Project Report: Hardening the Switched LAN - A Deep Dive into Layer 2 Security

Author: Samuel Chege

Transforming a Vulnerable Network into a Secure Fortress

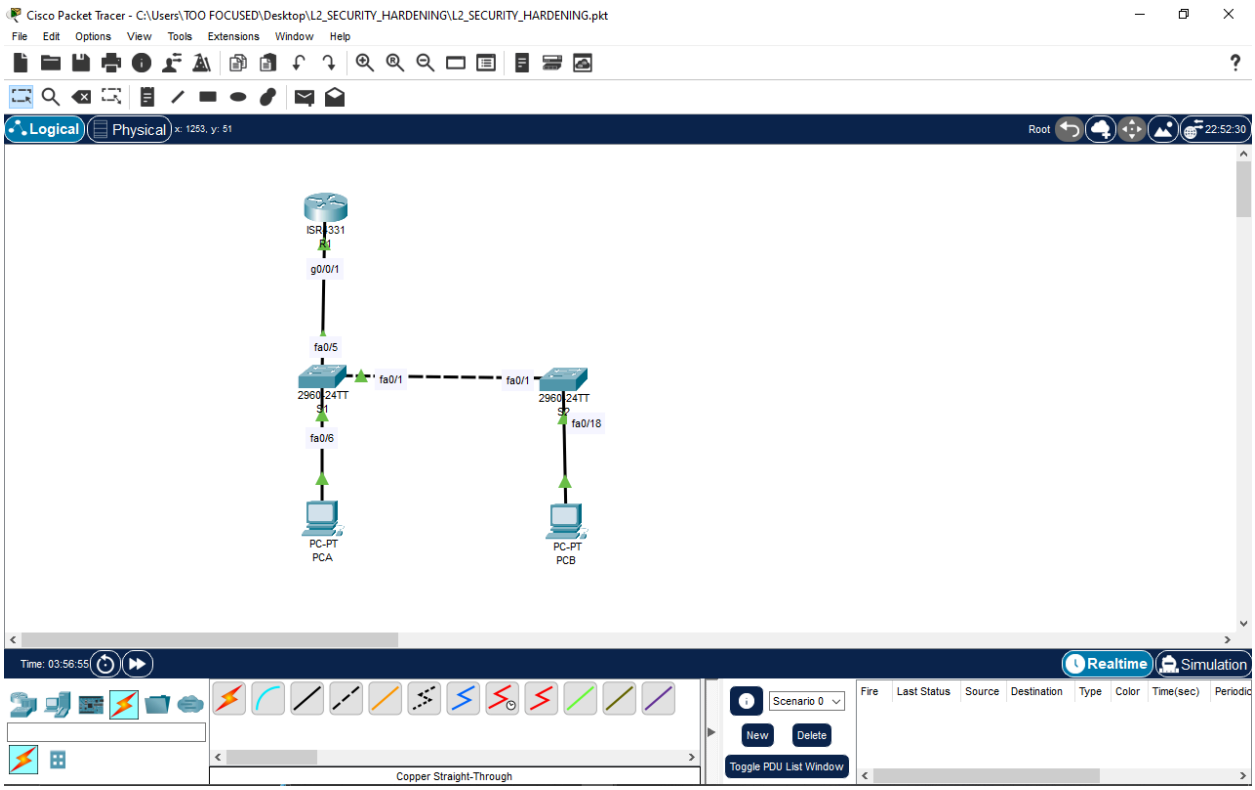
1.1 Introduction: The Unseen Dangers of the Access Layer

In the world of cybersecurity, the most devastating attacks often don't come from sophisticated external hackers, but from simple vulnerabilities on the inside. The access layer—the network switches that users and devices plug into every day—is the soft underbelly of most corporate networks. This project documents the process of transforming a standard, insecure switched network into a hardened, enterprise-grade infrastructure by implementing a multi-layered, defense-in-depth security strategy.

The objective was not just to connect devices, but to build a resilient and secure foundation that protects against a wide range of common Layer 2 attacks, from unauthorized device access to rogue server hijacks.

1.2 Methodology: A Step-by-Step Hardening Process

The project followed a methodical, multi-phase approach to security implementation.



Phase 1: Foundational Segmentation with VLANs

The first step in securing any network is segmentation. VLANs (Virtual Local Area Networks) were used to create logical, isolated broadcast domains.

- **The Why:** By default, all ports on a switch are in the same VLAN, creating a single, flat network. This is insecure and inefficient. By creating separate VLANs, we ensure that traffic from one segment (e.g., Management) is invisible to another, preventing unauthorized snooping and containing broadcast traffic.

Three strategic VLANs were created:

- **VLAN 10 (Management):** For the management interfaces (SVIs) of the switches themselves, providing a secure, dedicated network for administration.
- **VLAN 333 (Native):** Created specifically to be the Native VLAN for trunk links, moving it away from the default VLAN 1.
- **VLAN 999 (ParkingLot):** A "black hole" VLAN with no SVI and no uplinks. All unused ports are assigned here.

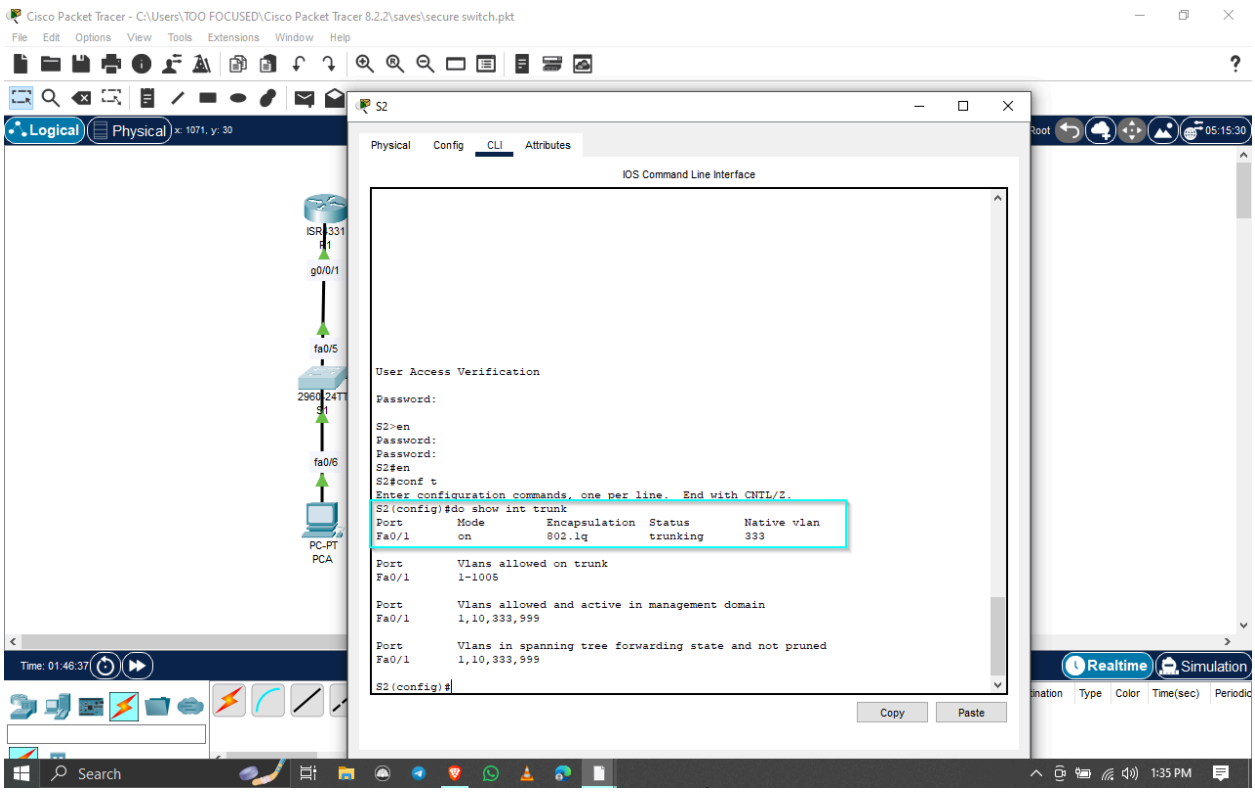
Key Commands:

vlan 10
name Management
vlan 333
name Native
vlan 999
name ParkingLot

Phase 2: Hardening the Inter-Switch Trunks

The links between switches (trunks) are a primary target for attackers. They were hardened with three specific actions:

1. **Manual Trunking & DTP Disabled:** Trunks were manually configured using `switchport mode trunk`, and the insecure Dynamic Trunking Protocol (DTP) was disabled with `switchport nonegotiate`.
   - **The Why:** DTP can be exploited by an attacker to trick a switch into forming a trunk link, giving them access to all VLANs. Disabling it is a critical security step.
2. **Non-Default Native VLAN:** The native VLAN on the trunks was explicitly set to VLAN 333 (`switchport trunk native vlan 333`).
   - **The Why:** VLAN hopping attacks often exploit the default Native VLAN 1. By moving it to an unused, dedicated VLAN, we effectively neutralize this attack vector.



Phase 3: Securing the Fortress Gates (Port Security)

This is the core of access layer defense, preventing unauthorized devices from simply plugging into a wall jack and gaining network access. A multi-faceted port security policy was implemented on user-facing ports.

- **The Why:** Port security acts as a dedicated security guard for each physical port, enforcing rules based on the unique MAC address of the connecting device.

The following features were configured:

- **MAC Address Sticky:** The switches were configured to dynamically learn the MAC address of the first legitimate device plugged in and "stick" it to the running configuration (switchport port-security mac-address sticky).
- **Violation Modes:** Different responses to a security violation were implemented to demonstrate various security postures:
  - **restrict:** When a violation occurs, this mode drops the offending traffic and sends a security alert (SNMP trap) and increments a counter.
  - **protect:** A "silent" mode that drops the offending traffic but does not send an alert, useful in certain low-threat environments.

Key Commands

```
interface FastEthernet0/6
 switchport mode access
 switchport port-security
 switchport port-security maximum 3
 switchport port-security violation restrict
 switchport port-security mac-address sticky
```

```
interface fa0/18
 switchport mode access
 switchport port-security
switchport port-security maximum 2
switchport port-security violation protect
```

`[Insert a screenshot of the 'show port-security interface' command output here to show a configured port.]`

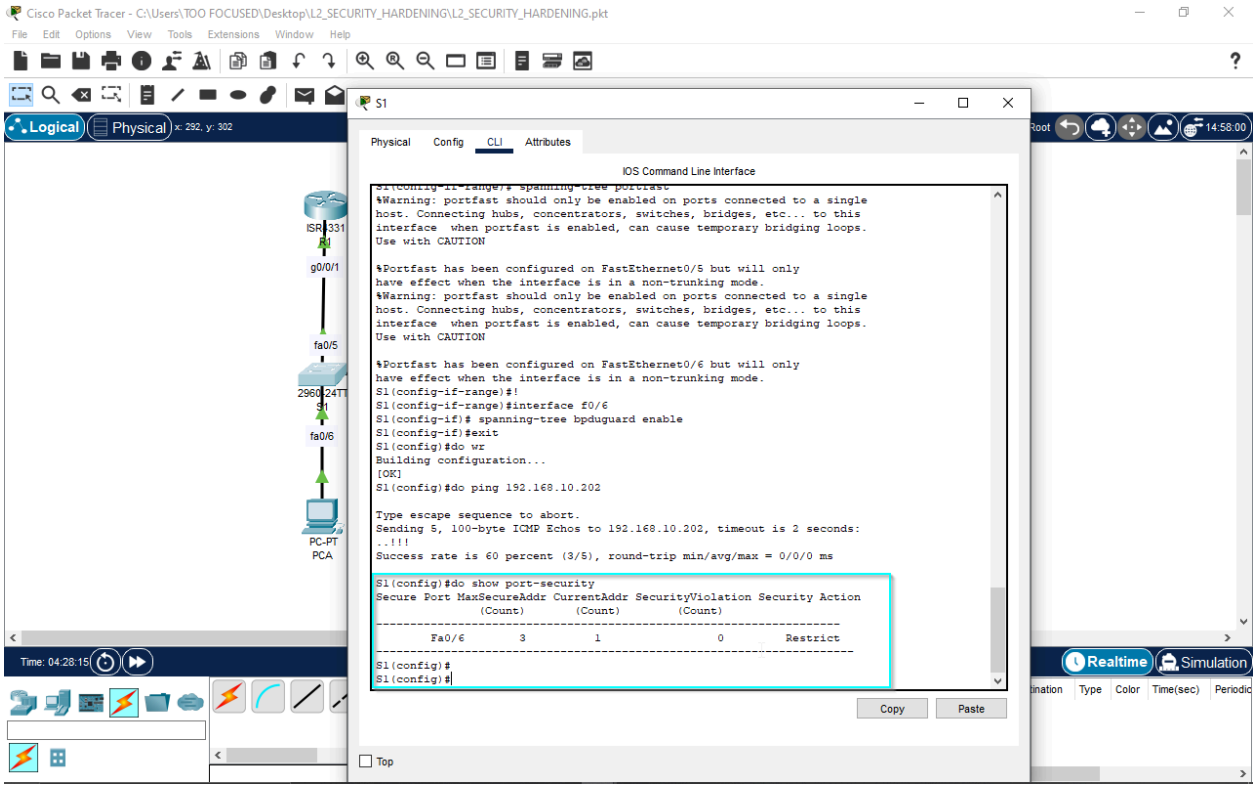
Phase 4: Mitigating Internal Threats (DHCP Snooping & PortFast)

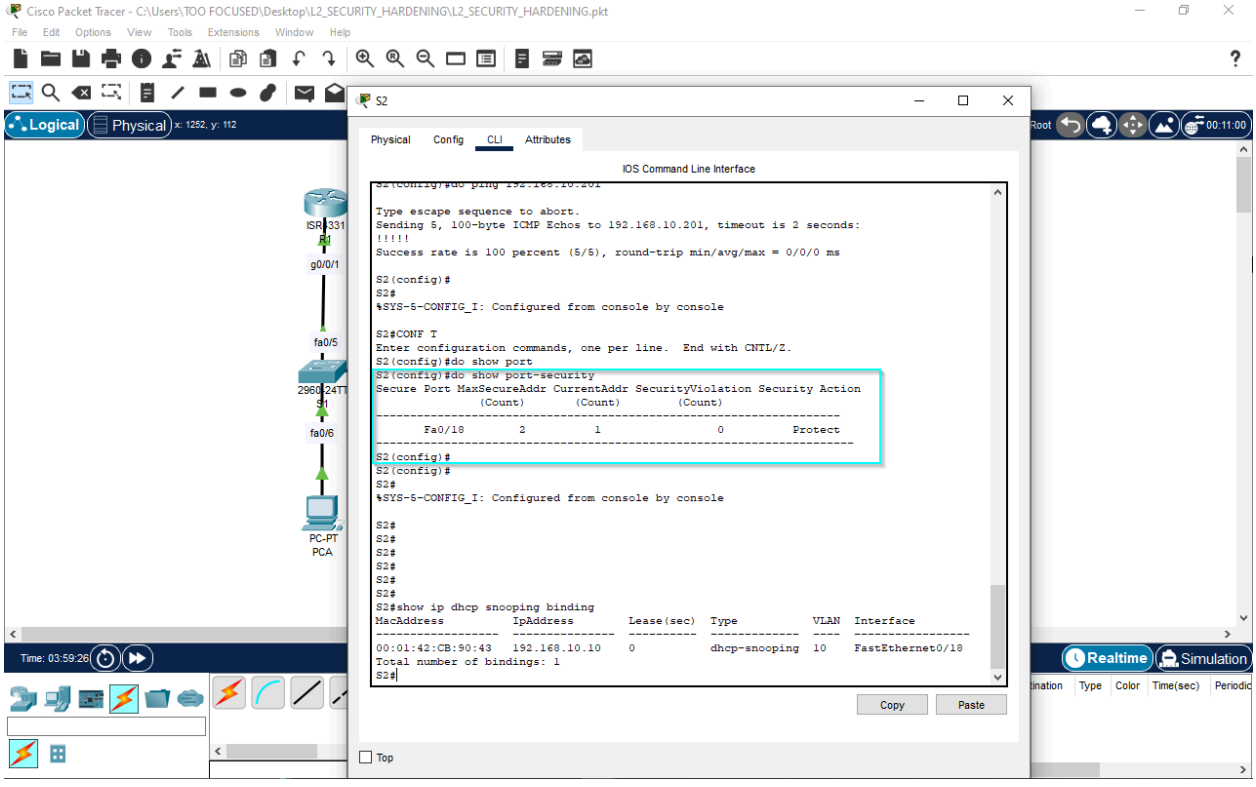
Finally, two advanced features were enabled to protect against common internal attacks and to improve user experience.

1. **DHCP Snooping:** This feature was enabled globally and on the user VLAN.
    - **The Why:** An attacker could plug in a rogue DHCP server and start handing out incorrect IP information, effectively hijacking all user traffic (a Man-in-the-Middle attack). DHCP snooping prevents this by only allowing DHCP server messages from a explicitly **trusted** port (our uplink to the router). Untrusted ports are rate-limited to prevent DHCP starvation attacks.
    - **Analogy:** It's like a building's mailroom only accepting official mail from a verified postal worker, and treating all other mail deliveries as suspicious.

Key Commands:

```
ip dhcp snooping
ip dhcp snooping vlan 10
! On the uplink/trunk interface
interface FastEthernet0/1
 ip dhcp snooping trust
! On a user-facing port
interface FastEthernet0/18
 ip dhcp snooping limit rate 5
```


Cisco Packet Tracer - C:\Users\TOO FOCUSED\Desktop\L2_SECURITY_HARDENING\L2_SECURITY_HARDENING.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
S1
Physical Config CLI Attributes
IOS Command Line Interface
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast has been configured on FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if-range)#!
S1(config-if-range)#interface f0/6
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)#exit
S1(config)#do wr
Building configuration...
[OK]
S1(config)#do ping 192.168.10.202
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.202, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms
S1(config)#do show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
(Count) (Count) (Count)
Fa0/6 3 1 0 Restrict
S1(config)#
S1(config)#
Copy
Paste
Top
ISR4331
g0/0/1
fa0/5
fa0/6
PC-PT
PCA
Time: 04:28:15
Realtime
Simulation


Cisco Packet Tracer - C:\Users\TOO FOCUSED\Desktop\L2_SECURITY_HARDENING\L2_SECURITY_HARDENING.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
S2
Physical Config CLI Attributes
IOS Command Line Interface
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.201, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S2(config)#
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#do show port
S2(config)#do show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
(Count) (Count) (Count)
Fa0/18 2 1 0 Protect
S2(config)#
S2(config)#
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#
S2#
S2#
S2#
S2#
S2#
S2#show ip dhcp snooping binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
00:01:42:CB:90:43 192.168.10.10 0 dhcp-snooping 10 FastEthernet0/18
Total number of bindings: 1
S2#
Copy
Paste
Top
ISR4331
g0/0/1
fa0/5
fa0/6
PC-PT
PCA
Time: 03:59:26
Realtime
Simulation

2. **PortFast & BPDU Guard:** These two features were enabled on all user-facing access ports.
    - **PortFast (spanning-tree portfast):** This command immediately places a port into the forwarding state, bypassing the usual 30-50 second Spanning Tree listening/learning delay. This means a user can plug in their PC and get on the network instantly.
    - **BPDU Guard (spanning-tree bpduguard enable):** This is the critical safety mechanism for PortFast. If a PortFast-enabled port ever receives a BPDU packet (which should only come from another switch), BPDU Guard immediately puts the port into an err-disabled state.
    - **The Why:** This combination provides a great user experience while protecting the network. An employee gets instant connectivity, but if someone accidentally (or maliciously) plugs another switch into a wall jack, the port is instantly shut down, preventing a catastrophic STP loop or network hijack.

1.3 Conclusion: A Blueprint for a Secure Access Layer

This project successfully demonstrates that network security is not a single feature, but a layered strategy. By combining VLAN segmentation, trunk hardening, port security, DHCP snooping, and STP enhancements, a standard, vulnerable network was transformed into a resilient and secure infrastructure. The insights gained from implementing and verifying each of these distinct but interconnected features provide a comprehensive blueprint for securing any enterprise access layer network.