IY4T705
MSc (Hons) Applied Cyber Security
Final Project Proposal Form

Student Name: Sami ul haq Chishti

Student Number: 30135209

Working Title of the Dissertation

Secure Utilization of VXLAN in Multi-Tenant Environments

Aims:

This project aims to explore the use of VXLAN (Virtual Extensible LAN) in multi-tenant environments, focusing on its security aspects. It will evaluate potential security vulnerabilities, mitigation strategies, and performance impacts when securing VXLAN-based networks. The goal is to enhance isolation, confidentiality, and integrity in multi-tenant data centres, ensuring secure network virtualization.

Research Objectives

- Investigate VXLAN security risks in multi-tenant environments.
- Analyze existing security mechanisms (EVPN, MACsec, IPsec) for VXLAN protection.

Development Objectives

- Deploy a VXLAN-based multi-tenant network in a simulated environment.
- Implement security enhancements such as encryption, authentication, and intrusion detection.

Evaluation Objectives

- Assess the effectiveness of security measures in preventing VXLAN-specific attacks.
- Compare the performance impact (latency, overhead) of secured vs. non-secured VXLAN implementations.

Why are you going to do it?

Problem Statement:

Traditional VLANs have scalability limits, making VXLAN essential for modern networks. However, VXLAN introduces new security challenges, such as:

- Lack of inherent encryption (traffic is exposed in transit).
- Potential for spoofing and unauthorized access due to shared underlay networks.
- Difficulties in monitoring and intrusion detection within VXLAN tunnels.

Benefits:

- **Improved tenant isolation**:
  Enhanced network security for multi-tenant environments.
- **Stronger encryption and authentication**:
  Secure VXLAN tunnels using MACsec/IPsec.
- **Better threat detection**:
  Identifying VXLAN-specific vulnerabilities and improving IDS/IPS capabilities.
- **Scalability and compliance**:
  Ensuring VXLAN deployments meet security compliance requirements.

Target Audience:

- Cloud service providers, deploying multi-tenant architectures.
- Enterprise IT teams, managing virtualized networks.
- Cybersecurity professionals, focusing on network security.
- Academic researchers, studying network virtualization and security.

Research methodology:

Approach:

This research will follow a practical, experimental approach, combining theoretical study with real-world simulations and security testing.

Steps:

1. **Literature Review**:
   Study existing VXLAN architectures, security risks, and mitigation techniques.
   Analyze case studies of VXLAN security implementations.
2. **Experimental Setup**:
   Deploy a simulated multi-tenant cloud environment with VXLAN overlays.
   Implement different security mechanisms (EVPN, MACsec, IPsec).
3. **Security Testing & Analysis**:
   Conduct penetration testing (e.g., spoofing, DoS attacks).
   Use packet analysis (Wireshark, Suricata, Snort) to monitor VXLAN traffic.
   Compare performance overhead of security-enhanced VXLAN vs. standard VXLAN.
4. **Findings & Recommendations**:
   Evaluate results based on security effectiveness and performance trade-offs.
   Propose best practices for securing VXLAN in multi-tenant setups.

Are there any risks are there involved in the project?

Resource Constraints:
Simulating a multi-tenant environment with real-world security scenarios requires adequate hardware and software resources, which may be limited.

Compliance and Ethical Considerations:
Testing security vulnerabilities must be conduct in a controlled environment to avoid unintentional disruptions and ethical concerns.

Required Hardware and Software Resources:

Hardware:

- **Virtualized environment:** VMware ESXi, or Proxmox.
- **Physical or virtual routers/switches:** Cisco, Juniper, or Open vSwitch.
- **Linux-based servers or VMs:** Ubuntu, CentOS.

Software:

- **Networking Simulators:** GNS3, EVE-NG, Mininet, or Cisco VIRL, VMware NSX/OpenStack Neutron.
- **VXLAN Configuration:** FRRouting, Open vSwitch, iproute2.
- **Security Tools:** Wireshark, Suricata, Snort, nmap, Metasploit.
- **SDN Controllers:** OpenDaylight, ONOS.

End Deliverable:

1. A detailed research report analyzing VXLAN security risks and mitigation techniques.
2. A working simulation demonstrating secure VXLAN implementation in a multi-tenant network.
3. Performance and security analysis results, including comparative data on attack prevention.
4. A security guideline document with best practices for securing VXLAN in enterprise and cloud environments.

This section will be completed once your proposal has been agreed with the project co-ordinator.

First Supervisor:

Signed:

Date:

Second Supervisor:

Signed:

Date:

Student:

Signed:

Date:

PLEASE NOTE: A copy of this signed proposal MUST be included in the appendices of your final submission. It is the student's responsibility to keep a record of this signed document.