THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

UT DALLAS

Office of Internal Audit
800 W. Campbell Rd. SPN 32, Richardson, TX 75080
Phone 972-883-4876 Fax 972-883-6846

December 12, 2016

Dr. Richard C. Benson, President
Ms. Lisa Choate, Chair of the Institutional Audit Committee:

We have completed an audit of the UNIX environment as part of our fiscal year 2016 Audit Plan, and the report is attached for your review. The audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. The objective of our audit was to ensure that adequate controls existed over the UNIX environment.

Controls within the UNIX environment can be strengthened as outlined in the attached report. Management has reviewed the recommendations and has provided responses and anticipated implementation dates. Though management is responsible for implementing the course of action outlined in the response, we will follow up on the status of implementation subsequent to the anticipated implementation dates. We appreciate the courtesies and considerations extended to us during our engagement. Please let me know if you have any questions or comments regarding this audit.

Toni Stephens

Toni Stephens
Institutional Chief Audit Executive

UT Dallas Responsible Parties:
Kishore Thakur, Associate Director, Information Technology – Systems and Operations;
Casey Horn, Aaron Simpson, and Eric Romine, Managers in Information Technology – Systems and Operations
Members of the UT Dallas Institutional Audit Committee:
External Members:
Mr. Bill Keffler
Ms. Julie Knecht
Mr. Ed Montgomery
Dr. Hobson Wildenthal, Executive Vice President and Provost
Mr. Brian Dourty, Interim Vice President and Chief Information Officer
Dr. George Fair, Vice President for Diversity and Community Engagement
Dr. Gene Fitch, Vice President for Student Affairs
Dr. Bruce Gnade, Vice President for Research
Dr. Calvin Jamison, Vice President for Administration
Mr. Terry Pankratz, Vice President for Budget and Finance
Dr. Inga Musselman, Senior Vice Provost
Mr. Tim Shaw, University Attorney, ex-officio

The University of Texas System:
System Audit Office

State of Texas Agencies:
Legislative Budget Board
Governor's Office
State Auditor's Office
Sunset Advisory Commission

Executive Summary

UNIX Environment, Report No. 1706

Audit Objective and Scope: The objective of our audit was to ensure that adequate controls exist over the UNIX environment.

The following is a summary of the audit recommendations by risk level. See the Appendix for additional details.

Recommendation	Risk Level	Estimated Implementation Date
(1) Ensure Adequate Network and Host Security Protections Are Implemented	**High**	May 31, 2017
(2) Strengthen Netgroup Management	**Medium**	March 31, 2017
(3) Enhance Remote Management Controls	**Medium**	Completed (OIT only) *(Internal Audit Comment: Management intends to centralize management of all Unix assets under OIT. Internal Audit will follow up August 31, 2017 to assess the status)*
(4) Discontinue Inconsistent Management of UNIX Assets	**Medium**	March 31, 2017
(5) Improve Controls over System Security Configurations within the UNIX Environment	**Low**	August 31, 2017

Responsible Vice President:

- Mr. Brian Dourty, Interim Vice President and Chief Information Officer

Responsible Parties:

- Kishore Thakur, Associate Director, Information Technology – Systems and Operations;
- Casey Horn, Aaron Simpson, and Eric Romine, Managers in Information Technology – Systems and Operations

Staff Assigned to Audit:

- Project Leader: Ali Subhani, CISA, CIA, GSNA, IT Audit Manager
- Staff: Colby Taylor, CISA, IT Staff Auditor; student interns from the Internal Auditing Education Partnership Program: Seth Hale and Saran Bezawada

Table of Contents

Background 4

Audit Objective 6

Scope and Methodology 6

Audit Results and Management's Responses 7

Audit Recommendations 7
(1) Ensure Adequate Network Security Protections Are Implemented 7
(2) Strengthen Netgroup Management 8
(3) Enhance Remote Management Controls 9
(4) Discontinue Inconsistent Management of UNIX Assets 11
(5) Improve Controls over System Security Configurations within the UNIX Environment 12

Status of Prior Audit Recommendations 13

Conclusion 13

Appendix 1: Priority Findings and Risk Matrix 14

Appendix 2: Survey 15

Background

An organization's technology assets provide a wide variety of services to internal and external users. Often the criticality of technology assets is only recognized when they do not function as designed, resulting in a disruption to the operations of an organization. One critical piece within the technology landscape of an organization is a *server* which is a computing device that offers different types of functionality such as; serving web content, delivering email, operating a database or facilitating the storage of files.

A server must be configured to utilize an *operating system (OS)* which is the software that manages computer hardware and software resources to adequately offer the functionality that is desired. There are multiple OS options that are available in the marketplace. Historically, the back end critical technology assets have been deployed on the UNIX OS as it offers technology administrators greater flexibility on the functionality that is enabled which could translate into improved security.

However, the flexibility of the UNIX operating could also be its weakness as it offers organizations the ability to deploy any variant to satisfy its unique business needs. As a result, administrators must have good working knowledge of the variant that is in use. Depending on the organization, there may be a lot of differing variants; each with slightly different configuration options which ultimately have an impact on security.

Any compromise of the operating system exposes any application running on the server to vulnerabilities. Lack of proper controls in an operating system may lead to attack or break-in from one system to another. Therefore, it is critical that organizations carefully plan and address the security aspects at the OS level prior to the deployment of a computing device.

At University of Texas at Dallas administration of the UNIX OS is split between multiple departments. The Office of Information Technology (OIT) has a Linux team that provides backend support for many services to the campus. Additionally, various departments and schools across the institution also have responsibility for administering UNIX hosts

UNIX ASSETS

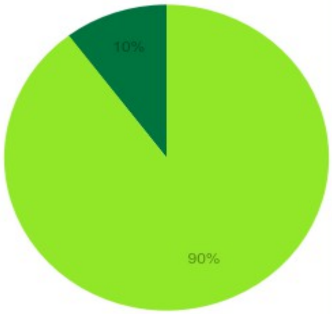
FISCAL YEAR
2016

AUDIT REPORT

UNIX HOSTS

Management of Unix hosts is split between various departments; however for hosts that are accessible from outside the university network the significant majority of hosts are administered by Office of Information Technology (OIT).

Public Unix Hosts
(Accessible from Outside)

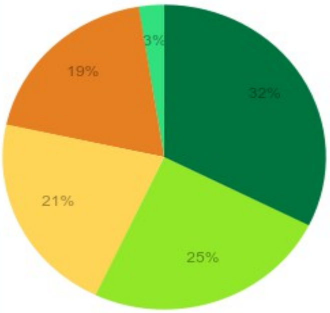


Explanation

Public Hosts are hosts that are accessible from outside of the university network and therefore are at higher risk of a being targeted by a malicious actor. Such hosts can serve content such as web pages or offer web applications that must be accessible even when individuals are not connected to the university network. Therefore administration of such assets by a central team is critical.

Private Hosts are hosts that are only accessible from within the university network.

Private Unix Hosts



SCHOOL OF ENGINEERING

INFORMATION SECURITY

OIT

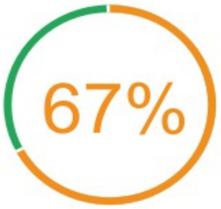
SCHOOL OF NATURAL SCIENCE

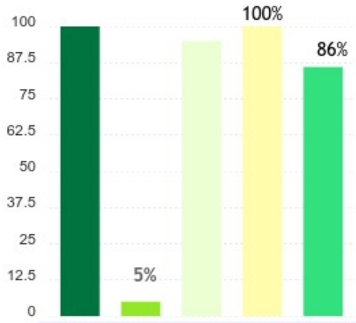
DEPARTMENTAL HOSTS

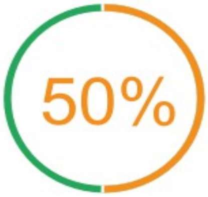
UNDERGRADUATE EDUCATION

ATEC

Survey Highlights







Percentage of Departments Surveyed that did not have a documented baseline configuration

Percentage of Assets Registered in Server Registry By Department

Percentage of Departments Surveyed that did not have a change management process

Audit Objective

The objective of our audit was to ensure adequate controls exist over the UNIX environment.

Scope and Methodology

The scope of this audit was FY 2015-16 operations, and our fieldwork concluded on August 4, 2016. To satisfy our objectives, we performed the following:

- Surveyed (see Appendix 2 on page 15) users in the Office of Information Technology, Undergraduate Education, Information Security, School of Arts Technology and Emerging Communication, and School of Engineering.
- Gained an understanding of the UNIX System Services group system administration and configuration policies and procedures.
- Determined if consistent configuration management procedures specific to UNIX administration were being utilized in various departments across the institution.
- Determined if adequate configuration management, standard baselines and patch management processes exist various departments across the institution.
- Reviewed the system logging architecture and configurations.
- Gained an understanding of the logical access controls within the UNIX System Services group.
- Gained an understanding of ensure adequate network security administrative and technical controls are in place within the UNIX System Services group.

Where applicable, we conducted our examination in accordance with the guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing*. The *Standards* set criteria for internal audit departments in the areas of independence, professional proficiency, scope and performance or audit work, and management of the internal auditing department.

Audit Results and Management's Responses

Controls
Our audit work indicated that the following controls currently exist:

- Remote administration of a server should be allowed only after careful consideration of the risks. The risk of enabling remote administration varies considerably depending on the location of the server on the network. OIT and ISO personnel have adequately configured dual authentication for all publically facing UNIX systems offering an additional layer of security.
- One of the most important functions of a server administrator is to maintain the integrity of the data on the server. The server administrator needs to perform backups of the server on a regular basis for several reasons. A server could fail as a result of a malicious or unintentional act or a hardware or software failure. Backup and recovery is being performed for mission critical servers administered by OIT.
- Logging is a cornerstone of a sound security posture. A central logging server that consolidates logs from various hosts has been implemented.

Audit Recommendations

Priority Findings – UT System - A UT System priority finding is defined by the UT System Audit Office as: "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*"[1] We have **no UT System Priority Findings** resulting from this audit.

Although the above controls are in place, opportunities exist to enhance controls in the UNIX environment as outlined below.

(1) Ensure Adequate Network and Host Security Protections Are Implemented
Risk Level: **High**★
(*prior audit recommendation)*

Network security controls and network segregation can be improved to help reduce the risk that network devices such as workstations and servers can be compromised via a network based attacks. By doing so network security will be improved for workstations and servers operating on the network. Additionally, enhanced network segregation benefits all assets on the network regardless of the operating system type.

[1] Appendix A defines the risks for all internal audit recommendations.

In reviewing controls over UNIX network and host security, we noted that network devices, such as routers and switches, do not provide adequate segregation of the network to protect the UNIX hosts (workstations/servers/etc). UNIX hosts can be probed, scanned, and potentially exploited from both of the internal networks (hard-wired and wireless networks). This observation was originally noted in a prior audit report dated July 9, 2009.

Recommendation: Network devices should be configured to only permit traffic from authorized networks and users with a business need to access the critical UNIX subnet(s).

Management's Response and Action Plan:
The Office of Information Technology has initiated a project to replace the existing edge firewall to provide additional capabilities and capacity over the existing firewall devices. This will allow for segregation of the client networks and datacenter networks. OIT will be partnering with the Information Security Office on this replacement. This effort will provide an additional level of protection to all hosts located in the ViaWest and AD datacenters. In addition, OIT is implementing host based firewalls on all OIT managed servers to provide an additional layer of security. It is our recommendation that host based firewalls be configured on all department managed devices housed in the ViaWest and AD datacenters unless a documented mitigating control is in place.

It is our recommendation that the system administration role for all server resources be provided by OIT. This will ensure standardization and compliance with standards and best practices. It will also allow for increased efficiencies by reducing duplicative effort across many departments.

Estimated Date of Implementation: *May 2017 – primarily driven by academic calendar to minimize disruption (OIT).*

Person Responsible for Implementation: *Kishore Thakur, Associate Director, Information Technology – Systems and Operations; Casey Horn, Aaron Simpson, and Eric Romine, Managers in Information Technology – Systems and Operations*

(2) <u>Strengthen Netgroup Management</u>

Risk Level: **Medium**☆

Netgroups are groups (sets) of users or hosts that can be defined for administrative purposes. Net groups can be utilized to:

- Define the set of users who can access a specific host.
- Define a set of client hosts to be given some specific file system access.
- Define a set of users who are to have administrator privileges on all the hosts.

During our review of the process around netgroup management we noted the following:

- There is no documentation that details the privileges that are provided through membership in a particular netgroup. As a result, the technical staff may not be in a position to validate the appropriateness of a user request to be added to a netgroup.

- A periodic review of assignments within the netgroup is not being performed. According to UTD Account Management Standard, *"Access lists should be reviewed at least quarterly in order to ensure that assignments of unnecessary access are removed."* Without formalized management of netgroups the risk of incorrect security privileges beings assigned or retained when no longer required is increased.

Recommendation: Formalized documentation to detail the privileges that are provided through each netgroup should be developed. The documentation should be utilized during the privilege setup process to ensure the correct privileges are being provided. A periodic review process should be implemented of all the netgroups.

Management's Response and Action Plan: *The Office of Information Technology will review the netgroup process and document the procedures required to remediate this finding. That effort will define a process and system to document netgroup owners and ensure that proper authorization is given prior to adding a user to a particular netgroup. A process to regularly audit the netgroup membership will also be created and will include the identified owner of each group.*

Estimated Date of Implementation: *March 2017*

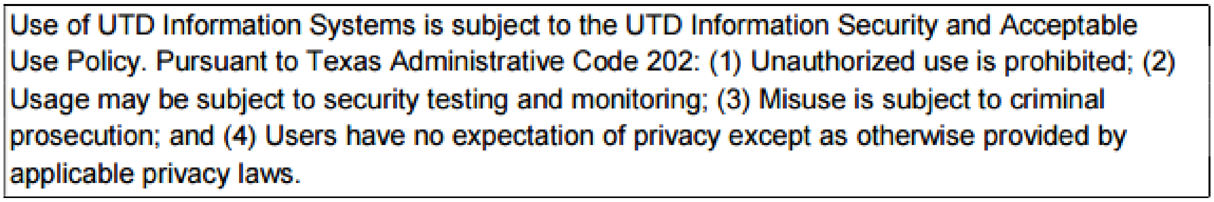
Person Responsible for Implementation: *Aaron Simpson, Manager, Information Technology – Systems and Operations*

(3) <u>Enhance Remote Management Controls</u>
Risk Level: **Medium**☆

SSH (Secure Shell) is used for secure data communications between systems. Additionally, it is a common way to remotely log on to UNIX based systems. As this opens up a potential gateway into the system, strengthening the SSH configuration is a best practice. During a review of the 13 UNIX servers, the following was noted:

- Two of the private servers (only accessible from within the UTD network) had the 'PermitRootLogin' parameter set to 'yes'. As a result, multiple system administrators within the organization with access to the respective servers could log in to the server directly with the default administrative account. This reduces accountability since user actions cannot be tied back to one specific individual.

- Two of the servers that were reviewed were missing logon banners. According to UTD Information Security Server Standards[2], a computer must have a logon banner with the following message:



Use of UTD Information Systems is subject to the UTD Information Security and Acceptable Use Policy. Pursuant to Texas Administrative Code 202: (1) Unauthorized use is prohibited; (2) Usage may be subject to security testing and monitoring; (3) Misuse is subject to criminal prosecution; and (4) Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

- Nine servers were displaying OS version information to users. Logon banners by default can provide sensitive information that may identify the underlying OS version to all users that may log in to the server. This information could be utilized to identify vulnerabilities that may exist on the server. As a best practice, OS version information should not be made available to non-administrative users.

Recommendation: Configurations that are put on UNIX assets to minimize risks associated with remote access should be set up with greater consistency. Consideration should be given to disabling the 'PermitRootLogin' parameter, and ensuring that sensitive information is not provided to users through system banners.

Management's Response and Action Plan: *The two OIT hosts with PermitRootLogin were identified during the discovery phase of this audit and were immediately remediated. Further investigation showed that these two hosts were set up during early implementation of new OS versions, before the automated installation for that OS version was completed. This investigation was followed by a scan of OIT managed Linux hosts for configuration mismatch, and no other instances were found. This setting was implemented as recommended in automated install configurations before the inauguration of this audit.*

Departments that manage their own servers are responsible for ensuring compliance to all university standards. It is our recommendation that the system administration role for all server resources be provided by OIT. This will ensure standardization and compliance with standards and best practices. It will also allow for increased efficiencies by reducing duplicative effort across many departments.

Estimated Date of Implementation: *Complete (OIT only)*

Person Responsible for Implementation: *Aaron Simpson, Manager, Information Technology – Systems and Operations*

Internal Audit Comment: *Management intends to centralize management of all Unix assets under OIT. Internal Audit will follow up August 31, 2017 to assess the status.*

[2] https://www.utdallas.edu/infosecurity/files/Servers-Standard.pdf

(4) Discontinue Inconsistent Management of UNIX Assets

Risk Level: **Medium**☆

The survey results indicated that there was inconsistency in adhering to UTD Information Security Standards [3] that had been adopted. Specifically, we noted that:

- A formalized change management process has not been adopted consistently in all departments. 50% of the departments surveyed did not have a change management process defined.
- A baseline configuration is not being documented when servers are being put into service. 67% of the departments surveyed did not have documented baseline configuration.
- Departments and schools are not consistently registering UNIX hosts that are being utilized as servers within the server registry tool. According to UTD's Server Standard[4], "*All servers must be recorded with the Information Security Office's Server Registry application to ensure accurate inventory is available in the event a security incident is detected."*
- Servers are not being consistently backed up. According to UTD's Server Standard[5], "All servers should be configured for automated backups consistent with the business requirements of recovery time objective (length of time the system can be offline) and recovery point objective (amount of data at risk since the most recent backup, replication, or other data protection event)."

Recommendation: Develop and publish standards or campus wide best practices that other departments can reference when managing UNIX assets. The intent of these best practices would be to provide UNIX specific guidance for helping meet the published Information Security Standards.

Management's Response: *Departments that manage their own servers are responsible for ensuring compliance to all university standards and best practices. It is our recommendation that the system administration role for all server resources be provided by OIT. This will ensure standardization and compliance with standards and best practices. It will also allow for increased efficiencies by reducing duplicative effort across many departments. In addition, the CIO will initiate a meeting with the UTD President and other key stakeholders to determine the overall strategy for managing the risks associated with departmental managed IT resources.*

Estimated Date of Implementation: *March 2017*

Person Responsible for Implementation: *UTD CIO (*Brian Dourty, interim)

[3] https://www.utdallas.edu/infosecurity/policy/
[4] https://www.utdallas.edu/infosecurity/files/Servers-Standard.pdf
[5] https://www.utdallas.edu/infosecurity/files/Servers-Standard.pdf

(5) ***Improve Controls over System Security Configurations within the UNIX Environment***

(prior audit recommendation)
Risk Level: **Low** ★

Security configuration procedures need to be improved to help ensure data is properly secured. The UT System Information Resources Use and Security Policy provides requirements and guidelines to establish accountability and prudent and acceptable practices regarding the use and safeguarding of UT System Information Resources; protect the privacy of personally identifiable information contained in the data that constitutes part of its information resources; and ensure compliance with applicable policies and state and federal laws regarding the management and security of Information Resources.

In reviewing the controls over the UNIX environment, we noted that OIT staff had taken steps to limit the software that was installed by default on Solaris (a Unix OS variant) hosts. However, at this time Linux hosts allowed software list has not been finalized. The UNIX System Services group does not have a standardized software library repository for Linux. Currently, the software binary repository on the configuration server has excessive software packages available for install to the end users that may be at the "end of life" and are no longer supported. This may allow a user to execute packages with known security vulnerabilities. In addition, excessive software packages are configured with the default Jumpstart image. Best practices advocate a minimal installation of services and applications. The greater the number of packages running, the more exposure to the risk of exploiting known vulnerabilities within those applications and/or the underlying services.

This observation was originally noted in a prior audit report dated July 9, 2009.

Recommendation: UNIX Services should establish a standardized software binary library of approved software packages for Linux hosts and perform periodic reviews of the software library assets to ensure software is current and vulnerable software is not available to install by end users.

Management's Response and Action Plan: *The Office of Information Technology is deprecating the use of Solaris by migrating workloads to Linux. OIT will consult with those departments that are running Solaris and will determine if a solution can be provided to continue the software repository for Solaris.*

As part of our deployment strategy for Linux we will provide a software repository that is managed by OIT. OIT cannot restrict package installation on systems managed by departments. It is our recommendation that the system administration role for all server resources be provided by OIT. This will ensure standardization and compliance with standards and best practices. It will also allow for increased efficiencies by reducing duplicative effort across many departments.

Estimated Date of Implementation: *Solaris deprecated August 2017, Linux Repository March 2017.*

Person Responsible for Implementation: *Aaron Simpson, Manager – Information Technology – Systems and Operations*

Status of Prior Audit Recommendations

The following is the status of implementation of the recommendations resulting from Internal Audit Report No. R909, UNIX Security, dated July 9, 2009.

Recommendation	Current Status
1) Ensure Adequate Network and Host Security Protections are Implemented	Not Implemented – See Recommendation (1)
2) Ensure System Audit Logging is Standardized across the Unix Environment.	Significantly Implemented – to be completed by January 2017
3) Improve Controls Over Data Backup and Recovery	Implemented
4) Improve Controls over System Security Configurations within the Unix Environment	Partially Implemented – See Recommendation (5)
5) Ensure Controls over Logical Access are strengthen	Implemented
6) Improve Unix Policies, Procedures and Guidelines	Implemented

Conclusion

Based on the results of the audit work performed, we conclude that improvements can be made to ensure that adequate controls exist over the UNIX environment.

We appreciate the courtesy and cooperation received from the management and staff of OIT, particularly the UNIX System Services group. In addition we appreciate participation from staff members from the following schools and departments that completed the survey: the School of Engineering, School of Natural Science and Mathematics, School of Arts and Technology, Information Security Office, and the Library.

Appendix 1: Definition of Risks

Risk Level	Definition
Priority	High probability of occurrence that would significantly impact UT System and/or UT Dallas. Reported to UT System Audit, Compliance, and Management Review Committee (ACMRC). Priority findings reported to the ACMRC are defined as "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*"
High	Risks are considered to be substantially undesirable and pose a moderate to significant level of exposure to UT Dallas operations. Without appropriate controls, the risk will happen on a consistent basis.
Medium	The risks are considered to be undesirable and could moderately expose UT Dallas. Without appropriate controls, the risk will occur some of the time.
Low	Low probability of various risk factors occurring. Even with no controls, the exposure to UT Dallas will be minimal.

Appendix 2: Survey

The following survey was sent to various schools, and the information was used to gather information for the audit.

How many UNIX/Linux assets within the department are you responsible for?

How many of those assets contain Category 1 data? Category 1 data is data protected specifically by federal or state law or University of Texas rules and regulations. For example: HIPAA; FERPA; specific donor, employee, or sensitive research data.

How many of those assets would be classified as Critical? Critical servers maintain functions that cannot be performed unless they are replaced by identical capabilities. Critical applications cannot be replaced by manual methods. Tolerance to interruption is very low; therefore, cost of interruption is high.

What percentage of the departments UNIX/Linux assets are configured to utilize a backup and recovery process?
______ % Utilizing backups

Does your department have any UNIX/Linux assets that are publicly accessible? Publicly accessible assets are able to be accessed by or present information to any entities on non-UTD networks.

○ Yes

○ No

Are you aware of the Information Security Server Registry webpage? Direct link:

○ Yes

○ No

What percentage of the assets are registered within the Server Registry tool that is provided by the Information Security Office?
______ % Registered

How often is an inventory of UNIX/Linux assets performed within the department?

○ Never

○ Once a Month

○ Once a Quarter

○ Once a Year

○ Every 2 or 3 Years

Do you follow a standard documented checklist when deploying a new UNIX/Linux asset within your department?

○ Yes

○ No

Which of the following are incorporated into the standard checklist that is utilized within the department? (Please check all that apply)

□ Requirement to validate that unnecessary ports are disabled
□ Requirement to validate that unnecessary services are disabled
□ Requirement to enable logging on high risk activities
□ Requirement to install missing patches prior to putting the asset into production
□ Requirement to remove or disable unneeded default accounts
□ Requirement to disable non-interactive accounts
□ Requirement to install anti-malware or anti-virus software
□ Requirement to enable host-based intrusion detection and prevention software.
□ Requirement for creating an asset baseline once the build process is complete
□ Other (Please specify)

You selected "Other" above, please let us know what you utilize on your checklist.

Would you be interested in receiving a comprehensive checklist if one were developed for the campus if it was based on best practices?
○ Yes
○ No

How long are these logs retained for?
○ Less than 30 days
○ Between 30 and 90 days
○ Greater than 90 days
○ Retention time varies depending on log type

What types of accounts do you allow to authenticate to each UNIX/Linux asset that is set up? (check all that apply)
□ Local Accounts
□ Accounts in specific Net Groups
□ LDAP Users

Are local accounts configured to use UTD's password policy regarding password length, complexity, and expiration time?
○ Yes
○ No

Are local accounts periodically reviewed by the department to confirm that the account should still be active?
○ Yes
○ No

Does your department maintain a list of which UNIX/Linux assets are accessible by which net groups?

○ Yes

○ No

Are net groups periodically reviewed to make sure all assigned users are appropriate for that group?

○ Yes

○ No

Does your department create or document a baseline configuration for each UNIX/Linux asset after they are fully configured?

○ Yes

○ No

Is there a formal documented change management process when deploying or modifying existing UNIX/Linux assets?

○ Yes

○ No

Are there any processes or programs in place to monitor for unauthorized changes to the departments UNIX/Linux assets?

○ Yes

○ No

Please list the names of any programs being utilized or generally describe the process doing the monitoring.

Thank you for assisting us with this feedback.
Internal Audit

If you have any other concerns or suggestions regarding UTD's UNIX/Linux environment, please share those below: