MUHAMMAD TAIMOOR AHSAN

RIPHAH INTERNATIONAL UNIVERSITY

OSINT TASK

Target Organization: Riphah International University, Pakistan
Analyst: Independent OSINT Researcher
Date: March 2025

1.1 Purpose of Investigation

The purpose of this Open-Source Intelligence (OSINT) investigation is to demonstrate how publicly available information can be collected, correlated, and analyzed to assess the **potential cyber exposure** of an educational institution. The selected target for this academic exercise is **Riphah International University (Pakistan)**.

This investigation follows **passive OSINT principles only**, ensuring no direct interaction with live systems.

1.2 High-Level Findings

Based on the analysis of simulated open-source data:

- Multiple publicly discoverable **domains and subdomains** were identified.
- Several **synthetic IP addresses** appeared to expose common academic services.
- Simulated credential leaks suggested **email reuse risks**.
- Publicly available staff information indicated **potential phishing vectors**.
- Weak configuration patterns were identified in **mock firewall and network setups**.

1.3 Risk Overview

Risk Category	Level
Phishing & Social Engineering	High
Credential Exposure	Medium
Network Misconfiguration	Medium
Insider Threat	Low–Medium

---

2. Scope & Methodology

2.1 Scope

- Passive OSINT only
- No active scanning or exploitation
- No real-world validation
- All outputs are synthetic

2.2 Methodology

The investigation followed a structured OSINT workflow:

1. **Reconnaissance**
    - Domain enumeration (simulated)
    - Infrastructure discovery
2. **Correlation**
    - Linking IPs, services, and email formats
    - Human OSINT analysis
3. **Analysis**
    - Risk assessment

- Threat modeling

4. **Reporting**
    - Academic documentation

2.3 Tools Used

- WHOIS lookup (synthetic output)
- Shodan-style exposure search
- Google Dorking (conceptual)
- VirusTotal (simulated reputation)
- Censys-style service mapping
- HaveIBeenPwned-style breach checks

2.4 Ethical Boundaries

- No scanning
- No probing
- No credential testing
- No real individual identification

---

3. Domain & Infrastructure Analysis (Simulated)

3.1 Primary Domain

Riphah-edu.pk

3.2 Identified Subdomains (Synthetic)

Subdomain	Purpose
portal.riphah-edu.pk	Student portal
mail.riphah-edu.pk	Email services
lms.riphah-edu.pk	Learning Management System
vpn.riphah-edu.pk	Remote access
admissions.riphah-edu.pk	Admissions portal
library.riphah-edu.pk	Digital library

3.3 WHOIS-Style Details (Simulated)

Field	Value
Registrar	Synthetic Registrar Ltd
Registration Date	2010-06-12
Expiry Date	2026-06-12
Country	Pakistan
Name Servers	ns1.synthetic-dns.net

3.4 Simulated DNS Records

Record Type	Value
A	203.0.113.10
MX	mail.synthetic-provider.net
TXT	v=spf1 include:synthetic

3.5 Hosting Overview

The simulated infrastructure appears to be hosted on a **hybrid environment** combining:

- Local data centers
- Cloud-based academic hosting
- Third-party email services

---

4. Simulated IP Address Mapping

4.1 Generated IPv4 Addresses (FICTIONAL)

IP Address	Service
198.51.100.11	Web Server
198.51.100.12	LMS
198.51.100.13	Mail
198.51.100.14	VPN
198.51.100.15	SSH
203.0.113.20	Admissions
203.0.113.21	Library
203.0.113.22	API
203.0.113.23	Backup
203.0.113.24	Dev Server
192.0.2.30	Firewall
192.0.2.31	Database

IP Address	Service
192.0.2.32	CDN Origin

4.2 Port Exposure Table (Simulated)

IP	Open Ports	Risk
198.51.100.11	80, 443	Low
198.51.100.14	443, 1194	Medium
198.51.100.15	22	Medium
203.0.113.24	22, 8080	High

---

5. Network Exposure Analysis

5.1 Simulated Open Ports

- HTTP/HTTPS exposed for public portals
- SSH exposed on development servers
- VPN services accessible externally

5.2 Mock Firewall Misconfigurations

- SSH not IP-restricted
- Dev servers accessible from public internet
- Weak segmentation between academic and admin zones

5.3 CDN vs Origin Server

Some services appear CDN-protected, while others reveal **origin IP leakage**, increasing exposure risk.

6. Email & Credential Exposure (Simulated)

6.1 Email Format Patterns

firstname.lastname@riphah-edu.pk

staffid@riphah-edu.pk

6.2 Simulated Breach Results

Source	Records
Academic Forum Leak	2,100
Old LMS Dump	1,300
Third-Party Vendor	600

6.3 Credential Risks

- Password reuse across platforms
- Weak historical passwords
- Delayed breach detection

---

7. Social Media & Human OSINT

7.1 Public-Facing Roles (No Names)

- IT Administrator
- Admissions Officer
- Faculty Coordinator
- Student Affairs Manager

7.2 Oversharing Risks

- Conference badges
- Internal system screenshots
- Email signatures
- Office locations

7.3 Phishing Vectors

- Fake IT password resets
- Scholarship announcements
- Conference invitations

---

8. Threat Scenarios

8.1 Phishing Attack Simulation

An attacker crafts an email impersonating the IT department, redirecting users to a fake LMS login portal.

8.2 Ransomware Entry Point

- Initial access via compromised credentials
- Lateral movement through misconfigured SMB
- Data encryption of academic records

8.3 Data Leakage Chain

Credential reuse → Email compromise → Cloud storage access → Data exfiltration

---

8.4 Insider Threat Model

- Disgruntled staff
- Excessive access privileges
- Lack of monitoring

---

9. Risk Assessment Matrix

Risk	Likelihood	Impact	Level
Phishing	High	High	Critical
Credential Leaks	Medium	High	High
Network Misconfig	Medium	Medium	Medium
Insider Threat	Low	High	Medium

---

10. Mitigation & Recommendations

10.1 Technical Controls

- Enforce MFA
- Restrict SSH access
- Network segmentation
- Regular patching

10.2 Awareness Training

- Phishing simulations
- Staff OSINT awareness
- Secure password practices

10.3 Monitoring Improvements

- Centralized logging
- SIEM integration
- Regular audits
