Title: Minimum Security Configuration Requirements for Red Hat Linux

1.0 Overview
New operating system installations typically have insecure default configurations. These systems must be secured before being allowed to operate on the Middle Georgia State University network.

2.0 Purpose
This policy will address the minimum requirements acceptable for connecting Redhat Linux systems to the Middle Georgia State University network.

3.0 Scope
The scope of this policy is to specify the minimum security configuration standard for Redhat Linux system installations connecting to the Middle Georgia State University network.

4.0 Policy

4.1 REQUIRED
The following security procedures must be performed.

Update all installed packages with available security patches from Red Hat. A listing is available at http://www.redhat.com/apps/support/errata/.

The Red Hat Network may be used at https://rhn.redhat.com/, or any of the utilities available for automating this task, such as the following:

Apt-RPM available at http://apt-rpm.tuxfamily.org/
RPMFIND available at http://rpmfind.net/linux/rpm2html/rpmfind.html

Enforce password composition and strength. Edit /etc/login.defs to include "PASS_ALWAYS_WARN yes" to warn user if a weak password is used. Edit /etc/login.defs to include "PASS_MIN_LEN 8" to force passwords of 8 characters or more.

Prevent rapid retries by editing /etc/login.defs to include "FAIL_DELAY 3".
Display last successful access and any intervening unsuccessful attempts by editing /etc/login.defs to include "FAILLOG_ENAB yes" and "LASTLOG_ENAB yes".

Rotate audit logs daily and save 90 days worth. This is accomplished by editing /etc/logrotate.conf to include "daily" and "rotate 90".

Disable any unnecessary daemon services:

Use the command "chkconfig servicename off" to disable a particular service. You can alternatively use the "ntsysv" command to display and disable particular services. Ask yourself the following questions. If the answer is "NO" or you don't know the answer, disable the service. Services can always be turned back on should you discover a need.

Is this system a print server, or is there a reason why users must submit print jobs from this system? If not disable this service with "chkconfig lpd off".

Title: Minimum Security Configuration Requirements for Red Hat Linux

Is this system a fileserver or sharing files via the NFS or the Windows filesharing protocols? If not disable this service with "chkconfig netfs off".

Does this system access file systems from remote servers via NFS? If not disable this service with "chkconfig nfslock off" and "chkconfig autofs off".

Is this system an NIS client? If not disable this service with "chkconfig ypbind off".

Is this system remotely monitored by a tool that relies on SNMP? If not disable this service with "chkconfig snmpd off".

Is this system an NFS client or server, an NIS (YP) or NIS+ client or server or run a third-party software application which is dependent on RPC support? If not disable this service with "chkconfig portmap off"

Is this system an NIS server? If not disable this service with "chkconfig ypserv off" and "chkconfig yppasswdd off".

Is this system sharing files via the Windows filesharing protocols? If not disable this service with "chkconfig smb off".

Is this system a DNS server, or nameserver? If not disable this service with "chkconfig named off".

Is this system an SQL (database) server? If not disable this service with "chkconfig postgresql off"

Is this system responsible for maintaining/receiving dynamic routes? If not disable this service with "chkconfig gated off"

Is there a need to administer the system through the remote webmin tool? If not disable this service with "chkconfig webmin off"

Does this system use the squid web cache to speed up web transactions? If not disable this service with "chkconfig squid off"

Is this system a Web server? If not disable this service with "chkconfig httpd off"

Depending on your configuration you may need to disable more or less. Many of the above are on the SANS/FBI Top Vulnerabilities to Unix Systems list at http://www.sans.org/top20.htm and should not be enabled unless absolutely necessary.

You can view open ports with the command "netstat -a | more". This will give you an idea of what services are operating with ports open. Of concern are active Internet connections with LISTEN under state.

Have the system vulnerability scanned. Once a new Red Hat system(s) is installed and secured, the IP address(s) must be provided to the Office of Network Administration for a vulnerability scan. All high severity vulnerabilities must be fixed. *This should be done before TCP Wrapper or personal firewall restrictions are applied so that the vulnerability scan is accurate.*

Restrict connections using TCP wrappers or a personal firewall.

Title: Minimum Security Configuration Requirements for Red Hat Linux

TCP Wrappers.
This statement in the "hosts.deny" denies all connection requests.

Edit /etc/hosts.deny to include only
ALL:ALL EXCEPT localhost:DENY

These statements in the "hosts.allow" are exceptions to the explicit "deny all" rule above and allow any Middle Georgia State University networks to connect.

Edit /etc/hosts.allow to include only
ALL:168.16.176.0/255.255.240.0
ALL:168.16.252.0/255.255.252.0

Any other authorized hosts or protocols must be placed in "hosts.allow" as well. For example, to allow the host at IP address 192.168.1.1 to use SSH and allow everyone to access your web site you would add the following.

sshd: 192.168.1.1
httpd: ALL

Consult the hosts.allow man page for additional details.

Personal firewall using iptables. A personal firewall is considered a more secure alternative to TCP Wrappers. A simple iptables personal firewall can be configured using the "lokkit" command. More complex firewall configurations can be achieved using the iptables command line. Those interested in restricting connections using the iptables command line can find more information at http://www.redhat.com/support/resources/networking/firewall.html.

For further reference and additional security measures, consult the "CIS Linux Benchmark" at http://www.cisecurity.org/ and "Securing and Optimizing Linux: Red Hat Edition" at http://www.linuxsecurity.com/docs/.

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	Definition
TCP	Transmission Control Protocol – Connection oriented transport layer protocol.
IP	Internet Protocol – network layer protocol.
SSH	Secure Shell – A secure remote console and good alternative to Telnet.

7.0 Revision History
12/13/2002- Original
09/17/2013 - Changed institution name to reflect consolidation
08/04/2015 - Changed institution name to reflect University status