**Windows 2003 Server Game Plan**:

Get the IP address of the machine:

Start->Command Prompt

Enter ipconfig /all

Let Mike know the IP address for offensive purposes

## 1 - Log in: User:Administrator Pass:changeme?

## 2 - Turn on Firewall ASAP!

**Option 1)** Fast:

Start->Command Prompt

Run the following

netsh firewall set opmode enable

netsh firewall add portopening TCP 25 SMTP enable

netsh firewall add portopening TCP 110 POP3 enable

Check to make sure each resulted in “Ok.”

This only filters incoming traffic, not outgoing.

Better way)

**Option 2)** Slow:

Start->Control Panel->Network Connections

Right Click on Local Area Connection->Properties->Advanced Tab

Under Windows Firewall, select Settings

Select “On”

Click Exceptions Tab

Click “Add Port”

Name: SMTP

Port Number 25

Protocol: TCP

Repeat for the following:

Name: POP3

Port number:110

Proto: TCP

Click OK

Click OK

Should show that the connection is Connected and Firewalled

If there are other connections, secure those as well.

## 3- Change passwords:

Control Panel->Administrative Tools->Computer Management

Local Users and Groups from the Left Pane

Double Click on Users

Make note of users that are on the box and don’t have a red X in the icon

For all enabled users-> Right Click->Set Password

Enter a new password, make sure to note which accounts have been changed and what they are changed to in case we need to submit it to the white team

## 4 – Disable IPV6 (for now)(unless it’s the only thing running):

Start->Control Panel->Network Connections

Right Click on Local Area Connection->Properties

Under General Tab in the section “This connection uses the following items:”

Uncheck Microsoft TCP/IP version 6

IMPORTANT: if you uncheck the above, make sure that the following is checked: Internet Protocol (TCP/IP)

If we’re only running IPV6 don’t disable it

## 5 - Get a list of the connections listening on the box:

Start->Command Prompt

netstat –ant

make a note of what these are so that we can look into them…

Move on to the next machine for now…

## Notes:

**ADDING AND REMOVING FIREWALL ENTRIES:**

Adding:

Start->Command Prompt

netsh firewall add portopening <TCP/UDP> <port number> <name> enable

Removing:

Start->Command Prompt

netsh firewall del portopening <TCP/UDP> <port number>

a result of “Ok.” means it was successful

**Checking for and removing Persistence:**

Start->cmd

reg query HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

If it comes up blank, might mean no persistence. If theres something ending with a .vbs value = BAD NEWS

Removing it:

reg delete HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /va

answer yes to prompt.