互联网网络安全信息通报

国家计算机网络应急技术处理协调中心广东分中心　　5 月 13 日

1.概述

（　　L c dl h

L cc 8gn

公

L c dl h HB7　　BH ，

们

业

全　　l cc Xgn

#

#

# #

一

1

# #

全

全

全 全

公

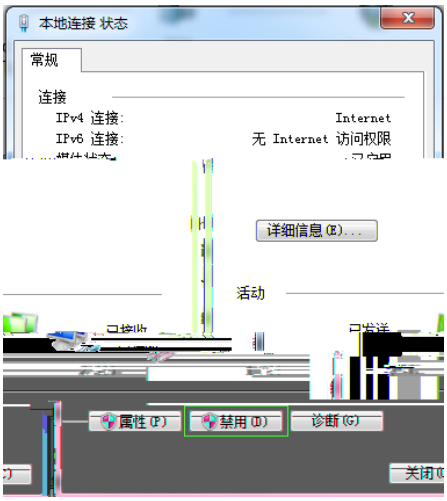
#(

- 全
- 445

  445
-

#(# **Win7 Win8 Win10**

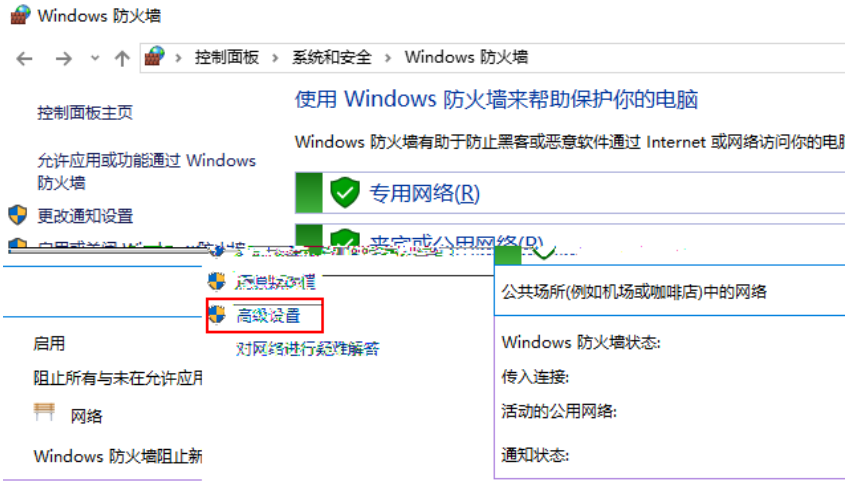
1) 全



2) 别 - -Windows 全 Windows

3)

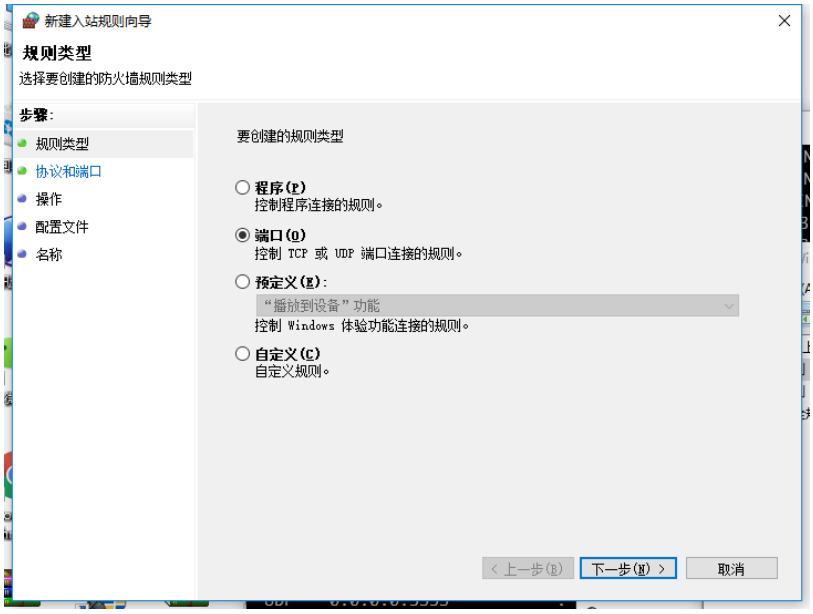
4)


Windows 防火墙
控制面板 › 系统和安全 › Windows 防火墙
控制面板主页
允许应用或功能通过 Windows 防火墙
更改通知设置
使用 Windows 防火墙来帮助保护你的电脑
Windows 防火墙有助于防止黑客或恶意软件通过 Internet 或网络访问你的电
专用网络(R)
高级设置
对网络进行疑难解答
启用
阻止所有与未在允许应用
网络
Windows 防火墙阻止新
公共场所(例如机场或咖啡店)中的网络
Windows 防火墙状态:
传入连接:
活动的公用网络:
通知状态:

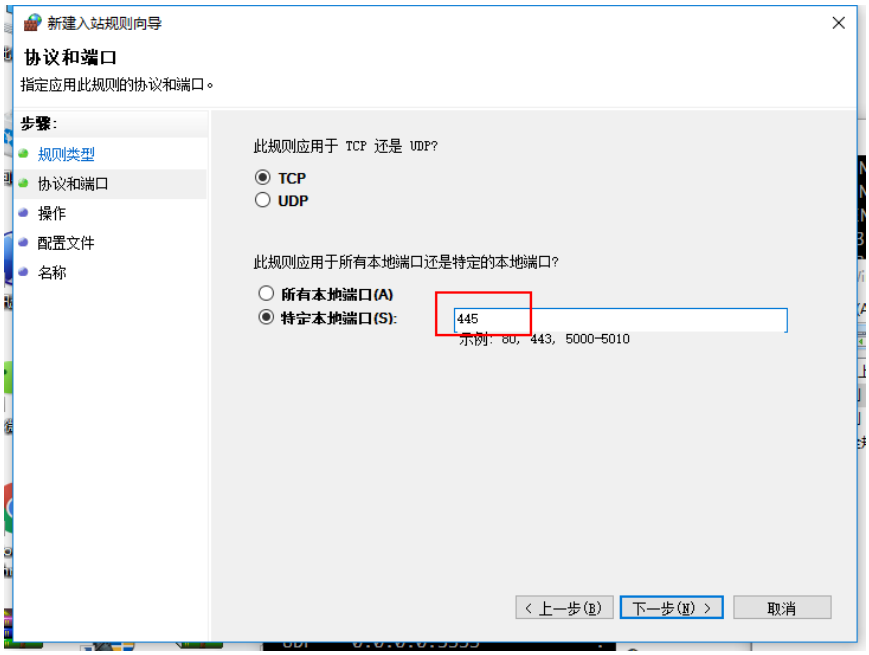
5) 445


高级安全 Windows 防火墙
文件(F) 操作(A) 查看(V) 帮助(H)
本地计算机 上的高级安全 Win
入站规则
出站规则
连接安全规则
监视
入站规则
名称
组
aapt
操作
新建规则...
按配置文件筛选
按状态筛选
按组筛选
查看
刷新

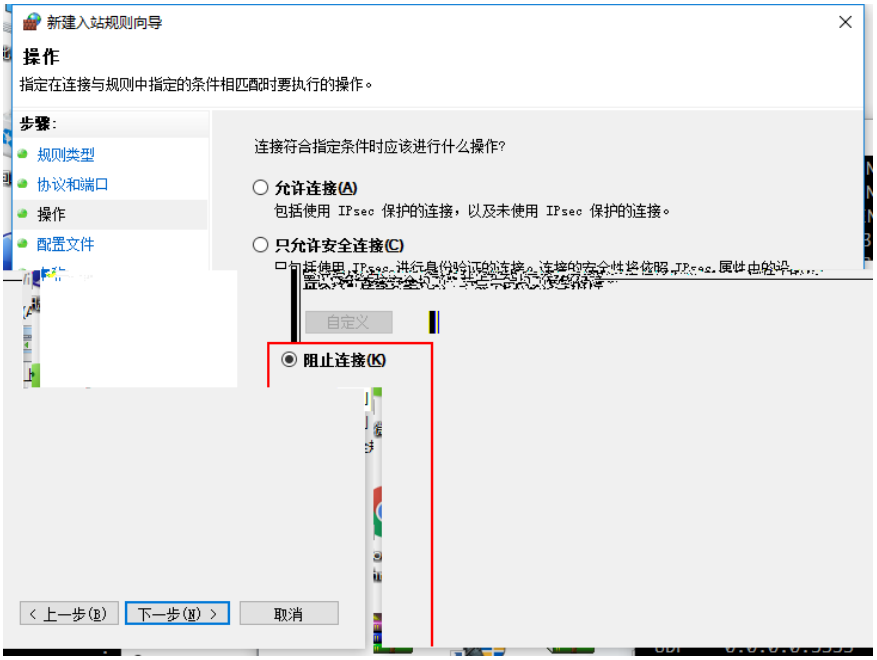
6) —


新建入站规则向导
规则类型
选择要创建的防火墙规则类型
步骤:
规则类型
协议和端口
操作
配置文件
名称
要创建的规则类型
程序(P)
控制程序连接的规则。
端口(O)
控制 TCP 或 UDP 端口连接的规则。
预定义(E):
"播放到设备"功能
控制 Windows 体验功能连接的规则。
自定义(C)
自定义规则。
< 上一步(B)
下一步(N) >
取消

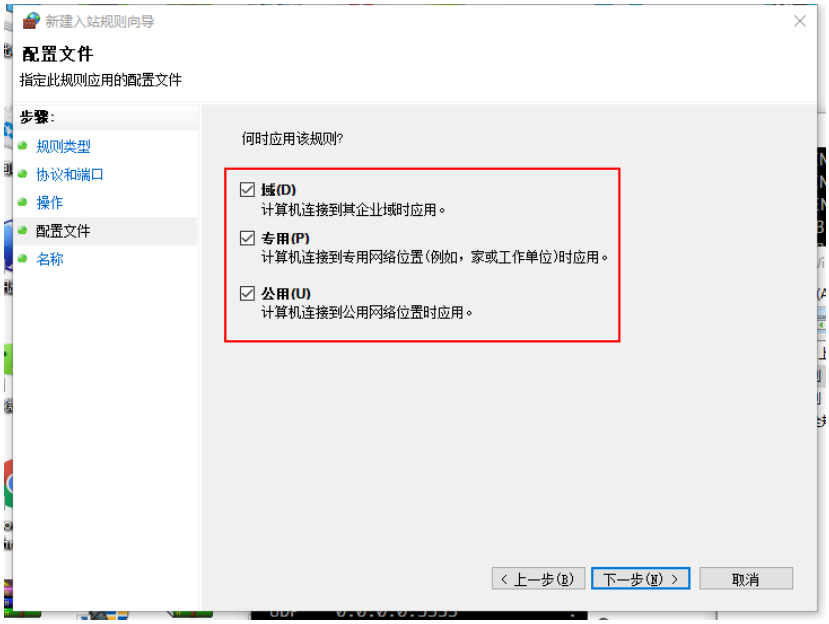
7) 445 —


新建入站规则向导
协议和端口
指定应用此规则的协议和端口。
步骤:
规则类型
协议和端口
操作
配置文件
名称
此规则应用于 TCP 还是 UDP?
TCP
UDP
此规则应用于所有本地端口还是特定的本地端口?
所有本地端口(A)
特定本地端口(S):
445
示例: 80, 443, 5000-5010
< 上一步(B)
下一步(N) >
取消

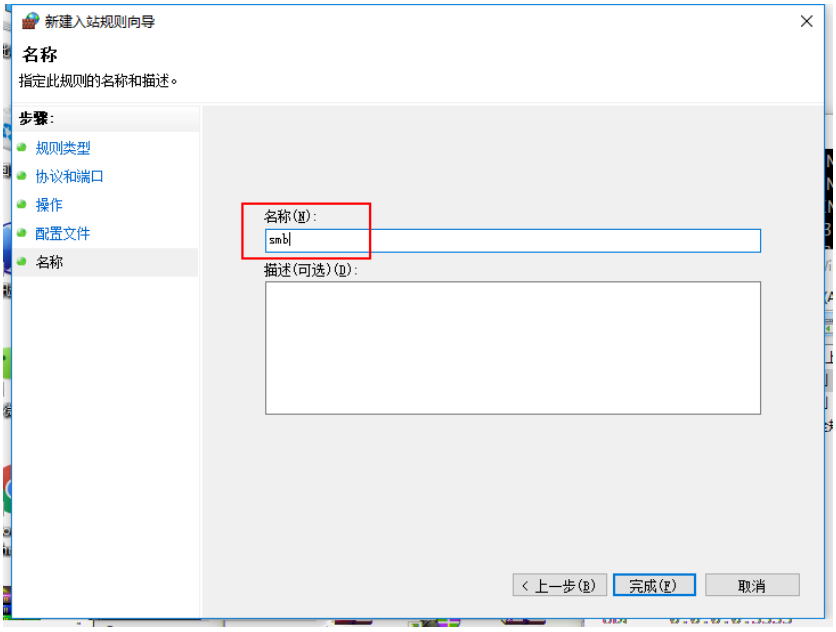
8) —


新建入站规则向导
操作
指定在连接与规则中指定的条件相匹配时要执行的操作。
步骤:
规则类型
协议和端口
操作
配置文件
连接符合指定条件时应该进行什么操作?
允许连接(A)
包括使用 IPsec 保护的连接，以及未使用 IPsec 保护的连接。
只允许安全连接(C)
自定义
阻止连接(K)
< 上一步(B)
下一步(N) >
取消

9) —



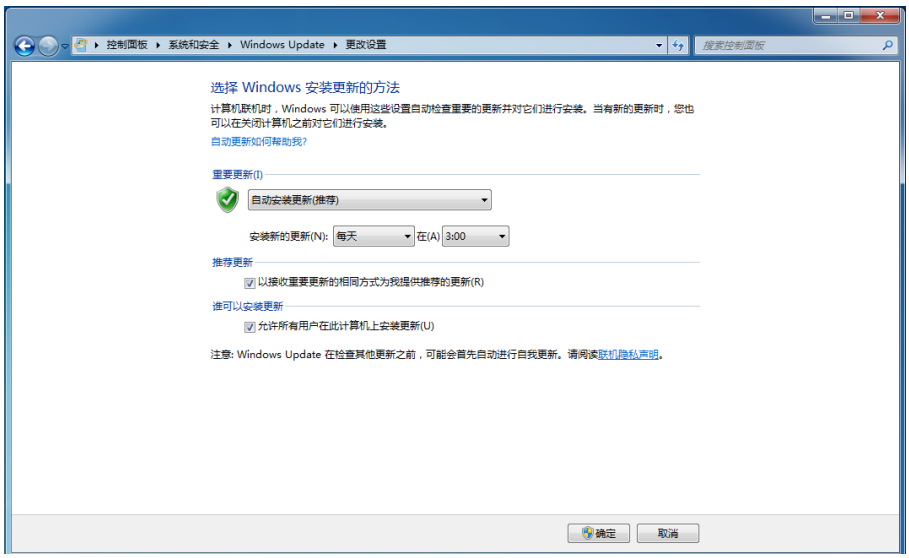
10)



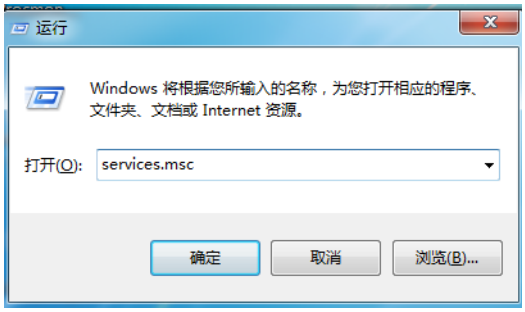
11) MS17-010 winxp_sp3 win10 win2003 win2016 —

https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/?from=timeline&isappinstalled=0

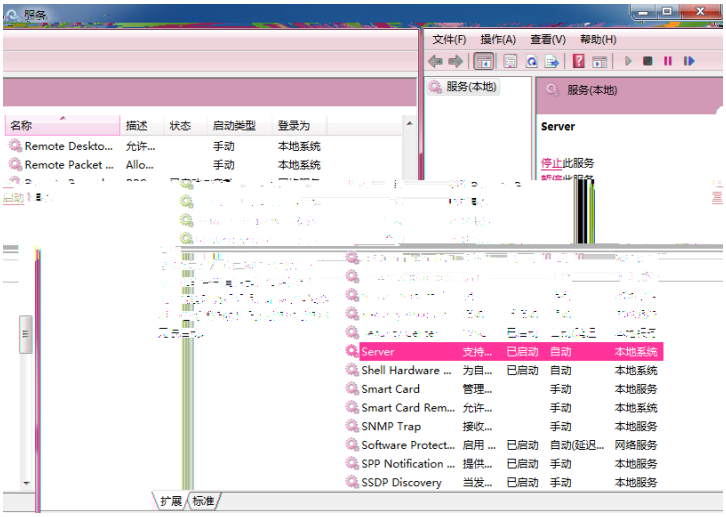
12)

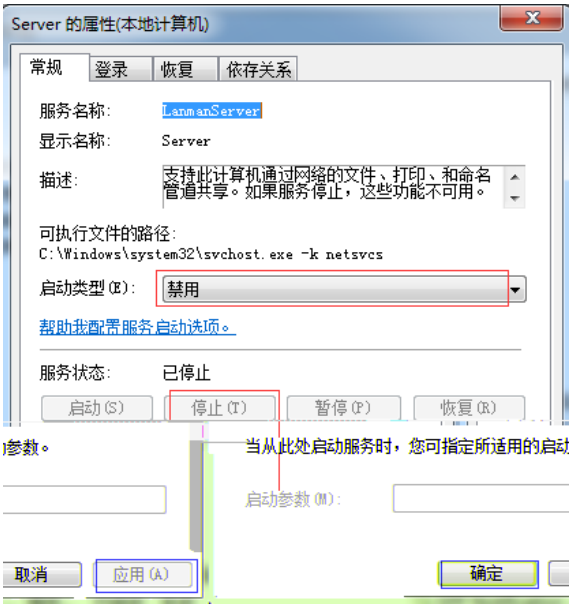


13) Win7 全 Server 445
server 全 services.msc
别

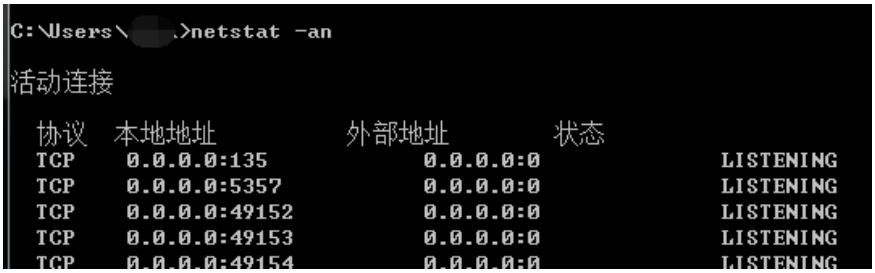


Server

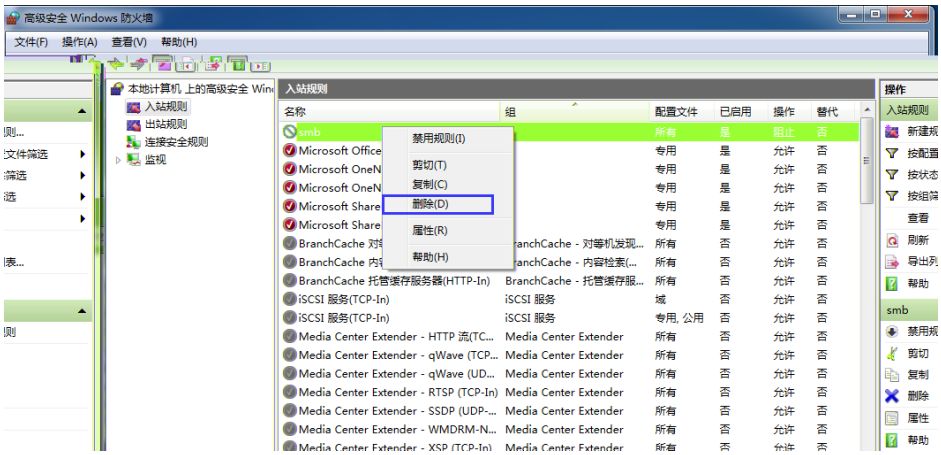




win7 netstat an 445

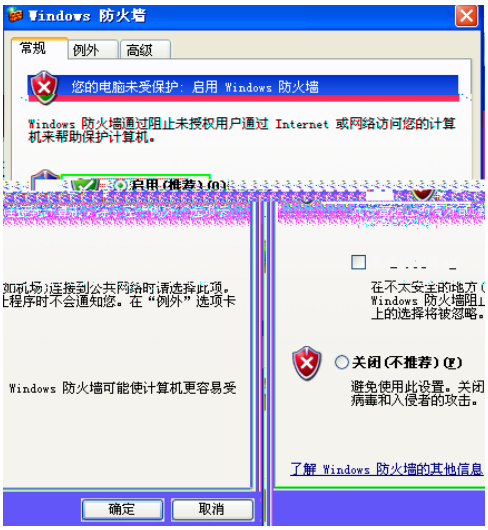


SMB

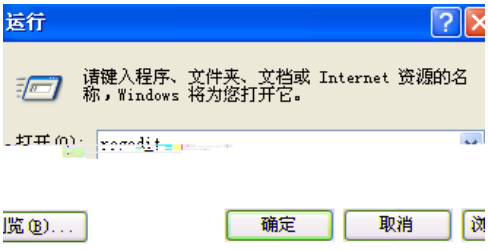


#(# Win ME

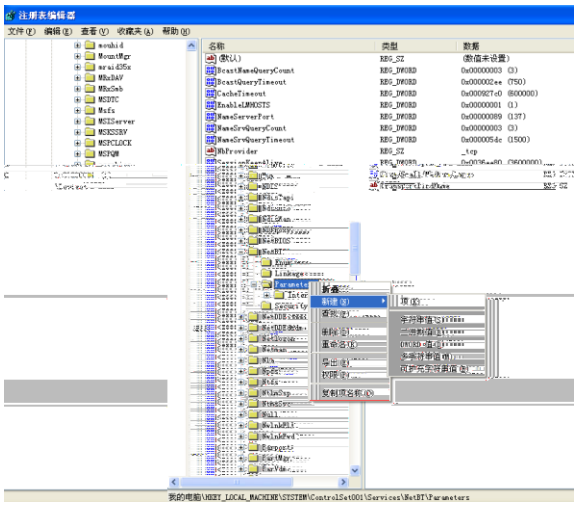
1) 别 Windows



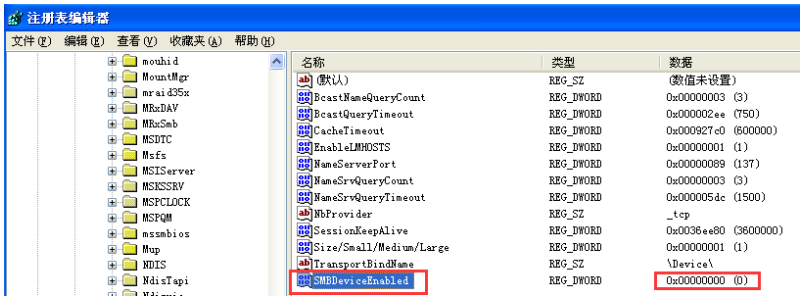
2) 全 445 regedit



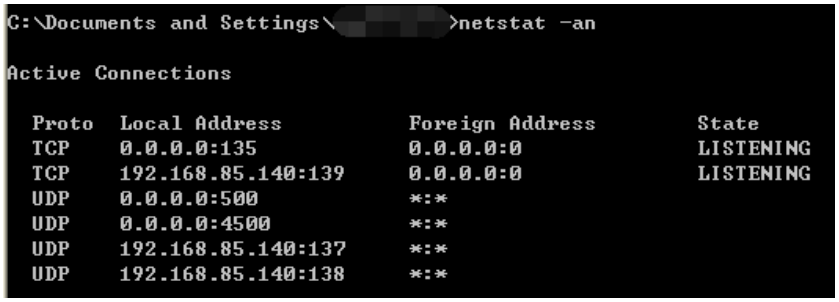
3) HKEY_LOCAL_MACHINE\System\Controlset\Services\NetBT\Parameters
Parameters DWORD



4) DWORD SMBDeviceEnabled 0



5) 445



6) Wannacry XP 击

删 /

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

#

击

68A 别

I8E))

68A I8E)) 一

68A I8E))

人

c e g /

h i [g l aa [b an c i [ai g cn l cc Xgn i gb cn)) [gdb egdidXda iXe

h i [g l aa [b an c i [ai g cn l cc Xgn i gb cn)) [gdb

hi c i dc edgi))

h i [g l aa [b an c i [ai g cn l cc Xgn i gb cn)) i] c hX g

h i [g l aa [b an c i [ai g cn l cc Xgn i gb [ai i] c XX ei

h i[dgl g c dei dch [b an c i [ai g d ie i cn l cc Xgn

h i[dgl g c dei dch [b an c i [ai g ce i cn l cc Xgn

h i ci g[X h P R c i [b an c i [ai g d ie i cn l cc Xgn

h i ci g[X h P R c i [b an c i[ai g ce i cn l cc Xgn

(8 /

/

Xa c bW g (

g a cn iXe hi c i dc edgi))

g a e gb i e

ci g[X P R

e X i [ai g (cWd c

e X i [ai g (d iWd c

/

Xa c bW g (

g a e gb i iXe hi c i dc edgi))

ig [[X Xa hh [g cn l cc Xgn
[b iX] Xa (

ig [[X W] k dg cn l cc Xgn
[ai g cn

fdh eda Xn cn l cc Xgn
Xa hh [g cn l cc Xgn W] k dg cn l cc Xgn

fdh eean eda Xn cn l cc Xgn adW a cWd c
fdh eean eda Xn cn l cc Xgn adW a d iWd c

ci g[X P R
fdh eean eda Xn cn l cc Xgn cWd c
fdh eean eda Xn cn l cc Xgn d iWd c

#(/

Xa c bW g (
g a cn iXe hi c i dc edgi f))
g a e gb i e

ig [[X Xa hh [g cn l cc Xgn ine c
[b iX] Xa (

ig [[X W] k dg cn l cc Xgn

ig [[X eda Xn cn l cc Xgn
Xa hh [g cn l cc Xgn W] k dg cn l cc Xgn eg X cX

```
 ci g[ X  P                      R
ig [[ X eda Xn   cn l cc Xgn    cWd c
ig [[ X eda Xn   cn l cc Xgn   d iWd c
```

 # #) 8 hXd /

```
     /
 e   XX hh a hi  mi c      cn l cc Xgn
  cn iXe  cn  cn  f ))
e gb i  e  cn  cn

 ci g[ X  P                      R
 e   XX hh  gd e   cn l cc Xgn   c
 e   XX hh  gd e   cn l cc Xgn  d i

     /
 e   XX hh a hi   cn l cc Xgn
  cn iXe  cn  cn  f ))
e gb i  e  cn  cn

 ci g[ X  P                      R
 e   XX hh  gd e   cn l cc Xgn   c
 e   XX hh  gd e   cn l cc Xgn  d i
```

 # # /

```
 e   XX hh a hi  mi c      cn l cc Xgn
  cn iXe  cn  cn  f ))
e gb i  e  cn  cn
 ci g[ X   P                     R
```

e XX hh gd e cn l cc Xgn c

e XX hh gd e cn l cc Xgn d i

#(

CH6 公 全

CH6

ME (公 全

CH6

CH6 公一]iie/ a#(h [#Xdb ch ch idda# m

全 击

击

8 GI 88 8 GI

8C8 GI 88 8C8 GI

击 双

件

lll#X gi#dg #Xc

b a 5X gi#dg #Xc

\- (-()