Denegación de servicios

- Ataque sin solución?

- Andrés Ricardo Almanza Junco. Msc. ITIL v3.
- andres_almanza@hotmail.com

AGENDA

ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:
Una nueva década para avanzar

C:\WINDOWS\system32\cmd.exe - TC.EXE

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP

```
#include (presentacion.inc);

If (presentacion)
{
   version_presentacion("1.0");
   attribute:"Conferencista",value:"Andrès Ricardo Almanza";
   attribuite:"Contenido", value: String("
                              1. Introducción
                              2. Definiciones
                              3. Tipo
                              4. Protección
                              5. Retos y Conclusiones
                              6. Referencias
                              7. FIN ")
    exit(0);
 }
# Comienza  presentación
Tiempo= 3600;

estado = "susto";

if (estado && Conferencista)
      comienza_presentacion();

comienza_presentacio()
{

  for  (i =1; i< Tiempo; i++)
            hablar(Contenido);

  if  (presentacion != "Buena")
       exit(0);

  if (preguntas == "Dificil")
       exit(0);
  else
       contestar;
  return(0); }
```

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

INTRODUCCION

ACIS XI Jornada de Seguridad Informática
Seguridad de la Información:
Una nueva década para avanzar

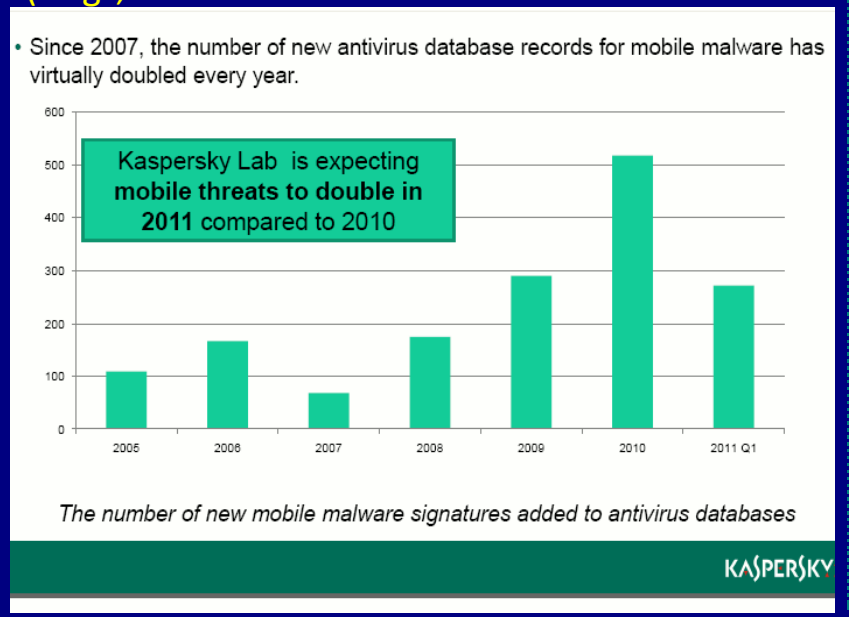
C:\WINDOWS\system32\cmd.exe - TC.EXE

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP

```
void hablar(Contenido) {
 si ( Contenido[0] != "1.  INTRODUCCION" )  exit(0);        /**  PANORAMA GENERAL **/
 else {
  slide() {
    printtf("%s","                                    printf("%g",
```

- ✓ Aumentan considerablemente el malware por año.
- ✓ Dos variables dentro de las premisas del nuevo malware.
  - ✓ Sofisticación, Epidemias
- ✓ Se pasa de ataques entusiastas, a fraude colectivo.
- ✓ Se atacan todo lo que tenga un bit.
  - ✓ Dispositivos móviles, implantes subcutáneos, redes sociales.
- ✓ Se ensanchan las brechas entre protección e infección
- ✓ Según CSI. Las infecciones son mayores y generan mayores perdidas a las organizaciones, y al común de las personas o usuarios de casa");




```
 ); }
```

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP

```
void hablar(Contenido) {
 si ( Contenido[0] != "1.  INTRODUCCION" )  exit(0);        /**  PANORAMA GENERAL **/
 else {
  slide() {
     printtf("%s","                                    printf("%g",
```

- ✓ Entre los mas recientes ataques están:
- ✓ Sony. Afecta la PSN
- ✓ Amazon, Paypal, MasterCard. Anonymous
- ✓ Portales de Gobierno en Linea. AnonymousCO
- ✓ Informes de vulnerabilidades como
  - ✓ Sans Institute. 7 menciones de Denegaciones de Servicios en productos comerciales. (Symantec, Citrix, Apache, SCADA, Oracle)
- ✓ Ataques a Twiter, Facebook, Google

```
        ");                                    );
}
```

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

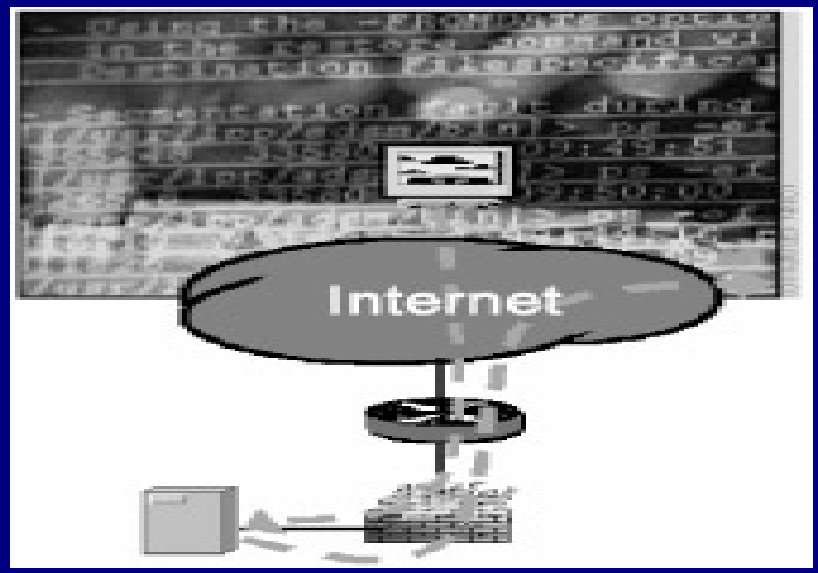
File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP

```
void hablar(Contenido) {
 si ( Contenido[0] != "2. DEFINICIONES" ) exit(0);        /** PANORAMA GENERAL **/
 else {
  slide() {
     printtf("%s","                                    printf("%g", imagen(
```

Denegación de Servicios (DoS y DDoS)

- ✓Tipo de ataque que busca la inutilización de un recurso informático (Computador, Red)
- ✓Conjunto de esfuerzos concentrados de una persona o grupo de personas para interrumpir la operación de un sitio en internet, o un servicio de su correcto funcionamiento, de manera temporal o de manera indefinida.
- ✓Usualmente se escogen sitios de Internet importantes tales como Servicios Financieros, Servicios de Gobierno, Servicios de Nombres de Dominio, entre otros.");



);); }

1:1

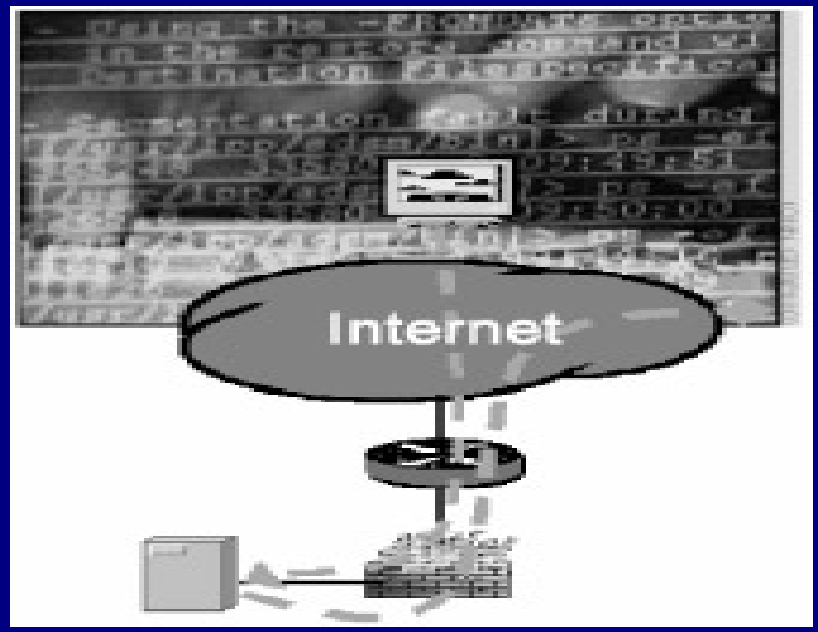
F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
si( Contenido[0] != "2  DEFINICIONES")  exit(0);
else {
 slide() {
    printtf("%s","                                    printf("%g", imagen(
```

Denegación de Servicios (DoS y DDoS)

- ✓El método común de operación es saturar el sistema, o red para que este no responda a la operación normal, o responda de manera muy lenta.
- ✓El enfoque fundamental estará centrado en que el sistema deba reiniciarse.




```
");                                    ););                    }
```

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP — /** PANORAMA GENERAL **/

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

File Edit Search Run Compile Debug Project Options Window Help

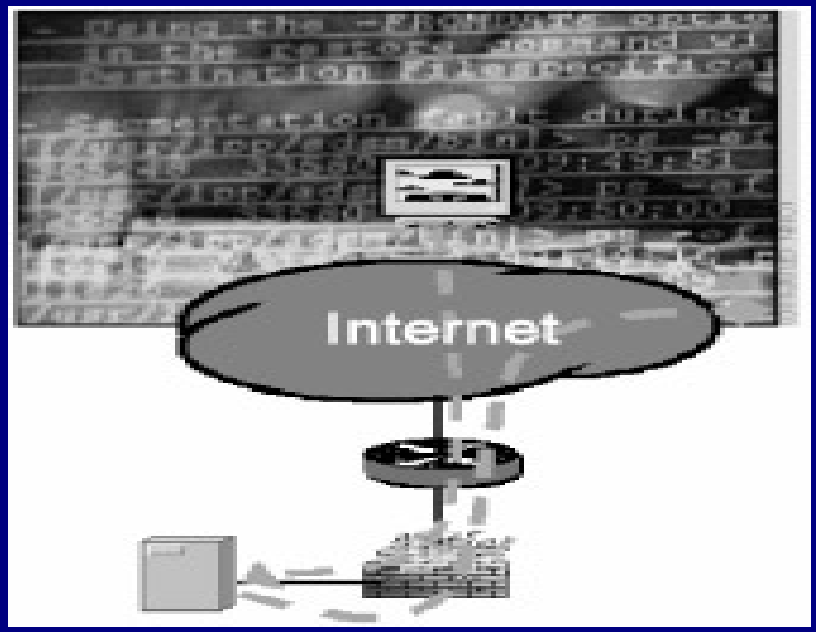
PRESENTA.CPP

```
void hablar(Contenido) {
if( Contenido[0] != "3 TIPOS" ) exit(0);
else {
 slide() {
    printtf("%s","                                    printf("%g", imagen(
```

Existen una gran gamas de ataques de (D)DoS:

✓Basados en la Inundación: De un solo atacante (DoS), de múltiples fuentes (DDoS). Gran esfuerzo del atacante

✓Basados en la malformación de la operación de protocolo o servicio. Poco esfuerzo del atacante




```
");                                    ););                    }
```

1:1

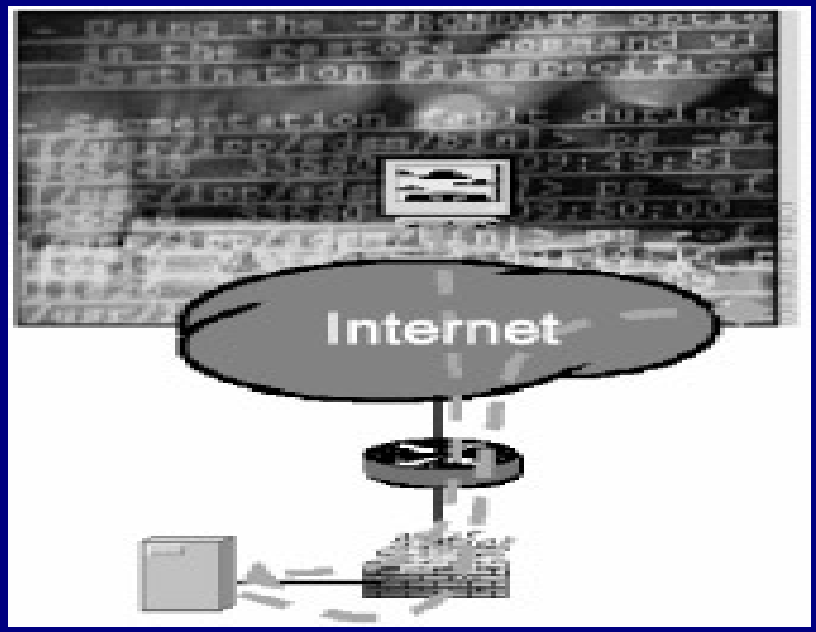
F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "3 TIPOS" ) exit(0);
else {
 slide() {
    printtf("%s","                                    printf("%g", imagen(
```

De igual manera con muchos síntomas para identificar

- ✓Usualmente desempeño disminuido notorio en la red o sistema informático
- ✓Inutilización de un servicio, usualmente servicios Web, o su acceso.
- ✓Incremento elevado de SPAM recibido.




```
");                                    ););                    }
```

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP /** PANORAMA GENERAL **/

1:1

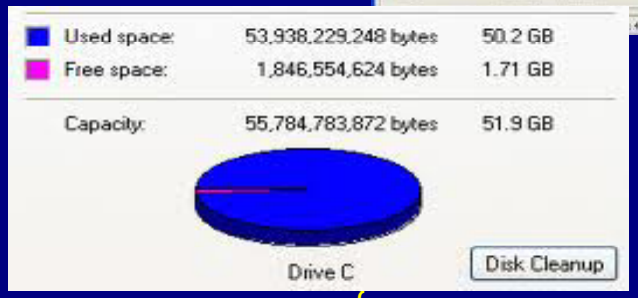
F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "3    TIPOS" ) exit(0);
else {
 slide() {
    printtf("%s","                                    printf("%g", imagen(
```

Existen cinco básicos efectos de los ataques de (D)DoS

- ✓Consumo de recursos computacionales.
  - ✓Ancho de Banda
  - ✓Espacio de almacenamiento
  - ✓Tiempo de Procesamiento.
- ✓Interrupción de la información de configuración. Ej.: routing
- ✓Interrupción del estado de las sesiones TCP.
- ✓Interrupción de componentes físicos de red
- ✓Obstrucción de los medios de comunicación



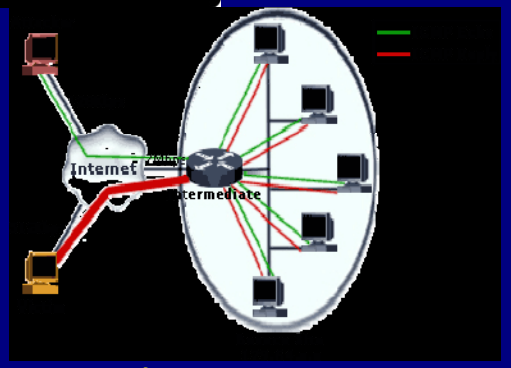

```
"); );};
```

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "3 TIPOS" ) exit(0);
else {
 slide() {
    printtf("%s","                                    printf("%g", imagen(

      Dentro de los basicos ataques de DOS basados en
      inundacion están

      ICMP Flood.  Herramientas como Hping y Scapy,
      ayudan a generar estos tipos de ataques

      ✓Ping de la muerte

      ✓Ataque de los pitufos ( Smurf Attack)

      ✓Ping flood

        ");                                    ););                    }
```

```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Z>ping 127.0.0.1 -n 5 -l 65500

Pinging 127.0.0.1 with 65500 bytes of data:

Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Z>_
```



File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP /** PANORAMA GENERAL **/

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

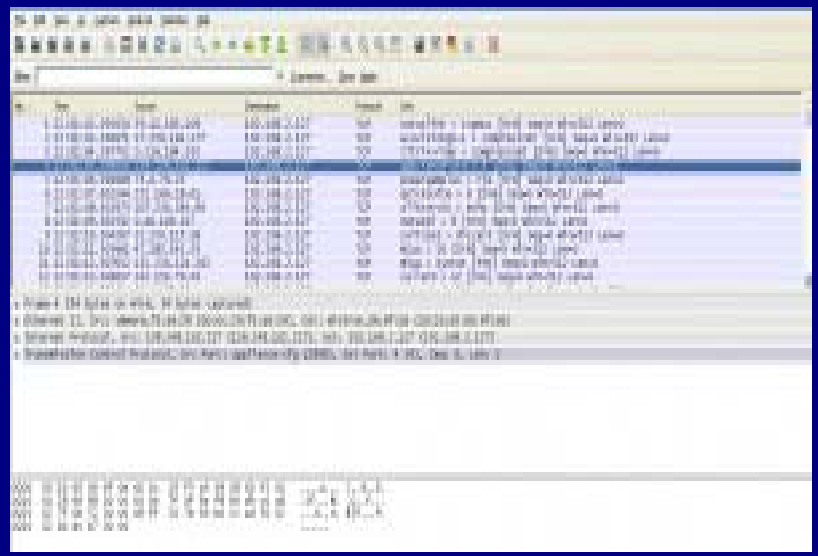
C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "3    TIPOS" ) exit(0);
else {
 slide() {
    printtf("%s","                                    printf("%g", imagen(
```

TCP Flood. Herramientas como Hping y Scapy, ayudan a generar estos tipos de ataques

✓Syn flood : Es el ataque mas comun que aprovecha la falla de control de TCP en el manejo de las sesiones. Se envian un volumen muy alto de SYN, a puertos TCP disponibles, haciendo que el servidor se sature.

✓Programas como syn.c, land.c, HPING3. son de los comunes que se utilizan para estos ataques.



```
");                                    ););                    }
```

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP /** PANORAMA GENERAL **/

1:1

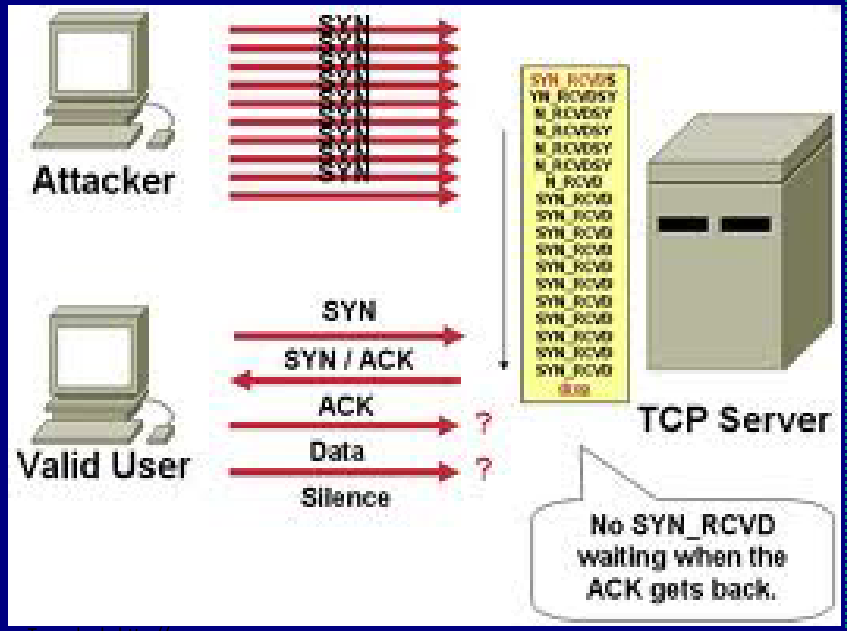
F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP 1=[↕]

```
void hablar(Contenido) {
if( Contenido[0] != "3 TIPOS" ) exit(0);
else {
 slide() {
    printtf("%s","                                  printf("%g", imagen(
      .....

      for (i = 0; i < loop; i++)   {
          bla = ntohl(s_ip),
          bla++;
          s_ip = htonl(bla);
          putchar('.');
          send_pkt(s, s_ip, d_ip, 4+i, atoi(argv[3]),
      TH_SYN, 123, 3, 512, NULL, 0);
      }
      .....

        ");                                  ););                    }
```



Tomado de http://geego.com

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "3    TIPOS" ) exit(0);
else {
 slide() {
    printtf("%s","                                    printf("%g", imagen(
```

Denegación de Servicios Distribuidad (DDoS)

- ✓Ocurre cuando multiples elementos inundan o afectan de un sistema escogido.
- ✓En este caso el atacante se vale de sistemas controlados (zombies) que tienen la instrucción de atacar otro sistema
- ✓Algunos tipos de Malware (MyDooM) , son ejemplos de generacion de DDoS, con condiciones que se activan
- ✓Usualmente trojanizan los zombies y estos son controlados por el atacante y desde cada punto se lanza el ataque a la victima.

Tomado de http://upload.wikimedia.org/wikipedia/commons/thumb/3/3f/Stachledraht_DDos_Attack.svg/220px-Stachledraht_DDos_Attack.svg.png

```
");                                    ););                    }
```

File Edit Search Run Compile Debug Project Options Window Help
PRESENTA.CPP 1:1
/** PANORAMA GENERAL **/
F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

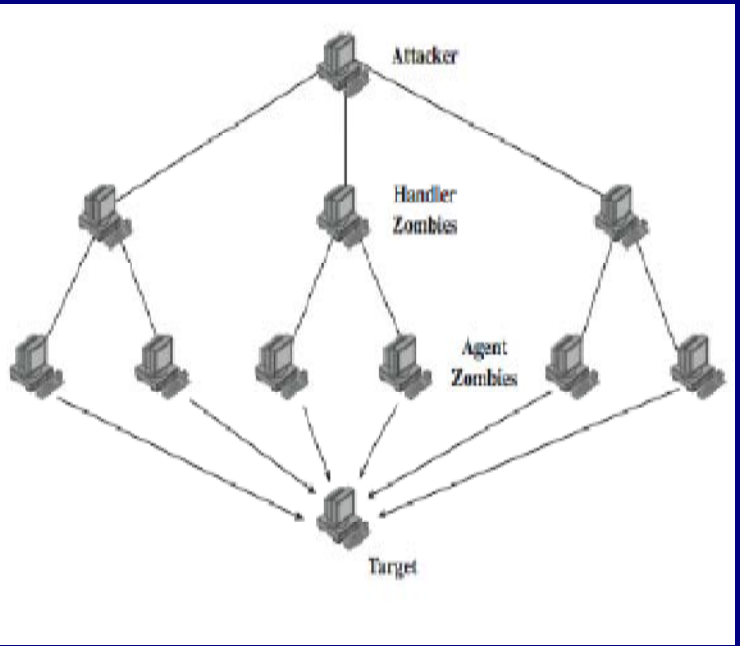
File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP

```
void hablar(Contenido) {
si( Contenido[0] != "3 TIPOS" ) exit(0);
else {
 slide() {
    printtf("%s","                                    printf("%g", imagen(
```

Denegación de Servicios Distribuido (DDoS)

- ✓Stacheldraht. Es un ejemplo de un tool de DDoS. Normalmente este tipo de tool tiene
- ✓Manejador: Quien controla la botnet
- ✓Sistema Agente (Zombie): Controlado a través de clientes, manejados por el atacante donde se dan instrucciones a los zombies, dotados estos componentes para conectar muchos zombies.
- ✓Ejemplos de esto en la historia están:
  - ✓Tribe Fllod Network (TFN), TFN2K




```
");                                    ););                    }
```

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

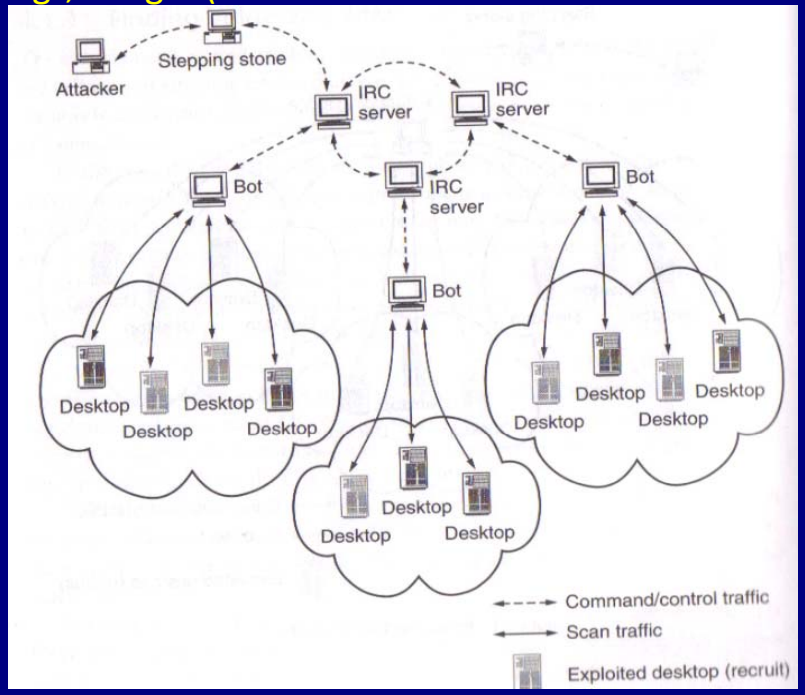
C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "3    TIPOS" ) exit(0);
else {
 slide() {
    printtf("%s","
     Denegación de Servicios Distribuido  (DDoS)

      ✓Utilización de Scanner, para encontrar múltiples
      victimas.  IRC Boot, gusanos
      ✓Los gusanos son mas letales, utilizan robot de
      infecciones dentro de la lógica de programación
      ✓Se propagan muy rápido por  sus patrones de
      paralelos de propagación
      ✓Pueden servir de agentes, aun si la maquina es
      identificada, no todos los componentes son
      eliminados. Ej: RedCode
      ✓Distribuyen el malware desde el atacante, hasta el
      agente y de ahí a los zombies,  TFTP como protocolo
      de propagación
          ");
```

File Edit Search Run Compile Debug Project Options Window Help

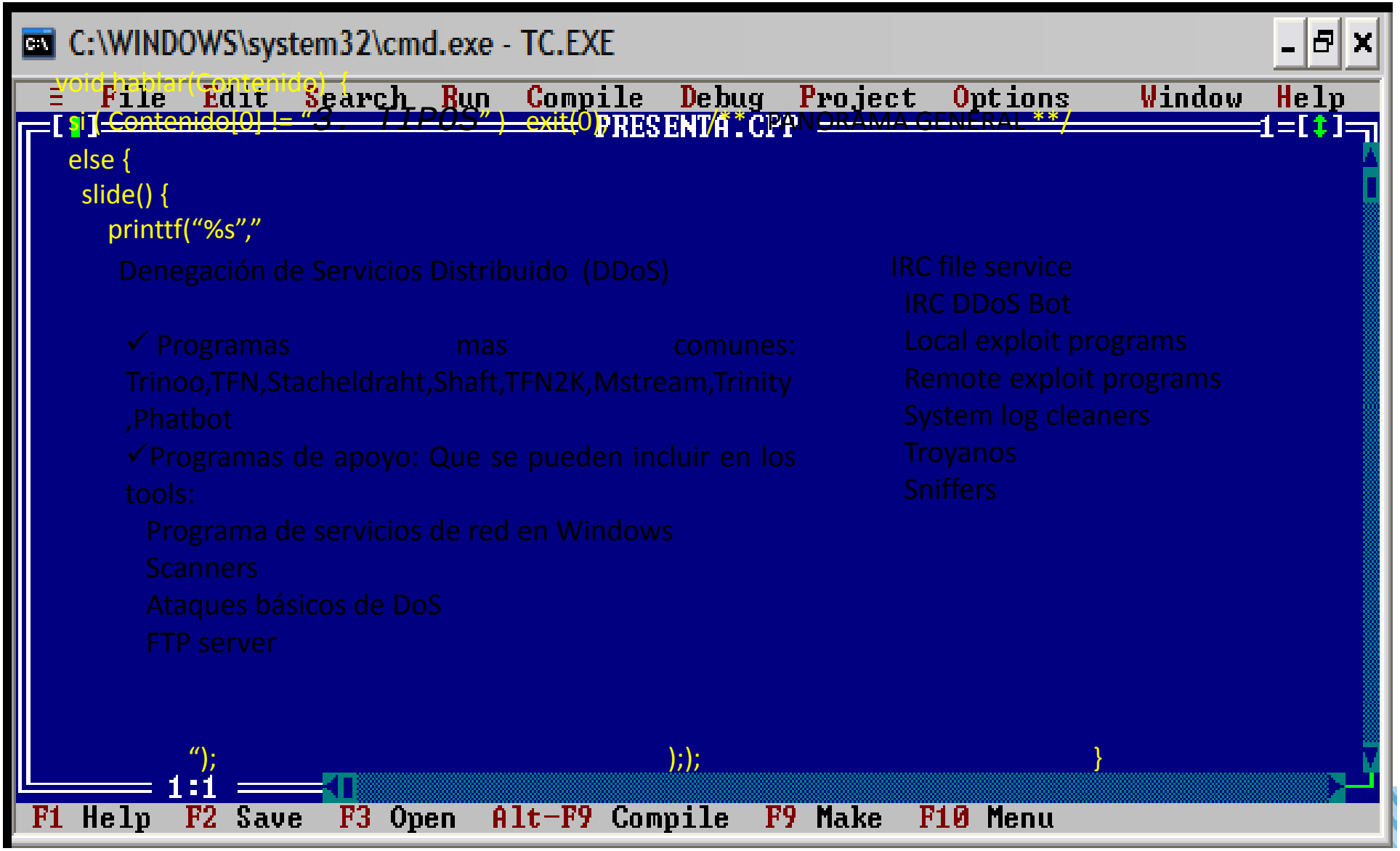
PRESENTA.CPP

```
/** PANORAMA GENERAL **/
printf("%g", imagen(
););
}
```



1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu


C:\WINDOWS\system32\cmd.exe - TC.EXE
File Edit Search Run Compile Debug Project Options Window Help
PRESENTA.CPP
1:1
F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu
void hablar(Contenido) {
if(Contenido[0] != "3 TIPOS") exit(0);
/** PANORAMA GENERAL **/
else {
slide() {
printtf("%s","
Denegación de Servicios Distribuido (DDoS)
✓ Programas mas comunes:
Trinoo,TFN,Stacheldraht,Shaft,TFN2K,Mstream,Trinity
,Phatbot
✓Programas de apoyo: Que se pueden incluir en los
tools:
Programa de servicios de red en Windows
Scanners
Ataques básicos de DoS
FTP server
IRC file service
IRC DDoS Bot
Local exploit programs
Remote exploit programs
System log cleaners
Troyanos
Sniffers
");
);};
}

C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "4   PROTECCION" ) exit(0);
else {
 slide() {
    printtf("%s","
```

- ✓Tener presente que estamos ante una amenaza que no tiene solución
- ✓Depende del tipo de ataque:
  - ✓Por malformación de paquetes: Estudio significativo de los patrones del ataque
  - ✓Por inundación: Estudio de la red para identificar la constancia del ataque.
- ✓Sin importar el tipo (D)DoS existen algunas características importantes

- ✓Simplicidad: Fácil uso, fácil adquisición, no requieren gran experiencia.
- ✓Variedad de Trafico: Dificultad en la identificación, por su parecido con el trafico de la red.
- ✓Spoofing: Característica que hace aun mas difícil de identificar
- ✓Volumen de trafico: En la inundación esto es su enemigo, se requiere generar un alto volumen de trafico que lo puede hacer detectable.
- ✓Numerosos agentes: Entre mas agentes existan mucho mas efectivo un DDoS

```
");                                    ););                    }
```

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP /** PANORAMA GENERAL **/ 1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "4  PROTECCION" ) exit(0);
else {
 slide() {
    printtf("%s","
```

Prevención:

- ✓Mejoramiento de la infraestructura de nuestra red y servicios. Capacidad
- ✓Aseguramiento de los servicios e infraestructura, evitando posibles infecciones electrónicas
- ✓Monitoreo de los patrones de comportamiento de la red
- ✓Buenas practicas de seguridad en el desarrollo de aplicaciones
- ✓Contactar con centros de atención de incidentes, identifican

Reacción

- ✓Sistemas de protección perimetrales e IDS/IPS son mecanismos técnicos de apoyo
- ✓Acciones manuales en caso de identificación del ataque. Reiniciar los sistemas.

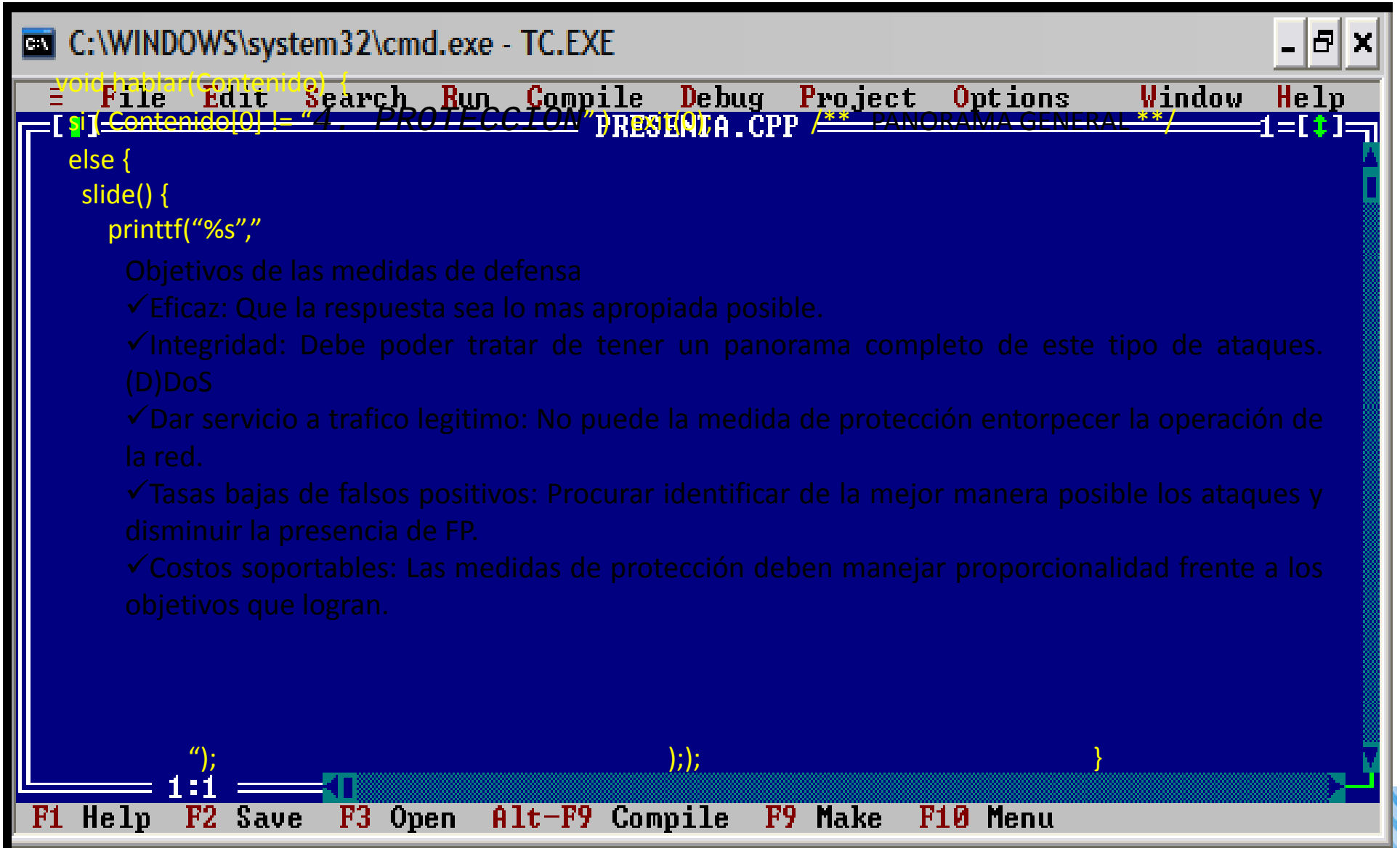
```
");                                    ););                    }
```

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP /** PANORAMA GENERAL **/

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu


C:\WINDOWS\system32\cmd.exe - TC.EXE
File Edit Search Run Compile Debug Project Options Window Help
PRESENTA.CPP
/** PANORAMA GENERAL **/
void hablar(Contenido) {
si(Contenido[0] != "4 PROTECCION") exit(0);
else {
slide() {
printtf("%s","
Objetivos de las medidas de defensa
✓Eficaz: Que la respuesta sea lo mas apropiada posible.
✓Integridad: Debe poder tratar de tener un panorama completo de este tipo de ataques. (D)DoS
✓Dar servicio a trafico legitimo: No puede la medida de protección entorpecer la operación de la red.
✓Tasas bajas de falsos positivos: Procurar identificar de la mejor manera posible los ataques y disminuir la presencia de FP.
✓Costos soportables: Las medidas de protección deben manejar proporcionalidad frente a los objetivos que logran.
");
);};
}
1:1
F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

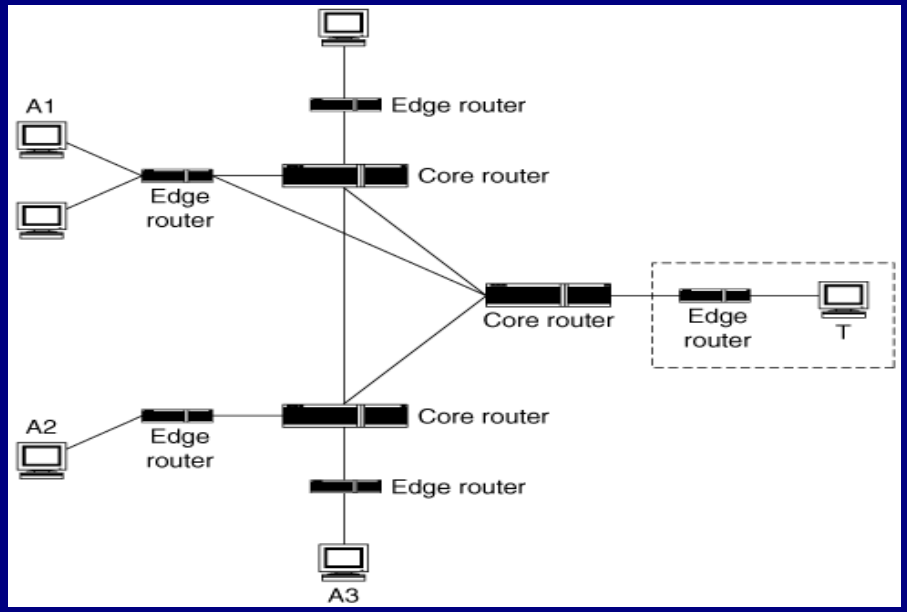
C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "4 PROTECCION" ) exit(0);
else {
 slide() {
    printtf("%s","                                printf("%g",
```

Esquemas de protección (D)DoS

Cerca de la victima:

- ✓Todo se ubica donde se considera que pueda ser atacada una victima.
- ✓Alta comunicación y notificación de los ataques
- ✓Máximo control de la protección y ajustes rápidos frente a FP
- ✓Problemas con las volúmenes de los ataques, por lo tanto deben ser suficientes para soportar un ataque
- ✓Interacción del humano para ayudar a responder




```
");                                    ););                    }
```

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

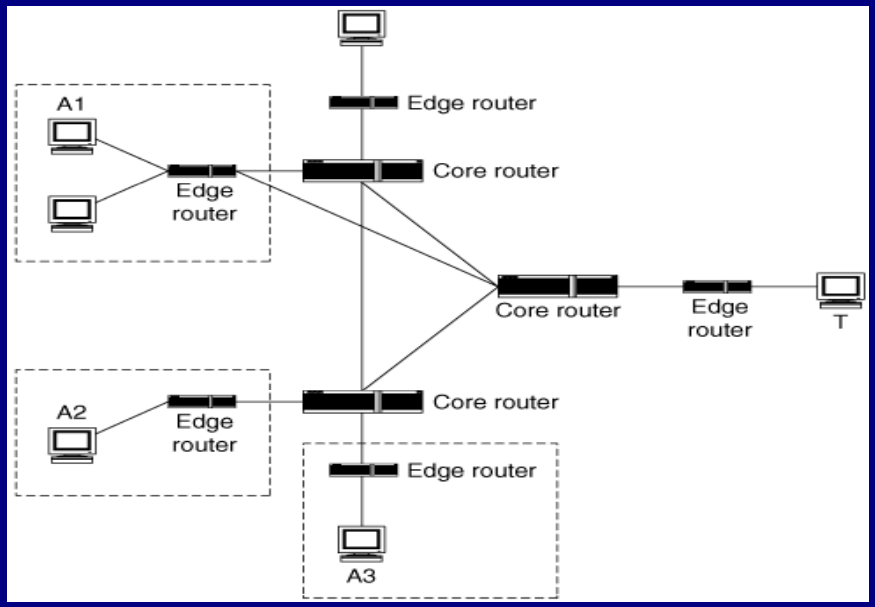
C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
si( Contenido[0] != "4   PROTECCION"  ) exit(0);
else {
 slide() {
    printtf("%s","                                printf("%g",
```

Esquemas de protección (D)DoS

Cerca del atacante

- ✓Se crean mecanismos de protección de todas las fuentes posibles. Elevados costos si se tienen muchas interconexiones
- ✓Son mecanismos que limitan el trafico, por lo tanto no sufrirán las consecuencias las redes bajo protección
- ✓Podría ser los mecanismo implementados por nuestros ISP




```
");                                    ););                    }
```

File Edit Search Run Compile Debug Project Options Window Help

DRESENTA.CPP /** PANORAMA GENERAL **/

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

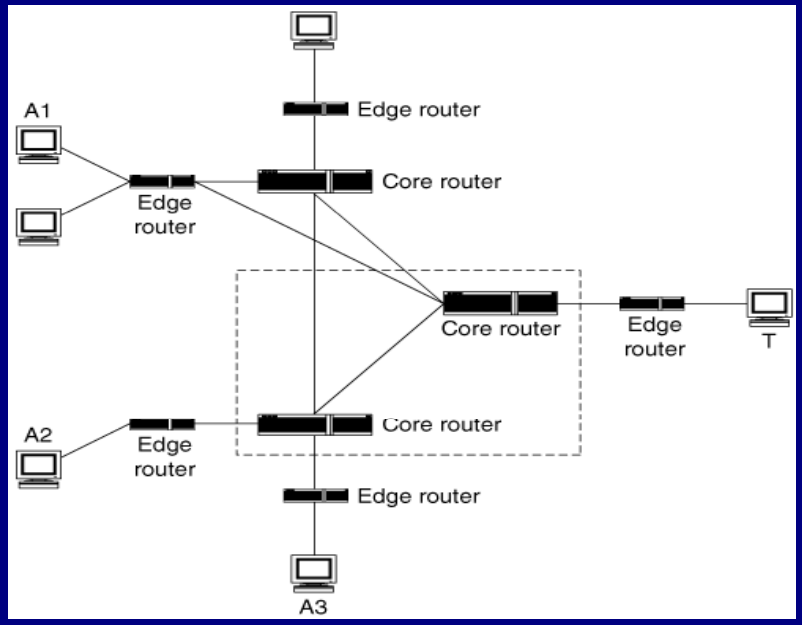
C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "4 PROTECCION" ) exit(0);
else {
 slide() {
    printtf("%s","                    printf("%g",
```

Esquemas de protección (D)DoS

En el medio

- ✓La típica protección que se coloca en nuestros elementos de comunicaciones entre red local e Internet
- ✓Cuellos de botella, pueden ser complejos y no atendidos con celeridad generando problemas de comunicaciones




```
");                    ););                    }
```

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

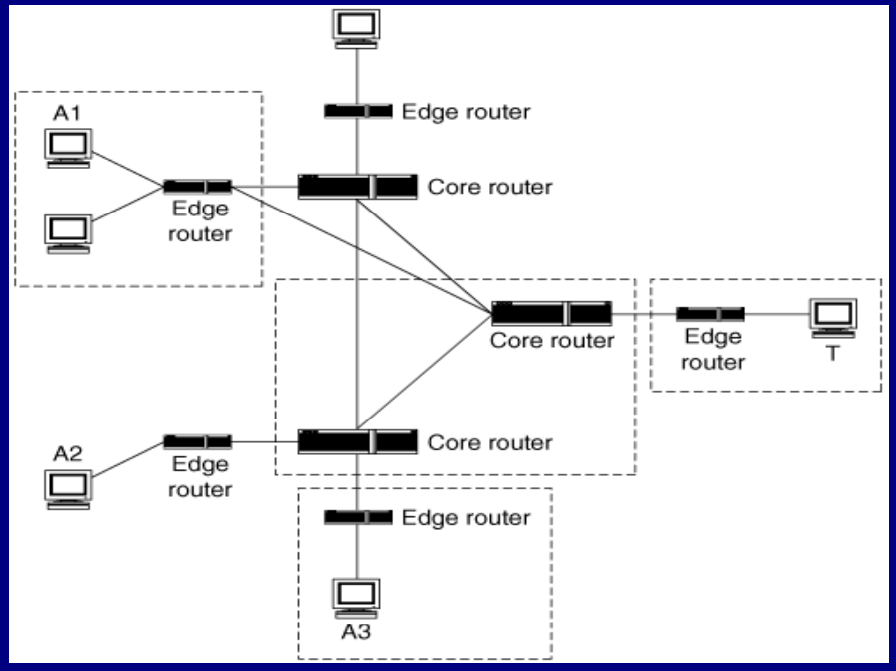
C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "4 PROTECCION" ) exit(0);
else {
 slide() {
    printtf("%s","                    printf("%g",
```

Esquemas de protección (D)DoS

Esquemas mixtos

- ✓Protección distribuida, para ataques distribuidos
- ✓Requiere interacción de muchas partes y mucha coordinación para demostrar su efectividad.
- ✓Se pueden llegar a convertir en puntos vulnerables los mismo mecanismos de protección.




```
");                                    ););                    }
```

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP /** PANORAMA GENERAL **/

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "4 - PROTECCION" ) exit(0);
else {
 slide() {
    printtf("%s","                                printf("%g",
```

Estrategia General de Protección

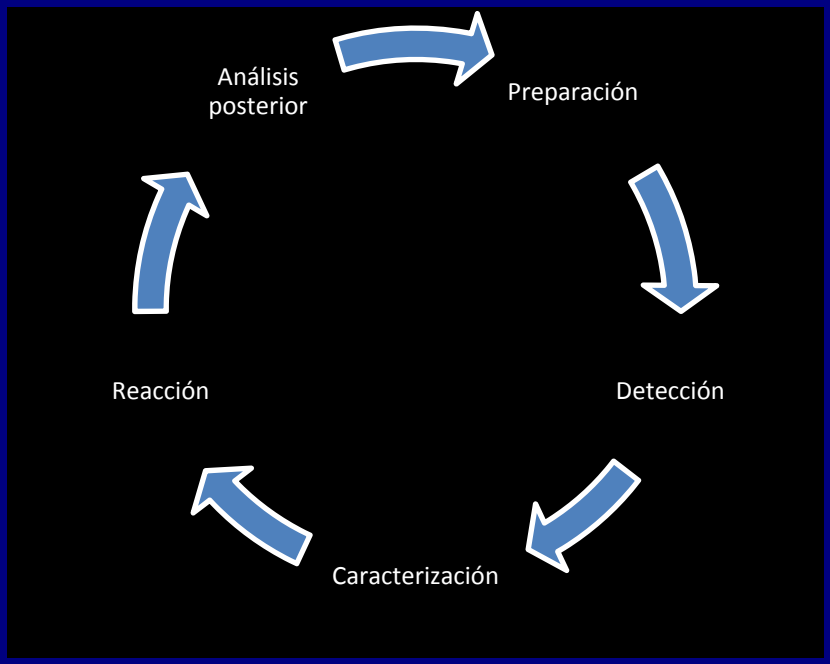
Preparación: Conocimiento del ambiente de red, y disponer de las herramientas adecuadas

Detección: Como se identifican los ataques de (D)DoS

Caracterización: Tipos de Ataques a los que se esta siendo sometido

Reacción: Bloquear el trafico, identificar equipos comprometidos, y reunir pruebas, invocación de planes de contingencia

Análisis posterior: Revisión de todos lo ejecutado para su contención



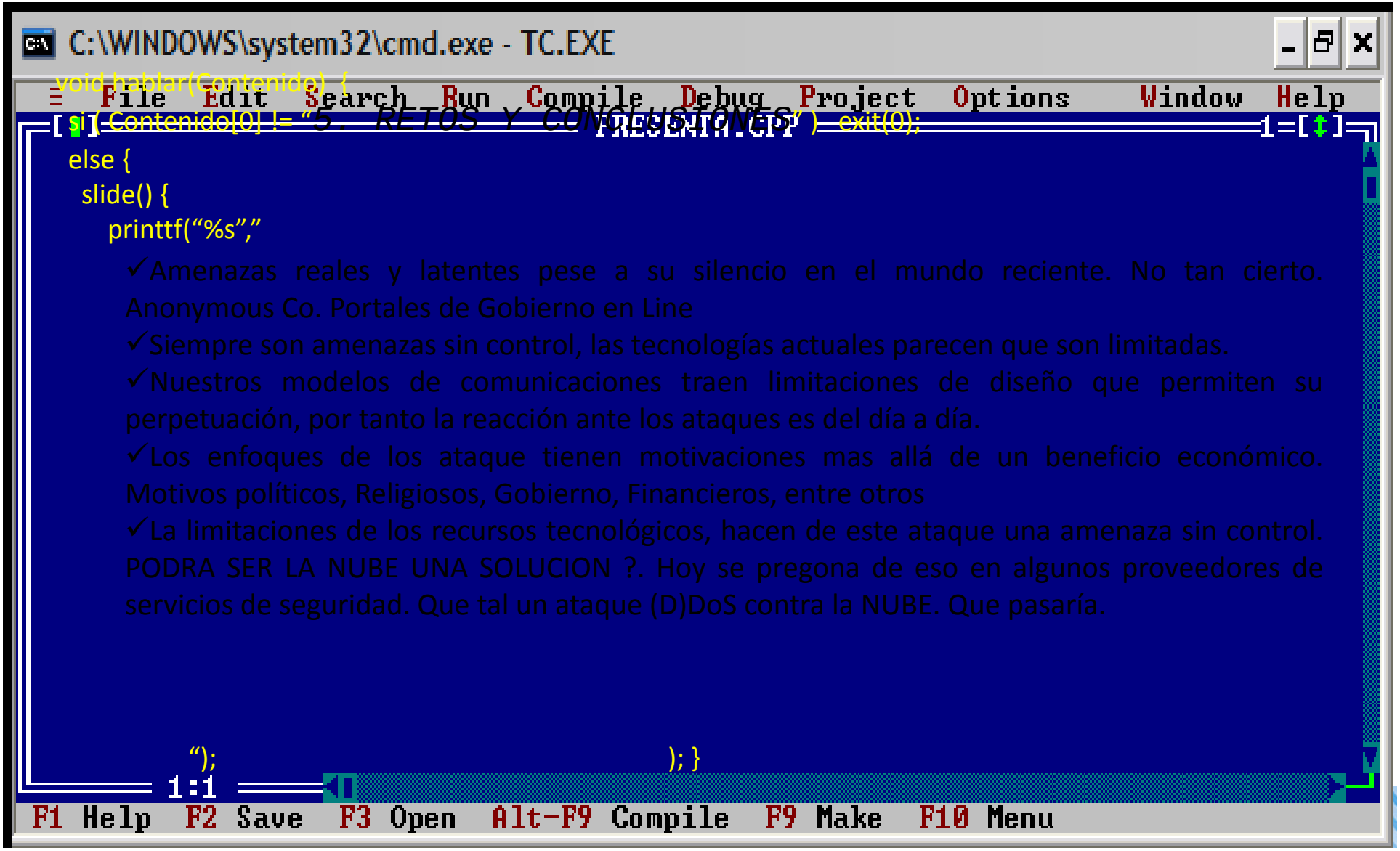

```
");                                    ););                    }
```

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP /** PANORAMA GENERAL **/

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu


C:\WINDOWS\system32\cmd.exe - TC.EXE
File Edit Search Run Compile Debug Project Options Window Help
PRESENTA.CPP
5 RETOS Y CONCLUSIONES
void hablar(Contenido) {
if(Contenido[0] != "5 RETOS Y CONCLUSIONES") exit(0);
else {
slide() {
printtf("%s","
✓Amenazas reales y latentes pese a su silencio en el mundo reciente. No tan cierto. Anonymous Co. Portales de Gobierno en Line
✓Siempre son amenazas sin control, las tecnologías actuales parecen que son limitadas.
✓Nuestros modelos de comunicaciones traen limitaciones de diseño que permiten su perpetuación, por tanto la reacción ante los ataques es del día a día.
✓Los enfoques de los ataque tienen motivaciones mas allá de un beneficio económico. Motivos políticos, Religiosos, Gobierno, Financieros, entre otros
✓La limitaciones de los recursos tecnológicos, hacen de este ataque una amenaza sin control. PODRA SER LA NUBE UNA SOLUCION ?. Hoy se pregona de eso en algunos proveedores de servicios de seguridad. Que tal un ataque (D)DoS contra la NUBE. Que pasaría.
");
); }
1:1
F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "5 - RETOS Y CONCLUSIONES" ) exit(0);
else {
 slide() {
    printtf("%s","
```

- ✓No existe una solución única para su control, muchas investigaciones de distintos proveedores, pero nada en concreto frente a esta gran amenaza, por lo tanto todos los mecanismos de protección son validos. Firewall, Proxys, IDS/IPS, SIEM, Políticas, Atención de Incidentes, Código Seguro, entre otros mecanismos son validos para disminuir la situación.
- ✓Mejorar nuestras relaciones en términos contractuales para ayudar en la protección de estos tipos de ataques.
- ✓Ideal Centros de atención de respuestas nacionales, NAP Colombia debería tener mecanismo de protección.
- ✓Mejora continua de las infraestructuras que permitan disminuir los riesgos frente a estos tipos de ataques. Tecerizar puede ser una opción, se debe evaluar que tanto nos afecta la interrupción del servicios. Acuerdos de Servicios serán la clave en este escenario.

```
");                                    ); }
```

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP 1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "5 RETOS Y CONCLUSIONES" ) exit(0);
else {
 slide() {
   printtf("%s","
```

- ✓Sofisticación de las medidas de protección, harán de la sofisticación de los ataques de (D)DoS, por lo tanto existen algunas características de su futuro
  - ✓Aumento del Tamaño: Mayor numero de Zombies, (botnets) de 1 millón de maquinas.
  - ✓Aumento de la sofisticación: En defensa, por lo tanto los ataques variaran su espectro, afectaran otros protocolos, o aplicaciones
  - ✓Ataques a los servicios, en la actualidad se ve que DNS, Servicios WEB, y aplicaciones son el foco de acción, atrás están quedando los ataques directos a las redes.
  - ✓Tendencia reciente de la degradación y no la denegación, enfoque de estos en las guerras económicas.
  - ✓Anteriormente se utilizaba esto como demostración de conocimiento de los Hackers, ahora hay motivaciones mas oscuras que permiten su utilización

```
");                                    ); }
```

C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
if( Contenido[0] != "5 - RETOS Y CONCLUSIONES" ) exit(0);
else {
 slide() {
    printtf("%s","
```

- ✓Legislación de muchos países ha contemplado tener presente este tipo de ataques, como respuesta a protegerse post el ataque.
- ✓Mucha investigación al respecto del tema, y tecnología emergente como mecanismo de apoyo a la protección
- ✓Conciencia corporativa en la protección, ejemplo ciclos de actualizaciones de plataformas, gestión de parches, gestión de vulnerabilidades, gestión de procesos de seguridad, responsabilidades en seguridad informática y de información
- ✓Mejorar el trabajo conjunto (técnico y humano) entre todos los actores. Proveedores de Internet, Proveedores de tecnología de comunicaciones, ISP's locales, organismos gubernamentales, las asociaciones profesionales de redes y administradores de sistemas.
- ✓Esta su compañía preparado en estos tipos de ataque. El Firewall no es la única solución.

```
");                                          ); }
```

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP 1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
  if(Contenido[0] != "6. REFERENCIAS") exit(0);else {
```

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP

```
slide() {
   printtf("%s","
```


- ✓ From CERT: CA-99-17, CA-2000-01, IN-99-07. http://www.cert.org/reports/dsit_workshop.pdf
- ✓ Dave Dittrich's analyses: http://staff.washington.edu/dittrich/misc/trinoo.analysis http://staff.washington.edu/dittrich/misc/tfn.analysis http://staff.washington.edu/dittrich/misc/stacheldraht.analysis
- ✓ Scanning tool: http://www.fbi.gov/nipc/trinoo.htm
- ✓ "Types of DDoS Attacks". 2001.
- ✓ "CERT Advisory CA-1997-28 IP Denial-of-Service Attacks". CERT. 1998.

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
  if( Contenido[0] != "8. REFERENCIAS") exit(0);else {
    slide() {
      printtf("%s","
```


- ✓ "Permanent Denial-of-Service Attack Sabotages Hardware". Dark Reading. 2008.
- ✓ The "stacheldraht" distributed denial of service attack tool
- ✓ Phillip Boyle (2000). "SANS Institute - Intrusion Detection FAQ: Distributed Denial of Service Attack Tools: n/a". SANS Institute.
- ✓ Pirate Bay Hit With DDoS Attack After "Selling Out", 8:01 AM - July 1, 2009, by Jane McEntegart - Tom's Hardware
- ✓ Ongoing denial-of-service attack, August 6, 2009, Twitter Status Blog
- ✓ Ongoing denial-of-service attack, August 6, 2009, Twitter Status Blog

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

C:\WINDOWS\system32\cmd.exe - TC.EXE

```
void hablar(Contenido) {
File  Edit  Search  Run  Compile  Debug  Project  Options  Window  Help
if( Contenido[0] != "6.  REFERENCIAS") exit(0); else {
slide() {
   printtf("%s","
```


- ✓ "WikiLeaks Under Denial of Service Attack (DDoS)". Security Week. 2010-11-28.
- ✓ Addley, Esther; Halliday, Josh (December 8, 2010). "Operation Payback cripples MasterCard site in revenge for WikiLeaks ban". *The Guardian* (London)
- ✓ http://techie-buzz.com/tech-news/4chan-attacks-mastercard-paypal-and-more-in-defense-of-wikileaks.html
- ✓ Froutan, Paul (June 24, 2004). "How to defend against DDoS attacks". *Computerworld*.


```
   );          return(0); }}}
1:1
F1 Help  F2 Save  F3 Open  Alt-F9 Compile  F9 Make  F10 Menu
```

C:\WINDOWS\system32\cmd.exe - TC.EXE

File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP

```
void hablar(Contenido) {
si ( Contenido[0] != "7. FIN" )  exit(0); else {
   slide() {

     si ( Tiempo == 3600 && estado != "susto" ) {
      do {
        printf("%g", "
```

```
/* ANDRES RICARDO ALMANZA JUNCO */
/* andres_almanza@hotmail.com */

      } while ( preguntas );

    ");
     printf("%s", "GRACIAS");
}
```

1:1

F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu