Simulation of Using Defense Strategies against a Cyber Attack

by

David Mariyasin

B.S. Security Systems, 2025

Senior Project Submitted in Partial Fulfillment of the

Requirements for the Degree of

Bachelor's in Security Systems

in the

Department of Computer Security

Faculty of Dr. Tarik Eltaeib

Farmingdale State College

Fall 2025

Declaration of Committee

Name:	**David Mariyasin**	
Degree:	**Bachelor's in Security Systems**	
Title:	**Simulation of Using Defense Strategies against a Cyber Attack**	
Committee:	**Chair:**	**Nazuri Islam** Computer Security, Chair
	Advisor:	**Tarik Eltaeib** Computer Security, Professor

Academic Integrity Policy

Because intellectual honesty is a cornerstone of all academic and scholarly work, each member of the Farmingdale State College campus community is expected to maintain academic integrity. Farmingdale State College has developed regulations concerning academic dishonesty and integrity to protect all students and to maintain an ethical academic environment. For more information, click the updated link for the college-wide Academic Integrity Policy

It is important for you to understand the concept of plagiarism. Plagiarism is intentionally representing the words, images or ideas of another as one's own in any academic exercise. This includes words, images or ideas in either print or electronic format.

Abstract

The objective for this project via Cisco Packet Tracer was to simulate how layered security measures can protect an organizational network from unauthorized access and malicious activity. Using Cisco Packet Tracer, a network topology was designed with multiple VLANs connected through routers and switches, along with a server. The defense strategies used for this simulation implemented ACLs on routers to block the Employee VLAN from accessing the Admin VLAN. port security on switches to prevent MAC address spoofing and unauthorized device connections, and firewall-like ACLs on R2 to allow only HTTP traffic to the server while denying all other protocols.

Dedication

Table of Contents

List of Tables

Admin Network

Default Gateway- 192.168.10.1

IP Address Range- 192.168.10.2–254

Employee Network

Default Gateway- 192.168.20.1

IP Address Range- 192.168.20.2/254

Server Network

Default Gateway- 192.168.30.1

HTTP Server- 192.168.30.10

IP Address Range- 192.168.30.2/254

Outside Network (Simulated Internet)

DNS Server – 8.8.8.8

External Website – 203.0.113.10

List of Acronyms

ACL	Access Control List
VLAN	Virtual Local Area Network
IP	Internet Protocol
HTTP	Hypertext Transfer Protocol
MAC	Media Access Control
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
SSH	Secure Shell
ISP	Internet Service Provider

Glossary

Access Control List	A filter that is used to prevent or allow certain packets in or out of a network
Virtual Local Area Network	A broadcast domain that is isolated from other networks on the switch
IP Address	32 numbers that are used to identify a device in a network
MAC Address	A hardware identifier assigned to a network interface for communication on the physical network
Port Security	A feature on switches that limits the number of MAC addresses allowed on a port to prevent unauthorized access
Firewall	A security system that monitors and controls incoming and outgoing network traffic based on predetermined rules
Hypertext Transfer Protocol	Used for transmitting web pages over the internet
DHCP	A protocol that automatically assigns IP addresses to devices within the set ranges
DNS	Changes website IP addresses into easily memorable names

Chapter 1. Introduction

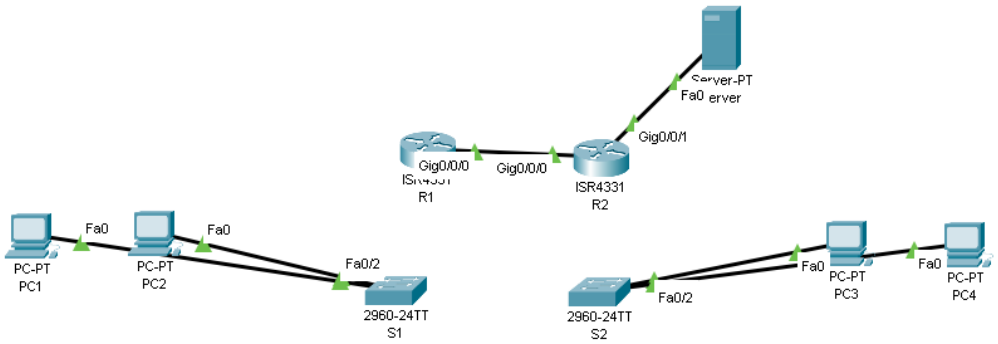
For this project, I used Cisco Packet Tracer to design and implement a secure network topology that demonstrates practical methods for mitigating cyber threats. Cisco Packet Tracer is widely recognized as a powerful simulation tool for network design and testing, enabling realistic scenarios for academic and professional environments (Yousif & Al-Saffar, 2018). The network consists of multiple VLANs representing Administration and Employees, interconnected through routers and switches, and includes a server hosting essential services.

The primary objective was to apply layered security measures to protect the network from unauthorized access and malicious activities. These measures included ACLs on routers to restrict inter-VLAN communication, port security on switches to prevent MAC address spoofing, and firewall-like ACL configurations to allow only HTTP traffic to the server while blocking all other protocols. Such strategies align with research emphasizing proactive security measures and defense-in-depth approaches to counter modern cyber threats (MohanaPriya & Shalinie, 2017).

This simulation reflects real-world scenarios where organizations must safeguard sensitive data and maintain operational integrity. Similar approaches have been applied in studies involving IoT-based smart networks, where segmentation and layered security were critical for maintaining integrity and resilience (Gurjar & Dangra, 2022). By implementing these strategies, the project emphasizes the importance of network segmentation, traffic filtering, and endpoint security in defending against any cyber-attack. Testing scenarios validated the effectiveness of these configurations by simulating

unauthorized access attempts and device spoofing, demonstrating how proactive security measures can significantly reduce vulnerabilities.

Chapter 2. Organization Network Topology



The network topology created for this project was designed to replicate and simulate an organizational environment with both an administration and employees, each represented by distinct VLANs to ensure segmentation and security. Using Cisco Packet Tracer, the setup included two switches (S1 and S2), two routers (R1 and R2), and a server connected to R2 which is ultimately the device where a cyber attack will be implemented. 2 VLANs with an IP addess was created:

The Admin VLAN, configured with the IP range 192.168.10.0/24 and a default gateway of 192.168.10.1, and the Employee VLAN, configured with the IP range 192.168.20.0/24 and a default gateway of 192.168.20.1. A third segment was dedicated to the server network, using the IP range 192.168.30.0/24 with a default gateway of 192.168.30.1, and hosting an HTTP server at 192.168.30.10. Routers R1 and R2 provided inter-VLAN routing and enforced security policies through ACLs, while switches implemented port security to prevent unauthorized device connections.

This design reflects a real-world organizational network where segmentation and access control are critical for reducing attack surfaces. This topology supported testing scenarios such as VLAN isolation, MAC address spoofing prevention, and traffic

filtering to validate the effectiveness of the implemented security strategies needed to work in this simulation.

Chapter 3. Implementing the attacks

```
R1>ena
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 100 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
R1(config)#access-list 100 permit ip any any
R1(config)#int g0/0/1.10
R1(config-subif)#ip access-group 100 in
R1(config-subif)#exit
R1(config)#
```

```
S1>ena
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int range fa0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport port-security
S1(config-if-range)#switchport port-security maximum 1
S1(config-if-range)#switchport port-security violation shutdown
S1(config-if-range)#switchport port-security mac-address sticky
S1(config-if-range)#exit
S1(config)#
```

```
S2>ena
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int range fa0/1-3
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport port-security
S2(config-if-range)#switchport port-security maximum 1
S2(config-if-range)#switchport port-security violation shutdown
S2(config-if-range)#switchport port-security mac-address sticky
S2(config-if-range)#exit
S2(config)#
```

```
R2>ena
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 101 permit tcp any host 192.168.30.10 eq 80
R2(config)#access-list 101 deny ip any host 192.168.30.10
R2(config)#access-list 101 permit ip any any
R2(config)#interface g0/0/1.30
R2(config-subif)#ip access-group 101 in
R2(config-subif)#exit
R2(config)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.30, changed state to
up
```

To simulate defense strategies against potential cyber attacks, the first stage of the project required configuring security measures on routers and switches within the network. The main focus was on restricting unauthorized access between VLANs using ACLS. On R1, an extended ACL was created to block traffic originating from the Employee VLAN (192.168.20.0/24) attempting to reach the Admin VLAN (192.168.10.0/24). This was achieved by applying the command: access-list 100 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255, followed by a permit statement to allow all other traffic. The ACL was then applied inbound on the Admin VLAN sub interface to enforce the restriction.

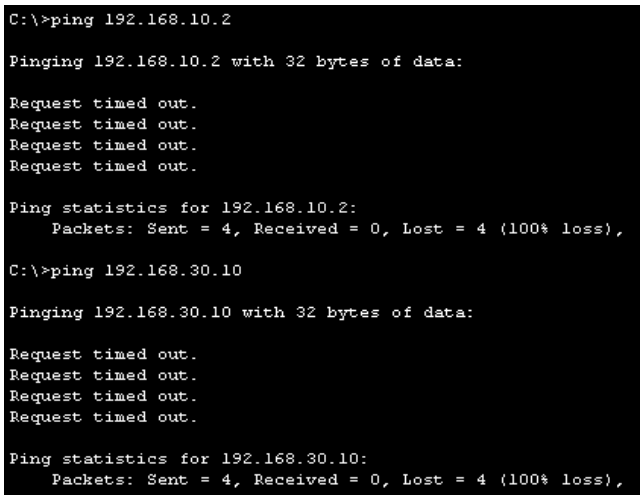
The second security measure focused on port security at the switch level to prevent MAC address spoofing and unauthorized device connections. On S1, ports Fa0/1 and Fa0/2 were configured in access mode and secured using the switchport port-security

feature. The configuration limited each port to a single MAC address, enabled sticky MAC learning, and set the violation mode to shutdown, ensuring that any unauthorized attempt would disable the port, shutting down any connection. A similar configuration was applied to S2 on ports Fa0/1 through Fa0/3, providing consistent protection across the network.

The third layer of defense simulated firewall functionality on R2 to control traffic directed toward the server. An ACL was implemented to allow only HTTP traffic to the server at IP address 192.168.30.10 while denying other protocols. This was accomplished with the command: access-list 101 permit tcp any host 192.168.30.10 eq 80, followed by a deny statement for all other IP traffic to the server and a final permit for all remaining traffic. The ACL was applied inbound on the Server VLAN interface, ensuring that only authorized web traffic could reach the server.

These configurations collectively established a multi-layered security framework, combining network segmentation, access control, and traffic filtering to mitigate common attack vectors such as unauthorized VLAN access, MAC spoofing, and unrestricted service exposure.

Chapter 4. Outcome of Implementations



```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
S2#sh port-security int fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00FF.AABB.CCDD:20
Security Violation Count   : 1
```

After configuring each security measure, the network was tested to confirm that the implemented strategies worked as intended. The first test involved verifying the Access Control List on R1. From PC3 and PC4 in the Employee VLAN, attempts were made to ping the Admin PC at 192.168.10.2. These attempts failed, confirming that the ACL successfully blocked unauthorized access between VLANs.

Next, the firewall-like ACL on Router R2 was tested. Attempts to ping the server at 192.168.30.10 from the Employee VLAN were unsuccessful, while HTTP traffic was permitted. This demonstrated that the ACL correctly filtered traffic, allowing only authorized web services to reach the server.

The third test focused on port security. A MAC address change was simulated on a PC connected to S2 by assigning the following MAC address: 00FF.AABB.CCDD. This triggered a security violation, and the port was automatically placed in a shutdown state. The command: sh port-security int fa0/1 confirmed that the port was disabled due

to the violation, proving that port security effectively prevented unauthorized device access.

Finally, the recovery process was tested by re-enabling the shutdown port on S2. Using the commands: shutdown followed by no shutdown on config mode, the port was restored to operational status. Sticky MAC configurations were cleared to allow normal functionality, and verification commands confirmed that the interface was restored to normal functionality.

These tests validated the effectiveness of the implemented security measures. ACLs successfully restricted Inter-VLAN communication, port security prevented MAC spoofing, and traffic filtering ensured that only authorized services were accessible. The ability to recover from violations without compromising security further demonstrated the effectiveness and strength of the network design used.

Chapter 5. Conclusion

The main objective of this project was to simulate and implement defense strategies against potential cyber attacks within an organizational network using Cisco Packet Tracer. By applying layered security measures such as Access Control Lists, port security, and firewall-like configurations, the network was successfully protected against unauthorized access, MAC address spoofing, and unfiltered traffic. Testing's were done to confirm that the ACLs effectively restricted Inter-VLAN communication, port security prevented unauthorized devices from connecting, and traffic filtering allowed only permitted HTTP services to reach the server. These results demonstrate the importance of combining multiple security mechanisms to create a robust defense posture.

This project highlights how network segmentation, access control, and proactive monitoring can significantly reduce vulnerabilities in real-world environments. If expanded further, additional features such as VPN implementation, advanced firewall systems, and centralized authentication using RADIUS could enhance security even more. This simulation validates that layered security strategies are essential for safeguarding organizational assets and maintaining operational integrity against evolving cyber threats. If such situation were to happen in a real-world network, these methods overall, would be effective.

Additionally, the use of Cisco Packet Tracer as a simulation tool proved to be highly effective in modeling realistic network scenarios, as supported by Yousif and Al-Saffar’s work on communication networks. Its software is very helpful for students as well as IT and Cybersecurity professionals in general to get an idea of how routing,

firewalls, command prompt, etc works to protect against cyber-attacks, Also, the integration of smart technologies and IoT-based systems, as discussed by Gurjar and Dangra, further emphasizes the growing need for adaptable and scalable security frameworks in modern infrastructures. Moreover, the relevance of machine learning-based detection systems, such as the Restricted Boltzmann Machine approach explored by MohanaPriya and Shalinie, suggests that future enhancements could include intelligent threat detection mechanisms to counter more sophisticated attacks. Overall, this project displays a strong foundation for future research and development in secure network design using simulation environments that can help tech professionals of today to better understand such situation as those being trained to work in the tech field in the future who will need these skills and tools to perform these tasks well.

References

Gurjar, N., & Dangra, J. (2022). *Analysis and implementation of 5G-IoT based smart residential buildings using Cisco Packet Tracer 8.1*. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 8(6), 343–352. https://doi.org/10.32628/CSEIT228539

Yousif, M. K., & Al-Saffar, S. K. (2018). *Project scenario of communication network using Cisco Packet Tracer*. *International Journal of Computer Applications*, 180(47), 1–5. https://doi.org/10.5120/ijca2018917262

MohanaPriya, P., & Shalinie, S. M. (2017). *Restricted Boltzmann machine based detection system for DDoS attack in software defined networks*. In *Proceedings of the Fourth International Conference on Signal Processing, Communication and Networking* (pp. 1–6). IEEE. https://doi.org/10.1109/ICSCN.2017.8085731

Appendix A.

Cisco Packet Tracer can be downloaded here to view the project file:

https://www.netacad.com/cisco-packet-tracer