Old Dominion University

IT 417 Management of Information Security

Network Infrastructure Design and Implementation

Professor: Vijay Kalburgi

Brian Delos Santos
&
Chase Seider

November 9, 2022

Table of Contents

Introduction 3

Network Diagram 4

Second Floor 5

Functional Diagram 6

Network Inventory 7

Risk Assessment 8

Threat Vulnerability Asset Worksheet (Pre) 9

Hardware Baseline Configurations 10

Security Configurations 11

File Server 12

Access Control Policy 13

Policy and Procedures 14

University Firewall Policy 15

Policy and Procedures 16

Intrusion Detection and Prevention Policy 17

Definitions 18

Host Server and Hardening Policy 19

Policy and Procedures 20

Threat Vulnerability Asset Worksheet (Post) 21

Bibliography 22

Introduction

This document will serve as a roadmap and implementation guidance for a secure computer network supporting the Strome College of Business at Old Dominion University. The design will be formatted to fit the Constant Hall building located on 5115 Hampton Blvd, North, Virginia, 23529.

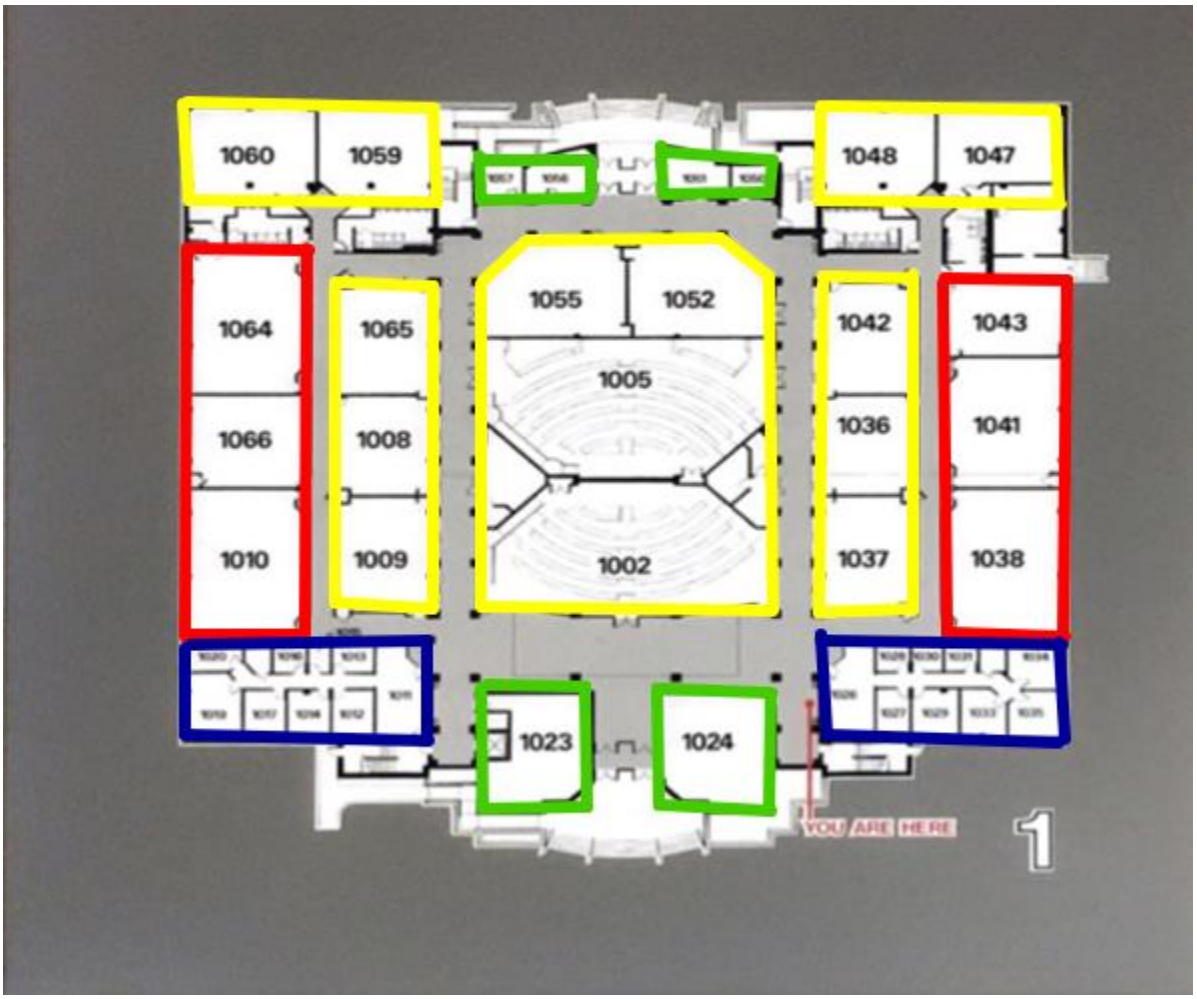
This new secure computer network will utilize a fresh domain of SCB.odu.edu and logically separate the network into three wired subnets, the lab environments, classrooms, and faculty offices. Each of the three subnets will have varying hardware and software requirements, respective to their purpose and users. Although, each subnet will share commonalities such as two domain controllers, network attached storage, and web servers utilizing private IP addressing for the internal network. This network will be built using Microsoft Windows and Cisco products with additional compatible security products as documented in the following pages. Constant hall's building layout is shown below in the Network Diagram section with the first floor primarily used for classroom and lab environments and the second floor used for teacher offices and few podium style lecture rooms.

- Each lab environments will contain 33 desktop style hosts with teaching peripheral technology and will make up the lab subnet.

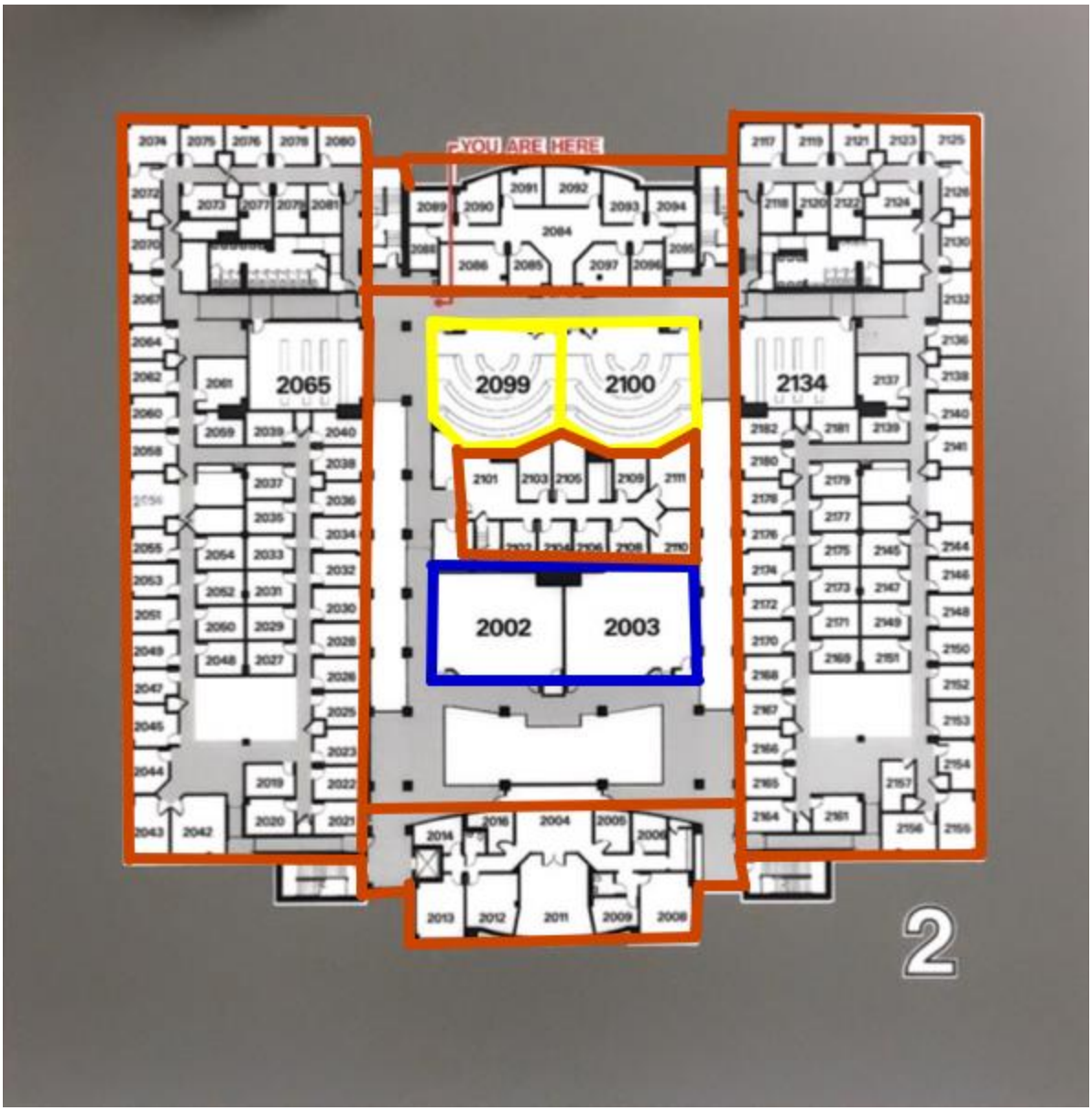
- Each classroom and lecture halls will contain one desktop style host each with teaching peripherals and will make up the classroom subnet.

- Each office located on the second floor will contain one desktop style host each and will make up the faculty subnet.

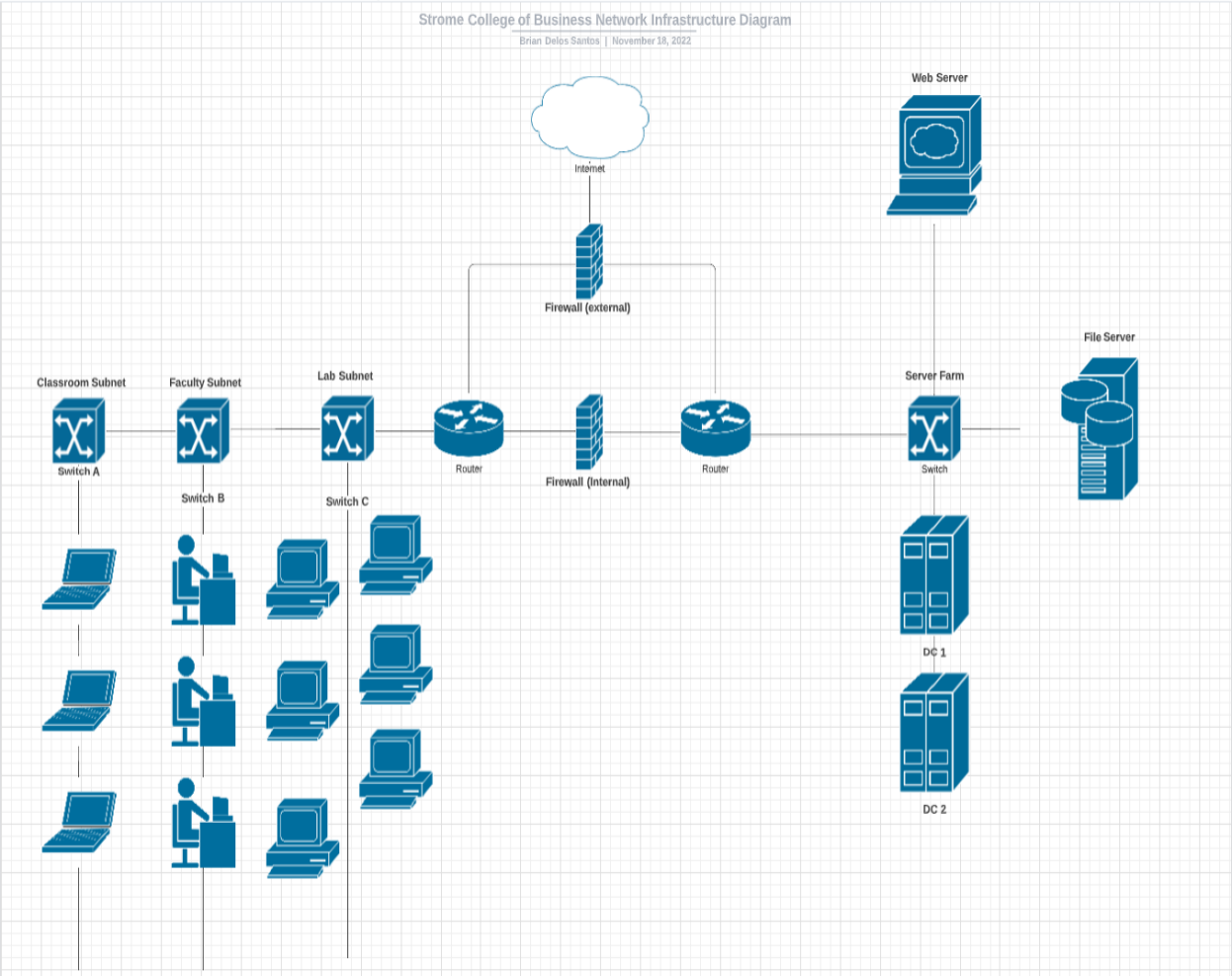
Network Diagram



The first floor has a total of 43 rooms. 6 of which are lab environments filled with 33 desktop style hosts each that will make up the lab subnet shown in red. 14 are classrooms which will contain only one host each with peripheral teaching equipment shown in yellow. 6 rooms are student lounges with no provided technology highlighted in green. 17 rooms are not classrooms, labs, or offices and will be used for storage, server rooms, switches, routers and other miscellaneous or management purposes shown in blue for the first floor.



There are 145 rooms total on the second floor of constant hall. 2 of which are podium style lecture rooms shown in yellow and will be on the classroom subnet. Room 2002 and 2003 will be the server rooms that host the domain controllers, file server and web servers shown in blue. The rest of the 141 rooms shown in orange will be teacher offices and will make up the faculty subnet.



This is a visual representation of how the network will function. I chose to separate the faculty, classroom, and lab subnets by using their own switch stacks for each subnet. The subnets connect to the internet through a single Cisco router and will utilize a firewall appliance to filter traffic from the internet to each of the three subnets. The domain controllers, file server, and web servers will be on a separate subnet with their own router that connects them to the internet. Another firewall will be placed between the three subnets and the servers in order to control internal traffic to and from the subnets to the supporting servers.

Network Inventory

Network Inventory	Classroom Subnet	Faculty Subnet	Lab Subnet	Total
Hosts	16 Dell Desktop PC	141 Dell Desktop PC	198 Dell Desktop PC	$226,845.00
Router	1 Central shared Cisco Router	1 Central shared Cisco Router	1 Central shared Cisco Router	$6,700.00
Switch	1, 48 port Cisco Switch	3, 48 port Cisco switches	4, 48 port Cisco switches	$33,600.00
Domain Controllers	2 Shared Windows Server DC	2 Shared Windows Server DC	2 Shared Windows Server DC	$1,688.00
File Servers	2 Shared Windows File Servers	2 Shared Windows File Servers	2 Shared Windows File Servers	$3,164.22
Web Server	1 Shared Windows Web Server	1 Shared Windows Web Server	1 Shared Windows Web Server	$2,008.99
				$274,006.21

Hardware Base Cost	Make	Model	Cost
Hosts	Dell	OptiPlex 3280 All-in-One Desktop	$639.00
Router	Cisco	CISCO ISR4331-SEC/K9 Isr 4331	$3,350.00
Switch	Cisco	Cisco SG350-52MP-k9	$4,200.00
Domain Controller	Lenovo	ThinkSystem SR250 Rack Server	$844.00
File Server	Lenovo	ThinkSystem SR570 Rack Server	$1,582.26
Web Server	Lenovo	ThinkSystem SR655 Rack Server	$2,008.99

The Dell OptiPlex 3280 All-in-One Desktop is great for setting up large networks because it is a fair priced bundle that comes with mouse, keyboard, integrated graphics card, medium storage space, and a moderately future proofed processor capable of handling all SCB.odu.edu student, faculty, and administration loads.

For servers I chose the Lenovo Think system Rack servers for affordability and scalability just in case more hosts or lab environments are added to the SCB.odu.edu domain. They are affordable and come stackable for ease of storage and future scalability.

The Cisco Catalyst 8500L edge router for large networks came highly recommended for high-capacity networks like SCB.odu.edu. The reason for this router is to not have any throughput issues with the large number of hosts it supports. Same with the Cisco Catalyst 9500 48 port switch, with the large amount of hosts on the faculty and lab subnet, we want a high capacity, quality switch to ensure high availability and security with one of Cisco's industrial style switches.

Risk Assessment

Threats

Malware and Viruses

- University systems are all installed with an approved anti-virus software. The university firewall and IPS/IDS systems are configured to make it hard for users to mistakenly install malware and attackers to get into university systems

Dos or DDOS attacks

- The university has an internal firewall that is configured to filter traffic to the different university subnets and servers. During unaccounted for times of high traffic, certain services and protocols will automatically be rate limited to ensure critical operations of the university network can still function

Environmental hazards

- The university network has access to a limited supply of batteries in the case of a full power outage. In that limited time (around 50 minutes) the network power must be connected to backup generators, so the network does not go down.

Internal threats (Social engineering/phishing attacks/Human error)

- University employees and students can be an unintentional threat to the network. Every faculty member and student are required to use the university designated two factor authentication on all their accounts. Educational programs about phishing emails and scams will be freely available and recommended/required in some circumstances to all faculty and students at the university

Threat	Vulnerability	Asset	Impact	Likelihood	Risk
(High) Malware And Virues	(Medium) Antivirus software is not impervious to everything	(Critical) University systems/ network	(High) Potential loss or disruption of certain educational systems or parts of the network	(Low)	(Medium) Potential loss or disruption of systems and networks will have a high cost for the university depending on the amount of downtime
Dos or DDOS attacks	(Low) Firewall and IPS systems are correctly configured to handle extreme loads from ddos attacks	(Critical) University Servers / network	(Critical) Server and network extended downtime	(Medium)DDOS attempts on networks are fairly common each year	(High) Extened periods of server and network downtime will have extreme costs for the university and disrupt student education
Environmental Threat (Local threats are hurricanes and flooding)	(Low) University servers are on upper floors and in sturdy buildings that should not be impacted hard by a hurricane	(Critica) University Servers	(Critical) Server outage	(Low) Flooding happens often but is not a threat to server buildings. Hurricanes typically happen once a year	(High) Extened server outage disrupts staff and student educations use and can prevent access to the university website causing a loss in profit and function
Insider Threats	(High) Disgruntled Employees and Employee mistakes are something that can never be avoided, only minimized	(Critical) Could potentially affect any unviersity systems/ Servers/ networks	(High(Server outage/ Data deletion/ network outage	(Medium) Insider threats will always be a thing but the University has strong access control which can prevent these situations	(High) While not too likely to happen, these threats have the potential to affect the university as a whole and cost it a lot of money

Threat Vulnerability Asset Worksheet Pre-Control Implementation

Threat Vulnerability Asset Worksheet Pre						
	Hosts	Router	Switch	Domain Controllers	File Server	Web Server
Malware and viruses						
Dos or DDOS						
Environmental hazards						
Internal Threats						
Critical						
Medium						
Low						

Pre control/system and policy implementation, the network will have a lot of vulnerable areas that can be mitigated with little to no cost. First, base implementation of hosts in lab, classroom, and teacher environments will not have host-based firewalls in place that will leave them vulnerable to malware, Dos, or DDOS attacks from outside the network. Initially, the hosts will not have restrictions on user actions and installed software which allows for internal threats to have full control of the system to perform attacks from within the network.

The router and switches will be vulnerable to the attacks from the internet without a firewall appliance to filter traffic to and from outside the internet. They will also not be protected from outside connections that may try to reconfigure, reroute, or otherwise corrupt the hardware which can cause availability outages.

The severs will have the same issue if left in the pre-control state. Without policy, permissions, and IDPS capability, this system will be vulnerable to breaches in confidentiality, availability and integrity breaches.

Baseline System Configurations and Applications

Domain Controllers:

Operating System: Windows Server 2022

Hardware: Lenovo Think system SR250 Rack sever

Additional Software: Windows Active Directory with Domain Services

Roles: Students, Faculty, and Administrators

Use Case: Used to authenticate authorized users to access hosts and network resources with set permissions. Stores the active directory database

Hosts:

Hardware: Dell OptiPlex 3280 All-in-one

Operating System: Windows 10 Professional

Use case: Found in lab environments for students to utilize for class activities. Found in teacher offices for personal and faculty use. Used by administration for troubleshooting and management purposes.

Web server:

Hardware: Lenovo Think System SR655 Rack Server

Operating System: Windows Server 2022

Applications Hosted: Apache HTTP server, Microsoft Office 365, Myodu.edu portal, WordPress, Google G suite.

Use case: Utilizes Apache Web server application to host myodu.edu portal, Microsoft office applications, WordPress, and Google G suite for SCB.odu.edu Domain.

File Server:

Hardware: Lenovo Think System SR655 Rack Server

Operating System: Windows Server 2022

Application: FileZilla FTP server

Storage Space: scalable with additional HDD/SSD

Use case: Used to store and access files for faculty and administrators on the SCB.odu.edu domain. Only accessible by faculty and administration. Students will only be capable of saving local files that will not remain on the system after signing off.

Security Configurations

Domain Controllers:

As standard practice only one of the domain controllers will be always on and the other will remain offline just in case something happens to the first for fault tolerance and to promote high availability.

Only administrators will have the ability to have access to the domain controllers to promote confidentiality and integrity of user credentials and group permissions.

Windows event viewer will be utilized on the domain controller to log all action taken by authorized users on the domain controller to promote system integrity.

The domain controller will only have limited access to the internet as necessary for updates and authentication purposes. This limits the exposure to outsider threats.

Hosts:

All hosts require authentication from the domain controller before gaining access to a host for any reason.

Windows defender firewall will be active on all hosts as an IDPS on the SCB.odu.edu domain to monitor and prevent viruses and malicious software. This software will be updated with the most recent signatures of malware each month.

Students accounts will be unable to download software from the internet to lower the risk of unintentional and intentional malware from entering the private network.

Web Server:

Only administrators will have permission to access the web sever in order to maintain the confidentiality of internal applications and the uses who rely on them.

The Apache Web server will force HTTPS, the secure version of HTTP to prevent information from being intercepted, stolen, or changed during transmission of data.

Windows event view will be utilized on the web server to log all actions taken by authorized users to promote system integrity.

File Server:

The file server will only be accessible to administration and faculty groups. Student accounts will not be able to communicate to the file server and therefore only allowed to save files locally.

Windows event viewer will be utilized as a logging tool to ensure all files accessed by authorized users and that no file is created, saved, deleted in an unauthorized manner.

FileZilla FTP sever application will be forced to utilize SFTP to protect the integrity of files accessed on the network. This will prevent files from being intercepted, manipulated, or stolen in transit.

Access Control Policy

Purpose:

Access controls are designed to minimize potential exposure to the University resulting from unauthorized use of resources and to preserve and protect the confidentiality, integrity and availability of the University networks, systems, and applications.

Scope:

This policy applies to all University staff, students, student employees, volunteers, and contractors that connect to the university network, applications, or servers that contain or transmit protected or private university data. University servers, applications, and network devices that contain or transmit this data are considered “High Security Systems”.

Definitions:

User - Anyone that accesses and uses the University’s information technology resources

High Security System - Servers, applications, or network devices that transmit or receive protected university data

Policy Statement

Access to High Security Systems will only be provided to users based on business requirements, job function, responsibilities, or a need-to-know basis. All additions, changes, and deletions to individual system access must be approved by the appropriate supervisor and the University Information Security Officer. Access controls to High Security Systems are implemented via an automated control system. Account creation, deletion, and modification as well as access to protected data and network resources is completed by the University Information Security Department.

Policy and Procedures

User Access

Users with access to High Security Systems will be required to use a separate account that must abide by the following standards

- The password is required to follow the university password guidelines
- Two factor authentication must be set up on the account
- Inactive accounts will be disabled after 90 days of inactivity
- Access to this account will be monitored and only accessible during the allotted timeslot needed

Administrators have the authority to disable accounts and remove permissions if there is a breach in security or malicious activity on an account

Physical Access

ITS data centers must abide by the following security requirements

- Video surveillance systems must be installed and used to monitor access in and out of data centers
- Proper identification must be used to be granted access to data centers
- Access is limited to ITS personnel and approved University employees or contractors that are required to be there
- Visitors of ITS data centers must be accompanied by ITS personnel
- Modifications to any data in the center must be logged

Policy Adherence

Failure to adhere to this policy can result in disciplinary action including termination as provided in the University Staff Handbook

University Firewall Policy

Introduction

The university operates a firewall to increase security between the internet and the University network to create a safe and reliable network for students and staff. This Firewall Policy governs how the firewall will filter Internet traffic to mitigate the risks and losses associated with security threats to the University network and information systems.

Purpose

A firewall is a key component of security for the campus network. It reduces the threat of outsiders damaging or intruding into university systems. A firewall does not prevent malicious or illegal activities from happening within the firewall.

This policy is designed to protect the student, faculty, and staff computers from outside threats such as hacking attacks and malware by restricting access to computers on the University campus from users who are off campus.

Scope

This policy applies to all University staff, students, student employees, volunteers, and contractors that use the University network.

Definitions

Firewall - A firewall is a network security device that monitors incoming and outgoing network traffic and permits, or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

User - Anyone that accesses and uses the University's information technology resources.

Firewall Administrator - Individual with permission to monitor alters and configure/implement firewall policies.

Policy Statement

The University operates a flexible and adaptive security environment to meet its academic research and administrative missions. This firewall is set up and managed by Information Technology Services network and security staff.

Policy and Procedures

The firewall permits the following for outbound and inbound internet traffic:

- Outbound: Allow ALL internet traffic to hosts and services outside of the university except for known security vulnerabilities and websites the university deems dangerous or inappropriate. This allows users of the network to utilize all services on the internet apart from services the university blocks.
- Inbound: Only specific services which support the university's mission will be allowed to be accessed from the internet.

Operational Procedures

Only firewall system administrators are permitted to login to the firewall.

- Access to firewall hosts must be tightly controlled. Only firewall system administrators are allowed to have user accounts on firewall hosts.
- Firewall system administrators muse have personal accounts. No group accounts are allowed.
- Direct remote root access is never allowed. All root access must be through an administrative login.

Only personnel with the appropriate authorization can make changes to the firewall access rules, software, hardware, or configuration.

- All changes should be a result of a request recorded using the Firewall Change Request Form although emergency modifications can be requested by phone, with a follow up email and change request.
- Only authorized personnel must be able to implement the changes and an audit log must be retained.

Intrusion Detection and Prevention Policy

Introduction

Intrusion Detection and Prevention systems focus on identifying possible incidents, logging information about them, and reporting attempts to security administrators. It plays an important role in implementing and enforcing security policies.

Scope

The Intrusion Detection and Prevention Policy applies to all individuals that are responsible for the installation and operation of IDS and IPS systems in the university network.

Policy Statement

Audit logging, alarms and alert functions of operating systems, user accounting, application software, firewalls and other network perimeter access control systems will be enabled and reviewed annually. System integrity checks of the firewalls and other network perimeter access control systems will be performed annually.

Automated tools will provide real-time notification of detected wrongdoing and vulnerability exploitation. Where possible, a security baseline will be developed, and the tools will report exceptions. These tools will be deployed to monitor:

- Internal Traffic
- Mail traffic
- Operating system security parameters

Definitions

Intrusion Detection System (IDS) - A system that passively monitors network traffic for suspicious activity and alerts when such activity is detected

Intrusion Prevention System (IPS) - A system that monitors network traffic for suspicious activity like an IPSs system but instead of just alerting that there is a threat, it actively prevents them

Policy and Procedures

Network Monitoring

- All suspected and/or confirmed instances of host, server, or network intrusions will be reported immediately to the designated ITS personnel
- Operating system, user accounting and application software audit processes will be enabled on all host and server systems where resources permit
- Alarm and alert functions, as well as audit logging of any firewalls and other network perimeter access control systems will be enabled
- Logs from the firewalls and network perimeter access control systems will be monitored and reviewed as risk management decisions warrant
- Logs for servers and devices will be reviewed as warranted based on risk management decisions

Host and Server Hardening Policy

Introduction

University Host systems are expected to be safe, secure, and reliable when being used by university personnel or students. Servers are depended upon to deliver data in a secure, reliable fashion. There must be assurances that data integrity, confidentiality and availability are maintained. Hosts and Servers need to be installed and maintained in a way that prevents unauthorized access and disruptions to their services.

Scope

The Host and Server Hardening Policy applies to individuals that oversee installing and maintaining the university systems and teachers and students that use university hosts for their educational needs.

Policy Statement

The university provides and requires strict host and server hardening guidelines to ensure that individuals using them are operating in a safe and secure learning environment.

Definitions

Host - Any university device that communicated and connects to the university network

Server - A computer dedicated to running one or more such services, to serve the needs of programs running on other computers on the same network

Hardening - The enhancement of security through various means to ensure that hosts and servers are operating in a safe and secure environment

Policy and Procedures

Host and Server Hardening - A server or host cannot be connected to the university network until it is in an approved secure state. The following regulations must be met to be considered being in an approved state

- The operating system is installed from a university approved source and proper licenses are used
- A reserved IP address must be assigned from the university network administrator
- All unnecessary software, system services, and drivers must be removed from the system
- University appropriate file protections and security parameters must be set

- Audit logging must be enables on all university hosts and servers
- The default password and account on the system must be changed to meet university requirements

After connecting to the university network for the first time, the university approved antivirus software must be installed to the system and all systems and applications must be updated to the latest secure versions

All hosts and servers must pass a vulnerability assessment before being allowed to connect to the wide university network

Threat Vulnerability Asset Worksheet Post-Control Implementation

Threat Vulnerability Asset Worksheet Post						
	Hosts	Router	Switch	Domain Controllers	File Server	Web Server
Malware and viruses						
Dos or DDOS						
Environmental hazards						
Internal Threats						
Critical						
Medium						
Low						

Post control implementation, the threat vulnerability chart looks a lot more tolerable. Even with protections and policy in place, one cannot rule out the possibility of intrusions and incidents.

With protections, hosts and severs will have host-based firewalls and windows defender antivirus with advanced malware protection which uses current known virus signatures updated monthly with signatures from Microsoft. This software will protect hosts and servers from known malicious viruses and can be configured to alert in the event of anomalous activity. Implementation of policy and security configurations will prevent unauthorized users from utilizes network resources without authentication and an active account on the domain controller. Accounts will have permissions, severs access will be restricted, protected and actions will be logged through windows event viewer so individual actions can be traced back to the individual that performed them.

The threat vulnerability asset post sheet shows that the confidentiality of information systems and data utilized in Constant Hall will not be compromised by any non-sophisticated threat. The integrity of data stored, in transit, or processed will not be at significant risk. Also, high availability of information systems will be held with industry standard technology, security configurations and policy.

Bibliography

https://ww1.odu.edu/ts/labs-classrooms/technology-classrooms/const

https://www.dell.com/en-us/shop/desktop-computers/optiplex-3280-all-in-one/spd/optiplex-3280-aio/s212do3280aious?gacd=9684992-1084-5761040-350588223-0&dgc=st&gclid=Cj0KCQiA1NebBhDDARIsAANiDD0T5JDknoAQp1HoWKlA-Rhdzm_BOzUA7BYUqZWSG-Bedz_q_JRD0zYaAhuOEALw_wcB&gclsrc=aw.ds&nclid=xablBDqMUHRDEY1Bn8ZWNOBt44NuF2kprp3tU4QxwvNILPZPKZ3QcuDeCl7HQ8qQ

Cisco SG350-52MP-k9 52-Port Gigabit Max-PoE Managed Switch - ServerSupply.com

https://www.serversupply.com/NETWORKING/ROUTER/3%20PORT/CISCO/ISR4331-SECK9_224714.htm?gclid=Cj0KCQiA1ZGcBhCoARIsAGQ0kkoI8aeYqiCeB7cJneOmqcqrHnCpwNwDFROckXN1Xsq2AOK7m75dCh4aAs8GEALw_wcB

https://www.lenovo.com/us/en/p/servers-storage/servers/racks/77xx7srsr25/7y51a08cna?cid=us:sem|se|google|isg_ecomm_pla_nonbrand_us_nonalliance|||7Y51A08CNA|17961596360|140558480140|pla-1718945170734|shopping|nonbrand&gclid=Cj0KCQiA1ZGcBhCoARIsAGQ0kkpXOnrT7ha4AS7JJwOZ3Zfc7hfruz44Aa15I8xYM6jkHVRcU2RVnNEaAgrbEALw_wcB

https://www.lenovo.com/us/en/p/servers-storage/servers/racks/thinksystem-sr655/77xx7srsr75?cid=us:sem|se|google|DCG+eCommA_PLA_nonBrand_US_AMD||||17639230718|138558017659|pla-1653265257278|shopping|nonbrand|&gclid=Cj0KCQiA1ZGcBhCoARIsAGQ0kkqvyIkMgnRmdJS_hpswz58XBTbiog8n0V74w9bSZs4qLvifaQ12hRwaAqVXEALw_wcB

https://www.lenovo.com/us/en/p/servers-storage/servers/racks/thinksystem-sr570/77xx7srsr57?cid=us:sem|se|google|DCG+eCommD_PLA_NonBrand_US_DCF||||10443733156|103596613357|pla-1650052389489|shopping|nonbrand|&gclid=Cj0KCQiA1ZGcBhCoARIsAGQ0kkqU2pm_37Y5FdEN9Ikdh1evV8CQKbEoralfztT_E0fL4XOhpcCfGQgaAsraEALw_wcB