Chad Ballay

[CIS411-342N](https://cyberactive.bellevue.edu/webapps/blackboard/execute/courseMain?course_id=_493170_1)

Assigment 7-1

June 9th, 2020

**Chapter 7 - Auditing Windows Servers**

* *Determine whether the server is running the company-provisioned firewall.*
* *Determine whether the server is running a company-provisioned antivirus program.*

Identify the job roles of the IT staff that have Server Support responsibilities. Alignment within this subset of employees will ensure that consistency in policy enforcement will be done.

Identify list of all Windows servers from scanning network or from existing IT asset list. (Nmap)

Establish login credentials to access boxes in an adhoc fashion.

-or-

Gain access to any config management tools like PowerShell DSC or Ansible in use.

Establish what is the company standards for Antivirus or Firewall configurations. This should be explicitly enumerated and may have variations by role of server. But some codex should exist and be captured.

For each Windows server, ascertain if it is running a firewall as per the standard. This may be a local firewall on the server(pslist/advfirewall/etc) or may be an upstream firewall that should be probed/identified.

For each Windows server, ascertain if it is running antivirus as per the standard. I wouldn’t use the GUI mechanism since the investment in a scriptable check allows for this verification to scale in how frequent this checked and number of servers that can be checked.

The Server Support admins will document the server reporting process for ensuring that existing systems are verified to have firewalls and antivirus enabled. This includes validation checks for rebuilds, os patches, new deployments, and other desktop lifecycle events. The work product is report that can be audited periodically by methodically checking a subset of desktops for compliance vs the reported compliance.

**Chapter 8 - Auditing Unix and Linux Operating Systems**

* *Ensure that passwords are shadowed and use strong hashes where possible.*
* *Evaluate the file permissions for the password and shadow password files.*

**These two items are so tightly linked that I would tackle them at the same time. Not sure why they separated them.**

Identify the job roles of the IT staff that have Server Support responsibilities. Alignment within this subset of employees will ensure that consistency in policy enforcement will be done.

Identify list of all Unix/Linux servers from scanning network or from existing IT asset list. (Nmap)

Establish login credentials to access boxes in an adhoc fashion.

-or-

Gain access to any config management tools like Puppet or Ansible.

For each identified unix/linux system gather commands needed to run to check

* The presence of /etc/shadow
* The hashing algorithm used.
* The permissions on /etc/passwd and /etc/shadow
* The ownership/group on /etc/passwd and /etc/shadow

This information should be checked locally against expected values for that specific OS/kernel version.

Any servers that are not correct should be marked and tracked for later evaluation and assignment within the reporting structure for eventual correction or exceptions being generated.

New server creation and onboarding process should be reviewed to establish that these configurations are part of the standards.

The Server Support admins will document the servers reporting process for ensuring that existing systems are verified to not have drifted out of alignment with the standards. This includes validation checks for rebuilds, os patches, new deployments, and other server lifecycle events. The work product is report that can be audited periodically by methodically checking a subset of desktops for compliance vs the reported compliance.