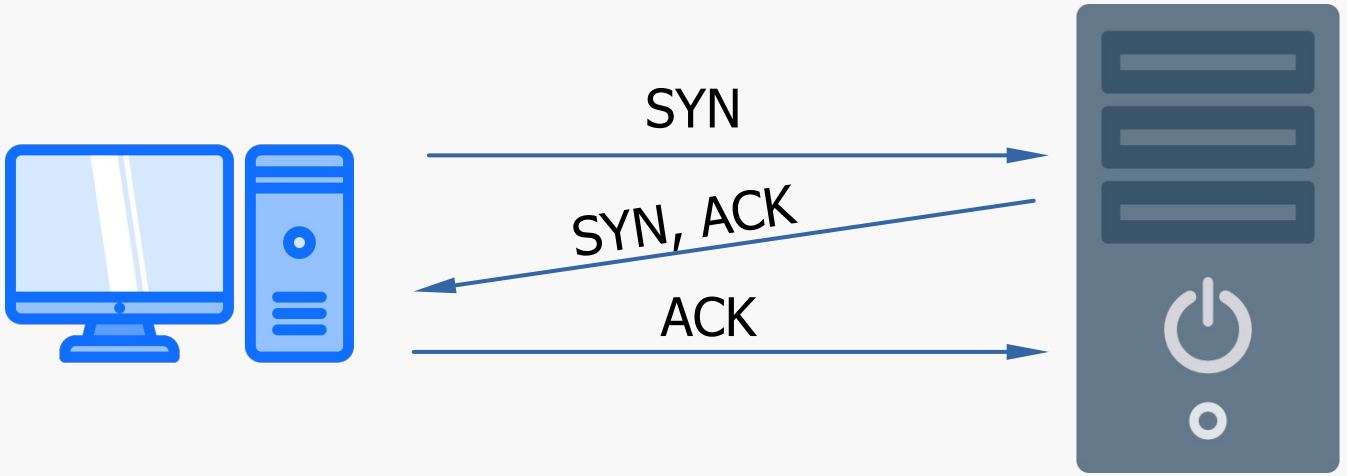
Protocolo TCP

- Protocolo confiable.
- Orientado a conexión.
- Control de flujo.
- Segmentación y reenvío



Fuente: RFC 793 (https://tools.ietf.org/html/rfc793)

Handshake TCP

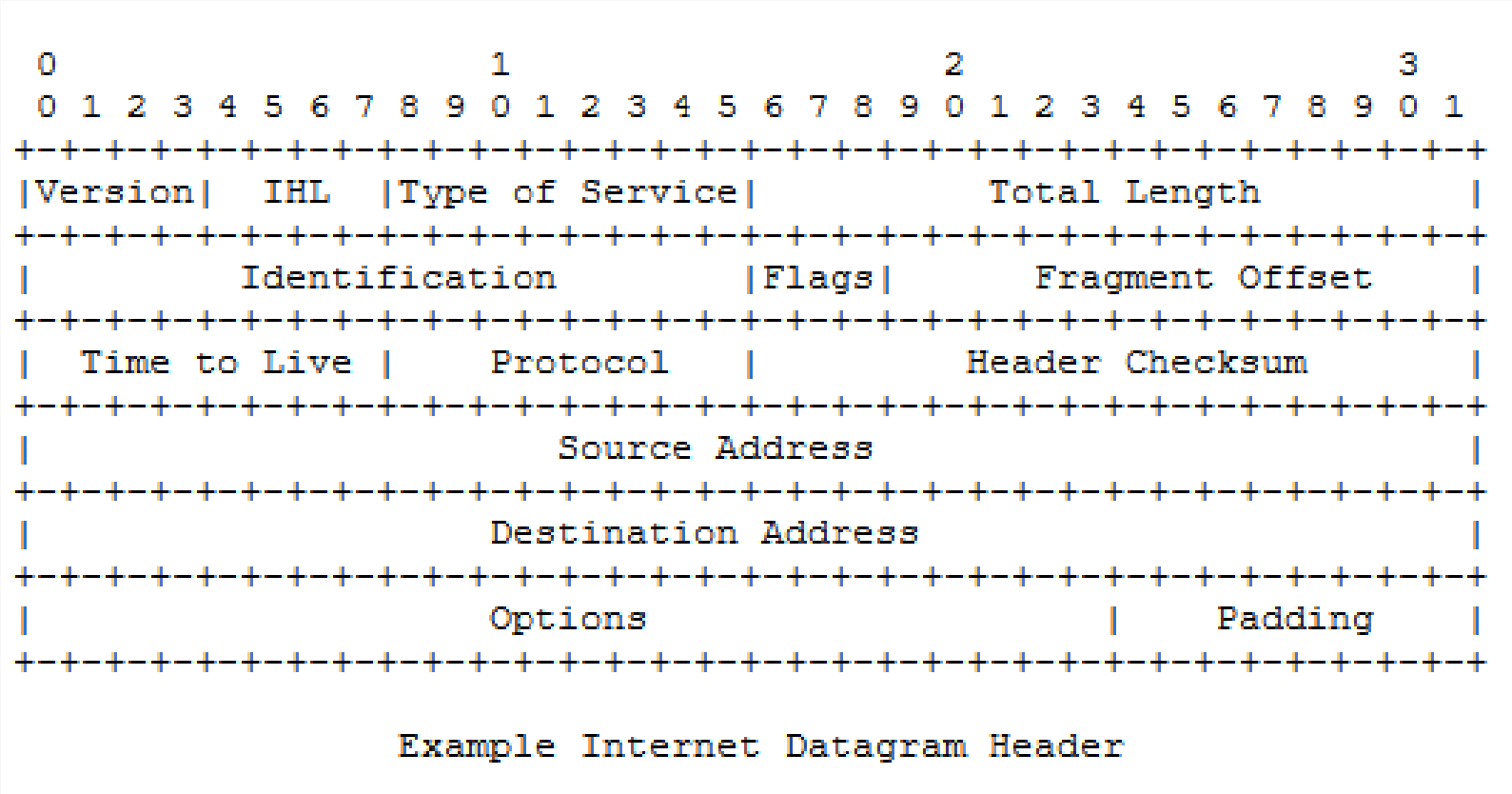


Recordar :

- Si no hay respuesta, debe estar filtrado.
- Si está cerrado, responde con RST+ACK.

Protocolo IP

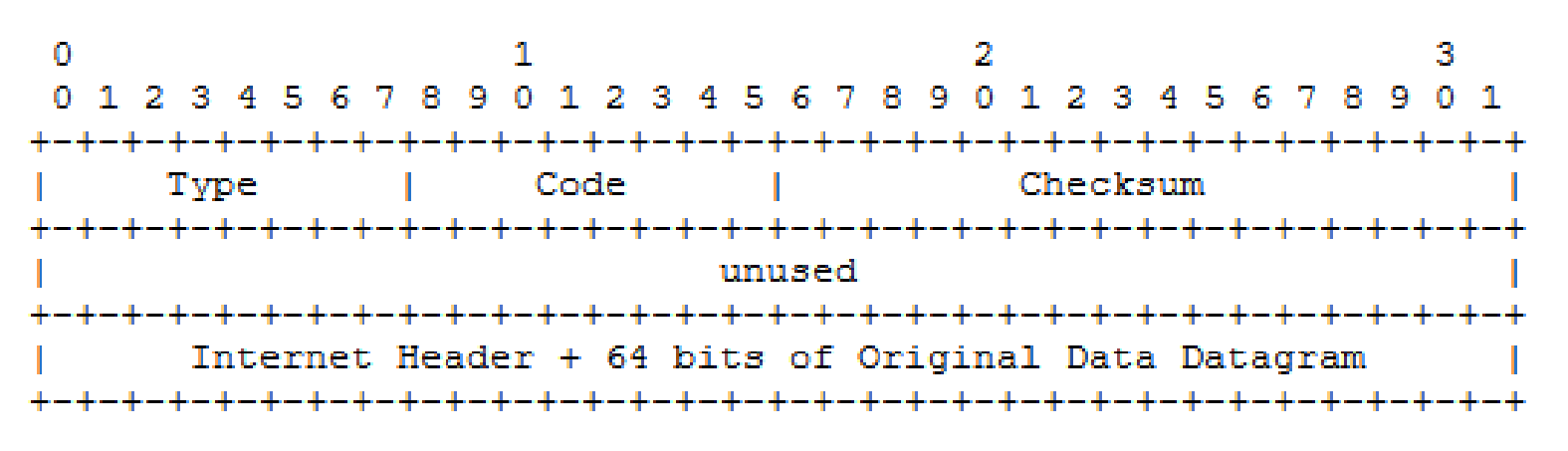
- Protocolo de máximo esfuerzo.
- No orientado a conexión.



Fuente: RFC 791 (https://tools.ietf.org/html/rfc791)

Protocolo ICMP

- Utilizado para la verificación de conectividad de host a host.
- Utilizado para informar de errores en el entorno de comunicación.



Protocolo ICMP

Tipo	Código	Función
0/8	0	Echo/Echo Reply
3	0-5	Destino inalcanzable (Destination Unreachable)
4	0	Source Quench
5	0-3	Redirección (Redirect)
11	0-1	Tiempo excedido (Time Exceeded)
12	0	Problema de parámetro (Parameter Problem)
13/14	0	Timestamp/Timestamp Reply

Fuente: RFC 792 (https://tools.ietf.org/html/rfc792)

Infraestructura

Linux orientado al Pentesting

Para que sirve saber manejar Linux y MS Windows desde la Línea de Comandos (CLI)

- El pentester en el mundo real usa Linux y pocas veces sus herramientas tienen una GUI
- El primer acceso a un sistema a nivel de infraestructura es mediante ejecución de comandos
- El pentester debe aceptar que puede ser vulnerado y por ello debe poder analizar su entorno constantemente
- El pentester encontrará targets basados en Linux (muchas variantes) y MS Windows (de haber éxito, TAL VEZ, pueda usar RDP luego de la penetración inicial.

Uso de Linux orientado al Pentesting

Revisar configuración básica :

- ifconfig
- route -n
- cat /etc/resolv.conf

```
[redacted]$ ifconfig
eth0      Link encap:Ethernet  HWaddr e8:9a:8f:9c:07:ac
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:40

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:32 errors:0 dropped:0 overruns:0 frame:0
          TX packets:32 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1880 (1.8 KB)  TX bytes:1880 (1.8 KB)

wlan0     Link encap:Ethernet  HWaddr 74:e5:0b:0c:65:88
          inet addr:192.168.1.170  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::76e5:bff:fe0c:6588/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:61198 errors:0 dropped:0 overruns:0 frame:0
          TX packets:59467 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:55840784 (55.8 MB)  TX bytes:15082545 (15.0 MB)
```

```
[redacted]; route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
192.168.1.0     0.0.0.0         255.255.255.0   U     2      0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0
[redacted]$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Configuración de Red

- **Configurar interfaz de red**

  `ifconfig interfaz direccion_ip netmask mascara`

  Ejemplo : `ifconfig eth0 192.168.1.120`

- **Configurar router default**

  `route add default gw ip_router`

  Ejemplo : `route add default gw 192.168.1.1`

- **Configurar servidores DNS**

  Editar el /etc/resolv.conf y colocar

  nameserver ip_DNS_1

  nameserver ip_DNS_2

Procesos

- ps
- top

```
root@kali2019:~# ps
  PID TTY          TIME CMD
 1435 pts/0    00:00:00 bash
 1458 pts/0    00:00:00 ps
```

```
root@kali2019:~# top

top - 13:48:18 up 5 min,  1 user,  load average: 0,14, 0,42, 0,23
Tasks: 178 total,   2 running, 176 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0,8 us,  0,3 sy,  0,0 ni, 98,8 id,  0,0 wa,  0,0 hi,  0,0 si,  0,0 st
MiB Mem :   3946,6 total,   2857,6 free,    693,2 used,    395,8 buff/cache
MiB Swap:   3069,0 total,   3069,0 free,      0,0 used.   3024,3 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  982 root      20   0  363052  56964  38184 S   0,7   1,4   0:04.38 Xorg
 1074 root      20   0  164484   2740   2252 S   0,7   0,1   0:00.47 VBoxClient
 1459 root      20   0    9108   3668   3220 R   0,7   0,1   0:00.67 top
   30 root      20   0       0      0      0 I   0,3   0,0   0:00.29 kworker/1+
 1125 root      20   0 3312616 297944 113028 S   0,3   7,4   0:20.94 gnome-she+
 1428 root      20   0  474272  43920  33696 S   0,3   1,1   0:02.19 gnome-ter+
    1 root      20   0  100912  10256   7852 S   0,0   0,3   0:05.80 systemd
    2 root      20   0       0      0      0 S   0,0   0,0   0:00.00 kthreadd
    3 root       0 -20       0      0      0 I   0,0   0,0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I   0,0   0,0   0:00.00 rcu_par_gp
    5 root      20   0       0      0      0 I   0,0   0,0   0:00.00 kworker/0+
    6 root       0 -20       0      0      0 I   0,0   0,0   0:00.00 kworker/0+
    7 root      20   0       0      0      0 I   0,0   0,0   0:00.04 kworker/0+
    8 root      20   0       0      0      0 I   0,0   0,0   0:00.06 kworker/u+
```

Conexiones de Red

Ver estado de conexiones de red

- `netstat -nap | more`
- `netstat -nap | grep nombre_servicio`

Ejemplo: `netstat -nap | grep firefox`

```
root@kali2019:~# netstat -nap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      1/init
tcp6       0      0 :::111                  :::*                    LISTEN      1/init
udp        0      0 192.168.1.68:68         0.0.0.0:*                           497/NetworkManager
udp        0      0 0.0.0.0:111             0.0.0.0:*                           1/init
udp6       0      0 :::111                  :::*                                1/init
raw6       0      0 :::58                   :::*                    7           497/NetworkManager
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ]         DGRAM                    11776    1/init               /run/systemd/journal/s
yslog
unix  2      [ ACC ]     STREAM     LISTENING     11781    1/init               /run/systemd/journal/s
tdout
unix  7      [ ]         DGRAM                    11784    1/init               /run/systemd/journal/s
ocket
unix  2      [ ACC ]     STREAM     LISTENING     11802    1/init               /run/systemd/fsck.prog
ress
```

Tabla de enrutamiento

Ver tabla de enrutamiento

- `route -n`

```
root@kali2019:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    100    0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

Scripting bash

¿Que es un script?

- Un tipo de programa o código fuente.
- Se ejecuta por un intérprete.

Script Bash

- En Linux suelen estar identificados por el encabezado "**shebang**" (#!/bin/bash).
- La extensión que se usa es **.sh**

```
wcuestas@[redacted]:~$ cat tecsup.sh
ifconfig eth1 [redacted]
route add default gw [redacted]
cp /etc/resolv.conf /root/resolv.conf.antestecsup
echo "nameserver [redacted]" > /etc/resolv.conf
echo "nameserver [redacted]" >> /etc/resolv.conf
```

Ejemplo de Script Bash

```
#!/bin/bash
fping -g $1 $2 > fping_lista.txt 2>/dev/null
grep "is alive" fping_lista.txt > activos.txt
echo "Lista de Direcciones IP Activas"
echo "------------------------------"
for host in `cat activos.txt | cut -d " " -f 1`
    do
        echo $host
    done
arp -an | grep ether | cut -d " " -f 2,4,7
```

```
root@kali2019:~/tools# bash portscan.sh 192.168.1.0 192.168
Lista de Direcciones IP Activas
------------------------------
192.168.1.2
192.168.1.1
192.168.1.34
192.168.1.68
192.168.1.88
192.168.1.100
(192.168.1.1) 1c:b0:44:f6:f4:7b eth0
(192.168.1.88) 04:d3:95:62:f4:ee eth0
(192.168.1.34) 3c:07:71:09:55:a7 eth0
(192.168.1.2) 58:6d:8f:ec:2a:be eth0
(192.168.1.100) 08:62:66:4c:7f:b3 eth0
```

Ejemplo de Script Bash – analizando...

fping -g $1 $2 > fping_lista.txt 2>/dev/null

Salida y Error Estándar :

0 Entrada

1 Salida

2 Error

Parámetros :

$0 el programa mismo

Los demás, del $1 en adelante

Ejemplo de Script Bash – analizando...

for host in `cat activos.txt | cut -d " " -f 1`

- **for** basado en una lista
- La lista se construye a partir de las entradas de un archivo, en este caso...
- Fijarse en las tildes invertidas `
  - Se ejecuta todo lo que esta dentro de las tildes invertidas
  - Eso devuelve la lista que requiere el **for**

Otra mas con Linux

Se acaba de penetrar un host Linux y se ve que es posible alcanzar otros hosts de la red.

- ¿Se desea escanear puertos ?
  - ¿Instalamos nmap ?
  - ¿Podemos usar echo?
  - Podemos mandarlo con msf !

Pero podemos hacer nuestro propio script, así que veamos cómo.

Loop While + /dev/tcp = portscanner.sh

```
#!/bin/bash
port=1
echo "Puertos abiertos en $1" > $2
echo "================================" >>
$2
while [ $port -le 1024 ]
do
    (echo > /dev/tcp/$1/$port) 2>/dev/null
    if [ $? = 0 ]
    then
        echo "El puerto $port esta abierto" >> $2
    fi
    port=`expr $port + 1`
done
```

Forma de ejecución:
bash ./portscanner.sh direccion_ip nombre_reporte

Loop While + /dev/tcp = portscanner.sh

while [$port -le 1024]

- Loop basado expresión y comparación numérica
- -le --> menor o igual

Loop While + /dev/tcp = portscanner.sh

```
(echo > /dev/tcp/$1/$port) 2>/dev/null
    if [ $? = 0 ]
    then
            echo "El puerto $port esta abierto" >> $2
    fi
    port=`expr $port + 1`
```

- **/dev/tcp** ---> pseudo-dispositivo para networking que bash los usa como cualquier otro dispositivo (device). Pseudo-device --> no existe dispositivo como tal
- El mensaje de error que se puede producir por un puerto cerrado aparece en línea, no se puede redireccionar como stdout ni como stderr, PERO, se puede invocar un subshell y dejar "limpio" el stdout.
- **expr** evalua y ejecuta expresiones : contador

Algunos comandos mas...

- cut → columnas
- grep → filas
- sort → ordenar
- sed → buscar y buscar/reemplazar
- cat
- chmod
- mount/umount
- sudo

Infraestructura

Windows orientado al Pentesting

Uso de Windows para Pentesting

- Revisar configuración de red.
- Uso de CMD
- Conexiones y tabla de enrutamiento

```
C:\Users\test>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : testlab2
   Primary Dns Suffix  . . . . . . . : redteam.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : redteam.com

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-13-66-42
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d79:2d46:4575:72e%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.66(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 101187623
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-0E-12-66-08-00-27-13-66-42
   DNS Servers . . . . . . . . . . . : 192.168.1.200
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Configuración de Red

- **Configurar Interfaz de red**

  netsh interface ip set address name="Local Area Connection" static 192.168.1.20 255.255.255.0 192.168.1.1

- **Configurar Interfaz para DHCP**

  netsh interface ip set address "Local Area Connection" dhcp

- **Configurar servidor DNS:**

  netsh interface ip set dns "Local Area Connection" static 200.48.225.130

  netsh interface ip ADD dns "Local Area Connection" 8.8.8.8 Index=2

- **Configurar Interfaz para DNS por DHCP**

  netsh interface ip set dns "Local Area Connection" dhcp

Procesos

- **TaskList**

  C:\>tasklist

- **TaskKill**

  C:\>taskkill /PID

```
C:\Users>tasklist /V /FO LIST

Image Name:   System Idle Process
PID:          0
Session Name: Services
Session#:     0
Mem Usage:    4 K
Status:       Unknown
User Name:    NT AUTHORITY\SYSTEM
CPU Time:     0:43:03
Window Title: N/A

Image Name:   System
PID:          4
Session Name: Services
Session#:     0
Mem Usage:    1,692 K
Status:       Unknown
User Name:    N/A
```

```
C:\Users>taskkill /PID 1196
SUCCESS: Sent termination signal to the process with PID 1196.

C:\Users>
```

```
C:\Users>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          4 K
System                           4 Services                   0      1,696 K
smss.exe                       256 Services                   0        332 K
csrss.exe                      332 Services                   0      1,440 K
wininit.exe                    396 Services                   0        584 K
csrss.exe                      404 Console                    1      1,668 K
winlogon.exe                   452 Console                    1      3,688 K
services.exe                   476 Services                   0      4,032 K
lsass.exe                      484 Services                   0      8,592 K
svchost.exe                    564 Services                   0     10,992 K
svchost.exe                    612 Services                   0      5,316 K
dwm.exe                        716 Console                    1     42,264 K
svchost.exe                    828 Services                   0     15,160 K
svchost.exe                    852 Services                   0     30,704 K
svchost.exe                    868 Services                   0     17,448 K
svchost.exe                    876 Services                   0     14,200 K
svchost.exe                    908 Services                   0      6,336 K
svchost.exe                    924 Services                   0     57,424 K
VBoxService.exe               1000 Services                   0      3,184 K
svchost.exe                   1048 Services                   0     21,568 K
spoolsv.exe                   1324 Services                   0      5,748 K
svchost.exe                   1604 Services                   0     10,608 K
dasHost.exe                   1616 Services                   0      8,568 K
diskpls.exe                   1652 Services                   0      3,232 K
diskbss.exe                   1676 Services                   0      4,440 K
FileZilla Server.exe          1772 Services                   0      5,676 K
svchost.exe                   1788 Services                   0      3,096 K
```

Tabla de enrutamiento

- Route PRINT
- Se pueden agregar rutas manualmente

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.97     11
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      169.254.0.0      255.255.0.0         On-link    169.254.55.216    266
   169.254.55.216  255.255.255.255         On-link    169.254.55.216    266
  169.254.255.255  255.255.255.255         On-link    169.254.55.216    266
      192.168.1.0    255.255.255.0         On-link     192.168.1.97    266
     192.168.1.97  255.255.255.255         On-link     192.168.1.97    266
    192.168.1.255  255.255.255.255         On-link     192.168.1.97    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.1.97    266
        224.0.0.0        240.0.0.0         On-link    169.254.55.216    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.1.97    266
  255.255.255.255  255.255.255.255         On-link    169.254.55.216    266
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0      192.168.1.1       1
===========================================================================
```

Conexiones de red

- Netstat –nao
- Netstat –s –p [tcp/udp/ip/icmp]

```
C:\Users\Fenix>netstat -nao

Conexiones activas

  Proto  Dirección local          Dirección remota        Estado           PID
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING       4192
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1092
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1536           0.0.0.0:0              LISTENING       852
  TCP    0.0.0.0:1537           0.0.0.0:0              LISTENING       788
  TCP    0.0.0.0:1538           0.0.0.0:0              LISTENING       1672
  TCP    0.0.0.0:1539           0.0.0.0:0              LISTENING       2340
  TCP    0.0.0.0:1540           0.0.0.0:0              LISTENING       2504
  TCP    0.0.0.0:1541           0.0.0.0:0              LISTENING       3404
  TCP    0.0.0.0:1543           0.0.0.0:0              LISTENING       844
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       4596
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       1288
  TCP    0.0.0.0:17500          0.0.0.0:0              LISTENING       8480
  TCP    127.0.0.1:843          0.0.0.0:0              LISTENING       8480
  TCP    127.0.0.1:1001         0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:1146         127.0.0.1:1147         ESTABLISHED     2464
  TCP    127.0.0.1:1147         127.0.0.1:1146         ESTABLISHED     2464
```

Scripting Batch

Loop for + ftp => port_ scanner.bat

@echo off

for /L %%p in (20,1,82) do echo Chequeando Puerto %%p: >> puertos.txt & echo open 192.168.1.171 %%p > comftp.txt & echo quit >> comftp.txt & echo quit >> comftp.txt & echo quit >> comftp.txt & **ftp -s:comftp.txt 2>>** puertos.txt

Scripting Batch

```
C:[redacted]s>port_scanner.bat
ftp> open 192.168.1.76 20
ftp> quit
ftp> open 192.168.1.76 21
Conectado a 192.168.1.76.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
202 UTF8 mode is always enabled. No need to send this command.
Usuario (192.168.1.76:(none)):
331 Password required for quit

530 Login or password incorrect!
ftp> quit
221 Goodbye
ftp> open 192.168.1.76 22
ftp> quit
ftp> open 192.168.1.76 23
ftp> quit
ftp> open 192.168.1.76 24
ftp> quit
```

Scripting Batch – analizando...

for /L %%p in (20,1,82) do ....

- Loop basado en contador (/L)
- (inicio, incremento, fin)
- %%p ira tomando los valores : el contador

Scripting Batch – analizando...

echo **Chequeando Puerto %%%p: >> puertos.txt &** echo open 192.168.1.171 %%%p > comftp.txt & echo quit >> comftp.txt & echo quit >> comftp.txt & echo quit >> comftp.txt & **ftp -s:comftp.txt 2>> puertos.txt**

- **&** ejecuta comando tras comando
- En **puertos.txt** estará el reporte
- En **comftp.txt** estarán las instrucciones que usará ftp para INTENTAR abrir una conexión
- Doble **quit** para prevenir servicios que reciben el comando, lo encuentran válido o errado y se quedan esperando otro comando.

Comandos importantes

- echo %username%
- sc query
- systeminfo
- schtasks /query /fo LIST /v
- arp -a
- net view
- net share
- route print
- netsh advfi fi sh rule name=all

netsh advfirewall show allprofiles state
net users
net localgroup <grupo>
net group /domain
net group “<nombre de grupo>” /domain
net group administrators /domain
net user /domain
net user <usuario> /domain
net accounts /domain
nltest /domain_trusts
nltest /dclist:<dominio>
net session | find "\\"
“icacls” o“calcs”
runas

Infraestructura

Análisis de tráfico de red

Wireshark

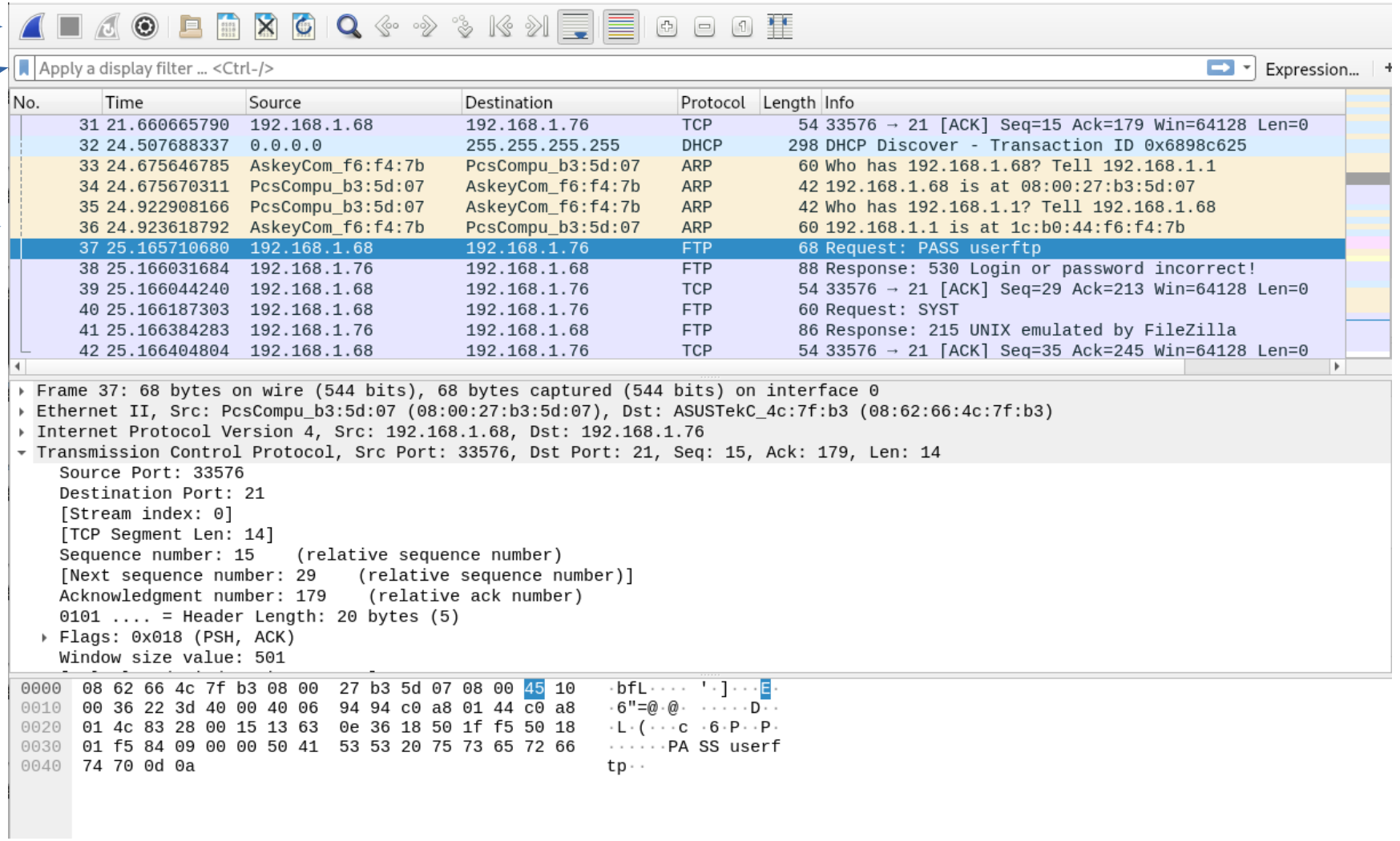
Barra de herramientas

Barra de filtro

Panel de paquetes capturados

Panel de detalle

Panel de bytes
(visualización Hex, ASCII, bits)



Open-Sec

Real Pentesting / Real Red Teaming

Hacking Ético
level 1

Sesión 1

Conceptos e Infraestructura