Security assessment on a VXLAN-based network

Guido Pineda Reyes

MSc. Systems and Networking Engineering
University of Amsterdam

February 5, 2014
Outline

1. Introduction
   - Virtual eXtensible LAN
   - Research question
   - Approach

2. VXLAN prototype

3. Security assessment
   - MAC Flood Attack
   - Double-Encapsulated 802.1Q/Nested VLAN Attack
   - ARP Attack
   - UDP Flood Attack
   - Future research
   - Conclusions

4. Q&A
Outline

1 Introduction
   - Virtual eXtensible LAN
     - Research question
     - Approach
2 VXLAN prototype
3 Security assessment
   - MAC Flood Attack
   - Double-Encapsulated 802.1Q/Nested VLAN Attack
   - ARP Attack
   - UDP Flood Attack
   - Future research
   - Conclusions
4 Q&A

Guido Pineda Reyes

Security assessment on a VXLAN-based network
Virtual eXtensible LAN

Introduction

- Still an Internet Draft, current revision: 7th
- Allows to extend logical networks
- Encapsulates layer MAC-based Layer 2 frames within a UDP packet
- Up to 16 million logical networks
- Security measurements have not been performed yet
Virtual eXtensible LAN

Typical use case
Outline

1. Introduction
   - Virtual eXtensible LAN
   - Research question
   - Approach

2. VXLAN prototype

3. Security assessment
   - MAC Flood Attack
   - Double-Encapsulated 802.1Q/Nested VLAN Attack
   - ARP Attack
   - UDP Flood Attack
   - Future research
   - Conclusions

4. Q&A

Guido Pineda Reyes

Security assessment on a VXLAN-based network
Main question: How feasible are the known VLAN attacks in a VXLAN environment?

Subquestions:
- Which attacks were successful?
- What is the difference between these attacks in a VLAN and a VXLAN environment?
- Is there anyway to prevent them or mitigate them?
Outline

1. Introduction
   - Virtual eXtensible LAN
   - Research question
   - Approach
2. VXLAN prototype
3. Security assessment
   - MAC Flood Attack
   - Double-Encapsulated 802.1Q/Nested VLAN Attack
   - ARP Attack
   - UDP Flood Attack
   - Future research
   - Conclusions
4. Q&A

Guido Pineda Reyes

Security assessment on a VXLAN-based network
Approach

■ Build the VXLAN prototype.
■ Deploy the security assessment on the prototype.
■ Focus on successful attacks.
■ Understand how these attacks work to give a solution on how to mitigate or prevent them.
VXLAN prototype

Design

- VNI = 6010 (20.0.0.0/8) - 239.1.1.1
- VNI = 7777 (10.0.0.0/8) - 239.2.2.2
VXLAN prototype

Options

- VMware vSphere products
- VMware vSphere + Cisco Nexus 1000v
- VXLAN Linux implementation (needs kernel modification)
## VXLAN prototype

Connectivity tests: UDP encapsulated traffic

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>247 55.149004000</td>
<td>192.168.0.1</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>248 55.149352000</td>
<td>192.168.0.1</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>249 55.149403000</td>
<td>192.168.0.1</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>250 55.149418000</td>
<td>192.168.0.1</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>251 55.149430000</td>
<td>192.168.0.1</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>252 55.149759000</td>
<td>192.168.0.1</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>253 55.149809000</td>
<td>192.168.0.1</td>
<td>UDP</td>
<td></td>
</tr>
</tbody>
</table>
VXLAN prototype
Connectivity tests: VXLAN encapsulation

- Frame 436: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
- Ethernet II, Src: Parallel_b0:6e:42 (00:1c:42:b0:6e:42), Dst: Dell_8b:82:ab (b8:ac:6f:8b:82:ab)
- User Datagram Protocol, Src Port: 56992 (56992), Dst Port: otv (8472)
- Virtual extensible Local Area Network
  - Flags: 0x08
    - Reserved: 0x000000
    - VXLAN Network Identifier (VNI): 6010
    - Reserved: 0
  - Internet Protocol Version 4, Src: 20.0.0.4 (20.0.0.4), Dst: 20.0.0.3 (20.0.0.3)
  - Internet Control Message Protocol
Security Assessment

- MAC Flood Attack
- Double-Encapsulated 802.1Q/Nested VLAN Attack
- ARP Attack
- UDP Flood Attack
- Evaluation
Outline

1. Introduction
   - Virtual eXtensible LAN
   - Research question
   - Approach
2. VXLAN prototype
3. Security assessment
   - MAC Flood Attack
   - Double-Encapsulated 802.1Q/Nested VLAN Attack
   - ARP Attack
   - UDP Flood Attack
   - Future research
   - Conclusions
4. Q&A
MAC Flood Attack

Scenarios
MAC Flood Attack

- Tool: macof
- Results:
  - Attacker on physical net: Successful
  - Attacker on logical net: Failed
- Mitigation/Prevention:
  - Restrict the number of MAC addresses to one port
  - Specify static MAC address association
  - IDS
Outline

1. Introduction
   - Virtual eXtensible LAN
   - Research question
   - Approach

2. VXLAN prototype

3. Security assessment
   - MAC Flood Attack
   - Double-Encapsulated 802.1Q/Nested VLAN Attack
   - ARP Attack
   - UDP Flood Attack
   - Future research
   - Conclusions

4. Q&A

Guido Pineda Reyes
Security assessment on a VXLAN-based network
Double-Encapsulated 802.1Q/Nested VLAN Attack

Scenario
Double-Encapsulated 802.1Q/Nested VLAN Attack

Concept

<table>
<thead>
<tr>
<th>Outer Ether</th>
<th>Outer IP</th>
<th>UDP (dst.port=8472)</th>
<th>VXLAN (VNI=7777)</th>
<th>VXLAN (VNI=6010)</th>
<th>Inner Ether</th>
<th>Inner IP</th>
<th>Payload</th>
<th>FCS</th>
</tr>
</thead>
</table>

Victim's VXLAN header
Double-Encapsulated 802.1Q/Nested VLAN Attack

- **Tool:** scapy
- **Results:**
  - Attacker on logical net: Failed
Outline

1. Introduction
   - Virtual eXtensible LAN
   - Research question
   - Approach

2. VXLAN prototype

3. Security assessment
   - MAC Flood Attack
   - Double-Encapsulated 802.1Q/Nested VLAN Attack
   - ARP Attack
   - UDP Flood Attack
   - Future research
   - Conclusions

4. Q&A
ARP Attack

Scenarios
ARP Attack

Summary

- Tool: arpspoof
- Results:
  - Attacker on physical net: Successful
  - Attacker on logical net: Successful
- Mitigation/Prevention:
  - Blocking direct communication between the attacker and the victim.

- Configuring private communication between the hosts at the service provider level.

```
vnm@VM2:~$ ping 20.0.0.3
PING 20.0.0.3 (20.0.0.3) 56(84) bytes of data.
64 bytes from 20.0.0.3: icmp_seq=1 ttl=64 time=0.916 ms
64 bytes from 20.0.0.3: icmp_seq=2 ttl=64 time=0.724 ms
From 20.0.0.5: icmp_seq=3 Redirect Host (New next hop: 20.0.0.3)
From 20.0.0.5: icmp_seq=4 Redirect Host 64 bytes from 20.0.0.3: icmp_seq=4
From 20.0.0.5: icmp_seq=5 Redirect Host (New next hop: 20.0.0.3)
```

Attacker IP Address
ARP Attack

Scenarios

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Source MAC</th>
<th>Destination IP</th>
<th>Destination MAC</th>
<th>Protocol</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 9.546994000</td>
<td>00:00:00:00:00:00:01</td>
<td>20.0.0.5</td>
<td>00:00:00:00:00:00:02</td>
<td>ICMP</td>
<td>126 Redirect</td>
</tr>
<tr>
<td>26 9.547013000</td>
<td>00:00:00:00:00:00:03</td>
<td>20.0.0.3</td>
<td>00:00:00:00:00:00:04</td>
<td>ICMP</td>
<td>98 Echo (ping) reply</td>
</tr>
<tr>
<td>27 10.001877000</td>
<td>CadmusCo_c1:09:db</td>
<td>CadmusCo_c82:35:ae</td>
<td></td>
<td>ARP</td>
<td>42 20.0.0.4 is at 08:00</td>
</tr>
<tr>
<td>28 10.547709000</td>
<td>00:00:00:00:00:00:05</td>
<td>20.0.0.4</td>
<td>00:00:00:00:00:00:06</td>
<td>ICMP</td>
<td>98 Echo (ping) request</td>
</tr>
<tr>
<td>29 10.547745000</td>
<td>00:00:00:00:00:00:07</td>
<td>20.0.0.5</td>
<td>00:00:00:00:00:00:08</td>
<td>ICMP</td>
<td>126 Redirect</td>
</tr>
</tbody>
</table>
Outline

1. Introduction
   - Virtual eXtensible LAN
   - Research question
   - Approach

2. VXLAN prototype

3. Security assessment
   - MAC Flood Attack
   - Double-Encapsulated 802.1Q/Nested VLAN Attack
   - ARP Attack
   - UDP Flood Attack
   - Future research
   - Conclusions

4. Q&A
UDP Flood Attack

Summary

- Tool: `flood.pl`
- Results:
  - Attacker on physical net: Failed
- Mitigation/Prevention:
  - IDS to detect unusual UDP traffic
Outline

1 Introduction
   - Virtual eXtensible LAN
   - Research question
   - Approach

2 VXLAN prototype

3 Security assessment
   - MAC Flood Attack
   - Double-Encapsulated 802.1Q/Nested VLAN Attack
   - ARP Attack
   - UDP Flood Attack
   - Future research
   - Conclusions

4 Q&A
Further research

Possible vulnerability

- Trying to modify the FDB and redirect all traffic to the attacker.
Outline

1. Introduction
   - Virtual eXtensible LAN
   - Research question
   - Approach

2. VXLAN prototype

3. Security assessment
   - MAC Flood Attack
   - Double-Encapsulated 802.1Q/Nested VLAN Attack
   - ARP Attack
   - UDP Flood Attack
   - Future research
   - Conclusions

4. Q&A
Conclusions

Most relevant points

- Building the prototype is not trivial
- Some attacks are feasible
- Double-Encapsulation attack and MAC flooding attacks failures show that VXLAN segments are isolated from each other.
- ARP attacks show that Man in the Middle Attacks or DoS are possible from within any network (physical & logical).

<table>
<thead>
<tr>
<th>Attack</th>
<th>Results: Scenario on</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Overlay Network</td>
<td>Tenant Network</td>
</tr>
<tr>
<td>MAC Flooding Attack</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td>Double-Encapsulated/Nested VLAN Attack</td>
<td>N/A</td>
<td>Failed</td>
</tr>
<tr>
<td>ARP Attack</td>
<td>Successful</td>
<td>Successful</td>
</tr>
<tr>
<td>UDP Flood Attack</td>
<td>Failed</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Questions?