Outline

- **Introduction**
- Virtual LAN concepts
- Common Attack Methods
  - Overview of Attacks
  - Why They Are Effective
  - Mitigation Strategies
- Future Work in Virtualized Environments
  - Planned Attacks
  - Planned Test Scenarios
- Questions
Introduction

- Researching Layer 2 network security in virtualized environments
- Already conducted successful experiments using:
  - MAC flooding
    - Open vSwitch based virtual networks are vulnerable!
    - Results made public at DerbyCon 4.0
    - Submitted vulnerability report to http://cert.org and security@openvswitch.org
- DHCP attacks
  - Multiple scenarios evaluated on each platform
  - All tested platforms were found vulnerable!
# MAC Flooding Summary

<table>
<thead>
<tr>
<th>Test Environments</th>
<th>Eavesdropping</th>
<th>Performance Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Xen w/ Linux Bridging</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>OS Xen w/ Open vSwitch 1.11.0</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>OS Xen w/ Open vSwitch 2.0.0</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Citrix XenServer 6.2</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MS Server 2008 R2 w/Hyper-V</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MS Hyper-V 2008 Free</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>VMware vSphere (ESXi) 5.5</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### DHCP Attack Summary

<table>
<thead>
<tr>
<th>Test Environments</th>
<th>Shell Shock</th>
<th>Poisoned DNS</th>
<th>Invalid DG</th>
<th>Malicious DG</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Xen w/ Linux Bridging</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>OS Xen w/ Open vSwitch 1.11.0</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>OS Xen w/ Open vSwitch 2.0.0</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Citrix XenServer 6.2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MS Server 2008 R2 w/Hyper-V</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MS Hyper-V 2008 Free</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>VMware vSphere (ESXi) 5.5</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Next Step

- Next step: evaluate VLAN security in virtualized environments:
  - All virtual switch products support the creation of VLANs
  - VLANs allow service providers to *logically* separate and isolate multi-tenant virtual networks within their environments
- Do the current known vulnerabilities in commonly used VLAN protocols apply to virtualized networks?
  - Could allow for:
    - Eavesdropping of traffic on restricted VLANs
    - Injection of packets onto a restricted VLAN
    - DoS attacks
    - Covert channels
Outline

- Introduction
- **Basic VLAN concepts**
- Common Attack Methods
  - Overview of Attacks
  - Why They Are Effective
  - Mitigation Strategies
- Future Work in Virtualized Environments
  - Planned Attacks
  - Planned Test Scenarios
- Questions
Virtual LAN Concepts

- Virtual LAN (VLAN)
  - Allows for separation of physical network into multiple logical networks
  - Each logical network is considered as a single broadcast domain
    - Layer 2 connectivity
    - Broadcast traffic reaches all logically connected nodes
    - Separated by Layer 3 devices (*routers*)
    - Broadcast domains can span multiple network segments by the use of a *bridge* or *switch*
Virtual LAN Concepts

• Switch Ports *(managed switches)*
  • *Trunk port*
    • Port on switch configured to carry traffic for multiple VLANs to other connected switches
    • Allows VLANs to expand beyond a single switch
      • *ie.* between buildings
  • *Access port*
    • Port on switch configured to provide access to a single VLAN
    • Tags all traffic entering port from connected devices with associated VLAN ID *(ie.* VLAN 102)*
    • No need to configure connected device with specific VLAN information
Virtual LAN Concepts

- Types of VLANs
  - **Native VLAN**
    - Allows for the passing of un-tagged frames between devices
    - Trunk connections between switches
    - CDP, DTP, VTP messages between switches
    - VLAN 1 traffic between devices on a network
    - Typically used for management purposes
    - Default VLAN on an un-configured switch
    - Defaults to VLAN 1
Virtual LAN Concepts

• Types of VLANs (cont.)
  • Access VLAN
    • Restricted VLAN used for client access to a logical network
    • All traffic is tagged with the ID of the access VLAN
    • Un-tagged traffic or traffic tagged with a different VLAN ID is prevented from accessing the logically separated broadcast domain
  • Used to isolate traffic on a network
    • Separate traffic from different departments
    • Increase security by preventing unauthorized access to network resources
Virtual LAN Concepts

- Standard Ethernet frames consist of the following fields:
  - Destination MAC address
  - Source MAC address
  - Type of frame or frame length
  - The data payload
  - A frame check sequence

<table>
<thead>
<tr>
<th>Dst MAC</th>
<th>Src MAC</th>
<th>Type/Len</th>
<th>Data</th>
<th>FCS</th>
</tr>
</thead>
</table>
Virtual LAN Concepts

- Ethernet frames are modified for VLAN traffic:
  - Addition of a 802.1q VLAN header
  - 32 bits of extra information wedged in

<table>
<thead>
<tr>
<th>Dst MAC</th>
<th>Src MAC</th>
<th>802.1q VLAN Tag</th>
<th>Type/Len</th>
<th>Data</th>
<th>FCS</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>TPID</th>
<th>TPI</th>
<th>DEI</th>
<th>VID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x8100</td>
<td>(3 bits)</td>
<td>(1 bit)</td>
<td>(12 bits)</td>
</tr>
</tbody>
</table>

- 4 Bytes
- 2 Bytes
Virtual LAN Concepts

- The IEEE 802.1ad standard also known as Q-in-Q allows for the addition of multiple 802.1q VLAN tags to a frame
- Useful for:
  - Provider bridging
  - Stacked VLANs

```
<table>
<thead>
<tr>
<th>Dst MAC</th>
<th>Src MAC</th>
<th>802.1q VLAN Tag</th>
<th>Type/Len</th>
<th>Data</th>
<th>FCS</th>
</tr>
</thead>
</table>
```

```
<table>
<thead>
<tr>
<th>Dst MAC</th>
<th>Src MAC</th>
<th>802.1q VLAN Tag</th>
<th>802.1q VLAN Tag</th>
<th>Type/Len</th>
<th>Data</th>
<th>FCS</th>
</tr>
</thead>
</table>
```
Outline

- Introduction
- Virtual LAN concepts
- **Common Attack Methods**
  - Overview of Attacks
  - Why They Are Effective
  - Mitigation Strategies
- Future Work in Virtualized Environments
  - Planned Attacks
  - Planned Test Scenarios
- Questions
VLAN Hopping

- VLAN Hopping
  - An attack method used to gain unauthorized access to another Virtual LAN on a packet switched network
  - Consists of attacker sending frames from one VLAN to another that would otherwise be inaccessible

- Two methods
  - Switch Spoofing
  - Double Tagging
Switch Spoofing
Switch Spoofing

- CVE-2005-1942
  - “Cisco switches that support 802.1x security allow remote attackers to bypass port security and gain access to the VLAN via spoofed Cisco Discovery Protocol (CDP) messages.”
Switch Spoofing

- Cisco Discovery Protocol
  - Cisco proprietary Layer 2 protocol
  - Allows connected Cisco devices to share information
    - Operating system
    - IP address
    - Routing information
    - Duplex settings
    - VTP domain
    - VLAN information
Switch Spoofing

- CVE-1999-1129
  - “Cisco Catalyst 2900 Virtual LAN (VLAN) switches allow remote attackers to inject 802.1q frames into another VLAN by forging the VLAN identifier in the trunking tag.”

- Combine with ...

- **DTP**: Dynamic Trunking protocol. "If a switch port were configured as DTP auto and were to receive a fake DTP packet, it might become a trunk port and it might start accepting traffic destined for any VLAN" (Cisco).
  - **DTP Auto is the default setting!**
Switch Spoofing

- Dynamic Trunking Protocol
  - Cisco proprietary Layer 2 protocol
  - Allows automatic configuration of trunk ports on Cisco switches
    - Automatically configures VLAN trunking for all supported VLANs
  - Provides ability to negotiate the trunking method with neighbor devices
  - Pair this with CDP and your Cisco devices can pretty much configure themselves \textit{(not very securely!)}
Switch Spoofing

All ports configured in dynamic desirable mode by default

VLAN 1 - Native VLAN
VLANs 2,3 - Access VLANs
Switch Spoofing

All ports configured in dynamic desirable mode by default

VLAN 1 - Native VLAN
VLANs 2,3 - Access VLANs
Switch Spoofing

All ports configured in dynamic desirable mode by default

VLAN 1 - Native VLAN
VLANs 2,3 - Access VLANs

Attacker sends spoofed DTP packet to switch
Switch Spoofing

All ports configured in dynamic desirable mode by default

VLAN 1 - Native VLAN
VLANs 2,3 - Access VLANs
Switch Spoofing

All ports configured in dynamic desirable mode by default

VLAN 1 - Native VLAN
VLANs 2,3 - Access VLANs
Switch Spoofing

- Consequences
  - Attacker's system has a trunk connection to the switch
    - Attacker can generate frames for any VLAN supported by the trunk connection
  - Attacker can communicate with any device on any of the associated VLANs
  - Two-way communication can occur between the attacker and a targeted node because the attacker can actually place themselves on the VLAN
  - Also allows attacker to eavesdrop on the traffic within a target VLAN
Switch Spoofing

- Mitigation
  - Disable unused switch ports
  - Disable CDP and DTP
    - Or use on an as need, per port basis!
  - Restrict the amount of trunk ports
    - Should only be configured when connecting devices require it (ie. other switches)
    - Limit VLAN access on trunk ports to only what the connected segments require
  - Configure all other ports as access ports (no trunking) with no access to the native VLAN
  - Don't use Cisco switches...
Double Tagging
Double Tagging

- CVE-2005-4440
  - [CVE Details](http://www.cvedetails.com/cve/CVE-2005-4440/)
  - "The 802.1q VLAN protocol allows remote attackers to bypass network segmentation and spoof VLAN traffic via a message with two 802.1q tags, which causes the second tag to be redirected from a downstream switch after the first tag has been stripped."
- A.K.A: "Double-Tagging VLAN jumping attack"
Double Tagging

VLAN 1 - Native VLAN
VLANs 2,3 - Access VLANs
Double Tagging

- **VLAN 1** - Native VLAN
- VLANs 2,3 - Access VLANs
### Double Tagging

<table>
<thead>
<tr>
<th>Dst MAC</th>
<th>Src MAC</th>
<th>Type/Len</th>
<th>Data</th>
<th>FCS</th>
</tr>
</thead>
</table>

**Standard 802.3 Ethernet Frame:**

4 Bytes

<table>
<thead>
<tr>
<th>Dst MAC</th>
<th>Src MAC</th>
<th>802.1q VLAN Tag</th>
<th>Type/Len</th>
<th>Data</th>
<th>FCS</th>
</tr>
</thead>
</table>

**802.3 Ethernet Frame Tagged with 4 Byte 802.1q header:**

4 Bytes 4 Bytes

<table>
<thead>
<tr>
<th>Dst MAC</th>
<th>Src MAC</th>
<th>802.1q VLAN Tag</th>
<th>802.1q VLAN Tag</th>
<th>Type/Len</th>
<th>Data</th>
<th>FCS</th>
</tr>
</thead>
</table>

**802.3 Ethernet Frame Tagged with multiple 4 Byte 802.1q headers – Q-in-Q:**
Double Tagging

VLAN 1 - Native VLAN
VLANs 2,3 - Access VLANs
Double Tagging

VLAN 1 - Native VLAN
VLANs 2,3 - Access VLANs
Double Tagging

- Consequences
  - Attacker can send packets to a target VLAN
  - Targeted system cannot respond back
    - Attacking system is on the native VLAN
    - Target is on an access VLAN isolated from the native VLAN broadcast domain
  - Not a good attack for eavesdropping
  - Excellent method for DoS attacks
  - Can be used as one way covert channels
Double Tagging

- Mitigation Techniques
  - Do not assign any hosts to VLAN 1 (*native VLAN*)
    - If necessary significantly limit access
    - Disable VLAN 1 on unnecessary ports
  - Change native VLAN on all trunk ports to something different than VLAN 1
  - Restrict access to switches by MAC address
    - Can spoof MAC addresses to get around this
  - Heart of this attack is having access to the native VLAN!
    - This is the default VLAN for all ports on a switch!
Outline

• Introduction
• Virtual LAN concepts
• Common Attack Methods
  • Overview of Attacks
  • Why They Are Effective
  • Mitigation Strategies
• Future Work in Virtualized Environments
  • Planned Attacks
  • Planned Test Scenarios
• Questions
Future Work

• What can be done in Virtualized environments?
• **Switch Spoofing**
  • Targets vulnerability in Cisco proprietary protocols
  • Would be useless on non-Cisco based vSwitches
  • Testing on Cisco Nexus 1000v switches is planned
• **Double Tagging**
  • Targets vulnerability in 802.1q standard
    • 802.1ad sub-standard
  • Could potentially work on any vSwitch
  • Attack requires two or more switches to be successful
  • Many scenarios can be explored
Future Work

- Scenarios:
  - Switch Spoofing
    - DTP/CDP spoofing attacks
      - Cisco Nexus 1000v switch (*advanced and essentials editions*)
        - VM → vSwitch (DTP) → VM (VLAN XX)
        - PC → Switch → vSwitch (DTP) → VM (VLAN XX)
        - VM → vSwitch (DTP) → Switch → PC (VLAN XX)
Future Work

• Scenarios (cont.):
  • Double Tagging (*requires at least 2 switches*)
    • PC → Switch → vSwitch → VM
    • VM → vSwitch → Switch → PC
    • VM → vSwitch → vSwitch → VM
      • Between different environments and vSwitches
    • VM → vSwitch → Switch → vSwitch → VM
      • Between different environments and vSwitches
Future Work

- Lab infrastructure upgrades and design changes are required to safely support test scenarios
  - Addition of multiple physical switches that support VLANs to lab and server rack (acquired!)
  - Direct 1Gb Ethernet connection from lab switch to server rack switch (waiting on approval)
    - Connections currently go through multiple campus switches
    - Requires facilities to install cabling between lab on 3rd floor and server room in basement.
- Isolation of lab network with router (locating hardware)
- Approval of VLAN ID usage from SUNY Poly ITS administrators (waiting on approval)
Future Work

- Infrastructure and design changes (cont.)
  - Addition of Cisco Nexus 1000v essentials & advanced vSwitches in VMWare environments
  - Two Servers (*locating hardware*)
  - Software license fees ~$5000.00 (*acquired funding*)
    - Academic VMWare vSphere Essentials (*purchased*)
    - Academic VMWare vCenter (*purchased*)
    - Cisco Nexus 1000v Advanced Edition (*purchased*)
  - DTP/CDP Switch spoofing scenarios
  - Configuration of VLAN IDs (*once approved*) on all physical and virtual switches
  - Allocation of new target virtual machines on each of the test VLANs
Outline

• Introduction
• Virtual LAN concepts
• Common Attack Methods
  • Overview of Attacks
  • Why They Are Effective
  • Mitigation Strategies
• Future Work in Virtualized Environments
  • Planned Attacks
  • Planned Test Scenarios
• Questions


References


References


References


References


References


References


• Open vSwitch. How to install open vswitch on linux, freebsd and netbsd. Retrieved December 4, 2013 from http://git.openvswitch.org/cgi-bin/gitweb.cgi?p=openvswitch;a= blob_plain;f=INSTALL;hb=HEAD/.
References


• Rouiller, S. VLAN Security: weaknesses and countermeasures - v1.4b. SANS Institute.


