vTunnel

Adam Welle

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA  15213
vTunnel

Allows a tunnel to be established one way:

- Guest side to host side
- Host side to guest side
Range Management Traffic

Relies on networked applications

Injects activity into exercise

Logs network and system activity

Scores student actions
vTunnel

Tunnels IP traffic between guest and host networks

Uses VSOCK to transmit data via hypervisor

Traffic is hidden from participants
vTunnel

Disadvantages of in-game management traffic

• Participants can be tipped off to injects
• Participants can block the traffic
• Participants can manipulate the traffic

Advantages of using vTunnel to hide management traffic

• Traffic in game stays on localhost
• Simplifies client configuration
vTunnel

Command and Control
• GHOSTS tasks
• Ansible configuration
• File copy

Allows system modifications
vTunnel

Logs
- Netflow records
- System logs
- GHOSTS results

Allows tracking of exercise performance
vTunnel

Student activity
• xAPI logs to LRS

xAPI
• Student activity
• Actor, Verb, Object

Learning Record Store
• Receives xAPI
• Multiple sources
WELLE-D
Wireless Emulation Link-Layer Exchange Daemon

Adam Welle
Wireless Security Training

Cyber security training relies heavily on virtualization.

But not for wireless training…

No native virtual wireless adapters.
Problems with Physical Devices

- Cost
- Time
- Security Policy
- Interference
Problems with Physical Devices
Advantages of Virtual Devices

- Cost effective
- Efficient
- Compliant
- Secure
- Scalable
- Repeatable training
- Enables distance education
Advantages of Virtual Devices
WELLE-D

Implementation
WELLE-D
Wireless Emulation Link-Layer Exchange Daemon

Leverages frames from mac80211_hwsim driver

Uses VSOCK to transfer frames

Simulates wireless medium

Provides GPS simulation

Enables high-fidelity use of full-featured operating systems

Open Source: https://github.com/cmu-sei/welled
Wireless Emulation Link-Layer Exchange Daemon

[user@Fedora-WLAN ~]$ iwconfig
lo       no wireless extensions.
virbr0    no wireless extensions.
wlan0     IEEE 802.11 ESSID:"OpenWrt"
          Mode:Managed Frequency:5.18 GHz Access Point: 00:0C:41:00:00:00
          Bit Rate=6.5 Mb/s   Tx-Power=20 dBm
          Retry short limit:7  RTS thr:off  Fragment thr:off
          Power Management:on
          Link Quality=47/70   Signal level=-63 dBm
          Rx invalid nwid:0   Rx invalid crypt:0   Rx invalid frag:0
          Tx excessive retries:0 Invalid misc:23 Missed beacon:0

virbr0-nic no wireless extensions.
WELLE-D
Wireless Emulation Link-Layer Exchange Daemon

Hosts
• Linux
• ESXi
• Windows

Linux Guests
• OpenWrt
• Fedora
• Android
• Ubuntu
WELLE-D
Implementation
Host Configuration
WMASTERD
Wireless Master Daemon

Receives frames from virtual machine nodes

Can calculate distance between nodes

Can produce GPS data as NMEA sentences

Enables simulation across multiple virtual machines

Isolates traffic from different users based on roomid
WELLE-D

Implementation

Guest Configuration
WELLED
Wireless Emulation Link-Layer Exchange Daemon

Receives frames from mac80211_hwsim,
transmits frames to wmasterd

Receives frames from wmasterd,
transmits frames to driver

Applies signal variations based on distance
GELLED
GPS Emulation Link-Layer Exchange Daemon

Receives NMEA from wmasterd, 
transmits NMEA to serial device

Allows GPSD to track location

Allows kismet to log network locations
GELLED-CTRL
GPS Emulation Link-Layer Exchange Daemon Control

Manipulates guest’s GPS feed

- Speed
- Course
- Climb
- Follow
- Latitude
- Longitude
- Altitude
GELLED-GUI
GPS Emulation Link-Layer Exchange Daemon GUI

Changes guest’s position
  Uses open street maps
  Executes gelled-ctrl

Enables war driving scenarios
Training Scenarios

Wireless Monitoring with kismet/kismon
Wardriving with kismet/gelled-gui
Eavesdropping
WPS attacks
WPA2 deauthentication
MiTM attacks with evil twin
Rogue APs
Krack attacks
Wireless surveys
WPA Enterprise
WELLE-D Training Lab Overview

Investigating WELLE-D Configuration
• wmasterd on host
• welled on Linux VMs

Performing a Wireless Attack
• Capture packets
• Perform deauthentication attack
• Perform dictionary attack
• Decrypt traffic

Wardriving Walt Disney World
• Run kismet and kismon
• Move VM using gelled-ctrl
Questions ?