Global Information Assurance Certification Paper

Submission for GIAC Security Essentials Certification
Practical Assignment Version 1.4 Option 1

Deploying Secure Public Kiosk Networks Jon Shaffer

Abstract

The purpose of this paper is to provide a "how-to" for building a public kiosk network while keeping in mind the theory of "defense in layers". A kiosk is a controlled way of providing information to general users. Kiosks work well in large public areas as a compliment to information booths and public displays. Kiosks, by nature of their public location, are vulnerable to hacks and malicious activity. When setting up a public Kiosk you must have a clear idea of what information you are going to provide. The information could consist of corporate specific news and events, travel information like arrival and departure changes at an airport, controlled Internet access, or controlled intranet access to internal corporate data. This "how-to" will go over a generic design that has the flexibility to provide control in all of the above scenarios. Kiosks become especially troublesome if they are connected to a corporate network, providing access to internal corporate information. The approach taken in this document is to add layers of defense in multiple areas of the protocol stack to deter the hacker from easily affecting the proper operation of these devices.

The layers of defense addressed in this paper will be broken out into 4 areas; the Kiosk Workstation Physical/Bios layer, the MAC layer-Switch port configuration, the Network Layer-ipchains and commercial firewalls, and the Application Layer-Active Directory and Group policies. One section is added to the end of the paper to include some miscellaneous tips.

Design and Components

The components used for the purpose of this paper will consist of the following:

- Windows 2000 servers implementing group policies
- Window 2000 workstations with Fixed mouse control running internet explorer in Kiosk mode
- Managed switches (i.e. Nortel Networks Business Policy Switches)
- Linux compatible workstation with ipchains installed
- Commercially available firewall installed on compatible hardware (i.e. Symantec Enterprise firewall)

The components are shown together in a network design on Page 5.

Workstation Security

Kiosk workstation Bios Configuration

The Modern Bios will provide basic security from hacking through a Bios Password. Chose the "**Protect BIOS configuration"** option in the system BIOS configuration. This will stop BIOS access but still allow the computer to reboot without human intervention. The password should be considered hard to guess by following a set of hard to guess password rules:

- The password should be at least eight characters long
- Contain a mixture of digits, punctuation, upper, and lower case letters.
- Should never contain personal information or interests. (e.g. birthdays, names, etc.)
- Easy to remember by using acronyms. (e.g. **I n**eed **t**o **p**rotect **t**his **p**ublic **k**iosk **24*7** = InTpTpK24*7)

The physical box must be secured in order to prevent access to the interior of the PC because removing a jumper on the motherboard or removing the bios battery can reset Bios passwords. The physical security of the workstation will be discussed later.

After securing the bios with a password there are several other bios settings to configure that can deter a hacker from using the Kiosk as a malicious tool.

Disable Floppy and CD drive access and remove them from the boot order.

If physical access to the workstation is obtained you want to make it difficult for the intruder to load malicious software through the floppy and CD drives. There are also commercial locking products that cover the opening and prevent inserting media into these drives. An example can be found at http://www.kensington.com/products/pro_c1378.html .

Enable restart after power outage

This should be enabled because, in most cases, the physical access to the power button on the workstation will be restricted and following a power outage you will want the kiosk to power back up without user intervention.

Kiosk Workstation Physical Security - Restrict Physical Access to the workstation

Upon completion of the bios settings it must be insured that physical access to the workstation is secured. Building a locked structure with adequate ventilation should be enough of a deterrent. More security can be added through surveillance cameras or extending the video and mouse connections from a secure remote location holding the workstation. It is also important to limit access to the keyboard because certain key combinations can foil security during the boot process.

If it is not possible to place the workstation inside of a secure location, secure physical access to the interior of the pc by placing a padlock on the system that locks the case to the chassis of the computer and secure the chassis of computer to the counter.

A fixed mouse control, like those available from Interlink Electronics at http://www.interlinkelec.com/products/retail/durapoint.htm#durapointoem, can be securely surface mounted and provide enough flexibility for the user to access the corporate content through a well designed html kiosk page. The html kiosk page will become the default home page loaded automatically on boot up.

Switch Security-Mac Layer

Management Access

The first step to securing switches on the network is to check what management access is available on the switch used. This design uses managed Nortel Business Policy switches.

These managed switches, like most, allow console/configuration access through several methods[1]:

1) Console Interface through a serial connection directly to the switch on an RS232 management port
2) Console Interface from a Telnet connection through any of the switched ports on the management VLAN[2]
3) GUI Interface from SNMP requests through any of the switched ports on the management VLAN
4) Web browser Interface through any of the switched ports on the management VLAN

During the initial configuration you must connect directly through the RS232 port. You should set a password on the telnet, RS232 and Web access. Passwords should follow the hard to guess password rule as described above. The telnet sessions can and should be configured to only allow connections from management IP addresses.

Note: These switches can be configured with multiple VLANS. If multiple VLANS exist on one switch, then one VLAN must be dedicated as the "management" VLAN, resulting in access to the managed settings only through ports designated as participants in that VLAN. This could be another layer of defense by separating management VLANS from other "public traffic" VLANS.

CERT Advisory CA-2002-03, http://www.cert.org/advisories/CA-2002-03.html, recommends looking at SNMP very closely when configuring your network devices[3]. There have been vulnerabilities noted in the SNMPv1 protocol. The advisory suggests combining some of the following measures to secure your device.

1) Apply a patch provide by your vendor.
2) If not used, disable the SNMP protocol on your device.
3) Use Ingress filtering to prevent externally initiated access to SNMP services. The more common SNMP ports and their use are:

---

[1] Nortel Networks. "Using the Business Policy Switch 2000 Version 2.0" 208700c.pdf Pgs 88-91, 154-161
[2] Nortel Networks. "Getting Started with the Business Policy Switch 2000 Management Software " 209321a.pdf Pgs 17-20.
[3] Carnegie Mellon University CERT. "Cert Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP).".

snmp 161/udp # Simple Network Management Protocol
snmp 162/udp # SNMP system management messages

4) Filter SNMP traffic from non-authorized internal hosts.
5) Change the default SNMP community names. The defaults are usually public for read only access and private for read /write access.
6) Segregate all SNMP traffic onto a separate network. You could use the multiple VLANS technique mentioned above to separate this traffic.

Switch Port Security

Next in line is configuring the actual ports on the switch. You should turn off all unused ports on the switch. Making the only active ports to be the ones currently used by the Kiosk or other connections to other network devices.

You should also enable some MAC level security by associating the Kiosk MAC address with the physical port it is connected to on the switch. This will make it more difficult for someone to attach a foreign device to the network through the Kiosk physical connection. If the device does not have the exact MAC address of the assigned kiosk, the switch will deny access to the network. It is also a good idea to configure the switch to send intrusion detection SNMP traps to your network management system if a foreign MAC is detected on a secured port.

Note: In W2K you can get the MAC address information using the computer management plug-in for MMC under my computer/ control panel/ computer management/ system information/ components/ Network/ adapter. Or in NT4.0 and W2K you can get the MAC address using **ipconfig /all** at the command prompt.

Switch Physical Access Security

Like the workstation, the switch must be placed in a physically secured place with adequate environmental controls. Preferably a locked cabinet in a telecommunications closet secured with an electronic access control system allowing a method to track access in the event of an intrusion incident. Some cabinets provide other security features like environmental sensors to monitor the room or electronic triggers to turn on cameras when a cabinet is opened. An example of this type of equipment can be seen at http://www.wrightline.com/products/rackbotz.html.

Network Layer Security

This section will cover the overall design and configuration of the network. A diagram of the network is shown in Figure 1 on page 5. This includes the placement of Network Layer routing devices. This design uses a new segment added to an existing network infrastructure. It makes it easier if you are implementing a new segment because you can design it from the ground up with security in mind. In this design a new segment is created by placing a Linux workstation, that has two NICS, between the Kiosk network and the corporate

intranet segment. The intranet segment is connected to an interface on the commercial firewall that is connected to the Internet. The intranet segment could house corporate data that is only accessible from the Kiosks.

When using the devices shown in Figure 1, network layer IP based rules can be implemented in two locations:

1) Basic packet filtering at the Linux Router using ipchains with NAT through IP masquerading.

2) Complete Stateful packet inspection at the commercial firewall. This design uses Symantec Enterprise Firewall installed on a Windows 2000 server.

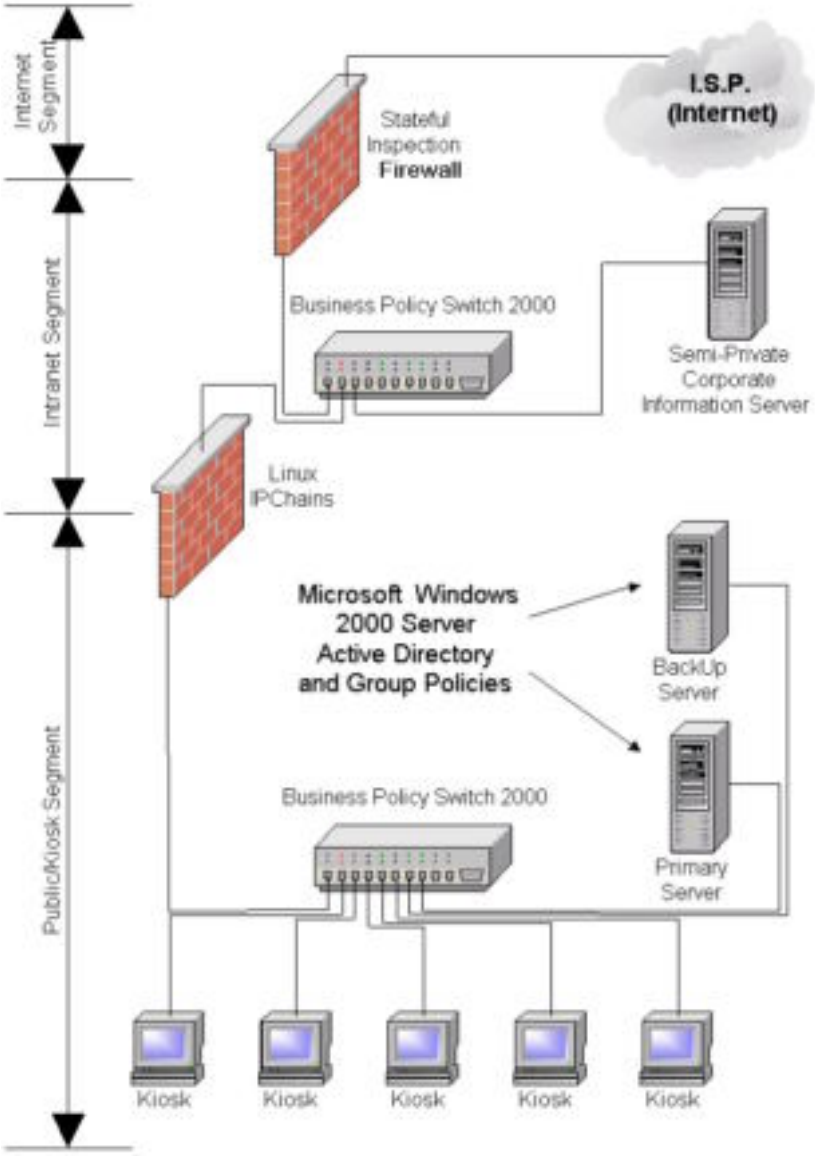

Figure 1. Network Design

Linux - ipchains

The installation of a linux router allows for some added filtering control and protection while removing some of the load from the interface on the commercial firewall by lowering the number of rules needed in the commercial firewall rule table. The ipchains, written by Paul "Rusty" Russell, is one more defensive layer added to the security of the network. The same functionality could also be achieved with iptables[4] and netfilter[5] the replacement for ipchains.

Using specially designed rules in ipchains, the forwarding characteristics of the router can be secured. Control is maintained by providing access to the interfaces of the router and adding rules that affect the way the packets are handled during the forwarding process. If access to an Internet resource is allowed, the packet source address is masqueraded and forwarded to the Symantec firewall. One rule is created in the Symantec firewall that allows access to the Internet for the masquerade address. This way you are able to add rules to the Linux router that specifically allow access to a particular Internet resource and have the commercial firewall deny all other non-masqueraded requests. By having the Symantec firewall deny the request you can configure a 403 forbidden html message page of something like "I am sorry but the web site you are attempting to reach is restricted access from this terminal" that will show on the screen for a few seconds and then refresh to the default Kiosk home page. Basically providing the user of the Kiosk with a "no harm, no foul" type of experience. For the Symantec enterprise firewall version 6.5.2 place the custom 403.html page in the raptor\firewall\sg\msgs\webroot directory.

Ipchains has three default lists of rules (chains). They are input, forward and output. Figure 2 shows the flow of the packet.[6]

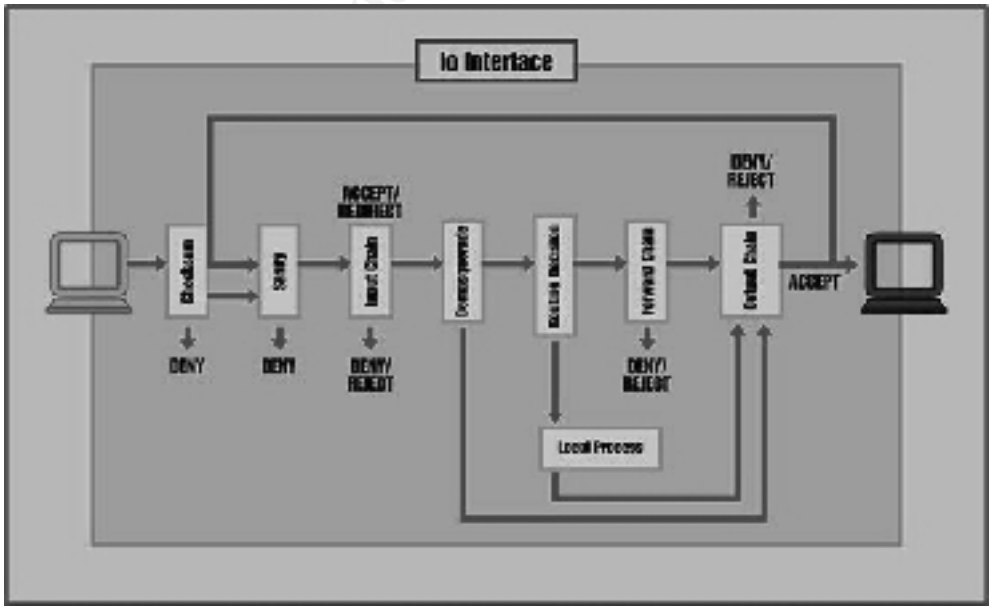

Figure 2. ipchains packet flow

[4] Oskar Andreasson, Iptables Tutorial 1.1.9
[5] Netfilter Core Team, The netfilter /iptables project
[6] Paul "Rusty" Russell, ipchains: Packet Filtering for Linux 2.2, figure 1.

The input chain is applied as the packet reaches the network card on the linux router. If the chain allows the packet to pass and its destination is through another network card then the packet has to pass through the forward chain. If the packet passes the forward chain requirements it is sent to the output chain and if it passes the output chain it is sent out.[7]

The basic commands are as follows:

ipchains -A chain appends to chain
ipchains -D chain deletes matching rule from chain
ipchains -L lists all the rules in all the chains
ipchains -F removes all the rules (Be careful with this one)

The syntax is:

ipchains -A *chain* -s *source* -d *destination* –i *interface* -p *protocol* -j *command*

The *chain* can be one of the defaults (input, output or forward), the *source* is where the packets are coming from, the *destination* is where the packets are going, the interface specifies the NIC dev, the *protocol* can be any of the protocol names in the /etc/protocol file, the command following the –j will cause ipchains to jump and do a particular command that determines the fate of the packet immediately (i.e. –j Accept to accept, -j reject to reject or –j MASQ to do NAT on the packet).

To find the current rules applied to the system run "ipchains –L" or "ipchains –L –n". The –n option will eliminate DNS lookup of the ipaddresses listed in the rules and will give quicker results.

To control what is be forwarded you should first set the default action of DENY on the forward chain.

ipchains –P forward DENY

Configuring the forward chain to accept and MASQ the packet when it is destined to an allowed web site.

An example chain rule looks like

ipchains –A forward –s 192.168.250.0/24 –d 64.12.37.89/32 –i eth0 –j MASQ

In this case the packet from the network 192.168.250.0 would be forwarded to the commercial firewall with a destination of 64.12.37.89 and would have its source address changed to the address of the interface of linux router. The commercial firewall would then be set up to accept requests having the linux router as the source and forward it to its destination.

After adding some of the allowed web sites to the chain rules, save the rule using the ipchains-save command.

[7] Paul "Rusty" Russell, IP Firewalling Chains, section 4.1.

ipchains-save > filename

This allows for easy restore using

ipchains-restore < filename

You can manually edit the saved filename as long as you follow the format and execute ipchains –F (be careful you are now accepting all traffic) followed by an ipchains-restore < filename to load the manually edited changes.

You also want to make sure the desired rules are in place on a reboot. In Redhat version 7.2 a default script has been added called ipchains located in the init.d directory that will apply the chains at boot up. You can view the contents of the script using vi to see the way it works. There are start/stop/panic options that can be run from the command line (i.e. from the init.d directory running ./ipchains panic will invoke chains denying access to all packets). The script calls the default configuration file called ipchains in the etc/sysconfig/ directory. This file can be manually edited (although it says it is not recommended) to contain the rules desired. The lines separate each rule and the format is the same as the command line with the command ipchains removed.

When deploying a linux box be sure to remove any services that are not needed.

The final say in access Stateful inspection (Symantec Enterprise Firewall)

The firewall in this design could provide Internet access for corporate users. It is a stateful inspection firewall.

Stateful Inspection is defined by Webopedia at http://www.webopedia.com/TERM/S/stateful_inspection.html as being;

> A firewall architecture that works at the network layer. Unlike static packet filtering which examines a packet based on the information in its header, stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid. An example of a stateful firewall may examine not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Because of this, filtering decisions are based not only on administrator-defined rules (as in static packet filtering) but also on context that has been established by prior packets that have passed through the firewall.[8]

Through this process of checking the "state" of the packet being transmitted, another level of protection is added. Only one rule is needed in this firewall that allows access to the Internet for the masquerade address of the Linux router. This firewall will be able to have the last say in Internet access.

[8] Internet resource Webopedia Stateful inspection, INT Media Group, incorporated, http://www.webopedia.com/TERM/S/stateful_inspection.html

The logs provide helpful information when trying to configure the Linux router rules. Due to the large number of sub-links on some sites it is best to view what IP addresses are accessed when visiting a particular web by looking at the logs in the commercial router and then adjusting the rules on the Linux router.

Application Security

Securing the Kiosk workstation applications and operating system

The main application on the Kiosk in this design is Internet Explorer. The basic concept is to force the workstation Kiosk to boot up, automatically logon and start Internet Explorer in Kiosk mode. The default home page of the Kiosk should allow the user to select from a menu the areas of access provided. Drop down menus work well in this application. The Kiosk page could be the home page of the corporation or a page specially developed for the Kiosk.

The first step in securing the Kiosk is applying the latest security patches to the operating system and browser. One of the more difficult tasks is keeping these patches up to date.

After the patches have been applied an audit should be completed to baseline all the services running. Baseline the router and kiosks by running nmap against them and keep a record of open ports. Another tool to use is Languard Network Scanner from GFI located at http://www.gfi.com/downloads/downloads.asp?pid=8&lid=1 for Windows 95/98/ME or Windows NT/2000/XP. Disable any unnecessary services to limit the exposure to future security related bugs. Also disable the on screen keyboard. You will want to design your Kiosk home page to provide point and click accessibility with dropdown menus to complete forms.

Kiosk operational overview

By design the Kiosk workstation should be set up so when the computer starts, the system is automatically logged in, a very restrictive group policy is applied, and the Kiosk application starts. The group policy should be such that nothing is displayed or accessible on the desktop. The policy should also prevent the users from:

- Accessing local resources (i.e. hard drives, floppy drives, and cdroms)
- Saving data
- Adding applications
- Making application or system configuration changes
- Accessing the command prompt directly or from any applications that the user is allowed to run
- Restarting or shutting down the system
- Logging off
- Closing the Kiosk application[9]

[9] Microsoft Corporation. Intellimirror.MSI "Implementing Common Desktop Management Scenarios." Pgs 39-49.

The Kiosk should be configured to automatically logon so the users will not need a password or user name and should not be able to change their password. It is also important that the users be restricted from making the screen saver password protected.

To get this type of customized setting in the policy it is best to create a structure in the active directory that allows you to place the users and computers in special containers and create policies that are applied at the container level. In Figure 3, on page 10, you can see the Group Policy "Public Display Kiosk Policy" is being applied to the container holding the user names being used when the Kiosks automatically logon.

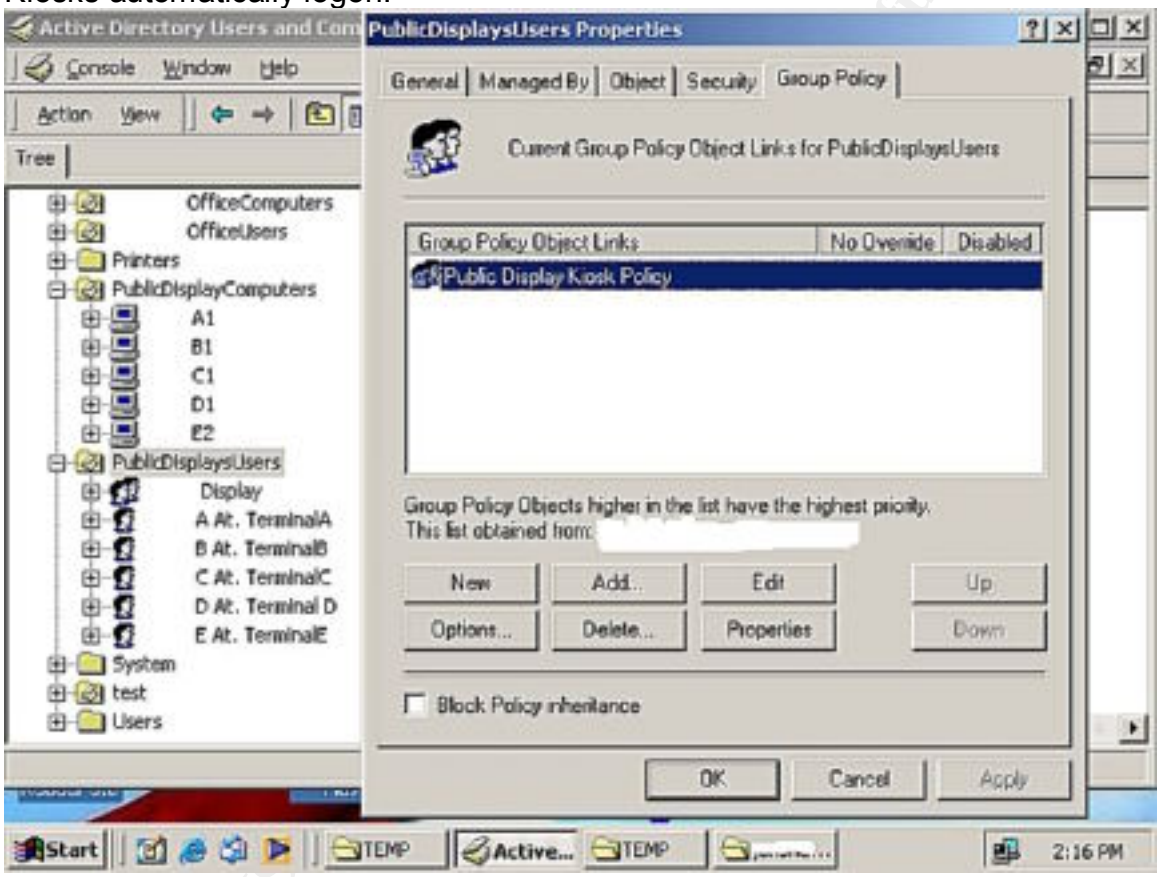

Figure 3. Active Directory and Group Policy Design

There is a white paper called "Implementing Common Desktop Management Scenarios" from Microsoft that provides several scenarios for using Active Directory and group policies to create a particular environment for a workstation. Download and install the IntellimirrorScenarios.MSI file from http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicy.asp. There is a handy excel spreadsheet in this install that can be used as a reference point or template when setting up the Group Policies. The sheet displays all the policies in one spreadsheet. In one of the scenarios they explore the setting for a public kiosk. The setup used in this paper follows the Microsoft setting very closely with some exceptions. Listed below are some notable exceptions.

The Group Policy for the container that holds the User Names in active directory need the following policy settings changes from the Mircrosoft kiosk example.

1. Run only allowed Windows applications Enabled
2. Run these programs at user logon Enabled
3. Hard set in the policy Home page URL to Kiosk homepage

The following pages show where these changes are made and explain how they affect the workstation.

Policy Change #1 (Figure 4)

User Configuration

Administrative Templates

System

Run only allowed Windows applications Enabled

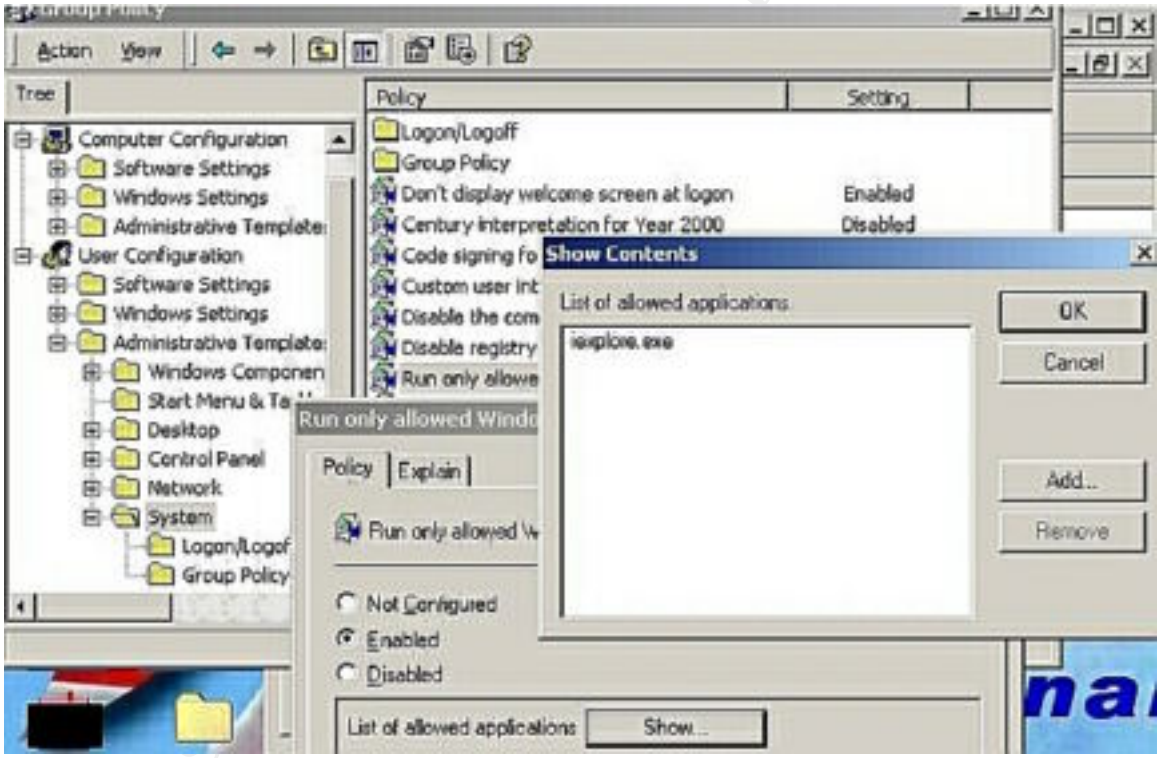

Figure 4. Run only allowed Windows applications

When this policy is enabled you can restrict the list of Windows applications that are allowed to run. In this case Internet Explorer is the kiosk application. You add the application by double clicking on the policy bringing up sub-option called “List of allowed applications” and a “show” button. Click on the show button and add iexplorer.exe.

Policy Change #2 (Figure 5)

User Configuration

Administrative Templates

System

Logon/Logoff

Run these programs at user logon Enabled

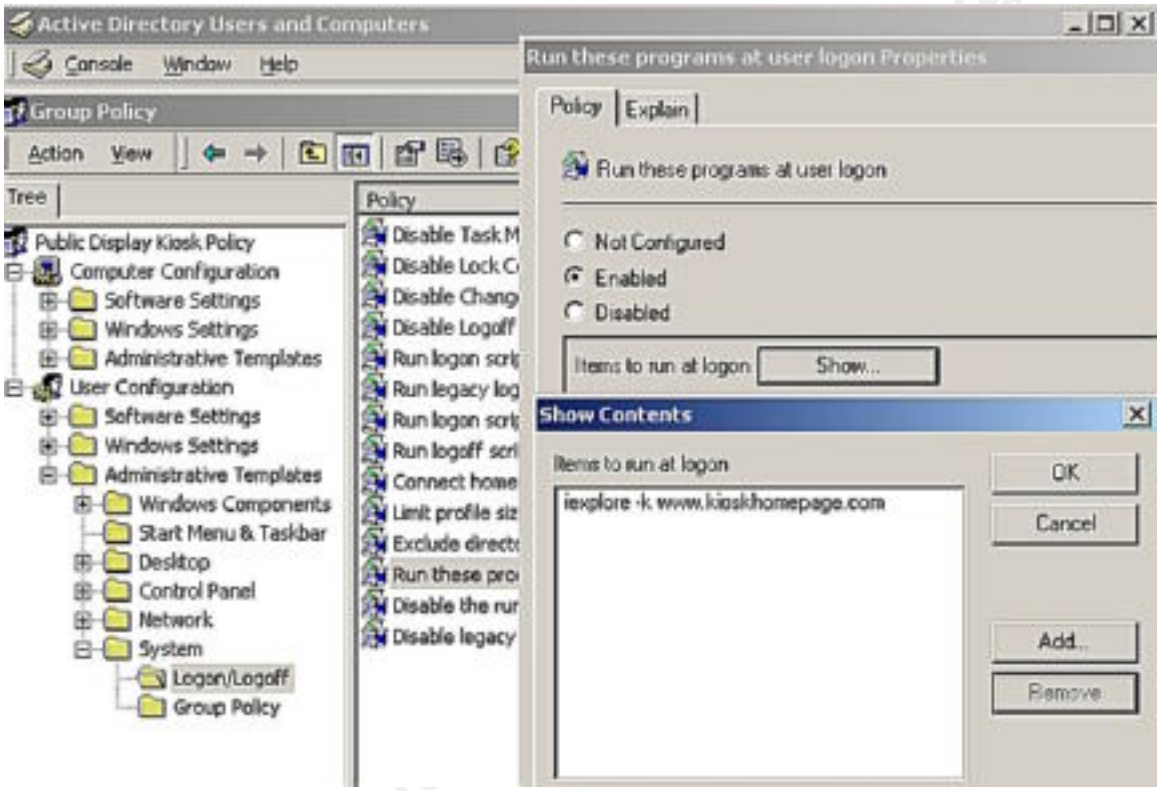

Figure 5. Run these programs at user logon

This policy will force Internet Explorer to run in kiosk mode on boot up. This is accomplished by running iexplore –k www.kioskhomepage.com (the location of your default Kiosk page) when the system starts up.

Policy Change #3 (Figure 6)

User Configuration

Windows Settings

URLs

Important URLs

Home page URL

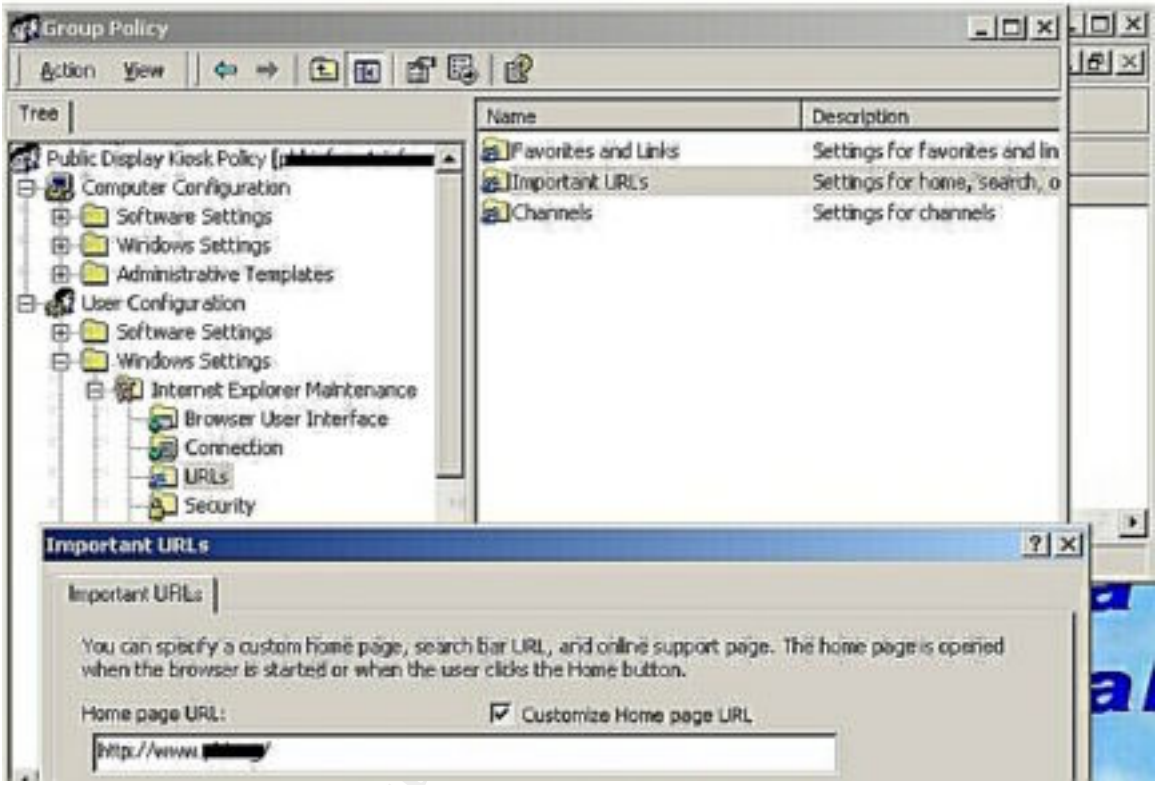

Figure 6. Home page URL

This policy change will force the home page of the kiosk to be set to the desired html page. In the event that a user selects the home button this will insure that the user is taken to the Kiosk home page.

The above settings in combination with the ones given in the Microsoft Scenario for public Kiosks will increase the security of the application environment.

Miscellaneous Configurations

This section will cover some miscellaneous configuration settings that will complete the secure Kiosk network environment.

Auto Logon

Although this may seem risky, it is necessary to have the computer automatically logon so the Group policies can be put in effect, the workstation is recognized by the network and can be remotely monitored, shutdown,

reconfigured or rebooted. To insure the workstation automatically logs onto the network the following registry changes need to be made.

HKEY_LOCAL_MACHINE\Software
\Microsoft
\Windows NT
\CurrentVersion
\Winlogon

AutoAdminLogon	REG_SZ	1
DefaultUsername	REG_SZ	KioskUserName
DefaultPassword	REG_SZ	KioskPassword
DefaultDomainName	REG_SZ	KioskDomain[10]

If one or more of these keys don't exist you will have to create them in the specified location. It is important to remember that automatic logon can be bypassed by holding down the shift key when the computer starts to load the windows operating system.

Remote Rebooting of the workstations

Sometimes it may be necessary to reboot the workstations remotely. A utility called "shutdown.exe" from the Windows resource kit will come in handy.

Configure DHCP

Using the windows 2000 DHCP server to designate a fixed IP address to a specified MAC address and then reserving the other addresses will allow enforcement of the ipchains and stateful inspection firewall rules and still provide some flexibility in configuring Kiosks. The rules are based on the IP addresses of the Kiosks and forcing them to be a particular address insures the rules are applied to the correct requestor of service. The flexibility comes into play if network changes are needed later they can be pushed out through DHCP to the Kiosks.

Conclusion

This paper shows some of the defensive layers that exist and how to configure them to improve security on systems that are exposed for public use. The physical security of the Kiosk workstation, the MAC level filtering at the switches, the firewall packet filtering, the firewall stateful inspection, and the Active Directory Group Policies all play a part in making the job of network intruder more complex and difficult.

[10] Microsoft Corporation. Intellimirror.MSI "Implementing Common Desktop Management Scenarios." Pg 45.

References

IS staff at Purdue North Central. “Passwords.” 15 Jan. 2002. URL:http://www.purduenc.edu/is/password_guide.htm (22 May 2002).

Cross, Graeme. “Linux Security 101.” Feb. 1998. URL:http://www.luv.asn.au/overheads/security/index.html (22 May 2002).

Nortel Networks. “Using the Business Policy Switch 2000 Version 2.0 208700c.pdf.” Nov. 2001. URL:http://www.nortelnetworks.com/index.html (24 May 2002).

Nortel Networks. “Getting Started with Business Policy Switch 2000 Management Software 209321a.pdf.” Aug. 2000. URL:http://www.nortelnetworks.com/index.html (24 May 2002).

Carnegie Mellon University CERT. “Cert Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP).” 23 May 2002 10:34:25 EDT. URL:http://www.cert.org/advisories/CA-2002-03.html (30 May 2002).

Paul “Rusty” Russell. “ipchains: Packet Filtering for Linux 2.2.” Spring 1999. URL: http://www.linux-mag.com/1999-05/bestdefense_01.html (June 11,2002).

Paul “Rusty” Russell. “IPCHAINS-HOWTO.” v1.0.8. 14 June 2000 4:20:53 EST. URL:http://www.tldp.org/HOWTO/IPCHAINS-HOWTO.html#toc2 (01 June 2002).

INT Media Group, Incorporated. “Stateful inspection.” URL:http://www.webopedia.com/TERM/S/stateful_inspection.html (01 June 2002).

Peter V. Valchev. “Firewall.” v 1.11. 29 April 2001. URL:http://www.toxiclinux.org/firewall.html (02 June 2002).

Microsoft Corporation. “Implementing Common Desktop Management Scenarios.” IntellmirrorScenarios.MSI. 15 Sept 2000. download IntellmirrorScenarios.MSI from URL:http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicy.asp (10 June 2002).

Microsoft Corporation. “How to Use Kiosk Mode in Microsoft Internet Explorer (Q154780).” 10 Oct. 2001. URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;Q154780 (10 June 2002).

Andreasson,Oskar. “Iptables Tutorial 1.1.9.” 21 March 2002. URL: http://people.unix-fu.org/andreasson/iptables-tutorial/iptables-tutorial.html (13 June 2002).

Kadlecsik,Jozsef. Welte,Harald. Morris,James. Boucher,Marc. Russell,Rusty.(The Netfilter core team). “The netfilter/iptables project.” URL: http://netfilter.samba.org/ (13 June 2002).

Product References

Interlink Electronics. DuraPoint (VP2000).
URL: http://www.interlinkelec.com/products/retail/durapoint.htm (22 May 2002).

APW-Wrightline. Smart Environmental Monitoring Devices.
URL:http://www.wrightline.com/products/rackbotz.html (01 June 2002).

Kensington Technology Group. PC Locking Mechanisms.
URL:http://www.kensington.com/products/pro_c1378.html (22 May 2002).

GFI Ltd. LANguard Network Security Scanner v2.0.
URL:http://www.gfi.com/downloads/downloads.asp?pid=8&lid=1 (01 June 2002).

Insecure.org. Nmap. URL:http://www.insecure.org/nmap/ (01 June 2002).