

# Denegación de servicios

- Ataque sin solución?
- Andrés Ricardo Almanza Junco. Msc. ITIL v3.
- andres\_almanza@hotmail.com

# ACIS X | Jornada de Seguridad Informática

## AGENDA

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 == "Difícil")
    exit(0);
  else
    contestar;
  return(0); }
F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu
```



# XI Jornada de Seguridad Informática

# INTRODUCCION

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() {
      printf("%s",

```

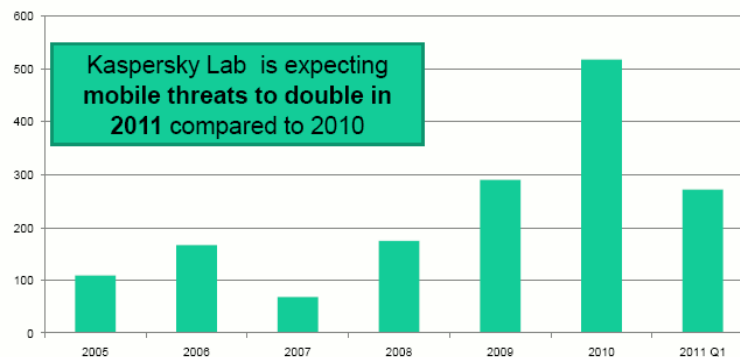
- ✓ Aumentan considerablemente el malware por año.
- ✓ Dos variables dentro de las premisas del nuevo malware.
  - ✓ Sofisticación, Epidemias
- ✓ Se pasa de ataques entusiastas, a fraude colectivo.
- ✓ Se atacan todo lo que tenga un bit.
  - ✓ Dispositivos móviles, implantes subcutáneos, redes sociales.
- ✓ 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");

```

printf("%g",

```

• Since 2007, the number of new antivirus database records for mobile malware has virtually doubled every year.



The number of new mobile malware signatures added to antivirus databases

KASPERSKY

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

# 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",
        ✓ 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
```

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

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

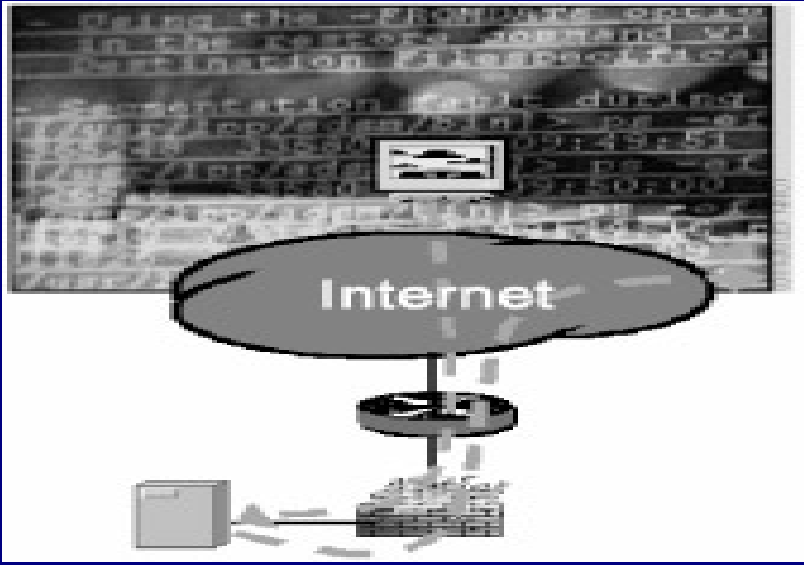
File Edit Search Run Compile Debug Project Options Window Help

PRESENTA.CPP

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

```
            printf("%g", imagen(  
            );  
        }  
    }  
};
```



The diagram shows a central cloud labeled 'Internet' supported by a server rack. A computer monitor is positioned above the server rack, displaying a blurred image of a network or data flow. The entire scene is set against a dark background with a grid pattern.

1:1

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



# ACIS XI Jornada de Seguridad Informática

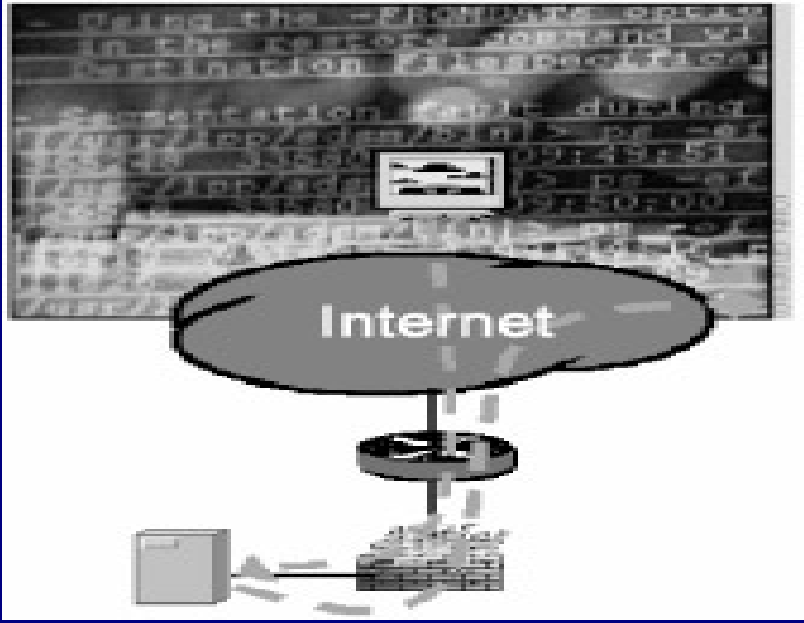
Seguridad de la Información:  
Una nueva década para avanzar

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

```
void hablar(Contenido) {
s[Contenido] != "2" DEFUNCTONE PRESENTA CPP /** PANORAMA GENERAL **/
else {
slide() {
printf("%s",
printf("%g", imagen(
");
);
}
```

Denegación de Servicios (DoS y DDoS)

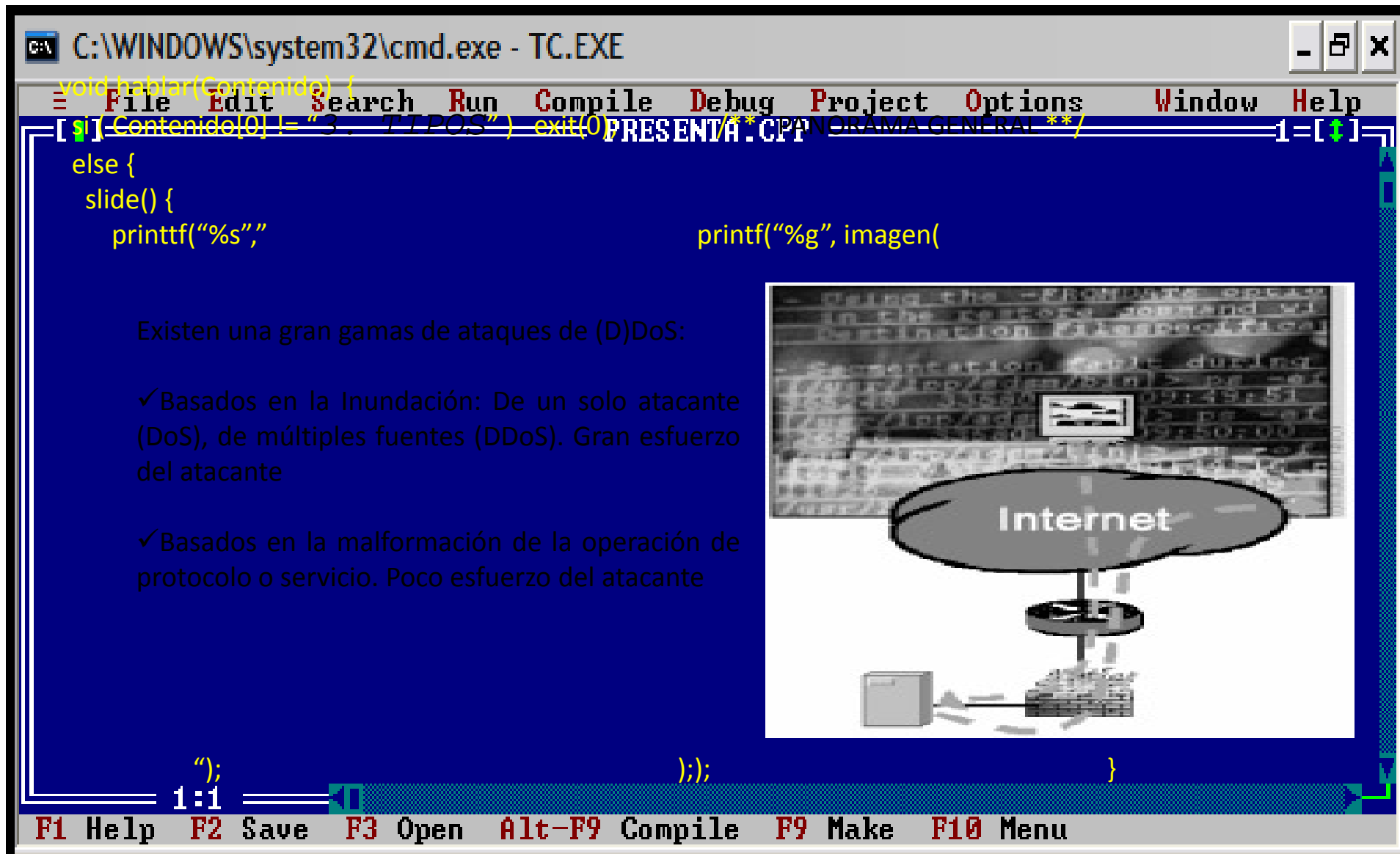
- ✓ El método común de operación es saturar el sistema, o red para que este no responda a la operación normal, o responda de manera muy lenta.
- ✓ El enfoque fundamental estará centrado en que el sistema deba reiniciarse.



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

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar



The screenshot shows a Turbo C++ IDE window titled "C:\WINDOWS\system32\cmd.exe - TC.EXE". The menu bar includes File, Edit, Search, Run, Compile, Debug, Project, Options, Window, and Help. The code editor displays a C++ program with the following visible lines:

```
void hablar(Contenido) {  
    [s] [Contenido] != "3 - TTPOS") exit(0);  
    else {  
        slide() {  
            printf("%s",  
                printf("%g", imagen(  
                    "D:\img\...")  
                );  
            );  
        }  
    }  
}
```

Below the code, the text reads: "Existen una gran gamas de ataques de (D)DoS:" followed by two bullet points:

- ✓ 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

To the right of the text is a diagram illustrating a Denial of Service (DoS) attack. It shows a computer monitor displaying a network diagram with a central cloud labeled "Internet". Below the cloud, a server rack is shown with a large, dark, irregular shape representing an attack or flood of traffic directed at the server.

The IDE status bar at the bottom shows "1:1" and function key shortcuts: F1 Help, F2 Save, F3 Open, Alt-F9 Compile, F9 Make, F10 Menu.

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

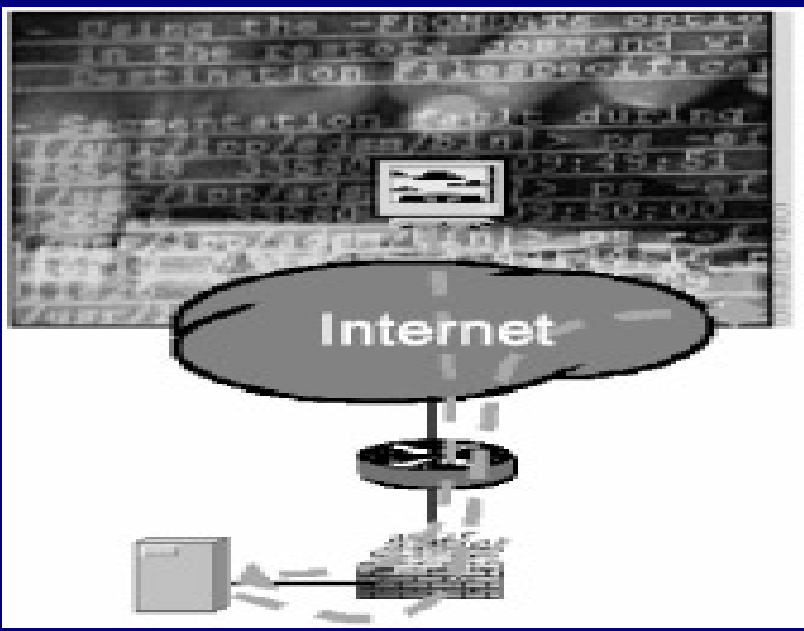
C:\WINDOWS\system32\cmd.exe - TC.EXE

File Edit Search Run Compile Debug Project Options Window Help

```
void hablar(Contenido) {  
    [s] [Contenido] != "3 - TTPOS") exit(0)  
    else {  
        slide() {  
            printf("%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.



The diagram illustrates a network configuration. At the bottom, a computer is connected to a server rack. Above the server, a cloud is labeled 'Internet'. The background of the diagram shows a blurred image of a server room.

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



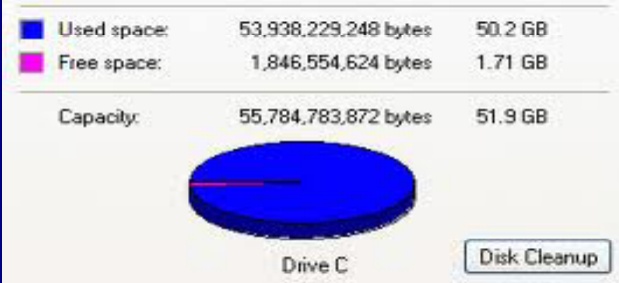

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

```
C:\WINDOWS\system32\cmd.exe - TC.EXE  
void hablar(Contenido) {  
s[Contenido] != "3 - TTPOS") exit(0);  
else {  
slide() {  
printf("%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



Category	Value	Percentage
Used space	53,938,229,248 bytes	50.2 GB
Free space	1,846,554,624 bytes	1.71 GB
Capacity	55,784,783,872 bytes	51.9 GB

Drive C

Disk Cleanup

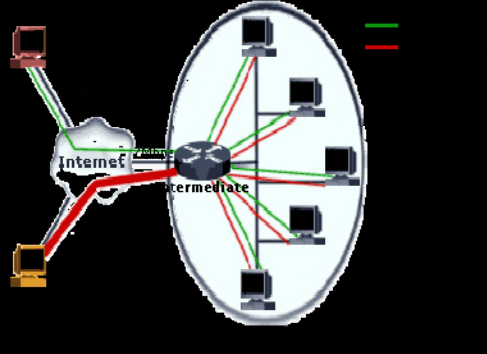
F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

```
C:\WINDOWS\system32\cmd.exe - TC.EXE  
void hablar(Contenido) {  
    if (Contenido[0] != "3 - TTPOS") exit(0);  
    else {  
        slide() {  
            printf("%s",  
                "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>



# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

```
void hablar(Contenido) {
    if (Contenido[0] != "3 - TTPOS") exit(0);
}

else {
    slide() {
        printf("%s",
            "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.

            ");
        printf("%g", imagen(
            "img2 192.168.100.10 --rand-source --destport 80 --syn -c 100
            hping 192.168.100.10 setip 192.168.100.10): S set, 40 leaders + 0 data bytes
            ");
    }
};
```

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

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

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

```
void hablar(Contenido) {
[ s ] [Contenido] != "3 - TTPOS" ) exit(0) PRESENTA.CPP
File Edit Search Run Compile Debug Project Options Window Help
else {
  slide() {
    printf("%s",
    .....
    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);
    }
    .....
  );
  printf("%g", imagen(
  );
  }
1:1
F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu
```

Attacker

Valid User

TCP Server

No SYN\_RCVD waiting when the ACK gets back.


Tomado de <http://geego.com>

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

```
C:\WINDOWS\system32\cmd.exe - TC.EXE  
void hablar(Contenido) {  
    if (Contenido[0] != "3 - TTPOS") exit(0);  
    else {  
        slide() {  
            printf("%s",  
                "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](http://upload.wikimedia.org/wikipedia/commons/thumb/3/3f/Stachledraht_DDos_Attack.svg/220px-Stachledraht_DDos_Attack.svg.png)



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



# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

```
C:\WINDOWS\system32\cmd.exe - TC.EXE  
void hablar(Contenido) {  
    [Content] != "3 - TTPOS") exit(0);  
    else {  
        slide() {  
            printf("%s",  
                Denegación de Servicios Distribuido (DDoS)  
                printf("%g", imagen(  
                );  
                );  
            }  
        }  
    }  
};  
};  
};
```

File Edit Search Run Compile Debug Project Options Window Help

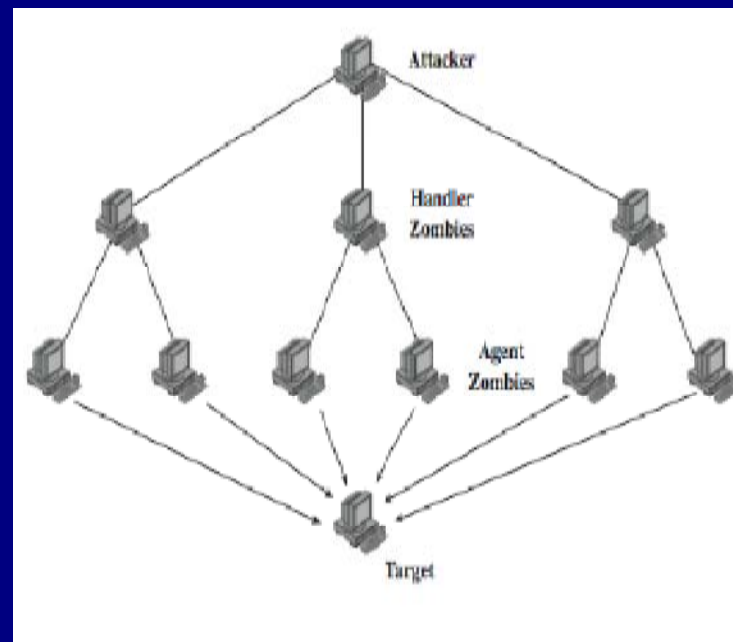
PRESENTA.CPP

1:1

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

## 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 Flood Network (TFN), TFN2K



# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

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

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

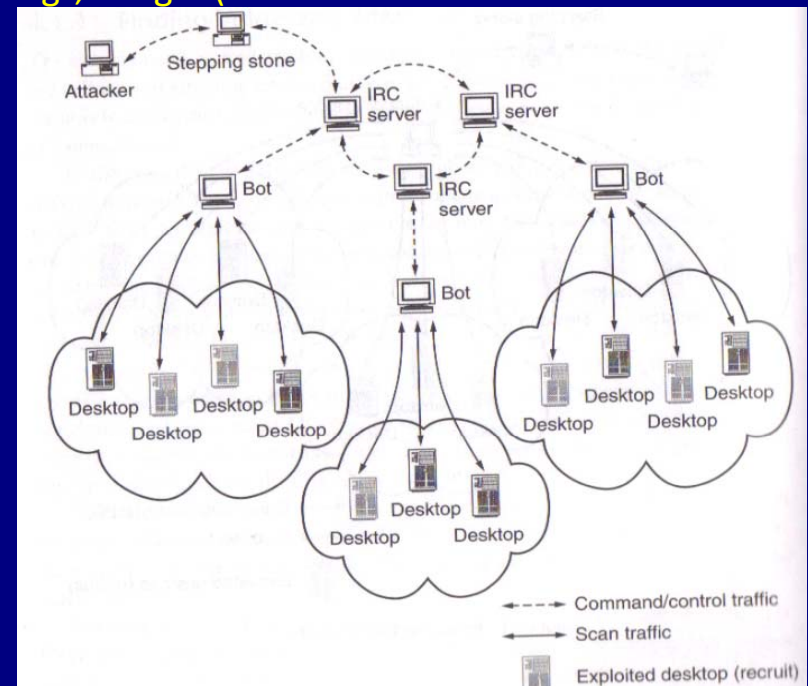
```
else {  
slide() {
```

```
printf("%s",
```

```
Denegación de Servicios Distribuido (DDoS)
```

- ✓ Utilización de Scanner, para encontrar múltiples víctimas. 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

```
printf("%g", imagen(  
};
```



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

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

```
void hablar(Contenido) {
  [Content] != "3 - TTPOS") exit(0)
  else {
    slide() {
      printf("%s",
        Denegación de Servicios Distribuido (DDoS)
        IRC file service
        IRC DDoS Bot
        Local exploit programs
        Remote exploit programs
        System log cleaners
        Troyanos
        Sniffers
        ✓ 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
      );
    });
  }
}
```

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

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

The screenshot shows a Turbo C++ IDE window titled "C:\WINDOWS\system32\cmd.exe - TC.EXE". The menu bar includes File, Edit, Search, Run, Compile, Debug, Project, Options, Window, and Help. The code editor displays a C++ function named `void hablar(Contenido) {` with a comment `/* PANORAMA GENERAL */`. The function body contains an `else {` block with a `slide() {` function call and a `printf("%s",` statement. Below the code, a list of characteristics for Denial of Service (DoS) attacks is presented in a two-column format.

```
void hablar(Contenido) {  
    /* PANORAMA GENERAL */  
    else {  
        slide() {  
            printf("%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  
                ");  
        };  
    };  
}
```

1:1

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

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

```
void hablar(Contenido) {
s[Contenido] != "4 - PROTECCION" PRESENTA.CPP /** PANORAMA GENERAL **/
else {
slide() {
printf("%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.
);
});
}
1:1
```

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



# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

```
void hablar(Contenido) {  
[s] [Contenido] != "4. PROTECCION" PRESENTA.CPP /** PANORAMA GENERAL **/  
else {  
  slide() {  
    printf("%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.  
    );  
  });  
}
```

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

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

```
C:\WINDOWS\system32\cmd.exe - TC.EXE  
void hablar(Contenido) {  
[s] [Contenido] != "4. PROTECCION" PRESENTA.CPP /** PANORAMA GENERAL **/  
else {  
  slide() {  
    printf("%s",  
    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  
    ");  
  });  
}
```

The diagram illustrates a network topology. A central Core router is connected to five Edge routers. On the left, two Edge routers are connected to hosts A1 and A2. At the bottom, one Edge router is connected to host A3. On the right, one Edge router is connected to host T, which is enclosed in a dashed box. The Core router is connected to all five Edge routers.

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

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

```
C:\WINDOWS\system32\cmd.exe - TC.EXE  
void hablar(Contenido) {  
[s] [Contenido] != "4. PROTECCION" PRESENTA.CPP /** PANORAMA GENERAL **/  
else {  
  slide() {  
    printf("%s", "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 tráfico, por lo tanto no sufrirán las consecuencias las redes bajo protección  
    ✓ Podría ser los mecanismo implementados por nuestros ISP  
    ");  
  };  
};  
}
```

The diagram illustrates a network topology for protection. It features a central Core router connected to multiple Edge routers. On the left, a dashed box encloses two Edge routers connected to nodes A1 and A2. Another dashed box at the bottom encloses an Edge router connected to node A3. A final Edge router on the right is connected to a terminal labeled 'T'. The Core router is the central hub connecting all these components.

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

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

```
C:\WINDOWS\system32\cmd.exe - TC.EXE  
void hablar(Contenido) {  
[s] [Contenido] != "4. PROTECCION PRESENTA.CPP /** PANORAMA GENERAL */"  
else {  
  slide() {  
    printf("%s", "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  
  );  
  });  
}
```

The diagram illustrates a network topology. A central Core router is connected to five Edge routers. The Edge routers are connected to various devices: A1, A2, A3, and T. A dashed box highlights the Core router and its connections to the Edge routers.

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

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

```
C:\WINDOWS\system32\cmd.exe - TC.EXE  
void hablar(Contenido) {  
[s] [Contenido] != "4 - PROTECCION" PRESENTA.CPP /** PANORAMA GENERAL **/  
else {  
  slide() {  
    printf("%s",  
      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.  
    printf("%g",  
  );  
  });  
}
```

The diagram illustrates a network topology. A central Core router is connected to four Edge routers. The Edge routers are further connected to various hosts. Hosts A1 and A2 are connected to one Edge router, A3 to another, and T to a third. The fourth Edge router is not connected to any host. Dashed boxes group the Edge routers and their associated hosts.

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



# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

The screenshot shows a Turbo C++ IDE window titled "C:\WINDOWS\system32\cmd.exe - TC.EXE". The menu bar includes File, Edit, Search, Run, Compile, Debug, Project, Options, Window, and Help. The code editor displays a C++ program with the following content:

```
void hablar(Contenido) {  
[s] [Contenido] != "4 . PROTECCION" PRESENTA.CPP /** PANORAMA GENERAL **/  
else {  
  slide() {  
    printf("%s", "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  
");  
    printf("%g", "Reacción");  
  };  
};  
}
```

At the bottom of the IDE, a status bar shows function key shortcuts: F1 Help, F2 Save, F3 Open, Alt-F9 Compile, F9 Make, and F10 Menu.

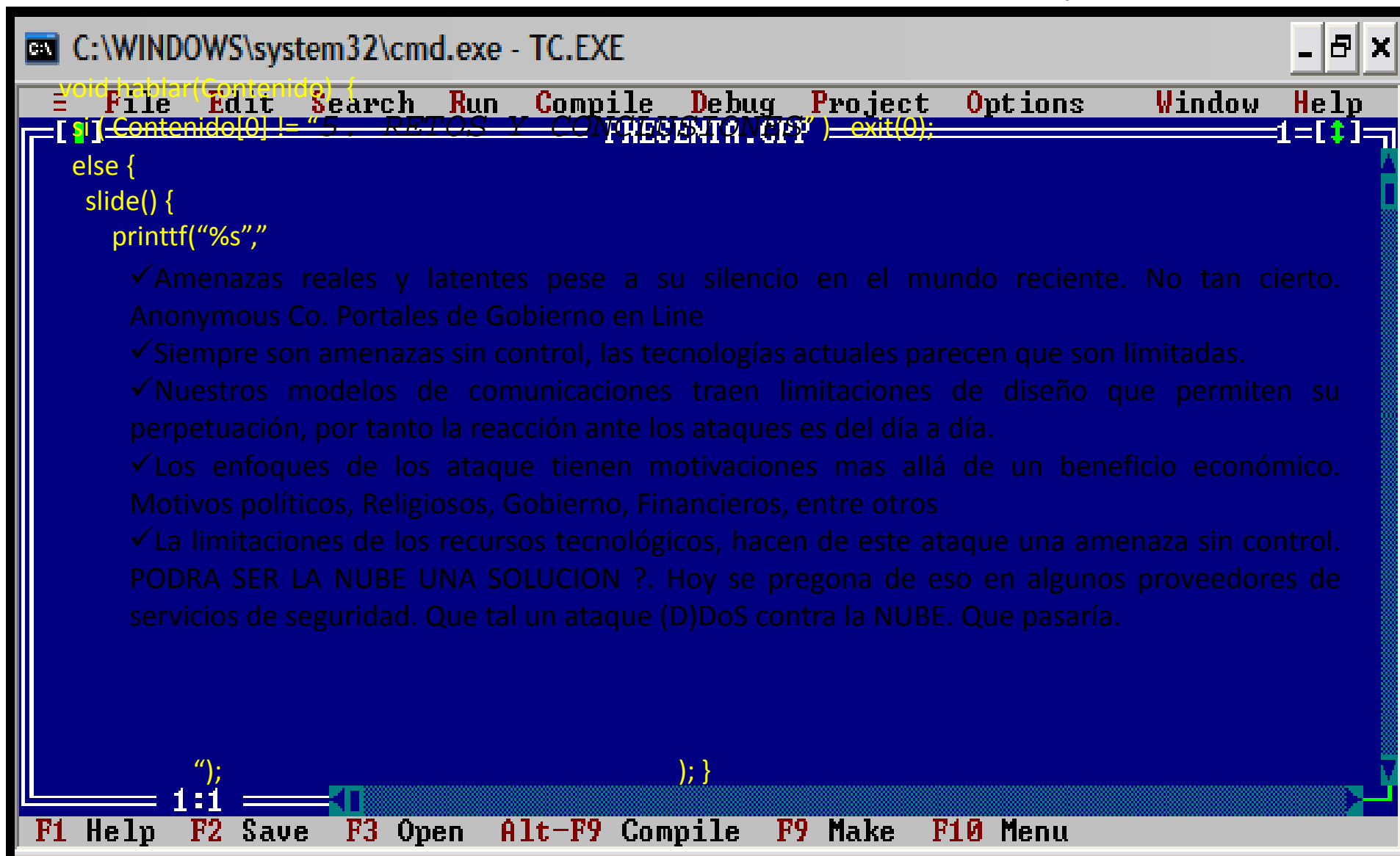
Overlaid on the right side of the IDE is a circular diagram illustrating the protection strategy cycle. The cycle consists of five stages connected by arrows in a clockwise direction:

- Análisis posterior
- Preparación
- Detección
- Caracterización
- Reacción

```
graph TD; A[Análisis posterior] --> B[Preparación]; B --> C[Detección]; C --> D[Caracterización]; D --> E[Reacción]; E --> A;
```

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar



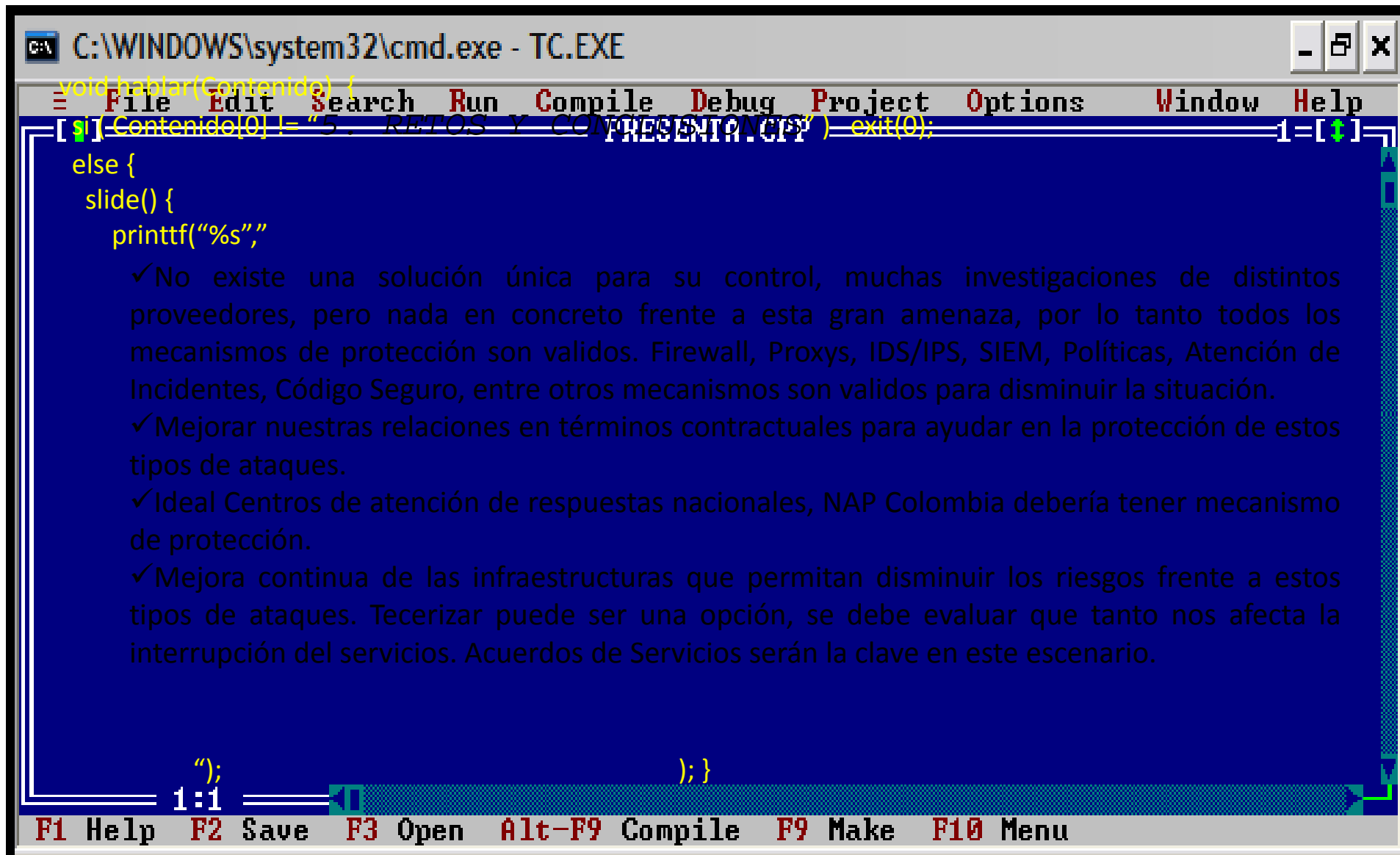
The screenshot shows a Turbo C++ IDE window titled "C:\WINDOWS\system32\cmd.exe - TC.EXE". The menu bar includes File, Edit, Search, Run, Compile, Debug, Project, Options, Window, and Help. The code editor displays a C++ function named "hablar" that prints a slide of text. The slide content is as follows:

```
void hablar(Contenido) {  
    if (Contenido[0] != "5 . RETOS Y CONVICIONES") exit(0);  
    else {  
        slide() {  
            printf("%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.  
            );  
        };  
    }  
};
```

The status bar at the bottom shows function key shortcuts: F1 Help, F2 Save, F3 Open, Alt-F9 Compile, F9 Make, and F10 Menu.

# ACIS XI Jornada de Seguridad Informática

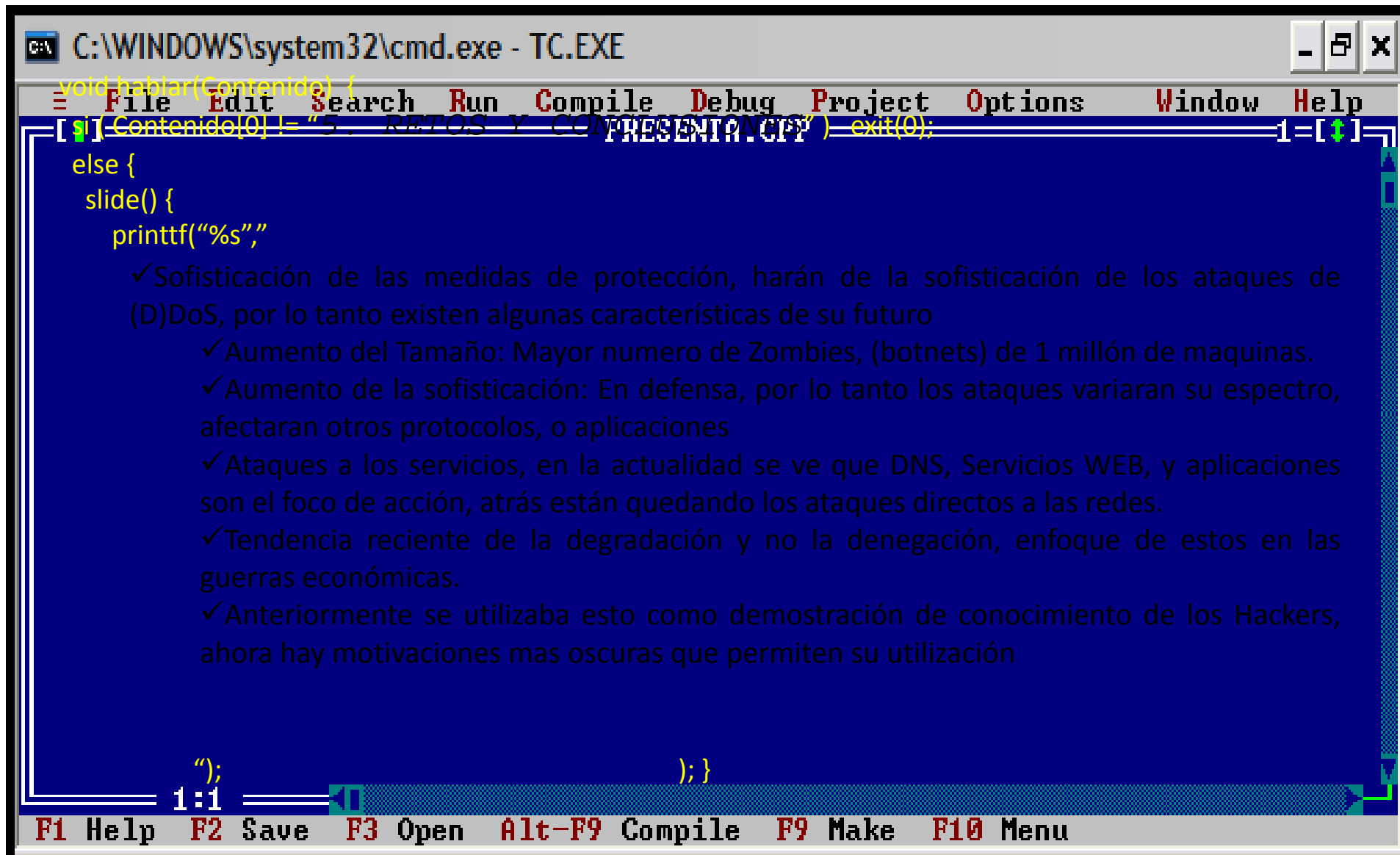
Seguridad de la Información:  
Una nueva década para avanzar



```
C:\WINDOWS\system32\cmd.exe - TC.EXE
File Edit Search Run Compile Debug Project Options Window Help
[ s ] [ Contenido ] != "5. RETOS Y CONCEPTOS" ) exit(0);
else {
  slide() {
    printf("%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.
    );
  };
};
F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu
```

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

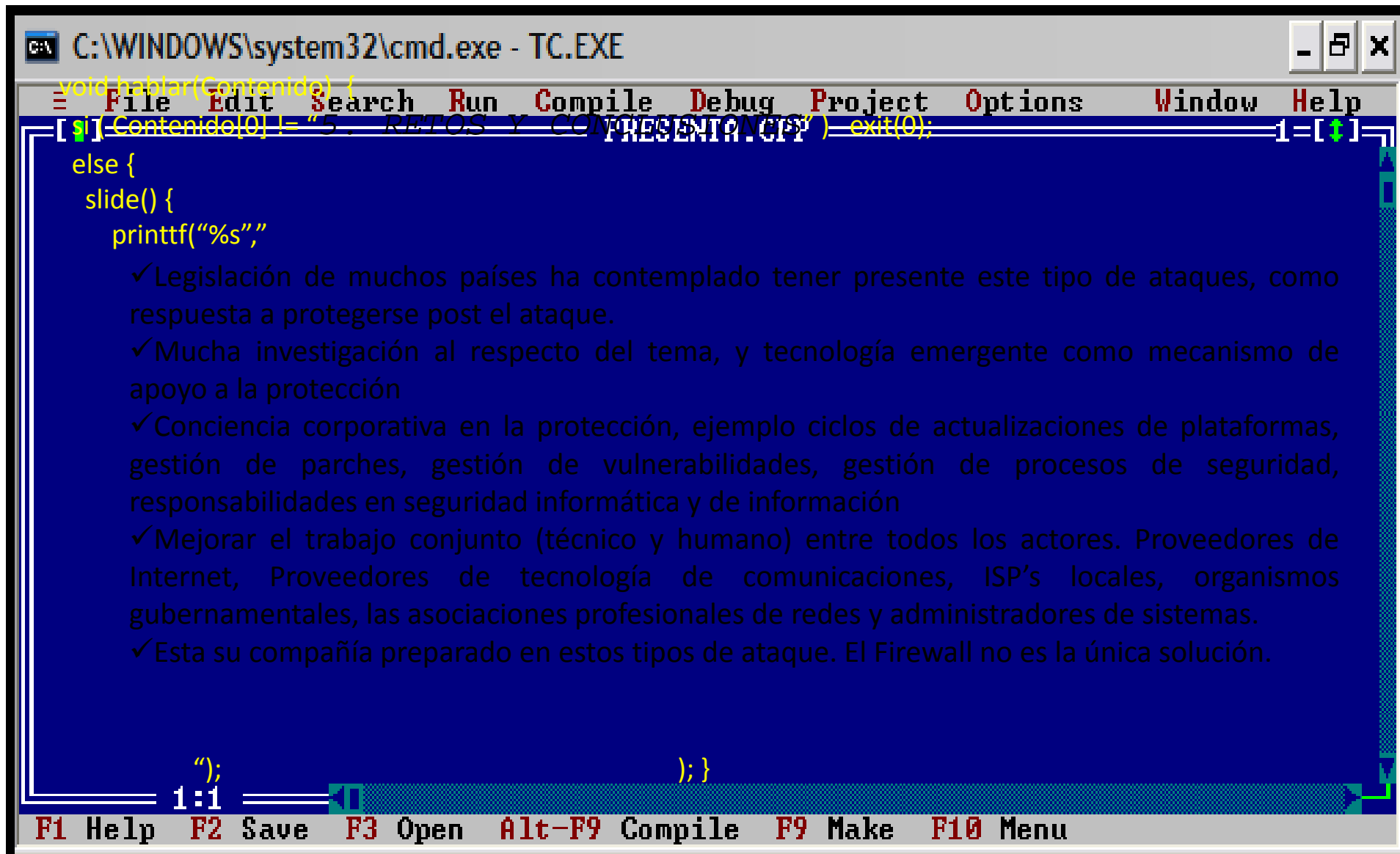


```
void hablar(Contenido) {
s[Contenido] != "5. RETOS Y CONCEPTOS") exit(0);
else {
slide() {
printf("%s",
    ✓Sofisticación de las medidas de protección, harán de la sofisticación de los ataques de
(D)DoS, por lo tanto existen algunas características de su futuro
    ✓Aumento del Tamaño: Mayor numero 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
");
};
};
```

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

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar



The image shows a screenshot of a Turbo C++ IDE window. The title bar reads "C:\WINDOWS\system32\cmd.exe - TC.EXE". The menu bar includes "File", "Edit", "Search", "Run", "Compile", "Debug", "Project", "Options", "Window", and "Help". The main window displays a presentation slide with the following content:

```
void hablar(Contenido) {  
    [s] [Contenido] != "5. RETOS Y CONCEPTOS" ) exit(0);  
    else {  
        slide() {  
            printf("%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.  
            );  
        };  
    }  
};
```

At the bottom of the window, there is a status bar with the following text: "1:1" and "F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu".



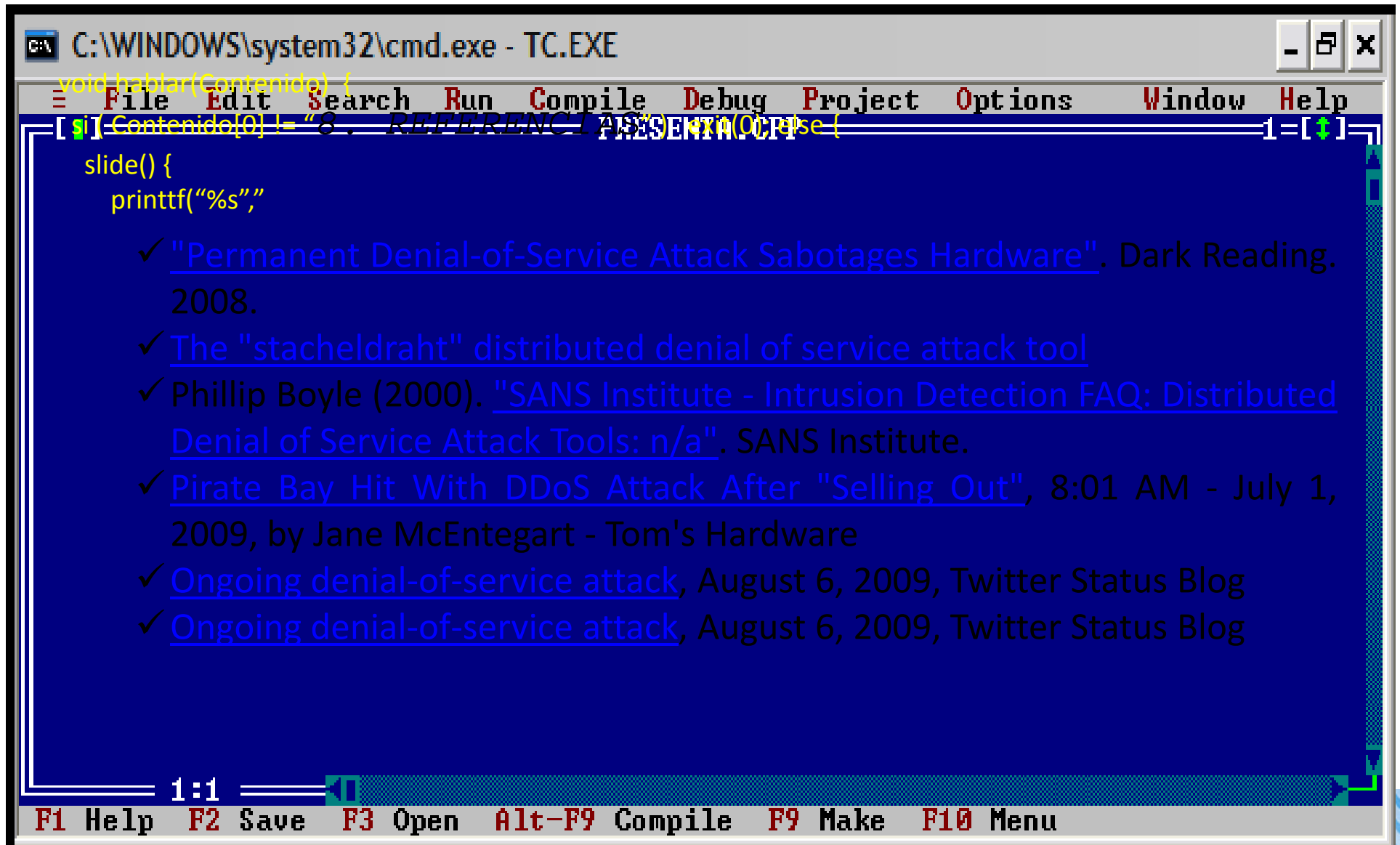
# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar

```
C:\WINDOWS\system32\cmd.exe - TC.EXE
void hablar(Contenido) {
[ s ] [ Contenido ] := "6 . REFERENCIAS PRESENTACIONES {
slide() {
  printf("%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
```

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar



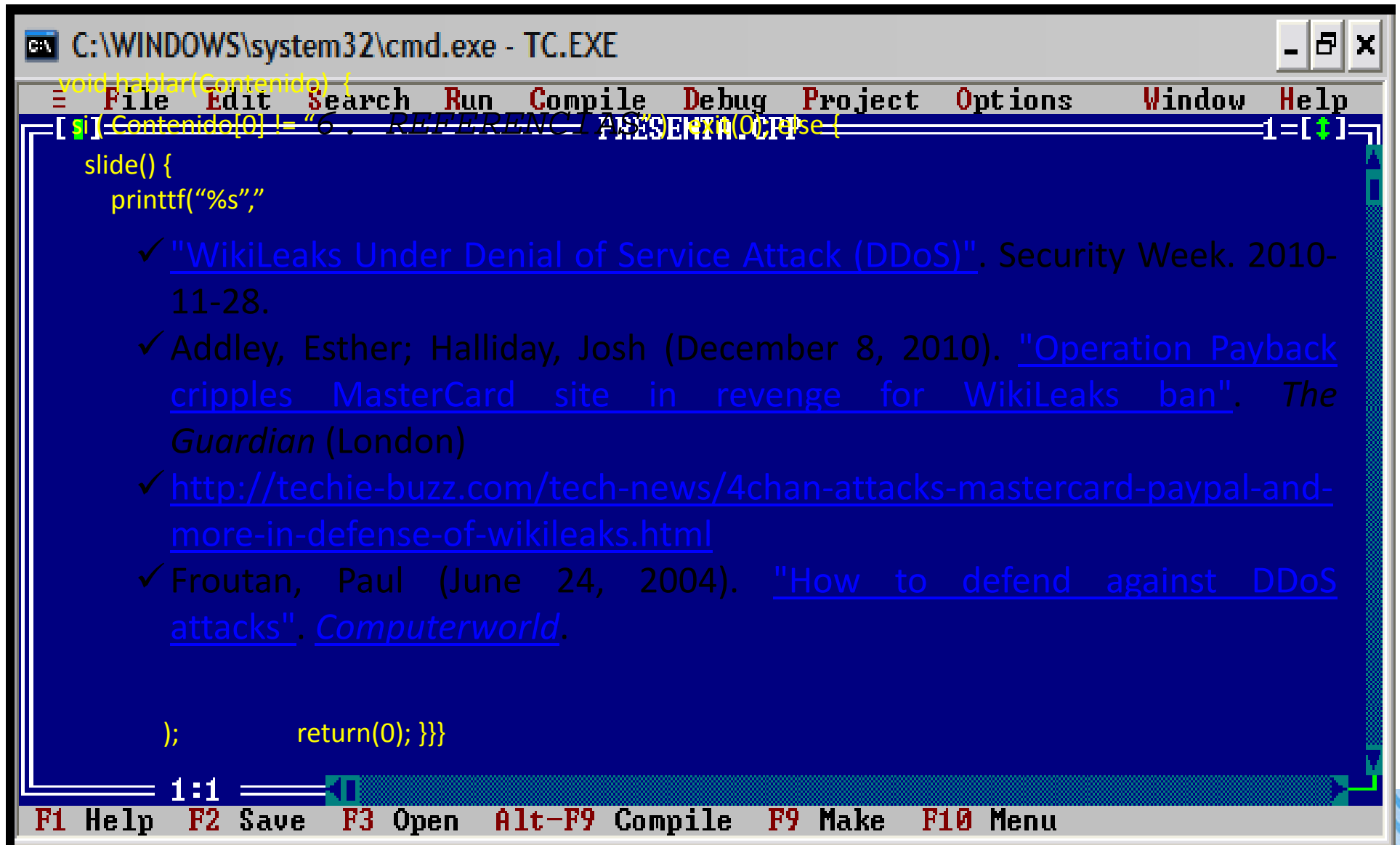
The screenshot shows a Turbo C++ IDE window titled "C:\WINDOWS\system32\cmd.exe - TC.EXE". The menu bar includes File, Edit, Search, Run, Compile, Debug, Project, Options, Window, and Help. The main text area displays a slide with the following content:

```
void hablar(Contenido) {  
[s] [Contenido] != "8 . REFERENCIAS PRESENTACION" {  
slide() {  
printf("%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
```

At the bottom of the window, there is a status bar with the text "1:1" and a set of keyboard shortcuts: F1 Help, F2 Save, F3 Open, Alt-F9 Compile, F9 Make, and F10 Menu.

# ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:  
Una nueva década para avanzar



The screenshot shows a Turbo C++ IDE window titled "C:\WINDOWS\system32\cmd.exe - TC.EXE". The menu bar includes File, Edit, Search, Run, Compile, Debug, Project, Options, Window, and Help. The main editing area contains C++ code with a slide of references. The code is as follows:

```
void hablar(Contenido) {  
    [s] [Contenido] != "6 . REFERENCIAS PRESENTACION" {  
        slide() {  
            printf("%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); }  
    }
```


The status bar at the bottom shows "1:1" and function key shortcuts: F1 Help, F2 Save, F3 Open, Alt-F9 Compile, F9 Make, and F10 Menu.

# 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 1=[↑]
si ( Contenido[0] != "\n.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
```